A MITEL
PRODUCT
GUIDE

Unify OpenScape 4000

IP Solutions

Service Documentation
04/2025

A31003-H31A0-S100-51-7620

Mitel

Notices

The information contained in this document is believed to be accurate in all respects but is not warranted by Mitel Europe Limited. The information is subject to change without notice and should not be construed in any way as a commitment by Mitel or any of its affiliates or subsidiaries. Mitel and its affiliates and subsidiaries assume no responsibility for any errors or omissions in this document. Revisions of this document or new editions of it may be issued to incorporate such changes. No part of this document can be reproduced or transmitted in any form or by any means - electronic or mechanical - for any purpose without written permission from Mitel Networks Corporation.

Trademarks

The trademarks, service marks, logos, and graphics (collectively “Trademarks”) appearing on Mitel’s Internet sites or in its publications are registered and unregistered trademarks of Mitel Networks Corporation (MNC) or its subsidiaries (collectively “Mitel), Unify Software and Solutions GmbH & Co. KG or its affiliates (collectively “Unify”) or others. Use of the Trademarks is prohibited without the express consent from Mitel and/or Unify. Please contact our legal department at iplegal@mitel.com for additional information. For a list of the worldwide Mitel and Unify registered trademarks, please refer to the website: http://www.mitel.com/trademarks.

© Copyright 2025, Mitel Networks Corporation

All rights reserved

Contents

1 Goal of this Document 22

2 Gateways HG 3500 and HG 3575 23
2.1 Terms 23
2.1.1 Key Words 23
2.1.2 Fax or Modem Transmission and Detection 25
2.1.3 Codec Standards 26
2.1.4 Voice Quality 27
2.1.5 Jitter Buffer 30
2.1.5.1 Jitter Buffer Functionality 30
2.1.5.2 Jitter Buffer Modes 31
2.1.5.3 Considerations when Configuring the Delay for Static Jitter Buffer 32
2.1.5.4 Clock Drift with Static Jitter Buffer 33
2.1.5.5 Minimum Delay for Adaptive Jitter Buffer 35
2.1.5.6 Packet Loss Control in Adaptive Jitter Buffer 35
2.1.5.7 Parameters for Jitter Buffer Configuration 36
2.1.6 Runtime and Noticeable Effects 37
2.1.6.1 General Information on Delay 37
2.1.6.2 Delay and Echo 37
2.2 Architecture and System Requirements 38
2.2.1 Prerequisites 38
2.2.2 Power Requirements 38
2.2.3 Network Requirements 38
2.2.4 Network Data 39
2.2.4.1 TOS Byte 40
2.2.5 Bandwidth Requirements 45
2.2.5.1 Encoding 45
2.2.5.2 Sampling Time 45
2.2.5.3 IP Overhead 46
2.2.5.4 Required Bandwidth per Connection 46
2.2.5.5 Voice Activity Detection (VAD) 48
2.2.5.6 DMC Considerations 48
2.2.6 B Channels 49
2.2.6.1 B Channel Configuration 51
2.2.6.2 Displaying the B Channels currently Available/Configured (possible IP-Based Connections) 52
2.2.7 Traffic Considerations 53
2.3 Supported Gateways 53
2.3.1 HG 3500 (Common Gateway) 53
2.3.1.1 General Information 53
2.3.1.2 Board Replacement 54
2.3.1.3 Feature Capacities 55
2.3.1.4 Restrictions 58
2.3.2 HG 3575 58
2.3.2.1 General Information 59
2.3.2.2 Exchanging Boards 59
2.4 Features and Restrictions 60
2.4.1 Direct Media Connection (DMC) 60
2.4.2 Voice Compression 60
2.4.3 Voice Activity Detection (VAD) 61
2.4.4 Comfort Noise Generation (CNG) 62
2.4.5 Echo Cancellation 62

2.4.6 Redundant LAN Interface..... 63
2.4.7 Security.....63
2.4.7.1 Access for Administration..... 63
2.4.7.2 Access to SNMP.....63
2.4.7.3 Security in CorNetTC Registration..... 63
2.4.7.4 Connecting IP Gateways to the Internet or via External Providers..... 64
2.4.8 Resource Manager (RM)..... 64
2.4.9 Restrictions.....64
2.4.9.1 Loadware-Update or Reset of the Board..... 64
2.4.9.2 Possible IP hops.....65
2.5 Load Concept for Gateway Boards.....65
2.5.1 Important Information..... 65
2.5.2 Notes on IP Gateway Loadware.....65
2.5.3 Load Concepts..... 66
2.5.4 Updating Loadware with Web-Based Management.....67
2.5.5 Updating Loadware with "LW Update Manager"..... 68
2.5.6 General Comments on Loading.....69
2.6 Save Configuration Data in Local Flash (local Backup & Restore)..... 69
2.6.1 Overview.....69
2.6.2 Feature Description.....69
2.6.3 Startup Scenarios.....70
2.6.4 Configuration..... 71
2.6.5 Special Use Cases.....71
2.7 Loadability of the FPGA on the STMI4/NCUI4 board.....72
2.8 Standby Board HG 3500.....76
2.8.1 Feature Description.....76
2.8.2 User Interface.....80
2.8.3 Service Information..... 80
2.8.4 Generation.....83
2.8.5 Service steps after the automatic switch over.....86
2.8.6 Relevant AMOs..... 87
2.9 DLS Client Bootstrapping.....92
2.9.1 Bootstrapping with "No PIN" PIN Mode.....92
2.9.2 Bootstrapping with "Default PIN" or "Individual PIN" PIN Mode.....93
2.10 How to reset an NCUI board..... 93
2.10.1 Reasons for resetting the NCUI.....93
2.10.2 Methods for transferring Loadware.....93
2.10.3 Important Notes.....93
2.10.4 Process.....94
2.11 How to reset an STMIX board..... 97
2.11.1 General description..... 97
2.11.2 Preparing the necessary files.....98
2.11.3 Tool configuration for flashing..... 99
2.11.4 STMIX USB configuration..... 104
2.11.5 STMIX re-flash.....106
2.11.6 STMIX and STMIY Factory reset.....112
2.12 Gateway HG 3575 - Changing Parameters with AMO STMIB..... 113
2.12.1 TYPE GLOBAL - Changing the Idle Bit Pattern..... 114
2.12.2 TYPE IFDATA - Changing the Interface-Specific Parameters of the Access Point.....114
2.12.3 TYPE SERVIF - Changing the Login and Password for Service Access..... 116
2.12.4 TYPE ASC - Changing the Payload QoS Setting of the Access Point.....117
2.12.5 TYPE ASC - Setting the Codec List for DMC Connections, RTP Packet Size, Voice Activity Detection and T.38 Fax..... 118
2.12.6 TYP ASC - Transmission of DTMF/Fax/Modem Tones..... 119
2.12.7 TYPE DSP - Jitter Buffer Size of the Access Point.....119
2.12.8 TYPE DMCDATA - Changing the Access Point Setting to Support Direct Media Connections.....119

2.12.9 TYPE H323 - Changing the H323 Settings at the Access Point..... 120
2.12.10 TYPE JB - Configuring the Jitter Buffer.....121
2.12.11 TYPE SIGQOS - Quality Monitoring for the Signaling Connection over IP.....121
2.12.12 TYPE SNMP - Changing the Community Strings for Read Access..... 121
2.12.13 TYPE MGNTDATA - Management Data and Backup Server..... 124
2.12.14 TYPE WBMDATA - Changing the Login and Password for WBM.....124
2.12.15 TYPE GWSECTOR - Changing the Access Point Sector Number for the Resource Manager.....125
2.12.16 TYPE DLSDATA - Configuring DLS Data.....125
2.12.17 Resetting the Parameters to Default Values.....125
2.13 General Information on How to Configure a HG 3500 Common Gateway.....126
2.13.1 Changing the common gateway configuration.....126
2.13.2 AMOs.....127
2.13.3 Rules.....127
2.13.4 Restrictions.....129
2.13.5 Overview of Configuration Steps..... 129
2.14 Gateway HG 3500 - Changing Parameters with AMO CGWB..... 129
2.14.1 TYPE ASC - Changing the Payload QoS Setting in Host System..... 129
2.14.2 TYPE ASC - Setting the Codec List for DMC Connections, RTP Packet Size, and Voice Activity Detection.....130
2.14.3 TYP ASC - Transmission of DTMF/Fax/Modem Tones.....130
2.14.4 TYPE DMCDATA - Changing the HG 3500 Setting to Support Direct Media Connections.....131
2.14.5 TYPE DSP - Changing the DSP (Signal Processor) Setting at an HG 3500.....132
2.14.6 TYPE GLOBIF - Changing the Idle Bit Pattern and Interface-Specific Parameters.....132
2.14.7 TYPE GWSECTOR - Changing the HG 3500 Sector Number for the Resource Manager.....133
2.14.8 TYP MGNTDATA - Connection to the OpenScape 4000 Assistant.....133
2.14.9 TYPE SERVIF - Changing the Login and Password for the Service Access..... 134
2.14.10 TYPE WBMDATA - Changing the Login and Password for WBM.....134
2.14.11 TYPE JB - Configuring the Jitter Buffer.....135
2.14.12 Resetting the Parameters to Default Values.....136
2.15 Codec Settings..... 136
2.15.1 HFA and Trunking..... 136
2.15.2 IPDA..... 137
2.16 Multiple Feature Support Configuration at the Common Gateway (Example)..... 138
2.16.1 Important Information / Restrictions..... 138
2.16.2 Configuring Functional Blocks with the AMO BFDAT.....138
2.16.3 Configuring the Common Gateway Board with the AMO BCSU..... 141
2.16.4 Configuring SIP Trunking..... 144
2.16.5 Completed and Uncompleted Functional Block.....144
2.16.5.1 Uncompleted functional block.....144
2.16.5.2 Completed configuration block..... 145
2.17 Resource Manager Functionality.....146
2.17.1 General.....146
2.17.2 Key Terms..... 147
2.17.2.1 Sector.....147
2.17.2.2 Cluster.....147
2.17.2.3 Sector Path..... 148
2.17.2.4 Definitions.....148
2.17.3 Configuration Rules.....150
2.17.4 Used Bandwidth..... 150
2.17.5 Configuring the Resource Management for a HFA Configuration..... 151
2.17.5.1 Basic Situation..... 151
2.17.5.2 Codec Settings for the HFA Subscribers.....152
2.17.5.3 Sectors for the LAN/WAN.....152
2.17.5.4 Allocation of the Gateways and Subscribers.....153
2.17.5.5 Define Sector Paths.....156
2.17.5.6 Assign the sector paths.....156

2.17.6 Configuring the Resource Management for an IPDA Configuration with TDM Phones..... 160
2.17.6.1 Basic Situation..... 160
2.17.6.2 Sectors for the LAN/WAN..... 161
2.17.6.3 Sectors for the Gateways..... 161
2.17.6.4 Allocation of the Gateways to their Sectors..... 162
2.17.6.5 Define Sector Paths..... 162
2.17.6.6 Assign the Sector Path..... 162
2.17.7 Configuring the Resource Management for an IPDA Configuration with TDM Phones and HFA in Access Point..... 165
2.17.7.1 Basic Situation..... 166
2.17.7.2 Settings for the HFA Subscribers..... 167
2.17.7.3 Sectors for the LAN/WAN..... 168
2.17.7.4 Sectors for the Gateways..... 168
2.17.7.5 Assignment of the HFA Subscribers to the Sectors..... 169
2.17.7.6 Allocation of the Gateways to their Sectors..... 169
2.17.7.7 Define Sector Paths..... 169
2.17.7.8 Assign the Sector Path..... 169
2.17.8 Notes and Restrictions..... 171
2.17.9 Diagnostics..... 172
2.18 Command Line Interface CLI in HG 3500..... 172
2.18.1 General Information..... 172
2.18.2 General Operations..... 173
2.18.3 Access control..... 173
2.18.4 Gateway Setup..... 174
2.18.5 Image/File Handling..... 174
2.18.6 Maintenance..... 174
2.18.7 SSL for WBM..... 176
2.18.8 DLS..... 176
2.18.9 Changing the Login and Password for WBM/CLI..... 178
2.19 Command Line Interface CLI at HG 3575 V4..... 178
2.20 SNMP Support HG 3500 / HG 3575..... 178
2.21 IP Ports..... 242
2.21.1 General Information..... 242
2.21.2 Port Range..... 242
2.21.2.1 IP Trunking + DMC (IP Trunking and IPDA) Master Connections..... 242
2.21.2.2 IPDA (HG 3575/HG 3500) + DMC (HG 3575) master connections..... 242
2.21.3 Information for Network Administrators..... 243
2.21.4 Examples..... 243
2.21.4.1 Payload..... 243
2.21.4.2 Signaling..... 244
2.21.4.3 SNMP..... 245
2.21.4.4 Diagnostics..... 246
2.22 WBMs of the Boards..... 246
2.23 HG 3500 / HG 3575 Diagnostic Options..... 246
2.24 Gateways HG 3500 and HG 3575 - Changing Gateway UI MODE..... 247
2.25 Frequently asked Questions..... 248

3 OpenScape 4000 SoftGate..... 253
3.1 Overview..... 253
3.1.1 Functional Overview..... 253
3.1.2 Variants..... 253
3.1.3 Features..... 254
3.1.4 LAN Interfaces..... 256
3.1.5 Ports..... 257
3.1.6 Advantages..... 257
3.1.7 Restrictions..... 258

3.1.8 Hints for Diagnosis regarding the peripheral Slots....259
3.1.9 Hardware Requirements....259
3.2 OpenScape 4000 SoftGate Upgrade....259
3.2.1 Upgrade via Assistant Gateway Manager....259
3.2.2 Upgrade via the Local WBM in OpenScape 4000 SoftGate....261
3.3 Mediatrix Gateways....263
3.3.1 Released Mediatrix Gateways....263
3.3.2 Configuration Notes....263
3.3.3 Configuration Examples....263
3.3.3.1 ISDN (S0) Subscriber (Mediatrix 44xx)....264
3.3.3.2 S0 Trunking (Mediatrix 44xx)....270
3.3.3.3 ISDN (S0) Data Connections (Mediatrix 44xx)....279
3.3.3.4 S2 Interface (Mediatrix 36xx)....286
3.3.3.5 Analog Stations (Mediatrix 41xx)....296
3.3.3.6 Analog Trunking (Mediatrix 1204)....303
3.3.4 Error Detection with Syslog for Mediatrix 44xx and 36xx....314
3.4 Video Connections....317
3.4.1 Restrictions....317
3.4.2 Scenarios....318
3.4.3 Features....318
3.4.4 Configuration....318
3.5 Music on Hold (MOH) - OpenScape 4000 SoftGate as Music on Hold or Announcement Source Provider....318
3.5.1 Feature Description....318
3.5.2 Service Information....319
3.5.3 Generation (Example)....321
3.5.4 Relevant AMOs....322
3.6 Gatekeeper Redundancy for HFA/ SIP Subscriber....322
3.6.1 Feature Description....323
3.6.1.1 Solution concept....323
3.6.1.2 Switchover....323
3.6.1.3 Prerequisites for switching over....324
3.6.1.4 Switchover process....324
3.6.1.5 Gatekeeper Redundancy with APE....329
3.6.2 Service Information....330
3.6.3 Generation (Example)....331
3.6.4 Relevant AMOs....339
3.7 Survivable OpenScape 4000 SoftGate....340
3.7.1 Feature Description....340
3.7.2 Service Information....342
3.7.3 Generation (example)....342
3.8 IPv6....342
3.8.1 Feature Description....343
3.8.2 Service Information....343
3.8.3 Generation (Example)....343
3.8.3.1 Important Note....343
3.8.3.2 IPv6 Networking Connectivity for OpenScape 4000 SoftGate (Trunking)....343
3.8.3.3 IPv6 Internal Connectivity....350
3.8.3.4 NGS Backup and Restore....352
3.8.4 Relevant AMOs....354
3.9 Load Balancing....355
3.9.1 Feature Description....355
3.9.2 Service Information....355
3.9.3 Generation (Example)....356
3.9.3.1 SIP Load Balancer Properties....356
3.9.3.2 Outgoing/Incoming Calls via SIP Load Balancing Server....357

3.9.3.3 Registration of Gateways....358
3.9.3.4 Registration of UC Media Server Farm....360
3.10 Secure Remote Subscriber....361
3.10.1 Feature Description....362
3.10.1.1 SoftGate Server Side Destination NAT (DNAT) Option....362
3.10.2 Service Information....363
3.10.2.1 Requirements....363
3.10.2.2 General....364
3.10.2.3 Restrictions....366
3.10.2.4 DMZ....366
3.10.3 Generation (Example)....370
3.10.3.1 Secure Remote Subscriber on STMIX/STMIY....376
3.10.3.2 Deployment Service (DLS) and DLS Contact-Me Proxy (DCMP) - Tips & Tricks....377
3.11 Picture CLIP....382
3.11.1 Feature Description....382
3.11.2 Service Information....383
3.11.3 Generation (Example)....384
3.11.3.1 OpenScape 4000 SoftGate configuration....384
3.11.3.2 Phone Configuration....385
3.11.3.3 LDAP directory server configuration....388
3.11.3.4 Testing LDAP access....390
3.12 MFC-R2....391
3.12.1 Feature Description....391
3.12.2 Service Information....392
3.12.3 Generation (Example)....392
3.13 OpenScape Cordless E Integration....393
3.13.1 Feature Description....393
3.13.2 Service Information....396
3.13.3 Generation (Example)....396
3.14 WBMs of the Boards....397
3.15 Centralized IP for HFA....397
3.15.1 WBM GUI enhancements....399

4 LAN Connectivity (LAN Separation / LAN Redundancy)....402
4.1 Separate LAN Connectivity for Administration and VoIP....402
4.1.1 Feature Description....402
4.1.2 Service Information....402
4.1.3 Generation (Example)....403
4.1.3.1 Configuration for Common Gateway (HG 3500/ HG 3575), STMIX and STMIY....403
4.1.3.2 Configuration for OpenScape 4000 SoftGate or Enterprise Gateway....403
4.1.4 Relevant AMOs....405
4.2 Separate LAN Interfaces for HFA and SIP....406
4.2.1 Feature Description....406
4.2.2 Generation (Example)....406
4.3 LAN Redundancy....408
4.3.1 Feature Description....408
4.3.2 Redundant LAN Interfaces (Bonding)....408
4.3.2.1 Feature Description....409
4.3.2.2 Generation (Example)....409

5 OpenScape Access and OpenScape Branch....411

6 OpenScape Enterprise Gateway....412

7 Large Enterprise Gatekeeper (LEGK)....413
7.1 General Information....413
7.1.1 Overview....413

7.1.2 Gatekeeper Function....413
7.1.2.1 General Information....413
7.1.2.2 Key words....414
7.1.3 Gatekeeper Restrictions....414
7.2 Guidelines for Installing an IP Feature....414
7.3 Configuring the Feature....415
7.3.1 Important Information....415
7.3.2 Sequence of Generation....415
7.3.3 Activating the Large Enterprise Gatekeeper....416
7.3.4 Configuring the FLEXAMA Memory in the Database....418
7.3.4.1 Number of Internal and External Gateways....418
7.3.4.2 Number of Internal HG 3500 Gateways in a System....418
7.3.4.3 Number of LCR Digit Patterns for Digit Pattern Pools 1 through 8....419
7.3.4.4 Number of Cache Elements for Cache Pools 1 through 8....420
7.3.5 Configuring a HG 3500 on the LAN Segment....421
7.3.5.1 Configuring the HG 3500 Gateway....421
7.3.6 Configuring the HG 3500 Directory Number....437
7.3.7 Configuring IP Trunking in the LCR....439
7.3.8 Configuring Circuits and Terminals....443
7.3.8.1 Configuring Circuits....444
7.3.8.2 Configuring Terminals....444
7.3.9 Changing the System Bandwidths....444

8 HiPath Feature Access (HFA)....447
8.1 Overview....447
8.2 Application Example....447
8.2.1 Feature Description....448
8.2.1.1 Technical background....449
8.2.1.2 HFA user registration....449
8.2.2 User interface....451
8.2.3 Restrictions....452
8.2.4 Generation....452
8.2.4.1 Configuration of the HG 3500 board....452
8.2.4.2 Configuration of the HFA users....453
8.2.5 Generation via OpenScape 4000 Assistant....453
8.2.5.1 Setting up HG 3500 via the OpenScape 4000 Assistant....453
8.2.5.2 Configure a HFA User via the OpenScape 4000 Assistant....457
8.2.6 Deletion....458
8.2.7 Tuning the voice quality....458
8.2.8 Activation of the voice compression....459
8.2.9 Relevant AMOs....460
8.3 Frequently Asked Questions....466

9 Mobile HFA Logon....469
9.1 Feature Description....469
9.1.1 Mobility Session....469
9.1.2 Shared Desk Area....471
9.2 User Interface....473
9.2.1 Activation/Deactivation via DAR....473
9.2.1.1 HFA Logon....473
9.2.1.2 HFA Logoff....474
9.2.2 Activation via menu....474
9.2.3 Activation with AMO ACTDA....474
9.3 Prerequisites....474
9.4 Service Information....475
9.4.1 Mobile HFA in Connection with other Features....475

9.4.1.1 OpenStage terminal in combination with an optiClient....476
9.4.1.2 Malicious Call Identification at visited switch....477
9.4.1.3 Signaling and Payload Encryption (SPE)....477
9.4.2 Restriction....477
9.4.3 Language Support....477
9.4.4 Logon Sequences....478
9.5 Generation....478
9.5.1 Example 1: Two HFA subscribers in the same Host....478
9.5.2 Example 2: Two HFA subscriber at different systems....479
9.5.3 Relevant AMOs....481

10 IP Distributed Architecture (IPDA)....489
10.1 IPDA Feature Description....489
10.1.1 Scalable Increase in System Capacity....491
10.1.2 Distributed Circuit Switching....491
10.1.3 Time Synchronization....491
10.1.4 Call Scenarios....492
10.1.4.1 Internal Access Point Call....492
10.1.4.2 Call Between Two Access Points....493
10.1.4.3 Call Between an Access Point and the Central System....494
10.1.4.4 Trunk Access / Networking....495
10.1.5 Survivability for Signaling and Payload....495
10.1.5.1 Signaling Survivability....496
10.1.5.2 Payload Survivability....496
10.1.6 Signaling and Payload Separation (SPS)....497
10.1.6.1 Feature Description....497
10.1.6.2 Prerequisites....497
10.1.6.3 Configuration....498
10.1.7 Redundant LAN Interface....498
10.1.8 LAN Monitoring....498
10.1.8.1 Feature Description....498
10.1.8.2 Service Information....499
10.1.8.3 Generation (Example)....500
10.1.8.4 Relevant AMOs....500
10.1.9 Different Time Zones (DTZ)....500
10.1.10 A-Law/µ-Law Conversion in AP Shelf....501
10.1.11 Different Announcements, Tones and MFV DialTone Receivers per Access Point....501
10.1.12 Different Display Languages per Access Point....501
10.1.13 Additional Features....501
10.2 Configuring the IPDA Feature....502
10.2.1 OpenScape 4000 LAN Segment....503
10.2.2 Access Point....524
10.2.2.1 Configuring a “Networked” Access Point....525
10.2.2.2 Configuring a “Direct Link“ Access Point....535
10.2.2.3 Changing Access Point Parameters with the AMO STMIB....545
10.2.2.4 Deleting an Access Point....545
10.2.2.5 Local Configuration of an Access Point....548
10.2.2.6 Reference Clock in Access Point....551
10.2.2.7 Loading new Loadware on a HG 3575....551
10.2.2.8 Updating Access Point Loadware during an RMX Upgrade (New Fix Release/Minor Release)....553
10.2.2.9 Information on Exchanging HG 3575 Boards....554
10.2.2.10 Information on the 19“ AP 3500 IP Access Point....555
10.2.2.11 Information on the 19“ AP 3700 IP Access Point....556
10.2.3 HG 3500 as HG3570 in the OpenScape 4000 System....557
10.2.4 Subscriber, CO/Tie Trunk Circuits in Access Points....562

10.2.5 Special Routes ... 569
10.2.5.1 Special Routes Between Access Points ... 570
10.2.5.2 Special Routes between Access Point and OpenScape 4000 LAN Segment ... 573
10.2.6 Signaling Survivability ... 581
10.2.7 Quality Monitoring for the Signaling Connection over IP ... 581
10.2.7.1 Restriction of the Available Signaling Bandwidth (Traffic Shaping) ... 582
10.2.7.2 Monitoring the Runtime for Signaling Messages (Round Trip Delay) ... 584
10.2.7.3 Monitoring Message Throughput ... 586
10.2.7.4 Advanced Criteria for Signaling Survivability ... 587
10.2.7.5 Output of Statistical Information on the Signaling Connection ... 588
10.2.7.6 Error Messages from Quality Monitoring for the Signaling Connection over IP ... 588
10.2.8 Source Dependent Routing ... 591
10.2.9 Payload Survivability ... 596
10.2.9.1 When is Payload Survivability Used? ... 596
10.2.9.2 How is Payload Survivability Configured? ... 599
10.2.9.3 Payload Survivability in OpenScape 4000 Networks ... 607
10.2.9.4 Restrictions ... 609
10.2.10 Signaling and Payload Separation (SPS) ... 609
10.2.10.1 General Restrictions and Limitations ... 610
10.2.10.2 Effects on Features with SPS ... 611
10.2.10.3 Configuration ... 615
10.2.11 Divert Call in Survivability Mode to another Access Point ... 615
10.2.11.1 Prerequisites ... 616
10.2.11.2 User Scenarios ... 616
10.2.11.3 Use Cases ... 618
10.2.11.4 Generation ... 622
10.2.12 External Music on Hold ... 622
10.2.13 Information on CMI ... 626
10.2.14 IP Address Changes ... 626
10.2.14.1 Change of Address in a Network Segment to which Access Points are Connected ... 626
10.2.14.2 Changing the Address of the Survivability Network ... 628
10.2.14.3 Changes in the OpenScape 4000 LAN Segment ... 629
10.2.15 A-Law/µ-Law Conversion in AP Shelf ... 634
10.2.15.1 Feature Description ... 634
10.2.15.2 Service Information ... 634
10.2.15.3 Generation (Example) ... 635
10.2.16 Different Announcements, Tones and DTMF DialTone Receivers per Access Point ... 635
10.2.16.1 Feature Description ... 635
10.2.16.2 Service Information ... 636
10.2.16.3 Generation Example ... 637
10.2.16.4 Relevant AMOs ... 638
10.2.17 Different Languages/National Character Sets for Displaying Text for Individual Access Points ... 640
10.2.17.1 Feature Description ... 641
10.2.17.2 Service Information ... 641
10.2.17.3 Generation (Example) ... 643
10.2.17.4 Relevant AMOs ... 644
10.3 Load Calculation ... 645
10.3.1 Load Calculation for Access Points ... 647
10.3.2 Load Calculation for a HG 3500 ... 654
10.3.3 Calculation Basis - Configuring Payload Packets ... 660
10.3.3.1 MTU Packet ... 660
10.3.3.2 Configuring Ethernet MAC Frames ... 662
10.3.3.3 Configuring IP Frames ... 663
10.4 Local Access Point Administration at CLI via Terminal ... 663
10.4.1 Networked access point ... 664
10.4.2 Direct link access point ... 666

10.4.3 Assignment of parameter names in LW-CLI to the AMO parameters..... 668
10.5 Spreadsheets - IPDA Configuration..... 669
10.6 Information for network administrators..... 678
10.6.1 Central Processor..... 678
10.6.2 HG 3500 Voice Gateway..... 679
10.6.3 Access Points with HG 3575..... 680
10.6.4 Redundant LAN Interface..... 682
10.7 IPDA Wizard..... 683
10.7.1 Functions..... 684
10.8 FAQs - Frequently Asked Questions..... 686

11 Access Point Emergency (APE)..... 694
11.1 Access Point Emergency Feature Description..... 694
11.1.1 Access Point Emergency Implementation Scenarios..... 694
11.1.1.1 LAN Scenario..... 694
11.1.1.2 LAN/WAN Scenario..... 695
11.1.1.3 Branch (WAN) Scenario..... 696
11.1.2 Access Point Emergency and Signaling Survivability..... 697
11.1.3 Survivability Unit in AP 3700 IP..... 698
11.1.4 Survivability unit on OpenScape 4000 SoftGate..... 698
11.1.5 Allocating Access Points/OpenScape 4000 SoftGates to a Survivability Unit..... 698
11.1.6 Switchover in Emergency Mode..... 699
11.1.7 Reverting to Normal Operation..... 700
11.1.8 Configuration Data..... 700
11.1.9 Transferring new System Releases and Patches..... 701
11.1.10 Connection Between Subsystems (Islands)..... 701
11.1.11 Time Synchronization..... 702
11.1.12 Feature Licensing..... 702
11.1.13 Application Support in Emergency Mode..... 703
11.2 Configuring the APE Feature (Access Point Emergency)..... 703
11.2.1 Configuring or Modifying a CC-AP/Survivable OpenScape 4000 SoftGate in OpenScape 4000..... 704
11.2.2 Deleting a CC-AP/Survivable OpenScape 4000 SoftGate in OpenScape 4000..... 706
11.2.3 Configuring or Modifying an Emergency Group..... 707
11.2.4 Deleting an Emergency Group..... 711
11.2.5 Configuring Access Points/OpenScape 4000 SoftGates for AP Emergency..... 712
11.2.6 Examples for Determination of Weights..... 714
11.2.7 Removing Access Points/OpenScape 4000 SoftGates from the AP Emergency Configuration..... 716
11.2.8 Deleting the entire AP Emergency Configuration..... 717
11.2.9 Configuring the Display for AP Emergency on the Terminal..... 717
11.2.10 Defining the Switchover Delay..... 718
11.2.11 Querying the Connection Data..... 720
11.2.11.1 Querying the Connection Data via Configuration Management..... 720
11.2.11.2 Querying the Connection Data via AMO..... 720
11.2.12 Administration Switchover of Access Points/OpenScape 4000 SoftGates..... 722
11.2.12.1 Administration Switchover of Access Points/OpenScape 4000 SoftGates via Configuration Management..... 723
11.2.12.2 Administrator Switchover of Access Points/OpenScape 4000 SoftGates via AMO..... 723
11.2.13 Time Synchronization Between the Host System and CC-AP/Survivable OpenScape 4000 SoftGate..... 726
11.2.14 Initial Startup of the CC-AP/Survivable OpenScape 4000 SoftGate..... 726
11.2.14.1 Preparation..... 726
11.2.14.2 C-AP..... 726
11.2.14.3 Survivable OpenScape 4000 SoftGate..... 727
11.2.15 Verification and Acceptance of the AP Emergency Configuration..... 727
11.3 Backup & Restore..... 727
11.3.1 OpenScape 4000 Assistant Backup & Restore on OpenScape 4000 Host System..... 727

11.3.1.1 Configuring an AP Backup Server with OpenScape 4000 Assistant Backup & Restore....728
11.3.1.2 Creating a Schedule for the Backup....730
11.3.1.3 Performing the First Backup....732
11.3.1.4 Using OpenScape 4000 Assistant Backup & Restore for more extensive Changes in the System....732
11.3.1.5 Checking the Regular Activities of OpenScape 4000 Assistant Backup & Restore....733
11.3.2 OpenScape 4000 Assistant Backup & Restore Configuration on the CC-AP/Survivable OpenScape 4000 SoftGate....734
11.3.2.1 Configuring the AP Backup Server on the CC-AP/Survivable OpenScape 4000 SoftGate....734
11.3.2.2 Configuring a Routine Configuration Data Backup to Hard Disk....735
11.4 Service Scenarios....736
11.4.1 Upgrading the AP Emergency Server (New Fix Release/Minor Release)....736
11.4.2 Replacing the DSCXL2 in the AP Emergency Server....737
11.5 Spreadsheets - APE Configuration....737
11.6 Information for network administrators....739
11.6.1 Survivability Unit for AP Emergency....739
11.7 Quick Guide to Setting up an AP Emergency (IPDA)....741
11.7.1 Introduction....741
11.7.2 Requirement....742
11.7.3 Configuration Steps in OpenScape 4000....743
11.7.4 Configuration Steps in the CC-AP....748
11.7.5 Verification and Acceptance of the AP Emergency Configuration....753
11.8 FAQs - Frequently Asked Questions....753

12 Different Time Zones (DTZ)....756
12.1 Feature Description....756
12.2 Service Information....757
12.3 Generation Example....757
12.3.1 Configuring the Time Classes....759
12.3.2 Assigning the Time Classes to an AP Shelf....760
12.3.3 Assigning the Time Classes to an HFA Station....761
12.3.4 Deleting a Time Class....761
12.3.5 Deleting the Daylight Savings Time Changeover....762
12.3.6 Changing the System Date/Time with AMO DATE....763
12.4 Relevant AMOs....763

13 Signaling Survivability....766
13.1 Feature Description....766
13.1.1 How is the Fault Detected?....767
13.1.2 What is Used as an Alternative Route for Signaling?....769
13.1.2.1 Signaling Survivability via PSTN Network....770
13.1.2.2 Signaling Survivability via Alternate LAN....771
13.1.3 HSR via UDP....772
13.2 Service Information....773
13.3 Generation (Example)....775
13.3.1 Signaling Survivability via PSTN Network....775
13.3.1.1 Configuring the OpenScape 4000....775
13.3.1.2 Configuring the Modem....778
13.3.1.3 Configuring the Router....779
13.3.2 Signaling Survivability via alternate LAN....788
13.3.2.1 Configuring the OpenScape 4000....789
13.3.2.2 Configuring the LAN Interface....790
13.3.2.3 Configuring the Router....791
13.3.2.4 Replacement of a defect NCUI Board with a new NCUI Board....791
13.3.3 Is Signaling Survivability Currently Active? (DIS-UCSU)....792
13.4 Relevant AMOs....795

14 SIP Connectivity 798
14.1 Overview 798
14.1.1 Interfaces 798
14.1.1.1 SIP Subscriber 798
14.1.1.2 UFIP Devices 798
14.1.1.3 SIP Trunking 798
14.1.2 Supported RFCs (Request for Comments) for SIP Interfaces 798
14.1.3 Boards Used 803
14.1.4 Gateway Port Configuration 803
14.2 SIP Subscriber 803
14.2.1 SIP Endpoints 804
14.2.2 Service Information 804
14.2.3 Features 805
14.2.4 Restrictions 810
14.2.4.1 Restrictions of System Features 810
14.2.4.2 Restrictions of Terminal Features 810
14.2.4.3 General restrictions 811
14.2.5 Configuration 811
14.2.5.1 STMI2/4 and STMIX/STMIY Board Configuration 812
14.2.5.2 Configuring a SIP Subscriber 812
14.2.5.3 Removing a SIP Subscriber 813
14.2.5.4 Changing a SIP Subscriber 813
14.2.5.5 Enabling/Disabling DMC 813
14.2.5.6 SIP Session Timer 814
14.2.5.7 Subscriber Parameters 815
14.2.5.8 Message Waiting Indication (MWI) 815
14.2.5.9 SIP Subscriber as DSS Key on a Desktop Phone 816
14.2.5.10 SIP Peer Filtering 817
14.2.5.11 Call Forwarding 817
14.2.5.12 Display of the SIP Subscribers 818
14.2.5.13 Busy override, emergency intrusion and emergency disconnect for SIP (UFIP) subscribers 818
14.2.5.14 UFIP in Pickup Group 819
14.2.5.15 Relevant AMOs 821
14.3 SIP Trunking 826
14.3.1 SIP-Q Trunking 826
14.3.1.1 Features 826
14.3.1.2 Restrictions 828
14.3.1.3 Configuration 829
14.3.2 Native SIP Trunking 829
14.3.2.1 Features 829
14.3.2.2 Restrictions 830
14.3.2.3 Use Cases 831
14.3.2.4 Configuration 832
14.3.3 SIP Trunk Profiles 833
14.3.3.1 General Information 834
14.3.3.2 Default Profiles 834
14.3.3.3 Activating the SIP Trunk Profiles 835
14.3.3.4 "SIP Trunk Profiles" menu 836
14.3.3.5 Configuration of SIP Trunks with Registration 839
14.4 Built-in SBC 844
14.4.1 General SBC specifications (Source Wikipedia) 844
14.4.2 Built-in SBC Function 845
14.5 Configuration of SIP Service Provider / SIP Carrier 847
14.5.1 Motivation 848
14.5.2 Configuration Basics 848

14.5.2.1 Configuration....848
14.5.2.2 Notes....849
14.5.3 Scenario 1: Gateway direct to SIP Carrier....849
14.5.3.1 Initial Situation....849
14.5.3.2 AMO Configuration....850
14.5.3.3 Gateway Configuration in WBM....853
14.5.4 Scenario 2: Gateway via Session Border Controller to SIP Carrier....854
14.5.4.1 Initial Situation....854
14.5.4.2 AMO Configuration....856
14.5.4.3 HG 3500 Configuration in WBM....856
14.5.4.4 Configuration in the Session Border Controller....857
14.5.4.5 SG vHG direct connectivity (USEWANIF)....857
14.5.5 SIP Provider Telekom Deutschland GmbH....858
14.5.5.1 Service Information....858
14.5.5.2 Restrictions....859
14.5.5.3 Configuration....860
14.5.5.4 Connection Examples....864
14.5.5.5 Configuration Example OpenScape SBC....866
14.5.5.6 Configuration Example OpenScape SBC (CompanyFlex)....881
14.5.5.7 FAQ....884
14.5.6 Near-end NAT support for SG vHG boards....885
14.5.6.1 AMO-CGWB configurations....885
14.5.7 SIP trunks with near-end destination NAT (STMIX/STMIY)....886
14.5.7.1 Important Information....886
14.5.7.2 Configuration options....887
14.5.8 Multisite emergency calls via centralized SIP trunk....888
14.5.9 Emergency Calls....888
14.6 Configuration of SIP-Q-Trunking / Native SIP Trunking....889
14.6.1 Configuration using AMOs....889
14.6.1.1 Trunking Protocol....890
14.6.1.2 Configuring a HG 3500 as a Local Gateway....890
14.6.1.3 Backup & Restore of the WBM Configuration Data....897
14.6.1.4 Displaying Link Status....898
14.6.1.5 Procedure for Adding Supplementary HG 3500 Boards to the Network....898
14.6.1.6 Relevant AMOs....898
14.6.2 Configuration with OpenScape 4000 Assistant....900
14.6.2.1 Configure Common Gateway HG 3500....901
14.6.2.2 Delete IPGW....903
14.6.2.3 Modify Board Data of IPGW....903
14.6.3 Configuration using SIP Trunk Profiles in WBM....904
14.6.4 SIP-Q Trunking between OpenScape 4000 and OpenScape Voice....904
14.6.4.1 Restrictions....904
14.6.4.2 OpenScape 4000 Configuration....904
14.6.4.3 OpenScape Voice Configuration....907
14.6.5 Number management between OpenScape 4000 and OpenScape Voice for Italy....909
14.7 Configuration Guide for OpenScape 4000 / OpenScape Voice Networking....910
14.7.1 General....911
14.7.2 Introduction and Overview....911
14.7.3 Requirements and Released Combinations....911
14.7.4 Configuration on OpenScape 4000....912
14.7.4.1 Settings for STMI2/STMI4/STMIX/STMIY....912
14.7.5 Configuration on OpenScape Voice....931
14.7.5.1 OpenScape Voice Endpoint Profile....931
14.7.5.2 OpenScape Voice Endpoint....932
14.7.5.3 Set IP-Address for OpenScape 4000 to trusted in case of Digest Authentication....936
14.7.6 DNS-SRV for HG 3500....937

14.7.6.1 Example of Web-GUI for Geo-Separated OpenScape Voice with TLS Configuration..... 938
14.7.6.2 Branch Example with Geo-Separated OpenScape Voice and TLS..... 939
14.7.7 Signaling and Payload Encryption (SPE)..... 940
14.7.8 OpenScape Voice Route to OpenScape 4000..... 949
14.7.9 OpenScape Voice Routing for International Dialing - Extend Dialed Numbers to International Number..... 951
14.7.9.1 For 5 or 6 Digit Extension Dialing..... 952
14.7.9.2 Dialing with Local Code..... 953
14.7.9.3 Dialing with Local Code (Closed Numbering)..... 954
14.7.9.4 Dialing with National Code..... 955
14.7.9.5 Dialing with National Code (Closed Numbering)..... 956
14.7.9.6 Dialing with International Code..... 957
14.7.9.7 Dialing with International Code (Closed Numbering)..... 958
14.7.9.8 Change Type of Number to “International”..... 959
14.7.9.9 Match International Number for “HOME DN”..... 960
14.7.9.10 Configuration of Default Route if Number did not Match in “HOME DN”..... 961
14.7.9.11 Complete International Number Selection for single external Destination Number..... 962
14.7.10 OpenScape Voice Loop detection..... 963
14.7.11 Restrictions..... 963
14.8 Interworking with Microsoft Lync Communication Server 2010/2013..... 964
14.8.1 Important Information..... 964
14.8.2 Feature Description..... 964
14.8.3 Realization..... 965
14.8.4 Service Information..... 965
14.8.4.1 Restrictions..... 965
14.8.4.2 Available Features..... 966
14.8.5 Configuration Example..... 968
14.8.5.1 OpenScape 4000..... 968
14.8.5.2 Microsoft Lync Server/Mediation Server..... 970
14.9 Skype for Business..... 976
14.9.1 Feature Overview..... 976
14.9.1.1 Features available (Overview):..... 976
14.9.1.2 Feature detailed description..... 976
14.9.2 Restrictions..... 979
14.9.3 Specific configuration..... 979
14.9.3.1 OpenScape 4000 routing..... 979
14.9.3.2 vHG 3500 WBM configuration..... 980
14.9.3.3 Configure Skype for Business Server 2015..... 981
14.9.3.4 Adding OpenScape 4000 vSTMI as a gateway to the Skype for Business Server 2015 Topology..... 981
14.9.3.5 Define Dial Plan..... 986
14.9.3.6 Create Voice Policy..... 986
14.9.3.7 Define Trunk Configuration..... 988
14.10 MS Teams DR with Audio Codes SBC..... 989
14.10.1 Feature Overview..... 989
14.10.1.1 Features available (Overview):..... 990
14.10.2 Restrictions and Hints..... 990
14.10.3 Configuration..... 990
14.11 MS Teams Direct Routing with OpenScape SBC..... 991
14.11.1 Network Topology..... 991
14.11.2 OpenScape 4000 Configuration..... 991
14.11.2.1 AMO Configuration..... 991
14.11.2.2 STMIX/STMIY/vHG WBM configuration..... 992
14.11.3 OpenScape SBC Configuration..... 994
14.11.3.1 Core Realm Interface..... 994
14.11.3.2 SIP Server..... 994

14.11.3.3 Certificates....997
14.11.3.4 Teams Media Profile....999
14.11.3.5 OpenScape 4000 Media Profile....1000
14.11.3.6 General Media Settings....1001
14.11.3.7 Remote Endpoints....1002
14.11.4 MS Teams Direct Routing Configuration....1008
14.11.5 Features Available (Overview)....1009
14.11.6 General Restrictions and Limitations....1009
14.12 SIP URI Dialing....1009
14.12.1 Video Dial Out....1010
14.12.1.1 Call Routing of external alphanumeric SIP URIs....1011
14.12.1.2 SIP URI dialing via CSTA interface....1011
14.12.1.3 SIP-Q Support....1011
14.12.2 Video Dial In....1011
14.12.2.1 Call Processing - Invites from OS-SBC (Internet)....1012
14.12.2.2 URI Mapping Service....1012
14.12.3 SIP URI format for video dial out....1013
14.12.4 Configuration....1013

15 OpenScape Mobile Pro Client....1015
15.1 Overview....1015
15.1.1 General Restrictions and Limitations....1017
15.1.1.1 OSMO Pro Combined Mode Restrictions....1018
15.1.1.2 Notes for SIP device as OpenScape Mobile Pro Client Deskphone....1018
15.1.2 Configuration....1019
15.1.3 Configuration Example....1020
15.1.3.1 Configuration on OpenScape 4000....1021
15.1.3.2 CICA Connectivity to OS4K....1025
15.1.3.3 OpenScape Mobile Pro Client Configuration....1025
15.1.3.4 OpenScape SBC Configuration Example....1026
15.1.3.5 Facade and UC configuration....1038

16 Unify Phone Connectivity....1039
16.1 Overview....1039
16.1.1 Features....1039
16.1.2 Architecture....1040
16.2 Feature interaction and restrictions....1040
16.3 Configuration....1042
16.3.1 Connector configuration....1042
16.3.1.1 **Configure Unify Phone Telephony Connector**....1042
16.3.1.2 Configure OpenScape 4000....1042
16.3.1.3 Configure OpenScape SBC....1046
16.3.2 User configuration....1049
16.3.2.1 Configure Unify Video....1049
16.3.2.2 Configure OpenScape 4000....1050
16.3.3 Mass migration from Circuit....1052

17 H323 / H323 Annex Connectivity....1054
17.1 Overview....1054
17.2 DTMF Outband Signaling....1054
17.3 Configuration Example....1055
17.3.1 Configuration using AMOs....1055
17.3.1.1 Trunking Protocol....1055
17.3.1.2 Configuring a HG 3500 as a Local Gateway....1055
17.3.1.3 Backup & Restore of the WBM Configuration Data....1061
17.3.1.4 Displaying Link Status....1062
17.3.1.5 Procedure for Adding Supplementary HG 3500 Boards to the Network....1062

17.3.1.6 Relevant AMOs....1062
17.3.2 Configuration with OpenScape 4000 Assistant....1063
17.3.2.1 Configure Common Gateway HG 3500....1063
17.3.2.2 Delete IPGW....1065
17.3.2.3 Modify Board Data of IPGW....1065

18 Signaling and Payload Encryption (SPE)....1067
18.1 Feature Description....1067
18.1.1 Encrypted Signaling and Payload Connections....1067
18.1.2 Scenarios - Overview....1067
18.1.3 Solution Concepts....1068
18.1.3.1 PKI (Public Key Infrastructure)....1068
18.1.3.2 Signaling encryption....1069
18.1.3.3 TLS Version....1070
18.1.3.4 Certificate Verification Level....1071
18.1.3.5 Minimum Length of RSA Keys....1073
18.1.3.6 ECDSA certificates....1073
18.1.3.7 Maximum Re-Keying Interval....1074
18.1.3.8 Enforce Secure Renegotiation (RFC 5746)....1074
18.1.3.9 Voice Encryption....1074
18.1.4 MIKEY (Multimedia Internet KEYing)....1075
18.1.4.1 MIKEY Option 0....1076
18.1.4.2 MIKEY Option 1....1076
18.1.5 Session Description (SDES) Protocol....1076
18.1.6 Master Encryption Key (MEK)....1076
18.1.7 Secure SIP Connections....1077
18.1.7.1 SIP-Q Trunking....1078
18.1.7.2 Native SIP trunking....1078
18.1.7.3 SIP Subscriber....1079
18.2 Service Information....1079
18.2.1 Restrictions....1079
18.2.2 Generation of a Certificate....1080
18.2.3 Supported Certificates....1080
18.2.4 Renew a Certificate....1081
18.2.5 Board Replacement....1081
18.2.6 STMI Board....1081
18.2.7 Activating/Deactivating SPE for Subfunctions in the System....1081
18.2.8 Connecting Gateway....1082
18.2.9 SPE in Connection with Mobile HFA....1082
18.2.9.1 Terminology used....1082
18.2.9.2 Prerequisite....1083
18.2.9.3 Scenarios with Homogenous HiPath 4000/OpenScape 4000 Network with SPE Enabled....1083
18.2.9.4 Scenarios within a Network with SPE activated Nodes and SPE deactivated Nodes....1084
18.2.9.5 Network Wide Usage of Mobile HFA....1086
18.3 Configuration....1086
18.3.1 Prerequisites....1087
18.3.2 Activation / Deactivation of SPE for Gateways with AMO CGWB....1087
18.3.3 Trunk SPE Activation / Deactivation....1089
18.3.3.1 SPE for Analog / TDM Trunks....1089
18.3.3.2 SPE for IP Trunking....1090
18.3.3.3 Deactivation of SPE for SIP-Q / Native SIP Trunking....1096
18.3.4 Subscriber SPE Activation / Deactivation....1096
18.3.4.1 SPE for Analog/TDM Endpoints....1096
18.3.4.2 SPE for IP Subscribers....1097
18.3.4.3 Configuration....1097
18.3.4.4 Signaling at the Display....1101

18.3.4.5 Deactivating SPE for Subscribers..... 1103
18.3.5 Activation / Deactivation of SPE for Access Points..... 1103
18.3.5.1 New Access Point in an Active SPE System..... 1105
18.3.5.2 Deactivating SPE for Access Points with Soft Restart..... 1106
18.3.6 OpenScape 4000 SoftGate SPE Activation / Deactivation..... 1107
18.3.6.1 Features..... 1107
18.3.6.2 Restrictions..... 1107
18.3.6.3 Configuration..... 1108
18.4 Generation SPE Certificates with OpenScape 4000 Assistant..... 1109
18.4.1 SPE Root Certificate..... 1109
18.4.1.1 Open the SPE Root Certificate Dialog..... 1110
18.4.1.2 Creating a New Root Certificate..... 1110
18.4.1.3 Displaying/Downloading the newly Created SPE Root Certificate..... 1112
18.4.2 SPE Certificate..... 1112
18.4.2.1 Open the SPE Certificate Dialog..... 1112
18.4.2.2 Creating a new SPE Certificate..... 1113
18.4.2.3 Displaying/Downloading the newly created SPE Certificate..... 1115
18.5 Distribution of Certificates with the WBM of the Gateway..... 1116
18.5.1 Importing SPE CA Certificate on a Gateway..... 1116
18.5.2 Importing a SPE Certificate on a Gateway..... 1117
18.5.3 Importing a SPE Certificate on a vHG3500 HFA..... 1117
18.5.4 Certificates and Security on vHFA and WAN Interfaces..... 1117
18.6 Distribution of Certificates using Deployment Service (DLS)..... 1118
18.6.1 Distribution of Certificates to Gateways..... 1118
18.6.1.1 Creating a Virtual IP Device..... 1118
18.6.1.2 Scanning the IP Devices (IP Gateways)..... 1123
18.6.1.3 Distribution of the SPE CA Certificate..... 1127
18.6.1.4 Distribution of the SPE Certificate..... 1131
18.6.1.5 Resetting Bootstrapping..... 1136
18.6.2 Distribution of Certificates to Subscribers..... 1137
18.6.2.1 Distribution of a CA Certificate..... 1137
18.6.2.2 Scanning the IP Devices..... 1139
18.7 AutoSPE Configuration (DLS)..... 1142
18.7.1 OpenScape 4000..... 1143
18.7.2 Deployment Service (DLS)..... 1143
18.7.2.1 DLS Time Server..... 1143
18.7.2.2 Preparing DLS..... 1144
18.7.3 Device Configuration..... 1145
18.7.3.1 Preparations..... 1145
18.7.3.2 Time Server..... 1146
18.7.4 Automatic Certificate Creation..... 1146
18.7.5 Activate Voice Encryption..... 1147
18.7.6 Check Certificates..... 1148
18.7.7 Display of SPE Status..... 1148
18.7.8 Adding new Gateways after AutoSPE Activation..... 1148
18.8 MTLS Implementation on CGW and SG..... 1149
18.8.1 System Setting..... 1150
18.8.2 Enabling Enforce Secure TLS Renegotiation (RFC 5746)..... 1150
18.8.3 Device Setting..... 1150
18.8.3.1 OpenStage Phones..... 1150
18.8.3.2 OpenScape Desk Phones..... 1151
18.8.4 DLS Device Setting..... 1151
18.8.4.1 Protocol Setting..... 1151
18.8.4.2 Certificate Upload..... 1151
18.8.4.3 CA Certificate Upload..... 1153
18.8.5 HFA Implementation..... 1155

18.8.5.1 CGW....1155
18.8.5.2 SoftGate....1159
18.8.6 UFA IP Implementation....1162
18.8.6.1 CGW and Softgate....1162

19 Payload Switching DMC....1166
19.1 Feature Description....1166
19.2 Direct Media Connect (DMC) in Connection with HFA Subscriber....1166
19.2.1 Feature Description....1166
19.2.1.1 Motivation....1166
19.2.1.2 Notes concerning Direct Media Connections DMC....1167
19.2.1.3 Bandwidth Considerations....1167
19.2.1.4 Scenarios....1169
19.2.1.5 Domain concept....1172
19.2.1.6 DMC Interworking to HiPath 3000....1173
19.2.2 Service Information....1175
19.2.2.1 Features with DMC....1175
19.2.2.2 Feature activation while DMC is active....1176
19.2.3 Generation....1176
19.2.3.1 DMC Authorization....1176
19.2.3.2 Maximum number of DMC connections on IP boards....1177
19.2.3.3 Voice Activity Detection (VAD)....1177
19.2.3.4 Domains....1177
19.2.3.5 H.323 stack on IPDA boards....1178
19.2.3.6 Troubleshooting Hints....1178
19.2.4 Relevant AMOs....1179
19.3 Direct Media Connect (DMC) in Connection with SIP Subscriber....1181
19.3.1 Feature Description....1181
19.3.2 Restriction....1184
19.3.3 Scenarios....1184
19.3.3.1 SIP Subscriber at same OpenScape 4000....1184
19.3.3.2 SIP Subscriber at another OpenScape 4000....1184
19.3.3.3 SIP Subscriber at OpenScpae Voice....1185
19.3.3.4 SIP Subscriber at HiPath 3000....1186
19.3.3.5 HFA Subscriber at same OpenScape 4000....1186
19.3.3.6 HFA Subscriber at another OpenScape 4000....1186
19.3.3.7 HFA Subscriber at HiPath 3000....1188
19.3.3.8 TDM Subscriber/Network behind a Remote Shelf of a OpenScape 4000....1189
19.3.3.9 TDM Subscriber/Network at another OpenScape 4000 behind a Remote Shelf....1189
19.3.3.10 TDM Subscriber/Network at another OpenScape 4000....1190
19.3.3.11 TDM Subscriber at HiPath 3000....1192
19.4 Direct Media Connect (DMC) in Connection with OpenScape 4000 SoftGate....1192

20 T.38 Fax....1201
20.1 Definition....1201
20.2 Feature Description....1201
20.2.1 Important Notes....1201
20.2.2 Restrictions....1201
20.2.2.1 Delay problems in scenario with 2 and more IP-hops and certain fax machines....1201
20.2.2.2 DMC problem with AP1120....1202
20.2.2.3 DMC not established with MTX41xx....1202
20.2.2.4 Parameter “USE Previous Media Negotiation” has to be set....1203
20.2.3 Common Gateway....1204
20.2.4 OpenScape 4000 SoftGate/STMIX/STMIY....1204
20.2.5 IPDA....1204
20.3 Scenarios....1205

20.4 Service Information....1207
20.4.1 OpenScape 4000 SoftGate/STMIX/STMIY....1208
20.4.2 IPDA (NCUI/STMI)....1208
20.5 Generation (Example)....1208
20.6 Relevant AMOs....1209

21 IP Terminals....1211
21.1 Supported IP Terminals....1211
21.2 Boards....1211
21.3 optiPoint IP Terminals....1211
21.3.1 General Information....1212
21.3.2 optiPoint 410/420....1212
21.3.2.1 Terminal Types....1212
21.3.2.2 Adapters and key modules....1213
21.3.2.3 Modules for optiPoint Telephones....1214
21.3.2.4 Key Layout on optiPoint Telephones....1214
21.3.3 OpenStage WL3/WL4....1214
21.3.4 More Adapters and Ports....1215
21.3.4.1 OpenStage Busy Lamp Field....1215
21.3.4.2 optiPoint Recorder Adapter....1216
21.3.4.3 optiPoint Acoustic Adapter Data....1217
21.3.4.4 Microphone and Loudspeaker Port....1217
21.3.4.5 Headset Port....1218
21.3.4.6 Contact Port....1219
21.4 OpenStage IP Terminals....1219
21.4.1 Hardware and General Features....1219
21.4.2 Key Assignment....1220
21.4.3 Key Modules....1220
21.4.4 OpenStage Terminal in Connection with optiClient....1220
21.4.5 Busy Lamp Field....1221
21.5 OpenScape Desk Phone IP 35G/55G HFA....1222
21.5.1 Hardware and General Features....1222
21.5.2 Key Assignment....1222
21.5.3 Key Modules....1222
21.6 OpenScape Desk Phone CP HFA....1223
21.6.1 Hardware and General Features....1223
21.6.2 Key Assignment....1223
21.6.3 Key Modules....1223
21.7 Service Information....1224
21.8 IP Terminal Generation....1224
21.8.1 HFA (IP) Terminal at STMI....1224
21.8.2 PC after HFA (IP) Terminal....1226
21.8.3 HFA (IP) Terminal and USB for Simple Dialer....1227
21.8.4 OpenStage WL3/WL4 Configuration....1227
21.8.5 OpenStage Configuration....1229
21.8.6 OpenScape Desk Phone IP Configuration....1232
21.8.7 Desk Phones CP Configuration....1232
21.9 Deletion at the IP Port....1238
21.9.1 Deleting All Devices Assigned a Station Number at the IP Port....1238
21.9.2 Deleting Non-Voice Services at the IP Port....1239
21.9.3 Deleting the IP Telephone's Key Module....1239
21.9.4 Deleting the IP Telephone's Buy Lamp Field....1239
21.9.5 Deleting IP Telephone Adapters....1239

Index....1244

1 Goal of this Document

This document aims to provide an overview of the HG 3500 and HG 3575 gateways. Only the basic board configuration is described. Detailed information on specific functions such as IP Distributed Architecture and Access Point Emergency (IPDA & APE), HiPath Feature Access (HFA), Large Enterprise Gatekeeper, etc. are provided in the corresponding sections.

2 Gateways HG 3500 and HG 3575

2.1 Terms

2.1.1 Key Words

In order to prevent confusion, a number of key terms which are used frequently within the text are defined here in more detail.

<table>
<tr><td>Nodes:</td><td>Designates a device with a port/connection in a network.
This can be a router, a CGW module or any computer. Also frequently referred to as “Host“.</td></tr>
<tr><td>LAN segment:</td><td>Part of a network in which all nodes communicate with each other directly on Layer 2 (Ethernet MAC). The nodes are thus switched on the same “shared“ medium and interconnected via hubs or Layer 2 switches. In other words, they communicate without routers (Layer 3). The communication with nodes beyond this segment has to be realized via routers.</td></tr>
<tr><td>IP address:</td><td>A numerical Internet address comprising 4 sets of digits, e.g. 172.16.222.45. In this context, the term always designates the individual, complete and unequivocal address of a node.</td></tr>
<tr><td>Network mask (Netmask):</td><td>Internet addresses are broken down into network-specific and node-specific sections. The size of these sections differs, depending on the class of the address (determined by the first digit of the address).
<table>
<tr><td>Byte</td><td>1</td><td>2</td><td>3</td><td>4</td><td></td></tr>
<tr><td>Class</td><td></td><td></td><td></td><td></td><td></td></tr>
<tr><td>A</td><td>Network [1 .. 126]</td><td>Node</td><td>Node</td><td>Node</td><td></td></tr>
<tr><td>B</td><td>Network [128 .. 191]</td><td>Network</td><td>Node</td><td>Node</td><td></td></tr>
<tr><td>C</td><td>Network [192 .. 223]</td><td>Network</td><td>Network</td><td>Node</td><td></td></tr>
</table>
The netmask allows subnets to be generated within a network. Specific bits of the node section are used for the purposes of addressing. The network mask specifies which parts of the IP address are to be regarded as network/subnet sections by means of the specified bits. The remaining digits (bits not specified in the mask) designate the node section.</td></tr>
</table>

Network address:	In this document, the term network address is used for the entire network **and** subnet part of the IP address. The network address is yielded by a bit-by-bit AND operation of any IP address with the netmask.		
VLAN tagging	According to IEEE 802.1 p/q, there are two functions which are controlled using a common tag: the **priority** and the **VLAN ID**. The term VLAN tagging is generally applied once the tag is used - regardless of what it is being used for. The same applies in the case of IPDA. When reference is made to deactivating or activating VLAN tagging (AMOs SIPCO or CGWB: VLAN), it is the tag that is meant, not the VLAN function. According to the standard there are three types of frames:		
	• Untagged	Normal Ethernet frames without tagging	
	• Priority Tagged	Ethernet frames with tagging The priority bits are used The VLAN ID is 0.	
	• VLAN Tagged	Ethernet frames with tagging The priority bits are 0, The VLAN ID is > 0.	
	Some IP equipment vendors only allow priority bits to be used when VLAN ID > 0 is set. When tagging is being used, the IPDA components always use priority tagging, but allow a setting of VLAN ID > 0 The priority bits are fixed according to the traffic type. The values are specified in Table 3, “TOS values”		
TOS byte	The **T**ype **O**f **S**ervice byte is a component of the header for all IP packets in accordance with RFC 791. According to RFC 791 (*Internet Protocol*), the byte is split up as follows (most significant -> least significant bit)		
	3 bits for precedence 111 - Network Control 110 - Internetwork Control 101 - CRITIC/ECP 100 - Flash Override 011 - Flash 010 - Immediate 001 - Priority 000 - Routine	3 bits for priority D-T-R **Slight delay**: 0 = Normal, 1 = Low **Throughput**: 0 = Normal, 1 = High **Reliability**: 0 = Normal, 1 = High	2 bits reserved for future use

	According to RFC 2474 (*Differentiated Services*), the six high-order bits are used as DiffServ Code Point (DSCP), while the two least significant bits are reserved.
	Some of the values to be set are specified as 6-bit values without the 2 reserved bits, and others as 8-bit values (with the 2 reserved bits = 0). With IPDA, the entire TOS byte is always specified. The two least significant bits are always set to zero. A pure DiffServ Code Point must therefore be moved 2 bits to the left or multiplied by 4 in order to obtain the TOS byte setting for IPDA.

Table 1: Example: Class B IP address, netmask and network address

IP address			
172	16	222	45
1 0 1 0 1 1 0 0	0 0 0 1 0 0 0 0	1 1 0 1 1 1 1 0	0 0 1 0 1 1 0 1
Netmask			
255	255	240	0
1 1 1 1 1 1 1 1	1 1 1 1 1 1 1 1	1 1 1 1 0 0 0 0	0 0 0 0 0 0 0 0
Subnet		1 1 0 1	
Network address			
172	16	208	0
1 0 1 0 1 1 0 0	0 0 0 1 0 0 0 0	1 1 0 1 0 0 0 0	0 0 0 0 0 0 0 0

2.1.2 Fax or Modem Transmission and Detection

The “FMoIP“ (Fax/Modem over IP) feature is used for the transmission of fax and modem signals over the IP network.

The FMoIP feature provides the following functionality:

- DMC (Direct Media Connect) for fax/modem calls. This results in a maximum of one IP hop (2 IP/TDM conversions) for fax/modem connections within a local HiPath 4000/OpenScape 4000 network. DMC is supported for HG 3500 / HG 3575. This is the major improvement in comparison with the last version, where a switch back to master call was performed after tone detection.
- The DMC endpoints HG 3500 and HG 3575 support G.711 F/M.
- T.38

IMPORTANT: When connecting a fax adapter to a HG 3500 (SIP subscriber), DMC must be deactivated for this device (only then is T.38 transmission possible). If you want nonetheless to

connect DMC for this device, the codec must be set to G.711 (fax transmission with G.711, not T.38).

IMPORTANT: T.38 configuration/usage requires end-to-end DMC between OpenScape 4000 gateways (minimized IP hops) because of timing requirements according to T.38 standard. In case of multiple IP hops the fax transmission could fail with some fax machines. Negative list of affected fax machines can be found in the Release Notes.

IMPORTANT: In earlier versions only four T.38 connections were possible per DSP. From HiPath 4000 V6 R2 this limitation is removed and up to 60 T.38 parallel calls are supported and possible on STMI boards and 120 on vSTMI boards.

---

1) For more information on which scenarios are supported please refer to document “T.38 Fax”, Chapter 2, “Feature Description”.

- RFC2833 and RFC2198 for fax/modem tones are supported for HG 3500/75 to transfer the fax/modem signals over IP.
- Enhanced DSP tone detection (incl. tone information transfer based on RFC2833/RFC2198) for HG 3500/75 boards. Supported tones:
  - call initiation tones CNG and CT (calling side)
  - call answer tones ANS(CED), /ANS, ANSam, /ANSam (called side)

Restrictions

- When DMC is not able to reduce the number of IP hops for a connection to one IP hop, there will still be a certain risk of broken fax or modem connections because of the resulting delay, even though a G.711 channel optimized for analog data is chosen.
- Fax/Modem call: only supports basic call, no support for supplementary services initiated on basis of an existing connection, such as consultation call. Support of basic call includes forwarded calls (CFU).
- Due to the variety of the available modem and fax types on the market, there is no guarantee that all FMoIP scenarios will work with 100% reliability. The different behaviors of the modem and fax types (e.g. tolerance) and the typical IP conditions (jitter, delay etc.) can result in failed FMoIP scenarios.
- Clear Channel has to be disabled via AMO configuration because there is no RFC2833/RFC2198 tone detection for Clear Channel. Each fax/modem call should be configured as a regular voice call (G.711, G.729, ...).

2.1.3 Codec Standards

To transmit an analog voice signal over digital paths, it must be converted to a digital signal (and then back again). There are different methods for implementing this codec, each of which offer different levels of voice quality and requires different amounts of bandwidth.

Detailed information on the codec classmarks is provided in Table 14, “Classmark handling for codec type” in the document "IP Distributed Architecture (IPA) and Access Point Emergency (APE)".

2.1.4 Voice Quality

For the transmission of voice over IP networks, there are three other factors that influence the subjective voice quality experienced by the customer:

- **Delay**
- Occurs in the packetization of voice data (see Figure 1 Packet-by-packet voice transmission) and in the transmission of packets. Compression codecs (e.g. G.729) require processing time. In order to compensate for fluctuations in the packet runtime (jitter), a buffer is inserted on the receiver side (jitter buffer). The size of the jitter buffer also influences the overall delay.
- **Packet loss**
- Packets can sometimes be lost during transmission in IP networks. Fill data must then be inserted on the receive side in place of the required packet data.
- **Jitter**
- Fluctuation of the packet runtime above or below a mean value, see Figure 2 Jitter: variation of the transmission delay. The jitter buffer must intercept these fluctuations. The packet earmarked for use is lost if the deviation from

mean value is so great that it can no longer be intercepted by the jitter buffer. The effect is the same as for packet loss in the network.

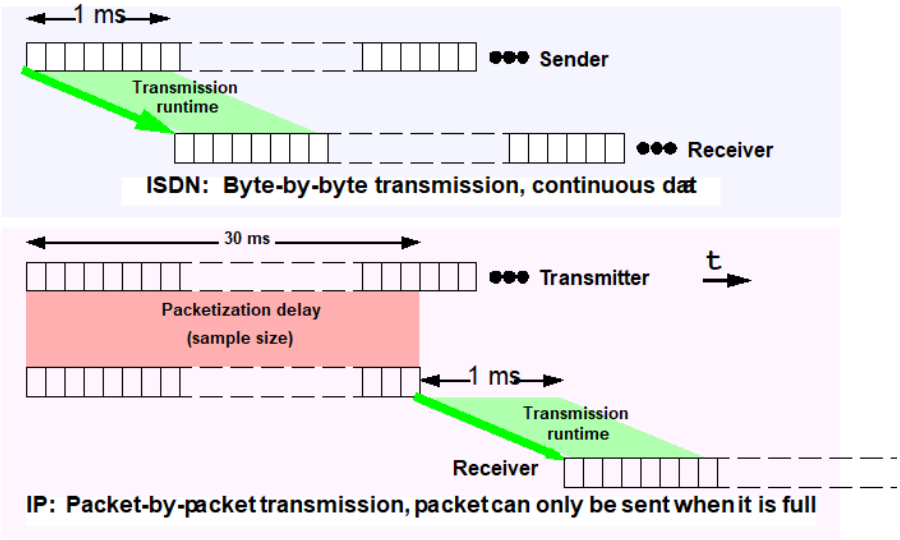


Figure 1: Packet-by-packet voice transmission

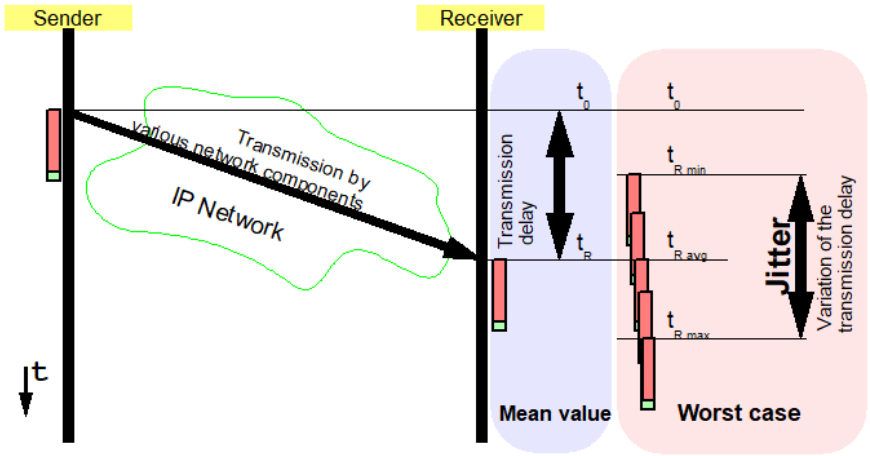


Figure 2: Jitter: variation of the transmission delay

The effectiveness of both parameters also depends on the sample size (how many milliseconds of voice per packet) and on the codec type.

Figure 3 Voice quality depending on delay illustrates an evaluation of voice quality depending on delay.

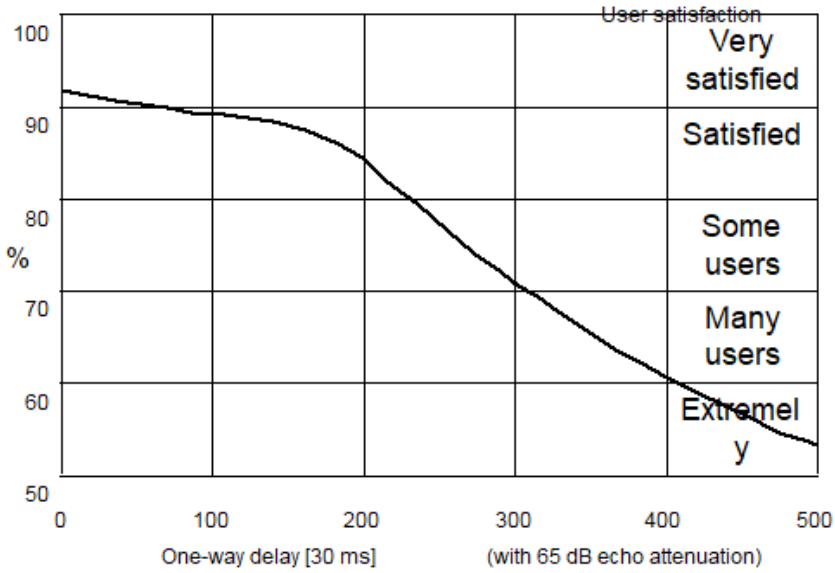


Figure 3: Voice quality depending on delay

Table 2, “Voice quality depending on delay and packet loss rate” illustrates an evaluation of voice quality depending on delay and packet loss rate.

Table 2: Voice quality depending on delay and packet loss rate

Scale of acceptance							
Value	Acceptance						
0 - 5	Very good						
6 - 10	Good						
11 - 19	Satisfactory						
20 or more	Unsatisfactory						
Delay [ms]	Packet loss rate in %						
	< 1%	1%	1.5%	2%	2.5%	3%	> 3%
50	0	4	6	8	10	12	30
100	0	4	6	8	10	12	30
150	0	4	6	8	10	12	30
200	3	7	9	11	13	15	33
250	10	14	16	18	20	22	40
300	15	19	21	23	25	27	45

350	20	24	26	28	30	32	50
400	25	29	31	33	35	37	55

For all solutions over IP, i.e. including OpenScape 4000, configurations with multiple IP-TDM (or TDM-IP) conversions in a connection should be avoided, as each conversion creates a delay. This is because of the potential losses in voice quality where the number of delays is too high. Every module in the HG 3500 family (and HG 3575 in the access point) as well as every terminal device distributed directly via HFA has a IP-TDM conversion. The maximum number of IP-TDM conversions should (not including HFA terminal devices) be no higher than two.

2.1.5 Jitter Buffer

2.1.5.1 Jitter Buffer Functionality

Transfer packets can arrive with different delays in TCP/IP-based networks. Because these delays cause interruptions, packets entering the data stream must be verified. The jitter buffer provides temporary storage for IP packets. It can balance out IP packet delays to a certain degree.

IP packets enter the jitter buffer in the order in which they arrive. Each packet contains a time stamp, which is stored in the RTP header of the packet. The actual order is determined using the packet time stamps. The jitter buffer ensures that packets leave in the right order and in sync. An average time (average delay) defines how long packets, which arrive at the expected time, are held in the jitter buffer. Packets which arrive later than expected are held for a shorter period in the jitter buffer; packets which arrive earlier than expected are held longer. If a packet arrives so late that it can no longer be assigned, it is lost. In theory, packets can also arrive so early that they cannot be assigned. This is, however, rarely the case in practice.

Figure 4 Jitter buffer functionality illustrates the jitter buffer functionality.

If one or two packets are lost during voice transmission, this is not an immediate problem. However, the delay should be as short as possible, as delays which are too long compromise voice quality when making calls.

To ensure data integrity, the number of packets lost during data transfer should be kept to a minimum. Delays, on the other hand, do not play a major role here.

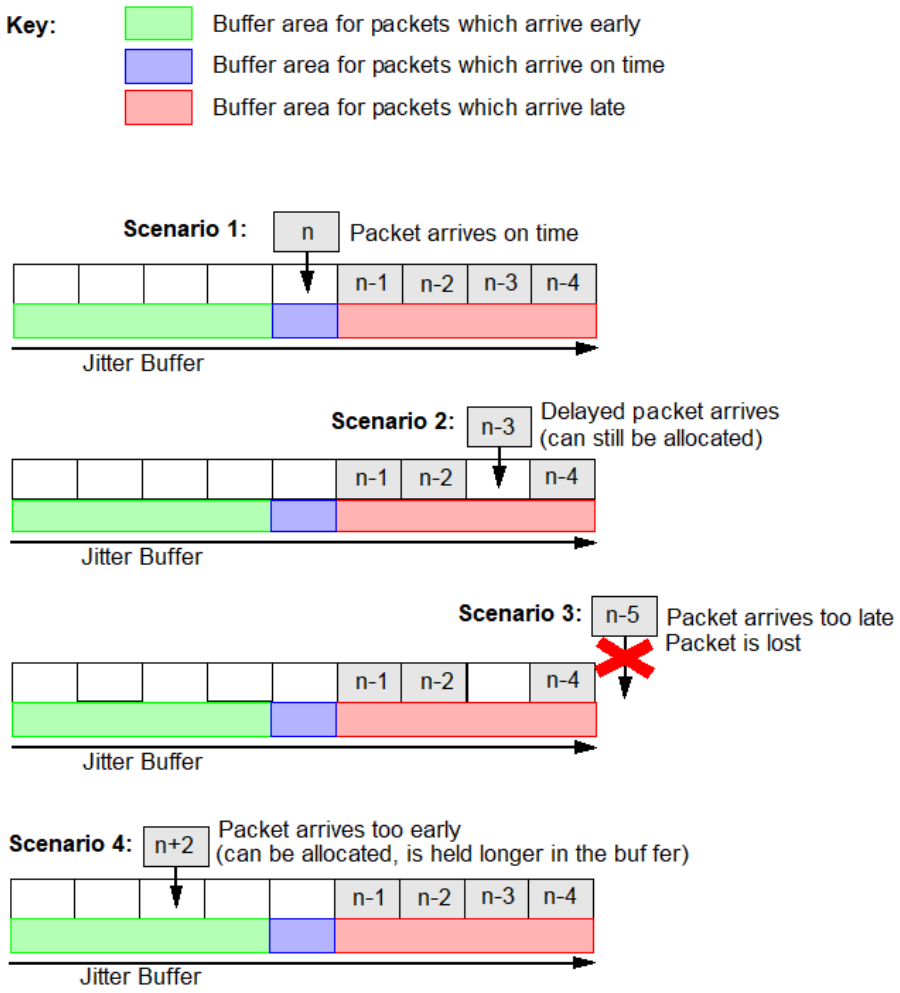


Figure 4: Jitter buffer functionality

2.1.5.2 Jitter Buffer Modes

The jitter buffer of the gateways HG 3500/3575 can be operated in two different modes, depending on the connection:

- **Static** jitter buffer
- **adaptive** (dynamic) jitter buffer

The adaptive jitter buffer is designed specifically for voice transmission. While the average packet delay remains constant in static mode, it automatically adapts to the situation in adaptive mode. Figure 5 Difference between static and adaptive jitter buffer illustrates the difference between static and adaptive jitter buffers in a situation where several packets with longer delays arrive.

In the adaptive jitter buffer, the average delay is simply the start value for the average delay. This is automatically adjusted to the respective receive ratios during operation (green line).

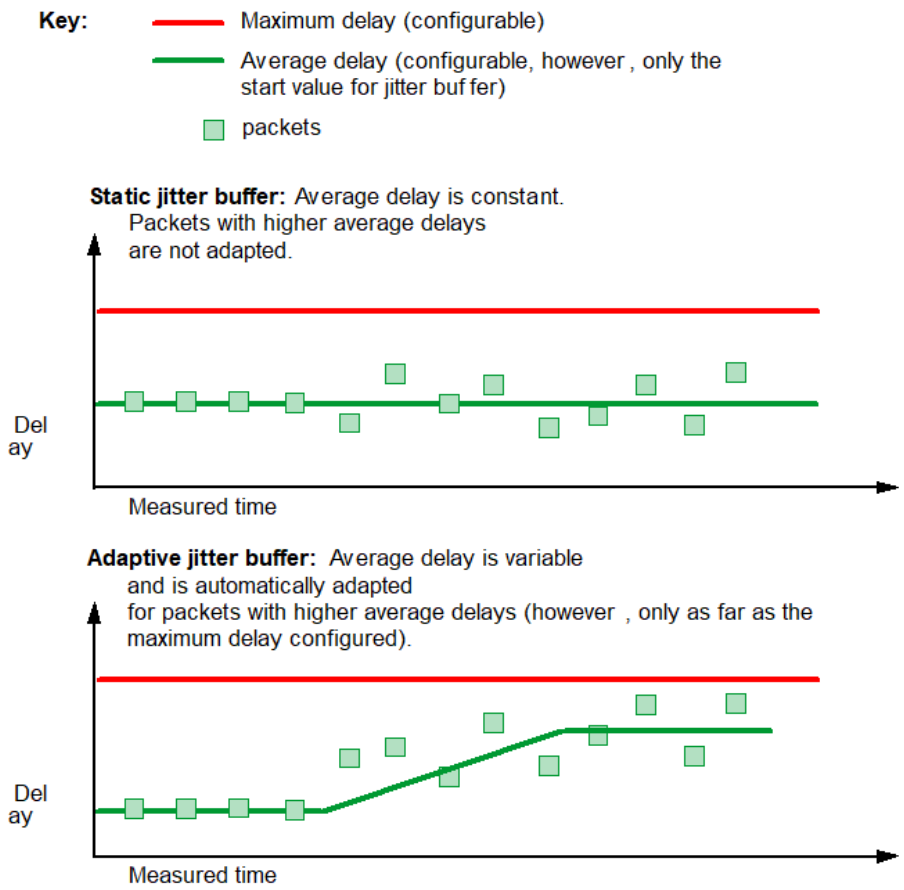


Figure 5: Difference between static and adaptive jitter buffer

2.1.5.3 Considerations when Configuring the Delay for Static Jitter Buffer

The lower the average and maximum delay is set, the more natural voice transmission will sound to subscribers. However this increases the danger of packet loss and in turn the danger of information loss and distortions. Higher delay values mean less packets get lost, however, it takes longer until a subscriber hears what the other subscriber is saying. Extensive delays can lead to communication difficulties. The following diagram illustrates this:

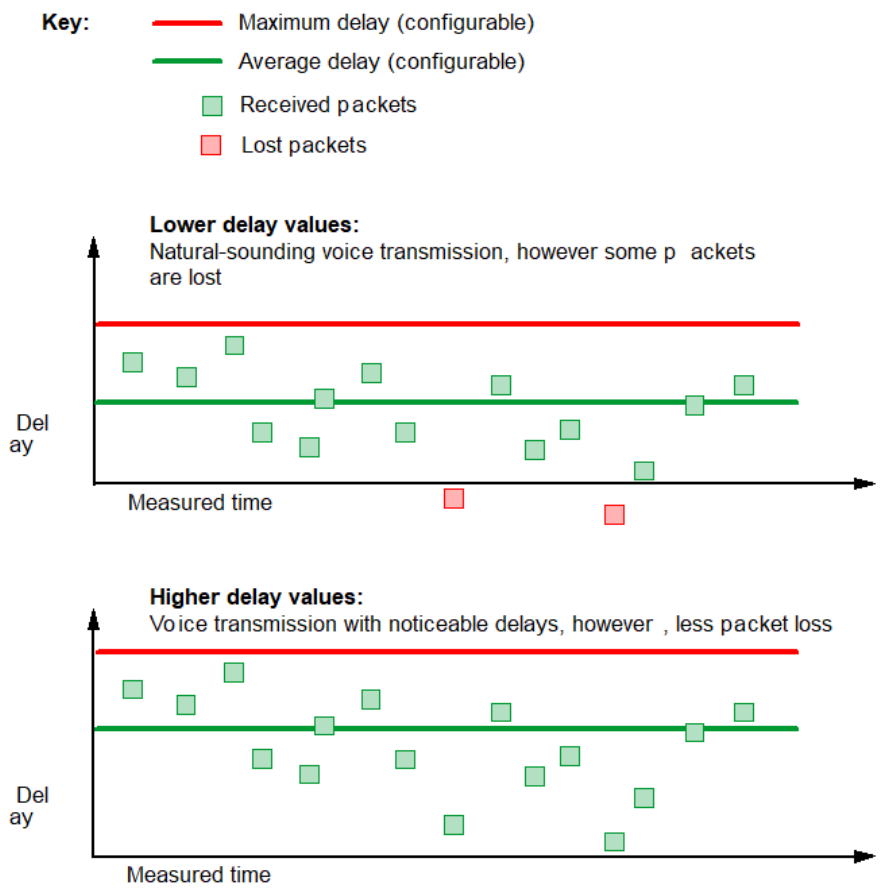


Figure 6: Settings for the static jitter buffer

When the HG 3500/75 board is being generated, generous values are set with which most installations will start without any problem. In many cases, these values can then be reduced selectively.

2.1.5.4 Clock Drift with Static Jitter Buffer

With digital voice transmission in ISDN, all transmission devices operate synchronously. In other words, the volume of voice data per time unit is absolutely the same for the sender and the receiver. For this purpose, transmission devices are synchronized to a common clock pulse (clock signal).

With digital voice transmission over IP, the transmission devices operate asynchronously. Exception: IPDA access point with digital trunk connection can synchronize with the clock signal. This asynchronicity means that more or fewer packets are created per second at the transmitting end than are expected at the receiving end. This discrepancy is called clock drift.

If more packets are created at the transmitting end than are expected by the receiver, more packets enter the jitter buffer than intended. This leads to a constant increase in the measured average delay. If this reaches the configured maximum delay value, the jitter buffer adjusts itself. It skips surplus packets until the measured average delay reverts to the set value for average delay. The entire procedure is then restarted. The following figure illustrates the procedure:

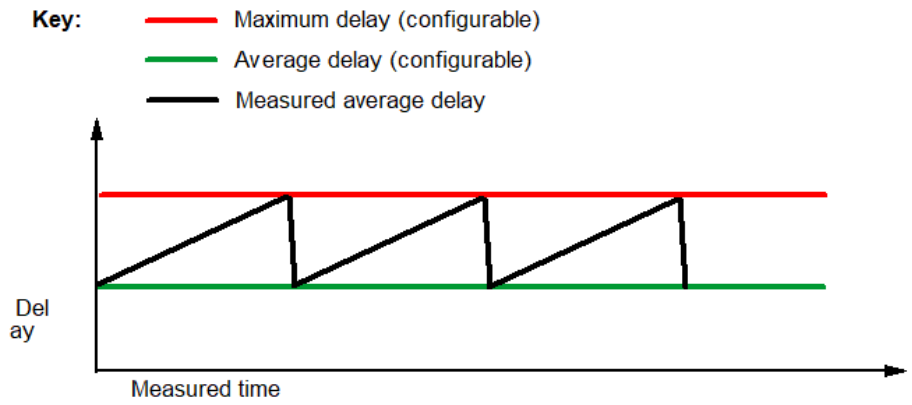


Figure 7: Clock drift in static jitter buffer [transmission quicker than receipt]

If, for example, the average delay is set to 40 ms and the maximum delay to 80 ms, this means that the measured overall delay will increase at intervals by 40 ms from the start value. The length of the interval will be determined by the clock pulse difference of the clock pulse generators in the central system (for all HG 3500 systems) or on the HG 3575 boards as well as on the configuration data (difference between the maximum and the average value). In the sample configuration (40 ms delay hub) the interval is between approximately 30 and 120 minutes long.

If fewer packets are generated at the transmitting end than are expected by the receiver, more packets enter the jitter buffer than intended. This leads to a constant decrease in the measured average delay. If, as a result, the number of packets located in the jitter buffer is reduced to zero, the jitter buffer adjusts itself and resets the measured average delay to the set value for average delay by inserting packets. The entire procedure is then restarted. The following figure illustrates the procedure:

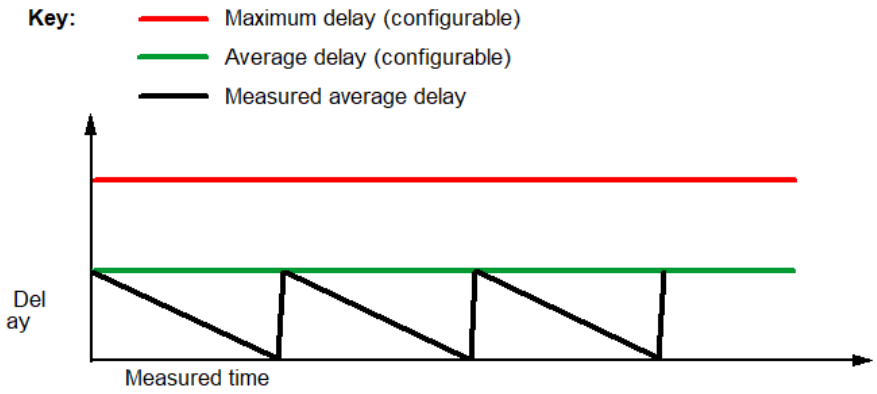


Figure 8: Clock drift in static jitter buffer [transmission slower than receipt]

If, for example, the average delay has been set to 40 ms, this means that the measured overall delay is reduced at intervals from the start value by 40 ms. The length of the interval depends on the clock pulse difference of the clock pulse generators in the central system (for all HG 3500 systems) or on the

HG 3575 boards as well as on the configuration data (difference between the maximum and the average values). In the sample configuration (40 ms delay hub) the interval is between approximately 30 and 120 minutes long.

The variation in the overall delay caused by clock drift can be completely avoided by synchronizing the components involved with a common clock pulse.

2.1.5.5 Minimum Delay for Adaptive Jitter Buffer

In adaptive working mode, the jitter buffer tries to keep the average delay as low as possible. In a situation where no jitter effect occurs, the average delay drops to a minimum. This minimum can be configured in the HG board. The average delay, which is continuously adapted based on the current delay measured, ranges between two values: the configurable minimum delay and the configurable maximum delay. The following diagram illustrates this:

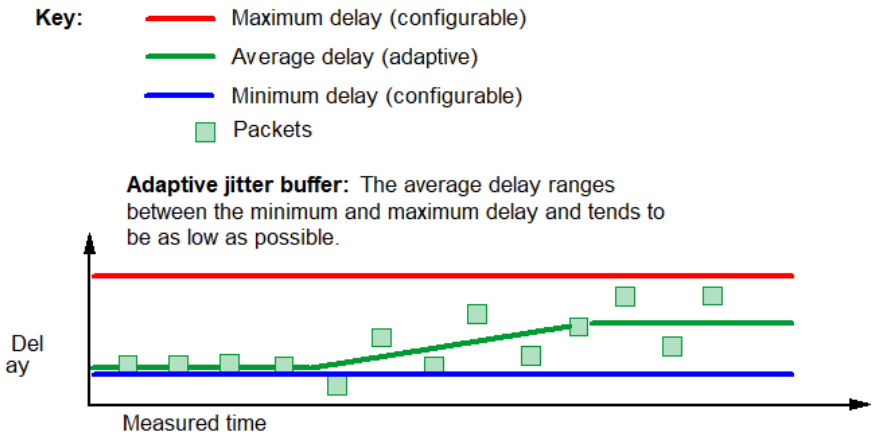


Figure 9: Minimum delay for adaptive jitter buffer

Minimum and maximum delay values are still adhered to if packets are lost.

2.1.5.6 Packet Loss Control in Adaptive Jitter Buffer

In the case of the adaptive jitter buffer, the average delay is automatically readjusted. The aim of this is to achieve a good balance between having the shortest possible average delay on the one hand and the lowest possible packet loss on the other.

You can set which of these factors is attributed more importance using the “Preference Parameter“. Using values from 0 to 8, you can specify whether decreasing the delay or avoiding packet loss should be prioritized when calculating the average delay. In this case, 0 denotes “Avoid packet loss as far as possible“ and 8 denotes “Maintain shortest possible average delay“. An average value (4) is predefined.

Rule of thumb: setting the value to 0 results in approx. 10 ms longer average delay and setting it to 8 results in approx. 10 ms shorter average delay than that applicable when the average value is set to 4.

2.1.5.7 Parameters for Jitter Buffer Configuration

To understand the delay parameters, it is important that the values are aligned with the compensable network jitter. As is the case for all IP gateways or terminals, the actual transmission times for voice packets in HG 3500 and HG 3575 also fluctuate around a constant ideal value. This deviation (jitter at transmitting end) is already taken into account during implementation.

These parameters can be set via the **AMO STMIB** (for HG3575) or the **AMO CGWB** (for HG 3500).

- **Jitter Buffer Type:**Select whether the jitter buffer should operate in static or adaptive mode. In adaptive mode, the jitter buffer adjusts the average delay according to the situation when the data is received. In this way, the jitter buffer tries to reduce as far as possible both the delay and the number of lost packets. In static mode, the average delay always remains the same.
- **Average Delay for Voice (msec):**With this parameter you can specify the average number of milliseconds for which an IP packet should be held in the jitter buffer in IP-based voice transmission. In the “adaptive“ jitter buffer, the value specified here only represents an initial value. 40 is the value recommended for most environments.
- **Maximum Delay for Voice (msec):**In the “static“ jitter buffer, this parameter is used to define how many milliseconds are allowed (before the jitter buffer begins to regulate the data stream) for an actual measured delay when IP packets arrive during voice transmission. In the “adaptive“ jitter buffer, the maximum number of milliseconds allowed for the average voice delay is entered in this field. If the actual measured delay is longer, packets are lost. 80 is the recommended value for most environments with the static jitter buffer; 120 is the recommended value for the adaptive jitter buffer. Either way, the value must be higher than that in the “Average Delay for Voice (ms)“ field.
- **Minimum Delay for Voice (msec):**If the “adaptive“ jitter buffer was selected, use this parameter to enter how many milliseconds are allowed for the minimum average voice delay. This means that in every case, the average delay value is higher than or equal to this value.
- **Packet Loss / Delay Preference:**In the case of adaptive jitter buffers, you can use values from 0 to 8 in this parameter to specify whether you would prefer packet loss or a longer delay in the case of large packet delays. 0 denotes minimum packet loss and acceptance of delays in the voice data stream, 8 denotes minimum delay in the voice data stream and acceptance of packet loss. 4 is the value recommended for most environments.
- **Average Delay for Data (msec):**With this parameter, you can specify the average number of milliseconds for which an IP packet should be held in the jitter buffer during data transfer. 60 is the value recommended for most environments.
- **Maximum Delay for Data (msec):**With this parameter you can specify the number of milliseconds allowed (before the jitter buffer begins to regulate transmission) for an actual measured delay when IP packets arrive during data transfer. 200 is the recommended value for most environments. A parameter setting does not make any difference for higher values (approx. 200 upwards) because packets then leave the buffer as soon as they are received in full. Values under 100 ms are possible, however they are not recommended for use.

2.1.6 Runtime and Noticeable Effects

2.1.6.1 General Information on Delay

A delay of 40-100 ms can be expected with each IP Hop (dependant on Frame size and Jitter value).

2.1.6.2 Delay and Echo

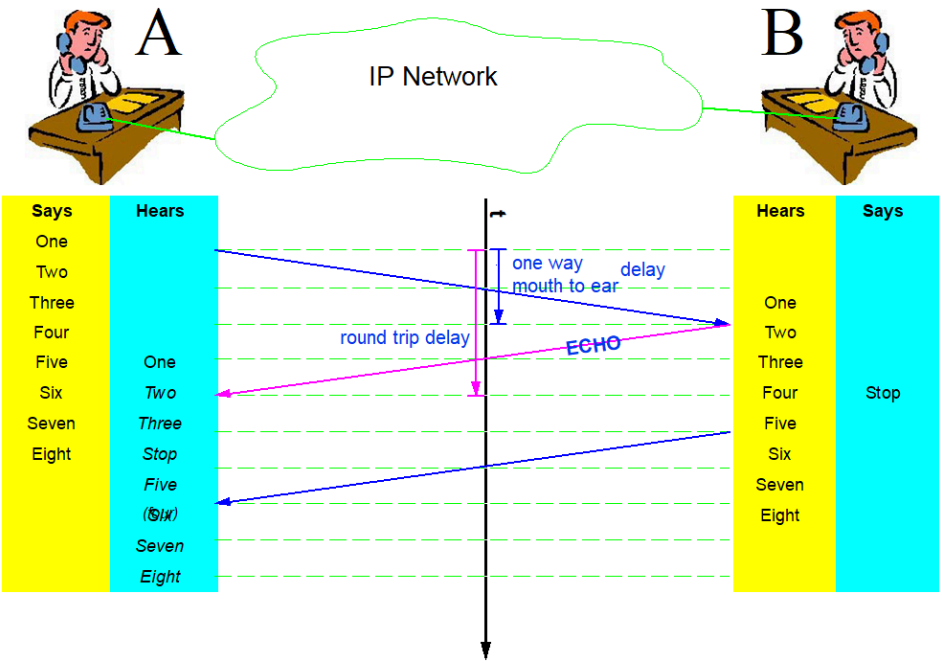


Figure 10: Delay and echo

Voice transmission generally requires more runtime than we are used to in conventional telephony. Figure 10 Delay and echo contains an example illustrating how this sounds. Here the mouth to ear delay is approximately 250 ms.

If Speaker *A* counts from **one** to **eight** and Speaker *B* says **stop** after he hears **three**, *A* hears **stop** while he is saying **eight**. Obviously, selecting a number and saying STOP during counting is not something that happens very often in real conversation. Nevertheless, the delay effect caused by round trip delays is noticeable in normal conversation. It often leads to *collisions* when the speaker changes.

If an echo is generated on the B side (e.g. because of the 2-wire/4-wire hybrid of analog terminal devices, also known as hybrid coil), this is noticed by the speaker, who finds himself speaking over what he said a half a second before, for example.

With high transmission runtimes, it is therefore generally necessary to have echo-free signals on the transmission path. With IPDA, this is achieved through

active echo cancellation in the HG 3500 and HG 3575 modules, which filters out the signal section received from A in the send signal from B (the echo) before transmission of the send signal from B.

2.2 Architecture and System Requirements

2.2.1 Prerequisites

Prior to installing IP line gateways at a customer site a network assessment is required that will determine whether the customer's IP network is capable of supporting IP phones. This network assessment will analyze the IP network and determine parameters like jitter, packet loss, available bandwidth, supported QOS mechanisms and assess overall VoIP readiness.

2.2.2 Power Requirements

The HG 3500 line gateway is a OpenScape 4000 peripheral card that plugs into an AP 3300 and an AP 3700 access points. However, HG 3500 cards require more than average power due to components with high power demands (DSPs). This limits the total number of HG 3500 cards to a maximum of 6 cards per AP 3700 IP (9 slot) and 10 cards per AP 3700 (13 slot).

2.2.3 Network Requirements

The HG 3500 / IPDA components place high demands on the network via which they are coupled to their IP endpoints. Just like signaling links between the CC and the access points, Voice-over-IP data streams are sensitive to packet runtime, runtime variance (jitter) and packet loss.

The availability and reliability of a HG 3500 / IPDA system depends heavily on the quality of the IP network used.

Therefore, the network must be examined prior to installation with regard to its suitability for VoIP for the use of HG 3500 / IPDA.

All OpenScape 4000 components **must** be connected to their own ports on Layer 2 switches.

Using hubs together with OpenScape 4000 can cause problems. For this reason, they are not permitted for use in corresponding VoIP scenarios. If hubs are available, they should be replaced with a switch.

In order to achieve a high Quality of Service (voice quality/real time behavior of signaling), the support of IEEE 802.1 p/q VLAN Tagging and IETF RFC 2474 DiffServ is recommended (see Section 2.4, “Network Data”).

IMPORTANT: If an access point is connected over **W**ide **A**rea **N**etworks in which the available **bandwidth is extremely restricted**, the control information (signaling) and voice data (payload) for access points must be given priority over other services.

Frequently, only explicitly familiar TCP/IP or UDP/IP port numbers are supported in the customer LAN for security reasons. All others are then blocked in such cases. Precisely which port numbers must be supported for the HG 3500 component in the network is described in Chapter 20, “IP Ports”

IP Interface MTU

The OpenScape 4000 IP interfaces use an IP interface MTU of 1500 bytes by default. In order to ensure optimal IP network throughput, it is recommended to likewise operate the IP network both for the IPDA LAN (Signaling/Media - Voice over IP) and the Management LAN with a MTU of 1500 bytes.

If this is not possible, for example because of WAN routers (PPPoE, IPSEC,...) with a smaller MTU, it is recommended to use TCP - MSS Clamping in these routers. This router configuration results in the OpenScape 4000 software components adapting the TCP packet size for the next TCP three-way handshake.

IMPORTANT: This procedure applies for TCP, but not for UDP. The UDP packets (e.g. RTP media) are generally smaller than 500 bytes however.

Exception: SIP-Q via UDP

In case of problems, it is possible to configure the IP interface MTU for CGW/ OpenScape 4000 SoftGate modules by means of the module's WBM. The IP interface MTU should not be set however to a value under 1000 bytes.

Furthermore, the OpenScape 4000 software stacks generally also react to ICMP Fragmentation Needed Packets, which then results in the packet sizes being adapted. This procedure can lead to longer runtimes however.

2.2.4 Network Data

This feature is used to configure additional nodes/IP gateways in the customer LAN. Every node/IP gateway requires configuration data which must be coordinated with the network administration of the customer, documented and configured precisely as agreed.

The following data must be specified for every new node/IP gateway in the customer LAN:

- IP address of the node
- Netmask for the network in which the new node is added
- Default router via which the other networks can be reached

Furthermore, the way in which Quality of Service is supported must be clarified for all networks in which OpenScape 4000 components are installed. As OpenScape 4000 supports IP distributed architecture processes for controlling the Quality of Service in a network on various protocol layers, the following must be clarified:

- Is IEEE 802.1 p/q VLAN Tagging (Layer 2) supported?
- To this end, it is crucial that all network components with which an OpenScape 4000 component communicates must support the standard and be configured accordingly. If the network contains nodes (particularly

switches and routers) which do not support IEEE 802.1 p/q, VLAN tagging must remain deactivated. The traffic type is assigned a fixed priority value.

- If DiffServ pursuant to RFC 2474 is supported, which CodePoints can be utilized?
- In the OpenScape 4000 components, TOS bytes must be set to partially differing values for the following traffic types. The default values assume DiffServ support on the part of the network and realize the Quality of Service strategy. For more information on the TOS baytes please refer to Section 2.4.1, “TOS Byte”.

There are a number of other common prioritization methods, which are managed in the affected routers:

- Prioritization based on the IP address
- The entire traffic from an interface is given (identical) priority. Traffic from IPDA components can thus be given a higher priority than other traffic by specifying the IP address.
- Prioritization of a port (socket) range
- In this case, the IPDA-specific ports (see Chapter 20, “IP Ports”) are given a higher priority than other ports in the network.

It is essential that the **signaling** and payload ports be taken into account here. This method is not recommended given the size of the port range for payload.

- Prioritization of specific services (TCP, UDP)
- Although prioritization of UDP traffic, for example, in the network would have a positive effect on the payload, it would restrict signaling (TCP/IP). This type of signaling is therefore **NOT** suitable for IPDA. It impairs system availability.

2.2.4.1 TOS Byte

The TOS byte can be read in a number of different ways:

- Two 3-bit values for precedence and priority
- One 6-bit value as a combination of both 3-bit values (DiffServ CP)
- The entire TOS byte including two fill bits

For IPDA, the entire TOS byte is specified. The two least significant bits are always set to zero. See also Section 1.1, “Key Words”.

Table 3: TOS values

Type	Traffic type	HW	TOS byte				IEEE 802.1 p/q Priority
	Package Handling Behavior How should packages of this traffic type be handled?		With DiffServ CodePoint (default)		Without DiffServ		
			Binary	Dec	Binary	Dec	

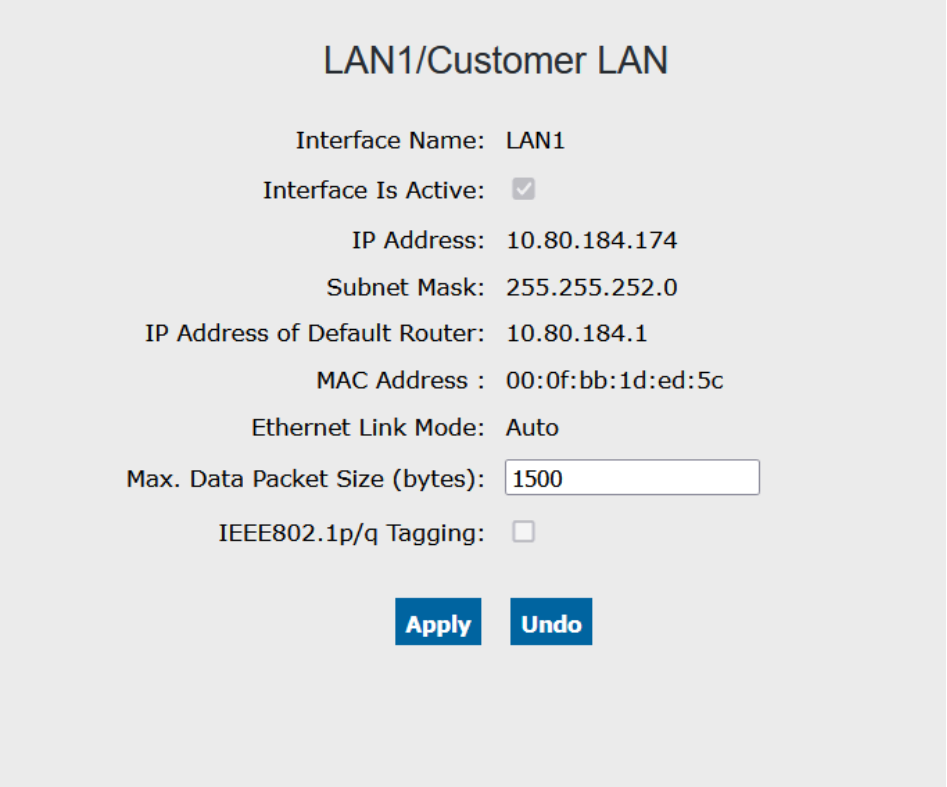
TOSPL	VoIP payload Minimal delay Slight packet loss	HG 3500 HG 3575	1011 1000 (EF)	184	0001 0000	16	5
TOSSIGNL	Signaling between OpenScape 4000 and access point Minimal packet loss Slight delay	OpenScape 4000	0110 1000 (AF31)	104	0001 0100	20	3
TOSLAN	Signaling via LAN Minimal packet loss Slight delay	AP	0110 1000 (AF31)	104	0001 0100	20	3
TOSMODEM	Signaling via Survivability connection Minimal packet loss Slight delay		0111 0000 (AF 32)	112	0001 0000	16	- N/A, as PPP connection

The values for **TOSSIGNL** (AMO CGWB, AMO SIPCO), **TOSLAN** (AMO STMIB) and **TOSMODEM** may not be zero. **TOSLAN** and **TOSMODEM** must be set differently to each other. **TOSPL** is set in AMO CGWB, AMO SIPCO and AMO STMIB.

It is important that the required behavior *(Package Handling Behavior)* is achieved in the network. The absolute numerical values for TOS and IEEE 802.1 priority are not important in this case. They are used solely for the purposes of identifying the required Package Handling Behavior.

The values mentioned in the table are the default settings of the IP gateway loadware (STMI/NCUI). These settings fulfill the OSCAR specifications.

You can change the L2 priority with **WBM** > **Configuration** > **Network &Routing** > **Network Interfaces** > **LAN1 (LAN1)**



The values for VLAN priority (layer 2) cannot be changed via AMO. Therefore the L2 priority for the signaling connection (CCA/CCB, AMO SIPCO) is hard coded.

IMPORTANT: If you change the TOS values for **HG 3500** with **AMO CGWB** you have to reboot the corresponding gateways with AMO BSSU. If you change the TOS values for **HG 3575** using **AMO STMIB** you have to an `EXEC-USSU:UPDATAP;` or a `REST-USSU:LTU;` depending which parameter you changed. Both commands will generate a restart of the shelf. If you want to change the values with **AMO SIPCO** please do a soft restart for CCA and CCB.

Value range of the TOS values (0-255)

As of HiPath 4000 V5 R1 the value range of the TOS values (0-255) has been extended (see Table 4, “TOS byte correspondences”.

IMPORTANT: The column “Decimal 8-Bit” contains the values which are needed for the AMO commands. The other columns are only for informational purposes.

Table 4: TOS byte correspondences

DSCP-value	Decimal 6-bit	Decimal 8-Bit	hexadecimal 6-Bit	hexadecimal 8-Bit
DSCP63	63	252	3F	FC

DSCP-value	Decimal 6-bit	Decimal 8-Bit	hexadecimal 6-Bit	hexadecimal 8-Bit
DSCP62	62	248	3E	F8
DSCP61	61	244	3D	F4
DSCP60	60	240	3C	F0
DSCP59	59	236	3B	EC
DSCP58	58	232	3A	E8
DSCP57	57	228	39	E4
CS7	56	224	38	E0
DSCP55	55	220	37	DC
DSCP54	54	216	36	D8
DSCP53	53	212	35	D4
DSCP52	52	208	34	D0
DSCP51	51	204	33	CC
DSCP50	50	200	32	C8
DSCP49	49	196	31	C4
CS6	48	192	30	C0
DSCP47	47	188	2F	BC
EF	46	184	2E	B8
DSCP45	45	180	2D	B4
DSCP44	44	176	2C	B0
DSCP43	43	172	2B	AC
DSCP42	42	168	2A	A8
DSCP41	41	164	29	A4
CS5	40	160	28	A0
DSCP39	39	156	27	9C
AF43	38	152	26	98
DSCP37	37	148	25	94
AF42	36	144	24	90
DSCP35	35	140	23	8C
AF41	34	136	22	88

DSCP-value	Decimal 6-bit	Decimal 8-Bit	hexadecimal 6-Bit	hexadecimal 8-Bit
DSCP33	33	132	21	84
CS4	32	128	20	80
DSCP31	31	124	1F	7C
AF33	30	120	1E	78
DSCP29	29	116	1D	74
AF32	28	112	1C	70
DSCP27	27	108	1B	6C
AF31	26	104	1A	68
DSCP2 5	25	100	19	64
CS3	24	96	18	60
DSCP23	23	92	17	5C
AF23	22	88	16	58
DSCP21	21	84	15	54
AF22	20	80	14	50
DSCP19	19	76	13	4C
AF21	18	72	12	48
DSCP17	17	68	11	44
CS2	16	64	10	40
DSCP15	15	60	F	3C
AF13	14	56	E	38
DSCP13	13	52	D	34
AF12	12	48	C	30
DSCP11	11	44	B	2C
AF11	10	40	A	28
DSCP9	9	36	9	24
CS1	8	32	8	20
DSCP7	7	28	7	1C
DSCP6	6	24	6	18
DSCP5	5	20	5	14

DSCP-value	Decimal 6-bit	Decimal 8-Bit	hexadecimal 6-Bit	hexadecimal 8-Bit
DSCP4	4	16	4	10
DSCP3	3	12	3	C
DSCP2	2	8	2	8
DSCP1	1	4	1	4
DF	0	0	0	0

2.2.5 Bandwidth Requirements

The actual bandwidth per active payload connection depends on the selected encoding algorithm, the specified sampling time and on the fact if the feature “Signaling and Payload Encryption (SPE)” is activated.

2.2.5.1 Encoding

For example, the following encoding can be selected:

- G.711 (PCM) with support for Annex 1 (packet loss enhancements) and Annex 2 (Voice Activity Detection with Comfort Noise Generation).
- G.729A voice compresses to 8Kpbs.
- G.729AB with Voice Activity Detection.

IMPORTANT: Note that there is virtually no delay introduced in generating G.711 encoding from TDM voice packets (Algorithmic Delay = 0 ms).

For more detailed information on codecs please refer to Section 1.3, “Codec Standards”.

2.2.5.2 Sampling Time

Voice needs to be digitized before it can be assembled into IP packets.

For telephony applications, voice is sampled every 125 µs at 8bits. It would not make sense to package each individual 8 bit sample into an IP packet. Instead, for G.711 encoding at least 240 8 bit samples are combined into an IP packet.

It takes 30 ms to acquire 240 voice samples.

The Sampling Time is defined as the time it takes to sample a specified number of voice samples that are sent out in one IP packet.

It is obvious that the longer the sampling time, the smaller the IP overhead gets. Thus, in order to minimize bandwidth, the sampling time will have to be increased.

However, increasing the sampling time will increase the overall delay!

IMPORTANT: There is always a trade off between minimizing the delay versus minimizing the required bandwidth.

For IP line gateways the sampling time can be set between 10 ms and 90 ms depending on codec type.

2.2.5.3 IP Overhead

The IP overhead includes the Real Time Protocol (RTP) header, User Datagram Protocol (UDP) header and IP headers as well as the Ethernet framing and additional octets for QOS Tagging. A typical IP overhead value for G.711 is 30%.

2.2.5.4 Required Bandwidth per Connection

Note that the bandwidth calculation is based on 70 bytes of overhead: RTP (12 bytes), UDP (8 bytes), IP (20 bytes), 802.1Q VLAN Tagging (4 Bytes), MAC (incl. Preamble, FCS, 26 Bytes).

IMPORTANT: Bandwidth requirements assume **Full Duplex** operation! When running Half Duplex, twice the bandwidth is required.

Bandwidth for active DMC master connections without SPE:

Table 5: Bandwidth for active DMC master connections without SPE

Codec	Sampling Time [ms]	Payload Frames per second	Payload [Bytes]	Total Bytes	Bandwidth [Bit/s]
G.711	10	100,00	80	150	120000
	20	50,00	160	230	92000
	30	33,33	240	310	82667
	40	25,00	320	390	78000
G.729AB	20	50	20	90	36000
	30	33,33	30	100	26667
	40	25,00	40	110	22000
	60	16,67	60	130	17333
G.723	30	33.33	24	94	25067
	60	16,67	48	118	15733

Bandwidth for active DMC master connections with SPE:

Table 6: Bandwidth for active DMC master connections with SPE

Codec	Sampling Time [ms]	Payload Frames per second	Payload [Bytes]	Total Bytes	Bandwidth [Bit/s]
G.711	10	100,00	90	160	128000
	20	50	170	240	96000
	30	33,33	250	320	85333
	40	25,00	330	400	80000
G.729AB	20	50	30	100	40000
	30	33,33	40	110	29333
	40	25,00	50	120	24000
	60	16,67	70	140	18667
G.723	30	33.33	34	104	27733
	60	16,67	58	128	17067

Bandwidth for master connections no longer used (without SPE):

Table 7: Bandwidth for master connections no longer used (without SPE)

Codec	Frame	Packets		Packet Size [Byte]		Bandwidth [kBit/s]	SID[1] relative to Active
	Length [Byte]	Length	Rate	Pure Data	Ethernet	Ethernet	Ethernet
G.711	1	1000 ms	1,00 /s	1	71	0,6	0,7%
G.729A	2	1000 ms	1,00 /s	2	72	0,6	1,6%
G.723	4	990 ms	1,01/s	4	74	0,6	2,4%

Bandwidth for master connections no longer used (with SPE):

[1] rate between active master connections and master connections no longer used

Table 8: Bandwidth for master connections no longer used (with SPE)

Codec	Frame	Packets		Packet Size [Byte]		Bandwidth [kBit/s]	SID[2] relative to Active
	Length [Byte]	Length	Rate	Pure Data	Ethernet	Ethernet	Ethernet
G.711	1	1000 ms	1,00 /s	11	81	0,6	0,8%
G.729A	2	1000 ms	1,00 /s	12	82	0,7	1,6%
G.723	4	990 ms	1,01/s	14	84	0,7	2,4%

2.2.5.5 Voice Activity Detection (VAD)

Voice activity detection conserves bandwidth in the IP network during pauses in speech and can further reduce the required network bandwidth from 50% to 75% (see Section 4.3, “Voice Activity Detection (VAD)” for more details).

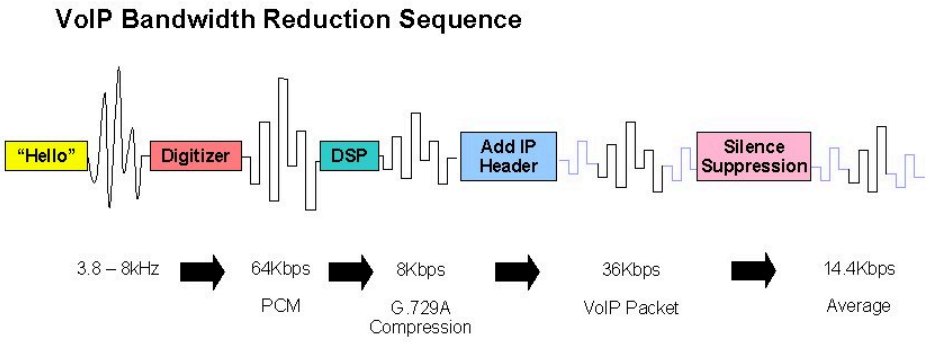


Figure 11: VoIP Bandwidth Reduction Sequence

2.2.5.6 DMC Considerations

Whenever a DMC connection is established, a “Master Connection” is setup as well.

The master connection is following the same path as the signaling through all the gateways between to IP clients.

The master connection ensures that the necessary resources are always available whenever a feature is invoked that results in a multi party call (e.g. conference). There is also no delay for invoking these types of features because the connection is already setup.

However, there are drawbacks to the master connection concept as well:

- Additional bandwidth is required for sustaining the master connection

[2] rate between active master connections and master connections no longer used

- Depending on the configuration significant delays and multiple hops can occur between IP clients when voice payload is using the master connection. Especially when IP end points are located on different IP Access Points on IP connected systems, delays may increase beyond acceptable levels.

In Figure 13 DMC and Master Connection the DMC and Master Connection is shown between two IP networked OpenScape 4000 systems for a call between two IP clients (one on each system).

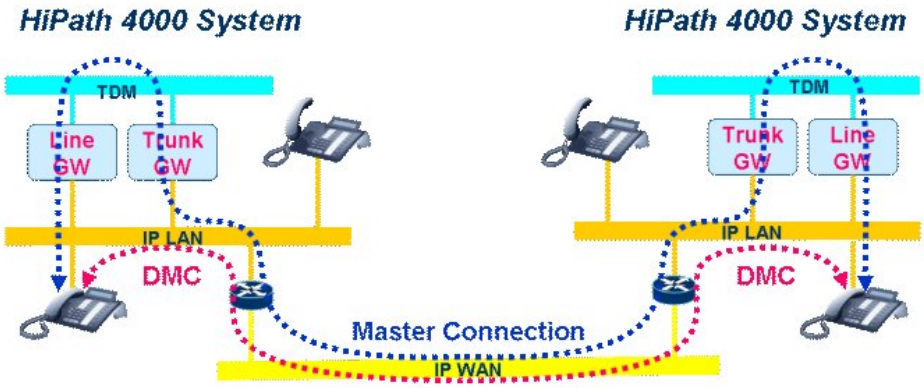


Figure 12: DMC and Master Connection

Enabling VAD will reduce the required bandwidth on the master connection to negligible levels.

Note that delays for each TDM to IP conversion accumulate. In the example above the master connection goes through 3 hops which will result in approximately 200ms end to end delay assuming G.711 encoding with 30ms sampling time and a high quality network (20ms delay). The DMC connection goes only through one hop resulting in an end to end delay of about 80ms.

For more details please refer to Section 4.1, “Direct Media Connection (DMC)”.

2.2.6 B Channels

The following table provides an overview of the number of available B channels that are dependent on enabled features.

Table 9: Number of B channels dependent on enabled features

	STMI2		NCUI2+		STMI4		NCUI4		STMIX	STMIY
	2 DSP (Q2316-X)	4 DSP (Q2316-X10)	2 DSP **(Q2305-X35)**	4 DSP **(2305-X40)**	2 DSP (Q2324-X500)	5 DSP **(Q2324-X511)**	**2 DSP (Q2324-X)**	**5 DSP (Q2324-X11)**	**(Q2343)**	**(Q2361)**
Standards	60	120	60	120	60	120	60	120	120	120
QDC	56	112	56	112	60	120	60	120	120	120
SRTP	45	90	45	90	50	120	50	120	120	120

	STMI2		NCUI2+		STMI4		NCUI4		STMIX	STMIY
	2 DSP (Q2316-X)	4 DSP (Q2316-X10)	2 DSP **(Q2305-X35)**	4 DSP **(2305-X40)**	2 DSP (Q2324-X500)	5 DSP **(Q2324-X511)**	**2 DSP (Q2324-X)**	**5 DSP (Q2324-X11)**	**(Q2343)**	**(Q2361)**
QDC+ SRTP	42	84	42	84	50	120	50	120	120	120
DMC	45	90	45	90	50	100	50	100	120	120
QDC+ DMC	42	84	42	84	50	100	50	100	120	120
DMC+ SRTP	32	63	32	63	40	100	40	100	120	120
QDC+ DMC +SRTP	30	60	30	60	40	100	40	100	120	120

Important Notes for QDC

QDC is activated on the gateway via WBM and needs additional performance resources.

QDC is **not automatically considered for channel reduction**. Therefore the **number of channels has to be adapted manual** (depending on the type of the board) to the values mentioned in the table above when QDC is activated. If no adaption takes place performance problems will occur.

Automatic b channel reduction

Using the features for signaling and payload encryption (SPE) and also DMC, automatic b channel reduction is performed, i.e. the current values set are reduced by a fixed percentage. This percentage depends on the hardware used.

IMPORTANT: The automatic b channel reduction is not performed with the feature QDC. This b channel reduction has to be done manually referring to Table 9, “Number of B channels dependent on enabled features”.

This reduction is not only calculated on board level but on function level. This means that the percentage values from above will be calculated per configured function.

Examples for single feature support (STMI2/STMI4):

1) DMC is activated for HG 3550 on Q2324-X511

2) **DMC** activated on Q2324-X511: reduction of the b channels of 17% (= minus 20 b channels)

=> Maximum number of available b-channels: 120-20=**100**

3) SPE and DMC is activated for HG 3550 on Q2316-X.
4) **SPE** activated on Q2316-X: reduction of the b channels of 25% (= minus 15 b channels)

   => 60-15=**45**

   DMC additionally activated on Q2316-X: reduction of the b channels of 25% (of the maximum number of available b channels / depending on the board and/or number of DSPs = minus 15 b channels)

   => Maximum number of available b-channels: 45-15=**30**

Example for multiple feature support (STMI2/STMI4):

1) **DMC** is activated for 2 HG 3550 circuits with 40 b-channels on Q2324-X500. The remaining 20 b-channels are configured for HG 3530.
2) **SPE** activated on Q2324-X500 for HG 3550: reduction of the b channels of 17% (of 40 b channels = minus 7 b channels)

   => Maximum number of available b-channels for HG 3550: 40-7=**33**

   The HG 3530 gateway cannot act as DMC endpoint. Therefore the 20 b channels won't be reduced for HG 3530.
3) SPE is activated for 2 HG 3550 circuits with 40 b-channels and HG 3530 for 20 b channels on Q2324-X500.
4) **SPE** activated on Q2324-X500 for HG 3550: reduction of the b channels of 17% (of 40 b channels = minus 7 b channels)

   => Maximum number of available b-channels for **HG 3550**: 40-7=**33**

   SPE activated on Q2324-X500 for HG 3530: reduction of the b channels of 17% (of 20 b channels = minus 3 b channels)

   => Maximum number of available b-channels for **HG 3530**: 20-3=**17**

   These reduced b-channel values are the upper limit for path selection.

   The B channel number increases appropriately when features are deactivated.

   Summary:

   In the AMO BFDAT, only the maximum number of B channels can be configured. Using the AMO BCSU, the number of currently available B channels can be displayed and the B channels configured.

   The following tables provide an overview of the number of available B channels that are dependent on enabled features.

2.2.6.1 B Channel Configuration

2.2.6.1.1 AMO BFDAT

Using the AMO BFDAT, the profile of the board is defined with a maximum number of B channels.

- ADD-BFDAT, parameter **BRDBCHL**
- The parameter **BRDBCHL** determines if a block for a board with 60 or 120 b channels will be configured.
- ADD-BFDAT, parameter **FUNCTION**

- With the parameter **FUNCTION** you can configure the functions of the common gateway (i.e. HG 3500, HG 3530, etc.).
- CHANGE-BFDAT, parameter **BCHLCNT**
- With the parameter **BCHLCNT** you can configure the maximum number of b channels per function. This value must not be higher than the maximum number of b channels possible for this function (see Section 2.6.1.2, “AMO BCSU”, parameter **BCHLCNT**).

2.2.6.1.2 AMO BCSU

The profile configured with AMO BFDAT (maximum number of b channels (**BRDBCHL**) and configured functions (**FUNCTION**)) is evaluated by AMO BCSU. Additionally the activated features in the system (i.e. DMC, SPE) will be considered. An automatic b channeled reduction will be performed (see Section 2.6.1.2, “In the case of bandwidth problems, etc. the current value of the B channels that can be used f

With DISPLAY-BCSU the following information can be found:

- How many b channels are available on the board (**BCHANNELS**).
- How many b channels have been configured wit AMO BFDAT per function (**BCHANNELS**).
- How many b channels are possible per function (**BCHLCNT**). The parameter **BCHLCNT** depends on what feature has been activated (see Section 2.6, “B Channels”). The value in parameter **BCHLCNT** can be lower than the configured number of b channels for this function in AMO BFDAT. But only the amount of b channels of parameter **BCHLCNT** are available for the function.

In the case of bandwidth problems, etc. the current value of the B channels that can be used for each configured function must be reduced. This can be done in AMO BCSU with the b channel parameters (i.e. **BCHL3530**, **BCHLSIP**, **BCHL3550**).

2.2.6.2 Displaying the B Channels currently Available/Configured (possible IP-Based Connections)

The total number of B channels currently in use is shown as usual in the AMO BCSU. The number of B channels is configured in AMO BSCU with the corresponding B channel parameter for each function (**BCHL3530**, **BCHLSIP**, **BCHL3550**, **BCHLWAML** and **BCHL3570**). The AMO BFDAT includes the parameter **BRDBCHL**. This defines the maximum number of B channels for the board (60 or 120 B channels).

Using the AMO BCSU, you can query the number of B channels available for the common gateway board. The AMO UCSU must be used for configured HG3575 boards.

IMPORTANT: Determination of the B channel values differs for HG 3500 and HG 3575.

You can check the channels or bandwidth used with the AMO GKTOP following appropriate configuration.

`DISPLAY-BCSU:TAB,1,<LTU Number>;` command shows 3 b-channel values:

- The maximum number of B-channels supported by the board,
- the number of used b-channels per function and
- the maximum possible number of b-channels per function.

2.2.7 Traffic Considerations

From a trafficking point of view, HG 3500 IP line gateways can be treated like a trunk with either 60 or 120 connections. The number of connections required depends on the number of IP phones configured per HG 3500 and the traffic (C.C.S.) values of these phones. Using a standard ErlangB calculation allows determining the number of trunks/connections that are required on each gateway for a specific configuration.

The tools use a simplified approach and allow 240 standard users and 60/120 high traffic (e.g. call center agents) users on each gateway type. Note that you can mix and match standard and high traffic users but you will be limited to 60/120 users per gateway total. This ensures that call center agents will always be able to seize a line.

Capacities

A maximum of 240 IP clients can be configured per HG 3500 gateway.

Typically a 60 connections gateway is sufficient to serve 240 at 6 C.C.S. In case the users creating a higher amount of traffic, then a 120 connections gateway will be required.

Call center agents are typically trafficked at 32 C.C.S. and thus require a connection on the gateway for each agents. This will limit the number of call center agents to 60 or 120 depending on the HG 3500 type (60/120 connections).

IMPORTANT: Mixing of regular users and call center agents on the same card is possible. However, in order to guarantee connection availability to call center agents at all times, regular users will be trafficked at 1 Erlang (36 C.C.S.)

2.3 Supported Gateways

2.3.1 HG 3500 (Common Gateway)

2.3.1.1 General Information

HG 3500 is supported with the following boards:

- STMI2 (Q2316-X and Q2316-X10)
- STMI4 (Q2324-X500 and Q2324-X510)
- STMIX (Q2343-X)
- STMIY (Q2361-X)

IMPORTANT: Starting with V10R0 the support for STMI2 will not be offered anymore. The replacement for STMI2 is STMIX/ STMIY.

The HG 3500 replaces the following gateways:

- HG 3530 (HFA subscriber)
- HG 3540 (SIP Trunking (native & SIP-Q) and SIP subscriber)
- HG 3550 (IP Trunking)
- HG 3570 (IPDA (host side) - Master and IPDA (host side) - DMC)

With the HG 35000 gateway different sub features (e.g. trunking and IPDA) can be used in parallel on a board (**Multiple Feature Support** (**MFS**)). The gateway can also be used as **Single Feature Configuration**.

The HiPath Feature Access (HFA) concept will be made available for other functions.

IMPORTANT: Restriction: Only one trunking protocol may be configured for each board. There are no restrictions on interworking with other functions.

Configuration example for Multiple Feature Support: see Chapter 15, “Multiple Feature Support Configuration at the Common Gateway (Example)”.

Examples of single feature configuration can be found in the documents:

- HiPath Feature Access (HFA)
- IP Distributed Architecture (IPDA)
- Access Point Emergency (APE)
- SIP Connectivity > Chapter 6, “Configuration of SIP-Q-Trunking / Native SIP Trunking” or
- H323-/H323-Annex-trunking

2.3.1.2 Board Replacement

To replace an STMI/STMI2/STMI4 board please note the following:

- Replace a “small“ STMI/STMI2/STMI4 with a “small“ STMI/STMI2/STMI4: no problem
- Replace a “large“ STMI/STMI2/STMI4 with a “large“ STMI/STMI2/STMI4: no problem
- Replace a “small“ STMI/STMI2/STMI4 with a “large“ STMI/STMI2/STMI4: no problem
- Replace a “large“ STMI/STMI2/STMI4 with a “small“ STMI/STMI2/STMI4: only works if not more than 60 b-channels are used

Procedure:

- Change the board.
- It is not necessary to delete all circuits on the module and the module itself, but rather to change the part number with CHANGE-BCSU (if necessary).

```
CHANGE-BCSU:TYPE=PARTNO,LTG=<ltg>,LTU=<ltu>,SLOT=<slot>,PARTNO1=<part number of
board to be changed>,PARTNO2=<part number of new board>;
```

- Restart the board with

```
RESTART-BSSU:ADDRTYPE=PEN,LTG=<ltg>,LTU=<ltu>,SLOT=<slot>;
```

SIP profile configuration including credentials for SIP Provider (where used) are stored on board/hardware (i.e. STMI2/STMI4/STMIX/STMIY and vSTMI on SoftGate). Please be aware when exchanging hardware to consider a “Factory Reset” from Web-Based Management prior to exchanging the board to ensure all private data is removed.

NOTICE: Prior to this step is recommended to perform a HG3500 Backup to ensure the old data remains available for the new board that will be used.

2.3.1.3 Feature Capacities

IMPORTANT: Information on feature capacities for both HG 3500 and HG 3575 see Chapter 4, “Features and Restrictions”.

- The HG 3500 gateway has the capacity to convert 60/120 connections into Ethernet packets and provide TDM to IP conversion for 60/120 concurrent calls.
- HG 3500 gateways can be configured as a **gateways** providing backup capabilities in case of individual gateway failure.

More detailed information on gateways

One or multiple HG 3500 IP line gateways can be defined in the system that will take over in case any of the installed line gateways fails.

This concept is very efficient and cost effective because a single gateway can protect multiple gateways against failure. However, a single gateway cannot protect against multiple gateways failing simultaneously, which is highly unlikely.

In case of a failure, the system will reprogram a gateway with the parameters of the failed gateway which will enable the IP clients to re-login and resume standard operation.

IP phones will automatically register with the activated gateway and no administrative action is required. Note that users keep the same features and extensions while operating off the gateway.

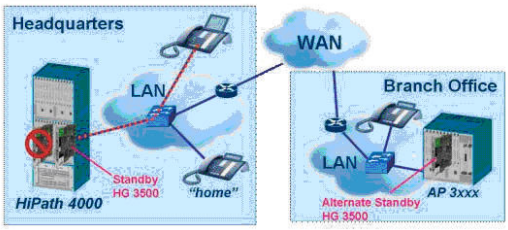


Figure 13: HG 3500 Gateway Operation

Gateways can be located in the host system and/or on an IP Access point. The only requirement is that all active and line gateways have to reside in the same local IP subnet.

IMPORTANT: Gateways and IP clients have to reside within the same system! E.g.: a gateway located in one system cannot control IP clients controlled normally by a gateway located in another system. gateways at IP Access Points will not protect IP users at the host against a host failure because failures at higher levels (e.g. shelf, AP, host or power failures) will not automatically trigger a switchover.

For configuration purposes please refer to Chapter 8, “Standby Board HG 3500”.

- The HG 3500 gateway supports **secondary gateways** that provide full redundancy to IP subscribers. Providing full redundancy for IP clients via secondary gateways will protect against higher level failures, like entire Access Point or host failures.

More detailed information on secondary gateways

In order to protect against higher level failures (e.g. Access Point, host failures) secondary gateways can be added to the system. A secondary gateway is an additional, fully configured gateway for an IP client located anywhere within an OpenScape 4000 system. Note that each IP user that is backed up via a secondary gateway will have 2 extensions, e.g. x1333 on the primary gateway and extension x5333 on the secondary gateway.

In case communication to the primary gateway is lost (e.g. due to a shelf or host failure), the IP phone will attempt to register with the secondary gateway. As long as the secondary gateway is operational and IP connectivity is available, all phones backed up with secondary gateways will register with their secondary gateway and will be fully operational.

While registered with the secondary gateway the users will have all features available that have been enabled on the secondary extension. Incoming calls terminating on the primary extension will be automatically forwarded to the secondary extension using a new feature called “Alternate Routing on Error”.

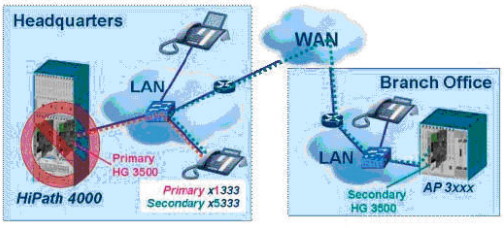


Figure 14: HG 3500 Secondary Gateway Operation

In order to minimize the number of secondary gateways and additional trunks required for operating in failure mode, the following measures can be taken:

- Secondary gateways can be configured with a higher blocking rate, which will limit the number of IP users that can make concurrent calls.
- Minimize the additional trunk required for secondary gateways via “undertrunking”.

Note that these measures are entirely optional and up to the customer’s preference. However, it may be a reasonable approach to limit resources (and thus cost) for operation in failure mode because this is a scenario that is very unlikely to become reality.

IMPORTANT: Secondary gateways and IP clients have to reside within the same system! Secondary gateways can automatically backup any IP user as long as the secondary gateway is operational and IP connectivity between the IP client and the gateway is available.

- The HG 3500 gateway supports **QoS**. VLAN-tagging according IEEE 802.1p/q on Layer 2 as well as DiffServ (defined in RFC 2474) on the IP Layer have been implemented in order to provide the best possible voice quality using an IP network.
- Of course all switches and routers in the customer's IP network must support IEEE 802.1p/q and/or DiffServ prioritization in order to take advantage of these mechanisms.
- The HG 3500 gateway supports "**secondary clients**".

More detailed information on secondary clients

- Secondary clients are soft clients configured with the same phone number as a regular IP phone.
  - Secondary Clients do not require a ComScendo license.
  - Secondary Clients require a soft clients SW license.

  The standard H225 signaling port is 1720 and this port is used at the soft client to establish calls from the board to the soft client. For the soft client it might be necessary to use a different port. In the case that an other H323 application is running in parallel to the soft client it is possible to configure a different H225 signaling port on the soft client. The soft client informs the HG 3500 at registration time and the HG 3500 will use this port for call establishment.

  The soft client can be used as a non standard VPN client. In this configuration the HG 3500 checks the delivered IP address and the real address on the connected CorNetTC socket and informs the soft client about its real IP address when these 2 addresses are different.

  Benefits of Secondary Clients:

  - Secondary clients provide remote access to all OpenScape 4000 features.
  - Starting the secondary client on a PC from any location automatically logs off the office IP phone (associated by the same phone number) and provides the same feature set and class or service to the end-user as the office IP phone.
  - After the remote user returns to the office, the IP phone will still be in the logged off state and the user is prompted to start the phone. This will put the IP phone into a normal operation mode until the IP phone is logged off again by an activation of the associated soft client.
- "**Overbooking**" is possible, meaning that more IP phones per HG 3500 gateway can be configured than there are available connections (maximum of 240 subscribers).

More detailed information on "Overbooking"

1) For overbooking, more stations (**LINECNT**) are configured than the number of actual subscribers (**BCHLCNT**). The actual number of subscribers is configured for the B channels.

   Example:

   Five employees are working at a warehouse. However, the warehouse is big enough to house 10 terminals. As only five employees can simultaneously make and receive calls, only five B channels are required.

   Parameters: LINECNT=10, BCHLCNT=5

- Please always consider the number of channels on an STMI card e.g. a 60 (DSP) channel STMI can have up to 240 IP subscribers configured, but not more than 60 parallel calls can be placed. The restriction of DSP channels does not apply to vSTMI cards.
- All IP phones do support **DHCP** and are supported in DHCP mode via the HG 3500 gateway. Note that a DHCP server has to be configured in the IP network; otherwise static IP addresses are required for all clients.
- The **connection of analog devices via an AP 1120** analog gateway is supported. For more details please refer to the E-Doku pages in the intranet (http://apps.g-dms.com:8081/edoku/jsp/searchresult_v2.jsp?edokutype=&search_mode=product&product=AP%201120&product_version_main=&product_version_sub=&search_term_type=all&term=&s
- Full user **mobility** is supported within a single system and networked systems.
- The HG 3500 gateway is supported in all **IP distributed Access Points**.

2.3.1.4 Restrictions

- CQR Viewer
- The CQR Viewer application is only supported for HFA (**FUNCTION=HG3530**) and IPDA (**FUNCTION=HG3570**), not for trunking (**FUNCTION=HG3550**).
- The HG 3500 supports only phone adapters that do not require their own B-channel.
- The following adapters are not supported:
  - phone-adapter,
  - a/b-Adapter,
  - S0-adapter
  - V.24-Adapter
- Autoset Relocate, Teleworking V2.6 and Workstation Protocol are not supported with HG 3500.
- HG 3500 line gateways do not operate in a load-sharing mode - there is a fixed assignment of the IP phones to one HG 3500 gateway.
- The HG 3500 integrated gateway does not interoperate with 3rd party (e.g. H.323/H.450 or SIP compatible) IP phones/clients.
- The HG 3500 integrated gateway requires a static IP address.
- NTP (Network Time Protocol) is not supported on the HG 3500

2.3.2 HG 3575

2.3.2.1 General Information

HG 3575 is supported with the following boards:

- NCUI2+ (Q2305-X35 and Q2305-X40)
- NCUI4 (Q2324-X and Q2324-X10)

In contrast to HG 3500, there is no Standby concept for HG 3575.

2.3.2.2 Exchanging Boards

OpenScape 4000 - Access Point

1) Deactivate the shelf
```
DEACTIVATE-USSU:LTG=1,LTU=17;
```
2) Remove the old board, insert the new one

If the new board has the same part number as the old one, proceed directly to Item 6. “Activate the shelf”.

3) Delete the AP
```
EXEC-USSU:ART=DELAP,LTU=17;
```
4) Assign the new part number to the shelf
```
CHANGE-UCSU:UNIT=AP,LTG=1,LTU=17,LTPARTNO=Q2305-X10;
```
5) Configure the AP
```
EXEC-USSU:MODE=CONFAP,LTU=17;
```
6) Activate the shelf
```
ACTIVATE-USSU:UNIT=LTG,LTG=1,LTU=17;
```

OpenScape 4000 - Switch

```
CHANGE-STMIB:MTYPE=NCUI2,LTU=18,SLOT=99,TYPE=GLOBAL,PATTERN=213;
CHANGE-STMIB:MTYP=NCUI2,LTU=18,TYPE=IFDATA,VLAN=NO,TOSLAN=72,TOSMO►
DEM=80,VLANID=0,BITRATE=100MBFD;
CHANGE-STMIB:MTYP=NCUI2,LTU=18,TYPE=SERVIF,LOGINTRM="TRM",LOGINPPP="PPP";
CHANGE-STMIB:MTYPE=NCUI2,LTU=18,TYPE=ASC,TOSPL=48=PRIO=PRIO1,CO►
DEC=G711,VAD=NO,RTP="30";
CHANGE-STMIB:MTYPE=NCUI2,LTU=18,TYPE=ASC,PRIO=PRIO2,CODEC=G729,VAD=NO,RTP="20";
CHANGE-STMIB:MTYPE=NCUI2,LTU=18,TYPE=ASC,PRIO=PRIO3,CODEC=NONE,VAD=NO,RTP="20";
CHANGE-STMIB:MTYPE=NCUI2,LTU=18,TYPE=ASC,PRIO=PRIO4,CODEC=NONE,VAD=NO,RTP="20";
CHANGE-STMIB:MTYPE=NCUI2,LTU=18,TYPE=ASC,PRIO=PRIO5,CODEC=NONE,VAD=NO,RTP="20";
CHANGE-STMIB:MTYPE=NCUI2,LTU=18,TYPE=ASC,PRIO=PRIO6,CODEC=NONE,VAD=NO,RTP="20";
CHANGE-STMIB:MTYPE=NCUI2,LTU=18,TYPE=ASC,PRIO=PRIO7,CODEC=NONE,VAD=NO,RTP="20";
CHA-STMIB:MYTPE=NCUI2,LTU=18,TYPE=JB,AVGDLY=40,MAXDLYV=120,MINDLYV=20,PACK►
LOSS=4,AVGDLYG=60,MAXDLYD=200,JBMODE=1;
CHA-STMIB:MTYPE=NCUI2,LTU=18,TYPE=SIGQOS,BANDW=0,MAX►
RTD=0,MINTHRPT=0,SIGPTHSW=STD,QOSSTAT=NO;
CHA-STMIB:MTYPE=NCUI2,LTU=18,TYPE=H323,Q931T1=50,Q931T2=500,GWNAME="HG3575-2";
CHA-STMIB:MTYPE=NCUI2,LTU=18,TYPE=DMCDATA,DMCALLWD=NO,DMCCONN=0;
CHA-STMIB:MYTPE=NCUI2,LTU=18,TYPE=SNMP,CS1="public";
CHA-STMIB:MYTPE=NCUI2,LTU=18,TYPE=WBMDATA,LOGINWBM="HP4K-DEVEL",ROLE=ENGR;
CHA-STMIB:MYTPE=NCUI2,LTU=18,TYPE=WBMDATA,LOGINWBM="HP4K-SU",ROLE=SU;
CHA-STMIB:MYTPE=NCUI2,LTU=18,TYPE=WBMDATA,LOGINWBM="HP4K-ADMIN",ROLE=ADMIN;
CHA-STMIB:MYTPE=NCUI2,LTU=18,TYPE=WBMDATA,LOGINWBM="HP4K-READER",ROLE=READONLY;
CHA-STMIB:MYTPE=NCUI2,LTU=18,TYPE=GWSECTOR,GWSECTNO=0;
CHA-STMIB:MYTPE=NCUI2,LTU=18,TYPE=DLSDATA,DLSPORT=10444,DLSACPAS=NO;
```

WBM configuration

Complete additional settings via WBM.

CLI configuration

So that a connection can be established again to the switch, the IP addresses in the new board must be configured via CLI.

2.4 Features and Restrictions

The following features are supported on HG 3500 **and** HG 3575. For features concerning HG 3500 only please refer to Section 3.1.3, “Feature Capacities”.

2.4.1 Direct Media Connection (DMC)

The HG 35xx gateways support **Direct Media Connection**s (**DMC**).

More detailed information on Direct Media Connections

The HG 35xx gateways support Direct Media Connections (DMC also referred to as peer-to-peer) between two IP phones or an IP phone and an IP board like another HG 3500 or HG 3575. Payload between two DMC endpoints (DMC endpoints = IP phone, HG 3500/3575) is switched entirely in the IP network without involvement or the TDM switching matrix. This ensures highest quality voice and minimal delays because only a single hop (TDM to IP to TDM conversion) is required.

IMPORTANT: Note that invoking any feature that results in a multi party call (more than 2 parties) will route the payload through all gateways in the payload path. This may result in undesirable delays in certain scenarios (see Section 2.5.6, “DMC Considerations” for more details).

Bandwidth is required for the master connection in addition to the DMC connection. The required bandwidth for the master connection can virtually be eliminated by using VAD for the IP clients. In case VAD cannot be enabled then twice the bandwidth is required.

For more information on DMC and bandwidth please refer to Section 2.5.6, “DMC Considerations”.

2.4.2 Voice Compression

The HG 35xx gateways support **voice compression** following standard G.711A encoding at 64Kbps. Compression according to G.729A and G.729AB is supported as well. Also supported codecs are G.711U, G.729 and G.729B.

Of course the actual bandwidth requirements per connection depend on the added IP overhead and various other settings (see Section 2.5.4, “Required Bandwidth per Connection”).

IMPORTANT: Note that the voice compression as well as the gateway functionality is performed on DSP modules.

More detailed information on voice compression

Voice compression uses complex algorithms to reduce the bandwidth of the voice signal, for example G.729, to an eighth of the bandwidth required by the original PCM signal. Impairment of voice quality is only minimal in this case.

Voice compression can be problematic when it is applied a number of times in succession. In other words, the original PCM signal is compressed using a specific method, transmitted and then expanded back to a standard PCM signal, then the whole procedure is repeated on another section. In the worst case scenario, with another procedure. Applying voice compression a number of times, particularly using different compression methods, severely impairs voice clarity and in the worst case scenario it can result in unintelligibility.

The linking of compressed transmission segments - particularly using different methods - must therefore be avoided wherever possible.

Given that all digital speech memory systems for announcements, voicemail etc. also compress speech, this type of equipment must be monitored carefully when used with compressed transmission paths.

Within the OpenScape 4000 system, connections to announcement/music on hold devices as well as to conference units are configured without compression in order to guarantee undistorted music or good voice clarity for conferences.

The factors specified in association with voice compression, such as compression to an eighth of the originally required (uncompressed) bandwidth, for example, always refer to the actual voice data. If this data is transferred using IP, the IP packaging, the “protocol overhead“, must also be taken into account. The voice data to be transferred is reduced by the specified factor by means of compression, but the overhead remains the same. The bandwidth required in the IP network is therefore never reduced by the specified compression factor, but instead by a lot less. Always take the values specified in Chapter 3, “Load Calculation” in the document “IP Distributed Architecture (IPDA)“ into account when dimensioning the bandwidth.

2.4.3 Voice Activity Detection (VAD)

The HG 35xx gateways support **VAD** (**V**oice **A**ctivity **D**etection).

More detailed information on Voice Activity Detection (VAD)

Voice **A**ctivity **D**etection (VAD) serves to save bandwidth in the IP network during pauses in speech.

Based on the knowledge that only one partner usually speaks at a time, while the other partner listens, the bandwidth seized during a call is only really used in one direction (speaking station -> listening station). In the other direction (listening station -> speaking station), only ambient noise and “silence“ are transmitted. Voice activity detection makes use of this knowledge, interrupts the data transmission and drastically reduces the data rate as soon as silence is detected. As soon as voice activity is detected again, transmission for that direction is immediately re-established (with full bandwidth).

If NOTHING is transmitted on a route, the receiving end generally tends to identify the absence of background noise as line failure and therefore as undesirable. Therefore, depending on the codec used, highly compressed background noise is sometimes transmitted or noise is supplied.

The problem with VAD is the difficulty in distinguishing between *ambient noise* and *silence* in transmission. Ambient noise in the room should fall under the category of *silence*, but softly spoken words should be categorized as *voice*. The impairment (or in the worst case, truncation) of the beginning or end of voice activity in the transition area is unavoidable.

Linking is also a problem with VAD. Using VAD on multiple transmission paths in succession can increase impairment effects. The linking of transmission paths with VAD must therefore be avoided.

The resulting bandwidth reduction is in the range of 50% to 75%.

The VAD classmark is deactivated by default, but can be activated at any time for voice connections.

IMPORTANT: VAD must not be activated in the case of fax, modem and digital data connections!

2.4.4 Comfort Noise Generation (CNG)

The HG 35xx gateways support **CNG** (**C**omfort **N**oise **G**eneration).

While using VAD, the DSP at the destination emulates background noise from the source side, preventing the perception that a call is disconnected.

2.4.5 Echo Cancellation

The HG 35xx gateways support on board **echo cancellation** (performed on the on-board DSP modules) compliant with the ITU-T G.168 standard.

More detailed information on echo cancellation

Echo arises at all analog 2-wire/4-wire hybrids, e.g. in the hybrid coil of an analog telephone, as well as through acoustic over-coupling of speaker and microphone in the recipient's handset.

If the runtime between the generation of an audible signal and the manifestation of the echo at the speaker (Round Trip Delay) is very slight, the echo has no interfering effect. However, the greater this runtime, the greater the disturbance of the echo. The runtimes in the case of IP transmission are very high. Thus, echoes are always perceived as extremely disturbing. Therefore, it is important that all signals are free of echo prior to being transmitted in the IP network. The resulting effects of delay and echo are explained in detail in Section 1.6.2, "Delay and Echo".

Echo cancellation suppresses the echo by filtering it out of the data stream. Echo cancellation should always be used as close to the source of the echo as possible.

The following example is intended to clarify this:

- Subscriber A is connected to Subscriber B via an IP route.

- The terminal device of Subscriber B generates an echo of the signal of Subscriber A.
- The echo is to be suppressed near the source, i.e. in the vicinity of Subscriber B, so that the signal from B to A is free of echo before being transmitted across the IP route.

Echo cancellation (echo suppression) is a very complex operation in digital signal processing, which only has a minimal effect on the transmitted wanted signal (without echo).

Echo cancellation is configured automatically for all circuits, but can be deactivated.

Analog modems and fax machines use complicated phase modulation procedures for data transfer which can be affected by interference caused by echo cancellation.

2.4.6 Redundant LAN Interface

The feature “Redundant LAN Interface” described in the document "IP Distributed Architecture (IPDA)” Chapter 6, “Information for network administrators” is generally supported. However, if the WAML function is configured, this feature is not supported.

2.4.7 Security

2.4.7.1 Access for Administration

Authentication methods are used for access to administration.

In order to protect all files and debug info on the HG 3500, access is only possible via https and SSH.

2.4.7.2 Access to SNMP

The access to SNMP is restricted via read and write Community strings. These Community strings can be configured with the **WBM > Maintenance > SNMP > Communities**.

2.4.7.3 Security in CorNetTC Registration

The log-on between the IP phones and HG 3500 is secured via SHA1. The payload and signaling connections are not encrypted.

2.4.7.4 Connecting IP Gateways to the Internet or via External Providers

The connection of IP gateways to the Internet or external providers reveals a security vulnerability ("insecure" LAN/WAN). An IP or MAC address filter must be set to combat this problem. This can be done via the board's WBM.

WBM > Configuration > Security > MAC Address Filtering or **WBM > Configuration > Security > IP Address Filtering**.

For a detailed description, see "OpenScape 4000 V, Gateways HG 3500 and HG 3575, Administrator Documentation" ().

2.4.8 Resource Manager (RM)

IMPORTANT: The Resource Manager is released for use in standalone systems with HFA and IPDA.

In a real, complex IP network the available bandwidth is typically not uniform in all sectors.

The Resource Manager (RM) can administer and monitor the bandwidth for up to 800 sectors in a given IP network.

The RM updates a cluster matrix whenever a call is setup or torn down. The matrix allows determination whether there is a resource shortage in any of the involved sectors. Based on the configured bandwidth and the actual bandwidth a call is either allowed to complete or rejected.

The RM calculates real bandwidth, taking compression settings, DMC, FAX, etc. into account.

For more information on the resource manager please refer to Chapter 16, "Resource Manager Functionality".

2.4.9 Restrictions

2.4.9.1 Loadware-Update or Reset of the Board

Problem description:

An HG 3500 is configured as a SIP trunking gateway. The parameters for the connection to the Web Based Management of the board (AMO CGWB, parameter **MGNTIP** and **MGNTPN**) and the backup server (AMO CGWB, parameter **BUSIP** and **BUSPN**) have to be configured.

After a reset of the board or after a loadware update the IP addresses (**MGNTIP** and **BUSIP**) are restored but not the port numbers (**MGNTPN** and **BUSPN**). These parameter values are set to the default value (in both cases „0“). Therefore a connection to the backup server cannot be established anymore. The needed configuration data for SIP trunking that has been configured in the WBM and has been saved on the backup server cannot be restored. The SIP trunking connection cannot be re-established again.

Solutions:

Check parameter in AMO CGWB and configure it again:

```
CHANGE-CGWB:MTYPE=CGW,LTU=<number>,SLOT=<number>,TYPE=MGNTDATA,MGNTPN=8000,BUS►
PN=443;
```

Or save the configuration data in the local flash of the board during installation of the board:

WBM > Maintenance > Config & Update > Save Local Configuration for Upgrade

For a detailed description, see "OpenScape 4000 V, Gateways HG 3500 and HG 3575, Administrator Documentation" ().

2.4.9.2 Possible IP hops

IMPORTANT: More than 3 IP hops can lead to restrictions in a Voice over IP system, i.e. the delay can be too long and the result is poor speech quality or malfunctioning features.

2.5 Load Concept for Gateway Boards

2.5.1 Important Information

- This chapter only describes how to update the loadware for gateway boards.
- To update the system as a whole, use the conventional OpenScape 4000 Assistant features Software Transfer and Software Activation.
- To minimize system downtime, you can upgrade the gateway boards first with the load concept described in the following sections and afterwards upgrade the system with the Software Transfer and Software Activation functions.
- The STMIX/STMIY Hardware board Software supply is via HTTPS only.

2.5.2 Notes on IP Gateway Loadware

- Although you can store two loadware images on the IP gateway HG3575, only one of these is the "golden load" that is loaded after a cold start (power off).
- Loadware ID check
- A loadware ID check is performed every time the HG3575 is started and compares the board loadware that is being downloaded with the loadware version on the hard disk (:PDS:APSP/LTG/LGA0/PZKNCI40).

  If the result of the check is negative, that is, if there is a discrepancy with the loadware stored on the HD, then the loadware is transferred from the HD to the NCUI via FTP and then installed/restarted.
- Installation of NCUI loadware (PZKNCUI40)

- A NCUI loadware (PZKNCUI40) loaded/transfered in the background will be installed with a warm boot.

  This warm boot can be started with the following actions/events:

  – Deactivate/activate with AMO USSU (`DEACTIVATE-USSU/ACTIVATE-USSU`).
  – Restart of the access point with `EXEC-USSU:UPDATAP,<ap-number>;`. New configuration data will be loaded to the access point and a warm boot will be initiated.
  – New startup after loadware transfer (initiated through negative LW ID check during startup).
  – after connection failure in TCP (**ALVTIME**).
- Golden loadware check
- In HG 3575, the latest loadware to be downloaded is called "golden loadware" (as-delivered NCUI2+/NCUI4 boards include loadware in the flash memory).

  The golden loadware check is always performed after new loadware is downloaded/restarted (loadware upgrade/loadware ID check negative). If this check is successful, the download pointer is rewritten as appropriate so that the golden loadware corresponds to the new loadware.

2.5.3 Load Concepts

Load concept for HG 3500/HG 3575

- The loadware for HG 3500/HG 3575 is loaded via HTTPS (see Section 5.4, “Updating Loadware with Web-Based Management” and Section 5.5, “Updating Loadware with "LW Update Manager"”).
- Loadware can be loaded in the background during normal operation, that is the activation of new loadware can be delayed (until off-peak hours). The new loadware should nevertheless be activated as quickly as possible to avoid problems.
- Optimized loading for HG 3500 gateways
- As the common gateway development has combined the software of all previous gateways (HG 3530, HG 3540, HG 3550 and HG 3570) in a single software/loadware package, the size of the software has increased accordingly. This has increased the loading time to approximately 15 minutes. The load concept for STMI loadware was adapted in response to this change.

  There are two CGW-STMI2 boards and two CGW-STMI4 boards. These boards all have a different HW ID but have the same loadware file.The optimized methodology for CGW-STMI boards means that the loadware file is only downloaded once for these boards, even if they have different HW IDs.

  This results in the following implementation scenarios:

  – Configuration featuring both STMI4 types and an STMI2 type => loadware file is only transferred once and then distributed to all corresponding boards.

– Configuration featuring both STMI2 types present => loadware file must be transferred twice because the STMI2 firmware can no longer be modified.

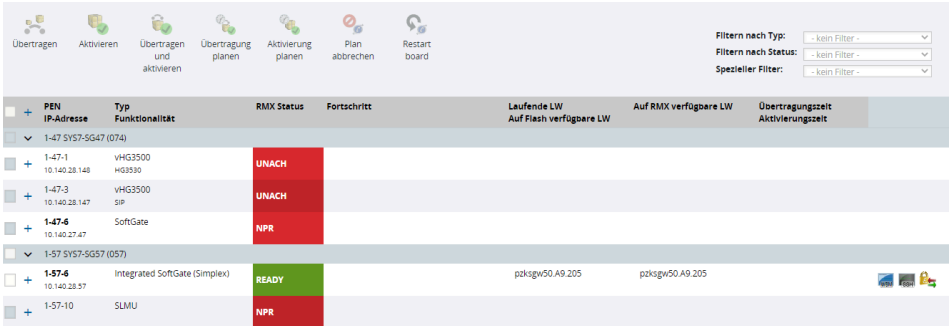
STMI4 boards must have at least the firmware **STMI4_FW_070725** in order to use the optimized load concept for the different CGW-STMI boards.

IMPORTANT: Starting with V10R0 the support for STMI2 will not be offered anymore. The replacement for STMI2 is STMIX/ STMIY.

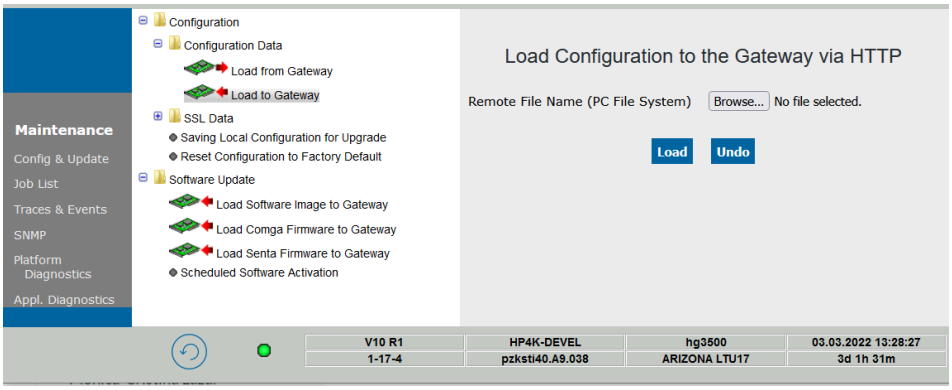
2.5.4 Updating Loadware with Web-Based Management

IMPORTANT: Disadvantage You can only upgrade one IP gateway board at a time.

- To use this option, log on to OpenScape 4000 Assistant and select **Expert mode > Gateway Manager.**

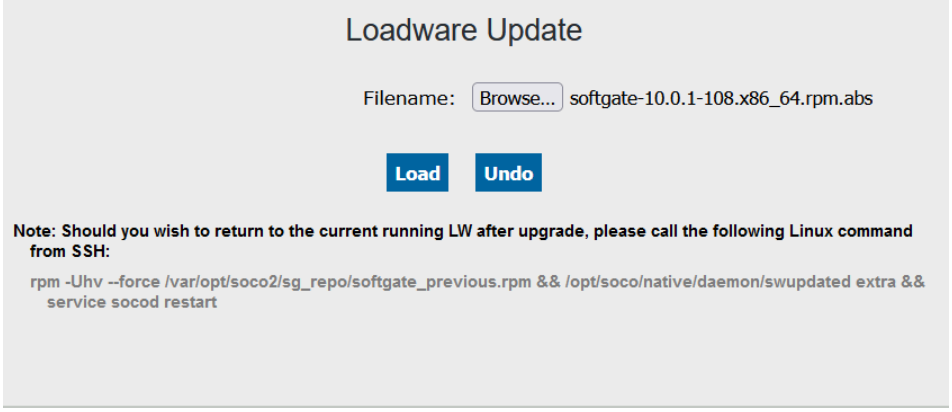


- Now select the required board and click the link **WBM**. WBM for HG 35xx now opens.
- Now select **Maintenance > Config and Update > Software Update > Load Software Image to Gateway**
- Select **Load via HTTP**.



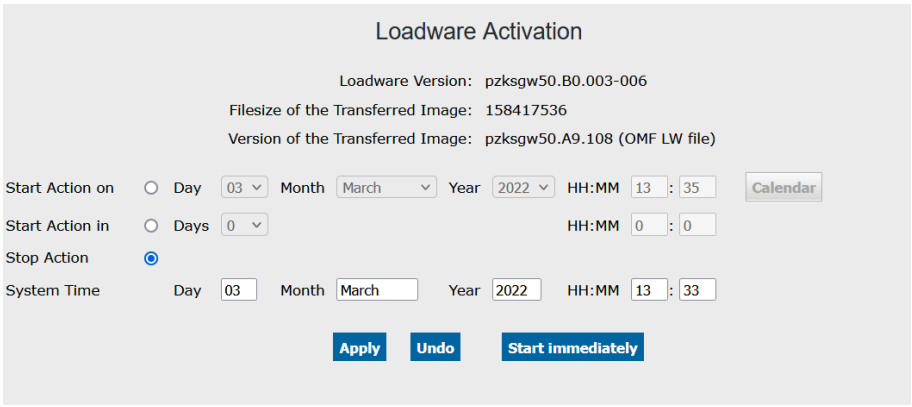
- In the field **Remote File Name (PC File System)** you must enter the software (loadware) saved previously on your PC. This is performed using the **Browse** button.
- Now select the **Load** button to start loading. Loading can take up to five minutes. The loadware is saved in the flash memory of the board.

IMPORTANT: The LAN must be connected but the IP gateway must not be rebooted during the load operation (AMO USSU, AMO BSSU).



- Activate (decompress and install) the loadware.
- Activation (loadware decompression and installation) now takes less than five minutes.

  You can activate the software (loadware) immediately with **Activate Now** or use the **Schedule Activation** button to implement time-controlled activation on a particular day.



2.5.5 Updating Loadware with "LW Update Manager"

IMPORTANT: Advantage You can upgrade multiple IP gateway boards at once.

Key features of "LW Update Manager"

- The "LW Update Manager" function lets you upgrade individual boards or all boards supported.
- The LW Update is made up of two parts: Loadware Transfer and Loadware Activation.
- Loadware can be updated immediately or after a delay, that is time-controlled with the scheduler.

Activating "LW Update Manager"

To activate this feature, log on to OpenScape 4000 Assistant and select **Expert mode > LW Update Manager**.

For more information, refer to the online help for the "LW Update Manager" or "Openscape 4000 Assistant V, Loadware Update Manager, Administrator Documentation" on the intranet (http://apps.g-dms.com:8081/techdoc/en/P31003H3440M1450176A9/index.htm).

2.5.6 General Comments on Loading

Download speed

It takes approximately 8.5 minutes to load a CGW-STMI board (excluding miscellaneous restore times). More time is needed in the case of an access point with a slow IP connection (see also "Flow control (TCP)").

Flow control (TCP)

The system performs flow control. If the necessary bandwidth (quality of service) is not available, the process slows down, that is, the speed is dictated by the slowest access point when loading all access points simultaneously.

2.6 Save Configuration Data in Local Flash (local Backup & Restore)

2.6.1 Overview

There are some customer scenarios, where the gateway boards and OpenScape 4000 Assistant are in separated IP-networks (no routing between these two networks) and therefore backup and restore functionality via OpenScape 4000 Assistant is not possible. In these cases the WBM configuration data/certificates can be saved in local flash of the board. Then backup and restore is still possible when connectivity to OpenScape 4000 Assistant backup server is missing or the backup server cannot be reached.

2.6.2 Feature Description

When "Save configuration data in local flash" is activated, a backup file is created on the local flash at the set time of the day (default 03:00).

When "Save configuration data in local flash" is activated, a backup file is created on the local flash whenever data is saved in the WBM. This means that virtually no data is lost any more when loadware is updated via HDLC.

This backup file is only used in the event of a loadware upgrade which is performed per HDLC (with an STMI) or FTP (with an NCUI). If such as upgrade is initialized, the restore is executed using the existing backup file when the new loadware version is started (still in startup - before the gateway status "system ready"). Then a check is made whether the OpenScape 4000 Assistant "Backup and Restore" is reachable or whether a more up-to-date backup is available. This is the case if between 3:00 and the current time a manual or an automatic

backup of the board was created. If there is a more up-to-date backup available on the OpenScape 4000 Assistant "Backup and Restore" and the backup server can be reached, a second restore is carried out.

If the loadware upgrade is done via the loadware manager of the assistant, then the backup file in the local flash (03:00) is not used. In this case a current backup is created in the local flash before the new software is activated with the old load. Then the new loadware version is loaded and started. During startup the backup created shortly before is imported. This ensures that this upgrade with the local backup/restore always contains the latest configuration data. The OpenScape 4000 Assistant "Backup and Restore" must still be contacted to check the backup file. This is important in the case of HFA : Here there is a backup on the OpenScape 4000 Assistant backup server with the same IP address but old MAC address which then must be imported.

Notes on rebooting

- If the backup is created from the OpenScape 4000 Assistant "Backup and Restore" before the "system ready" status of the board, then there is no additional reboot. If the backup is created after the "system ready" status because the OpenScape 4000 Assistant backup server is not reachable immediately, then the board is automatically rebooted in the case of SPE (because of certificates and MEK).
- The local backup is restored during the startup phase (before the board is operational) and therefore an additional automatic gateway reboot is only necessary in exceptional cases (e.g. SPE certificates available).
- If additionally a OpenScape 4000 Assistant "Backup and Restore" server is configured/present, the currentness of the backup determines applying board data, i.e. restore from the local backup or the OpenScape 4000 Assistant "Backup and Restore" backup. If the OpenScape 4000 Assistant "Backup and Restore" backup is more up-to-date, this can possibly lead to an additional reboot.

2.6.3 Startup Scenarios

Normal restart

Check if the backup server is configured and reachable.

- Backup server is **configured**, **reachable** and **contains a newer version** of configuration data as on the local flash of the board:
- -> Configuration data will be loaded from the backup server. This is normally the case after upgrade over HDLC or exchanging the physical board.
- Backup server is **configured** and **reachable**, but **no backup** with configuration data is stored/found:
- The gateway starts up using its default configuration data. No retry to reach the backup server is executed.
- Backup server is **configured but not reachable**:
- A retry to reach the backup server is executed.
- Backup server is **not configured**.

- The gateway starts up using its default configuration data. No retry to reach the backup server is executed.

  Loadware Update via HDLC

  Same procedures as normal restart. When upgrading via HDLC the board can't have stored the current configuration data to the local flash (TFFS).

  Configuration data is essentially no longer lost when a loadware update is performed via HDLC as a backup file is created on the local flash whenever data is saved in the WBM.

  Loadware Update via OpenScape 4000 Assistant / WBM

  After activating the new loadware the gateway will be automatically rebooted. The new gateway loadware is loaded. The new loadware image loads the previously stored configuration data. The data on the backup server can not be more up-to-date, therefore it is not taken into consideration.

  For more information on the loadware update via OpenScape 4000 Assistant / WBM please refer to Chapter 5, "Load Concept for Gateway Boards".

  Loadware Update via OpenScape 4000 Assistant / WBM: backup server not configured

  Same as „Loadware Update via OpenScape 4000 Assistant / WBM".

  Loadware Update via OpenScape 4000 Assistant / WBM: backup server configured but not reachable (via IP)

  Same as „Loadware Update via OpenScape 4000 Assistant / WBM".

  Loadware Update via OpenScape 4000 Assistant / WBM: backup server configured and reachable, but no backup with configuration data is stored/ found

  Same as „Loadware Update via OpenScape 4000 Assistant / WBM".

  Loadware Update via OpenScape 4000 Assistant / WBM: backup server configured and reachable, but on the backup server an older configuration than the current one is found

  Same as„Loadware Update via OpenScape 4000 Assistant / WBM".

2.6.4 Configuration

The feature will be configured with the WBM of the board.

WBM > Maintenance > Config & Update > Configuration > SSL Data > Saving Local Configuration for Upgrade

2.6.5 Special Use Cases

- Board replacement
- The new board has already a stored backup file in the local flash (but with another functionality than the one that will be replaced).

  Because there is a backup file in the local flash it will be used for restoring the data. But because of the board replacement the MAC address of the

board has changed. Therefore Backup & Restore is contacted to perform a restore with the backup file of the backup server. After the restore from the backup server the correct data is configured on the board. In this case the backup server must be reachable otherwise the board has stored the wrong configuration data.

After the restore the backup of the local flash should be updated with the current configuration data.

- Default configuration (empty data base)
- An empty data base can be configured as follows:

  WBM > Maintenance > Config & Update > Configuration > SSL Data > Reset Configuration to Factory Default ...

  With choosing this option the board will be reseted automatically. During the startup of the board the parameters configured via AMO will be loaded. The WBM parameters will be set to default.

2.7 Loadability of the FPGA on the STMI4/NCUI4 board

It is possible to load the FPGA code on the gateway boards STMI4 and NCUI4.

Usually the FPGA code is supplied with a LW hotfix (or via fix release, minor release, hotfix). There are three files:

- the SENTA file,
- COMGA file for STMI4 and
- COMGA file for NCUI4.

IMPORTANT: The update of the SENTA/COMGA firmware (FPGA code) cannot be done from remote!

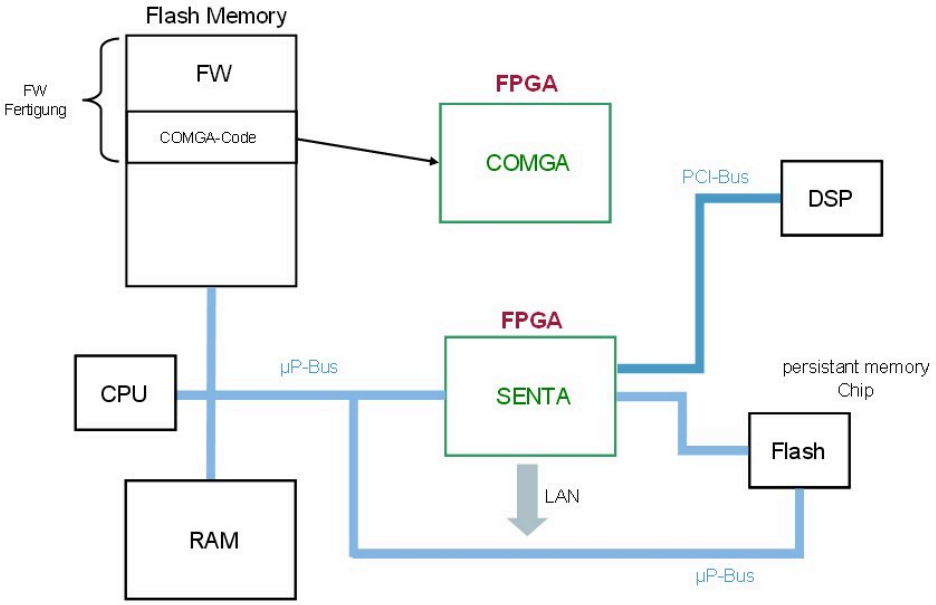


Figure 15: FPGA - Hardware components involved

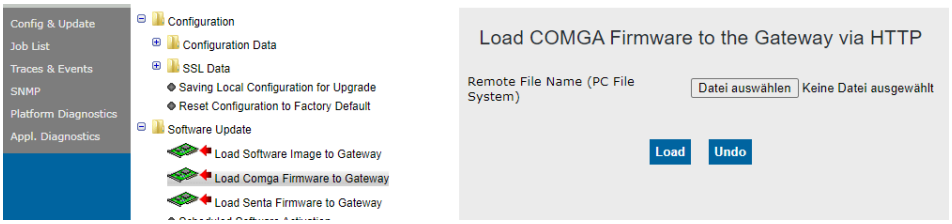
Prerequisite:

The loadware for SENTA /COMGA must be saved via PCHI tool / ftp transfer (**binary**) on the PC. Before the update can be executed, the loadware must be transferred to a PC in the customer's network and which has access to the WBM of the board (WBM client).

Update:

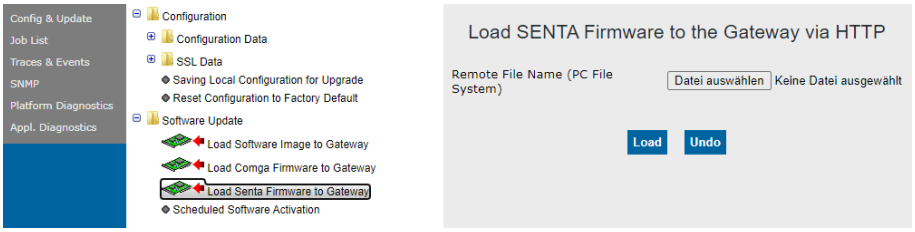
The update of SENTA loadware and COMGA loadware is done via WBM. In the section **Maintenance > Config and Update > Software Update** you have two possibilities:

- **Load COMGA-Firmware via HTTP** or
- **Load SENTA-Firmware via HTTP**.



IMPORTANT: The following description of the firmware update is done for SENTA loadware. For COMGA firmware the instructions are the same but choose **Load COMGA-Firmware via HTTP** from the menu.

1) Choose **Load SENTA-Firmware via HTTP** from the menu.
2) Select the new file of the SENTA loadware from your local PC by pressing the **Browse** button.



3) Press the **Load** button for staring the loadware transfer to the flash memory of the board.
4) Upload process has finished when the following screen appears.

   Confirm with **OK**.
5) Activate the new SENTA firmware by pressing the **Activate now** button.

IMPORTANT: After completion of the activation process the gateway will be rebooted automatically!

6) Confirm the activation process by clicking **OK**.

   The new SENTA firmware will be updated, activated and the gateway will be rebooted.

Trace:

The whole process can be monitored with switched on trace SWCONF, level 9.

The phase of downloading of the SENTA firmware

```
(SWCONF tEmWeb 0x353c4c0 "08/25/2008 15:43:43.688177" cswconfigsvc03.cpp 175)
Creating Job! Type=0x1f001b, ID=3
(SWCONF tEmWeb 0x353c4c0 "08/25/2008 15:43:43.701594" cswconfigsvc03.cpp 377)
Created Job 3
(SWCONF tEmWeb 0x353c4c0 "08/25/2008 15:43:43.702931" cswconfjob02.cpp 3357)
Firmware type: SENTA
(SWCONF tEmWeb 0x353c4c0 "08/25/2008 15:43:43.759732" cswconfjob02.cpp 3419)
First block. Retrieving image header.
(SWCONF tEmWeb 0x353c4c0 "08/25/2008 15:43:43.760800" cswconfjob02.cpp 3429)
 offset |  0  1  2  3  4  5  6  7  8   9  a  b  c  d  e  f |
--------+-------------------------------------------------+-----------------
00000000| B2 00 00 00 04 30 37 2F  31 30 2F 30 38 31 33 3A | .....07/10/0813:
00000010| 30 36 3A 35 34 17 45 4C  46 3E 49 33 38 36 50 5A | 06:54.ELF>I386PZ
00000020| 4B 53 45 4E 30 31 2E 4F  31 2E 30 31 32 00 00 00 | KSEN01.O1.012...
00000030| 00 00 30 00 99 78 70 7A  6B 73 65 6E 30 31 00 00 | ..0..xpzksen01..
00000040| 00 00 00 00 00 00 00 00  00 00 00 00 68 00 00 00 | ............h...
00000050| 00 00 00 00 50 D9 10 00  00 00 00 00 00 00 00 00 | ....P...........
00000060| 00 00 00 00 00 00 00 00                          | ........
(SWCONF tEmWeb 0x353c4c0 "08/25/2008 15:43:43.761791" cswconfjob02.cpp 3652)
Transfer status for job 3 is 1% (11540/1092718)
(SWCONF tBackupTask 0x30622e8 "08/25/2008 15:43:43.774272" cswconfigsvc01.cpp 43
9)
Execute Job in Queue:
    ID = 3, Action=0x1f001b
(SWCONF tEmWeb 0x353c4c0 "08/25/2008 15:43:44.120524" cswconfjob02.cpp 3652)
Transfer status for job 3 is 47% (515348/1092718)
(SWCONF tEmWeb 0x353c4c0 "08/25/2008 15:43:44.497264" cswconfjob02.cpp 3652)
Transfer status for job 3 is 93% (1019156/1092718)
(SWCONF tEmWeb 0x353c4c0 "08/25/2008 15:43:44.590766" cswconfjob02.cpp 3522)
Writing block of 1104096 bytes, remaining 1 bytes
(SWCONF tEmWeb 0x353c4c0 "08/25/2008 15:43:50.465757" cswconfjob02.cpp 3532)
Writing block finished OK.
(SWCONF tEmWeb 0x353c4c0 "08/25/2008 15:43:50.467342" cswconfjob02.cpp 3652)
Transfer status for job 3 is 101% (1104209/1092718)
(SWCONF tEmWeb 0x353c4c0 "08/25/2008 15:43:50.474411" cswconfjob02.cpp 3543)
Got last part of the buffer
(SWCONF tEmWeb 0x353c4c0 "08/25/2008 15:43:50.474737" cswconfjob02.cpp 3552)
Writing remaining buffer: 0 bytes
(SWCONF tEmWeb 0x353c4c0 "08/25/2008 15:43:50.480742" cswconfjob02.cpp 3614)
 offset |  0  1  2  3  4  5  6  7  8   9  a  b  c  d  e  f |
--------+-------------------------------------------------+-----------------
00000000| 70 7A 6B 73 65 6E 30 31  17 45 4C 46 3E 49 33 38 | pzksen01.ELF>I38
00000010| 36 50 5A 4B 53 45 4E 30  31 2E 4F 31 2E 30 31 32 | 6PZKSEN01.O1.012
00000020| 00 00 00 00 00 30 00 00  00 99 78 30 37 2F 31 30 | .....0....x07/10
00000030| 2F 30 38 20 20 31 33 3A  30 36 3A 35 34          | /08  13:06:54
(SWCONF tEmWeb 0x353c4c0 "08/25/2008 15:43:50.481125" cswconfjob02.cpp 3641)
Writing loadware ID finished OK.
(SWCONF tEmWeb 0x353c4c0 "08/25/2008 15:43:50.481718" cswconfjob02.cpp 3652)
Transfer status for job 3 is 101% (1104209/1092718)
(SWCONF tEmWeb 0x353c4c0 "08/25/2008 15:43:50.492219" cswconfigsvc02.cpp 1010)
Progress Response:
    Transferred File Size=1104209
    Complete File Size=1092718
(SWCONF tEmWeb 0x353c4c0 "08/25/2008 15:43:51.596658" cswconfigsvc02.cpp 1010)
Progress Response:
```

```
    Transferred File Size=1104209
    Complete File Size=1092718
(SWCONF tEmWeb 0x353c4c0 "08/25/2008 15:43:55.651796" cswconfigsvc02.cpp 845)
Progress Response:
    Transferred File Size=1104209
    Complete File Size=1092718
(SWCONF tEmWeb 0x353c4c0 "08/25/2008 15:43:57.721041" cswconfigsvc02.cpp 845)
Progress Response:
    Transferred File Size=1104209
    Complete File Size=1092718
The second phase of the process:
(SWCONF tEmWeb 0x353c4c0 "08/25/2008 15:44:22.147227" cswconfjob07.cpp 422)
File info: compressed size: 1104096, uncompressed size: 12491489
(SWCONF tEmWeb 0x353c4c0 "08/25/2008 15:44:23.146807" cswconfjob07.cpp 446)
Uncompression successful
(SWCONF tEmWeb 0x353c4c0 "08/25/2008 15:44:23.147303" util.c 4765)
... writing SENTA FPGA code to SENTA flash
(SWCONF tEmWeb 0x353c4c0 "08/25/2008 15:44:33.140242" util.c 4769)
writing SENTA FPGA code to SENTA flash is still running
(SWCONF tEmWeb 0x353c4c0 "08/25/2008 15:44:43.140240" util.c 4769)
writing SENTA FPGA code to SENTA flash is still running
(SWCONF tEmWeb 0x353c4c0 "08/25/2008 15:44:53.140241" util.c 4769)
writing SENTA FPGA code to SENTA flash is still running
(SWCONF tEmWeb 0x353c4c0 "08/25/2008 15:45:03.140241" util.c 4769)
writing SENTA FPGA code to SENTA flash is still running
(SWCONF tEmWeb 0x353c4c0 "08/25/2008 15:45:13.140241" util.c 4769)
writing SENTA FPGA code to SENTA flash is still running
(SWCONF tEmWeb 0x353c4c0 "08/25/2008 15:45:23.140242" util.c 4769)
writing SENTA FPGA code to SENTA flash is still running
(SWCONF tEmWeb 0x353c4c0 "08/25/2008 15:45:33.140478" util.c 4769)
writing SENTA FPGA code to SENTA flash is still running
(SWCONF tEmWeb 0x353c4c0 "08/25/2008 15:45:43.140469" util.c 4769)
writing SENTA FPGA code to SENTA flash is still running
(SWCONF tEmWeb 0x353c4c0 "08/25/2008 15:45:53.140444" util.c 4769)
writing SENTA FPGA code to SENTA flash is still running
(SWCONF tEmWeb 0x353c4c0 "08/25/2008 15:46:03.140352" util.c 4769)
writing SENTA FPGA code to SENTA flash is still running
(SWCONF tEmWeb 0x353c4c0 "08/25/2008 15:46:13.140249" util.c 4769)
writing SENTA FPGA code to SENTA flash is still running
(SWCONF tEmWeb 0x353c4c0 "08/25/2008 15:46:23.140241" util.c 4769)
writing SENTA FPGA code to SENTA flash is still running
(SWCONF tEmWeb 0x353c4c0 "08/25/2008 15:46:33.140242" util.c 4769)
writing SENTA FPGA code to SENTA flash is still running
(SWCONF tEmWeb 0x353c4c0 "08/25/2008 15:46:43.140244" util.c 4769)
writing SENTA FPGA code to SENTA flash is still running
(SWCONF tEmWeb 0x353c4c0 "08/25/2008 15:46:53.140248" util.c 4769)
writing SENTA FPGA code to SENTA flash is still running
(SWCONF tEmWeb 0x353c4c0 "08/25/2008 15:47:03.140247" util.c 4769)
writing SENTA FPGA code to SENTA flash is still running
(SWCONF tEmWeb 0x353c4c0 "08/25/2008 15:47:13.140245" util.c 4769)
writing SENTA FPGA code to SENTA flash is still running
(SWCONF tEmWeb 0x353c4c0 "08/25/2008 15:47:23.140242" util.c 4769)
writing SENTA FPGA code to SENTA flash is still running
(SWCONF tEmWeb 0x353c4c0 "08/25/2008 15:47:33.140246" util.c 4769)
writing SENTA FPGA code to SENTA flash is still running
(SWCONF tEmWeb 0x353c4c0 "08/25/2008 15:47:43.140245" util.c 4769)
```

```
writing SENTA FPGA code to SENTA flash is still running
(SWCONF tEmWeb 0x353c4c0 "08/25/2008 15:47:53.140244" util.c 4769)
writing SENTA FPGA code to SENTA flash is still running
(SWCONF tEmWeb 0x353c4c0 "08/25/2008 15:48:03.140245" util.c 4769)
writing SENTA FPGA code to SENTA flash is still running
(SWCONF tEmWeb 0x353c4c0 "08/25/2008 15:48:13.140245" util.c 4769)
writing SENTA FPGA code to SENTA flash is still running
(SWCONF tEmWeb 0x353c4c0 "08/25/2008 15:48:23.140245" util.c 4769)
writing SENTA FPGA code to SENTA flash is still running
(SWCONF tEmWeb 0x353c4c0 "08/25/2008 15:48:33.140242" util.c 4769)
writing SENTA FPGA code to SENTA flash is still running
(SWCONF tEmWeb 0x353c4c0 "08/25/2008 15:48:43.140240" util.c 4769)
writing SENTA FPGA code to SENTA flash is still running
(SWCONF tEmWeb 0x353c4c0 "08/25/2008 15:48:53.140243" util.c 4769)
writing SENTA FPGA code to SENTA flash is still running
(SWCONF tEmWeb 0x353c4c0 "08/25/2008 15:48:53.140552" util.c 4771)
programming SENTA flash finished
.....
(SWCONF tEmWeb 0x440e168 "08/29/2008 10:43:37.050407" util.c 3928)
active SENTA version on revision 1: 12
(SWCONF tEmWeb 0x440e168 "08/29/2008 10:43:37.056302" cswconfjob07.cpp 539)
!!! Initializing reboot !!!
(EVTLOG tEvtLogTask 0x36de430 "08/29/2008 10:43:37.058440" cevtlogsvc01.cpp 942)
EventLogEntry from SYSTEM (tEmWeb "08/29/2008 10:43:37.056510" cswconfjob07.cpp
544):
  EventType: Information
  EventCode: MSG_ADMIN_REBOOT
  EventText: Reboot initiated by Admin (Firmware Activation)
Executing Shutdown and Reboot for EvtCode 100 (MSG_ADMIN_REBOOT)
Exiting Security Task*** Shutdown.
Failure:
In the case of failure, a popup window appears in the WBM with an error code.
(SWCONF tFPGAWrite 0x4e39e88 "08/28/2008 15:06:53.579613" util.c 3666)
call of xsvfExecute returned error:2
The activation of the loadware and the reboot of the gateway is not performed.
```

2.8 Standby Board HG 3500

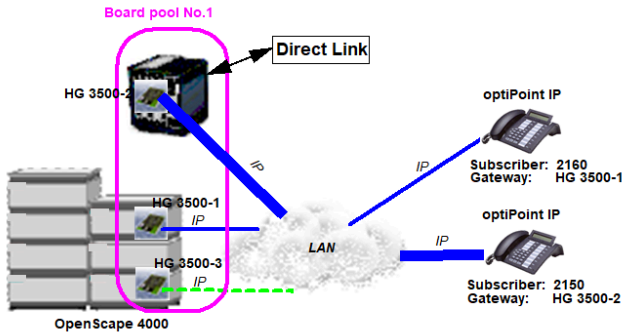
The feature “Standby Board HG 3500” is supported for all common gateway boards. Regardless of the boards configuration as single feature mode or as multiple feature support (MFS).

IMPORTANT: Restriction In case of MFS, only the entire board can be transferred to the standby-board!

2.8.1 Feature Description

This feature is designed to increase the availability of IP terminals (HFA/SIP), IP trunking lines (HG3550) and IPDA function boards (HG3570) in the event of board failure or LAN cable defects. All these features are supported for the Standby Board Feature, either with single feature mode or with multi feature

support (MFS). Basically the Standby Board will overtake all configured features from the Normal board in failure case.



HFA infrastructure

NOTICE: Usage of the "Standby Board HG3500" Feature between STMI2/4 boards together with STMIX/STMIY boards is only restrictively compatible. In case the StandBy Feature (one BPOOL) between STMI2/4 <-> STMIX/STMIY is used and configuration data like SIP Profile Settings, SPE certificates, etc. stored on the e. g. STMI2/4 board these cannot be exchanged to the STMIX/STMIY (and vice versa). Usually the Standby feature uses the Assistant HBR HG3500M backup & restore mechanism (backup sets) to distribute the data to the Standby board in failure cases. Due to the restriction that the backup sets between STMI2/4 to STMIX/STMIY and vice versa are not compatible, this affects the Standby feature for that data. Background information: StandBy boards checks, receives and imports the Assistant HBR set when going in service! in case it is configured in CGGWB and an existing backup set is available... In case you want to use mixed gateways (STMI2/4 with STMIX/STMIY) and you use Assistant HBR for data not stored in the AMO (e.g. trunk profiles, SPE cert, etc.), then you would need to do a manual WBM configuration synchronization to ensure configuration consistency. Optimal solution: Use one BPOOL consisting of only STMI2/4 boards and another BPOOL with only STMIX/STMIY boards.

This is achieved through the introduction of a board. In the event of a board or LAN cable defect, boards can inherit the IP stations or IP trunking lines, etc. assigned to an active board. If appropriately configured, this action can be performed automatically, that is, without manual intervention or use of AMO commands. This is illustrated in the following example which depicts a common gateway with HFA stations.

In the example in Figure 2 HFA infrastructure, the board is the HG 3500-3. If, for example, an HG 3500-1 fails, the IP Phone 2160 will be reconfigured to HG 3500-3 and goes into operation with the new board.

Provided this feature was preconfigured (see below), automatic switchover takes place in the following events:

- When the board is removed without prior deactivation
- Faults on the LAN connection cable. Please note that LAN faults that are located “behind“ routers, hubs or IP switches do not trigger a switchover,

and nor do faults on IP terminal devices. The switchover mechanism is only triggered by a signaled Layer 1 fault, that is, a general cable defect.

- Faults that are detected by the security system and that lead to the DC status “DEF“ (on board level), for example, “Message not transmittable. Exception: a statistic overflow does not lead to a switchover.

The automatic switchover mechanism is not triggered if either the board or hierarchically superior elements (LTU, LTG) are disabled.

The IP terminals go out of operation during switchover and are automatically put back into operation following a successful switchover. The duration of the switchover process is determined by the board data loading time and by timers on the board and in the terminal device. It normally takes between one and two minutes.

Please note that following the switchover operation, the board sends a “gratuitous ARP” (Address Resolution Protocol) request to the LAN on startup so that the MAC address (which has changed with the board) associated with the IP address is updated in the LAN components immediately rather than waiting until the aging timer expires. On the LAN side, take care that the ARP request does not get blocked by any routers that may be involved.

The automatic switchover is signaled at the service terminal. SYSDEP-NMC also receives a message confirming switchover. Designed specially for this purpose is the NMC alarm 36 (PER-BOARD SWITCHOVER). The message at the service terminal is as follows:

```
F5880 M4 N0542 NO ACT   BPA   BOARD    RECONFIGURATION
    06-11-09 10:13:30
      ALARM CLASS:CENTRAL:036
        P101 :LTG1 :LTU3 :055:  0-239:90 Q2316-X10  STMI2/1
    BST:01  PLS:-06
      FORMAT:43
      REASON:00H  BOARD RECONFIGURATION OK
      SOURCE BOARD      : P117:LTG1 :LTU17:097:
      DESTINATION BOARD : P101:LTG1 :LTU3 :055:
```

If the service personnel has replaced the defective board on which the IP stations were originally configured with an intact board, then the IP stations can be configured back in the course of manual startup. The board that took over operation after the defect was discovered resumes its role as board and is ready for switchover in the event of future defects.

Apart from automatically switching IP stations to a board when a defect occurs, this feature also offers manual switchover options that can be implemented with the AMO BSSU. This lets the IP stations maintain their group relationships, which means there is no need for station reconfiguration with the AMO SBCSU, AMO AUN, etc.

The feature must be preconfigured before it can be put into operation. This involves the following steps (for AMO details see Section 8.4, “Generation”):

1) Configure the common gateway board: Both the normal boards (on which the IP stations are configured) and the boards are configured as usual with the AMO BFDAT and AMO BCSU. No distinction is made at this stage between the two functions.

2) Configure common gateway board data: The common gateway boards are normally parameterized with the AMO CGWB. The parameters set here determine whether the board will be used as a normal board with IP stations or as a board. The normal boards must be assigned an IP address (as in

previous configurations), whereas the boards are programmed with no IP address or other parameters.

3) All common gateway boards that want to use the feature must be grouped together in a board pool with the AMO BPOOL. A board pool is administered by means of a pool number and must contain both the normal boards and the boards. Only when this is complete can a normal board switch over to a board in the event of a defect. Please note that following a defect, a pool-based board can only be automatically switched to a board in the same pool. In the case of AMO-activated manual switchover, on the other hand, the board and can be located in separate pools; both boards must, however, belong to a pool (any pool) for this function to work.

4) As usual, the IP stations are configured on the normal boards and put into operation with the AMO SBCSU. Stations cannot be configured on a board.

Besides the functionalities described above, the feature also offers the following functions:

- The following attributes can be set on a pool-specific basis:
  - SINGLE / MULTI

    This setting specifies whether automatic switchover should be performed once (SINGLE) or several times, such as when further defects occur.

    - **SINGLE**

      If SINGLE automatic switchover is configured, further defects do not trigger a switchover to a board, even if there are boards available in the pool. This setting allows stations to be switched back manually after the defective board has been replaced, without having to specify their current location.
    - **MULTI**

      If MULTI automatic switchover is configured, defects continue to trigger switchovers until there are no more boards available in the pool. When switching back manually, you must specify the boards from which and to which the stations should be switched. In other words, you must know or find out the source board and the target board.
  - INFO

    The purpose of this is to provide clarity when operating multiple pools. It may be useful to assign names to pools.

- Trace pool history

  A History field is provided for every board in the pool. The following information can be entered here and read out with the AMO BPOOL:

  – Board (LTU, slot) from which the stations currently configured were switched
  – Board (LTU, slot) to which the stations previously configured were switched
  – Date and time at which the IP stations were switched to or from the board
  – Counter indicating how often the stations currently configured were switched

  This information is available separately for automatic switchover (following a defect) and for manual switchover. The AMO BPOOL can be used to reset the history data (but only for all data simultaneously).

  The history only contains information on the last switchover performed. Only the counters provide information on all switchover stages.

IMPORTANT: For automatic IP station switchover to work, the boards must be in operation (DC status “Ready“) at the time of the defect. The feature is not implemented if a defect is discovered when starting up the board or the system; in this case, an automatic restart is performed. This is necessary for system stability reasons. **Exception**: A detached LAN cable results in a successful start; the later detection of the LAN cable failure activates the automatic switchover as long as a board is available.

2.8.2 User Interface

No particular consequences for telephone users. During the switchover phase, the telephone is “dead“; its display is cleared and reappears as soon as the telephone becomes operational on the new board. Before this point, additional temporary messages such as PBX NOT FOUND may appear on the display.

2.8.3 Service Information

IP station switchover can be likened to a reconfiguration. This means that reconfiguration does not take effect after a system reload unless the static data was written to the hard disk with EXEC-UPDAT:BP,ALL;

IMPORTANT: If a system reload is performed after the IP stations have been switched over to a board and before backing up the database to the hard disk with the AMO UPDAT, the IP stations remain configured on their old board after the reload. If this old board is still defective or has been removed, switchover is not performed because the condition that the board must be in operation at the time of the defect is not satisfied (exception: a defective LAN cable cannot be detected until the board is in operation, and in this case a switchover is performed).

The type branch to **SMODE** was introduced in the AMO CGWB for this feature. **SMODE** describes the common gateway board's mode. **SMODE** mode determines whether a board is configured as a normal board with IP stations, IP address, etc., or whether it is a Standby board.

There are two versions of board's mode:

STBYRDY: Means " Ready" and describes a board that is ready to inherit stations. Normally, the DC status of this board is "Ready" because the board evaluates the mode and sends a positive load acknowledgment to the system in response to STBYRDY". The LAN status can be "Ready" or "DEF". If a board is to serve as a board, both its DC status and the LAN status must be "Ready".

STBYDEF: Means " Defect" and describes a board from which the IP stations were switched on account of a defect. This board cannot serve as a board because its DC target status is "DEF". Normally, the DC status of this board is "DEF" or "NL" if the board is inserted or "NPR" if the board is removed. The loadware that evaluates the mode sends a negative acknowledgment to the system in response to STBYDEF (DEF ON REQUEST).

Boards that are in mode do not have a separate IP address or any board data. The board only receives all the board data (including the IP address) when they are transferred to it from the source (defective) board on switching over the IP terminals. Following switchover, the source board is transformed into a board (for example, STBYDEF), which means it no longer has an IP address. Although the board is physically connected to the LAN, meaning that Layer 1 remains in operation, the higher layers are deactivated. LAN-based access, for example over FTP, Telnet or SNMP, is therefore impossible with a board.

IMPORTANT: Please note that the Ethernet bit rate configured in the board data is also transferred from the source board to the board. The LAN segment to which the board is connected must therefore have the same bit rate as the source board's LAN segment.

The feature is restricted to a single system: cross-system application is not supported.

It is possible, however, to organize the IPDA architecture in such a way that the common gateway boards and boards are randomly distributed over the OpenScape 4000 host system or in the AP (Access Point). In this case, all boards must be connected to the LAN.

IMPORTANT: It is important to note that LAN-based availability is guaranteed so that not only the active board but also the board can reach the IP stations and vice versa. In addition, be sure to trigger the change in mapping of IP address to MAC address with the previously mentioned ARP requests in the LAN components. This "gratuitous ARP" request may not be blocked (e.g. in the router configuration).

We recommend testing the automatic switchover mechanism in the course of initial start to ensure it is in working condition and ready to tackle real defects.

As board data is also transferred in the course of manual and automatic station switchover, restrictions apply if the switchover takes place between

fully configured (for example, Q2316-X10) and partially configured boards (for example, Q2316-X). Please note the following in this case:

- No restrictions apply if the pool only contains boards of the same type, that is, boards that have the same DSP resources and thus the same number of active connections.
- If you are switching from a partially configured board to a fully configured board, then, following switchover, the number of active connections is restricted to the number supported by the partially configured system. You must increase the UDP port range to be able to use all of the fully configured board's resources. Please note that any existing firewalls must be adapted in line with the new UDP range.
- If you are switching from a fully configured board to a partially configured board, then, following switchover, only a reduced number of active connections is possible on the new board, that is, the number supported by the partially configured board. This can lead to frequent blockages in configurations with many stations and high switching loads.

If manually switching the IP stations from a source board to a target board (command: RESTART-BSSU:...,CGWSW=SWITCH,...;), then please note the following points:

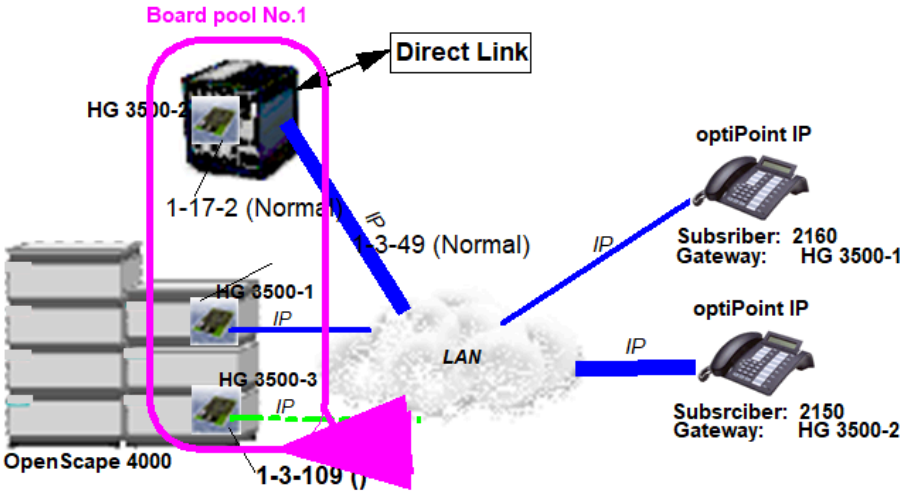
- The target board must be in **STBYRDY** mode and its DC status must be "Ready" (for example, not locked by means of an AMO), and its LAN cable must be connected.
- The source board must not be in mode, that is, **SMODE=NORMAL** must be set. Otherwise, the board can display any DC status - it can even be locked by means of an AMO. If this is the case, the manual lock is transferred to the target board. If the DC status or the status of the source board's LAN connection is "DEF" prior to switchover, **SMODE=STBYDEF** is entered after switchover. In all other cases, **SMODE=STBYRDY** is set, meaning that this board can once again operate as a board.

IMPORTANT: To the extent that it plays a role in the switchover, the LAN connection status (Layer 1) can be queried with the AMO BPOOL. And of course you can use the AMO SDSU as before.

IMPORTANT: To perform a SW update via GW Manager also the STMIX/STMIY StandBy board needs a management IP address (CGWB) and a running interface.

For Software Management functions like LW and OS Update from Assistant it is important to configure the STMIX/STMIY with a management IP address (CGWB) as described under Chapter , "Separate LAN Connectivity for Administration and VoIP".

2.8.4 Generation



In the interest of clarity and to keep things simple, we will not discuss the general configuration of DPLN, LTU, etc. here. However, a list of all common gateway specific commands is provided:

Configure the DIMSU memory for the common gateway boards:

```
ADD-DIMSU:TYPE=SYSTEM,CGW=4;
```

Configure the common gateway boards:

FCTBLK=1 : HG 3500-1

```
ADD-BFDAT:FCTBLK=1,FUNCTION=HG3530,BRDBCHL=BCHL60;
CHANGE-BFDAT:CONFIG=CONT,FCTBLK=1,FUNCTION=HG3530,LINECNT=60,BCHLCNT=30;
CHANGE-BFDAT:CONFIG=OK,FCTBLK=1,ANSW=YES;
```

FCTBLK=2 : HG 3500-2

```
ADD-BFDAT:FCTBLK=2,FUNCTION=HG3530,BRDBCHL=BCHL120;
CHANGE-BFDAT:CONFIG=CONT,FCTBLK=2,FUNCTION=HG3530,LINECNT=120,BCHLCNT=60;
CHANGE-BFDAT:CONFIG=OK,FCTBLK=2,ANSW=YES;
```

FCTBLK=3 : HG 3500-3 (Reserve-Baugruppe)

```
ADD-BFDAT:FCTBLK=3,FUNCTION=STANDBY,BRDBCHL=BCHL60&BCHL120;
```

Assigning a function block to a board:

```
ADD-BCSU:MTYPE=IPGW,LTG=1,LTU=3,SLOT=49,PARTNO=Q2316-X,FCTID=1,FCTBLK=1; /*HG
3500-1
ADD-BCSU:MTYPE=IPGW,LTG=1,LTU=17,SLOT=2,PARTNO=Q2316-X10,FCTID=1,FCTBLK=2; /*HG
3500-2
ADD-BCSU:MTYPE=IPGW,LTU=3,SLOT=109,PARTNO=Q2316-X,FCTID=1,FCTBLK=3; /* board HG
3500-3
```

Configuration of common and global feature board data of the common gateway board. In this example 2 normal and one board will be configured:

```
ADD-CGWB:LTU=3,SLOT=49,SMODE=NORMAL,IPADR=192.16.16.12,NETMASK=255.255.255.0; /
*HG 3500-1
ADD-CGWB:LTU=17,SLOT=2,SMODE=NORMAL,IPADR=192.16.16.10,NETMASK=255.255.255.0; /
*HG 3500-2
```

ADD-CGWB:LTU=3,SLOT=109,SMODE=STBYRDY; /* board HG 3500-3

Load the board data to the boards:

```
RESTART-BSSU:ADDRTYPE=PEN,LTU=17,SLOT=2,WTIME=10;
RESTART-BSSU:ADDRTYPE=PEN,LTU=3,SLOT=109,WTIME=10;
RESTART-BSSU:ADDRTYPE=PEN,LTU=3,SLOT=49,WTIME=10;
```

Configure a board pool with all boards including board(s):

```
ADD-BPOOL:MTYPE=CGW,LTU=17,SLOT=2,POOLNO=1,HOPAUT=SINGLE,INFO="TEST1";
ADD-BPOOL:MTYPE=CGW,LTU=3,SLOT=109,POOLNO=1; /*  Board */
ADD-BPOOL:MTYPE=CGW,LTU=3,SLOT=49,POOLNO=1;
```

Configure the IP stations:

```
ADD-SBCSU:STNO=2150,OPT=OPTI,CONN=IP2,PEN=1-17-2-29, DVCFIG=OP►
TIIP,COS1=5,COS2=6,LCOSV1=11,LCOSV2=12,LCOSD1=21,LCOSD2=22;
ADD-SBCSU:STNO=2160,OPT=OPTI,CONN=IP2,PEN=1-3-49-0, DVCFIG=OP►
TIIP,COS1=5,COS2=6,LCOSV1=11, LCOSV2=12,LCOSD1=21,LCOSD2=22;
```

Reset FUNSU bit to shorten the Reload time of the STMI2 board

```
CHANGE-FUNSU:PIT=FLASH,PARTNO="Q2316-X",FCTID=3,ACTION=RESET;
```

1) Automatic switchover: This is not controlled by AMO commands but rather is triggered when an active board goes out of service.

2) Example prior to automatic switchover:

```
DIS-BPOOL;
H500: AMO BPOOL STARTED
+-------------------------------------------------------------------------------+
| POOLNO = 1                    MTYPE = CGW                    HOPAUT = SINGLE  |
| INFO = TEST1                                                                  |
+-------------------------------------------------------------------------------+
| LTU = 3   SLOT = 49            HOP-AUT-CNT = 0             HOP-MAN-CNT = 0    |
| DC-STATUS = READY             LAN_VERB = READY           SMODE = NORMAL       |
+-------------------------------------------------------------------------------+
| LTU = 3   SLOT = 109           HOP-AUT-CNT = 0             HOP-MAN-CNT = 0    |
| DC-STATUS = READY             LAN_VERB = READY           SMODE = STBYRDY      |
+-------------------------------------------------------------------------------+
| LTU = 17  SLOT = 2             HOP-AUT-CNT = 0             HOP-MAN-CNT = 0    |
| DC-STATUS = READY             LAN_VERB = READY           SMODE = NORMAL       |
+-------------------------------------------------------------------------------+
```

If board 1-3-49 now becomes defective, all board data and all IP stations are switched to board 1-3-109. This provides the following AMO BPOOL output after the switchover:

```
DIS-BPOOL;
H500: AMO BPOOL STARTED
+-------------------------------------------------------------------------------+
| POOLNO = 1                    MTYPE = CGW                    HOPAUT = SINGLE  |
| INFO = TEST1                                                                  |
+-------------------------------------------------------------------------------+
| LTU = 3    SLOT = 49           HOP-AUT-CNT = 0             HOP-MAN-CNT = 0    |
| DC-STATUS = NPR               LAN_VERB =                 SMODE = STBYDEF      |
| SWITCHED AUTTO BRD LTU = 3      SLOT = 109      DATE/TIME : 2003-09-25 18:07  |
+-------------------------------------------------------------------------------+
| LTU = 3    SLOT = 109          HOP-AUT-CNT = 1             HOP-MAN-CNT = 0    |
| DC-STATUS = READY             LAN_VERB = READY           SMODE = NORMAL       |
| SWITCHED AUTFR BRD LTU = 3      SLOT = 49       DATE/TIME : 2003-09-25 18:07  |
+-------------------------------------------------------------------------------+
| LTU = 17   SLOT = 2            HOP-AUT-CNT = 0             HOP-MAN-CNT = 0    |
| DC-STATUS = READY             LAN_VERB = READY           SMODE = NORMAL       |
```

+----------+

Explanation of important abbreviations in the output:

HOPAUT: Automatic switchover between the boards in this pool is permitted once (SINGLE) or several times (MULTI).

SMODE: mode (see Section 8.3, “Service Information”)

HOP-AUT-CNT: Number of automatic switchovers

HOP-MAN-CNT: Number of manual switchovers

DC-STATUS: The board’s DC status (see also AMO SDSU)

LAN_VERB: LAN connection status; READY generally means “LAN cable connected”, DEF means “LAN cable disconnected or defective”. If the field is empty, the LAN connection has a DC status which does not get interpreted by the AMO BPOOL. In this case, the LAN status has no effect on switchover. If this is of interest, you can use the AMO SDSU.

The following history data is only displayed after a switchover:

SWITCHED AUTFR BRD: The IP stations were automatically switched away from this board (for example, on account of a defect) (see also **DATE/TIME**)

SWITCHED AUTTO BRD: The IP stations were automatically switched back to this board (for example, on account of a defect in another board) (see also **DATE/TIME**)

SWITCHED MANFR BRD: The IP stations were manually switched away from this board (with the AMO BSSU) (see also **DATE/TIME**)

SWITCHED MANTO BRD: The IP stations were manually switched back to this board (with the AMO BSSU) (see also **DATE/TIME**)

The history data can be reset with the following AMO command:

CHANGE-BPOOL:MTYPE=CGW,TYPE=HISTRES,LTU=3,SLOT=109;

All functions assigned to board 1-3-49 are now transferred to board 1-3-109, including the board’s IP address and all IP stations. The supplementary information shows the history of the last switching operation. This example shows that on 25.9.2003, a switchover occurred from 1-3-49 to 1-3-103 because board 1-3-49 was removed (DC status NPR).

The counters HOP-AUT-CNT and HOP-MAN-CNT are set for boards with SMODE=NORMAL. All history data is deleted for boards.

3) Manual switchover with the AMO BSSU:

a) The stations switched away from 1-3-49 on account of a board defect should be switched back into service following the repair of 1-3-49:

RESTART-BSSU:ADDRTYPE=PEN,LTU=3,SLOT=49,CGWSW=IPSTNBCK;

or

ACTIVATE-BSSU:LTU=3,SLOT=49,CGWSW=IPSTNBCK;

All IP stations assigned to board 1-3-49 should be switched to board 1-3-109:

RESTART-BSSU:ADDRTYPE=PEN,LTU=3,SLOT=49,CGWSW=SWITCH, LTU2=3,SLOT2=109;

Please note that any AMO lock set will be transferred to the target board (see also Section 8.3, “Service Information”)

A board that is in **STBYDEF** mode because of a defect, for example, and because the IP stations were switched away should resume its board role. This generally occurs after it has been repaired or the board has been replaced. The following command can be used for this:

RESTART-BSSU:ADDRTYPE=PEN,LTU=3,SLOT=49,CGWSW=STBYRDY;

4) Shorten the Reload time of the common gateway board

CHANGE-FUNSU:PIT=FLASH,PARTNO=”Q2316-X”,FCTID=1,ACTION=RESET;

2.8.5 Service steps after the automatic switch over

Two steps can be different after a switch over in case of error:

1) The subscribers which are switched over should get their original pens.

2) In this case the board pool has to be defined as **HOPAUT=SINGLE**!

- Change the defective board resp. reconnect the LAN connection.
- Switch back the subscribers with the AMO command

RESTART-BSSU:ADDRTYPE=PEN,LTU=xx,SLOT=xx,CGWSW=CGWSWBCK;

(xx -> Pen of the board with status **STDBYDEF**)

- Reset the history data of the Board Pool:

CHANGE-BPOOL:MTYPE=CGW,TYPE=HISTRES,LTU=y,SLOT=zz;

3) The subscribers which are switched over should remain on the new pens.

4) In this case the board pool has to be defined as **HOPAUT=MULTI**!

- Change the defective board resp. reconnect the LAN connection.
- Switch the STDBYDEF board to **STDBYRDY** with the AMO command

RESTART-BSSU:ADDRTYPE=PEN,LTU=xx,SLOT=xx,CGWSW=STBYRDY;

2.8.6 Relevant AMOs

AMO	Parameter	Sprache/ Language	Beschreibung/ Description
BCSU	ALARMNR	d	Alarm Nummer
	ALARMNO	e	Alarm number
	BKAN3530	d	Anzahl der B-Kanaele fuer die HG3530 Funktion
	BCHL3530	e	Number of b-channels for HG3530 function
	FCTID	d	Function Id (muss immer 1 sein)
	FCTID	e	Function id (must always be set to 1)
	FCTBLK	d	Funktionsblock-Index (einen beliebigen freien Funktionsblock zwischen 1-20 wählen)
	FCTBLK	e	Function block index (choose a free function block between 1-20)
	LWVAR	d	Index auf Loadware Block der T1 Baugruppe
	LWVAR	e	Index to loadware block for the t1 board
	SACHNR	d	Baugruppensachnummer (2. und 3. Block) Q2316-X, Q2316-X10, Q2324-X500, Q2324-X510
	PARTNO	e	Part numver (2nd and 3rd bloc) Q2316-X, Q2316-X10, Q2324-X500, Q2324-X510
	TYP=IPGW	d	IP Gateway (Common Gateway Baugruppe)
	MTYPE=IPGW	e	IP gateway (common gateway board)
BFDAT	ANZBKAN	d	Anzahl der funktionsbezogenen B-Kanäle.
	BCHLCNT	e	Defines the number of b-channels related to the selected function.
	ANZSATZ	d	Anzahl der funktionsbezogenen Saetze. Mögliche Werte: 1-240
	LINECNT	e	Defines the number of lines related to the selected function.

AMO	Parameter	Sprache/ Language	Beschreibung/ Description
	BGBKAN	d	Block fuer Baugruppe mit 60 und/oder 120 B-Kanaelen
	BRDBCHL	e	Dedicates the block for boards with 60 and/or 120 b-channels
	CONFIG=WEITER	d	Weitere Block-Konfiguration ermöglichen
	CONFIG=CONT	e	continue block configuration
	CONFIG=OK	d	Block-Konfiguration abschließen
	CONFIG=OK	e	Finish block configuration
	FCTBLK	d	Dieser Index beschreibt den Funktionsblock welcher auf dem Common Gateway konfiguriert werden soll. Anhand des Funktionsblocks wird die Konfiguration der benötigten pyhsikalischen Lines (Sätze der Baugruppe) festgelegt.
	FCTBLK	e	This index describes the function block which should be configured on the common gateway board. With that index the amount of needed physical lines (board circuits) is calculated.
	FUNCTION	d	Dieser Parameter legt das Konfigurationsprofile des Common Gateways fest. Dabei muss die eventuell benötigte HG 3570 Funktion als erste angeführt werden. Falls ein bestimmter Line-Bereich für die Funktionen HG 3530 oder HG 3550 vorreserviert werden soll, muss die entsprechende Funktion am Ende stehen und mit dem Wert HG35xxR abgeschlossen sein. Die Funktion kann nur als Einzel-Funktion konfiguriert werden.
	FUNCTION	e	This parameter defines the configuration profile of the CGW board. If HG3570 functionality is used, it must be configured at first position. If a prereservation of a certain line range of functions HG3530, HG3540 or HG3550 is desired, this function must be at the end of the profile just suffixed by the according HG35xxR value. The function can only be configured as single function.

AMO	Parameter	Sprache/ Language	Beschreibung/ Description
BPOOL	ART	d	Art der Pool-Daten: ALLE = Alle Pools löschen ATTR = Pool-Attribut ändern BAUGR = Baugruppe aus Pool löschen HISTRES = Historie der Baugruppe rücksetzen POOL = Einen bestimmten Pool löschen
	TYPE	e	Type of pool data: ALL = Delete all Pools ATTR = Change pool attribute BOARD = Delete board from pool HISTRES = Reset history for a board POOL = Delete a specific pool
	EBT	d	Einbauteilung
	SLOT	e	Slot
	HOPAUT	d	Pool-Attribut für die Hop-Kontrolle beim automatischen Umschalten: SINGLE = nur automatisches einmaliges Umschalten erlaubt MULTI = mehrfaches automatisches Umschalten erlaubt
	HOPAUT	e	Pool attribute for the hop control for automatic switchover: SINGLE = Automatic switchover is allowed only once MULTI = Automatic switchover is allowed several times
	INFO	d	Pool-Attribut: Informationstext
	INFO	e	Pool attribute: Information text
	LTU	d	Line Trunk Unit
	LTU	e	Line Trunk Unit
	MTYP	d	Modultyp, derzeit nur CGW möglich
	MTYPE	e	Module Type, currently onl CGW possible
	POOLNR	d	Nummer des Baugruppen-Rekonfigurations-Pools

AMO	Parameter	Sprache/ Language	Beschreibung/ Description
	POOLNO	e	Number of the Board Reconfiguration Pool
BSSU	CGWSA	d	CGW Schaltauftrag: CGWSWBCK: Rückschalten aller automatisch weggeschalteter IP Teilnehmer auf die Original-CGW-Baugruppe KEIN: Kein CGW bezogener Schaltauftrag STBYRDY: Verwendung als CGW - Baugruppe (Reserve-Baugruppe) UMSCH: Umschalten der IP Teilnehmer der CGW-Baugruppe auf eine andere Baugruppe
	CGWSW	e	CGW switching activity: CGWSWBCK: Switch IP stations back to original CGW board NONE: No CGW specific activities STBYRDY: Act as CGW board SWITCH: Switchover IP stations of CGW board to another board
	LTG2	d	Line Trunk Group der Zielbaugruppe bei CGWSA=UMSCH
	LTG2	e	Line Trunk Group of the destination board of CGWSW=SWITCH
	LTU2	d	Line Trunk Unit der Zielbaugruppe bei CGWSA=UMSCH
	LTU2	e	Line Trunk Unit of the destination board of CGWSW=SWITCH
	EBT2	d	Einbauteilung der Zielbaugruppe bei CGWSA=UMSCH
	SLOT2	e	Slot of the destination board of CGWSW=SWITCH

AMO	Parameter	Sprache/ Language	Beschreibung/ Description
CGWB	SMODE	d	Mode oder Normal Mode **Normal**: Eine Baugruppe im Normal Mode hat gültige Baugruppendaten und normalerweise auch OPTIIPs konfiguriert. **STDBYRDY**: Eine Baugruppe im Ready Mode hat keine gültigen Baugruppendaten, auf diese Baugruppe können OPTIIPs umgeschaltet werden, falls eine andere Baugruppe aus demselben Baugruppen-Pool (AMO BPOOL) defekt wurde. **STDBYDEF**: Eine Baugruppe im Defekt Mode hat ebenfalls keine gültigen Baugruppendaten, diese Baugruppe hat aufgrund eines Defekts seine OPTIIPs und seine Baugruppendaten abgegeben.
	SMODE	e	Mode or Normal Mode **NORMAL**: A board in Normal Mode has valid board data and normally also OPTIIPs assigned to it. **STDBYRDY**: A board in Ready Mode has no valid board data, to this board OPTIIPs can be switched over if another board of the same board reconfiguration pool (AMO BPOOL) becomes defective. **STDBYDEF**: A board in Defect Mode has also no valid board data, this board has lost its OPTIIPs and its board data to another board because it's gone defective.
	IPADR	d	IP Adresse der Common Gateway Baugruppe (Source Adresse)
	IPADR	e	Source IP address of common gateway board
	NETMASK	d	IP-Netzmaske des LAN-Segmentes. Die IP-Netzmaske bestimmt die Grenze zwischen Netz- und Host-Teil in der IP-Adresse. Alle IP-Adressen am LAN-Segment müssen bezüglich des Netzanteils der IP-Adresse gleich und bezüglich des Host-Teils unterschiedlich sein (auch der Default Router muss dieser Bedingung entsprechen).

AMO	Parameter	Sprache/ Language	Beschreibung/ Description
	NETMASK	e	IP net mask of LAN segment The IP net mask determines the network and the host partition of an IP address. All IP addresses of a LAN segment must contain the identical network address part but different host address parts (also the Default Router must fulfill this requirement)
FUNSU	AKTION	d	Ladeart der Baugruppe: Damit der LW Code nicht bei jedem Baugruppen-Reset geladen wird, sollte RESET eingestellt sein.
	ACTION	e	Action set or reset loadware on board: In order to avoid loading of the LW code, it is recommended to set this parameter to RESET.

2.9 DLS Client Bootstrapping

DLS client bootstrapping is a procedure that must be performed once to allow the DLS server to exchange configuration data with the gateway. This procedure generates an individual (DLS) certificate for the gateway and transfers it to the gateway. The gateway and DLS can then use these certificates for unique reciprocal authentication.

2.9.1 Bootstrapping with "No PIN" PIN Mode

Variant A:

1) Create a virtual IP device in the DLS under **IP Devices > IP Device Management > IP Device Configuration**.
2) Contact the gateway in DLS via **IP Devices > IP Device Interaction > Scan IP Devices**. Enter **8084** in the Port field in the **"IP Ranges"** tab.

If everything is in order, the value **Secure** appears in the **Security Status:** field in the DLS under **IP Devices > IP Device Management > IP Device Configuration > "DLS Connectivity"** tab.

Variant B:

1) Create a virtual IP device in the DLS under **IP Devices > IP Device Management > IP Device Configuration**.
2) Enter the IP address of the DLS server at the gateway with the CLI command `set dls ip_address`. The port is usually 18443.
3) Enter the CLI command `contact DLS` at the gateway.

2.9.2 Bootstrapping with "Default PIN" or "Individual PIN" PIN Mode

Variant A:

1) Create a virtual IP device in the DLS under **IP Devices > IP Device Management > IP Device Configuration > "DLS Connectivity"** tab and then select the required PIN mode.
2) Contact the gateway in DLS via **IP Devices > IP Device Interaction > Scan IP Devices**. Enter **8084** in the Port field in the **"IP Ranges" tab**.
3) Enter the CLI command `activate dls pin <pin>` at the gateway with the PIN displayed under 1.

Variant B:

1) Create a virtual IP device in the DLS under **IP Devices > IP Device Management > IP Device Configuration > "DLS Connectivity"** tab and then select the required PIN mode.
2) Enter the IP address of the DLS server at the gateway with the CLI command `set dls ip_address`. The port is usually 18443.
3) Enter the CLI command `contact DLS` at the gateway.
4) Enter the CLI command `activate dls pin <pin>` at the gateway with the PIN displayed under 1

2.10 How to reset an NCUI board

2.10.1 Reasons for resetting the NCUI

- The logon data to the board is unknown and changed from the defaults.
- The board may not boot completely, but the boot menu is still accessible.
- A format of the board is required.

2.10.2 Methods for transferring Loadware

There are two methods for transferring the loadware which will be shown as:

- Method 1: Using a PC on the LAN with TFTP Server
- Method 2: Using a FTP Server (the OpenScape 4000 itself can also be used for this function)

2.10.3 Important Notes

- The resetting of the NCUI board is carried out via the **OpenScape 4000 Expert Access** application (also known as Comwin).
- Use the “Telnet Terminal screen” as the normal dialogue prevents the NCUI's prompts from being displayed correctly. The settings are 38400, 8, none, 1. Check 'End Of Command' (under **Telnet > Parameter > Edit**) is set to **CR** and not **ETX**. Of course other terminal programs can be used.
- When entering commands to the NCUI card it is important to use the correct case as it does make a difference. The lower case “w” will load software

image via FTP and copy to TFFS whereas the upper case “W” will load file via FTP and copy to TFFS.

The output from the NCUI board is shown in `courier` font, manual actions or text inputs are shown in blue.

2.10.4 Process

How to enter the boot menu:

Connect Comwin with the v24 port with the settings above.

Press Reset Button and the following prompts will be observed.

RS232 initialized for Output: 38400,8,n,1

loading FPGA: Load O.K.

testing Checksum Firmware: Test O.K.

testing Data-Bus DRAM: Test O.K.

testing Address-Bus DRAM: Test O.K.

testing Pattern 0x55555555: Test O.K.

testing Pattern 0xAAAAAAAA: Test O.K.

Look for the “stop auto-boot” prompt, then press any key and enter the correct password:

Total TFFS size: 31846400 bytes / free: 17645568 bytes

SW_IMAGE.001 10/18/07 10:03:31

SW_IMAGE.002 05/16/06 13:27:14

Press any key to stop auto-boot...

Boot password: HIPATH4000

[NCUI2 Boot CLI]:

How to format the NCUI board:

(Optional unless login details to the board are not known!)

(Low level format is also optional!)

NCUI2 Boot CLI]: y

Format the flash file system, all files will be deleted.

Do you want to format the flash file system y/[n]? y

Do you want to low-level format the flash file system y/[n]? n

Formatting the flash file system!

Format ok!

[NCUI2 Boot CLI]:

Uploading the software - Method 1: Using a PC on the LAN with TFTP Server

You will need a copy of the NCUI's loadware and make it available to that TFTP server as this is how the NCUI card gets its loadware. The loadware can be found on the system under:

`:PDS:APSP/LTG/LGA0/PZKNCUI20` (NCUI2) or

`:PDS:APSP/LTG/LGA0/PZKNCUI40` (NCUI2+/NCUI4) depending upon the board.

IMPORTANT: There may of course be later versions in SWS.

- Enter lower case to center the following settings (adjust IP addresses as necessary):

[NCUI2 Boot CLI]: c

'.' = clear field; '-' = go to previous field; ^D = quit

boot device : tffs/0 emac

processor number : 0

host name :

file name : SW_IMAGE.002 PZKNCI40

inet on ethernet (e) : 192.168.112.65:ffffff00 */ Change if needed

inet on backplane (b):

host inet (h) : 192.168.111.134

gateway inet (g) :

user (u) :

ftp password (pw) (blank = use rsh):

flags (f) : 0x1000 0x80

target name (tn) :

startup script (s) :

other (o) : emac

- Optionally enter z to save the parameters for another time:

[NCUI2 Boot CLI]: z

Copy content of /tffs/bootline.act into /tffs/bootline.bck.

Write /tffs/bootline.act ok!

- Enter w for the new image to be loaded and additionally the suffix image 001:

[NCUI2 Boot CLI]: w

SW_IMAGE.001 11/28/13 02:29:13

SW_IMAGE.002 11/22/13 08:21:30

Input a new suffix SW_IMAGE.x: 001

You should now see the LW transferring:

Attached TCP/IP interface to emac0.

Attaching network interface lo0... done.

Loading...

1448 bytes

.

.

10270624 bytes

Loading ok.

- Now answer the question with y that the next boot should use this image:

Change bootline to the loaded image

and write bootline to TFFS (y/n)? y

- Finally instruct the card to reboot with @:

[NCUI2 Boot CLI]: @

Uploading the Software - Method 2: Using an FTP Server

NOTICE: The OpenScape 4000 itself can act as the FTP server, as shown in the example below.

Any FTP server can be used and you will need a valid FTP server with the loadware in the root directory of where the FTP client connects. The loadware can be found on the system under:

`:PDS:APSP/LTG/LGA0/PZKNCUI20` (NCUI2) or

`:PDS:APSP/LTG/LGA0/PZKNCUI40` (NCUI2+/NCUI4) depending upon the board.

IMPORTANT: There may of course be later versions in SWS.

IMPORTANT: If using the OpenScape 4000, the loadware will need to be copied into the root directory of: PDS: area. The IP “host inet” must then be the IP of the active CC (meaning CCA or CCB).

- Enter lower case to c enter the following settings (adjust IP addresses as necessary):

[NCUI2 Boot CLI]: c

'.' = clear field; '-' = go to previous field; ^D = quit

boot device : tffs/0 emac

processor number : 0

host name :

file name : SW_IMAGE.002 PZKNCI40

inet on ethernet (e) : 192.168.112.65:ffffff00 */ Change if needed

inet on backplane (b):

host inet (h) : 192.168.111.134

gateway inet (g) : 192.168.112.254 */ Not needed for Direct Link AP

user (u) : hicom */ default user for 4K

ftp password (pw) (blank = use rsh): hipath */ default password for 4K

flags (f) : 0x1000 0

target name (tn) :

startup script (s) :

other (o) : emac

- Optionally enter z to save the parameters for another time:

[NCUI2 Boot CLI]: z

Copy content of /tffs/bootline.act into /tffs/bootline.bck.

Write /tffs/bootline.act ok!

- Enter w for the new image to be loaded and additionally the suffix image 001:

[NCUI2 Boot CLI]: w

SW_IMAGE.001 11/28/13 02:29:13

SW_IMAGE.002 11/22/13 08:21:30

Input a new suffix SW_IMAGE.x: 001

- You should now see the loadware transferring:
- Now answer the question with y that the next boot should use this image:

Change bootline to the loaded image

and write bootline to TFFS (y/n)? y

- Finally instruct the card to reboot with @:

[NCUI2 Boot CLI]: @

2.11 How to reset an STMIX board

2.11.1 General description

The STMIX can be re-flashed in case the board is not booting or not becoming READY in RMX.

The process can also be used to factory reset an STMIX board. All customer saved data will be erased from the board.

Hardware and cabling requirements

- PC or Notebook with Windows OS: A connection must be established between the PC/Notebook and the STMIX board via a LAN cable connected to STMIX LAN1.

  In the example provided in this document the STMIX uses the 192.0.2.101 IP address. It is strongly recommended for the PC to use **192.0.2.100** with netmask 255.255.255.0. Do NOT configure any other IP address on the same interface to avoid issues.

  INFO: It is possible to use a secondary PC network interface if available.

- USB cable, type A to type B cable (e.g. USB printer cable): connect the Windows PC via USB (type A) and the STMIX via USB (type B).
- STMIX in OpenScape 4000, any type shelf: AP37009, AP370013, LTUW, etc.

Software requirements

- DHCP Server + TFTPD Server: e.g. tftpd64.exe from https://tftpd64.software.informer.com/download/

  INFO: Use the 32 bit version in case of 32 bit Windows OS.

- HTTP fileserver: e.g. HFS.exe from https://www.rejetto.com/hfs/?f=dl
- Decompression tool which supports .exe and .gz unzipping: e.g. 7zip.
- SSH client (e.g. Putty) for SSH access to OpenScape 4000 and for COM port access to STMIX via USB port.
- SFTP client (e.g. WinSCP) for downloading files from the OpenScape 400 platform.
- STMIX USB Driver from OS4K Installation ISO: e.g. OS4K_V10_R0.28.0_InstallImage.iso\DriversAndTools \STMIX_USB_Serial_Console_Driver\
- JeOS image for STMIX, generated on the OS4K Linux platform.

  NOTICE: Minimum required OS4K PLT version: V8 R2.22.9 or V10 R0.28.5.

2.11.2 Preparing the necessary files

1) Create a working folder on the PC (e.g. D:\stmix-image-repo) and copy the HTTP fileserver (hfs.exe) and the TFTPD/DHCP server (tftpd64.exe).

NOTICE: The tftpd64.exe file can be either installed or extracted from the installer (using 7-zip) and copied to the working folder. The hfs.exe does not require installation.

2) Connect with SSH to the Platform Linux of any OS4K deployment type (Simplex, Duplex, Survivable, Standalone etc.) and generate the STMIX image with the following command:
`bash /opt/yaps/create_stmix_PXE_boot_image.sh`

   The result will be saved on the OpenScape 4000 Platform Linux, under the following path: /stmix-image-repo.
3) The generated files must be copied to the working folder created on the PC (D:\stmix-image-repo) via SFTP client.
4) Select and right-click on the .pxeboot file, then choose 7-Zip "Open archive" option. Now double click and open the shown .tar.gz file.
5) Extract the contents using "Extract" option (or drag drop the folder contents) to the working folder (D:\stmix-image-repo).
6) The working folder should now contain the following files:

```
STMIX_JeOS_SLES11_SP4.x86_64-V10_R0.28.0.tar.gz
STMIX_JeOS_SLES11_SP4.x86_64-V10_R0.28.0.tar.gz.md5
STMIX_JeOS_SLES11_SP4.x86_64-V10_R0.28.0.tar.gz.pxeboot
pxelinux.cfg\default
initrd
menu.c32
pxelinux.0
vmlinuz
hfs.exe
tftpd64.exe
```

INFO: A folder with Paxheaders may also be generated, but it can be ignored.

NOTICE: The file " D:/stmix-image-repo/pxelinux.cfg/default" is preconfigured for the network 192.0.2.0/24. If the default values are not used, the file must be edited in order to match the IP configuration.

2.11.3 Tool configuration for flashing

NOTICE: It is recommended to run the tools as administrator. Otherwise, the settings may not be saved.

Tool configuration:

1) Run the webserver hfs.exe file:

   Menu -> Add files

   Select and open the following files from the "D:/stmix-image-repo" folder:
   `STMIX_JeOS_SLES11_SP4.x86_64-V10_R0.28.0.tar.gz`

STMIX_JeOS_SLES11_SP4.x86_64-V10_R0.28.0.tar.gz.md5

Menu -> IP Address

Select the IP address used on the interface connected to the STMIX LAN port (e.g. 192.0.2.100).

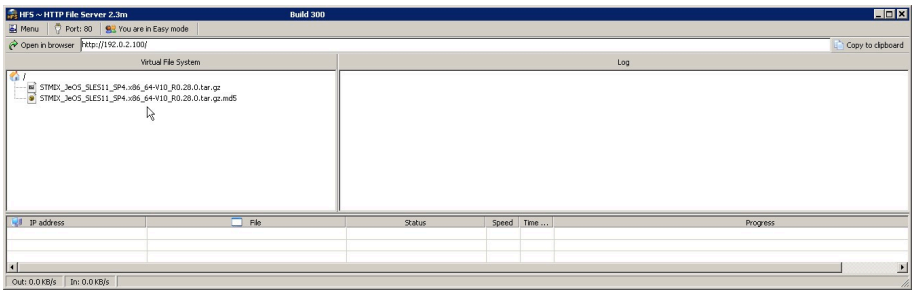


Figure 16: IP settings for hfs.exe

2) Run the tftpd64.exe. Make sure the following settings are in place:

- **Current directory**: D:/stmix-image-repo

  Server interfaces: select the interface connected with the STMIX

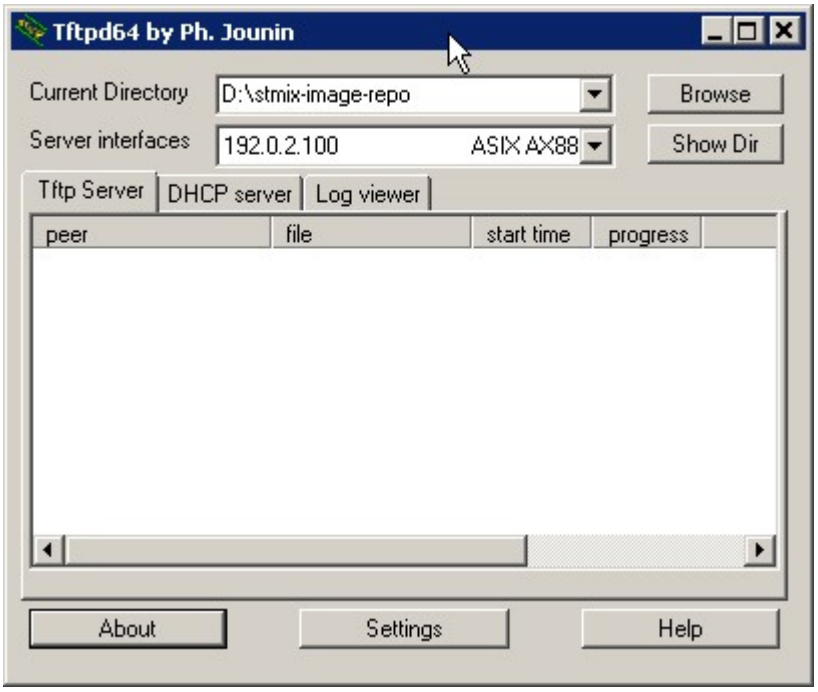


Figure 17: Settings for tftpd64.exe

- **Under the GLOBAL tab ensure:**
  - The “TFTP Server” box is checked.
  - The “DHCP Server” box is checked.

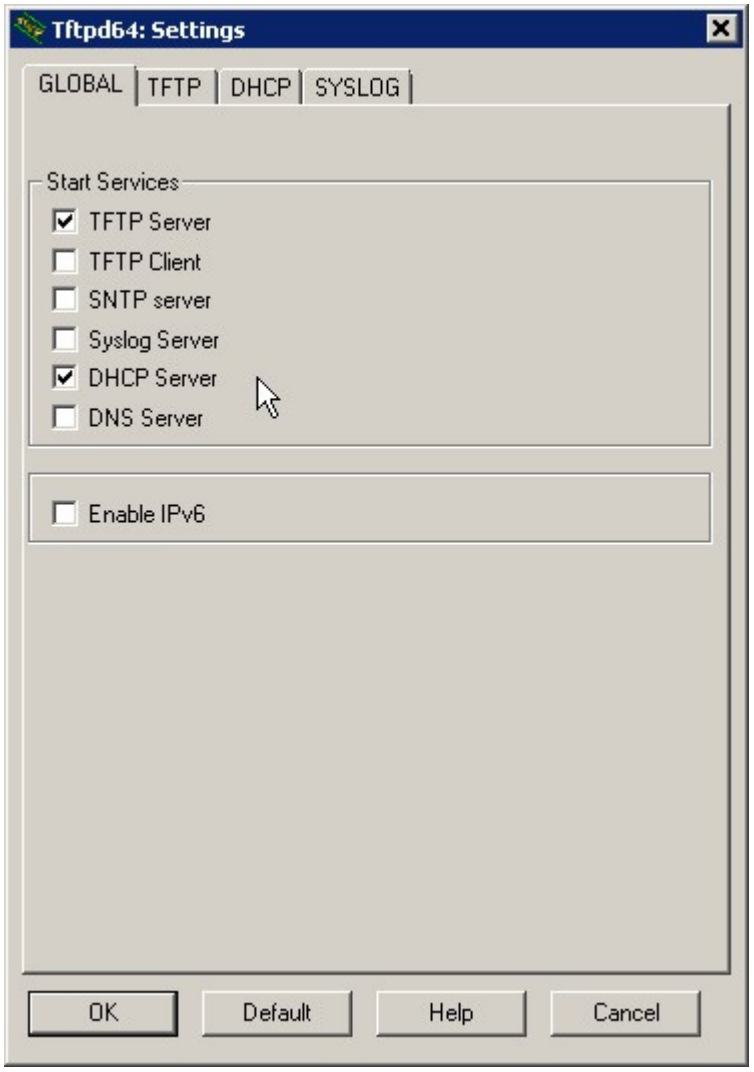


Figure 18: GLOBAL settings for tftpd64.exe

- **Under the TFTP tab ensure**:
  - The Base Directory is set to "D:/stmix-image-repo".
  - The "PXE Compatibility" box is checked.
  - The "Bind TFTP" box is checked and the IP address of Windows PC Lan interface connected to STMIX is selected from the drop down menu.

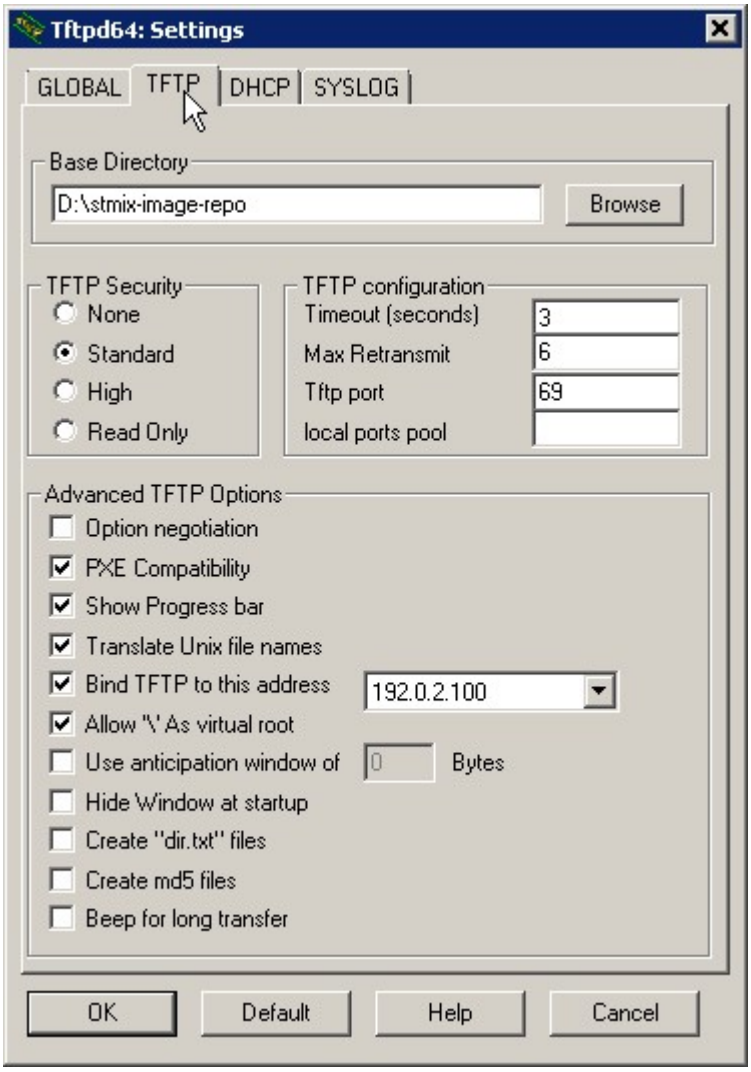


Figure 19: TFTP settings for tftpd64.exe

- **Under the DHCP tab ensure**:
  - IP pool start address: IP Address of STMIX (e.g. 192.0.2.101)
  - Size of pool: 1
  - Boot file: pxelinux.0
  - Mask: 255.255.255.0
  - Persistent leases: box must not be checked
  - Bind DHCP to this address: IP of Windows PC LAN interface connected to the STMIX (e.g. 192.0.2.100)

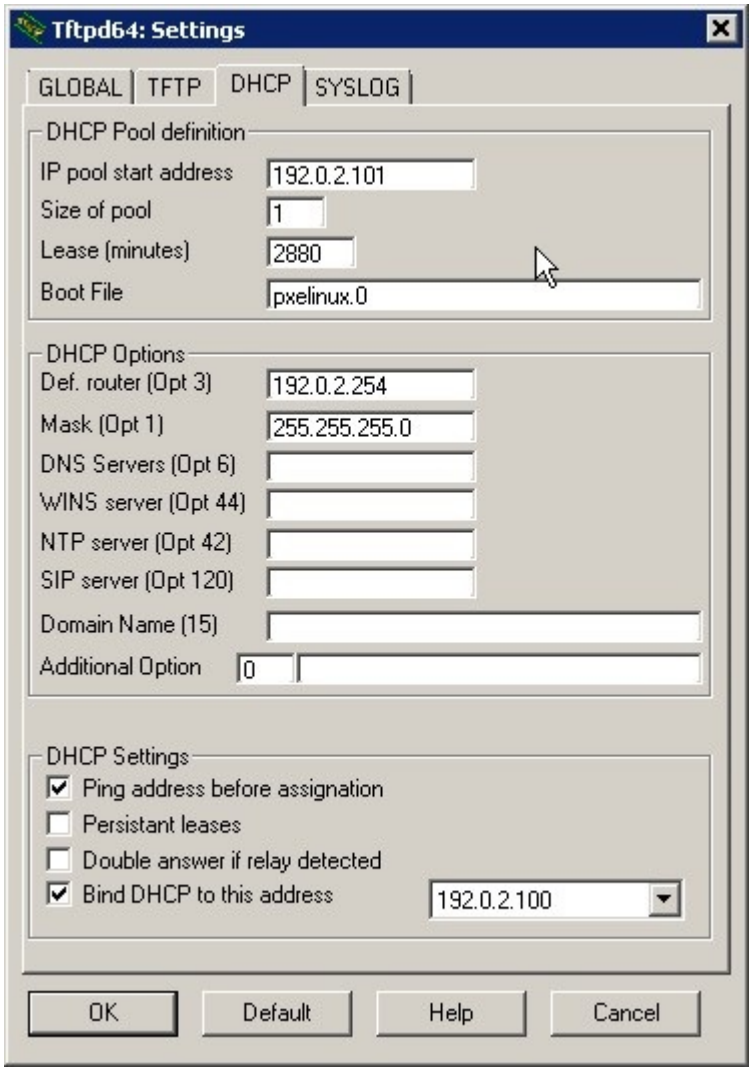


Figure 20: DHCP settings for tftpd64.exe

IMPORTANT: After proceeding with the above steps, exit and restart the tfdtp64 tool to initialize the configured settings.

2.11.4 STMIX USB configuration

USB Terminal

Install the STMIX USB driver on the Windows PC.

With the USB cable connected and the STMIX board powered on, identify the COM port allocated to the STMIX in the Device Manager of Windows PC:

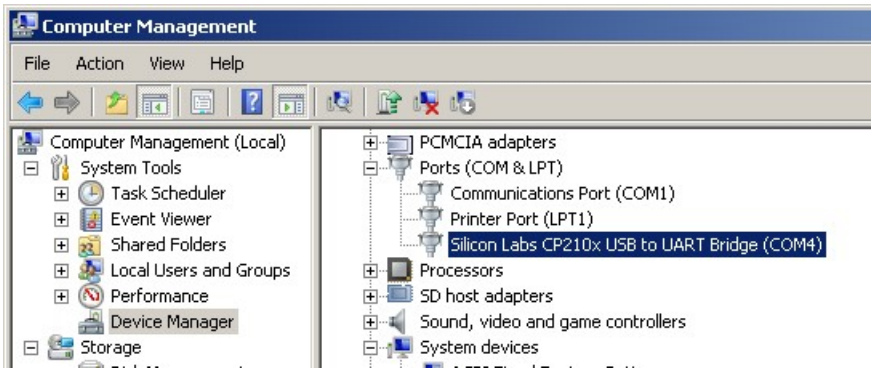


Figure 21: Device Manager, COM port

Configure in Putty a new connection for the identified COM port. The Serial port should be configured with "115200", "8", "1", "None", "None" values.

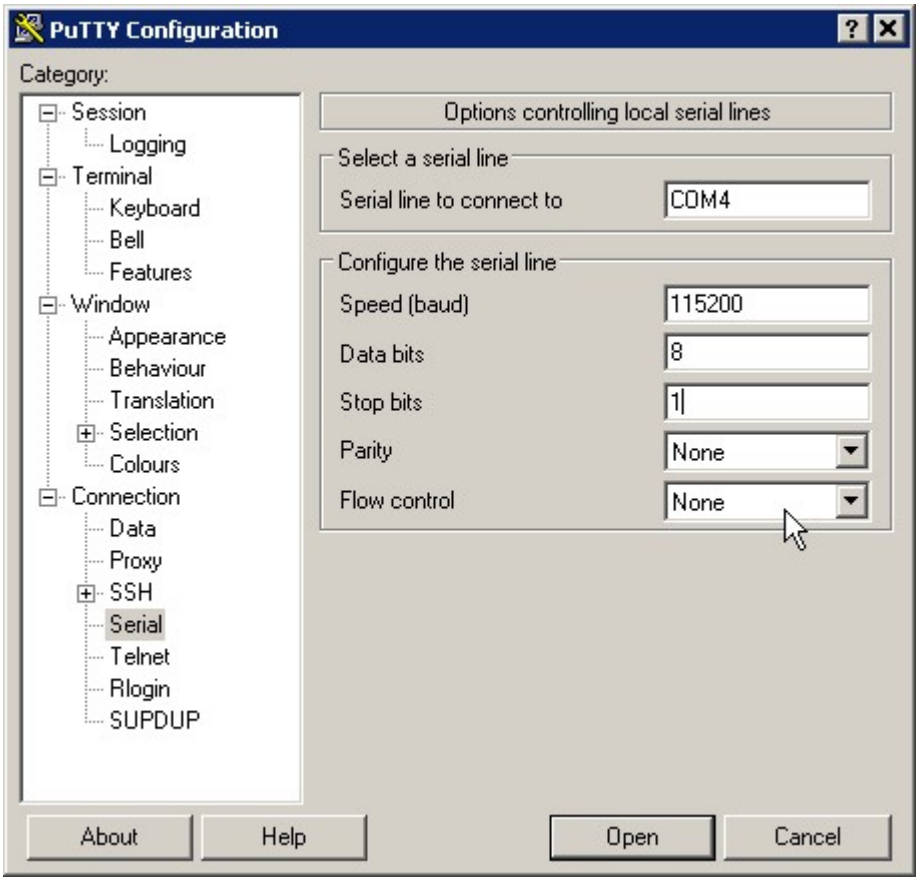


Figure 22: PuTTY configuration

The Keyboard should be set to type "Linux", shown under “The Function keys and keypad”.

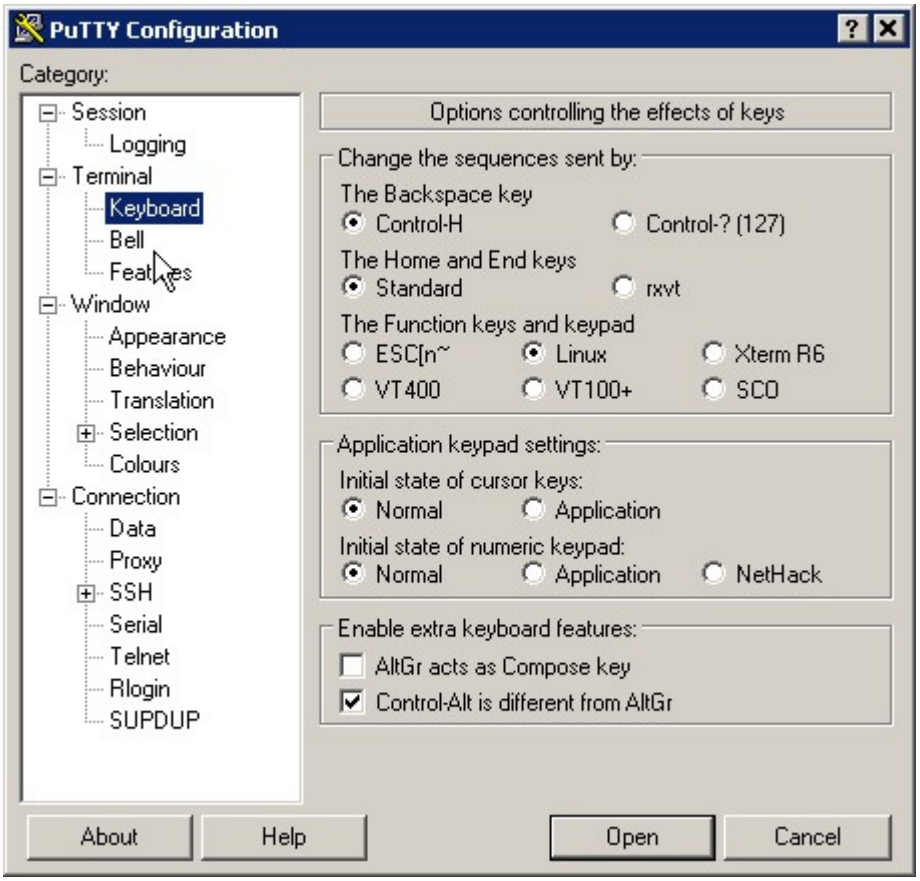


Figure 23: Settings for the keyboard

Save the session. You can now connect to the STMIX USB-COM. The username is TRM and the password is as configured in AMO CGWB.

2.11.5 STMIX re-flash

1) Reboot the STMIX via SSH or power cycle the card via re-plug.

2) Ensure the STMIX BIOS settings.

In the terminal you will see the STMIX booting. Immediately press ESC or DEL to access the BIOS Setup.

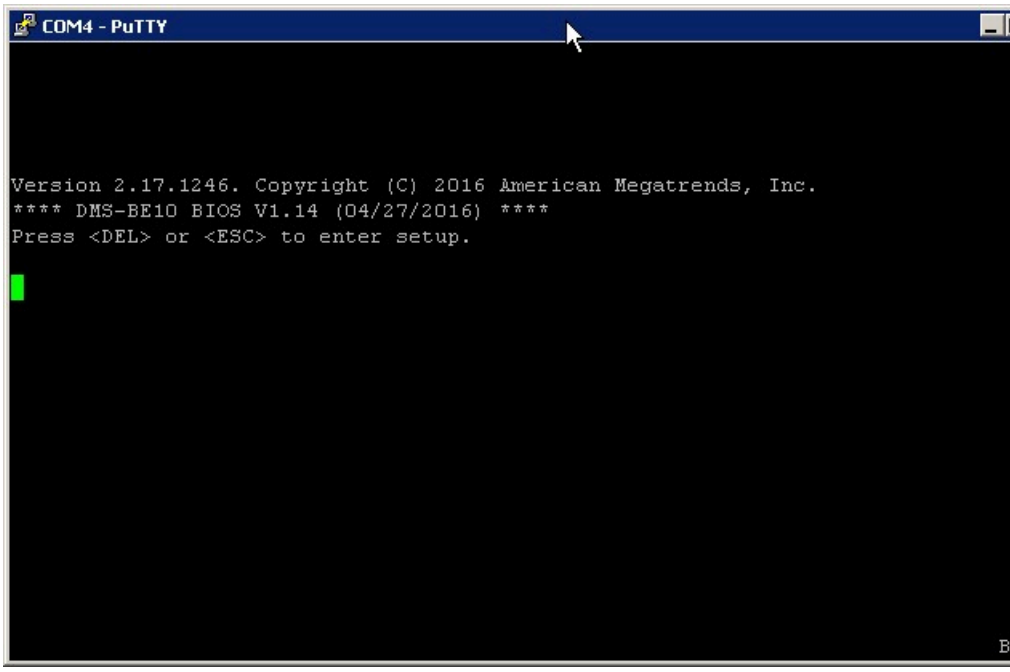


Figure 24: Reset STMIX via PuTTY

In the Save & Exit section go to "Realtek PXE" boot option and press Enter.

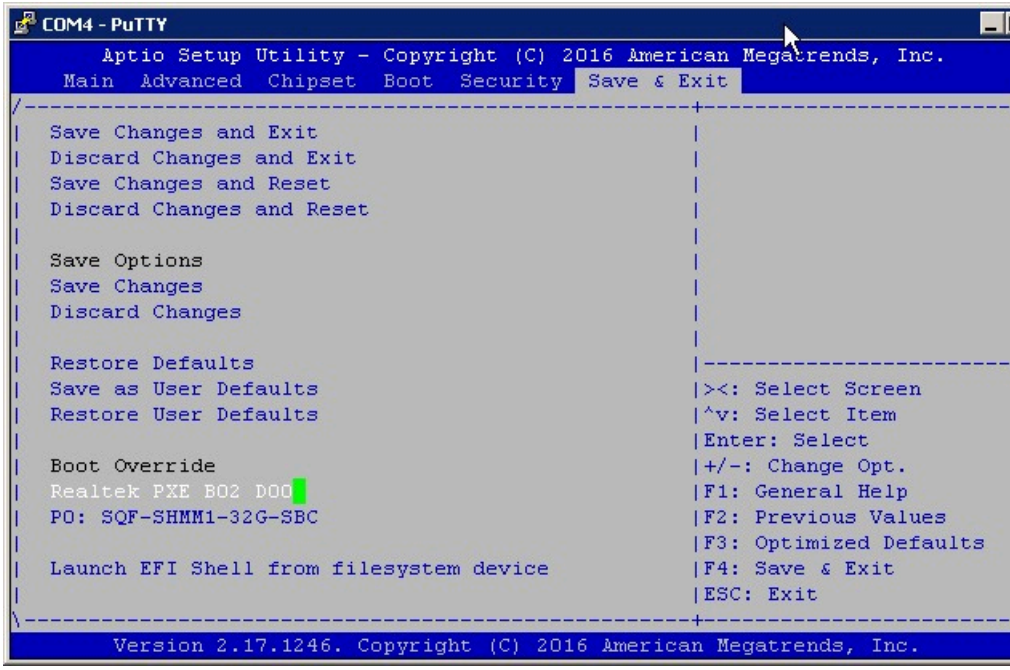


Figure 25: STMIX boot

NOTICE: If there is no option for "Realtek PXE" boot, first enable it under **Chipset -> South Bridge -> Lan1 Option-ROM -> Enable -> Save**. Exit and start over.

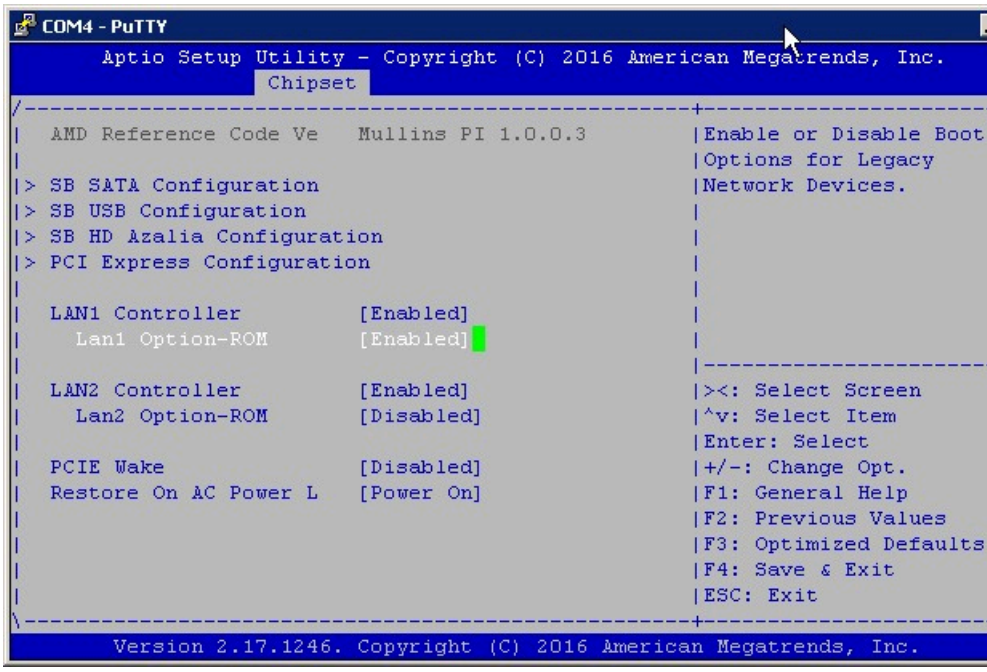


Figure 26: Enable Lan1 Option-ROM

3) Upon boot you will see STMIX PXE Boot in the terminal.



Figure 27: STMIX PXE Boot screen

You should now see in the dhcp/tftpd program popup messages with the allocated IP address and the files loading to STMIX.

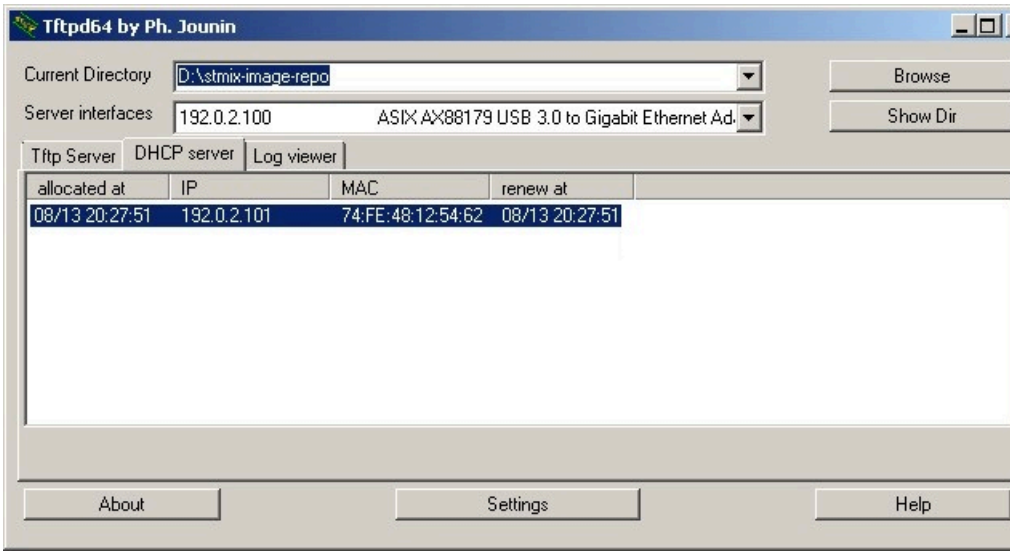


Figure 28: DHCP allocated address

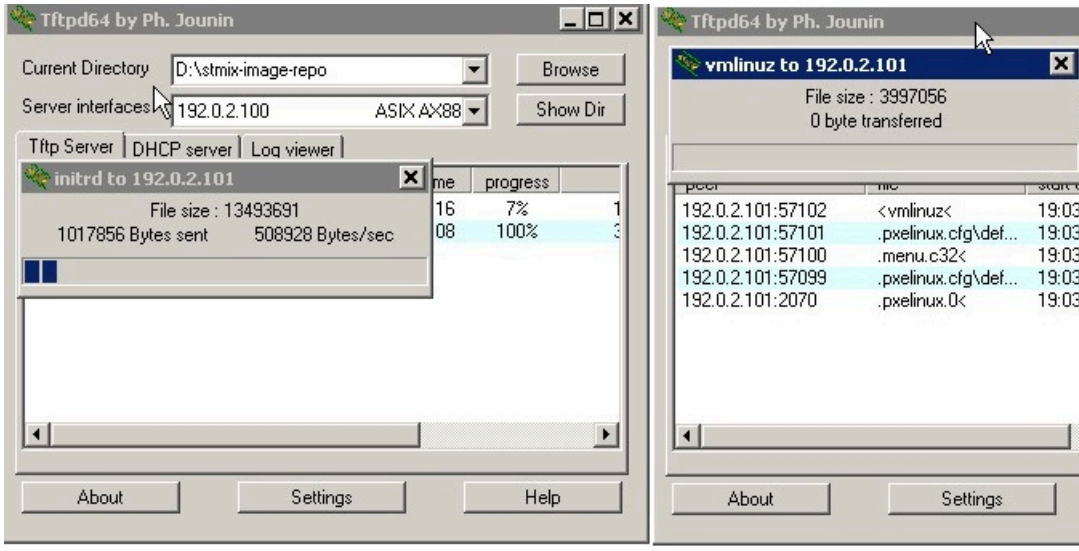


Figure 29: tftpd pop-ups

The output in the STMIX terminal should now show:

- Loading vmlinuz.....
- Loading initrd.....

The loader will be started and will fetch the image. Should see in terminal “Will fetch the following image: http://192.0.2.100/STMIX_JeOS_SLES11_SP4.x86_64-V10_R0.28.0.tar.gz”

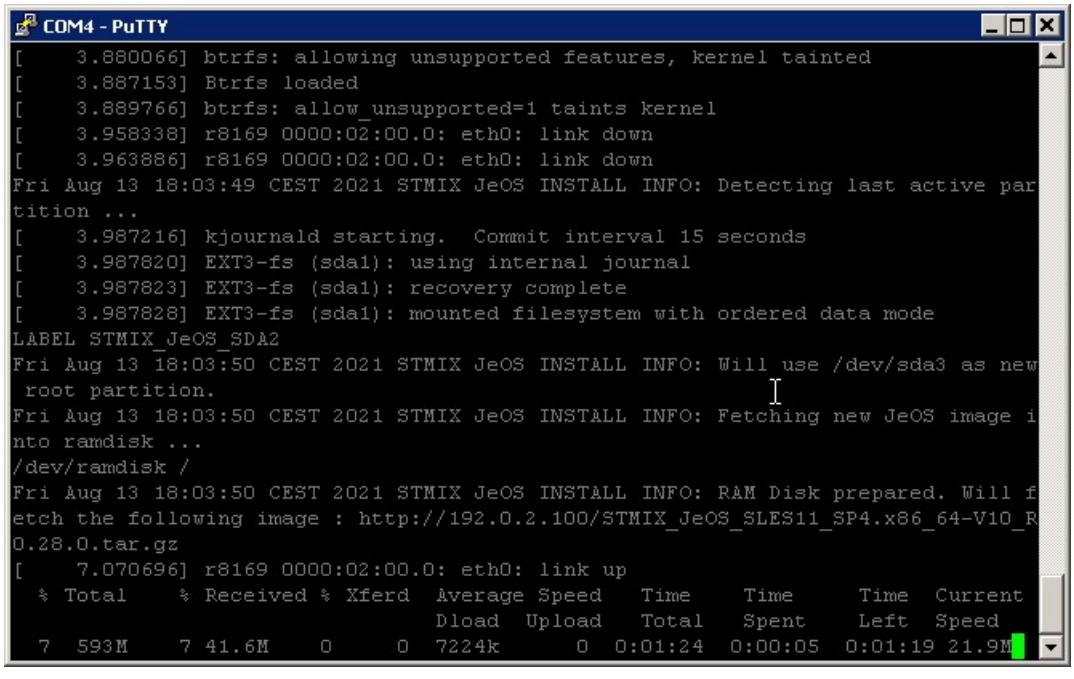


Figure 30: JeOS image fetch

The Fileserver will show in log screen the image and checksum loaded.

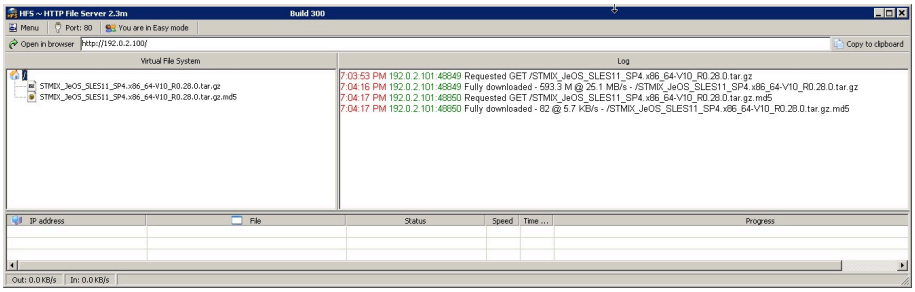


Figure 31: Image loaded

It will write the image to either sda2 or sda3, which will activate the partition and will reboot.

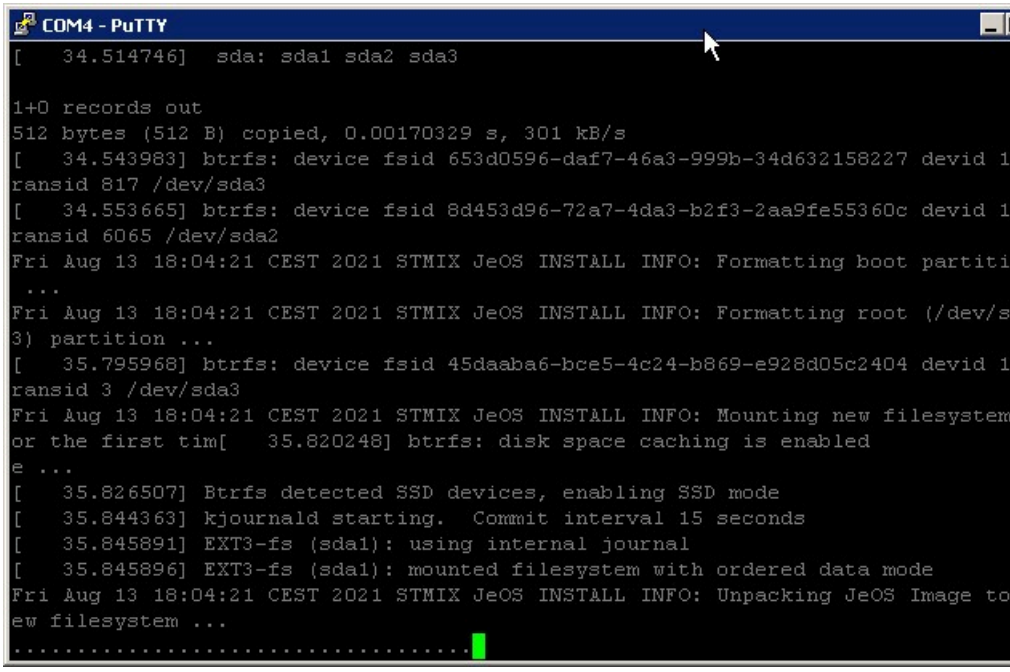


Figure 32: Image writing

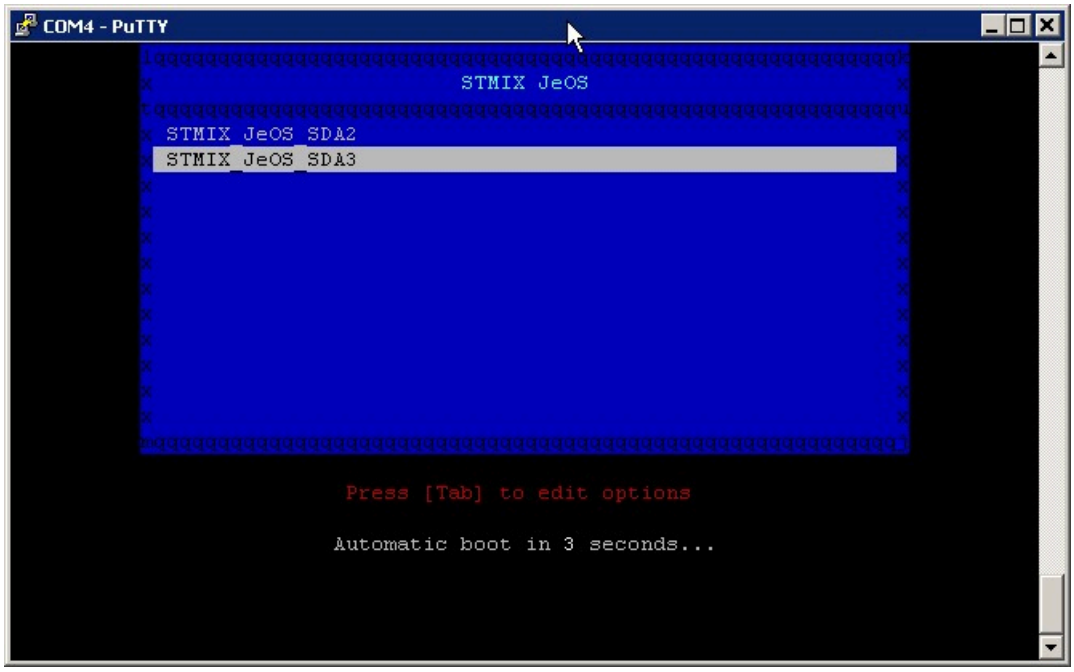


Figure 33: Automatically reboot

SDA2 will be written if SDA3 was the last known good partition that still booted.

SDA3 will be written if SDA2 was the last known good partition that still booted.

4) The STMIX should now boot from the just written sda2/sda3 which will be automatically activated by the flashing process (and become READY in RMX if configured).

NOTICE: When flashing more than one STMIX board in a row, before the next PXE boot process clear the DHCP Server cache (tftpd program's DHCP Server tab, right click on already used allocation and Delete). Otherwise, it will not allocate the IP address 192.0.2.101 again to another MAC address.

2.11.6 STMIX and STMIY Factory reset

The factory reset procedure for STMIX and STMIY boards is performed via WBM page with the path : **WBM> Maintenance> Backup/Restore> Factory Reset**.

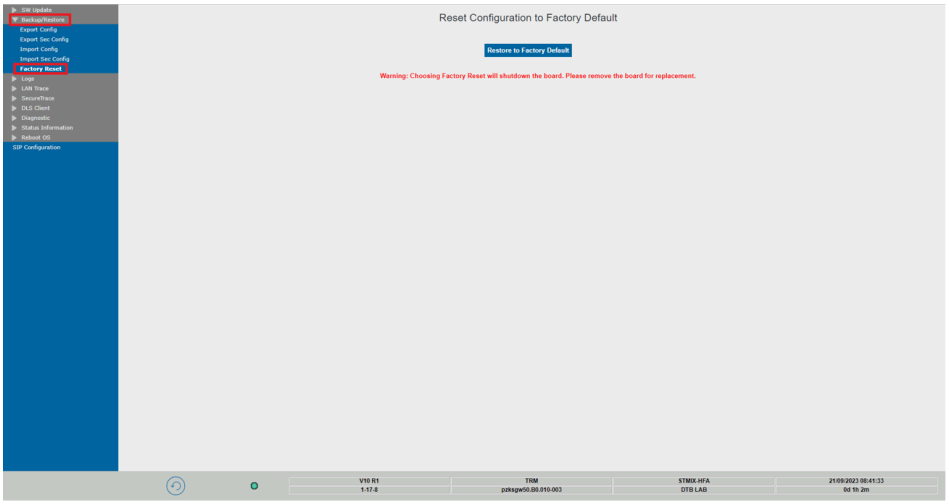


Figure 34: WBM page layout

The action can only be performed once, and after the procedure ends, the board can be removed and used somewhere else.

Description

1) Activation of the **Factory Reset**, will clear all the directories that contain sensitive customer data from the board.

   NOTICE: Some files will be purged or replaced with templates (initial status before adding customer specific configuration).

2) The filesystem will be then synced to SSD.
3) Any data in the alternative passive partitions will be deleted.
4) The board will then shutdown at the end of the process and can be safely removed.

2.12 Gateway HG 3575 - Changing Parameters with AMO STMIB

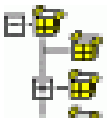
IMPORTANT: Any of the settings that can be made here with AMOs are read-only in WBM.

The following branches are supported:

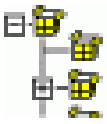
- TYPE GLOBAL - Changing the Idle Bit Pattern
- TYPE IFDATA - Changing the Interface-Specific Parameters of the Access Point
- TYPE SERVIF - Changing the Login and Password for Service Access
- TYPE ASC - Changing the Payload QoS Setting of the Access Point
- TYPE ASC - Setting the Codec List for DMC Connections, RTP Packet Size, Voice Ac
- TYP ASC - Transmission of DTMF/Fax/Modem Tones
- TYPE DSP - Jitter Buffer Size of the Access Point
- TYPE DMCDATA - Changing the Access Point Setting to Support Direct Media Conne
- TYPE H323 - Changing the H323 Settings at the Access Point
- TYPE JB - Configuring the Jitter Buffer

- TYPE SIGQOS - Quality Monitoring for the Signaling Connection over IP
- TYPE SNMP - Changing the Community Strings for Read Access
- TYPE MGNTDATA - Management Data and Backup Server
- TYPE WBMDATA - Changing the Login and Password for WBM
- TYPE GWSECTOR - Changing the Access Point Sector Number for the Resource Manage
- TYPE DLSDATA - Configuring DLS Data
- Resetting the Parameters to Default Values

2.12.1 TYPE GLOBAL - Changing the Idle Bit Pattern

	**Configuration Management > System Data > IPDA > IPDA Access Point** Click **Search** and select the access point. Enter idle bit pattern on the **General** tab and **Save**.
	`CHANGE-STMIB:MTYPE=NCUI2,LTU=99,SLOT=99,TYPE=GLOBAL,PATTERN=213;`

This change does not become effective until the access point is restarted.

	**Configuration Management > System Data > IPDA > IPDA System Data** Click **Search** and select the access point. Click **Execute** on the **Action** pull-down menu and select the mode of action **Update AP**, confirm with **OK**.
	`EXEC-USSU:MODE=UPDATAP,LTU=99;`

IMPORTANT: Connections are cleared down without further warning. Prior to the `EXEC-USSU:UPDATAP`, the configuration must be updated on the system hard disk.

2.12.2 TYPE IFDATA - Changing the Interface-Specific Parameters of the Access Point

The settings can differ from access point to access point.

The following parameters can be set:

- For the physical Ethernet interface [`BITRATE`]
- For QoS support on Layer 2 to IEEE 802.1 q/q [`VLAN, VLANID`]
- For QoS support on Layer 3 to IETF RFC 2474 (DiffServ) [`TOSLAN, TOSMODEM`]

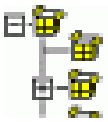
The Ethernet interface setting **must** be **identical** for both connected interface partners (HG 3575 or LAN switches, routers).

IMPORTANT: The setting of a fixed interface partner leads to problems with the “Autonegotiate“ setting of the other partner. Incorrect settings cannot normally be detected by the system and therefore go unreported. If one device is operating in full duplex and the other in half duplex mode, this is not immediately noticeable. Where there is a high payload, the device set to half duplex will report a higher number of late collisions and the packet delay will increase sharply. If the LAN port connected to the HG 3575 does not support autonegotiation or if it does not work reliably, fixed values must be set for the HG 3575’s Ethernet interface.

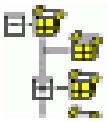
VLAN tagging should only be activated when all routers in the network segment of the access point support VLAN tagging. The same applies for the DiffServ CodePoints. If the routers do not support DiffServ, the standard TOS values must be configured without DiffServ. If DiffServ is supported, but not the CodePoints, the values specified by the network carrier must be configured.

Given that some network component vendors only support prioritization with VLAN ID > 0 pursuant to IEEE 802.1 p/q, the VLAN ID can also be set. The HG 3575 module generally sets the priority bits when the VLAN option is activated. For values, see Table 3, “TOS values”. According to the standard, the VLAN ID must then be set to zero, which also happens for the default setting.

In the example, VLAN tagging is deactivated (reset to the default value), the standard TOS values are configured without DiffServ (see Table 3, “TOS values”) and the Ethernet interface is set to 10 Mbps half duplex.

	**Configuration Management > System Data > IPDA > IPDA Access Point** Click **Search** and select the access point. Enter the TOS bytes under Layer 2 and Layer 3 on the **Quality of Service** tab. Set the transmission speed and mode on the **Ethernet Interface** tab and **Save**.
	`CHANGE-STMIB:MTYPE=NCUI2,LTU=99,TYPE=IFDATA,VLAN=NO,TOSLAN=20,TOSMODEM=16,BITRATE=100MBFD;`

This change does not become effective until the access point is restarted.

	**Configuration Management > System Data > IPDA > IPDA System Data** Click **Search** and select the access point. Click **Execute** on the **Action** pull-down menu and select the mode of action **Update AP**, confirm with **OK**.
	`EXEC-USSU:MODE=UPDATAP,LTU=99;`

IMPORTANT: Connections are cleared down without further warning. Prior to the `EXEC-USSU:UPDATAP`, the configuration must be updated on the system hard disk.

2.12.3 TYPE SERVIF - Changing the Login and Password for Service Access

The HG 3575 allows the connection of a TAP/Service PC via RS232/V.24 interface.

There are two operating modes:

- Terminal Mode
- In terminal mode, communication with the HG 3575 Loadware is realized directly via the Command Line Interface.

  IMPORTANT: Two-stage CLI is not supported.

  ```
  CHANGE-
  STMIB:MTYPE=NCUI2,LTU=<LTU>,SLOT=<SLOT>,TYPE=SERVIF,LOGINTRM=<User
  login for terminal mode>,LOGINPPP=<User login for PPP
  connection>,PASSW=<Password for terminal mode>;
  ```

  The standard login data is:

  Login: TRM (parameter (**LOGINTRM**)

  Password: PUBLIC (parameter **PASSW**)

  After successful login the following message appears:

  Welcome to the HG 3575 V4.0 <currently loaded LW-version> Command Line Interpreter.

  vxTarget>

  A list of available commands can be now requested via the local help function which is available via the `help` command.
- PPP Mode
- In PPP mode, a link between the TAP/Service PC and the customer network is established via the HG 3575 using the IP address configured with the AMO APRT, parameter **TAIPADDR**.

  Login (default setting): PPP

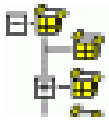
  Password: No password is required for PPP!

  IMPORTANT: For security reasons, the configured password cannot be exported or regenerated. The passwords are therefore deleted when a system is

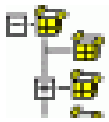
regenerated from the REGEN batch. Logins and passwords set in the system are always stored in uppercase.

These 3 parameters can be configured differently per module.

In the example, the login for AP 17 is set to TERMINAL and SURV, while the password is set to HG3575:

	**Configuration Management > System Data > IPDA > IPDA Access Point** Click **Search** and select the access point. Enter the user data on the **Security** tab and **Save**.
	`CHANGE-STMIB:MTYPE=NCUI2,LTU=17,TYPE=SERVIF, LOGINTRM=TERMINAL,LOGINPPP=SURV,PASSW2=HG3575;`

This change does not become effective until the access point is restarted.

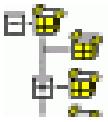
	**Configuration Management > System Data > IPDA > IPDA System Data** Click **Search** and select the access point. Click **Execute** on the **Action** pull-down menu and select the mode of action **Update AP**, confirm with **OK**.
	`EXEC-USSU:MODE=UPDATAP,LTU=17;`

IMPORTANT: Connections are cleared down without further warning. Prior to the `EXEC-USSU:UPDATAP`, the configuration must be updated on the system hard disk.

2.12.4 TYPE ASC - Changing the Payload QoS Setting of the Access Point

In this branch, the Quality of Service for the payload of an access point can be configured. The settings can differ from access point to access point. If the routers do not support DiffServ, the standard TOS value must be configured without DiffServ. If DiffServ is supported, but not the CodePoints, the value specified by the network operator must be configured.

In the example, the standard TOS value is set for AP 99 without DiffServ (see also Table 3, “TOS values”).

	**Configuration Management > System Data > IPDA > IPDA Access Point** Click **Search** and select the access point. Enter the TOS bytes under Layer 3-Diffserv on the **Quality of Service** tab and **Save**.
	`CHANGE-` `STMIB:MTYPE=NCUI2,LTU=99,TYPE=ASC,TOSPL=16;`

This change is started directly on the access point and is effective immediately without an interruption in operation.

2.12.5 TYPE ASC - Setting the Codec List for DMC Connections, RTP Packet Size, Voice Activity Detection and T.38 Fax

See also Chapter 14, “Codec Settings”.

Codec list

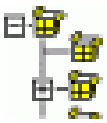
With NCUI2, direct media connections from IP phones, trunking gateways or HG 3500/75 gateways associated with networked OpenScape 4000 systems can be terminated on the board. Unlike for IPDA, the codec type for DMC connections is not selected using classmarks but rather on the basis of a codec list which provides the relevant partners with information about the codec types supported and preferred.

HG 3575 supports two codec types: G.711 and G.729

The sequence in which the codec types are named defines the preference. The type named first is preferred.

In the example, NCUI2 supports G.711 and G.729 but G.729 is preferred. The audio sample size for G.711 and G.729A is set to 60 ms.

T.38 Fax

	**Configuration Management > System Data > IPDA > IPDA Access Point** Click **Search** and select the access point. Select **G729**, **G711** on the **General** tab under **DMC Codec List** in the **Direct Media Connection** section and **Save**.

	`CHANGE-`
	`STMIB:MTYPE=NCUI2,LTU=99,TYPE=ASC,PRIO=PRIO1,CODEC=G729,RTP=60;`
	`CHANGE-`
	`STMIB:MTYPE=NCUI2,LTU=99,TYPE=ASC,PRIO=PRIO2,CODEC=G711,RTP=60;`

This change is started directly on the access point and is effective immediately without an interruption in operation.

2.12.6 TYP ASC - Transmission of DTMF/Fax/Modem Tones



```
CHANGE-
STMIB:MTYPE=NCUI2,LTU=99,TYPE=ASC,RFCFMOIP=YES,RFCDTMF=YES,REDRFCTN=YES;
```

REDRFCTN	Redundant transmission of the RFC2833 tones in accordance with RFC2198
RFCDTMF	Transmission of DTMF tones in accordance with RFC2833.
RFCFMOIP	Transmission of fax/modem tones in accordance with RFC2833

IMPORTANT: The parameters mentioned above must have the same value in all IPDA gateways (STMI2/4/STMIX/STMIY with regard to AMO CGWB & NCUI2+/4 with regard to AMO STMIB). This avoids problems and a common function across all systems is achieved!

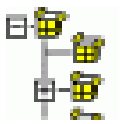
With the introduction of the feature "Codec Switch on the fly" in STMI4/STMIX/STMIY/NCUI4/OpenScape 4000 SoftGate setting **RFCMOIP=NO** in AMO CGWB and AMO STMIB is the better option for fax/modem calls. Therefore, the default value was changed from YES to NO. There is no necessity to change the parameter in existing installations.

2.12.7 TYPE DSP - Jitter Buffer Size of the Access Point

The parameter JITBUFD only takes effect if the parameter JBMODE in the JB branch is set to 0 (LEGACY MODE).

2.12.8 TYPE DMCDATA - Changing the Access Point Setting to Support Direct Media Connections

These parameters are used to set if or how many direct media connections are permitted simultaneously on a specific HG 3575. The connections are counted both in the OpenScape 4000 central system's software and on the board itself.



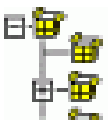
Configuration Management > System Data > IPDA > IPDA Access Point

Click **Search** and select the access point.

Enter under **Direct Media Connection (DMC) enabled** on the **General** tab and **Save**.

	The access point must be switched off if you want to change the value for **DMCALLWD**.
	`DEACT-USSU:LTU=19;`
	If you only want to change the number of DMC connections (**DMCCONN**) then the access point must not be deactivated.
	`CHANGE-`
	`STMIB:MTYPE=NCUI2,LTU=99,TYPE=DMCDATA,DMCALLWD=YES,DMCCONN=30;`

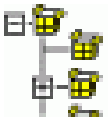
This change does not become effective until the access point is restarted or switched on again.

	**Configuration Management > System Data > IPDA > IPDA System Data** Click **Search** and select the access point. Click **Execute** on the **Action** pull-down menu and select the mode of action **Update AP**, confirm with **OK**.
	IF DMCALLWD has been changed the access point must be switched on again: `ACT-USSU:LTU=19;` If the number of DMC connections (**DMCCONN**) has been changed an UPDATPA must be performed: `EXEC-USSU:MODE=UPDATAP,LTU=99;`

IMPORTANT: Connections are cleared down without further warning when performing UPDATAP. Prior to the `EXEC-USSU:UPDATAP`, the configuration must be updated on the system hard disk.

2.12.9 TYPE H323 - Changing the H323 Settings at the Access Point

Direct media connections use the H323 fast connect mechanism to set up connections. The NCUI2/4 and STMI2/4/STMIX/STMIY platform consequently supports H.323. Two timers from the H.323 stack and the gateway name can be modified.

	**Configuration Management > System Data > IPDA > IPDA Access Point** Click **Search** and select the access point. Enter under **Direct Media Connection (DMC) enabled** on the **General** tab and **Save**.

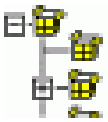
	`CHANGE-`
	`STMIB:MTYPE=NCUI2,LTU=99,TYPE=H323,Q931T1=50,`
	`Q931T2=500,GWNAME="HG3575-2";`

This change is started directly on the access point and is effective immediately with the next H.323.

2.12.10 TYPE JB - Configuring the Jitter Buffer

A basic understanding of procedures and configuration parameters is required to perform jitter buffer configuration. Refer to Section 1.5, “Jitter Buffer”.

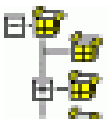
The adaptive jitter buffer (JBMODE=2) that reduces delays is set by default.

	**Configuration Management > System Data > IPDA > IPDA Access Point** Click **Search** and select the access point. Enter the parameter on the **General** tab under **Jitter Buffer** and click **Save**.
	`CHANGE-STMIB:MTYPE=NCUI2,LTU=99,TYPE=JB, AVGDLYV=40,MAXDLYV=120,MINDLYV=20,PACKLOSS=4, AVGDLYD=60,MAXDLYD=200,JBMODE=2;`

These changes are started directly on the access point and become effective when the next connection is set up.

2.12.11 TYPE SIGQOS - Quality Monitoring for the Signaling Connection over IP

Generation

	**Configuration Management > System Data > IPDA > Access point** Click **Search** and enter or change the required parameters on the **Quality of Service** tab in the **Signaling Quality of Service** section, then click **Save**.
	`CHANGE-STMIB:MTYPE=NCUI2,LTU=99,TYPE=SIGQOS, BANDW=40,MAXRTD=500,MINTHRPT=30, SIGPTHSW=EXTEND,QOSSTAT=NO;`

The setting becomes effective immediately.

IMPORTANT: If the Bandwidth to the shelf is less than 64kbits/s then **BANDW** should also be specified accordingly. If Signaling Survivability is not installed then **SIGPTHSW=STD** should be used.

2.12.12 TYPE SNMP - Changing the Community Strings for Read Access

The HG 3575 board operates an SNMP agent that can be address over LAN.

HG 3575’s SNMP agent exclusively supports read-only access.

Access authorization and access rights are controlled by the SNMP agent over community strings.

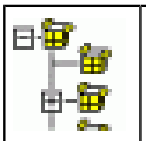
A MIB browser that sends queries to the SNMP agent, identifies itself as belonging to a community. The community is identified by a community string. This is a simple, unencrypted text.

The standard setting - and default for community string 1 (CS1) - is “public“, CS2 is not used.

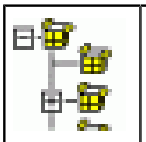
These values can be modified. CS2 can be used to assign read-only access to a second community on the SNMP agent.

If, for example, CS1=“ToP_SeCrEt23“ is set and CS2=“11!$ZwY?“, access attempts using all other community strings (including “public“) are rejected.

For the parameters CS1 and CS2, all ASCII characters between «!» (exclamation mark, 33 Dec) and «~» (tilde, 126 Dec) are used with the exception of the characters «”» (34 Dec), «/» (47 Dec), «\» (92 Dec), and «^» (94 Dec). The space character « » (32 Dec) may not be used.

	**Configuration Management > System Data > IPDA > IPDA Access Point** Click **Search** and select the access point. Enter on the **Security** tab under **SNMP** and **Save**.
	`CHANGE-STMIB:MTYPE=NCUI2,LTU=99,TYPE=SNMP, CS1=“ToP_SeCrEt23“,CS2=“11!$ZwY?“;`

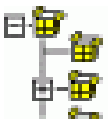
This change does not become effective until the access point is restarted.

	**Configuration Management > System Data > IPDA > IPDA System Data** Click **Search** and select the access point. Click **Execute** on the **Action** pull-down menu and select the mode of action **Update AP**, confirm with **OK**.
	`DEACTIVATE-USSU:LTG=1,LTU=99;` `ACTIVATE-USSU:UNIT=LTG,LTG=1,LTU=99;`

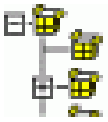
IMPORTANT: Connections are cleared down without further warning.

CS1 cannot be deleted. The following procedure is recommended for deleting CS2:

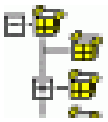
- Reset all parameters in the SNMP AMO branch to the default value (CS1=“public“, CS2 inactive)

	Initialization can only be initiated in expert mode. **Expert Mode > OpenScape 4000 > Expert Access > Open ...**<IP> with AMO (see AMO command)
	`CHANGE-STMIB:MTYPE=INITNCU2,LTU=99,TYPE=SNMP;`

- Restore the required values for CS1

	**Configuration Management > System Data > IPDA > IPDA Access Point** Click **Search** and select the access point. Enter on the **Security** tab under **SNMP** and **Save**.
	`CHANGE-STMIB:MTYPE=NCUI2,LTU=99,TYPE=SNMP,` `CS1="ToP_SeCrEt23";`

- This change does not become effective until the access point is restarted.

	**Configuration Management > System Data > IPDA > IPDA System Data** Click **Search** and select the access point. Click **Execute** on the **Action** pull-down menu and select the mode of action **Update AP**, confirm with **OK**.
	`DEACTIVATE-USSU:LTG=1,LTU=99;` `ACTIVATE-USSU:UNIT=LTG,LTG=1,LTU=99;`

IMPORTANT: Connections are cleared down without further warning.

2.12.13 TYPE MGNTDATA - Management Data and Backup Server

For STMIB branch **TYPE=MGNTDATA**, the following parameters are not used anymore: MGNTIP, MGNTPN, BUSIP and BUSPN. They are ignored by AMO STMIB, as described in HINT 57 (H57).



```
<CHANGE-
STMIB:NCUI2,67,MGNTDATA,192.168.10.0,1024,192.168.10.1,1024;
H500:  AMO STMIB STARTED
H57: MGNTIP, MGNTPN, BUSIP & BUSPN ARE IGNORED AND DERIVED FROM
 AMO SIPCO

AMO-STMIB-111       CONFIGURATION OF HG3575-2 BOARDS

CHANGE COMPLETED;
  <
```

The Assistant IP address is derived from SIPCO and it is only displayed.



```
<DISPLAY-STMIB:MTYPE=NCUI2,LTU=67,TYPE=MGNTDATA;
H500:  AMO STMIB STARTED
+-----------------------------------------------------+
  NCUI2 BOARD DATA             SOCO1000
+-----------------------------------------------------+
  LTU = 67   SOURCE GROUP INDEX = 6

+-----------------------------------------------------+


  MANAGEMENT STATION AND BACK-UP SERVER

  -------------------------------------

  ASSISTANT IP   = 10.133.42.146 *

  UIMODE         = SECURITY (CLASSIC)

  * DERIVED FROM SIPCO

AMO-STMIB-111       CONFIGURATION OF HG3575-2 BOARDS

DISPLAY COMPLETED;
  <
```

2.12.14 TYPE WBMDATA - Changing the Login and Password for WBM

WBM access can be configured in this branch.



```
CHANGE-
STMIB:MTYPE=NCUI2,LTU=<LTU>,SLOT=<SLOT>,TYPE=WBMDATA,LOGINWBM=<User login
for WBM connection>,PASSWWBM=<Password for WBM connection>,ROLE=<Role of
the WBM user; sets access rights>;
```

Table 10: WBM rights

Role	Rights
ADMIN	Administrator (default value)
ENGR	Developer (access to all features)
READONLY	Administrator with read-only access
SU	Superuser (access to all features)

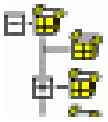
The data for initial login as **engr** is:

User name: `HP4K-DEVEL`

Password: `4K-admin`

2.12.15 TYPE GWSECTOR - Changing the Access Point Sector Number for the Resource Manager

In this branch, the parameter GWSECTNO is used to assign the HG 3575 gateway a sector number from the Resource Manager's sector concept.

	**Configuration Management > System Data > IPDA > IPDA Access Point** Click **Search** and select the access point. Enter the **Gateway Sector Number** on the **General** tab and click **Save**.
	`CHANGE-STMIB:MTYPE=NCUI2,LTU=99,TYPE=GWSECTOR,GWSECTNO=7;`

This change becomes effective immediately and without interrupting operation.

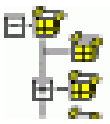
2.12.16 TYPE DLSDATA - Configuring DLS Data

	`CHANGE-STMIB:MTYPE=NCUI2,LTU=99,TYPE=DLSDATA,DLSIPADR=<number>,DLSPORT=<number>,DLSACPAS=<param>;`

2.12.17 Resetting the Parameters to Default Values

If the parameters of one or all branches of the NCUI2/4 data are to be reset to default values, e.g. after being changed temporarily for diagnostic work, this can

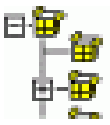
be performed in the INITNCU2 branch. The example sets all ASC parameters to their default values.

	Initialization can only be initiated in expert mode. **Expert Mode > OpenScape 4000 > Expert Access > Open ...**<IP> with AMO (see AMO command)
	`CHANGE-STMIB:MTYPE=INITNCU2,LTU=17,TYPE=ASC;`

The changes under TYPE ASC, DSP, H323, JB, SNMP, MGNTDATA, WBMDATA and DLSDATA **become effective immediately** without interrupting operation.

Changes under TYPE GLOBAL, IFDATA, SERVIF, DMCDATA and SIGQOS **become effective after the access point has been restarted**.

This behaviour is also valid for the command `CHANGE-STMIB:MTYPE=INITNCU2,LTU=17, TYPE=ALL;`. Therefore it is recommended to restart the access point after resetting all parameters.

	**Configuration Management > System Data > IPDA > IPDA System Data** Click **Search** and select the access point. Click **Execute** on the **Action** pull-down menu and select the mode of action **Update AP**, confirm with **OK**.
	`EXEC-USSU:MODE=UPDATAP,LTU=17;`

IMPORTANT: Connections are cleared down without further warning. Prior to the `EXEC-USSU:UPDATAP`, the configuration must be updated on the system hard disk.

2.13 General Information on How to Configure a HG 3500 Common Gateway

2.13.1 Changing the common gateway configuration

Please note that the entire board must be reconfigured if changes are made to the common gateway configuration.

2.13.2 AMOs

- The STMI boards are configured with the AMO CGWB or, if the IPDA was set, with the AMO BCSU (see Chapter 15, “Multiple Feature Support Configuration at the Common Gateway (Example)”).
- The NCUI board is still configured with the AMO STMIB.
- AMO BFDAT is used for block configuration.
- Functions are consolidated on a single board using the AMO BCSU.
- The DB line range of a board must be consecutive.
- All HG 3500 modules must be connected at the OpenScape 4000 LAN segment.
- The lines configured for a board cannot be subsequently modified. The entire board must be reconfigured if additional lines are required on a board.
- The parameter FCTID in the AMO BCSU must always be set to 1.

2.13.3 Rules

- The parameter for the functional block (**FCTBLK**) can be freely assigned. It may not, however, remain unassigned.
- A completed (configured) functional block may be assigned to one or more boards.
- The parameter for the boards to be used (**BRDBCHL**) determines how many B channels are available to the board.
- If the value **BCHAN60&BCHAN120** is set, an STMI[3] with 60 or 120 B channels can be used. This value is also useful if a small STMI with 60 B channels becomes defective. This can then be replaced with a large STMI with 120 B channels. It is not possible to replace a large STMI with a small one.
- Parameter **UNITS**
  - 1 unit corresponds to 10 B channels
  - If the number of units (**UNITS**) is not specified for the configuration, 10 B channels (**UNITS=1**) are configured for each circuit.
  - Up to three units can be specified for each circuit.
  - The total number of B channels for the function is calculated by multiplying the number of circuits (**LINECNT**) by the number of B channels in a unit (**UNITS**). Example: LINECNT=4, UNITS=3. 4 multiplied by 3 multiplied by 10 equals 120 B channels.
- If an IPDA function (HG3570) is to be configured for a multiple feature configuration, this must be configured first.
- For **IPDA**, only the number of B channels (**BCHLCNT**) must be specified.
- For **IP trunking**, the number of circuits (**LINECNT**) and the number of units (**UNITS**) must be specified.
- For **HFA** and **SIP**, the number of circuits (**LINECNT**) and the number of B channels (**BCHLCNT**) must be specified.

IMPORTANT: If reserved HFA or SIP circuits are to be configured, the B channels designated for this purpose must

---

[3] STMI stands for STMI2 (Q2316-X, Q2316-X10) and STMI4 (Q2324-X500,Q2324-X510 and STMIX Q2343-X)

also be specified here. This is not necessary for reserved trunk circuits as the assignment is performed based on the number of units (**UNITS**).

- For **WAML**, only the number of units (**UNITS**) must be specified.

  IMPORTANT: Only one circuit is possible for WAML. This parameter can be omitted if **UNITS=1**. It is not possible to configure WAML on STMIX/STMIY.

- **Reserve function**
- Since the board configuration can only be modified by removing the board, an option has been created that allows users to reserve circuits for use at a later stage. If this feature is to be used for the functions HG3530, HG3540 or HG3550, the relevant function must be configured directly after the actual function (HG3550&HG3550R, for instance). The Reserve function must always be specified after the actual function (i.e. at the end).

  The combination HG3550&HG3530&HG3550R is not permitted as this would lead to invalid circuit distribution (Trunk - HFA - Trunk).

  It is not possible to configure several Reserve functions on a single board.

  The reserved circuits can be subsequently converted to usable circuits with

  CHANGE-BCSU:TYPE=IPGW,LTU=<LTU>,SLOT=<slot>,CHNGRSLN=<number>;

  /*<number>: Number of circuits that should be converted to usable circuits.

  IMPORTANT: Now you must reset the board. `RESET-BSSU:ADDRTYPE=PEN,LTU=<ltu>,SLOT=<slot>;`

- The function can only be configured as a single feature.
- Eleven single-feature standard profiles are configured in the database (see AMO description, AMO BFDAT).
- You can configure a functional block with

  CHANGE-BFDAT:**CONFIG=OK**,FCTBLK=<number>,**ANSW=YES**;

  You can check the status with `DISPLAY-BFDAT:FCTBLK=<number>;`

  If the configuration of the functional block is complete **STATUS=OK** is displayed.

  If a configuration error is detected when the block configuration is complete, the functional block must be deleted (`DELETE-BFDAT:FCTBLK=<number>,ANSW=YES;`) and reconfigured.

  If the configuration of a functional block is not complete **STATUS=CONT** is displayed. The functional block may not be assigned to a board. This is refused by the AMO BCSU with the Fault message F89.

  F89: THE SPECIFIED FUNCTION BLOCK IS NOT YET FULLY CONFIGURED:

  PLEASE COMPLETE THE CONFIGURATION FIRST WITH THE AMO BFDAT.

2.13.4 Restrictions

- Only one trunking protocol can be configured for each board (AMO CGWB). There are no restrictions on interworking with other functions.
- The entire board must be reconfigured if the changes are made to the configuration.

2.13.5 Overview of Configuration Steps

An overview of the configuration steps for a HG 3500 common gateway is provided below:

1) Configure functional blocks with the AMO BFDAT (Assistant: **Configuration Management > System Data > Board > CGW Functional Block**)
2) Assign the functional block to a board using the AMO BCSU (Assistant: **Configuration Management > System Data > Board > Board**)
3) Administrate features using the AMO CGWB

2.14 Gateway HG 3500 - Changing Parameters with AMO CGWB

IMPORTANT: Any of the settings that can be made here with AMOs are read-only in WBM.

The following branches are supported:

- TYPE ASC - Changing the Payload QoS Setting in Host System
- TYPE ASC - Setting the Codec List for DMC Connections, RTP Packet Size, and Voic
- TYP ASC - Transmission of DTMF/Fax/Modem Tones
- TYPE DMCDATA - Changing the HG 3500 Setting to Support Direct Media Connectio
- TYPE DSP - Changing the DSP (Signal Processor) Setting at an HG 3500
- TYPE GLOBIF - Changing the Idle Bit Pattern and Interface-Specific Parameters
- TYPE GWSECTOR - Changing the HG 3500 Sector Number for the Resource Manag
- TYP MGNTDATA - Connection to the OpenScape 4000 Assistant
- TYPE SERVIF - Changing the Login and Password for the Service Access
- TYPE WBMDATA - Changing the Login and Password for WBM
- TYPE JB - Configuring the Jitter Buffer
- Resetting the Parameters to Default Values

2.14.1 TYPE ASC - Changing the Payload QoS Setting in Host System

In this branch, the Quality of Service for the payload of an access point can be configured. The settings can differ from HG 3500 to HG 3500. If the routers do not support DiffServ, the standard TOS value must be configured without DiffServ. If DiffServ is supported, but not the CodePoints, the value specified by the network operator must be configured.

In the example, the standard TOS value is set for HG 3500 in LTU 5, mounting slot 91 without DiffServ (see also Table 3, “TOS values”).

	**Configuration Management > System Data > IPDA > IPDA System Data** Enter settings under **Payload Connections** on the **System Data** tab and click **Save**.
	`CHANGE-` `CGWB:MTYPE=CGW,LTU=5,SLOT=91,TYPE=ASC,TOSPL=16;`

This change is loaded directly to the board and is effective immediately without interrupting operation.

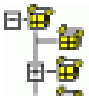
2.14.2 TYPE ASC - Setting the Codec List for DMC Connections, RTP Packet Size, and Voice Activity Detection

See also Chapter 14, “Codec Settings”.

This branches' parameters only apply to one HG 3500 board. Therefore each HG 3500 board could be configured differently in an OpenScape 4000 system.

To ensure the usability and the correct diagnosis of the system, these parameters must have identical settings (FUNCTION=HG3570) for all HG 3500 boards.

In the example, the audio sample size for G.711 and G.729 is set to 60 ms for the common gateway HG 3500 1-5-91. This results in a higher packeting delay, but a comparatively low transmission bandwidth requirement.

	**Configuration Management > System Data > Board > Board** Click **Search** and select **STMI**. Set the times for G.711 and G.729 on the **STMI Board Data** tab and click **Save**.

	`CHANGE-`
	`CGWB:MTYPE=CGW,LTU=5,SLOT=91,TYPE=ASC,PRIO=PRIO1,CO-`
	`DEC=G711,RTP=60; CHANGE-`
	`CGWB:MTYPE=CGW,LTU=5,SLOT=91,TYPE=ASC,PRIO=PRIO2,CO-`
	`DEC=G729,RTP=60;`

These changes are loaded directly to the HG 3500 and become effective immediately without interrupting operation.

2.14.3 TYP ASC - Transmission of DTMF/Fax/Modem Tones

	`CHANGE-`
	`CGWB:MTYPE=CGW,LTU=5,SLOT=91,TYPE=ASC,RFCFMOIP=YES,RFC-`
	`DTMF=YES,REDRFCTN=YES;`

REDRFCTN	Redundant transmission of the RFC2833 tones in accordance with RFC2198

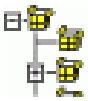
RFCDTMF	Transmission of DTMF tones in accordance with RFC2833.
RFCFMOIP	Transmission of fax/modem tones in accordance with RFC2833

IMPORTANT: The parameters mentioned above must have the same value in all IPDA gateways (STMI2/4/STMIX/STMIY with regard to AMO CGWB & NCUI2+/4 with regard to AMO STMIB). This avoids problems and a common function across all systems is achieved!

With the introduction of the feature "Codec Switch on the fly" in STMI4/STMIX/STMIY/NCUI4/OpenScape 4000 SoftGate setting **RFCMOIP=NO** in AMO CGWB and AMO STMIB is the better option for fax/modem calls. Therefore, the default value was changed from YES to NO. There is no necessity to change the parameter in existing installations.

2.14.4 TYPE DMCDATA - Changing the HG 3500 Setting to Support Direct Media Connections

Use this parameter to set the number of simultaneous direct media connections permitted on a certain HG 3500. The connections are counted both in the OpenScape 4000 central system's software and on the board itself.

	**Configuration Management > System Data > Board > Board** Click **Search** and select **STMI**. Make the settings on the **STMI Board Data** tab under **Number of DMC connections** and **Save**. **Configuration Management > System Data > Maintenance > Board Maintenance** Click **Search** and select **STMI**. Click **Execute** on the **Action** pull-down menu, select **Restart** and confirm with **OK**.
	`CHANGE-CGWB:MTYPE=CGW,LTU=5,SLOT=91,TYPE=DMCDATA,DMCCONN=30;` This change does not become effective on the HG 3500 until this board is restarted with `RESTART-BSSU:ADDRTYPE=PEN,LTU=5,SLOT=91.`

IMPORTANT: Existing **links are disconnected.**

2.14.5 TYPE DSP - Changing the DSP (Signal Processor) Setting at an HG 3500

The parameter **JITBUFD** only takes effect if the parameter JBMODE in the JB branch is set to 0 (LEGACY MODE).

The parameter **VADEN** is no longer valid. To configure Voice Activity Detection, you should use the parameter branch TYPE=ASC, parameter VAD (see Section 13.2, “TYPE ASC - Setting the Codec List for DMC Connections, RTP Packet Size, and Voice Activit

2.14.6 TYPE GLOBIF - Changing the Idle Bit Pattern and Interface-Specific Parameters

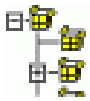
The setting for the physical Ethernet interface may be different for individual HG 3500s.

The Ethernet interface setting must be identical for both connected interface partners (HG 3500 or LAN switches, routers).

IMPORTANT: The setting of a fixed interface partner leads to problems with the "Autonegotiate" setting of the other partner. Incorrect settings cannot normally be detected by the system and therefore go unreported. If one device is operating in full duplex and the other in half duplex mode, this is not immediately noticeable. Where there is a high payload, the device set to half duplex will report a higher number of late collisions and the packet delay will increase sharply. If the LAN port connected to the HG 3500 does not support autonegotiation or if it does not work reliably, fixed values must be set for the HG 3500’s Ethernet interfaces.

The QoS-relevant parameters are set identically for all HG 3500 modules together with SL100/200 via the AMO SIPCO.

In the example, the Ethernet interface is set to 10 Mbps half duplex and the idle bit pattern is set to 213.



Configuration Management > System Data > Board > Board

Click **Search** and select **Board Name=STMI2**,**Board Name=STMI4 or Board Name=STMIX or Board Name=STMIY**.

Enter appropriate settings on the **STMI Board Data** tab and click **Save**.

Configuration Management > System Data > Maintenance > Board Maintenance

Click **Search** and select **STMI**.

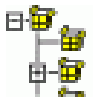
Click **Execute** on the **Action** pull-down menu, select **Restart** and confirm with **OK**.

	CHANGE- CGWB:MTYPE=CGW,LTU=5,SLOT=91,TYPE=GLOBIF,PATTERN=213, BI TRATE=100MBFD; This change does not become effective on the HG 3500 until this board is restarted with RESTART- BSSU:ADDRTYPE=PEN,LTU=5,SLOT=91.

IMPORTANT: Existing **links are disconnected.**

2.14.7 TYPE GWSECTOR - Changing the HG 3500 Sector Number for the Resource Manager

In this branch, the parameter GWSECTNO is used to assign the HG 3500 gateway a sector number from the Resource Manager's sector concept.

	**Configuration Management > System Data > Board > Board** Click **Search** and select **STMI**. Make the settings on the **STMI Board Data** tab under **Gateway Sector Number** and **Save**.
	CHANGE- CGWB:MTYPE=CGW,LTU=5,SLOT=91,TYPE=GWSECTOR,GWSECTNO=1;

This change becomes effective immediately and without interrupting operation.

2.14.8 TYP MGNTDATA - Connection to the OpenScape 4000 Assistant

For CGWB branch **TYPE=MGNTDATA**, the following parameters are not used anymore: MGNTIP, MGNTPN, BUSIP and BUSPN.

They are ignored by AMO CGWB, as described in HINT 76 (H76).

	<CHANGE- CGWB:CGW,1,14,MGNTDATA,192.168.10.0,1024,192.168.10.1,1024; H500: AMO CGWB STARTED H76: MGNTIP, MGNTPN, BUSIP & BUSPN ARE IGNORED AND DERIVED FROM AMO SIPCO AMO-CGWB -111 CONFIGURATION OF HG3500 BOARD CHANGE COMPLETED; <

The Assistant IP address is derived from SIPCO and it is only displayed.



```
<DISPLAY-CGWB:LTU=1,SLOT=14,TYPE=MGNTDATA;
H500:  AMO CGWB  STARTED
------------------------------------------------------------
|  CGW BOARD DATA                                          |
------------------------------------------------------------
|   HG3530     SIP         HG3550            HG3570       |
------------------------------------------------------------
|   LTU = 1    SLOT = 14   SMODE = NORMAL    POOLNO: 0    |
------------------------------------------------------------


  MANAGEMENT STATION AND BACK-UP SERVER

  -------------------------------------

  ASSISTANT IP   = 10.133.42.146 *

  UIMODE         = SECURITY (CLASSIC)

  * DERIVED FROM SIPCO

AMO-CGWB -111       CONFIGURATION OF HG3500 BOARD

DISPLAY COMPLETED;
  <
```

2.14.9 TYPE SERVIF - Changing the Login and Password for the Service Access

In the parameter tree TYPE=SERVIF you can define the access data for the Command Line Interface.

For more information on CLI please refer to Chapter 17, “Command Line Interface CLI in HG 3500”.



```
CHANGE-
CGWB:MTYPE=CGW,LTU=<LTU>,SLOT=<SLOT>,TYPE=SERVIF,LOGIN-
TRM=<User login for terminal mode>,PASSW=<Password for
terminal mode>;
```

The standard login data is:

Login: TRM (parameter (**LOGINTRM**)

Password: PUBLIC (parameter **PASSW**)

2.14.10 TYPE WBMDATA - Changing the Login and Password for WBM

WBM access can be configured in this branch.

	CHANGE- CGWB:MTYPE=CGW,LTU=<LTU>,SLOT=<SLOT>,TYPE=WBMDATA,LOGIN- WBM=<User login for WBM connection>,PASSWWBM=<Password for WBM con nection>,ROLE=<Role of the WBM user; sets access rights>;

Table 11: WBM rights

Role	Rights
ADMIN	Administrator (default value)
ENGR	Developer (access to all features)
READONLY	Administrator with read-only access
SU	Superuser (access to all features)

The data for initial login as **engr** is:

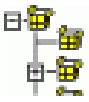
1) User name: `HP4K-DEVEL`

Password: `4K-admin`

2.14.11 TYPE JB - Configuring the Jitter Buffer

A basic understanding of procedures and configuration parameters is required to perform jitter buffer configuration. Refer to Section 1.5, “Jitter Buffer”.

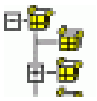
The adaptive jitter buffer that reduces delays is set by default.

	**Configuration Management > System Data > IPDA > IPDA Access Point** Click **Search** and select the access point. Enter the parameter on the **General** tab under **Jitter Buffer** and **Save**.
	CHANGE-CGWB:MTYPE=CGWB,LTU=5,SLOT=91,TYPE=JB, AVGDLYV=40,MAXDLYV=120,MINDLYV=20,PACKLOSS=4, AVGDLYD=60,MAXDLYD=200, JBMODE=2;
WBM	**Configuration > Payload > HW Modules > Edit DSP Jitter Settings**

These changes are started directly on the access point and become effective when the next connection is set up.

2.14.12 Resetting the Parameters to Default Values

If the parameters of one or all branches of the STMI2/4/STMIX/STMIY data are to be reset to default values, e.g. after being changed temporarily for diagnostic work, this can be performed in the INITCGW branch. The example sets all DMCDATA parameters to their default values.

	Initialization and reloading (where required) can only be performed in expert mode. **Expert Mode > OpenScape 4000 > Expert Access > Open ...**<IP> using AMO (see AMO command)
	`CHANGE-` `CGWB:MTYP=INITCGW,LTU=5,EBT=91,TYP=DMCDATA;`

The changes under TYPE ASC, DSP, MGNTDATA, SIPTRERH, WBMDATA, DLSDATA (DLSACPAS) and JB **become effective immediately** without interrupting operation.

Changes under TYPE DMCDATA, GKDATA, GLOBIF, GWDATA, GWSECTOR, H235DATA, SIPTRSSA and DLSDATA (DLSIPADR & DLSPORT) **become effective after the HG 3500 has been restarted** with `RESTART-BSSU:ADDRTYPE=PEN,LTU=5,SLOT=91.`

IMPORTANT: Existing **links are disconnected.**

2.15 Codec Settings

2.15.1 HFA and Trunking

A priority list of the codecs is configured in the AMO CGWB for HG 3500, and accordingly in the AMO STMIB for HG 3575. During codec negotiations, the gateways use the codecs configured in this way.

Examples:

- Gateway is a DMC endpoint
- Master connections for HFA and IP trunking

Example

- HG 3500 (STMI)

```
CHANGE-
CGWB:MTYPE=CGW,LTU=3,SLOT=11,TYPE=ASC,UDPPRTLO=29100,UDPPRTHI=30099,TOSPL="184",
TOSSIGNL="104",T38FAX=YES,RFCFMOIP=YES,RFCDTMF=YES,REDRFCTN=YES,PRIO=PRIO1,CO▶
DEC=G711A,VAD=NO,RTP="20";
CHANGE-CGWB:MTYPE=CGW,LTU=3,SLOT=11,TYPE=ASC,PRIO=PRIO2,CO▶
DEC=G729A,VAD=NO,RTP="20";
CHANGE-CGWB:MTYPE=CGW,LTU=3,SLOT=11,TYPE=ASC,PRIO=PRIO3,CO▶
DEC=G711U,VAD=NO,RTP="20";
```

```
CHANGE-CGWB:MTYPE=CGW,LTU=3,SLOT=11,TYPE=ASC,PRIO=PRIO4,CODEC=NONE;
CHANGE-CGWB:MTYPE=CGW,LTU=3,SLOT=11,TYPE=ASC,PRIO=PRIO5,CODEC=NONE;
CHANGE-CGWB:MTYPE=CGW,LTU=3,SLOT=11,TYPE=ASC,PRIO=PRIO6,CODEC=NONE;
CHANGE-CGWB:MTYPE=CGW,LTU=3,SLOT=11,TYPE=ASC,PRIO=PRIO7,CO▶
DEC=G729AB,VAD=YES,RTP="20";
CHANGE-CGWB:MTYPE=CGW,LTU=3,SLOT=11,TYPE=ASC,PRIO=PRIO8,CO▶
DEC=G722,VAD=NO,RTP="20";
CHANGE-CGWB:MTYPE=CGW,LTU=3,SLOT=11,TYPE=ASC,PRIO=PRIO9,CO▶
DEC=OPUS,VAD=NO,RTP="20";
```

- HG 3575 (NCUI)

```
CHANGE-
STMIB:MTYPE=NCUI2,LTU=18,TYPE=ASC,UDPPRTLO=29100,UDPPRTHI=30099,TOSPL="184",T38F
AX=NO,RFCFMOIP=YES,RFCDTMF=YES,REDRFCTN=YES,PRIO=PRIO1,CO▶
DEC=G711A,VAD=NO,RTP="20";
CHANGE-STMIB:MTYPE=NCUI2,LTU=18,TYPE=ASC,PRIO=PRIO2,CODEC=G729A,VAD=NO,RTP="20";
CHANGE-STMIB:MTYPE=NCUI2,LTU=18,TYPE=ASC,PRIO=PRIO3,CODEC=G711U,VAD=NO,RTP="20";
CHANGE-STMIB:MTYPE=NCUI2,LTU=18,TYPE=ASC,PRIO=PRIO4,CODEC=NONE;
CHANGE-STMIB:MTYPE=NCUI2,LTU=18,TYPE=ASC,PRIO=PRIO5,CODEC=NONE;
CHANGE-STMIB:MTYPE=NCUI2,LTU=18,TYPE=ASC,PRIO=PRIO6,CODEC=NONE;
CHANGE-STMIB:MTYPE=NCUI2,LTU=18,TYPE=ASC,PRIO=PRIO7,CO▶
DEC=G729AB,VAD=YES,RTP="20";
CHANGE-STMIB:MTYPE=NCUI2,LTU=18,TYPE=ASC,PRIO=PRIO8,CODEC=NONE;
CHANGE-STMIB:MTYPE=NCUI2,LTU=18,TYPE=ASC,PRIO=PRIO9,CODEC=NONE;
```

2.15.2 IPDA

For IPDA, the codecs for the master connection are switched by DNIL and configured in AMO SDAT / AMO TDCSU, etc., i.e. in the user/trunk data of the affected devices (see IP Distributed Architecture (IPDA), Section 2.4, “Subscriber, CO/Tie Trunk Circuits in Access Points”).

IMPORTANT: This means that the codecs do not need to be configured in the AMOs CGWB and STMIB for the IPDA master connection.

For IPDA connections, the codecs are configured as previously described in the AMOs STMIB or CGWB (see also Section 11.5, “TYPE ASC - Setting the Codec List for DMC Connections, RTP Packet Size, Voice Activ
Section 13.2, “TYPE ASC - Setting the Codec List for DMC Connections, RTP Packet Size, and Voice
bzw. Section 11.6, “TYP ASC - Transmission of DTMF/Fax/Modem Tones”).

IMPORTANT: The **RFCFMOIP**, **RFCDTMF** and **REDRFCTN** parameters in the **TYP=ASC** branch must have the same value in all IPDA gateways (STMI2/4/STMIX/STMIY with regard to AMO CGWB & NCUI2+/4 with regard to AMO STMIB). This avoids problems and a common function across all systems is achieved!

2.16 Multiple Feature Support Configuration at the Common Gateway (Example)

2.16.1 Important Information / Restrictions

- **IPDA** If the function IPDA (HG3570) is configured on an STMI board, the IP address of the common gateway must be assigned with the AMO BCSU. For all other functions of the board, the IP address must be assigned with the AMO CGWB.
- **IPDA** If several functions are defined in a function block (IPDA and others), the IP address for IPDA must be set with AMO BCSU, for the other functions the **same** IP address must be configured using the AMO CGWB!
- **VLAN settings** in AMO CGWB: When MFS is configured, the following AMOs are used:
  - MFS with IPDA functionality: AMO SIPCO
  - MFS without IPDA functionality: AMO CGWB
- **Trunking protocols** Only one trunking protocol can be configured for each common gateway board (either SIP or H323)! If both protocols should be used for trunking, individual boards must be used.
- **IPDA/WAML** No support of WAML **and** HG3570 (IPDA) functionality on **one** common gateway board because it causes path problems at APNW access points.

2.16.2 Configuring Functional Blocks with the AMO BFDAT

- Functional block 1: IPDA (HG3570)
- Functional block 2: IPDA (HG3570), IP trunking (HG3550) and HFA subscriber (HG3530)
- Functional block 3: IPDA (HG3570), IP trunking (HG3550), WAML and HFA subscriber (HG3530)
- Functional block 4: IPDA (HG3570), IP trunking (HG3550), WAML and HFA subscriber (HG3530)
- Functional block 5: IPDA (HG3570), IP trunking (HG3550), WAML and HFA subscriber (HG3530)
- Functional block 6: IP trunking (HG3550) and HFA subscriber (HG3530)
- Functional block 7: IP trunking, HFA subscriber (HG3530) and reserve HFA subscriber (HG3530R)

Functional block 1

/* Functional block 1: Adding the IPDA function (HG3570)

```
ADD-BFDAT:FCTBLK=1,FUNCTION=HG3570,BRDBCHL=BCHAN120;
```

>>>>> IPDA with 120 B channels

```
CHANGE-BFDAT:CONFIG=CONT,FCTBLK=1,FUNCTION=HG3570,BCHLCNT=120;
```

>>>>> End configuration of this block

```
CHANGE-BFDAT:CONFIG=OK,FCTBLK=1,ANSW=YES;
```

Functional block 2

/* Functional block 2: Adding the functions IPDA (HG3570), IP trunking (HG3550) and HFA subscriber (HG3530)

```
ADD-BFDAT:FCTBLK=2,FUNCTION=HG3570&HG3550&HG3530,BRDBCHL=BCHAN;
```

>>>>> IPDA with 30 B channels

```
CHANGE-BFDAT:CONFIG=CONT,FCTBLK=2,FUNCTION=HG3570,BCHLCNT=30;
```

>>>>> IP trunking with one circuit with three units (=30 B channels)

```
CHANGE-BFDAT:CONFIG=CONT,FCTBLK=2,FUNCTION=HG3550,LINECNT=1,UNITS=3;
```

>>>>> HFA with 60 circuits with 60 B channels

```
CHANGE-BFDAT:CONFIG=CONT,FCTBLK=2,FUNCTION=HG3530,LINECNT=60,BCHLCNT=60;
```

>>>>> End configuration of this block

```
CHANGE-BFDAT:CONFIG=OK,FCTBLK=2,ANSW=YES;
```

Functional block 3

/* Functional block 3: Adding the functions IPDA (HG3570), IP trunking (HG3550), WAML and HFA subscriber (HG3530)

```
ADD-BFDAT:FCTBLK=3,FUNCTION=HG3570&HG3550&WAML&HG3530,BRDBCHL=BCHAN120;
```

>>>>> IPDA with 30 B channels

```
CHANGE-BFDAT:CONFIG=CONT,FCTBLK=3,FUNCTION=HG3570,BCHLCNT=30;
```

>>>>> IP trunking with one circuit with three units (=30 B channels)

```
CHANGE-BFDAT:CONFIG=CONT,FCTBLK=3,FUNCTION=HG3550,LINECNT=1,UNITS=3;
```

>>>>> WAML

```
CHANGE-BFDAT:CONFIG=CONT,FCTBLK=3,FUNCTION=WAML,UNITS=3;
```

>>>>> HFA with 30 circuits with 30 B channels

```
CHANGE-BFDAT:CONFIG=CONT,FCTBLK=3,FUNCTION=HG3530,LINECNT=30,BCHLCNT=30;
```

>>>>> End configuration of this block

```
CHANGE-BFDAT:CONFIG=OK,FCTBLK=3,ANSW=YES;
```

Functional block 4

/* Functional block 4: Adding the functions IPDA (HG3570), IP trunking (HG3550), WAML and HFA subscriber (HG3530)

```
ADD-BFDAT:FCTBLK=4,FUNCTION=HG3570&HG3550&WAML&HG3530,BRDBCHL=BCHAN120;
```

>>>>> IPDA with 30 B channels

```
CHANGE-BFDAT:CONFIG=CONT,FCTBLK=4,FUNCTION=HG3570,BCHLCNT=30;
```

>>>>> IP trunking with one circuit with one unit (=10 B channels)

```
CHANGE-BFDAT:CONFIG=CONT,FCTBLK=4,FUNCTION=HG3550,LINECNT=1,UNITS=1;
```

>>>>> WAML with one unit (=10 B channels)

```
CHANGE-BFDAT:CONFIG=CONT,FCTBLK=4,FUNCTION=WAML;
```

>>>>> HFA with 70 circuits with 70 B channels

```
CHANGE-BFDAT:CONFIG=CONT,FCTBLK=4,FUNCTION=HG3530,LINECNT=70,BCHLCNT=70;
```

>>>>> End configuration of block

```
CHANGE-BFDAT:CONFIG=OK,FCTBLK=4,ANSW=YES;
```

Functional block 5

/* Functional block 5: Adding the functions IPDA (HG3570), IP trunking (HG3550), WAML and HFA subscriber (HG3530)

```
ADD-BFDAT:FCTBLK=5,FUNCTION=HG3570&HG3550&WAML&HG3530,BRDBCHL=BCHAN120;
```

>>>>> IPDA with 30 B channels

```
CHANGE-BFDAT:CONFIG=CONT,FCTBLK=5,FUNCTION=HG3570,BCHLCNT=30;
```

>>>>> IP trunking with one circuit with 10 B channels

```
CHANGE-BFDAT:CONFIG=CONT,FCTBLK=5,FUNCTION=HG3550,LINECNT=1;
```

>>>>> WAML with one unit (=10 B channels)

```
CHANGE-BFDAT:CONFIG=CONT,FCTBLK=5,FUNCTION=WAML;
```

>>>>> HFA with 140 circuits with 70 B channels

```
CHANGE-BFDAT:CONFIG=CONT,FCTBLK=5,FUNCTION=HG3530,LINECNT=140,BCHLCNT=70;
```

>>>>> End configuration of block

```
CHANGE-BFDAT:CONFIG=OK,FCTBLK=5,ANSW=YES;
```

Functional block 6

/* Functional block 6: Adding the functions IP trunking (HG3550) and HFA subscriber (HG3530)

```
ADD-BFDAT:FCTBLK=6,FUNCTION=HG3550&HG3530,BRDBCHL=BCHAN120;
```

>>>>> IP trunking with one circuit with 30 B channels

```
CHANGE-BFDAT:CONFIG=CONT,FCTBLK=6,FUNCTION=HG3550,LINECNT=1,UNITS=3;
```

>>>>> HFA with 90 circuits with 90 B channels

```
CHANGE-BFDAT:CONFIG=CONT,FCTBLK=6,FUNCTION=HG3530,LINECNT=90,BCHLCNT=90;
```

>>>>> End configuration of this block

```
CHANGE-BFDAT:CONFIG=OK,FCTBLK=6,ANSW=YES;
```

Functional block 7

/* Functional block 7: IP trunking, HFA subscriber function (HG3530) and reserve HFA subscriber (HG3530R)

IMPORTANT: The reserved HFA B channels must be specified during configuration of the HG3530 function as subscriber B channels are not accepted during reservation.

```
ADD-BFDAT:FCTBLK=7,FUNCTION=HG3550&HG3530&HG3530R,BRDBCHL=BCHAN120;
```

>>>>> HFA with 80 circuits with 80 B channels and 20 reserve B channels

```
CHANGE-BFDAT:CONFIG=CONT,FCTBLK=7,FUNCTION=HG3530,LINECNT=80,BCHLCNT=100;
```

>>>>> Reserve HFA subscriber with 20 circuits

```
CHANGE-BFDAT:CONFIG=CONT,FCTBLK=7,FUNCTION=HG3530R,LINECNT=20;
```

>>>>> IP trunking with 10 circuits with one unit (=10 B channels)

```
CHANGE-BFDAT:CONFIG=CONT,FCTBLK=7,FUNCTION=HG3550,LINECNT=10,UNITS=1;
```

Displaying all functional blocks

```
DISPLAY-BFDAT;
H500:  AMO BFDAT STARTED
------------------------------------------------------------------------------
| FCTBLK =  1    BRDBCHL: BCHAN120                    STATUS=      OK          |
------------------------------------------------------------------------------
|  1st FUNCT : HG3570       1 LINES    UNITS ??  BCHLCNT 120  TOTAL BCHAN 120  |
------------------------------------------------------------------------------
------------------------------------------------------------------------------
| FCTBLK =  2    BRDBCHL : BCHL120                    STATUS=      OK          |
```

```
-------------------------------------------------------------------------------
|  1st FUNCT : HG3570       1 LINES    UNITS 30  BCHLCNT  30  TOTAL BCHAN  30  |
|  2nd FUNCT : HG3550       1 LINES    UNITS  3  BCHLCNT  30  TOTAL BCHAN  30  |
|  3rd FUNCT : HG3530      60 LINES    UNITS 60  BCHLCNT  60  TOTAL BCHAN  60  |
-------------------------------------------------------------------------------
-------------------------------------------------------------------------------
| FCTBLK =  3    BRDBCHL : BCHL120                  STATUS=      OK           |
-------------------------------------------------------------------------------
|  1st FUNCT : HG3570       1 LINES    UNITS 30  BCHLCNT  30  TOTAL BCHAN  30  |
|  2nd FUNCT : HG3550       1 LINES    UNITS  3  BCHLCNT  30  TOTAL BCHAN  30  |
|  3rd FUNCT : WAML         1 LINES    UNITS  3  BCHLCNT  30  TOTAL BCHAN  30  |
|  4th FUNCT : HG3530      30 LINES    UNITS 30  BCHLCNT  30  TOTAL BCHAN  30  |
-------------------------------------------------------------------------------
-------------------------------------------------------------------------------
| FCTBLK =  4    BRDBCHL : BCHL120                  STATUS=      OK           |
-------------------------------------------------------------------------------
|  1st FUNCT : HG3570       1 LINES    UNITS 30  BCHLCNT  30  TOTAL BCHAN  30  |
|  2nd FUNCT : HG3550       1 LINES    UNITS  1  BCHLCNT  10  TOTAL BCHAN  10  |
|  3rd FUNCT : WAML         1 LINES    UNITS  1  BCHLCNT  10  TOTAL BCHAN  10  |
|  4th FUNCT : HG3530      70 LINES    UNITS 70  BCHLCNT  70  TOTAL BCHAN  70  |
-------------------------------------------------------------------------------
-------------------------------------------------------------------------------
| FCTBLK =  5    BRDBCHL : BCHL120                  STATUS=    CONT           |
-------------------------------------------------------------------------------
|  1st FUNCT : HG3570       1 LINES    UNITS 30  BCHLCNT  30  TOTAL BCHAN  30  |
|  2nd FUNCT : HG3550       1 LINES    UNITS  1  BCHLCNT  10  TOTAL BCHAN  10  |
|  3rd FUNCT : WAML         1 LINES    UNITS  1  BCHLCNT  10  TOTAL BCHAN  10  |
|  4th FUNCT : HG3530     140 LINES    UNITS 70  BCHLCNT  70  TOTAL BCHAN  70  |
-------------------------------------------------------------------------------
-------------------------------------------------------------------------------
| FCTBLK =  6    BRDBCHL : BCHL120                  STATUS=      OK           |
-------------------------------------------------------------------------------
|  1st FUNCT : HG3550       1 LINES    UNITS  3  BCHLCNT  30  TOTAL BCHAN  30  |
|  2nd FUNCT : HG3530      90 LINES    UNITS 90  BCHLCNT  90  TOTAL BCHAN  90  |
-------------------------------------------------------------------------------
-------------------------------------------------------------------------------
| FCTBLK =  7    BRDBCHL : BCHL120                  STATUS=      OK           |
-------------------------------------------------------------------------------
|  1st FUNCT : HG3530      80 LINES    UNITS 80  BCHLCNT 100  TOTAL BCHAN 100  |
|  2nd FUNCT : HG3530R     20 LINES    UNITS 20  BCHLCNT   0  TOTAL BCHAN   0  |
|  3rd FUNCT : HG3550      10 LINES    UNITS 10  BCHLCNT  10  TOTAL BCHAN  10  |
-------------------------------------------------------------------------------
AMO-BFDAT-54        CONFIGURATION OF FUNCTIONAL BLOCKS FOR CGW BOARDS
DISPLAY COMPLETED;
  <
```

2.16.3 Configuring the Common Gateway Board with the AMO BCSU

Assignment for functional block 1

```
ADD-BCSU:TYPE=IPGW,LTG=1,LTU=2,SLOT=37,PARTNO=Q2316-X10,FCTID=1,FCTBLK=1,IPAD►
DR=198.16.16.45;
DISPLAY-BCSU:TYPE=TBL,LTG=1,LTU=2;
H500:  AMO BCSU  STARTED
```

```
ADDRESS :  LTG  1   LTU 2    SOURCE GROUP 1    ALARMNO-LTU 0

-----+-----------+--------+---+-+-+---+-+------------+------------+------------
     |           |        |   |S|H|AL-| |            |            |
     | ASSIGNED  | MODULE |FCT|E|W|ARM| | INSERTED   |    HW-     | MODULE
 PEN | MODULE    | TYPE   |ID |C|Y|NO | | MODULE     |STATE INFO  | STATUS
-----+-----------+--------+---+-+-+---+-+------------+------------+------------
  19 | Q2258-X    ACGEN             0|*| AVAILABLE  |            | NPR
  25 | Q2205-X    WAML       1   A  0|*|            |            | NPR
  31 | AVAILABLE                    0| | AVAILABLE  |            |
  37 | Q2316-X10  STMI2      1   A  0|*|            |            | NPR
     +--------------------------------+-+------------+------------+------------
     | IP ADDRESS : 198. 16. 16. 45         B-CHANNELS : 120    BCHLCNT :   2
     | BLOCK NO   :   1                     PRERESERVED LINES ASSIGNED  :  NO
     |  1st FUNCT  : STMI2-IPDA    1 LINES   B-CHANNELS : 120    BCHLCNT :   2
     +--------------------------------+-+------------+------------+------------
  43 | Q6401-X    PBCDG-FU   3   A  0|*|            |            | NPR
  49 | AVAILABLE                    0| | AVAILABLE  |            |
  55 | Q2214-X    TMOM2          A  0|*|            |            | NPR
  61 | Q2195-X    DIU-N4     1   A  0|*|            |            | NPR
  67 |                              0| |            |            |
  73 | Q2248-X    LTUCE             0|*| AVAILABLE  |            | NPR
  79 | Q2096-X200 DIU-S2         A  0|*|            |            | NPR
  85 | Q2096-X200 DIU-S2         A  0|*|            |            | NPR
  91 | Q2096-X200 DIU-S2         A  0|*|            |            | NPR
  97 | Q2096-X200 DIU-S2         A  0|*|            |            | NPR
 103 | AVAILABLE                    0| | AVAILABLE  |            |
 109 | AVAILABLE                    0| | AVAILABLE  |            |
 115 | Q2096-X200 DIU-S2         A  0|*|            |            | NPR
 121 | Q2174-X    STMD           A  0|*|            |            | NPR
DISPLAY COMPLETED;
```

Assignment for functional block 2

```
ADD-BCSU:TYPE=IPGW,LTG=1,LTU=1,SLOT=31,PARTNO=Q2316-X10,FCTID=1,FCTBLK=2,IPAD►
DR=198.16.16.31;
```

Assignment for functional block 3

```
ADD-BCSU:TYPE=IPGW,LTG=1,LTU=1,SLOT=37,PARTNO=Q2316-X10,FCTID=1,FCTBLK=3,IPAD►
DR=198.16.16.37;
```

Assignment for functional block 4

```
ADD-BCSU:TYPE=IPGW,LTG=1,LTU=1,SLOT=43,PARTNO=Q2316-X10,FCTID=1,FCTBLK=4,IPAD►
DR=198.16.16.43;
```

Assignment for functional block 5

```
ADD-BCSU:TYPE=IPGW,LTG=1,LTU=1,SLOT=49,PARTNO=Q2316-X10,FCTID=1,FCTBLK=5,IPAD►
DR=198.16.16.49;
```

Assignment for functional block 6

```
ADD-BCSU:TYPE=IPGW,LTG=1,LTU=1,SLOT=55,PARTNO=Q2316-X10,FCTID=1,FCTBLK=6,IPAD►
DR=198.16.16.55;
```

Assignment for functional block 7

```
ADD-BCSU:TYPE=IPGW,LTG=1,LTU=1,SLOT=61,PARTNO=Q2316-X10,FCTID=1,FCTBLK=7,IPAD►
DR=198.16.16.59;
```

Converting reserved HFA circuits to usable circuits

```
CHANGE-BCSU:TYPE=IPGW,LTG=1,LTU=1,SLOT=61,CHNGRSLN=13;
DISPLAY-BCSU:TYPE=TBl,LTG=1,LTU=1;
H500:  AMO BCSU  STARTED
ADDRESS :  LTG  1   LTU 1    SOURCE GROUP 1    ALARMNO-LTU 0
-----+----------+--------+---+-+-+---+-+-----------+-----------+-----------
     |          |        |   |S|H|AL-| |           |           |
     | ASSIGNED | MODULE |FCT|E|W|ARM| | INSERTED  |    HW-    | MODULE
 PEN | MODULE   | TYPE   |ID |C|Y|NO | | MODULE    |STATE INFO | STATUS
-----+----------+--------+---+-+-+---+-+-----------+-----------+-----------
  19 | Q7065-X    APPS              0|*| AVAILABLE |           | NPR
  25 | Q2117-X    SLMS          A   0|*|           |           | NPR
  31 | Q2316-X10  STMI2     1   A   0|*|           |           | NPR
     +--------------------------------+-+-----------+-----------+-----------
     | IP ADDRESS : 198. 16. 16. 31         B-CHANNELS : 120    BCHLCNT : 120
     | BLOCK NO   :   2                     PRERESERVED LINES ASSIGNED  :  NO
     |  1st FUNCT  : STMI2-IPDA    1 LINES   B-CHANNELS :  30    BCHLCNT :  30
     |  2nd FUNCT  : STMI2-IPGW    1 LINES   B-CHANNELS :  30    BCHLCNT :  30
     |  3rd FUNCT  : STMI-HFA2    60 LINES   B-CHANNELS :  60    BCHLCNT :  60
     +--------------------------------+-+-----------+-----------+-----------
  37 | Q2316-X10  STMI2     1   A   0|*|           |           | NPR
     +--------------------------------+-+-----------+-----------+-----------
     | IP ADDRESS : 198. 16. 16. 37         B-CHANNELS : 120    BCHLCNT : 120
     | BLOCK NO   :   3                     PRERESERVED LINES ASSIGNED    NO
     |  1st FUNCT  : STMI2-IPDA    1 LINES   B-CHANNELS :  30    BCHLCNT :  30
     |  2nd FUNCT  : STMI2-IPGW    1 LINES   B-CHANNELS :  30    BCHLCNT :  30
     |  3rd FUNCT  : STMI2-WAML    1 LINES   B-CHANNELS :  30    BCHLCNT :  30
     |  4th FUNCT  : STMI-HFA2    30 LINES   B-CHANNELS :  30    BCHLCNT :  30
     +--------------------------------+-+-----------+-----------+-----------
  43 | Q2316-X10  STMI2     1   A   0|*|           |           | NPR
     +--------------------------------+-+-----------+-----------+-----------
     | IP ADDRESS :  198. 16. 16. 43        B-CHANNELS : 120    BCHLCNT : 120
     | BLOCK NO   :   4                     PRERESERVED LINES ASSIGNED  :  NO
     |  1st FUNCT  : STMI2-IPDA    1 LINES   B-CHANNELS :  30    BCHLCNT :  30
     |  2nd FUNCT  : STMI2-IPGW    1 LINES   B-CHANNELS :  10    BCHLCNT :  10
     |  3rd FUNCT  : STMI2-WAML    1 LINES   B-CHANNELS :  10    BCHLCNT :  10
     |  4th FUNCT  : STMI-HFA2    70 LINES   B-CHANNELS :  70    BCHLCNT :  70
     +--------------------------------+-+-----------+-----------+-----------
  49 | Q2316-X10  STMI2     1   A   0|*|           |           | NPR
     +--------------------------------+-+-----------+-----------+-----------
     | IP ADDRESS : 198. 16. 16. 49         B-CHANNELS : 120    BCHLCNT : 120
     | BLOCK NO   :   5                     PRERESERVED LINES ASSIGNED  :  NO
     |  1st FUNCT  : STMI2-IPDA    1 LINES   B-CHANNELS :  30    BCHLCNT :  30
     |  2nd FUNCT  : STMI2-IPGW    1 LINES   B-CHANNELS :  10    BCHLCNT :  10
     |  3rd FUNCT  : STMI2-WAML    1 LINES   B-CHANNELS :  10    BCHLCNT :  10
     |  4th FUNCT  : STMI-HFA2   140 LINES   B-CHANNELS :  70    BCHLCNT :  70
     +--------------------------------+-+-----------+-----------+-----------
  55 | Q2316-X10  STMI2     1   A   0|*|           |           | NPR
     +--------------------------------+-+-----------+-----------+-----------
     | IP ADDRESS :  198. 16. 16. 55        B-CHANNELS : 120    BCHLCNT : 120
     | BLOCK NO   :   6                     PRERESERVED LINES ASSIGNED  :  NO
```

```
     |  1st FUNCT  : STMI2-IPGW    1 LINES   B-CHANNELS :  30    BCHLCNT :  30
     |  2nd FUNCT  : STMI-HFA2    90 LINES   B-CHANNELS :  90    BCHLCNT :  90
     +-------------------------------+-+------------+------------+------------
  61 | Q2316-X10  STMI2      1   A   0|*|            |            | NPR
     +-------------------------------+-+------------+------------+------------
     | IP ADDRESS :  198. 16. 16. 59        B-CHANNELS : 120    BCHLCNT : 120
     | BLOCK NO   :   7                     PRERESERVED LINES ASSIGNED  : YES
     |  1st FUNCT  : STMI-HFA2    93 LINES   B-CHANNELS : 100    BCHLCNT : 100
     |  2nd FUNCT  : STMI-HFA2R    7 LINES   B-CHANNELS :   0    BCHLCNT :   0
     |  3rd FUNCT  : STMI2-IPGW   10 LINES   B-CHANNELS :  10    BCHLCNT :  10
     +-------------------------------+-+------------+------------+------------
  67 | AVAILABLE                      0| | AVAILABLE  |            |
  73 | Q2248-X    LTUCE               0|*| AVAILABLE  |            | NPR
  79 | Q2164-X    SLMO16     1   A    0|*|            |            | NPR
  85 | Q2168-X    SLMO24     1   A    0|*|            |            | NPR
  91 | Q2153-X100 SLMQ           A    0|*|            |            | NPR
  97 | Q2150-X    SLMB           A    0|*|            |            | NPR
 103 | Q2480-X    SLMAR          A    0|*|            |            | NPR
 109 | Q2246-X    SLMA24         A    0|*|            |            | NPR
 115 | Q2025-X300 TMBD           A    0|*|            |            | NPR
 121 | AVAILABLE                      0| | AVAILABLE  |            |
AMO-BCSU -54        BOARD CONFIGURATION, SWITCHING UNIT
DISPLAY COMPLETED;
```

Seven common gateway boards (in this case: Q2316-X10, STMI2) have been configured.

2.16.4 Configuring SIP Trunking

Configuring SIP trunking on the STMI2 board in 1-1-55:

```
ADD-CGWB:LTU=1,SLOT=55,SMODE=NORMAL,IPADDR=198.16.16.55,NET►
MASK=255.255.255.0,TRPRSIP=30;
```

IMPORTANT: Starting with V10R0 the support for STMI2 will not be offered anymore. The replacement for STMI2 is STMIX/ STMIY.

IMPORTANT: Only one trunking protocol can be configured for each common gateway board.

2.16.5 Completed and Uncompleted Functional Block

2.16.5.1 Uncompleted functional block

/* Functional block 4: Adding the functions IPDA (HG3570), IP trunking (HG3550), WAML and HFA subscriber (HG3530)

```
ADD-BFDAT:FCTBLK=4,FUNCTION=HG3570&HG3550&WAML&HG3530,BRDBCHL=BCHAN120;
```

>>>>> IPDA with 30 B channels

```
CHANGE-BFDAT:CONFIG=CONT,FCTBLK=4,FUNCTION=HG3570,BCHLCNT=30;
```

>>>>> IP trunking with one circuit and one unit (=10 B channels)

```
CHANGE-BFDAT:CONFIG=CONT,FCTBLK=4,FUNCTION=HG3550,LINECNT=1,UNITS=1;
```

>>>>> WAML with one unit (=10 B channels)

```
CHANGE-BFDAT:CONFIG=CONT,FCTBLK=4,FUNCTION=WAML;
```

>>>>> HFA with 70 circuits and 70 B channels

```
CHANGE-BFDAT:CONFIG=CONT,FCTBLK=4,FUNCTION=HG3530,LINECNT=70,BCHLCNT=70;
```

>>>>> Do not end configuration of block

```
CHANGE-BFDAT:CONFIG=OK,FCTBLK=4,ANSW=NO;
```

Displaying a functional block

```
DISPLAY-BFDAT:FCTBLK=4;
H500:  AMO BFDAT STARTED
-------------------------------------------------------------------------------
| FCTBLK =  4    BRDBCHL : BCHL120                    STATUS=   CONT            |
-------------------------------------------------------------------------------
|  1st FUNCT : HG3570       1 LINES    UNITS 30  BCHLCNT  30  TOTAL BCHAN  30  |
|  2nd FUNCT : HG3550       1 LINES    UNITS  1  BCHLCNT  10  TOTAL BCHAN  10  |
|  3rd FUNCT : WAML         1 LINES    UNITS  1  BCHLCNT  10  TOTAL BCHAN  10  |
|  4th FUNCT : HG3530      70 LINES    UNITS 70  BCHLCNT  70  TOTAL BCHAN  70  |
-------------------------------------------------------------------------------
AMO-BFDAT-54        CONFIGURATION OF FUNCTIONAL BLOCKS FOR CGW BOARDS
DISPLAY COMPLETED;
```

Assignment for functional block 4

```
ADD-BCSU:TYPE=IPGW,LTG=1,LTU=1,SLOT=43,PARTNO=Q2316-X10,FCTID=1,FCTBLK=4,IPAD►
DR=198.16.16.43;
H500:  AMO BCSU  STARTED
F89: THE GIVEN FUNCTIONAL BLOCK IS NOT COMPLETELY CONFIGURED.
     PLEASE FINISH CONFIGURATION BY MEANS OF AMO_BFDAT FIRST.
AMO-BCSU -54        BOARD CONFIGURATION, SWITCHING UNIT
ADD NOT COMPLETED;
```

IMPORTANT: If the configuration of a functional block with the AMO BFDAT is not completed, the block cannot be assigned to any board with the AMO BCSU. The functional block must be completely configured with the AMO BFDAT before the command can be successfully run.

2.16.5.2 Completed configuration block

>>>>> End configuration of block

```
CHANGE-BFDAT:CONFIG=OK,FCTBLK=4,ANSW=YES;
```

Displaying a functional block

```
DISPLAY-BFDAT:4;
H500:  AMO BFDAT STARTED
-------------------------------------------------------------------------------
| FCTBLK =  4    BRDBCHL : BCHL120                    STATUS=      OK           |
```

```
------------------------------------------------------------------------------
|  1st FUNCT : HG3570       1 LINES    UNITS 30  BCHLCNT  30  TOTAL BCHAN  30  |
|  2nd FUNCT : HG3550       1 LINES    UNITS  1  BCHLCNT  10  TOTAL BCHAN  10  |
|  3rd FUNCT : WAML         1 LINES    UNITS  1  BCHLCNT  10  TOTAL BCHAN  10  |
|  4th FUNCT : HG3530      70 LINES    UNITS 70  BCHLCNT  70  TOTAL BCHAN  70  |
------------------------------------------------------------------------------
AMO-BFDAT-54        CONFIGURATION OF FUNCTIONAL BLOCKS FOR CGW BOARDS
DISPLAY COMPLETED;
```

Assignment for functional block 4

```
ADD-BCSU:TYPE=IPGW,LTG=1,LTU=1,SLOT=43,PARTNO=Q2316-X10,FCTID=1,FCTBLK=4,IPAD►
DR=198.16.16.43;
H500:  AMO BCSU  STARTED
H01: BD  1.1 . 43 ASSIGNED
AMO-BCSU -54        BOARD CONFIGURATION, SWITCHING UNIT
ADD COMPLETED;
```

2.17 Resource Manager Functionality

2.17.1 General

With the resource management for the features HFA (without the feature HFA Mobile) and IPDA and DMC there are two different methods of resource administering, observing and evaluating:

- The available bandwidth in certain sectors of a network and the exploitation by connections and
- the (DSP) channels of the gateways.

The resource Manager (RM) exists in every OpenScape 4000 system since V2.0 up to the latest release and is always active. For the calculation of the bandwidth required, the RM has to have knowledge of the current topology of the IP network. If the topology is not configured, then the RM assumes that infinite bandwidth is available.

For what RM is necessary?

A kind of resource Management was already available in HiPath 4000 V1.0 for IPDA. The number of B channels, which are connected to the customer IP net, can be limited for a HG 3570/3575 board. But this method, which is still available, can not be used for all configurations.

- HFA phones in a company branch behind a WAN connection with limited bandwidth can only be controlled by the Resource Manager. SIP subscriber can be used as well. The configuration of SIP subscriber in the AMOs are identically to HFA subscribers.
- Several access points IP installed in one location, which are connected via a WAN with limited bandwidth to the Host (the path to the Host must be limited, not the calls between the access points).

The following concepts Sector and cluster are essential for the broader understanding of the function.

2.17.2 Key Terms

2.17.2.1 Sector

A sector is a section of a customer network defined at the network planning stage which is regarded in the framework of the resource management.

A sector can be assigned to either a gateway or an arbitrary section in the IP network.It is left to the user which physical equipment in the network combine to form a sector.In order not to complicate the administration, it is reasonably large, summarizing broadband sections and concentrating itself on particularly resource weak sections (e.g. narrowband connections in the WAN).

Sector definitions

- LAN sectors are sectors with unlimited bandwidth
- WAN sectors have a limited bandwidth and connect the LAN sectors
- Gateway (GW) sectors are sectors in HG 3570/3575
- HFA sectors are LAN sectors to which a HFA phone is connected

2.17.2.2 Cluster

The location of endpoints in the network is determined by their membership of a sector. To simplify the administration the endpoints (devices, trunks) that have the same accessibility are combined in a so called cluster. A cluster can contain:

- all HFA devices in the OpenScape 4000 system
- all HFA devices in one access point

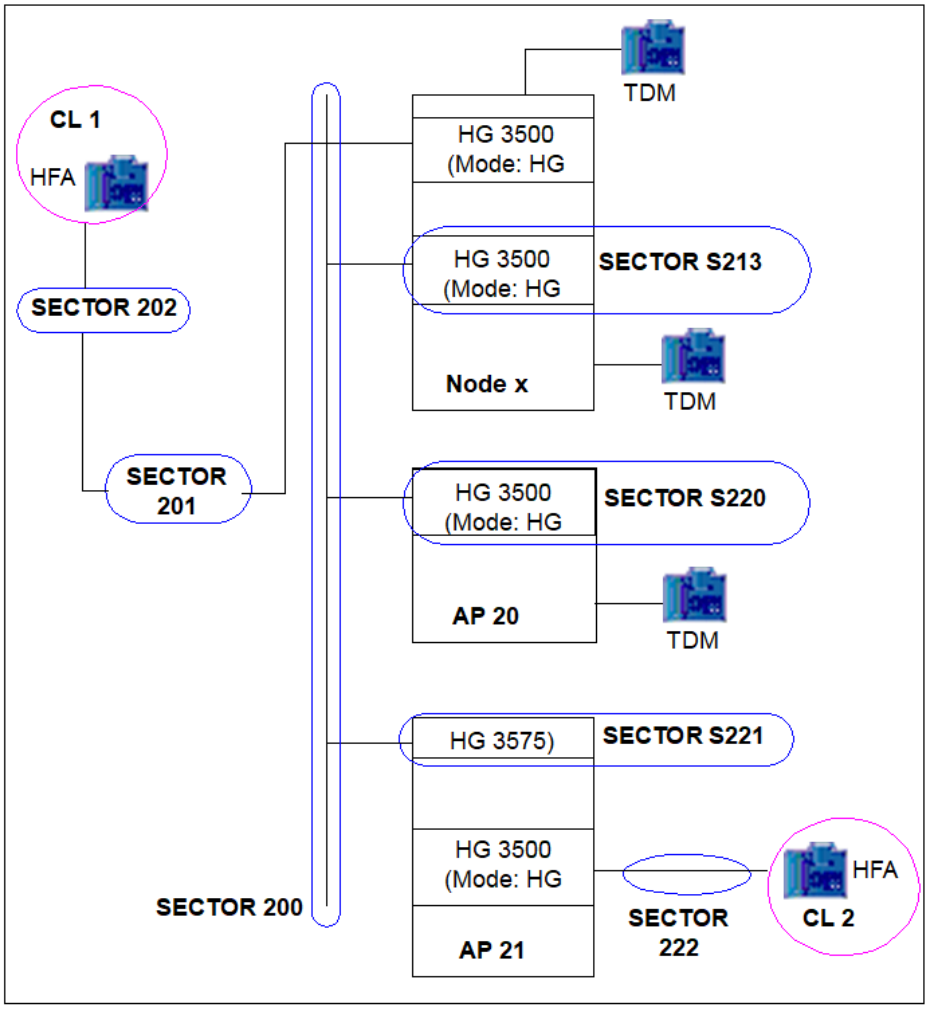


Figure 35: Sector /cluster definition in one OpenScape 4000 node (example)

HFA terminals can be assigned to different clusters even though they are configured on the same board.This is the case when the terminals are connected to different local area network/WAN sectors.

2.17.2.3 Sector Path

A sector path is the description of a way through the Customers LAN and WAN between two enpoints. A sector path is always defined from the perspective of the system for reaching a gateway sector or a LAN/WAN sector.

2.17.2.4 Definitions

2.17.2.4.1 AMO GKTOP: Parameters in the Branch TYPE=RESMGMT1

In principle, a distinction is made between the 2 sector types.

One sector type describes a gateway (GW), the other an IP segment of the customer's network (LAN or WAN), which have respectively to be established as sector attributes.

Further description to the Attributes:

SECATTR: GW

This attribute must be set for gateway sector (HG 3570/HG 3575). Every GW sector must be connected to a LAN sector (unlimited bandwidth).

SECATTR: LAN / WAN

This attribute describes an IP segment in the customer's network. It has to be set only in addition to the attributes **OWN**&**EXCL**.

The following rule must be considered:

The attribute **LAN** must be set, if the sector in the customer IP net is unlimited.

The attribute **WAN** must be set, if the sector in the customer IP net is limited.

WAN sectors are always located between LAN sectors!

HFA phones are not configured at a WAN sector. They are always assigned to a LAN sector.

SECATTR: OWN & EXCL

The sector is managed by RM as an own (**OWN**) node exclusively (**EXCL**). Without the attribute **EXCL** the RM does not seize bandwidth (for LAN) or does not count Channels (GW).

SECATTR: HHS / AP

These attributes are to be set (either/or) only in addition to the attribute GW and identify the shelf types that the GW situated are.

If the attribute **AP** is set, a sector path must be assigned to this sector (GW).

SECATTR: NODMC

This attribute blocks DMC (Direct Media Connection), if this sector is used for a call.

Sector attribute Sector type	O W N	E X C L	A P	H H S	N O D M C
GW	X	X	A	A	
LAN/WAN	X	X			O

- The unrestricted used attributes are marked with "X".
- Attributes, which are inside of a group defined with double lines, marked with "A" can only be used alternatively.
- Attributes, marked with "O", can be set optionally (depending on the use case).

The administration of the following parameters can be dispensed with depending on application case (sector types/attributes).

BANDWI:

Bandwidth in Kbit/s (Attention: BANDWI=0 means unlimited!)

GWLAN:

Sector number of the LAN in which the gateway is connected. The used B channels of a HG 3570/HG 3575 board can only be displayed with AMO GKTOP, if the **GWLAN** number is entered.

SECPANO1:

Sector path number 1 is used for the feature HFA and IPDA. Sector -path number 1 (**SECPANO1**) defines the way from the host to the remote sector, at which HFA phones or a HG 3575 gateway is connected to.

Under this sector path number all sectors passed through to reach this sector from a HHS are entered. The sector path number 1 begins with the sector nearest the HHS and ends with the most remote.

All sectors, which are between the HHS and the end point, have to be entered for this sector path.

The destination sector is not part of the sector path.

Because the RM is not released for IP trunking, the **SECPANO2** and **SECPANO3** are not used.

Example for the illustration “Example of Sector/cluster definition.....”: Sector path for cluster 1: 200&201 (not 202)

2.17.2.4.2 AMO GKTOP: Parameter in the Branch TYPE=IPDA (only for HFA)

GWSEC

A **GWSEC** must only be defined, if a HG 3530 is installed in an AP-IP. In this case the sector number of the HG 3575 must be entered.

HFASEC

For cluster with HFA phones the sector number of the LAN to which the phones are connected is entered.

2.17.3 Configuration Rules

- To each HG 3570/3575 a GW sector must be assigned.
- Every GW sector must be connected to a LAN sector (**BANDW=0**, unlimited bandwidth).
- A sector path has to be assigned to every endpoint. Endpoints include:
  - A GW sector in the access point (HG 3575)
  - A HFA sector
- The endpoint (GW sector / HFA sector) is not part of the path description.
- A cluster ID has to be assigned to all HFA subscribers.
- A cluster ID whose HFA subscribers are configured in the host system must be assigned to a HFA sector.
- A cluster ID whose HFA subscribers are configured in the access point must be assigned to a HFA sector and the GW sector of the access point.

2.17.4 Used Bandwidth

```
DISPLAY-SIPCO:TYPE=BANDW;
```

IMPORTANT: Bandwidth table must be adjust customer specific. `CHANGE-SIPCO:TYPE=BANDW,.....;`

2.17.5 Configuring the Resource Management for a HFA Configuration

2.17.5.1 Basic Situation

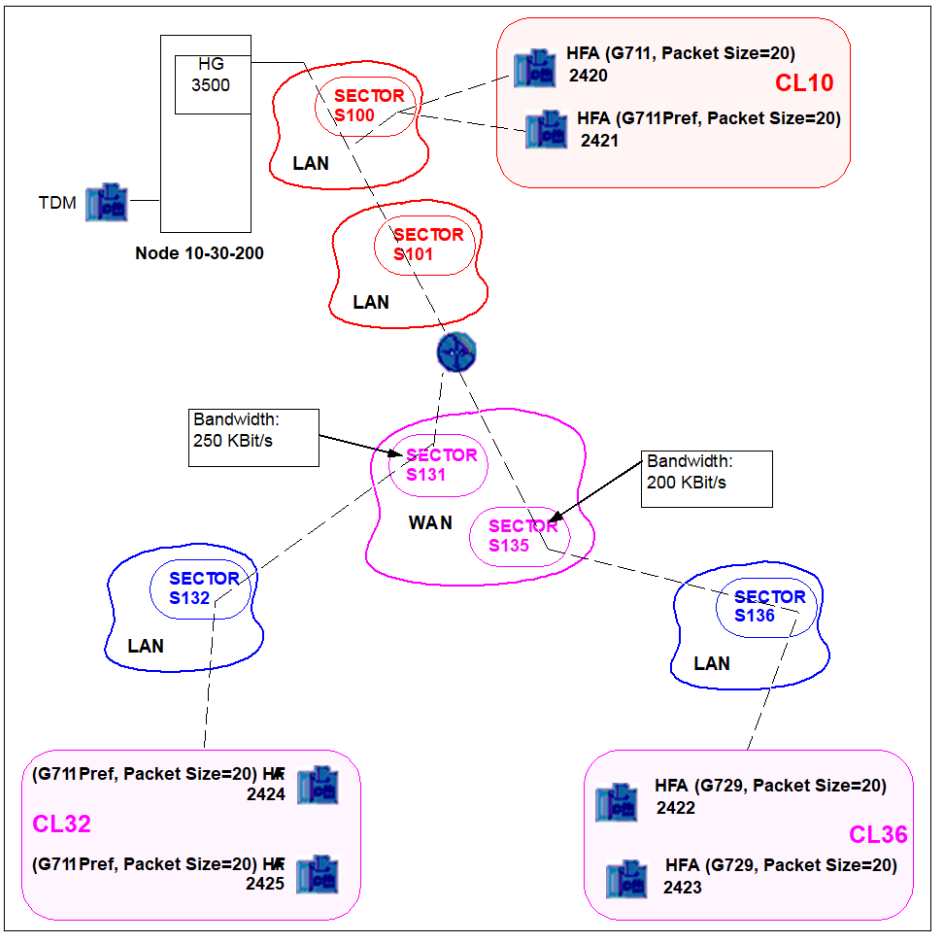


Figure 36: Resource management for HFA configuration

Network plan for the Resource Management

The basic situation is as following:

At node 10-30-200 there is the feature HFA. This feature is already configured. It is assumed that four (2x2) HFA subscribers lay behind a bandwidth limited WAN routes and two HFA phones are located in the local IP network of the Host. These routes are described for the resource management in sectors131/135 (limited bandwidth), sectors 132/136 (HFA in the local unlimited LAN) and the sectors 100/101 (local, unlimited network at the Host).The sector 101 is only used to describe a DMC connection between cluster 32 and 36.

Sector paths have to be defined, that a connection from sector 132N (136) to the Host can be calculated.

The HFA subscriber are set in cluster 32 (to S132), cluster 36 (to S136) and cluster 10 (to S100).

All HFA subscribers have the attribute “DMC allowed”:

```
CHANGE-SDAT:STNO=2420&&2425,TYPE=ATTRIBUT,AATTR=DMCALLWD;
```

The RTP-sample size has an influence on the bandwidth. All IP-phones in this documentation are using 20ms sample size for both G711 and G.729A. This can be configured in the database of the IP-phone or via DLS.

2.17.5.2 Codec Settings for the HFA Subscribers

The codec information used for a call must be available to the resource manager in order to calculate the required bandwidth.

In the case of HFA terminals, the setting in the AMO **must** match the setting in the terminal (configuration). In our example, the HFA subscribers have been configured via DLS or the local WBM such that the HFA devices in the host prefer G.711 and the HFA subscribers behind the WAN route force G.729A.

The sample size of the IP phones impacts the required bandwidth. A sample size of 20ms is assumed here both for G.711 and G.729 A. These values can be changed on the terminal (or via DLS).

```
CHANGE-SBCSU:STNO=2420&2421,OPT=OPTI,IPCODEC=G711P;
CHANGE-SBCSU:STNO=2422&2423,OPT=OPTI,IPCODEC=G729A;
CHANGE-SBCSU:STNO=2424&2425,OPT=OPTI,IPCODEC=G711P;
```

2.17.5.3 Sectors for the LAN/WAN

The sectors, which describe the LAN/WAN are defined first. These are the sectors S100, S101, S131, S132, S135 and S136. The sectors S131 and S135 are WAN sectors. The bandwidth is limited to 200kBits/s and 250 kBits/s.

Sector 100, 101, 132 and 136:

The attributes **OWN**&**EXCL** must be entered. The sectors are LAN sectors with unlimited bandwidth.

```
ADD-GKTOP:TYPE=RESMGMT1,SECNO=100,SECATTR=OWN&EXCL&LAN,PNNO=10-30-200,BAND►
WI="0";
ADD-GKTOP:TYPE=RESMGMT1,SECNO=101,SECATTR=OWN&EXCL&LAN,PNNO=10-30-200,BAND►
WI="0";
ADD-GKTOP:TYPE=RESMGMT1,SECNO=132,SECATTR=OWN&EXCL&LAN,PNNO=10-30-200,BAND►
WI="0";
ADD-GKTOP:TYPE=RESMGMT1,SECNO=136,SECATTR=OWN&EXCL&LAN,PNNO=10-30-200,BAND►
WI="0";
```

Sector 131 and 135:

The attributes **OWN**&**EXCL** must be entered. The sectors are WAN sectors with limited bandwidth.

```
ADD-GKTOP:TYPE=RESMGMT1,SECNO=131,SECATTR=OWN&EXCL&WAN,PNNO=10-30-200,BAND►
WI="250";
ADD-GKTOP:TYPE=RESMGMT1,SECNO=135,SECATTR=OWN&EXCL&WAN,PNNO=10-30-200,BAND►
```

```
WI="200";
```

2.17.5.4 Allocation of the Gateways and Subscribers

Here is defined that the subscribers 2420 and 2421 are in cluster 10 and attached to HFA LAN (sector 100).

```
ADD-GKTOP:TYPE=IPDA,CLUSTNO=10,HFASEC=100;
CHANGE-SDAT:STNO=2420,TYPE=DATA1,CLUSTID=10;
CHANGE-SDAT:STNO=2421,TYPE=DATA1,CLUSTID=10;;
```

Here is defined that the subscribers 2422 and 2423 are in cluster 36 and attached to HFA LAN (sector 136).

```
ADD-GKTOP:TYPE=IPDA,CLUSTID=36,HFASEC=136;
CHANGE-SDAT:STNO=2422,TYPE=DATA1,CLUSTID=36;
CHANGE-SDAT:STNO=2423,TYPE=DATA1,CLUSTID=36;;
```

Here is defined that the subscribers 2424 and 2425 are in cluster 32 and attached to HFA LAN (sector 132).

```
ADD-GKTOP:TYPE=IPDA,CLUSTID=32,HFASEC=132;
CHANGE-SDAT:STNO=2424,TYPE=DATA1,CLUSTID=32;
CHANGE-SDAT:STNO=2425,TYPE=DATA1,CLUSTID=32;;
```

Example for the bandwidth situation after these steps:

Call situation from 2424 to 2425 (cluster internal).

```
DISPLAY-GKTOP:TYPE=ALL,SCOPE=DYN;
   ---------+-------------------------------------------------------------+

   SECTOR   |               100                                           |

   ---------+-------------------------------------------------------------+

   PNNO     |        10- 30-200                                           |

   ---------+-------------------------------------------------------------+

   S-BW     |        UNLIMITED                                            |

   USED-BW  |                 0                                           |

   R-GW-MC  |                 0                                           |

   R-GW-DMC |                 0                                           |

   ---------+-------------------------------------------------------------+

   SECTOR   |               101                                           |

   ---------+-------------------------------------------------------------+

   PNNO     |        10- 30-200                                           |

   ---------+-------------------------------------------------------------+

   S-BW     |        UNLIMITED                                            |
```

```
USED-BW  |                0                                          |
R-GW-MC  |                0                                          |
R-GW-DMC |                0                                          |
---------+-----------------------------------------------------------+
SECTOR   |              131                                          |
---------+-----------------------------------------------------------+
PNNO     |        10- 30-200                                         |
---------+-----------------------------------------------------------+
S-BW     |              250                                          |
USED-BW  |                0                                          |
R-GW-MC  |                0                                          |
R-GW-DMC |                0                                          |
---------+-----------------------------------------------------------+
SECTOR   |              132                                          |
---------+-----------------------------------------------------------+
PNNO     |        10- 30-200                                         |
---------+-----------------------------------------------------------+
S-BW     |        UNLIMITED                                          |
USED-BW  |              182                                          |
R-GW-MC  |                0                                          |
R-GW-DMC |                0                                          |
---------+-----------------------------------------------------------+
SECTOR   |              135                                          |
---------+-----------------------------------------------------------+
PNNO     |        10- 30-200                                         |
---------+-----------------------------------------------------------+
S-BW     |              200                                          |
USED-BW  |                0                                          |
```

```
   R-GW-MC  |                 0                                                |
   R-GW-DMC |                 0                                                |
   ---------+------------------------------------------------------------------+
   SECTOR   |               136                                                |
   ---------+------------------------------------------------------------------+
   PNNO     |        10- 30-200                                                |
   ---------+------------------------------------------------------------------+
   S-BW     |        UNLIMITED                                                 |
   USED-BW  |                 0                                                |
   R-GW-MC  |                 0                                                |
   R-GW-DMC |                 0                                                |
   ---------+------------------------------------------------------------------+

DISPLAY-SIPCO:TYPE=BANDW;

  BANDWIDTH COMPUTING TABLE :

  ------------------------------------------------------------------------
  +-------+----------------------+-----------------+---------------+
  | INDEX |  CODEC TYPE          |   FRAME SIZE    |    RESERVED   |
  |       |                      |      (MS)       | BANDW.(KBIT)  |
  +-------+----------------------+-----------------+---------------+
  |    1  | G711_HFA             |       30        |        89     |
  |    2  | G729_HFA             |       40        |        22     |
  |    3  | G723_HFA             |       30        |        25     |
  |    4  | G711_F10_IPDA        |       10        |       120     |
  |    5  | G711_F20_IPDA        |       20        |        92     |
  |    6  | G711_F30_IPDA        |       30        |        83     |
  |    7  | G711_F60_IPDA        |       60        |        74     |
  |    8  | G729_F20_IPDA        |       20        |        36     |
```

```
|    9  | G729_F40_IPDA        |       40        |        22     |

|   10  | G729_F60_IPDA        |       60        |        18     |

|   11  | G711_DMC             |       30        |       182     |

|   12  | G729_DMC             |       40        |        72     |

|   13  | G723_DMC             |       30        |        27     |

|   14  | G711_FS_UNKNOWN      |       60        |        83     |
```

Interpretation:

Only bandwidth in sector 132, to which the subscribers are assigned, is reserved. Both subscribers are using G711 with DMC (AMO SIPCO:BANDW -> Index 11). If the value of the bandwidth of index 11 is smaller as the double value of index 1, two times of index 1 is calculated and displayed.

The bandwidth for the master connection is not reserved yet, because there are no sector paths defined at this moment.

All bandwidths used in these examples in the AMO SIPCO do not claim to be true. The defined values are used for demonstration purposes only!!! The table in the AMO SIPCO must always be configured for the respective customer.

2.17.5.5 Define Sector Paths

The sector paths are necessary to calculate the bandwidth in all used sectors.

In this example 2 sector paths are necessary.

Sector path 1 defines the path from the Host to the destination sector 132:

```
ADD-GKTOP:TYPE=SECPATH,SECPANO=1,SECDE=100&101&131;
```

Sector path 2 defines the path from the Host to the destination sector 136:

```
ADD-GKTOP:TYPE=SECPATH,SECPANO=2,SECDE=100&101&135;
```

2.17.5.6 Assign the sector paths

```
CHANGE-GKTOP:TYPE=RESMGMT1,SECNO=132,SECPANO1=1;
CHANGE-GKTOP:TYPE=RESMGMT1,SECNO=136,SECPANO1=2;
```

Example for the bandwidth situation after these steps:

Call situation from 2424 to 2425 (cluster internal).

```
DISPLAY-GKTOP:TYPE=ALL,SCOPE=DYN;
```

```
---------+-------------------------------------------------------------+
SECTOR   |               100                                           |
---------+-------------------------------------------------------------+
PNNO     |        10- 30-200                                           |
---------+-------------------------------------------------------------+
S-BW     |        UNLIMITED                                            |
```

```
   USED-BW  |               178                                          |
   R-GW-MC  |                 0                                          |
   R-GW-DMC |                 0                                          |
   ---------+------------------------------------------------------------+
   SECTOR   |               101                                          |
   ---------+------------------------------------------------------------+
   PNNO     |        10- 30-200                                          |
   ---------+------------------------------------------------------------+
   S-BW     |        UNLIMITED                                           |
   USED-BW  |               178                                          |
   R-GW-MC  |                 0                                          |
   R-GW-DMC |                 0                                          |
   ---------+------------------------------------------------------------+
   SECTOR   |               131                                          |
   ---------+------------------------------------------------------------+
   PNNO     |        10- 30-200                                          |
   ---------+------------------------------------------------------------+
   S-BW     |                72                                          |
   USED-BW  |               178                                          |
   R-GW-MC  |                 0                                          |
   R-GW-DMC |                 0                                          |
   ---------+------------------------------------------------------------+
   SECTOR   |               132                                          |
   ---------+------------------------------------------------------------+
   PNNO     |        10- 30-200                                          |
   ---------+------------------------------------------------------------+
   S-BW     |        UNLIMITED                                           |
   USED-BW  |               182                                          |
   R-GW-MC  |                 0                                          |
   R-GW-DMC |                 0                                          |
   ---------+------------------------------------------------------------+
   SECTOR   |               135                                          |
   ---------+------------------------------------------------------------+
   PNNO     |        10- 30-200                                          |
   ---------+------------------------------------------------------------+
   S-BW     |               200                                          |
   USED-BW  |                 0                                          |
   R-GW-MC  |                 0                                          |
   R-GW-DMC |                 0                                          |
   ---------+------------------------------------------------------------+
   SECTOR   |               136                                          |
   ---------+------------------------------------------------------------+
   PNNO     |        10- 30-200                                          |
   ---------+------------------------------------------------------------+
   S-BW     |        UNLIMITED                                           |
   USED-BW  |                 0                                          |
   R-GW-MC  |                 0                                          |
   R-GW-DMC |                 0                                          |
   ---------+------------------------------------------------------------+

DISPLAY-SIPCO:TYPE=BANDW;

  BANDWIDTH COMPUTING TABLE :
  ------------------------------------------------------------------
  +-------+----------------------+-----------------+---------------+
  | INDEX |  CODEC TYPE          |   FRAME SIZE    |   RESERVED    |
```

```
  |       |                      |      (MS)       |  BANDW.(KBIT) |
  +-------+----------------------+-----------------+---------------+
  |    1  | G711_HFA             |       30        |        89     |
  |    2  | G729_HFA             |       40        |        22     |
  |    3  | G723_HFA             |       30        |        25     |
  |    4  | G711_F10_IPDA        |       10        |       120     |
  |    5  | G711_F20_IPDA        |       20        |        92     |
  |    6  | G711_F30_IPDA        |       30        |        83     |
  |    7  | G711_F60_IPDA        |       60        |        74     |
  |    8  | G729_F20_IPDA        |       20        |        36     |
  |    9  | G729_F40_IPDA        |       40        |        22     |
  |   10  | G729_F60_IPDA        |       60        |        18     |
  |   11  | G711_DMC             |       30        |       182     |
  |   12  | G729_DMC             |       40        |        72     |
```

Interpretation:

The Resource Manager determines “resulting sector paths”, to reserve bandwidth for the master connection. Therefore the sector paths of both end points are compared. In this example the sector path of the A-party 2424 is S100&S101&S131, destination sector S132. The sector path of the B-party 2425 is S100&S101&S131, destination sector S132. This leads to the result, that all sectors are common sectors. Therefore the sectors S100, S101 and S131 must be the sectors for the master connection (reserved bandwidth with two times Index 1). The DMC connection uses the destination sector (sector S132). There the bandwidth of 182 kBit/s (Index 11) is reserved.

Second example for the bandwidth situation after these steps:

Call situation from 2424 to 2422 (cluster to cluster).

```
DISPLAY-GKTOP:TYPE=ALL,SCOPE=DYN;
   ---------+-------------------------------------------------------------+
   SECTOR   |               100                                           |
   ---------+-------------------------------------------------------------+
   PNNO     |        10- 30-200                                           |
   ---------+-------------------------------------------------------------+
   S-BW     |         UNLIMITED                                           |
   USED-BW  |               111                                           |
   R-GW-MC  |                 0                                           |
   R-GW-DMC |                 0                                           |
   ---------+-------------------------------------------------------------+
   SECTOR   |               101                                           |
   ---------+-------------------------------------------------------------+
   PNNO     |        10- 30-200                                           |
   ---------+-------------------------------------------------------------+
   S-BW     |        UNLIMITED                                            |
   USED-BW  |               182                                           |
   R-GW-MC  |                 0                                           |
   R-GW-DMC |                 0                                           |
   ---------+-------------------------------------------------------------+
   SECTOR   |               131                                           |
   ---------+-------------------------------------------------------------+
   PNNO     |        10- 30-200                                           |
   ---------+-------------------------------------------------------------+
   S-BW     |                68                                           |
   USED-BW  |               182                                           |
   R-GW-MC  |                 0                                           |
```

```
 R-GW-DMC |                 0                                                |
 ---------+------------------------------------------------------------------+
 SECTOR   |               132                                                |
 ---------+------------------------------------------------------------------+
 PNNO     |        10- 30-200                                                |
 ---------+------------------------------------------------------------------+
 S-BW     |        UNLIMITED                                                 |
 USED-BW  |               182                                                |
 R-GW-MC  |                 0                                                |
 R-GW-DMC |                 0                                                |
 ---------+------------------------------------------------------------------+
 SECTOR   |               135                                                |
 ---------+------------------------------------------------------------------+
 PNNO     |        10- 30-200                                                |
 ---------+------------------------------------------------------------------+
 S-BW     |                18                                                |
 USED-BW  |               182                                                |
 R-GW-MC  |                 0                                                |
 R-GW-DMC |                 0                                                |
 ---------+------------------------------------------------------------------+
 SECTOR   |               136                                                |
 ---------+------------------------------------------------------------------+
 PNNO     |        10- 30-200                                                |
 ---------+------------------------------------------------------------------+
 S-BW     |        UNLIMITED                                                 |
 USED-BW  |               182                                                |
 R-GW-MC  |                 0                                                |
 R-GW-DMC |                 0                                                |
 ---------+------------------------------------------------------------------+
```

```
DIS-SIPCO:TYPE=BANDW;

  BANDWIDTH COMPUTING TABLE :
  ---------------------------------------------------------------------
  +-------+----------------------+-----------------+----------------+
  | INDEX |  CODEC TYPE          |   FRAME SIZE    |    RESERVED    |
  |       |                      |      (MS)       |  BANDW.(KBIT)  |
  +-------+----------------------+-----------------+----------------+
  |    1  | G711_HFA             |       30        |        89      |
  |    2  | G729_HFA             |       40        |        22      |
  |    3  | G723_HFA             |       30        |        25      |
  |    4  | G711_F10_IPDA        |       10        |       120      |
  |    5  | G711_F20_IPDA        |       20        |        92      |
  |    6  | G711_F30_IPDA        |       30        |        83      |
  |    7  | G711_F60_IPDA        |       60        |        74      |
  |    8  | G729_F20_IPDA        |       20        |        36      |
  |    9  | G729_F40_IPDA        |       40        |        22      |
  |   10  | G729_F60_IPDA        |       60        |        18      |
  |   11  | G711_DMC             |       30        |       182      |
  |   12  | G729_DMC             |       40        |        72      |
  |   13  | G723_DMC             |       30        |        27      |
  |   14  | G711_FS_UNKNOWN      |       60        |        83      |
```

Interpretation:

The Resource Manager determines “resulting sector paths”, to reserve bandwidth for the master connection. Therefore the sector paths of both end

points are compared. In this example the sector path of the party A 2424 is S100&S101&S131, destination sector S132. The sector path of the party B 2422 is S100&S101&S135, destination sector S136. This leads to the result, that sector S101 is the last common sector. Therefore the sector S100 must be the sector for the master connection (reserved bandwidth with one time Index 1 plus one time Index 2). The DMC connection uses the last common sector (sector S101). The bandwidth of 182 kBit/s (Index 11) is reserved in all affected sectors (S101, S131, S135, S132 and S136).

2.17.6 Configuring the Resource Management for an IPDA Configuration with TDM Phones

2.17.6.1 Basic Situation

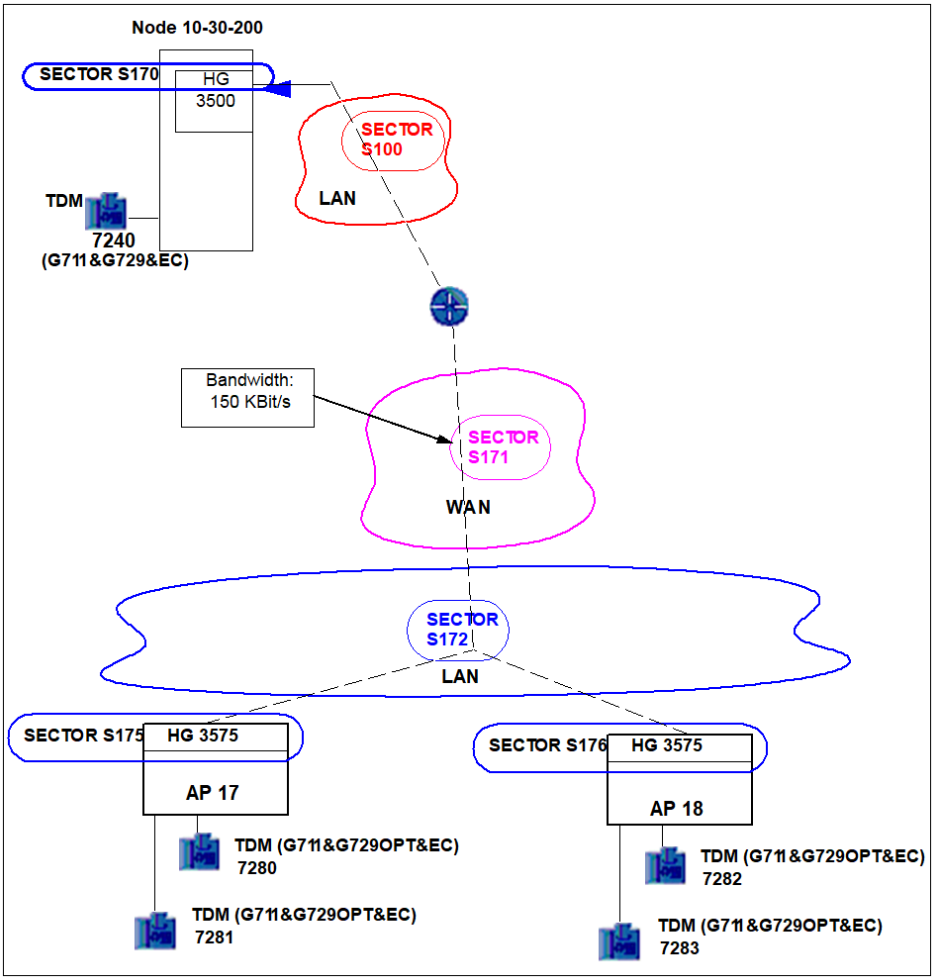


Figure 37: Resource management for IPDA configuration with TDM phones

The basic situation is as following:

There is the feature IPDA at node 10-30-200. The feature is already configured with access points 17 and 18. It is assumed, that both access points are located behind a bandwidth limited WAN. This situation is described for the resource management in sector S171 (bandwidth limited) and in bandwidth unlimited LAN sectors S100 (Host) and S172 (access points). gateway sectors are necessary for HG 3570 and HG 3575 in the IPDA feature (S170, S175 and S176). The sector S172 is necessary, to describe the direct connection between both HG 3575 gateways. Sector paths must be defined for the HG 3575 gateways, to describe their location to the Host correctly.

The Frame Size for G711 is set to 20 ms for all HG 3570/75:

```
CHANGE-CGWB:MTYPE=CGW,LTU=1,SLOT=61,TYPE=ASC,PRIO=PRIO2,CODEC=G711A,RTP=20;
CHANGE-STMIB:MTYPE=NCUI2,LTU=17,TYPE=ASC,PRIO=PRIO1,CODEC=G711A,RTP=20;
CHANGE-STMIB:MTYPE=NCUI2,LTU=18,TYPE=ASC,PRIO=PRIO1,CODEC=G711A,RTP=20;
```

The Codec G729 should be used for a call between a Host terminal and an AP terminal. The Codec G711 should be used for a call between an AP terminal of access point 17 and an AP terminal in access point 18.

```
CHANGE-SDAT:STNO=7240,TYPE=DATA1,CLASSMRK=G711&G729A&EC;
CHANGE-SDAT:STNO=7280&&7282,TYPE=DATA1,CLASSMRK=G711&G729AOPT&EC;
```

2.17.6.2 Sectors for the LAN/WAN

The sectors, which describe the LAN/WAN are defined first. These are the sectors S100, S171 and S172. The sector 171 ist a WAN sector. The bandwidth is limited to 150 kBit/s.

Sector 100 and 172:

The attributes **OWN**&**EXCL** must be entered. The sectors are LAN sectors with unlimited bandwidth.

```
ADD-GKTOP:TYPE=RESMGMT1,SECNO=100,SECATTR=OWN&EXCL&LAN,PNNO=10-30-200,BAND►
WI="0";
ADD-GKTOP:TYPE=RESMGMT1,SECNO=172,SECATTR=OWN&EXCL&LAN,PNNO=10-30-200,BAND►
WI="0";
```

Sector 171:

The attributes **OWN**&**EXCL** must be entered. The sector is a WAN sector with limited bandwidth.

```
ADD-GKTOP:TYPE=RESMGMT1,SECNO=171,SECATTR=OWN&EXCL&WAN,PNNO=10-30-200,BAND►
WI="150";
```

2.17.6.3 Sectors for the Gateways

The sectors S170, S175 and S176 are defined.

The sector 170 has the attributes **OWN**&**EXCL** (see before) and HHS (is located in the Host) and GW (is a gateway).

```
ADD-GKTOP:TYPE=RESMGMT1,SECNO=170,SECATTR=OWN&EXCL&HHS&GW,PNNO=10-30-200,GW►
LAN=100;
```

The sectors 175 and 176 have the attributes **OWN**&**EXCL** (see before) and AP (are located in an access point) and GW (are gateways).

```
ADD-GKTOP:TYPE=RESMGMT1,SECNO=175,SECATTR=OWN&EXCL&AP&GW,PNNO=10-30-200,GW►
LAN=172;
```

```
ADD-GKTOP:TYPE=RESMGMT1,SECNO=176,SECATTR=OWN&EXCL&AP&GW,PNNO=10-30-200,GW►
LAN=172;
```

2.17.6.4 Allocation of the Gateways to their Sectors

```
CHANGE-CGWB:MTYPE=CGW,LTU=1,SLOT=61,TYPE=GWSECTOR,GWSECTNO=170;
CHANGE-STMIB:MTYPE=NCUI2,LTU=17,TYPE=GWSECTOR,GWSECTNO=175;
CHANGE-STMIB:MTYPE=NCUI2,LTU=18,TYPE=GWSECTOR,GWSECTNO=176;
```

2.17.6.5 Define Sector Paths

In this example only one sector path is necessary, because access point 17 and 18 are reached via the same path from the Host.

```
ADD-GKTOP:TYPE=SECPATH,SECPANO=1,SECDE=100&171&172;
```

2.17.6.6 Assign the Sector Path

```
CHANGE-GKTOP:TYPE=RESMGMT1,SECNO=175,SECPANO1=1;
CHANGE-GKTOP:TYPE=RESMGMT1,SECNO=176,SECPANO1=1;
```

1st example for bandwidth reservation after these steps:

Call situation from 7280 to 7282 (GW SECTOR 175 to GW SECTOR 176).

```
DISPLAY-GKTOP:TYPE=ALL,SCOPE=DYN;
---------+-------------------------------------------------------------------+
   SECTOR   |               100                                               |
   ---------+-------------------------------------------------------------------+
   PNNO     |        10- 30-200                                               |
   ---------+-------------------------------------------------------------------+
   S-BW     |        UNLIMITED                                                |
   USED-BW  |                 0                                               |
   R-GW-MC  |                 0                                               |
   R-GW-DMC |                 0                                               |
   ---------+-------------------------------------------------------------------+
   SECTOR   |               170                                               |
   ---------+-------------------------------------------------------------------+
   PNNO     |        10- 30-200                                               |
   ---------+-------------------------------------------------------------------+
   S-BW     |        UNLIMITED                                                |
   USED-BW  |                 0                                               |
   R-GW-MC  |                60                                               |
   R-GW-DMC |                 0                                               |
   ---------+-------------------------------------------------------------------+
   SECTOR   |               171                                               |
   ---------+-------------------------------------------------------------------+
   PNNO     |        10- 30-200                                               |
   ---------+-------------------------------------------------------------------+
   S-BW     |               150                                               |
   USED-BW  |                 0                                               |
   R-GW-MC  |                 0                                               |
   R-GW-DMC |                 0                                               |
   ---------+-------------------------------------------------------------------+
```

```
   SECTOR   |               172                                                |
   ---------+------------------------------------------------------------------+
   PNNO     |        10- 30-200                                                |
   ---------+------------------------------------------------------------------+
   S-BW     |        UNLIMITED                                                 |
   USED-BW  |               184                                                |
   R-GW-MC  |                 0                                                |
   R-GW-DMC |                 0                                                |
   ---------+------------------------------------------------------------------+
   SECTOR   |               175                                                |
   ---------+------------------------------------------------------------------+
   PNNO     |        10- 30-200                                                |
   ---------+------------------------------------------------------------------+
   S-BW     |        UNLIMITED                                                 |
   USED-BW  |                 0                                                |
   R-GW-MC  |                59                                                |
   R-GW-DMC |                 0                                                |
   ---------+------------------------------------------------------------------+
   SECTOR   |               176                                                |
   ---------+------------------------------------------------------------------+
   PNNO     |        10- 30-200                                                |
   ---------+------------------------------------------------------------------+
   S-BW     |        UNLIMITED                                                 |
   USED-BW  |                 0                                                |
   R-GW-MC  |                59                                                |
   R-GW-DMC |                 0                                                |
   ---------+------------------------------------------------------------------+
```

```
DIS-SIPCO:TYPE=BANDW;
  BANDWIDTH COMPUTING TABLE :
  ------------------------------------------------------------------------
  +-------+----------------------+-----------------+---------------+
  | INDEX |  CODEC TYPE          |    FRAME SIZE   |   RESERVED    |
  |       |                      |       (MS)      |  BANDW.(KBIT) |
  +-------+----------------------+-----------------+---------------+
  |    1  | G711_HFA             |       30        |        89     |
  |    2  | G729_HFA             |       40        |        22     |
  |    3  | G723_HFA             |       30        |        25     |
  |    4  | G711_F10_IPDA        |       10        |       120     |
  |    5  | G711_F20_IPDA        |       20        |       184     |
  |    6  | G711_F30_IPDA        |       30        |        83     |
  |    7  | G711_F60_IPDA        |       60        |        74     |
  |    8  | G729_F20_IPDA        |       20        |        36     |
  |    9  | G729_F40_IPDA        |       40        |        22     |
  |   10  | G729_F60_IPDA        |       60        |        18     |
  |   11  | G711_DMC             |       30        |       182     |
  |   12  | G729_DMC             |       40        |        72     |
  |   13  | G723_DMC             |       30        |        27     |
  |   14  | G711_FS_UNKNOWN      |       60        |        83     |
```

Interpretation:

Only bandwidth in sector (172), which connect the two GW sectors of AP17 and AP18, is reserved. Both subscribers use G711 with 20ms frame size (AMO SIPCO:BANDW -> Index 5).

You can see, that only 59 B-channels are available in the GW sectors 175 and 176.

2nd example for bandwidth reservation after these steps:

Call situation from 7282 to 7240 (GW SECTOR 175 to GW SECTOR 170).

```
DISPLAY-GKTOP:TYPE=ALL,SCOPE=DYN;

---------+-----------------------------------------------------------------+
   SECTOR   |               100                                             |
   ---------+-----------------------------------------------------------------+
   PNNO     |        10- 30-200                                             |
   ---------+-----------------------------------------------------------------+
   S-BW     |        UNLIMITED                                              |
   USED-BW  |                72                                             |
   R-GW-MC  |                 0                                             |
   R-GW-DMC |                 0                                             |
   ---------+-----------------------------------------------------------------+
   SECTOR   |               170                                             |
   ---------+-----------------------------------------------------------------+
   PNNO     |        10- 30-200                                             |
   ---------+-----------------------------------------------------------------+
   S-BW     |        UNLIMITED                                              |
   USED-BW  |                 0                                             |
   R-GW-MC  |                59                                             |
   R-GW-DMC |                 0                                             |
   ---------+-----------------------------------------------------------------+
   SECTOR   |               171                                             |
   ---------+-----------------------------------------------------------------+
   PNNO     |        10- 30-200                                             |
   ---------+-----------------------------------------------------------------+
   S-BW     |                78                                             |
   USED-BW  |                72                                             |
   R-GW-MC  |                 0                                             |
   R-GW-DMC |                 0                                             |
   ---------+-----------------------------------------------------------------+
   SECTOR   |               172                                             |
   ---------+-----------------------------------------------------------------+
   PNNO     |        10- 30-200                                             |
   ---------+-----------------------------------------------------------------+
   S-BW     |        UNLIMITED                                              |
   USED-BW  |                72                                             |
   R-GW-MC  |                 0                                             |
   R-GW-DMC |                 0                                             |
   ---------+-----------------------------------------------------------------+
   SECTOR   |               175                                             |
   ---------+-----------------------------------------------------------------+
   PNNO     |        10- 30-200                                             |
   ---------+-----------------------------------------------------------------+
   S-BW     |        UNLIMITED                                              |
   USED-BW  |                 0                                             |
   R-GW-MC  |                60                                             |
   R-GW-DMC |                 0                                             |
   ---------+-----------------------------------------------------------------+
   SECTOR   |               176                                             |
   ---------+-----------------------------------------------------------------+
```

```
   PNNO     |        10- 30-200                                                |
   ---------+------------------------------------------------------------------+
   S-BW     |        UNLIMITED                                                 |
   USED-BW  |                 0                                                |
   R-GW-MC  |                59                                                |
   R-GW-DMC |                 0                                                |
   ---------+------------------------------------------------------------------+
```

```
DISPLAY-SIPCO:TYPE=BANDW;

  BANDWIDTH COMPUTING TABLE :
  ------------------------------------------------------------------------
  +-------+----------------------+-----------------+---------------+
  | INDEX |  CODEC TYPE          |    FRAME SIZE   |    RESERVED   |
  |       |                      |       (MS)      |  BANDW.(KBIT) |
  +-------+----------------------+-----------------+---------------+
  |     1 | G711_HFA             |       30        |        89     |
  |     2 | G729_HFA             |       40        |        22     |
  |     3 | G723_HFA             |       30        |        25     |
  |     4 | G711_F10_IPDA        |       10        |       120     |
  |     5 | G711_F20_IPDA        |       20        |       184     |
  |     6 | G711_F30_IPDA        |       30        |        83     |
  |     7 | G711_F60_IPDA        |       60        |        74     |
  |     8 | G729_F20_IPDA        |       20        |        72     |
  |     9 | G729_F40_IPDA        |       40        |        22     |
  |    10 | G729_F60_IPDA        |       60        |        18     |
  |    11 | G711_DMC             |       30        |       182     |
  |    12 | G729_DMC             |       40        |        72     |
  |    13 | G723_DMC             |       30        |        27     |
  |    14 | G711_FS_UNKNOWN      |       60        |        83     |
```

Interpretation:

Bandwidth in all used sectors (172&171&100), which connect AP18 to the Host, is reserved. The Codec G729A with 20ms Frame size is used for this call (AMO SIPCO:BANDW -> Index 8).

You can see, that only 59 B-channels are available in the GW sectors 170 and 176.

2.17.7 Configuring the Resource Management for an IPDA Configuration with TDM Phones and HFA in Access Point

2.17.7.1 Basic Situation

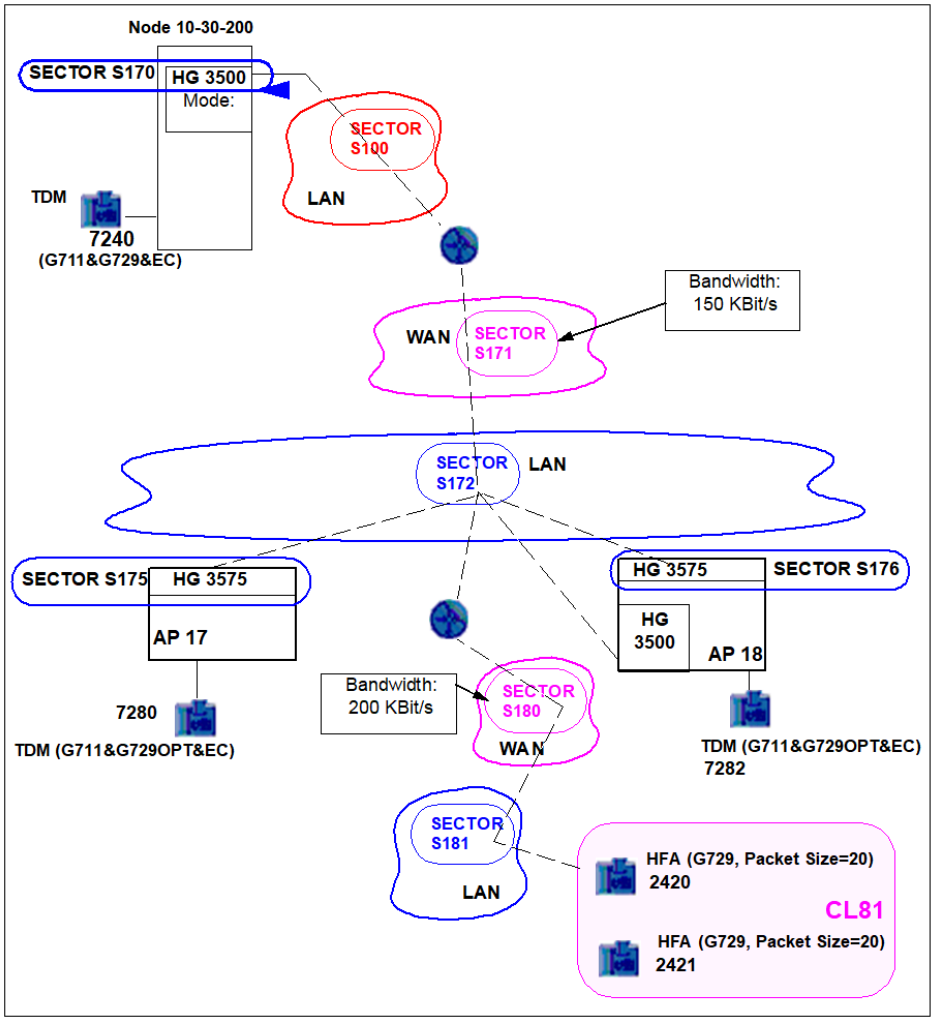


Figure 38: Resource management for IPDA configuration with TDM & HFA phones

The basic situation is as following:

There is the feature IPDA at node 10-30-200. The feature is already configured with access points 17 and 18. The feature HFA is configured in AP18. It is assumed, that both access points are located behind a bandwidth limited WAN. This situation is described for the resource management in sector S171 (bandwidth limited) and in bandwidth unlimited LAN sectors S100 (Host) and S172 (access points). gateway sectors are necessary for HG 3570 and HG 3575 in the IPDA feature (S170, S175 and S176). The sector S172 is necessary, to describe the direct connection between both HG 3575 gateways. Sector paths must be defined for the HG 3575 gateways, to describe their location to the Host correctly.

The WAN for HFA is connected to the location of the displaced shelf. This situation is described for the resource management in the way, that the WAN sector 180 borders on the sector 172 and from the other side on sector 181 to which the HFA cluster 81 is connected.

The frame size for G711 is set to 20 ms for all HG 3570/75:

```
CHANGE-CGWB:MTYPE=CGW,LTU=1,SLOT=61,TYPE=ASC,PRIO=PRIO2,CODEC=G711A,

RTP=20;
CHANGE-STMIB:MTYPE=NCUI2,LTU=17,TYPE=ASC,PRIO=PRIO1,CODEC=G711A,RTP=20;
CHANGE-STMIB:MTYPE=NCUI2,LTU=18,TYPE=ASC,PRIO=PRIO1,CODEC=G711A,RTP=20;
```

The codec G729 should be used for a call between a Host terminal and an AP terminal. The Codec G711 should be used for a call between an AP terminal of access point 17 and an AP terminal in access point 18.

```
CHANGE-SDAT:STNO=7240,TYPE=DATA1,CLASSMRK=G711&G729A&EC;
CHANGE-SDAT:STNO=7280&&7282,TYPE=DATA1,CLASSMRK=G711&G729AOPT&EC;
```

All HFA subscribers have the attribute “DMC allowed”.

```
CHANGE-SDAT:STNO=2420&&2421,TYPE=ATTRIBUT,AATTR=DMCALLWD;
```

The IPDA gateways should support DMC.

- HG 3570:

CHANGE-SIPCO:TYPE=DMCDATA,DMCALLWD=YES;

CHANGE-CGWB:MTYPE=CGW,LTU=1,SLOT=61,TYPE=DMCDATA,DMCCONN=45;

- HG 3575:

CHANGE-STMIB:MTYPE=NCUI2,LTU=17,TYPE=DMCDATA,DMCALLWD=YES, DMCCONN=45;

CHANGE-STMIB:MTYPE=NCUI2,LTU=18,TYP=DMCDATA,DMCALLWD=YES, DMCCONN=45;

Settings of the Codec list for the gateways (for DMC connections).

```
CHANGE-CGWB:MTYPE=CGW,LTU=1,SLOT=69,TYPE=ASC,PRIO=PRIO1,CODEC=G711A,RTP=20;
CHANGE-CGWB:MTYPE=CGW,LTU=1,SLOT=69,TYPE=ASC,PRIO=PRIO2,CODEC=G729A,RTP=20;
CHANGE-STMIB:MTYPE=NCUI2,LTU=17,TYPE=ASC,PRIO=PRIO1,CODEC=G711,RTP=20;
CHANGE-STMIB:MTYPE=NCUI2,LTU=17,TYPE=ASC,PRIO=PRIO2,CODEC=G729A,RTP=20;
CHANGE-STMIB:MTYPE=NCUI2,LTU=18,TYPE=ASC,PRIO=PRIO1,CODEC=G711,RTP=20;
CHANGE-STMIB:MTYPE=NCUI2,LTU=18,TYPE=ASC,PRIO=PRIO2,CODEC=G729A,RTP=20;
```

2.17.7.2 Settings for the HFA Subscribers

The Codec information, which will be used for a call, must be available for the Resource Manager for reserving the necessary bandwidth.

The setting in the AMO **must** be corresponding to the setting at the terminal (Administration) for the HFA subscriber.

```
CHANGE-SBCSU:STNO=2420&2421,OPT=OPTI,IPCODEC=G729A;
```

Codec setting of the HFA subscribers for the master connection in the IPDA section.

```
CHANGE-SDAT:STNO=2420&&2421,TYPE=DATA1,CLASSMRK=G711&G729AOPT&EC;
```

2.17.7.3 Sectors for the LAN/WAN

The sectors, which describe the LAN/WAN are defined first. These are the sectors S100, S171 and S172. The sector 171 ist a WAN sector. The bandwidth is limited to 150 kBit/s.

Sector 100 and 172:

The attributes **OWN**&**EXCL** must be entered. The sectors are LAN sectors with unlimited bandwidth.

```
ADD-GKTOP:TYPE=RESMGMT1,SECNO=100,SECATTR=OWN&EXCL&LAN,PNNO=10-30-200,BAND►
WI="0";
ADD-GKTOP:TYPE=RESMGMT1,SECNO=172,SECATTR=OWN&EXCL&LAN,PNNO=10-30-200,BAND►
WI="0";
```

Sector 171:

The attributes **OWN**&**EXCL** must be entered. The sector is a WAN sector with limited bandwidth.

```
ADD-GKTOP:TYPE=RESMGMT1,SECNO=171,SECATTR=OWN&EXCL&WAN,PNNO=10-30-200,BAND►
WI="150";
```

Sector 181:

The sectors 181 (LAN) and 181 (WAN) are necessary for the HFA configuration.

The attributes **OWN**&**EXCL** must be entered. The sector is a LAN sector with unlimited bandwidth.

```
ADD-GKTOP:TYPE=RESMGMT1,SECNO=181,SECATTR=OWN&EXCL&LAN,PNNO=10-30-200,BAND►
WI="0";
```

SECTOR 180:

The attributes **OWN**&**EXCL** must be entered. The sector is a WAN sector with limited bandwidth.

```
ADD-GKTOP:TYPE=RESMGMT1,SECNO=180,SECATTR=OWN&EXCL&WAN,PNNO=10-30-200,BAND►
WI="200";
```

2.17.7.4 Sectors for the Gateways

The sectors S170, S175 and S176 are defined.

The sector 170 has the attributes **OWN**&**EXCL** (see before) and HHS (is located in the Host) and GW (is a gateway).

```
ADD-GKTOP:TYPE=RESMGMT1,SECNO=170,SECATTR=OWN&EXCL&HHS&GW,PNNO=10-30-200,GW►
LAN=100;
```

The sectors 175 and 176 have the attributes **OWN**&**EXCL** (see before) and AP (are located in an access point) and GW (are gateways).

```
ADD-GKTOP:TYPE=RESMGMT1,SECNO=175,SECATTR=OWN&EXCL&AP&GW,PNNO=10-30-200,GW►
LAN=172;
ADD-GKTOP:TYPE=RESMGMT1,SECNO=176,SECATTR=OWN&EXCL&AP&GW,PNNO=10-30-200,GW►
LAN=172;
```

2.17.7.5 Assignment of the HFA Subscribers to the Sectors

The subscribers 2420 and 2421 are configured in cluster 81 and are connected to the HFA LAN sector 181. Because they are subscribers of the AP18 additionally, it is necessary to add the GW sector of their HG 3575 in the parameter **GWSEC** (S176).

```
ADD-GKTOP:TYPE=IPDA,CLUSTID=81,HFASEC=181,GWSEC=176;
CHANGE-SDAT:STNO=2420,TYP=DATA1,CLUSTID=81;
CHANGE-SDAT:STNO=2421,TYP=DATA1,CLUSTID=81;
```

2.17.7.6 Allocation of the Gateways to their Sectors

```
CHANGE-CGWB:MTYPE=CGW,LTU=1,SLOT=61,TYPE=GWSECTOR,GWSECTNO=170;
CHANGE-STMIB:MTYPE=NCUI2,LTU=17,TYPE=GWSECTOR,GWSECTNO=175;
CHANGE-STMIB:MTYPE=NCUI2,LTU=18,TYPE=GWSECTOR,GWSECTNO=176;
```

2.17.7.7 Define Sector Paths

In this example only one sector path is necessary, because access point 17 and 18 are reached via the same path from the host.

```
ADD-GKTOP:TYPE=SECPATH,SECPANO=1,SECDE=100&171&172;
```

An own sector path from the host to the destination sector 181 of the HFA subscribers in cluster 81 must be defined.

```
ADD-GKTOP:TYPE=SECPATH,SECPANO=2,SECDE=100&171&172&180;
```

2.17.7.8 Assign the Sector Path

```
CHANGE-GKTOP:TYPE=RESMGMT1,SECNO=175,SECPANO1=1;
CHANGE-GKTOP:TYPE=RESMGMT1,SECNO=176,SECPANO1=1;
CHANGE-GKTOP:TYPE=RESMGMT1,SECNO=181,SECPANO1=2;
```

Example for bandwidth reservation after these steps:

Call situation from 2420 to 7280 (SECTOR 181 to GW SECTOR 175).

```
DISPLAY-GKTOP:TYPE=ALL,SCOPE=DYN;

---------+-------------------------------------------------------------+
   SECTOR   |               100                                         |
   ---------+-------------------------------------------------------------+
   PNNO     |        10- 30-200                                         |
   ---------+-------------------------------------------------------------+
   S-BW     |        UNLIMITED                                          |
   USED-BW  |                 0                                         |
   R-GW-MC  |                 0                                         |
   R-GW-DMC |                 0                                         |
   ---------+-------------------------------------------------------------+
   SECTOR   |               170                                         |
   ---------+-------------------------------------------------------------+
   PNNO     |        10- 30-200                                         |
   ---------+-------------------------------------------------------------+
   S-BW     |        UNLIMITED                                          |
   USED-BW  |                 0                                         |
```

```
R-GW-MC  |                60                                          |
R-GW-DMC |                45                                          |
---------+--------------------------------------------------------------+
SECTOR   |               171                                          |
---------+--------------------------------------------------------------+
PNNO     |        10- 30-200                                          |
---------+--------------------------------------------------------------+
S-BW     |               150                                          |
USED-BW  |                 0                                          |
R-GW-MC  |                 0                                          |
R-GW-DMC |                 0                                          |
---------+--------------------------------------------------------------+
SECTOR   |               172                                          |
---------+--------------------------------------------------------------+
PNNO     |        10- 30-200                                          |
---------+--------------------------------------------------------------+
S-BW     |        UNLIMITED                                           |
USED-BW  |               220                                          |
R-GW-MC  |                 0                                          |
R-GW-DMC |                 0                                          |
---------+--------------------------------------------------------------+
SECTOR   |               175                                          |
---------+--------------------------------------------------------------+
PNNO     |        10- 30-200                                          |
---------+--------------------------------------------------------------+
S-BW     |        UNLIMITED                                           |
USED-BW  |                 0                                          |
R-GW-MC  |                58                                          |
R-GW-DMC |                44                                          |
---------+--------------------------------------------------------------+
SECTOR   |               176                                          |
---------+--------------------------------------------------------------+
PNNO     |        10- 30-200                                          |
---------+--------------------------------------------------------------+
S-BW     |        UNLIMITED                                           |
USED-BW  |                 0                                          |
R-GW-MC  |                59                                          |
R-GW-DMC |                45                                          |
---------+--------------------------------------------------------------+
SECTOR   |               180                                          |
---------+--------------------------------------------------------------+
PNNO     |        10- 30-200                                          |
---------+--------------------------------------------------------------+
S-BW     |               122                                          |
USED-BW  |                78                                          |
R-GW-MC  |                 0                                          |
R-GW-DMC |                 0                                          |
---------+--------------------------------------------------------------+
SECTOR   |               181                                          |
---------+--------------------------------------------------------------+
PNNO     |        10- 30-200                                          |
---------+--------------------------------------------------------------+
S-BW     |        UNLIMITED                                           |
USED-BW  |                78                                          |
R-GW-MC  |                 0                                          |
R-GW-DMC |                 0                                          |
```

```
   ---------+-------------------------------------------------------------+

DISPLAY-SIPCO:TYPE=BANDW;

  BANDWIDTH COMPUTING TABLE :
  ---------------------------------------------------------------------
  +-------+----------------------+-----------------+---------------+
  | INDEX |  CODEC TYPE          |   FRAME SIZE    |    RESERVED   |
  |       |                      |      (MS)       |  BANDW.(KBIT) |
  +-------+----------------------+-----------------+---------------+
  |     1 | G711_HFA             |        30       |         89    |
  |     2 | G729_HFA             |        40       |         36    |
  |     3 | G723_HFA             |        30       |         25    |
  |     4 | G711_F10_IPDA        |        10       |        120    |
  |     5 | G711_F20_IPDA        |        20       |        184    |
  |     6 | G711_F30_IPDA        |        30       |         83    |
  |     7 | G711_F60_IPDA        |        60       |         74    |
  |     8 | G729_F20_IPDA        |        20       |         36    |
  |     9 | G729_F40_IPDA        |        40       |         22    |
  |    10 | G729_F60_IPDA        |        60       |         18    |
  |    11 | G711_DMC             |        30       |        182    |
  |    12 | G729_DMC             |        40       |         78    |
  |    13 | G723_DMC             |        30       |         27    |
  |    14 | G711_FS_UNKNOWN      |        60       |         83    |
```

Interpretation:

The bandwidth in the sectors for HFA (S180 and S181) is reserved. There the bandwidth using Index 12 is reserved for the compressed DMC connection, because the flat rate value in Index 12 is greater than the double value of Index 2. The master connection between the two access points with G711 (Index 5) will be added with the bandwidth of the master connection of the HFA subscribers to the HG 3530 (G729, Index 2) in sector 172.

The master connection is only active in the GW sector 176, i.e. only one master channel is used (59 available). The master connection and one DMC connection is active in the sector 175, i.e. 2 DSP channels are used. One of them is used the master connection and the other for the DMC connection (58/44 available).

2.17.8 Notes and Restrictions

Comments on RM:

- RESMAN should never contain a route with more than 16 sectors.
- **Only** WAN sectors are supported for bandwidth calculation and **not** LAN sectors.
- Each **RESMGMT1** from AMO GKTOP must contain the AMO ZAND **PKNNO** under the **PKNNO** parameter, i.e. this is **not** the AMO KNDEF entry.
- IP TRUNKING is not supported.
- Network-wide configuration is extremely time intensive and if an incorrect sector is received from a partner system DMC is not switched (see MSC15245 for an alternative simpler configuration).
- When a DMC connection is made the bandwidth is not reduced if the CODEC is of a lower quality until the call is disconnected. If the bandwidth

is more i.e. a higher bandwidth is used for the DMC connection the value is increased normally.

- MOBHFA is supported. Upon successful logon the cluster ID of the guest station is also stored. Bandwidth calculation will take into account the path from the guest station to the home gateway and then from the home gateway to the called party. DMC can also increase the bandwidth dependant on which CODEC is used for the master connection.
- The bandwidth is **always** calculated as configured i.e. from host system in direction of the AP. If the call is between two APs the routes are overlaid (compared) to establish the true route.
- AMO SBCSU parameter **IPCODEC** must be configured for HFA phones to calculate the bandwidth correctly.
- When using AMO KCSU no bandwidth reservation will be made during ringing state (first by connect).
- Each gateway should be connected to a LAN sector (not directly to WAN!).

2.17.9 Diagnostics

Checking of the used bandwidth of all sectors:

```
DISPLAY-GKTOP:TYPE=RESMGMT1,SCOPE=DYN;
```

When it is required to check the implementation of the resource management, it is sufficient at first to establish speech connections over all configured paths. Then when the permitted bandwidth in a sector is exceeded, a path occupancy should be obtained.

No bandwidth available

When Resource Manager is configured sometimes connections will be blocked if no resources are free. In such a case an F4436 advisory message is signalled. Usually the reason for the error message is a correct one and defined by configuration i.e. more connections are attempting to use a path than are allowed in the AMO GKTOP configuration or that a DMC connection was restricted via the AMO GKTOP attribute **NODMC**. In some rarer cases, the advisory is signalled due to hanging bandwidth, meaning a DIS-GKTOP will show bandwidth is used even though no connections are active over the specific path. Hanging bandwidth can be verified by executing a DIS-GKTOP in a low period of traffic.

The F4436 error message contains important information regarding exactly which route is not available.

2.18 Command Line Interface CLI in HG 3500

2.18.1 General Information

The common gateway supports a Command Line Interface (CLI) for installation and basic configuration, e.g. IP infra structure. In V.24 CLI it is possible to change security relevant data (e.g. SSL Configuration), because the V.24 is considered to be secure. Additionally the CLI allows the monitoring of important counters and statistics.

The CLI can be accessed via V.24. The CLI can not be accessed via Telnet because it is an insecure protocol.

To get an overview of the commands type in the command `help` and you get an alphabetic list of all commands.

Please refer to Section 13.9, “TYPE SERVIF - Changing the Login and Password for the Service Access” on how to configure the access data for CLI.

The basic function of the CLI are described below. In the following sections the CLI commands are divided into seven categories:

1) General Operations

- Access control
- Gateway Setup
- Image/File Handling
- Maintenance
- SSL for WBM
- DLS

NOTICE: The CLI is not supported on STMIX/STMIY.

2.18.2 General Operations

When starting a session the administrator is asked for authentication. That is done by entering the admin name and the password.

- To leave the session use the

logout

1) command.

- The list of all supported commands except the hidden commands can be obtained with:

help

2.18.3 Access control

- The configuration write access has to be acquired before a store, upload or download command can be done. Because of the implemented “soft lock“ handling, at first a check if somebody else has set the write access is required.

who has write access

get write access

release write access

2.18.4 Gateway Setup

To permit system initialization and basic management configuration activities following commands are needed.

- Setting and changing the gateway name:

set hostname <hostname>

1) The parameter `hostname` terms an arbitrary name for the gateway and it must be a string of characters (e.g. set hostname Gateway1). It corresponds with the boot line parameter "targetname".

- Setting and changing the IP-Address for the ethernet port:

set ip address <ip address>

set ip subnet <ip subnet mask>

1) The parameter `ip address` is a string in the form of x.x.x.x and x is an integer (e.g. 1.2.3.4)

The parameter `ip subnet mask` is a string in the form of x.x.x.x and x is an integer between 0 and 255 (e.g. 255.255.255.224).

A set or a change of the IP-address or IP subnet for the ethernet port will probably require a gateway reboot to become effective.

- Setting and changing the IP-address of the default gateway from static routes table:

set default gateway <ip address>

1) The parameter `ip address` is a string in the form of x.x.x.x and x is an integer (e.g. 1.2.3.4)

- Display/change chosen identifier:

get id <parameter name>

set id <parameter name>

2.18.5 Image/File Handling

In common gateway software configuration and distribution as well as upload and download of configuration data via CLI is not required because it is done via WBM.

Additionally operations for analyzing event and trace data are supported.

The trace /event logs are available as:

/trace/trace.txt /trace/trace.bak

/evtlog/evtlog.txt /evtlog/evtlog.bak

2.18.6 Maintenance

The maintenance commands permit the current operational status of the gateway to be inspected, and provides access to diagnostic tools and interface and gateway controls.

Display

- Commands which provide information on the gateway’s software configuration:

show version

show uptime

- Display of IP-address, subnet and gateway:

show all parameters

- Display of hostnames and IP-addresses:

show host

- Get the name of the gateway:

show hostname

- Display of arp-cache:

show arp cache

1) It is also stored in the bootline as targetname.

- Display of the IP address and subnetmask for the ethernet port:

show ip address

show ip subnet

- Showing the time will display the time and the date:

show time

- Command to get the IP address of the default gateway from the static routes table:

show default gateway

- Command to display the static routes entries:

show routes

- To display the statistics of the interface table:

show if counters

- To list all existing interfaces:

show interfaces

- To get admin and operating states:

show if states

Ping and tracert

- Diagnosis Commands:

ping <ip address>

Target shell

- vxWorks shell logon/logout:

shell

exit

Gateway Reboot

From the administrator point of view two different ways of a reboot command are of interest. At first there is the need to reboot the gateway with the current configuration. On the other side there could be the need to support a configuration data exchange, i.e. to take a configuration data file from extern or to skip the latest configuration data storage and take the next older one.

It is in the responsibility of the administrator to coordinate a gateway reboot!

- Normal reboot of the gateway, using the current configuration data:

reset

- Reset any configuration data to factory defaults and reboot:

reset factory

- Special reboot of the gateway using an existing self-extracting image in order to complete a software download:

activate software

2.18.7 SSL for WBM

SSL for WBM (i.e. https) is enabled in the factory delivered status. It cannot be disabled.

To permit a basic configuration of SSL following commands are needed.

- Display the fingerprint of the currently active certificate for WBM access via https.

show fingerprint

1) Before accepting a certificate warning in the browser, it is strongly recommended that the administrator should compare the fingerprint of the certificate displayed in the browser against the fingerprint shown in CLI. The certificate must be accepted only, if both fingerprints are identical!

2.18.8 DLS

- Set the IP address of the DLS server

set dls ip_address <ip address[:port]>

1) You can set the IP address of the DLS server manually with `set dls ip_address` (optional). The IP address is automatically set if you use the function **IP Devices > IP Device Interaction > Scan IP Devices** (activate the checkbox **Send DLS Address** in the **"Configuration"** tab for this).

- Show the IP address of the DLS server

show dls ip_address

1) The gateway contains a DLS client. This setting makes sure that the gateway automatically recognizes the IP address of the DLS client.

- DLS PIN

- **IP Devices > IP Device Management > IP Device Configuration > "DLS Connectivity"**

  Three security settings are available under **PIN Mode** for creating a virtual device in the DLS:

  – **No PIN**,
  – **Default PIN**,
  – **Individual PIN**.

  See also Chapter 9, “DLS Client Bootstrapping”.

  If you set **dls pin_required** to **TRUE** in the gateway, the gateway declines a connection if **No PIN** is set in the DLS. This setting offers added security.

  The PIN is automatically generated by the DLS and displayed in the **Default PIN:** field in the DLS under **Administration > Workpoint Interface Configuration > "Secure mode"** tab. It has the same function as a password.

  `set dls pin_required <value>`

  Possible values:

  – **0**: A PIN is not needed. **"No PIN"** is set as the PIN mode in the DLS.
  – **1**: A PIN is needed. **"Default PIN"** or **"Individual PIN"** is set as the PIN mode in the DLS.

  show dls pin_required

  Possible values:

  – **FALSE**: A PIN is not needed. **"No PIN"** is set as the PIN mode in the DLS.
  – **TRUE**: A PIN is needed. **"Default PIN"** or **"Individual PIN"** is set as the PIN mode in the DLS.
- Activate the DLS PIN

activate dls pin <pin>

1) If you select **Default PIN** or **Individual PIN** as the PIN mode in the DLS, you must use this command to enter the PIN displayed in the DLS.

- Bootstrapping
- The command `reset dls bootstrapping` resets the gateway defaults for DLS client bootstrapping; you can then repeat bootstrapping (see also Chapter 9, “DLS Client Bootstrapping”).

  reset dls bootstrapping
- DLS client status
- Shows the value "secure" or "insecure." This is followed by a number in brackets which is used for diagnostic purposes.

  show dls_client_state

  Possible values:

  – **secure**: DLS client bootstrapping has already taken place.
  – **insecure**: DLS client bootstrapping has not yet been performed or was unsuccessful.
- Contact the DLS server

contact dls

1) This command tries to contact the DLS server.

You only need to do this to start DLS client bootstrapping after manually configuring the DLS server's IP address with `set dls ip_address`.

Otherwise, you can use `contact dls` to test if communication is possible between the gateway and DLS server. An appropriate message appears.

2.18.9 Changing the Login and Password for WBM/CLI

For CLI login, the same accounts as for WBM login have to be used. The accounts can be set up and changed via AMO CGWB. The parameter ROLE defines the access rights.

IMPORTANT: Two-stage CLI is not supported.

```
CHANGE-STMIB:MTYPE=CGW,LTU=<ltu>,SLOT=<slot>,TYPE=WBMDATA,LOGINWBM=<user login
for wbm connection>,PASSWWBM=<password for wbm connection>,ROLE=<role of the wbm
user>;
```

The initial login as **engr** is

username: HP4K-DEVEL

Passowrd: 4K-admin

After successful login the following message appears:

Welcome to the HG 3575 <currently loaded LW-version> Command Line Interpreter.

vxTarget>

2.19 Command Line Interface CLI at HG 3575 V4

Please refer to IP Distributed Architecture (IPDA) , Chapter 4, "Local Access Point Administration at CLI via Terminal".

2.20 SNMP Support HG 3500 / HG 3575

The HG 3500 / HG 3575 module supports the request of data via SNMP.The standards MIB (MIB-2) and two Private Enterprises MIB-s for company specific gateway data are supported:

MIB-2:

1) (1) System Group (RFC1213)

- (2) Interfaces Group (RFC2233)
- (3) AT Group (RFC1213)
- (4) IP Group (RFC2011/RFC1213)
- (5) ICMP Group (RFC2011)
- (6) TCP Group (RFC2012)
- (7) UDP Group (RFC2013)
- (8) EGP Group (RFC1213)
- (10) Transmission Group (RFC2127)
- (11) SNMP Group (RFC1213)
- (16) RMON Group (RFC1757)
- (30) ianaifType (IANA)
- (31) ifMIB Group (RFC2233)

SNI specific (hg3550) MIB:

- (1) Error Sig Group
- (2) Control Group
- (3) Monitoring Group
- (4) Statistics Group
- (5) Send Alarm with Values (traps)
- (6) File Overflow (traps)
- (7) All Serve Group
- (8) Ethernet Statistics Group
- (9) QOS Statistics Group
- (10) B-Channel Statistics Group
- (11) Notification Group (traps)
- (12) IP Phone Group
- (13) RG2500 MIB (platform, management, global data, traps, ...)

Company specific (hg3550 v11) MIB:

- (2) I&C Admin MIB (systemOID)

Notes

To make the MIB-s known to a MIB browser, the following files are required:

MIB-2 parts:

- mib-2.my: standard MIB-II (1.3.6.1.2.1.1-11)
- iana.my: IANAifType (1.3.6.1.2.1.30)
- my_rmon2.my: RMON MIB (1.3.6.1.2.1.16.19)
- rfc2127.my: ISDN-MIB (1.3.6.1.2.1.10.20)
- rfc2233.my: IF-MIB (1.3.6.1.2.1.2 and 1.3.6.1.2.1.31)

SNI specific (hg3550) MIB parts:

- hg1500.my: HG3550 MIB (1.3.6.1.4.1.231.7.2.7.1-12)
- ar2500_platform.my: Platform MIB (1.3.6.1.4.1.231.7.2.7.13.1)
- ar2500_management.my: Management MIB (1.3.6.1.4.1.231.7.2.7.13.2)
- cg2500.my: CG2500 MIB (1.3.6.1.4.1.231.7.2.7.13.3)

Company specific (hg3550 v11) MIB parts:

- hg3550_v11.my: system OID for hg3550 V2 (1.3.6.1.4.1.4329.2.24)

These files are part of each official production, packed in a zip file.

The SNMP MIBs can be downloaded via the **SNMP Configurator**, tab **SNMP Control** of the OpenScape 4000 Assistant (**Diagnostics > Faul Management**) or via sftp from the directory **/opt/ncc/mib**.

For all information on Object Identifiers (OID) please refer to https://wpb.global-intra.net/comwiki/bin/view.pl/Standardization/OIDs.

You can find more information on the SNMP Configurator in the online help or in the OpenScape 4000 Assistant documentation for Simple Network Management Protocol.

The SNMP Signaling of specific Eventlog messages can be controlled under the Reaction Table in WBM: Maintenance > Traces & Events > Events > Reaction Table.

Some MIB objects and MIB files have old, historical names. These MIB objects and MIB files have been created earlier, for previous products (CG2500, AR2500, HG1500 etc.). These objects and files could been inherited for the new products with minor (or without any) changes, thus the old, unchanged object and file names are continuously used in the new products (HG 3500, HG 3575) too.

The following tables describe the details of the supported objects, sorted by object ID. The last table contains a repeated and collected list of the SNMP traps in the MIB object tree.

The SNMP traps are marked by “TRAP” in the Syntax column. They are collected and repeated in the last table.

The Access column contains shortcuts of the object data access possibilities:

- RO: Read-Only
- RW: Read-Write
- RC: Read-Create

If no Access shortcut is present, then the object is not a data container object, thus it is not directly accessible.

The texts in the Description column are generally extracted from the MIB source files, thus they may contain references to old, historical product names. These are valid for the current products too.

For more information see the referenced MIB files.

Table 12: Data in the standard MIB-2

Object-ID	Object name	Syntax	Access	Description
1.3.6.1.2.1.1	system			System MIB, see mib-2.my
1.3.6.1.2.1.1.1	sysDescr	DisplayString (SIZE (0..255))	RO	Textual description of the system, including the full name and version identification of the system's hardware type, software operating-system, and networking software

Object-ID	Object name	Syntax	Access	Description
1.3.6.1.2.1.1.2	sysObjectID	OBJECT IDENTIFIER	RO	The vendor's authoritative identification of the network management subsystem contained in the entity
1.3.6.1.2.1.1.3	sysUpTime	TimeTicks	RO	The time (in hundredths of a second) since the network management portion of the system was last re-initialized
1.3.6.1.2.1.1.4	sysContact	DisplayString (SIZE (0..255))	RW	The textual identification of the contact person for this managed node, together with information on how to contact this person
1.3.6.1.2.1.1.5	sysName	DisplayString (SIZE (0..255))	RW	An administratively-assigned name for this managed node. By convention, this is the node's fully-qualified domain name
1.3.6.1.2.1.1.6	sysLocation	DisplayString (SIZE (0..255))	RW	The physical location of this node
1.3.6.1.2.1.1.7	sysServices	INTEGER (0..127)	RO	A value which indicates the set of services that this entity primarily offers
1.3.6.1.2.1.2	interfaces			Interfaces MIB, see mib-2.my and rfc2233.my
1.3.6.1.2.1.2.1	ifNumber	INTEGER	RO	The number of network interfaces (regardless of their current state) present on this system.
1.3.6.1.2.1.2.2	ifTable	SEQUENCE OF IfEntry		A list of interface entries. The number of entries is given by the value of ifNumber.
1.3.6.1.2.1.2.2.1	ifEntry	IfEntry		An entry containing management information applicable to a particular interface.
1.3.6.1.2.1.2.2.1.1	ifIndex	INTEGER	RO	A unique value, greater than zero, for each interface.
1.3.6.1.2.1.2.2.1.2	ifDescr	DisplayString (SIZE (0..255))	RO	A textual string containing information about the interface.
1.3.6.1.2.1.2.2.1.3	ifType	INTEGER	RO	The type of interface.
1.3.6.1.2.1.2.2.1.4	ifMtu	INTEGER	RO	The size of the largest packet which can be sent/received on the interface, specified in octets.

Object-ID	Object name	Syntax	Access	Description
1.3.6.1.2.1.2.2.1.5	ifSpeed	Gauge	RO	An estimate of the interface's current bandwidth in bits per second.
1.3.6.1.2.1.2.2.1.6	ifPhysAddress	PhyCountersAddress	RO	The interface's address at its protocol sub-layer.
1.3.6.1.2.1.2.2.1.7	ifAdminStatus	INTEGER	RW	The desired state of the interface. - up(1) ready to pass packets - down(2) - testing(3) in some test mode
1.3.6.1.2.1.2.2.1.8	ifOperStatus	INTEGER	RO	The current operational state of the interface. - up(1) ready to pass packets - down(2) - testing(3) in some test mode - unknown(4) status can not be determined for some reason. - dormant(5) - notPresent(6) some component is missing - lowerLayerDown(7) down due to state of lower-layer interface(s)
1.3.6.1.2.1.2.2.1.9	ifLastChange	TimeTicks	RO	The value of sysUpTime at the time the interface entered its current operational state.
1.3.6.1.2.1.2.2.1.10	ifInOctets	Counter	RO	The total number of octets received on the interface, including framing characters.
1.3.6.1.2.1.2.2.1.11	ifInUcastPkts	Counter	RO	The number of packets, delivered by this sub-layer to a higher (sub-)layer, which were not addressed to a multicast or broadcast address at this sub-layer.
1.3.6.1.2.1.2.2.1.12	ifInNUcastPkts	Counter	RO	The number of packets, delivered by this sub-layer to a higher (sub-)layer, which were addressed to a multicast or broadcast address at this sub-layer. deprecated

Object-ID	Object name	Syntax	Access	Description
1.3.6.1.2.1.2.2.1.13	ifInDiscards	Counter	RO	The number of inbound packets which were chosen to be discarded even though no errors had been detected to prevent their being deliverable to a higher-layer protocol.
1.3.6.1.2.1.2.2.1.14	ifInErrors	Counter	RO	For packet-oriented interfaces, the number of inbound packets that contained errors preventing them from being deliverable to a higher-layer protocol.
1.3.6.1.2.1.2.2.1.15	ifInUnknownProtos	Counter	RO	For packet-oriented interfaces, the number of packets received via the interface which were discarded because of an unknown or unsupported protocol.
1.3.6.1.2.1.2.2.1.16	ifOutOctets	Counter	RO	The total number of octets transmitted out of the interface, including framing characters.
1.3.6.1.2.1.2.2.1.17	ifOutUcastPkts	Counter	RO	The total number of packets that higher-level protocols requested be transmitted, and which were not addressed to a multicast or broadcast address at this sub-layer, including those that were discarded or not sent.
1.3.6.1.2.1.2.2.1.18	ifOutNUcastPkts	Counter	RO	The total number of packets that higher-level protocols requested be transmitted, and which were addressed to a multicast or broadcast address at this sub-layer, including those that were discarded or not sent. deprecated
1.3.6.1.2.1.2.2.1.19	ifOutDiscards	Counter	RO	The number of outbound packets which were chosen to be discarded even though no errors had been detected to prevent their being transmitted.
1.3.6.1.2.1.2.2.1.20	ifOutErrors	Counter	RO	For packet-oriented interfaces, the number of outbound packets that could not be transmitted because of errors. For character-oriented or fixed-length interfaces, the number of outbound transmission units that could not be transmitted because of errors.

Object-ID	Object name	Syntax	Access	Description
1.3.6.1.2.1.2.2.1.21	ifOutQLen	Gauge	RO	The length of the output packet queue (in packets).
1.3.6.1.2.1.2.2.1.22	ifSpecific	OBJECT IDENTIFIER	RO	A reference to MIB definitions specific to the particular media being used to realize the interface. deprecated
1.3.6.1.2.1.3	at			Address Translation MIB, see mib-2.my Note: This group is deprecated by MIB-II. That is, it is being included solely for compatibility with MIB-I nodes, and will most likely be excluded from MIB-III nodes
1.3.6.1.2.1.3.1	atTable	SEQUENCE OF AtEntry		The MIB module to describe generic objects for network interface sub-layers. This MIB is an updated version of MIB-II's ifTable, and incorporates the extensions defined in RFC 1229.
1.3.6.1.2.1.3.1.1	atEntry	AtEntry		Each entry contains one NetworkAddress to `physical' address equivalence
1.3.6.1.2.1.3.1.1.1	atIfIndex	INTEGER	RW	The interface on which this entry's equivalence is effective
1.3.6.1.2.1.3.1.1.2	atPhysAddress	PhysAddress	RW	The media-dependent `physical' address
1.3.6.1.2.1.3.1.1.3	atNetAddress	NetworkAddress	RW	The NetworkAddress (e.g., the IP address) corresponding to the media-dependent `physical' address
1.3.6.1.2.1.4	ip			IP MIB, see mib-2.my
1.3.6.1.2.1.4.1	ipForwarding	INTEGER	RW	The indication of whether this entity is acting as an IP gateway in respect to the forwarding of datagrams received by, but not addressed to, this entity forwarding(1): acting as a gateway not-forwarding(2): NOT acting as a gateway

Object-ID	Object name	Syntax	Access	Description
1.3.6.1.2.1.4.2	ipDefaultTTL	INTEGER	RW	The default value inserted into the Time-To-Live field of the IP header of datagrams originated at this entity, whenever a TTL value is not supplied by the transport layer protocol
1.3.6.1.2.1.4.3	ipInReceives	Counter	RO	The total number of input datagrams received from interfaces, including those received in error
1.3.6.1.2.1.4.4	ipInHdrErrors	Counter	RO	The number of input datagrams discarded due to errors in their IP headers, including bad checksums, version number mismatch, other format errors, time-to-live exceeded, errors discovered in processing their IP options, etc.
1.3.6.1.2.1.4.5	ipInAddrErrors	Counter	RO	The number of input datagrams discarded because the IP address in their IP header's destination field was not a valid address to be received at this entity
1.3.6.1.2.1.4.6	ipForwDatagrams	Counter	RO	The number of input datagrams for which this entity was not their final IP destination, as a result of which an attempt was made to find a route to forward them to that final destination
1.3.6.1.2.1.4.7	ipInUnknownProtos	Counter	RO	The number of locally-addressed datagrams received successfully but discarded because of an unknown or unsupported protocol
1.3.6.1.2.1.4.8	ipInDiscards	Counter	RO	The number of input IP datagrams for which no problems were encountered to prevent their continued processing, but which were discarded (e.g., for lack of buffer space)
1.3.6.1.2.1.4.9	ipInDelivers	Counter	RO	The total number of input datagrams successfully delivered to IP user-protocols (including ICMP)
1.3.6.1.2.1.4.10	ipOutRequests	Counter	RO	The total number of IP datagrams which local IP user-protocols (including ICMP) supplied to IP in requests for transmission

Object-ID	Object name	Syntax	Access	Description
1.3.6.1.2.1.4.11	ipOutDiscards	Counter	RO	The number of output IP datagrams for which no problem was encountered to prevent their transmission to their destination, but which were discarded (e.g., for lack of buffer space)
1.3.6.1.2.1.4.12	ipOutNoRoutes	Counter	RO	The number of IP datagrams discarded because no route could be found to transmit them to their destination
1.3.6.1.2.1.4.13	ipReasmTimeout	INTEGER	RO	The maximum number of seconds which received fragments are held while they are awaiting reassembly at this entity
1.3.6.1.2.1.4.14	ipReasmReqds	Counter	RO	The number of IP fragments received which needed to be reassembled at this entity
1.3.6.1.2.1.4.15	ipReasmOKs	Counter	RO	The number of IP datagrams successfully re-assembled
1.3.6.1.2.1.4.16	ipReasmFails	Counter	RO	The number of failures detected by the IP re-assembly algorithm (for whatever reason: timed out, errors, etc)
1.3.6.1.2.1.4.17	ipFragOKs	Counter	RO	The number of IP datagrams that have been successfully fragmented at this entity
1.3.6.1.2.1.4.18	ipFragFails	Counter	RO	The number of IP datagrams that have been discarded because they needed to be fragmented at this entity but could not be, e.g., because their Don't Fragment flag was set
1.3.6.1.2.1.4.19	ipFragCreates	Counter	RO	The number of IP datagram fragments that have been generated as a result of fragmentation at this entity
1.3.6.1.2.1.4.20	ipAddrTable	SEQUENCE OF IpAddrEntry		The table of addressing information relevant to this entity's IP addresses
1.3.6.1.2.1.4.20.1	ipAddrEntry	IpAddrEntry		The addressing information for one of this entity's IP addresses
1.3.6.1.2.1.4.20.1.1	ipAdEntAddr	IpAddress	RO	The IP address to which this entry's addressing information pertains

Object-ID	Object name	Syntax	Access	Description
1.3.6.1.2.1.4.20.1.2	ipAdEntIfIndex	INTEGER	RO	The index value which uniquely identifies the interface to which this entry is applicable
1.3.6.1.2.1.4.20.1.3	ipAdEntNetMask	IpAddress	RO	The subnet mask associated with the IP address of this entry
1.3.6.1.2.1.4.20.1.4	ipAdEntBcastAddr	INTEGER	RO	The value of the least-significant bit in the IP broadcast address used for sending datagrams on the (logical) interface associated with the IP address of this entry
1.3.6.1.2.1.4.20.1.5	ipAdEntReasmMaxSize	INTEGER (0..65535)	RO	The size of the largest IP datagram which this entity can re-assemble from incoming IP fragmented datagrams received on this interface
1.3.6.1.2.1.4.21	ipRouteTable	SEQUENCE OF IpRouteEntry		This entity's IP Routing table
1.3.6.1.2.1.4.21.1	ipRouteEntry	IpRouteEntry		A route to a particular destination
1.3.6.1.2.1.4.21.1.1	ipRouteDest	IpAddress	RW	The destination IP address of this route. An entry with a value of 0.0.0.0 is considered a default route
1.3.6.1.2.1.4.21.1.2	ipRouteIfIndex	INTEGER	RW	The index value which uniquely identifies the local interface through which the next hop of this route should be reached
1.3.6.1.2.1.4.21.1.3	ipRouteMetric1	INTEGER	RW	The primary routing metric for this route
1.3.6.1.2.1.4.21.1.4	ipRouteMetric2	INTEGER	RW	An alternate routing metric for this route
1.3.6.1.2.1.4.21.1.5	ipRouteMetric3	INTEGER	RW	An alternate routing metric for this route
1.3.6.1.2.1.4.21.1.6	ipRouteMetric4	INTEGER	RW	An alternate routing metric for this route
1.3.6.1.2.1.4.21.1.7	ipRouteNextHop	IpAddress	RW	The IP address of the next hop of this route
1.3.6.1.2.1.4.21.1.8	ipRouteType	INTEGER	RW	The type of route
1.3.6.1.2.1.4.21.1.9	ipRouteProto	INTEGER	RO	The routing mechanism via which this route was learned

Object-ID	Object name	Syntax	Access	Description
1.3.6.1.2.1.4.21.1.10	ipRouteAge	INTEGER	RW	The number of seconds since this route was last updated or otherwise determined to be correct
1.3.6.1.2.1.4.21.1.11	ipRouteMask	IpAddress	RW	Indicate the mask to be logical-ANDed with the destination address before being compared to the value in the ipRouteDest field
1.3.6.1.2.1.4.21.1.12	ipRouteMetric5	INTEGER	RW	An alternate routing metric for this route
1.3.6.1.2.1.4.21.1.13	ipRouteInfo	OBJECT IDENTIFIER	RO	A reference to MIB definitions specific to the particular routing protocol which is responsible for this route, as determined by the value specified in the route's ipRouteProto value
1.3.6.1.2.1.4.22	ipNetToMediaTable	SEQUENCE OF IpNetToMediaEntry		The IP Address Translation table used for mapping from IP addresses to physical addresses
1.3.6.1.2.1.4.22.1	ipNetToMediaEntry	IpNetToMediaEntry		Each entry contains one IpAddress to `physical' address equivalence
1.3.6.1.2.1.4.22.1.1	ipNetToMediaIfIndex	INTEGER	RW	The interface on which this entry's equivalence is effective
1.3.6.1.2.1.4.22.1.2	ipNetToMediaPhysAddress	PhysAddress	RW	The media-dependent `physical' address
1.3.6.1.2.1.4.22.1.3	ipNetToMediaNetAddress	IpAddress	RW	The IpAddress corresponding to the media- dependent `physical' address
1.3.6.1.2.1.4.22.1.4	ipNetToMediaType	INTEGER	RW	The type of mapping
1.3.6.1.2.1.4.23	ipRoutingDiscards	Counter	RO	The number of routing entries which were chosen to be discarded even though they are valid
1.3.6.1.2.1.5	icmp			ICMP MIB, see mib-2.my
1.3.6.1.2.1.5.1	icmpInMsgs	Counter	RO	The total number of ICMP messages which the entity received
1.3.6.1.2.1.5.2	icmpInErrors	Counter	RO	The number of ICMP messages which the entity received but determined as having ICMP-specific errors (bad ICMP checksums, bad length, etc.)

Object-ID	Object name	Syntax	Access	Description
1.3.6.1.2.1.5.3	icmpInDestUnreachs	Counter	RO	The number of ICMP Destination Unreachable messages received
1.3.6.1.2.1.5.4	icmpInTimeExcds	Counter	RO	The number of ICMP Time Exceeded messages received
1.3.6.1.2.1.5.5	icmpInParmProbs	Counter	RO	The number of ICMP Parameter Problem messages received
1.3.6.1.2.1.5.6	icmpInSrcQuenchs	Counter	RO	The number of ICMP Source Quench messages received
1.3.6.1.2.1.5.7	icmpInRedirects	Counter	RO	The number of ICMP Redirect messages received
1.3.6.1.2.1.5.8	icmpInEchos	Counter	RO	The number of ICMP Echo (request) messages received
1.3.6.1.2.1.5.9	icmpInEchoReps	Counter	RO	The number of ICMP Echo Reply messages received
1.3.6.1.2.1.5.10	icmpInTimestamps	Counter	RO	The number of ICMP Timestamp (request) messages received
1.3.6.1.2.1.5.11	icmpInTimestampReps	Counter	RO	The number of ICMP Timestamp Reply messages received
1.3.6.1.2.1.5.12	icmpInAddrMasks	Counter	RO	The number of ICMP Address Mask Request messages received
1.3.6.1.2.1.5.13	icmpInAddrMaskReps	Counter	RO	The number of ICMP Address Mask Reply messages received
1.3.6.1.2.1.5.14	icmpOutMsgs	Counter	RO	The total number of ICMP messages which this entity attempted to send
1.3.6.1.2.1.5.15	icmpOutErrors	Counter	RO	The number of ICMP messages which this entity did not send due to problems discovered within ICMP such as a lack of buffers
1.3.6.1.2.1.5.16	icmpOutDestUnreachs	Counter	RO	The number of ICMP Destination Unreachable messages sent
1.3.6.1.2.1.5.17	icmpOutTimeExcds	Counter	RO	The number of ICMP Time Exceeded messages sent
1.3.6.1.2.1.5.18	icmpOutParmProbs	Counter	RO	The number of ICMP Parameter Problem messages sent
1.3.6.1.2.1.5.19	icmpOutSrcQuenchs	Counter	RO	The number of ICMP Source Quench messages sent
1.3.6.1.2.1.5.20	icmpOutRedirects	Counter	RO	The number of ICMP Redirect messages sent

Object-ID	Object name	Syntax	Access	Description
1.3.6.1.2.1.5.21	icmpOutEchos	Counter	RO	The number of ICMP Echo (request) messages sent
1.3.6.1.2.1.5.22	icmpOutEchoReps	Counter	RO	The number of ICMP Echo Reply messages sent
1.3.6.1.2.1.5.23	icmpOutTimestamps	Counter	RO	The number of ICMP Timestamp (request) messages sent
1.3.6.1.2.1.5.24	icmpOutTimestampReps	Counter	RO	The number of ICMP Timestamp Reply messages sent
1.3.6.1.2.1.5.25	icmpOutAddrMasks	Counter	RO	The number of ICMP Address Mask Request messages sent
1.3.6.1.2.1.5.26	icmpOutAddrMaskReps	Counter	RO	The number of ICMP Address Mask Reply messages sent
1.3.6.1.2.1.6	tcp			TCP MIB, see mib-2.my
1.3.6.1.2.1.6.1	tcpRtoAlgorithm	INTEGER	RO	The algorithm used to determine the timeout value used for retransmitting unacknowledged octets
1.3.6.1.2.1.6.2	tcpRtoMin	INTEGER	RO	The minimum value permitted by a TCP implementation for the retransmission timeout, measured in milliseconds
1.3.6.1.2.1.6.3	tcpRtoMax	INTEGER	RO	The maximum value permitted by a TCP implementation for the retransmission timeout, measured in milliseconds
1.3.6.1.2.1.6.4	tcpMaxConn	INTEGER	RO	The limit on the total number of TCP connections the entity can support. In entities where the maximum number of connections is dynamic, this object should contain the value -1
1.3.6.1.2.1.6.5	tcpActiveOpens	Counter	RO	The number of times TCP connections have made a direct transition to the SYN-SENT state from the CLOSED state
1.3.6.1.2.1.6.6	tcpPassiveOpens	Counter	RO	The number of times TCP connections have made a direct transition to the SYN-RCVD state from the LISTEN state

Object-ID	Object name	Syntax	Access	Description
1.3.6.1.2.1.6.7	tcpAttemptFails	Counter	RO	The number of times TCP connections have made a direct transition to the CLOSED state from either the SYN-SENT state or the SYN-RCVD state, plus the number of times TCP connections have made a direct transition to the LISTEN state from the SYN-RCVD state
1.3.6.1.2.1.6.8	tcpEstabResets	Counter	RO	The number of times TCP connections have made a direct transition to the CLOSED state from either the ESTABLISHED state or the CLOSE-WAIT state
1.3.6.1.2.1.6.9	tcpCurrEstab	Gauge	RO	The number of TCP connections for which the current state is either ESTABLISHED or CLOSE- WAIT
1.3.6.1.2.1.6.10	tcpInSegs	Counter	RO	The total number of segments received, including those received in error
1.3.6.1.2.1.6.11	tcpOutSegs	Counter	RO	The total number of segments sent, including those on current connections but excluding those containing only retransmitted octets
1.3.6.1.2.1.6.12	tcpRetransSegs	Counter	RO	The total number of segments retransmitted - that is, the number of TCP segments transmitted containing one or more previously transmitted octets
1.3.6.1.2.1.6.13	tcpConnTable	SEQUENCE OF TcpConnEntry		A table containing TCP connection-specific information
1.3.6.1.2.1.6.13.1	tcpConnEntry	TcpConnEntry		Information about a particular current TCP connection
1.3.6.1.2.1.6.13.1.1	tcpConnState	INTEGER	RW	The state of this TCP connection
1.3.6.1.2.1.6.13.1.2	tcpConnLocalAddress	IpAddress	RO	The local IP address for this TCP connection
1.3.6.1.2.1.6.13.1.3	tcpConnLocalPort	INTEGER (0..65535)	RO	The local port number for this TCP connection
1.3.6.1.2.1.6.13.1.4	tcpConnRemAddress	IpAddress	RO	The remote IP address for this TCP connection

Object-ID	Object name	Syntax	Access	Description
1.3.6.1.2.1.6.13.1.5	tcpConnRemPort	INTEGER (0..65535)	RO	The remote port number for this TCP connection
1.3.6.1.2.1.6.14	tcpInErrs	Counter	RO	The total number of segments received in error (e.g., bad TCP checksums)
1.3.6.1.2.1.6.15	tcpOutRsts	Counter	RO	The number of TCP segments sent containing the RST flag
1.3.6.1.2.1.7	udp			UDP MIB, see mib-2.my
1.3.6.1.2.1.7.1	udpInDatagrams	Counter	RO	The total number of UDP datagrams delivered to UDP users
1.3.6.1.2.1.7.2	udpNoPorts	Counter	RO	The total number of received UDP datagrams for which there was no application at the destination port
1.3.6.1.2.1.7.3	udpInErrors	Counter	RO	The number of received UDP datagrams that could not be delivered for reasons other than the lack of an application at the destination port
1.3.6.1.2.1.7.4	udpOutDatagrams	Counter	RO	The total number of UDP datagrams sent from this entity
1.3.6.1.2.1.7.5	udpTable	SEQUENCE OF UdpEntry		A table containing UDP listener information
1.3.6.1.2.1.7.5.1	udpEntry	udpEntry		Information about a particular current UDP listener
1.3.6.1.2.1.7.5.1.1	udpLocalAddress	IpAddress	RO	The local IP address for this UDP listener
1.3.6.1.2.1.7.5.1.2	udpLocalPort	INTEGER (0..65535)	RO	The local port number for this UDP listener
1.3.6.1.2.1.8	egp			EGP MIB, see mib-2.my
1.3.6.1.2.1.8.1	egpInMsgs	Counter	RO	The number of EGP messages received without error
1.3.6.1.2.1.8.2	egpInErrors	Counter	RO	The number of EGP messages received that proved to be in error
1.3.6.1.2.1.8.3	egpOutMsgs	Counter	RO	The total number of locally generated EGP messages

Object-ID	Object name	Syntax	Access	Description
1.3.6.1.2.1.8.4	egpOutErrors	Counter	RO	The number of locally generated EGP messages not sent due to resource limitations within an EGP entity
1.3.6.1.2.1.8.5	egpNeighTable	SEQUENCE OF EgpNeighEntry		The EGP neighbor table
1.3.6.1.2.1.8.5.1	egpNeighEntry	EgpNeighEntry		Information about this entity's relationship with a particular EGP neighbor
1.3.6.1.2.1.8.5.1.1	egpNeighState	INTEGER	RO	The EGP state of the local system with respect to this entry's EGP neighbor
1.3.6.1.2.1.8.5.1.2	egpNeighAddr	IpAddress	RO	The IP address of this entry's EGP neighbor
1.3.6.1.2.1.8.5.1.3	egpNeighAs	INTEGER	RO	The autonomous system of this EGP peer
1.3.6.1.2.1.8.5.1.4	egpNeighInMsgs	Counter	RO	The number of EGP messages received without error from this EGP peer
1.3.6.1.2.1.8.5.1.5	egpNeighInErrs	Counter	RO	The number of EGP messages received from this EGP peer that proved to be in error (e.g., bad EGP checksum)
1.3.6.1.2.1.8.5.1.6	egpNeighOutMsgs	Counter	RO	The number of locally generated EGP messages to this EGP peer
1.3.6.1.2.1.8.5.1.7	egpNeighOutErrs	Counter	RO	The number of locally generated EGP messages not sent to this EGP peer due to resource limitations within an EGP entity
1.3.6.1.2.1.8.5.1.8	egpNeighInErrMsgs	Counter	RO	The number of EGP-defined error messages received from this EGP peer
1.3.6.1.2.1.8.5.1.9	egpNeighOutErrMsgs	Counter	RO	The number of EGP-defined error messages sent to this EGP peer
1.3.6.1.2.1.8.5.1.10	egpNeighStateUps	Counter	RO	The number of EGP state transitions to the UP state with this EGP peer
1.3.6.1.2.1.8.5.1.11	egpNeighStateDowns	Counter	RO	The number of EGP state transitions from the UP state to any other state with this EGP peer

Object-ID	Object name	Syntax	Access	Description
1.3.6.1.2.1.8.5.1.12	egpNeighIntervalHello	INTEGER	RO	The interval between EGP Hello command retransmissions (in hundredths of a second)
1.3.6.1.2.1.8.5.1.13	egpNeighIntervalPoll	INTEGER	RO	The interval between EGP poll command retransmissions (in hundredths of a second)
1.3.6.1.2.1.8.5.1.14	egpNeighMode	INTEGER	RO	The polling mode of this EGP entity, either passive or active active(1), passive(2)
1.3.6.1.2.1.8.5.1.15	egpNeighEventTrigger	INTEGER	RW	A control variable used to trigger operator- initiated Start and Stop events start(1), stop(2)
1.3.6.1.2.1.8.6	egpAs	INTEGER	RO	The autonomous system number of this EGP entity
1.3.6.1.2.1.10	transmission			Transmission MIB, see rfc2127.my
1.3.6.1.2.1.10.20	isdnMib			The MIB module to describe the management of ISDN interfaces
1.3.6.1.2.1.10.20.1	isdnMibObjects			ISDN MIB object definitions
1.3.6.1.2.1.10.20.1.1	isdnBasicRateGroup			This group describes physical basic rate interfaces
1.3.6.1.2.1.10.20.1.1.1	isdnBasicRateTable	SEQUENCE OF IsdnBasicRateEntry		Table containing configuration and operational parameters for all physical Basic Rate interfaces on this managed device
1.3.6.1.2.1.10.20.1.1.1.1	isdnBasicRateEntry	IsdnBasicRateEntry		An entry in the ISDN Basic Rate Table
1.3.6.1.2.1.10.20.1.1.1.1.1	isdnBasicRateIfType	INTEGER	RW	The physical interface type For 'S/T' interfaces, also called 'Four-wire Basic Access Interface', the value of this object is isdns(75). For 'U' interfaces, also called 'Two-wire Basic Access Interface', the value of this object is isdnu(76)
1.3.6.1.2.1.10.20.1.1.1.1.2	isdnBasicRateLineTopology	INTEGER	RW	The line topology to be used for this interface pointToPoint(1), pointToMultipoint(2)

Object-ID	Object name	Syntax	Access	Description
1.3.6.1.2.1.10.20.1.1.1.3	isdnBasicRateIfMode	INTEGER	RW	The physical interface mode. For TE mode, the value of this object is te(1). For NT mode, the value of this object is nt(2)
1.3.6.1.2.1.10.20.1.1.1.4	isdnBasicRateSignalMode	INTEGER	RW	The signaling channel operational mode for this interface. If active(1) there is a signaling channel on this interface. If inactive(2) a signaling channel is not available.
1.3.6.1.2.1.10.20.1.2	isdnBearerGroup			This group describes physical basic rate interfaces
1.3.6.1.2.1.10.20.1.2.1	isdnBearerTable	SEQUENCE OF IsdnBearerEntry		This table defines port specific operational, statistics and active call data for ISDN B channels. Each entry in this table describes one B (bearer) channel
1.3.6.1.2.1.10.20.1.2.1.1	isdnBearerEntry	IsdnBearerEntry		Operational and statistics information relating to one port. A port is a single B channel
1.3.6.1.2.1.10.20.1.2.1.1.1	isdnBearerChannelType	INTEGER	RW	The B channel type. If the B channel is connected to a dialup line, this object has a value of dialup(1). In this case, it is controlled by an associated signaling channel. If the B channel is connected to a leased line, this object has a value of leased(2). For leased line B channels, there is no signaling channel control available
1.3.6.1.2.1.10.20.1.2.1.1.2	isdnBearerOperStatus	INTEGER	RO	The current call control state for this port. idle(1): The B channel is idle, no call or call attempt is going on. connecting(2): A connection attempt (outgoing call) is being made on this interface. connected(3): An incoming call is in the process of validation. active(4): A call is active on this interface
1.3.6.1.2.1.10.20.1.2.1.1.3	isdnBearerChannelNumber	INTEGER (1..30)	RO	The identifier being used by a signaling protocol to identify this B channel, also referred to as B channel number

Object-ID	Object name	Syntax	Access	Description
1.3.6.1.2.1.10.20.1.2.1.1.4	isdnBearerPeerAddress	DisplayString	RO	The ISDN address the current or last call is or was connected to
1.3.6.1.2.1.10.20.1.2.1.1.5	isdnBearerPeerSubAddress	DisplayString	RO	The ISDN subaddress the current or last call is or was connected to
1.3.6.1.2.1.10.20.1.2.1.1.6	isdnBearerCallOrigin	INTEGER	RO	The call origin for the current or last call unknown(1), originate(2), answer(3), callback(4)
1.3.6.1.2.1.10.20.1.2.1.1.7	isdnBearerInfoType	INTEGER	RO	The Information Transfer Capability for the current or last call. speech(2) refers to a non-data connection, whereas audio31(6) and audio7(7) refer to data mode connections
1.3.6.1.2.1.10.20.1.2.1.1.8	isdnBearerMultirate	TruthValue	RO	This flag indicates if the current or last call used multirate
1.3.6.1.2.1.10.20.1.2.1.1.9	isdnBearerCallSetupTime	TimeStamp	RO	The value of sysUpTime when the ISDN setup message for the current or last call was sent or received
1.3.6.1.2.1.10.20.1.2.1.1.10	isdnBearerCallConnectTime	TimeStamp	RO	The value of sysUpTime when the ISDN connect message for the current or last call was sent or received
1.3.6.1.2.1.10.20.1.2.1.1.11	isdnBearerChargedUnits	Gauge32	RO	The number of charged units for the current or last connection
1.3.6.1.2.1.10.20.1.3	isdnSignalingGroup			Signaling channel configuration table
1.3.6.1.2.1.10.20.1.3.1	isdnSignalingGetIndex	TestAndIncr	RW	The recommended procedure for selecting a new index for isdnSignalingTable row creation is to GET the value of this object, and then to SET the object with the same value. If the SET operation succeeds, the manager can use this value as an index to create a new row in this table
1.3.6.1.2.1.10.20.1.3.2	isdnSignalingTable	SEQUENCE OF IsdnSignalingEntry		ISDN signaling table containing configuration and operational parameters for all ISDN signaling channels on this managed device
1.3.6.1.2.1.10.20.1.3.2.1	isdnSignalingEntry	IsdnSignalingEntry		An entry in the ISDN Signaling Table

Object-ID	Object name	Syntax	Access	Description
1.3.6.1.2.1.10.20.1.3.2.1.1	isdnSignalingIndex	INTEGER (1..2147483647)		The index value which uniquely identifies an entry in the isdnSignalingTable
1.3.6.1.2.1.10.20.1.3.2.1.2	isdnSignalingIfIndex	InterfaceIndex	RO	The ifIndex value of the interface associated with this signaling channel
1.3.6.1.2.1.10.20.1.3.2.1.3	isdnSignalingProtocol	IsdnSignalingProtocol	RC	The particular protocol type supported by the switch providing access to the ISDN network to which this signaling channel is connected
1.3.6.1.2.1.10.20.1.3.2.1.4	isdnSignalingCallingAddress	DisplayString	RC	The ISDN Address to be assigned to this signaling channel
1.3.6.1.2.1.10.20.1.3.2.1.5	isdnSignalingSubAddress	DisplayString	RC	Supplementary information to the ISDN address assigned to this signaling channel
1.3.6.1.2.1.10.20.1.3.2.1.6	isdnSignalingBchannelCount	Integer32 (1..65535)	RC	The total number of B channels (bearer channels) managed by this signaling channel
1.3.6.1.2.1.10.20.1.3.2.1.7	isdnSignalingInfoTrapEnable	INTEGER	RC	Indicates whether isdnMibCallInformation traps should be generated for calls on this signaling channel
1.3.6.1.2.1.10.20.1.3.2.1.8	isdnSignalingStatus	RowStatus	RC	This object is used to create and delete rows in the isdnSignalingTable
1.3.6.1.2.1.10.20.1.3.3	isdnSignalingStatsTable	SEQUENCE OF IsdnSignalingStatsEntry		ISDN signaling table containing statistics information for all ISDN signaling channels on this managed device
1.3.6.1.2.1.10.20.1.3.3.1	isdnSignalingStatsEntry	IsdnSignalingStatsEntry		An entry in the ISDN Signaling statistics Table
1.3.6.1.2.1.10.20.1.3.3.1.1	isdnSigStatsInCalls	Counter32	RO	The number of incoming calls on this interface
1.3.6.1.2.1.10.20.1.3.3.1.2	isdnSigStatsInConnected	Counter32	RO	The number of incoming calls on this interface which were actually connected
1.3.6.1.2.1.10.20.1.3.3.1.3	isdnSigStatsOutCalls	Counter32	RO	The number of outgoing calls on this interface
1.3.6.1.2.1.10.20.1.3.3.1.4	isdnSigStatsOutConnected	Counter32	RO	The number of outgoing calls on this interface which were actually connected

Object-ID	Object name	Syntax	Access	Description
1.3.6.1.2.1.10.20.1.3.3.1.5	isdnSigStatsChargedUnits	Counter32	RO	The number of charging units on this interface since system startup
1.3.6.1.2.1.10.20.1.3.4	isdnLapdTable	SEQUENCE OF IsdnLapdEntry		Table containing configuration and statistics information for all LAPD (D channel Data Link) interfaces on this managed device
1.3.6.1.2.1.10.20.1.3.4.1	isdnLapdEntry	IsdnLapdEntry		An entry in the LAPD Table
1.3.6.1.2.1.10.20.1.3.4.1.1	isdnLapdPrimaryChannel	TruthValue	RW	If set to true(1), this D channel is the designated primary D channel if D channel backup is active
1.3.6.1.2.1.10.20.1.3.4.1.2	isdnLapdOperStatus	INTEGER	RO	The operational status of this interface
1.3.6.1.2.1.10.20.1.3.4.1.3	isdnLapdPeerSabme	Counter32	RO	The number of peer SABME frames received on this interface
1.3.6.1.2.1.10.20.1.3.4.1.4	isdnLapdRecvdFrmr	Counter32	RO	The number of LAPD FRMR response frames received
1.3.6.1.2.1.10.20.1.4	isdnEndpointGroup			The Terminal Endpoint group and table
1.3.6.1.2.1.10.20.1.4.1	isdnEndpointGetIndex			The recommended procedure for selecting a new index for isdnEndpointTable row creation is to GET the value of this object, and then to SET the object with the same value. If the SET operation succeeds, the manager can use this value as an index to create a new row in this table
1.3.6.1.2.1.10.20.1.4.2	isdnEndpointTable	SEQUENCE OF IsdnEndpointEntry		Table containing configuration for Terminal Endpoints
1.3.6.1.2.1.10.20.1.4.2.1	isdnEndpointEntry	IsdnEndpointEntry		An entry in the Terminal Endpoint Table
1.3.6.1.2.1.10.20.1.4.2.1.1	isdnEndpointIndex	INTEGER (1..2147483647)		The index value which uniquely identifies an entry in the isdnEndpointTable
1.3.6.1.2.1.10.20.1.4.2.1.2	isdnEndpointIfIndex	InterfaceIndex	RO	The ifIndex value of the interface associated with this Terminal Endpoint
1.3.6.1.2.1.10.20.1.4.2.1.3	isdnEndpointIfType	IANAifType	RC	The interface type for this Terminal Endpoint. Interface types of x25ple(40) and isdn(63) are allowed

Object-ID	Object name	Syntax	Access	Description
1.3.6.1.2.1.10.20.1.4.2.1.4	isdnEndpointTeiType	INTEGER	RC	The type of TEI (Terminal Endpoint Identifier) used for this Terminal Endpoint. In case of dynamic(1), the TEI value is selected by the switch. In case of static(2), a valid TEI value has to be entered in the isdnEndpointTeiValue object
1.3.6.1.2.1.10.20.1.4.2.1.5	isdnEndpointTeiValue	INTEGER (0..255)	RC	The TEI (Terminal Endpoint Identifier) value for this Terminal Endpoint
1.3.6.1.2.1.10.20.1.4.2.1.6	isdnEndpointSpid	DisplayString	RC	The Service profile IDentifier (SPID) information for this Terminal Endpoint
1.3.6.1.2.1.10.20.1.4.2.1.7	isdnEndpointStatus	RowStatus	RC	This object is used to create and delete rows in the isdnEndpointTable
1.3.6.1.2.1.10.20.1.5	isdnDirectoryGroup			The Directory Number group
1.3.6.1.2.1.10.20.1.5.1	isdnDirectoryTable	SEQUENCE OF IsdnDirectoryEntry		Table containing Directory Numbers
1.3.6.1.2.1.10.20.1.5.1.1	isdnDirectoryEntry	IsdnDirectoryEntry		An entry in the Directory Number Table
1.3.6.1.2.1.10.20.1.5.1.1.1	isdnDirectoryIndex	INTEGER (1..'7fffffff'h)		The index value which uniquely identifies an entry in the isdnDirectoryTable
1.3.6.1.2.1.10.20.1.5.1.1.2	isdnDirectoryNumber	DisplayString	RC	A Directory Number. Directory Numbers are used to identify incoming calls on the signaling channel given in isdnDirectorySigIndex
1.3.6.1.2.1.10.20.1.5.1.1.3	isdnDirectorySigIndex	INTEGER (1..2147483647)	RC	An index pointing to an ISDN signaling channel
1.3.6.1.2.1.10.20.1.5.1.1.4	isdnDirectoryStatus	RowStatus	RC	This object is used to create and delete rows in the isdnDirectoryTable
1.3.6.1.2.1.10.20.2	isdnMibTrapPrefix			
1.3.6.1.2.1.10.20.2.0	isdnMibTraps			

Object-ID	Object name	Syntax	Access	Description
1.3.6.1.2.1.10.20.2.0.1	isdnMibCallInformation	TRAP		This trap/inform is sent to the manager under the following conditions: - on incoming calls for each call which is rejected for policy reasons (e.g. unknown neighbor or access violation) - on outgoing calls whenever a call attempt is determined to have ultimately failed. In the event that call retry is active, then this will be after all retry attempts have failed. - whenever a call connects. In this case, the object isdnBearerCallConnectTime should be included in the trap.
1.3.6.1.2.1.10.20.3	isdnMibConformance			
1.3.6.1.2.1.10.20.3.1	isdnMibCompliances			
1.3.6.1.2.1.10.20.3.2	isdnMibGroups			
1.3.6.1.2.1.11	snmp			SNMP MIB, see mib-2.my
1.3.6.1.2.1.11.1	snmpInPkts	Counter	RO	The total number of Messages delivered to the SNMP entity from the transport service
1.3.6.1.2.1.11.2	snmpOutPkts	Counter	RO	The total number of SNMP Messages which were passed from the SNMP protocol entity to the transport service
1.3.6.1.2.1.11.3	snmpInBadVersions	Counter	RO	The total number of SNMP Messages which were delivered to the SNMP protocol entity and were for an unsupported SNMP version
1.3.6.1.2.1.11.4	snmpInBadCommunityNames	Counter	RO	The total number of SNMP Messages delivered to the SNMP protocol entity which used a SNMP community name not known to said entity
1.3.6.1.2.1.11.5	snmpInBadCommunityUses	Counter	RO	The total number of SNMP Messages delivered to the SNMP protocol entity which represented an SNMP operation which was not allowed by the SNMP community named in the Message

Object-ID	Object name	Syntax	Access	Description
1.3.6.1.2.1.11.6	snmpInASNParseErrs	Counter	RO	The total number of ASN.1 or BER errors encountered by the SNMP protocol entity when decoding received SNMP Messages
1.3.6.1.2.1.11.7				not used
1.3.6.1.2.1.11.8	snmpInTooBigs	Counter	RO	The total number of SNMP PDUs which were delivered to the SNMP protocol entity and for which the value of the error-status field is `tooBig'
1.3.6.1.2.1.11.9	snmpInNoSuchNames	Counter	RO	The total number of SNMP PDUs which were delivered to the SNMP protocol entity and for which the value of the error-status field is `noSuchName'
1.3.6.1.2.1.11.10	snmpInBadValues	Counter	RO	The total number of SNMP PDUs which were delivered to the SNMP protocol entity and for which the value of the error-status field is `badValue'
1.3.6.1.2.1.11.11	snmpInReadOnlys	Counter	RO	The total number valid SNMP PDUs which were delivered to the SNMP protocol entity and for whichéíthe value of the error-status field is `readOnly'
f30h++				
1.3.6.1.2.1.11.12	snmpInGenErrs	Counter	RO	The total number of SNMP PDUs which were delivered to the SNMP protocol entity and for which the value of the error-status field is `genErr'
1.3.6.1.2.1.11.13	snmpInTotalReqVars	Counter	RO	The total number of MIB objects which have been retrieved successfully by the SNMP protocol entity as the result of receiving valid SNMP Get-Request and Get-Next PDUs
1.3.6.1.2.1.11.14	snmpInTotalSetVars	Counter	RO	The total number of MIB objects which have been altered successfully by the SNMP protocol entity as the result of receiving valid SNMP Set-Request PDUs

Object-ID	Object name	Syntax	Access	Description
1.3.6.1.2.1.11.15	snmpInGetRequests	Counter	RO	The total number of SNMP Get-Request PDUs which have been accepted and processed by the SNMP protocol entity
1.3.6.1.2.1.11.16	snmpInGetNexts	Counter	RO	The total number of SNMP Get-Next PDUs which have been accepted and processed by the SNMP protocol entity
1.3.6.1.2.1.11.17	snmpInSetRequests	Counter	RO	The total number of SNMP Set-Request PDUs which have been accepted and processed by the SNMP protocol entity
1.3.6.1.2.1.11.18	snmpInGetResponses	Counter	RO	The total number of SNMP Get-Response PDUs which have been accepted and processed by the SNMP protocol entity
1.3.6.1.2.1.11.19	snmpInTraps	Counter	RO	The total number of SNMP Trap PDUs which have been accepted and processed by the SNMP protocol entity
1.3.6.1.2.1.11.20	snmpOutTooBigs	Counter	RO	The total number of SNMP PDUs which were generated by the SNMP protocol entity and for which the value of the error-status field is `tooBig.'
1.3.6.1.2.1.11.21	snmpOutNoSuchNames	Counter	RO	The total number of SNMP PDUs which were generated by the SNMP protocol entity and for which the value of the error-status is `noSuchName'
1.3.6.1.2.1.11.22	snmpOutBadValues	Counter	RO	The total number of SNMP PDUs which were generated by the SNMP protocol entity and for which the value of the error-status field is `badValue'
1.3.6.1.2.1.11.23				not used
1.3.6.1.2.1.11.24	snmpOutGenErrs	Counter	RO	The total number of SNMP PDUs which were generated by the SNMP protocol entity and for which the value of the error-status field is `genErr'
1.3.6.1.2.1.11.25	snmpOutGetRequests	Counter	RO	The total number of SNMP Get-Request PDUs which have been generated by the SNMP protocol entity

Object-ID	Object name	Syntax	Access	Description
1.3.6.1.2.1.11.26	snmpOutGetNexts	Counter	RO	The total number of SNMP Get-Next PDUs which have been generated by the SNMP protocol entity
1.3.6.1.2.1.11.27	snmpOutSetRequests	Counter	RO	The total number of SNMP Set-Request PDUs which have been generated by the SNMP protocol entity
1.3.6.1.2.1.11.28	snmpOutGetResponses	Counter	RO	The total number of SNMP Get-Response PDUs which have been generated by the SNMP protocol entity
1.3.6.1.2.1.11.29	snmpOutTraps	Counter	RO	The total number of SNMP Trap PDUs which have been generated by the SNMP protocol entity
1.3.6.1.2.1.11.30	snmpEnableAuthenTraps	INTEGER	RW	Indicates whether the SNMP agent process is permitted to generate authentication-failure traps. enabled(1), disabled(2)
1.3.6.1.2.1.16	rmon			RMON MIB, see my_rmon2.my
1.3.6.1.2.1.16.19	probeConfig			This group controls the configuration of various operating parameters of the probe
1.3.6.1.2.1.16.19.1	probeCapabilities	BITS	RO	This group controls the configuration of various operating parameters of the probe
1.3.6.1.2.1.16.19.2	probeSoftwareRev	DisplayString (SIZE(0..15))	RO	The software revision of this device
1.3.6.1.2.1.16.19.3	probeHardwareRev	DisplayString (SIZE(0..31))	RO	The hardware revision of this device
1.3.6.1.2.1.16.19.4	probeDateTime	OCTET STRING	RW	Probe's current date and time

Object-ID	Object name	Syntax	Access	Description
1.3.6.1.2.1.16.19.5	probeResetControl	INTEGER	RW	Setting this object to warmBoot(2) causes the device to restart the application software with current configuration parameters saved in non-volatile memory. Setting this object to coldBoot(3) causes the device to reinitialize configuration parameters in non-volatile memory to default values and restart the application software. When the device is running normally, this variable has a value of running(1)
1.3.6.1.2.1.16.19.6	probeDownloadFile	DisplayString (SIZE(0..127))	RW	The file name to be downloaded from the TFTP server when a download is next requested via this MIB
1.3.6.1.2.1.16.19.7	probeDownloadTFTPServer	IpAddress	RW	The IP address of the TFTP server that contains the boot image to load when a download is next requested via this MIB
1.3.6.1.2.1.16.19.8	probeDownloadAction	INTEGER	RW	When this object is set to downloadToRAM(2) or downloadToPROM(3), the device will discontinue its normal operation and begin download of the image specified by probeDownloadFile from the server specified by probeDownloadTFTPServer using the TFTP protocol. If downloadToRAM(2) is specified, the new image is copied to RAM only (the old image remains unaltered in the flash EPROM). If downloadToPROM(3) is specified, the new image is written to the flash EPROM memory after its checksum has been verified to be correct. When the download process is completed, the device will warm boot to restart the newly loaded application. When the device is not downloading, this object will have a value of notDownloading(1).

Object-ID	Object name	Syntax	Access	Description
1.3.6.1.2.1.16.19.9	probeDownloadStatus	INTEGER	RO	The status of the last download procedure, if any. This object will have a value of downloadStatusUnknown(2) if no download process has been performed
1.3.6.1.2.1.16.19.13	trapDestTable	SEQUENCE OF TrapDestEntry		A list of trap destination entries
1.3.6.1.2.1.16.19.13.1	trapDestEntry	TrapDestEntry		This entry includes a destination IP address to which to send traps for this community
1.3.6.1.2.1.16.19.13.1.1	trapDestIndex	Integer32 (1..65535)		A value that uniquely identifies this trapDestEntry
1.3.6.1.2.1.16.19.13.1.2	trapDestCommunity	OCTET STRING (SIZE(0..127))	RC	A community to which this destination address belongs
1.3.6.1.2.1.16.19.13.1.3	trapDestProtocol	INTEGER	RC	The protocol with which to send this trap ip(1), ipx(2)
1.3.6.1.2.1.16.19.13.1.4	trapDestAddress	OCTET STRING	RC	The address to send traps on behalf of this entry
1.3.6.1.2.1.16.19.13.1.5	trapDestOwner	DisplayString	RC	The entity that configured this entry and is therefore using the resources assigned to it
1.3.6.1.2.1.16.19.13.1.6	trapDestStatus	RowStatus	RC	The status of this trap destination entry
1.3.6.1.2.1.30	ianaifType			IANA MIB, see iana.my The MIB module which defines the IANAifType textual convention, and thus the enumerated values of the ifType object defined in MIB-II's ifTable
1.3.6.1.2.1.31	ifMIB			IF MIB, see rfc2233.my The MIB module to describe generic objects for network interface sub-layers. This MIB is an updated version of MIB-II's ifTable, and incorporates the extensions defined in RFC 1229.
1.3.6.1.2.1.31.1	ifMIBObjects			

Object-ID	Object name	Syntax	Access	Description
1.3.6.1.2.1.31.1.1	ifXTable	SEQUENCE OF IfXEntry		A list of interface entries. The number of entries is given by the value of ifNumber. This table contains additional objects for the interface table.
1.3.6.1.2.1.31.1.1.1	ifXEntry	IfXEntry		An entry containing additional management information applicable to a particular interface.
1.3.6.1.2.1.31.1.1.1.1	ifName	DisplayString	RO	The textual name of the interface.
1.3.6.1.2.1.31.1.1.1.2	ifInMulticastPkts	Counter	RO	The number of packets, delivered by this sub-layer to a higher (sub-)layer, which were addressed to a multicast address at this sub-layer.
1.3.6.1.2.1.31.1.1.1.3	ifInBroadcastPkts	Counter	RO	The number of packets, delivered by this sub-layer to a higher (sub-)layer, which were addressed to a broadcast address at this sub-layer.
1.3.6.1.2.1.31.1.1.1.4	ifOutMulticastPkts	Counter	RO	The total number of packets that higher-level protocols requested be transmitted, and which were addressed to a multicast address at this sub-layer, including those that were discarded or not sent.
1.3.6.1.2.1.31.1.1.1.5	ifOutBroadcastPkts	Counter	RO	The total number of packets that higher-level protocols requested be transmitted, and which were addressed to a broadcast address at this sub-layer, including those that were discarded or not sent.
1.3.6.1.2.1.31.1.1.1.6	ifHCInOctets	Counter64	RO	The total number of octets received on the interface, including framing characters.
1.3.6.1.2.1.31.1.1.1.7	ifHCInUcastPkts	Counter64	RO	The number of packets, delivered by this sub-layer to a higher (sub-)layer, which were not addressed to a multicast or broadcast address at this sub-layer.
1.3.6.1.2.1.31.1.1.1.8	ifHCInMulticastPkts	Counter64	RO	The number of packets, delivered by this sub-layer to a higher (sub-)layer, which were addressed to a multicast address at this sub-layer.

Object-ID	Object name	Syntax	Access	Description
1.3.6.1.2.1.31.1.1.1.9	ifHCInBroadcastPkts	Counter64	RO	The number of packets, delivered by this sub-layer to a higher (sub-)layer, which were addressed to a broadcast address at this sub-layer.
1.3.6.1.2.1.31.1.1.1.10	ifHCOutOctets	Counter64	RO	The total number of octets transmitted out of the interface, including framing characters.
1.3.6.1.2.1.31.1.1.1.11	ifHCOutUcastPkts	Counter64	RO	The total number of packets that higher-level protocols requested be transmitted, and which were not addressed to a multicast or broadcast address at this sub-layer, including those that were discarded or not sent.
1.3.6.1.2.1.31.1.1.1.12	ifHCOutMulticastPkts	Counter64	RO	The total number of packets that higher-level protocols requested be transmitted, and which were addressed to a multicast address at this sub-layer, including those that were discarded or not sent.
1.3.6.1.2.1.31.1.1.1.13	ifHCOutBroadcastPkts	Counter64	RO	The total number of packets that higher-level protocols requested be transmitted, and which were addressed to a broadcast address at this sub-layer, including those that were discarded or not sent.
1.3.6.1.2.1.31.1.1.1.14	ifLinkUpDownTrapEnable	INTEGER	RW	Indicates whether linkUp/linkDown traps should be generated for this interface. enabled(1), disabled(2)
1.3.6.1.2.1.31.1.1.1.15	ifHighSpeed	Gauge	RO	An estimate of the interface's current bandwidth in units of 1,000,000 bits per second.
1.3.6.1.2.1.31.1.1.1.16	ifPromiscuousMode	TruthValue	RW	’true(1)’ when the station accepts all packets/frames transmitted on the media. ’false(2)’ if this interface only accepts packets/frames that are addressed to this station.
1.3.6.1.2.1.31.1.1.1.17	ifConnectorPresent	TruthValue	RO	'true(1)' if the interface sublayer has a physical connector ’false(2)' otherwise.

Object-ID	Object name	Syntax	Access	Description
1.3.6.1.2.1.31.1.1.1.18	ifAlias	DisplayString	RW	This object is an 'alias' name for the interface as specified by a network manager, and provides a non-volatile 'handle' for the interface.
1.3.6.1.2.1.31.1.1.1.19	ifCounterDiscontinuityTime	TimeStamp	RO	The value of sysUpTime on the most recent occasion at which any one or more of this interface's counters suffered a discontinuity.
1.3.6.1.2.1.31.1.2	ifStackTable	SEQUENCE OF IfStackEntry		The table containing information on the relationships between the multiple sub-layers of network interfaces.
1.3.6.1.2.1.31.1.2.1	ifStackEntry	IfStackEntry		Information on a particular relationship between two sub-layers, specifying that one sub-layer runs on 'top' of the other sub-layer.
1.3.6.1.2.1.31.1.2.1.1	ifStackHigherLayer	Integer32		The value of ifIndex corresponding to the higher sub-layer of the relationship, i.e., the sub-layer which runs on 'top' of the sub-layer identified by the corresponding instance of ifStackLowerLayer.
1.3.6.1.2.1.31.1.2.1.2	ifStackLowerLayer	Integer32		The value of ifIndex corresponding to the lower sub- layer of the relationship, i.e., the sub-layer which runs 'below' the sub-layer identified by the corresponding instance of ifStackHigherLayer.
1.3.6.1.2.1.31.1.2.1.3	ifStackStatus	RowStatus	RC	The status of the relationship between two sub- layers.
1.3.6.1.2.1.31.1.3	ifTestTable	SEQUENCE OF IfTestEntry		This table contains one entry per interface. It defines objects which allow a network manager to instruct an agent to test an interface for various faults. Deprecated
1.3.6.1.2.1.31.1.3.1	ifTestEntry	IfTestEntry		An entry containing objects for invoking tests on an interface. Deprecated
1.3.6.1.2.1.31.1.3.1.1	ifTestId	TestAndIncr	RW	This object identifies the current invocation of the interface's test Deprecated

Object-ID	Object name	Syntax	Access	Description
1.3.6.1.2.1.31.1.3.1.2	ifTestStatus	INTEGER	RW	This object indicates whether or not some manager currently has the necessary 'ownership' required to invoke a test on this interface Deprecated
1.3.6.1.2.1.31.1.3.1.3	ifTestType	AutonomousType	RW	A control variable used to start and stop operator- initiated interface tests Deprecated
1.3.6.1.2.1.31.1.3.1.4	ifTestResult	INTEGER	RO	This object contains the result of the most recently requested test, or the value none(1) if no tests have been requested since the last reset Deprecated
1.3.6.1.2.1.31.1.3.1.5	ifTestCode	OBJECT IDENTIFIER	RO	This object contains a code which contains more specific information on the test result, for example an error-code after a failed test Deprecated
1.3.6.1.2.1.31.1.3.1.6	ifTestOwner	OwnerString	RW	The entity which currently has the 'ownership' required to invoke a test on this interface Deprecated
1.3.6.1.2.1.31.1.4	ifRcvAddressTable	SEQUENCE OF IfRcvAddressEntry		This table contains an entry for each address (broadcast, multicast, or uni-cast) for which the system will receive packets/frames on a particular interface.
1.3.6.1.2.1.31.1.4.1	ifRcvAddressEntry	IfRcvAddressEntry		A list of objects identifying an address for which the system will accept packets/frames on the particular interface identified by the index value ifIndex.
1.3.6.1.2.1.31.1.4.1.1	ifRcvAddressAddress	PhysAddress		An address for which the system will accept packets/frames on this entry's interface.
1.3.6.1.2.1.31.1.4.1.2	ifRcvAddressStatus	RowStatus	RC	This object is used to create and delete rows in the ifRcvAddressTable.

Object-ID	Object name	Syntax	Access	Description
1.3.6.1.2.1.31.1.4.1.3	ifRcvAddressType	INTEGER	RC	This object has the value nonVolatile(3) for those entries in the table which are valid and will not be deleted by the next restart of the managed system. Entries having the value volatile(2) are valid and exist, but have not been saved, so that will not exist after the next restart of the managed system. Entries having the value other(1) are valid and exist but are not classified as to whether they will continue to exist after the next restart.
1.3.6.1.2.1.31.1.5	ifTableLastChange	TimeTicks		The value of sysUpTime at the time of the last creation or deletion of an entry in the ifTable. If the number of entries has been unchanged since the last re-initialization of the local network management subsystem, then this object contains a zero value.
1.3.6.1.2.1.31.1.6	ifStackLastChange	TimeTicks	RO	The value of sysUpTime at the time of the last change of the (whole) interface stack.

Table 13: Data in the SNI specific MIB

Object-ID	Object name	Syntax	Access	Description
1.3.6.1.4.1.231.7.2.7	hg3550mib			hg3550 MIB, see hg1500.my
1.3.6.1.4.1.231.7.2.7.1	errorSigGrouphlb20			Error Signalisation Group MIB containing administration-level trap event history
1.3.6.1.4.1.231.7.2.7.1.1	numberOfTrapHistoryEntries	INTEGER	RW	Contains the number of traps to be found in the trap history table. This value can be used to delete all entries (value = 0).
1.3.6.1.4.1.231.7.2.7.1.2	hlb20TrapHistoryTable	SEQUENCE OF Hlb20TrapHistoryEntry		This table contains information about traps sent by the device.
1.3.6.1.4.1.231.7.2.7.1.2.1	hlb20TrapHistoryEntry	Hlb20TrapHistoryEntry		The trap history table entries.
1.3.6.1.4.1.231.7.2.7.1.2.1.1	trapIndex	INTEGER	RO	Identification of an table entry enabled by this index.
1.3.6.1.4.1.231.7.2.7.1.2.1.2	trapDateTime	DateAndTime	RO	Time, when the trap event occurred.

Object-ID	Object name	Syntax	Access	Description
1.3.6.1.4.1.231.7.2.7.1.2.1.3	hg3trapSeverity	INTEGER	RO	Contains information about the error severity. - normal(1) - warning(2) - minor(3) - major(4) - critical(5)
1.3.6.1.4.1.231.7.2.7.1.2.1.4	hg3trapErrorClass	INTEGER	RO	Contains the error class number (type of trap). - general(1) - voice(2) - data(3) - security(4) - client(5)
1.3.6.1.4.1.231.7.2.7.1.2.1.5	hg3trapErrorCode	INTEGER	RO	Contains the error code.
1.3.6.1.4.1.231.7.2.7.1.2.1.6	hg3trapDescription	DisplayString	RO	Detailed information about the trap event.
1.3.6.1.4.1.231.7.2.7.1.2.1.7	hg3trapHandling	INTEGER	RO	Forwarded(1), if the error produced a trap. Stored(2), if the error data was stored without sending a trap.
1.3.6.1.4.1.231.7.2.7.1.3	hg3numberOfErrorTableEntries	INTEGER	RW	Contains the number of traps to be found in the trap history table. This value can be used to delete all entries (value = 0). deprecated
1.3.6.1.4.1.231.7.2.7.1.4	hg3hlb20ErrorTable	SEQUENCE OF Hlb20ErrorEntry		This table contains information about expert level error events that occur on the hg3550 device. deprecated
1.3.6.1.4.1.231.7.2.7.1.4.1	hg3hlb20ErrorEntry	Hlb20ErrorEntry		The trap history table entries. deprecated
1.3.6.1.4.1.231.7.2.7.1.4.1.1	hg3errorIndex	INTEGER	RO	Contains the error/trace class. deprecated
1.3.6.1.4.1.231.7.2.7.1.4.1.2	hg3errorTimeStamp	OCTET STRING	RO	System-specific timestamp for the error. deprecated

Object-ID	Object name	Syntax	Access	Description
1.3.6.1.4.1.231.7.2.7.1.4.1.3	errorClass	INTEGER	RO	Contains the error/trace class. deprecated
1.3.6.1.4.1.231.7.2.7.1.4.1.4	errorDescription	DisplayString	RO	Detailed information about errors. deprecated
1.3.6.1.4.1.231.7.2.7.2	controlGrouphlb20			Control Group MIB
1.3.6.1.4.1.231.7.2.7.2.1	indexOfLastTrapSent	INTEGER	RO	Contains the index of the last trap which was sent.
1.3.6.1.4.1.231.7.2.7.2.2	trapTypesToBeSent	INTEGER	RW	Defines which error events are signaled as a trap.
1.3.6.1.4.1.231.7.2.7.2.3	sysState	INTEGER	RW	The actual error state of the hg3550 device. - normal(1) - warning(2) - minor(3) - major(4) - critical(5)
1.3.6.1.4.1.231.7.2.7.2.4	sysConnectionState	INTEGER	RO	Indicates if the connection between Hicom 150E Office and hg3550 / Hicom Xpress @LAN was successfully established. - disconnected(1) - connected(2)
1.3.6.1.4.1.231.7.2.7.2.5	sysMacAddress	DisplayString	RO	Contains the MAC Address of this device. (Object not available in hg3550 / Xpress @LAN 1.0)
1.3.6.1.4.1.231.7.2.7.2.6	sysSoftwareVersion	DisplayString	RO	Contains the version string of the system software. (Object not available in HG1500 / Xpress @LAN 1.0)
1.3.6.1.4.1.231.7.2.7.2.7	sysSnmpAgentVersion	DisplayString	RO	Version number of the systems SNMP agent (formatting: x.y.z.)

Object-ID	Object name	Syntax	Access	Description
1.3.6.1.4.1.231.7.2.7.2.8	sysShadowSoftwareVersion	DisplayString	RO	Contains the version string of the inactive software version (flash image) that had been transferred to the device recently. (Object not available in HG1500 / Xpress @LAN 1.0) deprecated
1.3.6.1.4.1.231.7.2.7.2.9	sysHardwareVersion	DisplayString	RO	Hardware version identifier of the device. (Object not available in HG1500 / Xpress @LAN 1.0)
1.3.6.1.4.1.231.7.2.7.2.10	sysOperatingMode	INTEGER	RO	Operating mode of the device. In standard mode (1), the device serves as a normal gateway. In gatekeeper mode (2), it additionally operates as a gatekeeper for voice over IP endpoints. (Object not available in HG1500 / Xpress @LAN 1.0)
1.3.6.1.4.1.231.7.2.7.2.11	sysSwitchoverDateTime	DateAndTime	RW	Date and time for the switchover to the new system software.
1.3.6.1.4.1.231.7.2.7.2.12	sysDownloadAction	INTEGER	RW	When this object is set to downloadAndImmediateSwitchover (2), the device will download the new software from the configured host. After the download is finished, the device will automatically restart with the new software. If downloadAndDelayedSwitchover (3) is specified, the new image is copied to the device. When the tftpDateTime value is matched, the device discontinues its normal operation and does the software switchover. After an automatic reset, it starts with the new system software. Setting downloadWithoutSwitchover (4) initiates a download without switching over to the new software. When the device is not downloading, this object will have a value of notDownloading(1).

Object-ID	Object name	Syntax	Access	Description
1.3.6.1.4.1.231.7.2.7.2.1.13	sysSwitchoverState	INTEGER	RW	The values readyForSwitchover (1) and notReadyForSwitchover (2) indicate whether the system is ready to be switched over to the new software that was downloaded to the shadow flash area, or not. If it is not possible, h150eShadowFlashState gives details on the reason. Setting this object to switchoverNow (3) causes the device to switchover immediately to the new software which was downloaded to the shadow flash area before and restart the system. initSwitchoverDelayed(4) causes a delayed switchover. deprecated
1.3.6.1.4.1.231.7.2.7.2.1.14	sysFirmwareVersion	DisplayString	RO	Version number of the systems firmware.
1.3.6.1.4.1.231.7.2.7.2.1.15	sysHlbSymbolSubInfo	DisplayString	RO	Contains an URL to detailed symbol information in addition to the symbol information contained in the common MIB object deviceSymbolInfo.
1.3.6.1.4.1.231.7.2.7.2.1.16	sysHlbBranding	DisplayString	RO	Contains the branding string of the device.
1.3.6.1.4.1.231.7.2.7.3	monitoringGrouphlb20			Monitoring Group MIB
1.3.6.1.4.1.231.7.2.7.3.1	numberOfIdleMonTableEntries	INTEGER	RO	Contains the number of idle/load monitoring table entries.
1.3.6.1.4.1.231.7.2.7.3.2	hlb20IdleMonTable	SEQUENCE OF Hlb20IdleMonTableEntry		This table contains information about the system idle/load time (scanned every 5 minutes) for the last 24 hours.
1.3.6.1.4.1.231.7.2.7.3.2.1	hlb20IdleMonTableEntry	Hlb20IdleMonTableEntry		The idle/load monitoring table entries.
1.3.6.1.4.1.231.7.2.7.3.2.1.1	idleIndex	INTEGER	RO	Identification of an table entry.
1.3.6.1.4.1.231.7.2.7.3.2.1.2	idleValue	INTEGER	RO	The load level value.
1.3.6.1.4.1.231.7.2.7.3.3	numberOfIdleLatestTableEntries	INTEGER	RO	Contains the number of precision idle/load monitoring table entries.

Object-ID	Object name	Syntax	Access	Description
1.3.6.1.4.1.231.7.2.7.3.4	hlb20IdleLatestTable	SEQUENCE OF Hlb20IdleLatestTableEntry		This table contains information about the system idle/load time (scanned every minute) for the last 10 minutes.
1.3.6.1.4.1.231.7.2.7.3.4.1	hlb20IdleLatestTableEntry	Hlb20IdleLatestTableEntry		The precision idle/load monitoring table for the ten latest values.
1.3.6.1.4.1.231.7.2.7.3.4.1.1	idleLatestIndex	INTEGER	RO	Identification of an table entry.
1.3.6.1.4.1.231.7.2.7.3.4.1.2	idleLatestValue	INTEGER	RO	Identification of an table value.
1.3.6.1.4.1.231.7.2.7.3.5	numberOfIdleMonYellowAlarms	INTEGER	RO	Contains the number of yellow load monitoring alarms.
1.3.6.1.4.1.231.7.2.7.3.6	numberOfIdleMonRedAlarms	INTEGER	RO	Contains the number of red load monitoring alarms.
1.3.6.1.4.1.231.7.2.7.3.7	flagIdleMonYellowAlarm	INTEGER	RO	1, if load monitoring is on yellow alert. 0 otherwise
1.3.6.1.4.1.231.7.2.7.3.8	flagIdleMonRedAlarm	INTEGER	RO	1, if load monitoring is on red alert. 0 otherwise
1.3.6.1.4.1.231.7.2.7.3.9	thresholdIdleMonYellowAlarm	INTEGER (0..100)	RW	idle threshold value for generation of yellow alert.
1.3.6.1.4.1.231.7.2.7.3.10	thresholdIdleMonRedAlarm	INTEGER (0..100)	RW	idle threshold value for generation of red alert.
1.3.6.1.4.1.231.7.2.7.3.11	idleMonHighWaterMark	INTEGER	RO	contains the load peak level of the device.
1.3.6.1.4.1.231.7.2.7.3.12	idleMonLastValue	INTEGER	RO	contains the latest load monitoring value.
1.3.6.1.4.1.231.7.2.7.3.13	numberOfFreeMemBuffersTableEntries	INTEGER	RO	Contains the number of memory buffers table entries. Item available in newer rel. 1.1 devices deprecated
1.3.6.1.4.1.231.7.2.7.3.14	freeMemBuffersTable	SEQUENCE OF FreeMemBuffersTableEntry		This table contains information about the number of free memory buffers for the different buffer sizes. Table available in newer rel. 1.1 devices deprecated
1.3.6.1.4.1.231.7.2.7.3.14.1	freeMemBuffersTableEntry	FreeMemBuffersTableEntry		The free memory buffers of this device. deprecated

Object-ID	Object name	Syntax	Access	Description
1.3.6.1.4.1.231.7.2.7.3.14.1.1	bufferIndex	INTEGER	RO	Identification of an table entry. deprecated
1.3.6.1.4.1.231.7.2.7.3.14.1.2	bufferType	DisplayString	RO	The type/size of this buffer. deprecated
1.3.6.1.4.1.231.7.2.7.3.14.1.3	numOfFreeBuffers	INTEGER	RO	The number of free buffers of this type. deprecated
1.3.6.1.4.1.231.7.2.7.3.15	loadBalanceMeasureControl	INTEGER	RW	Measuring the load balance of the processes of the device is controlled by this object. Setting the object to active (2) starts the measuring, inactive (1) stops it. Item available in newer rel. 1.1 devices
1.3.6.1.4.1.231.7.2.7.3.16	numberOfLoadBalanceTableEntries	INTEGER	RO	Contains the number of load balance measurement entries. deprecated
1.3.6.1.4.1.231.7.2.7.3.17	loadBalanceTable	SEQUENCE OF LoadBalanceTableEntry		This table contains detailed information about load balance of the different processes of the device. deprecated
1.3.6.1.4.1.231.7.2.7.3.17.1	loadBalanceTableEntry	LoadBalanceTableEntry		The load balance for the processes of this device. deprecated
1.3.6.1.4.1.231.7.2.7.3.17.1.1	loadBalanceIndex	INTEGER	RO	Identification of an table entry. deprecated
1.3.6.1.4.1.231.7.2.7.3.17.1.2	processDescription	DisplayString	RO	Textual description of the process. deprecated
1.3.6.1.4.1.231.7.2.7.3.17.1.3	loadProportionValue	DisplayString	RO	Load proportion for every process. deprecated
1.3.6.1.4.1.231.7.2.7.4	statisticsGrouphlb20			Statistics Group MIB
1.3.6.1.4.1.231.7.2.7.4.1	globalVcapiClientStatGroup			global statistic data: vCAPI client
1.3.6.1.4.1.231.7.2.7.4.1.1	statVcapiInstalledClients	INTEGER	RO	Contains the number of vCAPI Clients installed deprecated

Object-ID	Object name	Syntax	Access	Description
1.3.6.1.4.1.231.7.2.7.4.1.2	statVcapiLoggedInClients	INTEGER	RO	Contains the total number of vCAPI Client logins since the last system restart. deprecated
1.3.6.1.4.1.231.7.2.7.4.1.3	statVcapiActiveClients	INTEGER	RO	Contains the number of active vCAPI clients (or b-channels if channel bundling is configured). deprecated
1.3.6.1.4.1.231.7.2.7.4.2	globalH323ClientStatGroup			global statistic data: H323 client
1.3.6.1.4.1.231.7.2.7.4.2.1	statH323InstalledClients	INTEGER	RO	Contains the number of H323 Clients installed (which means they are configured in the customer database) deprecated
1.3.6.1.4.1.231.7.2.7.4.2.2	statH323ActiveClients	INTEGER	RO	Contains the number of H323 Clients in an active connection state. deprecated
1.3.6.1.4.1.231.7.2.7.4.3	globalTfaClientStatGroup			global statistic data: TFA client
1.3.6.1.4.1.231.7.2.7.4.3.1	statTfaInstalledClients	INTEGER	RO	Contains the number of TFA Clients installed (which means they are configured in the customer database). deprecated
1.3.6.1.4.1.231.7.2.7.4.3.2	statTfaActiveClients	INTEGER	RO	Contains the number of TFA Clients in active connection state. deprecated
1.3.6.1.4.1.231.7.2.7.4.3.3	statTfaRegistratedClients	INTEGER	RO	Contains the number of TFA Clients that have registered themselves to their hg3550 since the last system restart. deprecated
1.3.6.1.4.1.231.7.2.7.4.3.4	statTfaClientLogonSuccess	INTEGER	RO	Contains the number of successful TFA Clients logons since the last system restart. deprecated

Object-ID	Object name	Syntax	Access	Description
1.3.6.1.4.1.231.7.2.7.4.3.5	statTfaClientLogonFailed	INTEGER	RO	Contains the number of failed TFA Clients logons since the last system restart. deprecated
1.3.6.1.4.1.231.7.2.7.4.4	globalVoiceClientCallStatGroup			global statistic call data for H323 and TFA clients
1.3.6.1.4.1.231.7.2.7.4.4.1	statOutgoingRtp	INTEGER	RO	Contains the number of outgoing RTP packets (H323 + TFA Clients).
1.3.6.1.4.1.231.7.2.7.4.4.2	statOutgoingLostRtp	INTEGER	RO	Contains the number of outgoing RTP packets lost (H323 + TFA Clients).
1.3.6.1.4.1.231.7.2.7.4.4.3	statIncomingRtp	INTEGER	RO	Contains the number of incoming RTP packets (H323 + TFA Clients).
1.3.6.1.4.1.231.7.2.7.4.4.4	statIncomingLostRtp	INTEGER	RO	Contains the number of incoming RTP packets lost (H323 + TFA Clients).
1.3.6.1.4.1.231.7.2.7.4.4.5	statTotalBytesSentRtp	INTEGER	RO	Contains the number of bytes sent (RTP).
1.3.6.1.4.1.231.7.2.7.4.4.6	statTotalBytesRecvRtp	INTEGER	RO	Contains the number of bytes received (RTP).
1.3.6.1.4.1.231.7.2.7.4.5	indivVoiceClientCallStatBuffer			individual statistic data: H323 client
1.3.6.1.4.1.231.7.2.7.4.5.1	numOfClientStatIndTableEntries	INTEGER	RO	Contains the number of individual H323 client statistics table entries.
1.3.6.1.4.1.231.7.2.7.4.5.2	hlb20ClientStatIndTable	SEQUENCE OF Hlb20ClientStatIndTableEntry		This table contains individual statistic information for every H323 client. Usually, this table is empty. It is designed for expert level debugging only.
1.3.6.1.4.1.231.7.2.7.4.5.2.1	hlb20ClientStatIndTableEntry	Hlb20ClientStatIndTableEntry		The individual H323 client statistic information table entries.
1.3.6.1.4.1.231.7.2.7.4.5.2.1.1	statIndVoiceCliIndex	Hlb20ClientStatIndSnmpIndex	RO	Identification of an table entry enabled by this index.
1.3.6.1.4.1.231.7.2.7.4.5.2.1.2	statIndVoiceCliCallId	OCTET STRING (SIZE (1..21))	RO	Contains the call ID (canonial name) of the call target.
1.3.6.1.4.1.231.7.2.7.4.5.2.1.3	statIndVoiceCliLocalIpAddress	TransportLabel	RO	Contains the IP address of the local endpoint.

Object-ID	Object name	Syntax	Access	Description
1.3.6.1.4.1.231.7.2.7.4.5.1.2.1.4	stat2ndVoiceCliTimeBegin	DateAndTime	RO	Contains the time stamp for the start of the call.
1.3.6.1.4.1.231.7.2.7.4.5.1.2.1.5	stat2ndVoiceCliTimeEnd	DateAndTime	RO	Contains the time stamp for the end of the call.
1.3.6.1.4.1.231.7.2.7.4.5.1.2.1.6	stat2ndVoiceCliEncoder	INTEGER	RO	Contains encoder information.
1.3.6.1.4.1.231.7.2.7.4.5.1.2.1.7	stat2ndVoiceCliDecoder	INTEGER	RO	Contains decoder information.
1.3.6.1.4.1.231.7.2.7.4.5.1.2.1.8	stat2ndVoiceCliOutgoingRtp	INTEGER	RO	Contains the number of outgoing RTP packets.
1.3.6.1.4.1.231.7.2.7.4.5.1.2.1.9	stat2ndVoiceCliOutgoingLostRtp	INTEGER	RO	Contains the number of outgoing RTP packets lost.
1.3.6.1.4.1.231.7.2.7.4.5.1.2.1.10	stat2ndVoiceCliIncomingRtp	INTEGER	RO	Contains the number of incoming RTP packets.
1.3.6.1.4.1.231.7.2.7.4.5.1.2.1.11	stat2ndVoiceCliIncomingLostRtp	INTEGER	RO	Contains the number of incoming RTP packets lost.
1.3.6.1.4.1.231.7.2.7.4.5.1.2.1.12	stat2ndVoiceCliTotalBytesSentRtp	INTEGER	RO	Contains the number of bytes sent.
1.3.6.1.4.1.231.7.2.7.4.5.1.2.1.13	stat2ndVoiceCliTotalBytesRecvRtp	INTEGER	RO	Contains the number of bytes received.
1.3.6.1.4.1.231.7.2.7.4.5.1.2.1.14	stat2ndVoiceCliDelay	INTEGER	RO	Contains the average network delay.
1.3.6.1.4.1.231.7.2.7.4.5.1.2.1.15	stat2ndVoiceCliJitter	INTEGER	RO	Contains the average jitter.
1.3.6.1.4.1.231.7.2.7.4.5.1.2.1.16	stat2ndVoiceConnectionCondId	OCTET STRING (SIZE (1..21))	RO	Contains the conference ID (canonial name) which is unique for all parties involved in the call or conference.
1.3.6.1.4.1.231.7.2.7.4.5.1.2.1.17	stat2ndVoiceConnectionQuality	INTEGER	RO	The overall quality of the call or call - section. - normal(1) - warning(2) - minor(3) - major(4) - critical(5)
1.3.6.1.4.1.231.7.2.7.4.5.1.2.1.18	stat2ndVoiceCliRemoteIpAddress	TransportLabel	RO	Contains the IP address of the remote endpoint.
1.3.6.1.4.1.231.7.2.7.4.5.3	voIPQualityNotificationCounter	INTEGER	RO	Total number of VoIP quality traps that were sent since agent start.
1.3.6.1.4.1.231.7.2.7.4.6	audioStreamStatGroup			individual statistic data: H323 client

Object-ID	Object name	Syntax	Access	Description
1.3.6.1.4.1.231.7.2.7.4.11	statAudioStreamSccRxErrors	INTEGER	RO	Contains the number of errors (buffer underruns) in the communication between the CPU and the receiving DSP's. (Object not available in hg3550 / Xpress @LAN 1.0) deprecated
1.3.6.1.4.1.231.7.2.7.4.12	statAudioStreamSccTxErrors	INTEGER	RO	Contains the number of errors (buffer overflows) in the communication between the CPU and the sending DSP's. (Object not available in HG1500 / Xpress @LAN 1.0)
1.3.6.1.4.1.231.7.2.7.5	sendAlarmWithValues	TRAP		If an error occurs, there will be checked if the errorClass is configured to trigger a immediate signaling. If so, a trap will be send to the management station containing the information shown above.
1.3.6.1.4.1.231.7.2.7.6	fileOverflowError	TRAP		Inform the manager that the trap history table got too big. Unless the size of the table is reduced by the manager (by resetting numberOfTrapHistoryEntries), the oldest trap informations will be overridden from now on.
1.3.6.1.4.1.231.7.2.7.7	allServeGrouphlb20			HiPath AllServe Group MIB
1.3.6.1.4.1.231.7.2.7.7.1	registrationState	INTEGER	RO	Contains information about the HiPath AllServe registration state. - registered(1) - notRegistered(2)
1.3.6.1.4.1.231.7.2.7.7.2	numberOfCallAddrTableEntries	INTEGER	RO	Contains the number of call address table entries.
1.3.6.1.4.1.231.7.2.7.7.3	numberOfCallAddrCacheEntries	INTEGER	RO	Contains the number of call address cache entries.
1.3.6.1.4.1.231.7.2.7.7.4	numberOfNodeIpTableEntries	INTEGER	RO	Contains the number of node IP table entries.
1.3.6.1.4.1.231.7.2.7.7.5	hlb20NodeIpTable	SEQUENCE OF Hlb20NodeIpTableEntry		This table contains information about the assignment of IP addresses to HiPath AllServe nodes.

Object-ID	Object name	Syntax	Access	Description
1.3.6.1.4.1.231.7.2.7.7.5.1	hlb20NodeIpTableEntry	Hlb20NodeIpTableEntry		The node IP table entries.
1.3.6.1.4.1.231.7.2.7.7.5.1.1	nodeIndex	INTEGER	RO	Identification of an table entry, identical to node id.
1.3.6.1.4.1.231.7.2.7.7.5.1.2	nodeIpNumOfIpAddr	INTEGER	RO	Number of IP address entries for this node.
1.3.6.1.4.1.231.7.2.7.7.5.1.3	nodeIpAddresses	DisplayString	RO	Assigned IP addresses for this node.
1.3.6.1.4.1.231.7.2.7.7.6	numberOfNuPortDataTableEntries	INTEGER	RO	Contains the number of networking unit port data table entries.
1.3.6.1.4.1.231.7.2.7.7.7	hlb20NuPortDataTable	SEQUENCE OF Hlb20NuPortDataTableEntry		This table contains information about the networking unit port data of this device.
1.3.6.1.4.1.231.7.2.7.7.7.1	hlb20NuPortDataTableEntry	Hlb20NuPortDataTableEntry		The networking unit port data table entries.
1.3.6.1.4.1.231.7.2.7.7.7.1.1	nuPortDataIndex	INTEGER	RO	Identification of an table entry.
1.3.6.1.4.1.231.7.2.7.7.7.1.2	nuCardPort	INTEGER	RO	The lw_port to the system.
1.3.6.1.4.1.231.7.2.7.7.7.1.3	nuPortDataProtocol	INTEGER	RO	The networking protocol.
1.3.6.1.4.1.231.7.2.7.7.7.1.4	nuPortDataNumOfBchn	INTEGER	RO	The amount of B-channels to the system.
1.3.6.1.4.1.231.7.2.7.7.7.1.5	nuPortDataActiveBchn	INTEGER	RO	The number of active B-channels.
1.3.6.1.4.1.231.7.2.7.7.8	numberOfNuTransDataTableEntries	INTEGER	RO	Contains the number of networking unit transaction data table entries.
1.3.6.1.4.1.231.7.2.7.7.9	hlb20NuTransDataTable	SEQUENCE OF Hlb20NuTransDataTableEntry		This table contains information about the networking unit transaction data of this device.
1.3.6.1.4.1.231.7.2.7.7.9.1	hlb20NuTransDataTableEntry	Hlb20NuTransDataTableEntry		The networking unit transaction data table entries.
1.3.6.1.4.1.231.7.2.7.7.9.1.1	nuTransDataIndex	INTEGER	RO	Identification of an table entry.
1.3.6.1.4.1.231.7.2.7.7.9.1.2	nuTransStepState	INTEGER	RO	The step table state.
1.3.6.1.4.1.231.7.2.7.7.9.1.3	nuTransCallDirection	INTEGER	RO	The call direction - incoming(1) = to mainboard - outgoing(2) = from mainboard
1.3.6.1.4.1.231.7.2.7.7.9.1.4	nuTransCallRefSys	INTEGER	RO	The call reference to the mainboard.

Object-ID	Object name	Syntax	Access	Description
1.3.6.1.4.1.231.7.2.7.7.9.1.5	vuTransBchnIndex	INTEGER	RO	The channel index in the TSA message.
1.3.6.1.4.1.231.7.2.7.7.9.1.6	vuTransTimeSlot	INTEGER	RO	The timeslot on the PCM / IOM interface.
1.3.6.1.4.1.231.7.2.7.7.9.1.7	vuTransPartnerIpAddr	IpAddress	RO	The IP address of the HiPath AllServe partner node.
1.3.6.1.4.1.231.7.2.7.7.9.1.8	vuTransCallRefIp	INTEGER	RO	The call reference to the IP network.
1.3.6.1.4.1.231.7.2.7.8	ethernetStatGrouphlb20			Ethernet Statistics Group MIB
1.3.6.1.4.1.231.7.2.7.8.1	ethernetStatState	INTEGER	RW	Initialize the ethernet statistics data to zero by setting value 2. - counting(1) - reset(2)
1.3.6.1.4.1.231.7.2.7.8.2	goodFramesTransmitted	INTEGER	RO	Successfully sent ethernet frames
1.3.6.1.4.1.231.7.2.7.8.3	goodFramesReceived	INTEGER	RO	Correct received ethernet frames
1.3.6.1.4.1.231.7.2.7.8.4	sendRetries	INTEGER	RO	successful ethernet send retries
1.3.6.1.4.1.231.7.2.7.8.5	receiveCollisions	INTEGER	RO	Collisions on Ethernet
1.3.6.1.4.1.231.7.2.7.8.6	sendRetryError	INTEGER	RO	16 failed send attempts
1.3.6.1.4.1.231.7.2.7.8.7	macEngineDefer	INTEGER	RO	MAC-Engine had to defer
1.3.6.1.4.1.231.7.2.7.8.8	excessiveDeferral	INTEGER	RO	excessive deferral
1.3.6.1.4.1.231.7.2.7.8.9	lossOfCarrier	INTEGER	RO	loss of carrier
1.3.6.1.4.1.231.7.2.7.8.10	lateCollision	INTEGER	RO	late Collision
1.3.6.1.4.1.231.7.2.7.8.11	xBufferError	INTEGER	RO	transmit buffer - fatal error
1.3.6.1.4.1.231.7.2.7.8.12	underflowError	INTEGER	RO	underflow error - hardware error
1.3.6.1.4.1.231.7.2.7.8.13	checksumError	INTEGER	RO	receive checksum error
1.3.6.1.4.1.231.7.2.7.8.14	framingError	INTEGER	RO	receive framing error
1.3.6.1.4.1.231.7.2.7.8.15	missedFrames	INTEGER	RO	missed frames
1.3.6.1.4.1.231.7.2.7.8.16	runtPackets	INTEGER	RO	runt packets
1.3.6.1.4.1.231.7.2.7.8.17	frameTooShort	INTEGER	RO	Received frame too short
1.3.6.1.4.1.231.7.2.7.8.18	frameTooLong	INTEGER	RO	Received frame too long
1.3.6.1.4.1.231.7.2.7.8.19	bufferLimitReached	INTEGER	RO	Low Buffer limit reached.

Object-ID	Object name	Syntax	Access	Description
1.3.6.1.4.1.231.7.2.7.8.20	rcvBufferError	INTEGER	RO	receive buffer - fatal error
1.3.6.1.4.1.231.7.2.7.8.21	overflowError	INTEGER	RO	overflow error - hardware error
1.3.6.1.4.1.231.7.2.7.8.22	collisionErrorInt	INTEGER	RO	transceiver test failed - hardware error
1.3.6.1.4.1.231.7.2.7.8.23	memoryErrorInt	INTEGER	RO	system bus timeout - hardware error
1.3.6.1.4.1.231.7.2.7.8.24	excessiveInts	INTEGER	RO	excessive interrupt occurrence
1.3.6.1.4.1.231.7.2.7.8.25	linkChanged	INTEGER	RO	link changed
1.3.6.1.4.1.231.7.2.7.8.26	linkMode	INTEGER	RO	Operational mode of the ethernet link. - halfDuplex10BaseT(1) - halfDuplex100BaseT(3) - fullDuplex10BaseT(2) - fullDuplex100BaseT(4) - auto(0)
1.3.6.1.4.1.231.7.2.7.8.27	good8021pFramesReceived	INTEGER	RO	The number of correct 802.1p frames received.
1.3.6.1.4.1.231.7.2.7.8.28	babblingReceiveInts	INTEGER	RO	The number of frames received with a length that is greater than the maximum allowed ethernet frame size (1518 or 1522 bytes).
1.3.6.1.4.1.231.7.2.7.8.29	babblingTransmitInts	INTEGER	RO	The number of frames transmitted with a length that is greater than the maximum allowed ethernet frame size (1518 or 1522 bytes).
1.3.6.1.4.1.231.7.2.7.8.30	unexpectedInts	INTEGER	RO	The number of unexpected interrupt events that have occur red. The presence of such unexpected interrupts may indicate a major problem on the device.
1.3.6.1.4.1.231.7.2.7.9	qosStatGrouphlb20			Quality Of Service Statistics Group MIB
1.3.6.1.4.1.231.7.2.7.9.1	numOfQosStatTableEntries	INTEGER	RW	Contains the number of entries in the quality of service (qos) statistics table. The only valid write value is 0, which resets all qos statistic counters.

Object-ID	Object name	Syntax	Access	Description
1.3.6.1.4.1.231.7.2.7.9.2	qosStatTable	SEQUENCE OF QosStatTableEntry		This table contains statistic information for quality of service (QOS) mechanisms.
1.3.6.1.4.1.231.7.2.7.9.2.1	qosStatTableEntry	QosStatTableEntry		The QOS statistic information table entries.
1.3.6.1.4.1.231.7.2.7.9.2.1.1	qsIndex	INTEGER	RO	Identification of an table entry enabled by this index.
1.3.6.1.4.1.231.7.2.7.9.2.1.2	interface	DisplayString	RO	The interface for which the QOS statistic data is collected.
1.3.6.1.4.1.231.7.2.7.9.2.1.3	remarkedFrames	INTEGER	RO	The number of remarked frames.
1.3.6.1.4.1.231.7.2.7.9.2.1.4	droppedPackets	DisplayString	RO	The number of dropped packets for each queue.
1.3.6.1.4.1.231.7.2.7.10	bChannelStatGroup	hlb20		B-Channel Statistics Group MIB
1.3.6.1.4.1.231.7.2.7.10.1	numOfBChannelStatTableEntries	INTEGER	RW	Contains the number of entries in the b-channel statistics table. The only valid write value is 0, which resets all b-channel counters.
1.3.6.1.4.1.231.7.2.7.10.2	bChannelStatTable	SEQUENCE OF BChannelStatTableEntry		This table contains statistic information of B-Channels.
1.3.6.1.4.1.231.7.2.7.10.2.1	bChannelStatTableEntry	BChannelStatTableEntry		The B-Channel statistic information table entries.
1.3.6.1.4.1.231.7.2.7.10.2.1.1	bChannelStatIndex	INTEGER	RO	Identification of an table entry enabled by this index.
1.3.6.1.4.1.231.7.2.7.10.2.1.2	bChannelIdentifier	DisplayString (SIZE (0..255))	RO	The B-Channel identifier. 'Total' is the sum of all B-Channels.
1.3.6.1.4.1.231.7.2.7.10.2.1.3	frmLenViolation	INTEGER	RO	Number of frames received with invalid length.
1.3.6.1.4.1.231.7.2.7.10.2.1.4	octetAligned	INTEGER	RO	Number of frames with an invalid number of bits.
1.3.6.1.4.1.231.7.2.7.10.2.1.5	abortSequence	INTEGER	RO	Number of times the HDLC abort sequence was detected.
1.3.6.1.4.1.231.7.2.7.10.2.1.6	crcError	INTEGER	RO	Number of frames received with CRC checksum errors.
1.3.6.1.4.1.231.7.2.7.10.2.1.7	rcvBusyInt	INTEGER	RO	Number of frames received when no receive buffer descriptor was available.

Object-ID	Object name	Syntax	Access	Description
1.3.6.1.4.1.231.7.2.7.10.2.1.9	qmcMrfInt	INTEGER	RO	Early indication for the number of frame length violations.
1.3.6.1.4.1.231.7.2.7.10.2.1.9	qmcXmInt	INTEGER	RO	Number of qmc transmitter underruns.
1.3.6.1.4.1.231.7.2.7.10.2.1.10	qmcIqov	INTEGER	RO	Number of overruns in the qmx interrupt ringbuffer.
1.3.6.1.4.1.231.7.2.7.10.2.1.31	qmcXunGov	INTEGER	RO	This critical error leads to a reset. It occurs when there's an buffer overrun in the internal qmc fifo buffers.
1.3.6.1.4.1.231.7.2.7.10.3	numOfDspChannelsExisting	INTEGER	RO	Contains the number of DSP channels physically existing.
1.3.6.1.4.1.231.7.2.7.10.4	numOfDspChannelsAvailable	INTEGER	RO	Contains the number of DSP channels available.
1.3.6.1.4.1.231.7.2.7.10.5	numOfDspChannelsInUse	INTEGER	RO	Contains the number of DSP channels actually used.
1.3.6.1.4.1.231.7.2.7.11	notificationGrouphlb20			Notification Group MIB containing trap specifications
1.3.6.1.4.1.231.7.2.7.11.1	sendVoIPQualityNotification	TRAP		This notification will be sent when the latest voice over IP connection had quality problems.
1.3.6.1.4.1.231.7.2.7.11.2	sendIpPhoneTableNotification	TRAP		This notification will be sent whenever the errorState of an IP phone table entry changes or when the configuration of IP phones is changed.
1.3.6.1.4.1.231.7.2.7.12	ipPhoneGrouphlb20			IP Phone Group MIB
1.3.6.1.4.1.231.7.2.7.12.1	numOfIpPhoneTableEntries	INTEGER	RO	Contains the number of entries in the IP Phone table.
1.3.6.1.4.1.231.7.2.7.12.2	ipPhoneTable	SEQUENCE OF IpPhoneTableEntry		This table contains information on all configured OptiPoints and OptiCients, but not standard H.323 phones.
1.3.6.1.4.1.231.7.2.7.12.2.1	ipPhoneTableEntry	IpPhoneTableEntry		The IP Phone table entries.
1.3.6.1.4.1.231.7.2.7.12.2.1.1	ipPhoneIndex	INTEGER	RO	Identification of an table entry enabled by this index.
1.3.6.1.4.1.231.7.2.7.12.2.1.2	subscriberNumber	DisplayString	RO	Subscriber call number which is assigned to the phone.

Object-ID	Object name	Syntax	Access	Description
1.3.6.1.4.1.231.7.2.7.12.2.1.3	ipAddress	IpAddress	RO	Contains the IP address of the phone.
1.3.6.1.4.1.231.7.2.7.12.2.1.4	operationalState	INTEGER	RO	Contains information about the operational state of the phone. - installed(1) means that the phone has been configured in hg3550, but it is not operational. - registered(2) means that the phone is operational. - active(3) means that the phone is actually in use.
1.3.6.1.4.1.231.7.2.7.12.2.1.5	errorState	INTEGER	RO	Contains information about the error state of the phone. - normal(1) - warning(2) - minor(3) - major(4) - critical(5) - unknown(6)
1.3.6.1.4.1.231.7.2.7.12.3	indexOfLastIpPhoneNotification	INTEGER	RO	Contains the index of the last notification trap that indicated configurational or status changes in the IP phone table.
1.3.6.1.4.1.231.7.2.7.12.4	typeOfLastIpPhoneNotification	INTEGER	RO	Contains the type of the last notification trap that indicated configurational or status changes in the IP phone table.
1.3.6.1.4.1.231.7.2.7.12.5	subscriberNoOfLastIpPhoneNotification	DisplayString	RO	The subscriber number of the IP phone involved.
1.3.6.1.4.1.231.7.2.7.12.6	ipAddressOfLastIpPhoneNotification	IpAddress	RO	Contains the IP address of the IP phone involved. If the IP address is 0.0.0.0, all phones may be involved

Object-ID	Object name	Syntax	Access	Description
1.3.6.1.4.1.231.7.2.7.12.7	errorStateOfLastIpPhoneNotification	INTEGER	RO	Contains information about the error state of the phone involved. - normal(1) - warning(2) - minor(3) - major(4) - critical(5) - unknown(6)
1.3.6.1.4.1.231.7.2.7.13	rg2500			RG2500 MIB
1.3.6.1.4.1.231.7.2.7.13.1	gwPlatformMib			The Platform MIB for the company's VoIP Gateway. See ar2500_platform.my
1.3.6.1.4.1.231.7.2.7.13.1.1	gwPlatformMibObjects			
1.3.6.1.4.1.231.7.2.7.13.1.1.1	gwPlatformHardwareGroup			
1.3.6.1.4.1.231.7.2.7.13.1.1.1.1	gwPlatformHwConfigGroup			The Hardware Configuration MIB
1.3.6.1.4.1.231.7.2.7.13.1.1.1.2	gwPlatformHwDspModuleCount	INTEGER (0..12)	RO	The Number of DSP modules fitted.
1.3.6.1.4.1.231.7.2.7.13.1.1.1.3	gwPlatformHwCpuType	DisplayString	RO	The processor type.
1.3.6.1.4.1.231.7.2.7.13.1.1.1.4	gwPlatformHwCpuSpeed	INTEGER (0..1024)	RO	The CPU speed in MHz.
1.3.6.1.4.1.231.7.2.7.13.1.1.1.5	gwPlatformHwFlashMemory	INTEGER (0..1024)	RO	The flash memory size in MB (1024x1024 bytes).
1.3.6.1.4.1.231.7.2.7.13.1.1.1.6	gwPlatformHwDram	INTEGER (0..1024)	RO	The DRAM size in MB (1024x1024 bytes).
1.3.6.1.4.1.231.7.2.7.13.1.1.1.7	gwPlatformHwDspSlotCount	INTEGER (0..12)	RO	The number of DSP slots.
1.3.6.1.4.1.231.7.2.7.13.1.1.1.10	gwPlatformHwMacAddress	OCTET STRING (SIZE(6))	RO	The MAC address.
1.3.6.1.4.1.231.7.2.7.13.1.1.1.11	gwPlatformHwBootline	DisplayString	RO	The bootline.
1.3.6.1.4.1.231.7.2.7.13.1.1.1.12	gwPlatformHwSystemSerialNumber	DisplayString	RO	The system serial number.
1.3.6.1.4.1.231.7.2.7.13.1.1.1.13	gwPlatformHwMotherboardVersion	DisplayString	RO	The motherboard version.
1.3.6.1.4.1.231.7.2.7.13.1.1.1.14	gwPlatformHwPartListVersion	DisplayString	RO	The part-list version.
1.3.6.1.4.1.231.7.2.7.13.1.1.1.15	gwPlatformHwBootromVersion	DisplayString	RO	The boot ROM version.

Object-ID	Object name	Syntax	Access	Description
1.3.6.1.4.1.231.7.2.7.13	gwPlatformHwDspModuleTable	SEQUENCE OF GwPlatformHwDspModuleEntry		Table containing types of DSP modules installed.
1.3.6.1.4.1.231.7.2.7.13	gwPlatformHwDspModuleEntry	GwPlatformHwDspModuleEntry		An entry in the DSP Module Table.
1.3.6.1.4.1.231.7.2.7.13	gwPlatformHwDspModuleIndex	INTEGER (1..12)	RO	The index into the dsp module table.
1.3.6.1.4.1.231.7.2.7.13	gwPlatformHwDspModuleType	DisplayString	RO	The type indicator of the DSP module.
1.3.6.1.4.1.231.7.2.7.13	gwPlatformHwDspModuleDescription	DisplayString	RO	The descriptive name of the dsp module, e.g. The written part name, and type of dsp, and size of RAM on the module.
1.3.6.1.4.1.231.7.2.7.13	gwPlatformHwResourceGroup			The Hardware Resources Group
1.3.6.1.4.1.231.7.2.7.13	gwPlatformHwDramFree	Unsigned32	RO	The DRAM free in KBytes, sysMemPart+safeMemPart
1.3.6.1.4.1.231.7.2.7.13	gwPlatformHwFlashFree	Unsigned32	RO	The Flash free, in KBytes.
1.3.6.1.4.1.231.7.2.7.13	gwPlatformSwConfigGroup			The Software Configuration
1.3.6.1.4.1.231.7.2.7.13	gwPlatformSwBuild	DisplayString	RO	The reported build identification of the loaded software.
1.3.6.1.4.1.231.7.2.7.13	gwManagementMib			The Management MIB for the company's RG 2500 Communication Gateway. See ar2500_management.my
1.3.6.1.4.1.231.7.2.7.13	gwMIBManagementMibObjects			
1.3.6.1.4.1.231.7.2.7.13	gwMIBManagementMgmtGroup			The Management Group
1.3.6.1.4.1.231.7.2.7.13	gwMIBManagementRouterPropertiesGroupTable	SEQUENCE OF GwManagementRouterPropertiesGroupEntry		The group of gateway property settings.
1.3.6.1.4.1.231.7.2.7.13	gwMIBManagementRouterPropertiesGroupEntry	GwManagementRouterPropertiesGroupEntry		Properties (Group Entry) in the table of gateway properties settings.
1.3.6.1.4.1.231.7.2.7.13	gwMIBManagementRouterPropertiesGroupIndex	RO	Configuration Group Index	The index into the table of gateway properties settings.
1.3.6.1.4.1.231.7.2.7.13	gwMIBManagementRouterPropertiesSystemName	DisplayString (SIZE(0..20)	RW	Allows the name of the gateway to be set.

Object-ID	Object name	Syntax	Access	Description
1.3.6.1.4.1.231.7.2.7.13.2.1.1.1.9	gwManagementRouterProperties	DisplayString (SIZE(0..20)	RW	Allows the location of the gateway to be set.
1.3.6.1.4.1.231.7.2.7.13.2.1.1.1.4	gwManagementRouterProperties	DisplayString (SIZE(0..20))	RO	IP address
1.3.6.1.4.1.231.7.2.7.13.2.1.1.1.5	gwManagementRouterProperties	DisplayString (SIZE(0..20))	RO	Subnet mask
1.3.6.1.4.1.231.7.2.7.13.2.1.8	gwManagementMgmtConfigGroup			The Management Configuration Group
1.3.6.1.4.1.231.7.2.7.13.2.1.8.14	gwManagementCommConfigTable	SEQUENCE OF GwManagementCommConfigEntry		The group of management SNMP settings.
1.3.6.1.4.1.231.7.2.7.13.2.1.8.14.1	gwManagementCommConfigEntry	GwManagementCommConfigEntry		The entry (row type) in the table of management SNMP configuration settings.
1.3.6.1.4.1.231.7.2.7.13.2.1.8.14.1.1	gwManagementCommConfigIndex	RCMgmtConfigIndex		The index for the table of management SNMP configuration settings.
1.3.6.1.4.1.231.7.2.7.13.2.1.8.14.1.2	gwManagementCommConfigSetting	DisplayString	RC	This column holds the value which must be interpreted according to the type indicated by the preceding column.
1.3.6.1.4.1.231.7.2.7.13.2.1.8.14.1.3	gwManagementCommConfigIpAddr	DisplayString	RC	The part of the setting which holds the IP-Address.
1.3.6.1.4.1.231.7.2.7.13.2.1.8.14.1.4	gwManagementCommConfigSettingType	RCMgmtConfigSnmpSettingType	RC	Type of SNMP setting the data held in this row of the table. - readCommunity(1) - writeCommunity(2) - trapReceiver(3)
1.3.6.1.4.1.231.7.2.7.13.2.1.8.14.1.5	gwManagementCommConfigRowStatus	RowStatus	RC	The row status for the table of management SNMP configuration settings.
1.3.6.1.4.1.231.7.2.7.13.2.1.6	gwManagementStaticRouteConfigTable	SEQUENCE OF GwManagementStaticRouteConfigEntry		The table of StaticRoute Configurations. This table is used to configure the ipRouteTable at system start.
1.3.6.1.4.1.231.7.2.7.13.2.1.6.1	gwManagementStaticRouteConfigEntry	GwManagementStaticRouteConfigEntry		The entry (row type) in the table of StaticRoute Configurations.
1.3.6.1.4.1.231.7.2.7.13.2.1.6.1.1	gwManagementStaticRouteConfigIndex	RCStaticRouteConfigIndex	RC	The index for the StaticRoute Configurations table.

Object-ID	Object name	Syntax	Access	Description
1.3.6.1.4.1.231.7.2.7.13.2.1.1.6.1.2	gwManagementStaticRouteDestination	IpAddress	RC	The destination IP address of this route.
1.3.6.1.4.1.231.7.2.7.13.2.1.1.6.1.3	gwManagementStaticRouteMask	IpAddress	RC	Indicate the mask to be logical-ANDed with the destination address before being compared to the value in the ipRouteDest field.
1.3.6.1.4.1.231.7.2.7.13.2.1.1.6.1.4	gwManagementStaticRouteNextHop	IpAddress	RC	The IP address of the next hop of this route.
1.3.6.1.4.1.231.7.2.7.13.2.1.1.6.1.5	gwManagementStaticRouteMetric1	INTEGER	RC	The primary routing metric for this route.
1.3.6.1.4.1.231.7.2.7.13.2.1.1.6.1.6	gwManagementStaticRouteType	INTEGER	RC	The type of route.
1.3.6.1.4.1.231.7.2.7.13.2.1.1.6.1.7	gwManagementStaticRouteStatus	RowStatus	RC	The status of this static route entry.
1.3.6.1.4.1.231.7.2.7.13.2.1.1.4.1	globalDataTable	SEQUENCE OF GlobalDataEntry		Table containing global data of the rg2500 gateway.
1.3.6.1.4.1.231.7.2.7.13.2.1.1.4.1.1	globalDataEntry	GlobalDataEntry		Entry in the global data table.
1.3.6.1.4.1.231.7.2.7.13.2.1.1.4.1.1.1	globalDataID	Integer32 (0..1)	RC	Index to lookup an entry in the global data table.
1.3.6.1.4.1.231.7.2.7.13.2.1.1.4.1.1.2	systemLocation	DisplayString (SIZE(0..20))	RW	
1.3.6.1.4.1.231.7.2.7.13.2.1.1.4.1.1.3	systemName	DisplayString (SIZE(0..20))	RW	
1.3.6.1.4.1.231.7.2.7.13.2.1.1.4.1.1.4	systemIPAddress	DisplayString (SIZE(0..20))	RO	
1.3.6.1.4.1.231.7.2.7.13.2.1.1.4.1.1.5	systemSubnetMask	DisplayString (SIZE(0..20))	RO	
1.3.6.1.4.1.231.7.2.7.13.2.1.1.4.1.1.6	systemDateTime	DisplayString (SIZE(14..20))	RW	
1.3.6.1.4.1.231.7.2.7.13.2.1.1.4.1.1.7	systemCountryCode	Integer32	RW	
1.3.6.1.4.1.231.7.2.7.13.2.1.1.4.1.1.8	systemUpTime	TimeTicks	RW	
1.3.6.1.4.1.231.7.2.7.13.2.1.1.4.1.1.9	gwEnableGatekeeperUsage	BooleanValue	RW	
1.3.6.1.4.1.231.7.2.7.13.2.1.1.4.1.1.10	gwEnableQSIGProtocolTunneling	BooleanValue	RW	
1.3.6.1.4.1.231.7.2.7.13.2.1.1.4.1.1.11	gwEnableH323TerminalSupport	BooleanValue	RW	
1.3.6.1.4.1.231.7.2.7.13.2.1.1.4.1.1.12	gwEnablePreH450CallForward	BooleanValue	RW	
1.3.6.1.4.1.231.7.2.7.13.2.1.1.4.1.1.13	gwEnablePreH450CallTransfer	BooleanValue	RW	
1.3.6.1.4.1.231.7.2.7.13.2.1.1.4.1.1.14	gwEnableH450FeatureSupport	BooleanValue	RW	
1.3.6.1.4.1.231.7.2.7.13.2.1.1.4.1.1.15	gwEnableH235Profile1Support	BooleanValue	RW	

Object-ID	Object name	Syntax	Access	Description
1.3.6.1.4.1.231.7.2.7.13.2.1.4.1.16	u2DmlineHelp	DisplayString (SIZE(0..20))	RW	
1.3.6.1.4.1.231.7.2.7.13.2.1.4.1.17	u2DmlineImplementation	DisplayString (SIZE(0..20))	RW	
1.3.6.1.4.1.231.7.2.7.13.2.1.4.3.18	server4SystemID	DisplayString (SIZE(0..20))	RW	
1.3.6.1.4.1.231.7.2.7.13.2.1.4.1.19	server4IntegrOnOff	BooleanValue	RW	
1.3.6.1.4.1.231.7.2.7.13.2.1.4.1.20	server4AudIpAddress	DisplayString (SIZE(0..20))	RW	
1.3.6.1.4.1.231.7.2.7.13.2.1.4.1.21	server4AudPort	Integer32	RW	
1.3.6.1.4.1.231.7.2.7.13.3	gwMSCandApplications			HG3550 V2 / HiPath 4000 V2 MIB. See cg2500.my
1.3.6.1.4.1.231.7.2.7.13.3.1	msc			
1.3.6.1.4.1.231.7.2.7.13.3.1.1	mscStats			
1.3.6.1.4.1.231.7.2.7.13.3.1.1.1	mscStatsOverall			msc overall statistics
1.3.6.1.4.1.231.7.2.7.13.3.1.1.1.1	mscOutgoingRTPpackets	Counter	RO	Outgoing RTP packets (overall).
1.3.6.1.4.1.231.7.2.7.13.3.1.1.1.2	mscOutgoingRTPLostpackets	Counter	RO	Outgoing RTP packets lost (overall).
1.3.6.1.4.1.231.7.2.7.13.3.1.1.1.3	mscIncomingRTPpackets	Counter	RO	Incoming RTP packets (overall).
1.3.6.1.4.1.231.7.2.7.13.3.1.1.1.4	mscIncomingRTPLostpackets	Counter	RO	Incoming RTP packets lost (overall).
1.3.6.1.4.1.231.7.2.7.13.3.1.1.1.5	mscTotalBytesSent	Counter	RO	Total bytes sent.
1.3.6.1.4.1.231.7.2.7.13.3.1.1.1.6	mscTotalBytesReceived	Counter	RO	Total bytes received.
1.3.6.1.4.1.231.7.2.7.13.3.1.1.2	mscStatsPerCallTable	SEQUENCE OF MscStatsPerCallEntry		The table of per-call msc statistics.
1.3.6.1.4.1.231.7.2.7.13.3.1.1.2.1	mscStatsPerCallEntry	MscStatsPerCallEntry		The Msc statistics about one resource.
1.3.6.1.4.1.231.7.2.7.13.3.1.1.2.1.1	mscStatsPerCallInd	INTEGER		The table index
1.3.6.1.4.1.231.7.2.7.13.3.1.1.2.1.2	mscPeerCanonicalName	OCTET STRING (SIZE (0..64))	RO	The connection name of the number called.

Object-ID	Object name	Syntax	Access	Description
1.3.6.1.4.1.231.7.2.7.13.3.1.2.1.3	mscCallDestIP	OCTET STRING (SIZE (0..15))	RO	The destination IP address (H.323).
1.3.6.1.4.1.231.7.2.7.13.3.1.2.1.4	mscCallStartTime	OCTET STRING (SIZE (0..64))	RO	Time when the last call started.
1.3.6.1.4.1.231.7.2.7.13.3.1.2.1.5	mscEncoder	INTEGER	RO	Encoder used with this call. - g711ULaw(0) - g723(4) - g711ALaw(8) - g729(18)
1.3.6.1.4.1.231.7.2.7.13.3.1.2.1.6	mscDecoder	INTEGER	RO	Decoder used with this call. - g711ULaw(0) - g723(4) - g711ALaw(8) - g729(18)
1.3.6.1.4.1.231.7.2.7.13.3.1.2.1.7	mscSpecOutgoingRTPpackets	Counter	RO	Outgoing RTP packets (per-call).
1.3.6.1.4.1.231.7.2.7.13.3.1.2.1.8	mscSpecOutgoingRTPpacketsLost	Counter	RO	Outgoing RTP packets lost (per-call).
1.3.6.1.4.1.231.7.2.7.13.3.1.2.1.9	mscSpecIncomingRTPpackets	Counter	RO	Incoming RTP packets (per-call).
1.3.6.1.4.1.231.7.2.7.13.3.1.2.1.10	mscSpecIncomingRTPpacketsLost	Counter	RO	Incoming RTP packets lost (per-call).
1.3.6.1.4.1.231.7.2.7.13.3.1.2.1.11	mscSpecBytesSent	Counter	RO	Total bytes sent.
1.3.6.1.4.1.231.7.2.7.13.3.1.2.1.12	mscSpecBytesReceived	Counter	RO	Total bytes received.
1.3.6.1.4.1.231.7.2.7.13.3.1.2.1.13	mscSpecRndTripNetworkDelay	Integer32	RO	Round Trip Network Delay (in ms) for this connection.
1.3.6.1.4.1.231.7.2.7.13.3.1.2.1.14	mscSpecActualJitter	Integer32	RO	The actual jitter (in ms) for this connection.
1.3.6.1.4.1.231.7.2.7.13.3.1.2.1.15	mscSpecJitterBufferDepth	Integer32	RO	Current size of the DSP jitter buffer (in ms).
1.3.6.1.4.1.231.7.2.7.13.3.1.2.1.16	mscSpecRtpEncodings	Integer32	RO	Number of collected frames in one RTP packet sent from this gateway.
1.3.6.1.4.1.231.7.2.7.13.3.1.2.1.17	mscSpecAverageNetworkDelay	Integer32	RO	Average network delay for this call (in ms).
1.3.6.1.4.1.231.7.2.7.13.3.1.2.1.18	mscSpecJitterLan	Integer32	RO	Jitter in the LAN of this connection.

Object-ID	Object name	Syntax	Access	Description
1.3.6.1.4.1.231.7.2.7.13.3.1.2.1.19	mscFraction	Integer32	RO	Fraction of RTP data packets from a specific source that were lost since the previous receiver report was sent.
1.3.6.1.4.1.231.7.2.7.13.3.1.2.1.20	mscMaxFractionLostOutgoing	Integer32	RO	Maximum fractional packet loss among all currently participating session members except ourself.
1.3.6.1.4.1.231.7.2.7.13.3.1.2.1.21	mscSpecCumLatePacketOutgoing	Integer32	RO	The number of late packets, since the beginning of the connection.
1.3.6.1.4.1.231.7.2.7.13.3.1.2.1.22	mscEncTimePerPacket	Integer32	RO	Encoding time (in ms) per packet.
1.3.6.1.4.1.231.7.2.7.13.3.1.2	mscConfig			Msc configuration
1.3.6.1.4.1.231.7.2.7.13.3.1.2.1	mscRtpPortLow	INTEGER (1024..65535)	RW	The low port boundary of RTP/ RTCP ports.
1.3.6.1.4.1.231.7.2.7.13.3.1.2.2	mscRtpPortHigh	INTEGER (1024..65535)	RW	The high port boundary of RTP/ RTCP ports.
1.3.6.1.4.1.231.7.2.7.13.3.1.2.3	mscT38PortLow	INTEGER (1024..65535)	RW	The low port boundary of TCP ports (T38-fax).
1.3.6.1.4.1.231.7.2.7.13.3.1.2.4	mscT38PortHigh	INTEGER (1024..65535)	RW	The high port boundary of TCP ports (T38-fax).
1.3.6.1.4.1.231.7.2.7.13.3.1.2.5	mscTrafficStatistic	BooleanValue	RW	TrafficStatistic on / off; Generating of the per call statistic (by the GW / GK) is enabled or disabled.
1.3.6.1.4.1.231.7.2.7.13.3.1.2.9	mscJitterBufferAdaptation	BooleanValue	RW	If this is set by host the DSP jitter buffer adapts its depth based on its statistics. If not, host has to explicitly adjust the jitter buffer depth at run time, based on statistics generated by the DSP.
1.3.6.1.4.1.231.7.2.7.13.3.1.2.10	mscJitterType	INTEGER	RW	Jitter buffer adaptation algorithm (0..TIS, 1..HLB2)
1.3.6.1.4.1.231.7.2.7.13.3.1.2.11	mscJitterCacheUpdateInterval	INTEGER (5..10)	RW	Jitter Cache update interval: 5 - 10 seconds.
1.3.6.1.4.1.231.7.2.7.13.3.1.2.15	mscJitterTotalFractionLostWeight	INTEGER (0..1000)	RW	Factor for smoothing the varying fraction lost of incoming RTP packets caused by jitter in 10th of percents, i.e. 1000 is 100.0%. Default: 300 (30%).

Object-ID	Object name	Syntax	Access	Description
1.3.6.1.4.1.231.7.2.7.13.3.1.2.1.16	mscJitterMinFractionLost	INTEGER (0..1000)	RW	Lower threshold for the adaptive control of jitter buffer size for incoming RTP packets in 10th of percents, i.e. 1000 is 100.0%. Default: 5 (0.5%).
1.3.6.1.4.1.231.7.2.7.13.3.1.2.1.17	mscJitterMaxFractionLost	INTEGER (0..1000)	RW	Upper threshold for the adaptive control of jitter buffer size for incoming RTP packets in 10th of percents, i.e. 1000 is 100.0%. Default: 40 (4%).
1.3.6.1.4.1.231.7.2.7.13.3.1.2.1.18	mscJitterFactor	INTEGER (0..1000)	RW	Factor for resizing the jitter buffer with respect to the average jitter: Default: 4.
1.3.6.1.4.1.231.7.2.7.13.3.1.2.1.19	mscJitterIncrement	INTEGER (100..300)	RW	Increment of jitter buffer, if jitterMinFractionLost is exceeded in 100 microsecond steps: Default: 200 (20ms).
1.3.6.1.4.1.231.7.2.7.13.3.1.2.1.20	mscJitterDecrement	INTEGER (100..300)	RW	Decrement of jitter buffer, if smoothed average jitter falls below jitterMaxFractionLost in 100 microsecond steps: Default: 100 (10ms).
1.3.6.1.4.1.231.7.2.7.13.3.1.2.1.21	mscJitterBufferAvarageDelay	INTEGER (0..300)	RW	The depth of the jitter buffer in ms. Set by host at the configuration time. The DSP will round the value to multiple of 10 ms. Range: 0 - 300 ms
1.3.6.1.4.1.231.7.2.7.13.3.1.3	mscDspConfig			Msc DSP configuration
1.3.6.1.4.1.231.7.2.7.13.3.1.3.1	mscVadEnable	BooleanValue	RW	Voice Activity Detection on / off; VAD is explicitly performed for G.711 only.
1.3.6.1.4.1.231.7.2.7.13.3.1.3.4	mscEchoCancellerEnable	BooleanValue	RW	Echo Canceller on / off; Compensation for echos which can occur in the case of connection via the voice gateway to analog telephones.
1.3.6.1.4.1.231.7.2.7.13.3.1.3.5	mscDtmfReceiveEnable	BooleanValue	RW	Dtmf Outband Signalization on / off.
1.3.6.1.4.1.231.7.2.7.13.3.1.3.6	mscDtmfDefaultToneLength	INTEGER (50..300)	RW	Default length of pulse of the DTMF tones.
1.3.6.1.4.1.231.7.2.7.13.3.1.3.7	mscG711MaxRecvBytes	INTEGER (80..960)	RW	Max. Bytes of G711 coded RTP data.

Object-ID	Object name	Syntax	Access	Description
1.3.6.1.4.1.231.7.2.7.13.3.1.3.7	mscG723MaxRecvBytes	INTEGER (24..96)	RW	Max. Bytes of G723A coded RTP data.
1.3.6.1.4.1.231.7.2.7.13.3.1.3.9	mscG729MaxRecvBytes	INTEGER (20..120)	RW	Max. Bytes of G729A/AB coded RTP data.
1.3.6.1.4.1.231.7.2.7.13.3.1.3.10	mscG711EncTimePerPacket	INTEGER (10..120)	RW	Defines the encoding time (in ms) per packet for G711 encoder control.
1.3.6.1.4.1.231.7.2.7.13.3.1.3.12	mscG723EncTimePerPacket	INTEGER (30..120)	RW	Defines the encoding time (in ms) per packet for G723 encoder control.
1.3.6.1.4.1.231.7.2.7.13.3.1.3.13	mscG729EncTimePerPacket	INTEGER (20..120)	RW	Defines the encoding time (in ms) per packet for G729 encoder control.
1.3.6.1.4.1.231.7.2.7.13.3.1.3.18	mscDtmfDefaultPauseLength	INTEGER (50..300)	RW	Default length of pause of the sent DMTF tones.
1.3.6.1.4.1.231.7.2.7.13.3.2	gwApplications			
1.3.6.1.4.1.231.7.2.7.13.3.2.1	deviceConfiguration			
1.3.6.1.4.1.231.7.2.7.13.3.2.2	deviceResourceStatistics			
1.3.6.1.4.1.231.7.2.7.13.3.2.2.1	deviceResourceMgmtTable	SEQUENCE OF DeviceResourceMgmtEntry		Device resource management statistics table
1.3.6.1.4.1.231.7.2.7.13.3.2.2.1.1	deviceResourceMgmtEntry	DeviceResourceMgmtEntry		

Object-ID	Object name	Syntax	Access	Description
1.3.6.1.4.1.231.7.2.7.13.2.2.1.1	devId	INTEGER	RO	unique id of a device - devIdISDNSubs(0) - devIdISDNTrunk(1) - devIdHFA(2) - devIdPayload(3) - devIdMoH(4) - devHXG3RTP(5) - devHXG3Fax(6) - devHXG3PPP(7) - devHXG3Vcapi(8) - devIdWAML(10) - devIdISDNTrunk1(11) - devIdISDNTrunk2(12) - devIdISDNTrunk3(13) - devIdISDNTrunk4(14) - devIdDMC(15) - devIdRTP(100) - devIdFax(101) - devIdPPP(102) - devIdVcapi(103) - devIdNu(104) - devIdLegk(105) - devIdUnused(106) - deviceId_Rtp_H323(110) - deviceId_Fax_H323(111) - deviceId_Rtp_SIP(120) - deviceId_Fax_SIP(121)
1.3.6.1.4.1.231.7.2.7.13.2.2.1.2	devMaxCh	Integer32	RO	Effective max. number of useable channels. unique id of a device - deviceId_Rtp_H323(110) - deviceId_Fax_H323(111) - deviceId_Rtp_SIP(120) - deviceId_Fax_SIP(121)

Object-ID	Object name	Syntax	Access	Description
1.3.6.1.4.1.231.7.2.7.13.3.2.1.13	devSeizedChannels	Integer32	RO	Number of channels currently in use.unique id of a device - deviceId_Rtp_H323(110) - deviceId_Fax_H323(111) - deviceId_Rtp_SIP(120) - deviceId_Fax_SIP(121)
1.3.6.1.4.1.231.7.2.7.13.3.2.2	gwParameters			Gateway Parameters
1.3.6.1.4.1.231.7.2.7.13.3.2.3.2	gwGlobalTrace			
1.3.6.1.4.1.231.7.2.7.13.3.2.3.2.1	gwGlobalTraceID	Integer32	RW	
1.3.6.1.4.1.231.7.2.7.13.3.2.3.2.2	gwConsoleTraceOnOff	BooleanValue	RW	Switch whole console tracing on or off.
1.3.6.1.4.1.231.7.2.7.13.3.2.3.2.3	gwFileTraceOnOff	BooleanValue	RW	Switch whole file tracing on or off.
1.3.6.1.4.1.231.7.2.7.13.3.2.3.2.4	gwTraceMaxFileSize	Integer32	RO	Maximum size of trace file.
1.3.6.1.4.1.231.7.2.7.13.3.2.3.2.5	gwTraceTimerValue	Integer32	RO	Timer for tracing.
1.3.6.1.4.1.231.7.2.7.13.3.2.3.2.6	gwTraceMaxBuffSize	Integer32	RO	Maximum buffer size for tracing.
1.3.6.1.4.1.231.7.2.7.13.3.2.4	gwEventLog			
1.3.6.1.4.1.231.7.2.7.13.3.2.4.1	gwTrapGenerationTbl	SEQUENCE OF GwTrapGenerationEntry		The trap generation table indicates for which events traps are generated and for which not.
1.3.6.1.4.1.231.7.2.7.13.3.2.4.1.1	gwTrapGenerationEntry	GwTrapGenerationEntry		An entry in the trap generation table for a particular event.
1.3.6.1.4.1.231.7.2.7.13.3.2.4.1.1.1	gwTrapEventID	Integer32	RC	This index of the trap generation table identifies a particular event.
1.3.6.1.4.1.231.7.2.7.13.3.2.4.1.1.2	gwTrapEventName	OCTET STRING (SIZE (0..64))	RC	
1.3.6.1.4.1.231.7.2.7.13.3.2.4.1.1.3	gwTrapType	Integer32	RC	This determines whether a trap is generated for that event or not.
1.3.6.1.4.1.231.7.2.7.13.3.2.4.1.1.4	gwTrapFlag	BooleanValue	RC	
1.3.6.1.4.1.231.7.2.7.13.3.2.4.1.1.5	gwRebootFlag	BooleanValue	RC	
1.3.6.1.4.1.231.7.2.7.13.3.2.4.1.1.6	gwRebootType	Integer32	RC	This determines whether a trap is generated for that event or not.
1.3.6.1.4.1.231.7.2.7.13.3.2.4.1.1.7	gwTrapGenRowCmd	RowCmd	RC	Setting this to destroy will delete this entry.

Object-ID	Object name	Syntax	Access	Description
1.3.6.1.4.1.231.7.2.7.13.9.2.5	gwStatistics			Gateway Statistics
1.3.6.1.4.1.231.7.2.7.13.9.2.5.1	gwStatNumLANVoiceCallsRcvd1H	Counter	RO	Number of incoming voice calls received in the last hour.
1.3.6.1.4.1.231.7.2.7.13.9.2.5.2	gwStatNumLANVoiceCallsRcvd24H	Counter	RO	Number of incoming voice calls received in the last 24 hours.
1.3.6.1.4.1.231.7.2.7.13.9.2.5.3	gwStatNumLANFaxCallsRcvd1H	Counter	RO	Number of incoming fax calls received in the last hour.
1.3.6.1.4.1.231.7.2.7.13.9.2.5.4	gwStatNumLANFaxCallsRcvd24H	Counter	RO	Number of incoming fax calls received in the last 24 hours.
1.3.6.1.4.1.231.7.2.7.13.9.2.5.5	gwStatNumLANVoiceCallsConn1H	Counter	RO	Number of incoming voice calls connected in the last hour.
1.3.6.1.4.1.231.7.2.7.13.9.2.5.6	gwStatNumLANVoiceCallsConn24H	Counter	RO	Number of incoming voice calls connected in the last 24 hours.
1.3.6.1.4.1.231.7.2.7.13.9.2.5.7	gwStatNumLANFaxCallsConn1H	Counter	RO	Number of incoming fax calls connected in the last hour.
1.3.6.1.4.1.231.7.2.7.13.9.2.5.8	gwStatNumLANFaxCallsConn24H	Counter	RO	Number of incoming fax calls connected in the last 24 hours.
1.3.6.1.4.1.231.7.2.7.13.9.2.5.9	gwStatNumPBXVoiceCallsRcvd1H	Counter	RO	Number of outgoing voice calls received in the last hour.
1.3.6.1.4.1.231.7.2.7.13.9.2.5.10	gwStatNumPBXVoiceCallsRcvd24H	Counter	RO	Number of outgoing voice calls received in the last 24 hours.
1.3.6.1.4.1.231.7.2.7.13.9.2.5.11	gwStatNumPBXFaxCallsRcvd1H	Counter	RO	Number of outgoing fax calls received in the last hour.
1.3.6.1.4.1.231.7.2.7.13.9.2.5.12	gwStatNumPBXFaxCallsRcvd24H	Counter	RO	Number of outgoing fax calls received in the last 24 hours.
1.3.6.1.4.1.231.7.2.7.13.9.2.5.13	gwStatNumPBXVoiceCallsConn1H	Counter	RO	Number of outgoing voice calls connected in the last hour.
1.3.6.1.4.1.231.7.2.7.13.9.2.5.14	gwStatNumPBXVoiceCallsConn24H	Counter	RO	Number of outgoing voice calls connected in the last 24 hours.
1.3.6.1.4.1.231.7.2.7.13.9.2.5.15	gwStatNumPBXFaxCallsConn1H	Counter	RO	Number of outgoing fax calls connected in the last hour
1.3.6.1.4.1.231.7.2.7.13.9.2.5.16	gwStatNumPBXFaxCallsConn24H	Counter	RO	Number of outgoing fax calls connected in the last 24 hours.
1.3.6.1.4.1.231.7.2.7.13.9.2.5.17	gwStatCumLANCallDuration1H	Counter	RO	Cumulative call duration in seconds in the last hour.
1.3.6.1.4.1.231.7.2.7.13.9.2.5.18	gwStatCumLANCallDuration24H	Counter	RO	Cumulative call duration in seconds in the last 24 hours.

Object-ID	Object name	Syntax	Access	Description
1.3.6.1.4.1.231.7.2.7.13.3.2.5.19	gw2stat19	Counter	RO	Cumulative call duration in seconds in the last hour.
1.3.6.1.4.1.231.7.2.7.13.3.2.5.20	gw2stat20	Counter	RO	Cumulative call duration in seconds in the last 24 hours.
1.3.6.1.4.1.231.7.2.7.13.3.2.5.25	gw2stat25	Counter	RO	Cumulative number of current calls
1.3.6.1.4.1.231.7.2.7.13.3.2.5.30	gw2stat30	Counter	RO	Number of incoming LAN data calls received in the last hour.
1.3.6.1.4.1.231.7.2.7.13.3.2.5.31	gw2stat31	Counter	RO	Number of incoming LAN data calls received in the last 24 hours.
1.3.6.1.4.1.231.7.2.7.13.3.2.5.32	gw2stat32	Counter	RO	Number of incoming LAN data calls connected in the last hour.
1.3.6.1.4.1.231.7.2.7.13.3.2.5.33	gw2stat33	Counter	RO	Number of incoming LAN data calls connected in the last 24 hours.
1.3.6.1.4.1.231.7.2.7.13.3.2.5.34	gw2stat34	Counter	RO	Number of incoming PBX data calls received in the last hour.
1.3.6.1.4.1.231.7.2.7.13.3.2.5.35	gw2stat35	Counter	RO	Number of incoming PBX data calls received in the last 24 hours.
1.3.6.1.4.1.231.7.2.7.13.3.2.5.36	gw2stat36	Counter	RO	Number of incoming PBX data calls connected in the last hour.
1.3.6.1.4.1.231.7.2.7.13.3.2.5.37	gw2stat37	Counter	RO	Number of incoming PBX data calls connected in the last 24 hours.
1.3.6.1.4.1.231.7.2.7.13.3.2.7.0	gw2TrapGroup			The HXG3 SNMP Traps
1.3.6.1.4.1.231.7.2.7.13.3.2.7.1	gw2Trap1	TRAP		Indicates a problem with the RG2500 software. Sent when the Admin server detects a trapable event in the event log.
1.3.6.1.4.1.231.7.2.7.13.3.2.7.3	gw2Startup	TRAP		Indicates the startup of HG3550 V2.
1.3.6.1.4.1.231.7.2.7.13.3.2.7.4	gw2Reboot	TRAP		Indicates the reboot of HG3550 V2.
1.3.6.1.4.1.231.7.2.7.13.3.2.7.5	gw2Threshold	TRAP		Indicates that a threshold has reached in HG3550 V2.
1.3.6.1.4.1.231.7.2.7.13.3.2.7.6	gw2WanLinkUp	TRAP		Indicates a WAN Linkup of HG1500.
1.3.6.1.4.1.231.7.2.7.13.3.2.7.7	gw2WanLinkDown	TRAP		Indicates a WAN Linkdown of HG3550 V2.
1.3.6.1.4.1.231.7.2.7.13.3.2.7.8	gw2IpLinkUp	TRAP		Indicates an IP Link up of HG3550 V2.

Object-ID	Object name	Syntax	Access	Description
1.3.6.1.4.1.231.7.2.7.13.9.2.8.9	gwV2pbIpLinkDown	TRAP		Indicates an IP Linkdown of HG3550 V2.
1.3.6.1.4.1.231.7.2.7.13.9.2.8.10	gwV2AuxTrap	TRAP		Indicates an auxiliary trap of HG3550 V2.
1.3.6.1.4.1.231.7.2.7.13.3.2.9	trap2Num	DisplayString	RO	Defines a software error number - use with type of trap and info like software component ID or board/ port to isolate exact error.
1.3.6.1.4.1.231.7.2.7.13.3.2.10	trap2Text	DisplayString	RO	Defines text to be sent up with the trap.
1.3.6.1.4.1.231.7.2.7.13.3.2.11	trap2Type	INTEGER	RO	The type of error occurred. - software(1) - hardware(2) - startup(3) - reboot(4) - threshold(5) - wanLinkUp(6) - wanLinkDown(7) - ipLinkUp(8) - ipLinkDown(9) - auxTrap(10)
1.3.6.1.4.1.231.7.2.7.13.9.2.12	gwV2trap2Severity	DisplayString	RO	Defines the severity of the trap.

Table 14: Definitions in the company's specific MIB

Object-ID	Object name	Description
1.3.6.1.4.1.4329	siemens	HG3550-V11 MIB, see hg3500_v11.my
1.3.6.1.4.1.4329.2	iandcAdmin	
1.3.6.1.4.1.4329.2.24	hg3550v11	Definition of the system OID for hg3550 V2

Table 15: Collected list of traps (repeated)

Object-ID	Object name	Description
1.3.6.1.2.1.10.20.2.0.1	isdnMibCallInformation	This trap/inform is sent to the manager under the following conditions: - on incoming calls for each call which is rejected for policy reasons (e.g. unknown neighbor or access violation) - on outgoing calls whenever a call attempt is determined to have ultimately failed. In the event that call retry is active, then this will be after all retry attempts have failed. - whenever a call connects. In this case, the object isdnBearerCallConnectTime should be included in the trap.
1.3.6.1.4.1.231.7.2.7.5	sendAlarmWithValues	If an error occurs, there will be checked if the errorClass is configured to trigger a immediate signaling. If so, a trap will be send to the management station containing the information shown above.
1.3.6.1.4.1.231.7.2.7.6	fileOverflowError	Inform the manager that the trap history table got too big. Unless the size of the table is reduced by the manager (by resetting numberOfTrapHistoryEntries), the oldest trap informations will be overridden from now on.
1.3.6.1.4.1.231.7.2.7.11.1	sendVoIPQualityNotification	This notification will be sent when the latest voice over IP connection had quality problems.
1.3.6.1.4.1.231.7.2.7.11.2	sendIpPhoneTableNotification	This notification will be sent whenever the errorState of an IP phone table entry changes or when the configuration of IP phones is changed.
1.3.6.1.4.1.231.7.2.7.13.8.2.1	gw2Trap	Indicates a problem with the RG2500 software. Sent when the Admin server detects a trapable event in the event log.
1.3.6.1.4.1.231.7.2.7.13.9.2.3	gw2Startup	Indicates the startup of HG3550 V2.
1.3.6.1.4.1.231.7.2.7.13.9.2.4	gw2Reboot	Indicates the reboot of HG3550 V2.
1.3.6.1.4.1.231.7.2.7.13.9.2.5	gw2Threshold	Indicates that a threshold has reached in HG3550 V2.
1.3.6.1.4.1.231.7.2.7.13.9.2.6	gw2WanLinkUp	Indicates a WAN Linkup of HG1500.
1.3.6.1.4.1.231.7.2.7.13.9.2.7	gw2WanLinkDown	Indicates a WAN Linkdown of HG3550 V2.
1.3.6.1.4.1.231.7.2.7.13.9.2.8	gw2IpLinkUp	Indicates an IP Link up of HG3550 V2.
1.3.6.1.4.1.231.7.2.7.13.9.2.9	gw2IpLinkDown	Indicates an IP Linkdown of HG3550 V2.
1.3.6.1.4.1.231.7.2.7.13.9.2.10	gw2AuxTrap	Indicates an auxiliary trap of HG3550 V2.

2.21 IP Ports

2.21.1 General Information

The port assignments are available in the Interface Management Database (IFMDB).

You can access the IFMDB via Intranet or Partner Portal portal:

- Intranet
- Homepage > Index “I” > IFMDB (Interface Management DataBase)
- Partner Portal Portal
- Support > Interface Management (IFMDB)

2.21.2 Port Range

2.21.2.1 IP Trunking + DMC (IP Trunking and IPDA) Master Connections

Port value range with AMO CGWB

The UDP port range is configured with the **AMO CGWB** for IP trunking master connections and DMC slave connections where HG 3500 is a DMC endpoint (i.e. for IP trunking or IPDA). The corresponding parameter is **UDPPRTLO** in the **TYP=ASC** branch. **UDPPRTHI** can not be modified. It is calculated from the value of **UDPPRTLO** + 999 Ports.

The standard value for **UDPPRTLO** is 29100.

IMPORTANT: Because connections can be switched with(out) DMC and/or SPE (depending on the configuration), the maximum number of ports must always be reserved by the gateway, even if possibly only a lower number of ports is used!

2.21.2.2 IPDA (HG 3575/HG 3500) + DMC (HG 3575) master connections

- IPDA master connections
- The **UDPPORT** parameter in the AMO SIPCO is used for the payload stream in the IPDA master connection, i.e. for connections between the IPDA-HG 3500 and the HG 3575 and vice versa and for connections from HG 3575 to HG 3575.

  For IPDA master connections, only the start value is defined in the AMO SIPCO, **TYPE=DIFFSERV**, **UDPPORT=<4352 ... 65083>**. The upper value (=maximum number of ports actually used) is calculated on the basis of the number of B channels of the board used.

  The port with the lowest value can be set to even values in the range [4352 ... 65280].
- DMC slave connections

- The **UDPPORT** parameter applies to the AMO SIPCO for DMC slave connections where NCUI2+/NCUI4 is the DMC endpoint. The following ports are used automatically.

  The port range from the AMO CGWB (**UDPPRTLO-UDPPRTHI**) applies to slave connections where STMI2/STMI4 and STMIX/STMIY is the DMC endpoint.

  IMPORTANT: The ports in use cannot be modified with the exception of ports for "UDP-Payload".

2.21.3 Information for Network Administrators

IMPORTANT: IP packets with the used ports (hard-coded and configured using AMOs) must be routed transparently in the IP network, i.e. the packets must be unmanipulated, e.g. by a firewall). Functional problems can be the result of non-transarent routing!

2.21.4 Examples

The following are a few examples to clarify the traffic restrictions applied to certain ports.

2.21.4.1 Payload

Depending on the board in use (HG 3500 or HG 3575), ports used are taken from a certain port range defined by the parameter UDPPORT (AMO SIPCO). The port range for RTP/RTCP is defined by the following interval: [UDPPORT .. UDPPORT + 960].

Port 4007 is used for a path test in the case of poor payload quality. See Section 2.9.1, “When is Payload Survivability Used?” in the document "IP Distributed Architecture (IPDA)" - keyword "UDP-PINA".

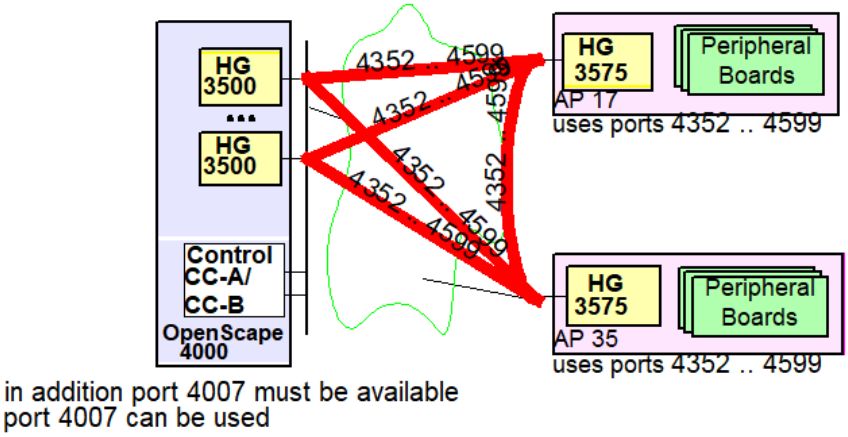


Figure 39: Example: Port usage for payload

2.21.4.2 Signaling

The term signaling refers to the entire data exchange between CC and access point. This includes loading and controlling peripheral boards, security messages, routine tests and naturally, all call processing messages including telephone display texts.

Every access point, that is, every HG 3575, has a signaling connection to the active CC. The connection for this is always set up by the CM. The source port alternates between 1124 and 1125. The destination port (ASC HG 3575) is 4000.

The HG 3575 loadware is loaded over FTP. The HG 3575 logs on to the CM's FTP server for this. The FTP server grants read-only access to the HG 3575 configured and allows only one download at a time.

If signaling survivability is configured additional connections are used.

The supervisory connection monitors the principal availability of the path from the CM to the HG 3575 in the IP network - in parallel to the signaling connection. The connection for this is always set up by the CC. The source port alternates between 1126 and 1127. The destination port (ASC HG 3575) is 4001.

If the supervisory connection is interrupted, the signaling connection is re-routed over a PSTN router and modem. The signaling connection's IP address and ports are retained.

The modem-based availability of a HG 3575 with signaling survivability is cyclically tested in normal mode. The connection for this is always set up by the CM. The source port alternates between 1128 and 1129. The destination port (ASC HG 3575) is 4002.

IMPORTANT: For SURVPATH test: There will be an ARP request from active CC (physical linux address from V6) for the MAC of the WAML. Afterwards packets will be routed on port 4002 to the WAML using the IP Address of the NCUI on the WAML MAC. **For normal Signaling Survivability**: Normal Signaling happens on port 4000. Once the keep alive fails for the supervisory port 4001, there will be an ARP request from active CC (physical linux address from V6) for the MAC of the WAML. Afterwards packets will be instantly routed on port 4000 to the WAML using the IP address of the NCUI but the WAML MAC on same TCP session, i.e. TCP session is not re-established, only the destination MAC address is replaced by the WAML MAC.

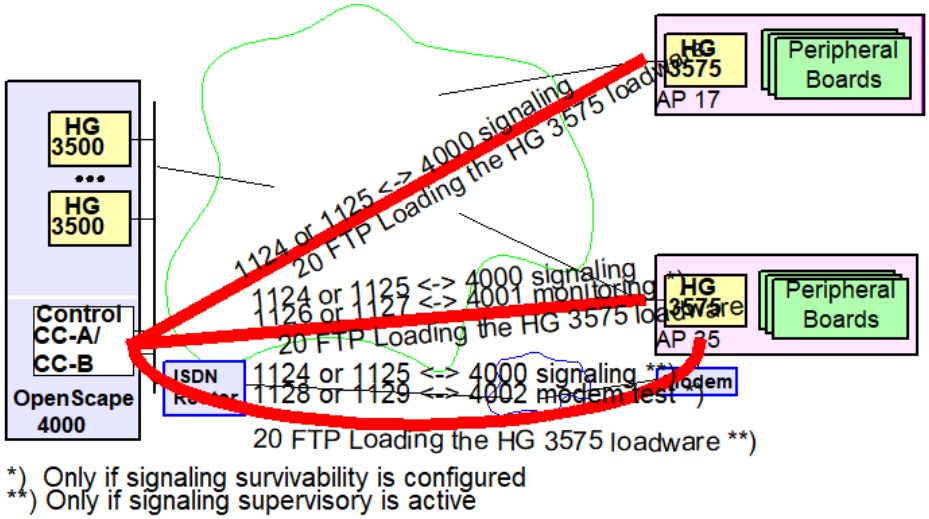


Figure 40: Example: Port usage for signaling

2.21.4.3 SNMP

The gateways HG 3500 and HG 3575 come with an SNMP agent which provides read-only access to MIB-2 data and a gateway-specific MIB. Please refer to Chapter 19, “SNMP Support HG 3500 / HG 3575”. Read-only access is supported. No parameters may be changed. No traps are transferred.

The SNMP agent waits by default at port 161.

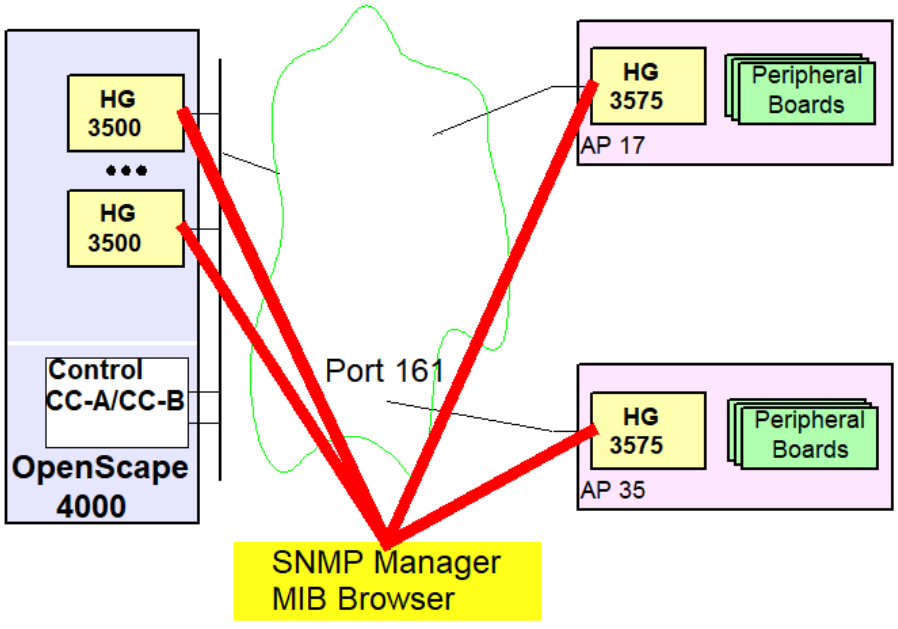


Figure 41: Example: Port usage for SNMP access

2.21.4.4 Diagnostics

Additional services that are normally inaccessible (ports blocked) can be activated on the gateways HG 3500 and HG 3575 for fault diagnosis.

These are

SSH	Port 22	TCP
HTTPS/WBM:	Port 443	Web server for accessing diagnostic data

Logons with passwords can be configured to protect access for the HG 3575. HG 3500 uses fixed values for this.

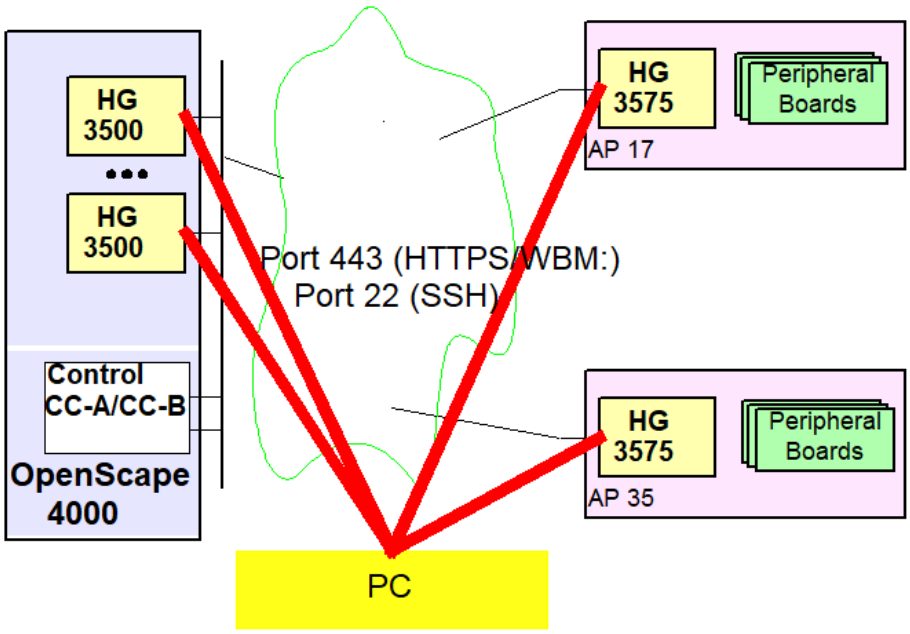


Figure 42: Example: Port usage for diagnosis

2.22 WBMs of the Boards

For a description of the graphical user interface of the WBMs of HG 3500 and HG 3575 please refer to the following link:

http://apps.g-dms.com:8081/techdoc/en/P31003H3180M1000176A9/index.htm

2.23 HG 3500 / HG 3575 Diagnostic Options

All diagnostic options for the gateways HG 3500 and HG 3575 are part of the WBM. The trace components can be configured in WBM. More information is provided in the WBM Online help.

- Retrieving/deleting an event protocol in the **T**rue **F**lash **F**ile **S**ystem (TFFS) via WBM
- **Maintenance** -> **Traces & Events** -> **Events**

- Retrieving/deleting a trace protocol in the **T**rue **F**lash **F**ile **S**ystem (TFFS) via WBM
- **Maintenance** -> **Traces & Events** -> **Events**
- Retrieving/deleting a customer trace protocol in the **T**rue **F**lash **F**ile **S**ystem (TFFS) via WBM.
- **Maintenance** -> **Traces & Events** -> **Events** -> **Event Configuration**
- V24 trace / console trace
- LAN trace for XTracer client
- Service center
- In the event of a system crash, the DDC log must be retrieved via WBM.
- Retrieving busy resources

2.24 Gateways HG 3500 and HG 3575 - Changing Gateway UI MODE

IP gateways access can be secured using parameter `UIMODE`, which can be accessed in `AMO CGWB` and `STMIB` or from Assistant (**Access Management -> Security Mode Configuration**).

UIMODE:

1) **CLASSIC**

   When the board is in CLASSIC mode, you can quickly access the SSH, WBM, and SFTP buttons (Remote access) from the Gateway Manager page. You can also use browsers or SSH clients like Putty and WinSCP to access the gateways directly. Other operations that you can perform during CLASSIC mode include Backup & Restore, OS upgrades, Loadware upgrades, Platform HF upgrades, Bootstrapping (DLS SPE), SNMP, and more.

   There is **no filtering** based upon the origin/source address of the HTTPS and SSH client.

2) **MAINTAIN**

   When the function of the board is changed from CLASSIC mode to MAINTAIN, the same operations that can be performed in CLASSIC mode can also be performed in the Assistant Gateway Manager.

   NOTICE: In MAINTAIN mode **direct** access from Browser and SSH clients like putty, WinSCP is not possible anymore, only via Assistant Gateway Manager.

   The difference between **CLASSIC** and **MAINTAIN** mode in Gateway Manager is that a lock appears in the menu next to the board (see Figure 43: Gateway Manager – Padlock icon after enabling MAINTAIN mode on page 248) and by clicking that lock from **MAINTAIN** you can switch the board to **SECURE**.

3) **SECURE**

   When the board has **SECURE** mode activated, not even Gateway Manager can access the HTTPS or SSH functions. The remote access buttons in the Gateway Manager are no longer available and there is no longer access to the operations presented in the **CLASSIC/MAINTAIN** mode (backup & restore, OS upgrade, LW upgrade, Platform HF upgrade and so on) (see

Figure 44: Gateway Manager – Padlock icon after enabling SECURE mode on page 248).

IMPORTANT:

The current `UIMODE` configuration of any board will not be changed during the update.
Starting with V11, the default UIMODE is changed from "**CLASSIC**" to "**MAINTAIN**" .

You can change a board from **CLASSIC UIMODE** to **MAINTAIN UIMODE** from`CGWB -> MTYPE (CGW) -> MGNTDATA -> UIMODE -> MAINTAIN`.

Assistant – GW Manager:

A gateway in **MAINTAIN/SECURE** mode will display a padlock icon (after board list is updated):

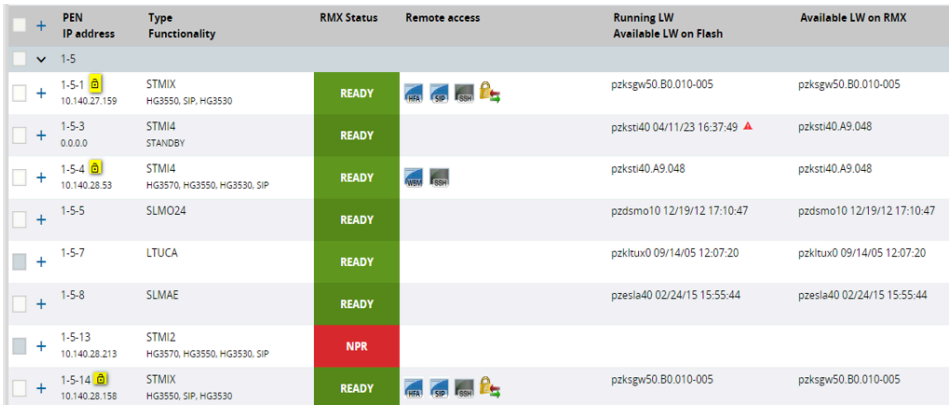


Figure 43: Gateway Manager – Padlock icon after enabling MAINTAIN mode

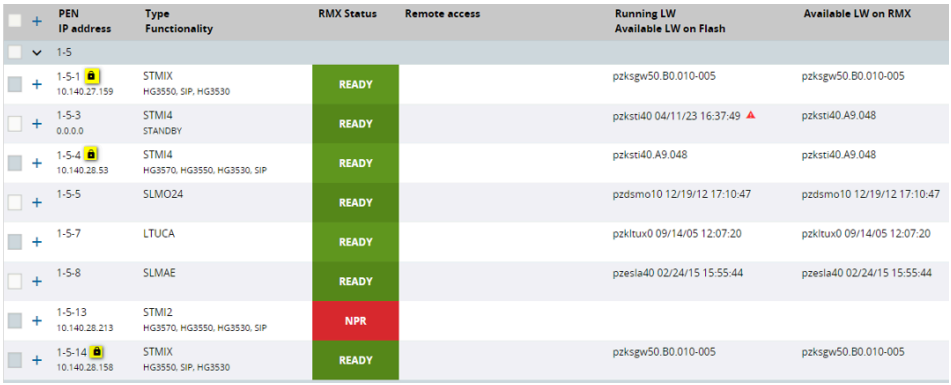


Figure 44: Gateway Manager – Padlock icon after enabling SECURE mode

2.25 Frequently asked Questions

1) **Question**: Are HG 3500 gateways supported on the Hicom 300 H?

Answer: No. Customers have to upgrade to HiPath 4000 V4 or higher in order to take advantage of integrated IP gateways.

2) **Question**: Why does the HG 3500 require a static IP address?

   Answer: From an IP networking point of view the HG 3500 is a gateway/ voice-router. Gateways/routers always require static IP addresses. This ensures that all IP devices always find their gateway/router without having to be reprogrammed constantly. Having dynamic IP addresses on gateways/routers does not make any practical sense.

3) **Question**: Is the HG 3500 supported on IP distributed Access Points?

   Answer: Yes. The HG 3500 version is supported on IP distributed Access Points. Excessive delays that resulted from multiple TDM to IP conversions when IP users on the IP Access Points call IP users on other IP Access Points or IP users on the host are eliminated using DMCs.

4) **Question:** Why do HG 3500 and HG 3575 not support DHCP?

   Answer: Consider HG 3500/3575 as a voice router. These voice routers must always be available and know each other. As is the case with IP router ports, it is useful to work with fixed IP addresses. For complete system availability, it is also better to avoid dependencies on DHCP and/or DNS servers.

5) **Question**: Why does the HG 3500 not support the G.722 codec?

   Answer: There is absolutely no need for the HG 3500 to support G.722 because there is no wideband quality available on the TDM side; G.722 strictly works between IP clients and it is the clients that negotiate the codec type. The HG 3500 will pass the signaling between any IP clients that support G.722, enabling high quality voice.

6) **Question:** Why is the default value for the jitter buffer set to 60 milliseconds on HG 3500/75? Can lower values also be set without leading to problems?

   Answer: The default setting should ensure that initial startup runs relatively smoothly. 60 ms is definitely too high for modern campus LAN installations that only use device connections at Layer-2 switch ports and have sufficient bandwidth reserves. A jitter buffer depth of 20 ms has been shown to be satisfactory. On the other hand, 60 ms may sometimes be too low for installations over WAN links with extremely low bandwidth and no reserve. Setting the jitter buffer depth too high causes an unnecessarily high voice delay. Setting it too low leads to poor transmission quality as a result of high packet loss rates. This poses problems particularly for fax, modem, and ISDN data connections.

7) **Question:** The maximum value that can be set for the jitter buffer is 210 ms. I assume that the system works properly with this setting. Can I specify this value in my WAN tender specification as a carrier requirement?

   Answer: The system has no problems with a 210 ms jitter buffer. This setting can balance out an extremely high jitter value of up to 210 ms without impairing voice comprehension. It should be noted, however, that the size of the jitter buffer has a direct effect on voice delay. See also

Section 1.4, “Voice Quality”. Voice delay (mouth-to-ear delay) is influenced by five elements:

a) Packet size/sample size/the number of audio milliseconds per packet

- Processing time on the receiving end
- Transmission time in the LAN/WAN
- Jitter buffer
- Processing time on the receiving end

Figure 3 Voice quality depending on delay illustrates user satisfaction in relation to the mouth-to-ear delay. Satisfaction drops dramatically at around 150 ms. Users start to notice interference at around 250 ms and become dissatisfied.

Please note that a similar installation can also cause delays in trunk calls at the other end of the CO trunk. In other words, only one half of the tolerable delays may be caused by each end.

The following table shows a couple of sample calculations (all values in ms)

Sample size	20	60	20	20	60	60	60	20
Transmission time in the LAN/WAN	10	10	10	40	40	40	60	0
Processing time Send+receive direction	32	32	32	32	32	32	32	32
Jitter buffer	20	20	60	60	60	120	**210**	**210**
Mouth-to-ear delay	82	122	122	152	192	252	**362**	**262**

It is not possible to achieve delays under 262 ms with a 210 ms jitter buffer.

8) **Question:** Both the HG 3500 and the HG 3575 have a fixed MAC address for the Ethernet port assigned to the board. The IP addresses, however, are assigned from the system database on the basis of the board’s “PEN“. If I switch a HG 3500 in a particular slot with another board of the same type, the IP address is maintained from the IP network’s perspective. However, the MAC address to which the packets are sent changes. Doesn’t this mean that the new board cannot be reached on account of the modified MAC address until *aging* makes the ARP entries obsolete in the IP stacks?

Answer: The standard solution for this problem which is principally an address resolution issue is also implemented on the HG 3500 and HG 3575 gateways. After activating the hardware interface, the gateway sends an ARP request “gratuitous ARP“ to the actual IP address. This way, all IP devices on the LAN segment learn the new IP <-> MAC address assignment.

9) **Question:** We regularly encounter statistic overflow problems in a customer installation. Individual HG 3500/75 boards are temporarily taken out of service. This clears down all calls over these boards but does not

have any other visible effect. What causes this problem and what can be done about it?

Answer: A statistical evaluation of error messages is performed for the HG 3500/75 in the same way as for other boards. This also includes the loss of the signaling connection in HG 3575 and “bad quality“ messages for the HG 3500/75 payload connections.

Poor IP connection quality between the HG 3500/75 gateways or the OpenScape 4000 central system and the HG 3575 over a sustained period can lead to a large number of error messages in a short space of time, which in the end causes a statistic overflow and a board reset.

Resetting the board should prevent a temporary board fault from turning into a problem.

If the fault clearly originates in the network, no improvements will be achieved by resetting the board.

You can use the AMO PSTAT to increase the threshold values for the STMI and NCUI counters or deactivate the statistical evaluation entirely by setting the threshold values to zero.

```
CHANGE-
PSTAT:TYPE=CTRLTAB,LEVEL=BOARD,BOARD=NCUI,FAULT=1 or 2,
MAXCOUNT=xxx;
```

Stage 1 (COUNT1, counts pairs of in-service and out-of-service messages) and stage 2 (COUNT2, counts messages that could develop into a message flood) should also be taken into consideration.

Separate counters are used for NCUI/STMI and NCUI2/STMI2

NCUI STMI	COUNT1	Byte1	61	10	2	4
	COUNT2	Byte2	61	6	2	2
	COUNT3	Byte3	21	10	2	4
	COUNT4	Byte4	19	10	2	4
NCUI2 STMI2	COUNT1	BYTE1	241	10	2	4
	COUNT2	Byte2	241	6	2	2
	COUNT3	Byte3	21	10	2	4
	COUNT4	Byte4	19	10	2	4

Details on the AMO PSTAT can be found in the AMO description in the OpenScape 4000 Service Manual.

Modifying the statistics prevents the boards from being reset when quality problems that affect the overall function of the system occur in the IP network. Your objective must be get these problems under control.

10) **Question:** Where can I hear how packet loss concealment affects the G.711 or G.729 codec?

    The suggestion to provide acoustic samples in the electronic version of the handbook was rejected by Service and Sales because this information is not relevant for service technicians and sales managers. Sorry!

11) **Question:** Which is the difference between TOSLAN, **TOSSIGNL** and **TOSPL**?

AMO SIPCO	
TOSSIGNL	QoS value for the TCP stream from HSR > NCUIs
TOSPL	QoS value for the payload stream outgoing from the IPDA-STMI (HHS)
AMO STMIB	
TOSLAN	QoS value for the TCP stream from NCUI > HSR
TOSPL	QoS value for the payload stream outgoing from the NCUI
AMO CGWB	
TOSSIGNL	QoS value for the TCP stream from STMI > STMI (IP Trunking) or STMI > IP-Phone
TOSPL	QoS value for the payload stream outgoing from the STMI (HFA/IP Trunking)

Notes:

If MFS is used with IPDA functionality then the TOSPL (AMO SIPCO & AMO CWGB) must be the same.

The TOS values for the packets sent by the IP phone can be setup in the IP phone only.

3 OpenScape 4000 SoftGate

3.1 Overview

3.1.1 Functional Overview

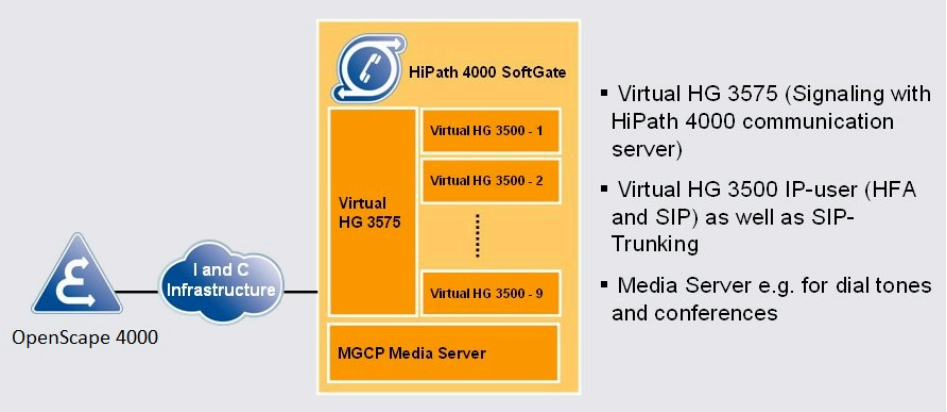


Figure 45: Topology

The OpenScape 4000 SoftGate provides cost-effective branch offices with reliable OpenScape 4000 survivability options and an easy IT integration in the OpenScape 4000 solution and management suite. This software application offers full HiPath Feature Access (HFA) for IP Endpoints, SIP Service Provider connectivity and native SIP connectivity for trunking and subscriber with basic feature set based upon a standard x86 server with Linux.

Any OpenScape 4000 SoftGate site integrates seamless in the communication system and network like an IPDA Access Point (AP 3700 IP) - in terms of features and administration.

With this application customers can reduce capital cost (CAPEX) plus operational cost (OPEX) and deploy centralized applications with uniform user experience.

3.1.2 Variants

With OpenScape 4000 V8 only one SoftGate Application ordering number is available.

The older SoftGate variants OpenScape 4000 SoftGate can still be seen and configured in the system, e.g. when upgrading from V7 to V8:

- OpenScape 4000 SoftGate 50 Up to 50 ports for IP subscribers (HFA and SIP subscribers) or SIP trunking (native SIP / SIP-Q).
- OpenScape 4000 SoftGate 500 Up to 500 ports for IP subscribers (HFA and SIP subscribers) or SIP trunking (native SIP / SIP-Q).
- OpenScape 4000 SoftGate 1000 Up to 1000 ports for IP subscribers (HFA and SIP subscribers) or SIP trunking (native SIP / SIP-Q)/a maximum number of 256 active ports.

With OpenScape 4000 V8 R2 it is possible to configure and start a SoftGate instance on a running Enterprise Gateway or Survivable Enterprise Gateway. This additional SoftGate is called "Integrated SoftGate" or sometimes in short "iSoftGate", it is running inside a Linux Container and it is acting and supporting most of features like any Standalone SoftGate.

With OpenScape 4000 V10 R1 it is possible to configure and start a SoftGate instance on both nodes of a Duplex or separated Duplex System. This additional SoftGate is called "Integrated SoftGate" or sometimes in short "iSoftGate", it is running inside a Linux Container and it is acting and supporting most of features like any Standalone SoftGate.

3.1.3 Features

OpenScape 4000 SoftGate offers the following features:

- Runs on standard server hardware.
- Operated with the Suse Linux Enterprise Server (SLES) operating system.
- Integrated media server.
- Administration via OpenScape 4000 Assistant/Manager.
- Integration in OpenScape 4000 networks.
- Supports all functions of IP Distributed Architecture (IPDA) (see Chapter 1, “IPDA Feature Description”).
  - Supports OpenScape 4000 IPDA survivability options: signaling survivability and connection to existing AP emergency servers.
  - Supports a/µ law conversion per OpenScape 4000 SoftGate. For more information on a/µ law conversion please refer to the service manual **“OpenScape 4000 V/, Section 4- IP Solutions > IP Distributed Architecture”**.
- Each OpenScape 4000 SoftGate has the following sources available:
  - 64 TSLs for conference
  - 32 receivers for DTMF signaling (CR)
  - 32 sender for DTMF signaling (CS)
  - 2 continuous-tone dial tone receivers (DTR-DT)
  - 2 cadenced-tone dial tone receivers (DTR-TT)
  - 2 test receivers (TESTR)
  - 1 test sender (TESTS)
  - up to 18 different tones and 6 different announcements (for a detailed description please refer to **IP Distributed Architecture >** Section 2.16, “Different Announcements, Tones and DTMF DialTone Receivers per Access Point”.)
  - 5 different display languages/national character sets different to the host system and/or different for each OpenScape 4000 SoftGate (for a detailed description please refer to **IP Distributed Architecture >** Section 2.17, “Different Languages/ National Character Sets for Displaying Text for Individual Access Points”.)
  - 1 music on hold
  - 1 TDS port
- Maximum number of parallel calls: 250
- Supports DMC - OpenScape 4000 SoftGate is DMC endpoint (see “Payload Switching DMC”, Chapter 4, “Direct Media Connect (DMC) in Connection with OpenScape 4000 SoftGate”). Activation of DMC does not cause a channel reduction like in STMI/NCUI, as

DSPs are software not hardware based. Maximum number of calls remains as configured, with or without DMC.

- Supports T.38 Fax (see T.38 Fax).
- Supports signaling and payload encryption
- More information about “Signaling and Payload Encryption (SPE)” can be found in the respective section.
- Supports ISDN calls in the public network. PSTN connections are conducted via Mediatrix SIP gateways.
- Analogue and fax connection
  - via AP 3700 in conjunction with OpenScape 4000 SoftGate 1000.
  - via Mediatrix 41xx SIP gateway in conjunction with OpenScape 4000 SoftGate 50 (see Section 3.3.5, “Analog Stations (Mediatrix 41xx)”).
- S0 connection via Mediatrix 44xx SIP gateways:
  - S0 subscriber: Section 3.3.1, “ISDN (S0) Subscriber (Mediatrix 44xx)”
  - S0 trunking: Section 3.3.2, “S0 Trunking (Mediatrix 44xx)”
  - S0 data connection: Section 3.3.3, “ISDN (S0) Data Connections (Mediatrix 44xx)”
- Mediatrix 35xx for PRI interface for T1.
- Mediatrix 36xx for PRI interface (see Section 3.3.4, “S2 Interface (Mediatrix 36xx)”) for E1.
- Mediatrix 1204 for analog trunking (see Section 3.3.6, “Analog Trunking (Mediatrix 1204)”).
- Video integration with LifeSize terminals (see Chapter 5, “Video Connections”).
- Supports native SIP and SIP-Q trunking.
- IPv6 for SIP-Q and native SIP trunking with OpenScape 4000 SoftGate (see Chapter 12, “IPv6”).
- End-to-end payload connections between native SIP trunks and SIP stations.
- Native SIP trunking enhancements:
  - configurable voice codecs for HG 3500 per destination gateway or IP sub network
  - native SIP trunking features: message waiting indication, call transfer and call forwarding
- SIP service provider connections are possible.
-

  NOTICE: The firewall and SBC (session border control) configuration is dependent on the customer network and NAT (network address translation).

- HiPath Cordless IP V1 has been released for connection to the OpenScape 4000 SoftGate (see HiPath Cordless IP).
- For increased resilience, OpenScape 4000 SoftGate can be connected with two LAN cables to different switches/router (see Chapter 6, “LAN Redundancy”).
- Gatekeeper Redundancy for HFA Subscriber (see Chapter 10, “Gatekeeper Redundancy for HFA/ SIP Subscriber”).
- Survivable OpenScape 4000 SoftGate (see Chapter 11, “Survivable OpenScape 4000 SoftGate”).
- SIP Load balancing for inbound native SIP trunks. With load balancing the system is to be able to scale the performance of involved SIP servers, to

avoid overloading of the server and to achieve high availability of the SIP services (see Chapter 13, “Load Balancing”).

- OpenScape Access modules can be connected directly to the OpenScape 4000 SoftGate. For information on licensing see OpenScape Access/Branch service documentation.
- With the release of OpenScape Access/Branch the vNCUI can act as (secure) DMC endpoint.
- QDC is supported.
- OpenScape Cordless E Integration (see Chapter 17, “OpenScape Cordless E Integration”).
- MFC-R2 support (see Chapter 16, “MFC-R2”).
- 16 peripheral slots for virtual boards and OpenScape Access modules
- Each virtual board within the OpenScape 4000 SoftGate uses one slot of it. Due to the enhanced number of slots, the installation of virtual boards consumes no longer hardware slots on OpenScape Access and OpenScape 4000 SoftGate.

  For traces please make sure that the assignment between slot and PBC number is correct (see Section 1.8, “Hints for Diagnosis regarding the peripheral Slots”).

3.1.4 LAN Interfaces

The OpenScape 4000 SoftGate offers the following LAN interfaces:

- IPDA LAN
- For connecting to the OpenScape 4000 host system.
- Management LAN
- The feature "Separate LAN Connectivity for Administration and Voice Over IP" is supported. The Voice LAN can now be split fully from the Management LAN.
- WAN
- The OpenScape 4000 SoftGate offers a WAN interface to the Internet.

  You can find a scenario using the WAN interface of the OpenScape 4000 SoftGate in Chapter 14, “Secure Remote Subscriber”.
- Signaling Survivability
- A LAN interface for signaling survivability is supported.
- XLINK
- The XLINK interface is used for OpenScape Access/Branch and RG 8350 A.

  The only official way to configure/reconfigure LAN interfaces is using the firstinstall XML file. This includes Bitrate, Bond, VLAN and IP configuration. The XML file is used during first installation or when calling the Recovery Tool. For further details please refer to the documentation “OpenScape 4000, Installation, Configuration and Migration, Installation Guide”.

NOTICE: Should different VLANs be required for individual vSTMI boards of the SoftGate, then the SoftGate LAN interface must be selected as eth<n> or bond<n>. Afterwards any appropriate LAN interface tagging must be configured under the AMO interface. The SoftGate LAN interface can be selected in either the Portal (SoftGate LAN Wizard) or through XML configuration. If the requirement is that all traffic

from the SoftGate is used within the same VLAN, it is also possible to select vlan<n> as the SoftGate interface. No AMO VLAN configuration is required either for this second use case, but the prerequisite is the VLAN must be specified as an interface in the XML installation file.

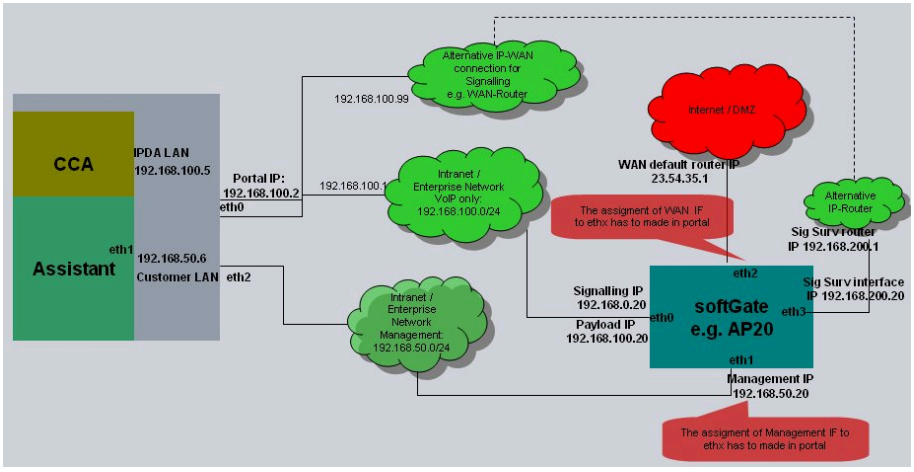


Figure 46: LAN interfaces of OpenScape 4000 SoftGate

3.1.5 Ports

see “Gateways HG 3500 and HG 3575 > Chapter “IP Ports””.

3.1.6 Advantages

OpenScape 4000 SoftGate benefits compared with existing branch scenarios:

Table 16: OpenScape 4000 SoftGate advantages compared with existing branch scenarios

Existing branch scenarios	OpenScape 4000 SoftGate benefits
Remote IP endpoints	• Local PSTN connection, local a/b-connection • Hot- signaling survivability • Less WAN bandwidth between headquarter and branch
Small remote side branch with HiPath 2000 or HiPath 3000	• Centralized switch architecture • Homogenous management with OpenScape 4000 Administration • Homogenous applications • Less WAN bandwidth between headquarter and branch

Existing branch scenarios	OpenScape 4000 SoftGate benefits
IPDA access point	• No proprietary hardware • More effective TCO • Video endpoints

3.1.7 Restrictions

For all variants of OpenScape 4000 SoftGate:

- For signaling survivability no other ISDN modems as released for OpenScape 4000 will be supported.
- Analogue modem connectivity is not supported.
- Codec G.723 is not supported.
- The following restrictions apply when connecting to CO over Mediatrix gateways:
  - Accounting is not supported.
  - Callback functionality not supported.
- A maximum number of 83 OpenScape 4000 SoftGates 50/1000 or IP Access Points can be connected to one OpenScape 4000 system.
- Limitations to DMC (see “Payload Switching DMC”, Chapter 4, “Direct Media Connect (DMC) in Connection with OpenScape 4000 SoftGate”):
  - End-to-end payload can also be achieved to a native SIP trunk (depending on the trunk profile).
  - The MediaCapabilities (e.g. codecs) can be renegotiated/changed between the SIP partners (on the OpenScape 4000 SoftGate) even after the DMC connection has been established.
  - If a SIP device or a SIP native trunk on the 4000 SoftGate communicates with an DMC endpoint (not the DMC proxy!), then a MediaRelay is activated between them on the OpenScape 4000 SoftGate. This corresponds to an RTP proxy which always routes the media stream (RTP) via the OpenScape 4000 SoftGate.
  - If a SIP device or SIP native trunk on the OpenScape 4000 SoftGate communicates with a DMC proxy on the common gateway, then the MediaCapabilities are passed on transparent and an E2E payload connection is established. However due to the restrictions of the DMC proxies on the CGW, it is not possible to renegotiate codecs.

For OpenScape 4000 SoftGate 50 only:

- Provider access requires OpenScape Access modules or direct SIP provider connections.

For OpenScape 4000 SoftGate 1000 only:

- Signaling Survivability via PSTN network is not supported for OpenScape 4000 SoftGate 1000.
- Provider access requires AP 3700 IP or direct SIP provider connections.

For Integrated SoftGate on Enterprise Gateway:

- XLink is not supported

- date, time and timezone are the same as the Enterprise Gateway on which the Integrated SoftGate is running
- Signaling Survivability via PSTN network is not supported
- iSG must be have the same connection type as the EntGW/SurvEntGW (AMO-UCSU: CONNTYPE =APNW/APDL)

3.1.8 Hints for Diagnosis regarding the peripheral Slots

Slot number and PBC numbers differ. Please refer to the following tables for a correct assignment.

Slot	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17
PBC	1	2	3	4	5	21	9	10	11	12	13	14	15	16	6	7	8
Quarter	1.				2.	---	3				4				2.		

PBC	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	21
Slot	1	2	3	4	5	15	16	17	9	10	11	12	13	14	15	16	6
Quarter	1.				2.				3.				4.				---

3.1.9 Hardware Requirements

Please refer to the White List for the latest hardware requirements for a OpenScape 4000 SoftGate server. The White List is part of the latest Release Note.

3.2 OpenScape 4000 SoftGate Upgrade

The functionalities of both the virtual HG 3575 and the virtual HG3500 (HFA/SIP) are contained in the OpenScape 4000 SoftGate image. All functionalities are therefore always upgraded at the same time in a OpenScape 4000 SoftGate upgrade.

The upgrade is performed either via **LW Update Manager** (see Section 2.1, “Upgrade via Loadware Update Manager”) or via the board’s local **WBM** application (see Section 2.2, “Upgrade via the Local WBM in OpenScape 4000 SoftGate”).

3.2.1 Upgrade via Assistant Gateway Manager

The OpenScape 4000 SoftGate image can be transferred either with the LW Update Manager or with the PCHI tool on the RMX hard disk.

- OpenScape 4000 SoftGate image (RPM format with OMF 386 header):
- `softgate-5.0-0.i586.rpm.abs`
- Directory on the RMX hard disk:

- `:A1H1E:/APSP/LTG/LGA0/`

  under:

  `PZKSGW50`

LW Update Manager

1) Start the file transfer operation with the OpenScape 4000 Assistant Gateway Manager:

OpenScape 4000 Assistant > Expert Mode > LW Update Manager

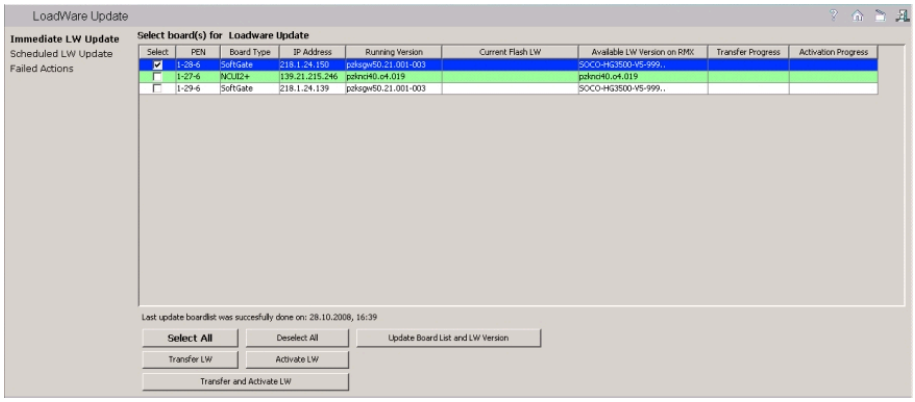


Figure 47: OpenScape 4000 Assistant: Loadware Update

2) Select the OpenScape 4000 SoftGate that you want to upgrade from the list of boards.

3) The following options are now available:

- **Transfer LW** button: The loadware is transferred but not activated. You can press the **Activate LW** button either now or later to activate the loadware on the required boards.
- **Transfer and Activate LW** button: The loadware is transferred and activated.

IMPORTANT: Please note that the board is briefly removed from service when the loadware is being activated.

3.2.2 Upgrade via the Local WBM in OpenScape 4000 SoftGate

1) Activate the local Web-Based Management application.

   To do this, select **OpenScape 4000 Assistant > Expert Mode > Gateway Dashboard** or activate the application in the browser with the IP address of OpenScape 4000 SoftGate, e.g. https://218.1.24.139.

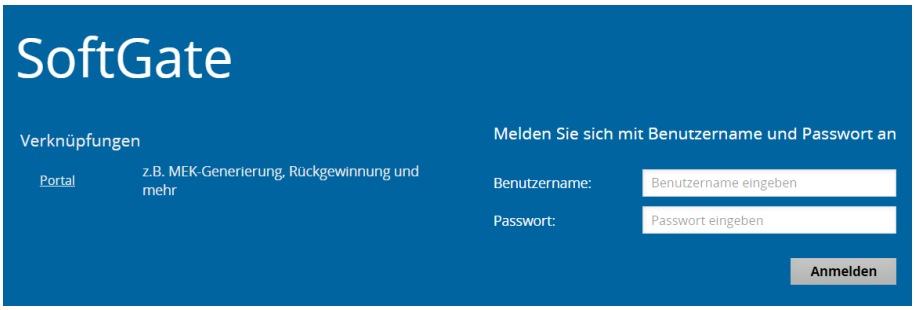


Figure 48: WBM - Login

2) Log on with user: **TRM**, ... and the corresponding password.

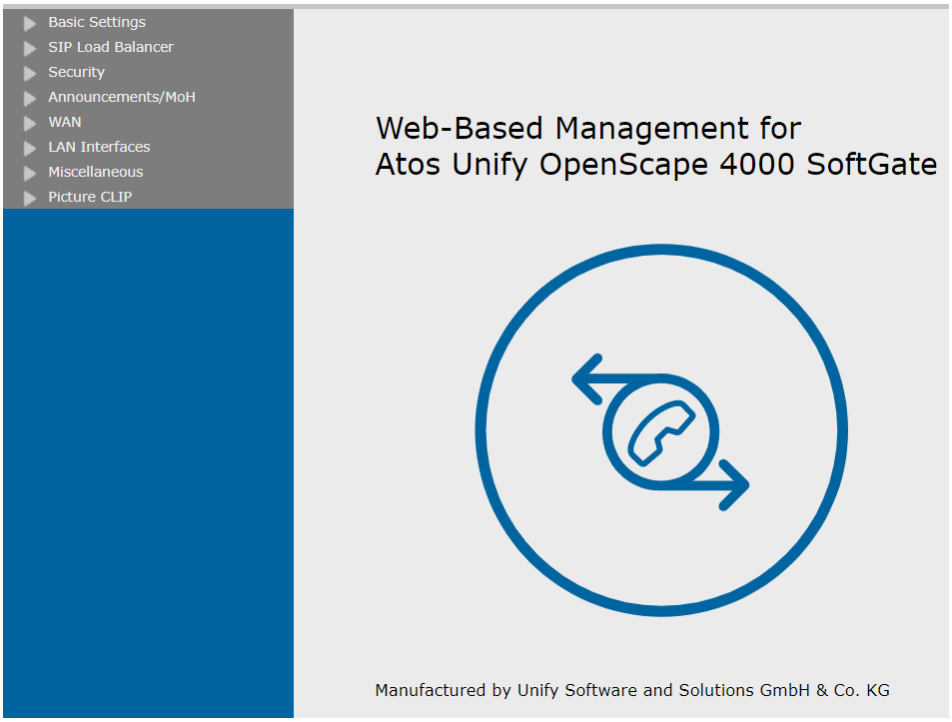


Figure 49: WBM - Start page

1) Select the menu **SW-Update**

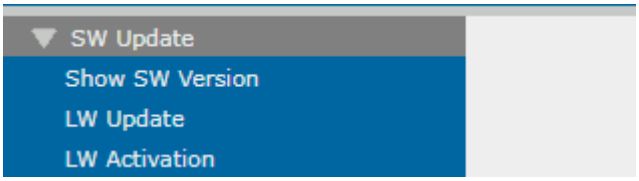


Figure 50: WBM - Software Update

1) Transfer the OpenScape 4000 SoftGate image with an OMF 386 header:

2) `softgate-5.0-0.i586.rpm.abs`

Select the **Software Update** function.

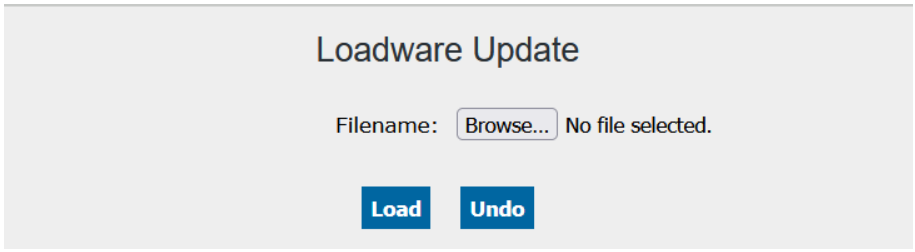


Figure 51: WBM - Software Update

3) Click the **Browse** button to enter the OpenScape 4000 SoftGate image in the "Filename" field.

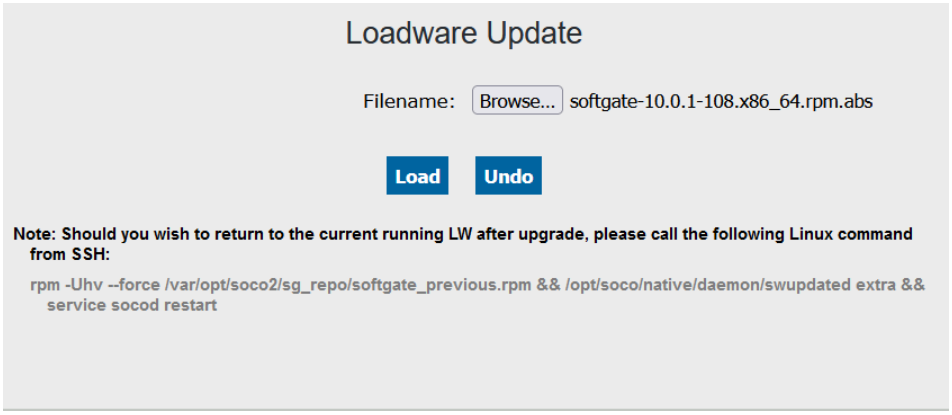


Figure 52: WBM - Software Update: Entering a file

1) Press **Load** to load the OpenScape 4000 SoftGate image.
2) Activate the new software.
3) After the upload of the image has finished, the screen for activating the new software appears automatically.

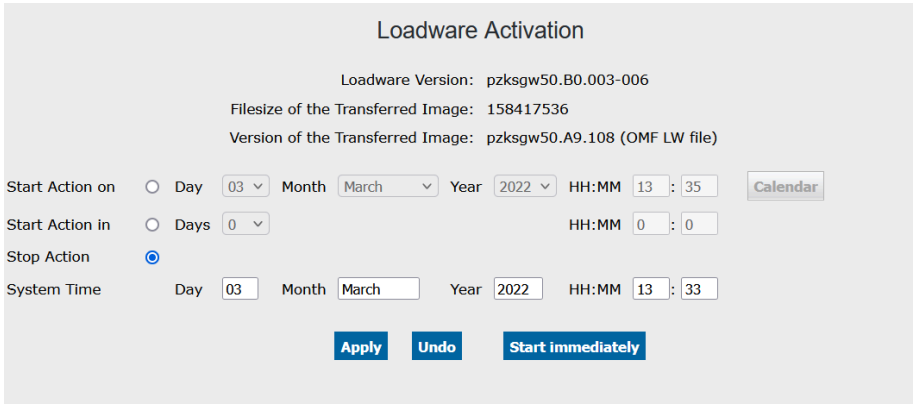


Figure 53: WBM - Software Activation

You now have the possibility to activate the new OpenScape 4000 SoftGate image immediately (with the button Start Immediately) or to schedule the activation for later (enter the desired date and time in the screen and press **Apply**).

3.3 Mediatrix Gateways

3.3.1 Released Mediatrix Gateways

- Mediatrix 4402 Advance: 2x BRI (Basic Rate Interface = ISDN S0) (native SIP Trunking)
  - Section 3.3.1, “ISDN (S0) Subscriber (Mediatrix 44xx)”
  - Section 3.3.2, “S0 Trunking (Mediatrix 44xx)”
  - Section 3.3.3, “ISDN (S0) Data Connections (Mediatrix 44xx)”
- Mediatrix 4404 Advance: 4x BRI (Basic Rate Interface = ISDN S0) (native SIP Trunking)
  - Section 3.3.1, “ISDN (S0) Subscriber (Mediatrix 44xx)”
  - Section 3.3.2, “S0 Trunking (Mediatrix 44xx)”
  - Section 3.3.3, “ISDN (S0) Data Connections (Mediatrix 44xx)”
- Mediatrix 35xx (2x ISDN PRI =Primary Line Interface) for T1
- Mediatrix 3631 (1x ISDN PRI =Primary Rate Interface) for E1
  - Section 3.3.4, “S2 Interface (Mediatrix 36xx)”
- Mediatrix 3632 (2x ISDN PRI =Primary Line Interface) for E1
  - Section 3.3.4, “S2 Interface (Mediatrix 36xx)”
- Mediatrix analog adapter 4104, 4108, 4116, 4124 (analog stations)
  - Section 3.3.5, “Analog Stations (Mediatrix 41xx)”
- Mediatrix 1204 (analog trunking)
  - Section 3.3.6, “Analog Trunking (Mediatrix 1204)”

3.3.2 Configuration Notes

IMPORTANT: For information on how to configure gateways for the first time with the IP address, etc., refer to the documentation supplied with the Mediatrix gateways. The screenshots displayed depict the Mediatrix gateway’s web interface. More information is available directly from Mediatrix at: http://www.mediatrix.com or https://support.mediatrix.com/DownloadPlus/Download.asp

IMPORTANT: G.711 must always be configured wether T.38 will be used or G.729. This restriction is valid for all Mediatrix gateways connected directly to an OpenScape 4000 system or connected via an OpenScape Voice system at an OpenScape 4000 system.

3.3.3 Configuration Examples

This section describes, using screenshots, how to configure specific Mediatrix gateway parameters based on a specific application scenario.

3.3.3.1 ISDN (S0) Subscriber (Mediatrix 44xx)

A Mediatrix 4400 gateway can simultaneously support both an ISDN subscriber line and a line to the private network.

3.3.3.1.1 Requirements

- Every station at a Mediatrix gateway must be configured as an SIP subscriber in the OpenScape 4000.
- Mediatrix 44xx gateways do not support telephony features for ISDN phones.
- Refreshing is not supported for ISDN phone displays.
- ISDN connections are only supported if Mediatrix 44xx gateways are used.
- ISDN voice connections are only supported for stations or trunks that are configured on the same OpenScape 4000 SoftGate.
- Subscriber calls (i.e. for incoming calls from Mediatrix gateway subscribers) always have to supply their calling number (internal/extension number).
  - If the ISDN terminal does not do this, calling number insertion can also be configured in the Mediatrix gateway as required. A configuration of this kind is possible in the Mediatrix gateway (e.g. based on the ISDN port).
  - The connection of multiple ISDN subscribers via an ISDN bus to a Mediatrix gateway ISDN port may not be straightforward – unless a distinction can be made between the subscribers based on call type (bearer type).

3.3.3.1.2 Sample Scenario with Mediatrix 4402 Gateway

In this sample scenario a Mediatrix gateway is used for subscribers.

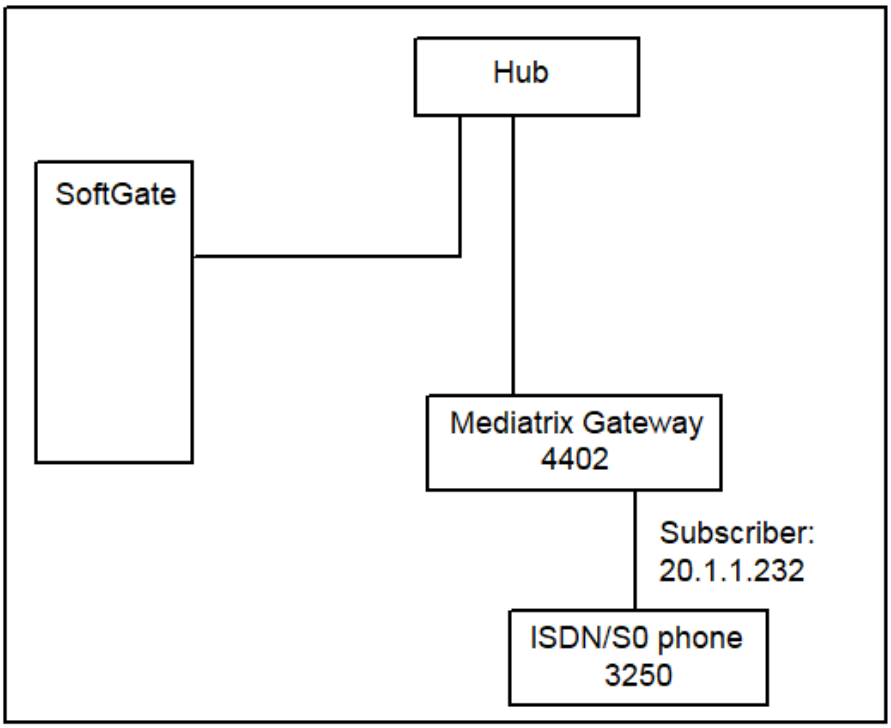


Figure 54: OpenScape 4000 SoftGate scenario with Mediatrix gateway - S0 subscriber

3.3.3.1.3 Configuration

The figures in this section depict the configuration in the sample scenario.

Overview

- Network -> Host
- Network -> Interfaces
- SIP -> Gateways
- SIP -> Servers
- SIP -> Registrations
- ISDN -> Basic Rate Interface
- Telephony -> Call Routing Config

Network -> Host

Set **Static** for the host domain, the default gateway, the DNS source and the SNTP source.

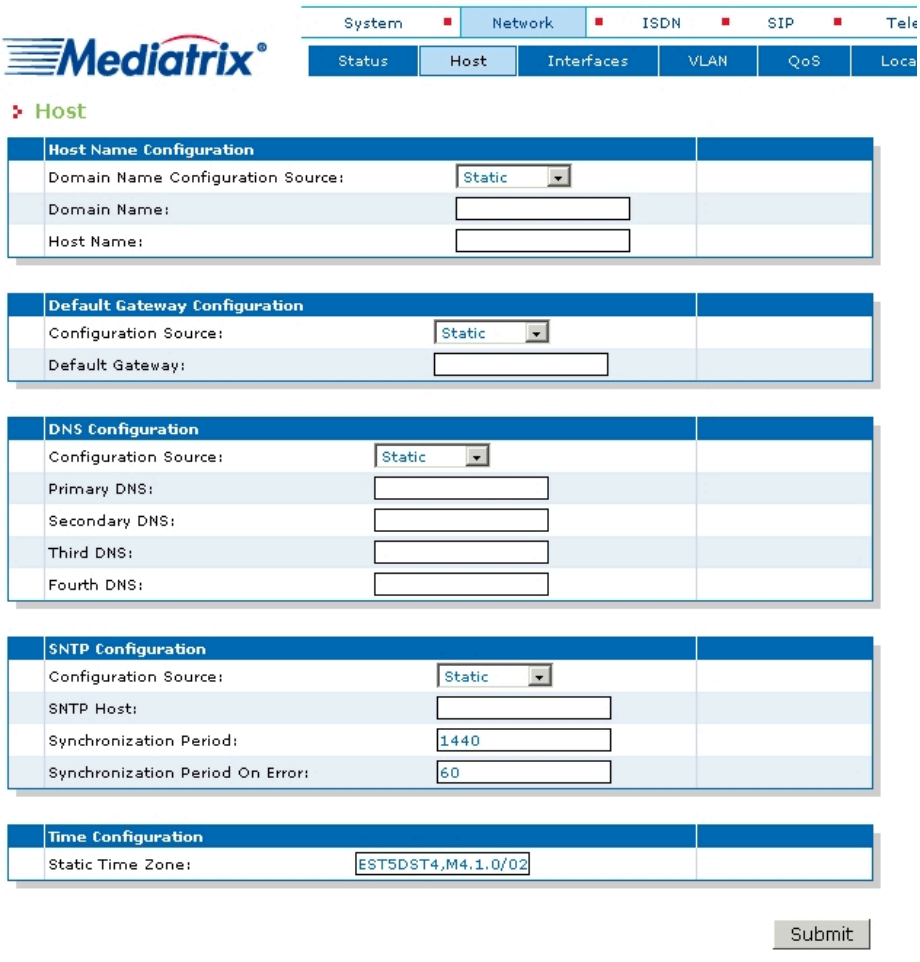


Figure 55: Mediatrix 44xx Gateway (Subs.) - Network -> Host

Network -> Interfaces

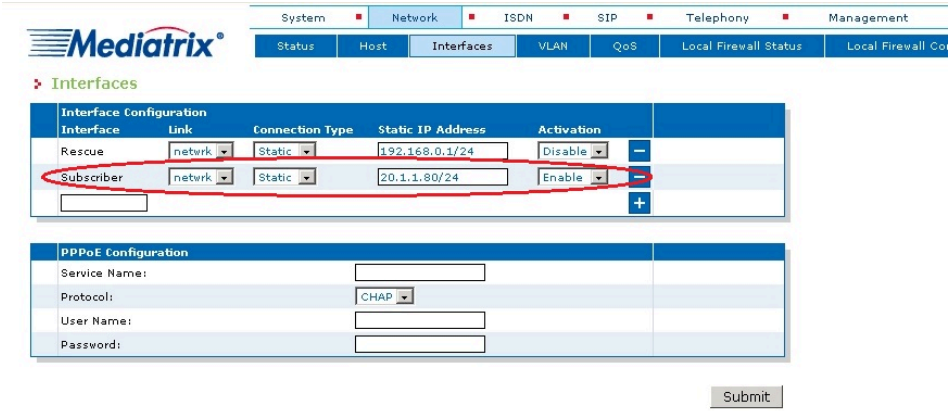
The network interfaces should be configured with unique LAN IP addresses. A Mediatrix 4400 gateway can support up to 48 network interfaces.

IMPORTANT: Care must be taken when assigning IP addresses to ensure that they can be reached by OpenScape 4000 SoftGate.

A OpenScape 4000 SoftGate (or vHG3500)can only operate one network interface in the Mediatrix gateway. It may be necessary to configure subscriber and trunking scenarios over a network interface.

Configure a "subscriber interface" in this mask.

IMPORTANT: The name "Subscriber" can be chosen at random and does not yet define usage.



Mediatrix 44xx Gateway (Subs.) - Network -> Interfaces

SIP -> Gateways

Select the value **Subscriber** in the "SIP Gateway Configuration" field.

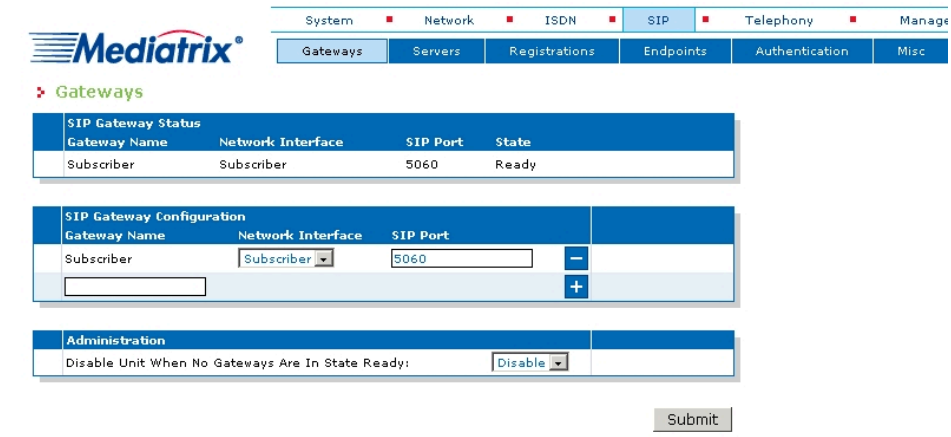


Figure 56: Mediatrix 44xx Gateway (Subs.) - SIP -> Gateways

SIP -> Servers

Enter values for "Registrar Host " and "Proxy Host" in the "SIP Default Servers" field.

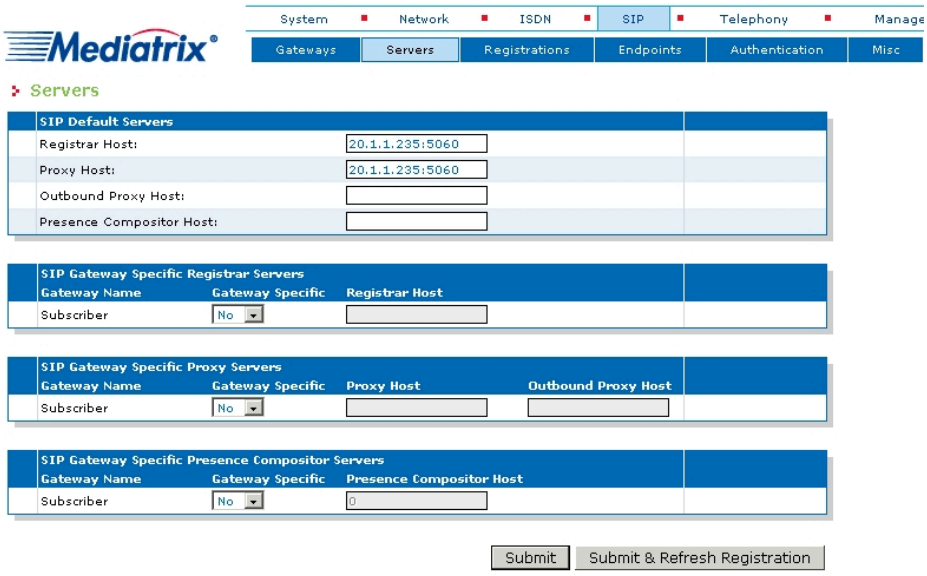


Figure 57: Mediatrix 44xx Gateway (Subs.) - SIP -> Servers

SIP -> Registrations

Enter the phone numbers of the ISDN stations for registration at the SIP server. Add the subscriber terminals and select the SoftGate subscriber. The "User Name" field contains the telephone number.

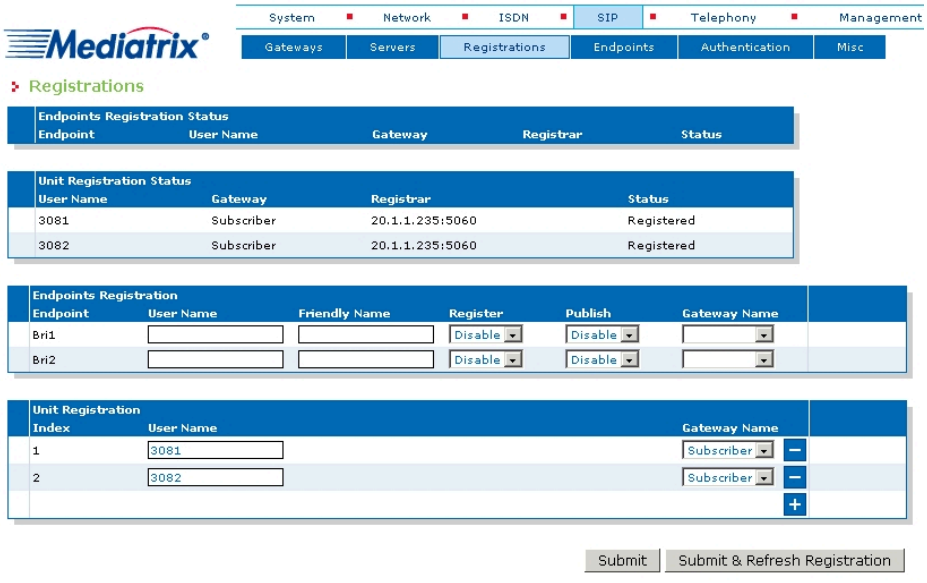


Figure 58: Mediatrix 44xx Gateway (Subs.) - SIP -> Registrations

ISDN -> Basic Rate Interface

Configure the ISDN parameters for every interface that should be used.

- Endpoint Type: **NT**
- Connection Type: e.g.: **Point To Multipoint**

In a subscriber-only scenario, the other interfaces are generally identical to the first one. "Exclusive B-Channel Selection" is usually enabled.

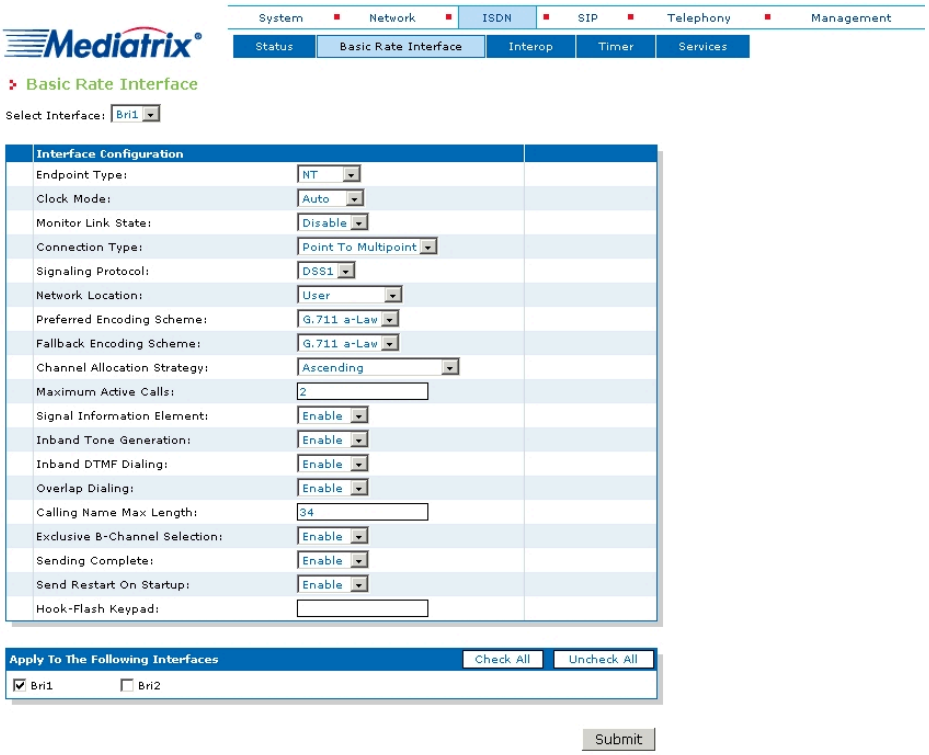
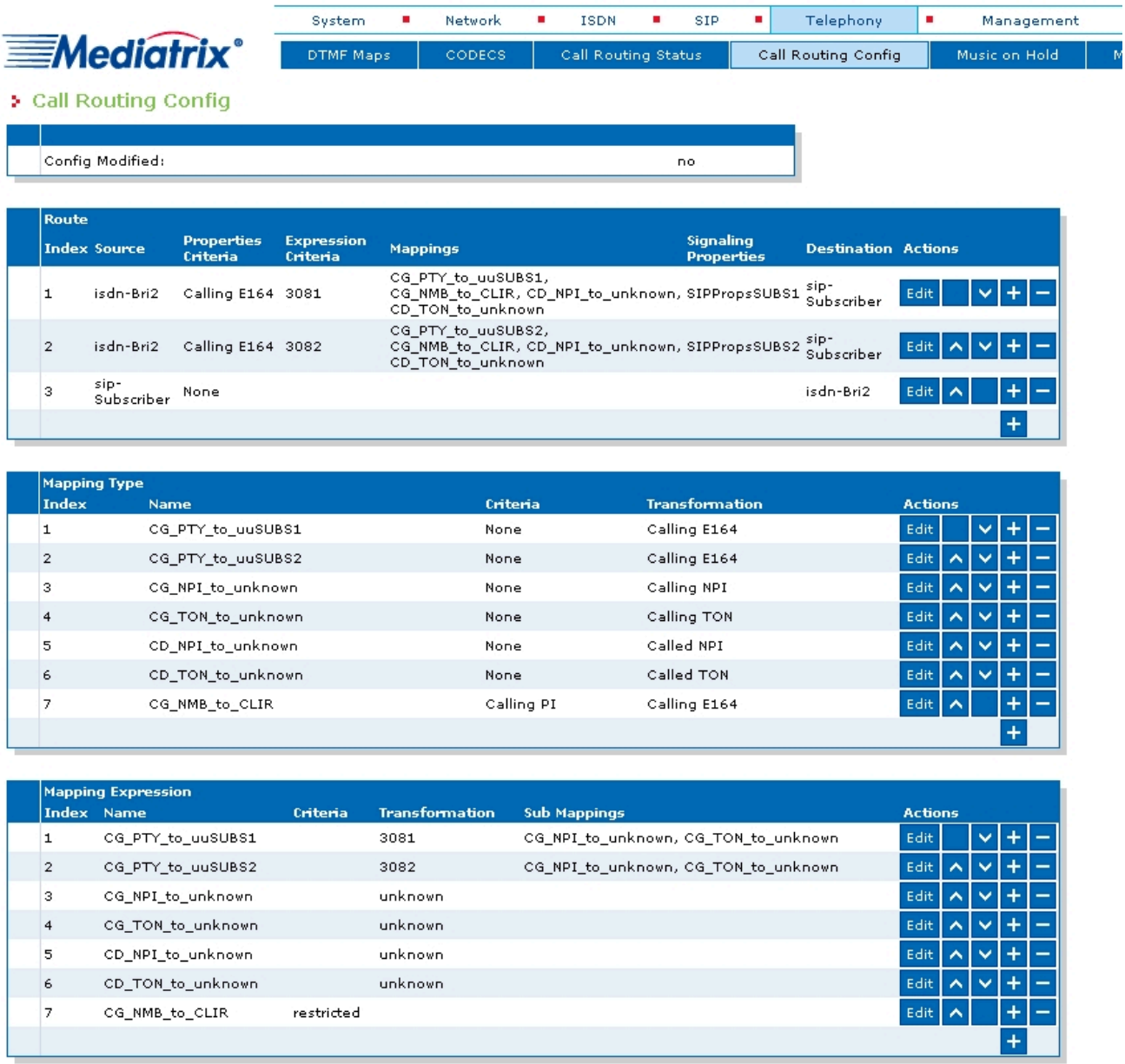


Figure 59: Mediatrix 44xx Gateway (Subs.) - ISDN -> Basic Rate Interface

Telephony -> Call Routing Config

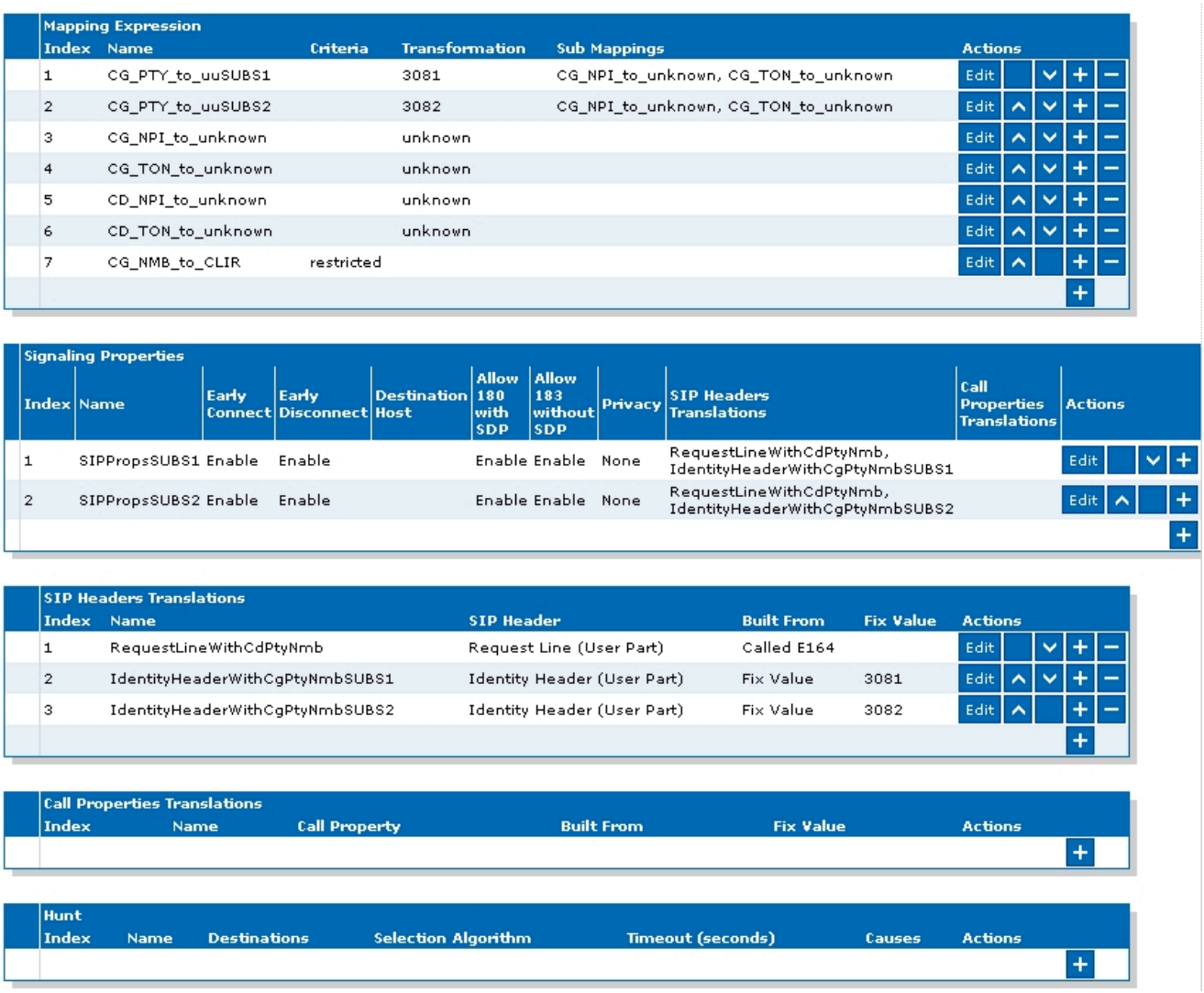
Use this mask to define how calls from/to the VoIP network should be routed to the ISDN telephones.

The example shows a configuration with two stations (3081 and 3082), which are both connected over an ISDN bus to the gateway's BRI2. This example assumes that both subscribers supply their station numbers. This example shows a number of exceptional configurations for CLIR that are usually only used very rarely. The Mediatrix gateway also has a default selection for using CLIR.



Mediatrix 44xx Gateway (Subs.) - Telephony -> Call Routing Config 1

The "RequestLineWithCdPtyNmb" configuration may be needed in certain situations for SIP protocol synchronization between the Mediatrix gateway and OpenScape 4000 SoftGate.



Mapping Expression

Index	Name	Criteria	Transformation	Sub Mappings	Actions
1	CG_PTY_to_uuSUBS1		3081	CG_NPI_to_unknown, CG_TON_to_unknown	Edit
2	CG_PTY_to_uuSUBS2		3082	CG_NPI_to_unknown, CG_TON_to_unknown	Edit
3	CG_NPI_to_unknown		unknown		Edit
4	CG_TON_to_unknown		unknown		Edit
5	CD_NPI_to_unknown		unknown		Edit
6	CD_TON_to_unknown		unknown		Edit
7	CG_NMB_to_CLIR	restricted			Edit

Signaling Properties

Index	Name	Early Connect	Early Disconnect	Destination Host	Allow 180 with SDP	Allow 183 without SDP	Privacy	SIP Headers Translations	Call Properties Translations	Actions
1	SIPPropsSUBS1	Enable	Enable		Enable	Enable	None	RequestLineWithCdPtyNmb, IdentityHeaderWithCgPtyNmbSUBS1		Edit
2	SIPPropsSUBS2	Enable	Enable		Enable	Enable	None	RequestLineWithCdPtyNmb, IdentityHeaderWithCgPtyNmbSUBS2		Edit

SIP Headers Translations

Index	Name	SIP Header	Built From	Fix Value	Actions
1	RequestLineWithCdPtyNmb	Request Line (User Part)	Called E164		Edit
2	IdentityHeaderWithCgPtyNmbSUBS1	Identity Header (User Part)	Fix Value	3081	Edit
3	IdentityHeaderWithCgPtyNmbSUBS2	Identity Header (User Part)	Fix Value	3082	Edit

Call Properties Translations

Index	Name	Call Property	Built From	Fix Value	Actions

Hunt

Index	Name	Destinations	Selection Algorithm	Timeout (seconds)	Causes	Actions

Mediatrix 44xx Gateway (Subs.) - Telephony -> Call Routing Config 2

3.3.3.2 S0 Trunking (Mediatrix 44xx)

A Mediatrix 4400 gateway can simultaneously support both an ISDN subscriber line and a line to the private network.

3.3.3.2.1 Requirements

- ISDN connections are only supported if Mediatrix 44xx gateways are used.
- ISDN voice connections are only supported for stations or trunks that are configured on the same OpenScape 4000 SoftGate.
- All gateways should be synchronized with a common clock. For instance, the gateways receive the clock pulse via a direct connection to the public network or via an internal ISDN S0 line (layer-0 connection) to another synchronized gateway, as shown in the sample scenario.

3.3.3.2.2 Sample Scenario with Mediatrix 4402 Gateway

In this sample scenario a Mediatrix gateway is used for s trunking to the public network.

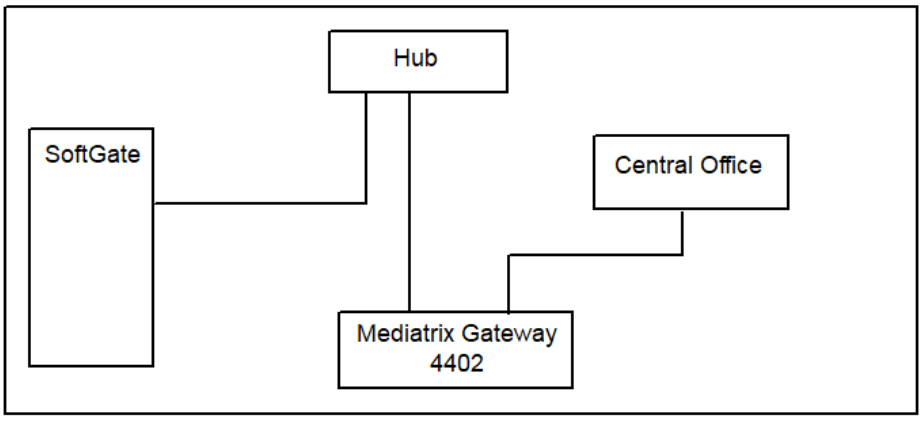


Figure 60: OpenScape 4000 SoftGate scenario with Mediatrix gateway - Trunking

3.3.3.2.3 Configuration

The figures in this section depict the configuration in the sample scenario.

Overview

- Network -> Host
- Network -> Interfaces
- SIP -> Gateways
- SIP -> Servers
- SIP -> Registrations
- ISDN -> Basic Rate Interface
- Telephony -> Call Routing Config

Network -> Host

Set **Static**

- in the section **Host Name Configuration** for **Domain Name Configuration Source**,
- in the section **Default Gateway Configuration** for **Configuration Source**,
- in the section **DNS Configuration** for **Configuration Source** and
- in the section **SNTP Configuration** for **Configuration Source**.

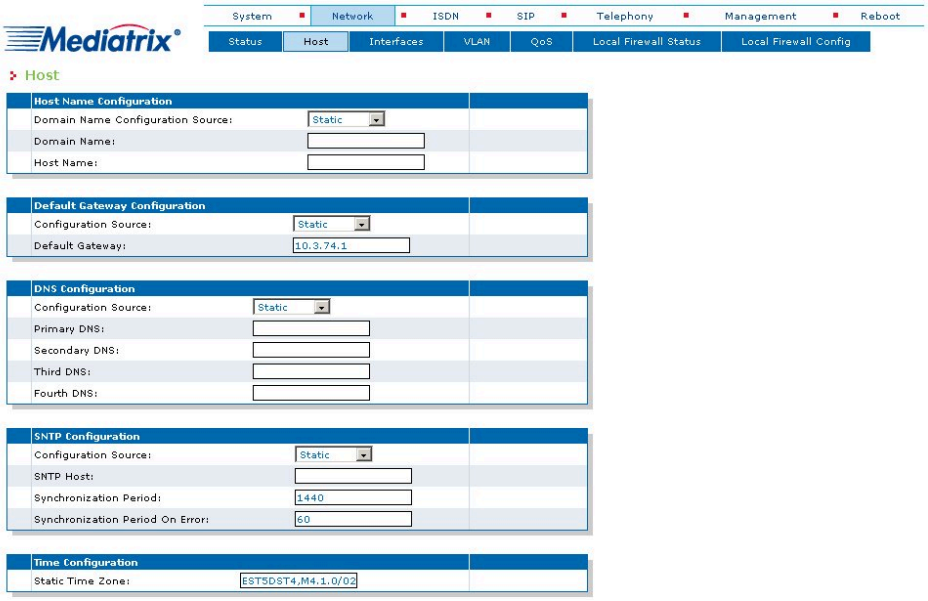


Figure 61: Mediatrix 44xx Gateway (Trunking) - Network -> Host

Network -> Interfaces

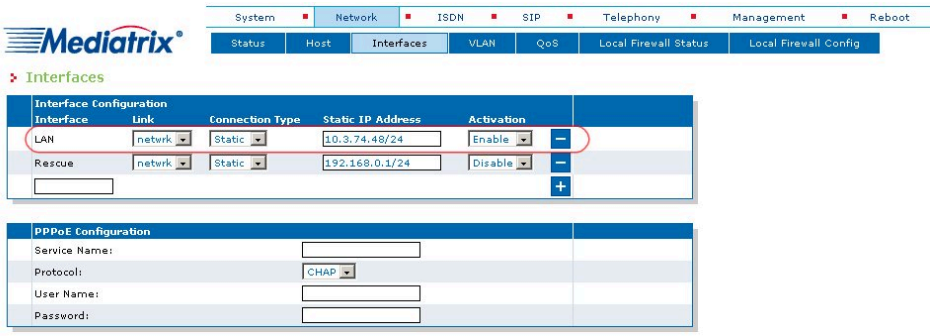
The network interfaces should be configured with unique LAN IP addresses. Theoretically, a Mediatrix 4400 gateway can support up to 48 network interfaces.

IMPORTANT: Care must be taken when assigning IP addresses to ensure that they can be reached by OpenScape 4000 SoftGate.

An OpenScape 4000 SoftGate (or vHG3500) can only operate one network interface in the Mediatrix gateway. It may be necessary to configure subscriber and trunking scenarios over a network interface.

Configure a LAN interface in this mask.

IMPORTANT: The name of the interface can be chosen at random and does not yet define usage. In this case we call it „LAN“.



Mediatrix 44xx Gateway (Trunking) - Network -> Interfaces

SIP -> Gateways

Configure your SIP gateway now. As **Gateway Name** you can chose „HG3550“ for example.

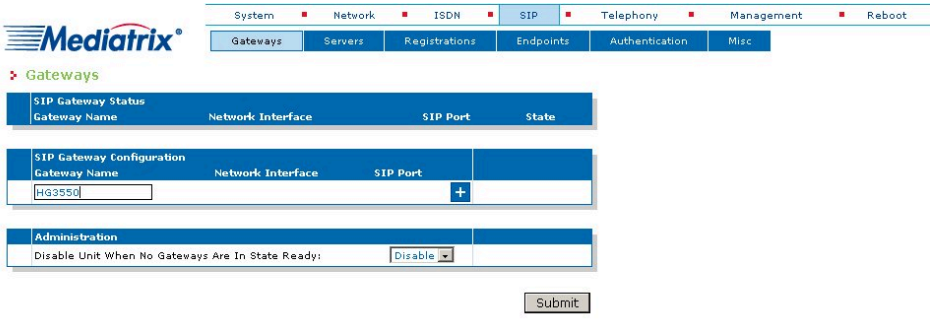


Figure 62: Mediatrix 44xx Gateway (Trunking) - SIP -> Gateways

Select the value „LAN“ in the **SIP Gateway Configuration** section in the field **Network Interface**.

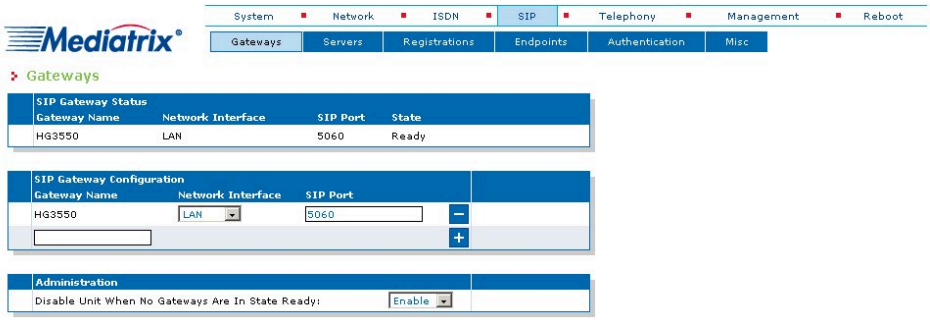


Figure 63: Mediatrix 44xx Gateway (Trunking) - SIP -> Gateways

SIP -> Servers

Enter the IP address of the virtual HG 3550 in the section **SIP Default Servers** in the field **Proxy Host** (in this case 10.3.74.38).

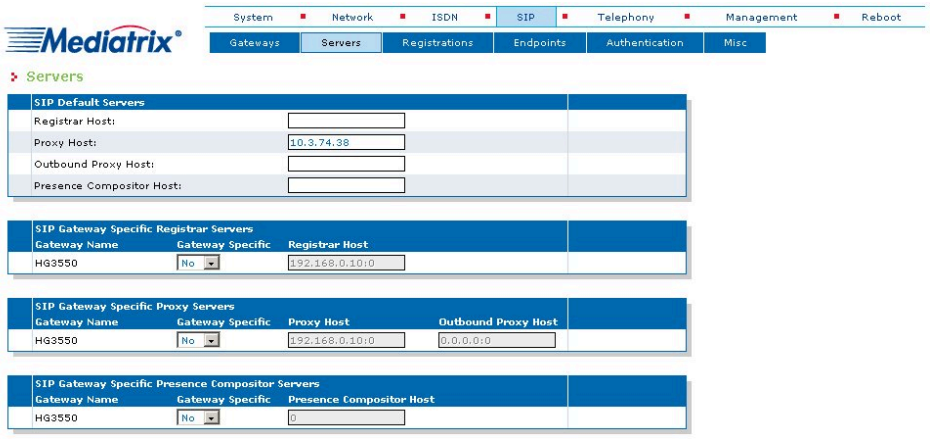
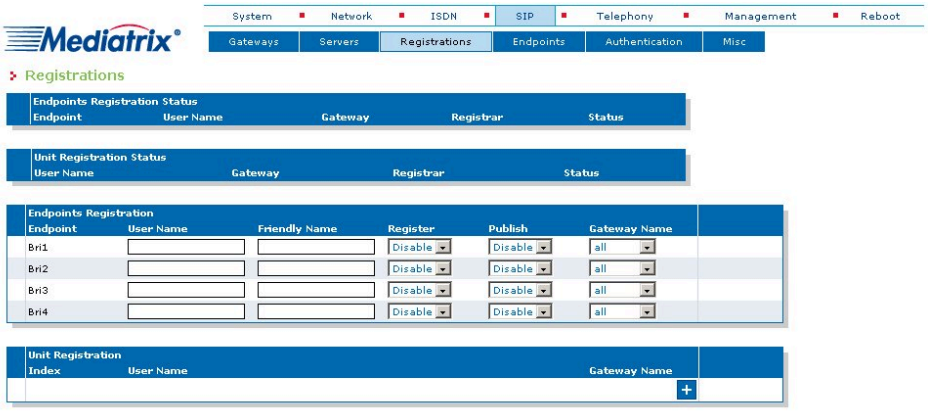


Figure 64: Mediatrix 44xx Gateway (Trunking) - SIP -> Servers

SIP -> Registrations

There are no endpoints in the trunking configuration, which is why registration is not necessary.

IMPORTANT: As the Mediatrix gateway only supports native SIP (not SIP-Q), a registration mechanism is not provided for trunking.



Mediatrix 44xx Gateway (Trunking) - SIP -> Registrations

ISDN -> Basic Rate Interface

Configure the ISDN parameters for every interface that should be used.

- Endpoint Type: **TE**
- Connection Type: e.g.: **Point To Point**

The ISDN trunking partner/CO provider protocol should be used, where applicable, to ensure that the "Exclusive B-Channel Selection" field is enabled for both interfaces.

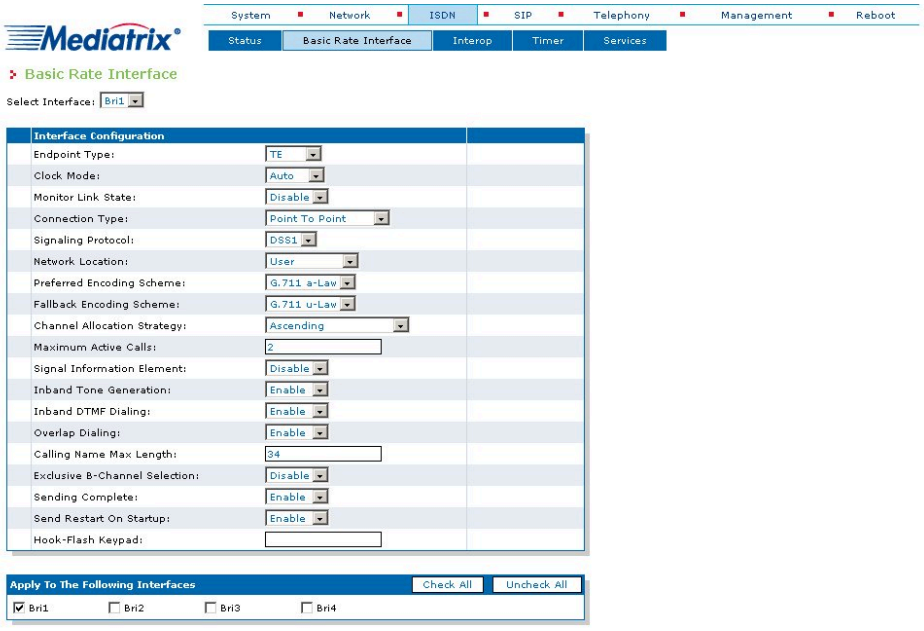


Figure 65: Mediatrix 44xx Gateway (Trunking) - ISDN -> Basic Rate Interface

Telephony -> Call Routing Config

The Mediatrix gateway's "Telephony - Call Routing Config" setting is not used in the general scenario for CO trunks (especially not for differentiation based on E.164 number). Station number handling is usually configured in the OpenScape 4000 system (see OpenScape 4000 sample configuration for S0 trunking).

OpenScape 4000 sample configuration for S0 trunking

```
ADD-BFDAT:FCTBLK=34,FUNCTION=HG3550&SIP,BRDBCHL=BCHL120,ATTR=SOCO
CHA-BFDAT:CONFIG=CONT,FCTBLK=34,FUNCTION=HG3550,LINECNT=1,UNITS=1;
CHA-BFDAT:CONFIG=CONT,FCTBLK=34,FUNCTION=SIP,LINECNT=20,BCHLCNT=2;
CHA-BFDAT:CONFIG=OK,FCTBLK=34,ANSW=YES;
/*  */
ADD-BCSU:TYPE=IPGW,LN=1,LTU=19,SLOT=8,PARTNO="Q2330-X    ",FCTID=1,LWVAR=0,FCT▶
BLK=34,BCHLSIP=2,BCHL3550=10,ALARMNO=0;
/*  */
ADD-CGWB:LTU=19,SLOT=8,SMODE=NORMAL,IPADDR=10.3.74.38,NETMASK=255.255.255.0;
CHANGE-
CGWB:MTYPE=CGW,LTU=19,SLOT=8,TYPE=GLOBIF,PATTERN=213,VLAN=NO,VLANID=0,DEFRT=0.0.
0.0,BITRATE=AUTONEG,TRPRSIP=10,TRPRSIPQ=0,TRPRH323=0,TPRH323A=0,TLSP=4060,DNSI▶
PADR=0.0.0.0;
CHANGE-CGWB:MTYPE=CGW,LTU=19,SLOT=8,TYPE=SERVIF,LOGINTRM="TRM";
CHANGE-CGWB:MTYPE=CGW,LTU=19,SLOT=8,TYPE=ASC,UDPPRTLO=29100,TOSPL=48,TOS▶
SIGNL=184, T38FAX=YES,RFCFMOIP=YES,RFCDTMF=YES,REDRFCTN=YES,PRIO=PRIO1,CO▶
DEC=G711A,VAD=NO,RTP=30;
```

REDRFCTN	Redundant transmission of the RFC2833 tones in accordance with RFC2198
RFCDTMF	Transmission of DTMF tones in accordance with RFC2833.
RFCFMOIP	Transmission of fax/modem tones in accordance with RFC2833

IMPORTANT: The parameters mentioned above must have the same value in all IPDA gateways (STMI2/4 and STMIX/Y (vSTMI) with regard to AMO CGWB & NCUI2+/4 (vNCUI) with regard to AMO STMIB). This avoids problems and a common function across all systems is achieved!

```
CHANGE-CGWB:MTYPE=CGW,LTU=19,SLOT=8,TYPE=ASC,PRIO=PRIO2,CO▶
DEC=G729A,VAD=NO,RTP=20;
CHANGE-CGWB:MTYPE=CGW,LTU=19,SLOT=8,TYPE=ASC,PRIO=PRIO3,CODEC=NONE,VAD=NO;
CHANGE-CGWB:MTYPE=CGW,LTU=19,SLOT=8,TYPE=ASC,PRIO=PRIO4,CO▶
DEC=NONE,VAD=NO,RTP=20;
CHANGE-CGWB:MTYPE=CGW,LTU=19,SLOT=8,TYPE=ASC,PRIO=PRIO5,CO▶
DEC=NONE,VAD=NO,RTP=20;
CHANGE-CGWB:MTYPE=CGW,LTU=19,SLOT=8,TYPE=ASC,PRIO=PRIO6,CO▶
DEC=NONE,VAD=NO,RTP=20;
CHANGE-CGWB:MTYPE=CGW,LTU=19,SLOT=8,TYPE=ASC,PRIO=PRIO7,CO▶
DEC=G729AB,VAD=YES,RTP=20;
CHANGE-CGWB:MTYPE=CGW,LTU=19,SLOT=8,TYPE=DSP,JITBUFD=60;
CHANGE-CGWB:MTYPE=CGW,LTU=19,SLOT=8,TYPE=MGNTDATA,MGNTPN=8000,BUSPN=443;
CHANGE-CGWB:MTYPE=CGW,LTU=19,SLOT=8,TYPE=DMCDATA,DMCCONN=0;
CHANGE-CGWB:MTYPE=CGW,LTU=19,SLOT=8,TYPE=WBMDATA,LOGINWBM="HP4K-DEVEL",ROLE=EN▶
```

```
GR;
CHANGE-CGWB:MTYPE=CGW,LTU=19,SLOT=8,TYPE=WBMDATA,LOGINWBM="HP4K-SU",ROLE=SU;
CHANGE-CGWB:MTYPE=CGW,LTU=19,SLOT=8,TYPE=WBMDATA,LOGINWBM="HP4K-ADMIN",ROLE=AD►
MIN;
CHANGE-CGWB:MTYPE=CGW,LTU=19,SLOT=8,TYPE=WBMDATA,LOGINWBM="HP4K-READ►
ER",ROLE=READONLY;
CHANGE-CGWB:MTYPE=CGW,LTU=19,SLOT=8,TYPE=GWDATA,GWID1="PRIMARYRASMANAGERID";
CHANGE-CGWB:MTYPE=CGW,LTU=19,SLOT=8,TYPE=H235DATA,SECSUBS=NO,SECTRNK=NO,GLO►
BID1="Gateway2003",TIMEWIN=100,GLOBPW=242-191-30-119-188-83-173-161-43-0-70-36-
218-74-169-221-78-102-174-170;
CHANGE-CGWB:MTYPE=CGW,LTU=19,SLOT=8,TYPE=LEGKDATA,GWNO=119,GWDIRNO=23;REGEXT►
GK=NO;
CHANGE-CGWB:MTYPE=CGW,LTU=19,SLOT=8,TYPE=SIPTRERH,GWAUTREQ=NO;
CHANGE-
CGWB:MTYPE=CGW,LTU=19,SLOT=8,TYPE=SIPTRSSA,SIPREG=NO,REGIP1=0.0.0.0,PORTTCP1=506
0,PORTTLS1=5061,REGTIME=120,REGIP2=0.0.0.0,PORTTCP2=5060,PORTTLS2=5061;
CHANGE-CGWB:MTYPE=CGW,LTU=19,SLOT=8,TYPE=DLSDATA,DLSIPADR=10.3.0.200,DL►
SPORT=18443,DLSACPAS=YES;
/*  */
ADD-GKREG:GWNO=19,GWATTR=EXTGW&HG3550V2&SIP,GWIPADDR=10.3.74.48,GWDIR►
NO=22,DIPLNUM=0,DPLN=0,LAUTH=1,INFO="",SECLEVEL=TRADITIO;
/*  */
ADD-BUEND:TGRP=119,NAME="CO AP19 MEDIATRIX",NO=10,TRACENO=0,ACDTHRH=*,PRIO►
NO=1,TDDRFLAG=ON,GDTRRULE=0,ACDPMGRP=0,CHARCON=NEUTRAL;
/*  */
ADD-TDCSU:OPT=NEW,PEN=1-19-008-0,COTNO=21,COP►
NO=21,DPLN=4,ITR=0,COS=1,LCOSV=1,LCOSD=1,CCT="            ",DESTNO=0,PROTVAR=EC►
MAV2,SEGMENT=8,DEDSVC=NONE,TRTBL=GDTR,SIDANI=N,ATNTYP=CO,CBMATTR=NONE,TCHARG=N,S
UPPRESS=0,TRACOUNT=31,SATCOUNT=MANY,ALARMNO=2,FIDX=1,CARRIER=1,ZONE=EMPTY,COTX=2
1,FWDX=1,CHIMAP=N,UUSCCX=16,UUSCCY=8,FNIDX=1,NWMUXTIM=10,CLASSMRK=EC&G711&G729AO
PT,TCCID="",TGRP=119,SRCHMODE=DSC,INS=Y,SECLEVEL=SECURE,DEV=HG3550CO,BCHAN=1&&6,
BCNEG=N,BCGR=1,LWPAR=0,LWPP=0,LWLT=0,LWPS=0,LWR1=0,LWR2=0,DMCALLWD=N;
/*  */
/* ------  LCR example for a national number------  */
/* ------  Number must go out as block dial------  */
/* ------  In the system either "prepared dial" must be activated  ------  */
/* ------  or LDPLN end with -Z and dial with # (SIP functionality------  */
/*  */
ADD-RICHT:MODE=LRTENEW,LRTE=119,LSVC=ALL,NAME="CO NATIONAL",TGRP=119,DNNO=1-1-
119,DTMFTEXT="",ROUTATT=YES,EMCYRTT=NO,INFO="",PDNNO=0,CONFTONE=NO,RERINGRP=NO,N
OPRCFWD=NO,NITO=NO,CLNAMEDL=NO,FWDSWTCH=NO,LINFEMER=NO,NOINTRTE=NO;
/*  */
ADD-LODR:ODR=19,CMD=OUTPULSE,DGTS=49;
ADD-LODR:ODR=19,CMD=ECHO,FIELD=4;
ADD-LODR:ODR=19,CMD=NPI,NPI=ISDN,TON=INTERNAT;
ADD-LODR:ODR=19,CMD=END;
/*  */
ADD-LDAT:LROUTE=119,LSVC=ALL,LVAL=1,TGRP=119,ODR=19,LAUTH=1,CARRIER=1,ZONE=EMP►
TY,LATTR=NONE,VCCYC=4,GW1=19-0;
/*  */
ADD-LDPLN:LCRCONF=LCRPATT,DIPLNUM=0,LDP=0-W-0-Z,LROUTE=119,LAUTH=1,PINDP=NO;
```

It is assumed that the OpenScape 4000 transmits all dial patterns (**subscr**, **national**, **internet**) in E164 ISDN / international format (block dialing must be configured).

The example here refers to a location with the number +49 (30) 430-xxx.

IMPORTANT: The longest number to be processed must be first with these criteria!

Outgoing calls from the OpenScape 4000 SoftGate to the CO Carrier

All dial patterns with an "+" at the beginning arrive on the Mediatrix gateway via the sip HG3550 interface This way the Mediatrix recognizes that it is an E164 number in ISDN / INTERNATIONAL format. Depending on the requirements of the CO carrier, the number to ISDN-BRI can be modified to a national ("CO_outg_national") or subscriber ("CO_outg_subscr") format. The modification applies to calling and called numbers.

Criteria/Transformation

Therefore the following criteria/transformation is applied:

- E164 -> E164 or TONE -> TONE.

Incoming calls from the CO carrier to the OpenScape 4000 SoftGate

The came applies to incoming calls to the sip HG3550.

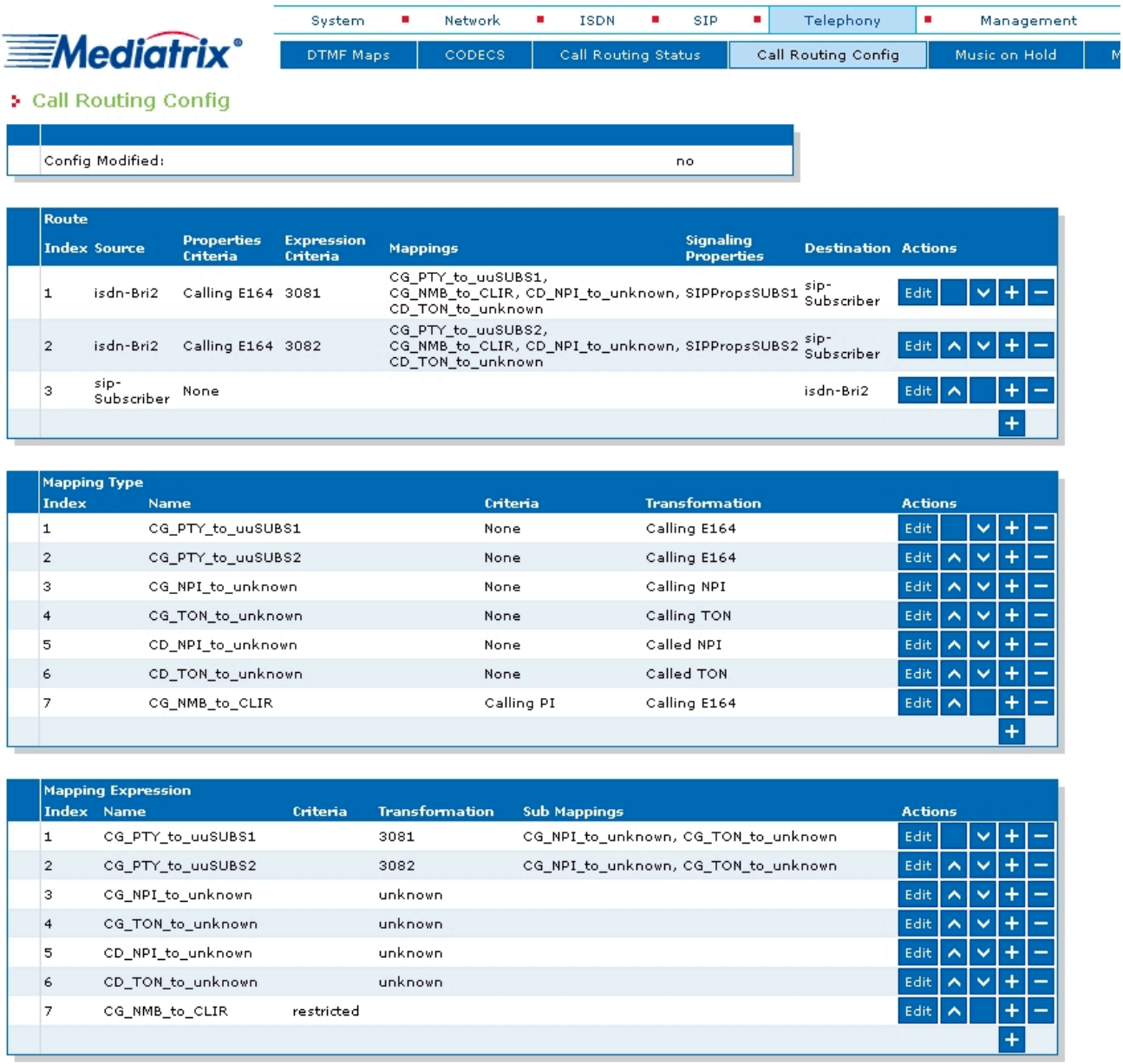
The called number in the subscriber format is converted to international ("CO_inc_called") format. If the carrier transmits the called number in national format, the routing must be changed from "CO_inc_called (.+) +4930\1" to "CO_inc_called (.+) +49\1".

The incoming number (calling number) is modified depending on format via the routing entries "CO_inc_calling_subscr_to_4930
" or "CO_inc_calling_national_to_49
". Different rules apply to the calling number as to the called number because the called number is always the same (depending on the carrier either subscriber or national) but the calling number can be different (**subscriber**, **national** or **international**).

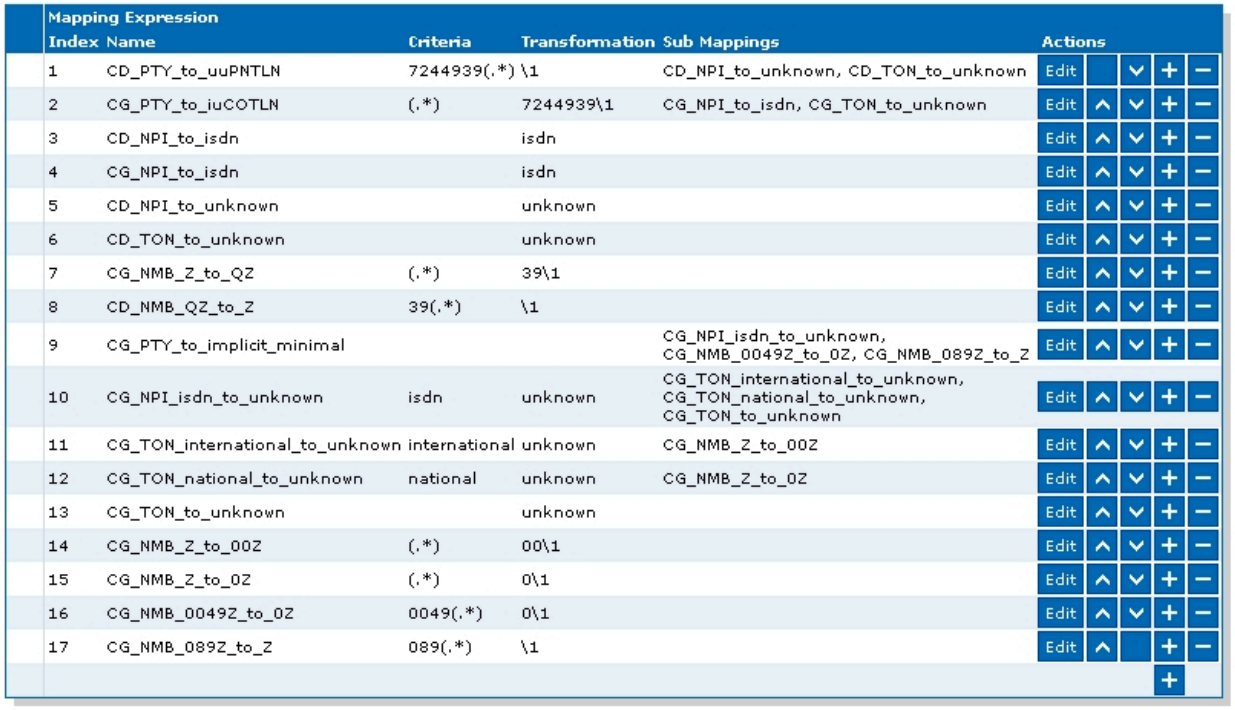
Criteria/Transformation

Therefore the following criteria/transformation is applied:

- Calling E164 -> Calling E164 or Calling TONE -> Calling TONE and
- Called E164 -> Called E164 or Called TONE -> Called TONE.



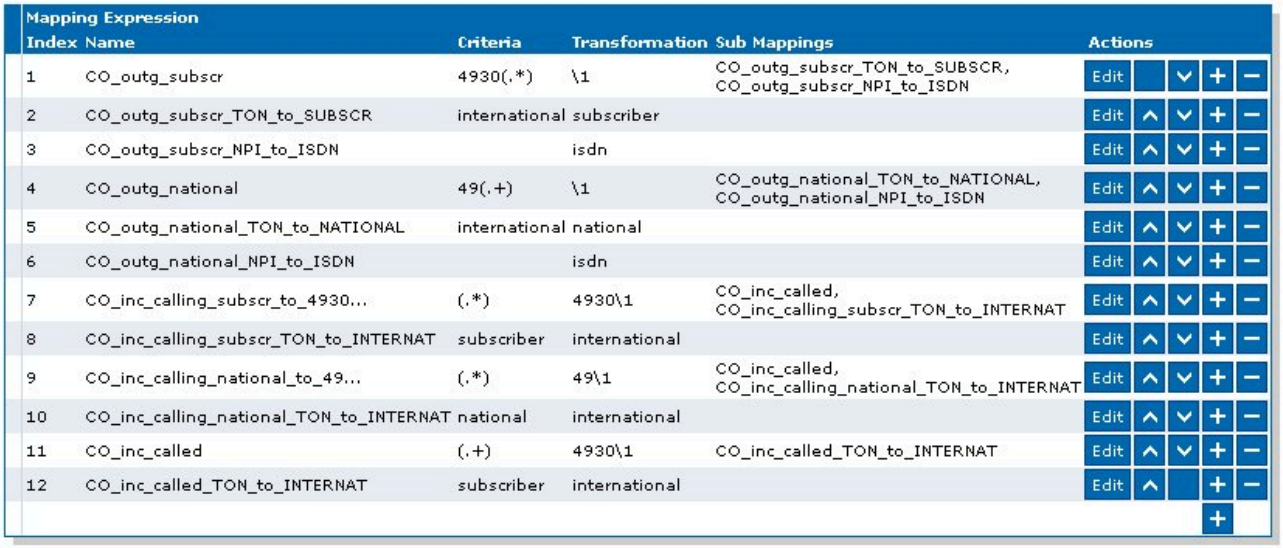
Mediatrix 44xx Gateway (Trunking) - Telephony -> Call Routing Config 1



Mapping Expression

Index	Name	Criteria	Transformation	Sub Mappings	Actions
1	CD_PTY_to_uuPNTLN	7244939(.*)	\1	CD_NPI_to_unknown, CD_TON_to_unknown	Edit
2	CG_PTY_to_iuCOTLN	(.*)	7244939\1	CG_NPI_to_isdn, CG_TON_to_unknown	Edit
3	CD_NPI_to_isdn		isdn		Edit
4	CG_NPI_to_isdn		isdn		Edit
5	CD_NPI_to_unknown		unknown		Edit
6	CD_TON_to_unknown		unknown		Edit
7	CG_NMB_Z_to_QZ	(.*)	39\1		Edit
8	CD_NMB_QZ_to_Z	39(.*)	\1		Edit
9	CG_PTY_to_implicit_minimal			CG_NPI_isdn_to_unknown, CG_NMB_0049Z_to_0Z, CG_NMB_089Z_to_Z	Edit
10	CG_NPI_isdn_to_unknown	isdn	unknown	CG_TON_international_to_unknown, CG_TON_national_to_unknown, CG_TON_to_unknown	Edit
11	CG_TON_international_to_unknown	international	unknown	CG_NMB_Z_to_00Z	Edit
12	CG_TON_national_to_unknown	national	unknown	CG_NMB_Z_to_0Z	Edit
13	CG_TON_to_unknown		unknown		Edit
14	CG_NMB_Z_to_00Z	(.*)	00\1		Edit
15	CG_NMB_Z_to_0Z	(.*)	0\1		Edit
16	CG_NMB_0049Z_to_0Z	0049(.*)	0\1		Edit
17	CG_NMB_089Z_to_Z	089(.*)	\1		Edit

Mediatrix 44xx Gateway (Trunking) - Telephony -> Call Routing Config 2



Mapping Expression

Index	Name	Criteria	Transformation	Sub Mappings	Actions
1	CO_outg_subscr	4930(.*)	\1	CO_outg_subscr_TON_to_SUBSCR, CO_outg_subscr_NPI_to_ISDN	Edit
2	CO_outg_subscr_TON_to_SUBSCR	international	subscriber		Edit
3	CO_outg_subscr_NPI_to_ISDN		isdn		Edit
4	CO_outg_national	49(.+)	\1	CO_outg_national_TON_to_NATIONAL, CO_outg_national_NPI_to_ISDN	Edit
5	CO_outg_national_TON_to_NATIONAL	international	national		Edit
6	CO_outg_national_NPI_to_ISDN		isdn		Edit
7	CO_inc_calling_subscr_to_4930...	(.*)	4930\1	CO_inc_called, CO_inc_calling_subscr_TON_to_INTERNAT	Edit
8	CO_inc_calling_subscr_TON_to_INTERNAT	subscriber	international		Edit
9	CO_inc_calling_national_to_49...	(.*)	49\1	CO_inc_called, CO_inc_calling_national_TON_to_INTERNAT	Edit
10	CO_inc_calling_national_TON_to_INTERNAT	national	international		Edit
11	CO_inc_called	(.+)	4930\1	CO_inc_called_TON_to_INTERNAT	Edit
12	CO_inc_called_TON_to_INTERNAT	subscriber	international		Edit

Mediatrix 44xx Gateway (Trunking) - Telephony -> Call Routing Config 3

3.3.3.3 ISDN (S0) Data Connections (Mediatrix 44xx)

3.3.3.3.1 Requirements for ISDN (S0) Data (Connections)

IMPORTANT: For basic information on installing S0 data scenarios refer to the description of how to install S0 subscribers and S0 trunking scenarios. This section describes the special

requirements for S0 data connections that also have to be taken into consideration.

- ISDN data connections are only supported if Mediatrix 44xx gateways are used.
- ISDN data connections are only supported for stations or trunks that are configured on the same OpenScape 4000 SoftGate.

IMPORTANT: Direct Media over LAN (DMC) is not possible for S0 data connections.

- All ISDN S0 gateways for data connections should be synchronized with a common clock. For instance, the gateways receive the clock pulse via a direct connection to the public network or via an internal ISDN line (layer-2 connection) to another synchronized gateway.

3.3.3.3.2 Sample Scenario with two Mediatrix 44xx Gateways

In this sample scenario, one Mediatrix gateway is used for subscribers, while the other is used for trunking to the public network.

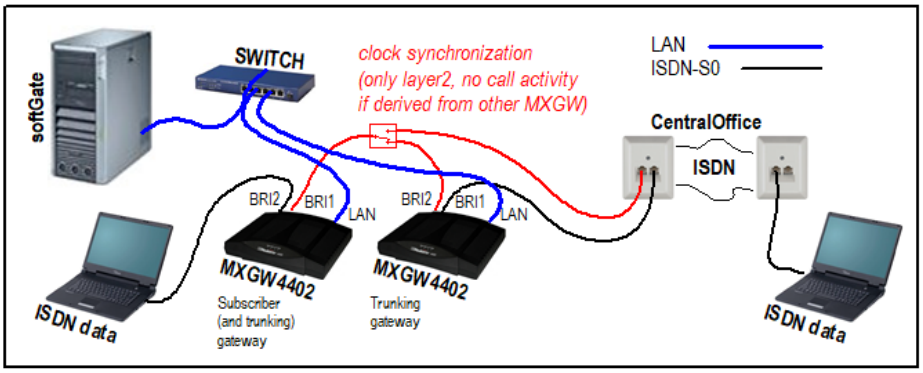


Figure 66: OpenScape 4000 SoftGate scenario with two Mediatrix gateways

This type of scenario is an alternative to the configuration of subscribers and trunking within a single gateway. This clock synchronization method is also needed if more than four ISDN S0 ports are to be configured (up to four S0 ports are available on a single Mediatrix gateway).

3.3.3.3.3 Trunking Gateway

Overview

- ISDN -> Basic Rate Interface (BRI 1)
- ISDN -> Basic Rate Interface (BRI 2)
- ISDN -> Status
- Codec Parameter Trunking and Subscriber Gateway

ISDN -> Basic Rate Interface (BRI 1)

The trunking gateway is linked to the public network via the BRI 1 port and synchronizes itself with the clock pulse received.

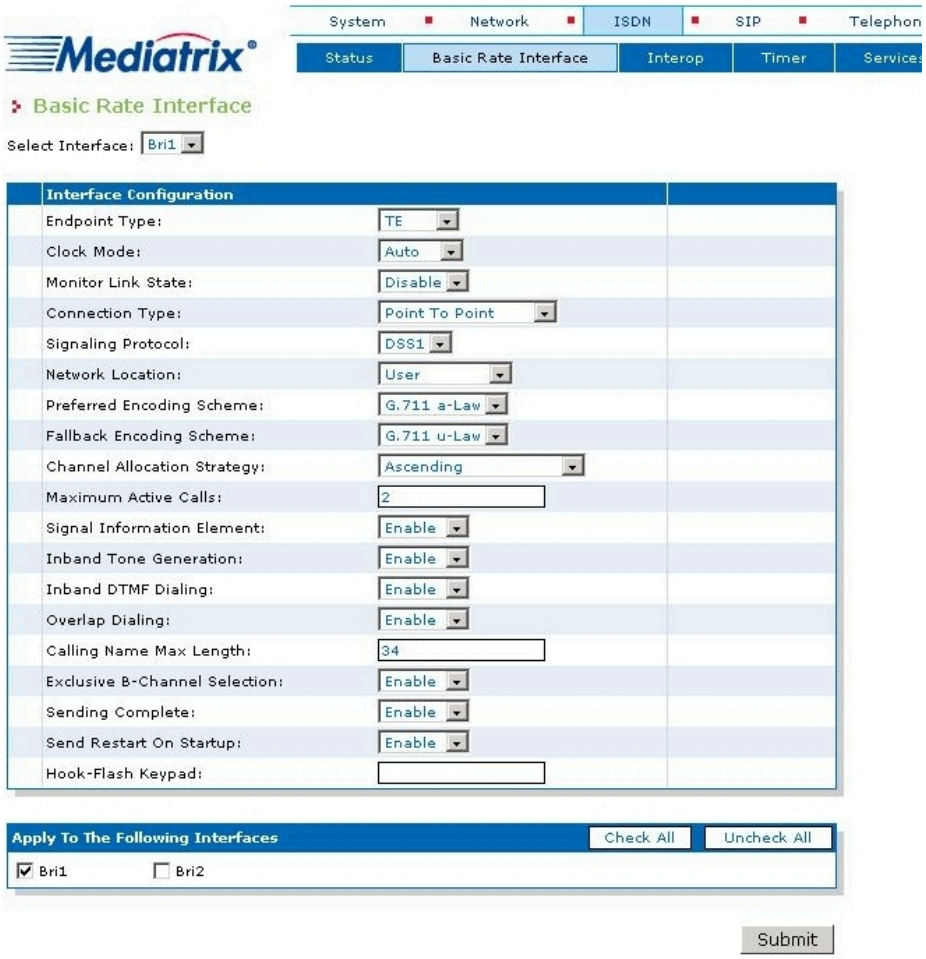


Figure 67: Mediatrix Gateway Trunking - ISDN -> Basic Rate Interface 1

ISDN -> Basic Rate Interface (BRI 2)

The BRI 2 port is used to forward the clock pulse to the subscriber gateway.

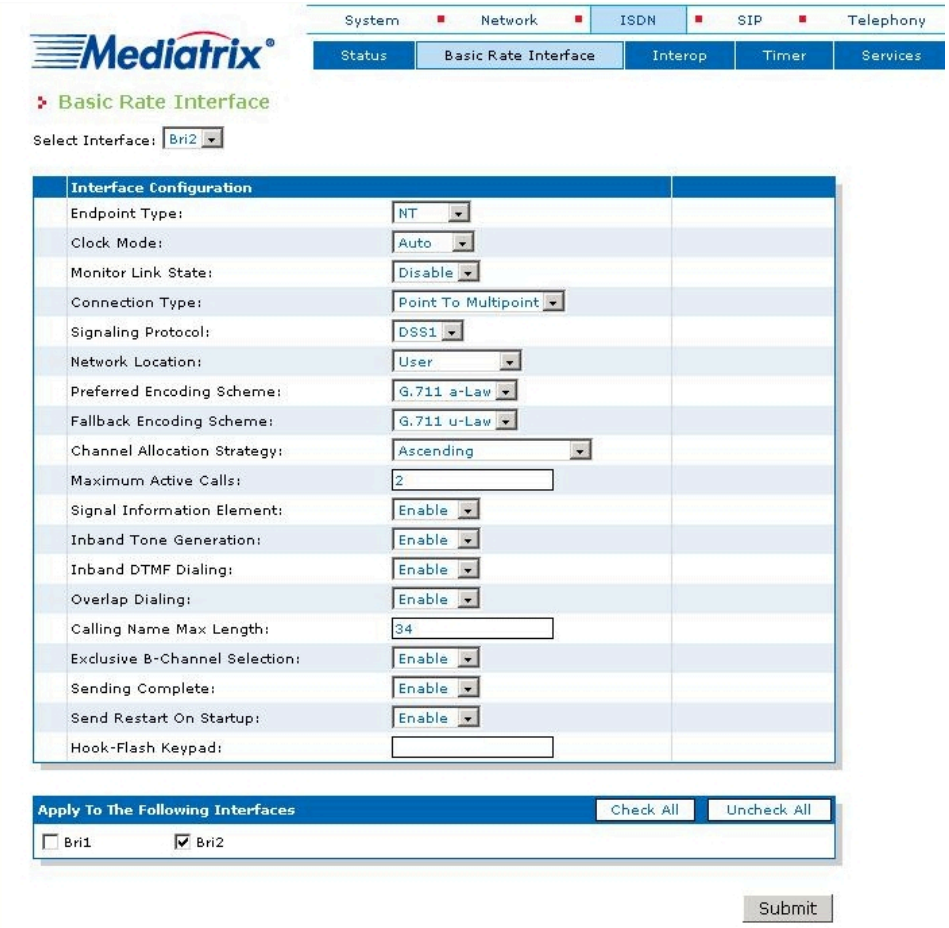


Figure 68: Mediatrix 44xx Gateway Trunking - ISDN -> Basic Rate Interface 2

ISDN -> Status

A status window indicates that clocking is performed via the BRI1 port which is connected to the public network. It also shows that the link on the BRI 2 port for transferring the clock pulse to the subscriber gateway is working (layer-3 signaling is not used for this link).

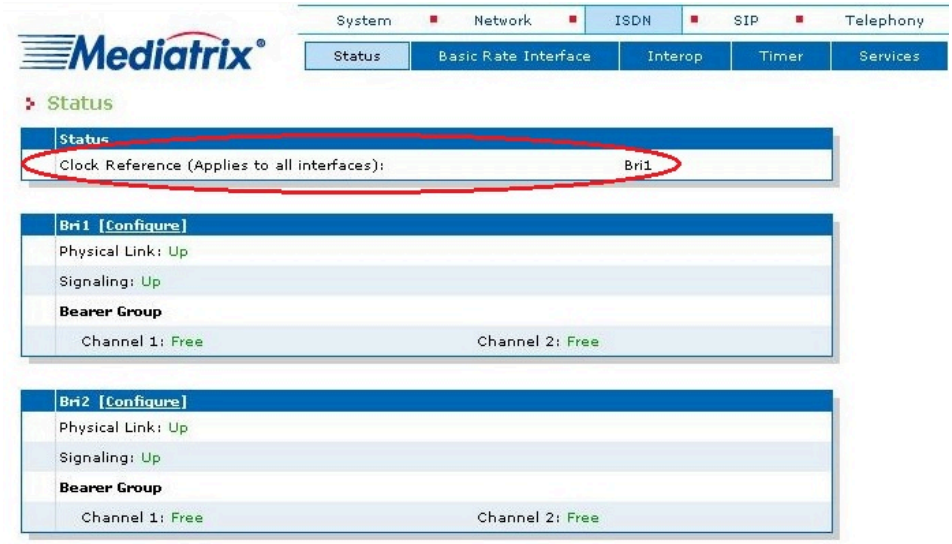


Figure 69: Mediatrix 44xx Gateway Trunking - ISDN -> Status

3.3.3.3.4 Subscriber Gateway

Overview

- ISDN -> Basic Rate Interface (BRI 1)
- ISDN -> Status
- Codec Parameter Trunking and Subscriber Gateway

ISDN -> Basic Rate Interface (BRI 1)

The subscriber gateway is linked to the trunking gateway (alternatively also to the public network) via the BRI 1 port without layer-3 signaling and synchronizes itself with the indirect clock pulse.



Figure 70: Mediatrix 44xx Gateway Subscriber - -> Basis Rate Interface 1

ISDN -> Status

A status window indicates that clocking is performed via the BRI1 port which is clocked either directly or indirectly via the public network.

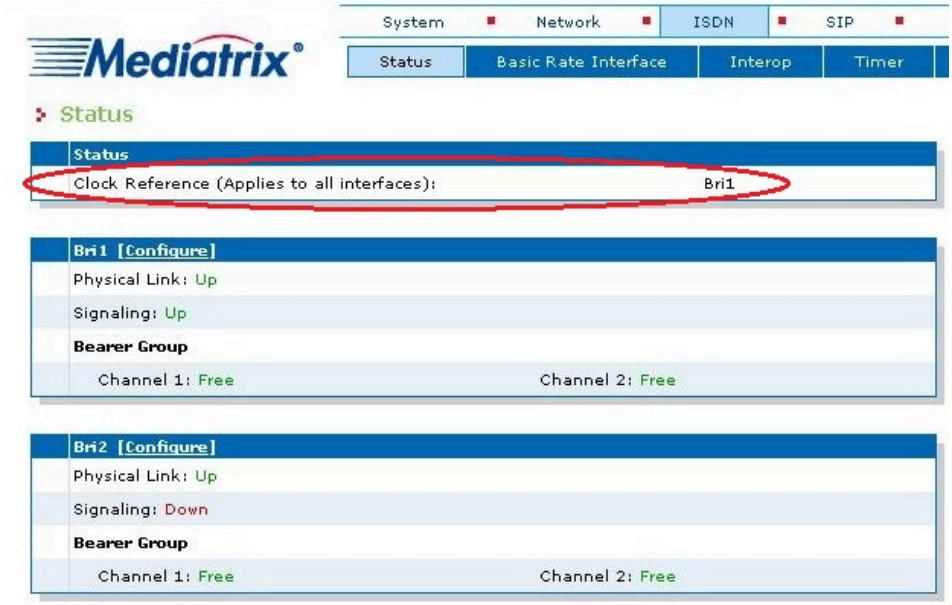


Figure 71: Mediatrix 44xx Gateway Subscriber - ISDN -> Status

3.3.3.3.5 Codec Parameter Trunking and Subscriber Gateway

The settings in the CODECS mask are identical for both gateways.

- Bearer-type mapping must be set to "ITC unrestricted" for the "Codec ClearMode".
- The "ITC" field must contain the value **unrestricted**.
- The setting in the "Jitter Buffer" field can be used to improve the data transmission quality if the delay time does not have to be optimized.

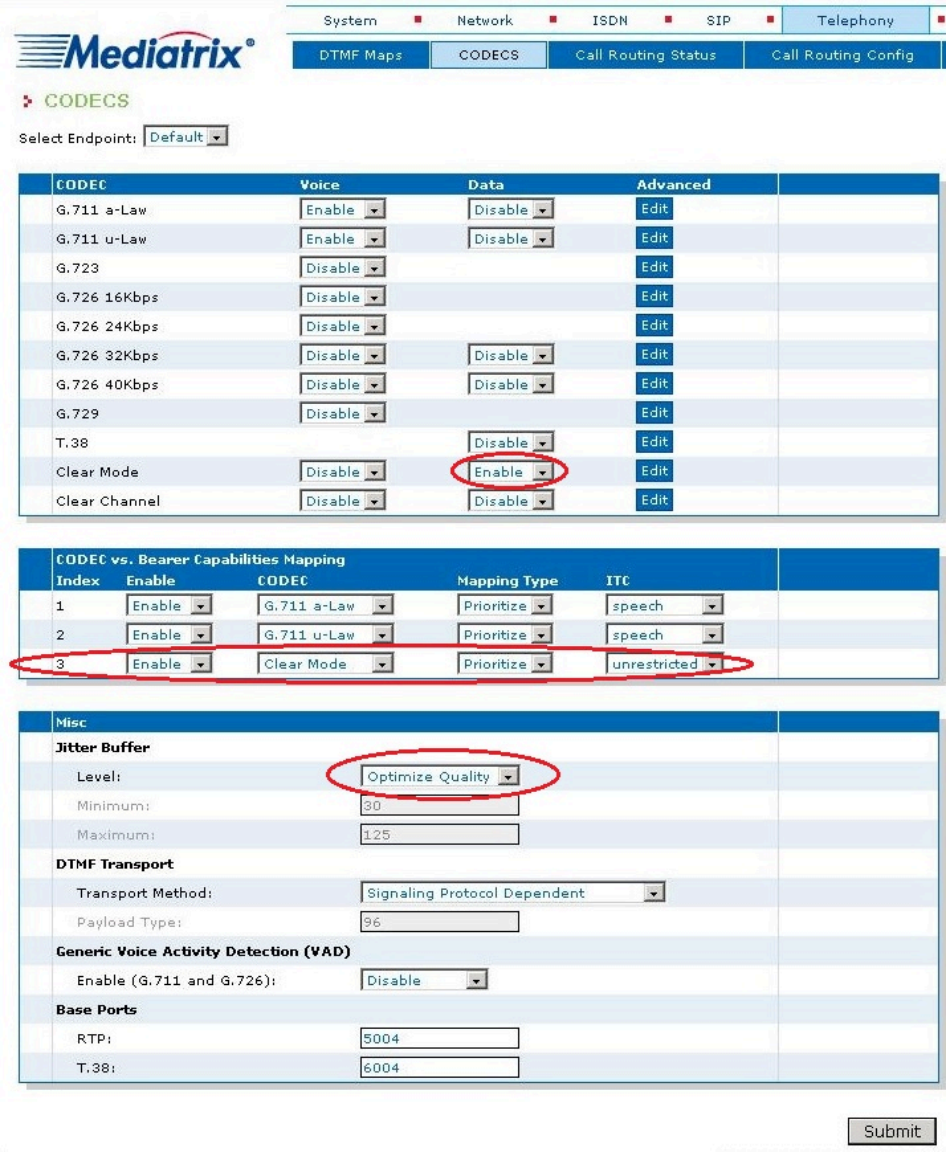


Figure 72: Mediatrix 44xx Gateway Subscriber and Trunking - Telephony -> CODECS

3.3.3.4 S2 Interface (Mediatrix 36xx)

In this sample scenario a Mediatrix gateway is used for trunking to the public network.

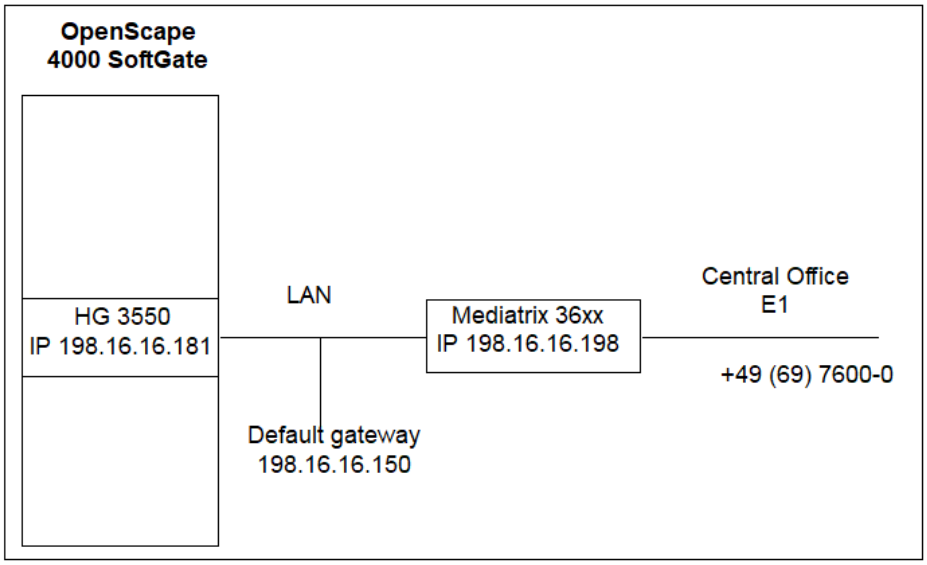


Figure 73: OpenScape 4000 SoftGate scenario with Mediatrix 36xx gateway - S2 Interface

Overview

- Network -> Host
- Network -> Interfaces
- SIP -> Gateways
- SIP -> Servers
- SIP > Registrations
- System -> Hardware
- ISDN -> Primary Rate Interface
- ISDN > Status
- Call Router -> Route Config

Network -> Host

Set **Static**

- in section **Host Name Configuration** for **Domain Name Configuration Source**,
- in section **DNS Configuration** for **Configuration Source**,
- in section **SNTP Configuration** for **Configuration Source**,
- in section **Default Gateway Configuration** for **Configuration Source**.

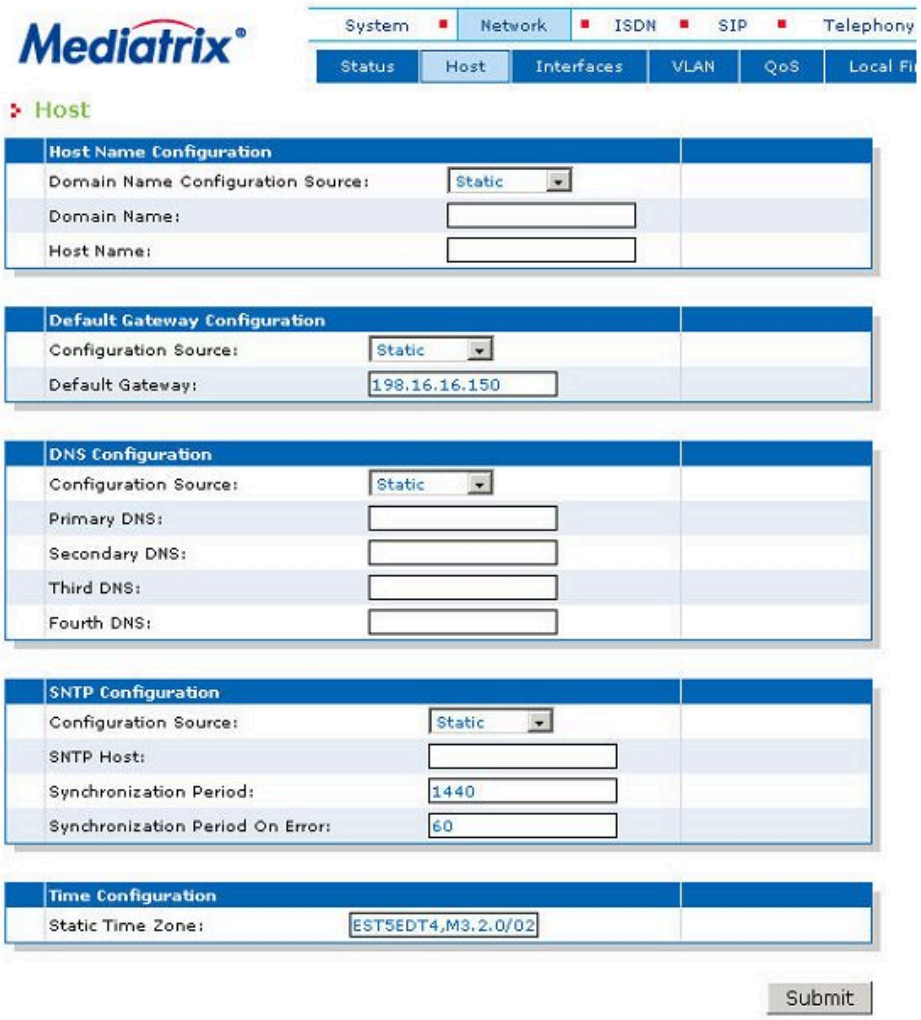
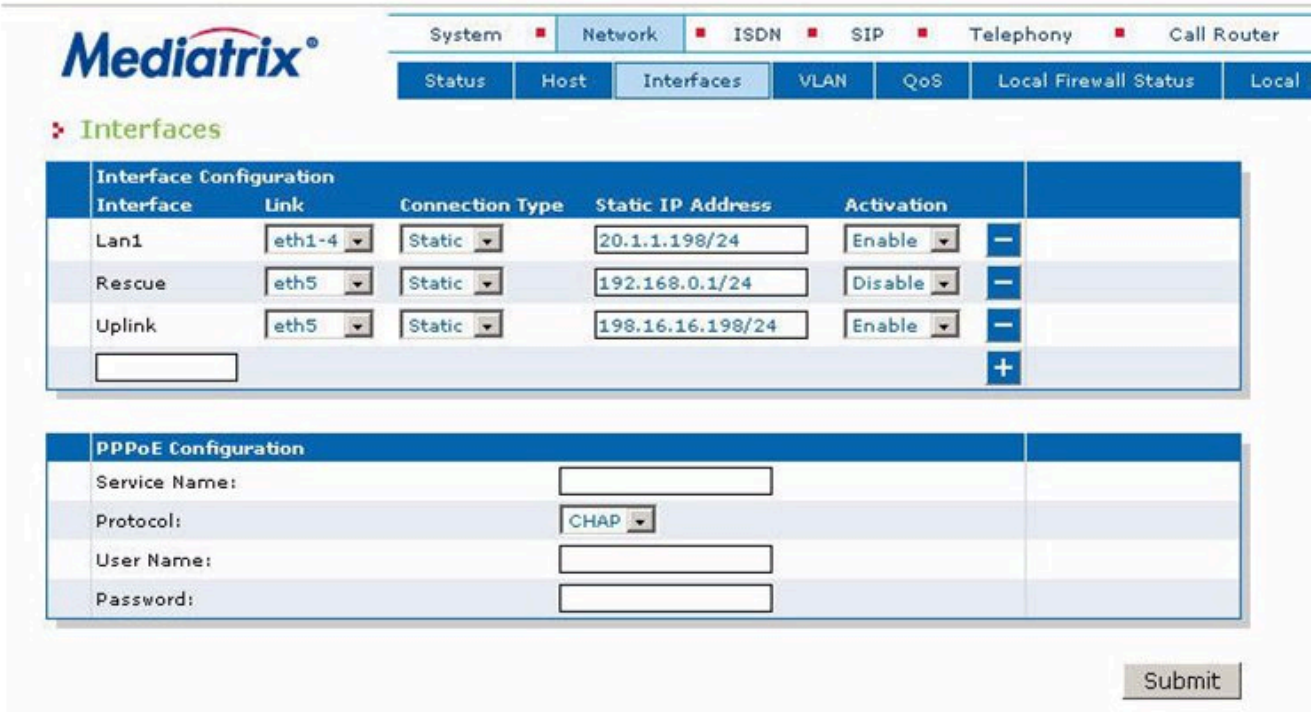


Figure 74: Mediatrix gateway 36xx - Network > Host

Network -> Interfaces

The network interfaces should be configured with unique LAN IP addresses. Currently only eth5 is used as uplink. Eth1-4 are not used yet (will be used as ports of a switch).

IMPORTANT: Take care that all IP addresses are reachable by the OpenScape 4000 SoftGate.



Mediatrix gateway 36xx - Network > Interfaces

You can check the status by selecting Network -> Status



Mediatrix gateway 36xx - Network > Status

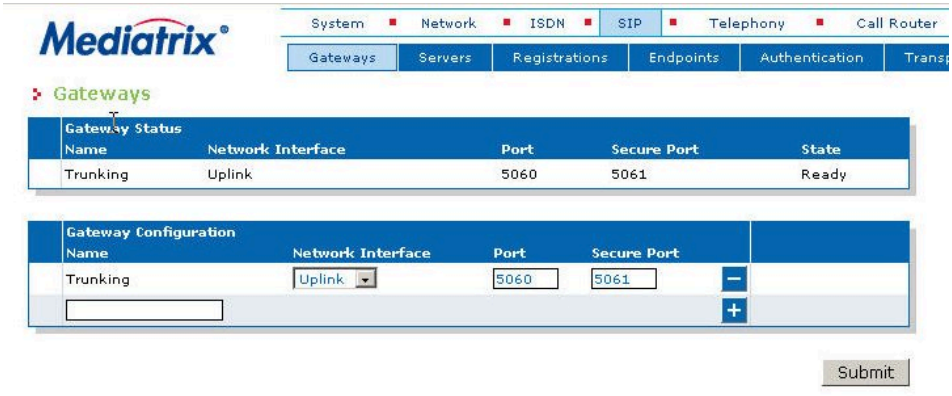
SIP -> Gateways

Configure your SIP gateway now.

SIP gateway configuration:

For this example we use "Trunking" as the **Gateway Name**.

In section **Gateway Configuration** field **Network Interface** select **Uplink**.



Mediatrix gateway 36xx - SIP > Gateways

SIP -> Servers

Configuring the vHG 3550 gateway address (198.16.16.181):

In section **SIP Default Servers** enter the IP address to field **Proxy Host**.

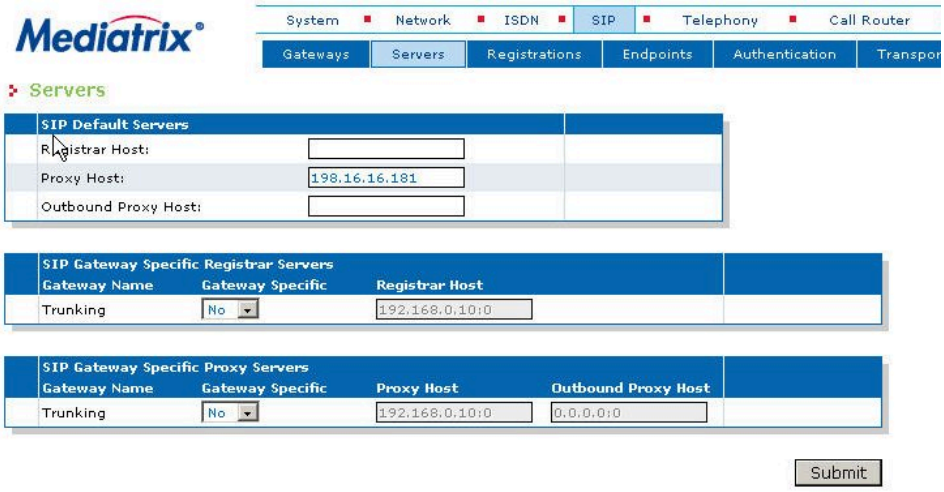
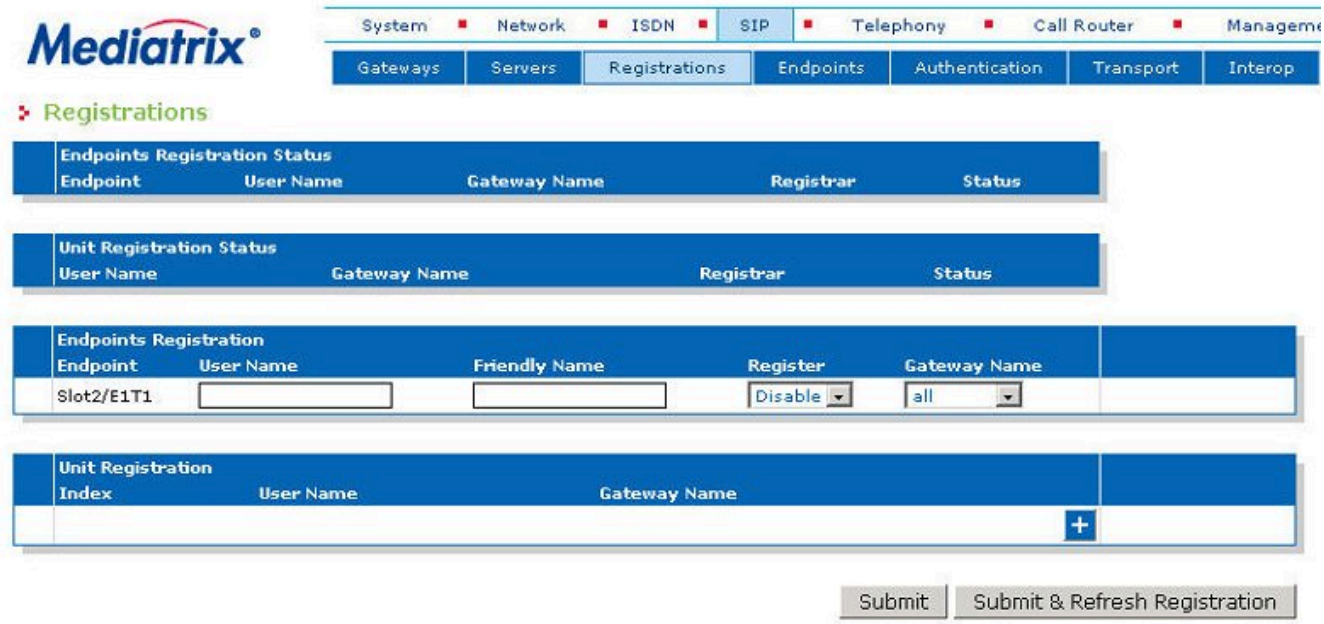


Figure 75: Mediatrix gateway 36xx - SIP > Servers

SIP > Registrations

There are no endpoints in the trunking configuration, therefore registration is not necessary.

IMPORTANT: As the Mediatrix gateway only supports native SIP (not SIP-Q), a registration mechanism is not provided for trunking.



Mediatrix gateway 36xx - SIP > Registrations

System -> Hardware

Hardware configuration of the PRI card.

In section **PRI Cards Configuration**:

- Select the **Line Type** (**E1** or **T1**)
- Select **Isdn** for **Signaling**

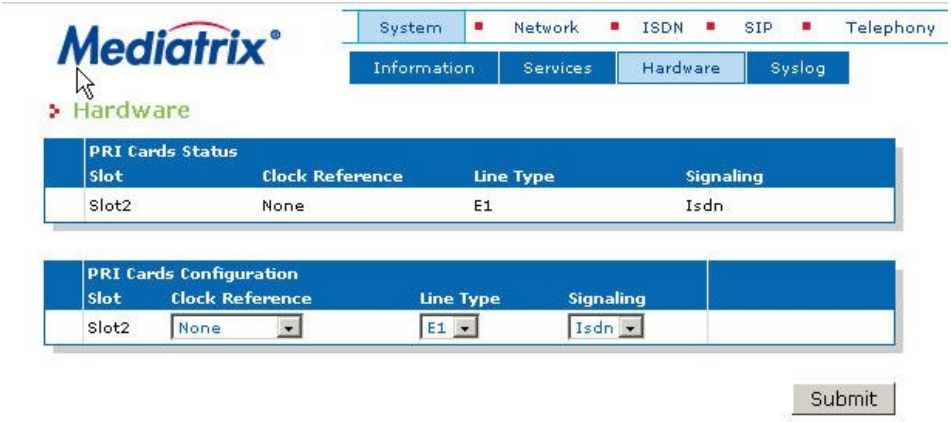


Figure 76: Mediatrix gateway 36xx - System > Hardware

ISDN -> Primary Rate Interface

Configure the primary rate interface.

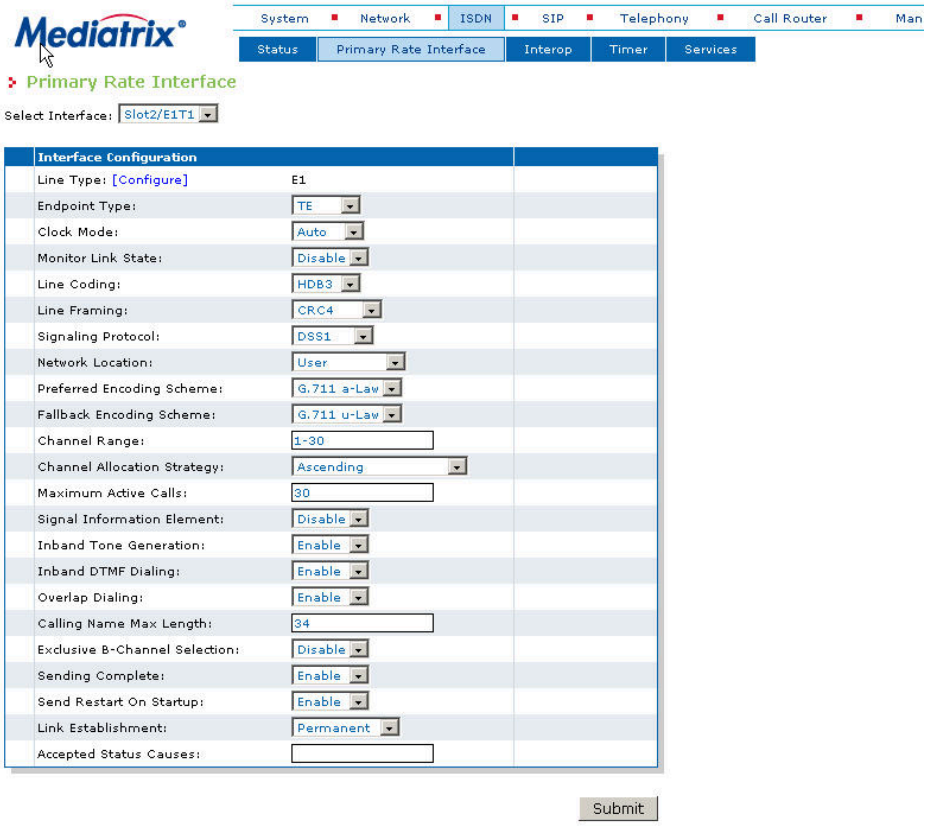


Figure 77: Mediatrix gateway 36xx - ISDN > Primary Rate Interface

ISDN > Status

Checking status by selecting ISDN > Status.

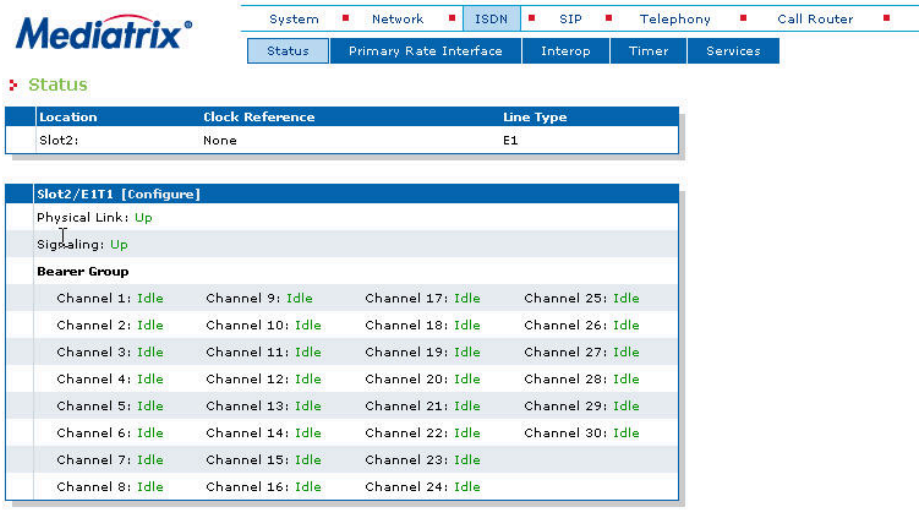


Figure 78: Mediatrix gateway 36xx - ISDN > Status

Call Router -> Route Config

The Mediatrix gateway's "Call Router - Route Config" setting is not used in the general scenario for CO trunks (especially not for differentiation based on E.164 number). Station number handling is usually configured in the OpenScape 4000 system (see OpenScape 4000 sample configuration for S2 interface).

OpenScape 4000 sample configuration for S2 interface

```
ADD-UCSU:UNIT=AP,LTG=1,LTU=18,LTPARTNO="Q2329-X    ",SRCGRP=18,FRMTYPE=SO▶
COAP,CONNTYPE=APDL,LSRTADDR=198.16.16.186,APRTADDR=198.16.16.150,LOCID=001,LOCA▶
TION="CPCI23 SOFTGATE18",PLCHECK=YES,BCHLCNT=120,CONVLAW=NO,TCLASS=0,ALARM▶
NO=0,SOCOTYPE=SOCO50;
ADD-BFDAT:FCTBLK=34,FUNCTION=HG3550&SIP,BRDBCHL=BCHL120,ATTR=SOCO;
CHA-BFDAT:CONFIG=CONT,FCTBLK=34,FUNCTION=HG3550,LINECNT=1,UNITS=3;
CHA-BFDAT:CONFIG=CONT,FCTBLK=34,FUNCTION=SIP,LINECNT=1,BCHLCNT=4;
CHA-BFDAT:CONFIG=OK,FCTBLK=34,ANSW=YES;
ADD-BCSU:MTYPE=IPGW,LTG=1,LTU=18,SLOT=1,PARTNO="Q2330-X    ",FCTID=1,LWVAR=0,FCT▶
BLK=34,BCHLSIP=4,BCHL3550=30,ALARMNO=0;
ADD-CGWB:LTU=18,SLOT=1,SMODE=NORMAL,IPADR=198.16.16.181,NETMASK=255.255.255.0;
CHANGE-CGWB:MTYPE=CGW,LTU=18,SLOT=1,TYPE=GLOBIF,DEFRT=198.16.16.150,BI▶
TRATE=100MBFD,TRPRSIP=30;
CHANGE-CGWB:MTYPE=CGW,LTU=18,SLOT=1,TYPE=LEGKDATA,GWNO=199,GWDIRNO=199,REGEXT▶
GK=NO;
ADD-BUEND:TGRP=18,NAME="AMT  SOCO18  S2      ",NO=60,TRACENO=0,ACDTHRH=*,PRIO▶
NO=1,TDDRFLAG=ON,GDTRRULE=0,ACDPMGRP=0,CHARCON=NEUTRAL;
ADD-COT:COTNO=60,PAR=RCL&IBSY&ANS&CEBC&CBBN&BSHT&LWNC&NLCR&TSCS&DFNN&NLRD&NTON;
ADD-COP:COPNO=60,PAR=L3AR&SPTR,TRK=TA,TOLL=TA;
ADD-TDCSU:OPT=NEW,PEN=1-18-001-0,COTNO=60,COP▶
NO=60,DPLN=0,ITR=0,COS=1,LCOSV=1,LCOSD=1,CCT="AMT  SOCO18   ",DESTNO=0,PROTVAR=EC▶
MAV2,SEGMENT=8,DEDSVC=NONE,TRTBL=GDTR,SIDANI=N,ATNTYP=CO,CBMATTR=NONE,TCHARG=N,S
UPPRESS=0,TRACOUNT=31,SATCOUNT=MANY,ALARMNO=2,FIDX=1,CARRIER=1,ZONE=EMPTY,COTX=2
1,FWDX=1,CHIMAP=N,UUSCCX=16,UUSCCY=8,FNIDX=1,NWMUXTIM=10,CLASSMRK=EC&G711&G729AO
PT,TCCID="",TGRP=18,SRCHMODE=DSC,INS=Y,SECLEVEL=TRADITIO,DEV=HG3550CO,BCHAN=1&&3
```

```
0,BCNEG=N,BCGR=1,LWPAR=0,LWPP=0,LWLT=0,LWPS=0,LWR1=0,LWR2=0,DMCALLWD=N;
ADD-GKREG:GWNO=199,GWATTR=INTGW&HG3550V2&SIP,DIPLNUM=0,DPLN=0,LAUTH=1,INFO="";
ADD-GKREG:GWNO=19,GWATTR=EXTGW&HG3550V2&SIP,GWIPADDR=198.16.16.198,GWDIR►
NO=119,DIPLNUM=0,DPLN=0,LAUTH=1,INFO="",SECLEVEL=TRADITIO;
/* -- LCR example for a national number -- */
/* -- Number must go out as block dial -- */
/* -- In the system either "prepared dial" must be activated -- */
/* -- or LDPLN end with -Z and dial with # (SIP functionality) -- */
ADD-RICHT:MODE=LRTENEW,LRTE=1011,LSVC=ALL,NAME="AMT-ORT SOCO18 ",TGRP=18,DNNO=1-
2-68,ROUTOPT=YES,DTMFCNV=SUFDIAL,DTMFDISP=DIGITS,DTMFTEXT="MFV-NACHWAHL
",DTMFPULS=PP300,DESTNO=60,ROUTATT=YES,EMCYRTT=NO,INFO="",PDNNO=0,CHARCON=NEU►
TRAL;
ADD-LODR:ODR=1011,CMD=OUTPULSE,DGTS=49;
ADD-LODR:ODR=1011,CMD=ECHO,FIELD=4;
ADD-LODR:ODR=1011,CMD=NPI,NPI=ISDN,TON=INTERNAT;
ADD-LODR:ODR=1011,CMD=END;
ADD-LDAT:LROUTE=1011,LSVC=ALL,LVAL=1,TGRP=18,ODR=1011,LAUTH=1,CARRI►
ER=1,ZONE=EMPTY,LATTR=WCHREG,VCCYC=4,GW1=19-0;
ADD-LDPLN:LCRCONF=LCRPATT,DIPLNUM=0,LDP=0-W-0-Z,LROUTE=1011,LAUTH=1,PINDP=N;
```

It is assumed that the OpenScape 4000 transmits all dial patterns (subscr, national, internat) in E164 ISDN / international format (block dialing must be configured).

The example here refers to a location with ISDN number +49 (69) 7600-XXXXX.

IMPORTANT: The longest number to be modified must be first with these criteria!

Outgoing calls from the OpenScape 4000 SoftGate to the CO Carrier

Between Mediatrix Gateway and the HG 3550 interface all numbers are send as E.164 International ISDN Numbers. This number format is signaled with a "+" at the beginning of each pattern.

Depending on the CO carriers requirements, the number format send to the ISDN interface may be modified to type of number "National" ("CO_outg_national") or "Subscriber" ("CO_outg_subscr").

The modification is executed for calling and called numbers.

Criteria/Transformation:

Therefore the following criteria/transformation is applied:

1) E164 -> E164 or TONE -> TONE.

Incoming calls from the CO carrier to the OpenScape 4000 SoftGate

The same applies to incoming calls to the sip HG 3550.

The called number in the subscriber format is converted to international ("CO_inc_called") format. If the carrier transmits the called number in national format, the routing must be changed from "CO_inc_called (.+) +4969\1" to "CO_inc_called (.+) +49\1".

The incoming number (calling number) is modified depending on format via the routing entries "CO_inc_calling_subscr_to_4969
" or "CO_inc_calling_national_to_49

". Different rules apply to the calling number as to the called number because the called number is always the same (depending on the carrier either subscriber or national) but the calling number can be different (subscriber, national or international).

Criteria/Transformation:

Therefore the following criteria/transformation is applied:

1) Calling E164 -> Calling E164 or Calling TONE -> Calling TONE and

- Called E164 -> Called E164 or Called TONE -> Called TONE.



Figure 79: Mediatrix gateway 36xx - Call Router > Route Config

3.3.3.5 Analog Stations (Mediatrix 41xx)

Analog stations for the "Voice" or "Fax" service can be configured at a Mediatrix 41xx gateway.

IMPORTANT: For this device only DGW firmware is released. If you use SIP firmware, there is a high risk, that some of your scenarios will not work.

Analog stations in a Mediatrix 41xx gateway must be configured as SIP subscribers in OpenScape 4000.

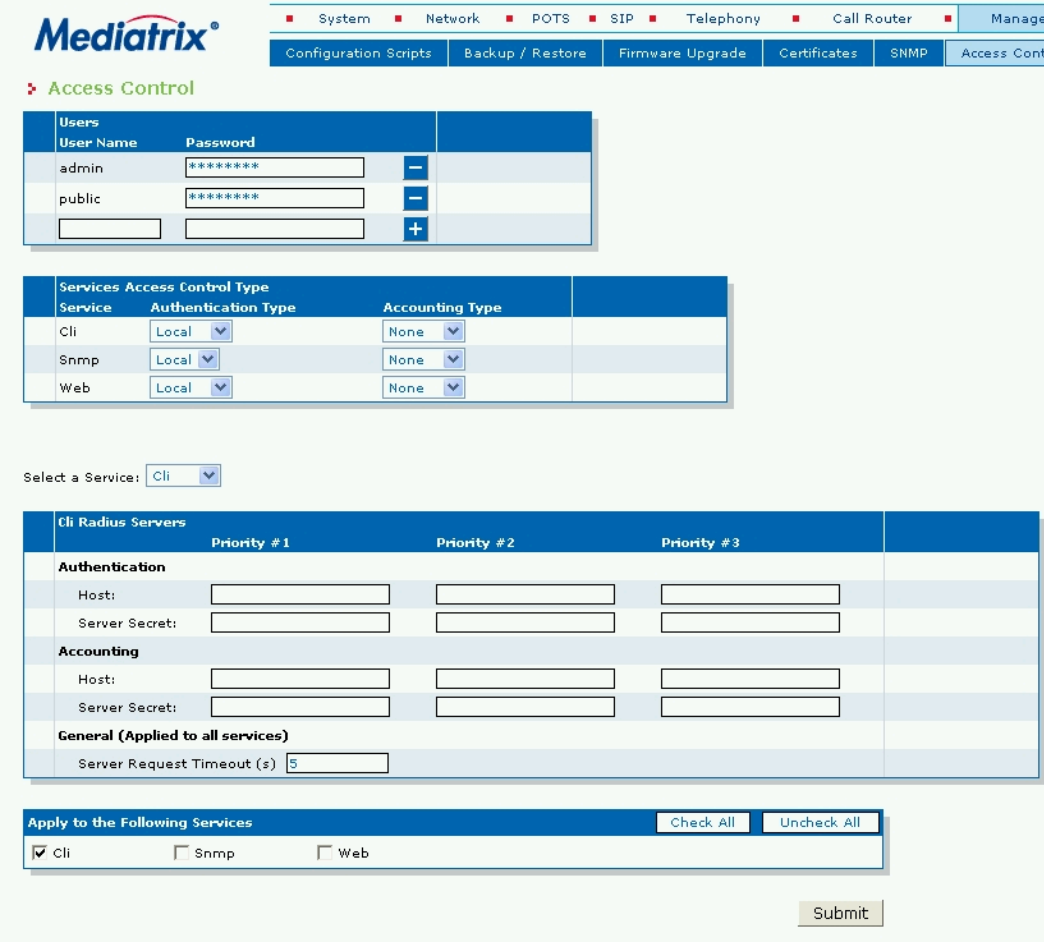
Example:

```
ADD-SBCSU:STNO=25030,OPT=OPTI,CONN=IP2,PEN=1-50-3-0,
DVCFIG=UFIP,TSI=1,COS1=2,COS2=2,LCOSV1=1,LCOSV2=1,LCOSD1=1,
LCOSD2=1,DPLN=0,ITR=0;
```

IMPORTANT: The DGW Mediatrix with default settings will not work correctly. Therefore, some of the parameters have to be changed manually. Please, pay attention to the sections SIP->Servers, SIP->Registrations, SIP->Interop, and SIP->Transport.

Management > Access Control

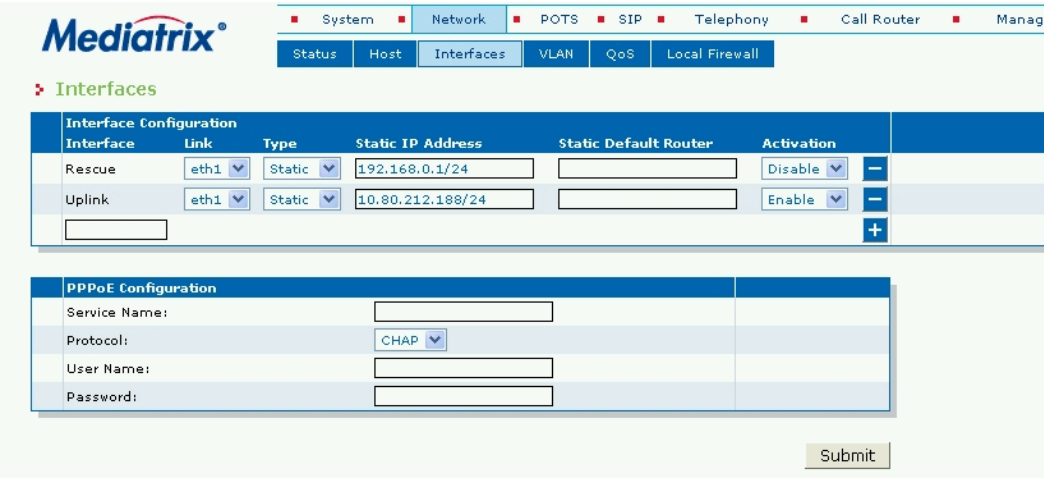
Configure the parameters for line administration and public.



Mediatrix 41xx - Management -> Access Control

Network > Interfaces

Configure the parameters for network settings in this mask. Configure the IP address, subnet mask, default router and SNMP port.



Mediatrix 41xx - Network -> Interfaces

Network > Host

Configure the parameters for network settings in this mask. Configure default router, DNS, SNTP.

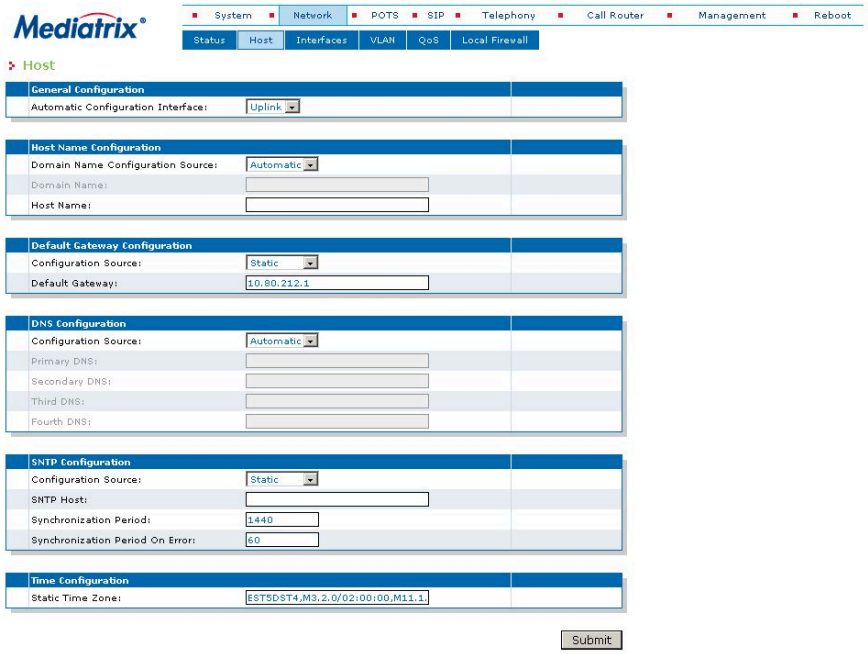
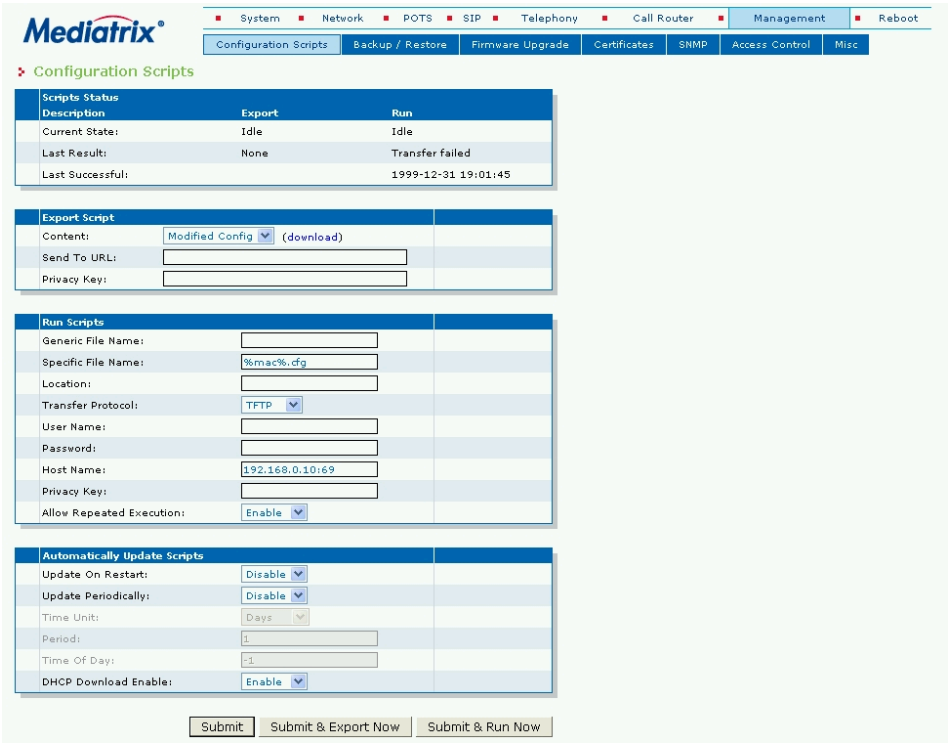


Figure 80: Mediatrix 41xx - Network -> Host

Management > Configuration Scripts

The download parameters for the configuration scripts are administered in this mask.

Enter the values for the configuration file server.



Mediatrix 41xx - Management -> Configuration Scripts

Management > Firmware upgrade

The download parameters for the firmware are administered in this window.

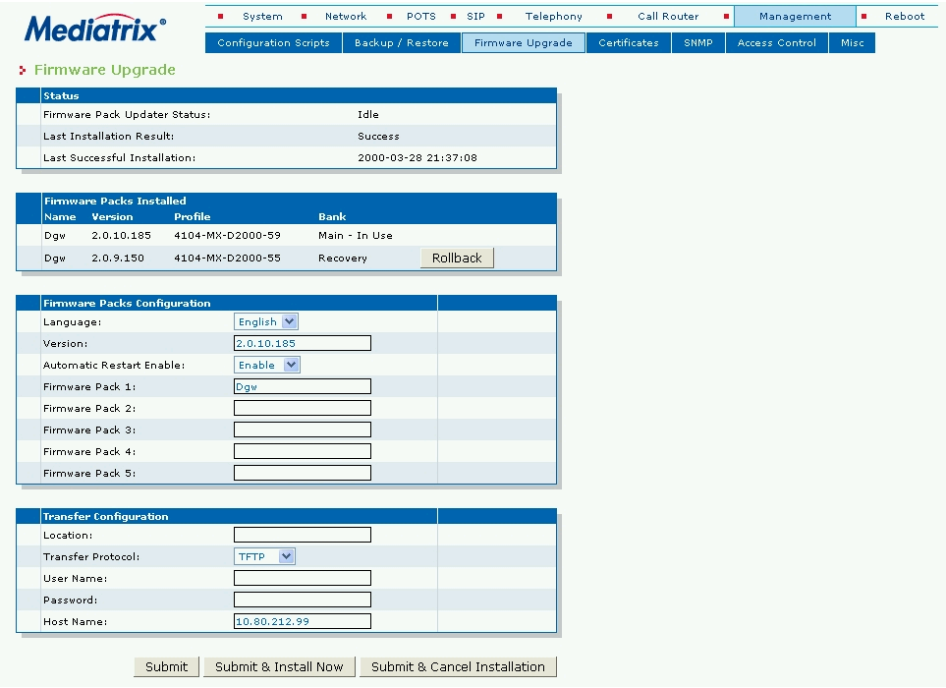


Figure 81: Mediatrix 41xx - Management -> Firmware Upgrade

SIP -> Servers

The parameters for the SIP servers are administered in this mask. Enter the IP address of the SIP server.

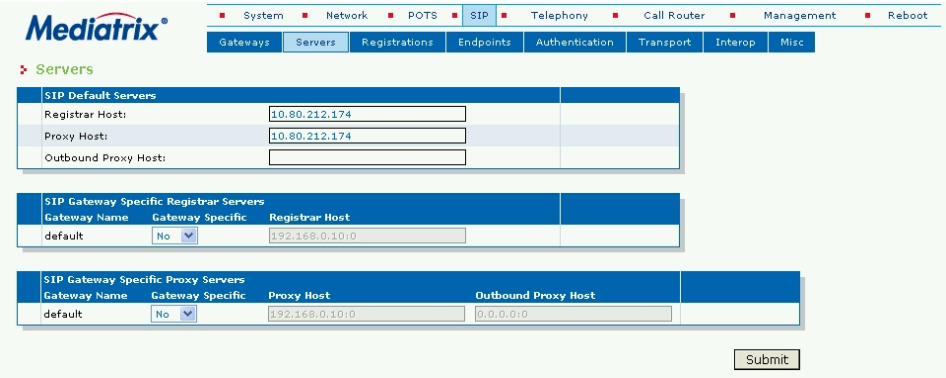
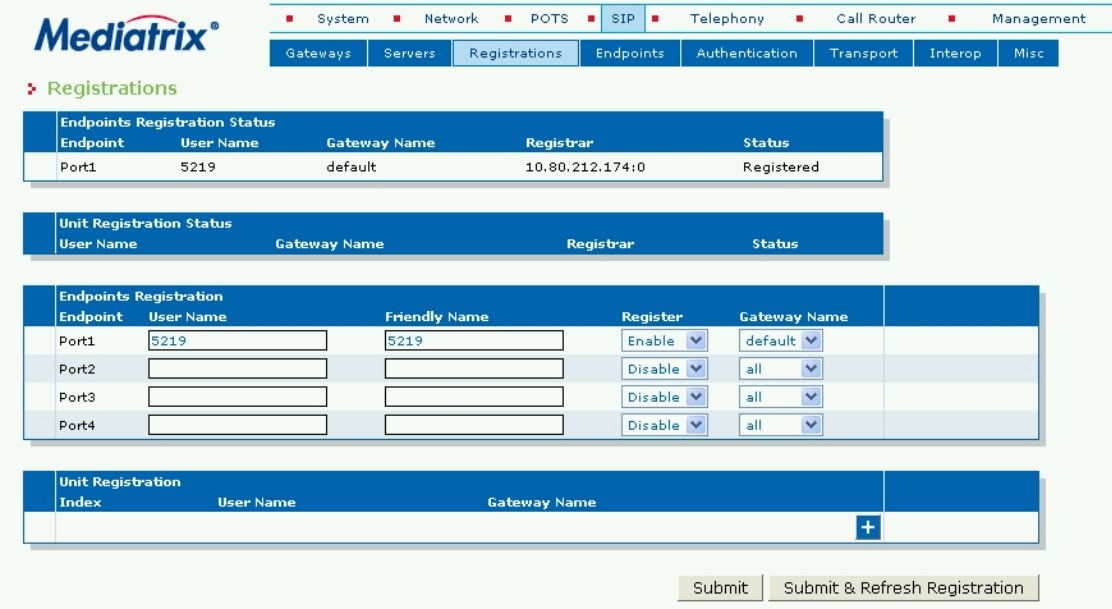


Figure 82: Mediatrix 41xx - SIP -> Servers

SIP -> Registrations

The parameters for the SIP subscribers are administered in this mask. Enter the station number and name for each subscriber. This data is also used to display caller ID information.



Mediatrix 41xx - SIP -> Registrations

SIP -> Interop

For correct functioning of Mediatrix 41xx, it is recommended to set values in boxes 406 and 488 to Use Previous Media Negotiation.

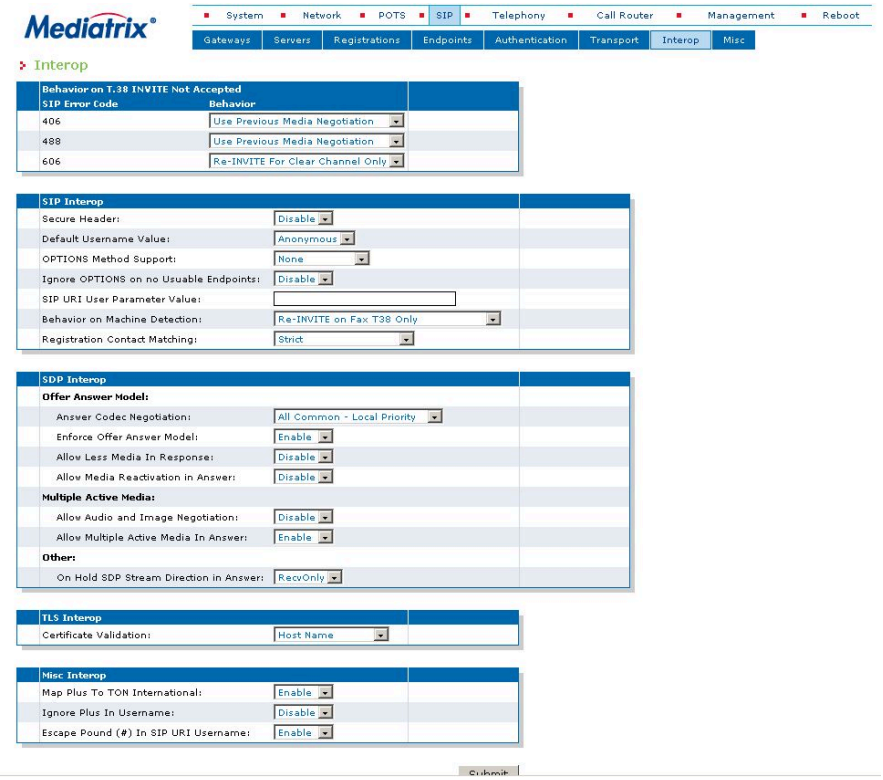


Figure 83: Mediatrix 41xx - SIP -> Interop

SIP -> Transport

For correct functioning of Mediatrix 41xx, it is recommended to set values for Transport to Enable.

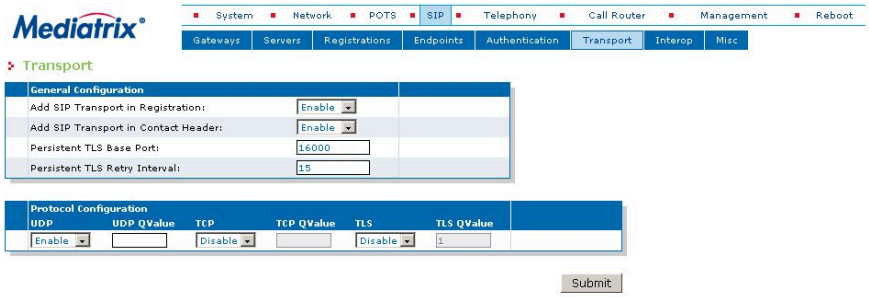


Figure 84: Mediatrix 41xx - SIP -> Transport

Telephony -> Codecs

Codec parameters are set in this mask (next three screenshots). The preferred codec is G.711 a-Law.

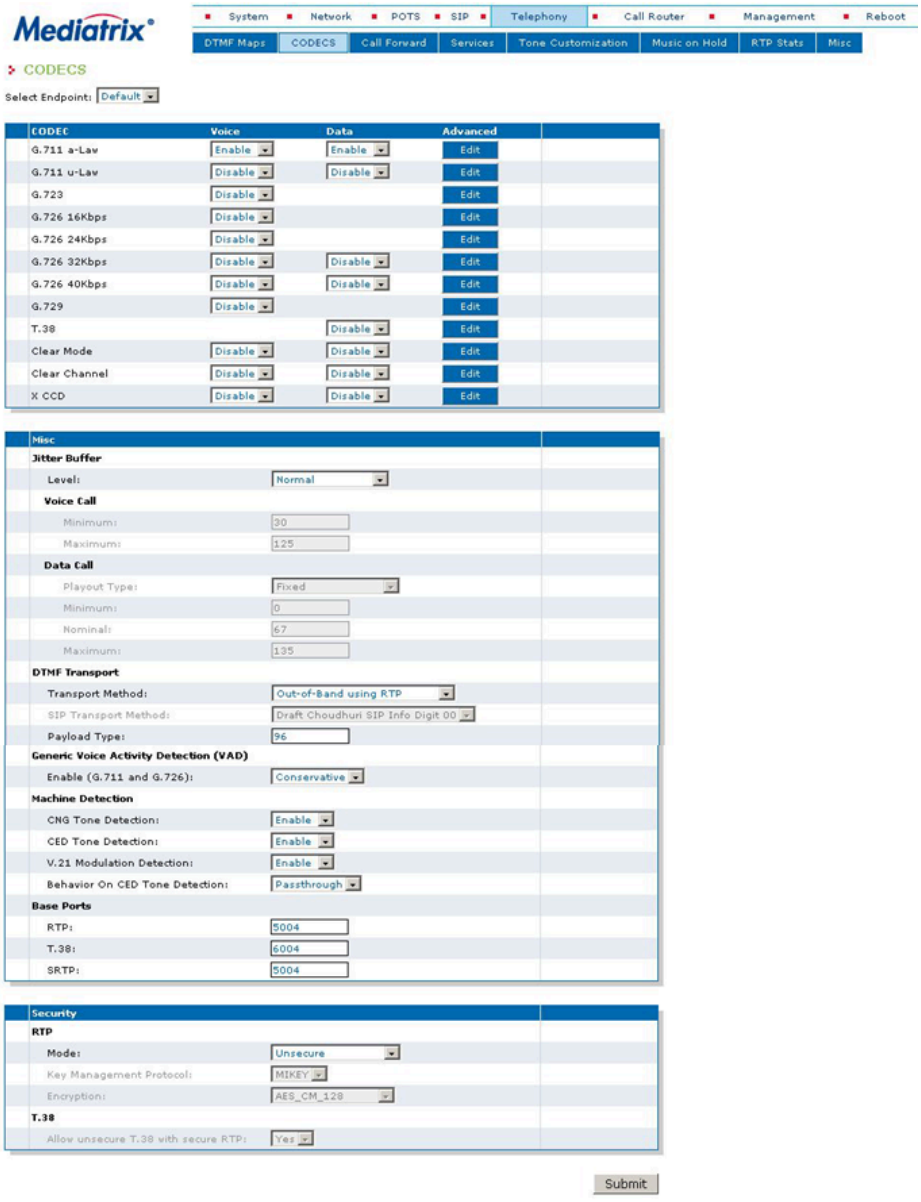


Figure 85: Mediatrix 41xx - Telephony -> Codecs

If more than one codec is needed to be allowed, then priority of each codec can be set under button **Edit**. Usable values are values in the range from 0 (lowest priority) to 10 (highest priority).



Mediatrix 41xx - Telephony -> Codecs

Telephony -> Misc

This mask allows you to configure country settings and custom tones.

- Country Selection germany1 = permanent dial tone
- Country Selection germany2 = interrupted dial tone (3 short beeps)



Figure 86: Mediatrix 41xx - Telephony -> Misc

3.3.3.6 Analog Trunking (Mediatrix 1204)

OpenScape 4000 SoftGate 50 > SIP trunk > Mediatrix 1204 > Analog trunk

3.3.3.6.1 Configuration on OpenScape 4000

Overview

- SoftGate 50 (SOCO) vIPDA shelf 50, direct link configuration with 120 B channels
- Slot 8, vSIP 04 trunk to Mediatrix 1204 (SIP <==> Telco analog trunk)
- NCUI configuration, LTU 50
- vSIP trunk to Mediatrix 1204 (SIP <==> Telco analog trunk)
- Mediatrix 1204 AMO configuration
- Set the Mediatrix proxy (ip 57) on OpenScape 4000 / SoftGate 50 / WBM SIP trunk (ip
- LCR settings

SoftGate 50 (SOCO) vIPDA shelf 50, direct link configuration with 120 B channels

```
ADD-UCSU:UNIT=AP,LTG=1,LTU=50,LTPARTNO=”Q2329-”,SRCGRP=50,FRMTYPE=SOCOAP,CONN▶
TYPE=APDL,LSRTADDR=155.75.27.50,APRTADDR=155.75.27.1,LOCID=050,LOCATION="DIRECT
LINK, CPCI#2",PHONE=9727145968,PLCHECK=YES,BCHLCNT=120,CON▶
VLAW=NO,TCLASS=0,ALARMNO=0,SOCOTYPE=SOCO50;
```

Slot 8, vSIP 04 trunk to Mediatrix 1204 (SIP <==> Telco analog trunk)

```
ADD-BCSU:MTYPE=IPGW,LTG=1,LTU=50,SLOT=8,PARTNO="Q2330-X ",FCTID=1,LWVAR=0,FCT▶
BLK=59,BCHL3550=4,ALARMNO=0;
```

NCUI configuration, LTU 50

```
CHANGE-STMIB:MTYPE=NCUI2,LTU=50,TYPE=GLOBAL,PATTERN=255;
CHANGE-STMIB:MTYPE=NCUI2,LTU=50,TYPE=IFDATA,VLAN=NO,TOSLAN=72,TOSMO▶
DEM=80,VLANID=0,BITRATE=100MBFD;
CHANGE-STMIB:MTYPE=NCUI2,LTU=50,TYPE=DSP,JITBUFD=60;
CHANGE-STMIB:MTYPE=NCUI2,LTU=50,TYPE=SERVIF,LOGINTRM="TRM",LOGINPPP="PPP";
CHANGE-STMIB:MTYPE=NCUI2,LTU=50,TYPE=SIGQOS,BANDW=0,MAX▶
RTD=0,MINTHRPT=0,SIGPTHSW=STD,QOSSTAT=NO;
CHANGE-
STMIB:MTYPE=NCUI2,LTU=50,TYPE=ASC,UDPPRTLO=29100,TOSPL=48,T38FAX=YES,RFCFMOIP=YE
S,RFCDTMF=YES,REDRFCTN=YES,PRIO=PRIO1,CODEC=G729,VAD=NO,RTP=20;
CHANGE-
STMIB:MTYPE=NCUI2,LTU=50,TYPE=ASC,UDPPRTLO=29100,T38FAX=YES,RFCFMOIP=YES,RFCDTMF
=YES,REDRFCTN=YES,PRIO=PRIO2,CODEC=G729A,VAD=NO,RTP=20;
CHANGE-
```

```
STMIB:MTYPE=NCUI2,LTU=50,TYPE=ASC,UDPPRTLO=29100,T38FAX=YES,RFCFMOIP=YES,RFCDTMF
=YES,REDRFCTN=YES,PRIO=PRIO3,CODEC=G711U,VAD=NO,RTP=20;
CHANGE-
STMIB:MTYPE=NCUI2,LTU=50,TYPE=ASC,UDPPRTLO=29100,T38FAX=YES,RFCFMOIP=YES,RFCDTMF
=YES,REDRFCTN=YES,PRIO=PRIO4,CODEC=G711A,VAD=NO,RTP=20;
CHANGE-
STMIB:MTYPE=NCUI2,LTU=50,TYPE=ASC,UDPPRTLO=29100,T38FAX=YES,RFCFMOIP=YES,RFCDTMF
=YES,REDRFCTN=YES,PRIO=PRIO5,CODEC=G729B,VAD=YES,RTP=20;
CHANGE-
STMIB:MTYPE=NCUI2,LTU=50,TYPE=ASC,UDPPRTLO=29100,T38FAX=YES,RFCFMOIP=YES,RFCDTMF
=YES,REDRFCTN=YES,PRIO=PRIO6,CODEC=G729AB,VAD=YES,RTP=20;
CHANGE-
STMIB:MTYPE=NCUI2,LTU=50,TYPE=ASC,UDPPRTLO=29100,T38FAX=YES,RFCFMOIP=YES,RFCDTMF
=YES,REDRFCTN=YES,PRIO=PRIO7,CODEC=NONE,VAD=NO,RTP=20;
```

REDRFCTN	Redundant transmission of the RFC2833 tones in accordance with RFC2198
RFCDTMF	Transmission of DTMF tones in accordance with RFC2833.
RFCFMOIP	Transmission of fax/modem tones in accordance with RFC2833

IMPORTANT: The parameters mentioned above must have the same value in all IPDA gateways (STMI2/4/X (vSTMI) with regard to AMO CGWB & NCUI2+/4 (vNCUI) with regard to AMO STMIB). This avoids problems and a common function across all systems is achieved!

```
CHANGE-STMIB:MTYPE=NCUI2,LTU=50,TYPE=H323,Q931T1=50,Q931T2=500,GWNAME="HG3575-
2";
CHANGE-STMIB:MTYPE=NCUI2,LTU=50,TYPE=DMCDATA,DMCALLWD=NO,DMCCONN=0;
CHANGE-STMIB:MTYPE=NCUI2,LTU=50,TYPE=SNMP,CS1="public";
CHANGE-STMIB:MTYPE=NCUI2,LTU=50,TYPE=MGNTDATA,MGNTPN=8000,BUSPN=443;
CHANGE-STMIB:MTYPE=NCUI2,LTU=50,TYPE=WBMDATA,LOGINWBM="HP4K-DEVEL",ROLE=ENGR;
CHANGE-STMIB:MTYPE=NCUI2,LTU=50,TYPE=WBMDATA,LOGINWBM="HP4K-SU",ROLE=SU;
CHANGE-STMIB:MTYPE=NCUI2,LTU=50,TYPE=WBMDATA,LOGINWBM="HP4K-ADMIN",ROLE=ADMIN;
CHANGE-STMIB:MTYPE=NCUI2,LTU=50,TYPE=WBMDATA,LOGINWBM="HP4K-READER",ROLE=READON►
LY;
CHANGE-STMIB:MTYPE=NCUI2,LTU=50,TYPE=GWSECTOR,GWSECTNO=0;
CHANGE-STMIB:MTYPE=NCUI2,LTU=50,TYPE=DLSDATA,DLSIPADR=192.0.2.40,DL►
SPORT=18443,DLSACPAS=NO;
CHANGE-STMIB:MTYPE=NCUI2,LTU=50,TYPE=SOCODATA,CLAIPADR=155.75.27.50;
```

vSIP trunk to Mediatrix 1204 (SIP <==> Telco analog trunk)

```
ADD-CGWB:LTU=50,SLOT=8,SMODE=NORMAL,IPADR=155.75.27.58,NETMASK=255.255.255.0;
CHANGE-
CGWB:MTYPE=CGW,LTU=50,SLOT=8,TYPE=GLOBIF,PATTERN=255,VLAN=NO,VLANID=0,DEFRT=155.
75.27.1,BITRATE=100MBFD,TRPRSIP=4,TRPRSIPQ=0,TRPRH323=0,TPRH323A=0,TLSP=4060,DN►
SIPADR=0.0.0.0;
CHANGE-CGWB:MTYPE=CGW,LTU=50,SLOT=8,TYPE=SERVIF,LOGINTRM="TRM";
CHANGE-
CGWB:MTYPE=CGW,LTU=50,SLOT=8,TYPE=ASC,UDPPRTLO=29100,TOSPL=48,TOSSIGNL=184,T38FA
X=YES,RFCFMOIP=YES,RFCDTMF=YES,REDRFCTN=YES,PRIO=PRIO1,CODEC=G729,VAD=NO,RTP=20;
```

REDRFCTN	Redundant transmission of the RFC2833 tones in accordance with RFC2198
RFCDTMF	Transmission of DTMF tones in accordance with RFC2833.
RFCFMOIP	Transmission of fax/modem tones in accordance with RFC2833

IMPORTANT: The parameters mentioned above must have the same value in all IPDA gateways (STMI2/4 (vSTMI) with regard to AMO CGWB & NCUI2+/4 (vNCUI) with regard to AMO STMIB). This avoids problems and a common function across all systems is achieved!

```
CHANGE-CGWB:MTYPE=CGW,LTU=50,SLOT=8,TYPE=ASC,PRIO=PRIO2,CO►
DEC=G729A,VAD=NO,RTP=20;
CHANGE-CGWB:MTYPE=CGW,LTU=50,SLOT=8,TYPE=ASC,PRIO=PRIO3,CO►
DEC=G711U,VAD=NO,RTP=20;
CHANGE-CGWB:MTYPE=CGW,LTU=50,SLOT=8,TYPE=ASC,PRIO=PRIO4,CO►
DEC=G711A,VAD=NO,RTP=20;
CHANGE-CGWB:MTYPE=CGW,LTU=50,SLOT=8,TYPE=ASC,PRIO=PRIO5,CO►
DEC=NONE,VAD=NO,RTP=20;
CHANGE-CGWB:MTYPE=CGW,LTU=50,SLOT=8,TYPE=ASC,PRIO=PRIO6,CO►
DEC=G729B,VAD=YES,RTP=20;
CHANGE-CGWB:MTYPE=CGW,LTU=50,SLOT=8,TYPE=ASC,PRIO=PRIO7,CO►
DEC=G729AB,VAD=YES,RTP=20;
CHANGE-CGWB:MTYPE=CGW,LTU=50,SLOT=8,TYPE=DSP,JITBUFD=60;
CHANGE-CGWB:MTYPE=CGW,LTU=50,SLOT=8,TYPE=MGNTDATA,MGNTPN=8000,BUSPN=443;
CHANGE-CGWB:MTYPE=CGW,LTU=50,SLOT=8,TYPE=DMCDATA,DMCCONN=4;
CHANGE-CGWB:MTYPE=CGW,LTU=50,SLOT=8,TYPE=WBMDATA,LOGINWBM="HP4K-DEVEL",ROLE=EN►
GR;
CHANGE-CGWB:MTYPE=CGW,LTU=50,SLOT=8,TYPE=WBMDATA,LOGINWBM="HP4K-SU",ROLE=SU;
CHANGE-CGWB:MTYPE=CGW,LTU=50,SLOT=8,TYPE=WBMDATA,LOGINWBM="HP4K-ADMIN",ROLE=AD►
MIN;
CHANGE-CGWB:MTYPE=CGW,LTU=50,SLOT=8,TYPE=WBMDATA,LOGINWBM="HP4K-READ►
ER",ROLE=READONLY;
CHANGE-CGWB:MTYPE=CGW,LTU=50,SLOT=8,TYPE=GWDATA,GWID1="PRIMARYRASMANAGERID";
CHANGE-CGWB:MTYPE=CGW,LTU=50,SLOT=8,TYPE=H235DATA,SECSUBS=NO,SECTRNK=NO,GLO►
BID1="Gateway2003",TIMEWIN=100,GLOBPW=242-191-30-119-188-83-173-161-43-0-70-36-
218-74-169-221-78-102-174-170;
CHANGE-CGWB:MTYPE=CGW,LTU=50,SLOT=8,TYPE=SIPTRERH,GWAUTREQ=NO;
CHANGE-
CGWB:MTYPE=CGW,LTU=50,SLOT=8,TYPE=SIPTRSSA,SIPREG=NO,REGIP1=0.0.0.0,PORTTCP1=506
0,PORTTLS1=5061,REGTIME=120,REGIP2=0.0.0.0,PORTTCP2=5060,PORTTLS2=5061;
CHANGE-CGWB:MTYPE=CGW,LTU=50,SLOT=8,TYPE=DLSDATA,DLSIPADR=192.0.2.40,DL►
SPORT=18443,DLSACPAS=NO;
```

Mediatrix 1204 AMO configuration

```
ADD-BUEND:TGRP=58,NAME="MEDIATRIX_1204 ",NO=8,TRACENO=0,ACDTHRH=*,PRIONO=1,TD►
DRFLAG=ON,GDTRRULE=0,ACDPMGRP=0,CHARCON=NEUTRAL;
ADD-TDCSU:OPT=NEW,PEN=1-50-008-
0,COTNO=59,COPNO=59,DPLN=0,ITR=0,COS=59,LCOSV=1,LCOSD=1,CCT="",DESTNO=58,PROTVAR
=ECMAV2,SEGMENT=8,DEDSVC=NONE,TRTBL=GDTR,SIDANI=N,ATNTYP=CO,CBMATTR=NONE,TCHARG=
N,SUPPRESS=0,TRACOUNT=31,SATCOUNT=MANY,NNO=58,ALARMNO=2,FIDX=1,CARRIER=1,ZONE=EM
```

```
PTY,COTX=59,FWDX=1,CHIMAP=N,UUSCCX=16,UUSCCY=8,FNIDX=1,NWMUXTIM=10,SRCGRP=50,CLA
SSMRK=EC&G711&G729AOPT,TGRP=58,SRCHMODE=CIR,INS=Y,SECLEVEL=SECURE,DEV=HG3550CO,B
CHAN=1&&4,BCNEG=N,BCGR=1,LWPAR=2,LWPP=0,LWLT=0,LWPS=0,LWR1=0,LWR2=0,DMCALLWD=N;
ADD-
COT:COTNO=59,PAR=PRI&RCL&ANS&KNOR&CEBC&CBBN&CBFN&FWDN&FNAN&COTN&BSHT&BLOC&PROV&A
TRS&TSCS&ICZO&TRSC&CFOS&CFVA&PINR&AOCC&BCNE&NTON;
```

Set the Mediatrix proxy (ip 57) on OpenScape 4000 / SoftGate 50 / WBM SIP trunk (ip 58)

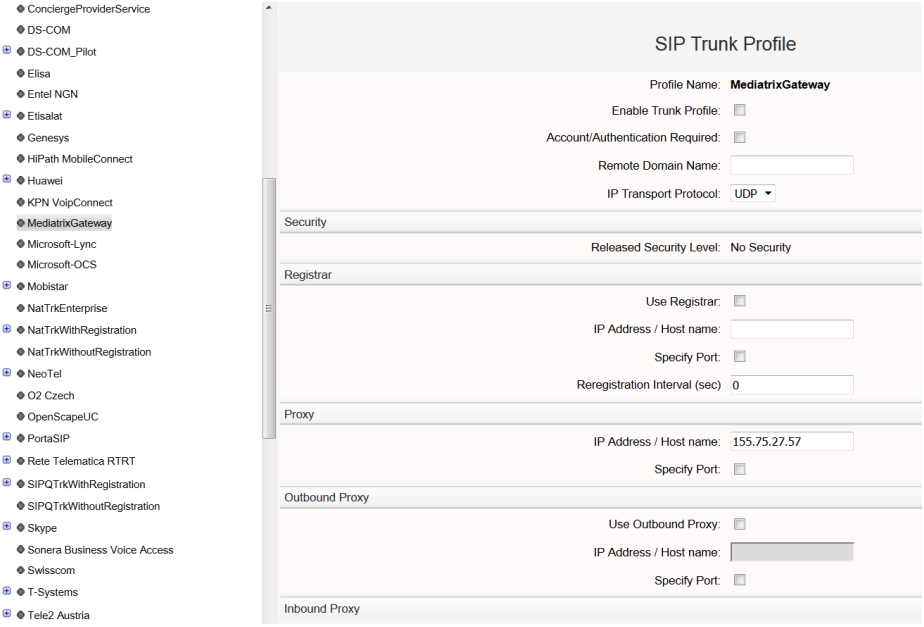


Figure 87: Mediatrix 1204 Gateway - WBM - SIP trunk profile

The MediatrixGateway folder should be activated, right mouse click > ACTIVATE ==> folder turns green.

LCR settings

AMO WABE - Access code for outbound call through Mediatrix 1204

```
ADD-WABE:CD=958,DAR=TIE,CHECK=N;
```

AMO LDPLN

```
ADD-LDPLN:LCRCONF=LCRPATT,DIPLNUM=0,LDP=958-W-Z,PROFIDX=58,LAUTH=1,PINDP=N;
```

W	second "external" dial tone
Z	any number and limited to total 22 digits, ended with timeout or # "pound" key by stations
LDP	If Telco is set to 10 digits then better LDP = 958-W-XXXXXXXXXX

AMO LPROF

```
ADD-LPROF:PROFNAME="SIP TRK SG 50-8",SRCGRP=1&25&50,LRTE=958,PROFIDX=58;
```

AMO LDAT - Attribute of CDR and send PUBNUM from station

```
ADD-LDAT:LROUTE=958,LSVC=ALL,LVAL=1,TGRP=58,ODR=959,LAUTH=1,CARRIER=1,ZONE=EMP►
TY,LATTR=WCHREG&PUBNUM,VCCYC=4;
```

AMO LODR - echo field 3 = Z from “958-W-Z”

```
ADD-LODR:ODR=959,CMD=ECHO,FIELD=3;
```

```
ADD-LODR:ODR=959,CMD=NPI,NPI=UNKNOWN,TON=UNKNOWN;
ADD-LODR:ODR=959,CMD=END;
ADD-LODR:ODR=959,INFO="SIP TRK SG 50-9";
```

AMO RICHT

```
ADD-RICHT:MODE=LRTENEW,LRTE=958,LSVC=ALL,NAME="MEDTRX1204 508",TGRP=58,DN►
NO=58,ROUTATT=YES,EMCYRTT=NO,PDNNO=0,CHARCON=NEUTRAL,CONFTONE=NO,RERINGRP=NO,NOP
RCFWD=NO,NITO=NO,CLNAMEDL=NO,FWDSWTCH=NO,LINFEMER=NO,NOINTRTE=NO;
```

3.3.3.6.2 Configuration Notes

On Default MDX1204 is set to DHCP. Get a wireshark or ethereal sniffer trace on mirrored port at customer data switch to find the ip assigned by DHCP to MDX or ask the customer IT department. If a recovery mode is performed, the Mediatrix 1204 uses the default IP address 192.168.0.1.

Overview

- LAN Settings on fixed IP 155.75.27.57
- General Configuration of Mediatrix 1204
- Configuration with Mediatrix software Unit Manager Express (UME)
- Mediatrix 1204 firmware upgrade

LAN Settings on fixed IP 155.75.27.57

Management > Network Settings

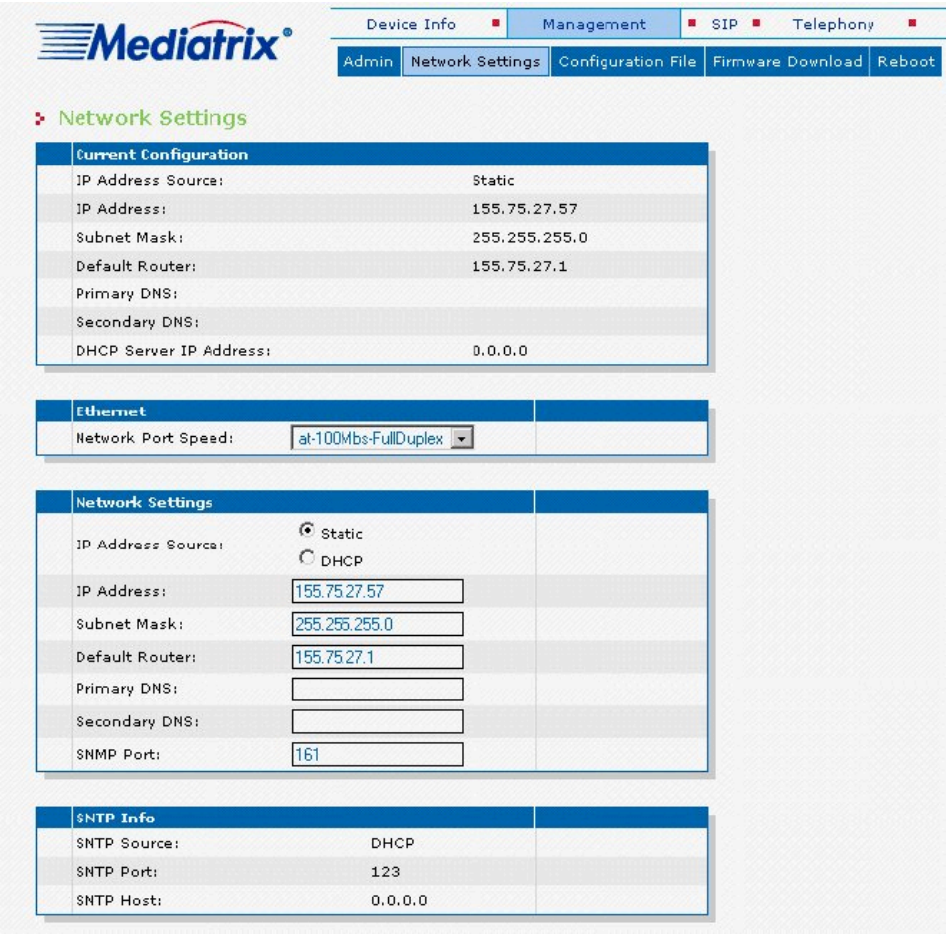


Figure 88: Mediatrix 1204 Gateway - LAN settings

General Configuration of Mediatrix 1204

Mediatrix 1204 pointing to OpenScape 4000 SoftGate 50 SIP trunk (AMO BCSU, PEN 1-50-8-0 = IP 155.75.27.58)

Port User Name = Telco Analog Trunk

Connected to the port of MDX, will appear 1234567890 on the display of the stations on Telco incoming calls from Line 1.

Incoming calls from Line 4 will display 333004 on OpenScape 4000 station; designated for line 4.

Also utilized on SIP: Invite 333004@ip_addr.

Management > Configuration File

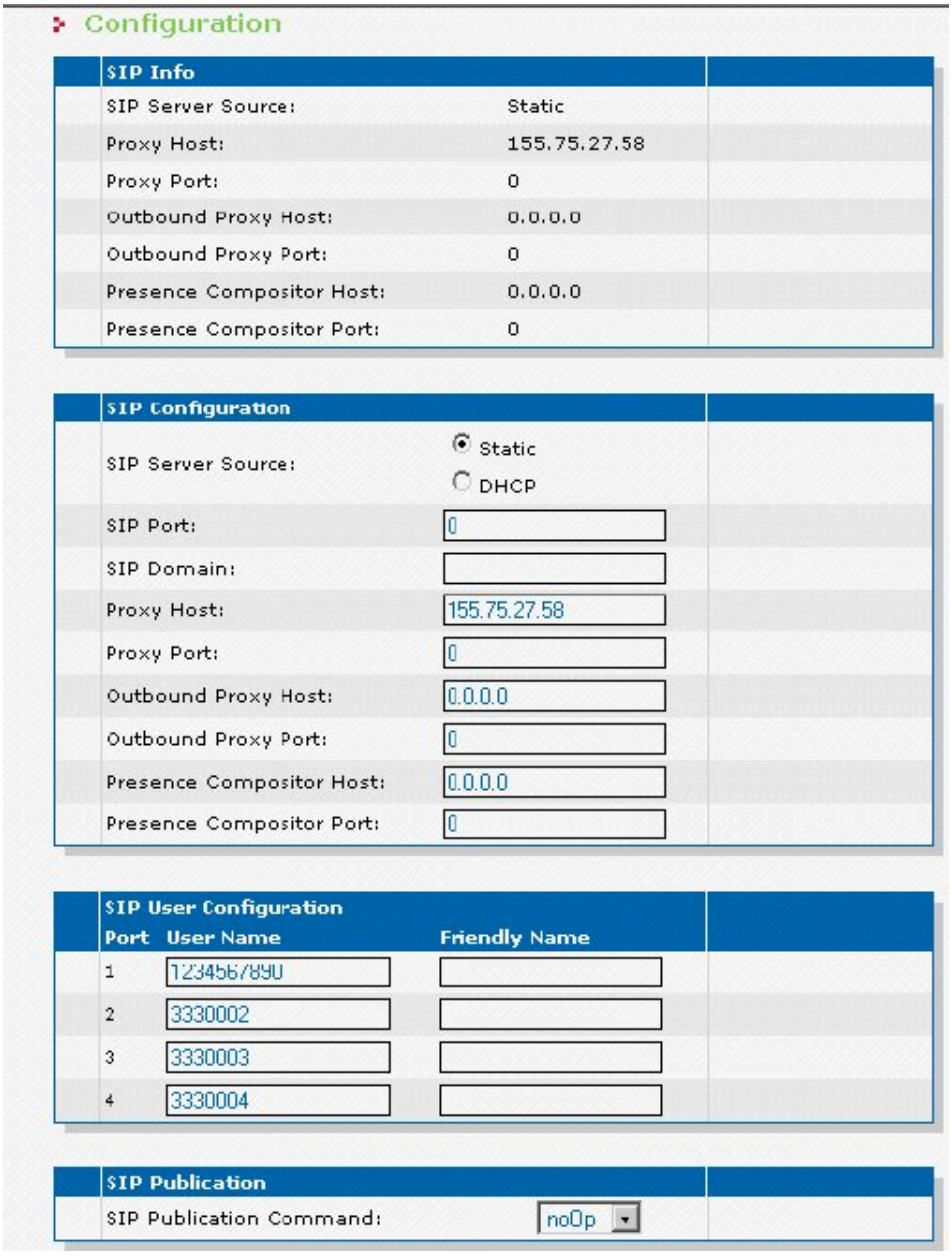


Figure 89: Mediatrix 1204 Gateway - configuration

Configuration with Mediatrix software Unit Manager Express (UME)

The following changes on MDX1204 requires an installation of Mediatrix software **UMN** (**U**nit **M**anager **N**etwork) on your PC. It can be found on **SWS > Partner Products > Mediatrix 1204** or on Internet (http://www.media5corp.com/support/mediatrix--media5boss/downloads). Also the documentation is on DMS or on MDX web site.

The **UME** (**U**nit **M**anager **E**xpress) below is a subprogram of UMN.

The Right Mouse Click on Field **fxoIfAnalogLineType** will show:

1) Get = retrieve the parameter and show it.

- Set = send your change of the parameter to MDX.

- mx1204_MIB_line_type_change_set = Telco analog trunk LS or GS on Lines 1 to 4.

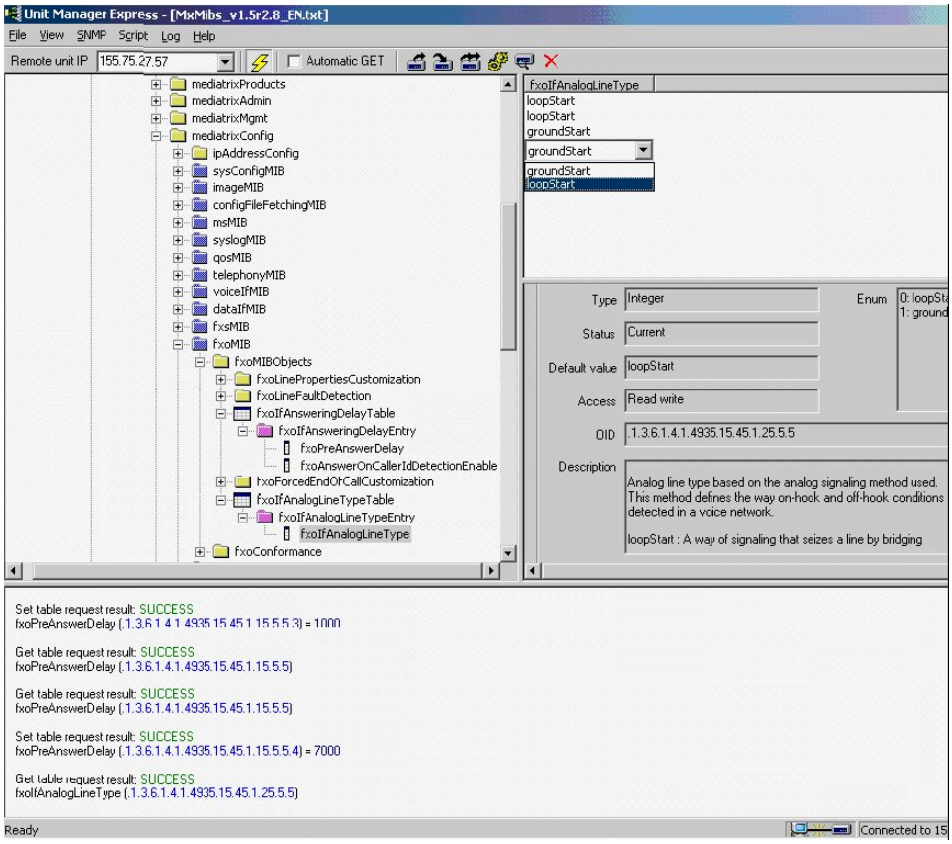


Figure 90: Mediatrix 1204 Gateway - Telco analog trunk LS or GS on lines 1 to 4

- mx1204_MIB_enable_incoming_ringing_direct_to_stn
- Has enabled on line 1 & 4 the incoming calls to ring direct to OpenScape 4000 station. The lines 2 & 3 will receive second dial tone from MDX on

incoming calls from Telco and the external party should dial the OpenScape 4000 station number to be connected.

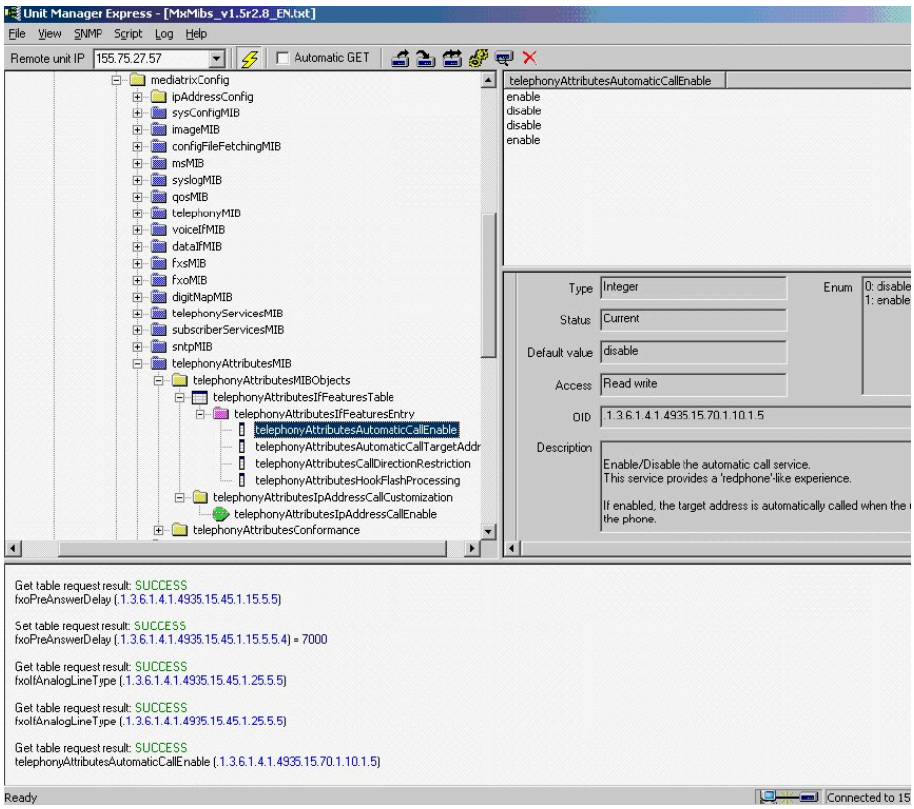


Figure 91: Mediatrix 1204 Gateway - Enable incoming ringing direct to station on line 1 and 4

Line 1 on incoming call from Telco will ring on station 25015

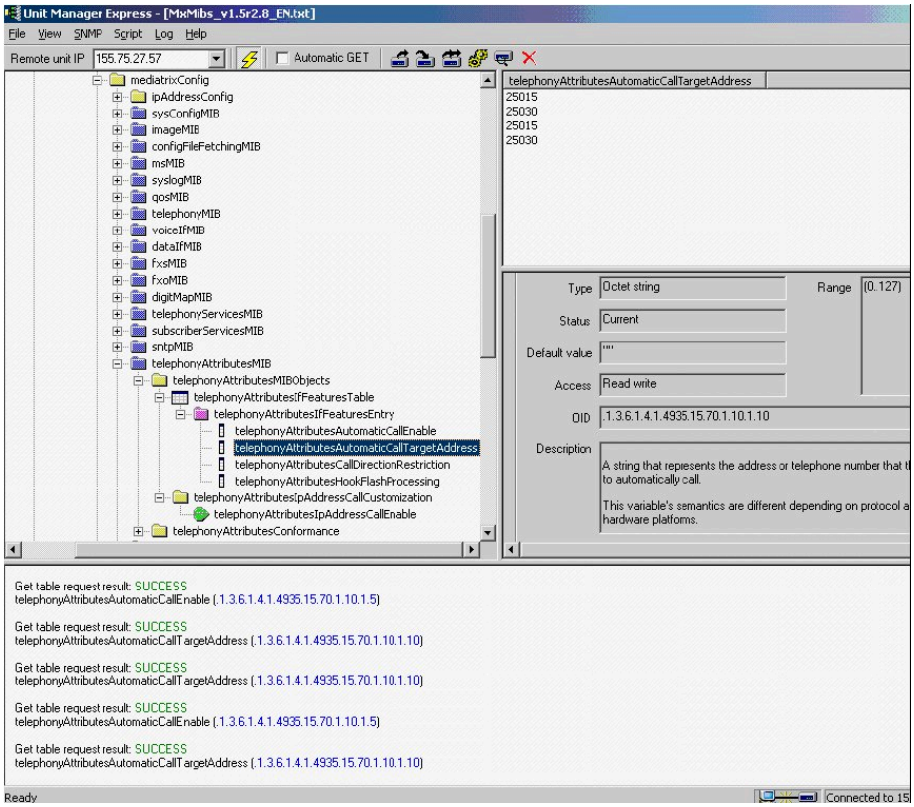


Figure 92: Mediatrix 1204 Gateway - Line 1 on incoming call from Telco will ring direct on station 25015

- mx1204_MIB_delay_incoming_ringing

- Lines 1 & 4 will be delayed in 1 second to ring on OpenScape 4000 station from Telco incoming calls.

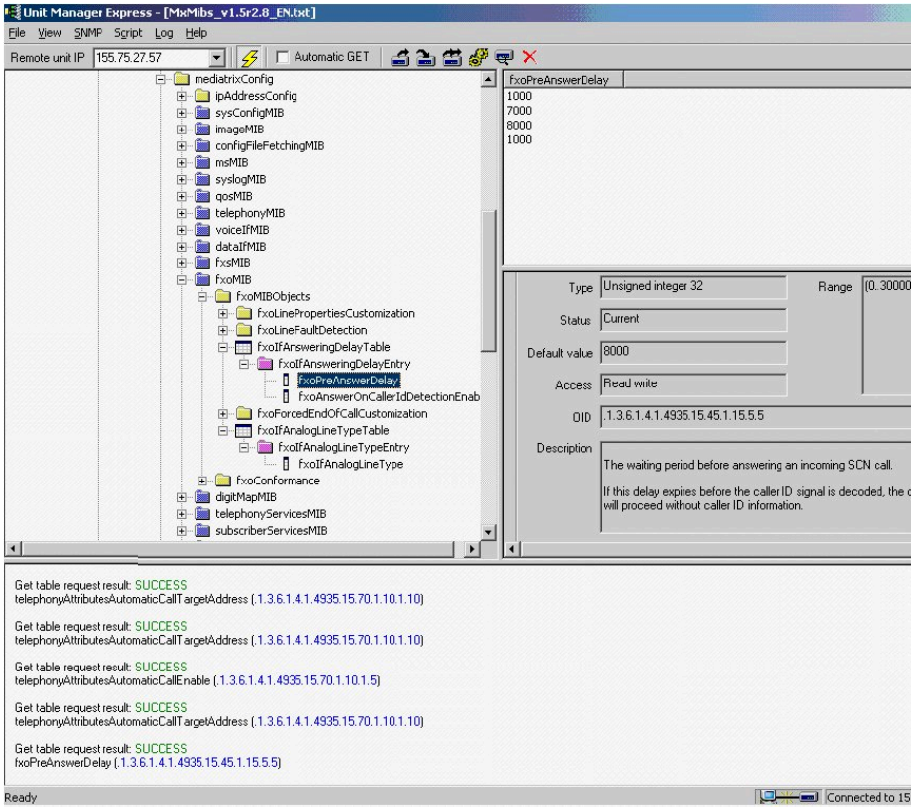


Figure 93: Mediatrix 1204 Gateway - Dealy of incoming ringing

Mediatrix 1204 firmware upgrade

SW version upgraded to:

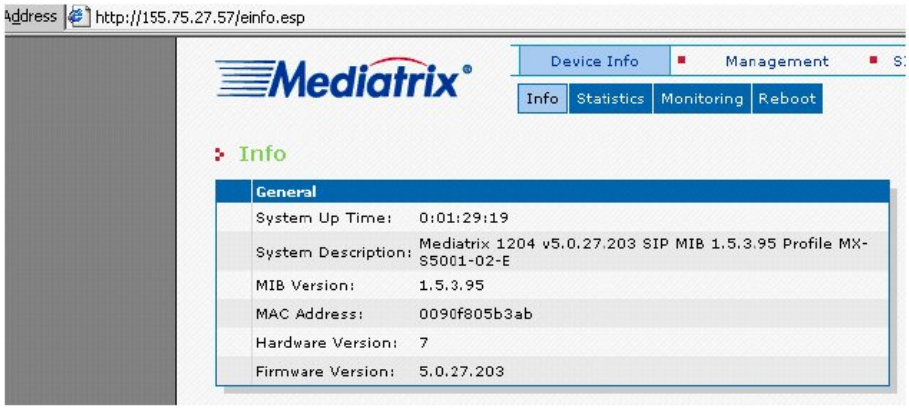


Figure 94: Mediatrix 1204 - Firmware

Procedure:

- Download the new version from MDX web page (http://www.media5corp.com/support/mediatrix--media5boss/downloads).
- Use a TFTP software (e.g. 3CDaemon, free on Internet)
- Unzip/Extract the download firmware file to a directory set on TFTP (our example C:\Documents and Settings\om837441\My Documents\0_Lixo\)

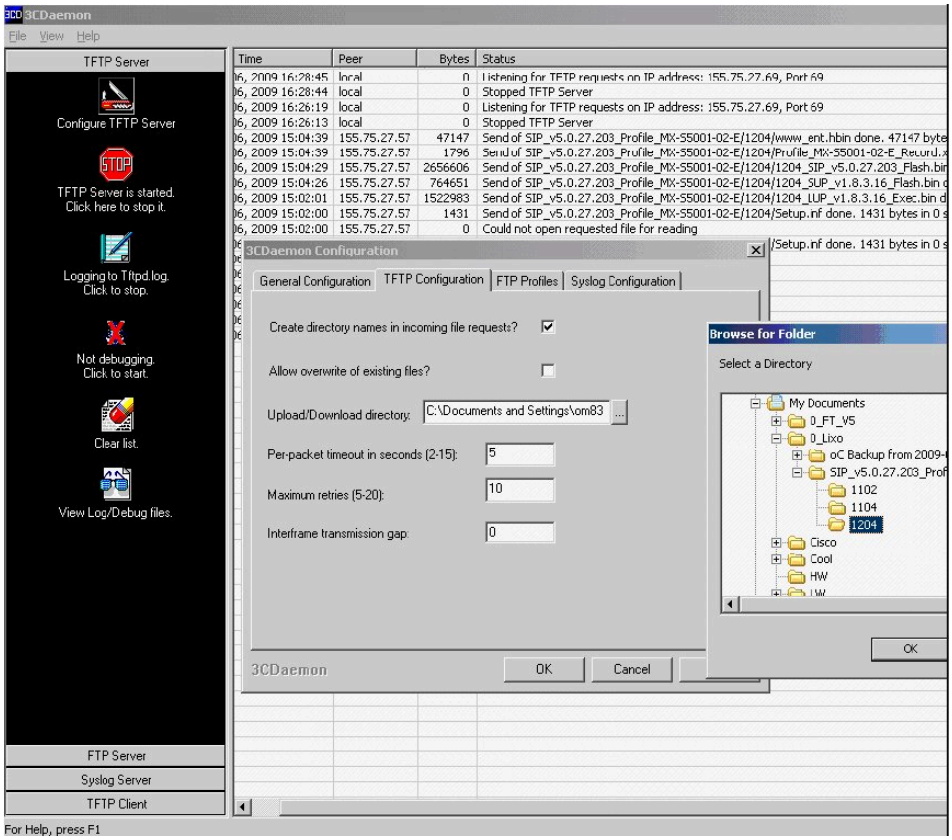


Figure 95: Mediatrix 1204 - Firmware download

Back on MDX, the Server Host is your PC IP Address 155.75.l27.69 where the 3CDaemon is running. Fill the Firmware Location, the final Status you see on window FW Download.

Path:

Attend that requires only the name SIP_v5.0.27.203_Profile_MX-S5001-02-E \1204 where the file Setup.inf is located after unzip is done!

C:\Documents and Settings\om837441\MyDocuments\0_Lixo \SIP_v5.0.27.203_Profile_MX-S5001-02-E\1204

FW Download on Restart = REBOOT THE Mediatrix1204 and the 3CDaemons log will show the FW being transfered (Send of Sip....) from your PC (IP.69) to MDX1204 (IP.57) as on 3CDaemon screenshot 15:02:00....

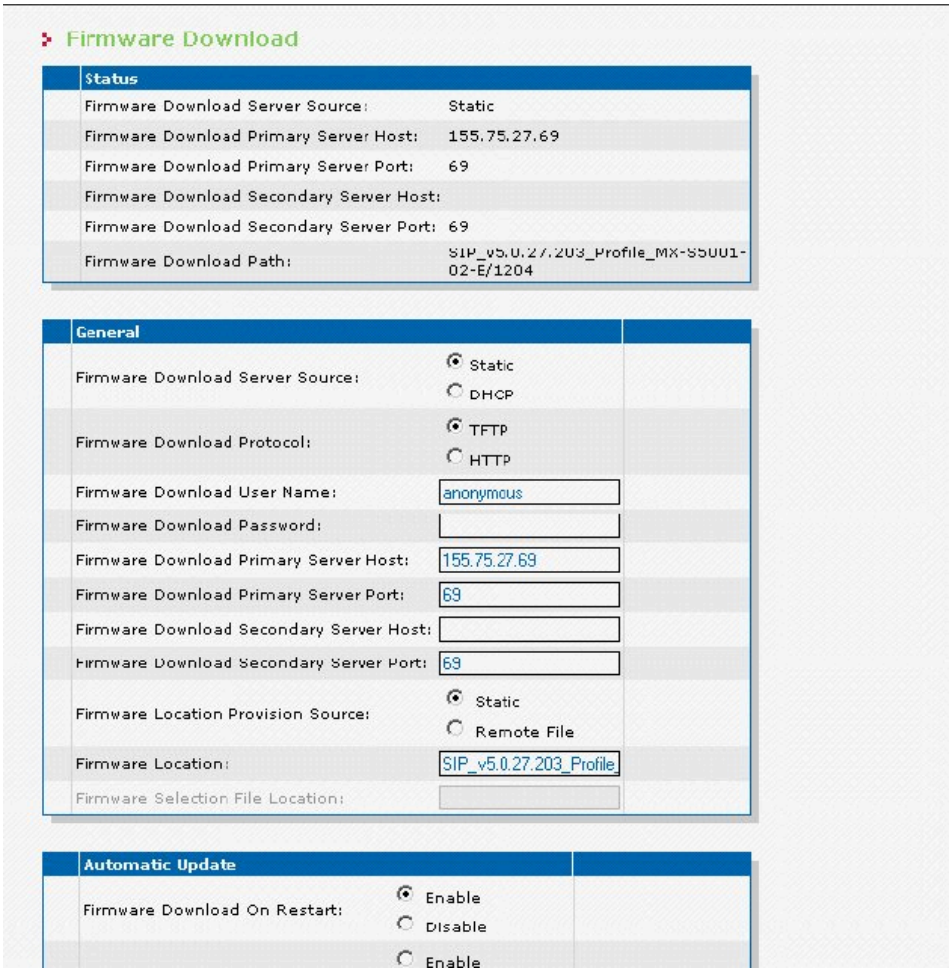


Figure 96: Mediatrix 1204 - Managent > Firmware Download

3.3.4 Error Detection with Syslog for Mediatrix 44xx and 36xx

Logging/trace information or debugging messages are sent to an external syslog-server. Therefore it is necessary to have a reachable syslog server e.g. 3CDaemon. You must configure the Syslog daemon server to capture those messages. Set the static IP address or domain name and port number of the device where the syslog-server is running in the Remote Host field.

If no Syslog daemon address is provided by a DHCP server or specified by the administrator, no messages are sent.

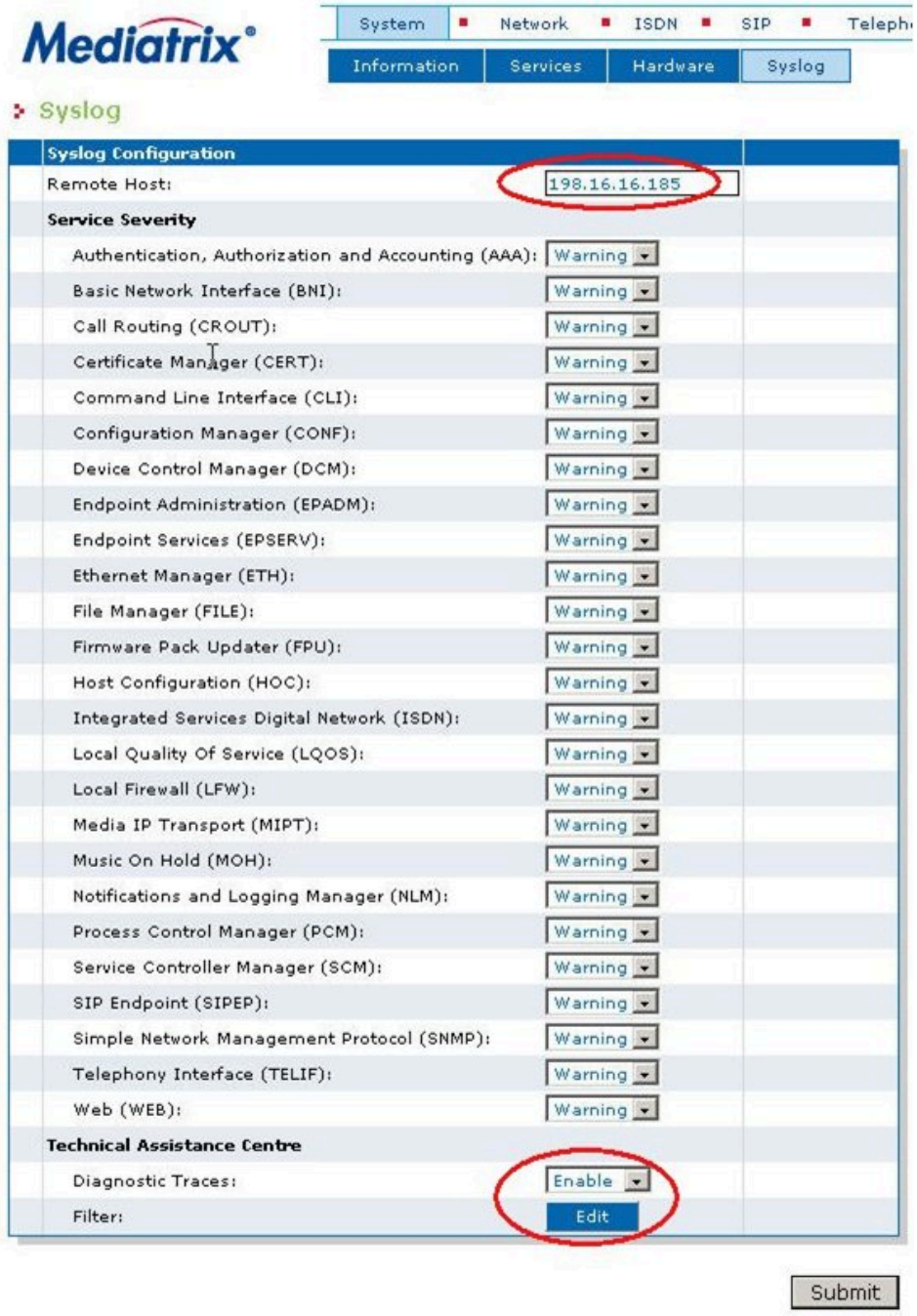


Figure 97: Syslog - System > Syslog > Diagnostic Traces

In the Service Severity section, select the minimal severity to issue a notification message for the various services in the corresponding drop-down menus.

When setting severity to Debug all notification messages are issued.

If you want to have detailed log information enable diagnostic traces by setting the **Diagnostic Traces** drop-down menu to **Enable**.

If applicable, define the filter applied to diagnostic traces by clicking the **Edit** button in the **Filter** field.



Figure 98: Syslog - System > Syslog > Diagnostic Traces > Edit

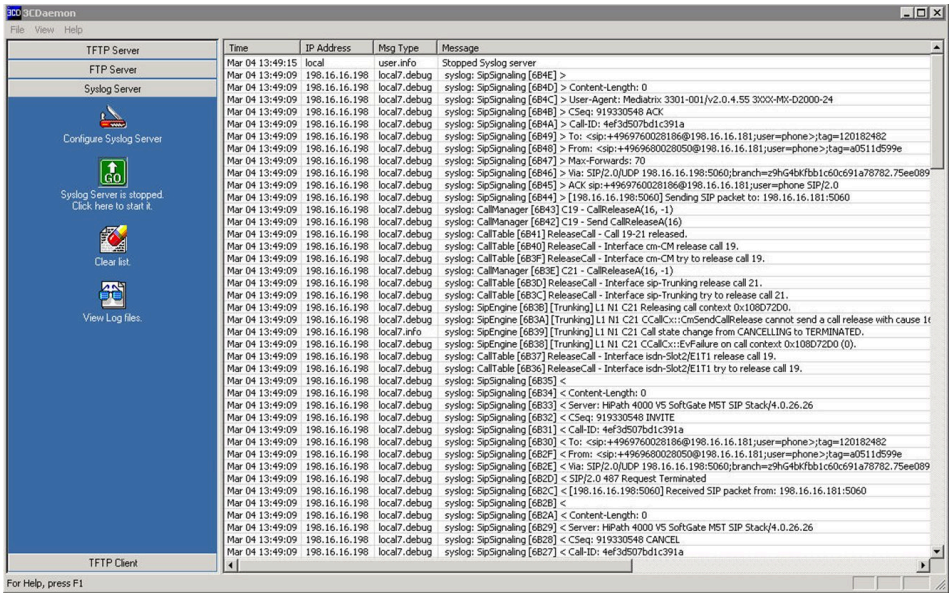
Problems with the ISDN interface:

- If you have problems with the ISDN interface (E1/T1/S0) it's recommended to set ISDN to All.
- You may not want the ISDN stack massages except the Layer 3 information, which is "ISDN Stack Q.931 Interpreted frames"
- For investigation problems with DTMF-Map, Mapping tables, hunting ... set Call Router to Debug
- SIP messages can be traced by setting SIP to Debug.

For general problems at least the following needs to be provided:

- An ethereal trace containing the SIP messages.
- A syslog trace with the following values set to debug:
  - Integrated Services Digital Network (Isdn)
  - Media IP Transport (Mipt)
  - SIP Endpoint (SipEp)
  - Telephony Interface (TelIf)
  - Diagnostic Traces

  Click edit for the filters and set to debug or ALL the following traces:
- call Router
- ISDN
- Line
- SIP
- Stream



3.4 Video Connections

OpenScape 4000 SoftGate (and the STMIX/STMIY) offers video support for both native SIP subcribers and trunks, using SIP Media Proxy (SMP) feature.

The SMP feature allows an SDP to traverse the OS4K transparently, resulting in E2E codec negotiation.

DMC feature configuration is mandatory to allow SMP negotiation.

The information required for SMP resulting in E2E video codec negotiation and payload is also transported networkwide via Cornet NQ protocol.

3.4.1 Restrictions

- Video endpoints are only supported at OpenScape 4000 SoftGate and STMIX/STMIY
- No interworking with HFA video endpoints and TDM video endpoints.
- Video is only possible for DMC slave connections.
- A video connection cannot be added to an existing audio connection and SDP re-negotiation cannot be performed (e.g. video/audio codecs) if the DMC connection is already ongoing.
- The DMC connection (Video) is interrupted if features such as hold, transfer, forward are used. Video connections cannot be established while these functions are active.
- The DMC connection is only re-established and video connections can only be set up again in case of retrieve after hold.
- Since ongoing DMC connections do not support SDP re-negotiation, no applications are supported in conjunction with a video connection (e.g. remote camera control).
- To support secure direct payload in transit scenarios all involved trunks have to be configured to the same RTP security mode.

3.4.2 Scenarios

- High-definition video and audio transmission for conferences
- Peer-to-peer video communication with SIP-based video connections

3.4.3 Features

Use of video with SMP has no direct impact on system features. Since SDP is negotiated E2E, any feature behaviour/restrictions are client specific.

3.4.4 Configuration

Since video endpoints are treated as normal SIP subscribers, they are also configured as such in the system.

For information on how to configure SIP subscribers, refer to Chapter 2, “SIP Subscriber” in the document "SIP Connectivity".

In addition to DMC configuration for the endpoint, AMO CGWB SMP=YES (TYPE=DMCDATA) must be activated.

Where the endpoint is a non-OS4K SIPQ partner, the parameter AMO CGWB SMP4OSV=YES (TYPE=DMCDATA) must be activated in addition to SMP=YES, which will generate an SMP operation for the SIPQ trunk.

Video is also supported for uaCSTA capable UC Clients (e.g WebRTC, Fusion).

NOTICE: Restriction: For details, refer to the Released Note document.

3.5 Music on Hold (MOH) - OpenScape 4000 SoftGate as Music on Hold or Announcement Source Provider

3.5.1 Feature Description

The OpenScape 4000 SoftGate can act as a music on hold (MOH) or announcement source provider. It works in a similar way as external equipment connected to an analog line. The OpenScape 4000 SoftGate provides virtual SLMA board and virtual TMOM board with saved voice files which emulate real SLMA and TMOM board with connected external music equipment. As music source audio files are used (for requirements please refer to Section 7.2, “Service Information”).

Music or announcement can be switched to any destination within OpenScape 4000 SoftGate (HFA phone, SIP phone, SIP trunk) as well as to any device in another access point or host shelf (TDM phone, analog phone,
).

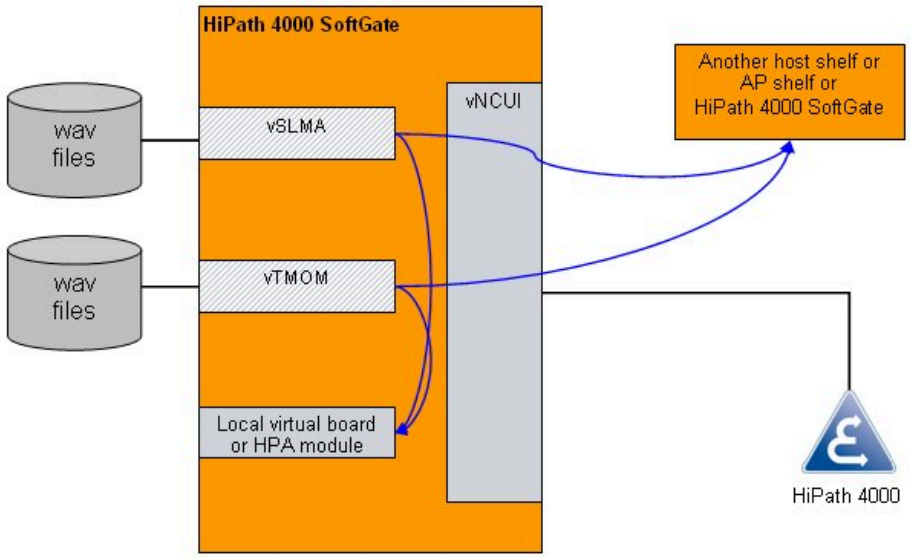


Figure 99: OpenScape 4000 SoftGate: Music on hold, announcements

3.5.2 Service Information

Important Information for Upgrade

If some vSLMA circuits are already configured and upgrade is not done using AMO REGEN it is necessary to delete all vSLMA circuits and configure them again with AMO SSC and AMO RCSU.

Supported Features

The following features are supported:

- Music source external
  - For a detailed description of “Music Source External” please refer to the appropriate chapter of the feature usage examples (http://apps.g-dms.com:8081/techdoc/en/P31003H3170S103017620/musicex_en.html).
  - using SLMA board
  - circuit configured with AMO SSC, **TYPE=EXTANN**
- Multiple music on hold
  - using SLMA board
  - circuit configured with AMO RCSU, **RECAPL=HMUSIC**
  - subscribers will be added to the music on hold device with AMO SCSU/ AMO SBCSU/AMO SSCSU
- MOH and announcements for Flexrouting
  - For more information on “Flexrouting” please refer to the appropriate chapter of the feature usage examples (http://apps.g-dms.com:8081/techdoc/en/P31003H3170S103017620/wwhelp/wwhimpl/js/html/wwhelp.htm?href=flexrout_en.html).
  - using SLMA board
  - circuit configured with AMO RCSU, **RECAPL=ACDR/ACDMUS**

- Synchronized announcements
  - For more information on “Synchronized Announcements” please refer to the appropriate chapter of the feature usage examples (http://apps.g-dms.com:8081/techdoc/en/P31003H3170S103017620/wwhelp/wwhimpl/js/html/wwhelp.htm?href=anse1_en.html).
  - using TMOM board
  - circuit configured with AMO TSCSU, **DEV=RAS**
- Announcement unit
  - For more information on “Announcement Unit” please refer to the appropriate chapter of the feature usage examples (http://apps.g-dms.com:8081/techdoc/en/P31003H3170S103017620/wwhelp/wwhimpl/js/html/wwhelp.htm?href=annuni_en.html).
  - using TMOM board
  - circuit configured with AMO TSCSU, **DEV=RA/ANS**

Details

From Openscape 4000 V7 vSLMA and vTMOM boards have dedicated part numbers and are able to access all four highways in the shelf. The AMO will automatically replace previous used part numbers for when adding the vSLMA and vTMOM boards with older part numbers.

Table 17: Overview classical and virtual boards

Classical Boards		Virtual Boards	
Q2246-X	SLMA24	Q2339-X	vSLMA
Q2146-X	SLMA2	Q2339-X	vSLMA
Q2214-X	TMOM2	Q2340-X	vTMOM
Q2214-X100	TMOM2	Q2340-X	vTMOM
Q2187-X	SIUX2	Q2341-X	vSIUX

The vSLMA board (Q2339-X) or vTMOM board (Q2340-X) can be configured into one or more OpenScape 4000 SoftGate slots with standard AMO BCSU command.

The supported features work as with a “real” SLMA/TMOM board.

Requirements for audio files

There are following requirements for the audio files:

- .wav format
- PCM16 encoding
- mono
- 8 kHz sampling rate

3.5.3 Generation (Example)

vSLMA board configuration

The vSLMA board (Q2339-X) can be configured into one or more OpenScape 4000 SoftGate slots with standard AMO BCSU command.

```
LTG  1  LTU 23  SRCGRP 2   ALARMNO-LTU 0     SOFTGATE50       10 PORTS USED
-----+----------+--------+---+-+-+---+-+-----------+-----------+-----------
     |          |        |   |S|H|AL-| |           |           |
     | ASSIGNED | MODULE |FCT|E|W|ARM| | INSERTED  |    HW-    | MODULE
 PEN | MODULE   | TYPE   |ID |C|Y|NO | | MODULE    |STATE INFO | STATUS
-----+----------+--------+---+-+-+---+-+-----------+-----------+-----------
   1 | Q2339-X  vSLMA          A   0| | Q2339-X   |  1  -10 - | READY
   2 | AVAILABLE                   0| | AVAILABLE |           |
   3 | Q2330-X  vHG3500   1    A   0| | Q2330-X   |  1  -07 - | READY
     +-------------------------------+-+-----------+-----------+-----------
     | IP ADDRESS : 172. 20. 12.133        B-CHANNELS : 120    BCHLCNT : 120
     | IP MODE    :     IPV4               DHCP V4    :   NO    DHCP V6 :   NO
     | BLOCK NO   :  40                    PRERESERVED LINES ASSIGNED :   NO
     |  1. FUNCT  : HG3530      240 LINES  B-CHANNELS : 120    BCHLCNT : 120
     +-------------------------------+-+-----------+-----------+-----------
   4 | Q2333-X  SLMO24    1    A   0| | Q2333-X   |  1  -11 - | READY
     +-------------------------------+-+-----------+-----------+-----------
     | MAC ADRESS : 00-01-E3-8B-C1-EA
     +-------------------------------+-+-----------+-----------+-----------
   5 | Q2331-X  SLMAE          A   0| | Q2331-X   |  1  -07 - | READY
     +-------------------------------+-+-----------+-----------+-----------
     | MAC ADRESS : 00-01-E3-96-E2-C7
     +-------------------------------+-+-----------+-----------+-----------
   6 | Q2329-X  SoftGate  1        0| | Q2329-X   |  1  -09 - | READY
     +-------------------------------+-+-----------+-----------+-----------
     | IP ADDRESS : 172. 20. 12.136        B-CHANNELS : 250    BCHLCNT : 250
     | IP MODE    :     IPV4               DHCP V4    :   NO    DHCP V6 :   NO
     +-------------------------------+-+-----------+-----------+-----------
   7 | Q2339-X  vSLMA          A   0| | Q2339-X   |  1  -10 - | READY
   8 | Q2340-X  vTMOM          A   0| | Q2340-X   |  1  -10 - | READY
   9 | Q2340-X  vTMOM          A   0| | Q2340-X   |  1  -10 - | READY
  10 | Q2341-X  vSIUX     3    0| | Q2341-X   |  1  -02 - | READY
```

Circuit and feature configuration

The circuits and the whole features can be configured with AMO SSC or AMO RCSU or AMO TSCSU in the same way as for real SLMA/TMOM board (see feature documentation links in Section 7.1, “Feature Description”).

Audio file configuration

The audio files can be configured per circuit by OpenScape 4000 SoftGate WBM **Configuration > Announcements**:

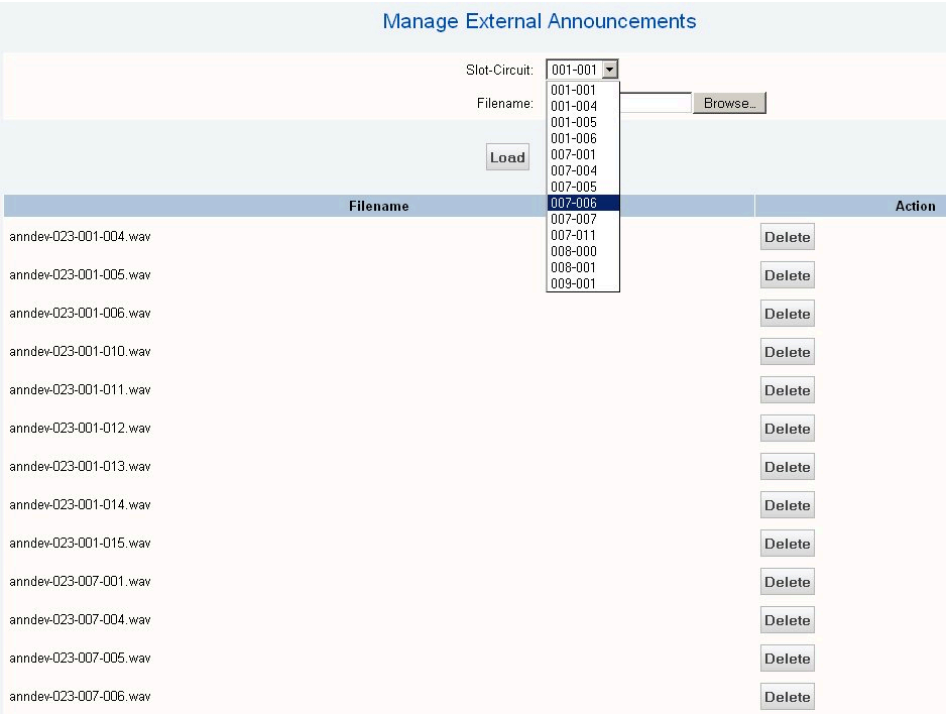


Figure 100: Audio file configuration with OpenScape 4000 SoftGate WBM

If the .wav file is loaded or changed for already active SLMA circuit, the circuit has to be restarted using RES-DSSU to activate the new .wav file (also virtual board or whole OpenScape 4000 SoftGate can be restarted).

3.5.4 Relevant AMOs

AMO	Parameter	Sprache/ Language	Beschreibung/ Description
BCSU		d	vSLMA-Baugruppe einrichten
		e	Configure vSLMA board
RCSU	ANWENDNG=WMUSIK	d	Anwendung Wartemusik
	RECAPL=HMUSIC	e	Music on hold recorder
SSC	TYP=EXTANS	d	Externes Ansagegerät
	TYPE=EXTANN	e	External announcement

3.6 Gatekeeper Redundancy for HFA/ SIP Subscriber

3.6.1 Feature Description

The gatekeeper redundancy function for HFA / SIP stations offers a further option to increase the availability of VoIP terminals in case of:

1) Failure of the connection between SoftGate and the host system

- Failure of the OpenScape 4000 SoftGate server hardware or
- Errors in the SoftGate application software

Starting with V8R2 the gatekeeper redundancy feature also supports a variety of SIP devices. The following SIP devices are supported.

- OpenScape Desk Phone CP family (DNSSRV required)
- OpenStage WL3/WL4 Phones
- OpenScape Xpert (DNSSRV required)
- Mediatrix C7 & 4100 Series Gateways

3.6.1.1 Solution concept

Two OpenScape 4000 SoftGates are connected to one another (redundantly) in a pool. The "active" or "standby" function is defined by the configuration of the associated vHG3530 (HFA) / vHG 3500 (SIP) pairs. It is possible to configure both active gateways (AMO CGWB, SMODE=**NORMAL**) and standby gateways (AMO CGWB, SMODE=**STBYRDY**) within a OpenScape 4000 SoftGate. Two vHG3530 (HFA) / vHG 3500 (SIP) always form a pair. One gateway has to be configured in OpenScape 4000 SoftGate A in this case and the other in OpenScape 4000 SoftGate B.

Both IP addresses (primary gateway and secondary gateway) must be configured on the HFA/SIP phone. This can be administered on the terminal itself or via DLS.

Not all SIP phones support administration of two IP addresses (primary and secondary server). In this case DNSSRV must be used.

3.6.1.2 Switchover

If the connection between CCA/CCB and vNCUI is lost (i.e. between the host system and OpenScape 4000 SoftGate), the error message "LTUC OUT OF ATTENDANCE LIST" is generated and the OpenScape 4000 SoftGate is switched over ("SOFTGATE RECONFIGURATION START") (see AMO HISTA).

The successful switch over of the individual boards is confirmed with "BOARD RECONFIGURATION OK". The end of the complete switchover is acknowledged with "SOFTGATE RECONFIGURATION END".

A (5 minute) timer is started when the reconfiguration starts . This timer is stopped with the message "RECONFIGURATION END". If an END message has still not been received following expiry of the timer, the message "SOFTGATE RECONFIGURATION TIME" is issued (AMO HISTA). This can happen if several OpenScape 4000 SoftGates or a large number of subscribers have to be switched over and simply serves as additional notification that the move is still pending.

From the FA perspective, it cannot be established whether an error has occurred at the application or PC level (error or planned shutdown) or whether there is an IP network error (no connection to OpenScape 4000 SoftGate - CCA/CCB).

IMPORTANT: The automatic switchover for failure cases e.g. cable disconnect/failure or OpenScape 4000 SoftGate outage is performed only once: from NORMAL to STBYRDY. Regardless of the state of the former NORMAL SoftGate there will be no further automatic switch back. In other words, the failure case happened and the automatic switchover was performed and the fault of the initial SoftGate has been repaired to STBYRDY, then a manual switchback needs to be executed to make the Automatic Switchover available again!

3.6.1.3 Prerequisites for switching over

The switchover is only performed if the following requirements are fulfilled:

- The affected AP must be a OpenScape 4000 SoftGate.
- The failed OpenScape 4000 SoftGate must have a redundancy OpenScape 4000 SoftGate available.
- The status of the destination OpenScape 4000 SoftGate must be LTU READY.

NOTICE: No switch over will be started during the startup of the system or the startup of the OpenScape 4000 SoftGate.

3.6.1.4 Switchover process

The following switchover process applies to all scenarios:

OpenScape 4000 SoftGate 18 is no longer accessible due to a hardware, software or IT network failure (connection to CCA/CCB lost). The switchover is therefore performed:

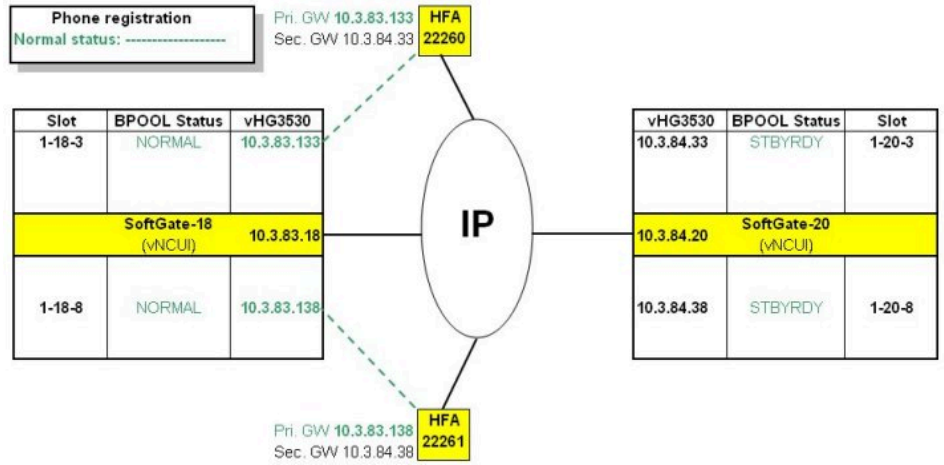
- OpenScape 4000 SoftGate is deactivated. The vHG 3530 / vHG 3500 gateways have the status **STBYDEF** (`AB-BPOOL:MTYP=AP;`)
- The associated gateways in OpenScape 4000 SoftGate 20 are restarted (warm standby) and enter the status **NORMAL**.
- The HFA / SIP stations are rewritten in the database (AMO SBCSU) from position 1-18-3 or 1-18-8 to positions 1-20-3 or 1-20-8 and the HFA / SIP terminals register automatically at the corresponding vHG 3530 / vHG 3500 gateway (secondary gateway).
- The IP addresses of the boards are not rewritten (as with the previous, traditional BPOOL concept). These are permanently configured with AMO CGWB.
- Manual switchover / Manual switchback
- A manual switchover can be performed with the AMO command `EXEC-USSU`, in other words in case of maintenance work or following an automatic

switchover (in the event of error), for switching back to the original configuration.

IMPORTANT: If a switchover is performed **manually** from OpenScape 4000 SoftGate 18 to OpenScape 4000 SoftGate 20 via AMO (`EX-USSU:ART=SGRED,LTU=18,SWTYPE=...`) owing to maintenance work or the like, the vHG3530 vHG3500 gateways in OpenScape 4000 SoftGate 18 enter the status **STBYRDY** (`AB-BPOOL:MTYP=AP,...;`). Only the boards configured in the relevant BPOOL are switched over here. All other boards in OpenScape 4000 SoftGate 18 are not affected by the switchover.

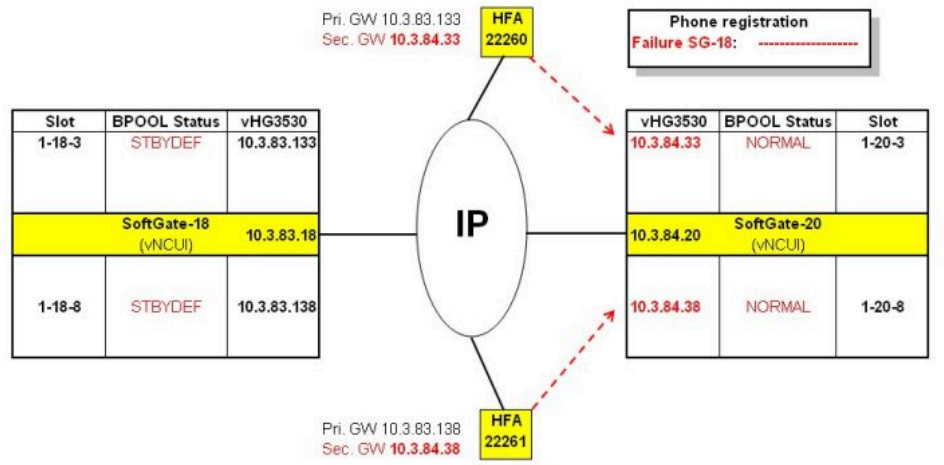
Scenario 1: All vHG 3530 boards in the failed OpenScape 4000 SoftGate are configured as active gateways

Normal status:



HFA gatekeeper redundancy "simple" mode - Normal status

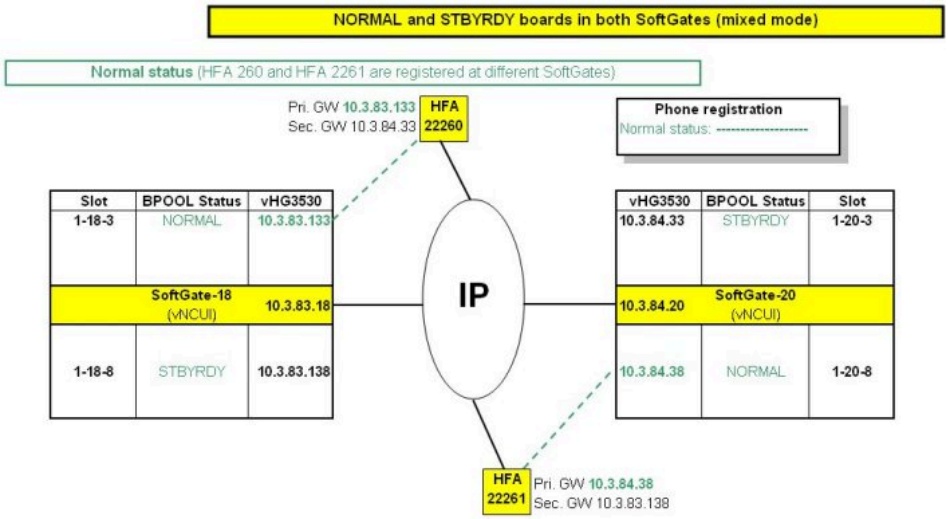
Upon failure of OpenScape 4000 SoftGate 18:



HFA gatekeeper redundancy "simple" mode - Failure of OpenScape 4000 SoftGate 18

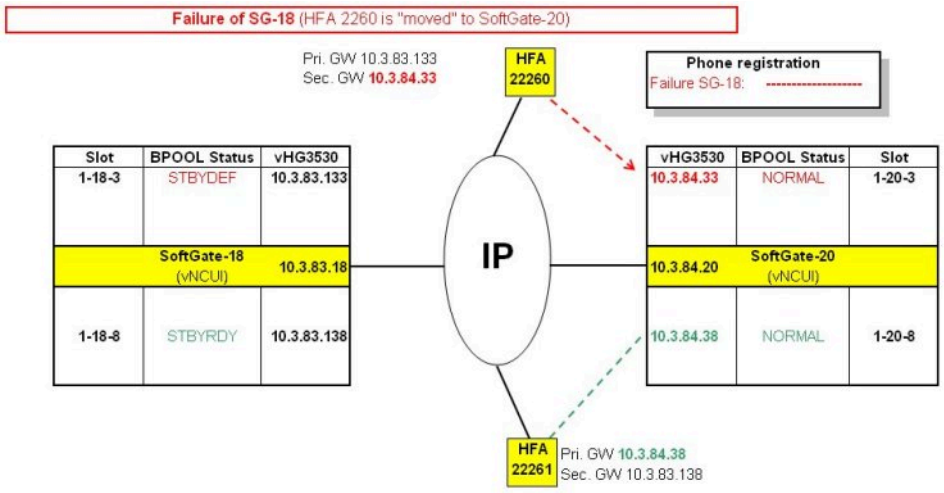
Scenario 2: There are active vHG 3530 gateways and standby vHG 3530 gateways in the failed OpenScape 4000 SoftGate.

Normal status:



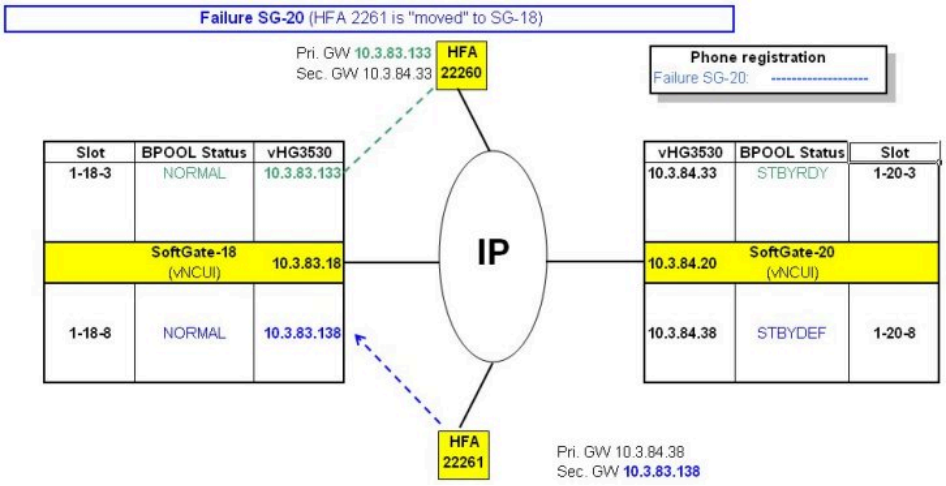
HFA gatekeeper redundancy "mixed" mode - Normal status

Upon failure of OpenScape 4000 SoftGate 18:



HFA gatekeeper redundancy "mixed" mode - Failure of OpenScape 4000 SoftGate 18

Upon failure of OpenScape 4000 SoftGate 20:



HFA gatekeeper redundancy "mixed" mode - Failure of OpenScape 4000 SoftGate 2

Scenario 3: All vHG 3500 boards in the failed OpenScape 4000 SoftGate are configured as active gateways

Normal status:

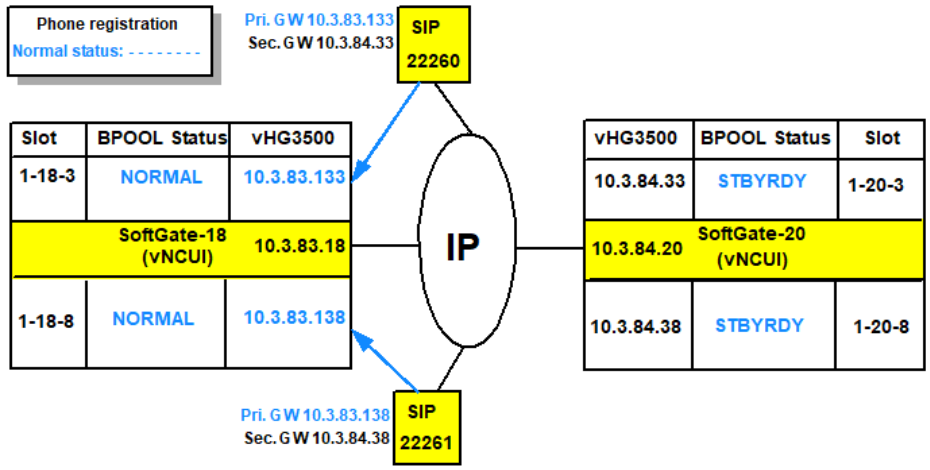
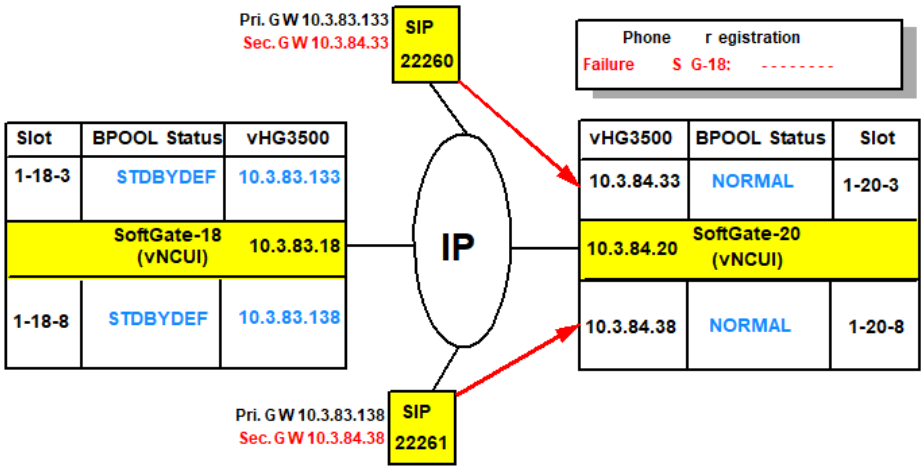


Figure 101: SIP gatekeeper redundancy "simple" mode - Normal status

Upon failure of OpenScape 4000 SoftGate 18:



SIP gatekeeper redundancy "simple" mode - Failure of OpenScape 4000 SoftGate 18

Scenario 4: There are active vHG 3500 gateways and standby vHG 3500 gateways in the failed OpenScape 4000 SoftGate.

Normal status:

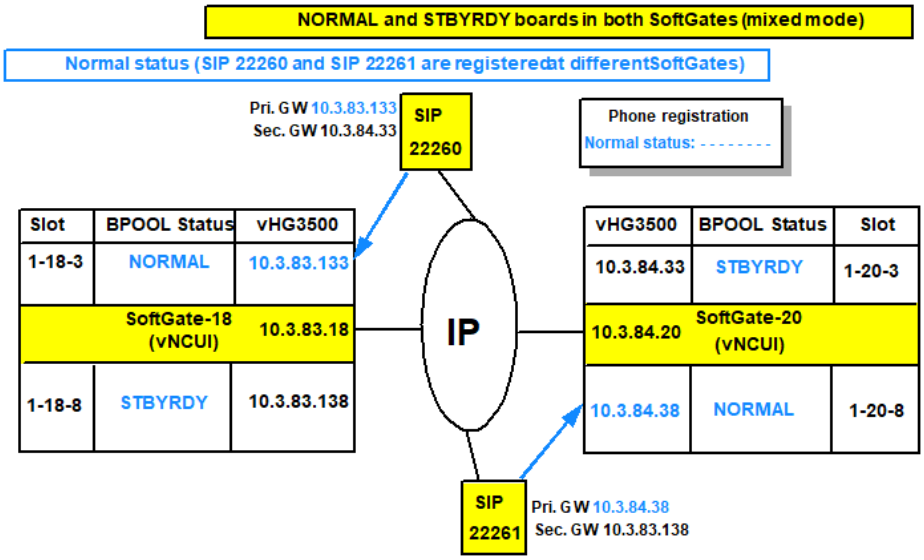
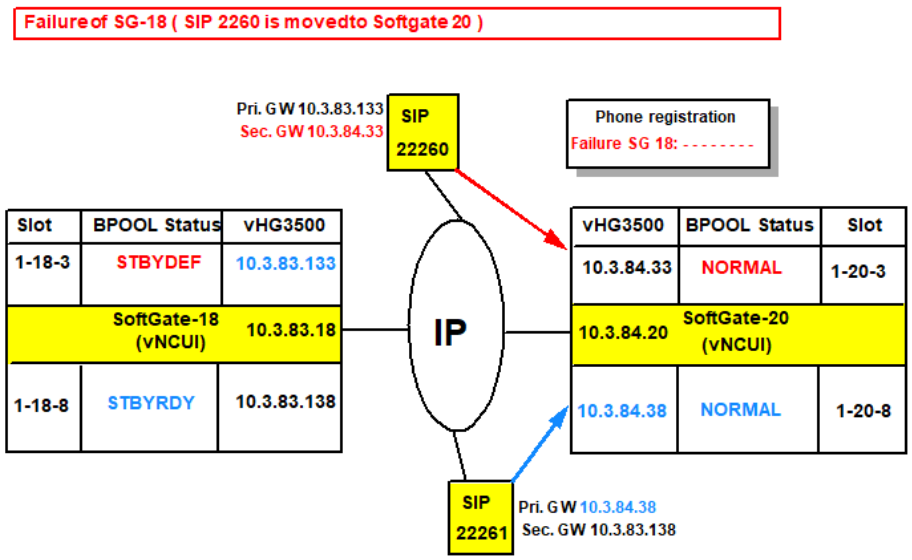


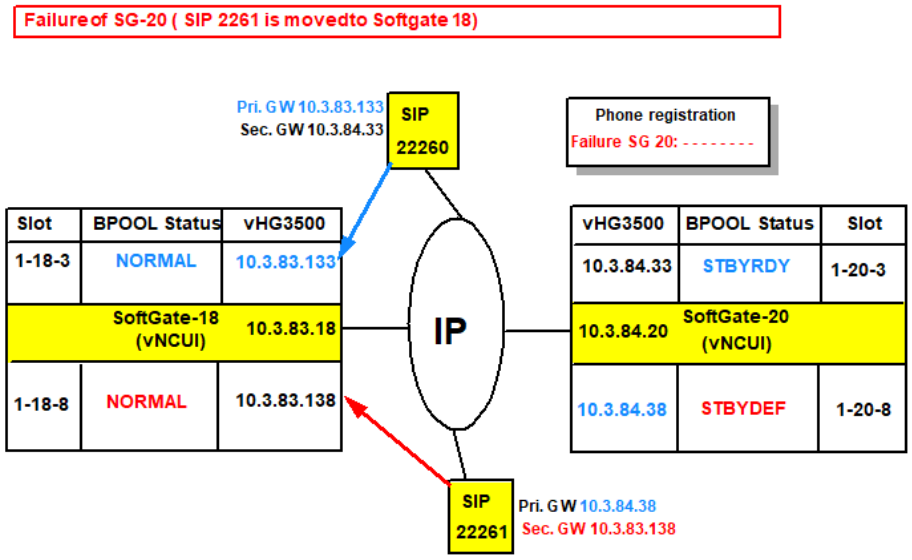
Figure 102: SIP gatekeeper redundancy "mixed" mode - Normal status

Upon failure of OpenScape 4000 SoftGate 18:



SIP gatekeeper redundancy "mixed" mode - Failure of OpenScape 4000 SoftGate 18

Upon failure of OpenScape 4000 SoftGate 20:



SIP gatekeeper redundancy "mixed" mode - Failure of OpenScape 4000 SoftGate 20

3.6.1.5 Gatekeeper Redundancy with APE

Prerequisites:

- The SoftGates that are paired for the Gatekeeper Redundancy feature (AMO BPOOL) must be members in the same APE Emergency Group.
- The SoftGates of the APE Emergency Group must only be switched to the CC-AP as group (single is not supported) i.e. when both SGs have lost their connection to the host. This means the Gatekeeper switchover will only then be triggered if just one SG has lost the connection to the currently

controlling CC. If the connections to both SGs are lost at the same time then no Gatekeeper switchover will occur.
- Both Automatic and Manual switchback are possible.

3.6.2 Service Information

- This feature is only implemented for OpenScape 4000 SoftGates.
- Virtual boards (vHG 3530) with pure HFA subscribers are switched.
- Virtual boards (vHG 3500) with pure SIP subscribers are switched.
- Boards with trunking functionality are not switched.
- The already existing feature “Standby Board HG3500” (hardware based solution for host system, shelves and hard AP shelves) remains unchanged.
- With MobileHFA or DeskSharing, a "forced logoff" is performed in case of failure/switchover of the OpenScape 4000 SoftGate. The "visitor" has to log in to the station again after the switchover.
- For administration or maintenance activities, the OpenScape 4000 SoftGate has to be blocked by AMO AUSS-USSU (status MAN_AMO). This is necessary to prevent a switchover when the PC is shut down.
- After a failure case occurred a further automatic switchback is not possible, regardless of whether the switchover was previously performed automatically (cable disconnect/failure or OpenScape 4000 SoftGate outage) or by AMO. The switchback must be always performed manually afterwards to reset to the initial configuration and thus to support again a failure case switchover.
- Switchover is possible only for same type of OpenScape 4000 SoftGate for active and standby OpenScape 4000 SoftGate (e.g. OpenScape 4000 SoftGate 50).
- **Only applies up to and including V6 R1**: After a switch over from OpenScape 4000 SoftGate A to OpenScape 4000 SoftGate B (i.e. OpenScape 4000 SoftGate A is down or a loss of LAN connectivity) AMO BPOOL will correctly show all ports in status **STBYDEF** on OpenScape 4000 SoftGate A.
- After OpenScape 4000 SoftGate A becomes active again, all ports should be in status **STBYRDY**, but the ports remain in **STBYDEF**.

  This is also the case if the boards are switched manually back to OpenScape 4000 SoftGate A via EXECUTE-USSU:SGRED,<SG B>,HOME;.

  AMO BPOOL then shows own ports in status **NORMAL**, but the standby Ports remain in status **STBYDEF**.

  This is an indication error of AMO BPOOL and can be solved by ADD-CGWB:<LTU>,<SLOT>,STBYRDY;.

  I.e. there is only a display problem in AMO BPOOL but there is no functional restriction/problem.
- It is recommended to not use the DLS synchronization for the phones running under the Gatekeeper Redundancy feature in order to avoid unwanted auto configuration changes.

  If DLS is in use, depending on Sync time and switchback, it requires time to perform manual CM synchronization.

3.6.3 Generation (Example)

The following generation example corresponds to Scenario 2 shown in Section 10.1.4, “Switchover process”. Each of the OpenScape 4000 SoftGates have NORMAL and STBYRDY boards (mixed mode).

IMPORTANT: The pairs configured in AMO BPOOL must have the same type in AMO UCSU, parameter **SOCOTYP** (e.g.: both **SOCO50** or both **SOCO1000**).

IMPORTANT: The pairs configured in AMO BPOOL cannot be changed. In case of an incorrect configuration, the pair has to be deleted and then reconfigured.

IMPORTANT: In case vHG-SIP boards are configured in BPOOL, the Standby SoftGate is not automatically informed that these are vHG-SIP boards (instead it treats them as vHG-HFA). To activate them correctly, it is necessary to restart the Standby SoftGate with e. g. RES-USSU.

```
                                /* BFDAT NORMAL boards */
ADD-BFDAT:FCTBLK=35,FUNCTION=HG3530,BRDBCHL=BCHL120,ATTR="SOCO";
CHANGE-BFDAT:CONFIG=CONT,FCTBLK=35,FUNCTION=HG3530,LINECNT=240,BCHLCNT=60;
CHANGE-BFDAT:CONFIG=OK,FCTBLK=35,ANSW=YES;
ADD-BFDAT:FCTBLK=30,FUNCTION=SIP,BRDBCHL=BCHL120,ATTR="SOCO";
CHANGE-BFDAT:CONFIG=CONT,FCTBLK=30,FUNCTION=SIP,LINECNT=120,BCHLCNT=120;
CHANGE-BFDAT:CONFIG=OK,FCTBLK=30,ANSW=YES;

                                /* BFDAT STBYRDY boards */
ADD-BFDAT:FCTBLK=45,FUNCTION=STANDBY,BRDBCHL=BCHL120,ATTR="SOCO";

                                /* OpenScape 4000 SoftGate 18 boards */
ADD-BCSU:MTYPE=IPGW,LTG=1,LTU=18,SLOT=3,PARTNO="Q2330-X ",FCTID=1,LWVAR="0",FCT▶
BLK=35,BCHL3530=30,ALARMNO=0,IPMODE=IPV4,DHCPV4=NO,DHCPV6=NO;
ADD-BCSU:MTYPE=IPGW,LTG=1,LTU=18,SLOT=11,PARTNO="Q2330-X ",FCTID=1,LW▶
VAR="0",FCTBLK=45,BCHLSIP=120,ALARMNO=0,IPMODE=IPV4,DHCPV4=NO,DHCPV6=NO;
ADD-BCSU:MTYPE=IPGW,LTG=1,LTU=18,SLOT=8,PARTNO="Q2330-X ",FCTID=1,LWVAR="0",FCT▶
BLK=45,BCHL3530=30,ALARMNO=0,IPMODE=IPV4,DHCPV4=NO,DHCPV6=NO;

                                /* OpenScape 4000 SoftGate 18 gateways */
ADD-CGWB:LTU=18,SLOT=3,SMODE=NORMAL,IPADR=10.3.83.133,NET▶
MASK=255.255.255.0,VLAN=NO,VLANID=0,DEFRT=10.3.83.1;
ADD-CGWB:LTU=18,SLOT=11,SMODE=STBYRDY,IPADR=10.3.83.140,NET▶
MASK=255.255.255.0,VLAN=NO,VLANID=0,DEFRT=10.3.83.1;
ADD-CGWB:LTU=18,SLOT=8,SMODE=STBYRDY,IPADR=10.3.83.138,NET▶
MASK=255.255.255.0,VLAN=NO,VLANID=0,DEFRT=10.3.83.1;

                                /* OpenScape 4000 SoftGate 20 boards */
ADD-BCSU:MTYPE=IPGW,LTG=1,LTU=20,SLOT=3,PARTNO="Q2330-X ",FCTID=1,LWVAR="0",FCT▶
BLK=45,BCHL3530=30,ALARMNO=0,IPMODE=IPV4,DHCPV4=NO,DHCPV6=NO;
ADD-BCSU:MTYPE=IPGW,LTG=1,LTU=20,SLOT=11,PARTNO="Q2330-X ",FCTID=1,LW▶
VAR="0",FCTBLK=30,BCHLSIP=120,ALARMNO=0,IPMODE=IPV4,DHCPV4=NO,DHCPV6=NO;
ADD-BCSU:MTYPE=IPGW,LTG=1,LTU=20,SLOT=8,PARTNO="Q2330-X ",FCTID=1,LWVAR="0",FCT▶
BLK=35,BCHL3530=30,ALARMNO=0,IPMODE=IPV4,DHCPV4=NO,DHCPV6=NO;
```

```
                                /* OpenScape 4000 SoftGate 20 gateways */
ADD-CGWB:LTU=20,SLOT=3,SMODE=STBYRDY,IPADR=10.3.84.33,NET►
MASK=255.255.255.0,VLAN=NO,VLANID=0,DEFRT=10.3.84.1;
ADD-CGWB:LTU=20,SLOT=11,SMODE=NORMAL,IPADR=10.3.84.40,NET►
MASK=255.255.255.0,VLAN=NO,VLANID=0,DEFRT=10.3.84.1;
ADD-CGWB:LTU=20,SLOT=8,SMODE=NORMAL,IPADR=10.3.84.38,NET►
MASK=255.255.255.0,VLAN=NO,VLANID=0,DEFRT=10.3.84.1;

                                /* BPOOL OpenScape 4000 SoftGate 18/20 */
ADD-BPOOL:MTYPE=AP,POOLNO=1,LTUA=18,SLOTA=3,LTUB=20,SLOTB=3,INFO="SG 18-20
POOL";
ADD-BPOOL:MTYPE=AP,POOLNO=1,LTUA=20,SLOTA=11,LTUB=18,SLOTB=11;
ADD-BPOOL:MTYPE=AP,POOLNO=1,LTUA=20,SLOTA=8,LTUB=18,SLOTB=8;
```

In case SIP boards are configured in BPOOL, to inform the Softgate about the new SIP function boards, it is necessary to restart the standby Softgate.

Manual switchover

Switching over from OpenScape 4000 SoftGate 18 to OpenScape 4000 SoftGate 20 (or in the other direction) can be performed manually with following command:

```
EXEC-USSU:ART=SGRED,LTU=18,SWTYPE=<param>;
```

SWTYPE=ALL will switch all vHG HFA (3530) & vHG SIP subscriber boards configured in that SoftGate BPOOL.

SWTYPE=HOME will only switch the vHG HFA (3530) & vHG SIP subscriber boards which are not in normal status of that specified OpenScape 4000 SoftGate. It can be seen as "Switch them back to Home/Initial state" after they had been switched before, either automatic or manually.

Terminal configuration (HFA):

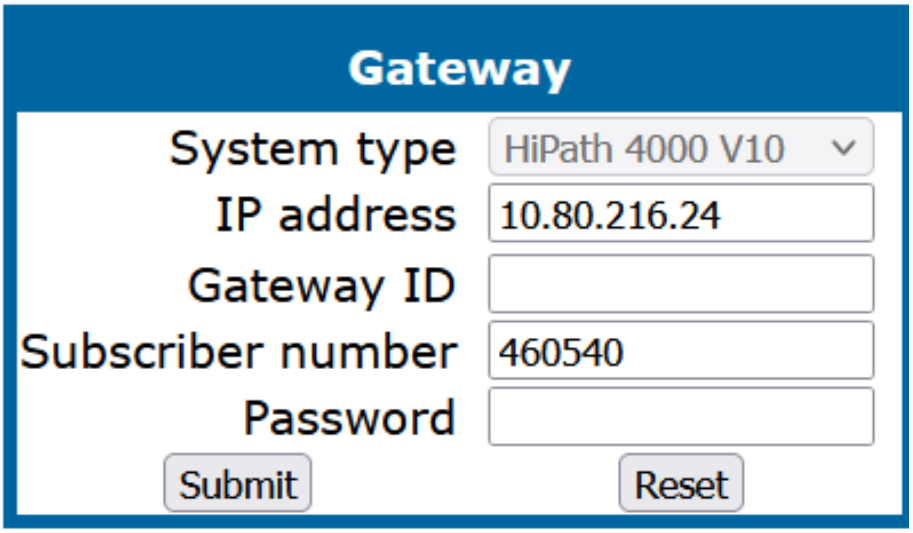
Both IP addresses (home gateway and standby gateway) must be known to the terminal.

Settings made using DLS:

- Active gateway
- **Main Menu > IP Devices > IP Phone Configuration > Gateway/Server >** Tab **Gateway (HFA) / SIP Server > Reg-Address (HFA) / SIP Server Address**
- Standby gateway
- **Main Menu > IP Devices > IP Phone Configuration > Gateway/Server >** Tab **Gateway (Standby) > Reg-Address**
- Configuration of subscriber redundancy at the terminal:
- **Main Menu > IP Devices > IP Phone Configuration > Small Remote Site Redundancy >** Tab **SRSR Settings** > Checkbox **SRSR freigeschaltet (SRSR Released???)**

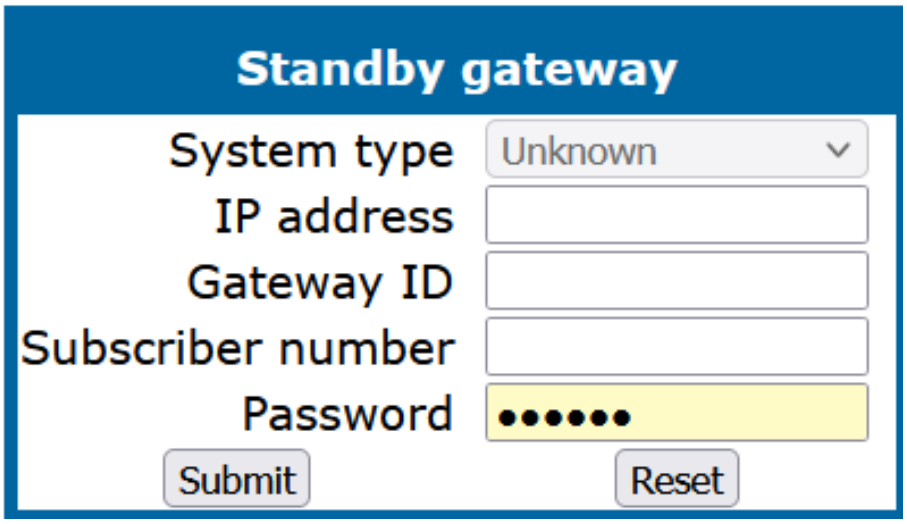
  Settings via WBM:
- OpenStage

- **Administrator > System > Gateway**



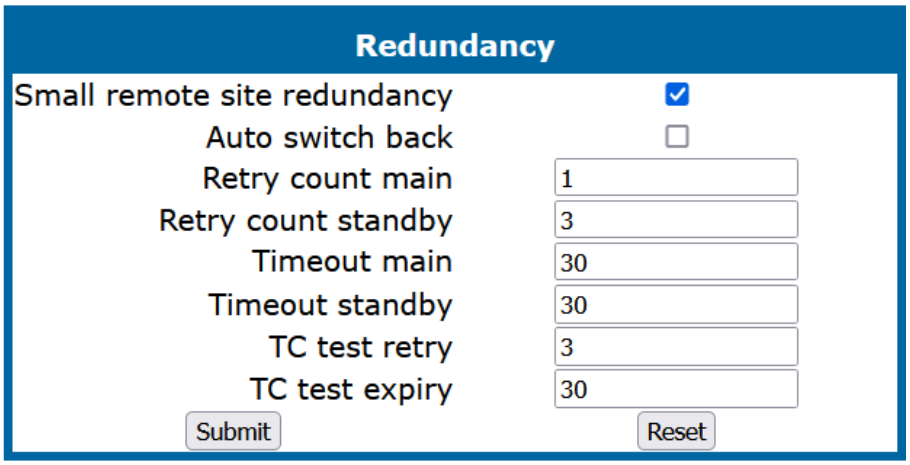
OpenStage - Subscriber Redundancy - Gateway

Administrator > System > Standby Gateway



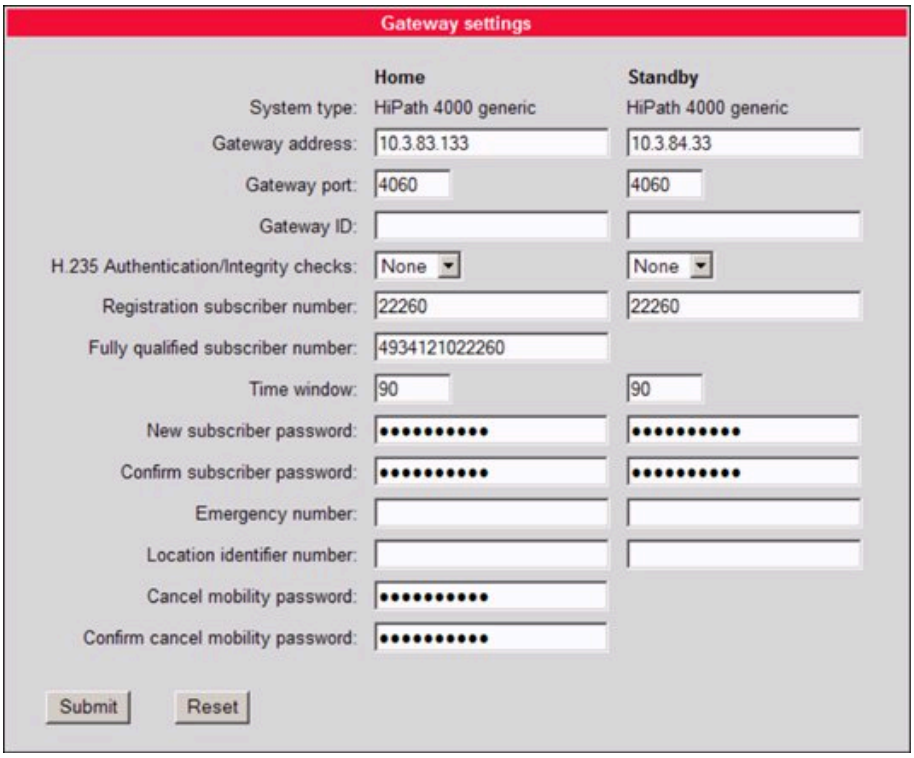
OpenStage - Subscriber Redundancy - Standby Gateway

Administrator > System > Redundancy



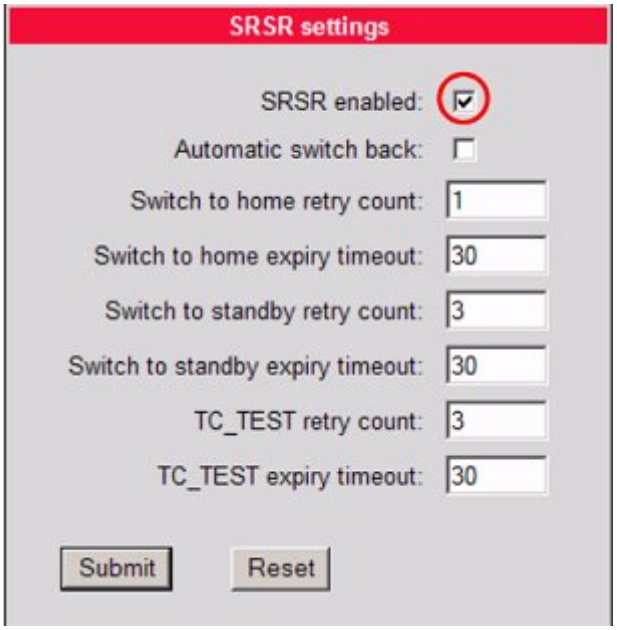
OpenStage - Activate Subscriber Redundancy

- optiPoint
- **Administrator > System > Gateway Settings**



optiPoint - Subscriber Redundancy - Gateways

Administrator > System > SRSR **Settings**



optiPoint - Activate Subscriber Redundancy

Terminal configuration (SIP CP Phones - please see official documentation "OpenScape Desk Phone CP Phone Administration" chapter 3.6.10 Resilience and Survivability):

Failover on must be set to Timeout and Error

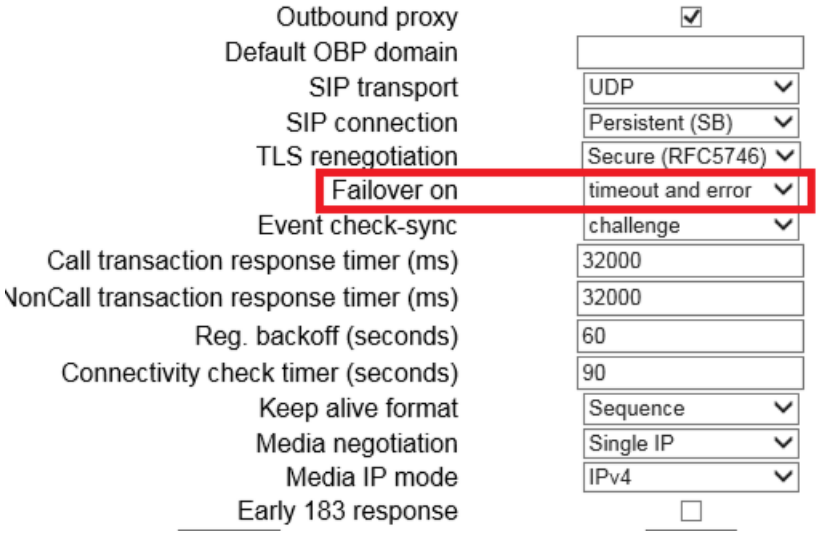


Figure 103: For CP Phones only DNS SRV method can be used for enhanced survivability.

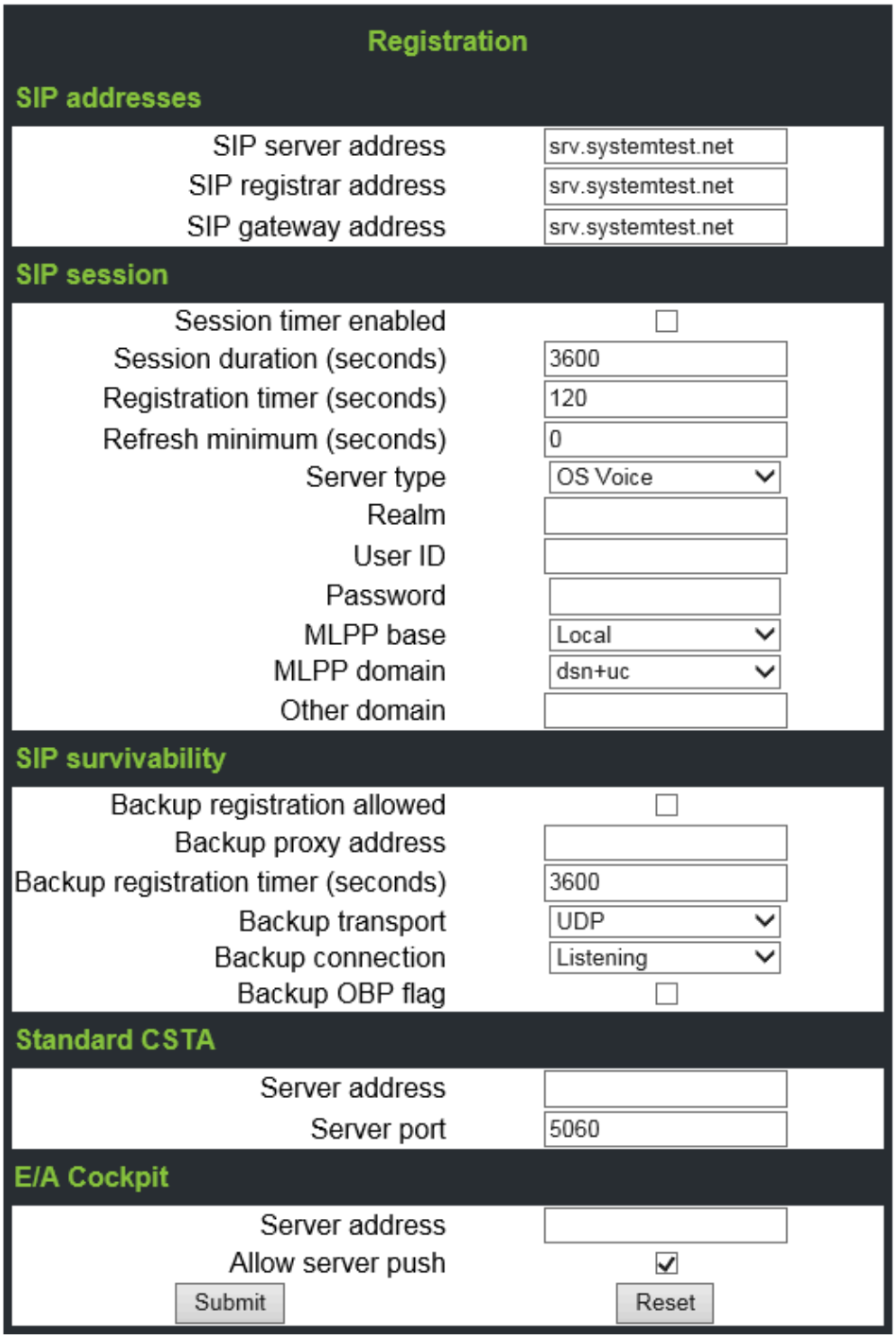


Figure 104: Configuration of Mediatrix C7 Series / AP1120

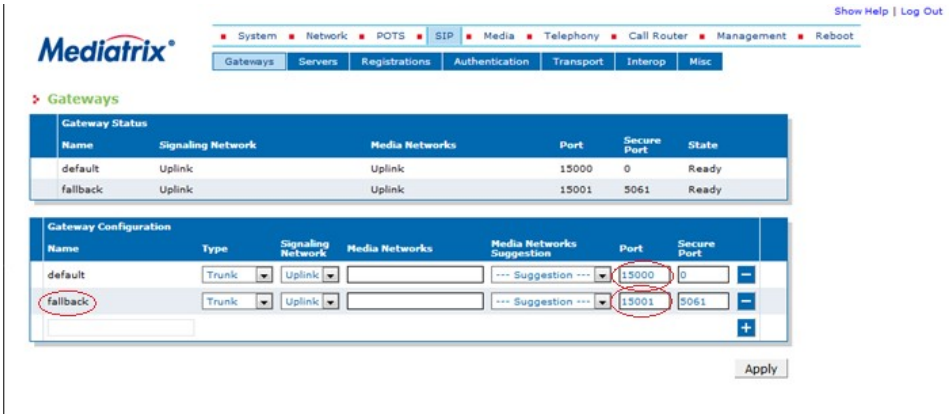
The Mediatrix C7 Series / AP1120 must be configured to try an alternative destination if call is rejected.

Cause value “21” must be added to the Hunting group causes. Please see Mediatrix C7 Series / AP1120 service documentation for details. E.g.

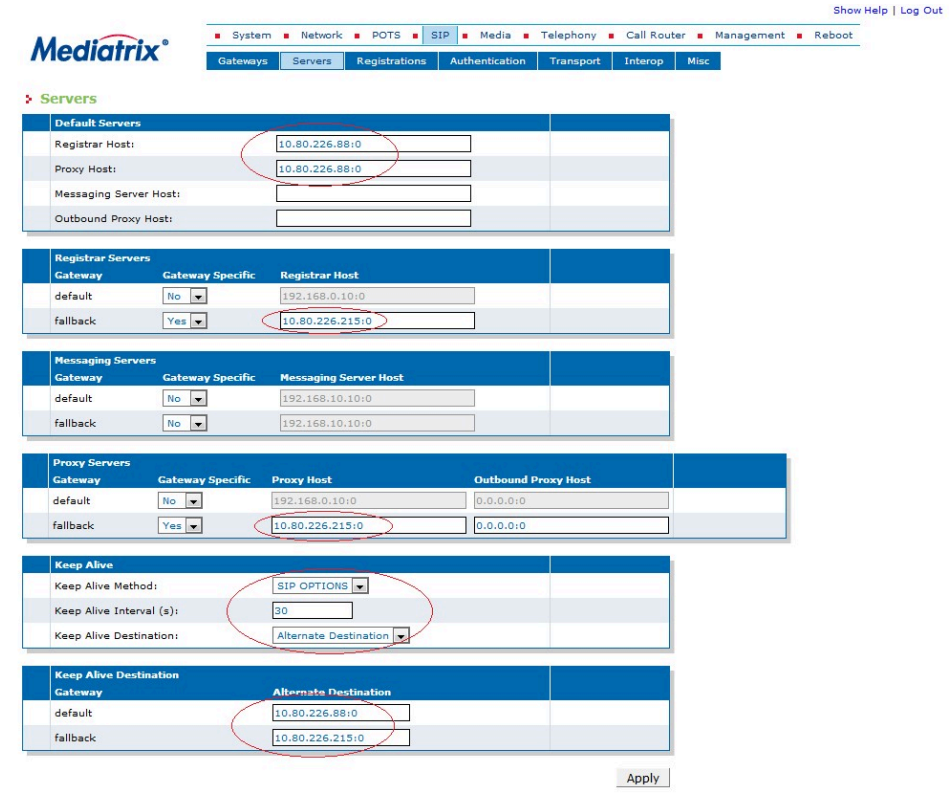
https://documentation.media5corp.com/display/DGWLATEST/Second+SIP+Gateway+Fallback+without+Gateway+Registration

Notes to configuration according to recommended Media5 Corporation documentation:

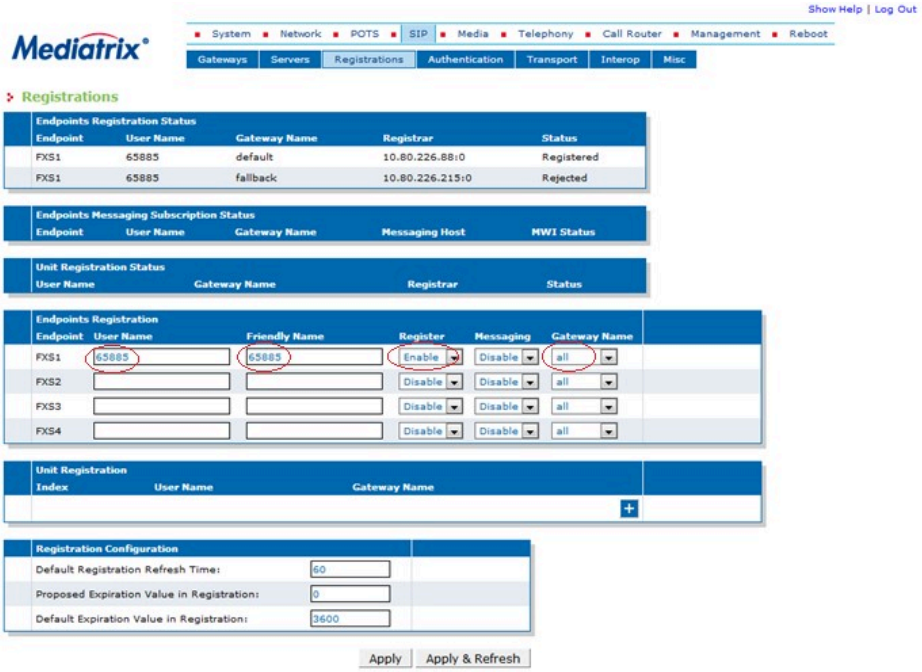
Configuration of default (Normal) and fallback (Redundancy) Gateways:



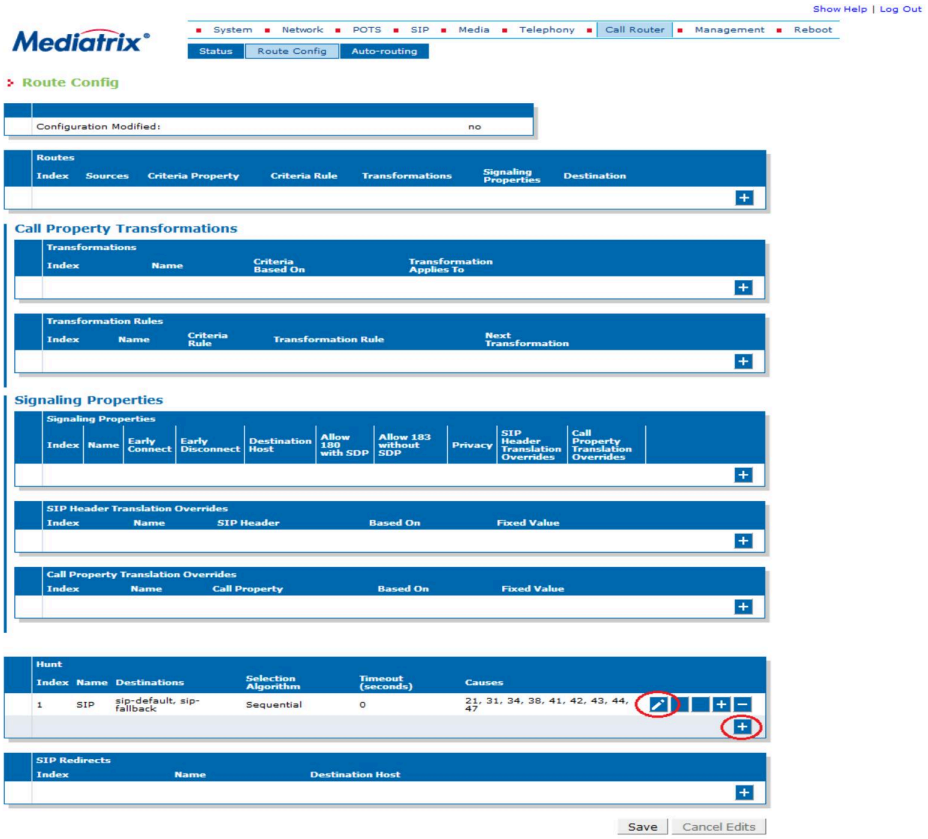
Configuration of Default (Normal) and Fallback servers (Registrar server and Proxy server) :



Status of SIP registration and Configuration of endpoints :

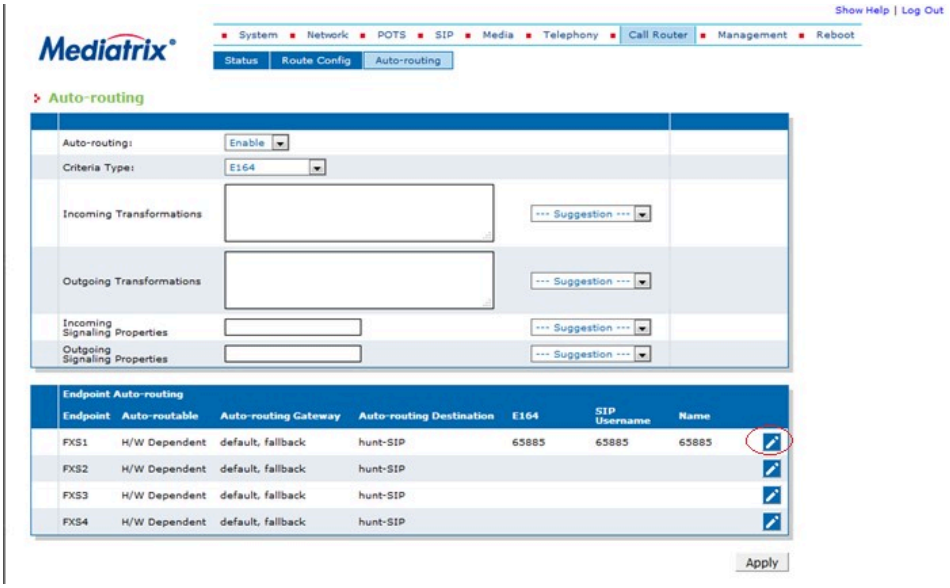


Configuration of Call Router for registration and to establish a call :



We can create Hunt Group definition by pressing the button [+] - see documentation of Media5 Corporation at the reference above. We can also edit Hunt Group by pressing button [pen].

Modify Auto-routing definition to Endpoint :



3.6.4 Relevant AMOs

AMO	Parameters	Sprache/ Language	Beschreibung/Description
BFDAT	FUNCTION=STANDBY	d	Funktionsblock für Standby konfigurieren
	FUNCTION=STANDBY	e	Configure function block for standby
BCSU	FCTBLK	d	Konfiguration der Funktionsblöcke für Normal-Betrieb und Standby
	FCTBLK	e	Function block configuration for main board and standby board
CGWB	SMODE	d	Eine vHG 3530 vHG 3500im normalen Modus (**NORMAL**) konfigurieren und eine im Standby-Ready-Modus (**STDBYRDY**) konfigurieren
	SMODE	e	Configure one vHG 3530 / vHG 3500 for normal mode (**NORMAL**) and one vHG 3530 / vHG 3500 for standby ready mode (**STDBYRDY**)
BPOOL	LTUA	d	LTU der Haupt-Baugruppe
	LTUA	e	LTU of main board
	LTUB	d	LTU der Standby-Baugruppe
	LTUB	e	LTU of standby board
	EBTA	d	Einbauteilung der Haupt-Baugruppe

AMO	Parameters	Sprache/ Language	Beschreibung/Description
	SLOTA	e	Slot of main board
	EBTB	d	Einbauteilung der Standby-Baugruppe
	SLOTB	e	Slot of standby board
USSU	ART=SGRED	d	SoftGate Redundancy
	MODE=SGRED	e	SoftGate Redundancy
	SWTYPE	d	Art der Umschaltung ALLE: Umschaltung aller vHG 3530 / vHG 3500 Baugruppen HOME: Umschaltung der vHG 3530 / vHG 3500 Baugruppen, die im Normalzustand nicht auf diesem OpenScape 4000 SoftGate “Zuhause” sind
	SWTYPE	e	Switch type ALL:switchover of all vHG 3530 / vHG 3500 boards HOME: switchover of all vHG 3530 / vHG 3500 boards which in normal state are not at home at this OpenScape 4000 SoftGate

3.7 Survivable OpenScape 4000 SoftGate

3.7.1 Feature Description

An optional survivability unit can transform a OpenScape 4000 SoftGate into a survivable access point.

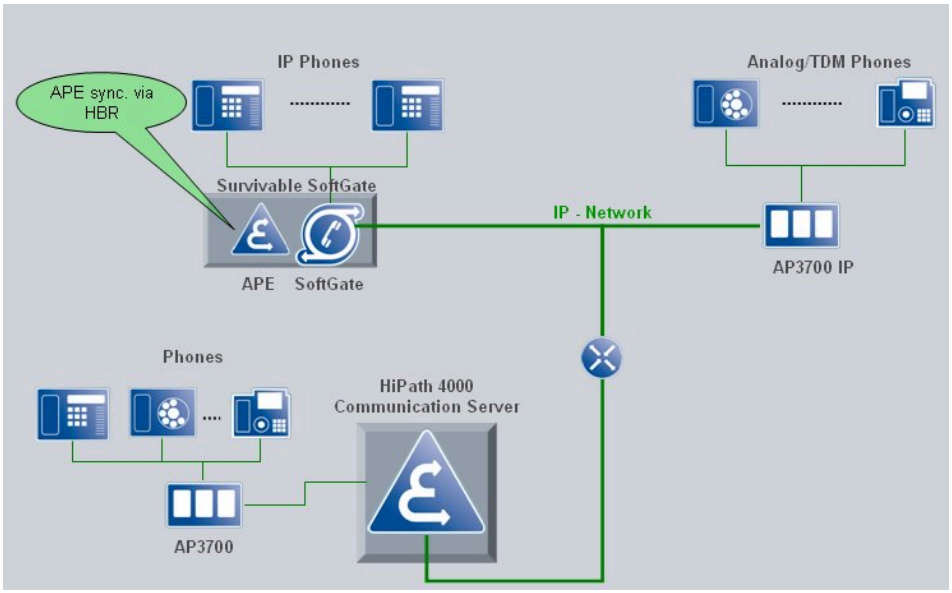


Figure 105: Survivable OpenScape 4000 SoftGate - Scenario

The survivability unit takes over control of its own OpenScape 4000 SoftGate and every other selected IP Access Point/OpenScape 4000 SoftGate without its own survivability unit if the central control fails (through loss of the IP connection to the central control or a call control failure).

The synchronization of the APE is done with OpenScape 4000 Assistant > Backup & Restore.

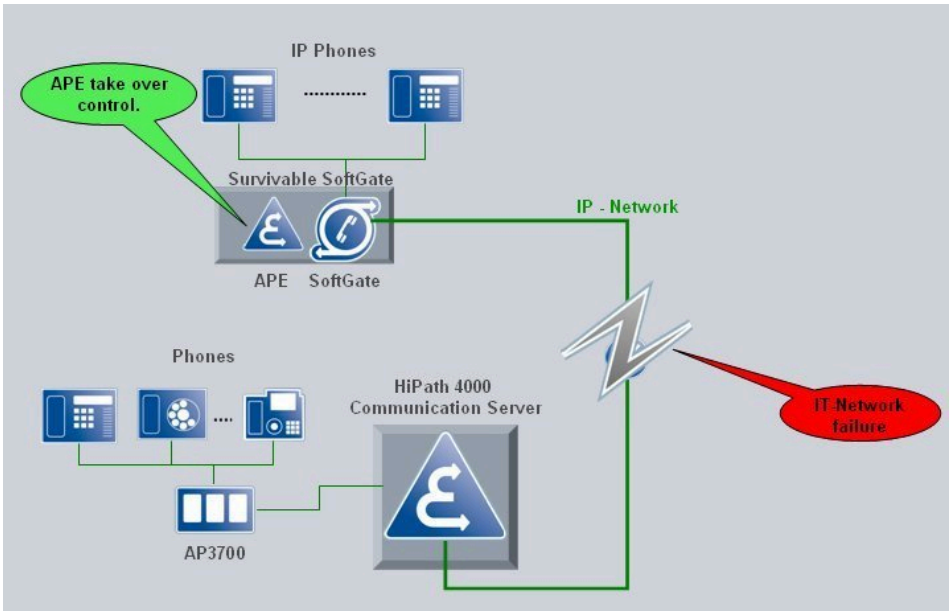


Figure 106: Survivable OpenScape 4000 SoftGate - IT network failure

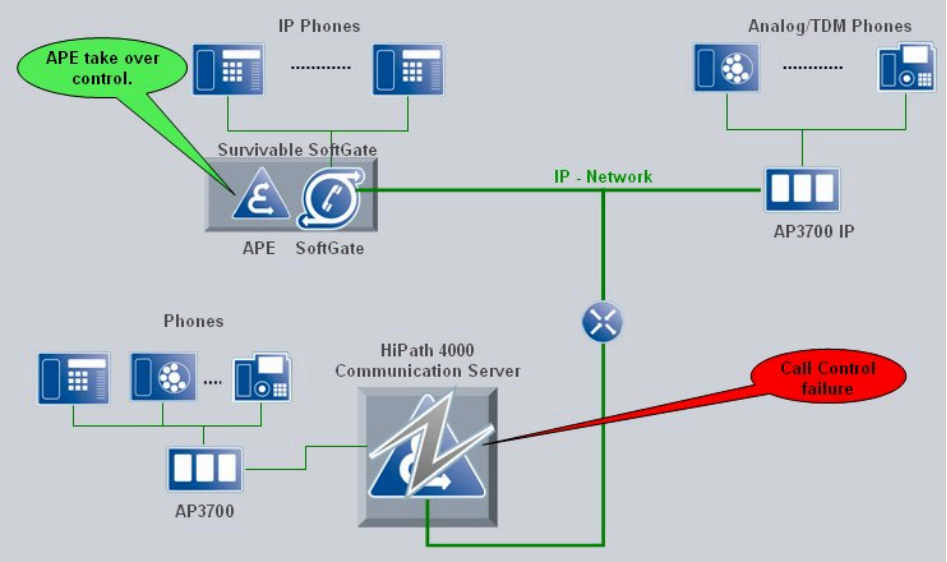


Figure 107: Survivable OpenScape 4000 SoftGate - Call control failure

3.7.2 Service Information

The feature is released on standard servers and OpenScape Access/Branch.

Possible configurations:

- Between 1 and 83 OpenScape 4000 SoftGates / AP 3700 IP with AP Emergency (own survivability unit).
- A group of AP 3300 IP, AP 3700 IP and OpenScape 4000 SoftGates (w/ o survivability unit) can connect up to an AP 3700 IP / OpenScape 4000 SoftGate with a survivability unit.

3.7.3 Generation (example)

1) First Installer
2) Select "Survivable OpenScape 4000 SoftGate" deployment.

IMPORTANT: Don’t select an interface for Atlantic LAN. Otherwise Xlink won’t work!

- For further configuration details, see "Access Point Emergency (APE)", Chapter 2, “Configuring the APE Feature (Access Point Emergency)”.

3.8 IPv6

3.8.1 Feature Description

IPv6 is to replace IPv4 in the near future. This is expected to overcome many limitations and problems that result from using IPv4. The use of IPv6 for VoIP offers some crucial benefits, for instance:

- With IPv6, NAT (Network Address Translation) will no longer be needed except for network masquerading, as the total amount of available IP addresses will be sufficient. When NAT is used, the delivery of audio packages in VoIP connections requires workarounds, which means that audio transmission problems may occur.
- IP packet routing is expected to be more efficient.
- IPv6 has built-in quality of service (QoS) capabilities, especially for realtime applications.
- Signaling (TLS) and payload encryption (SRTP) is also supported with IPv6 (see **"Signaling and Payload Encryption (SPE)"**).

3.8.2 Service Information

- IPv6 can be used in OpenScape 4000 Softgate on the vHG3500 SIP trunking (SIP-Q and native SIP) routes.
- SIP trunking can be used between different HiPath 4000 V6/OpenScape 4000 systems (SIP-Q) or between a HiPath 4000 V6OpenScape 4000 system and an external IPv6 partner, e.g. OpenScape Voice or SIP service providers (native SIP).
- For internal connectivity, IPv6 can be used between the OpenScape 4000 central switch and OpenScape 4000 SoftGates (TCP signaling) as well as between individual OpenScape 4000 SoftGates (RTP payload).
- Common gateways (HG 3500) and IPDA boards (NCUI) do not support IPv6.

3.8.3 Generation (Example)

3.8.3.1 Important Note

IMPORTANT: Following changes to the IPv6 configuration, an APE backup/restore must be performed promptly so that the APE can respond if necessary using the current/valid IP addresses and functionality is thus guaranteed.

3.8.3.2 IPv6 Networking Connectivity for OpenScape 4000 SoftGate (Trunking)

The trunking gateways (virtual HG 3500) on an OpenScape 4000 SoftGate support IPv6 networking connectivity for SIP-Q and native SIP trunking. The released IPv6 partners are listed in the Release Note.

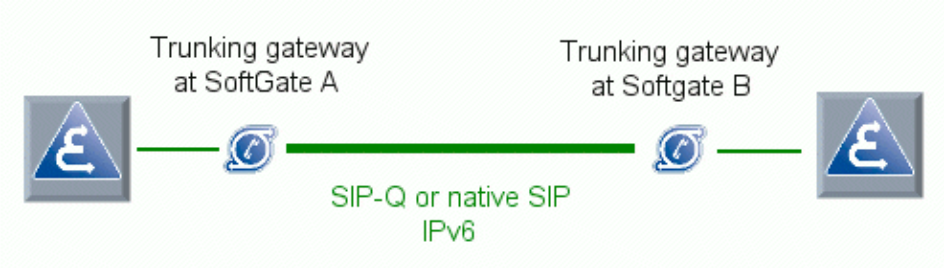


Figure 108: IPv6 for OpenScape 4000 SoftGate (trunking)

Configuration of an IPv6 connection is performed in three steps:

Configuring Trunking Gateways in OpenScape 4000

Configuring the IPv6 Address for OpenScape 4000 SoftGate Trunking Gateway (Next Generat

Configuration in the Virtual HG 3500 SIP WBM

3.8.3.2.1 Configuring Trunking Gateways in OpenScape 4000

An IPv6 trunking gateway is added to OpenScape 4000 SoftGate like an IPv4 trunking gateway via AMOs, except for configuring the IP mode.

With each IPv6 trunking gateway in a OpenScape 4000 SoftGate, "Dual Stack" mode or "IPv6 only" mode can be selected, but only if the functionality of the board is pure trunking (HG3550). This selection is done with AMO CGWB.

```
CHANGE-
CGWB:MTYPE=CGW,LTU=<ltu>,SLOT=<slot>,TYPE=IPCONF,IPMODE=DUALSTCK;
```

or

```
CHANGE-
CGWB:MTYPE=CGW,LTU=<ltu>,SLOT=<slot>,TYPE=IPCONF,IPMODE=IPV6;
```

The IPMODE default is **IPV4**.

"Dual Stack" mode has to be used when both IPv4 and IPv6 have to be supported on a SIP trunking route configured for IPv6. In this case, IPv6 is preferred. All IPv6 dual-stack partners have to be released explicitly. The released IPv6 partners are listed in the Release Note. Interworking with Full-ICE devices is not supported.

"IPv6 only" mode has to be used with pure IPv6 partners.

Remarks

- In order to avoid the IPv6 route being bypassed by IPv4 direct media connections, please ensure that **DMCEND** is configured for the IPv6 trunking gateway.

CHA-LDAT:LROUTE=<lroute>,LATTR=DMCEND;

- IPv6 is used for signaling and payload.
- All IPv6 addresses are configured/managed centrally in the Next Generation Server (NGS) of the OpenScape 4000 central switch.
- Switch Dual Stack/IPv6 board to IPv4:

- In order to change a board from Dual Stack/IPv6 to IPv4, AMO CGWB has to be used:

  CHANGE-CGWB:MTYPE=CGW,LTU=<ltu>,SLOT=<slot>,TYPE=IPCONF,IPMODE=IPv4;

  When an IPv6 or Dual Stack board is changed back to IPv4, all the IPv6 settings related to this board will be disabled automatically (IPv6 address, trunk profile configuration) or deleted (NGS entry). This means that if a further change is made back to IPv6 or Dual Stack, the IPv6 address has to be configured again in the NGS (see also Section 12.3.2.2, “Configuring the IPv6 Address for OpenScape 4000 SoftGate Trunking Gateway (Nex

3.8.3.2.2 Configuring the IPv6 Address for OpenScape 4000 SoftGate Trunking Gateway (Next Generation Server)

Configuring the IPv6 address for the OpenScape 4000 SoftGate trunking gateway is performed in the Next Generation Server via the OpenScape 4000 Platform Administration (Portal).

Following a restart, the vHG 3500 registers with the Next Generation Server and creates an entry for itself with its IPv4 address. An IPv6 address can now be configured in the Next Generation Server for the vHG 3500. Following configuration of the IPv6 address, a restart has to be performed for the vHG 3500 (RES-BSSU).

The Next Generation Server is the central point for IPv6 configuration. All IPv6 addresses are configured here.

IMPORTANT: The NGS IP address has to be configured using the OpenScape 4000 Platform Administration (Portal). It will then be automatically entered into AMO SIPCO and propagated to all SoftGates. The SoftGates need a Restart to get a new/ changed NGS IP address. Entering a NGS IP address in the WBM of each individual SoftGate is not necessary and not possible anymore.

The NGS can be reached via **OpenScape 4000 Platform Administration (Portal) > System > IPv6 Addresses**.

Once a virtual HG 3500 is configured as IPv6 or Dual Stack, it can be assigned an IPv6 address in the NGS table.

OpenScape 4000 Platform Administration (Portal) > System > IPV6 Addresses

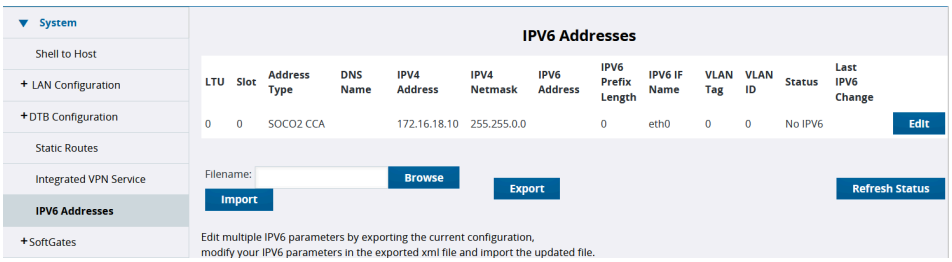


Figure 109: IPv6 address for vHG 3500

OpenScape 4000 Platform Administration (Portal) > System > IPv6 Addresses > Edit

The **IPV6 Address**, **IPV6 Prefix Length** and **IPV6 IF Name** must be specified for the IPv6 trunking gateway. A **DNS Name** can be configured optionally.

IMPORTANT: The **DNS Name** string is used in the contact field of SIP messages. There is no resolution of the DNS name in the vHG3500 and no consistency check between the DNS name and the configured IPv4 or IPv6 address. The interface name (IPV6 IF name) must correspond to the IP interface on the OpenScape 4000 SoftGate/OpenScape 4000 system (Linux OS), i.e. eth0, eth1, etc.



Figure 110: Options for IPv6 gateway

After configuring the IPv6 parameters, the trunking gateway has to be restarted (via AMO).

OpenScape 4000 Platform Administration (Portal) > System > IPV6 Addresses

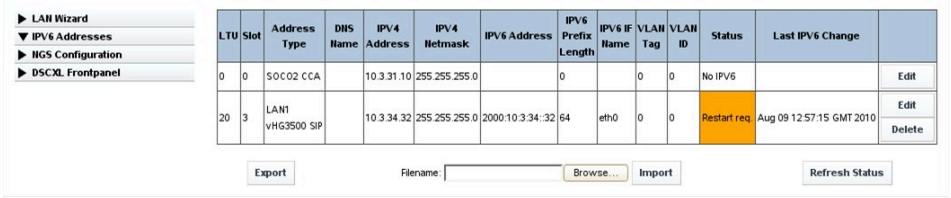


Figure 111: Status of IPv6 gateway (restart required)

After the restart, the status of the IPv6 trunking gateway should be "Confirmed".

OpenScape 4000 Platform Administration (Portal) > System > IPV6 Addresses

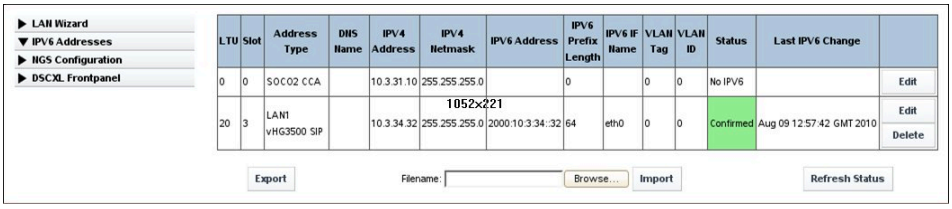


Figure 112: Status of IPv6 gateway (confirmed)

The **Status** field displays the configuration state of the IPv6 addresses, separately for each line of the IP address table:

- Changed (orange)

- An element of the IPv6 address data (IP address, prefix length, or interface name) has been modified.
- Fetched (yellow)
- The modified IP address data has been retrieved by the corresponding host (OpenScape 4000 SoftGate or OpenScape 4000 system). The NGS server now waits for an acknowledgment returned by the retrieving host, which is sent when the configuration of the modified IP address data on that host is completed.
- Confirmed (green)
- The retrieving host has acknowledged the successful setting of the modified IP address data.
- Failed (red)
- The retrieving host has returned a negative acknowledgment due to errors while setting the modified IP address data.

Information for "delete" button

The "Delete" button, corresponding to an entry in the NGS table, will only delete the selected entry in the portal / NGS database. It will not change the primary IP mode configuration in the OpenScape 4000 system database.

If the selected entry is still an active OpenScape 4000 SoftGate, whose IP mode should be changed from "IPv6 only" or "dualstack" to "IPv4 only", it is mandatory to change the IP mode with the appropriate AMOs (CGWB, STMIB) before. Otherwise the entry will re-appear without an IPv6 address after a restart.

This delete operation is mainly intended for entries (e.g. OpenScape 4000 SoftGates) which are not active anymore (e.g. powered off) and should be purged from the database.

Information on backing up and restoring the Next Generation Server can be found in Section 12.3.4, “NGS Backup and Restore”.

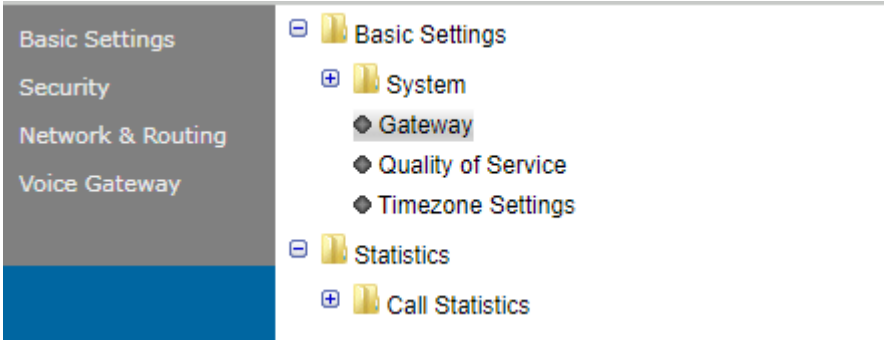
3.8.3.2.3 Configuration in the Virtual HG 3500 SIP WBM

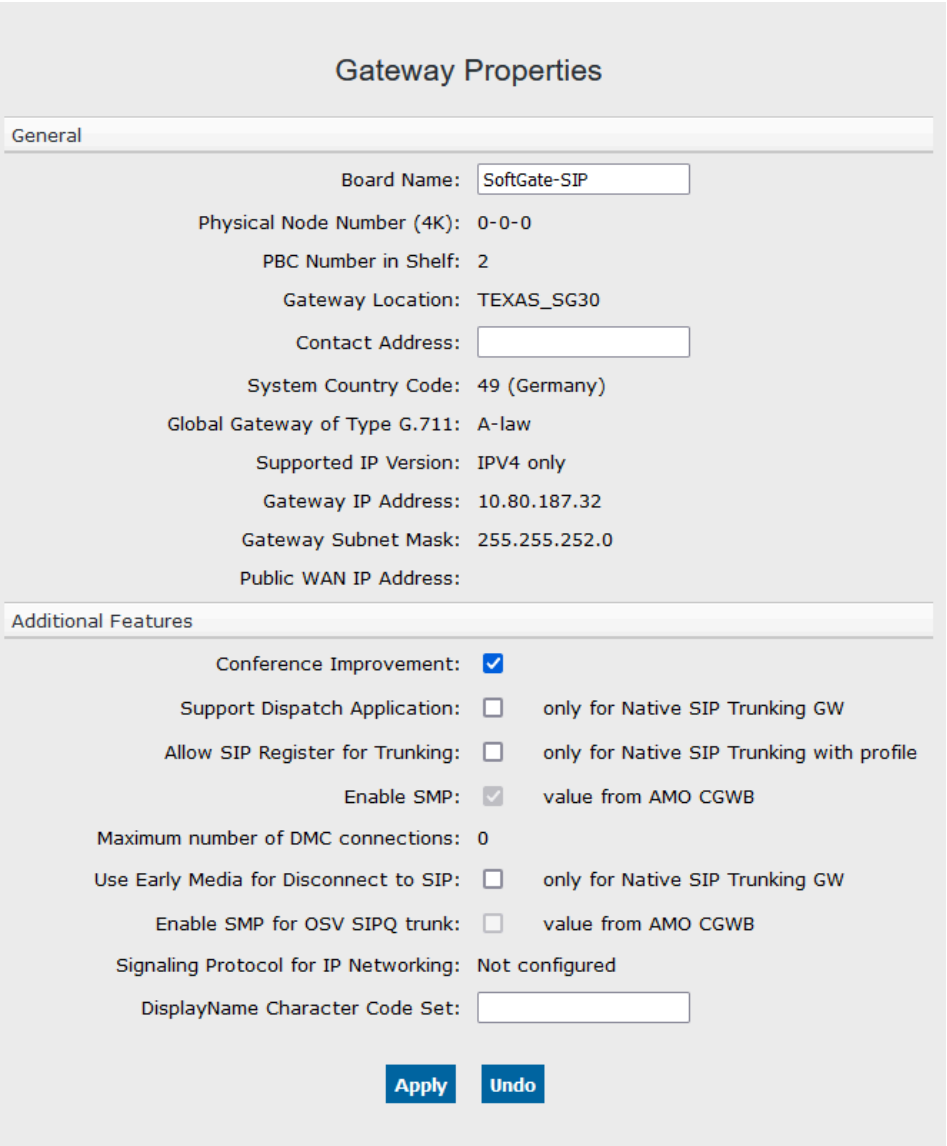
IMPORTANT: Each IPv6 trunking gateway still needs an IPv4 address for administration purposes.

1) Configuring the local gateway

The selected IP mode of an IPv6 trunking gateway can be verified via WBM.

WBM vHG 3500 SIP > Configuration> Basic Settings > Gateway





IP mode of an IPv6 trunking gateway

Following the restart, the OpenScape 4000 SoftGate recognizes the IPv6 address. It can be verified via WBM.

WBM vHG 3500 SIP > Configuration > Basic Settings > System > Gateway Properties

1) Configuring the trunking partner

Following the AMO configuration of the IP mode and the assignment of the IPv6 address via the NGS of the OpenScape 4000 SoftGate trunking gateway, the IPv6 trunking partner must now be configured using the SIP trunk profile (see **SIP Connectivity >** Section 3.3, “SIP Trunk Profiles”) in the WBM of the vHG 3500 SIP gateway.

Use of the trunking profile must be activated for the IP networking trunk type used (SIP-Q or native SIP).

WBM vHG 3500 SIP > Configuration > Voice Gateways > SIP Trunk Profile Parameter



Figure 113: SIP trunk profile parameter for IPv6 trunking partner

Use of profiles is activated as standard for native SIP trunks and deactivated for SIP-Q.

The IPv6 address or the FQDN (Fully Qualified Domain Names) under which the IPv6 trunking partner can be reached is configured in the SIP trunk profile. **Registrar**, **Proxy**, **Outbound Proxy** and **Inbound Proxy** may also have IPv6 addresses.

WBM vHG 3500 SIP > Configuration > Voice Gateways > SIP Trunk Profile

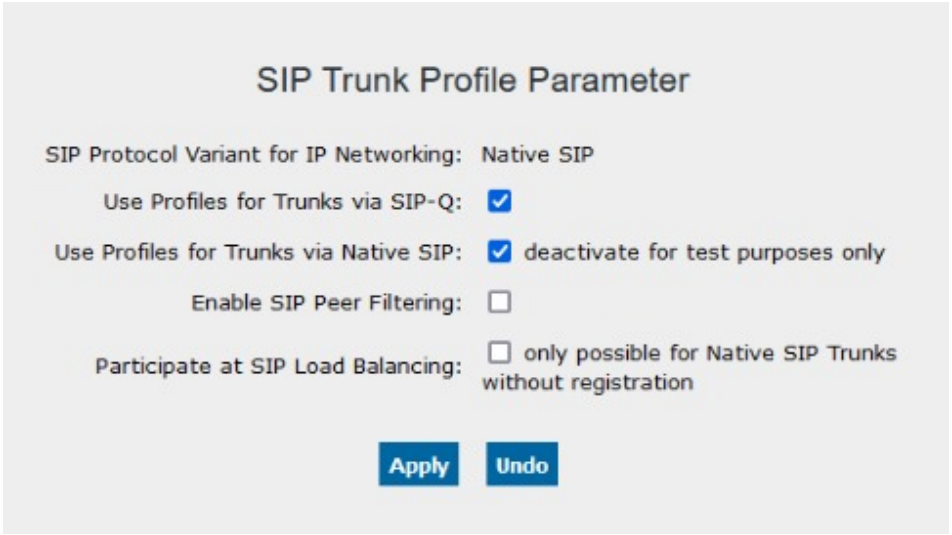


Figure 114: SIP trunk profile for IPv6 trunking partner

WBM vHG 3500 SIP > Configuration> Voice Gateways > SIP Trunk Profile > <Selected Trunk Partner Profile> **> Enable**

Because SIP trunk profiles have to be used, only one trunking partner can be configured for each gateway. Please note that, as a result, the number of IPv6 connections on a OpenScape 4000 SoftGate depends on the maximum number of SIP trunking gateways per OpenScape 4000 SoftGate (currently limited to 9).

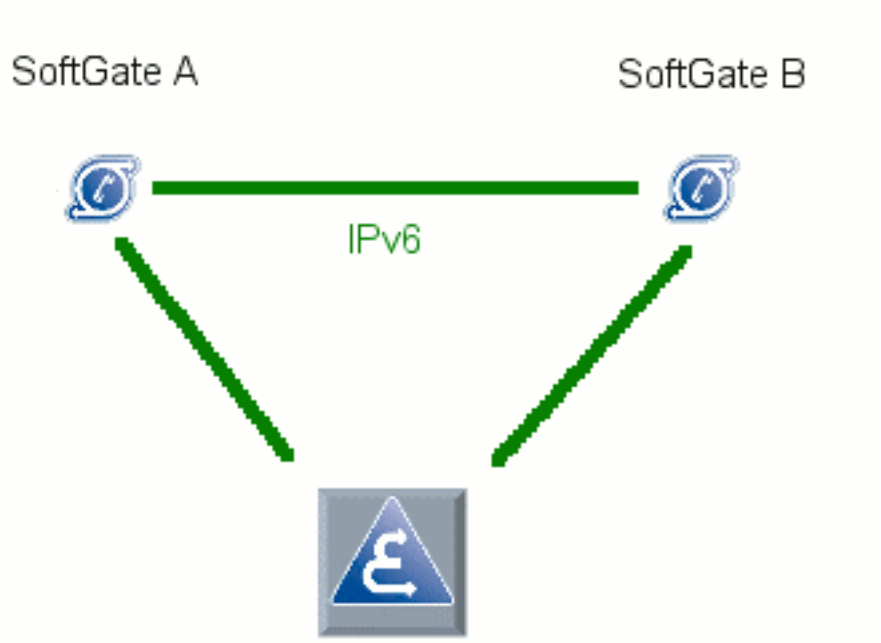
For IPv6/Dual Stack SIP-Q trunking, the profiles **SIPQ Trk Without Registration** and **SIPQ Trk With Registration** are provided.

IPv6/Dual Stack native SIP trunking uses the profiles of the corresponding released partners.

3.8.3.3 IPv6 Internal Connectivity

3.8.3.3.1 Overview

When using IPv6 for internal connectivity, the IP traffic between the OpenScape 4000 central switch and the OpenScape 4000 SoftGates (TCP signaling), as well as between individual OpenScape 4000 SoftGates (RTP payload), will use IPv6.



IPv6 for OpenScape 4000 SoftGate (internal connectivity)

IPv6 is used for signaling (HSR connection) and payload (IPDA master connection). In order to avoid bypassing the internal IPv6 connections by IPv4 direct media connections (DMC), DMC must not be enabled at the endpoints (IP phone).

When a call between two phones located at the same OpenScape 4000 SoftGate is made, only the signaling data (HSR connection) uses an IPv6 connection. The voice payload between the phones uses IPv4.

When a call between two phones located at two different OpenScape 4000 SoftGates is made, both the signaling data (HSR connection) as well as the voice payload use IPv6 connections.

3.8.3.3.2 Configuration

Prerequisite: IPv6 operation between the OpenScape 4000 central switch and all relevant OpenScape 4000 SoftGates must be configured in the system. The parameter **IPMODE=DUALSTCK** must be set for this purpose for each OpenScape 4000 SoftGate in AMO STMIB.

CHANGE-STMIB:MTYPE=NCUI2,LTU=1,TYPE=IPCONF,IPMODE=DUALSTCK;

The OpenScape 4000 SoftGate must then be supplied with the new configuration and restarted (`EXEC-USSU:MODE=UPDATAP,LTU=<ap-number>;`)!

To configure the internal IPv6 connections, the following address information is needed:

- IPv6 addresses of all hosts involved, i.e. the OpenScape 4000 central switch and OpenScape 4000 SoftGates and possibly APE / Survival OpenScape 4000 SoftGates.
- IPv4 addresses of the connected devices, in order to route the IP traffic via the IPv6 connections (tunnel) between the affected hosts.

The Next Generation Server of the OpenScape 4000 host system is the central point for IPv6 configuration. All IPv6 addresses are configured/administered here, including:

- every IPv6 address for every OpenScape 4000 SoftGate
- IPDA LAN host addresses of the OpenScape 4000 central switch (DSCXL-V2 or server),
- all IPv6 addresses of all APEs / survival OpenScape 4000 SoftGates.

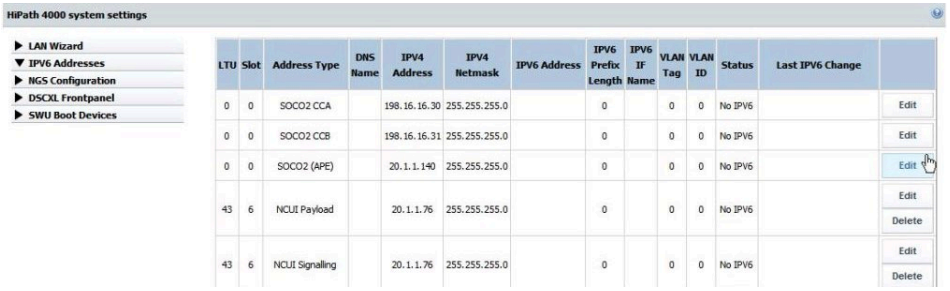


Figure 115: NGS - Administration/configuration of IPv6 addresses

The IPv4 addresses are provided locally on each host during installation with the OpenScape 4000 Platform Administration (Portal) on both the OpenScape 4000 central switch and the OpenScape 4000 SoftGate hosts.

After the first installation is completed, the OpenScape 4000 central switch and OpenScape 4000 SoftGates communicate the required IPv4 addresses to the NGS server using a notify mechanism.

The following addresses are stored in a table residing in the NGS server:

- CC-A, CC-B and CC_APE addresses
- Signaling and payload addresses of every OpenScape 4000 SoftGate

The IPv6 addresses have to be confirmed manually. The configuration of an IPv6 address requires specification of 3 elements:

- IPv6 address itself
- IPv6 prefix length
- Name of the network interface the IP address in the Linux OS of the host is bound to

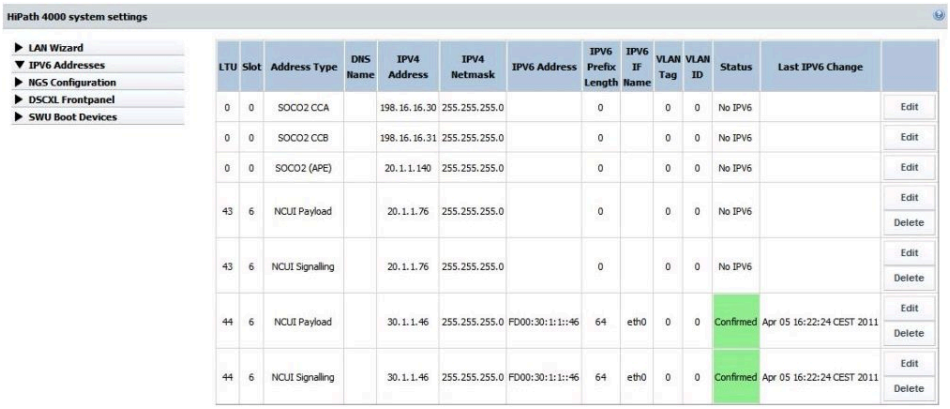


Figure 116: NGS - Confirming IPv6 addresses manually

IMPORTANT: - The interface name (**IPV6 IF name**) must correspond to the actual IP interface on the OpenScape 4000 SoftGate/OpenScape 4000 system/APE (Linux OS), e.g. eth0, eth1, etc.

IMPORTANT: OpenScape 4000 SoftGate polls the NGS server periodically for changes on the IPv6 address data. The polling period is a configurable parameter, where the default value is set to 5 minutes. Since the polling instances of all interconnected SoftGates operate independently of each other, it will in general take one full polling period to propagate the information about the modified IP address data to all these SoftGates. Therefore, the update of all affected IPv6 connections will also take at least one full polling period.

3.8.3.4 NGS Backup and Restore

The NGS database can be backed up using:

Export/ Import tool:

OpenScape 4000 Platform Administration (Portal) > System > IPv6 Addresses

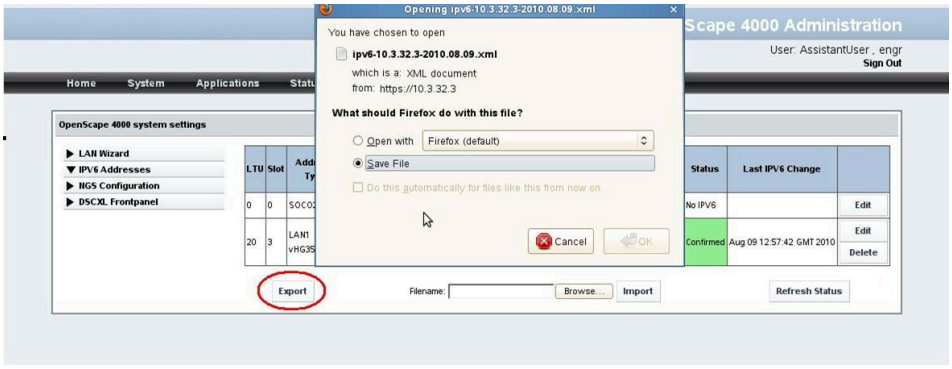


Figure 117: NGS database: Export

Using the "Export" option, the NGS database is exported as an ".xml" file, which can be handled, edited, printed out with tools like "Microsoft Office Excel":

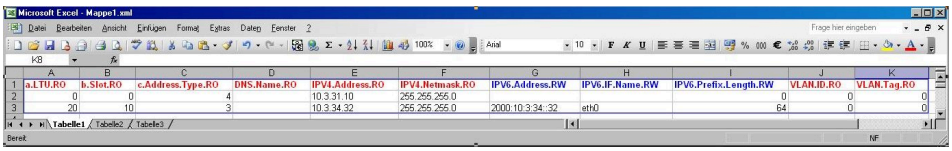


Figure 118: NGS database: Export file

If needed, the Read/Write (RW) marked fields can be edited manually before importing the table. The Read Only (RO) marked fields should not be changed manually.

After editing the table, the file has to be saved as "xml Data".

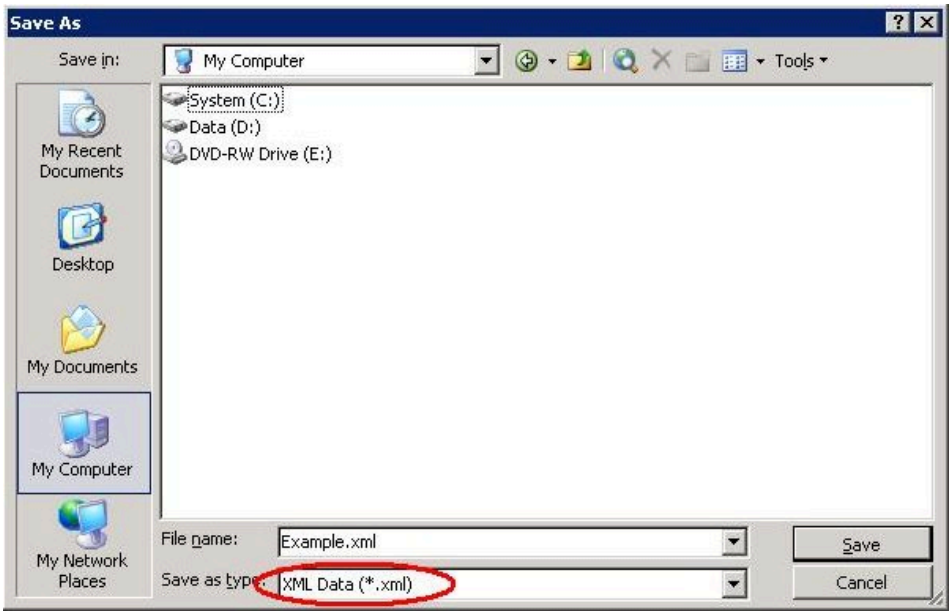


Figure 119: NGS database: Save export file

The key for accepting or rejecting an entry in the exported table is the PEN (LTU, Slot) of the board and the address type.

If a table containing an entry for one board which is no longer configured as IPv6 is imported, the corresponding entry will be dropped during the importing procedure.

OpenScape 4000 Platform Administration (Portal) > System > IPv6 Addresses

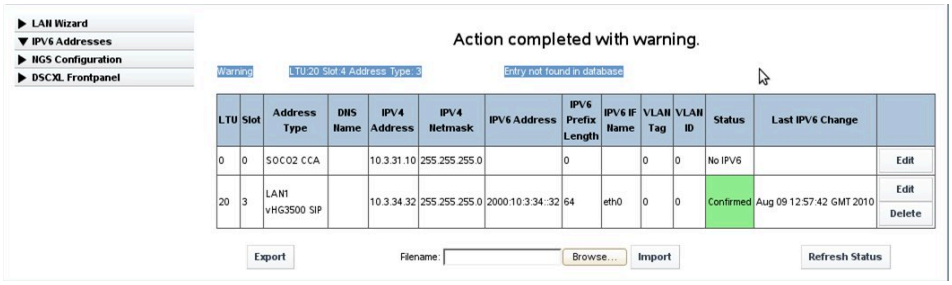


Figure 120: NGS database: Import with warnings

If a duplicate IP address is detected during the importing procedure, the whole action will fail. In this case, the table has to be rechecked manually in order to avoid database inconsistencies.

OpenScape 4000 Platform Administration (Portal) > System > IPv6 Addresses

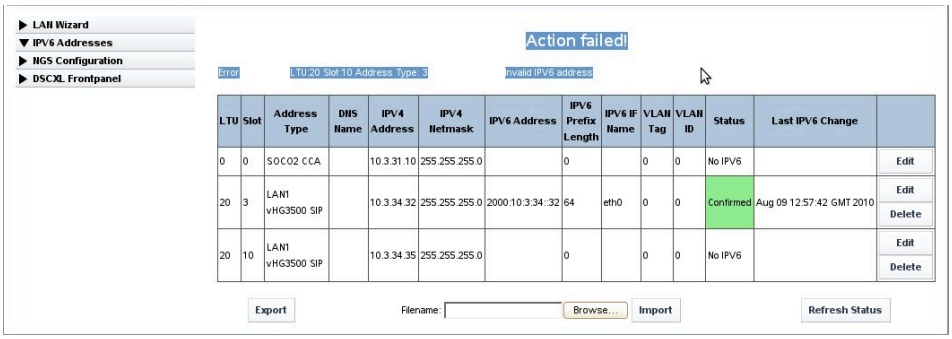


Figure 121: NGS database: Import failed

3.8.4 Relevant AMOs

AMO	Parameter	Sprache/ Language	Beschreibung/Description
CGWB	TYP=IPCONF	d	IP-Konfiguration
	TYPE=IPCONFIG	e	IP configuration
	IPMODE=DUALSTCK	d	IP-Version 4 und IP-Version 6
	IPMODE=DUALSTCK	e	IP version 4 and IP version 6
	IPMODE=IPV6	d	nur IP-Version 6
	IPMODE=IPV6	e	IP version 6 only
BCSU	TYP=IPCONF	d	IP-Konfiguration
	TYPE=IPCONFIG	e	IP configuration
	IPMODE=DUALSTCK	d	IP-Version 4 und IP-version 6
	IPMODE=DUALSTCK	e	IP version 4 and IP version 6
	IPMODE=IPV6	d	nur IP-Version 6
	IPMODE=IPV6	e	IP version 6 only
SIPCO	IPMODE	d	Possible values: IPV4, DUALSTCK
	IPMODE	e	Possible values: IPV4, DUALSTCK
STMIB	IPMODE	d	Possible values: IPV4, DUALSTCK
	IPMODE	e	Possible values: IPV4, DUALSTCK

AMO	Parameter	Sprache/ Language	Beschreibung/Description
	IPMODE=DUALSTACK	D	IP-Version 4 und IP-Version 6
	IPMODE=DUALSTACK	E	IP version 4 and IP version 6

3.9 Load Balancing

3.9.1 Feature Description

SIP Load Balancing is deployed to distribute load in SIP-related data traffic in the IP network. With SIP Load Balancing, the system is able to scale the performance of participating SIP servers in order to avoid overloading of the server and to achieve high availability of the SIP services.

Load Balancing distributes calls from a provider connection, an OpenScape UC or OpenScape Xpression to a number of gateways, for example if the connection has more than the maximum number of gateway channels. Only one target IP address can be configured in the case of a provider connection, which means that one provider connection would have to be available without Load Balancing for each gateway.

Calls can also be sent selectively by means of their phone number from one connection to a number of even geographically distributed gateway groups or OpenScape 4000 systems with the help of a routing number (e.g. local area code) which can be configured for each gateway. Within a group, the calls are sent to the gateway with the most free channels.

SIP Load Balancing can be activated for every SIP gateway (HG 3500 or vHG 3500 SIP) in the network. If the feature is activated correctly, the participating gateways register automatically at the SIP Load Balancing server.

SIP Load Balancing is also released for multiple OpenScape UC Media Server. These cannot register automatically to the SIP Load Balance server. Therefore, they must be configured manually in the OpenScape 4000 SoftGate WBM.

3.9.2 Service Information

The OpenSIPS Load Balancer is part of the OpenScape 4000 SoftGate software package and will be installed with each OpenScape 4000 SoftGate. It runs on a OpenScape 4000 SoftGate but has its own IP address (different from the IP address of the OpenScape 4000 SoftGate). The IP address is configured during installation.

Using its configured IP addresses, the Load Balancer automatically fetches its available DNS server names from the DNS server.

The "Load Balancing" feature is deactivated by default and must be activated with the WBM of the OpenScape 4000 SoftGate and the WBM of every participating gateway.

Features

- "Load Balancing" for inbound native SIP trunks towards virtual HG 3500 gateways (OpenScape 4000 SoftGate) and vxWorks based HG 3500 gateways (IPDA) (e.g. SIP Provider or OpenScape UC connectivity).
- Native SIP trunks without registration.
- Virtual HG 3500s of several OpenScape 4000 SoftGates and HG 3500 gateways of several access points can participate in Load Balancing.
- Error logging / tracing with OpenSIPS.
- Security of data communication between vHG 3500/HG 3500 and OpenSIPS (via authenticated https).
- Failover mechanism for inbound calls, which have been rejected by the gateway with an error response.
- Status monitoring of configured gateways by the Open SIPS Load Balancer.
- Load Balancing for several gateway groups.
- SPE supports TLS 1.2 protocol.
- SPE features include: Enforce Secure Renegotiation RFC, TLS renegotiation certificate revocation list, maximum re-keying interval and minimum RSA key length.

Requirements

- A OpenScape 4000 SoftGate must be available within the network.
- SIP Load Balancing can only be activated if the use of SIP trunking profiles is activated in the WBM.

  WBM > Configuration > Voice Gateway > SIP Trunk Profile Parameter
- For SIP Load Balancing to function, you must ensure that the (outbound) proxy settings in the SIP trunking profile are correctly configured.

  WBM > Configuration> Voice Gateway > SIP Trunk Profile Parameter

Restrictions

- The “SIP Load Balancing” feature can be used for Standalone or Surv. SoftGate deployments. This means, it is not available for e.g. “Integrated SoftGate” on Enterprise Gateway or Duplex.
- SIP Load Balancer supports a maximum of 2000 parallel channels.
- If TLS is used all connected Gateways need to be configured using SPE too.

3.9.3 Generation (Example)

IMPORTANT: Generation with AMOs is not possible.

3.9.3.1 SIP Load Balancer Properties

The SIP Load Balancer is activated via the WBM of the OpenScape 4000 SoftGate. The IP address of the Load Balancer and the network mask have to be entered for this purpose.

The OpenScape 4000 SoftGate has to be restarted every time the Load Balancer is activated/deactivated or every time the IP address is changed.

WBM > Configuration > SIP Load Balancer > Settings

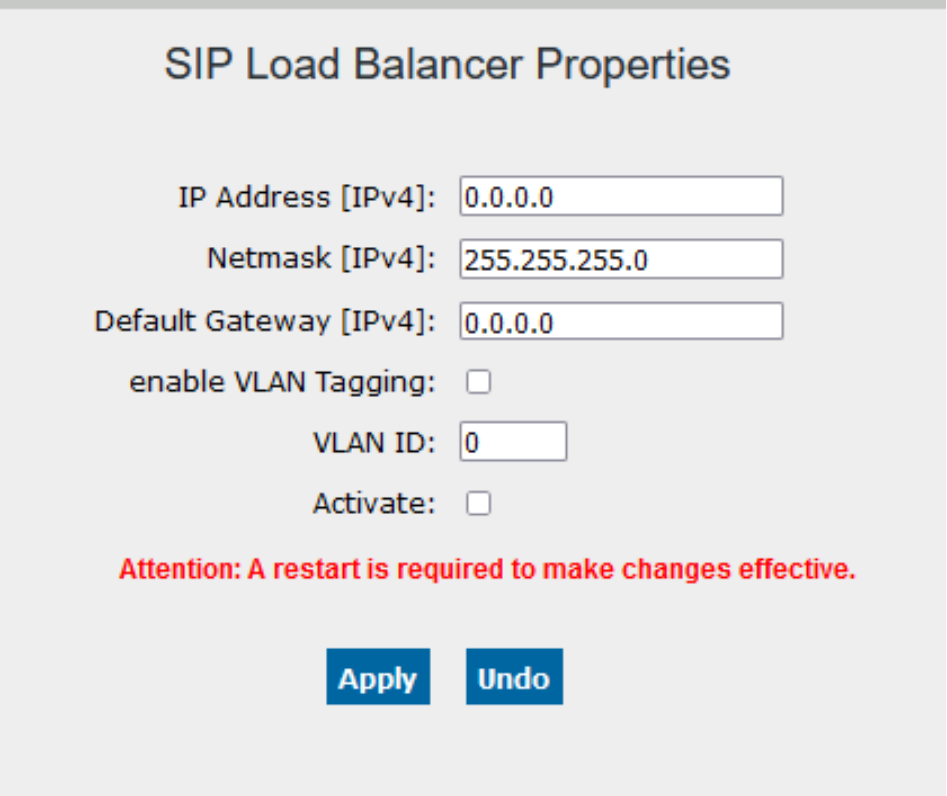


Figure 122: SIP Load Balancer Properties

3.9.3.2 Outgoing/Incoming Calls via SIP Load Balancing Server

Open **WBM > Configuration > Voice Gateway > SIP Trunk Profile Parameter**

Section **Security**

This section lists the following security settings: *Released Security Level, TLS used* and *Payload Encryption used.*

Section **Proxy**

You can configure the IP address of the Load Balancer via the Proxy.

Section **Outbound Proxy**:

For the routing of outgoing calls from the gateways via the Load Balancer to i.e. the provider, the IP address of the SIP Load Balance server has to be configured as an outgoing proxy in the corresponding trunk profile.

Section **Inbound Proxy**:

A DNS name is configured under Inbound Proxy for **IP Address/Host Name**. A number of IP addresses can be defined for this DNS name on the DNS server. This is important, because the IP address of incoming calls is checked against proxy or inbound proxy entries. OpenScape UC calls can come from more than two IP addresses and are then sent via DNS.

NOTICE: Instead of the IP address, the DNS server name of the Load Balance server can be entered as well.



Figure 123: SIP Load Balancer trunk profile parameter

Specific characteristic in case of OpenScape UC Media Server Farms

The SIP Load Balancer knows the IP addresses of the OpenScape UC Media Server. Thus, inbound and outbound proxies do not need to be configured. It is enough only to enter the proxy (=IP address of the SIP Load Balancer).

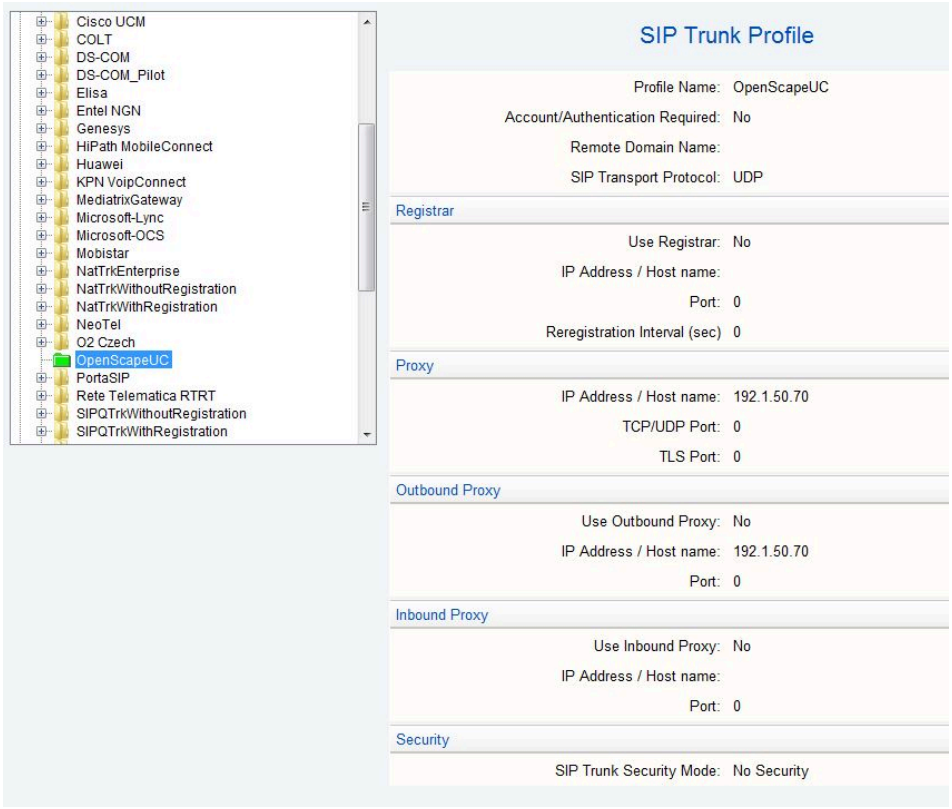


Figure 124: SIP Load Balancer trunk profile parameter for OpenScape UC Media Server

3.9.3.3 Registration of Gateways

The following section describes shortly how to configure the OpenScape 4000 SIP Load Balancer (SLB) in combination with Gateways.

The Gateways have to be added manually. The Gateway configuration is done in the WBM of the OpenScape 4000 SoftGate. One entry has to be configured for each Gateway.

WBM > Configuration > SIP Load Balancer > Status

- **Adding a rule in SLB**

  Enter all necessary/needed parameters in the text boxes at the bottom of the page and click **Add Rule**.
- **Changing an existing rule in SLB**

  If an existing rule must be modified simply add all necessary/needed parameters again in the text boxes and click **Add Rule**. The existing rule will be replaced with new parameters.

Necessary/needed fields

- **LTU**

  This parameter displays the unique identifier of the shelf.
- **Slot**

  In case of an OpenScape 4000 gateway this column can be used for the shelf configuration slot. However technically it does not affect the functionality itself and is used for orientation purpose.
- **Gateway IPv4 Address**

  IP address of the Gateway (e.g. 192.1.11.182)
- **IPv4 Port**

  SIP port of the Gateway (e.g. 5060)
- **IPv4 TLS Port**

  SIP Port is used for signaling data encrypted with TLS (Transport Layer Security) (e.g. 5061).
- **Gateway IPv6 Address**

  IP Address of the gateway in IPv6 format.
- **IPv6 Port**

  SIP Port is used for unencrypted signaling data (e.g. 5060).
- **IPv6 TLS Port**

  SIP Port is used for signaling data encrypted with TLS (Transport Layer Security) (e.g 5061).
- **Routing Number**

  The prefix of a dial-in number of a phone (e.g +498). It restricts the usage of the registered gateways for the phone numbers that have matching prefixes with the routing number (e.g. 49897000719999)
- **Max Number of B-Channels**

  In best case the maximum possible parallel channels of each gateway should be used. The maximum number of B channels for gateways is 120.

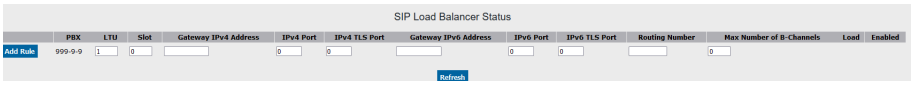


Figure 125: Registration of Gateways

3.9.3.4 Registration of UC Media Server Farm

See below screenshot for a typical Media Server farm configuration in a large or very large deployment. Each Media Server has an individual conference dial-in number known as **Trunk number** (e.g. +4982700332201) and a general conference dial-in number known as **Additional numbers** (e.g. +4982700332200).

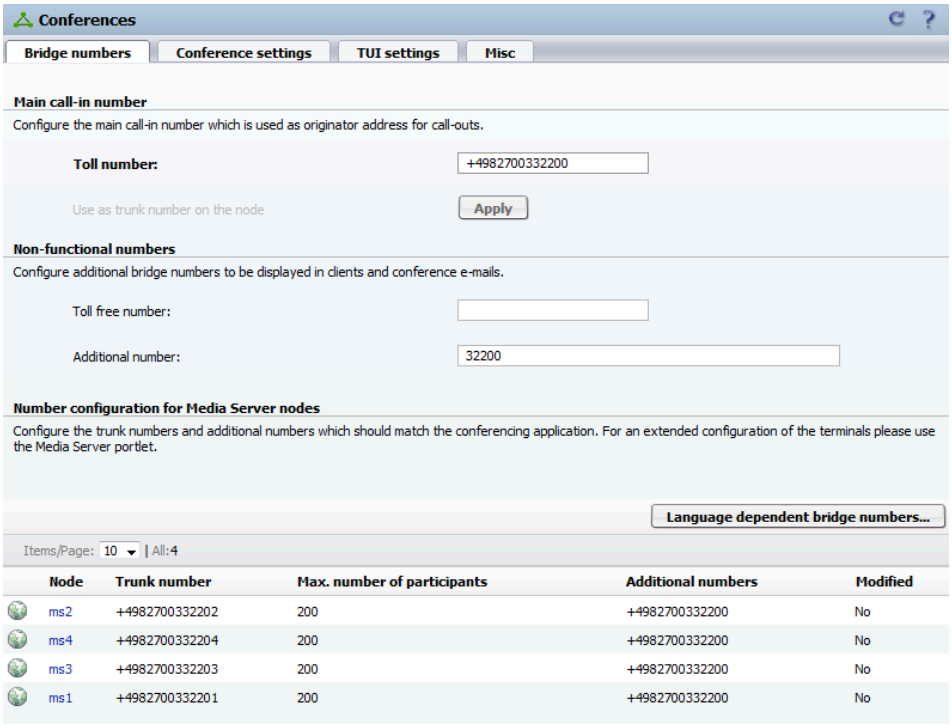


Figure 126: OpenScape UC Media Server farm

The following section describes shortly how to configure the OpenScape 4000 SIP Load Balancer (SLB) in combination with a Media Server farm.

The Media Servers have to be added manually. Both dial-in numbers, the individual and the general one, of each Media Server has to be configured in SLB. This means two entries have to be configured for each Media Server.

The Media Server configuration is done in the WBM of the OpenScape 4000 SoftGate.

WBM > Configuration > SIP Load Balancer > Status

- **Adding a rule in SLB**

  Enter all necessary/needed parameters in the text boxes at the bottom of the page and click **Add Rule**.
- **Changing an existing rule in SLB**

  If an existing rule must be modified simply add all necessary/needed parameters again in the text boxes and click **Add Rule**. The existing rule will be replaced with new parameters.

Necessary/needed fields

- **Slot**

  This field is normally used for the OpenScape 4000 configuration slots. In the Media Server case this parameter should be used as unique identifier. Useful would be to use e.g. "1" and "11" for the first Media Server to separate the conference dial-in numbers, "2" and "22" for the second Media Server and so on.
- **Gateway IPv4 Address**

  IP address of the Media Server (e.g. 192.1.11.182)
- **IPv4 Port**

  SIP port of the Media Server (e.g. 5060)
- **Routing Number**

  Dial-in numbers for the Media Server (e.g. +4982700332200 for "1" and +4982700332201 for "11")
- **Max Number of B-Channels**

  In best case the maximum possible parallel channels of each Media Server shall be used. Due to this a limitation of parallel channels from Media Server side can be prevented. In the example 2000 is used.

SIP Load Balancer Status

	PBX	LTU	Slot	Gateway IPv4 Address	IPv4 Port	IPv4 TLS Port	Gateway IPv6 Address	IPv6 Port	IPv6 TLS Port	Routing Number	Max Number of B-Channels	Load	Enabled
Delete Rule	12-1-750	17	85	192.1.11.24	5060	5061		5060	5061		30	0	yes
Delete Rule	12-1-750	18	8	192.1.33.78	5060	5061		5060	5060		10	0	yes
Delete Rule	999-9-9	9	1	192.1.11.182	5060	0		0	0	+4982700332200	2000	0	yes
Delete Rule	999-9-9	9	2	192.1.11.183	5060	0		0	0	+4982700332200	2000	0	yes
Delete Rule	999-9-9	9	3	192.1.11.184	5060	0		0	0	+4982700332200	2000	0	yes
Delete Rule	999-9-9	9	4	192.1.11.185	5060	0		0	0	+4982700332200	2000	0	yes
Delete Rule	999-9-9	9	11	192.1.11.182	5060	0		0	0	+4982700332201	2000	0	yes
Delete Rule	999-9-9	9	22	192.1.11.183	5060	0		0	0	+4982700332202	2000	0	yes
Delete Rule	999-9-9	9	33	192.1.11.184	5060	0		0	0	+4982700332203	2000	0	yes
Delete Rule	999-9-9	9	44	192.1.11.185	5060	0		0	0	+4982700332204	2000	0	yes
Add Rule	999-9-9	9	0		0	0		0	0		0		

Figure 127: Media Server configuration for SIP Load Balancing

NOTICE: For information on how to configure the OpenScape UC please refer to the OpenScape UC documentation.

3.10 Secure Remote Subscriber

The "Secure Remote Subscriber" feature provides HFA and SIP/UFIP features for a remote subscriber connected over the Internet. Signaling and payload encryption is supported for the remote subscriber as well as the route through the Internet.

3.10.1 Feature Description

The OpenScape 4000 offers an IP-based connectivity between the OpenScape 4000 SoftGate (communication service signaling/media control unit) and the endpoints. These endpoints can be:

- The full OpenScape 4000 feature sets. The abbreviation HFA is used for this functionality in the following sections.
- The Universal Feature Access IP sets. The abbreviation UFIP is used for this functionality in the following sections.
- Classic SIP devices (HW or SW clients) used for VoIP (Voice over IP) communication.

A secure IP (TLS/SSL-based) operating mode, called SPE (Signaling and Payload Encryption), is supported - signaling and payload connections for HFA and SIP subscribers are always encrypted even if SPE is not activated.

The OpenScape 4000 functionality can also be used on the phones in the user's remote office. The IP connectivity (HFA, SIP/UFIP) via the public internet to OpenScape 4000 SoftGate is therefore incorporated. The OpenScape 4000 SoftGate is located with one interface in the public network (WAN interface) and the other interface in a corporate network (IPDA interface).

There is also implemented an extended support for SoftGate side DNAT (DMZ) use cases.

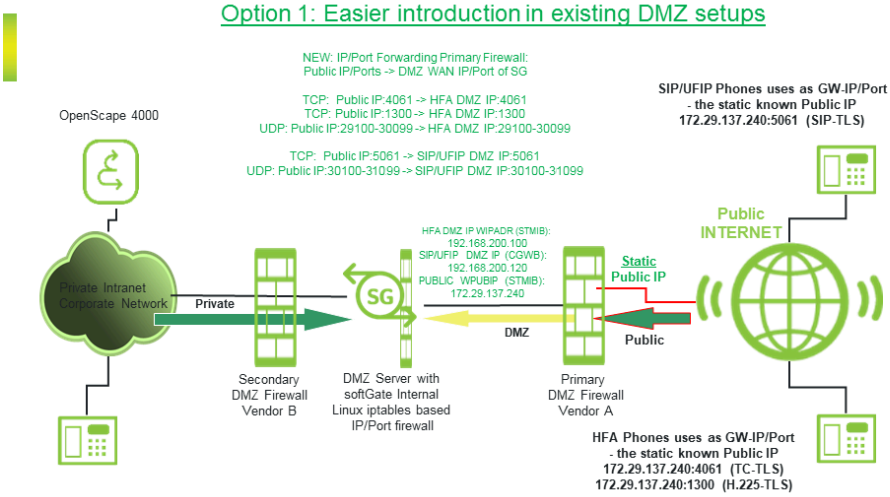
See RN (Release Note) for latest information about this improvement.

See Section 14.2.4, “DMZ” for more information about DMZ configuration.

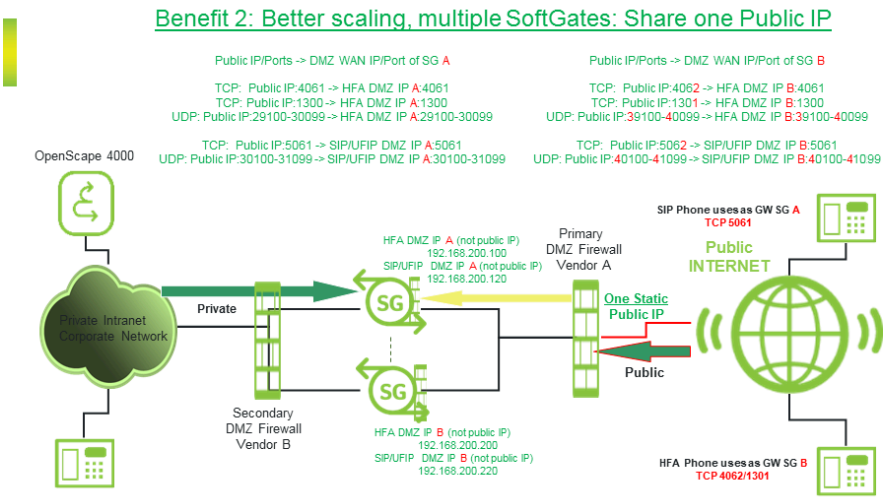
3.10.1.1 SoftGate Server Side Destination NAT (DNAT) Option

Basic Configuration

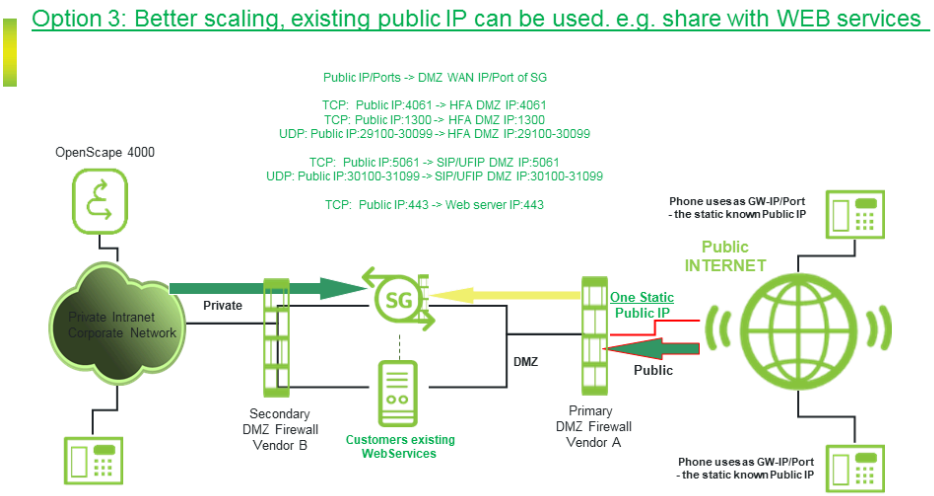
Option 1: Easier introduction in existing DMZ setups.



Option 2: Better scaling, multiple SoftGates: Share one Public IP.



Option 3: Better scaling, existing public IP can be used. e.g. share with Webservices



3.10.2 Service Information

3.10.2.1 Requirements

- The feature requires unrestricted Internet access with a static, public IP address for the OpenScape 4000 SoftGate server/service.
- An IP password must be assigned to the relevant phones in AMO SBCSU
- The phone in the remote office has to operate in secure mode, it has to be registered with TLS.
- The WAN interface of the OpenScape 4000 SoftGate requires a certificate. In case of SIP/UFIP the certificate is required for the Gateway to which SIP/UFIP subscribers are connected.

- The phone in the remote office has to use an NTP server (e.g. Internet Pool NTP) for time synchronization. The simplest way is to use an NTP server pool (e.g. 0.de.pool.ntp.org).
- For use of mobile HFA:
- To achieve a fully working mobile HFA scenario, the visit and home devices have to be configured on the same OpenScape 4000 SoftGate if the visit phone is the phone in the remote office.
- If an OpenScape Deployment Service (DLS) is used, both services, DCMP and DLS, have to be accessible via the public network. You will find additional information on the topic of "Configuring Home User Terminals for DLS/DCMP" in the Administrator Manual for the "OpenScape Deployment Service V8".
- For HFA SRS can be used across multiple vSTMI boards in a SoftGate. Hence the feature itself has no limit as to how many subscribers can be configured for SRS in the SoftGate.
- For SIP/UFIP phones however there is dedicated vSTMI board for SRS and its IP address must be known to the primary DMZ firewall and respective port forwarding rules for SIP signaling and media need to be configured. More vSTMI SIP cards (either on single SG or across multiple SoftGates) can be accessed only if there are created separate forwarding rules in the firewall distinguished by different ports, i.e. 5061, 5062, etc. (see Chapter 14, “Option 2: Scenario overview of DMZ with SoftGate DNAT option and multiple SoftGates”)

3.10.2.2 General

There is substantial difference between SRS for HFA and SIP/UFIP:

- HFA: Once the WAN Settings of the SoftGate are activated, a HFA Proxy will be used to query any HG3530 vSTMI boards when a phone tries to logon (meaning the HG3530 vSTMI doesn’t need any special configuration for this feature).
- SIP/UFIP: Dedicated SIP vSTMI must be configured for SRS and all remote subscribers must be configured on this board.
- Only one endpoint (phone or soft client) and a DSL router are required at the remote office location (e.g. Netgear, D-Link, FRITZ!Box, etc.). OpenStage, DPIP & CPx00 HFA terminals and the OpenScape Personal Edition Software Clients are supported as endpoints for HFA SRS (Info: OpenScape Personal Edition Software Clients additionally need to connect to DLS - see Section 14.2.3, “Restrictions”). OpenScape SIP terminals and wide scale of VoIP soft clients are supported for SIP/UFIP SRS.
- The solution is NAT aware and is suitable for a number of HFA devices behind one NAT router. Since V7R2 the solution supports also a so called near-end Destination NAT (DNAT) on the SoftGate Server Side. Hereby the SoftGate can be used also behind a DMZ firewall with port forwarding configuration.
- The OpenScape 4000 SoftGate offers a dedicated Ethernet port (WAN interface) for Internet connectivity including the necessary firewall configuration.
- OpenScape 4000 SoftGate administration including this feature is performed fully via the Intranet/enterprise IP connectivity to the OpenScape 4000 host system/OpenScape 4000 Assistant. External access over the Internet is not necessary.

- Centralized deployment via DLS is optional.
- Bandwidth requirement considerations
- Due to the best effort characteristic of the public Internet, a reliable bandwidth for RTP traffic between the user in the remote office and OpenScape 4000 SoftGate WAN access cannot be guaranteed.

  Based on our experiences during testing, we can make the following recommendations.

  – Subscriber side connection

  The minimum recommended DSL speed for a user with home Internet access is a DSL 6000 (max. download 6016 kbit/s - max. upload 512 kbit/s), assuming that this Internet Service Provider access is used in parallel for standard office working tasks (e.g. e-mail and "normal" Web browsing).

  – OpenScape 4000 SoftGate WAN interface

  The dimensioning of the bandwidth of the OpenScape 4000 SoftGate for Internet access must be considered carefully. Because the user's devices in the remote office cannot use DMC functionality, all calls (payload voice streams) are terminated in the OpenScape 4000 SoftGate. For the bandwidth calculation a payload voice channel (b/d channel in classical PBX wording) with the corresponding codec parameters based on the existing bandwidth tables (see **Gateways HG 3500 and HG 3575** > Section 2.5, “Bandwidth Requirements”) and traffic model calculation (http://intranet.mch4.global-intra.net/syseng/perfeng/tools/nert/index.htm) must be considered for each device.

  Sample calculation for dimensioning OpenScape 4000 SoftGate WAN access with G./11 (without VAD, 20 ms):

  – SDSL 1000 kbit/s (Note: symmetric connection, uplink speed/bandwidth= downlink speed/bandwidth)
  – User in remote office uses G.711 without VAD and with 30 ms sampling time => 85 kbit/s
  – This results in (1000/85 = 11.7 -> rounded down by ~5% for signaling and non-media, e.g. DLS, Picture CLIP) a maximum of 11 parallel channels
  – 11 channels with 1 % probability of blocking results according to Erlang calculator in 5.1599 Erlang (see also **Gateways HG 3500 and HG 3575** > Section 2.7, “Traffic Considerations”)
  – For 0.15 Erlang per user, this results in (5.1599/0.15 =>) a maximum of 34 users in the remote office.

  Sample calculation for dimensioning OpenScape 4000 SoftGate WAN access with G.729 (without VAD, 20ms):

  – SDSL 1000 KBit/s (Note: symmetric connection, uplink speed/bandwidth= downlink speed/bandwidth)
  – User in remote office uses G.729 without VAD and with 20 ms sampling time => 40 KBit/s
  – This results in (1000/40 = 25 -> rounded down for ~5% for signaling and non-media, e.g. DLS, Picture CLIP) a maximum of 24 parallel channels
  – 24 channels with 1 % probability of blocking results according to Erlang calculator in 15,2950 Erlang (see also **Gateways HG 3500 and HG 3575** > Section 2.7, “Traffic Considerations”)

  - For 0.15 Erlang per user, this results in (5.1599/0.15 =>) a maximum of 102 users in the remote office.

  Mixing of regular users and call center agents via the same WAN interface is possible. However, in order to guarantee connection availability to call center agents at all times, these users will be trafficked at 1 Erlang (36 C.C.S.). The WAN interface is subject to the same traffic model calculations like other communication models.

- Notes
  - OpenScape 4000 SoftGate has its own voice firewall based on HFA. It therefore behaves like a voice firewall. If customers require additional protection of the OpenScape 4000 SoftGate server and the corporate IT network, however, this can be achieved by setting up a DMZ. See also Section 14.2.4, “DMZ”.
  - Most providers of standard home (user) Internet connections perform a forced disconnect after 24 hours. The time of this forced disconnect can be controlled with many of the IADs (e.g. 03:00h). This disconnect leads to loss of any active calls and reregistration of the phone. This process corresponds to a "normal" L1 error.
  - Where mobile HFA is used, the disconnect described in Note 2 leads to the logging off of the mobile HFA.

3.10.2.3 Restrictions

- DMC is not supported for remote office phones.

  When the terminal is registering at the OpenScape 4000 SoftGate, it is detected as a remote subscriber and therefore automatically not treated like a DMC endpoint by the system, regardless of the AMO SDAT parameter **DMCALLWD**. To support partial DMC routes to the last possible endpoint (in this case the OpenScape 4000 SoftGate itself) it is recommended to activate **DMCALLWD** in AMO STMIB for the OpenScape 4000 SoftGate.
- The typical plug’n’play function is supported for remote subscribers but not in connection with DLS synchronization. If a synchronization has been started between OpenScape 4000 Assistant/Manager and DLS, the gateway IP addresses of the remote subscribers will be overwritten in the DLS database. They must be manually changed to the WAN gateway IP address afterwards.
- SIP/UFIP SRS does not support "mobile HFA" feature and it is necessary to have unique phone number for local phone and different one for SRS.
- The feature Secure Remote Subscriber is available on STMIX/STMIY only for SIP.
- HFA is only possible on SoftGates.
- Parallel connections of SIP SRS from LAN and WAN to the same gateway are not possible. The SRS for SIP phone numbers can only be connected via WAN interface.

3.10.2.4 DMZ

In most cases where the customer requires additional protection, an additional primary DMZ firewall where possible should suffice. In addition to the constantly

active internal OpenScape 4000 SoftGate voice firewall, this additional firewall could be activated between the Internet and the OpenScape 4000 SoftGate.

In the following example we consider a DMZ scenario, which consists of both a primary and a secondary DMZ firewall.

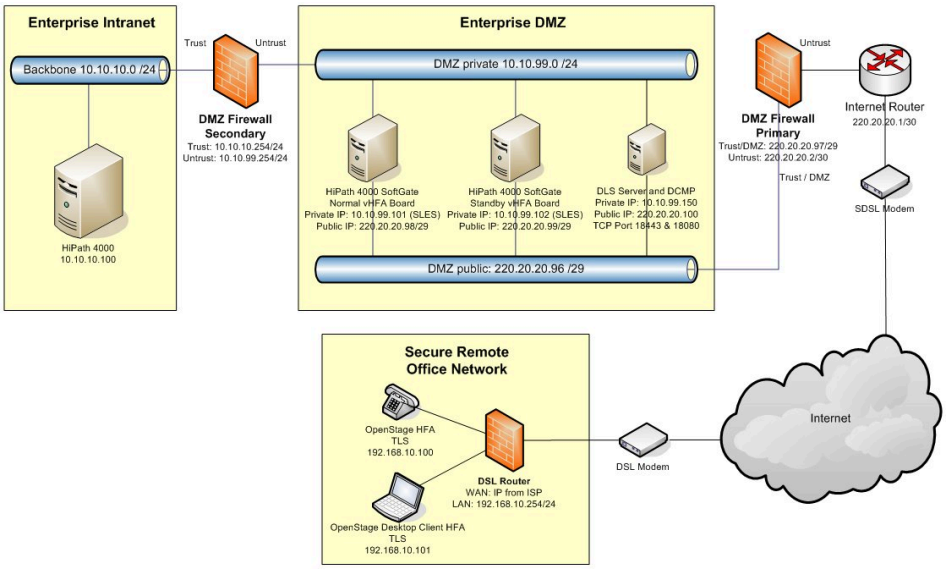


Figure 128: DMZ scenario

Figure 132 shows a network plan with a DMZ scenario consisting of corporate/ enterprise network, DMZ private and DMZ public/Internet. If such a DMZ is to be used, it must be checked whether all required ports have been enabled in the DMZ firewalls (typically primary and secondary DMZ firewalls).

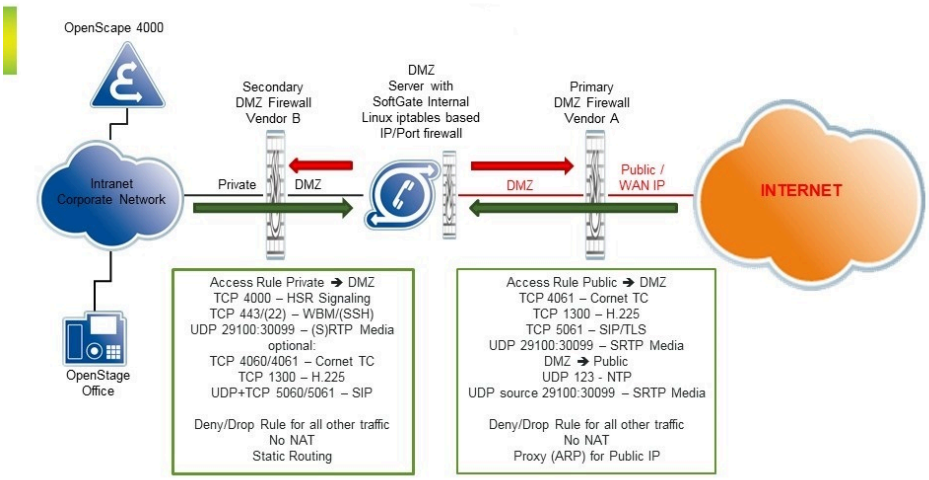


Figure 129: DMZ scenario - Required ports

Figure 133 shows a DMZ scenario from another perspective, in which the required ports will be discussed in greater detail. The respective ports as well as other ports are listed below and can also be found in the OpenScape 4000 Security Checklist.

The following ports (with reference to Figure 132 and Figure 133) have to be open in the firewall:

Primary DMZ firewall

- **Internet/Public (Untrust) => DMZ Public (Trust)**
  - TCP 4061 for Cornet TC/TLS
  - TCP 1300 for H.323/TLS
  - TCP 5061 for SIP/TLS
  - UDP ports for SRTP media (Default = 29100-30099, AMO STMIB:WANFD)

  Optional:

  - *TCP 443 for Picture CLIP (OpenStage 60/80)*
  - *TCP 8802 for WSI (CP400/600/700 HFA)*

    This port can be configured in Platform Portal (central host platform) and can be activated for WAN (by default off).
  - *TCP 18080/18443 for DLS and DCMP (e.g. use of SoftClient or Software Lifecycle)*
- **DMZ Public (Trust) => Internet/Public (Untrust)**
  - UDP 123 for NTP synchronization of OpenScape 4000 SoftGate via the Internet
  - UDP ports for SRTP media (Default = 29100-30099, AMO STMIB:WANFD)
  - Deny/drop rule for all other traffic
  - No NAT
  - Proxy (ARP) for Public IP

NOTICE: The blocking of DMZ Public (Trust) => Internet/ Public (Untrust) traffic is for the prevention of misuse of the OpenScape 4000 SoftGate server and the public IP.

Secondary DMZ firewall

- **Corporate/Enterprise Network (Trust) => DMZ Private (Untrust)**
  - TCP 4000 for the HSR signaling protocol. For signaling survivability, please refer to Section "**Signaling Survivability**" for the relevant ports.
  - TCP 443/22 for WBM/SSH administration ports
  - UDP ports for (S)RTP media (Default = 16384-<n - Ports>) - see **HG 3500 and HG 3575 Gateways** >Chapter 20, “IP Ports”
  - UDP ports for (S)RTP media (Default = 29100-30099) - see **HG 3500 and HG 3575 Gateways** > Chapter 20, “IP Ports”
  - Deny/drop rule for all other traffic
  - No NAT
  - Static routing

  Optional:

  - *TCP 4060 for Cornet TC/TCP: HFA terminal registers from the corporate/ enterprise network.*
  - *TCP 4061 for Cornet TC/TLS: HFA terminal registers from the corporate/ enterprise network.*
  - UDP & TCP 5060 for SIP terminal registers from the corporate/enterprise network.
  - TCP 5061 for SIP/TLS terminal registers from the corporate/enterprise network.
  - *TCP 1300 for H.323/TLS: HFA terminal registers from the corporate/ enterprise network.*
  - *TCP 1720 for DMC (e.g. OpenScape 4000 SoftGate vNCUI DMC activated)*
  - *TCP 18443/18444 for DLS functionality. Additional ports may be necessary depending on the manner of use of the DLS. See OpenScape Deployment Service Documentation or Release Note for a detailed list of ports.*
- **DMZ Private (Untrust) => Corporate/Enterprise Network (Trust)**
  - UDP ports for (S)RTP media (Default = 16384-<n - Ports>) - see **HG 3500 and HG 3575 Gateways** > Chapter 20, “IP Ports”.
  - UDP ports for (S)RTP media (Default = 29100-30099) - see **HG 3500 and HG 3575 Gateways** > Chapter 20, “IP Ports”.

  Optional:

  - *TCP 1720 for H.323/TCP: HFA terminal registers from the corporate/ enterprise network.*
  - *TCP 1720 for DMC (e.g. OpenScape 4000 SoftGate vNCUI DMC activated)*
  - *UDP ports for DMC from optiPoint (Default=5004-ff) / OpenStage (Default=5010-ff) terminals (see documentation for terminals).*
  - *TCP 443 for Backup Server (e.g. use of automatic restore concept)*
  - *TCP 8082/8084/8085 for DLS functionality: Additional ports may be necessary depending on the manner of use of the DLS. See OpenScape Deployment Service Documentation or Release Note for a detailed list of ports.*

NOTICE: Open ports in the direction of the protected corporate/enterprise network (known as firewall pinholes)

should be avoided for safety reasons if possible, but are required for the above-named exception scenarios.

3.10.3 Generation (Example)

The next diagram roughly outlines the IP communication relationship between the SPE-enabled HFA device and the OpenScape 4000 SoftGate.

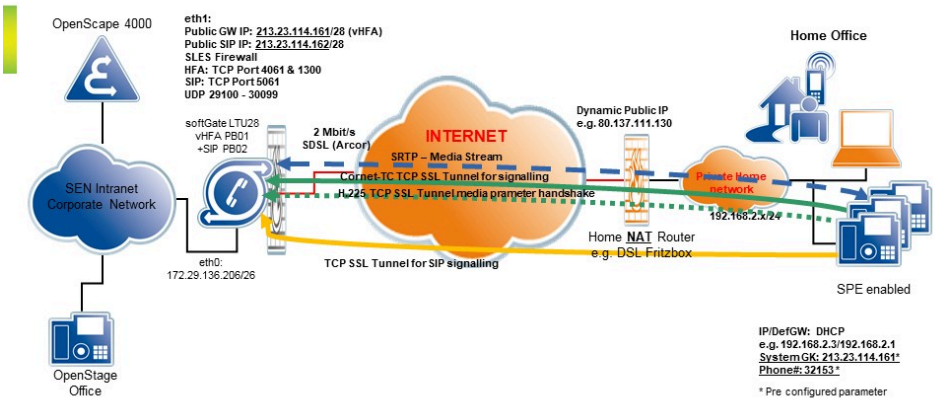


Figure 130: Secure IP connectivity for remote subscribers - Sample generation

Configuration steps

The following steps have to be performed following installation of the OpenScape 4000 SoftGate:

1) Generate the WAN interface with AMO STMIB (IP address, netmask and default router).

WAN interface data:

AMO STMIB is extended with the following parameters in a new **WANIF** branch:

WIPADR=<ip address>, **WNETMASK**=<ip address>, **WVLAN**=<YES/NO>, **WVLANID**=<number>, **WDEFRT**=<ip address>, WPUBIP=<ip address>

Example:

```
CHANGE-
STMIB:MTYPE=NCUI2,LTU=20,TYPE=WANIF,WIPADR=10.80.144.246,WNETMASK=255.255.248.0,WVLAN=NO,
WVLANID=0,WDEFRT=10.80.144.1,WPUBIP=172.16.1.126;
```

WANIF	WAN interface
WIPADR	IP address of WAN interface
WNETMASK	Netmask of WAN interface
WVLAN	VLAN tagging of WAN interface (YES/NO)

WVLANID	Virtual LAN ID of WAN interface
WDEFRT	IP address of the default router in the WAN segment
WPUBIP	Public IP address of WAN interface

After changing these parameters,

```
EXEC-USSU:MODE=UPDATAP,LTU=<LTU_of_OpenScape4000_SoftGate>;
```

of the OpenScape 4000 SoftGate must be performed. The OpenScape 4000 SoftGate is reset and the changes will be activated.

WAN feature data:

AMO STMIB is extended with the following parameters in a new **WANFD** branch:

WUDPPRTL=<number>, **WUDPPRTH**=<number>, **WTOSPL**=<string>, **WTOSSIGN**=<string>, **WTLSP**=<number>

Example:

```
CHANGE-
STMIB:MTYPE=NCUI2,LTU=20,TYPE=WANFD,WUDPPRTL=29100,WUDPPRTH=30099,WTOSPL="184",WTOSSIGN="
```

WANFD	Feature data of the WAN interface
WUDPPRTL	Lower limit for the released UDP port range
WUDPPRTH	Upper limit for the released UDP port range
WTOSPL	TOS, Payload outgoing WAN for HFA
WTOSSIGN	TOS, DiffServ Code Point for HFA signaling
WTLSP	HFA TLSP port

The OpenScape 4000 SoftGate itself does not have to be reset if these parameters are changed, rather the data is activated as soon as the AMO has made the changes.

WTOSSIGN	TOS, DiffServ code point for HFA signaling
WTLSP	HFA TLSP port

After changing these parameters,

RES-USSU:LTU,<LTU_of_OpenScape4000_SoftGate>;

of the OpenScape 4000 SoftGate must be performed. The OpenScape 4000 SoftGate is reset fully and the changes are activated.

NOTICE: (HFA only) The default UDP port range of 1000 open ports (Default = 29100-30099) can be restricted. It must be noted here that two UDP ports must be available for each HFA terminal in the remote office. If no UDP port is available at call setup, the HFA terminal is reset with an L1 error. So-called overbooking is not supported.

---

2) Configure the OpenScape 4000 SoftGate's WAN interface via the Web Based Management (WBM)

OpenScape 4000 SoftGate WBM > Configuration > WAN > Settings

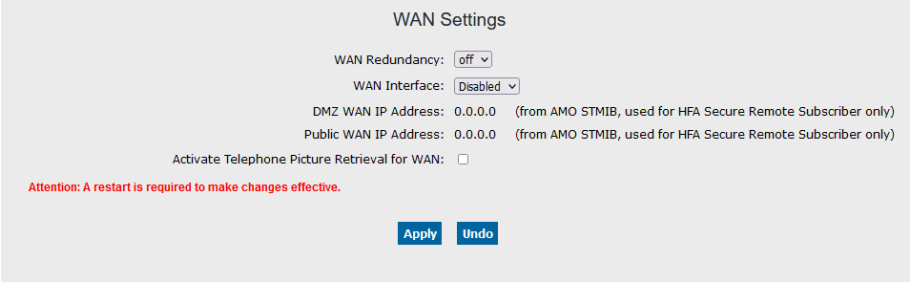


Figure 131: Secure Remote Subscriber - OpenScape 4000 SoftGate WAN settings

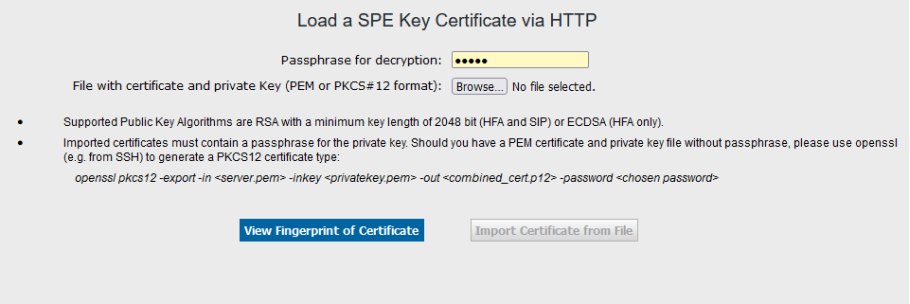
- Select a **WAN interface** (e.g. eth1). **Apply** the settings and then restart OpenScape 4000 SoftGate with the **Restart** button in the WBM.

  NOTICE: If the WAN interface is to be configured later, as described in point 3, via AMO STMIB, then the restart from the WBM can be relinquished. The necessary `EXEC-USSU:UPDATAP,<LTU_of_OpenScape4000_SoftGate>;` command essentially leads to a full OpenScape 4000 SoftGate reset.

- If the Picture CLIP (see Chapter 15, “Picture CLIP”) feature is required for subscribers in the remote office, it can be activated here. In this case, the required TCP Port 443 on the WAN interface is opened, though explicitly for this feature. The WBM is furthermore not accessible via the WAN interface as a result.
- If gatekeeper redundancy for HFA subscribers is required, this must likewise be configured (see Chapter 10, “Gatekeeper Redundancy for HFA/ SIP Subscriber”).

3) An SPE certificate has to be imported for the WAN interface of the OpenScape 4000 SoftGate.

OpenScape 4000 SoftGate WBM > Configuration > WAN > SPE > Import Keycert



Secure Remote Subscriber - OpenScape 4000 SoftGate SPE certificate

- The **Load a SPE Key Certificate via HTPP** screen is displayed.

Enter the decryption password and then search for the SPE certificate. Press **View Fingerprint of Certificate**. Now import the certificate with the **Import Certificate from File** button.

- The file containing the SPE certificate originates either from a customer-defined PKI certification authority (RA/CA) or (if not available to the customer) can be generated with the OpenScape 4000 Assistant. See documentation **Signaling and Payload Encryption** > Chapter 5, “Generation SPE Certificates with OpenScape 4000 Assistant”. The SPE certificate must be available in PEM or PKCS#12 format.

4) Configure SIP STMI board for SIP/UFIP SRS

WAN interface data for SIP STMI:

AMO CGWB is extended with the parameters USEWANIF

Example:

```
CHANGE-
CGWB:MTYPE=CGW,LTU=24,SLOT=4,TYPE=GLOBIF,IPADR=10.80.144.244,NETMASK=255.255.248.0,
DEFRT=10.80.144.190,USEWANIF=YES,WPUBIP=172.16.1.126,SIPTLSP=5061;
```

IPADR IP address of SIP WAN interface (eth1)

NETMASK Netmask of WAN interface

DEFRT IP address of the default router in the WAN segment

USEWANIF Enabling SIP SRS on the SIP STMI board

SIPTLSP TCP/TLS port for secure SIP communication

WPUBIP Public IP address of WAN interface

After changing these parameters,

```
RESTART-
BSSU:ADDRTYPE=PEN,LTU=<LTU_of_OpenScape4000_SoftGate>,SLOT=<SIP_STMI_slot>;
```

of the OpenScape 4000 SoftGate must be performed. The SIP STMI board is reset and the changes will be activated.

MANLANIF interface reconfiguration for SIP STMI:

AMO CGWB supports extra configuration of the management LAN interface (WBM) which is quite important in case of WAN configuration as web management access over the WAN interface is by default prohibited by

iptables rules on internal SoftGate firewall. Therefore the extra IPDA LAN IP address shall be configured for the SIP STMI board management.

Example:

```
CHANGE-
CGWB:MTYPE=CGW,LTU=24,SLOT=4,TYPE=MANLANIF,MIPADR=10.80.170.244,MNETMASK=255.255.240.0,MDEFRT
```

MIPADR IP address used for WBM management (eth0)

MNETMASK Netmask of MANLANIF

MDEFRT IP address of the default router in the IPDA/MANLANIF segment

ASC config data for SIP STMI media ports:

AMO CGWB allows to define range of SRTP media ports which are used as source/destination ports for media streams established towards SIP subscribers.

If SIP/UFIP SRS is used together with HFA SRS and they share single public IP address on the Primary DMZ firewall (AMO STMI WIPADR) then media port range configured for vHFA proxy MUST be different than port range for SIP STMI. I.e. default range 29100:30099 for vHFA and 30100:31099 for SIP STMI

Example:

```
CHANGE-CGWB:MTYPE=CGW,LTU=24,SLOT=4,TYPE=ASC,UDPPRTLO=30100,UDPPRTHI=31099;
```

UDPPRTLO Lowest UDP port used for SRTP media streams

UDPPRTHI Highest UDP port used for SRTP media streams

NOTICE: WAN interface is not configurable via SoftGate SIP STMI WBM but proper configuration can be verified in SIP STMI WBM as following:

OpenScape 4000 SoftGate SIP STMI WBM > Configuration > Basic Settings > Gateway



Figure 132: Configure SIP STMI board for SIP/UFIP SRS

SPE certificate import into SIP STMI cards:

SIP/UFIP SRS requires signaling and payload encryption (SPE) and therefore remote SIP/UFIP subscribers cannot register to the OpenScape 4000 SoftGate if SPE is not correctly configured on the SIP STMI board

dedicated for SRS. It includes but not restricts to the proper SPE certificate configuration.

OpenScape 4000 SoftGate SIP STMI WBM > Configuration > Security > Import SPE

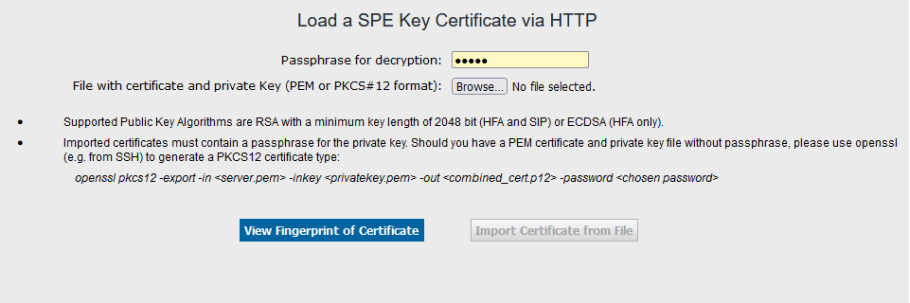


Figure 133: Configure SIP STMI board for SIP/UFIP SRS

- The Load a SPE Key Certificate via HTPP screen is displayed. Enter the decryption password and then search for the SPE certificate. Press View Fingerprint of Certificate. Now import the certificate with the Import Certificate from File button.
- The file containing the SPE certificate originates either from a customer-defined PKI certification authority (RA/CA) or (if not available to the customer) can be generated with the OpenScape 4000 Assistant. See documentation Signaling and Payload Encryption > Chapter 5, “Generation SPE Certificates with OpenScape 4000 Assistant”. The SPE certificate must be available in PEM or PKCS#12 format.
- If the HFA and SIP/UFIP SRS share the same Primary DMZ firewall with one Public IP then both certificates – one downloaded to the SoftGate (see step 2.) and this one downloaded to the SIP STMI shall be identical.

5) Generate the phone for the remote office with AMO SBCSU.

IMPORTANT: An IP password has to be configured in AMO SBCSU:

---

6) Configure the phone for the remote office via its own menu.

The following settings have to be entered in the phone's menu:

- Gateway IP address (=WAN IP address of the OpenScape 4000 SoftGate)
- Station number (AMO SBCSU)
- IP password (AMO SBCSU)
- Transport mode: TLS
- NTP server

The address of an NTP server pool (z. B. 0.de.pool.ntp.org) should be entered as the NTP address. The phone then always gets a list of active NTP servers.

Use of a server pool requires the availability of a DNS server in order to resolve the DNS name. If the phones are connected with the default routers via DHCP, the DNS is usually entered automatically and the name can be

resolved. If, however, the OpenStage phone in the remote office is assigned a static IP address, the DNS also has to be entered.

For the time change from daylight saving time to standard time, please change **Timezone offset (hours)** from 2 to 1 on the phone.

Service Menu > Admin > ok > (Password = 123456*) ok > Date and time > ok > Time source > ok > (Time source = SNTP, SNTP IP = <ip address of the NTP server pool or of the NTP server>**, Timezone offset (hours) = 1) > Save & exit > ok**

*please note that non-default password should be used.

- optional: DLS IP address

3.10.3.1 Secure Remote Subscriber on STMIX/STMIY

Additionally to the information provided under Secure Remote Subscriber for SoftGate, there are a few minor additions:

- STMIX/STMIY supports only SIP SRS (no HFA). In this case, STMIX/STMIY must have only SIP (HG3540) functionality (no MFS is allowed).
- Due to the limited number of physical interfaces, there is no possibility for an additional dedicated WAN interface. This means that USEWANIF=Y will be used only as a switch, activating additional firewall security and support for far-end (home based) NAT bypass (SIP@Home subscribers), enforcing subscriber security (CIPHER). Having no dedicated WAN interface means no extra WAN IP configuration (as opposed the SoftGate).

The following aspects must be considered when configuring a SIP secure remote subscriber on STMIX/STMIY:

- STMIX/STMIY must have only SIP (BFDAT) functionality.
- Since subscriber security is enforced (even if the rest of the system is not secure), SPE certificates are necessary.
- As for any secure subscriber, NTP is mandatory.
- Optional, configuring WPUBIP will activate support for near end NAT (DMZ scenario – described in “DMZ” chapter). In this case, if multiple gateways (vHG or STMIX/STMIY) are used for SRS feature, port forwarding using different port ranges for each gateway is required.
- USEWANIF=Y will activate support for far end NAT, respectively support for SIP SRS.
- Firewall restrictions enforced by USEWANIF result in mandatory usage of a separate management interface (MANLANIF) with its own IP address.
- Parallel connections of SIP SRS from LAN and WAN to the same gateway are not possible.

Considering the above, we have the following configuration steps:

- Standard SIP GW configuration, where GW IPADR will be the local/internal DMZ IP address.
- Enable near end NAT, by configuring the firewall public IP in WPUBIP:
  ```
  CHANGE-CGWB:MTYPE=CGW,LTU=17,SLOT=1,TYPE=GLOBIF,
   WPUBIP=1.2.3.4;
  ```
- Configuration of the management (WBM access) interface:

  ```
  CHANGE-CGWB:MTYPE=CGW, LTU=24,SLOT=4, TYPE=MANLANIF,
   MIPADR=10.80.170.244,
  ```

```
MNETMASK=255.255.240.0,MDEFRT=10.80.160.1;
```

Additional information:

- MIPADR IP address used for WBM management
- MNETMASK Netmask of MANLANIF
- MDEFRT IP address of the default router in the IPDA/MANLANIF segment

- Enable far end NAT, respectively SIP secure remote subscriber, via USEWANIF:

```
CHANGE-CGWB:MTYPE=CGW, LTU=17, SLOT=1, TYPE=GLOBIF,
 USEWANIF=YES;
```

- ASC config data for SIP STMI media ports. If SIP/UFIP SRS is used together with HFA SRS and they share a single public IP address on the Primary DMZ firewall, then the media port range configured for vHFA proxy MUST be different than the port range for SIP STMI. I.e. default range 29100:30099 for vHFA and 30100:31099 for SIP. Moreover, if multiple SIP gateways share the same public IP in the DMZ firewall, each one can be accessed/ distinguished only by having unique SIP signaling ports (i.e 5061, 5062) and of course proper forwarding rules in the DMZ firewall.

```
CHANGE-CGWB:MTYPE=CGW, LTU=24, SLOT=4, TYPE=ASC,
 UDPPRTLO=30100, UDPPRTHI=31099;
CHANGE-CGWB:MTYPE=CGW, LTU=17, SLOT=1, TYPE=GLOBIF,
 SIPTCPP=5065, SIPTLSP=5066;
```

Additional information:

- UDPPRTLO Lowest UDP port used for SRTP media streams
- UDPPRTHI Highest UDP port used for SRTP media streams

- Import SPE certificates.
- Generate the secure subscriber via SBCSU.

An IP password (IPPASSW) is mandatory.

NOTICE: The same configuration steps are applied for the SoftGate and are described in detail in the previous chapter, except for the WAN interface configuration.

3.10.3.2 Deployment Service (DLS) and DLS Contact-Me Proxy (DCMP) - Tips & Tricks

3.10.3.2.1 Background

Under normal circumstances, the Deployment Service (DLS) contacts the IP terminals via their IP address when a job has been created. In our remote office case, however, the IP terminals are located in the Internet, as it were behind a NAT router with a local IP address, which means that the DLS cannot reach them. The DLS and IP terminals support a proprietary solution in this case, which allows administration of IP terminals behind a NAT router. This solution is called DLS Contact-Me Proxy (DCMP). Communication is always opened by the IP terminal in this solution.

3.10.3.2.2 How it Works

The IP terminals poll the DCMP in a defined polling interval in this case and use the device ID to check whether the DCMP has a job active for the DLS for the respective IP terminal. If this is the case, the IP terminal contacts the DLS

in order to execute the job in question. Once completed, the DLS deletes the Contact-Me entry in the DCMP again.

3.10.3.2.3 Requirements

IP requirement:

In order for the IP terminals to access the DLS and DCMP, both must be accessible for the IP terminals via a public IP address. In other words from the Internet in the case of the remote office scenario.

Hardware requirement:

The DLS server requires two network cards for this solution. One network card sets up the connection to the corporate/enterprise network and the second is intended for the connection to the IP terminals in the Internet/NAT router.

3.10.3.2.4 Information on Configuration

The examples/information below refer to the DLS configuration from the DMZ scenario example (Figure 133) in Section 14.2.4, “DMZ”.

- The two network cards have to be configured first under Windows.

C:\Documents and Settings\dls-dmz>ipconfig

Windows IP Configuration

Ethernet adapter DMZ WAN:

Connection-specific DNS Suffix . :

IP Address. . . . . : 220.20.20.100

Subnet Mask . . . . . : 255.255.255.248

Default Gateway . . . . . : 220.20.20.97

Ethernet adapter DMZ LAN:

Connection-specific DNS Suffix . :

IP Address. . . . . : 10.10.99.150

Subnet Mask . . . . . : 255.255.255.0

Default Gateway . . . . . :

- The default gateway was configured for the DMZ-WAN interface. A permanent static route therefore has to be configured for the DMZ-LAN in order to access the corporate/enterprise network.

C:\Documents and Settings\dls-dmz>route ADD -p 10.10.0.0 MASK 255.255.0.0 10.10.99.254

C:\Documents and Settings\dls-dmz>route print

```
===========================================================
Interface List
0x1 ........................... MS TCP Loopback interface
0x2 ...00 1b 21 15 3d 7b ...... Intel(R) PRO/1000 MT Server Adapter - Packet
Scheduler Miniport
0x3 ...00 19 99 19 95 09 ...... Broadcom NetXtreme Gigabit Ethernet - Packet
Scheduler Miniport
===========================================================
===========================================================
Active Routes:
```

```
Network Destination        Netmask          Gateway       Interface  Metric
          0.0.0.0          0.0.0.0     220.20.20.97   220.20.20.100       20
        127.0.0.0        255.0.0.0        127.0.0.1       127.0.0.1       1
        10.10.0.0      255.255.0.0     10.10.99.254    10.10.99.150       1
       10.10.99.0    255.255.255.0     10.10.99.150    10.10.99.150       20
    10.10.99.150  255.255.255.255       127.0.0.1       127.0.0.1       20
    10.10.255.255  255.255.255.255     10.10.99.150    10.10.99.150       20
     220.20.20.96  255.255.255.248    220.20.20.100   220.20.20.100       20
   220.20.20.100  255.255.255.255       127.0.0.1       127.0.0.1       20
   220.20.20.255  255.255.255.255    220.20.20.100   220.20.20.100       20
        224.0.0.0        240.0.0.0     10.10.99.150    10.10.99.150       20
        224.0.0.0        240.0.0.0    220.20.20.100   220.20.20.100       20
  255.255.255.255  255.255.255.255     10.10.99.150    10.10.99.150       1
  255.255.255.255  255.255.255.255    220.20.20.100   220.20.20.100       1
Default Gateway:    220.20.20.97
                    ===========================================================

Persistent Routes:
  Network Address          Netmask  Gateway Address  Metric
        10.10.0.0      255.255.0.0     10.10.99.254       1
```

- Install the DLS on the Windows machine with DCMP (in this example, the DCMP is installed on the same machine). If the DLS has already been installed without the DCMP, it can be installed later. Detailed service documentation can be found in the administrator documentation for **OpenScape Deployment Service V8 > Installation and Initial Configuration > Set Up DCMP**.
- To configure the DCMP, navigate to **http://<ip address>:18080/dcmp** using a web browser. The user name is "admin." If the DCMP was installed together with the DLS, the password is the same as the admin password for the DLS.
- Please check and configure the **Local Host** field under Cluster Setup. This contains the IP address of the DCMP server. This example simply considers a standalone DLS without DLS cluster. Refer to the administrator documentation for **OpenScape Deployment Service V8** for additional information.

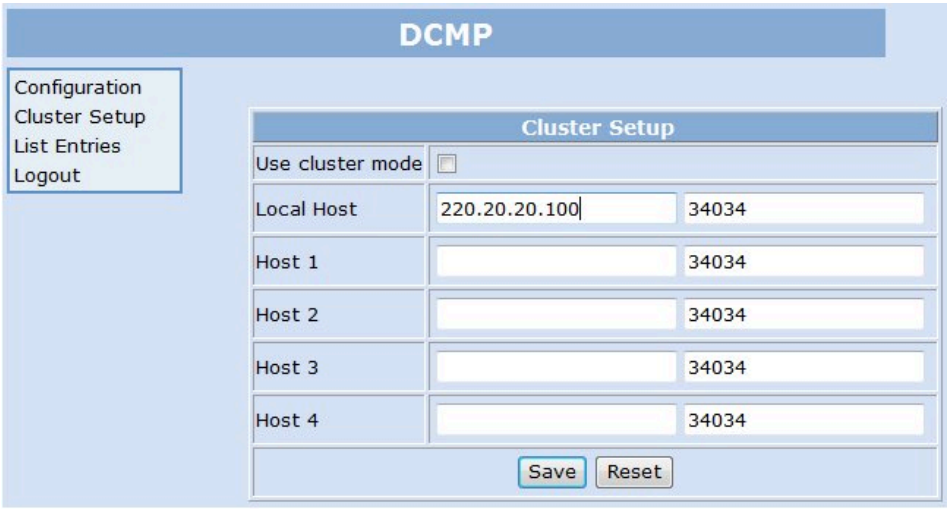


Figure 134: DCMP configuration for Secure Remote Subscriber

- The next step involves configuring the DLS for the DCMP.

Click the **Toggle DCMP** button under **Administration > Workpoint Interface Configuration > DCMP** tab in order to activate the DCMP.

If the DCMP is running on the DLS computer, the IP address of the DCMP server will be displayed in the **DLS-DCMP Host** field (or localhost), otherwise it must be entered here.

To test the communication between the DLS and DCMP, click the **Test** button.

The IP address to be contacted by the IP terminals must be entered in the **Device-DCMP Host** field (thus the IP address which is to be accessible from externally).

Define one or more **Device IP Ranges**. Each IP terminal within the IP range defined by **IP Address from** and **IP Address to** is updated via the DCMP. The DSL therefore always sends a message to the DCMP with a request to set the Contact-Me entry for this phone whenever a change is made to a phone within one of the listed IP ranges. In our example, the problem is that it is not always clear from which Internet Service Provider the respective IP terminal receives its IP address range. We have therefore entered the entire IP address range, with the exception of the corporate/enterprise network. If accurate IP address ranges must be known, only those needed can of course be entered. For example, IP terminals only register from a single ISP for which the IP address range is known.

A **Poll Interval** must also be assigned to the respective IP address range. This is the time in minutes after which the IP terminal polls the DCMP. A very short polling interval (e.g. 1 minute) can be selected for test purposes. Longer intervals are recommended in live mode.

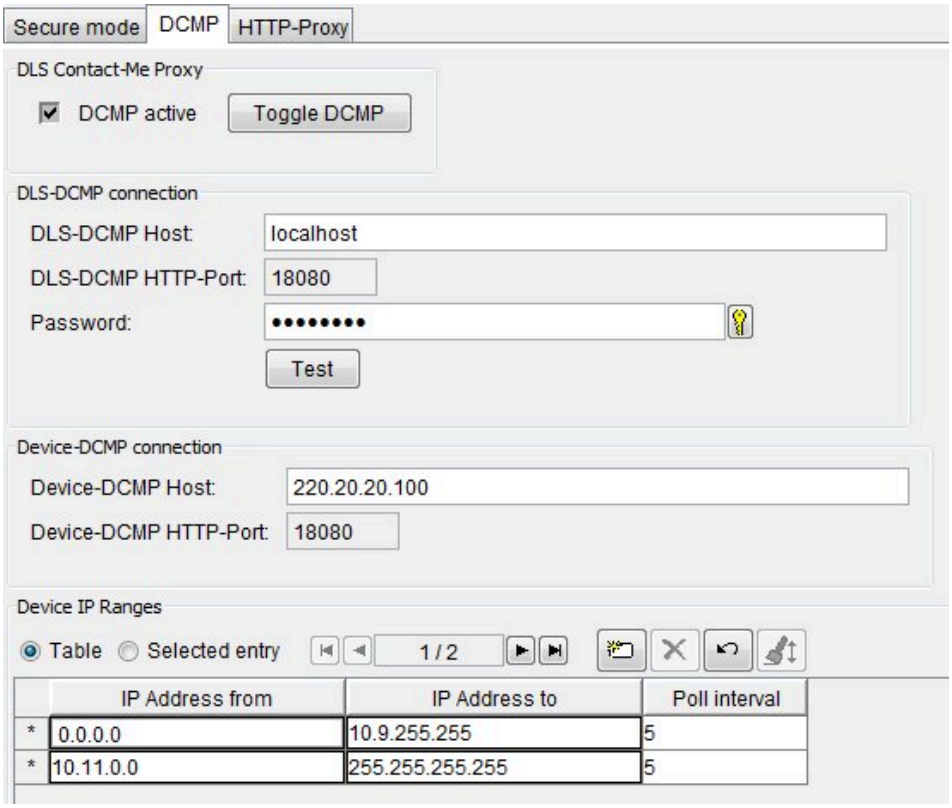
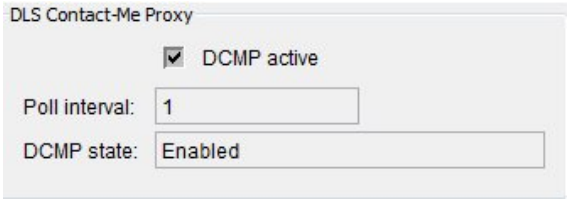


Figure 135: Configuring the DLS for the DCMP

- The DLS/DCMP configuration can now be tested with an IP terminal in the remote office.
- After entering the DLS/DCMP IP address (in the example 220.20.20.100) at a terminal in the remote office, the IP terminal registers with the DLS. Because the IP of the IP terminal is from an IP address range (public Internet IP address of the remote office NAT router) that was previously entered under the DCMP configuration, the IP terminal is informed that this is a DCMP terminal.

  Go to the **IP Devices > IP Device Management > IP Device Configuration > DCMP** tab. The checkbox **DCMP active** should be activated.



  Testing the DLS/DCMP configuration with an IP terminal in the remote office

  To test the function, go to **IP Devices > IP Phone Configuration > Gateway / Server** of the previously newly registered IP terminal and start reading the configuration. A job is thus generated. To see the job, go to **Job Coordination > Job Control**.

  Click the **List Entries** menu on the DCMP user interface. You should see the Contact-Me job in the list. The **Device ID** should be the MAC address of the phone.

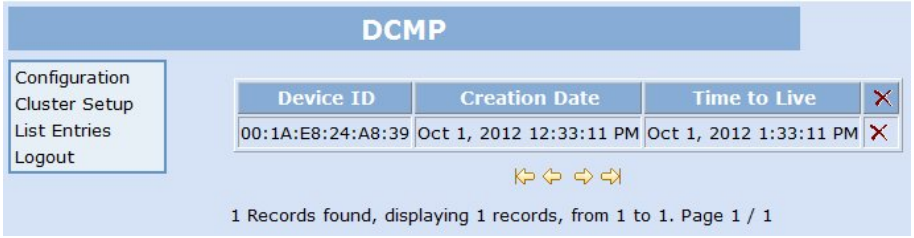


Figure 136: DCMP - List Entries menu before the IP terminal has fetched the Contact-Me job from the DCMP

The job should then be concluded once the IP terminal has fetched the job from the DCMP. The job likewise disappears from the DCMP **List Entries** menu when it has been fetched.

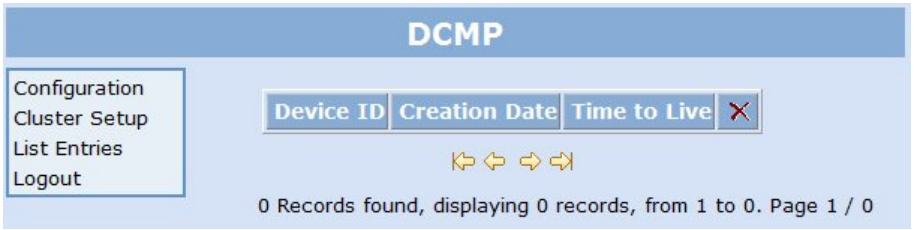


Figure 137: DCMP - List Entries menu after the IP terminal has fetched the Contact-Me job from the DCMP

NOTICE: If the job is not executed/fetched, a Wireshark trace on the DLS and/or DCMP side may assist in diagnosing the fault. With the Wireshark trace, incoming packets must

be received on the default port 18080 from the IP terminal (IP address of the remote office NAT router). This is the polling of the DCMP by the IP terminal. Communication from the IP terminal to the DLS must then take place on the default port 18443 for executing the job.

- Another DLS setting that makes sense in our example is the default job execution type under **Job Coordination > Job Configuration**. The **Immediately** (Execute immediately) option is set here by default. In the case of Secure Remote Subscribers it might well be that users disable their IP terminals in the remote office or disconnect them from the mains. The jobs would therefore not be executed after a certain time and would expire with "Timed out". It is recommended in this case to switch to **Immediately or after registration**.

3.11 Picture CLIP

3.11.1 Feature Description

The feature “Picture CLIP” provides the option of showing centrally stored contact data (name and picture) of the remote telephone party on an IP phone’s display.

In order to display centrally stored contact data, the OpenStage phones request the data from a OpenScape 4000 SoftGate, which then forwards the request to a central directory server, retrieves the data and makes it available to the OpenStage phones.

The display format (positioning, style, size etc.) of the contact data remains the same as for local phonebook lookup, since the same mechanisms are used.

The directory server is queried for all numbers. If an entry for the number is found on the LDAP directory server, the name and picture from the directory server are displayed. If there is no entry for the number in the directory server, the name from the local phonebook is displayed.

NOTICE: In the case of an outgoing call from the phone, the picture for the called contact is not shown, because the call icon (e.g. free, busy, forwarding symbol, etc.) must be displayed in this case.

Two different modes for picture retrieval are currently supported:

Direct picture retrieval:

Preconditions:

- Direct picture retrieval configured.
- Contact data with picture stored on LDAP server.

=> The user sees the name and picture of the remote party as stored in the LDAP directory.

The OpenStage phone performs a lookup on the OpenScape 4000 SoftGate. The OpenScape 4000 SoftGate forwards the request to the LDAP server

and receives the name and picture of the requested phone number in return. The name and picture are then forwarded together by the OpenScape 4000 SoftGate to the OpenStage phone and shown on the display.

Indirect picture retrieval:

Preconditions:

- Indirect picture retrieval configured.
- Contact data stored on LDAP server with valid reference to a picture stored on another web server.

=> The user sees the name of the remote party as stored in the LDAP directory and the picture as stored on the web server.

The OpenStage phone performs a lookup on the OpenScape 4000 SoftGate. The OpenScape 4000 SoftGate forwards the request to the LDAP server and receives the name and an URL of the web server with the relevant photo ID where the picture is stored. In the next step, the OpenScape 4000 SoftGate receives the picture on the basis of the previously received URL and photo ID. The name and picture are then forwarded together by the OpenScape 4000 SoftGate to the OpenStage phone and shown on the display.

3.11.2 Service Information

- This feature is supported for OpenScape 4000 SoftGate and OpenScape Access/Branch 500.
- If no picture is available, only the name and number from the LDAP directory entry are displayed.
- If the LDAP directory server is not available, the PBX name is displayed after a timeout.
- Only OpenStage 60/80 HFA support this feature.
- The OpenStage phones have to be able to access the OpenScape 4000 SoftGate or OpenScape Access/Branch 500, which is configured for Picture CLIP. The OpenStage phones therefore do not necessarily have to be configured on the respective OpenScape 4000 SoftGate or OpenScape Access/Branch 500.
- The OpenStage phones only accept pictures encoded in jpg and of max. 50k in size.
- An LDAP directory server is required for central storage of the contact data and pictures. A web server is needed additionally for indirect picture retrieval.
- The contact data is stored on the LDAP directory server using the keys that were configured on the OpenScape 4000 SoftGate via WBM.
- It is recommended that the telephone numbers are stored in a fully qualified format including country code and area code (e.g. 4989700754321). If the numbers are stored using separators such as brackets, dashes or plus signs (e.g. +49 (89) 7007-54321), then the LDAP directory server has to apply conversion rules when checking for a match. The OpenStage phone issues an LDAP query using plain digits without separators.
- The contact data from the LDAP directory server is only shown in some cases after a short delay, because a secure connection has to be established to the OpenScape 4000 SoftGate via https. During this time, the display entry provided by the OpenScape 4000 system may become visible briefly. In indirect retrieval mode, a further request/response cycle is needed to retrieve the picture.

3.11.3 Generation (Example)

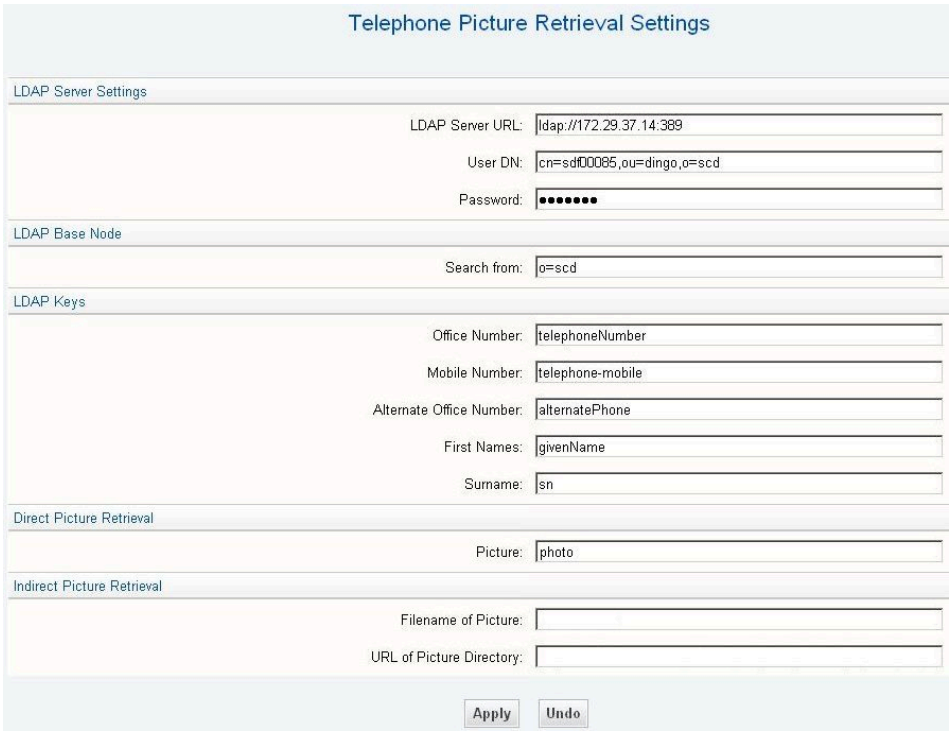
3.11.3.1 OpenScape 4000 SoftGate configuration

The OpenScape 4000 SoftGate configuration provides the information needed to access the LDAP directory server. It must be possible to access the LDAP directory server from the OpenScape 4000 SoftGate via IP.

The configuration of the OpenScape 4000 SoftGate is performed via WBM.

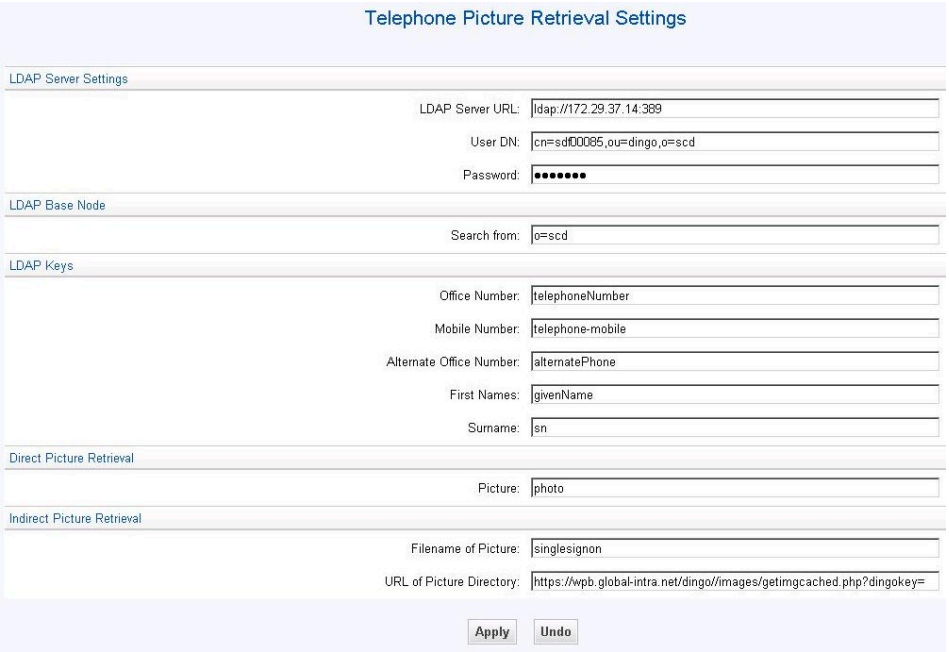
Configuration > Picture CLIP

- Direct picture retrieval:



Direct picture retrieval configuration in OpenScape 4000 SoftGate

- Indirect picture retrieval:



Indirect picture retrieval configuration in OpenScape 4000 SoftGate

---

IMPORTANT: The configured entries in the **Picture CLIP Settings** must correspond to the entries on the LDAP directory server.

The fields **Picture** (for direct picture retrieval) and **Filename of Picture** (for indirect picture retrieval) contain the matching keys on the LDAP directory server for the picture that is to be displayed.

For more information on the LDAP configuration, please refer to LDAP directory server configuration.

NOTICE: LDAPS can be used by changing URL to ldaps. The corresponding port and ldap configuration must of course support the feature. LDAPS with introduced starting with TLS1.2 support.

3.11.3.2 Phone Configuration

The phone configuration provides information needed in order to access the OpenScape 4000 SoftGate as well as information about the mode of operation.

The configuration can either be performed via the local phone menu, the Web interface (WBM) or via the OpenScape Deployment Service (DLS).

Configuration via the phone menu

Admin > Applications >XML applications > Add application

This is basically the data for connectivity to the server hosting the feature (usually OpenScape 4000 SoftGate) and the mode of operation.

- **Display name**:

- Name of the application displayed on the application tab of the phone's display. Enter **ldap**.
- **Application name**:
- Used internally to identify the XML application running on the phone. Enter **ldap**.
- **Server address**:
- The IP address of the OpenScape 4000 SoftGate (e.g. 172.29.136.224).
- **Server port**:
- The number of the http port used by the server to provide the XML documents for the application. Varies according to the protocol configured, but OpenScape 4000 SoftGate only allows **443**.
- **Protocol**:
- The protocol used for communication with the server. Choose **https**, because OpenScape 4000 SoftGate only allows **https**.
- **Program name**:
- Enter **ldap**.
- **Use proxy**:
- Must be set to **No**.

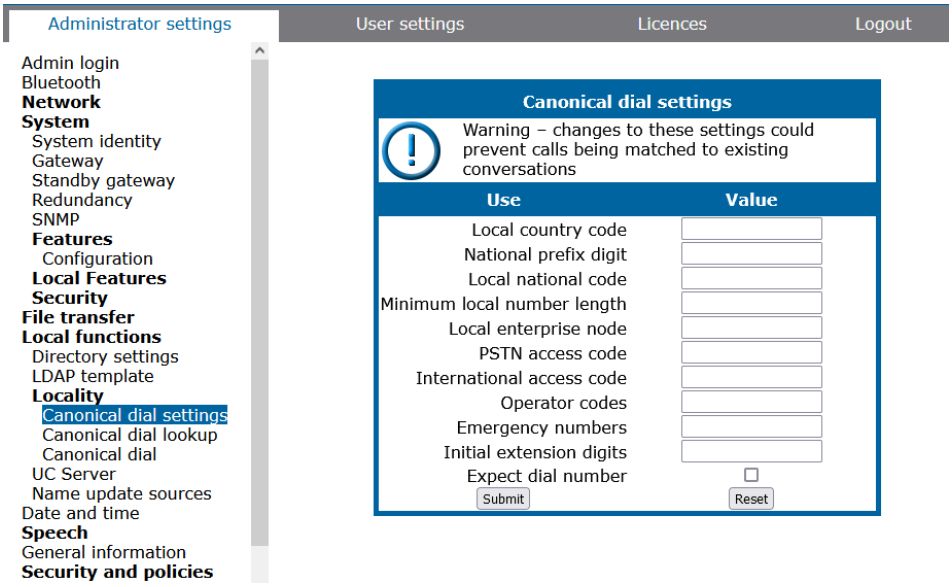
NOTICE: None of the other configuration items is currently evaluated for the feature.

IMPORTANT: If the feature is to be **deactivated**, the LDAP settings should be deleted.

Phone canonical settings

For retrieval of contact data from the LDAP directory server, the remote telephone number is converted according to the canonical dial settings (**Admin > Local functions > Locality > Canonical settings**) when a call arrives. The format of the resulting number should match the format the numbers are stored under on the LDAP directory server. It is recommended to convert the numbers to fully qualified format, i.e. adding country and area code to the subscriber number. This ensures that the number used for lookup is unique.

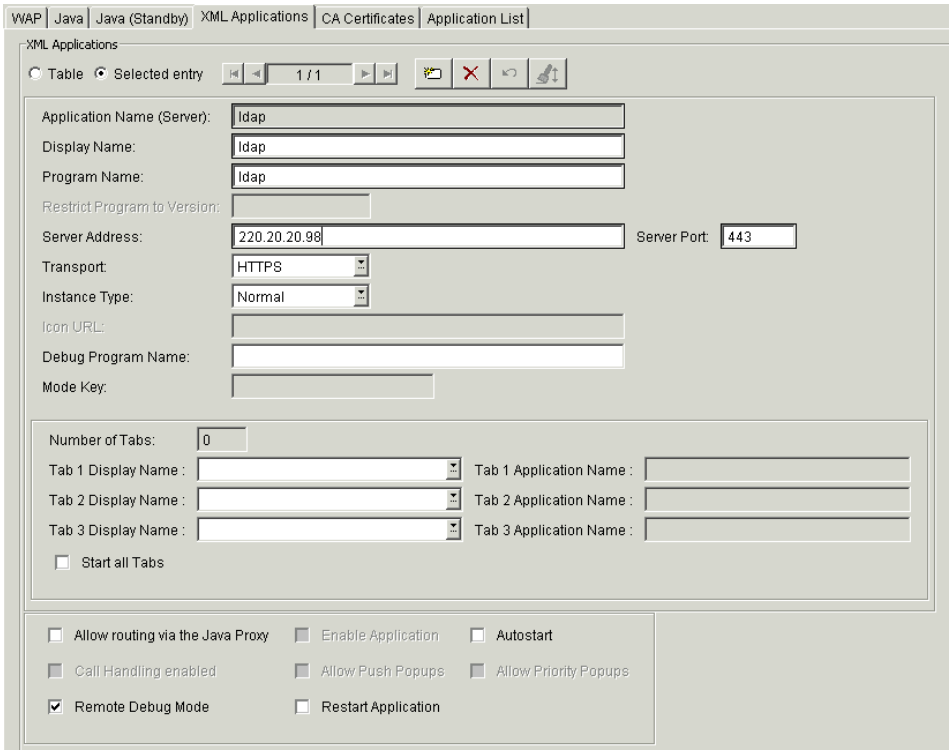
Example:



Canonical dial settings for picture retrieval

Phone configuration via OpenScape Deployment Service

IP Devices > IP Phone Configuration > Application



Picture retrieval configuration via DLS

Tab **XML Applications**:

- **Name of the Application**:
- Enter **ldap**.
- **Display Name**:
- Enter **ldap**.
- **Program-Name**:

- Enter **ldap**.
- **Server Address**:
- Enter the IP address of the OpenScape 4000 SoftGate.
- **Server Port**:
- Enter the server port of the OpenScape 4000 SoftGate.
- **Transport**:
- Select **http** or **https**. OpenScape 4000 SoftGate only supports **https**.

NOTICE: The subsequent entry GUI entry created in the phone menu under Applications is only a "dummy" entry to allow the feature to work. Navigating to it from the phone menu will result **"Unable to parse information from the server"**.

3.11.3.3 LDAP directory server configuration

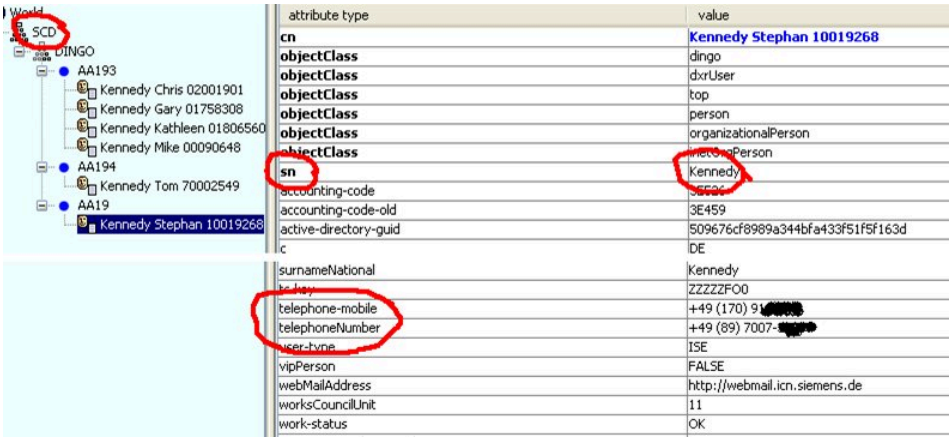
The LDAP directory server must offer an LDAP V2 or V3 interface and provide access using password-based, so-called "simple" security.

The contact data is stored on the LDAP directory server using the keys that were configured on the OpenScape 4000 SoftGate via WBM.

It is recommended that the telephone numbers are stored in a fully qualified format including country code and area code (e.g. 4989700754321). If the numbers are stored using separators such as brackets, dashes or plus signs (e.g. +49 (89) 7007-54321), then the LDAP directory server has to apply conversion rules when checking for a match. The OpenStage phone issues an LDAP query using plain digits without separators.

Example of an LDAP structure:

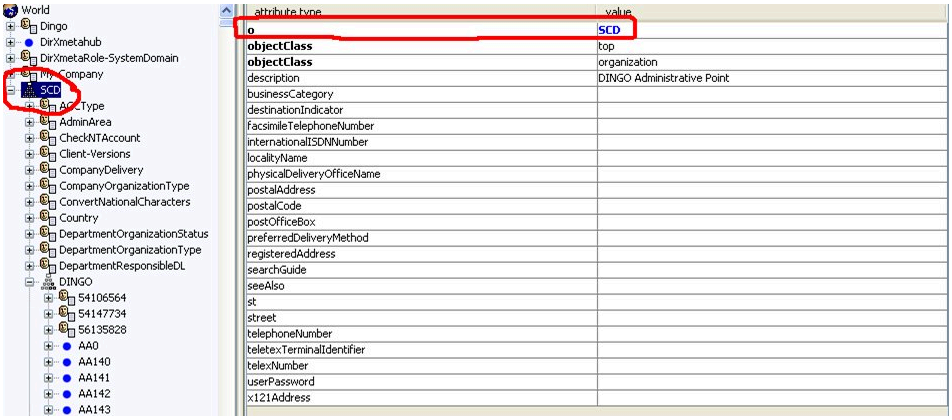
The entries in the **attribute type** column marked red must be provided to the OpenScape 4000 SoftGate via the WBM configuration (see OpenScape 4000 SoftGate configuration).



LDAP server - OpenScape 4000 SoftGate data

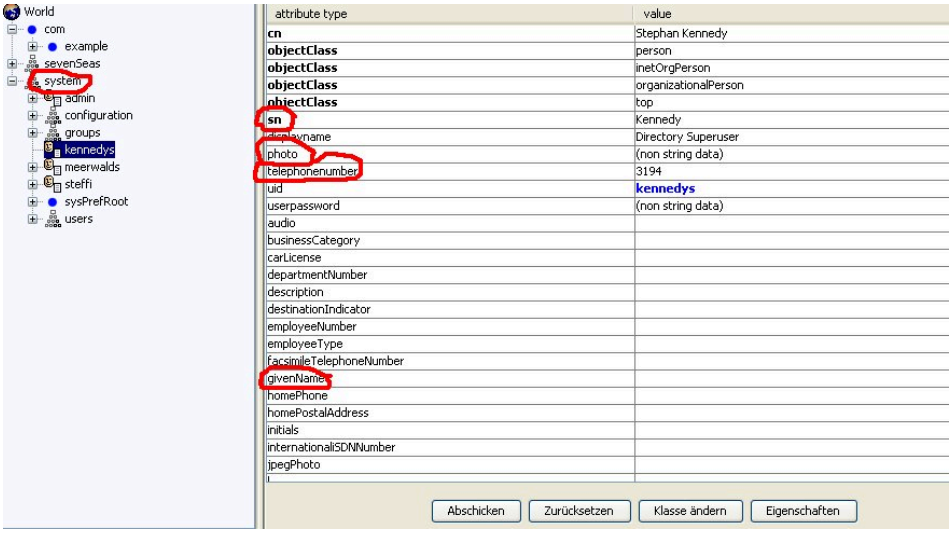
The screenshot below looks at the nodes where the telephone contact data is found.

The base node for searching is selected with o=scd.



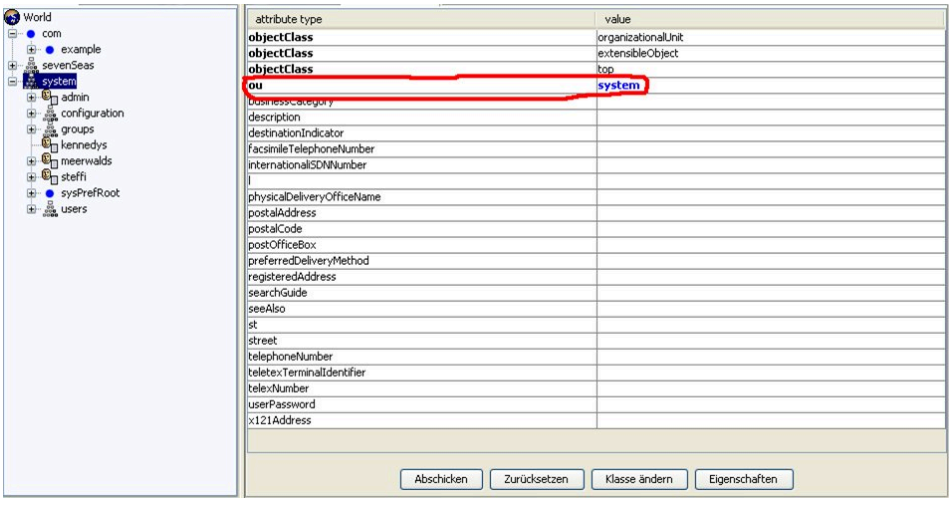
LDAP server - Telephone contact data

Another example using a different LDAP directory server in direct mode:



LDAP server - Example of direct picture retrieval (01)

As can be seen, the node structure in this server is very simple. The base node is selected with ou=system.



LDAP server - Example of direct picture retrieval (02)

3.11.3.4 Testing LDAP access

It is possible to use the OpenScape 4000 SoftGate WBM to verify whether LDAP server access is properly configured.

To do this, select the **Picture Clip > Test** function is the **Configuration** menu.

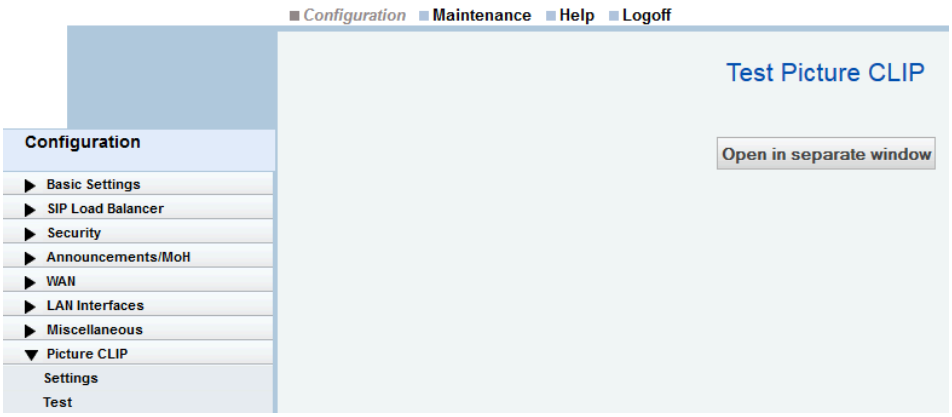
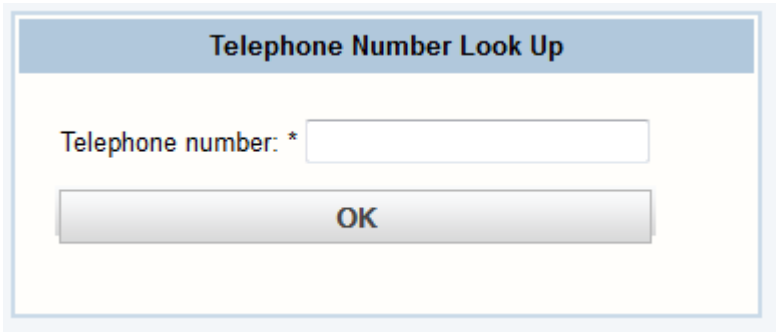


Figure 138: Launching the LDAP server access test

Now click the **Open in separate window** button.



Searching for phone numbers using the LDAP server

Enter a phone number and click **Ok**.

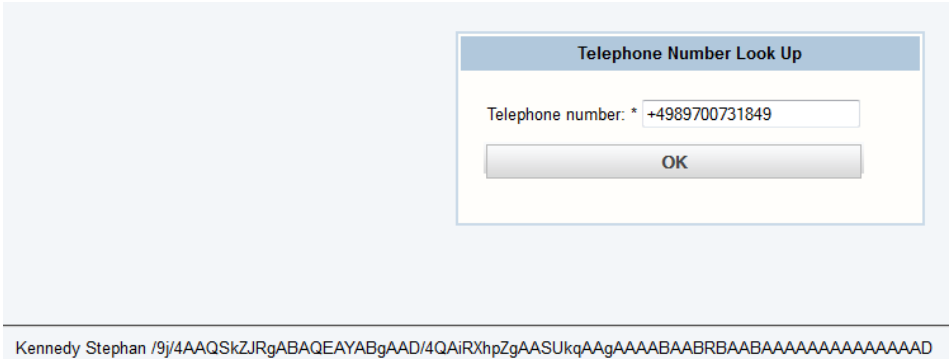


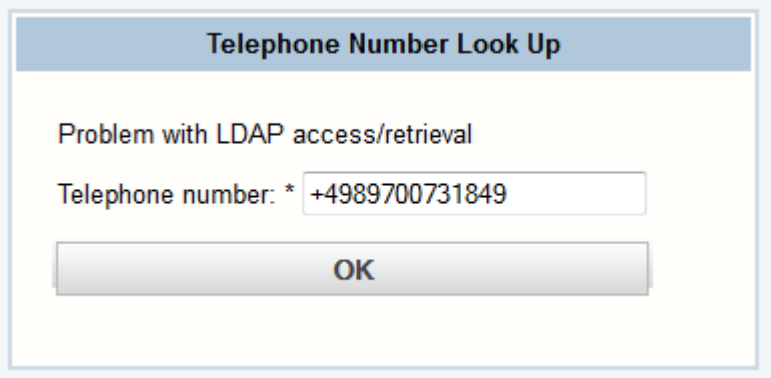
Figure 139: Correctly configured LDAP

If LDAP server access has been correctly configured and if an entry exists for the phone number in the LDAP directory, a "result" is displayed at the lower margin.

The last and first name can be identified. The subsequent characters indicate that a picture is also available.

If LDAP server access is not configured correctly, a unique error message is issued.

Example:



Incorrectly configured LDAP

It can therefore be verified that the parameters are correct as soon as the LDAP server configuration has been performed.

3.12 MFC-R2

3.12.1 Feature Description

MFC/R2 is a telephony signaling protocol which is used to provide signaling between switches. Signaling can be done over analog (TMxxx) or digital (DIUx) trunks with CAS (channel associated signaling).

MFC-R2 signals are provided from vSIUX2. SIUX functionality has been introduced as virtual board for OpenScape 4000 SoftGate/OpenScape Access/ Branch 500.

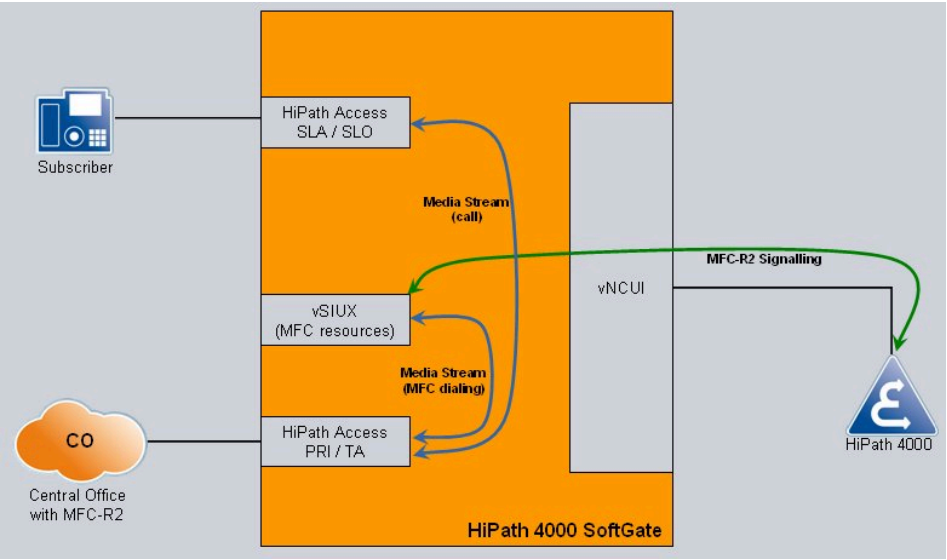


Figure 140: MFC-R2

For more details about MFC-R2, please refer to the service documentation:

1) OpenScape 4000, Section 3 - Feature Usage Examples > Networking > MFC-R2 Signaling

3.12.2 Service Information

MFC-R2 is supported with OpenScape 4000 SoftGate/OpenScape Access/ Branch.

3.12.3 Generation (Example)

The digital MFC-R2 line signaling version described by ITU-T Q.400-Q490 can be configured in OpenScape Access/Branch with the OpenScape Access PRI module.

The DIUT board must be configured in E1/CAS functionality (FCTID=2), for example

ADD-BCSU:**MTYPE=DIU**,LTG=1,LTU=19,SLOT=3,**PARTNO="Q2335-X"**,LWVAR=0,**FCTID=2**,HWYBDL=A,ALARMNO=0,MACADDR=00-1A-E8-32-60-5E,TDMLAW=0;

Additionally, a vSIUX2 must be configured. Configuration of vSIUX2 is the same as for standard SIUX2 boards. MFC-R2 functionality is selected by configuring the Q2341-X function ID3. Within the ID3 function, vSIUX only provides a MFC subset of R2, i.e. MFC-R2 forward and backward functionality (other MFC variants such as R1, SOCOTEL or MFP are not supported).

Depending on the configuration, you can set up a maximum of 8 MFC-R2 signal receivers and MFC signal transmitters on this. These always operate in pairs and the configuration is also always in pairs, for example

ADD-BCSU:MTYPE=SIUP,LTG=1,LTU=19,SLOT=5,**PARTNO="Q2341-X"**, MFCTYPE=R2B&R2B&R2F&R2F&R2F&R2F&R2F&R2F,LWVAR=0,**FCTID=3**;

is the configuration for 2 backward signal transmitters (which includes 2 forward receivers) and 6 forward transmitters (which includes 6 backward receivers).

Other SIUX functionality (e.g. DTMF, ANI,
) is not implemented in vSIUX2. If it is configured by AMO, the board remains unavailable.

IMPORTANT: Initialization can be performed in an active system but will only be activated when the shelf has been reloaded (AMO USSU). There is no indication from AMO BCSU that a restart has to be performed.

Initialization of MFC signals

A default initialization of MFC signals (frequency and attenuation) is performed in vSIUX2 code. The frequency of all signals is defined according to Q.441 of ITU-T Q.400-Q490, attenuation is set to -8dBm0.

It is possible for national applications to provide special signal definitions by means of special initialization files. By default there are three different files on the system's hard disk.

- APSP/LTG/LG25/PZJSMFD0 is the initialization file for default signals, A-law
- APSP/LTG/LG25/PZJSMFD1 is the initialization file for default signals, µ-law
- APSP/LTG/LG25/PZJSMFD2 is the initialization file for signals for Brazil (A-law, -13dmB0)

The initialization file can be selected by AMO ZAND, for example

1) `CHANGE-ZAND:TYPE=SIUXPER,LEVMFC=2;` for Brazil

Initialization file 0 is selected by default. In addition to the signal description, the file also indicates which HWY/TSL is to be used for which line on SIUX.

3.13 OpenScape Cordless E Integration

The OpenScape 4000 SoftGate supports DECT Cordless Multicell Integration (CMI) functionality. This means that besides HFA and SIP subscribers, DECT cordless subscribers can also be configured in a OpenScape 4000 SoftGate.

OpenScape Cordless Enterprise V7 - 3.9.3 Clock chain Synchronization. These informations are available in WBM (OpenScape 4000 V8, vHG 3575 for OpenScape 4000 SoftGate document - section 4.8.1.2 Peripheral Boards, 4.8.1.4 OpenScape Access Clocking).

3.13.1 Feature Description

In order to use the "OpenScape Cordless E Integration" feature, a software-based "virtual Subscriber Line Cordless" (**vSLC**) connector unit must be configured in the OpenScape 4000 SoftGate. As with the SLC24 line cards, the vSLC provides the option of generating up to 127 cordless handsets. The vSLC operates as a virtual home SLC for all administered subscribers. The visit SLCs together with the DECT base stations form the location areas at the site.

The number of CMI subscribers in the OpenScape 4000 SoftGate can be increased by adding on other vSLC applications. Up to six vSLC applications

with a maximum of 650 handsets (0.15 ERL per handset) can be configured in a OpenScape 4000 SoftGate.

NOTICE: Base stations cannot be connected to the vSLC at present.

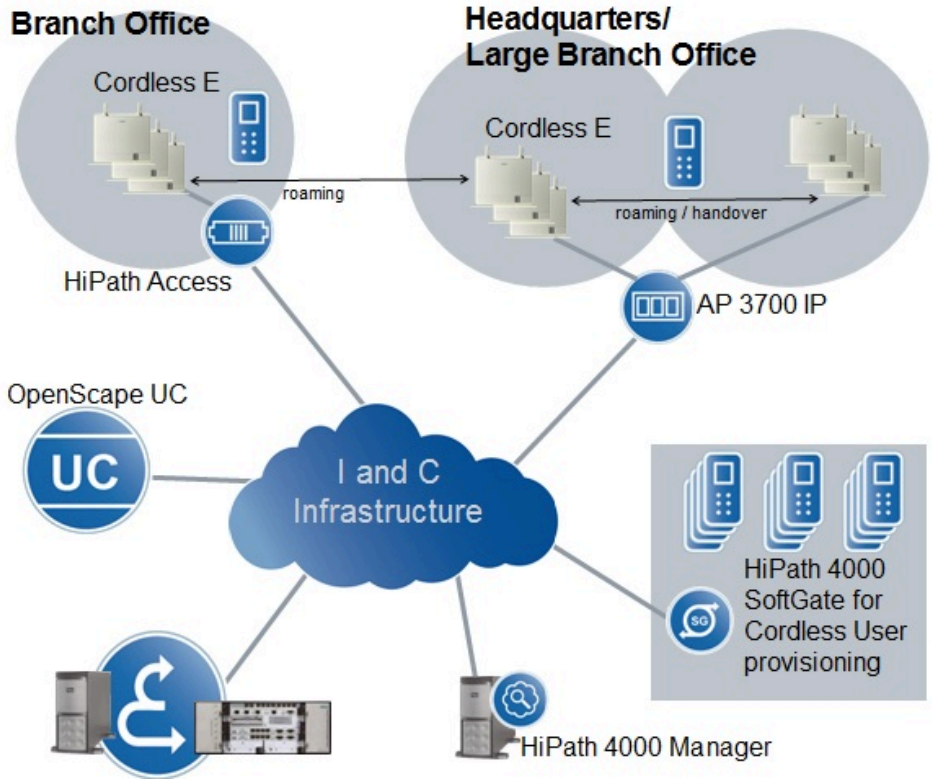


Figure 141: OpenScape Cordless E integration

If subscribers are not in the location area of their home SLC (always applies with vSLC), a data exchange must be performed between the home and visit SLC in order to fulfill the mobility concept. A prolonging connection is set up for this purpose.

Registering CMI subscribers

In the current OpenScape 4000 cordless systems, subscribers can only be registered in the location area of their home CMI node. CMI subscribers can be relocated following registration to another SLC within the CMI network with the "Relocation" feature.

Until a base station with an IP interface is available, registration of CMI subscribers for the vSLC must take place in another CMI node with a real base station. Following successful registration, the subscriber must then be relocated via the OpenScape 4000 Manager/Assistant to the new virtual CMI node.

Special characteristics in connection with OpenScape Access/Branch

If a OpenScape Access SLC module is connected to a OpenScape 4000 SoftGate with vSLC, then the Access SLC module should only be operated with visit functionality.

If OpenScape Access SLC modules are connected to a OpenScape 4000 SoftGate with vSLC, then the SLC modules operate with visit functionality only. The vSLC in the OpenScape 4000 SoftGate handles administration of all registered CMI subscribers.

This results in the following benefits:

- Fewer IP-based prolonging connections
- Fewer B channels are needed
- Reduced conversion delay between OpenScape 4000 SoftGate and the SLC module

Special characteristics in connection with OpenScape 4000 SoftGate and VMware

If a OpenScape 4000 SoftGate is operated in a VMware environment, the customer has the option to operate his entire Cordless E V7 redundantly.

All cordless subscribers have to be configured on virtual SLCs in the OpenScape 4000 SoftGate for this purpose. An additional base station is also installed at every base station location within a radius of approx. 1 - 2m. This additional base station is connected to a different SLC, which in turn must be connected to a different shelf (or also OpenScape 4000 system). The second base station is operated with reduced transmission power in order to avoid excessive alternation between base stations.

IMPORTANT: A project-specific release is absolutely mandatory for the redundancy scenario described.

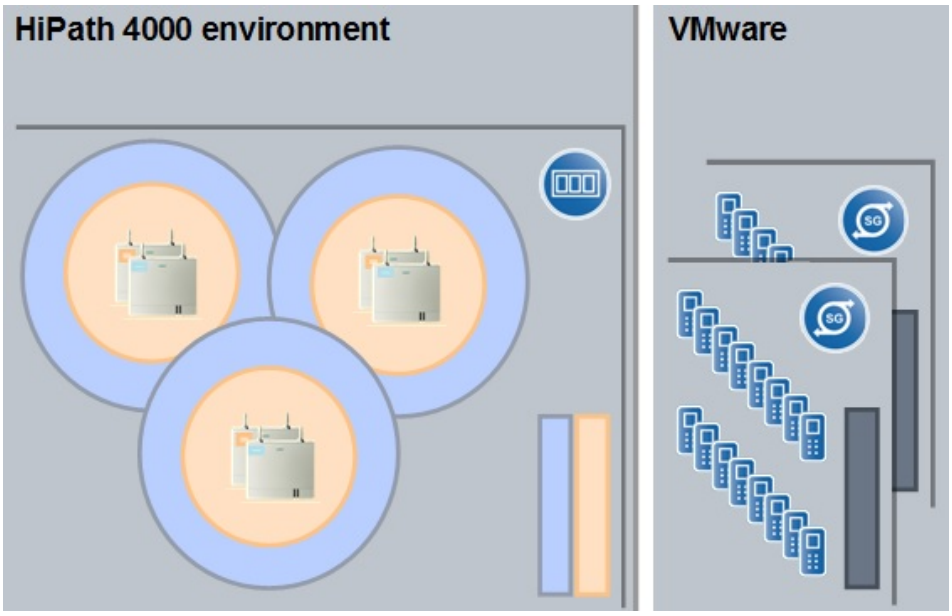


Figure 142: Cordless E redundancy scenario

This results in the following benefits:

- SLC / shelf failure does not mean subscriber failure
- OpenScape 4000 SoftGate redundancy via VMware
- Handsets maintain the same numbers and features despite any incidents

3.13.2 Service Information

- The vSLC application runs in a pure software environment, thus it supports IP-based network connectivity only. It cannot directly control the currently used DECT base stations with Up0 interface.
- As long as no "IP base station" is available/supported for the CMI feature, the mobility functionality has to be split into a virtual home functionality (vSLC application running in OpenScape 4000 SoftGate) and a real visit functionality (SLC24 and SLMC line cards with Up0 interface and real base stations). Every vSLC subscriber will thus use prolonging connections to reach the DECT base stations through real visit SLC cards. This means that at least one SLC24 line card with a base station connected is needed to establish calls.
- All DECT subscribers can be configured on a OpenScape 4000 SoftGate on vSLCs (home nodes).
- OpenScape 4000 SoftGate does not offer support for QDCL. It will be supported in V8 R2 version.
- You will find additional information on OpenScape Cordless E
  - on the TI-Online homepage

    https://ti-online.global-intra.net/index.html
  - in the service documentation in E-Doku or Partner Portal.

3.13.3 Generation (Example)

The vSLC is configured using CATool V7 on the "Boards and Base Stations" tab.

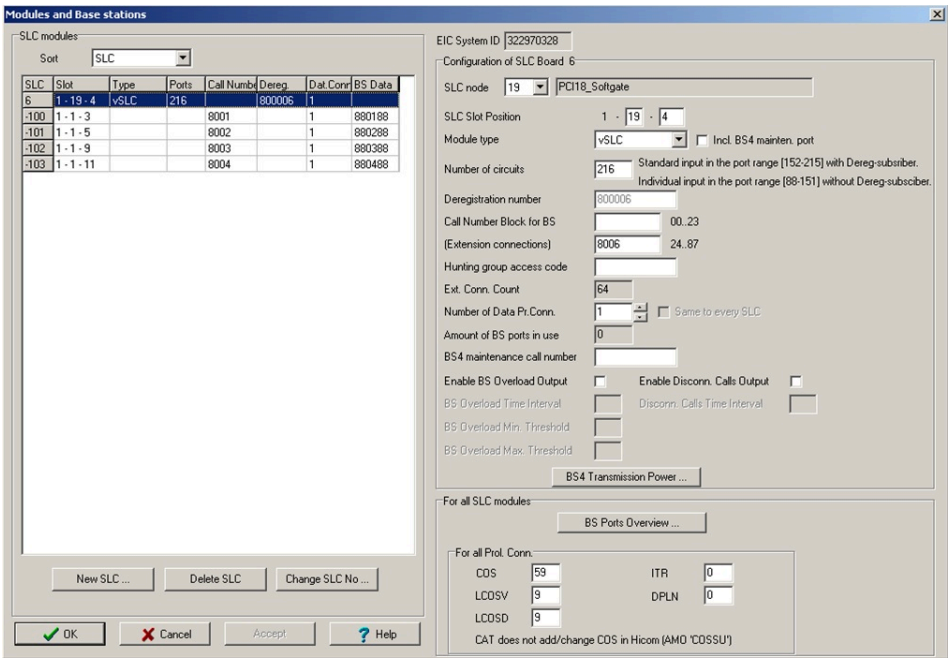


Figure 143: Configuring vSLC using CATool

Caution:

CMI subscribers can only be registered on a real SLC24 and SLMC.

The subscribers then have to be relocated to the vSLC with the "Relocation" feature in OpenScape 4000 Manager/Assistant.

3.14 WBMs of the Boards

For a description of the graphical user interface of the WBMs for vHG 3500 HFA, vHG 3500 SIP and vHG 3575 please refer to the following links.

vHG 3500 HFA:

http://apps.g-dms.com:8081/techdoc/en/P31003H310M1030176A9/index.htm

vHG 3500 SIP:

http://apps.g-dms.com:8081/techdoc/en/P31003H310M1010176A9/index.htm

vHG 3575:

http://apps.g-dms.com:8081/techdoc/en/P31003H310M1020176A9/index.htm

---

IMPORTANT: These documents are as online help part of the WBM.

3.15 Centralized IP for HFA

Starting with V11R0, it is possible to define one centralized IP address for all the HFA boards on a SoftGate and reduce the number of necessary IP addresses.

The centralized IP address can be configured via the AMO STMIB command, using the LIDHFA (LAN INTERFACE DATA) data type.

This TYPE requires the following parameters:

- **LIPADR** - IP Address used for HFA function.
- **LUDPPRTL** - payload UDP Port number low limit.
- **LUDPPRTH** - payload UDP Port number high limit
- **LTCPP** - TCP Port server port HFA
- **LTLSP** - TLS Port server port HFA

Example:

```
CHANGE-
STMIB:MTYPE=NCUI2,LTU=36,TYPE=LIDHFA,LIPADR=10.100.111.233,
    LUDPPRTL=29100,LUDPPRTH=30099,LTCPP=4060,LTLSP=4061;

DISP-STMIB:NCUI2,36,,;
H500:  AMO STMIB STARTED
+------------------------------------------------------------
+
  NCUI2 BOARD DATA              SOCO1000
+------------------------------------------------------------
+
  LTU = 36   SOURCE GROUP INDEX = 6

+------------------------------------------------------------
+
```

```
=========================OUTPUT
 REMOVED=========================
   LAN INTERFACE DATA - CONFIGURABLE VALUES:


 ------------------------------------------------------------


   LIPADR     =  10 .100.111.233

   LUDPPRTL   =  29100 (29100)          LUDPPRTH    = 30099
 (30099)
   LTCPP      =  4060    (4060)         LTLSP       = 4061
 (4061)

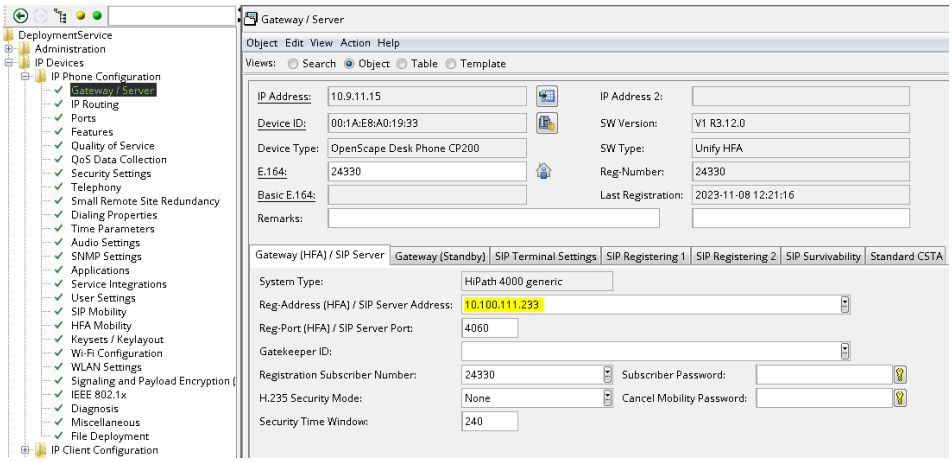
AMO-STMIB-111        CONFIGURATION OF HG3575-2 BOARDS

DISPLAY COMPLETED;
```

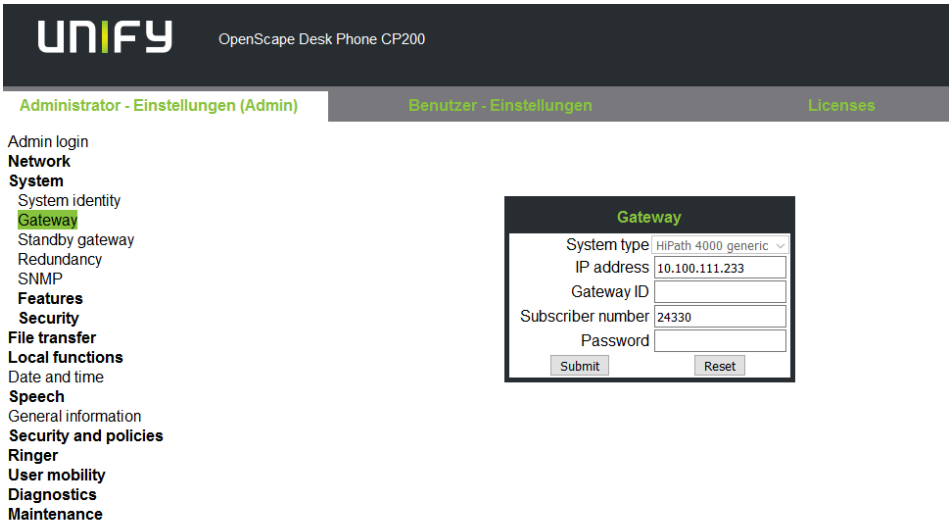
If the LIPADR parameter is configured and the IP address of the corresponding HFA board configured via CGWB is set to 0.0.0.0, then LIPADR will be used for HFA.

It is possible to use a combination of dedicated and centralized IP addresses.

You can also configure the centralized IP address where the phone is registered via DLS, as displayed in the figure below:



You can check if the phone correctly registers to the IP address of the HFA board via the phone's WBM page.



3.15.1 WBM GUI enhancements

Configuration > SPE

The WBM GUI has been enhanced with new options for the configuration of SPE certificates.

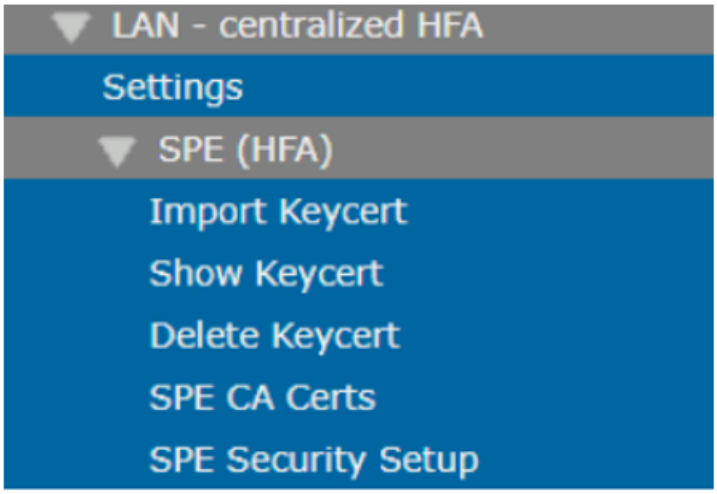


Figure 144: SPE certificates configuration

The table below presents a list of the new menu items and their usability:

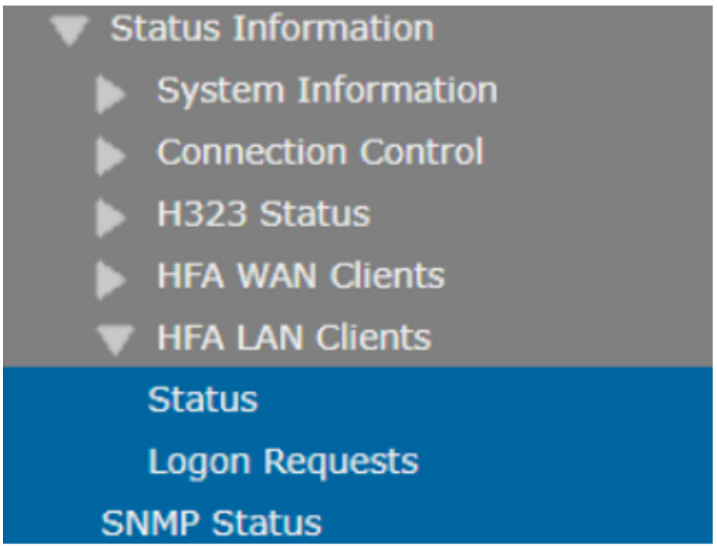
Menu items	Usability
Settings	Display the centralized IP address used for HFA.

Menu items	Usability
Import Keycert	Imports the SPE certificate.
Show Keycert	Prints the current SPE certificate (if any).
Delete Keycert	Deletes the current SPE certificate (if any). **NOTICE:** If SPE is active, the certificate cannot be deleted.
SPE CA Certs	Handles the SPE CA certificate (import, view, delete).
SPE Security Setup	Handles the TLS protocol settings for Centralized HFA IP secure connection.

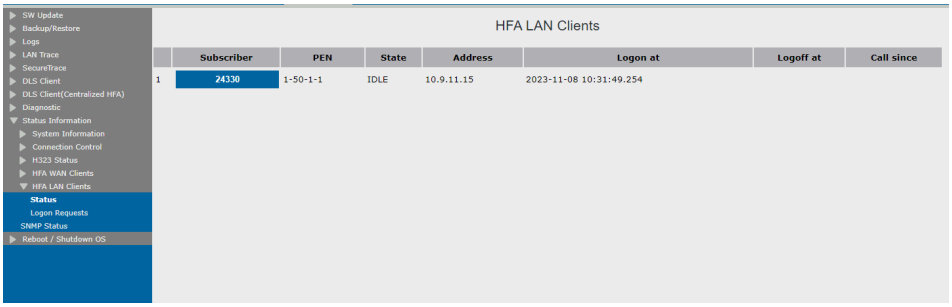
You can navigate

Maintenance > Status Information > HFA LAN Clients

By navigating to this area, you can view the status of the HFA clients and the logon requests, as displayed in the figure below:



When selecting the option **Status**, the following output is displayed:



4 LAN Connectivity (LAN Separation / LAN Redundancy)

NOTICE:

Configuration LAN Interface Bonding via SoftGate/Enterprise-Gateway WBM is no longer supported starting with V10R1.

LAN-Redundancy configured via Platform (firstinstall.xml) should be used instead.

For more information, refer to the OpenScape 4000 Installation, Configuration and Migration Guide.

IMPORTANT:

Customers using MAC based Network Access Control (NAC) with STMIX/STMIY and no LAN separation (Voice- and Management-LAN) must add both MAC address of the STMIX/STMIY (eth0 and eth1) to the related NAC equipment.

4.1 Separate LAN Connectivity for Administration and VoIP

4.1.1 Feature Description

The Voice LAN can be split fully from the Management LAN with the introduction of this feature. Before it was only possible to split the IPDA LAN from the Customer LAN.

If you want to separate the Management LAN from the Voice LAN, you have to enter an IP address for the Management LAN.

If an IP address is entered for the Management LAN, OpenScape 4000 Assistant will use it to connect to the gateway WBM and reaches it via the Customer LAN interface. If the IP address has the default value 0.0.0.0, OpenScape 4000 Assistant will use the IP address of the IPDA LAN.

Separation of the two interfaces can be configured via the gateway.

4.1.2 Service Information

IMPORTANT: If a board has a separate Management LAN interface configured, DLS bootstrapping will use the MAN IP address instead of the VOIP IP address.

- This feature is supported for OpenScape 4000 SoftGate, Enterprise Gateway, STMIX, STMIY, HG 3575 and HG 3500.
- The Management LAN interface data is provided for each OpenScape 4000 SoftGate, HG 3575 and HG 3500. It consists of IP address, netmask, default gateway, vLan tag and vLan ID.
- For SoftGate (vHG 3575 and vHG 3500) and Enterprise Gateway you have to configure in WBM the LAN interface name to use for Management LAN.

For STMI, NCUI, STMIX and STMIY this is not necessary as automatically LAN2 will be used for Management LAN.

4.1.3 Generation (Example)

An IP address has to be assigned for the Management LAN interface in AMO STMIB/AMO CGWB to activate the feature. In the case of an OpenScape 4000 SoftGate, an Ethernet interface has to be assigned additionally to the Management LAN in the WBM of the corresponding gateway.

4.1.3.1 Configuration for Common Gateway (HG 3500/ HG 3575), STMIX and STMIY

The Management LAN interface must be assigned an IP address with the assistance of AMO CGWB (HG 3500, STMIX, STMIY) or with AMO STMIB (HG 3575) in order to activate the feature.

Use the branch **MANLANIF** in AMO STMIB and AMO CGWB with the following parameters:

MIPADR=<number>, **MNETMASK**=<number>, **MVLAN**=<param>, **MVLANID**=<number>, **MDEFRT**=<number>

Only for STMI boards: If these parameters are changed, the board has to be reset twice in order to obtain the modified data. The first reset provides the new configuration data to the affected board and the second reset activates it.

HG 3500, HG 3575, STMIX and STMIY boards provide two Ethernet interfaces, LAN1 is now assigned automatically to the Voice LAN and LAN2 to the Management LAN.

NOTICE: Static route will automatically be created for IP defined under MGNTIP, derived from SIPCO:ASTIP, when it is in a different network to the Management Network. For any other IPs static routes must be manually created in the HG.

Note for STMI boards:

Static routes to Assistant will automatically be created for IPs defined under CGWB:MGNTDATA-MGNTIP and -BUSIP when they are in a different network to the Management Network. For any other IPs static routes must be manually created in the HG.

The default gateway is the one used for Voice IP in LAN1, configured via CGWB:GLOBIF-DEFTRT.

Assistant Gateway Manager should be used to access the board via MANLANIF from a different network, if static route is not added.

4.1.3.2 Configuration for OpenScape 4000 SoftGate or Enterprise Gateway

It is recommended to first perform the changes in the WBM and then in AMO STMIB.

IMPORTANT: If you change this sequence, you have to make sure that you do not update the board list in the dashboard (**Expert mode > Dashboard >** button **Update Board List**), because the board (vHG 3575) is still only accessible for administration via the old IP address even though the new IP address has already been assigned with the AMO. This applies for as long as the Management LAN interface is assigned in the WBM.

Step 1: Assign the Ethernet interface to the Management LAN

The Ethernet interface for the Management LAN has to be assigned in the WBM. You have to launch the dashboard for this purpose in the OpenScape 4000 Assistant.

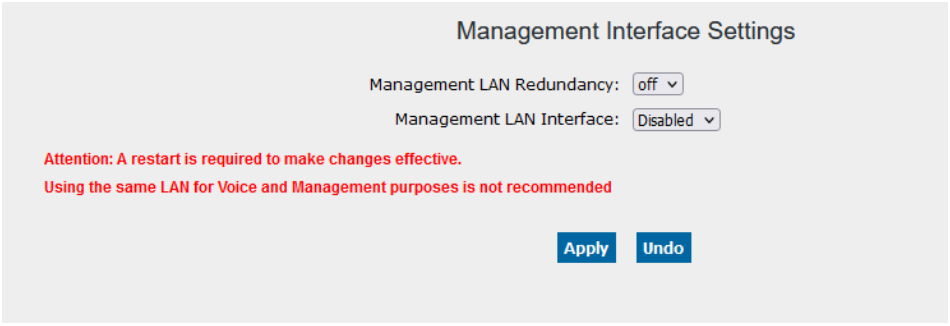
Expert mode > Manager



Figure 145: Separate LAN interfaces - Manager

Now select the board and start the WBM. Navigate to **Configuration > LAN Interfaces > Management Interface**.

In the drop-down list for the **Management LAN Interface** select an Ethernet interface and confirm your input with **Apply**.



Management LAN interface for OpenScape 4000 SoftGate (including vHG 3500) and Enterprise Gateway

Step 2: Assign the IP address

You will find the Management LAN data for OpenScape 4000 SoftGate (vHG 3575) or Enterprise Gateway in AMO STMIB and for vHG 3500 in AMO CGWB.

Use the branch **MANLANIF** with the following parameters:

MIPADR=<number>, **MNETMASK**=<number>, **MVLAN**=<param>, **MVLANID**=<number>, **MDEFRT**=<number>

If these parameters are changed, the boards must be reset to get the changed data.

4.1.4 Relevant AMOs

AMO	Parameter	Sprache/ Language	Beschreibung/ Discription
CGWB/ STMIB	MIPADR	d	IP Adresse der CGW Baugruppe (Source Adresse)
	MIPADR	e	Source IP address of CGW board
	MNETMASK	d	IP-Netzmaske des LAN-Segmentes Die IP-Netzmaske bestimmt die Grenze zwischen Netz- und Host-Teil in der IP-Adresse. Alle IP-Adressen am LAN-Segment müssen bzgl. des Netzanteils der IP-Adresse gleich und bzgl. des Host-Teils unterschiedlich sein (auch der Default Router muss dieser Bedingung entsprechen).
	MNETMASK	e	IP net mask of LAN segment The IP net mask determines the network and the host partition of an IP address. All IP addresses of a LAN segment must contain the identical network address part but different host address parts (also the Default Router must fulfill this requirement).
	MVLAN	d	Virtuelles LAN
	MVLAN	e	VLAN tagging on LAN-IF
	MVLANID	d	Identifikations-Nummer des virtuellen LAN Spezielle Einstellungen werden von einigen LAN-Einrichtungen (Router...) gefordert, ansonsten ist 0 der übliche Wert (Standardwert)
	MVLANID	e	Virtual LAN Identification Special settings are required by certain LAN equipment (routers...), in other cases the VLAN Id should be set to 0 (default)

AMO	Parameter	Sprache/ Language	Beschreibung/ Discription
	MDEFRT	d	IP-Adresse des Default Routers innerhalb des LAN-Segmentes Der Default Router übernimmt die Weiterleitung der Pakete, die eine Zieladresse außerhalb des eigenen LAN-Segmentes haben. 0.0.0.0 bedeutet, dass kein Default Router konfiguriert ist.
	MDEFRT	e	IP address of the default router within the LAN segment The default router takes care of routing forward all packets with a destination address with a network part different from the own LAN segment. 0.0.0.0 means that no default router is configured.

4.2 Separate LAN Interfaces for HFA and SIP

4.2.1 Feature Description

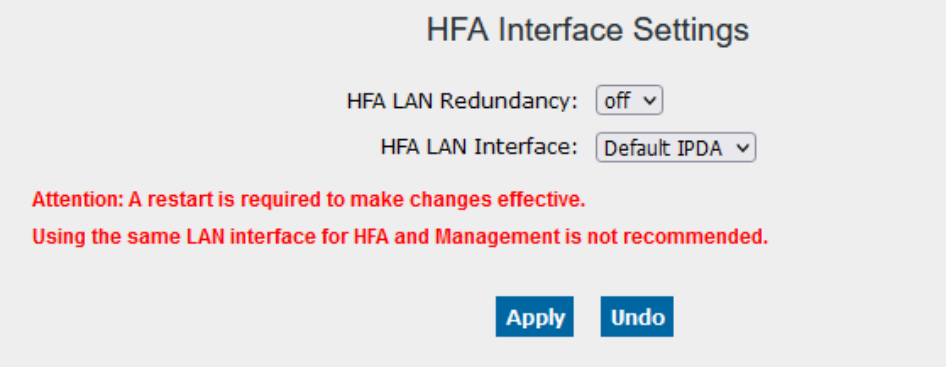
With the realization of the feature **Separate LAN Interfaces for HFA and SIP** it is possible to separate the HFA and SIP Signaling from the IPDA interface.

This features has been released for OpenScape 4000 V7 R1 and higher.

4.2.2 Generation (Example)

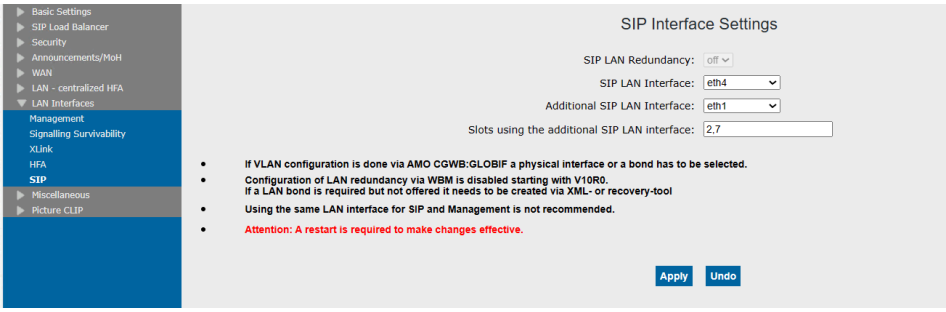
Separate LAN interfaces can be defined in the OpenScape 4000 SoftGate WBM in the LAN Interfaces menu for HFA and SIP. The IPDA LAN interface is used as standard (**HFA LAN Interface: Default IPDA** or **SIP LAN Interface: Default IPDA**).

Configuration > LAN Interfaces > HFA Interface > parameter **HFA LAN Interface**



OpenScape 4000 SoftGate - HFA interface

Configuration > LAN Interfaces > SIP Interface > parameter **SIP LAN Interface**



OpenScape 4000 SoftGate - SIP interface

It is possible to use the same interface for SIP and HFA. However, it is not recommended to operate SIP and HFA on the management interface, assuming this interface has been configured. It is also the case for SIP boards that a configured WAN interface is set up by preference. A separate SIP interface would not be considered in this case.

For SIP clients and SIP trunks it is possible to define an additional SIP LAN interface by choosing it from the selection list (i.e., none, bond0, eth2, etc.).

The slot configuration for the additional SIP LAN interface should be under the format of empty-string numbers or followed by comma.

If additional LAN interface is set to none (default) no slot can be entered.

The corresponding configuration data is contained in the HBR backup.

Redundant LAN (bonding) can also be configured for SIP and HFA. Additional information in this regard can be found in Chapter 19, “Redundant LAN Interfaces (Bonding)”.

The IP addresses that have been configured with AMO CGWB for the corresponding boards are configured at the relevant LAN interfaces when the OpenScape 4000 SoftGate is restarted.

4.3 LAN Redundancy

4.3.1 Feature Description

For increased resilience, OpenScape 4000 SoftGate can be connected with two LAN cables to different switches/router.

Additionally you have to activate the LAN Redundancy feature in the OpenScape 4000 Platform Administration (Portal) or by editing the initialcfg.xml file.

Scenarios when SoftGate server is starting up

Scenario 1: Both LAN cables are connected

LAN port 1 (1. Slave interface) will always be activated. LAN port 2 (2. Slave interface) will be on .

Scenario 2: Only one LAN cable is connected

The connected LAN port (LAN1 or LAN2) will be used.

Scenario when board is active

If the active LAN port is disconnected/disabled by peer or equipment (when both LAN ports are connected):

- The Linux OS activates the LAN port.
- The "new" active LAN port sends a GRATUITOUS ARP with the same MAC and IP addresses as the "old" port.
- If ports switch, the payload will be lost for < 2 sec - all active connections will be saved and NOT disconnected.
- If the "old" port comes up again, no port switchback will be performed.

4.3.2 Redundant LAN Interfaces (Bonding)

NOTICE:

LAN Interface Bonding configuration via SoftGate/Enterprise-Gateway WBM is no longer supported starting with V10R1.

LAN redundancy configured via Platform (firstinstall.xml) should be used instead. For more information, see the OpenScape 4000, Installation, Configuration and Migration document.

IMPORTANT: Customers using MAC based Network Access Control (NAC) with STMIX/STMIY and no LAN separation (Voice- and Management-LAN) must add both MAC addresses of the STMIX/STMIY (eth0 and eth1) to the related NAC equipment.

4.3.2.1 Feature Description

Redundant LAN interfaces can be configured in order to ensure higher failsafe reliability.

4.3.2.2 Generation (Example)

Redundant LAN interfaces (bonding) can be configured in the OpenScape 4000 SoftGate WBM in the **WAN** and **LAN Interfaces** menus in order to improve the failsafe reliability.

- Redundant LAN for WAN
- **Configuration > WAN > WAN Settings >** parameter **WAN Redundancy**

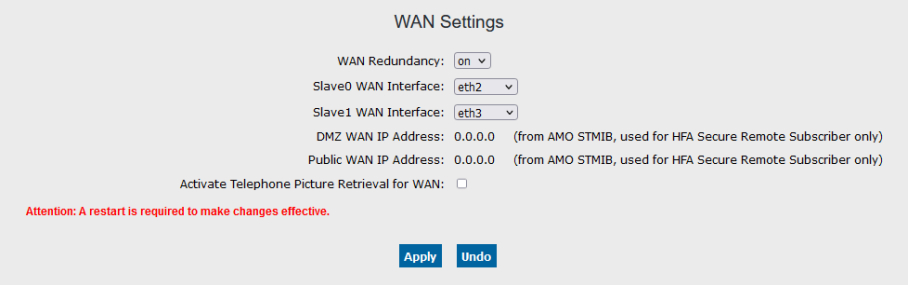


Figure 146: OpenScape 4000 SoftGate - Redundant WAN

- Redundant LAN for Management Interface
- **Configuration > LAN Interfaces > Management Interface >** parameter **Management LAN Redundancy**

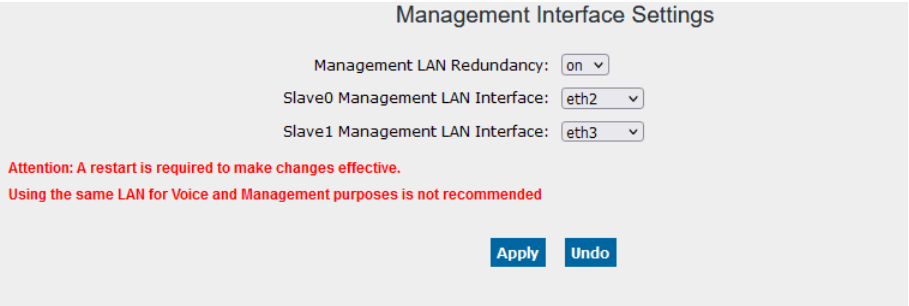


Figure 147: OpenScape 4000 SoftGate - Redundant Management LAN

- Redundant LAN for Signaling Survivability Interface

- **Configuration > LAN Interfaces > Signaling Survivability Interface >** Parameter **LAN Redundancy**

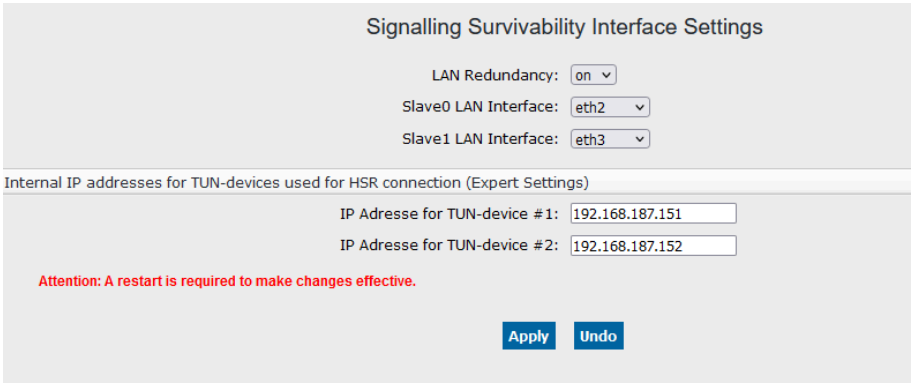


Figure 148: OpenScape 4000 SoftGate - Redundant Signaling Survivability LAN

- Redundant LAN for HFA Interface
- **Configuration > LAN Interfaces > HFA Interface >** parameter **HFA LAN Redundancy**

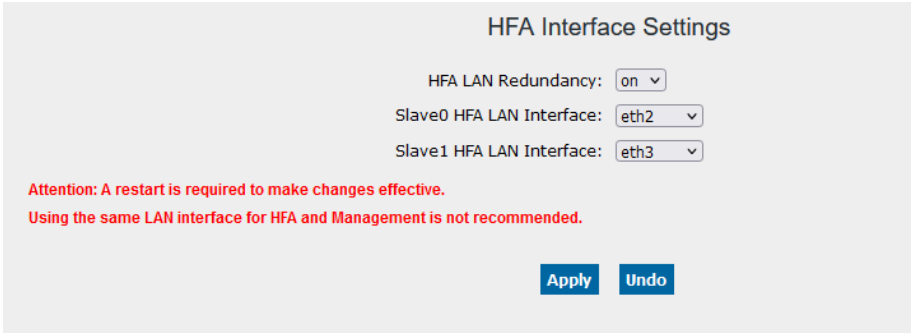


Figure 149: OpenScape 4000 SoftGate - Redundant LAN at HFA interface

- Redundant LAN for SIP Interface
- **Configuration > LAN Interfaces > SIP Interface >** parameter **SIP LAN Redundancy**

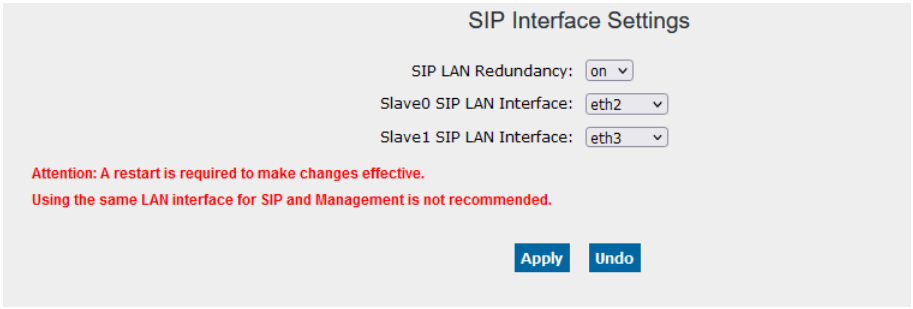


Figure 150: OpenScape 4000 SoftGate - Redundant LAN at SIP Interface

The IP addresses that have been configured with AMO CGWB for the relevant boards are configured at the relevant bonding network interfaces (e.g. bondhfa0) when the OpenScape 4000 SoftGate is restarted.

5 OpenScape Access and OpenScape Branch

OpenScape Access is based on hardware and software of OpenScape 4000. It offers a cost-saving alternative for branch office solutions with integrated PSTN connection.

For documentation on OpenScape Access/Branch please refer to the following manual:

1) OpenScape Access, Service Documentation

6 OpenScape Enterprise Gateway

OpenScape Enterprise Gateway is based on hardware and software of OpenScape 4000. It is successor of AP 3700-9 shelves with HG3575. The whole feature content of IP Distributed Architecture (IPDA) is available.

For more information please refer to the related service documentation:

1) OpenScape 4000 V8, Enterprise Gateway, Service Documentation

7 Large Enterprise Gatekeeper (LEGK)

7.1 General Information

7.1.1 Overview

The feature “Large Enterprise Gatekeeper (LEGK)” is part of the call processing software and has a gatekeeper function. Therefore the IP address resolution mechanism (gatekeeper function) for IP trunking is switchable in all network nodes.

For this function the STMI2/4 (HG 3500) board as hardware is required.

SIP-Protocol is used by default for trunking.

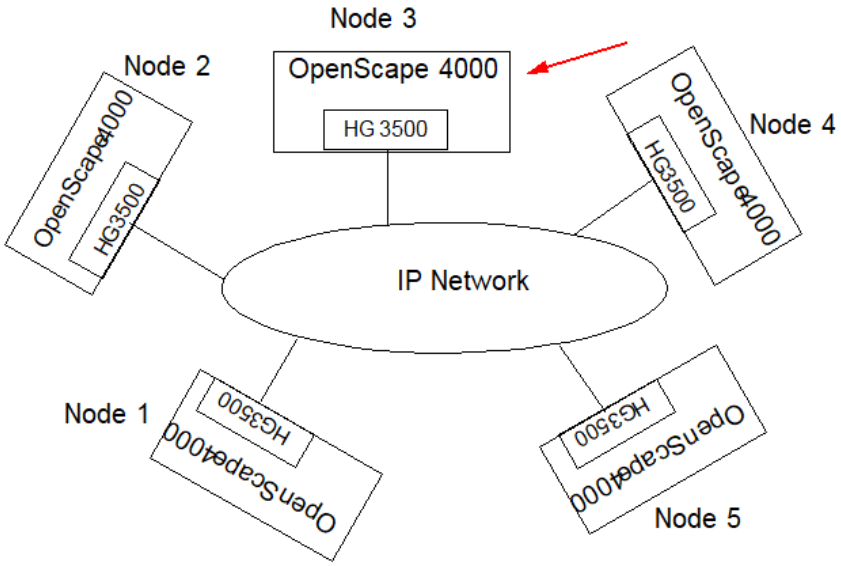


Figure 151: Example: IP trunking in an OpenScape 4000 networked system. LEGK is active in each node.

7.1.2 Gatekeeper Function

7.1.2.1 General Information

The Gatekeeper function is used to allocate the IP address of a destination gateway to a dialed extension (IP address resolution). The Large Enterprise Gatekeeper (LEGK) performs this function using a HG 3500.

The gatekeeper functionality (LEGK) is fully integrated in the LCR function in OpenScape 4000. The LEGK is therefore neither an external server nor a host in the IP network. The LEGK is a process within the OpenScape 4000 call processing software. The Gatekeeper function is consequently fully configured

using AMO commands. The Web Based Management (WBM) tool in HG 3500 is only needed for special settings, for example, codec selection and QoS. With the HG 3500 Common Gateway these features are also configurable via AMO - the WBM is now almost exclusively used for maintenance tasks.

If IP trunking is used in a purely OpenScape 4000 networked system, then all HG 3500 gateways connected must use the LEGK of their respective nodes. HG 3500s may not register with the LEGK of another node.

7.1.2.2 Key words

7.1.2.2.1 Local Gateway

This is the name given to an HG 3500 configured for trunking in an OpenScape 4000 with a gatekeeper, which it uses for address resolution.

With regard to the Figure 1 all HG 3500 Gateways displayed there are local Gateways.

7.1.2.2.2 Remote Gateway

This is the name given to an HG 3500 configured for trunking in an OpenScape 4000, which registers with another, external gatekeeper or registry for address resolution.

Only HG 3500 gateways that are not OpenScape 4000s, e.g. OpenScape Voice or an Internet Service Provider, may register as remote gateways with the system.

7.1.2.2.3 IP Address Resolution

A called party number is routed via LCR to an IP address in the destination gateway. IP Address Resolution may be configured in an OpenScape 4000 with LCR. This service is only available for local gateways.

7.1.3 Gatekeeper Restrictions

The Large Enterprise Gatekeeper can be operated together with the board HG 3500.

Maximum configuration:

An IP trunking network using HG 3500 is theoretically limited to a maximum of 9999 trunking boards (DIMSU). For the exact maximum, please refer to the release notes and/or technical specifications.

7.2 Guidelines for Installing an IP Feature

- Diagram of the customer IP network
- Create an OpenScape 4000 network plan with all gateways, access points, HFA terminals
- Define the number of LEGKs and HG 3500 gateways required
- Map the OpenScape 4000 network plan to the customer IP network
- Perform network analysis with the help of the IP service tool to determine the network’s VoIP capability.
- Confirm the feasibility of the IP components planned

7.3 Configuring the Feature

The Large Enterprise Gatekeeper (LEGK) is a feature for IP trunking address resolution for data transfer in IP networks. The configuration of this feature is broken down into the following steps which are to be performed in consecutive sequence:

- Configuration: Database flexama memory - Section 3.4, “Configuring the FLEXAMA Memory in the Database”, on page 545
- Configuration: HG 3500 - Section 3.5, “Configuring a HG 3500 on the LAN Segment”, on page 549
- Configuration: HG 3500 directory numbers - Section 3.6, “Configuring the HG 3500 Directory Number”, on page 567
- Configuration: LCR digit analysis - Section 3.7, “Configuring IP Trunking in the LCR”, on page 569
- Configuration: Subscriber, trunk and tie trunk connections in the local switch - Section 3.8, “Configuring Circuits and Terminals”, on page 574

The LEGK feature must be taken into consideration when configuring IP trunking. If IP trunking is already available, it must be re-generated.

The following sections contain configuration examples and detailed explanations of all requisite AMOs and AMO parameters. A distinction is made between

	configuration with OpenScape 4000 Assistant/Manager (Configuration Manager) or
	AMO-based configuration.

The Large Enterprise Gatekeeper can be implemented in all OpenScape 4000 system configurations. An LEGK can either be implemented in all nodes or in a single node in an OpenScape 4000 network.

7.3.1 Important Information

IMPORTANT: Registration of remote HG3500 gateways at OpenScape 4000 Large Enterprise Gatekeeper is not supported. Remaining solutions are the local registration with Large Enterprise Gatekeeper and HiPath OpenExchange Solution.

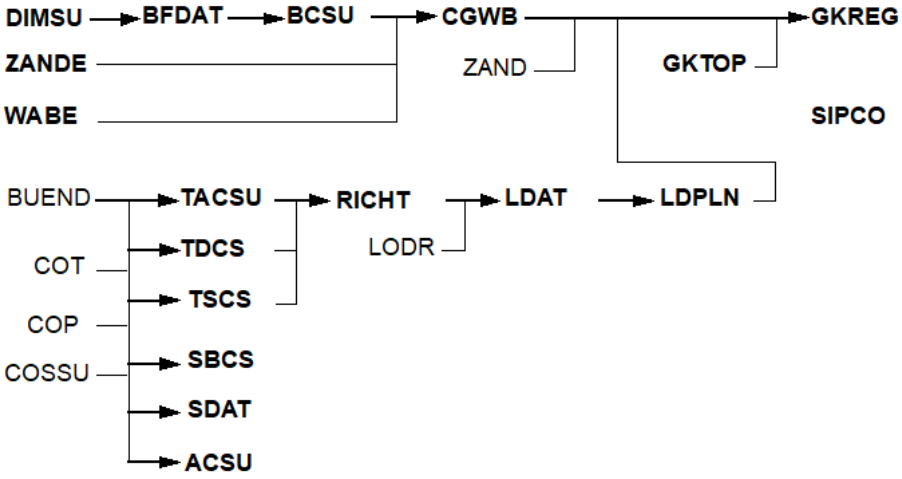
7.3.2 Sequence of Generation

This section describes the basic sequence for generating the “Large Enterprise Gatekeeper“ feature. This description focuses first and foremost on the AMOs that were extended for the purpose of administering the feature. These AMOs are shown in bold typeface.

The other AMOs displayed are also involved in the generation process but were not extended for the specific feature. The existing generation sequence is used here.

In the course of configuration, the AMOs GKREG and GKTOP do not check if the resources used, such as sectors, sector path, clusters, LCR dial plan numbers, node numbers, external gateways, etc. are already configured.

The user is responsible for the consistency of the IP network's administered topology resources (for example, bandwidth, B-channels, etc.). This task is not supported by the AMO GKTOP with plausibility checks.



IMPORTANT: The AMOs do not check the specified gatekeeper configuration data for plausibility or network-wide consistency. This is one of the technician's network planning tasks.

7.3.3 Activating the Large Enterprise Gatekeeper

This step is only necessary if you do not want to run a Large Enterprise Gatekeeper for least cost routing on the local OpenScape 4000 system. The feature is active by default.

If you do not want a gatekeeper at the local OpenScape 4000 system, then the feature must be deactivated in the system before HG 3500 is installed. The **GATEKPR** parameter in the AMO ZANDE is used for this.

IMPORTANT: You cannot enable or disable the gatekeeper function at an OpenScape 4000 system by simply activating or deactivating the AMO ZANDE once HG 3500 generation is complete. Instead, you must remove all STMI2/4 and STMIX/ STMIY HG 3500 boards, activate/deactivate the ZANDE parameter, and finally reinstall the boards. This sequence is necessitated by the different configurations of feature-specific data.

Generation

AMO ZANDE

The AMO ZANDE is used on every OpenScape 4000 system to specify whether or not this feature should be used.

	Configuration with the AMO ZANDE can only be executed in expert mode. **Expert Mode > Expert Access > Open ...<IP> with AMO** (see AMO command)
	`ADD-ZANDE:TYPE=ALLDATA,GATEKPR=YES;`

This command specifies that the LEGK address resolution function (AMO GKREG) should be operated and administered at the local OpenScape 4000 system.

Table 18: AMO ZANDE parameters in the CHANGE branch under TYPE=ALLDATA

AMO	Parameter	Sprache/ Language	Beschreibung/ Description
ZANDE	GATEKPR	d	Gatekeeper Konfigurierung Diese Parameter muss auf NEIN gesetzt werden wenn eine PBX ohne Gatekeeper betrieben werden soll. Standardmäßig wird JA, d.h. also ein Gatekeeper wird an der lokalen PBX betrieben, eingerichtet.
	GATEKPT	e	Gatekeeper configuration This Parameter must be set to NO when a PBX has to operate with-out a gatekeeper. Default value is YES, that means a gatekeeper will be configured on the local PBX.

Display

	Displaying with the AMO ZANDE can only be executed in expert mode. **Expert Mode > Expert Access > Open ...<IP> with AMO** (see AMO command)
	`DISPLAY-ZANDE:TYPE=ALLDATA;`

Use this command to output all central parameters in the ALLDATA branch, including the gatekeeper parameter.

7.3.4 Configuring the FLEXAMA Memory in the Database

First of all, a certain volume of feature-specific memory should be provided. You can only start to configure the gatekeeper data after this memory has been created with the AMO DIMSU.

The values specified with ADD-DIMSU become effective immediately.

7.3.4.1 Number of Internal and External Gateways

This step is used to configure a table containing general administrative data for all internal and external gateways in the network. An entry is required for each gateway.

IMPORTANT: You can skip this section if there is no gatekeeper configured at the local OpenScape 4000 system (AMO ZANDE: **GATEKPR=NO**).

Add:



```
ADD-DIMSU:TYPE=SYSTEM,GWREG=25;
```

Use this command to set the number of network-based gateways (in our case 25) that can address the Large Enterprise Gatekeeper.

Display:



```
DISPLAY-DIMSU:TYPE=SYSTEM;
```

Use this command to output all system parameters including the number of gateways permitted.



```
DISPLAY-DIMSU:TYPE=ALL,PARAM=GWREG;
```

Use this command to output only the number of gateways permitted.

7.3.4.2 Number of Internal HG 3500 Gateways in a System

This step is used to configure a table containing data for the internal gateways in every OpenScape 4000 system. An entry is required for each gateway.

Add:



```
ADD-DIMSU:TYPE=SYSTEM,CGW=6;
```

Use this command to set the maximum number of HG 3500 (in our case, 6).

Display:



```
DISPLAY-DIMSU:TYPE=SYSTEM;
```

Use this command to output all system parameters including the number of internal gateways permitted.



```
DISPLAY-DIMSU:TYPE=ALL,PARAM=CGW;
```

Use this command to output only the number of internal gateways permitted.

7.3.4.3 Number of LCR Digit Patterns for Digit Pattern Pools 1 through 8

This step configures the number of LCR digit patterns permitted in each of the eight available digit pattern pools. Up to 64,000 digit patterns are permitted in each pool. The digit patterns configured are evaluated during IP trunking as part of least cost routing.

IMPORTANT: You can skip this section if there is no gatekeeper configured at the local OpenScape 4000 system (AMO ZANDE: **GATEKPR=NO**). In this case, the default configuration is sufficient with LCR pool 1 and dial plan 0.

Add:



```
ADD-
DIMSU:TYPE=NETWORK,LDPLN1=50000,LDPLN2=12000,LDPLN4=5600;
```

Use this command to set the maximum number of LCR digit patterns per digit pattern pool, in our case:

- 50,000 digit patterns in digit pattern pool 1
- 12,000 digit patterns in digit pattern pool 2
- 5,600 digit patterns in digit pattern pool 4

Display:



```
DISPLAY-DIMSU:TYPE=NETWORK;
```

Use this command to output all parameters associated with network-wide features, including the number of digit pattern schemes in digit pattern pools 1 through 8.



```
DISPLAY-DIMSU:TYPE=ALL,PARAM=LDPLN2;
```

Use this command to output only the number of LCR digit pattern schemes permitted in pool 2.

7.3.4.4 Number of Cache Elements for Cache Pools 1 through 8

This step configures the number of cache elements permitted in each of the eight available cache pools. Up to 6,400 cache elements are permitted in each pool.

IMPORTANT: You can skip this section if there is no gatekeeper configured at the local OpenScape 4000 system (AMO ZANDE: **GATEKPR=NO**).

Add:



```
ADD-DIMSU:TYPE=NETWORK,LDPLN1=5000,LDPLN2=120,LDPLN4=100;
```

Use this command to set the maximum number of cache elements per digit pattern pool, in our case:

- 5,000 digit patterns in digit pattern pool 1
- 120 digit patterns in digit pattern pool 2
- 100 digit patterns in digit pattern pool 4

Display:



```
DISPLAY-DIMSU:TYPE=NETWORK;
```

Use this command to output all parameters associated with network-wide features, including the number of cache elements in cache pools 1 through 8.



```
DISPLAY-DIMSU:TYPE=ALL,PARAM=LDPLNC1;
```

Use this command to output only the number of cache elements permitted in cache pool 1.

7.3.5 Configuring a HG 3500 on the LAN Segment

The HG 3500 module (STMI2/4 and STMIX/STMIY) establishes the payload connections between the central OpenScape 4000 system and the OpenScape 4000 LAN segment.

- HG 3500 boards may be implemented both in peripheral shelves (LTU 1-15) in the central system and in access points (LTU 17-99). You can implement the same number of HG 3500 gateways that you configured with the AMO DIMSU (see Section 3.4.2, “Number of Internal HG 3500 Gateways in a System”, on page 546).
- Multiple HG 3500 modules can be implemented in an OpenScape 4000 system.
- All HG 3500 modules must be connected at the OpenScape 4000 LAN segment.
- The HG 3500 hardware is the STMI2/4 board. This board can simultaneously offer IP trunking, a WAML circuit, IPDA function, HFA function and SIP subscriber function. The type and number of circuits or B channels available in each case is set with the AMO BFDAT.

NOTICE: It is not possible to configure WAML on STMIX/ STMIY.

An OpenScape 4000 LAN segment is that part of the customer network where the central system’s IP components and directly connected (that is, not via router) access points are installed.

7.3.5.1 Configuring the HG 3500 Gateway

You must first configure the local LAN segment. Next you must install each HG 3500 gateway.

7.3.5.1.1 Configuring the HG 3500 Board

The configuration example applies to the OpenScape 4000 system with gatekeeper on the left (“N 1“). The HG 3500 to be administered with the relevant configuration data is colored yellow. The gatekeeper (CUSIP=192.168.2.11) in the partner system “N 2“ is colored in a lighter shade of yellow and will be described in more detail later in conjunction with the AMOs GKREG and GKTOP.

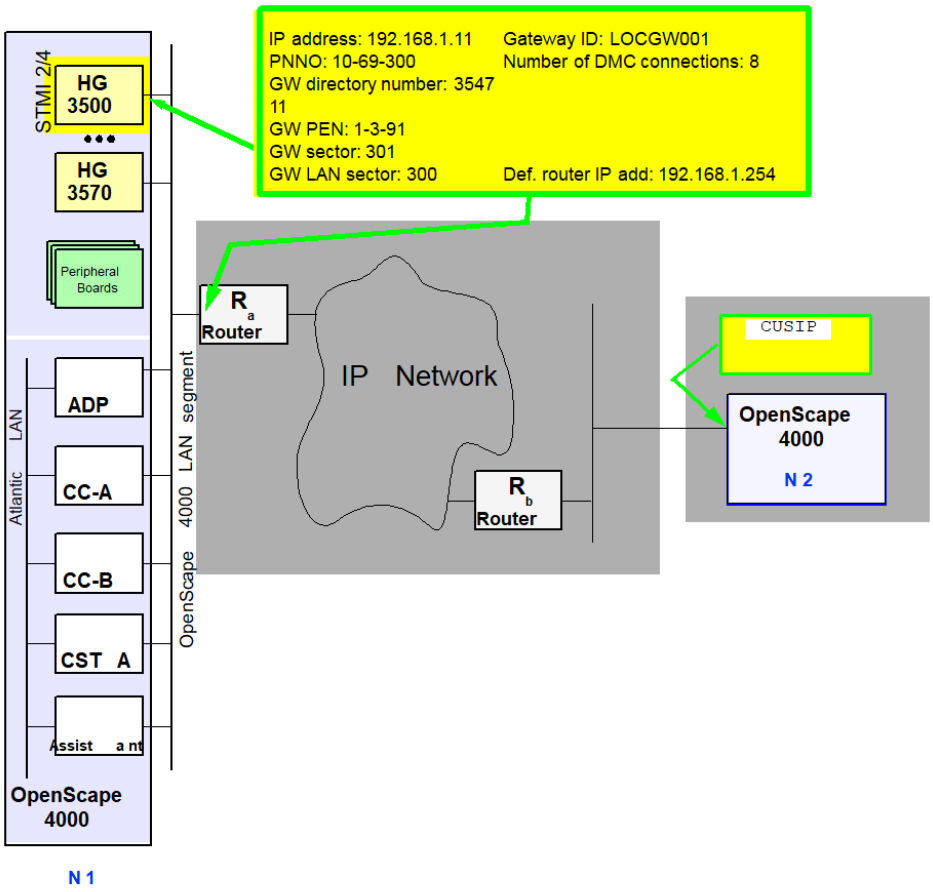


Figure 152: Configuring a HG 3500 gateway

ADD-BFDAT:	FCTBLK=1,	FUNCTION=HG3550,
	BRDBCHL=BCHL60&BCHL120;	
CHANGE-BFDAT:	CONFIG=CONT,	FCTBLK=1,
	FUNCTION=HG3550,	LINECNT=1,
	UNITS=3;	
CHANGE-BFDAT:	CONFIG=OK,	FCTBLK=1,
	ANSW=YES;	
ADD-BCSU:	MTYPE=IPGW,	LTG=1,
	LTU=3,	SLOT=91,
	PARTNO=Q2316-X10,	FCTID=1,
	FCTBLK=1,	BCHL3550=30;
ADD-CGWB:	MTYPE=CGW,	LTU=3,
	SLOT=91,	IPADR=192.168.1.11,
		NETMASK=255.255.255.0;
CHANGE-CGWB:	MTYPE=CGW,	LTU=3,
	SLOT=91,	TYPE=GWDATA,
	GWID1=LOCGW001;	
CHANGE-CGWB:	MTYPE=CGW,	LTU=3,
	SLOT=91,	TYPE=LEGKDATA,

Generation

A HG 3500 board is configured via 3 AMOs: BFDAT, BCSU and CGWB.

AMO BFDAT

The configuration of the functional blocks for the HG 3500 board is done with the AMO BFDAT.

	**Configuration Management > System Data > Board > CGW Function Block** Click **New**, enter data and click **Save**.
	ADD- BFDAT:FCTBLK=1,FUNCTION=HG3550,BRDBCHL=BCHL60&BCHL120; CHANGE-BFDAT:CONFIG=CONT,FCTBLK=1,FUNCTION=HG3550, LINECNT=1,UNITS=3; CHANGE-BFDAT=CONFIG=OK,FCTBLK=1,ANSW=YES;

Table 19: AMO BFDAT parameters

AMO	Parameter	Sprache/ Language	Beschreibung/ Description
BFDAT	ANTW	d	ANTW=JA Block-Konfiguration abschließen
	ANSW	e	ANSW=YES Finish block configuration
	ANZEINH	d	Anzahl der vordefinierten Blöcke mit ausgewählter Funktion pro Satz.
	UNITS	e	Defines the number of predefined blocks with the selected function per line.
	ANZSATZ	d	Anzahl der funktionsbezogenen Saetze.
	LINECNT	e	Defines the number of lines related to the selected function.
	BKANANZ	d	Block fuer Baugruppe mit 60 und/oder 120 B-Kanälen
	BRDBCHL	e	Dedicates the block for boards with 60 and/ or 120 b-channels
	CONFIG	d	CONFIG=WEITER Weitere Block-Konfiguration möglich CONFIG=OK Block-Konfiguration abschließen

AMO	Parameter	Sprache/ Language	Beschreibung/ Description
	CONFIG	e	CONFIG=CONT Continue block configuration CONFIG=OK Finish block configuration
	FCTBLK	d	Dieser Index beschreibt den Funktionsblock welcher auf dem Common Gateway konfiguriert werden soll. Anhand des Funktionsblocks wird die Konfiguration der benötigten pyhsikalischen Lines (Sätze der Baugruppe) festgelegt.
	FCTBLK	e	This index describes the function block which should be configured on the common gateway board. With that index the amount of needed physical lines (board circuits) is calculated.
	FUNCTION	d	Dieser Parameter legt das Konfigurationsprofile des CGW fest. Dabei muss die evtl. benötigte HG3570 Funktion als erste angeführt werden. Falls ein bestimmter Line-Bereich für die Funktionen HG3530, HG3540 oder HG3550 vorreserviert werden soll, muss die entsprechende Funktion am Ende stehen und mit dem Wert HG35xxR abgeschlossen sein. Die Funktion kann nur als Einzel-Funktion konfiguriert werden.
	FUNCTION	e	This parameter defines the configuration profile of the common gateway board. If HG3570 functionality is used, it must be configured at first position. If a prereservation of a certain line range of functions HG3530, HG3540 or HG3550 is desired, this function must be at the end of the profile just suffixed by the according HG35xxR value. The function can only be configured as single function.

AMO BCSU

The modules are configured in the system and activated with the AMO BCSU.

	**Co**nfiguration Management > System Data > Board > Board Click **New**, enter data and **Save**.
	ADD- BCSU:MTYPE=IPGW,LTG=1,LTU=3,SLOT=91,PARTNO=Q2316-X10,FC- TID=1,FCTBLK=1,BCHL3550=30; CHANGE- BCSU:TYPE=HWYBDL,LTU=3,SLOT=81,PARTNO=Q2316-X10,HWYBDL=A;

Table 20: AMO BCSU parameters

AMO	Parameter	Sprache/ Language	Beschreibung/ Description
BCSU	TYP	d	TYP=IPGW Common Gateway Baugruppe
	MTYPE	e	MTYPE=IPGW Common gateway board
	LTG	d	LTG-Nummer Parameter kann entfallen - oder muss auf 1 gesetzt werden.
	LTG	e	Line/Trunk Group Number Parameter can be omitted - or must be set to 1.
	LTU	d	LTU-Nummer des Rahmens, in dem die HG 3500 eingesetzt wird. Die HG 3500 darf nur in den Rahmen des OpenScape 4000 Zentralsystems (LTU 1..15) eingesetzt werden. Der Rahmen muss mit einer LTUCX Baugruppe ausgestattet sein.
	LTU	e	Line/Trunk Unit Number of the shelf where the HG 3500 is plugged. An HG 3500 may only be used in a shelf of the OpenScape 4000 central system (LTU 1..15). The shelf must be equipped with a LTUCX board.
	EBT	d	Einbauteilung des Steckplatzes der HG 3500
	SLOT	e	Slot where the HG 3500 resides.
	SACHNR	d	Sachnummer der HG 3500-Baugruppe
	PARTNO	e	Part Number of the HG 3500 Board

AMO	Parameter	Sprache/ Language	Beschreibung/ Description
	FCTID	d	Function ID
	FCTID	e	Function ID
	FCTBLK	d	Function Block Index
	FCTBLK	e	Function block index
	BKAN3550	d	Anzahl der B-Kanäle für die HG3550 Funktion
	BCHL3550	e	Amount of b-channels for HG3550 function
	HWYBDL	d	Highway Bündel Die HG 3500 / STMI2/4 Baugruppe unterstützt die Wideband Technologie. Deshalb muss der Baugruppe entweder das Highway Bündel A (default) oder F zugewiesen werden.
	HWYBDL	e	Highway bundle The HG 3500 / STMI2/4 board supports wideband technology. Thus either highway bundle A (default) or F must be assigned to this board.

AMO CGWB

Use the ADD branch to make the individual settings necessary for operating the HG 3500 board. Global and Ethernet-specific board data is configured. This data is not loaded to the board until the board is activated or deactivated and then re-activated (RESTART-BSSU).

The CHANGE branch MTYPE=CGW allows you to set a number of parameters that are located in different branches. Data from the branches TYPE=GWDATA, TYPE=DMCDATA, and TYPE=LEGKDATA is also needed for startup.

The specification of a GWNO depends on the operating scenario set (see AMO ZANDE)

- PBX with LEGK
- PBX without LEGK

Operation in mixed mode is not possible.

A gateway number is required if the gatekeeper is configured at the local PBX and you want to register the gateway here.

A gateway number is not required if a gateway registers at a foreign PBX’s gatekeeper. If entered, a gateway number would be ignored.

Adding Ethernet-specific board data

	**Configuration Management > System Data > Board > Board** Click **Search** and select **Board Name=STMI2**,**Board Name=STMI4, Board Name=STMIX or Board Name=STMIY** . Make the settings on the **STMI Board Data** tab and **Save**. **Configuration Management > System Data > Maintenance > Board Maintenance** Click **Search** and select **STMI**. Click **Execute** on the **Action** pull-down menu, select **Restart** and confirm with **OK**.
	`ADD-CGWB:LTU=3,SLOT=91,IPADDR=192.168.1.11,NETMASK=255.255.255.0;` The HG 3500 must be restarted in order for this change to become effective. Use `RESTART-BSSU:ADDRTYPE=PEN,LTU=3,SLOT=91;`

IMPORTANT: Established **connections are cleared down as a result!**

Table 21: AMO CGWB parameters

AMO	Parameter	Sprache/ Language	Beschreibung/ Description
CGWB	LTU	d	LTU-Nummer des Rahmens, in dem die HG 3500 gesteckt ist.
	LTU	e	Line/Trunk Unit Number of the shelf where the HG 3500 is plugged.
	EBT	d	Einbauteilung des Steckplatzes der HG 3500
	SLOT	e	Slot where the HG 3500 resides.
	IPADR	d	IP-Adresse der HG 3500 im Kunden LAN Legt die IP-Adresse fest, über die ein HG 3500 Gateway am OpenScape 4000 LAN-Segment erreicht werden soll.
	IPADR	e	IP-Address of HG 3500 on customer LAN Assigns the address with which a HG 3500 gateway can be reached on the OpenScape 4000 LAN-segment.
	NETMASK	d	Netzmaske des LAN-Segmentes
	NETMASK	e	Netmask of LAN-segment
	MUSTER	d	Ruhebitmuster Der Default-Wert ist 213 (dezimal)
	PATTERN	e	Idle Pattern Default value is 213 (decimal)

IMPORTANT: Before administering the ADD-CGWB command, use **ping** to check that the gateway IP address given to you by the administrator is reachable. *CUSIP* must not respond as this would indicate that the corresponding address has already been assigned. *CUSIP* must be set differently for every HG 3500. The AMO does not verify if this rule is observed.

TYPE=GWDATA - Changing gateway identification

	**Configuration Management > System Data > Board > Board** Click Search and select Board Name=STMI2, Board Name=STMI4, Board Name=STMIX or Board Name=STMIY. Make the settings on the **STMI2-IGW Board Data** tab and **Save**. **Configuration Management > System Data > Maintenance > Board Maintenance** Click **Search** and select **STMI**. Click **Execute** on the **Action** pull-down menu, select **Restart** and confirm with **OK**.

	`CHANGE-CGWB:MTYPE=CGW,TYPE=GWDATA,LTU=3,SLOT=91,GWID1=INTGW001;`
	The HG 3500 must be restarted in order for this change to become effective. Use
	`RESTART-BSSU:ADDRTYPE=PEN,LTU=3,SLOT=91;`
	for this.

IMPORTANT: Established **connections are cleared down as a result!**

Table 22: AMO CGWB parameters in the CHANGE branch under MTYPE=CGW, TYPE=GWDATA

AMO	Parameter	Sprache/ Language	Beschreibung/ Description
CGWB	LTU	d	LTU-Nummer des Rahmens, in dem die HG 3500 gesteckt ist.
	LTU	e	Line/Trunk Unit Number of the shelf where the HG 3500 is plugged.
	EBT	d	Einbauteilung des Steckplatzes der HG 3500
	SLOT	e	Slot where the HG 3500 resides.

AMO	Parameter	Sprache/ Language	Beschreibung/ Description
	GWID1	d	Gateway Identifikation 1. Teil Die Gateway Identifikation ist der 1. Teil einer beliebigen 64 Zeichen langen Zeichenkette. Die Eingabe ist CASE-sensitiv.
	GWID1	e	Gateway Identifikation 1. part A gateway identification is the 1. part of an idividual 64 character long characterstring. The input is CASE-sensitive.
STMIB	GWID2	d	Gateway Identifikation 2. Teil Die Gateway Identifikation ist der 2. Teil einer beliebigen 64 Zeichen langen Zeichenkette. Die Eingabe ist CASE-sensitiv.
STMIB	GWID2	e	Gateway Identifikation 2. part A gateway identification is the 2. part of an idividual 64 character long characterstring. The input is CASE-sensitive.

Resetting the parameters to default values

You can reset the initialization settings with the command:

```
CHANGE-CGWB:MTYPE=INITCGW,TYPE=GWDATA;
```

TYPE LEGKDATA - Changing the gateway directory number

	**Configuration Management > System Data > Board > Board** Click **Search** and select **Board Name=STMI2**, **Board Name=STMI4, Board Name=STMIX or Board Name=STMIY**. Make the settings on the **STMI2-IGW Board Data** tab and **Save**. **Configuration Management > System Data > Maintenance > Board Maintenance** Click **Search** and select **STMI**. Click **Execute** on the **Action** pull-down menu, select **Restart** and confirm with **OK**.

	`CHANGE-CGWB:MTYPE=CGW,TYPE=LEGKDATA,LTU=3,SLOT=91,GWNO=3,GWDIR►NO=354711;`
	The HG 3500 must be restarted in order for this change to become effective. Use
	`RESTART-BSSU:ADDRTYPE=PEN,LTU=3,SLOT=91;`
	for this.

IMPORTANT: Established **connections are cleared down as a result!**

Table 23: AMO CGWB parameters in the CHANGE branch under MTYPE=CGW, TYPE=LEGKDATA

AMO	Parameter	Sprache/ Language	Beschreibung/ Description
CGWB	LTU	d	LTU-Nummer des Rahmens, in dem die HG 3500 gesteckt ist.
	LTU	e	Line/Trunk Unit Number of the shelf where the HG 3500 is plugged.
	EBT	d	Einbauteilung des Steckplatzes der HG 3500
	SLOT	e	Slot where the HG 3500 resides.
	GWNR	d	Gateway Nummer Die Gateway Nummer dient zur Identifikaiton der HG 3500 und ist immer erforderlich, wenn ein Gatekeeper an der lokalen PBX betrieben wird. Verfügt die lokale PBX über keinen Gatekeeper so wird auch keine Gateway Nummer benötigt Der Default-Wert ist 0 (dezimal)
	GWNO	e	Gateway number A gateway number is used to identify a HG 3500 and it necessary, when a gatekeeper is operating on the lokal PBX. Is there no gatekeeper working on the lokal PBX then no gateway number is needed Default value is 0 (decimal)
	GWRNR	d	Gateway Rufnummer Legt eine Rufnummer fest, mit der das Gateway an der lokalen PBX erreichbar ist. Die Rufnummer muß eigens mit dem AMO WABE und Kennzahlpunkt QUER eingerichtet werden.
	GWSTNO	e	Gateway station number Assigns an access code, with which a gateway can be reached on the local PBX. The access code must be specially configured with AMO WABE and DAR = QUER.

AMO	Parameter	Sprache/ Language	Beschreibung/ Description
	REGEXTGKd		Gateway Registrierung an einem remote Gatekeeper Damit wird gesteuert, ob sich ein Gateway an einem remote Gatekeeper registrieren darf.
	REGEXTGKe		Gateway registration at remote gatekeeper Controls, if a gateway is permitted to register at a remote gatekeeper.

Resetting the parameters to default values

Resetting the CGWB parameters for the LEGKDATA is neither helpful nor supported. You can only set other values with the command:

```
CHANGE-CGWB: MTYPE=STMI2IGW,TYPE=LEGKDATA, ..... ;
```

TYPE DMCDATA - Changing the number of DMC connections

	**Configuration Management > System Data > Board > Board** Click **Search** and select the board. Make the settings on the **STMI Board Data** tab and **Save**. **Configuration Management > System Data > Maintenance > Board Maintenance** Click **Search** and select **STMI**. Click **Execute** on the **Action** pull-down menu, select **Restart** and confirm with **OK**.

	`CHANGE-CGWB:MTYPE=CGW,TYPE=DMCDATA,LTU=3,SLOT=91,DMCCONN=8;`
	The HG 3500 must be restarted in order for this change to become effective. Use
	`RESTART-BSSU:ADDRTYPE=PEN,LTU=3,SLOT=91;`
	for this.

IMPORTANT: Established **connections are cleared down as a result!**

Table 24: AMO CGWB parameters in the CHANGE branch under MTYPE=CGW, TYPE=DMCDATA

AMO	Parameter	Sprache/ Language	Beschreibung/ Description
CGWB	LTU	d	LTU-Nummer des Rahmens, in dem die HG 3500 gesteckt ist.

AMO	Parameter	Sprache/ Language	Beschreibung/ Description
	LTU	e	Line/Trunk Unit Number of the shelf where the HG 3500 is plugged.
	EBT	d	Einbauteilung des Steckplatzes der HG 3500
	SLOT	e	Slot where the HG 3500 resides.
	DMCCONN	d	Anzahl der möglichen DMC Verbindungen Legt den Maximalwert der möglichen DMC Verbindungen für die HG 3500 fest.
	DMCCONN	e	Number of possible DMC connections Assigns the maximum number of possible DMC connections for the HG 3500.

Resetting the parameters to default values

You can reset the initialization settings with the command:

```
CHANGE-CGWB:MTYPE=INITCGW,TYPE=DMCDATA;
```

TYPE GLOBIF - Changing the default router IP address

	**Configuration Management > System Data > Board > Board** Click **Search** and select the board. Make the settings on the **STMI2-IGW Board Data** tab and **Save**. **Configuration Management > System Data > Maintenance > Board Maintenance** Click **Search** and select **STMI**. Click **Execute** on the **Action** pull-down menu, select **Restart** and confirm with **OK**.

	`CHANGE-CGWB:MTYPE=CGW,TYPE=GLOBIF,LTU=3,SLOT=91,DE▶FRT=192.168.1.254;`
	The HG 3500 must be restarted in order for this change to become effective. Use
	`RESTART-BSSU:ADDRTYPE=PEN,LTU=3,SLOT=91;`
	for this.

IMPORTANT: Established **connections are cleared down as a result!**

Table 25: AMO CGWB parameters in the CHANGE branch under MTYPE=CGW, TYPE=GLOBIF

AMO	Parameter	Sprache/ Language	Beschreibung/ Description
CGWB	LTU	d	LTU-Nummer des Rahmens, in dem die HG 3500 gesteckt ist.
	LTU	e	Line/Trunk Unit Number of the shelf where the HG 3500 is plugged.
	EBT	d	Einbauteilung des Steckplatzes der HG 3500
	SLOT	e	Slot where the HG 3500 resides.
	DEFRT	d	IP-Adresse der Default Routers Der Default-Wert ist 0.0.0.0
	DEFRT	e	Default router IP-address Default value is 0.0.0.0

Resetting the parameters to default values

You can reset the initialization settings with the command:

```
CHANGE-CGWB:MTYPE=INITCGW,TYPE=GLOBIF;
```

TYPE GKDATA - Changing IP addresses for primary and secondary gateways

This step is only necessary if there is no gatekeeper configured on the local OpenScape 4000 system and a gateway should register at a foreign PBX's gatekeeper. Use this command to enter the IP addresses of the relevant gateways.

	Configuration Management > System Data > IPDA > IPDA Access Point Click **Search** and select the access point, change data and **Save**.

	`CHANGE-CGWB:MTYPE=CGW,TYPE=GKDATA,LTU=3,SLOT=91,PRIGK►IP=192.168.1.90,PRIGKPN=1719,PRIGKID1=PRIMARYRASMANAGERID;`
	In this case, only a primary gatekeeper is assigned.
	The HG 3500 must be restarted in order for this change to become effective. Use
	`RESTART-BSSU:ADDRTYPE=PEN,LTU=3,SLOT=91;`

IMPORTANT: Established **connections are cleared down as a result!**

Table 26: AMO CGWB parameters in the CHANGE branch under MTYPE=CGW, TYPE=GKDATA

AMO	Parameter	Sprache/ Language	Beschreibung/ Description
CGWB	LTU	d	LTU-Nummer des Rahmens, in dem die HG 3500 gesteckt ist.
	LTU	e	Line/Trunk Unit Number of the shelf where the HG 3500 is plugged.
	EBT	d	Einbauteilung des Steckplatzes der HG 3500
	SLOT	e	Slot where the HG 3500 resides.
	PRIGKIP	d	IP Adresse der HG 3500 des primär anzusprechenden Gatekeeper Jeder Gatekeeper wird durch eine IP-Adresse adressiert.
	PRIGKIP	e	IP address of the HG 3500 for the primary addressed gatekeeper Every gatekeeper is addressed by it’s own IP address
	PRIGKPN	d	Portnummer der HG 3500 Die Portnummer für HG 3500 ist standardmäßig 1719.
	PRIGKPN	e	Portnumber of HG 3500 The default portnumber for a HG 3500 is .1719.
	PRIGKID1	d	ID des primär anzusprechenden Gatekeeper - 1. Teil Der Default-Wert ist “PrimaryRASManagerID“. Die Eingabe ist CASE-sensitiv.
	PRIGKID1	e	ID of the primary addressed gatekeeper - 1. part Default value is “PrimaryRASManagerID“. The input is CASE-sensitive.
	PRIGKID2	d	ID des primär anzusprechenden Gatekeeper - 2. Teil Die Eingabe ist CASE-sensitiv.
	PRIGKID2	e	ID of the primary addressed gatekeeper - 2. part The input is CASE-sensitive.

AMO	Parameter	Sprache/ Language	Beschreibung/ Description
	SECGKIP	d	IP Adresse der HG 3500 des sekundär anzusprechenden Gatekeeper Jeder Gatekeeper wird durch eine IP-Adresse adressiert.
	SECGKIP	e	IP address of the HG 3500 for the secondary addressed gatekeeper Every gatekeeper is addressed by it's own IP address

Resetting the parameters to default values

You can reset the initialization settings with the command:

```
CHANGE-CGWB: MTYPE=INITCGW,TYPE=GKDATA;
```

Display:

AMO BCSU

When configuring a HG 3500, the distribution and number of available IP connections (B channels) is defined with the HG 3500 FCTID in the AMO BCSU.

In contrast to NCUI4 and STMI2/4 and STMIX/Y, no supplementary information, such as IP address, B channels, etc., is output for a HG 3500 gateway.

	Displaying can be performed with the OpenScape 4000 Assistant/Manager, Boards window.
	`DISPLAY-BCSU:TAB,1,LTU Number,Slot;` The AMO outputs typical board data for the common gateway.

```
DIS-BCSU:TBL,1,3,91;
H500:  AMO BCSU STARTED
 ADDRESS :  LTG  1   LTU 3    SOURCE GROUP 1
-----+----------+--------+---+-+-+---+-+-----------+-----------+----------|
     |          |        |   |S|H|AL-| |           |           |          |
     | ASSIGNED  | MODULE |FCT|E|W|ARM| | INSERTED  |    HW-    | MODULE   |
 PEN | MODULE    | TYPE   |ID |C|Y|NO | | MODULE    |STATE INFO | STATUS   |
-----+----------+--------+---+-+-+---+-+-----------+-----------+----------|
  91 | Q2316-X10  STMI2      1   A   0|*| Q2316-X10  | -05 -     | READY    |
     +-----------------------------------+-+-----------+-----------+----------|
     | IP ADDRESS : 192.168.  1. 11         B-CHANNELS : 120    BCHLCNT : 120 |
     | BLOCK NO   :   1                     PRERESERVED LINES ASSIGNED :   NO |
     |  1. FUNCT  : STMI2-IPGW    1 LINES   B-CHANNELS :  30    BCHLCNT :  30 |
     +-----------------------------------+-+-----------+-----------+----------|
```

AMO CGWB

	Displaying with the AMO CGWB can only be executed in expert mode. Expert Mode > Expert Access > Open ...<IP> with AMO (see AMO command)
	`DISPLAY-CGWB:CGW,<LTU Number>,<Slot>;` The AMO outputs all HG 3500 specific data.

Values must be configured for the following data to ensure correct operation:

1) Ethernet interface

- Gateway data
- Gatekeeper-specific data

Delete:

AMO BCSU

	Deletion with the AMO BCSU can only be executed in expert mode. Expert Mode > Expert Access > Open ...<IP> with AMO (see AMO command)
	`DELETE-BCSU:PER,,LTU Number,Slot,Part Number;` The AMO deletes the specified board from the OpenScape 4000 system.

AMO CGWB

The AMO does not feature a DELETE branch. The configuration data modified with the AMO CGWB (TYPE=LEGKDATA) for a local gateway is deleted when deleting the AMO GKREG.

This data can be restored at any time with the AMOs CGWB and GKREG.

Resetting the parameters to default values:

- Resetting the CGWB parameters for the LEGKDATA is neither helpful nor supported.
- You can reset the initialization settings for individual data types with the command:

`CHANGE-CGWB:MTYPE=INITCGW,TYPE=<param>;`

- You can reset the initialization settings for all data types with the command:

`CHANGE-CGWB:MTYPE=INITCGW,TYPE=ALL;`

7.3.5.1.2 Configuring HG 3500 Circuits

You must configure the appropriate number of circuits for every common gateway board based on its configuration (see AMO BFDAT: parameter FCTBLK). As for all circuits, the AMO TDCSU is used for this.

Please note that this step requires a number of HG 3500 specific parameters that are grouped together for all AMO commands in the branch EVN=HG3550IP.

The parameter **DMCALLWD** is used to define whether or not this circuit can be used in a direct media connection.

Please note that you may have to configure the necessary circuit data (for example, circuit and line parameters, trunk groups, etc.) in advance using the relevant AMOs.

Each circuit in HG 3500 must have a separate trunk group.

7.3.5.1.3 Changing the HG 3500 Gateway Registration

The OpenScape 4000 system does not support a direct change of the gateway registration type from remote to internal gatekeeper, and vice versa. Furthermore, the AMO ZANDE parameter **GATEKPR** must not be changed while a gateway is configured. This may cause major disruptions during operation!

Since the AMO CGWB has no DELETE branch, the AMO BCSU must be used to delete the internal HG 3500 configuration data and the extended board data.

- In a PBX **with/without** gatekeeper, the HG 3500 gateway(s) must always be deleted first and then reconfigured. Please note that in such a case all gateways will be registered either internally (PBX with gatekeeper) or remotely (PBX without gatekeeper).

  – Changing registration of gateway(s) from “internal“ to “remote“:

  Delete gateway(s) with AMO GKREG and AMO BCSU, change the **GATEKPR** parameter to **NO** and reconfigure the gateway with AMO BFDAT, AMO BCSU and AMO CGWB.

  – Change registration of gateway(s) from “remote“ to “internal“:

  Delete the gateway(s) with AMO GKREG and AMO BCSU, change the GATEKPR parameter to YES and reconfigure the gateway with AMO BFDAT, AMO BCSU, AMO CGWB and AMO GKREG.
- In a PBX **with** gatekeeper, the registration of some special, local gateway(s) can be changed from internal to remote:
- Delete the gateway data with AMO GKREG and then reconfigure the gateway with AMO CGWB (REGEXTGK=YES) !
- In a PBX **with** gatekeeper, an additional, local gateway can be configured for remote registration:
- Configure the gateway with AMO BFDAT, AMO BCSU and AMO CGWB (**REGEXTGK=YES**)!

7.3.6 Configuring the HG 3500 Directory Number

Every HG 3500 requires a directory number with which it can be contacted in the gatekeeper’s OpenScape 4000 system. The AMO CGWB presents the directory number to the HG 3500 (command: `ADD-CGWB:MTYPE=CGW,LTU=<number>,SLOT=<number>,TYPE=LEGKDATA,GWDIRNO=<directory number>;`).

A HG 3500 that has to register at a foreign OpenScape 4000 system with gatekeeper does not have to have an entry its own OpenScape 4000 system’s digit analysis scheme. However, the directory number must be configured under the GATEWAY digit analysis result or, if the number contains more than six digits, in the LCR in the system **with** gatekeeper.

The DPLN entry for a remote HG 3500 at the OpenScape 4000 system with gatekeeper requires the associated gateway number as supplementary information. This is administered, that is, the relevant DPLN entry is entered or deleted with the AMO GKREG in the course of configuration or deletion. This ensures that operation can only start if the gateway is correctly configured in the LEGK administration.

The HG 3500s own directory number must come from the station's numbering plan.

The gateway directory number must be configured under the TIE digit analysis result (TSC connection) in a HG 3500 that has to register at the local OpenScape 4000. A gateway number is not essential as supplementary information in this case.

The DPLN entry for a HG 3500 (GATEWAY digit analysis result) can only be deleted after the gateway number has been removed. Use the AMO GKREG to delete the gateway from the LEGK administration.

Generation

AMO WABE

Configure the directory number of a **remote** HG 3500 in the local system, that is, the gateway must register at the local LEGK. In this case, the gateway must be configured with the GATEWAY digit analysis result.

	Configuration can be performed with OpenScape 4000 Assistant/ Manager in the Extension window (TYPE=GATEWAY).
	`ADD-WABE:CD=35101,DAR=GATEWAY;` For the predefined traffic situations, the remote gateway's directory number (35101) is configured as the gateway digit analysis result in the digit analysis scheme.

Configure the directory number of a remote HG 3500 in the system with gatekeeper, that is, the gateway can register at the local gatekeeper. In this case, the gateway must be configured with the TIE digit analysis result.

	Configuration can be performed with OpenScape 4000 Assistant/ Manager in the Extension window (TYPE=TIE).
	`ADD-WABE:CD=452001,DAR=TIE;` For the predefined traffic situations, the local gateway's directory number (452001) is configured as the tie line digit analysis result in the digit analysis scheme.

Display:

	Configuration can be performed with OpenScape 4000 Assistant/ Manager in the Extension window.
	`DISPLAY-WABE:GEN,Directory Number;` The AMO outputs data on the specified directory number.

Delete:

	Configuration can be performed with OpenScape 4000 Assistant/ Manager in the Extension window.
	`DELETE-WABE:CD,Station Number,,Digit Analysis Result;` The AMO deletes the required directory number for the specified digit analysis result.

7.3.7 Configuring IP Trunking in the LCR

When resolving addresses for TDM connections, an LCR route is administered as destination address information and is subsequently used to determine the LODEN of a remote circuit for CO or TIE connections.

To satisfy the requirements of IP address resolution, new parameters for destination gateways (GW1 to GW5) are administered in the LCR data with the AMO LDAT. Information on destination gateways 1...5 consists of:

1) the gateway number

the sector path number

The gateway number can be used to determine the IP address of the destination gateway and therefore to reach every required OpenScape 4000 system in the customer’s IP network.

Enter all sectors to be crossed between the source and destination gateway under the sector path number. It does not contain the sector numbers of the source and destination gateway.

There are no multiple paths for this path type. In other words, there is only one defined path. To avoid having to configure an unnecessary number of sector paths, you can also specify a sector path that was defined for DMC here. If this is a multiple path, a search is performed here for the correct sector path segment. For the sake of clarity, however, separate sector paths should be defined for IP trunking and DMC.

The IP address resolution administration concept is embedded in the existing LCR device search and can be performed with the same AMOs (namely the AMOs RICHT, LDAT, and LDPLN).

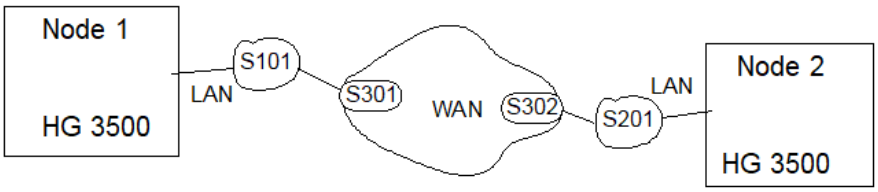


Figure 153: Example for sector path description

An outgoing seizure from gateway S13 to gateway S23 uses the following sector path:

1) S13 > S23: S101,S301,S302,S201

Generation

AMO RICHT

Use the branch MODE=LRTENEW to configure the LCR route for IP trunking. Alternatively, the trunk group number can be left out when configuring IP address resolution for a remote gateway (OpenScape 4000 system without gatekeeper) because B channels do not have to be seized at the gatekeeper's PBX in this case.

	Configuration can be performed with OpenScape 4000 Assistant/Manager in the LCR Route window.
	`ADD-RICHT:MODE=LRTENEW,LRTE=35,LSVC=ALL,NAME="STMI2 3-91",DNNO=1-69-300,REROUT=NO,ROUTATT=NO, EMCYRTT=NO,PDNNO=10-69-300, CHARCON=NEUTRAL,CONFTONE=NO,RERINGRP=NO;` Route 35 is configured on PEN 3-91 for all services for HG 3500; no trunk group number was entered.

AMO LDAT

Use this AMO to configure the necessary LCR route elements for IP trunking for an LCR route.

Every route element can contain up to five destination gateways from remote OpenScape 4000 systems. The parameters GW1 through GW5 define the connection setup sequence, that is, first the path described in GW1 and so on until finally the path in GW5.

If five destination gateways is not sufficient, then a new route element must be configured and in addition, the value LRTGCONT must be specified in the parameter LATTR. This creates five additional destination gateways for the same route element. All data associated with the route element already created is automatically adopted independently of the current AMO input.

As in the past, multiple route elements can also be configured with different LCR parameters for an LCR route. In this case, the parameter LATTR must not contain the value LRTGCONT.

The trunk group number can be left out. If a trunk group number is specified, all trunk-group-specific data is also adopted.

	Configuration can be performed with OpenScape 4000 Assistant/Manager in the LCR Route Element window.
	ADD-LDAT:LROUTE=35,LSVC=ALL,LVAL=1,ODR=2,LAUTH=1,CARRIER=1,ZONE=TIE01,LATTR=WCHREG,VCCYC=4,GW1=1-1; A route element is created for route 35 with path data for destination gateway 1. ADD-LDAT:LROUTE=35,LVAL=1,ODR=2,LAUTH=1,LATTR=LCRCONT,GW1=6-16; If the path data for all five destination gateways is entered in a route element for route 35, this follow-up command can be used to create another route element with the path data, for example, for the sixth destination gateway.

AMO LDPLN

Use this AMO to configure the LCR digit pattern for each destination gateway in the OpenScape 4000 systems in a customer network.

Up to 2,048 dial plans can be configured. But first, the required dial plan numbers must be administered with the AMO LDPLN. Dial plan number 0 is an exception. This configures fixes and cannot be administered in the branch LCRCOS=LCRADM. Random digit patterns can be configured here immediately.

If you want to save the LCR digit pattern under a dial plan number other than 0, then this must be configured before the first entry. The branch LCRCONF=LCRVADM is used for this. In the following AMOs, the user only uses the dial plan number (0-2047).

A dial plan number greater than the permanently set plan 0 is usually only needed if a gatekeeper is configured at the local system.

	Configuration can be performed with OpenScape 4000 Assistant/Manager in the LCR Digit Pattern window.
	ADD-LDPLN:LCRCONF=LCRADM, DIPLNUM=2,LWMPOOL=1; Dial plan number 2 is configured on the first unused dial plan in LCR digit pattern pool 1.

Use the following step to configure the required digit pattern.

	Configuration can be performed with OpenScape 4000 Assistant/Manager in the LCR Digit Pattern window.
	ADD-LD▶ PLN:LCRCONF=LCRPATT,DIPLNUM=2,LDP="00891242390",LAUTH=1,PINP=N; The digit pattern 00891242390 is created under dial plan number 2.

A digit pattern that leads to a gateway is an exception.

If a gateway directory number cannot be resolved with the dial plan (DPLN), it must be administered in the LCR dial plan DIPLNUM=0. The following command is required for this (see also Section 3.6, “Configuring the HG 3500 Directory Number”, on page 567).

	Configuration can be performed with OpenScape 4000 Assistant/Manager in the LCR Digit Pattern window.

	`ADD-LDPLN:LCRCONF=LCRPATT,DIPLNUM=0,LDP="008973114711",GW►`
	`NO=7,LAUTH=3;`
	The gateway directory number 008973114711 is assigned to destination gateway 7.

Display:

AMO RICHT

	Displaying can be performed with OpenScape 4000 Assistant/ Manager in the LCR Route window.
	`DISPLAY-RICHT:MODE=LRTE,LRTE=35;` The AMO outputs the LCR routing data for LRTE 35.

AMO LDAT

	Displaying can be performed with OpenScape 4000 Assistant/ Manager in the LCR Route Element window.
	`DISPLAY-LDAT:KIND=LCR,LROUTE=35;` The AMO outputs the routing data configured for all configured route elements for LCR route 35.

AMO LDPLN

Display the internal administration configuration for dial plan number 2.

	Displaying can be performed with OpenScape 4000 Assistant/ Manager in the LCR Digit Pattern window.
	`DISPLAY-LDPLN:LCRCONF=LCRADM,DIPLNUM=2;` The AMO outputs the administrative data LWMPOOL, DIALPLN and INFO for dial plan number 2.

Displaying the digit pattern configured for gateway 7.

	Displaying can be performed with OpenScape 4000 Assistant/ Manager in the LCR Digit Pattern window.
	`DISPLAY-LDPLN:LCRCONF=LDP,GWNO=7;` The AMO outputs the digit pattern data configured for gateway 7.

Delete:

AMO RICHT

	Deletion can be performed with OpenScape 4000 Assistant/ Manager in the LCR Route window.
	`DELETE-RICHT:MODE=LRTE,LRTE=35;` The AMO deletes LCR route 35.

AMO LDAT

	Deletion can be performed with OpenScape 4000 Assistant/ Manager in the LCR Route Element window.

	`DELETE-LDAT:KIND=LROUTE,LROUTE=35;`
	The AMO deletes all route elements and data for LCR route 35.
	OR
	`DELETE-`
	`LDAT:KIND=LRTEL,LROUTE=35,LRTEL=1,GWIDX=2;`
	The AMO deletes only the second gateway entry for LCR route 35 in route element 1.

The last gateway in an LCR route element cannot be deleted with GWIDX. In this case, the entire route element (LRTEL) must be deleted.

AMO LDPLN

Delete the internal administration configuration for dial plan number 2.

A dial plan number can only be deleted after all digit patterns have been deleted.

	Deletion can be performed with OpenScape 4000 Assistant/ Manager in the LCR Digit Pattern window.
	`DELETE-LDPLN:LCRCONF=LCRADM,DIPLNUM=2;` The AMO deletes dial plan number 2. Data can no longer be accessed on these dial plans. Dial plan number 2 should be reconfigured when next required.

Delete the digit pattern configured for a dial plan number.

	Deletion can be performed with OpenScape 4000 Assistant/ Manager in the Extension window.

	`DELETE-`
	`LDPLN:LCRCONF=LCRPATT,DIPLNUM=6,LDP="0307469412";`
	The AMO deletes the digit pattern 0307469412 configured for gateway 6.

7.3.8 Configuring Circuits and Terminals

7.3.8.1 Configuring Circuits

This feature does not change the underlying configuration of the analog (AMO TACSU) and digital line trunks (AMO TDCSU) or special circuits (TSCSU).

Parameter **CLASSMRK** is set to „HG3550: Bandwidth control for integrated HG 3550 IP gateway“.

7.3.8.2 Configuring Terminals

This feature does not change the underlying configuration of the terminal data (AMO SDAT) and attendant console (AMO ACSU).

Parameter **CLASSMRK** is set to „HG3550: Bandwidth check for HG 3550 IP trunk“.

The parameter **IPCODEC** was also added to the AMO SBCSU. This can be used to set the codec type for IP terminals. The value G711PREF is designed as the default value for STMI2/4/STMIX/STMIY-HFA terminals.

7.3.9 Changing the System Bandwidths

You can use the AMO SIPCO to change the default bandwidths set for IP connections under TYPE=BANDW.

A default bandwidth (in kilobits) established on the basis of previous experience was permanently set in the existing table for every codec type and sample size. These values can be changed with the AMO SIPCO.

Add:

Example: Change the setting for entry no. 3 to 90 kilobits

	**Configuration Management > System Data > IPDA > IPDA System Data** Click **Search**, deactivate the **Enable Autonegotiation** check box under **Type of Service** on the **Bandwidth Data** tab, enter **Speed** and **Mode**, and **Save**.
	`CHANGE-SIPCO:TYPE=BANDW,TBLIDX=3,BWRES=90;` This command changes the bandwidth for index 3 to 90 kilobits.

Example: Restore the default values for the entire table

	
	`CHANGE-SIPCO:TYPE=BANDW,TBLIDX=0,STANDBW=Y;` This command resets the entire table to the defined system bandwidths.

Table 27: AMO SIPCO parameters in the CHANGE branch under TYPE=BANDW

AMO	Parameter	Sprache/ Language	Beschreibung/ Description
SIPCO	TBLIDX	d	Index eines Eintrages in der Bandbreitentabelle
	TBLIDX	e	Index of an entry in the bandwidth encoding time table
	BWRES	d	neuer Wert für reservierte Bandbreite in kBit
	BWRES	e	new value for reserved bandwidth in kBit
	STANDBW	d	Rücksetzen auf Standardwerte Wird BWRES=0 angegeben so wird die gesamte Tabelle auf die Standardwerte zurückgesetzt sonsten nur der angegebene Index.
	STANDBW	e	reset to default values Is BWRES=0 entered then the whole table is reset to the default values, otherwise only the entered tableindex..

Delete:

Example: Delete index 5 in the system bandwidth table

	
	`DELETE-SIPCO:TYPE=BANDW,TBLIDX=5;` This command deletes the bandwidth for table index 5.

Table 28: AMO SIPCO parameters in the DISPLAY branch under TYPE=BANDW

AMO	Parameter	Sprache/ Language	Beschreibung/ Description
SIPCO	TBLIDX	d	Index eines Eintrages in der Bandbreitentabelle
	TBLIDX	e	Index of an entry in the bandwidth encoding time table

Display:

Example: Output the set system bandwidth table

	
	`DISPLAY-SIPCO:TYPE=BANDW;` This command outputs all configured entries from the system bandwidth table.

Table 29: AMO SIPCO parameters in the DISPLAY branch under TYPE=BANDW

AMO	Parameter	Sprache/ Language	Beschreibung/ Description
SIPCO	TBLIDX	d	Index eines Eintrages in der Bandbreitentabelle
	TBLIDX	e	Index of an entry in the bandwidth encoding time table

8 HiPath Feature Access (HFA)

8.1 Overview

The HG 3500 gateway provides IP phones and analog devices access to the full range of OpenScape 4000 features via CorNet IP.

The HG 3500 provides the following features and benefits:

- Provides the full OpenScape 4000 feature set to the following IP phones:
  - optiPoint 4x0 CorNet IP
  - OpenStage family,
  - AP 1120 analog adapter (For more details please refer to the E-Doku pages in the intranet (http://apps.g-dms.com:8081/edoku/jsp/searchresult_v2.jsp?edokutype=&search_mode=product&product=AP%201120&product_version_main=&product_version_sub=&search_term_type=all&
- The HG 3500 line gateway supports direct media connections between IP clients resulting in highest quality voice and minimal delays.
- High voice quality. On account of longer voice signal delays caused by the system in the IP network, voice quality will be impaired by echo unless this is removed prior to transmission. The HG 3500 therefore feature an integrated echo canceller.
- The HG 3500 provides a 10BT/100BT IP network interface and supports up to 240 IP phones off a single gateway.
- Lower bandwidth requirements.
- The HG 3500 supports all phone adapters that do not require their own b channel (not supported are: phone adapter, a/b adapter, S0 adapter, V.24 adapter).
- The HG 3500 supports gateways that protect multiple gateways against failure.
- The HG 3500 supports mobility including support for E911.
- Supports central administration via OpenScape 4000 Management identical to traditional subscribers.
- Support for IP phones provides user mobility and greatly simplified MAC.
- Takes advantage of existing IP infrastructure.
- Supports up to 12,000 IP subscribers off a single OpenScape 4000 including IP users on IP Access Points.
- Support for Quality of Service in the IP network through prioritization. The HG 3500 supports prioritization in the IP network on the basis of the following standards:
  - IEEE 802.1 p/q (VLAN Tagging) on Layer 2
  - IETF RFC 2474 (DiffServ) on the IP Layer
- Support of network management on the basis of SNMP. HG 3500 supports network management on the basis of the SNMP protocol. Statistical data from the applicable standard MIBs and additional data from proprietary MIBs can be queried.

8.2 Application Example

8.2.1 Feature Description

HiPath Feature Access (HFA) allows the smooth migration of the communication platform from a wire-connected to IP-based infrastructure. Consequently, it is sufficient for the customer just to install and operate an efficient Local Area Network (LAN) that supports Quality of Service (QoS). Data and voice communication share the available network bandwidth where the throughput rate is important for data traffic and the real-time capability is important for telephony. This means that, before the installation of an HFA system, the appraisal and actualization of the IP infrastructure regarding bandwidth and QoS-supporting LAN components (Router, Switch, Gateway) is crucial for the subsequent quality of the voice connections.

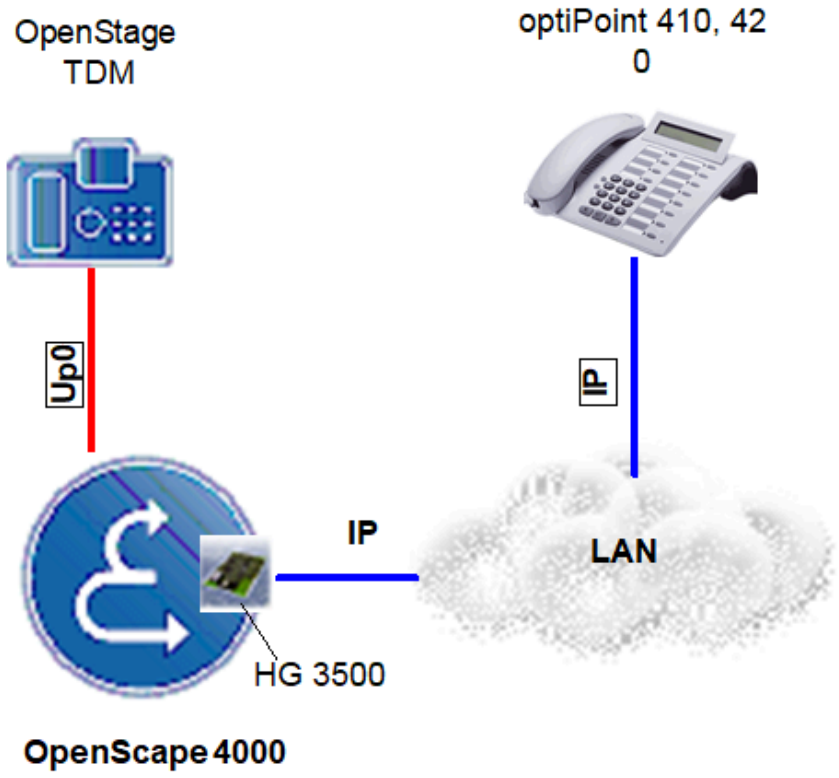


Figure 154: HFA infrastructure

To guarantee good voice quality even when the network is very busy the LAN segment that is used must consist of QoS-supporting LAN components. The use of a 100Mbit Ethernet is also recommended.

Supporting Quality of Service in the IP network through prioritization

1) IEEE 802.1 p/q (VLAN tagging) on Layer 2

- IETF RFC 2474 (DiffServ) on Layer 3.

There are no significant restrictions for the user, only Autoset-Relocate and Teleworking are not supported. Otherwise the IP terminals provide the same

functionality as UP0e-based terminals. However, no S0 or a/b adapters are supported.

G.711, G.723 and G.729 are supported with HG 3500. With a Direct Media Connection (DMC), the optiPoint 410 / 420 terminals also control G.722 with CD quality.

8.2.1.1 Technical background

In UP0e-based user connections the signaling connection (D channel) is separated from the voice connection (B channel) by subdividing the physical medium into time slots and assigning the two connections different time slots. In HFA, the two-wire line is replaced by an IP-based LAN as the physical medium of the digital user connection. The signaling connection between the terminal and HFA (Common) Gateway uses a secure TCP connection and the voice data are transferred via an H.323 connection using the RTP/RTCP protocol. Both connections can now be routed differently in a single LAN. This means it is possible for there to be signaling although the voice connection is temporarily interrupted.

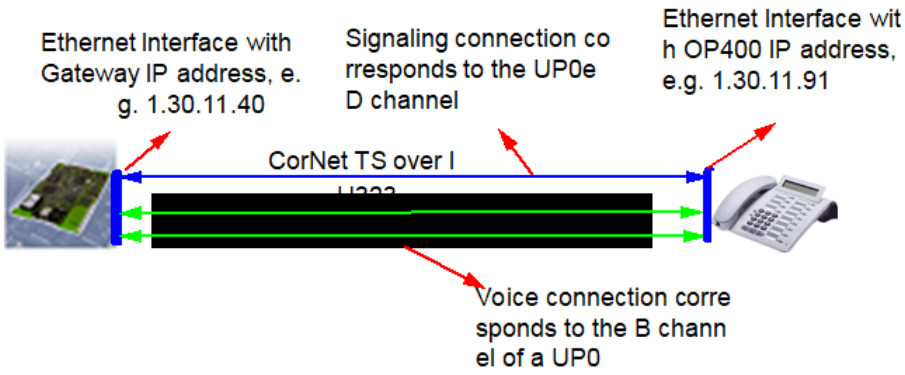


Figure 155: Technical relationship between UP0e and HFA user connection

In order to configure an HFA user, primarily it is necessary to determine the following points beforehand:

- IP address, subnetwork mask, subnetwork Gateway IP address of the Common Gateway
- IP address, subnetwork mask, subnetwork Gateway IP address of the HFA terminal

8.2.1.2 HFA user registration

Users are configured at a specific PEN (AMO SBCSU). While, however, a digital (or analog) terminal can go directly into operation after connecting to its module, in the case of an IP telephone settings must be first made at the terminal.

Firstly an HFA user needs a separate IP address, a subnetwork mask and - optionally - the specification of a default (customer network) router. In the case of a Soft Client, it has, of course, the advantage that it uses the network card of the PC and, consequently, no settings are required.

However, in the case of an HFA fixed device, the IP settings must be made. This is either done “automatically“ via DHCP (default setting of the HFA fixed terminals) or manually.

A HFA user with IP settings now attempts to register with the appropriate gatekeeper. Its gatekeeper is the HG 3500 at whose position it is configured. In order to find its “home“ HG 3500, its IP address must be set up at the terminal.

This alone, however, is not sufficient. The HG 3500 still has to check whether the user who is sending it a “Registration Request“ is actually authorized to register with it. The terminal must also send it the user number for checking the user identity. The HG 3500 then asks the OpenScape 4000 whether this user number is set up at its position. If it is, the HFA user is registered. If not, the HFA user is denied. Thus, the user number must be set up beforehand on the terminal.

To prevent a user simply registering himself with the subscriber number of another colleague, it is even possible to set up a so-called IP password (IPPASSW) in the AMO SBCSU. This can only be changed via the administrator, but not by the user at the terminal. If an IP password is set up in the AMO SBCSU, it must also be configured at the terminal. Otherwise, the subscriber is not registered.

Conclusion:

The IP address of the HG 3500, user number from the AMO SBCSU and, optionally, the IP password from the AMO SBCSU must be configured at the terminal. Otherwise, the HFA terminal will not be registered and, thus, will remain out of operation. The configuration of these data can take place at the terminal itself, via the WBM or via the DLS.

In case of a SoftClient, the respective configuration is made after the program is invoked.

Note:

In some customer networks it may also be necessary to preset the L2 prioritization and the VLAN ID at the HFA terminal. Here, however, it is also possible to automate this via DHCP.

Following successful registration, the HG 3500 transfers data concerning the HFA user to the AMO SBCSU such as, e.g. device type, IP address, etc. (AB-SBCSU / branch TYPE=OPTIDAT). These data can also be viewed in the UW7 via the Configuration Menu in the user overview!

In the following figure the registration for user 4711 has already been carried out. The other telephone has all IP settings, but is not yet registered.

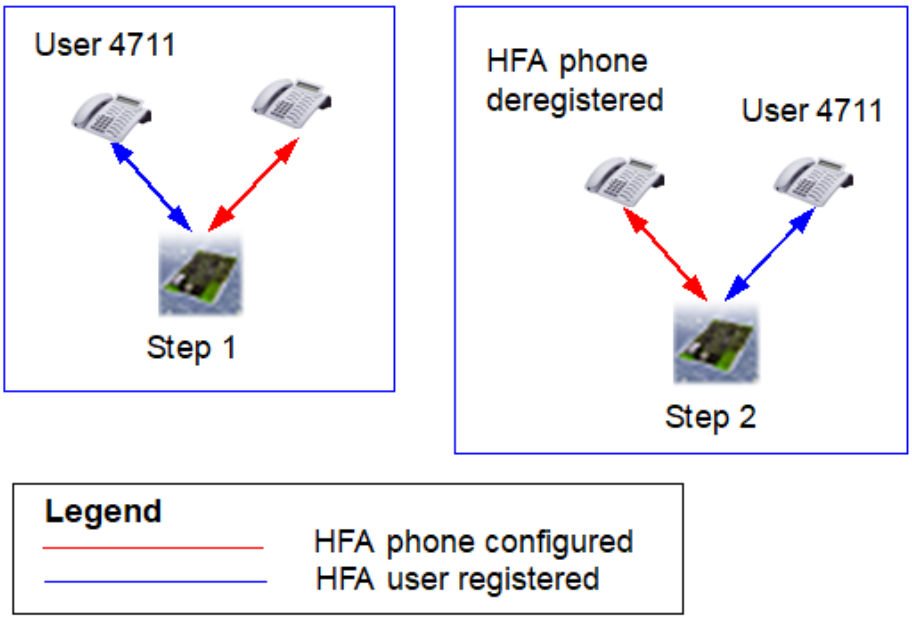


Figure 156: A user registers at another HFA phone

If an HFA user is already registered, he can change to another HFA terminal by registering there and declaring the IP address of his “home“ HG 3500, his user number and his optional IP password. The original terminal is automatically deregistered by the new registration. This is only not possible if there is an existing telephone connection to the original terminal. It is possible for HFA users to make the transfer to another terminal via a digit analysis result in the WABE. This means that the user at the terminal no longer needs to call up the hidden configuration menu for a transfer. How to set up “Mobile HFA” please refer to IP Solutions, “Mobile HFA Logon“.

8.2.2 User interface

The user interface for the administration of IP HFA terminals is specific to each terminal. More details are given in the administration handbooks for the relevant terminals and are not, therefore, included in this document.

To setup a HFA phone you can either use:

- direct administration at the phone or via WBM of the phone.
- Please refer to the appropriate documentation of your HFA phone (http://apps.g-dms.com:8081/techdoc/search_en.htm).
- OpenScape Deployment Service (DLS):
- Please refer to the documentation of the DLS (http://apps.g-dms.com:8081/techdoc/en/P31003S2330M1000176A9/index.htm).

The following parameters are mandatory for the phone to go into operation:

- fully qualified phone number (E.164)
- gateway (HG3500) address and port
- subscriber password

If a user has successfully registered, the same user interface is available as for the standard digital terminals.

8.2.3 Restrictions

The following functional restrictions apply:

- Autoset-Relocate is not usable for the HFA user
- Teleworking TW2.6 is not allowed for the HFA user
- No S0 or a/b adapter are supported

8.2.4 Generation

IMPORTANT: If T.38 is supposed to be used with AP 1120, G.711 must be configured as voice codec only, i.e. always in case a modem or fax is connected to an AP 1120 the only allowed codec in the AP 1120 has to set to G.711 (no option for compression).

Before the initial configuration of an HFA user, the memory configuration must be checked with the AMO-DIMSU:

TEST-DIMSU:LIST=Y;

Now to configure 4 modules, for example, the following configuration must be carried out:

ADD-DIMSU:TYPE=SYSTEM,CGW=4;

The G.711 code type setting (a law or µ law) of the IP voice data is carried out via the central system data (usually already correctly set):

CHANGE-ZAND:TYP=CONFC,CODE=<ALAW/ULAW>;

Now the configuration of the HG 3500 module can be started.

8.2.4.1 Configuration of the HG 3500 board

The configuration of the function blocks is carried out with AMO-BFDAT. In the following example an STMI4 (Q2324-X510) with 120 possible b-channels will be configured with HFA.

ADD-BFDAT:FCTBLK=6,FUNCTION=HG3530,BRDBCHL=BCHL120;

1) CHANGE-
BFDAT:CONFIG=CONT,FCTBLK=6,FUNCTION=HG3530,LINECNT=60,BCHLCNT=6
/*60 HG 3530 b-channels are configured

With the following command the configuration of the board is completed:

CHANGE-BFDAT:CONFIG=OK,FCTBLK=6,ANSW=YES;

The configuration of the module is carried out with the AMO BCSU.

ADD-BCSU:MTYPE=IPGW,LTG=1,LTU=3,SLOT=14,PARTNO="Q2324-X510",FCTID=1,LWVAR="0",FCTBLK=6,BCHL3530=60,ALARMNO=0;

For the configuration of the IP addresses, subnetwork masks, etc., the loadware is carried out via the AMO-CGWB.

ADD-CGWB:LTU=3,SLOT=14,SMODE=NORMAL,IPADR=172.28.145.240, NETMASK=255.255.255.0;

Now the module data and the circuit data have still to be loaded onto the module. This is done either by plugging in the STMI module after the generation with the AMO CGWB or using the command:

RESTART-BSSU:ADDRTYPE=PEN,LTG=1,LTU=3,SLOT=14,WTIME=<Wait time between switching off and switching on in seconds>;

8.2.4.2 Configuration of the HFA users

The HFA users (IP phones) can then be configured.

ADD-
SBCSU:STNO=<stno>,OPT=OPTI,CONN=IP2,PEN=1-3-14-0,DVCFIG=OPTIIP, COS1=33,COS2=30,LCOSV1=5,LCOSV2=1,LCOSD1=5,LCOSD2=1,DPLN=0,ITR=0, [IPPASSW=<Password>];

If a soft client has the special feature that it has TAPI 1st party as a feature, the following AMO SBCSU configuration is required:

ADD-
SBCSU:STNO=<stno>,OPT=OPTI,CONN=IP2,PEN=1-3-14-0,DVCFIG=OPTIIP&API, COS1=33,COS2=30,LCOSV1=5,LCOSV2=1,LCOSD1=5,LCOSD2=1,DPLN=0,ITR=0, APICLASS=TSX,[IPPASSW=<Password>];

Each HFA user can be issued with their own password for the registration which is determined by the Administrator and, similar to the PIN, cannot be administrated by the user himself. If no password is specified, the user call number is sufficient for the registration.

8.2.5 Generation via OpenScape 4000 Assistant

8.2.5.1 Setting up HG 3500 via the OpenScape 4000 Assistant

HG 3500 can be set up and administrated via the Configuration Management of the OpenScape 4000 Assistant.

First of all you have to set the function blocks (corresponding AMO: AMO BFDAT).

Start **Configuration Management - System Data - Board - CGW Function Block**.

Click the **Search** button to see which function blocks have already been configured. In the following screen 5 function blocks have been configured. You can display them by clicking through the object list.

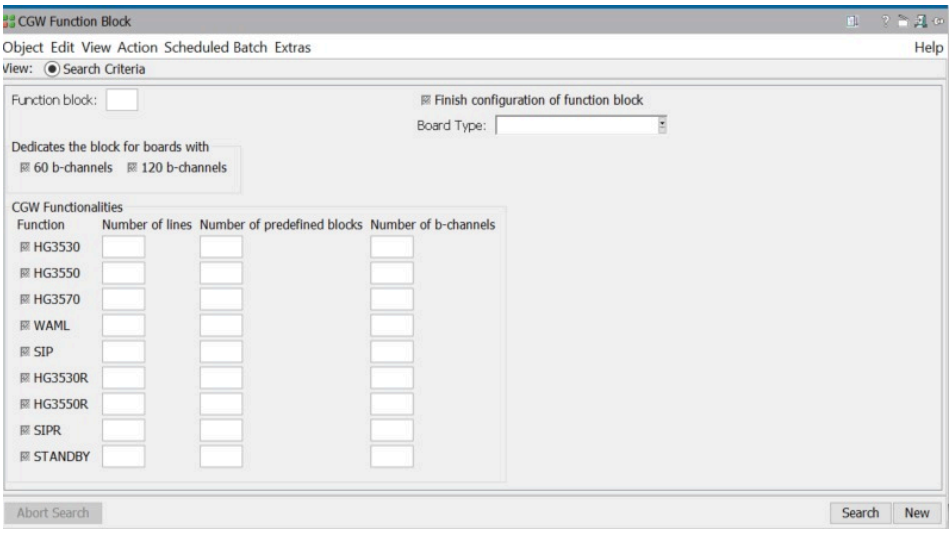


Figure 157: Configuration Management - System Data - Board - CGW Function Block - View Object

You also have the possibility to view them all in one table. Just select the radio button **Object List**.

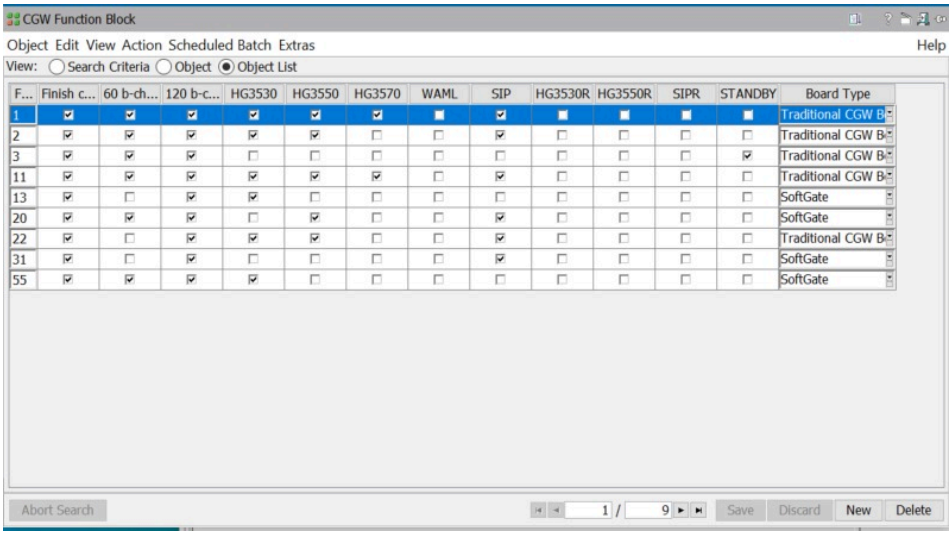
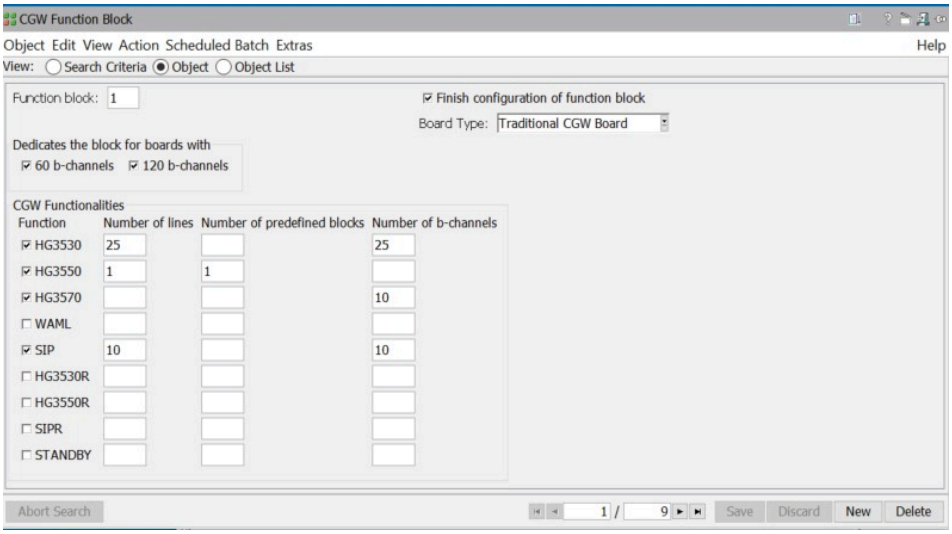


Figure 158: Configuration Management - System Data - Board - CGW Function Block - View Object List

To configure a new function block click **New**. Enter a free **Function block** number. Select the maximum number of b-channels of the common gateway board. Select the desired function(s) for this function block. Click **Save**. Now you have to enter the needed **Number of lines**, **Number of predefined blocks** and / or **Number of b-channels** for the selected functions. Click **Save** again. If you are done with the configuration of this function block select **Finish configuration of function block** and click **Save**.



Configuration Management - System Data - Board - CGW Function Block - Configure new Function block

Now you have to assign a common gateway board to the function block (corresponds to AMO BCSU). Start **Configuration Management - System Data - Board - Board**. Click **Search** to search for all boards configured in the system.

To configure a new common gateway board select the desired board (**Part number**) and click **New**. Enter the following data:

- LTU
- SLOT
- Part number
- Function ID (set always to 1)
- Board Name
- CGW Function block

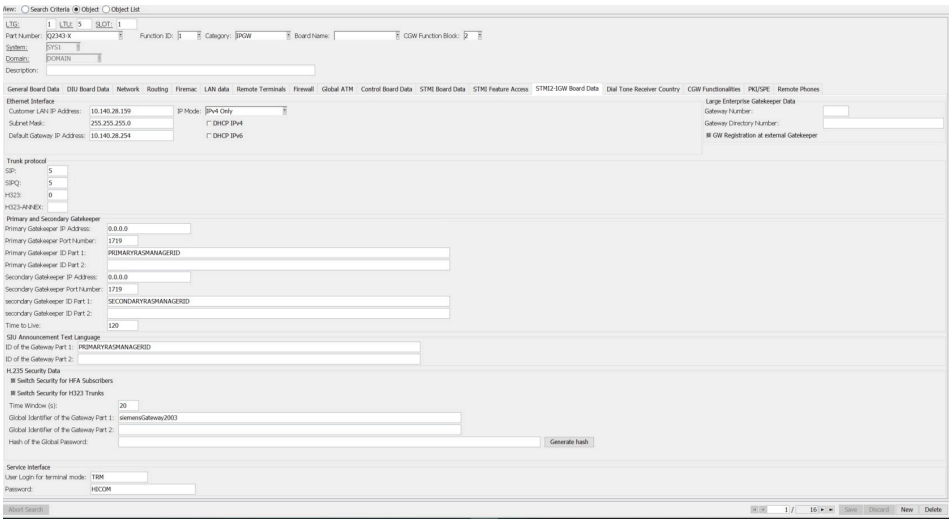


Figure 159: Configuration Management - System Data - Board - Board

Select the **STMI2-IGW Board Data** tab (corresponds to AMO BCSU and AMO CGWB). Here you have to enter

- Ethernet interface
  - IP address of customer LAN
  - Subnet mask
  - Standard gateway IP address
- Data for large enterprise gatekeeper
- CO protocol (not used in this example)
- Primary and secondary gatekeeper
- Gateway data
- H.235 security data
- Service interface

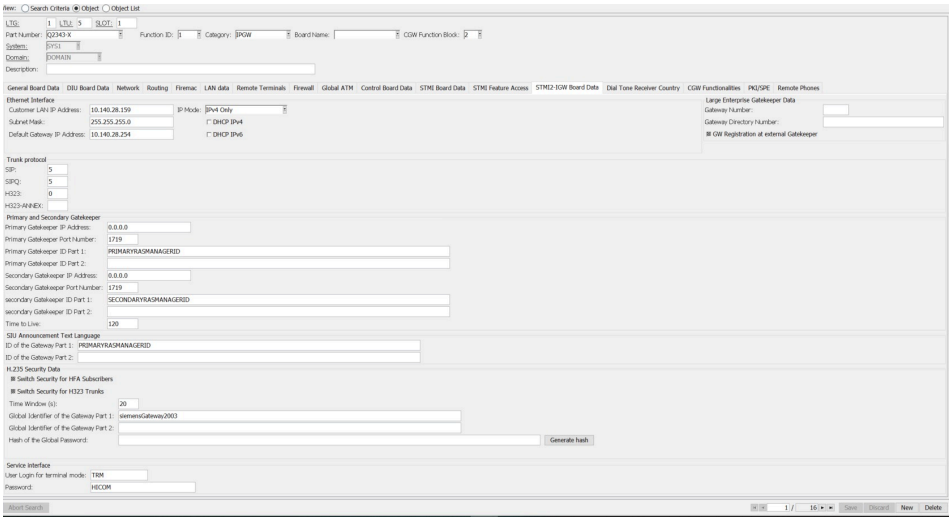


Figure 160: Configuration Management - System Data - Board - Board - STMI2-IGW Board Data tab

The next screen shows the **STMI Board Data** tab. Here you can configure for example the **Idle Pattern**, **IP Address** and **Number of DMC connections** (corresponds to AMO CGWB).

Save the completed settings using the **Save** button.

Use the **Search** button to go to the board you have already configured.

In the **STMI Feature Access** tab (corresponds to AMO CGWB) you can configure in which mode the common gateway should work (**Normal**, **Ready** or **Defect**), **Ethernet Interface** data and **Audio Stream Control Data**.

IMPORTANT: It is important to ensure that the number of UDP ports is at least twice as large as the number of b-channels of the common gateway module.

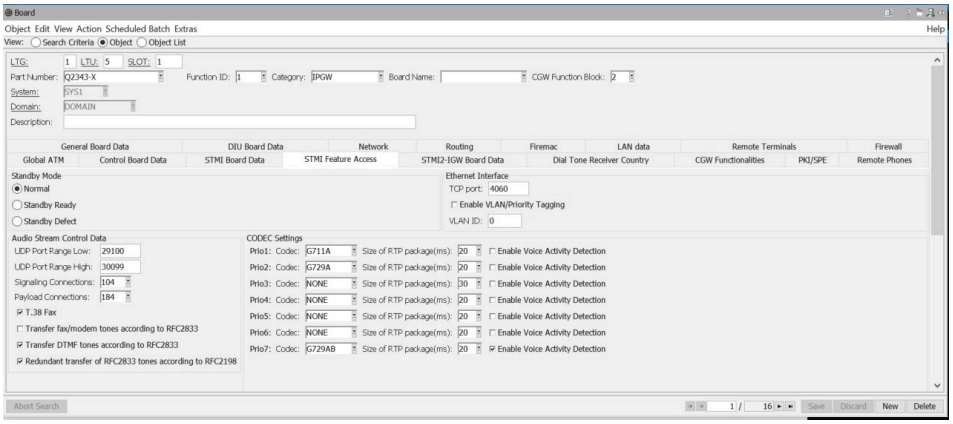


Figure 161: Configuration Management - System Data - Board - Board - STMI Feature Access tab

8.2.5.2 Configure a HFA User via the OpenScape 4000 Assistant

HFA users are configured like Up0/E users.

Start **Configuration Management - Station - Station**.

The **Station Number**, **PEN**, **Device Combination**, **Connection Type**, etc. can be entered in the header of the input window.

The **Basic 1** tab contains the default settings and other user data from the AMO SBCSU.

Not shown in the next figure is the **Basic 2** tab where the IPPASSW from the AMO SBCSU is entered. The IP address of a set-up user can also seen there.

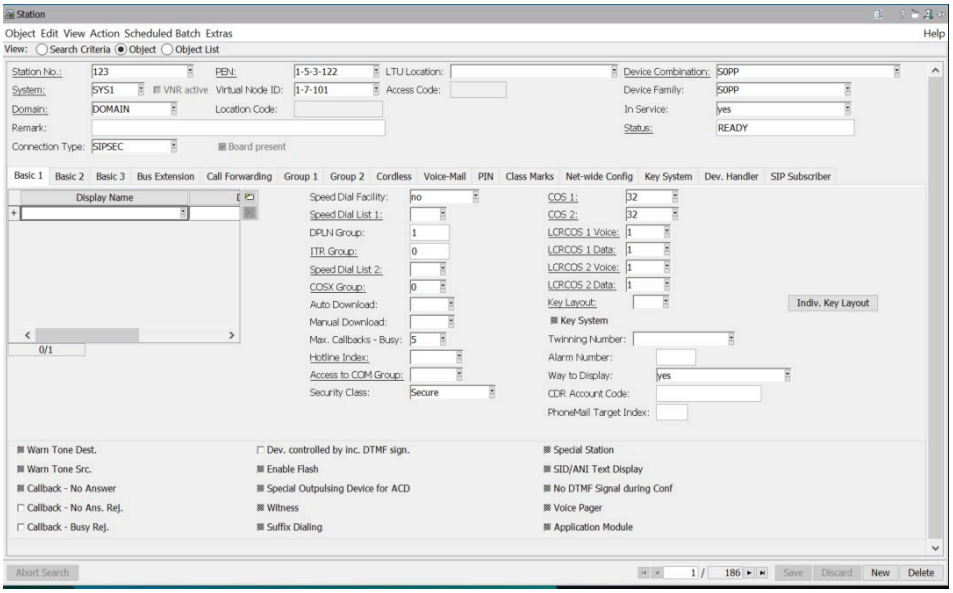


Figure 162: Configuration Management - Station - Station - Basic 1 tab

8.2.6 Deletion

The deletion of HFA components is not symmetrical to the generation: The AMO CGWB has no deletion branch because one-off set-up module data are always valid until deletion of the module with the AMO BCSU.

Example: The HFA components generated in the previous section are to be deleted.

First, the HFA users are deleted:

DELETE-SBCSU:STNO=<number>,SVC=ALL;

The common gateway board can then be immediately deleted. This also automatically deletes the board data, with the result that an AMO CGWB command is not required.

DELETE-BCSU:MTYPE=IPGW,LTG=<ltgno>,LTU=<ltuno>,SLOT=<slotno>;

Now you can reconfigure the board with other functions.

8.2.7 Tuning the voice quality

Depending on the available infrastructure, AMO CGWB (DSP branch)offers different configuration parameters:

- Noise suppression by Voice Activity Detection
- Problem fixing with packet delay and packet sequencing
- Echo suppression
- Sample length

This feature is controlled using the AMO CGWB. When used during operation, the board data does not need to be explicitly reloaded in this case. The data immediately comes into effect on the board.

HG 35XX supports various jitter buffer modes. For HG 3500, two different settings are available:

1) **Static jitter buffer with drift correction**. The length of the jitter buffer always remains constant (it is set to a fixed value in the same way as with "legacy mode," however, the runtime of the incoming signal is not modified).

CHA-CGWB:MTYPE=CGW,LTU=<ltuno>,SLOT=<slotno>,TYPE=JB,JBMODE=1;

1) **WBM > Configuration > Voice Gateway > Payload > HW Modules > Display DSP Jitter Settings > Jitter Buffer Type: Static**
2) The **adaptive jitter buffer** (default settings). This mode can both correct the drift as well as adapt its depth dynamically. The value set in the JITBUFD parameter is not evaluated in this method. The adaptive jitter buffer is activated via

CHA-CGWB:MTYPE=CGW,LTU=<ltuno>,SLOT=<slotno>,TYPE=JB,JBMODE=2;

1) **WBM > Configuration > Payload > HW Modules > Display DSP Jitter Buffer Settings > Jitter Buffer Type: Adaptive**

The jitter buffer can still be optimized with the values for

- **Average delay for voice (ms) - AVGDLYV**

This defines the standard value (initial value) for the jitter buffer.

- **Maximum delay for voice (ms) - MAXDLYV**

This defines the maximum length of the jitter buffer.

- **Minimum delay for voice (ms) - MINDLYV**

This defines the minimum length of the jitter buffer.

- **Packet loss/delay preference - PACKLOSS**

The jitter buffer can be optimized by the PACKLOSS parameter. The default value 4 should always be preset initially. If the value is set to 0, 1, 2 or 3, the algorithm attempts to prevent packet loss and increases the jitter buffer if problems occur. Conversely, if PACKLOSS= 5, 6, 7 or 8, the algorithm increasingly attempts to always work with a jitter buffer that is as small as possible and accepts a certain degree of packet loss.

- **Average delay for data (ms) - AVGDLYD**

This defines the standard value (initial value) for the jitter buffer for the data service.

- **Minimum delay for data (ms) - MINDLYD**

This defines the maximum length of the jitter buffer for the data service.

In HG 3500, it is recommended to use the **adaptive jitter buffer**. But, if there are older analog fax machines a static jitter buffer could be the better choice.

Other important parameters:

- **Voice Activity Detection**: **WBM > Configuration > Voice Gateway > Codec-Parameters**
- **Echo Canceller**: **WBM > Configuration > Payload > HW Modules > DSP Settings**

Additional parameters in AMO CGWB, TYPE=ASC:

Parameter	Description
VAD	Recognition of silence using Voice Activity Detection (AMO CGWB:TYPE=ASC, VAD=<yes,no>)
RTP	Sample length of the RTP packet depending on the codecs.

8.2.8 Activation of the voice compression

In HG 3500, voice compression is activated in the AMO CGWB (ASC branch). The parameter CODECLST is relevant for this setting. The codec sequence is important in this regard. In the example below, HG 3500 uses G.729 as first

choice, G.711A as second choice, and G.723 as third choice. The codec that is actually used depends on the settings of the remote system (user).

```
CHANGE-CGWB:MTYPE=CGW,LTU=<ltunr>,SLOT=<slotnr>,TYPE=ASC,PRIO=PRIO1,CODEC=G729;
CHANGE-CGWB:MTYPE=CGW,LTU=<ltunr>,SLOT=<slotnr>,TYPE=ASC,PRIO=PRIO2,CODEC=G711A;
CHANGE-CGWB:MTYPE=CGW,LTU=<ltunr>,SLOT=<slotnr>,TYPE=ASC,PRIO=PRIO3,
{354}CODEC=G723;
```

8.2.9 Relevant AMOs

AMO	Parameter	Sprache/ Language	Beschreibung/Description
BSSU	ADRART=LAGE	d	Adressierung ueber physikalische Lage
	ADDRTYPE=PEN	e	Physical board/module address
BCSU	ALARMNR	d	Alarm Nummer
	ALARMNO	e	Alarm number
	BKAN3530	d	Anzahl der B-Kanäle für die HG3530 Funktion
	BCHL3530	e	Amount of b-channels for HG3530 function
	FCTID	d	Function Id (muss immer 1 sein)
	FCTID	e	Function id (mustbe set to 1)
	FCTBLK	d	Funktionsblock-Index (einen beliebigen freien Funktionsblock zwischen 1-20 wählen)
	FCTBLK	e	Function block index (choose a free function block between 1-20)
	LWVAR	d	Index auf Loadware Block der T1 Baugruppe
	LWVAR	e	Index to loadware block for the t1 board
	SACHNR	d	Baugruppensachnummer (2. und 3. Block) Q2316-X, Q2316-X10, Q2324-X500, Q2324-X510
	PARTNO	e	Part number (2nd and 3rd bloc) Q2316-X, Q2316-X10, Q2324-X500, Q2324-X510

AMO	Parameter	Sprache/ Language	Beschreibung/Description
	SACHNR1	d	Sachnummer der zu ersetzenden Baugruppe (2. und 3. Block)
	PARTNO1	e	Part number of module that has to be replaced (2nd and 3rd bloc)
	SACHNR2	d	Sachnummer der neuen Baugruppe (2. und 3. Block)
	PARTNO2	e	Part number of new module (2nd and 3rd bloc)
	TYP=IPGW	d	IP Gateway (Common Gateway Baugruppe)
	MTYPE=IPGW	e	IP gateway (common gateway board)
BFDAT	ANZBKAN	d	Anzahl der funktionsbezogenen B-Kanäle.
	BCHLCNT	e	Defines the number of b-channels related to the selected function.
	ANZSATZ	d	Anzahl der funktionsbezogenen Saetze. Mögliche Werte: 1-240
	LINECNT	e	Defines the number of lines related to the selected function.
	BGBKAN	d	Block fuer Baugruppe mit 60 und/ oder 120 B-Kanaelen
	BRDBCHL	e	Dedicates the block for boards with 60 and/or 120 b-channels
	CONFIG=WEITER	d	Weitere Block-Konfiguration ermöglichen
	CONFIG=CONT	e	ontinue block configuration
	CONFIG=OK	d	Block-Konfiguration abschließen
	CONFIG=OK	e	Finish block configuration
	FCTBLK	d	Dieser Index beschreibt den Funktionsblock welcher auf dem Common Gateway konfiguriert werden soll. Anhand des Funktionsblocks wird die Konfiguration der benötigten pyhsikalischen Lines (Sätze der Baugruppe) festgelegt.

AMO	Parameter	Sprache/ Language	Beschreibung/Description
	FCTBLK	3	This index describes the function block which should be configured on the common gateway board. With that index the amount of needed physical lines (board circuits) is calculated.
	FUNCTION	d	Dieser Parameter legt das Konfigurationsprofile des Common Gateways fest. Dabei muss die eventuell benötigte HG 3570 Funktion als erste angeführt werden. Falls ein bestimmter Line-Bereich für die Funktionen HG 3530 oder HG 3550 vorreserviert werden soll, muss die entsprechende Funktion am Ende stehen und mit dem Wert HG35xxR abgeschlossen sein. Die Funktion kann nur als Einzel-Funktion konfiguriert werden.
	FUNCTION	e	This parameter defines the configuration profile of the CGW board. If HG3570 functionality is used, it must be configured at first position. If a prereservation of a certain line range of functions HG3530, HG3540 or HG3550 is desired, this function must be at the end of the profile just suffixed by the according HG35xxR value. The function can only be configured as single function.
BSSU	WTIME	d	Bei RESTART-Kommando: Wartezeit zwischen Aus- und Wiedereinschalten in Sekunden. Mögliche Werte: 0-20
	WTIME	e	For RESTART command: Wait time between switching off and switching on in seconds. Possible values: 0-20

AMO	Parameter	Sprache/ Language	Beschreibung/Description
CGWB	SMODE=NORMAL	d	Mode oder Normal Mode Eine Baugruppe im Normal Mode hat gültige Baugruppendaten und normalerweise auch OPTIIPs konfiguriert. Eine Baugruppe im Ready Mode hat keine gültigen Baugruppendaten, auf diese Baugruppe können OPTIIPs umgeschaltet werden, falls eine andere Baugruppe aus demselben Baugruppen-Pool (AMO BPOOL) defekt wurde. Eine Baugruppe im Defekt Mode hat ebenfalls keine gültigen Baugruppendaten, diese Baugruppe hat aufgrund eines Defekts seine OPTIIPs und seine Baugruppendaten abgegeben.
	SMODE=NORMAL	e	Mode or Normal Mode A board in Normal Mode has valid board data and normally also OPTIIPs assigned to it. A board in Ready Mode has no valid board data, to this board OPTIIPs can be switched over if another board of the same board reconfiguration pool (AMO BPOOL) becomes defective. A board in Defect Mode has also no valid board data, this board has lost its OPTIIPs and its board data to another board because it's gone defective.
	IPADR	d	IP Adresse der Common Gateway Baugruppe (Source Adresse)
	IPADR	e	Source IP address of common gateway board
	MTYP=INITCGWB	d	Zurücksetzen der Konfigurationsdaten der Common Gateway Baugruppe auf die Standardwerte
	MTYPE=INITCGWB	e	Reset configuration data of common gateway board to default values

AMO	Parameter	Sprache/ Language	Beschreibung/Description
	NETMASK	d	IP-Netzmaske des LAN-Segmentes. Die IP-Netzmaske bestimmt die Grenze zwischen Netz- und Host-Teil in der IP-Adresse. Alle IP-Adressen am LAN-Segment müssen bezüglich des Netzanteils der IP-Adresse gleich und bezüglich des Host-Teils unterschiedlich sein (auch der Default Router muss dieser Bedingung entsprechen).
	NETMASK	e	IP net mask of LAN segment The IP net mask determines the network and the host partition of an IP address. All IP addresses of a LAN segment must contain the identical network address part but different host address parts (also the Default Router must fulfill this requirement)
DIMSU	CGW	d	Anzahl der Common Gateway-Baugruppen
	CGW	e	Number of common gateway boards
	TYP=APPLIKAT	d	DIMSU-Option: Applikation
	TYPE=APPLICAT	e	DIMSU options: application
	WSPROT	d	Sprach/Daten Applikation mit Workstation Protokoll
	WSPROT	e	integrated voice/data application using workstation prot.
SBCSU	ANSCHL=IP2	d	Anschluss-Art der Geräte IP2=Anschluss ueber IP (HFA Gateway Version 2)
	CONN=IP2	e	Device Connection Type IP2=Connection via IP (HFA gateway version 2)
	ART=OPTI	d	Hauptrufnummer des IP-Telefonanschluss einrichten
	OPT=OPTI	e	Specification of bus type or unit to be expanded

AMO	Parameter	Sprache/ Language	Beschreibung/Description
	GERKON=OPTIIP	d	Geräte-Konstellation eines Teilnehmers OPTIIP=IP Sprachterminal
	DVCFIG=OPTIIP	e	Device Configuration OPTIIP=Digital IP voice terminal
	IPPASSW	d	passwort fuer ip login prozedur
	IPPASSW	e	Password for IP logon procedure
	SNU	d	Standard Tastaturbelegung
	STD	e	Standard Key Layout
ZAND	APIMAX	d	Maximale Anzahl der gleichzeitig aktiven API Sessions. DB-Initialisierung: 10
	APIMAX	e	Maximum number of allowable active API sessions. DB initialization: 10
	KENNL	d	Linearisierungs- und Kompandierungskennlinien bei der PCM-Kodierung/Dekodierung. Der eingegebene Wert wird zum einen in die zentralen Anlagendaten übernommen, zum anderen bei eingerichteter LTG auch in die entsprechenden COFI-Daten. Der Wert in den zentralen Anlagendaten ist auch gültig bei der Konfiguration von NCUI-Baugruppen in NBCS-Shelfs.Es sollte daher nach Konfiguration von NBCS-Shelfs dieser Wert nicht mehr geändert werden!
	CODE	e	Speech coding.The entered value will be issued once to central system data and once for assigned LTG in the according COFI-data. The value in central system data is also valid for configuration of NCUI-boards in NBCS shelfs. Therefore this value should not be changed after configuration of NBCS-shelfs!
	TYP=CIT	d	Konfigurieren von fiktiven Geräten, Einstellungen für API Schnittstelle

AMO	Parameter	Sprache/ Language	Beschreibung/Description
	TYPE=CIT	e	Configure virtual stations, settings for API interface
	TYP=CONFC	d	Länderspezifische Einstellung für KENNL, K- oder TDAEMPF. Dieser Zweig gilt nur für kompakte Hardware.
	TYPE=CONFC	e	Selection of country-specific settings for CODE, CONFAT STNAT. This branch is only for compact hardware.

8.3 Frequently Asked Questions

1) **Question**: How far can an IP phone be located from the host?
2) **Answer**: There are no hard distance limitations. However delays limit the practical distance: The larger the distance between the host and the IP workpoint, the more delay is introduced via the underlying network. If possible one way delays should be less than 200ms.
3) **Question**: How many IP phones are supported per OpenScape 4000?
4) **Answer**: Up to 12000 IP phones can be supported per OpenScape 4000. Note that the HG 3500 is supported on all IP Access Points.
5) **Question**: How many IP phones can be supported per HG 3500?
6) **Answer**: A maximum of 240 IP phones can be supported per HG 3500. Depending on the traffic requirements of the subscribers either a 60 connection GW or a 120 connection GW will be required.
7) **Question**: Are calls between IP phones switched in the IP network?
8) **Answer**: Yes. HG 3500 gateways support peer-to-peer (IP switching).
9) **Question**: Do IP phones connected to HG 3500 gateways support mobility?
10) **Answer**: Yes. The following is possible:

    a) The user can take an IP phone to a new office or location and all relevant information is transferred automatically and no manual intervention is necessary.

    - A user can log in from any location via a soft-client to his workpoint, which will automatically disconnect itself from the OpenScape 4000 gateway. The soft-client will provide the user with the same features and privileges as the standard workpoint.
    - A user can log in from any IP phone within a system or CorNet network and make this phone his temporary phone. The home phone will automatically be logged off and calls to the home phone are forwarded as defined for CFNR (Call Forwarding No Reply). The temporary phone will provide the user with the same features and privileges as the standard home workpoint.

11) **Question**: Do the Phones require static IP addresses?

12) **Answer**: No, the current version of the HG 3500 line gateway does support clients configured for DHCP. Note that a DHCP server has to be configured in the IP network; otherwise static IP addresses are required for all clients.
13) **Question**: Can I connect a user via a wireless connection?
14) **Answer**: Yes. Given that IP line gateways support standard TCP/IP protocol and have been designed to work over WAN links only excessive delays are a concern. Make sure that wireless transceivers are working like Ethernet bridges in order to minimize delays.
15) **Question**: When payload and/or signaling IP packets arrive out of sequence, are they automatically re-arranged?
16) **Answer**: As long as all the relevant payload IP packets are still held within the jitter buffer, out of sequence IP packets will be re-arranged automatically. Given that signaling is using TCP/IP out of sequence packets are correctly processed by the protocol.
17) **Question**: Which protocols are we using for signaling and QOS?
18) **Answer**: Signaling: TCP/IP, QOS: LAN-tagging according IEEE 802.1p/q; DiffServ according to RFC 2474.
19) **Question**: Is the H.323 fast connect procedure implemented on the HG 3500?
20) **Answer**: Yes, in order to minimize call setup time, the H.323 fast connect procedure is used to exchange H.245 logical channel information.
21) **Question**: If IP network is down and the 4000 does not see the IP phones what do callers get when calling?
22) **Answer**: If connectivity to the IP phone is lost, the phone will be in a reset state trying to reconnect to the gatekeeper. There is a display indicating that state. There will be no dial tone. Incoming calls can be re-directed using the feature “Alternate Routing On Error” that can use LCR rules for forwarding the call to anything you like, e.g. to PhoneMail.
23) **Question**: Do we have QoS/payload monitoring of the DMC connection?
24) **Answer**: No, the HG 3500 is not aware of DMC connections.
25) **Question**: How long does it take for IP phones to re-register with a gateway?
26) **Answer**: Based on performance testing with HG 3500s, it takes approximately 2 - 3 minutes for 240 phones to re-register onto a backup card.
27) **Question**: Why can’t we support more than 240 users on the 120 connection version?
28) **Answer**: Based on traffic values you could support over 600 users at 6 C.C.S and 1% blocking. However you would not be able to support the signaling traffic required for that many users. Customers would not configure that many users on a single card for reliability reasons either.
29) **Question:** The effect of default setting recommended by popular router manufacturers and the TOS byte default values documented for HFA, that is, the pre-defined DiffServ CodePoints (DSCP) is exactly the opposite of the intended effect. The packets we marked as high priority are rejected straightaway by the router. What is this nonsense about?
30) **Answer:** The default values used for HFA come from an internal company standard that was implemented in all HG 35xx gateways. The interoperability problem has since come to light with the result that the company standard will be modified shortly. The default values can be modified at any time and modified in line with actual conditions in the customer network.
31) **Question:** Does HFA support VLANs?

32) **Answer:** Yes but only in conjunction with priority tagging. In accordance with IEEE 802.1 p/q, tagging was introduced for HFA to support priority tagging. If tagging is activated then the permanently preset priority bits of the various types of traffic are always set. If tagging is active, the VLAN ID can also be set (default value is zero). VLAN ID is not supported without the set priority bits.
33) **Question:** Does HFA support subnetting (RFC 950)?
34) **Answer:** Yes. When the network mask is entered, a check is performed to determine whether the block of ones that has been set meets the minimum length required for the class of the address, i.e. 8 ones for Class A, 16 for B and 24 for C. If the number of ones is greater than the number required for the class, subnetting is activated.
35) **Question:** Does HG 3500 gateway (STMI2/STM4/STMIX/STMIY) supports ClassLessInterDomainRouting (CIDR), this means Subnetting/ Supernetting?
36) **Answer**: Yes.
37) **Question:** Does vHG 3500 gateway (OpenScape 4000 SoftGate) supports ClassLessInterDomainRouting (CIDR), this means Subnetting/ Supernetting?

9 Mobile HFA Logon

9.1 Feature Description

9.1.1 Mobility Session

This feature is an enhancement to the static HFA (HiPath Feature Access). HFA Mobility is supported network-wide and was introduced with HiPath 4000 V2.

The idea of mobile HFA is to use the characteristics (classmarks, name, number, keys, ...) of one subscriber (mobile user) on different phones, which might be spread all over the world. We call such a user a “mobile user”.

The mobile user has a phone at his home office and travels to another place (other office or an other country). There he uses a phone (visited phone) as a visitor. He enters a code for the activation of “Mobile HFA” , his home number, his PIN and a possible password to use the visited phone with the characteristics of his phone at home.

If this procedure ends successfully (sufficient classmarks, phone types, ...) his home phone is placed in an out of order state (forced log off). The mobile user can then use the visited phone like his home phone. E.g. the home phone number/name are displayed if a call is established by or to the mobile user, the home phone’s classmarks are valid ...

If the visitor cancels the mobile HFA logon by a logoff, the original characteristics of the home phone and the visited phone are reactivated. The time between a mobile HFA logon and logoff at a visited phone is called “mobility session”.

The owner of the visited phone is no longer reachable in this case. All calls to the owner of the visited phone are redirected to a CFNR destination.

Activation of feature

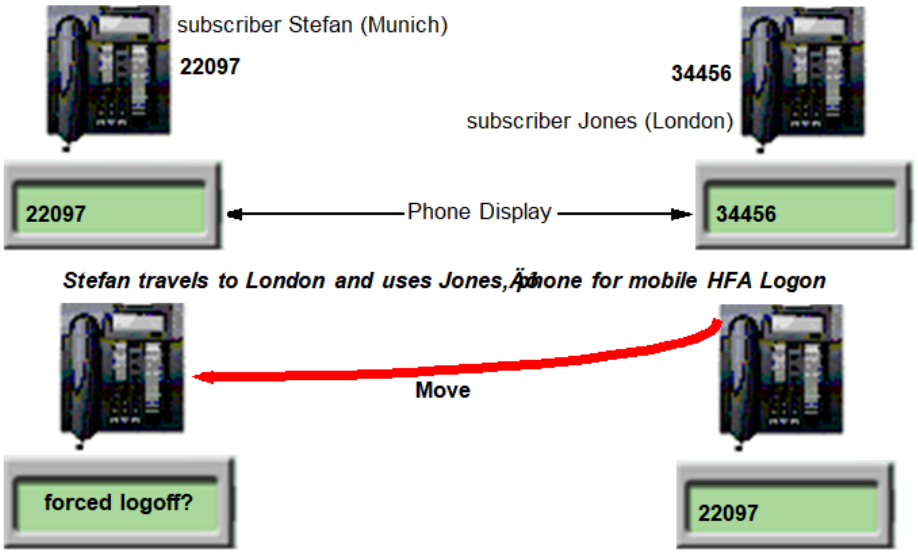


Figure 163: Activation of feature

All calls dialed for 34456 are now forwarded to the system CFNR (Call forwarding no reply) for subscriber Jones (admin by AMO ZIEL).

If Stefan travels back to Munich he performs the mobile logoff in London (DAR or menu) , or if he forgets he can also cancel it in Munich. In both cases the original status of both phones are redone within seconds.

While the London phone is in mobile use nobody can use Stefan's device in Munich.

Any call to Jones does not ring at Jones' device.

The feature can be protected against misuse with passwords, feature blocking and line dependent classmarks.

Call to mobile user

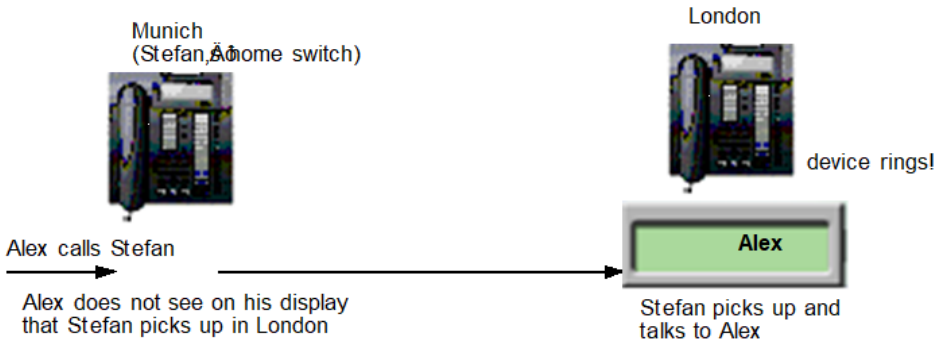


Figure 164: Call to mobile user

Call to visited phone

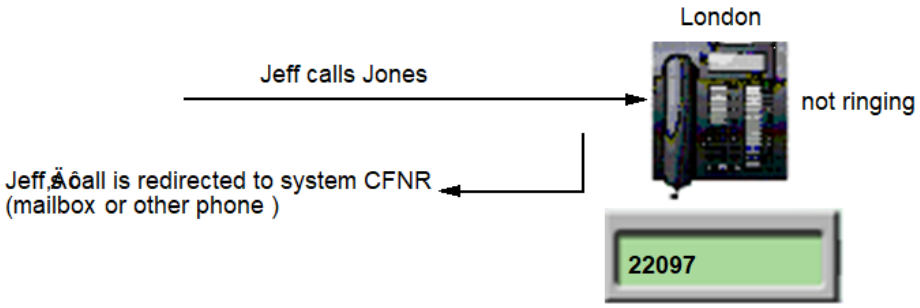


Figure 165: Call to visited phone

9.1.2 Shared Desk Area

Based on the feature “Mobile HFA Logon“,the functionality “Shared Desk Area“ can be used. The Shared Desk Area is a scenario, that allows a dynamic assignment of telephone devices to users. At a switch a number of users without fix phones, and phones with virtual subscribers are configured. The phones are spread over various rooms or buildings. The number of phones might be significantly lower than the number of users.

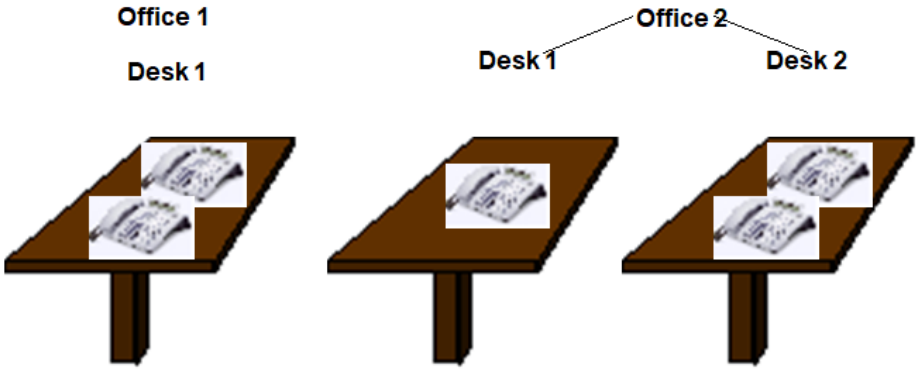
The real users can use any phone of the Desk Area. One terminal can be used by different users one after another.

E.g. user Jones can use a phone starting at 9.00 am. User Jeffrey can use the same phone afterwards when Jones has left the office. Both users can use the same phone using their own user characteristics.

User Jones comes to a phone and logs on with own phone number and password. If the logon succeeds he can phone as “Jones“.

His session is canceled if he logs off or if another user (Jeffrey) logs on to this phone.

After a logoff the phone comes up as configured. For this reason any physical phone must be configured with a virtual subscriber number (Dummy Number).



If a user logs off or his session is canceled by another user logging on at the device this user turns into visited state. That is that any call to him is redirected to the system CFNR destination.

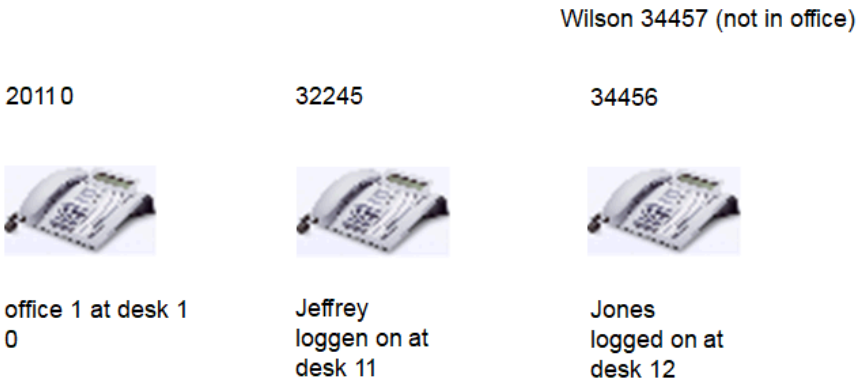
In the following example phone numbers starting with “3” indicate users of the shared desk areas configured at the switch. The dummies for the telephones have “names” like “office1 desk12” and corresponding numbers starting with “2”: 20112 (=office1, desk 12).



Figure 166: Jones and Wilson are logged on at the phones at desk10 and desk 11.

Calls to ...		
Name	Number	Action
Jeffrey	32245	are redirected to System CFNR
Jones	34456	ring at desk phone 10
Wilson	34457	ring at desk phone 11
desk10	20110	are redirected to System CFNR
desk11	20111	are redirected to System CFNR
desk12	20112	ring at desk phone 12

Now user Jeffrey logs on at desk phone 11 (knocks out Wilson). Jones logs off and moves to desk 12 for logon.



Calls to ...		
Name	Number	Action
Jeffrey	32245	ring at desk phone 11
Jones	34456	ring at desk phone 12
Wilson	34457	are redirected to System CFNR
desk10	20110	ring at desk phone 10
desk11	20111	are redirected to System CFNR
desk12	20112	are redirected to System CFNR

9.2 User Interface

IMPORTANT: For mobility and shared desk area the procedures for activation and deactivation are identical!

The user has two possibilities to activate a mobile logon:

- via DAR (Digit analysis Result) and
- via service menu.

A third possibility works for admin only: The administration via AMO ACTDA.

9.2.1 Activation/Deactivation via DAR

The feature via DAR is activated/deactivated at the visited phone.

9.2.1.1 HFA Logon

Enter the DAR for mobile HFA logon.

Then the user is asked to enter his home number (terminate with #) and his PIN (terminate with #).

Display says “MOBILE HFA LOGON STARTED”. If all checks run ok soon his own display on the home phone is displayed. As it he was really at home.

If the checks do not run OK (wrong password, wrong home number, missing attributes, ...) the rejection is shown on display.

- Mobility session (home phone physical extended)
- The home phone displays “Forced Logoff - Cancel mobility?” and is not usable, even not for fire brigade or other emergency calls. The only possible action is to cancel the mobility. But this action is protected by password (phone password - not the same as mobility password).
- Shared Desk Area (No physical home phone)
- If the home phone does not exist physically nothing can be displayed on the home. No cancellation from home phone is possible.

9.2.1.2 HFA Logoff

To logoff enter the DAR for logoff.

The display says “MOBILE HFA LOGOFF STARTED ... “

Soon afterwards the visitors own display comes up again at the visited phone and the home user’s phone comes up at the home switch.

9.2.2 Activation via menu

The menu items “MOBILE HFA LOGON/LOGOFF” for mobile HFA are located in the service menu. Activate the service menu at the visited phone and step forward/backward with the buttons “<“ and “>” until the menu items for mobile HFA logon/logoff are reached.

The mobile HFA feature can also be reached with service menu and digit “8’”(mobile HFA logon) and digit “9” (mobile HFA logoff).

After confirming logon the user is asked to enter home number and PIN like above.

After confirming an action the behavior is the same like DAR activation.

9.2.3 Activation with AMO ACTDA

AMO ACTDA needs three parameters. visited number, home number and PIN.

The Activation with AMO ACTDA is only possible at the switch where the visited phone is configured.

The AMO displays a message if logon runs ok or if it fails (with a reason).

9.3 Prerequisites

This feature is restricted with different flags in the switch of the visited phone and the switch of the home phone.

Possible phones for mobile HFA

The feature does not work with any type of phone. Both phones must have the capacity for mobile HFA in their firmware. Currently the following phones have this functionality:

- optipoint 410 (not 410 entry),
- optipoint 420 (electronic labeling keys)
- optipoint 600
- OpenStage 20/20G/40/40G/60/60G/80/80G

IMPORTANT: If the OpenStage terminal is operated in combination with an optiClient, "optiPoint 420 advance" must be set as the device type in the optiClient. For more information, refer to Section 4.1.1, “OpenStage terminal in combination with an optiClient”.

AMO prerequisites

- AMO FEASU bit **MOBHFA** must be set on both sides.
- The home phone must have the line attribute **MHFAHOME** in AMO SDAT.
- The visited phone must have the line attribute **MHFATBV** (to be visited) in AMO SDAT.
- For the home phone a PIN must be installed with COPIN attribute **MOBILE**.

Hardware

The mobile HFA phones are connected to the common gateway board (STMI2/4/STMIX/STMIY board).

Password settings

For the mobile user a mobile password should be added. This password prevents the “forced logoff“ at the home station from being canceled without a password.

- optiPoint terminals
- The password is assigned in the terminal Configuration menu, submenu “02=System”.
- OpenStage terminals
- The password can be assigned via the WBM of the terminal (**Administrator Pages > User mobility > Cancel mobility password**) or directly at the terminal via the menu **Admin > Password > Mobility**.

9.4 Service Information

9.4.1 Mobile HFA in Connection with other Features

9.4.1.1 OpenStage terminal in combination with an optiClient

General hints for the configuration of an optiClient together with an openStage phone

- The OpenStage of type "nn" has to be configured with the fitting standard key layout "openStage nn".
- It is not allowed to change the key assignment for an OpenStage phone (AMO TAPRO) while the optiClient is active.
- The individual change of key settings by the subscriber must not be enabled for the combination optiClient/openStage.
- When the user previously owned the combination optiClient/optiPoint then he/she is to be informed about the new key layout which can be seen in the optiClient application. Reason for this are the fixed key functions at OpenStage phones.
- In case of disregarding the mentioned restrictions the proper key assignment cannot assured when changing from OpenStage to optiClient and vice versa. This can be repaired only with deleting and configuring the complete connection again.
- This procedure counts also for the so called Tandem-Mode (optiClient uses the same number like the home station. In this case is the home station the OpenStage!)

Configuration of a new optiClient/OpenStage connection

- New configuration of the openStage phone with the proper standard key layout together with the configuration of the optiClient (OPTIIP&API).
- The device "optipoint 420 advance" has to be chosen in the optiClient application.

Replacement of an existing optiClient/optiPoint configuration with optiClient/OpenStage

1) Regeneration of the user data
2) Delete the connection completely

IMPORTANT: The deletion is necessary because it is currently the exclusive way to delete the so-called shadow table for key assignments. If it is not cleared correctly, the proper key assignment is not assured neither at the optiClient nor at the OpenStage. It depends on what had happened at the connection previously (i.e. different phone types were connected etc.) if the shadow table has to be cleared.

---

1) Now you can exchange the phones and then configure the OpenStage as described in General hints for the configuration of an optiClient together with an openStage phone or do it vice versa.

IMPORTANT: For additional information, refer to "'Mobile Registration' with OpenStage Hardware Terminals" in the optiClient readme file.

9.4.1.2 Malicious Call Identification at visited switch

If the feature “Malicious Call Identification” is activated at the visited switch (AMO PERSI) then the attempts for logon that fail because of wrong password entered, are output on the service terminal of the visited switch.

The output warning looks like this:

```
F2754 M4 N0063 MC TRACE BPA PIN TRACE 04-02-10 13:25:12
ALARM CLASS:CENTRAL:024
STNO INTERN:3581 PIN:25587
FORMAT:34
```

Read: At station 3581 a logon was attempted with PIN 25887.

9.4.1.3 Signaling and Payload Encryption (SPE)

Please refer to the documentation of „Signaling and Payload Encryption“.

9.4.2 Restriction

optiClient does not support the „Mobile HFA Logon“ feature. The user can realize this feature using different user profiles for logon. Users which want to use different calling numbers have to work with different user profiles.

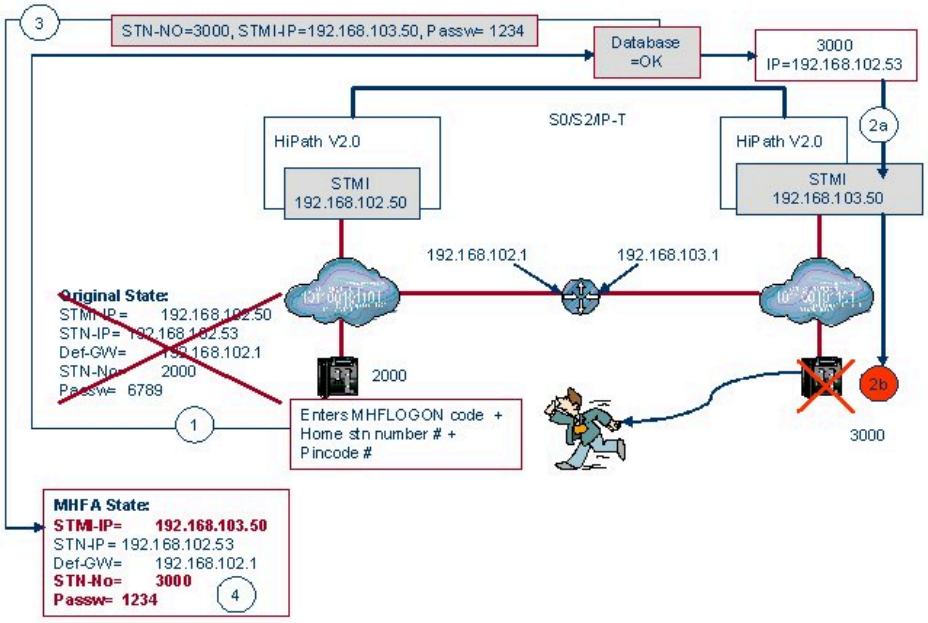
9.4.3 Language Support

The feature works with the language of the home switch. That means that menu and display texts, which are controlled by the switch software, are displayed in the switch language („Please dial“, „Enter password“,..).

Any messages controlled by the phone firmware (directly, not switch dependent) are only English („Cancel logoff“ , „logging on to home...“).

If the switch language is not set to English, texts are displayed in two languages.

9.4.4 Logon Sequences



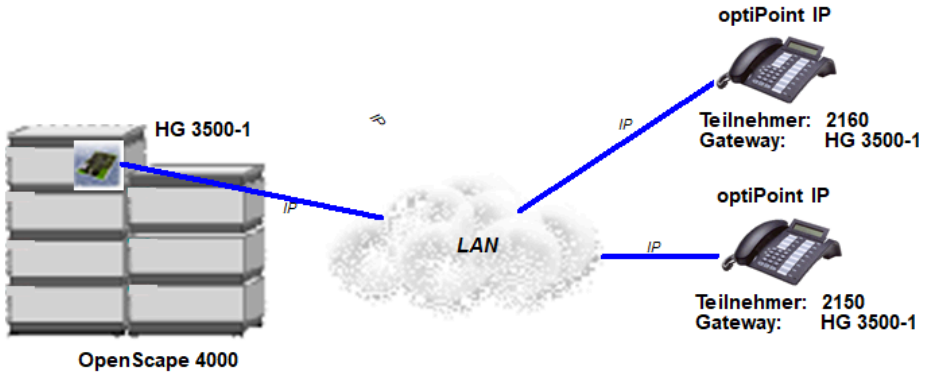
9.5 Generation

> **IMPORTANT:** Important time interval After all AM commands to install Mobile HFA are executed wait 3 minutes before starting a mobile HFA logon. HFA boards and IP phones need up to 3 minutes to perform a self-initialization. If a HFA logon is attempted before the self initalization has passed successfully, this logon will possibly fail.

- Preparation
  - Preparation: Reserve memory for boards and subscriber
  - Add board data
  - Add subscriber data
  - Add authorizations and classmarks for feature, subscriber ...
  - Add DARs
  - Add call forwarding destinations
  - Others

9.5.1 Example 1: Two HFA subscribers in the same Host

The subscriber 2150 shall get the right to be able to identify himself at the terminal of subscriber 2160. The subscriber 2160 shall not get any possibility of the identification. An incoming call for 2160 should be forwarded to subscriber 4444, if 2150 is using the phone of 2160.




```
ADD-DIMSU:TYPE=SYSTEM,CGW=1;
ADD-BFDAT:FCTBLK=1,FUNCTION=HG3530,BRDBCHL=BCHL60;
CHANGE-BFDAT:CONFIG=CONT,FCTBLK=1,FUNCTION=HG3530,LINECNT=30,BCHLCNT=30;
/* Configuration of 30 HG 3530 circuits with 30 b-channels
CHANGE-BFDAT:CONFIG=OK,FCTBLK=1,ANSW=YES;
ADD-BCSU:MTYPE=IPGW,LTG=1,LTU=3,SLOT=85,PARTNO="Q2316-X",FCTID=1,LWVAR="0",FCT▶
BLK=1,ALARMNO=0;
ADD-CGWB:LTU=3,SLOT=85,SMODE=NORMAL,IPADR=192.168.1.85,NETMASK=255.255.255.0;
RESTART-BSSU:ADDRTYPE=PEN,LTU=3,SLOT=85;
ADD-SBCSU:STNO=2150,OPT=OPTI,CONN=IP2,PEN=1-3-85-0,DVCFIG=OPTIIP, ...;

ADD-SBCSU:STNO=2160,OPT=OPTI,CONN=IP2,PEN=1-3-85-1,DVCFIG=OPTIIP, ...
ADD-WABE:CD=*95,DAR=MHFALGON,CHECK=N;

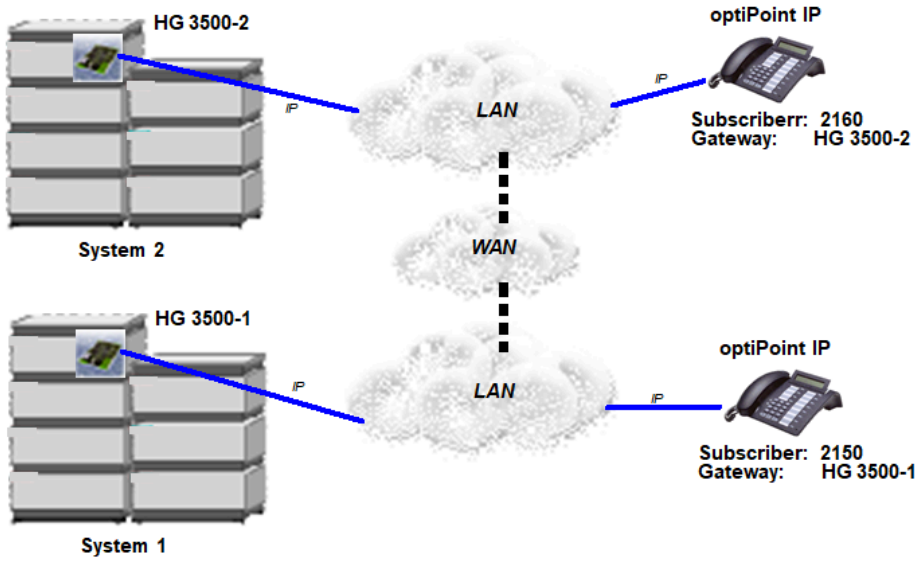
ADD-WABE:CD=*96,DAR=MHFALGOF,CHECK=N;
ADD-PERSI:TYPE=STN,STNO=2150,NAME="STEFAN*",PIN1="258861",PININDIV=Y;

CHANGE-PERSI:TYPE=COPIN,COPIN=1,COTYPE=MOBILE, ...;
CHANGE-SDAT:STNO=2150,TYPE=ATTRIBUT,AATTR=MHFAHOME;

CHANGE-SDAT:STNO=2160,TYPE=ATTRIBUT,AATTR=MHFATBV;
CHANGE-FEASU:TYPE=A,CM=MOBHFA;
ADD-ZIEL:TYPE=FWD,SRCNO=2160,SI=VOICE,DESTNOF=4444,DTYPE=CFNR,ITYPE=GEN,CF▶
VAR=SYSTEM;
REGENERATE-RICHT;
```

9.5.2 Example 2: Two HFA subscriber at different systems

The two subscribers 2150 and 2160 shall get the rights to be able to identify themselves at the terminal of the other subscriber. The calls for 2160 should be forwarded to his mobile number 017544444444, if his phone is used as “Mobile HFA Logon”. The calls for 2150 should be forwarded to the subscriber 4444, if his phone is used as “Mobile HFA Logon”.



Generation of the System 1:

```
ADD-DIMSU:TYPE=SYSTEM,CGW=1;
ADD-BFDAT:FCTBLK=1,FUNCTION=HG3530,BRDBCHL=BCHL60;
CHANGE-BFDAT:CONFIG=CONT,FCTBLK=1,FUNCTION=HG3530,LINECNT=30,BCHLCNT=30; /* Con▶
figuration of 30 HG 3530 circuits with 30 b-channels
CHANGE-BFDAT:CONFIG=OK,FCTBLK=1,ANSW=YES;
ADD-BCSU:MTYPE=IPGW,LTG=1,LTU=3,SLOT=85,PARTNO="Q2316-X",FCTID=1,LWVAR="0",FCT▶
BLK=1,ALARMNO=0;
ADD-CGWB:LTU=3,SLOT=85,SMODE=NORMAL,IPADR=192.168.1.85,NETMASK=255.255.255.0;
RESTART-BSSU:ADRART=LAGE,LTU=3,EBT=85;
ADD-SBCSU:STNO=2150,OPT=OPTI,CONN=IP2,PEN=1-3-85-0,DVCFIG=OPTIIP,....;
ADD-WABE:CD=*95,DAR=MHFALGON,CHECK=N;

ADD-WABE:CD=*96,DAR=MHFALGOF,CHECK=N;
ADD-PERSI:TYPE=STN,STNO=2150,NAME="OPTI IP 1*",PIN1="0512",PININDIV=YES;

CHANGE-PERSI:TYPE=COPIN,COPIN=1,COTYPE=MOBILE,....;
CHANGE-SDAT:STNO=2150,TYPE=ATTRIBUT,AATTR=MHFAHOME;

CHANGE-SDAT:STNO=2150,TYPE=ATTRIBUT,AATTR=MHFATBV;
CHANGE-FEASU:TYPE=A,CM=MOBHFA;
ADD-ZIEL:TYPE=FWD,SRCNO=2150,SI=VCE,DESTNOF=4444,DTYPE=CFNR,ITYPE=GEN,CFVAR=SYS▶
TEM;
REGENERATE-RICHT;
```

Generation of the system 2:

```
ADD-DIMSU:TYPE=SYSTEM,CGW=1;
ADD-BFDAT:FCTBLK=1,FUNCTION=HG3530,BRDBCHL=BCHL60;
CHANGE-BFDAT:CONFIG=CONT,FCTBLK=1,FUNCTION=HG3530,LINECNT=30,BCHLCNT=30; /* Con▶
figuration of 30 HG 3530 circuits with 30 b-channels
CHANGE-BFDAT:CONFIG=OK,FCTBLK=1,ANSW=YES;
ADD-BCSU:MTYPE=IPGW,LTG=1,LTU=3,SLOT=85,PARTNO="Q2316-X",FCTID=1,LWVAR="0",FCT▶
BLK=1,ALARMNO=0;
ADD-CGWB:LTU=3,SLOT=85,SMODE=NORMAL,IPADR=192.168.2.97,NETMASK=255.255.255.0;
RESTART-BSSU:ADDRTYPE=PEN,LTU=3,SLOT=85;
```

```
ADD-SBCSU:STNO=2160,OPT=OPTI,CONN=IP2,PEN=1-3-85-0,DVCFIG=OPTIIP,...;
ADD-WABE:CD=*95,DAR=MHFALGON,CHECK=N;

ADD-WABE:CD=*96,DAR=MHFALGOF,CHECK=N;
ADD-PERSI:TYPE=STN,STNO=2160,NAME="OPTI IP 10*",PIN1="0612",PININDIV=YES;

CHANGE-PERSI:TYPE=COPIN,COPIN=1,COTYPE=MOBILE,.....;
CHANGE-SDAT:STNO=2160,TYPE=ATTRIBUT,AATTR=MHFAHOME;

CHANGE-SDAT:STNO=2160,TYPE=ATTRIBUT,AATTR=MHFATBV;
CHANGE-FEASU:TYPE=A,CM=MOBHFA;
ADD-ZIEL:TYPE=FWD,SRCNO=2160,SI=VCE,DESTNOF=0017544444444,DTYPE=CF►
NR,ITYPE=GEN,CFVAR=SYSTEM;
REGENERATE-RICHT;
```

9.5.3 Relevant AMOs

AMO	Parameter	Sprache/ Language	Beschreibung/ Description
ACTDA	ABMED=GERFREI	d	Erlaubt das Abmelden nur im Freizustand.
	COND=IDLESTN	e	Allows the logoff only if station is idle.
	ABMED=UNBED	d	Erlaubt das Abmelden in jedem Fall.
	COND=UNCOND	e	Condition for logoff: Unconditional logoff
	ACTION=MLOGON	d	Aktivieren des Leistungsmerkmals: Logon eines Mobile HFA-users
	ACTION=MLOGON	e	Activate the feature: Logon of mobile hfa-user
	ACTION=MLOGOFF	d	Deaktivieren des Leistungsmerkmals: Logoff eines Mobile HFA-users
	ACTION=MLOGOFF	e	Deactivate the feature: Logoff of mobile hfa-user
	BESRNR	d	Rufnummer des besuchten Teilnehmers
	VISSTNO	e	Station number of the visited station
	HEIMPIN	d	PIN des Besuchers
	HOMEPIN	e	PIN of the visitor
	HEIMRNR	d	Heimrufnummer des Besuchers
	HOMESTNO	e	Home station no. of the visitor
BCSU	ALARMNR	d	Alarm Nummer

AMO	Parameter	Sprache/ Language	Beschreibung/ Description
	ALARMNO	e	Alarm number
	BKAN3530	d	Anzahl der B-Kanaele fuer die HG3530 Funktion
	BCHN2430	e	Number of b-channels for HG3530 function
	FCTID	d	Function Id ist immer 1
	FCTID	e	Function id is always set to 1
	FCTBLK	d	Funktionsblock-Index (einen beliebigen freien Funktionsblock zwischen 1-20 wählen)
	FCTBLK	e	Function block index (choose a free function block between 1-20)
	LWVAR	d	Index auf Loadware Block der T1 Baugruppe
	LWVAR	e	Loadware variant
	SACHNR	d	Baugruppensachnummer (2. und 3. Block) Q2316-X, Q2316-X10, Q2324-X500, Q2324-X510
	PARTNO	e	Part numver (2nd and 3rd bloc) Q2316-X, Q2316-X10, Q2324-X500, Q2324-X510
	TYP=IPGW	d	IP Gateway (Common Gateway Baugruppe)
	MTYPE=IPGW	e	IP gateway (common gateway board)
BFDAT	ANZBKAN	d	Anzahl der funktionsbezogenen B-Kanäle.
	BCHLCNT	e	Defines the number of b-channels related to the selected function.
	ANZSATZ	d	Anzahl der funktionsbezogenen Saetze. Mögliche Werte: 1-240
	LINECNT	e	Defines the number of lines related to the selected function.
	BGBKAN	d	Block fuer Baugruppe mit 60 und/oder 120 B-Kanaelen

AMO	Parameter	Sprache/ Language	Beschreibung/ Description
	BRDBCHL	e	Dedicates the block for boards with 60 and/or 120 b-channels.
	CONFIG=WEITER	d	Weitere Block-Konfiguration ermöglichen
	CONFIG=CONT	e	Continue block configuration
	CONFIG=OK	d	Block-Konfiguration abschließen
	CONFIG=OK	e	Terminate block configuration
	FCTBLK	d	Dieser Index beschreibt den Funktionsblock welcher auf dem Common Gateway konfiguriert werden soll. Anhand des Funktionsblocks wird die Konfiguration der benötigten pyhsikalischen Lines (Sätze der Baugruppe) festgelegt.
	FCTBLK	e	This index describes the function block which should be configured on the CGW board. With that index the amount of needed physical lines (board circuits) is calculated.
	FUNCTION	d	Dieser Parameter legt das Konfigurationsprofile des Common Gateways fest. Dabei muss die eventuell benötigte HG 3570 Funktion als erste angeführt werden. Falls ein bestimmter Line-Bereich für die Funktionen HG 3530 oder HG 3550 vorreserviert werden soll, muss die entsprechende Funktion am Ende stehen und mit dem Wert HG35xxR abgeschlossen sein. Die Funktion kann nur als Einzel-Funktion konfiguriert werden.
	FUNCTION	e	This parameter defines the configuration profile of the common gateway board. If HG3570 functionality is used, it must be configured at first position. If a prereservation of a certain line range of functions HG3530, HG3540 or HG3550 is desired, this function must be at the end of the profile just suffixed by the according HG35xxR value. The function can only be configured as single function.

AMO	Parameter	Sprache/ Language	Beschreibung/ Description
CGWB	SMODE=NORMAL	d	Mode oder Normal Mode Eine Baugruppe im Normal Mode hat gültige Baugruppendaten und normalerweise auch OPTIIPs konfiguriert. Eine Baugruppe im Ready Mode hat keine gültigen Baugruppendaten, auf diese Baugruppe können OPTIIPs umgeschaltet werden, falls eine andere Baugruppe aus demselben Baugruppen-Pool (AMO BPOOL) defekt wurde. Eine Baugruppe im Defekt Mode hat ebenfalls keine gültigen Baugruppendaten, diese Baugruppe hat aufgrund eines Defekts seine OPTIIPs und seine Baugruppendaten abgegeben.
	SMODE=NORMAL	e	Mode or Normal Mode A board in Normal Mode has valid board data and normally also OPTIIPs assigned to it. A board in Ready Mode has no valid board data, to this board OPTIIPs can be switched over if another board of the same board reconfiguration pool (AMO BPOOL) becomes defective. A board in Defect Mode has also no valid board data, this board has lost its OPTIIPs and its board data to another board because it's gone defective.
	IPADR	d	IP Adresse der Common Gateway Baugruppe (Source Adresse)
	IPADR	e	Source IP address of common gateway board
	NETMASK	d	IP-Netzmaske des LAN-Segmentes. Die IP-Netzmaske bestimmt die Grenze zwischen Netz- und Host-Teil in der IP-Adresse. Alle IP-Adressen am LAN-Segment müssen bezüglich des Netzanteils der IP-Adresse gleich und bezüglich des Host-Teils unterschiedlich sein (auch der Default Router muss dieser Bedingung entsprechen).

AMO	Parameter	Sprache/ Language	Beschreibung/ Description
	NETMASK	e	IP net mask of LAN segment The IP net mask determines the network and the host partition of an IP address. All IP addresses of a LAN segment must contain the identical network address part but different host address parts (also the Default Router must fulfill this requirement).
DIMSU	CGW	d	Speicherreservierung für eine Common Gateway Baugruppe und Baugruppen bezogene Teilnehmerdaten
	CGW	e	Number common gateway boards
FEASU	LM	d	LM=MOBHFA
	CM	e	CM=MOBHFA
	TYP	d	TYP=FREI Aktivieren des Leistungsmerkmals
	TYPE	e	TYPE=A Activate the feature
PERSI	COPIN	d	Class of PIN
	COPIN	e	Class of PIN
	PIN1	d	PIN (Passowrt für HFA)
	PIN1	e	PIN (password for HFA)
	PINTYP	d	PINTYP=MOBIL COPIN-Typ fuer netzweiten Transfer der COPIN im CorNet Protokoll
	COTYPE	e	COTYPE=MOBILE COPIN type
	RUFNU	d	Rufnummer des Teilnehmers
	STNO	e	Station number
	TYP=COPIN	d	Mindestens eine COPIN (1-15) muss das Attribut Mobil haben.
	TYPE=COPIN	e	At least one COPIN (1-15) must have the attribute Mobile.
	TYP=TLN	d	Teilnehemr einrichten

AMO	Parameter	Sprache/ Language	Beschreibung/ Description
	TYPE=STN	e	add a station
SBCSU	ANSCHL=IP2	d	Anschluss-Art der Geräte IP2=Anschluss ueber IP (HFA Gateway Version 2)
	CONN=IP2	e	Device Connection Type IP2=Connection via IP (HFA gateway version 2)
	ART=OPTI	d	Hauptrufnummer des IP-Telefonanschluss einrichten
		e	
	GERKON=OPTIIP	d	Geräte-Konstellation eines Teilnehmers OPTIIP=IP Sprachterminal
	DVCFIG=OPTIIP	e	Device Configuration OPTIIP=Digital IP voice terminal
	IPPASSW	d	passwort fuer ip login prozedur
	IPPASSW	e	Password for IP logon procedure
SDAT	EMERK	d	EMERK=MHFAMOE Merkmal des Heinat-Telefons EMERK=MHFATBV Merkmal des “besuchten“ Telefons
	AATTR	e	AATTR=MHFAMOE HFA home phone of visitor AATTR=MHFATBV mobile HFA phone which can be visited
	TLNNU	d	Teilnehmerrufnummer
	STNO	e	Station number
	Typ	d	TYP=MERKMAL Teilnehmermerkmale administrieren
	ATTRIBUT	e	TYPE=ATTRIBUT Administrate subscriber attributes (service=voice)
WABE	KZP=MFALGON	d	Kennzahlpunkt für Aktivierung

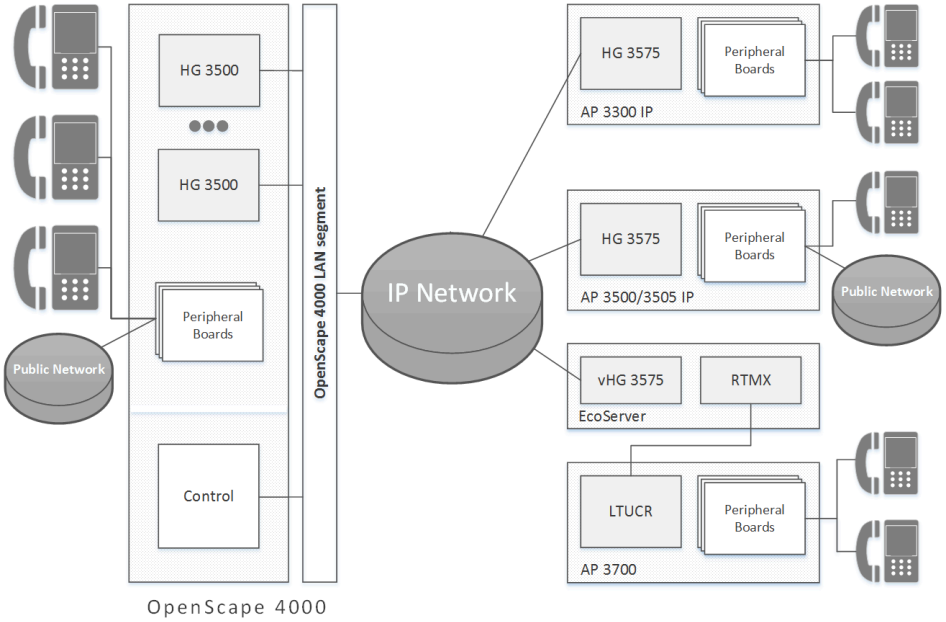
AMO	Parameter	Sprache/ Language	Beschreibung/ Description
	DAR=MFALGON	e	Logon by a mobile hfa subscriber
	KZP=MFALGOF	d	Kennzahlpunkt für Deaktivierung
	DAR=MFALGOF	e	Logoff by a mobile hfa subscriber
	PRUEF	d	Prüfumfang
	CHECK	e	Scope of check
	RNR	d	2 Rufnummern für Aktivierung / Deaktivierung (*95/*96)
	CD	e	2 station numbers for activation / deactivation (*95/*96)
	VKS	d	Verkehrssituation (5 = Teilnehmer-Vorwahl)
	CPS	e	Call progress state
	WABE	d	WABE-Gruppe
	DPLN	e	Feature access group
ZAND	APIMAX	d	Maximale Anzahl der gleichzeitig aktiven API Sessions. DB-Initialisierung: 10
	APIMAX	e	Maximum number of allowable active API sessions.
	KENNL	d	Linearisierungs- und Kompandierungskennlinien bei der PCM-Kodierung/Dekodierung. Der eingegebene Wert wird zum einen in die zentralen Anlagendaten übernommen, zum anderen bei eingerichteter LTG auch in die entsprechenden COFI-Daten. Der Wert in den zentralen Anlagendaten ist auch gültig bei der Konfiguration von NCUI-Baugruppen in IPDA-Shelfs.Es sollte daher nach Konfiguration von IPDA-Shelfs dieser Wert nicht mehr geändert werden!

AMO	Parameter	Sprache/ Language	Beschreibung/ Description
	CODE	e	Speech coding.The entered value will be issued once to central system data and once for assigned LTG in the according COFI-data. The value in central system data is also valid for configuration of NCUI-boards in IPDA shelfs. Therefore this value should not be changed after configuration of IPDA-shelfs!
	TYP=CIT	d	Konfigurieren von fiktiven Geräten, Einstellungen für API Schnittstelle
	TYPE=CIT	e	Configure virtual stations, settings for API interface
	TYP=CONFC	d	Länderspezifische Einstellung für KENNL, K- oder TDAEMPF. Dieser Zweig gilt nur für kompakte Hardware.
	TYPE=CONFC	e	Selection of country-specific settings for CODE, CONFAT STNAT. This branch is only for compact hardware.
ZIEL	AULVAR=SYSTEM	d	Systemumleitung
	CFVAR=SYSTEM	e	system call forwarding
	KART	d	KART=GEN (alle Anrufe) Kommende Belegungsart des AUL-Zieles
	ITYPE	e	ITYPE=GEN (all calls) incoming seizure of fwd feature
	QLRUFNU	d	Quellenrufnummer
	SRCNO	e	station number of source
	SI=VOICE	d	Service Sprache
	SI=VCE	e	service voice
	TYP=AUL	d	Verbindungstyp Anrufumleitung
	TYPE=FWD	e	Call Forwarding
	UART=CFNR	d	Anrufumlenkung bei nicht melden
	DTYPE=CFNR	e	call forwarding no reply
	ZLRUFNU	d	Zielrufnummer
	DESTNOF	e	destination number for forwarding

10 IP Distributed Architecture (IPDA)

10.1 IPDA Feature Description

OpenScape 4000 offers the possibility of distributing access points across an IP network. These access points are shelves which accommodate the standard OpenScape 4000 access modules. The subscriber line circuits at the access points are handled precisely as if they were linked directly - as has been customary in the past - to a OpenScape 4000 switch. Administration of all components distributed via IP is also realized as **one** system via an access point of the OpenScape 4000 system.



Overview of architecture

The “IP distributed architecture” comprises of the following main components:

• OpenScape 4000	The communication server, which also controls all components of the “IP Distributed Architecture“. The rich volume of call processing features is thus also available to the “IP Distributed Architecture“.
• HG 3500	This IP gateway module allows payload connections between subscriber line/CO and tie trunk circuits in the central part of the OpenScape 4000 system and subscriber/CO and tie trunk circuits in the distributed access points.
• IP Access Points	There are three types of IP based access points
• AP 3300 IP	This traditional Flexpack shelf with IP integration offers 16 slots for OpenScape 4000 peripheral modules

	• AP 3500 IP	19“ shelf (3 units high), which can be mounted in a 19“ rack, allows inexpensive configurations for small locations. As a basic box, it offers 3 slots for OpenScape 4000 peripheral modules. The number of slots can be increased to 7 with an AP 3505 IP expansion box (3 units high). Both the AP 3500 IP and the AP 3505 IP expansion box can be equipped with a redundant power supply.
	Both types of access point are equipped with a HG 3575 connection module, which establishes the connection to the IP infrastructure (10/100BT). The IP-based access points allow the use of the majority of current and future modules which can be operated in classic OpenScape 4000 shelves.	
• OpenScape 4000 SoftGate		The OpenScape 4000 SoftGate provides cost-effective branch offices with reliable OpenScape 4000 survivability options and an easy IT integration in the OpenScape 4000 solution and management suite. This software application offers full HiPath Feature Access (HFA) for IP Endpoints, SIP Service Provider connectivity and native SIP connectivity for trunking and subscriber with basic feature set based upon a standard server. Any OpenScape 4000 SoftGate site integrates seamless in the communication system and network like an IPDA Access Point (AP 3700 IP) - in terms of features and administration.
• Enterprise Gateway		OpenScape Enterprise Gateway is based on hardware and software of OpenScape 4000. It is successor of AP 3700-9 shelves with HG3575. The whole feature content of IP Distributed Architecture (IPDA) is available. For further information, please see OpenScape 4000 V8, Enterprise Gateway, Service Documentation.
	• OpenScape 4000 EcoServer/ OpenScape EcoServer	Enterprise GW deployment installed with optional APE (Survivable Enterprise GW)
	• AP 3700 IP	19“ shelf (10 units high), which can be mounted in a 19“ rack, features nine slots for OpenScape 4000 peripheral boards. The frame comes with three PSU modules which are operated in a 2+1 redundancy configuration.

	• LTUCR control board	The LTUCR (Line Trunk Unit Control Replacement) board is the interface between central and peripheral parts of the system. The LTUCR selects the signals from the active control unit and distributes them to the appropriate boards in the LTU shelf. The LTUCR also receives signals from the peripheral boards and transmits them to the common control.

The HG 3500 and HG 3575 modules are each equipped with two 10/100BT Ethernet connections for connecting to the IP network.

10.1.1 Scalable Increase in System Capacity

OpenScape 4000 supports up to 83 access points linked via IP (AP 3300 IP, AP 3500/3505 IP or AP 3700 IP), in addition to a maximum of 15 directly linked shelves (AP 3300 or AP 3700).

Thus, the maximum number of digital subscriber line circuits in a system can be increased to 12000.

10.1.2 Distributed Circuit Switching

With OpenScape 4000, the circuit switching of the payload (B channels) is not limited to the central switching network

- Calls within IP-based access points are switched to a local TDM switching network directly and, consequently, without runtime in the IP network. The switching network on the HG 3575 module has a capacity of 256 channels.
- Calls between different IP-based access points are switched in the IP network.
- Calls which go beyond IP-based access points are switched both in the IP network and in the central OpenScape 4000 system.

10.1.3 Time Synchronization

An exact time is required for many OpenScape 4000 functions (call detail recording, time-dependent channels, night service, etc.). All clocks in the system (up to 84) have to operate synchronously.

There are two ways of synchronizing the time:

1) The IP network has a time server, which supports time synchronization of all OpenScape 4000 processors (the central processor and all survivability units) using the Network Time Protocol.

2) A time server is **not** available in the IP network. The OpenScape 4000 platform then makes its local time available over the network for synchronizing all survivability units.

For more information on setting the date and time and the time synchronization please refer to the documentation **OpenScape 4000 V8, Installation, Configuration and Migration, Installation Guide**.

10.1.4 Call Scenarios

In order to gain a better understanding of the call processing procedures and their distribution across the components of the IP distributed architecture, a couple of typical call scenarios are described below.

10.1.4.1 Internal Access Point Call

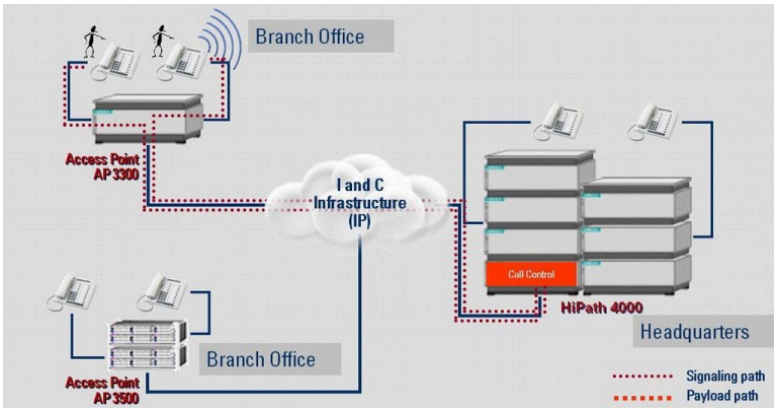


Figure 167: Signaling for an internal access point call

Signaling from and to the connected telephones is always transmitted over the IP network to the call processing infrastructure in the OpenScape 4000 central system, and from there back again.

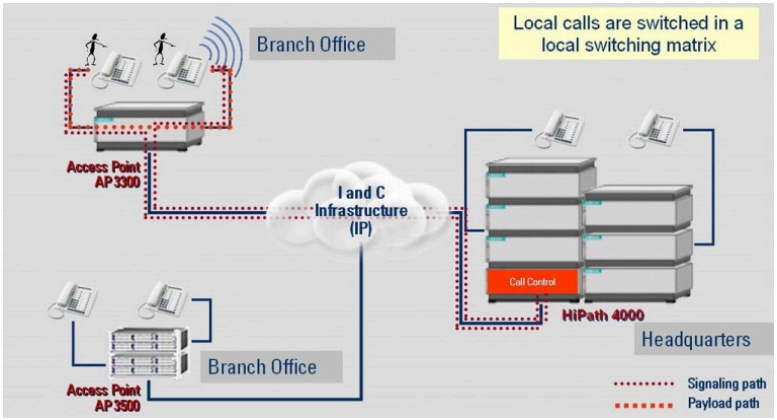


Figure 168: Voice link (payload) for an internal access point call

The central call processing infrastructure establishes the voice link and makes all features available. In this case, the voice link is switched within the access point in the TDM-based switching network of the HG 3575 module. This means that no payload is generated in the IP network and none of the channels of the transport capacity from the access point to the IP network are occupied.

10.1.4.2 Call Between Two Access Points

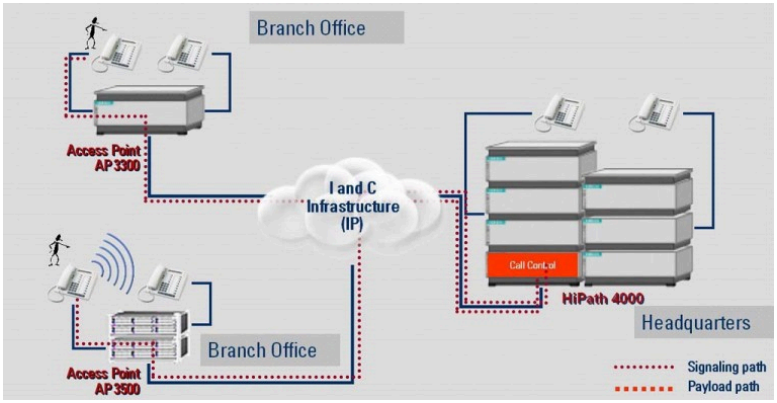


Figure 169: Signaling for an access point to another access point call

Signaling from and to the connected telephones is always transmitted over the IP network to the call processing infrastructure in the OpenScape 4000 central system, and from there back again.

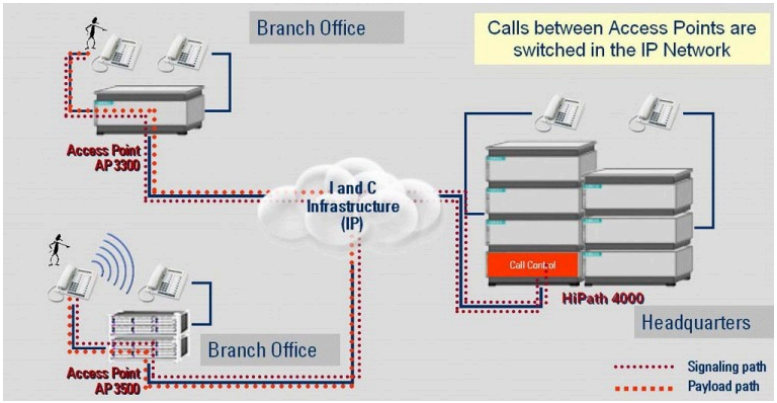


Figure 170: Voice link (payload) for an access point to another access point call

The central call processing infrastructure establishes the voice link and makes all features available. In this case, the voice link between the two access points is switched in the IP network with the aid of the HG 3575 modules. Each of the access points occupies one channel of the available transport capacity to the IP network.

10.1.4.3 Call Between an Access Point and the Central System

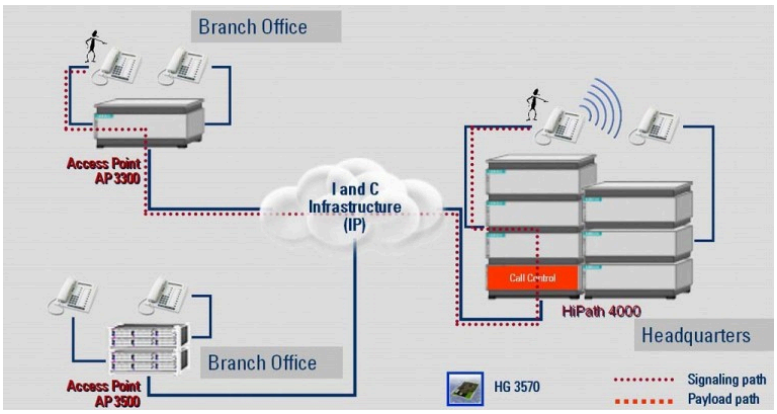


Figure 171: Signaling for an access point to a central system call

Signaling from and to the connected telephone in the access point is always transmitted over the IP network to the call processing infrastructure in the OpenScape 4000 central system, and from there back again.

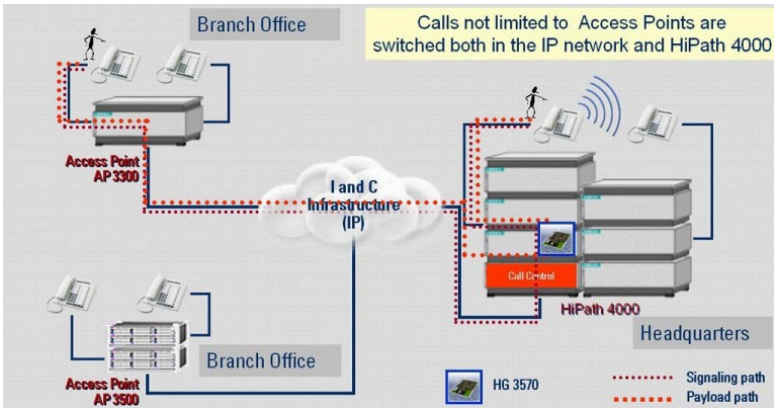


Figure 172: Voice link (payload) for an access point to a central system call

The central call processing infrastructure establishes the voice link and makes all features available. The voice link from the access point is switched to the IP network with the aid of the HG 3575 module. The HG 3500 module functions as a gateway and converts the IP data stream back into a PCM data stream that can be processed by the central system. This data stream is transferred to the connected subscriber within the central system. The call is therefore switched in both the IP network and in the OpenScape 4000 central system. The access point and the gateway module each occupy one channel of the available transport capacity to the IP network.

10.1.4.4 Trunk Access / Networking

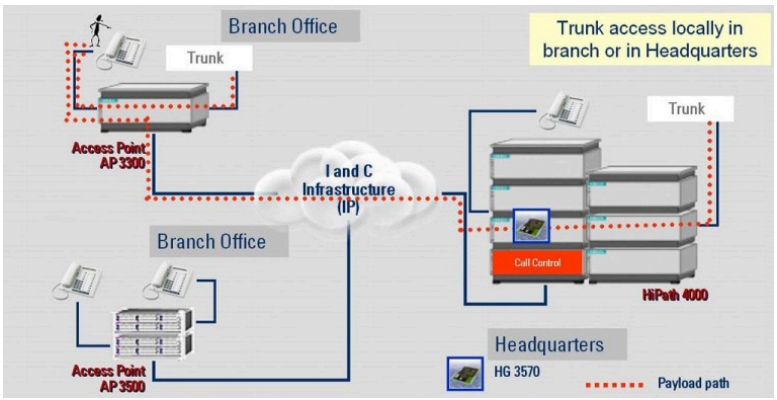


Figure 173: Trunk Access/Networking

Local trunk access can also be set up in an access point. The least cost routing function of the OpenScape 4000 decides which trunk access to use based on the subscriber's location.

10.1.5 Survivability for Signaling and Payload

In the basic configuration (without the survivability features), an IPDA installation function depends completely on the availability and reliability of the LAN/WAN infrastructure used. The failure of an access point's IP connection leads to failure of the access point.

Total failure of the IP infrastructure leads to the failure of all access points. Only the central system and the "classic" peripheral units connected continue to work.

Survivability for signaling and payload ensures that OpenScape 4000 also offers the greatest availability in distributed operation. The public telephone network/ an alternative LAN connection (in the case of Signaling Survivability) can be used as an alternative route in the event of an IP network failure or if the IP network temporarily fails to provide the requisite quality for voice transmission.

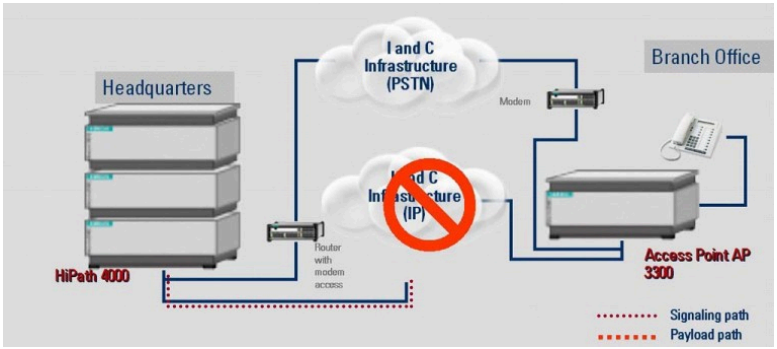


Figure 174: Survivability: failure in the IP network

If the IP connection from an access point/OpenScape 4000 SoftGate to the central system fails, there can be no interaction between the access point/ OpenScape 4000 SoftGate and the central system. Messages from the terminal devices and trunks in the access point/OpenScape 4000 SoftGate

are temporarily buffered on the (v)HG 3575, while messages from the central system are buffered in the central processor. If the duration of the failure exceeds a definable limit, the Access Point/OpenScape 4000 SoftGate is reset, thereby disconnecting all calls.

10.1.5.1 Signaling Survivability

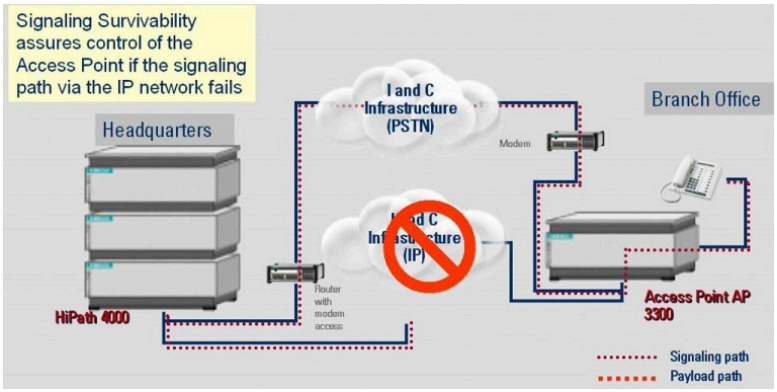


Figure 175: Signaling survivability examples: Signaling via PSTN

Signaling survivability takes over control of the Access Point/OpenScape 4000 SoftGate if signaling is no longer possible via the IP network.

For more information, see Section 2.6, “Signaling Survivability”

10.1.5.2 Payload Survivability

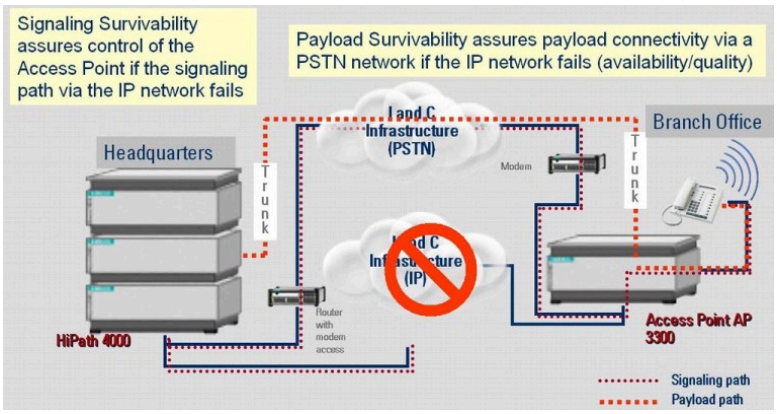


Figure 176: Payload survivability: Alternative route for the payload via PSTN

Payload survivability allows *internal system calls* to be routed via the CO. The OpenScape 4000 in effect "calls itself" and establishes an internal call between different parts of the system. The route for payload survivability is also selected automatically as a spillover route if the entire capacity of the HG 3575 is already in use in the IP network.

IMPORTANT: For information about feature restrictions with payload survivability, see Chapter 2, “Restrictions”.

10.1.6 Signaling and Payload Separation (SPS)

10.1.6.1 Feature Description

“Signaling and Payload Separation” which enables OpenScape 4000 in an IPDA environment to split the path of the network traffic in the meaning of

- signaling from host system (call control) to the access point is routed over the IP customer network (Enterprise WAN).
- payload is routed over the PSTN Network using payload survivability connections.

Signaling and payload separation is based on the existing survivability solution and therefore the signaling path is routed in the same way as in earlier OpenScape 4000 versions. The payload (RTP-Stream) is routed across connections built up from WAML or ISDN-Router via PSTN-Lines between the locations.

10.1.6.2 Prerequisites

- Central office connectivity via ISDN- lines.
- Signaling and payload connections has to be built up via WAML or external ISDN-Router.
- Bandwidth limitation has to be performed by the Resource Manager.
- Signaling and payload separation is restricted to star topology/IPDA-infrastructures.
- Using HG 3500 separate boards are needed for trunking and WAML functionality.
- Currently only 8 static routes can be configured on the HG 3500. Therefore the number of subnets for the APs is limited. In the worst case (each AP in another subnet, no combination of subnets via the netmask possible) this limits the amount of AP's using SPS without an external router to 8. In addition only 8 WAMLs can be used in the host.
- Delays in signaling may cause wrong interpretation with a result of wrong call treatment and can affect the features behavior (e.g. Hunt group, call pick up groups)
- Due to the fact, that in call pickup scenarios there is no connection before the picking user performs the pickup, cut trough times might be longer in SPS scenarios
- Payload separation is destination oriented and restricted to one OpenScape 4000 system. If other systems are connected to the OpenScape 4000 no networking features will be supported (e.g. network wide pick-up).
- Different trunk groups must be configured for payload separation without intercept parameters.

10.1.6.3 Configuration

For information on the configuration please refer to Section 2.10, “Signaling and Payload Separation (SPS)”.

10.1.7 Redundant LAN Interface

For increased resilience, IPDA V2.0 boards HG 3500 and HG 3575 should be connected with two LAN cables to different switches (please refer to Section 6.4, “Redundant LAN Interface”).

10.1.8 LAN Monitoring

The LAN monitoring feature has been introduced with the feature Separated Duplex. The separated LAN infrastructure of BPA and BPB increases the probability that the BP might still be able to establish LAN connections to the APs, even if there is a LAN problem at the active BP.

With the IPDA LAN L1 link monitoring feature a switch is only triggered by the LAN monitoring function if the L1 link monitoring does not work, i.e. the L1 links from the active BP and the BP are still active although all APs have failed.

10.1.8.1 Feature Description

Dependability checks during normal operation mode every minute the status of the LAN connections to the configured APs. If the check detects that no configured AP is connected and several conditions (see Section 1.8.2, “Service Information” > Conditions for switchover) are fulfilled, a switchover is triggered to try whether the BP can establish LAN connections to the APs.

In this implementation the BP is not asked before the switchover whether LAN connections to the APs are possible. Instead one switchover is triggered and then it is checked at the new active BP whether LAN connections can be established now. If not, then another switchover will be triggered back to the originally active BP.

If a BP successfully sets up a LAN connection to an AP, the LAN monitoring feature is reinitialized on this BP so as to enable a further switchover should all AP connections be lost again.

Special situations

- There is a special situation when `EXEC-USSU:UPDATAP;` is executed. In this scenario the LAN connections to all APs are stopped and restarted. This could trigger a switchover because all conditions of the LAN monitoring feature are fulfilled. Therefore dependability checks for this update scenario to avoid an unnecessary switchover.
- If the AMO command `RES-USSU:ALLE;` is executed, all APs will be reset. In order to ensure that there is no undesired switching in this scenario also, a switchover delay of 1 minute was integrated after which the switchover conditions are tested again. It is only then if these conditions are still fulfilled that the switchover is started.

10.1.8.2 Service Information

Conditions for switchover

The following conditions are checked before a switchover is triggered:

- The BP is active and in normal operation mode (i.e. last restart/reload is finished).
- There has not already been triggered a switchover because of this LAN monitoring feature.
- The partner BP is in state and the own DB and the DB of the partner BP are consistent. (-> necessary conditions for a successful switchover).

Note

If it happens at some point that after a second switchover caused by LAN monitoring feature the active BP still does not have LAN connectivity with APs then it will stay in this state until the defective LAN (on the active BP) is back in service. Then the LAN monitoring will start to work again.

A practical example: when both LANs are cut off simultaneously, LAN monitoring will do two switchovers, then will stop monitoring until the active BP's LAN is repaired.

DEP ADVISORY messages

The following DEP ADVISORY messages have been implemented for the LAN monitoring feature:

1) switchover has been triggered:

F4266 M8 N0096 SOFTREST BPA DEP ADVISORY xx-xx-xx yy:yy:yy

ALARM CLASS:CENTRAL:005

FORMAT:42

NO AP SHELF CONNECTED

PARTNER CC AVAILABLE

SWITCHOVER INITIATED

1) switchover is rejected because of AMO ZANDE switch NOLANMON:

F4266 M8 N1979 NO ACT BPA DEP ADVISORY xx-xx-xx yy:yy:yy

ALARM CLASS:CENTRAL:023

FORMAT:42

NO AP SHELF CONNECTED,

SWITCHOVER REJECTED:

CHECK AMO ZANDE NOLANMON

1) switchover is rejected because already one switchback has been triggered before:

F4266 M8 N1979 NO ACT BPA DEP ADVISORY xx-xx-xx yy:yy:yy

ALARM CLASS:CENTRAL:023

FORMAT:42

NO AP SHELF CONNECTED,

SWITCHOVER REJECTED:

NO FURTHER SWITCHBACK

1) switchover is rejected because partner BP is not :

F4266 M8 N1979 NO ACT BPA DEP ADVISORY xx-xx-xx yy:yy:yy

ALARM CLASS:CENTRAL:023

FORMAT:42

NO AP SHELF CONNECTED,

SWITCHOVER REJECTED:

PARTNER IS NOT

10.1.8.3 Generation (Example)

The LAN monitoring feature is activated by default.

It can be deactivated with AMO ZANDE parameter **NOLANMON**:

CHANGE-ZANDE:TYPE=ALLDATA2,NOLANMON=YES;

NOTICE: Although the LAN switchover feature is activated by default, it can be that some customers prefer not to switchover when they have a high number of fixed LTU shelves and only a single or a few IP shelves.

10.1.8.4 Relevant AMOs

AMO	Parameter	Sprache/ Language	Beschreibung/ Description
ZANDE	NOLANMON	d	Leistungsmerkmal LAN-Überwachung
	NOLANMON	e	LAN Monitoring feature

10.1.9 Different Time Zones (DTZ)

The “Different Time Zones (DTZ)“ feature is used in situations when an IPDA shelf or access point (AP-IP) or HFA IP telephones are located in different time zones than the host system. In these cases, the local time of day should be shown instead of the system time on the display of the digital telephones that are connected to the remote AP or on the display of the HFA IP telephones.

For a detailed description, refer to the section „Different Time Zones (DTZ)“.

10.1.10 A-Law/µ-Law Conversion in AP Shelf

It is possible to connect telephones in AP shelves that work with companding algorithms different to the host system (e.g. host system in Germany (A-law), access point in the USA (µ-law)).

For a detailed description, refer to Section 2.15, “A-Law/µ-Law Conversion in AP Shelf”.

10.1.11 Different Announcements, Tones and MFV DialTone Receivers per Access Point

It is possible to configure different languages/countries for each access point with AMO UCSU. Therefore different access points can have the same or different SIU-Init-Data files.

For a detailed description, refer to Section 2.16, “Different Announcements, Tones and DTMF DialTone Receivers per Access Point”.

10.1.12 Different Display Languages per Access Point

With HiPath 4000 V6 the system offers 5 simultaneous display languages for the terminals configured in the host system for the complete system (including access points).

Starting with OpenScape 4000 V7 it is possible to configure 5 different languages for each access point (AP shelf) different to the host system. Therefore a terminals connected to an acces point can have a different display language than a terminals connected to the host system.

For a detailed description, refer to Section 2.17, “Different Languages/ National Character Sets for Displaying Text for Individual Access Points”.

10.1.13 Additional Features

- High voice quality
- On account of longer voice signal delays caused by the system in the IP network, voice quality will be impaired by echo unless this is removed prior to transmission. The HG 3500 and HG 3575 modules therefore feature an integrated echo canceler.

  Lower bandwidth requirements

  If voice is transmitted via IP in uncompressed form (pursuant to G.711), the bandwidth requirement is greater than in the case of ISDN on account of the packaging in the IP protocol.

  If less bandwidth is to be occupied, the voice signal can be compressed. HG 3500 and HG 3575 offer optional compression pursuant to the G.729A standard (only 8 Kbps, instead of 64). Furthermore, additional bandwidth can be saved by suppressing voice pauses. Silence suppression suppresses the transmission of silence on the line. (G.729AB, or G.711 Annex 2)
- Support for Quality of Service in the IP network through prioritization

- OpenScape 4000 IP distributed architecture supports prioritization in the IP network on the basis of the following standards:
  - IEEE 802.1 p/q (VLAN Tagging) on Layer 2
  - IETF RFC 2474 (DiffServ) on the IP Layer
- Transport capacity in the IP network
- HG 3500 and HG 3575 can transmit up to 120 B channels simultaneously over the IP network regardless of the hardware and configuration in use (see "Gateways HG 3500 and HG 3575, Section 2.6, “B Channels”).
- Support of network management on the basis of SNMP
- HG 3500 and HG 3575 support network management on the basis of the SNMP protocol. Statistical data from the applicable standard MIBs and additional data from proprietary MIBs can be queried.

10.2 Configuring the IPDA Feature

IP distributed architecture is rather a platform expansion than a typical new feature. Therefore, the configuration of this feature is broken down in the following section into typical steps, which are to be performed in consecutive sequence:

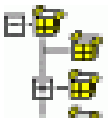
- Configuration: OpenScape 4000 LAN segment - Section 2.1, “OpenScape 4000 LAN Segment”
- Configuration: Access Point (*networked* or *direct link*) - Section 2.2, “Access Point”
- Configuration: HG 3500 as HG 3570 - Section 2.3, “HG 3500 as HG3570 in the OpenScape 4000 System”
- Configuration: Subscriber, trunk and tie trunk connections in access points - Section 2.4, “Subscriber, CO/Tie Trunk Circuits in Access Points”

If necessary, the following steps are performed subsequently:

- Configuration: Special routes - Section 2.5, “Special Routes”
- Configuration: Signaling survivability - Section 2.6, “Signaling Survivability”
- Configuration: Quality monitoring for the signaling connection over IP - Section 2.7, “Quality Monitoring for the Signaling Connection over IP”
- Configuration: Source dependent routing - Section 2.8, “Source Dependent Routing”
- Configuration: Payload survivability - Section 2.9, “Payload Survivability”
- Signaling and payload separation - Section 2.10, “Signaling and Payload Separation (SPS)”
- Divert call in survivability mode to another access point - Section 2.11, “Divert Call in Survivability Mode to another Access Point”
- Configuration: External music on hold - Section 2.12, “External Music on Hold”
- Information on CMI - Section 2.13, “Information on CMI”
- Configuration: IP address changes - Section 2.14, “IP Address Changes”
- These notes must be observed if the IP addresses in the OpenScape 4000 LAN segment are to be changed in an active system (for example, because the network carrier changes the network address).
- Configuration: a-law/µ-law conversion - Section 2.15, “A-Law/µ-Law Conversion in AP Shelf”

- Configuration: Different announcements, tones, DTMF dial tone receivers per access point - Section 2.16, “Different Announcements, Tones and DTMF DialTone Receivers per Access Point”
- Configuration: Different display languages/national character sets per access point - Section 2.17, “Different Languages/ National Character Sets for Displaying Text for Individual Access Points”

The corresponding sections contain configuration examples and detailed explanations of all requisite AMOs and AMO parameters. A distinction is made between

	configuration with Configuration Manager and
	configuration with AMO.

The creation of the “Access point Emergency“ feature is described in “Access Point Emergency (APE)”, Chapter 2, “Configuring the APE Feature (Access Point Emergency)”.

10.2.1 OpenScape 4000 LAN Segment

The OpenScape 4000 LAN segment is that part of the customer network in which the IP components of the central system and direct link (i.e. not via router) access points are installed.

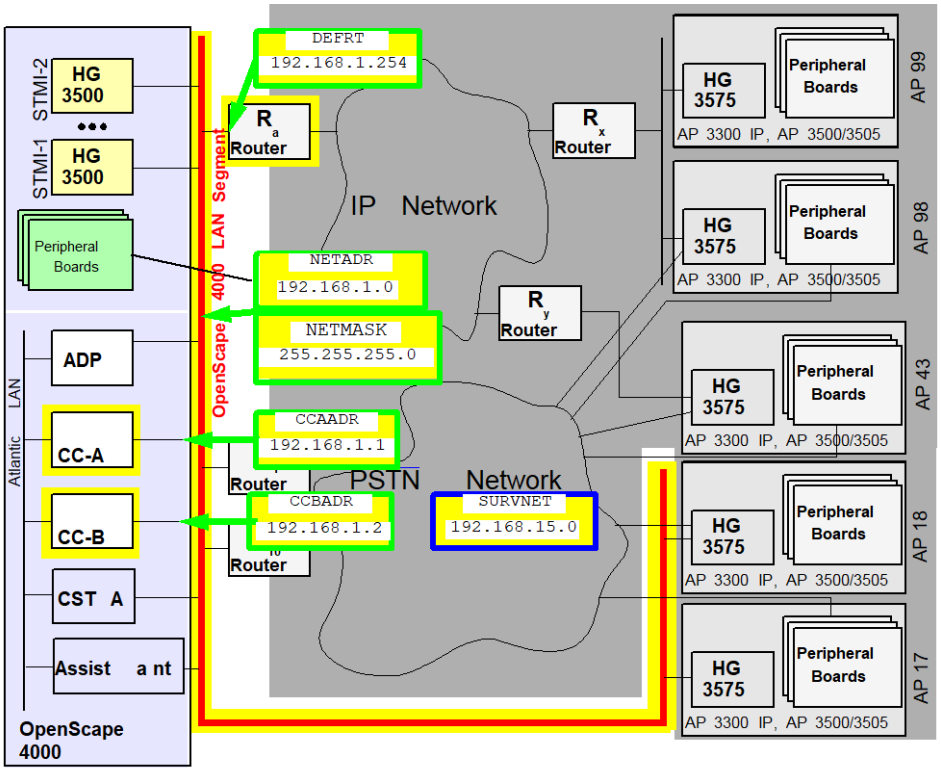


Figure 177: OpenScape 4000 LAN segment

ADD-SIPCO:	NETADDR=192.168.1.0,	NETMASK=255.255.255.0,
	IPMODE=IPV4,	DEFRT=192.168.1.254,
	CCAADDR=192.168.1.1,	CCBADDR=192.168.1.2,
	SURVNET=192.168.15.0;	

At maximum capacity, a configuration requires a considerable number of IP addresses in this network, namely.

• CC-A, CC-B, ADP:	3
• OpenScape 4000 Assistant:	1
• OpenScape 4000 CSTA:	1
• HG 3500:	Up to 83
• Directly linked HG 3575:	Up to 83
• Survivability routers:	Up to 10

Therefore, it is advisable to configure a dedicated LAN segment for the central part of a large OpenScape 4000 installation and not permit any more nodes within that segment (particularly file servers, etc.)

For demo installations in which the OpenScape 4000 LAN segment remains isolated, IP addresses from the private address range pursuant to RFC 1597 can be used. These do not require international coordination. For example, the

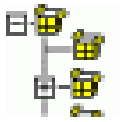
range from 192.168.1.1 to 192.168.1.255 with netmask 255.255.255.0 can be recommended as the Class C address range.

Generation

Addresses (LSNET)

The first step in configuring IP distributed architecture involves the configuration of the OpenScape 4000 LAN segment.

Configuration:

	**Configuration Management > System Data > IPDA > IPDA System Data** Click **Search**, enter the required IP addresses and **Save**.
	`ADD-SIPCO:NETADDR=192.168.1.0,NETMASK=255.255.255.0, DEFRT=192.168.1.254,IPMODE=IPV4,CCAADDR=192.168.1.1, CCBADDR=192.168.1.2,SURVNET=192.168.15.0;`

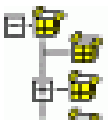
IMPORTANT: Although the CCA/CCB address already had to be entered when the configuration was performed with the LAN Wizard, it has to be configured again here with AMO SIPCO.

If an isolated configuration is to be set up, the default router must be configured with the zero address `0.0.0.0`. In this case, only “direct link“ access points can be configured (see Section 2.2.2, “Configuring a “Direct Link“ Access Point”). In Figure 12 “OpenScape 4000 LAN segment”, Router Ra is the default router.

If there is no second processor, the **CCBADDR** parameter need not be specified.

The **SURVNET** parameter can be dispensed with if signaling survivability is not required. If, however, the customer has purchased signaling survivability, i.e. if the corresponding license counter is greater than zero, then a survivability network address (see section **Signaling Survivability**) must be specified. This can also be achieved with a dummy entry (zero address `0.0.0.0`), though the signaling survivability function is not available in this case.

The licenses for signaling survivability can be queried as follows:

	**Configuration Management > HiPath Inventory Management > HIM System Data > Feature > Marketing Units** Click **Search** > **Sales Features** tab > **Signaling Survivability** entry
	`DISP-CODEW;` “SIGNALING SURVIVABILITY“ entry

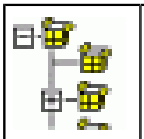
The values specified with ADD-SIPCO are immediately valid.

IMPORTANT: Prior to `ADD-SIPCO`, use **ping** to check that the IP addresses given to you by the administrator are reachable. **CCAADDR** and **CCBADDR** must not be reachable as this would indicate that the corresponding address had already been assigned. **DEFRT** must be reachable (if not `0.0.0.0`).

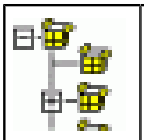
IMPORTANT: **Following** `ADD-SIPCO` the active processor must be reachable in its network segment. The standby processor in duplex systems does not respond (as long as it is in standby mode). Since routes have not yet been configured, the active processor cannot answer ping requests from other network segments!

Change:

All parameters configured here can be changed later.

	**Configuration Management > System Data > IPDA > IPDA System Data** Click **Search**, change the addresses and **Save**.
	`CHANGE-SIPCO:TYPE=LSNET;`

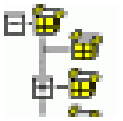
The parameters are not immediately effective after the CHANGE, but only once the system has been restarted. The database must be backed up beforehand to disk.

	The restart can only be performed in expert mode. **Expert Mode > Expert Access > Open ...<IP> with AMO** (see AMO command)
	`EXEC-UPDAT:BP,ALL; EXEC-REST:SYSTEM,RESTART;`

IMPORTANT: Changing the IP address has multifarious effects on a running system. If changes are necessary, a strict change sequence must be complied with, or else the access points will be irrevocably disconnected. In this context, see Section 2.14, “IP Address Changes”.

Delete:

If, for instance, IPDA is to be completely removed from the system after a test, all access points and HG 3500, as well as the SIPCO configuration, also have to be deleted after the uninstall routine is completed. The links/LAN modules for the OpenScape 4000 LAN segment can then also be removed. You must restart the system.

	Deletion can only be performed in expert mode. **Expert Mode > Expert Access > Open ...<IP> with AMO** (see AMO command)
	`DELETE-SIPCO;` `EXEC-UPDAT:BP,ALL; EXEC-REST:SYSTEM,RESTART;`

List of AMO parameters for Add / Change:

Table 30: AMO SIPCO parameters in ADD branch or for CHANGE under TYPE=LSNET

AMO	Parameter	Sprache/ Language	Beschreibung/ Description
SIPCO	NETADR	d	Netzadresse des OpenScape 4000 LAN Segments gilt für CC-A, CC-B, alle HG 3500 (STMI2/4/ STMIX/STMIY), Default-Router, Survivability-Router und direkt angeschlossene Access Points
	NETADDR	e	Network Address of the OpenScape 4000 LAN Segment valid for CC-A, CC-B, every HG 3500 (STMI2/4/STMIX/STMIY), default router, survivability router and directly linked Access Points
	NETMASK	d	Netzmaske des OpenScape 4000 LAN Segments gültig wie NETADR
	NETMASK	e	Netmask of the OpenScape 4000 LAN Segment valid like NETADDR
	DEFRT	d	Default-Router im OpenScape 4000 LAN Segment über diesen Router sollen alle nicht direkt im OpenScape 4000 LAN Segment angeschlossenen Access Points von den HG 3500 Baugruppen erreicht werden. Angegeben wird die IP-Adresse der Routers im OpenScape 4000 LAN Segment. Falls kein Default-Router benutzt werden soll, z. B. für isolierte Demo-Installationen mit “direct link“ APs, muss die Adresse 0.0.0.0 angegeben werden.

AMO	Parameter	Sprache/ Language	Beschreibung/ Description
	DEFRT	e	Default Router in the OpenScape 4000 LAN Segment via this router all Access Points that are not directly linked to the OpenScape 4000 LAN Segment shall be reached by all HG 3500 boards.. The IP address of this router in the OpenScape 4000 LAN Segment is to be given. If no default router shall be used, e.g. for stand-alone demo installations with “direct link“ APs, give the address 0.0.0.0.
	IPMODE	d	IP Mode. Muss für IPDA **IPV4** sein.
	IPMODE	e	IP mode. Must be set to **IPV4** for IPDA.
	CCAADR	d	IP-Adresse des CC-A Prozessors im OpenScape 4000 LAN Segment
	CCAADDR	e	IP address of the CC-A Prozessor in the OpenScape 4000 LAN Segment
	CCBADR	d	IP-Adresse des CC-B Prozessors im OpenScape 4000 LAN Segment Nicht angeben, wenn kein CC-B im System
	CCBADDR	e	IP address of the CC-B Prozessor in the OpenScape 4000 LAN Segment Omit, if no CC-B in the system
	SURVNET	d	Netzadresse des Survivability Netzes Die Netzmaske für das Survivability Netz ist mit 255.255.255.0 ebenso fest vorgegeben wie die Adressierung der einzelnen Knoten. Die Survivability-Router 1..10 haben die Adressen 1..10, die Access Points 17..99 die Adressen 17..99 im letzten Byte. Die vorgegebene Netzmaske schränkt die Klasse (A,B oder C) der Netzadresse nicht ein. Das Survivability Netz kann ein Subnetz eines Klasse A Netzes mit Netzmaske 255.255.255.0 sein.

AMO	Parameter	Sprache/ Language	Beschreibung/ Description
	SURVNET	e	Network Address of the Survivability Network The netmask for the Survivability Network is fixed to 255.255.255.0 as well as the individual node adresses. The survivability routers 1..10 are addressed 1..10, Access Points 17..99 have address 17..99 in the last byte. The given netmask does not limitate the class (A,B or C) of the network address. The Survivability Network can be a subnet of a class A network with netmask 255.255.255.0.

Quality of Service Parameters (DIFFSERV)

The following parameters can be set:

1) For QoS support on Layer 2 to IEEE 802.1 q/q [`VLAN, VLANID`]

- For QoS support on Layer 3 to IETF RFC 2474 (DiffServ) [`TOSPL, TOSSIGNL`]
- the lowest port used for payload connections (UDP/RTP+RTCP) [`UDPPORT`]

The Ethernet interface setting **must** be **identical** for all connected interface partners (CC-A and CC-B or LAN switches, routers).

IMPORTANT: The setting of a fixed interface partner leads to problems with the “Autonegotiate“ setting of the other partner. **Caution:** Incorrect settings cannot normally be detected by the system and therefore go unreported. If one device is operating in full duplex and the other in half duplex mode, this is not immediately noticeable. Where there is a high payload, the device set to half duplex will report a higher number of late collisions and the packet delay will increase sharply. If the LAN ports with which CC-A and CC-B are connected do not support autonegotiation, or if autonegotiation does not function reliably, the Ethernet interfaces of the central processors can be set to fixed values.

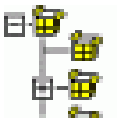
VLAN tagging should only be activated when all routers in the network segment of the access point support VLAN tagging. The same applies for the DiffServ CodePoints. If the routers do not support DiffServ, the standard TOS values must be configured without DiffServ. If DiffServ is supported, but not the CodePoints, the values specified by the network carrier must be configured.

Given that some network component vendors only support prioritization with VLAN ID > 0 pursuant to IEEE 802.1 p/q, the VLAN ID can also be set. The HG 3575 module generally sets the priority bits when the VLAN option is activated. For values, see Table 3 “TOS values” in document “Gateways HG

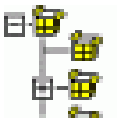
3500 and HG 3575”. According to the standard, the VLAN ID must then be set to zero, which also happens for the default setting.

The parameters for configuring the TOS bytes for the various traffic types are provisioned with the DiffServ CodePoints pursuant to the company’s QoS Recommendation. VLAN tagging pursuant to IEEE 802.1 p/q is deactivated (**VLAN=NO**).

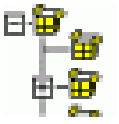
If VLAN tagging pursuant to IEEE 802.1 p/q is supported in the OpenScape 4000 LAN segment, it can be activated as follows:

	**Configuration Management > System Data > IPDA > IPDA System Data** Click **Search**, activate the **VLAN Tagging** checkbox under **Type of Service** on the **System Data** tab, then **Save**.
	`CHANGE-SIPCO:TYPE=DIFFSERV,VLAN=YES;`

If DiffServ is not supported, the TOS bytes must be configured with content pursuant to RFC 791 (see Table 3 “TOS values” in document “Gateways HG 3500 and HG 3575”).

	**Configuration Management > System Data > IPDA > IPDA System Data** Click **Search**, enter the TOS values under **Type of Service** on the **System Data** tab, then **Save**.
	`CHANGE-SIPCO:TYPE=DIFFSERV,TOSPL=16,TOSSIGNL=20;`

If either the **VLAN** or **VLANID** parameter has been changed, an update must be performed on the hard disk and then the system must be restarted.

	**Configuration Management > Network > System** Click **Save** on the Action pull-down menu. The restart can only be performed in expert mode. **Expert Mode > Expert Access > Open ...**<IP> with AMO (see AMO command)
	`EXEC-UPDAT:BP,ALL; EXEC-REST:SYSTEM,RESTART;`

Note:

VLAN tagging changes the packet header. Many L2 switches or routers understand either packets with or without tagging. In other words,

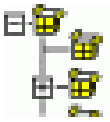
- the relevant switches/routers also have to be adjusted.

- while the settings do not correspond, it is possible that packets will not be transmitted.
  - the conversion of the HG 3500 system interrupts payload connections
  - the conversion of the OpenScape 4000 CCs interrupts the contact to all access points

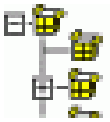
  A change of **TOSPL** is directly loaded on all HG 3500s and becomes effective immediately, without the operation of the modules having to be interrupted.

  The parameter **TOSSIGNL** does not become effective until the connection for which the **TOS** value is set has been cleared down and then set up again.

  The disconnection and re-establishment of the links between the OpenScape 4000 central system and access point can be realized through
- a soft restart on the OpenScape 4000 system, which then affects all subscribers

	The soft restart can only be performed in expert mode. **Expert Mode > Expert Access > Open ...**<IP> with AMO (see AMO command)
	`EXEC-REST:UNIT,BP,SOFT;`

- through DEACTIVATE-USSU and ACTIVATE-USSU for every individual access point, which then only affects the respective subscribers.

	**Configuration Management > System Data > IPDA > IPDA Access Point** Click **SEARCH** and select the access point. Click **Deactivate** on the Action pull-down menu. Once the system has confirmed deactivation of the AP, reactivate it with **Activate**.

	`DEACTIVATE-USSU:LTU=xx;`
	
	`ACTIVATE-USSU:UNIT=LTG,LTU=xx;`

The TOS bytes at the access points are configured specifically for every access point.

If you want to locate the payload connections in a customer network in a specific port range for reasons of port-based prioritization, for example, then this can be set as follows:

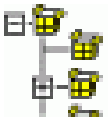
	**Configuration Management > System Data > IPDA > IPDA System Data** Click **Search**, enter the base address of the UDP port under **Type of Service** on the **System Data** tab, then **Save**.
	`CHANGE-SIPCO:TYPE=DIFFSERV,UDPPORT=40000;`

Table 31: AMO SIPCO parameters in CHANGE branch under TYPE=DIFFSERV

AMO	Parameter	Sprache/ Language	Beschreibung/ Description
SIPCO	TOSPL	d	TOS-Byte für die VoIP Payload-Verbindungen zwischen OpenScape 4000 und Access Point. Gültig für Pakete von beliebigen HG 3500 in Richtung Access Point.
	TOSPL	e	TOS Byte for the VoIP payload connections between OpenScape 4000 and Access Point. Valid for packets from any HG 3500 towards Access Point.
	TOSSIGNL	d	TOS-Byte für die Signalisierungsverbindungen zwischen OpenScape 4000 und Access Point. *(auch für Supervisory und RTO)* Gültig für Pakete vom CC-A, CC-B in Richtung Access Point.
	TOSSIGNL	e	TOS Byte for the Signaling connections between OpenScape 4000 and Access Point. *(also for Supervisory and RTO)* Valid for packets from CC-A, CC-B towards Access Point.
	VLAN	d	Schaltet VLAN-Tagging nach IEE 802.1p/q ein (JA) bzw. aus (NEIN). Gültig für VoIP Payload-Verbindungen von beliebigen HG 3500 in Richtung Access Point. Gültig für Pakete vom CC-A, CC-B in Richtung Access Point.

AMO	Parameter	Sprache/ Language	Beschreibung/ Description
	VLAN	e	Switches VLAN Tagging according to IEEE 802.1p/q on (YES) or off (NO). Valid for VoIP payload connections from any HG 3500 towards Access Point. Valid for packets from CC-A, CC-B towards Access Point.
	VLANID	d	VLAN-ID Wert für alle HG 3500 sowie CC-A und CC-B Nur von Bedeutung, wenn VLAN=JA. 12 Bit Wert, der gemäß IEEE 802.1 p/q Standard auf Null gesetzt sein muss, wenn Priorisierung verwendet wird (VLAN=JA). Von dieser Standardeinstellung darf nur abgewichen werden, wenn Netzwerkkomponenten bestimmter Hersteller erzwingen, dass bei Nutzung der Priorisierung eine VLAN-ID > 0 zu verwenden ist.
	VLANID	e	VLAN-ID value for all HG 3500, CC-A and CC-B Only relevant if VLAN=YES. 12 Bit value that, according to IEEE 802.1 p/q, has to be set to zero when prioritization is used (VLAN=YES). This standard setting may only be changed, if network components of certain vendors enforce the usage of VLAN-ID > 0 while using prioritization.
	UDPPORT	d	Einstellung des Basis-Ports (niedrigste Portnummer) für Payloadverbindungen im IPDA-System Für jede Payload-Verbindung werden an den beteiligten Gateways HG 3500 bzw. HG 3575 ein UDP Port für RTP und ein weiterer für RTCP benötigt. Die Portnummern werden in einem Bereich von [UDPPORT .. UDPPORT+247] vergeben. RTP belegt dabei immer eine gerade Nummer, RTCP die nächst höhere ungerade. Wertebereich: [4352 .. 65038], nur gerade Zahlen erlaubt.

AMO	Parameter	Sprache/ Language	Beschreibung/ Description
	UDPPORT	e	Setting of the Base Port (lowest port number) for Payload Connections in the IPDA System For every payload connection one UDP port is required for RTP and another for RTCP. The port numbers are assigned in a range of [UDPPORT .. UDPPORT+247]. RTP always uses an even number, RTCP the next higher odd one. Value range: [4352 .. 65038], only even numbers allowed.

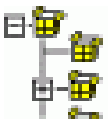
Additional parameters

With ADD-SIPCO, additional system parameters are also set to default values which can be changed by means of CHANGE-SIPCO. These parameters are broken down into 2 groups.

System timing (TIMING)

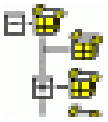
Under TYPE=TIMING, central values of the system timing can be set for the monitoring of IP links. If the values set here are exceeded, the system switches the communication between OpenScape 4000 and access point to the “signaling survivability“ modem link or the access point is temporarily put out of operation.

In order to render the changed values in the affected access points effective, they **all** have to be restarted with

	**Configuration Management > System Data > IPDA > IPDA System Data** Click **Search** and select the access point. Click **Execute** on the Action pull-down menu and select the mode of action **Update AP**, confirm with **OK**.
	`EXEC-USSU:MODE=UPDATAP,LTU=xx;`

IMPORTANT: Connections are cleared down without further warning. Prior to the `EXEC-USSU:UPDATAP`, the configuration must be updated on the system hard disk. Otherwise, the data on the system would conflict with the data on the HG 3575 when the system is reloaded and could only be synchronized again with `EXEC-USSU:UPDATAP`, LTU number, `UL`.

If the PINGTIME parameter has been changed, **all** HG 3500s must also be restarted with

	**Configuration Management > System Data > Maintenance > Board Maintenance** Click **Search** and select all **STMI2**, **STMI4 and STMIX/STMIY**. Click **Execute** on the **Action** pull-down menu, select **Restart** and confirm with **OK**.
	RESTART-BSSU:ADDRTYPE=PARTNO,PARTNO=Q2316-X; and RESTART-BSSU:ADDRTYPE=PARTNO,PARTNO=Q2316-X10; and RESTART-BSSU:ADDRTYPE=PARTNO,PARTNO=Q2324-X500; and RESTART-BSSU:ADDRTYPE=PARTNO,PARTNO=Q2316-X510; and RESTART-BSSU:ADDRTYPE=PARTNO,PARTNO=Q2343-X; and RESTART-BSSU:ADDRTYPE=PARTNO,PARTNO=Q2361-X

IMPORTANT: Existing links are disconnected.

IMPORTANT: It is crucial that TIMING changes are really loaded at all access points and HG 3500s, as otherwise the system reaction to the timer sequences would be inconsistent!

Table 32: AMO SIPCO parameters in CHANGE branch under TYPE=TIMING

AMO	Parameter	Sprache/ Language	Beschreibung/ Description
SIPCO	PINGTIME	d	Zeitdauer, während der nach einer **schlechten** VoIP Payload-Verbindung zwischen 2 HG 3500/HG 3575 die Verbindungsqualität getestet wird. Ist die Verbindungsqualität bei Beendigung einer Verbindung zwischen 2 HG 3500/75 als schlecht markiert, wird für die Zeitdauer PINGTIME die Verbindung getestet. Fällt während dieser Zeit die Prüfung gut aus, wird die Prüfung abgebrochen und die Verbindung zwischen den betroffenen HG 3500/75 sofort wieder auf gut gesetzt. Ist das Ergebnis schlecht, wird während der gesamten Zeit weiter geprüft und erst nach Ablauf der PINGTIME die Verbindung auf gut gesetzt wird. Weitere Informationen siehe Figure 30 “Blocks the IP connection for payload due to „Bad Quality“”. Der Wert wird in [s], Sekunden angegeben. **Wenn Payload Survivability konfiguriert ist, wird empfohlen, das Intervall des Parameters PINGTIME auf einen höheren Wert als den Standardwert von 60 Sekunden zu ändern.** **Z. B. 15 Minuten (900 Sekunden)**

AMO	Parameter	Sprache/ Language	Beschreibung/ Description
	PINGTIME	e	Time interval for testing the payload quality between 2 HG 3500/HG 3575 after a VoIP payload connection has been terminated with quality marked **bad**. If the payload quality for a connection between 2 HG 350075 is marked as bad upon connection termination, the connection is going to be tested for the duration of PINGTIME. With positive test results during this time interval the test is stopped immediately and the connection is marked good again. With negative results the tests will be continued until PINGTIME expires. After that the connection will be marked good again. For further Information see Figure 30 “Blocks the IP connection for payload due to „Bad Quality The value is entered in [s], seconds. **When Payload Survivability is configured, it is recommended to change the PINGTIME parameter interval to a value higher than the default 60 seconds.** **E.g. 15 minutes (900 seconds)**
	RESTIME	d	Zeit zwischen einem Schnittstellenfehler aus dem “Keep Alive” der Signalisierungsverbindung und dem Rücksetzen des Access Points (Wartezeit bis AP-Restart). Wird ein Schnittstellenfehler des “Keep Alive” der Signalisierungsverbindung gemeldet, startet das Zeitintervall RESTIME. Nach dem Schnittstellenfehler können keine neuen Gespräche vom/zu den betroffenen AP aufgebaut werden; bestehende Verbindungen bleiben abhängig vom IP-Netzwerk bestehen, jedoch kann es zu Nullwegen (100% Paktetloss) kommen. Nach Ablauf des Zeitintervalls wird der Access Point zurückgesetzt. Alle Payload-Verbindungen gehen verloren, es sind keine neuen Payload-Verbindungen möglich, bis es der OpenScape 4000 Zentrale wieder gelingt, Kontakt zum Access Point herzustellen. Der Wert wird in [s], Sekunden angegeben.

AMO	Parameter	Sprache/ Language	Beschreibung/ Description
	RESTIME	e	Time between an interface fault specified in the "Keep Alive" message from the signaling link and the access point reset. The RESTIME interval starts when an interface fault is reported in the "Keep Alive" message from the signaling link. New calls cannot be set up from/to the relevant AP following the interface fault; existing connections are maintained depending on the IP network, but null paths can occur (100% packet loss). The access point is reset when the time interval expires. All payload connections are lost and no payload connections are available until the OpenScape 4000 central system succeeds in establishing contact with the access point. The value is specified in seconds [s].
	SUPVTIME	d	Maximale Zeitdauer, während der auf ein Paket auf der Überwachungsverbindung (Supervisory-Verbindung) gewartet wird. Nur bei aktivierter Signaling Survivability. Auf der Supervisory-Verbindung werden in sehr kurzen Intervallen “Keep Alive” Meldungen gesendet. Kommt für länger als SUPVTIME kein Paket an, wird der Weg über das IP-Netz als gestört betrachtet, die Modemverbindung zum Access Point aktiviert und dieser Weg für die Signalisierungsverbindung zwischen OpenScape 4000 und Access Point verwendet. Der Wert wird in [s], Sekunden angegeben.
	SUPVTIME	e	Maximum time waiting for a packet on the Supervisory connection Only if Signaling Survivability is activated. On the Supervisory connection “keep alive” messages are sent in very short intervals. If SUPVTIME exceeds without a packet arrived, the way through the IP networks is considered as disturbed. The modem connection to the Access Point is activated. The signaling between OpenScape 4000 and Access Point is routed via the modem connection. The value is entered in [s], seconds.

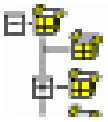
AMO	Parameter	Sprache/ Language	Beschreibung/ Description
	APESWDLYd		APE Umschalteverzögerung *nur wirksam mit dem Leistungsmerkmal AP Emergency!* siehe “Access Point Emergency” > Section 2.10, “Defining the Switchover Delay” Das Umschalten eines Access Points in den Emergency Mode kann um eine konfigurierbare Zeit verzögert werden. Es ist entweder Null - “schalte sofort“ einzutragen, oder die Zeit, welche von der OpenScape 4000 Zentrale benötigt wird, um einen RELOAD durchzuführen. Der Wert wird in Minuten angegeben. Wertebereich [0 .. 99].
	APESWDLYe		APE Switch Over Delay *only effective with the feature AP Emergency!* see “Access Point Emergency” > Section 2.10, “Defining the Switchover Delay” The switch-over of an Access Point into Emergency Mode can be delayed for a configurable amount of time. It shall either be set to zero - “switch immediately“, or to the amount of time which the central OpenScape 4000 system needs to perform a RELOAD. The value is entered in minutes. Range [0 .. 99].

AMO	Parameter	Sprache/ Language	Beschreibung/ Description
	ALVTIME	d	Maximale Zeitdauer für den “Keep Alive” Mechanismus der Signalisierungsverbindungen zwischen OpenScape 4000 und den Access Points. Vergeht diese Zeit ohne Antwort, wird ein Schnittstellenfehler gemeldet und der Access Point wird aus der ATTENDANCE LIST genommen (F5308, LTUC OUT OF ATTENDANCE LIST). Der Wert wird in [s], Sekunden angegeben. Wertebereich [20 .. 90] **Hinweis:** Wenn Signaling Survivability konfiguriert ist, muss dieser Parameter auf einen Wert eingestellt werden, der größer ist als die Maximalzeit für den kompletten Aufbau der Signalisierungsverbindung über Modem!
	ALVTIME	e	Maximum time interval for the “keep alive” mechanism of the signaling connections between OpenScape 4000 and the Access Points. If there is no answer during this interval, an interface error will be reported and the access point is taken out of the ATTENDANCE LIST (F5308, LTUC OUT OF ATTENDANCE LIST). The value is entered in [s], seconds. Range [20 .. 90]. **Note:** When Signaling Survivability is configured, this parameter must be set to a value greater than the maximium duration of the complete setup of signaling connection via modem!

Payload Quality (PLQUAL)

Under TYPE=PLQUAL the limiting values for monitoring the payload quality, i.e. the voice links, are configured. If the upper limits are exceeded, additional voice links between the respective modules (HG 3500 and/or 3575) are established via the alternative route, provided one has been configured. If the lower limits are exceeded, the standard route is returned to the IP network.

The delay values only ever refer to one direction (A -> B or B -> A), and not to the “round-trip delay“ (A -> B -> A). They are derived from the Real Time Transmission Control Protocol.

	**Configuration Management > System Data > IPDA > IPDA System Data** Click **Search**, enter the limiting values under **Payload Quality** on the **System Data** tab and **Save**.

	`CHANGE-`
	`SIPCO:TYPE=PLQUAL,DLYHILIM=200,DLYLOLIM=120,`
	`  LFRHILIM=3,LFR-`
	`LOLIM=2;`

The changed parameters are started on all access points and HG 3500s immediately and without interrupting operation.

Table 33: AMO SIPCO parameters in CHANGE branch under TYPE=PLQUAL

AMO	Parameter	Sprache/ Language	Beschreibung/ Description
SIPCO	DLYHILIM	d	Obere Grenze für die Verzögerung der VoIP Payload-Verbindung zwischen HG 3500/HG 3575. Bei Überschreiten dieses Wertes wird die Verbindung zwischen den 2 betroffenen HG 3500/75 als schlecht markiert. Künftige Verbindungen zwischen diesen HG 3500/75 werden solange über einen Alternativweg geführt (sofern einer eingerichtet ist), bis die Verbindung wieder auf gut gesetzt wird. Der Wert wird in [ms], Millisekunden eingegeben.
	DLYHILIM	e	Upper delay limit for VoIP payload connections between HG 3500/HG 3575. When delay exceeds this value, the connection between the 2 involved HG 3500/75 is marked as bad. Future connections between these HG 3500/75 will be routed via an alternate path (if set up) until the connection is marked good again. The value is entered in [ms], milliseconds.
	DLYLOLIM	d	Untere Grenze für die Verzögerung der VoIP Payload-Verbindung zwischen HG 3500/HG 3575. Bei Unterschreiten dieses Wertes wird eine vorher als schlecht markierte Verbindung zwischen 2 HG 3500/75 wieder auf gut gesetzt. Der Wert wird in [ms], Millisekunden eingegeben.

AMO	Parameter	Sprache/ Language	Beschreibung/ Description
	DLYLOLIM	e	Lower delay limit for VoIP payload connections between HG 3500/HG 3575. When delay falls below this value, a connection between 2 HG 3500/75 that was previously marked as bad is marked good again. The value is entered in [ms], milliseconds.
	LFRHILIM	d	Obere Grenze für die Paketverlustrate der VoIP Payload-Verbindung zwischen 2 HG 3500/HG 3575. Bei Überschreiten dieses Wertes wird die Verbindung zwischen den 2 betroffenen HG 3500/75 als schlecht markiert. Künftige Verbindungen zwischen diesen HG 3500/75 werden solange über einen Alternativweg geführt (sofern einer eingerichtet ist), bis die Verbindung wieder auf gut gesetzt wird. Der Wert gibt das Verhältnis von verlorenen zu gesendeten Paketen in Prozent an.
	LFRHILIM	e	Upper limit for the fraction of lost packets on VoIP payload connections between 2 HG 3500/HG 3575. When the fraction of lost packets exceeds this value, the connection between the 2 involved HG 3500/75 is marked as bad. Future connections between these HG 3500/75 will be routed via an alternate path (if set up) until the connection is marked good again. The value is the ratio of lost to sent packages in percent.
	LFRLOLIM	d	Untere Grenze für die Paketverlustrate der VoIP Payload-Verbindung zwischen 2 HG 3500/HG 3575. Bei Unterschreiten dieses Wertes wird eine vorher als schlecht markierte Verbindung zwischen 2 HG 3500/75 wieder auf gut gesetzt. Der Wert gibt das Verhältnis von verlorenen zu gesendeten Paketen in Prozent an.

AMO	Parameter	Sprache/ Language	Beschreibung/ Description
	LFRLOLIM	e	Lower limit for the fraction of lost packets on VoIP payload connections between 2 HG 3500/HG 3575. When the fraction of lost packets falls below this value, a connection between 2 HG 3500/75 that was previously marked as bad is marked good again. The value is the ratio of lost to sent packages in percent.

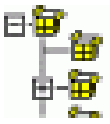
Bandwidth table (BANDW)

Change the system-wide bandwidth table with AMO SIPCO, CHANGE branch under TYPE=BANDW.

Direct media connection (DMCDATA)

The parameter **TYPE=DMCDATA** specifies DMC specific data within CGW IPDA pool.

In addition, the **NWDMC** parameter determines the codec type (G.711 or G.729) to be used for DMC connections in network scenarios with TDM subscribers. This information is provided for the Resource Manager only.

	**Configuration Management > System Data > IPDA > IPDA System Data** Click **Search**, enable or disable the **Direct Media Connection (DMC) activated** field on the **System Data** tab, select the code type, and **Save**.
	`CHANGE-SIPCO:TYPE=DMCDATA,DMCALLWD=N;NWDMC=G729;`

The modified parameters are effective.

Table 34: AMO SIPCO parameters in CHANGE branch under TYPE=DMCDATA

AMO	Parameter	Sprache/ Language	Beschreibung/ Description
SIPCO	DMCERL	d	Direct Media Connection erlaubt. Legt fest, ob Direct Media Connections auf allen HG 3500 zu unterstützen sind, oder nicht.

AMO	Parameter	Sprache/ Language	Beschreibung/ Description
	DMCALLWD	e	Direct Media Connections allowed. Specifies whether Direct Media Connections are to be supported by all HG 3500 gateways - or not.
	NWDMC	d	Codec-Typ für DMC-Verbindungen in Netzwerk-Szenarien mit TDM-Teilnehmern. G711 oder G729
	NWDMC	e	Codec Type for DMC connections in networking scenarios with TDM subscribers. G711 or G729

10.2.2 Access Point

When configuring an access point, a distinction must be made as to

- whether the **access point** involved **is networked via routers in a network segment other than the OpenScape 4000 LAN segment** (see Section 2.2.1, “Configuring a “Networked” Access Point”),

or

- whether the **access point is linked directly to the OpenScape 4000 LAN segment** (see Section 2.2.2, “Configuring a “Direct Link“ Access Point”).

Figure 13 “Difference between “networked“ and “direct link“ access point” illustrates the difference.

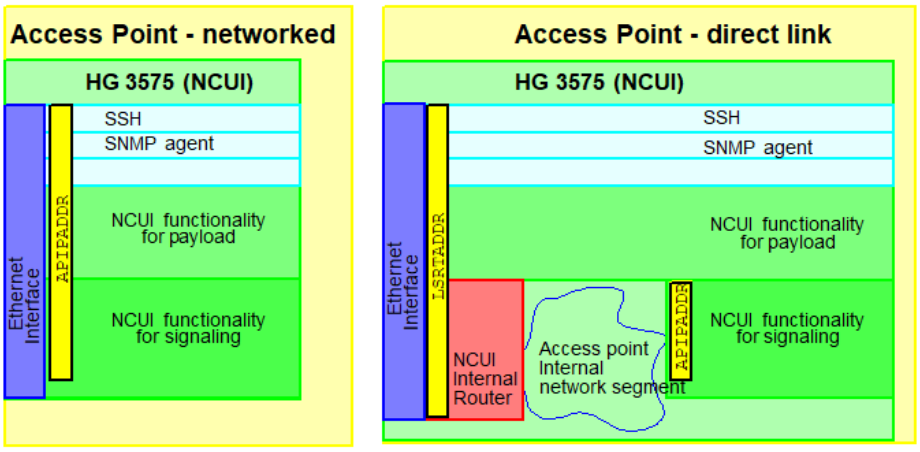


Figure 178: Difference between “networked“ and “direct link“ access point

In all cases, an access point need not only be configured in the system. In order to be able to address an access point, numerous data also has to be entered locally at the access point during its initial installation (see Section 2.2.5, “Local Configuration of an Access Point”). System administration should always be performed first, followed by the local installation of the access point. The data to be entered at the access point can be derived by Configuration

Management or directly from the data configured in the system using “Expert Access“.

10.2.2.1 Configuring a “Networked” Access Point

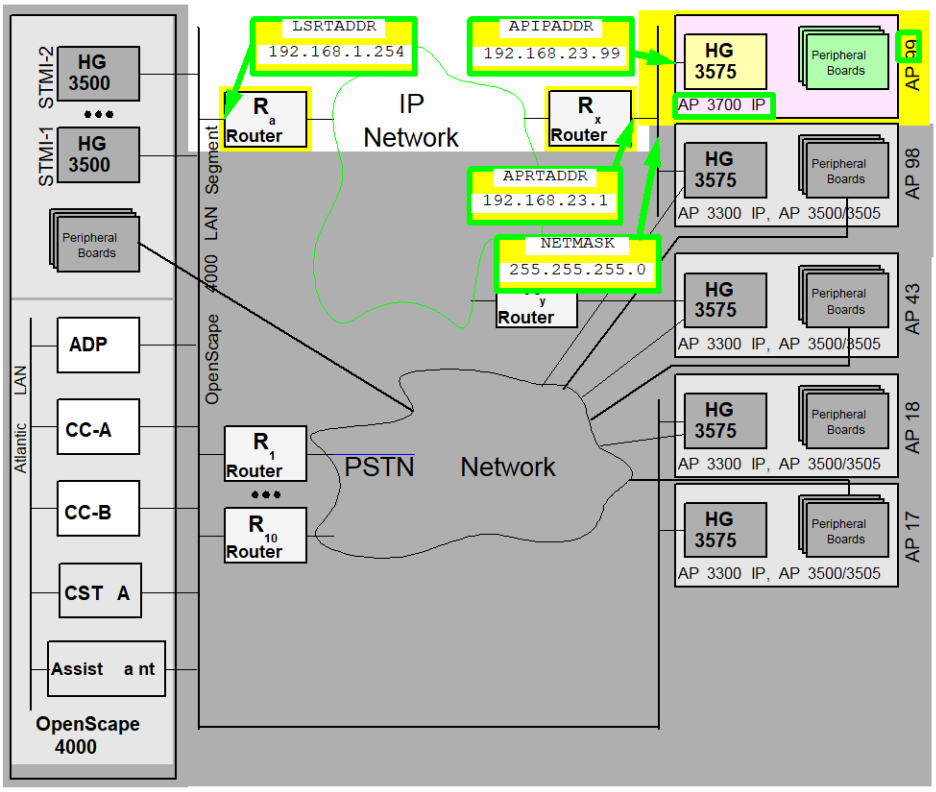


Figure 179: Configuring a “networked“ access point

ADD-UCSU:	UNIT=AP,	LTU=99,
	LTPARTNO=Q2305-X35	SRCGRP=2,
	FRMTYPE=AP 9837009,	CONNTYPE=APNW,
	LSRTADDR=192.168.1.254,	APRTADDR=192.168.23.1,
	LOCID=2,	LOCATION=“BLN ROHRDAMM 85. GEB. 30-222”,
	PHONE=03038612345,	FAX=03038654321,
	PLCHECK=YES,	BCHLCNT=40,
	CONVLAW=NO,	SIGMODE=HSRTCP;
ADD-APRT:	TYPE=APNET,	LTU=99,
	APIPADDR=192.168.23.99,	NETMASK=255.255.255.0;

Figure 14 “Configuring a “networked“ access point” shows the fundamental information required for configuring a “networked“ access point

- The fact that the access point is linked via router with the OpenScape 4000 LAN segment: Link type APNW, i.e. “networked“.
- The LTU number of the access point, i.e. 99.
- The LTU part number specifies the HG 3575 used.
- The access point’s shelf type is derived from the type designation.
- The IP address of the access point: 192.168.23.99.
- The IP address for the TAP/Service PC link at the access point: 192.168.23.199.
- The IP address of the router (port), via which AP99 accesses the OpenScape 4000 LAN segment: 192.168.23.1.
- The netmask in the segment of the AP99: 255.255.255.0.
- The IP address of the router (port) at the OpenScape 4000 LAN segment, via which the AP99 can be accessed by the central components in the OpenScape 4000 LAN segment, i.e. in this case: 192.168.1.254.
- By limiting the number of B-channels, the bandwidth available to AP99 is indirectly reduced in the configuration example. This mechanism works independently of the bandwidth limitation performed by the Resource Manager in the “Large Enterprise Gatekeeper” Feature. For further information, please refer to Chapter 3, “Load Calculation”.
- Should Payload Quality Handling be activated? For details see Section 2.9, “Payload Survivability”.
- The Source Group Index is explained in detail in Section 2.8, “Source Dependent Routing”.

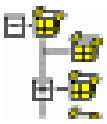
Additional data is explained in more detail with the corresponding AMO parameters.

Generation

An access point is configured with three AMOs (UCSU, APRT, STMIB) and activated with USSU.

UCSU

With the AMO UCSU, the access point is configured as a new shelf in the system and its reachability via routers is ensured.

	**Configuration Management > System Data > IPDA > IPDA Access Point** Click **New** and enter the LTU of the access point. Enter the relevant data on the **General** and **IP Interface (NW)** (Connect Type=APNW) tab and **Save**.
	`ADD-UCSU:UNIT=AP,LTU=99,LTPARTNO=Q2305-X35,SRCGRP=2, FRM-TYPE=AP37009,CONNTYPE=APNW,LSRTADDR=192.168.1.254,APRTAD-DR=192.168.23.1,LOCID=2,LOCATION=“BLN ROHRDAMM 85. GEB. 30-222”,PHONE=03038612345,FAX=03038654321, PLCHECK=YES,BCHLCNT=40,CONVLAW=NO;`

IMPORTANT: The parameters **FRMTYPE** and **CONNTYPE** cannot be changed after the ADD!

IMPORTANT: Prior to ADD-UCSU, use **ping** to check that the IP addresses given to you by the administrator are reachable. **LSRTADDR** and **APRTADDR** must respond.

Table 35: APNW: AMO UCSU parameters in ADD branch under TYPE=AP

AMO	Parameter	Sprache/ Language	Beschreibung/Description	
UCSU	LTSACHNR	d	Sachnummer der LTU-Baugruppe, hier die Sachnummer der verwendeten NCUI2+/ NCUI4.	
	LTPARTNO	e	Part Number of the LTU Board, here part number of the NCUI2+/NCUI4 used.	
	SRCGRP	d	Source Group Index Zuordnung des Access Points in eine Source Group für “Source Dependent Routing”. (Wegesuche in Abhängigkeit vom Rufenden) Dieser Parameter ist wichtig für Source Dependent Routing und Payload Survivability und wird dort näher beschrieben.	
	SRCGRP	e	Source Group Index Assignment of the Access Point to a Source Group for “Source Dependent Routing”. This parameter is relevant for Source Dependent Routing and Payload Survivability and will be described in more detail there.	
	FRAMETYP	d	Typ des LTU-Rahmens (Shelf Typ)	
			AP-Typ	FRAMETYP
			AP 3300 IP	L80XF
			AP 3500 IP	INCH19
			AP 3700 IP	AP37009
	FRMTYPE	e	Type of the LTU Frame (Shelf Type)	
			AP-Type	FRAMETYPE
			AP 3300 IP	L80XF
			AP 3500 IP	INCH19
			AP 3700 IP	AP37009

AMO	Parameter	Sprache/ Language	Beschreibung/Description
	VERBART	d	Art der Verbindung zwischen Access Point und Zentrale Für IPDA kommen nur die Werte APDL und APNW in Frage. APNW - Access Point via Network: Access Point und Zentrale werden in unterschiedlichen IP-Netzen betrieben, welche über Router miteinander verbunden sind.
	CONNTYPE	e	Type of the Connection between Access Point and the Central Switch Only the values APDL and APNW are possible for IPDA. APNW - Access Point via Network: Access Point and central switch are located in different IP-Networks interconnected by routers.
	LSRTADR	d	Adresse des Routers im OpenScape 4000 LAN Segment VERBART=APNW: IP Adresse des Routers (Ports) im OpenScape 4000 LAN Segment, über den der Access Point / das Netz, in dem sich der Access Point befindet, erreichbar ist.
	LSRTADDR	e	Address of the Router in the OpenScape 4000 LAN Segment CONNTYPE=APNW: IP address of the router (port) in the OpenScape 4000 LAN Segment, via which the Access Point / the network, where the Access Point is located, is reachable.

AMO	Parameter	Sprache/ Language	Beschreibung/Description
	APRTADR	d	Adresse des Routers im Netzwerk des Access Points IP Adresse des Routers (Ports) im Netz, in dem sich der Access Point befindet, über den der Access Point Adressen außerhalb dieses Netzes erreicht. VERBART=APNW: Über diesen Router muss der Access Point CC-A, CC-B, ADP und die HG 3500 Baugruppen im OpenScape 4000 LAN Segment erreichen sowie alle anderen Access Points *). *)Ausnahmen für Sonderrouten sind möglich und werden im Routing Table Zweig des AMO APRT eingerichtet.
	APRTADDR	e	Address of the Router in the Access Point's Network IP address of the router (port) in the network where the Access Point is located, via which the Access Point reaches addresses outside of this network. CONNTYPE=APNW: Via this router the Access Point must be able to reach CC-A, CC-B, ADP and the HG 3500 boards in the OpenScape 4000 LAN Segment as well as all other Access Points*). *) Exceptions for special routes are possible. They are administered in the routing table branch of AMO APRT.

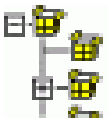
AMO	Parameter	Sprache/ Language	Beschreibung/Description
	STANDOID	d	Standort Identifikation Schlüsselzahl zur Identifikation des Standorts eines Access Points, der unterschiedlich zum Standort der Zentralanlage sein kann. Der Parameter wird benötigt, um den vertrieblichen Bestand (PARK-Daten) der Anlagenteile standortabhängig zu pflegen. Der Wert wird vom Konfigurator-Tool vergeben und muss so übernommen werden. Gegebenenfalls ist der Wert vom Systemplaner zu erfragen. Ist kein Tool-generierter Wert verfügbar, z.B. bei Teststellungen, soll der Wert 999 verwendet werden, um dies auszudrücken. Bei Erweiterungen an einem Standort (zusätzlicher Access Point) kann der Wert des bereits existierenden Access Points übernommen werden. Systemkomponenten in einem anderen Raum, Stockwerk, oder Gebäude werden unter einer anderen Standort-Identifikation geführt!
	LOCID	e	Location Identification Key number for identification of the location of an Access Point, which can differ from the location of the central switch. This parameter is necessary to maintain the sales database for the parts of the system, based on locations. The value is determined by the Configurator tool and must be taken over unchanged. If necessary, ask the system planner for the value. If no tool-generated value is available, e.g. for test and demo configurations, the value 999 shall be used to express this. For expansions at a certain location (additional Access Point), the value of the already exisiting Access Point can be taken. System components in another room, floor or building are listed under a different location ID.
	STANDORT	d	Angabe darüber, wo der Access Point zu finden ist. z.B. Firma, Ort, Straße, Gebäude, Stockwerk, Raumnummer, ... Maximal 48 Zeichen können eingegeben werden.

AMO	Parameter	Sprache/ Language	Beschreibung/Description
	LOCATION	e	Info, where to find the Access Point E.g. Company, city, street, building, floor, room number, ... A maximum of 48 characters is allowed.
	TEL	d	Telefonnummer am Standort des Access Points Nächstgelegenes Telefon, über das ein Techniker vor Ort am Access Point erreicht werden kann.
	PHONE	e	Phone number at the Access Point The nearest phone, where a service engineer can be reached at the Access Point.
	FAX	d	Faxnummer am Standort des Access Points Nächstgelegenes Faxgerät, über das ein Techniker vor Ort am Access Point erreicht werden kann.
	FAX	e	Fax number at the Access Point The nearest fax, where a service engineer can be reached at the Access Point.
	PLCHECK	d	Payload Quality Check Gibt an, ob für diesen Access Point auf schlechte Payload Qualität reagiert werden soll (durch Sperren der Verkehrsbeziehung bzw. Weg über Payload Survivability) oder nicht. -> Section 2.9, “Payload Survivability”
	PLCHECK	e	Payload Quality Check Defines whether this Access Point shall react on bad Payload Quality (by blocking of the relation or routing via Payload Survivability Path) or not. -> Section 2.9, “Payload Survivability”
	ANZBKAN	d	Anzahl B-Kanäle Gibt an, wieviele B-Kanäle an der Schnittstelle zwischen Access Point und LAN gleichzeitig genutzt werden dürfen. Auf diese Weise lässt sich die maximale Bandbreite, die der Access Point im LAN benötigt, grob begrenzen. siehe Chapter 3, “Load Calculation”

AMO	Parameter	Sprache/ Language	Beschreibung/Description
	BCHLCNT	e	B Channel Count Defines how many B channels may be used concurrently at the interface between Access Point and LAN. By this the maximum bandwidth needed by an Access Point can be limited coarsely. see Chapter 3, “Load Calculation”
	KONVLAW	d	Konvertierung von A-Law zu µ-Law bzw. µ-Law nach A-Law auf der HG 3575 Baugruppe.
	CONVLAW	e	Conversion from A-law to µ-law or µ-law to A-law on the HG 3575 board.

APRT

With the AMO APRT, the access point is assigned its own IP address.

	**Configuration Management > System Data > IPDA > IPDA Access Point** Click **Search** and select the access point. Enter IP addresses on the **IP Interface (NW)** tab and **Save**.
	`ADD-APRT:TYPE=APNET,LTU=99,APIPADDR=192.168.23.99, NET-MASK=255.255.255.0;`

IMPORTANT: Prior to `ADD-APRT`, use **ping** to check that the IP addresses given to you by the administrator are reachable. **APIPADDR** must not respond, as this would indicate that the corresponding address had already been assigned. **APIPADDR** must be set differently for every access point. The AMO does not verify if this rule is observed.

Table 36: APNW: AMO APRT parameters in ADD branch under TYPE=APNET

AMO	Parameter	Sprache/ Language	Beschreibung/Description
APRT	APIPADR	d	Eigene IP-Adresse des Access Points VERBART*)=APNW: IP-Adresse des Access Points an dessen Ethernet-Port. APIPADR muss für jede Baugruppe unterschiedlich sein. Der AMO prüft nicht die Einhaltung dieser Regel. *) AMO UCSU, ART=AP: siehe Parameter VERBART in Table 6 “APNW: AMO UCSU parameters in ADD branch under T
	APIPADDR	e	Own IP Address of the Access Point CONNTYPE*)=APNW: IP address of the Access Point’s ethernet port. APIPADDR must be different for every board. The AMO does not check compliance with this rule. *) AMO UCSU, ART=AP: see see parameter CONNTYPE in Table 6 “APNW: AMO UCSU parameters in ADD branch under T
	NETMASK	d	Netzmaske des Netzes, dem APIPADR angehört
	NETMASK	e	Netmask of the network which APIPADDR is part of

With the AMO APRT, additional functions of an access point can be configured.

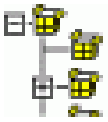
- Signaling survivability
- Payload survivability - alternative routes -> Section 2.9, “Payload Survivability”
- Additional routes in the IP network which cannot/should not be accessible via the default router in the network of the access point or in the OpenScape 4000 LAN segment -> Section 2.5, “Special Routes”

STMIB

Nothing special has to be configured with STMIB. The CHANGE branches allow a multitude of parameters to be set. Details are described in Section 2.2.3, “Changing Access Point Parameters with the AMO STMIB”.

USSU

In order to actually put the access point into operation after the configuration process, it has to be activated.

	**Configuration Management > System Data > IPDA > IPDA System Data** Click **Search** and select the access point. Click **Execute** on the **Action** pull-down menu and set the mode of action **Configure AP**, confirm with **OK**.
	`EXEC-USSU:MODE=CONFAP, LTU=xx;`

From this moment on, the OpenScape 4000 CC attempts to reach the access point and, as soon it achieves this, to start it.

IMPORTANT: Prior to `EXEC-USSU:CONFAP`, the configuration must be updated on the system hard disk, Otherwise, the data on the system would conflict with the data on the HG 3575 when the system is reloaded and could only be synchronized again with `EXEC-USSU:UPDATAP`,LTU number,`UL`.

In order to be able to reach the access point from the CC upon initial installation, various data has to be entered locally at the access point (see Section 2.2.5, “Local Configuration of an Access Point”).

10.2.2.2 Configuring a “Direct Link“ Access Point

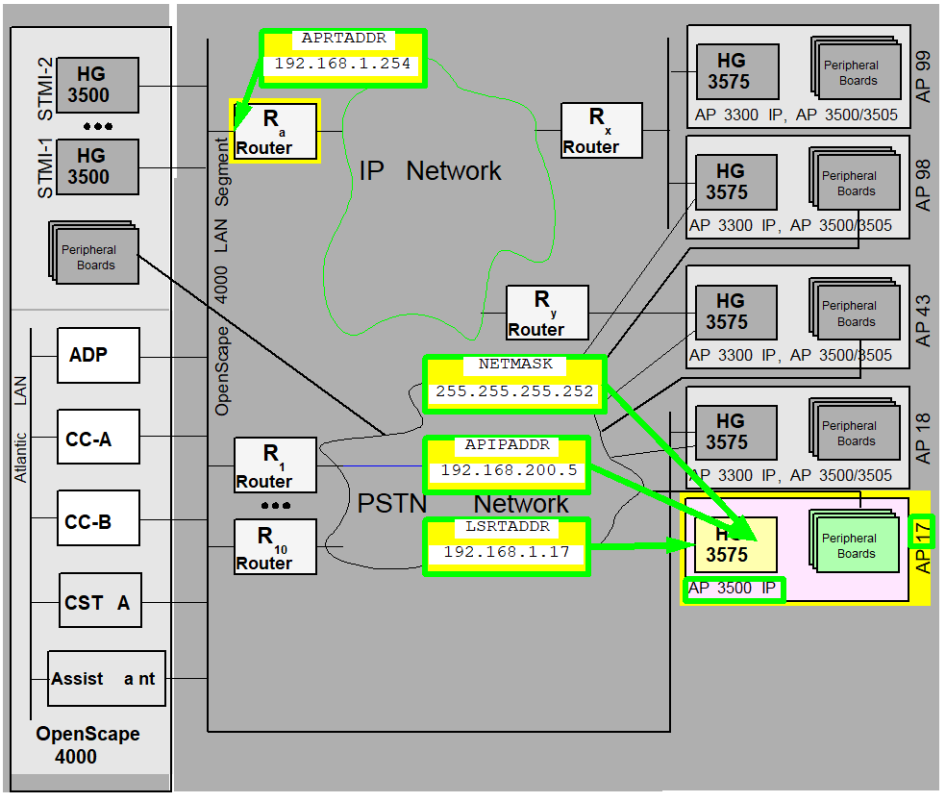


Figure 180: Configuring a “Direct Link“ access point

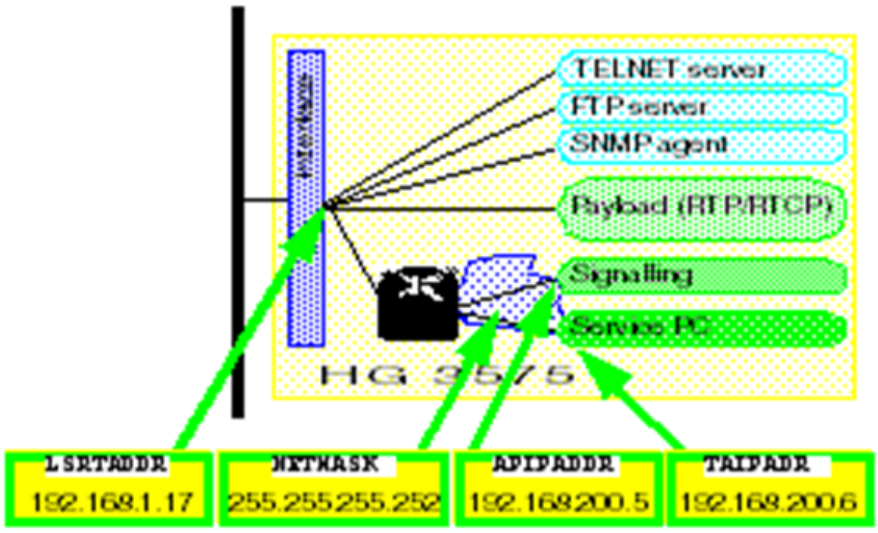


Figure 181: Internal address assignment of a “direct link“ access point

ADD-UCSU:	UNIT=AP,	LTU=17,
	LTPARTNO=Q2302-X10	SRCGRP=1,

	FRMTYPE=INCH19,	CONNTYPE=APDL,
	LSRTADDR=192.168.1.17,	APRTADDR=192.168.1.254,
	LOCID=1,	LOCATION="MCH MACHTLFINGERSTR.1 GEB. 7202-111",
	PHONE=08972223456,	FAX=08972265432,
	PLCHECK=YES,	BCHLCNT=20,
	CONVLAW=NO;	
ADD-APRT:	TYPE=APNET,	LTU=17,
	APIPADDR=192.168.200.5,	NETMASK=255.255.255.252;

In the case of a "direct link" access point, the Ethernet port of the access point is connected directly to the OpenScape 4000 LAN segment and can be reached from CC-A and CC-B without a router.

However, the signaling survivability feature requires the re-routing of a link in the event of a fault (from LAN to modem). In order for this to function, the access point may not be "logically" present in the OpenScape 4000 LAN segment. In this case, a router is activated within the access point which forwards the packets from the OpenScape 4000 LAN to the "logical", internal address of the access point.

To this end, the access point contains a "logical" IP network in which only itself and possibly the TAP/Service PC connection have an address. In order to save addresses, the netmask 255.255.255.252 can be used for this address.

Even these mini-networks and their addresses must be coordinated with the customer's network administrator and, obviously, may not overlap.

Figure 15 "Configuring a "Direct Link" access point" shows the following fundamental information required for configuring a direct link access point:

- The fact that the access point is linked with the OpenScape 4000 LAN segment: Link type APDL, i.e. "direct link".
- The LTU number of the access point, i.e. 17.
- The LTU part number specifies the HG 3575 used.
- The access point's shelf type is derived from the type designation.
- The internal IP address of the access point: 192.168.200.5.
- The IP address for the TAP/Service PC link at the access point: 192.168.200.6.
- The IP address of the own Ethernet port via which the AP17 accesses the OpenScape 4000 LAN segment: 192.168.1.17.
- The netmask in the internal segment of the AP17: 255.255.255.252.
- The IP address of the router (port) at the OpenScape 4000 LAN segment, via which the AP17 can reach access points which cannot be accessed directly at the OpenScape 4000 LAN segment (that is "networked" APs), in this case router Ra: 192.168.1.254. This router is omitted if there are no networked APs in the entire configuration or if this is an isolated demo installation. The default router **must** be configured with the zero address 0.0.0.0.

- By limiting the number of B-channels, the bandwidth available to AP99 is indirectly reduced in the configuration example. This mechanism works independently of the bandwidth limitation performed by the Resource Manager in the “Large Enterprise Gatekeeper” Feature. For further information, please refer to Chapter 3, “Load Calculation”.
- Should Payload Quality Handling be activated? For details see Section 2.9, “Payload Survivability”
- The Source Group Index is explained in detail in Section 2.8, “Source Dependent Routing”.

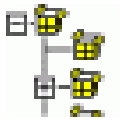
Additional data is explained in more detail with the corresponding AMO parameters.

Generation

An access point is configured with three AMOs (UCSU, APRT, STMIB) and activated with USSU.

UCSU

With the AMO UCSU, the access point is configured as a new shelf in the system and its reachability via routers is ensured.

	**Configuration Management > System Data > IPDA > IPDA Access Point** Click **New** and enter the LTU of the access point. Enter the relevant data on the **General** and **IP Interface (DL)** (Connect Type=APDL) tab and **Save**.
	`ADD-UCSU:UNIT=AP,LTU=17,LTPARTNO=Q2302-X10,SRCGRP=1,FRM-TYPE=INCH19,CONNTYPE=APDL,LSRTADDR=192.168.1.17,APRTAD-DR=192.168.1.254,LOCID=1,LOCATION=“MCH MACHTLFINGERSTR.1 GEB. 7202-111”,PHONE=08972223456,FAX=08972265432,PLCHECK=YES,BCHLCNT=20,CON-VLAW=NO;`

The parameters **FRMTYPE** and **CONNTYPE** cannot be changed after the ADD!

IMPORTANT: Prior to `ADD-UCSU`, use **ping** to check that the IP addresses given to you by the administrator are reachable. **APRTADDR** must respond. **LSRTADDR** must not respond, as this would indicate that the corresponding address had already been assigned. **LSRTADDR** must be set differently for every “direct link“ access point. The AMO does not verify if this rule is observed.

Table 37: APNW: AMO UCSU parameters in ADD branch under ART=AP

AMO	Parameter	Sprache/ Language	Beschreibung/Description
UCSU	LTSACHNR	d	Sachnummer der LTU-Baugruppe, hier die Sachnummer der verwendeten NCUI2+/ NCUI4.
	LTPARTNO	e	Part Number of the LTU Board, here part number of the NCUI2+/NCUI4 used.

AMO	Parameter	Sprache/ Language	Beschreibung/Description	
	SRCGRP	d	Source Group Index Zuordnung des Access Points in eine Source Group für “Source Dependent Routing”. (Wegesuche in Abhängigkeit vom Rufenden) Dieser Parameter ist wichtig für Source Dependent Routing und Payload Survivability und wird dort näher beschrieben.	
	SRCGRP	e	Source Group Index Assignment of the Access Point to a Source Group for “Source Dependent Routing”. This parameter is relevant for Source Dependent Routing and Payload Survivability and will be described in more detail there.	
	FRAMETYP	d	Typ des LTU-Rahmens (Shelf Typ)	
			AP-Typ	FRAMETYP
			AP 3300 IP	L80XF
			AP 3500 IP	INCH19
			AP 3700 IP	AP37009
	FRMTYPE	e	Type of the LTU Frame (Shelf Type)	
			AP-Type	FRAMETYPE
			AP 3300 IP	L80XF
			AP 3500 IP	INCH19
			AP 3700 IP	AP37009
	VERBART	d	Art der Verbindung zwischen Access Point und Zentrale Für IPDA kommen nur die Werte APDL und APNW in Frage. APDL - Access Point Direct Link: - Access Point ist direkt am OpenScape 4000 LAN Segment angeschlossen, d.h. im selben IP-Netz.	

AMO	Parameter	Sprache/ Language	Beschreibung/Description
	CONNTYPE	e	Type of the Connection between Access Point and the Central Switch Only the values APDL and APNW are possible for IPDA. APDL - Access Point Direct Link: - Access Point is connected directly to the OpenScape 4000 LAN Segment, i.e. in the same IP network.
	LSRTADR	d	Adresse des Routers im OpenScape 4000 LAN Segment VERBART=APDL: Dies ist die IP-Adresse am Ethernet-Port des Access Points, über den er mit dem OpenScape 4000 LAN Segment verbunden ist. Bei APDL enthält der Access Point einen lokalen Router der die IP-Adresse des Access Points (in einem eigenen Netzwerksegment) mit dem OpenScape 4000 LAN Segment verbindet. D.h. auch hier handelt es sich um die Adresse eines (wenn auch unsichtbaren) Routers. Diese IP-Adresse muss zum OpenScape 4000 LAN Segment gehören (siehe NETADR im AMO SIPCO). LSRTADR muss für jede Baugruppe unterschiedlich sein. Der AMO prüft nicht die Einhaltung dieser Regel.
	LSRTADR	e	Address of the Router in the OpenScape 4000 LAN Segment CONNTYPE=APDL: This is the IP address of the Access Point’s ethernet port connected to the OpenScape 4000 LAN Segment. With APDL the AP contains a local router that connects the own IP address of the Access Point (in its own network segment) to the OpenScape 4000 LAN Segment. It’s a router’s address, even with the router invisible. This IP address must belong to the OpenScape 4000 LAN Segment (see NETADDR in AMO SIPCO) LSRTADDR must be different for every board. The AMO does not check compliance with this rule.

AMO	Parameter	Sprache/ Language	Beschreibung/Description
	APRTADR	d	Adresse des Routers im Netzwerk des Access Points IP Adresse des Routers (Ports) im Netz, in dem sich der Access Point befindet, über den der Access Point Adressen außerhalb dieses Netzes erreicht. VERBART=APDL: Über diesen Router muss der direkt am OpenScape 4000 LAN Segment angeschlossene Access Point alle Access Points erreichen, die sich in anderen Netzen befinden. Meist ist dies der Default-Router des OpenScape 4000 LAN Segments, welcher mit dem Parameter DEFRT im AMO SIPCO eingerichtet wird*). Sind in der gesamten Konfiguration keine “networked“ APs enthalten, oder ist dies eine isolierte Demo-Installation, so enfällt dieser Router. Geben Sie dazu hier die Null-Adresse 0.0.0.0 an. *)Ausnahmen für Sonderrouten sind möglich und werden im Routing Table Zweig des AMO APRT eingerichtet.
	APRTADDR	e	Address of the Router in the Access Point’s Network IP address of the router (port) in the network where the Access Point is located, via which the Access Point reaches addresses outside of this network. CONNTYPE=APDL: Via this router an Access Point directly connected to the OpenScape 4000 LAN Segment must be able to reach all Access Points that are located in different networks. Usually this is the default router of the OpenScape 4000 LAN Segment, administered in parameter DEFRT with AMO SIPCO*). If there are no “networked“ APs in the whole configuration or if this is a stand-alone demo installation, this router is not needed. Give the address 0.0.0.0 for this purpose. *) Exceptions for special routes are possible. They are administered in the routing table branch of AMO APRT.

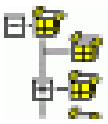
AMO	Parameter	Sprache/ Language	Beschreibung/Description
	STANDOID	d	Standort Identifikation Schlüsselzahl zur Identifikation des Standorts eines Access Points, der unterschiedlich zum Standort der Zentralanlage sein kann. Der Parameter wird benötigt, um den vertrieblichen Bestand (PARK-Daten) der Anlagenteile standortabhängig zu pflegen. Der Wert wird vom Konfigurator-Tool vergeben und muss so übernommen werden. Gegebenenfalls ist der Wert vom Systemplaner zu erfragen. Ist kein Tool-generierter Wert verfügbar, z.B. bei Teststellungen, soll der Wert 999 verwendet werden, um dies auszudrücken. Bei Erweiterungen an einem Standort (zusätzlicher Access Point) kann der Wert des bereits existierenden Access Points übernommen werden. Systemkomponenten in einem anderen Raum, Stockwerk, oder Gebäude werden unter einer anderen Standort-Identifikation geführt!
	LOCID	e	Location Identification Key number for identification of the location of an Access Point, which can differ from the location of the central switch. This parameter is necessary to maintain the sales database for the parts of the system, based on locations. The value is determined by the Configurator tool and must be taken over unchanged. If necessary, ask the system planner for the value. If no tool-generated value is available, e.g. for test and demo configurations, the value 999 shall be used to express this. For expansions at a certain location (additional Access Point), the value of the already exisiting Access Point can be taken. System components in another room, floor or building are listed under a different location ID.
	STANDORT	d	Angabe darüber, wo der Access Point zu finden ist. z.B. Firma, Ort, Straße, Gebäude, Stockwerk, Raumnummer, ... Maximal 48 Zeichen können eingegeben werden.

AMO	Parameter	Sprache/ Language	Beschreibung/Description
	LOCATION	e	Info, where to find the Access Point E.g. Company, city, street, building, floor, room number, ... A maximum of 48 characters is allowed.
	TEL	d	Telefonnummer am Standort des Access Points Nächstgelegenes Telefon, über das ein Techniker vor Ort am Access Point erreicht werden kann.
	PHONE	e	Phone number at the Access Point The nearest phone, where a service engineer can be reached at the Access Point.
	FAX	d	Faxnummer am Standort des Access Points Nächstgelegenes Faxgerät, über das ein Techniker vor Ort am Access Point erreicht werden kann.
	FAX	e	Fax number at the Access Point The nearest fax, where a service engineer can be reached at the Access Point.
	PLCHECK	d	Payload Quality Check Gibt an, ob für diesen Access Point auf schlechte Payload Qualität reagiert werden soll (durch Sperren der Verkehrsbeziehung bzw. Weg über Payload Survivability) oder nicht. -> Section 2.9, “Payload Survivability”
	PLCHECK	e	Payload Quality Check Defines whether this Access Point shall react on bad Payload Quality (by blocking of the relation or routing via Payload Survivability Path) or not. -> Section 2.9, “Payload Survivability”

AMO	Parameter	Sprache/ Language	Beschreibung/Description
	ANZBKAN	d	Anzahl B-Kanäle Gibt an, wieviele B-Kanäle an der Schnittstelle zwischen Access Point und LAN gleichzeitig genutzt werden dürfen. Auf diese Weise lässt sich die maximale Bandbreite, die der Access Point im LAN benötigt, grob begrenzen. siehe Chapter 3, “Load Calculation”
	BCHLCNT	e	B Channel Count Defines how many B channels may be used concurrently at the interface between Access Point and LAN. By this the maximum bandwidth needed by an Access Point can be limited coarsely. see Chapter 3, “Load Calculation”
	KONVLAW	d	Konvertierung von A-Law zu µ-Law bzw. µ-Law nach A-Law auf der HG 3575 Baugruppe.
	CONVLAW	e	Conversion from A-law to µ-law or µ-law to A-law on the HG 3575 board.

APRT

With the AMO APRT, the access point is assigned its own (internal) IP address.

	**Configuration Management > System Data > IPDA > IPDA Access Point** Click **Search** and select the access point. Enter IP addresses on the **IP Interface (DL)** tab and **Save**.
	`ADD-APRT:TYPE=APNET,LTU=17,APIPADDR=192.168.200.5, NET-MASK=255.255.255.252;`

IMPORTANT: If you want to check the (internal) **APIPADDR** IP address after startup using **ping**, you must configure the route to the AP internal network segment on the computer from which the **ping** is dispatched. => Host=APRT:**APIPADDR**, Netmask=APRT:**NETMASK**, Router=UCSU:**LSRTADDR**. **APIPADDR** must be set differently for every access point. The AMO does not verify if this rule is observed.

Table 38: APDL: AMO APRT parameters in ADD branch under TYPE=APNET

AMO	Parameter	Sprache/ Language	Beschreibung/Description
APRT	APIPADR	d	Eigene IP-Adresse des Access Points VERBART*)=APDL: IP-Adresse des Access Points in seinem eigenen Netzwerksegment - nicht die IP-Adresse the Ethernet-Ports, welche in diesem Fall vom internen Router belegt wird. APIPADR muss für jede Baugruppe unterschiedlich sein. Der AMO prüft nicht die Einhaltung dieser Regel. *) AMO UCSU, ART=AP: siehe Parameter VERBART in Table 6 “APNW: AMO UCSU parameters in ADD branch under TYPE
	APIPADDR	e	Own IP Address of the Access Point CONNTYPE*)=APDL: IP address of the Access Point in its own network segment - not the IP address of it’s ethernet port which is assigned to the internal router in this case. APIPADDR must be different for every board. The AMO does not check compliance with this rule. *) AMO UCSU, UNIT=AP: see parameter CONNTYPE in Table 6 “APNW: AMO UCSU parameters in ADD branch under TYPE
	NETMASK	d	Netzmaske des Netzes, dem APIPADR angehört
	NETMASK	e	Netmask of the network which APIPADDR is part of

With the AMO APRT, additional functions of an access point can be configured.

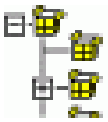
- Signaling survivability
- Payload survivability - alternative routes -> Section 2.9, “Payload Survivability”
- Additional routes in the IP network which cannot/should not be accessible via the default router in the network of the access point or in the OpenScape 4000 LAN segment -> Section 2.5, “Special Routes”

STMIB

Nothing special has to be configured with STMIB. The CHANGE branches allow a multitude of parameters to be set. Details are described in Section 2.2.3, “Changing Access Point Parameters with the AMO STMIB”.

USSU

In order to actually put the access point into operation after the configuration process, it has to be activated.

	**Configuration Management > System Data > IPDA > IPDA System Data** Click **Search** and select the access point. Click **Execute** on the **Action** pull-down menu and set the mode of action **Configure AP**, confirm with **OK**.
	`EXEC-USSU:MODE=CONFAP,LTU=xx;`

From this moment on, the OpenScape 4000 CC attempts to reach the access point and, as soon it achieves this, to start it.

IMPORTANT: Prior to `EXEC-USSU:CONFAP`, the configuration must be updated on the system hard disk, Otherwise, the data on the system would conflict with the data on the HG 3575 when the system is reloaded and could only be synchronized again with `EXEC-USSU:UPDATAP`, LTU number, `UL`.

In order to be able to reach the access point from the CC upon initial installation, various data has to be entered locally at the access point (see Section 2.2.5, “Local Configuration of an Access Point”).

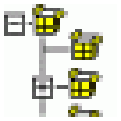
10.2.2.3 Changing Access Point Parameters with the AMO STMIB

Please refer to Chapter 11, “Gateway HG 3575 - Changing Parameters with AMO STMIB” in the document “Gateways HG 3500 and HG 3575”.

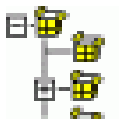
10.2.2.4 Deleting an Access Point

If an access point is to be removed from the configuration (in the example: AP 43), the following sequence must be complied with:

- If payload survivability is configured, it must first be checked whether the access point to be deleted provides the trunk access for a source group. If it does, a suitable replacement must be found.
- If payload survivability is configured and a source group becomes superfluous when an access point is deleted, the LCR must be adapted and the source group deleted if necessary.

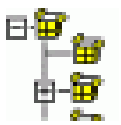
	**Configuration Management > System Data > IPDA > IPDA - Payload Survivability** Click **Search**, select the access point and **Delete**.
	`DELETE-APRT:TYPE=ALTROUT,SRCGRP=3;`

- Deletion of all peripheral modules configured within this access point (presupposes that no subscribers are configured on that module, etc.)
- If signaling survivability is configured for this access point:
- Delete the assignment of this access point to a survivability router

	**Configuration Management > System Data > IPDA > IPDA Access Point** Click **Search** and select the access point. Delete the desired router number on the **General** tab under **Signaling Survivability** and **Save**.
	`DELETE-APRT:TYPE=SURV,CONF=AP,LTU=43;`

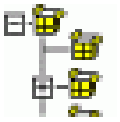
- If special routes are configured: (Section 2.5, “Special Routes”)
  - Delete the corresponding entries in the routing tables of other access points, if these entries lose their validity for additional access points.

  In the example in Figure 21 “Special routes between access points”, the route via Router Rz becomes superfluous if AP 43 is deleted. If, however, AP 98 was deleted instead of AP 43, the route would have to remain in place, as it is also valid for AP 99.

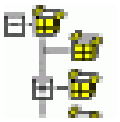
	**Configuration Management > System Data > IPDA > HG3575 Additional Routing** Click **Search** and select the access point. Enter zero addresses (0.0.0.0) in the lines of the routing table that are to be deleted and **Save**.

	`DEL-`
	`APRT:TYPE=ROUTTBL,MTYPE=NCUI,LTU=99,INDEX=1;`
	Note: No distinction is made here between hardware types. NCUI applies to NCUI2 and NCUI4.

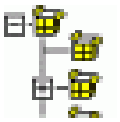
- Deactivating the access point with USSU:

	**Configuration Management > System Data > IPDA > IPDA Access Point** Click **Search** and select the access point. Click **Deactivate** on the **Action** pull-down menu.
	`DEACTIVATE-USSU:LTU=43;`

- Deactivating the IP connection of the access point with USSU:

	**Configuration Management > System Data > IPDA > IPDA System Data** Click **Search** and select the access point. Click **Execute** on the **Action** pull-down menu and select the mode of action **Update AP**, confirm with **OK**.
	`EXEC-USSU:MODE=DELAP,LTU=43;`

- Deleting the access point (CM):

	**Configuration Management > System Data > IPDA > IPDA Access Point** Click **Search** and select the access point, then click **Delete**.

- Deleting the IP network configuration of the access point:

	`DELETE-APRT:TYPE=APNET,LTU=43;`

- Deleting the access point with UCSU:

	`DELETE-UCSU:UNIT=AP,LTU=43;`

IMPORTANT: If the removed access point was configured for AP Emergency (i.e. it was assigned an emergency group), you must observe the following: The IP address of the removed access point can only be reused when this change has been saved on all CC APs, in other words, when “cloning“ is completed using OpenScape 4000 Assistant > Backup & Restore.

10.2.2.5 Local Configuration of an Access Point

If an access point has been configured in the OpenScape 4000 switch, it cannot be put into operation immediately. The central system cannot establish contact with the access point until this has been configured with the essential IP addresses, etc.

“Expert Access“ application is available in order to perform this initial access point configuration locally. To this end, the TAP/Service PC is connected to the RS232/V.24 interface of the HG 3575 with the designation “Service“ and the application started.

The terminal login must be used for login purposes. In the case of virgin modules, this is "TRM", and no password is set. If the module has already been in operation and the terminal login and password have been changed, these later values apply.

If there is a duplex processor (CC-B) in the OpenScape 4000 switch, the address must always be specified. After all, it is not possible to predict whether CC-A or CC-B will be playing the active role at this time. If there is no CC-B in the system, the IP address for this processor is not needed.

The IP address of the TAP need only be specified if the administration function of the OpenScape 4000 switch is to be accessed from this access point.

If VLAN tagging is used in the Ethernet segment to which the access point should be connected, a setting must be performed for it during initial startup. If the access point was operated in a network with VLAN tagging and should now run without VLAN tagging, this setting must also be changed locally.

If the access point is to be operated with fixed Ethernet interface settings for bit rate and mode or if this fixed setting is to be removed (in the event of relocation to another network), this setting too must be performed locally.

Of the parameters which are displayed and adjustable, only a certain number actually have to be entered. All other parameters are loaded from the OpenScape 4000 switch as soon as the central system can establish contact with the access point;

IMPORTANT: Changing a parameter value locally does **not** result in a change of the value in the system. Absolutely all parameters configured locally at the access point are overwritten by the values configured in the system upon loading the module from the OpenScape 4000 switch.

When configuring the access point locally, a distinction is again also made between “networked“ and “direct link“.

Networked access point

The following fields must be completed:

Table 39: Basic initialization parameters for “networked“ access points

Parameter	Note	AMO - Zweig - Parameter
IP address of the access point	May not be in the same network as the IP address of the CC-A	APRT TYPE=APNET - APIPADDR
Netmask in the network of the access point	The netmask must match the IP address class of the access point.	APRT TYPE=APNET - NETMASK
IP address of the default router in the network of the access point	Must be in the same network as the IP address of the access point	UCSU UNIT=AP - APRTADDR
IP address of the CC-A		SIPCO TYPE=LSNET - CCAADDR
IP address of the CC-B	Must be in the same network as the IP address of the CC-A	SIPCO TYPE=LSNET - CCBADDR
Netmask of the OpenScape 4000 LAN segment	The netmask must match the IP address class of the CC-A.	SIPCO TYPE=LSNET - NETMASK
VLAN tagging on/off		STMIB: MTYPE=NCUI2, TYPE=IFDATA - VLAN
VLAN ID		STMIB: MTYPE=NCUI2, TYPE=IFDATA - VLANID
Ethernet interface operating mode		STMIB: MTYPE=NCUI2, TYPE=IFDATA - BITRATE

Direct link access point

The following fields must be completed:

Table 40: Basic initialization parameters for “direct link“ access point

Parameter	Note	AMO - Branch - Parameter
IP address of the access point in the OpenScape 4000 LAN segment	Must be in the same network as the IP address of the CC-A	UCSU UNIT=AP - LSRTADDR
OpenScape 4000 LAN segment Netmask	The netmask must match the IP address class of the CC-A.	SIPCO TYPE=LSNET - NETMASK
IP address of the default router in the OpenScape 4000 LAN segment	Must be in the same network as the IP address of the CC-A	UCSU UNIT=AP - APRTADDR
IP address of the CC-A		SIPCO TYPE=LSNET - CCAADDR
IP address of the CC-B	Must be in the same network as the IP address of the CC-A	SIPCO TYPE=LSNET - CCBADDR
IP address of the access point in the internal AP network segment	May not be in the same network as the IP address of the CC-A	APRT TYPE=APNET - APIPADDR
Netmask of the internal AP network segment	The netmask must match the IP address class of the access point in the internal AP network segment.	APRT TYPE=APNET - NETMASK
VLAN tagging on/off		STMIB: MTYPE=NCUI2, TYPE=IFDATA - VLAN
VLAN ID		STMIB: MTYPE=NCUI2, TYPE=IFDATA - VLANID
Ethernet interface operating mode		STMIB: MTYPE=NCUI2, TYPE=IFDATA - BITRATE

Information on local configuration without the “Expert Access“ application can be found in Chapter 4, “Local Access Point Administration at CLI via Terminal”.

10.2.2.6 Reference Clock in Access Point

The OpenScape 4000 central system has a highly precise clock generator which can be synchronized from various sources. Possible sources include, for instance, digital trunk circuits. The corresponding connection modules can then supply the clock timing in the LTUs 1-15 and synchronize the central clock generator. The AMO REFTA is responsible for configuring which circuits can be used as reference clock suppliers and querying which supplier is currently active.

Access Points of the type AP 3300 IP, AP 3500 IP or AP 3700 IP are connected in asynchronous fashion via the IP network. Thus, the central clock generator cannot be synchronized from LTUs 17-99.

On account of this asynchronous connection, the access point itself is also unable to be synchronized from the central clock generator. Therefore, the HG 3575 module of the access point is equipped with its own highly precise clock generator.

The asynchronism of the clock generators in the OpenScape 4000 central system and in the various access points has no interfering effect on the communication between these components. The jitter buffers required for voice transmission also compensate smoothly for the slight slip between the clock generators.

However, if digital trunk or tie trunk circuits are operated in an access point, the local clock generator must be synchronized with the network clock (“CO Clock“).

To this end, management of the reference clock has been extended with the AMO REFTA. The basic principle is simple:

- Reference clock sources in LTUs 1-15 are used to synchronize the central clock generator.
- Reference clock sources in LTUs 17-99 are used to synchronize the local clock generators in the respective access point.

Thus, in a OpenScape 4000 switch with 83 access points of the type AP 3300 IP or AP 3500 IP, the synchronization of 84 clock generators has to be managed. This means that 84 active clock suppliers (central unit + 83 access points) may exist in such a system.

10.2.2.7 Loading new Loadware on a HG 3575

For the load concept via HTTPS for HG 3575 and HG 3500 please refer to “Gateways HG 3500 and HG 3575“, Chapter 5, “Load Concept for Gateway Boards”.

The loadware for a HG 3575 is very extensive. If, while the module is being loaded, it is determined that the loadware in the flash memory of the module does not match the loadware stored in the hard disk of the OpenScape 4000 central system, the loadware is reloaded on the HG 3575.

The loadware is transferred via FTP-Push (load functionality via hhtps hasn’t been used, i.e. loading via LW Update Manager), with the HG 3575 downloading the loadware from the FTP server of the HiPath 4000 central processor (in the RMX system).

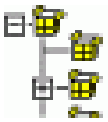
The FTP server can only transfer loadware to up to five HG 3575 boards at a time. If there are multiple HG 3575s in the system (up to 83 access points are

possible), the other modules wait their turn in case of a system reload. This takes quite a long time and considerably slows down startup of the system.

IMPORTANT: With the feature “AP Multicast Loading” the downtime of a system in case of a system update (system relaod with software/loadware version) will be reduced. For details please refer to Section 2.2.8, “Updating Access Point Loadware during an RMX Upgrade (New Fix Release/ Minor Release)”.

It is therefore possible for a HG 3575 to download new loadware from the FTP server in the background, which means while the system is running. Therefore the loadware update manager of the HiPath 4000 should be used (see „Gateways HG 3500 and HG 3575“, Section 5.5, “Updating Loadware with "LW Update Manager"”).

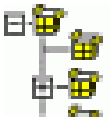
Alternative the loadware can be transferred via FTP-Push while the system is running, without executing it immediately. Actions of this type should be performed at off-peak times, as the loadware transfer reduces the bandwidth for signaling messages. The load operation can also be performed with signaling survivability. The effect on the available bandwidth is particularly critical in this case.

	**Configuration Management > System Data > IPDA > IPDA Access Point** Click **Search** and select the access point. Click **Execute** on the **Action** pull-down menu and select the mode of action **Background Loading of NCUI LW Files**, select **LW** under **Files to be Loaded** and confirm with **OK**.
	`EXEC-USSU:MODE=NCUILOAD,LTU=xx,FILES=LW;` If the LTU number is not specified, all HG 3575s that are ready (`READY`) at this time are loaded.

SIU files can also be loaded in this way.

`FILE=`		
	`SIUTONES`	`TONES`
	`SIURECV`	`SIU-RECEIVERS`
	`SIUANN`	`SIU-ANNOUNCEMENTS`
	`SIUMOH`	`SIU -MUSIC ON HOLD`
	`SIUTDS`	`SIU -TDS`
	`LW`	`LW file -- NCUI`
	`ALLSIU`	`All possible SIUs`
	ALL	**All loadable files**

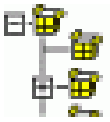
To apply the loadware while the system is active, the following actions are required:

	**Configuration Management > System Data > IPDA > IPDA Access Point** Click **Search** and select the access point. Click **Deactivate** on the **Action** pull-down menu. Once the system has confirmed deactivation of the AP, reactivate it with **Activate**.
	`DEACTIVATE-USSU:LTG=1,LTU=xx; ACTIVATE-USSU:UNIT=LTG,LTG=1,LTU=xx;`

IMPORTANT: Connections are cleared down without further warning!

Changing the music on hold (MOH) in the system (AMO ZAND:MELODY=X)

When changing the MELODY setting, the following command sequence must be executed (for each AP) so that the changes become effective immediately:

	**Configuration Management > System Data > IPDA > IPDA Access Point** Click **Search** and select the access point. Click **Deactivate** on the **Action** pull-down menu. Once the system has confirmed deactivation of the AP, reactivate it with **Activate**.
	`DEACTIVATE-USSU:LTG=1,LTU=xx; ACTIVATE-USSU:UNIT=LTG,LTG=1,LTU=xx;`

10.2.2.8 Updating Access Point Loadware during an RMX Upgrade (New Fix Release/ Minor Release)

The feature "**AP multicast loading**" lets you perform simultaneous loading operations for multiple access points. Originally, simultaneous loading operations were only possible for access points containing boards that already featured the latest loadware. With “AP multicast loading” it is also possible if the boards need new loadware.

Procedure

1) Use the traditional FTP solution to transfer the new loadware for the HG 3575 to the access point (up to five access points per run). See also Section 2.2.7, “Loading new Loadware on a HG 3575”.

2) Once the new loadware has been successfully transferred and activated, the TCP/IP connection is re-established between the host system (HSR) and the access point.

   To transfer the loadware downloaded in the background to the NCUI a warm boot is initiated and executed.

   The restart (warm boot) with the new loadware is followed by a golden loadware check. If this golden loadware check fails, the NCUI restarts with the old loadware and the new loadware (HD) is retransmitted.

   IMPORTANT: This step is skipped if there is no new loadware available for the HG 3575.

3) The loadware transfer for the peripheral boards starts.
4) The access points are entered in the load list once the loadware has been transferred.
5) The first access point in the load list is put into full operation immediately (takes approx. 15 minutes). While this access point is being put into operation, other access points that have already completed the loadware transfer/activation are entered in the load list.
6) As soon as the first access point has gone into operation, all access points that have been entered in the load list in the meantime are simultaneously loaded and put into operation.

   IMPORTANT: In the past, the APs in the load list were processed or put into operation in sequential order.

1) While these access points are being put into operation, other access points that have completed loadware transfer/activation are entered in the load list.
2) As soon as the access points have gone into operation, all access points grouped together on the load list are put into operation simultaneously.
3) These procedures are repeated until all access points have been upgraded.

10.2.2.9 Information on Exchanging HG 3575 Boards

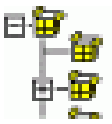
The following must be observed when exchanging a HG 3575 board in a system:

- The HG 3575 board must not be powered on or plugged in.
- The new board must be configured with the same basic configuration as the old board (IP addresses, etc.). To do this, the configuration of the old board can be read out using “Expert Access“ and stored on a file with which the new board can be configured. If this is no longer possible with the old board, the data must be taken from the system configuration.
- Every HG 3575 board has an individual Ethernet MAC address. The MAC address which is visible from the network changes when boards are changed.

  IMPORTANT: Please inform the network carrier of the change. The network provider needs the MAC addresses to find devices involved in IP address conflicts. The board’s MAC address can

be found on the sticker on the solder side of the printed circuit board.

- The following AMO action must be performed once the module has been booted:

	Unconditional loading can only be initiated in expert mode. **Expert Mode > Expert Access > Open** ...<IP> with AMO (see AMO command)
	EXEC-USSU:UPDATAP,LTU=<number>,UL;

1) This ensures that the entire system configuration data is written to the module. The access point is thus restarted and is booted using the latest data. This is necessary as the system does not always detect that the boardwas exchanged. This process is also required if the same board was removed from the system, reconfigured locally and put back in the same position in the system.

For more information on exchanging HG 3575 boards refer to document „Gateways HG 3500 and HG 3575“, Section 3.2.2, “Exchanging Boards”.

10.2.2.10 Information on the 19“ AP 3500 IP Access Point

Figure 17 “AP 3500 IP - front view” shows the front view of a AP 3500 IP. The shelf can be mounted in a 19“ rack using additional angle brackets and has a height of 3HE.

There is space on the left for 4 modules and the topmost slot is allocated to the HG 3575 (NCUI2/4). Peripheral modules of the OpenScape 4000 can be inserted into the other slots. These modules are covered by a metal panel that is inserted separately. In the figure, this panel has been removed from the bottom slot.

At the rear, either the usual main distribution cables can be attached or plug-in patch panels can be used to connect the devices directly using Western plugs.

In addition to the modules, the rack also contains 2 power supply modules on top of one another. The AP 3500 IP can be operated using a power supply module. A second may also be operated as a redundant unit.

A ventilator module is located at the right-hand side. Because the modules are in a horizontal position, the system has to be forced ventilated.

IMPORTANT: The ventilation openings on the left and right-hand side of the housing must not be obstructed. The operating position of the equipment is horizontal.

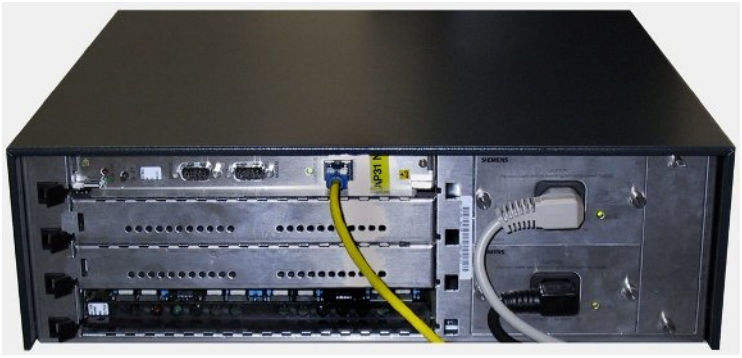


Figure 182: AP 3500 IP - front view

The AP 3500 IP can be extended by four slots using a AP 3505 IP with a similar structure (no HG 3575 in the AP 3505).

Special features

- The AP 3500 IP represents the left and the optional AP 3505 IP represents the right half of a conventional shelf.
- The slots are counted from bottom up and are numbered 1,2,3 and 4 in the AP 3500 IP (4 is HG 3575), and 5,6,7 and 8 in the optional AP 3505 IP.
- Boards with front connectors can only be used if they are fitted with a suitable metal panel (for example, STMI2, DIUN2 starting with status -X-7, SLC24 starting with status -X200-9, PBXXX starting with status -X-F3, ...)
- SIVAPAC modules with adapters are not supported, because they do not fit under the shielding cover. As an exception, a number of these boards are fitted with a new plastic panel C39228-A402-C21. (TMEW2, SLMA,TMDID,TMEMUS).

10.2.2.11 Information on the 19“ AP 3700 IP Access Point

The frame of an AP 3700 IP can be installed in 19“ cabinets. For this, it must be set on sliding rails/mounting rails installed in the cabinet and terminated at the cabinet uprights by means of the 19“ mounting bracket supplied.

AP 3700 IP required a height of 11 HE (10 HE + 1 HE play).

IMPORTANT: AP 3700 IP is not forced ventilated and consequently, does not feature a fan. For installation, please pay particular attention to requirements in terms of air supply and minimum air volume specified in the installation instructions.

The left half of the shelf can accommodate five peripheral boards (slot 1 to 5). HG 3575-2 (NCUI2) is supported on the central slot (slot 6). The correct shelf half accommodates four peripheral boards (slot 7 to 10).

If the peripheral boards are not already equipped with a suitable metal panel (for example, STMI2, slot 4 and 9), they are covered by a metal panel that is inserted separately. (on slot 1 and 2 in the diagram). Unused slots must be covered by a metal panel and guarantee the necessary level of shielding.

Boards with front connectors can only be used if they are fitted with a suitable metal panel (for example, STMI2, DIUN2 starting with status -X-7, SLC24 starting with status -X200-9, PBXXX starting with status -X-F3, ...)

SIVAPAC modules with adapters are not supported, because they do not fit under the shielding cover. As an exception, a number of these boards are fitted with a new plastic panel C39228-A402-C21. (TMEW2, SLMA,TMDID,TMEMUS).

The project planning guideline's instructions on the installation of peripheral boards should therefore be followed precisely.

At the rear, either the usual main distribution cables can be attached or plug-in patch panels can be used to connect the devices directly using Western plugs.

Up to three power supply modules can be connected side by side under the board. Two modules are sufficient for supplying the maximum configuration. A third module may also be connected as a redundant unit.

The power supply modules can be connected to the 115/230 V alternating current or 48 V direct current. The three modules are fed over a shared connected at the rear of the housing.

The right part of the AP 3700 IP can accommodate a survivability unit, a cPCI cassette with a standalone emergency control unit.

10.2.3 HG 3500 as HG3570 in the OpenScape 4000 System

For more information on HG 3500 gateway please refer to „Gateways HG 3500 and HG 3575“.

The common gateway HG 3500 - added as HG3570 - establishes the payload connections between the central OpenScape 4000 system and the access points distributed within the framework of the IP distributed architecture.

- HG 3500 gateways, configured as HG 3570, may only be used in the peripheral shelves (LTU 1-15) of the central system.
- The time slots required by the HG 3570 gateways in a half shelf must be nonblocking. The maximum number of B channels supported by the board hardware can be reduced using the BCHLCNT command in the AMO BFDAT.
- Every shelf in which a HG 3570 is installed must be equipped with an LTUCX module.
- Up to 83 HG 3570 gateways can be used in a OpenScape 4000 system. The payload connections between the central OpenScape 4000 system and the access points are distributed evenly across all HG 3500s.
- There is no assignment of payload connections from HG 3575 to HG 3500. The number of HG 3500s in the system is based on the traffic volume, not on the number of access points. If one HG 3500 fails, it is not assigned any new calls. The other available HG 3500s take on the payload.

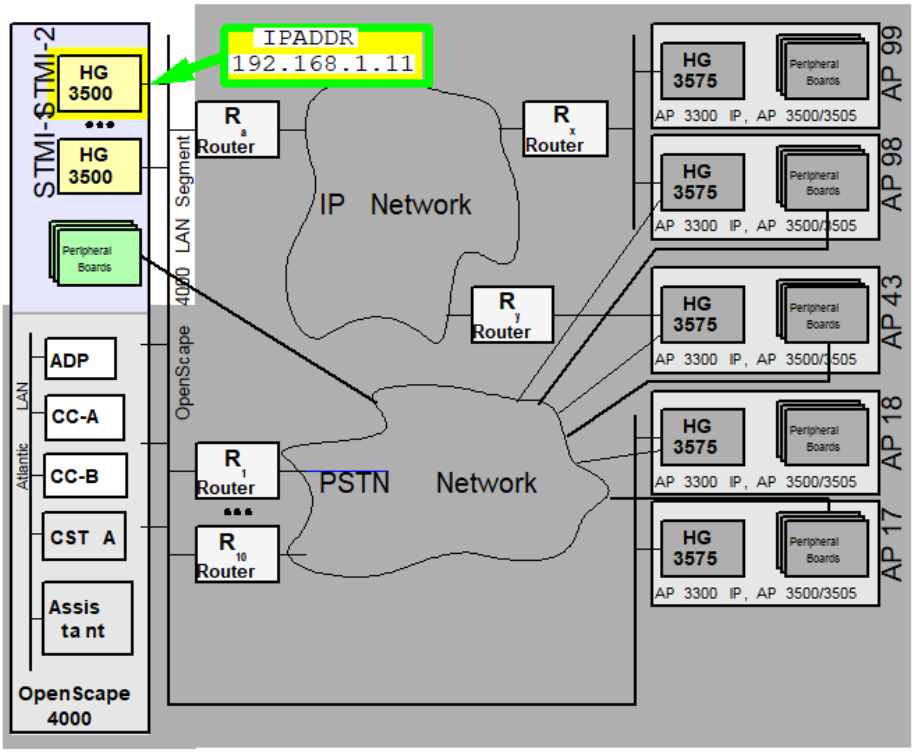


Figure 183: Configuring a HG 3500 for IPDA

ADD-BFDAT:	FCTBLK=1,	FUNCTION=HG3570,
	BRDBCHL=BCHL60&BCHL120;	
CHANGE-BFDAT:	CONFIG=CONT,	FCTBLK=1,
	FUNCTION=HG3570,	BCHLCNT=40;
CHANGE-BFDAT:	CONFIG=OK,	FCTBLK=1,
	ANSW=YES;	
ADD-BCSU:	MTYPE=IPGW,	LTU=5,
	SLOT=91,	PARTNO=Q2316-X,
	FCTID=1,	FCTBLK=1,
	IPADR=192.168.1.11,	BKAN3570=40;
CHNAGE-BCSU:	TYPE=HWYBDL,	LTU=5,
	SLOT=91,	PARTNO=Q2316-X,
	HWYBDL=A;	

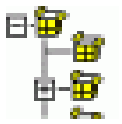
Generation

A HG 3500 module with **FUNCTION=HG3570** is configured with 3 AMOs: AMO BFDAT, AMO BCSU and AMO CGWB.

However, AMO CGWB is only needed if additional routes in the IP network are required in addition to the default router in the OpenScape 4000 LAN segment. Please refer to Section 2.5, “Special Routes”.

BFDAT

Configuration of the functional blocks for common gateway boards for IPDA.

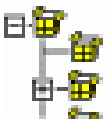
	**Configuration Management > System Data > Board > CGW Function Block** Click **New**, enter data and click **Save**.
	ADD-BFDAT:FCTBLK=1,FUNCTION=HG3570,BRDBCHL=NCHL&BCHL; CHA-BFDAT:CONFIG=CONT,FCTBLK=1,FUNCTION=HG3570,BCHLCNT=40; CHNAGE-BFDAT:CONFIG=OK,FCTBLK=1,ANSW=YES;

AMO	Parameter	Sprache/ Language	Beschreibung/ Description
BFDAT	ANZBKAN	d	Anzahl der funktionsbezogenen B-Kanäle.
	BCHLCNT	e	Defines the number of b-channels related to the selected function.
	ANTW	d	JA: Block-KOnfiguration abschließen
	ANSW	e	YES: Finish block configuration
	BGBKAN	d	Block fuer Baugruppe mit 60 und/oder 120 B-Kanaelen
	BRDBCHL	e	Dedicates the block for boards with 60 and/ or 120 b-channels.
	CONFIG	d	WEITER: Weitere Block-Konfiguration möglich OK: Block-Konfiguration abschließen
	CONFIG	e	CONT: Continue block configuration OK: Finish block configuration
	FCTBLK	d	Dieser Index beschreibt den Funktionsblock welcher auf dem CGW konfiguriert werden soll. Anhand des Funktionsblocks wird die Konfiguration der benötigten pyhsikalischen Lines (Sätze der Baugruppe) festgelegt.

AMO	Parameter	Sprache/ Language	Beschreibung/ Description
	FCTBLK	e	This index describes the function block which should be configured on the CGW board. With that index the amount of needed physical lines (board circuits) is calculated.
	FUNCTION	d	Dieser Parameter legt das Konfigurationsprofile des Common Gateways fest. Dabei muss die benötigte HG3570 Funktion als erste angeführt werden. Falls ein bestimmter Line-Bereich für die Funktionen HG3530, HG3540 oder HG3550 vorreserviert werden soll, muss die entsprechende Funktion am Ende stehen und mit dem Wert HG35xxR abgeschlossen sein. Die Funktion STANDBY kann nur als Einzel-Funktion konfiguriert werden.
	FUNCTION	e	This parameter defines the configuration profile of the CGW board. If HG3570 functionality is used, it must be configured at first position. If a prereservation of a certain line range of functions HG3530, HG3540 or HG3550 is desired, this function must be at the end of the profile just suffixed by the according HG35xxR value. The function STANDBY can only be configured as single function.

BCSU

The modules are configured in the system and activated with the AMO BCSU.

	**Configuration Management > System Data > Board > Board** Click **New**, enter data (**IP Address**, section **IP Gateway**, **STMI Board Data** tab) and **Save**.
	`ADD-BCSU:MTYPE=IPGW,LTU=5,SLOT=91,PARTNO=Q2316-X,FCTID=1,FCTBLK=1,IPADDR=192.168.1.11,BCHL3570=40;` `CHANGE-BCSU:TYPE=HWYBDL,LTU=5,SLOT=91,PARTNO=Q2316-X,HWYBDL=A;`

IMPORTANT: Prior to `ADD-BCSU`, use **ping** to check that the IP addresses given to you by the administrator are reachable. **IPADDR** must not respond as this would indicate that the corresponding address has already been assigned. **IPADDR** must be set differently for every board. The AMO does not verify if this rule is observed.

AMO	Parameter	Sprache/ Language	Beschreibung/ Description
BCSU	BKAN3570	d	Anzahl der B-Kanaele fuer die IPDA (HG3570) Funktion
	BCHL3570	e	Amount of b-channels for IPDA (HG3570) function
	LTG	d	LTG-Nummer Parameter kann entfallen - oder muss auf 1 gesetzt werden.
	LTG	e	Line/Trunk Group Number Parameter can be omitted - or must be set to 1.
	LTU	d	LTU-Nummer des Rahmens, in dem die HG 3500 eingesetzt wird. Die HG 3500 darf nur in den Rahmen des OpenScape 4000 Zentralsystems (LTU 1..15) eingesetzt werden. Der Rahmen muss mit einer LTUCX Baugruppe ausgestattet sein.
	LTU	e	Line/Trunk Unit Number of the shelf where the HG 3500 is plugged. An HG 3500 may only be used in a shelf of the OpenScape 4000 central system (LTU 1..15). The shelf must be equipped with a LTUCX board.
	EBT	d	Einbauteilung des Steckplatzes der HG 3500
	SLOT	e	Slot where the HG 3500 resides.
	SACHNR	d	Sachnummer der HG 3500-Baugruppe
	PARTNO	e	Part Number of the HG 3500 Board
	FCTID	d	Function ID
	FCTID	e	Function ID
	LWVAR	d	LW Parametrisierung Wird für HG 3500 nicht benötigt. Wert sollte ausgelassen oder auf 0 gesetzt werden.
	LWVAR	e	LW Parametrization Not needed for HG 3500. Parameter should be omitted or set to 0.

AMO	Parameter	Sprache/ Language	Beschreibung/ Description
	IPADR	d	IP-Adresse der HG 3500 Baugruppe Diese IP-Adresse muss zum OpenScape 4000 LAN Segment gehören (siehe NETADR im AMO SIPCO, Table 1 “AMO SIPCO parameters in ADD branch or for CHANGE under TYPE=LSNET”) IPADR muss für jede Baugruppe unterschiedlich sein. Der AMO prüft nicht die Einhaltung dieser Regel.
	IPADDR	e	IP Address of the HG 3500 Board This IP address must belong to the OpenScape 4000 LAN Segment (see NETADDR in AMO SIPCO, Table 1 “AMO SIPCO parameters in ADD branch or for CHANGE under TYPE=LSNET” on page 2-650) IPADDR must be different for every board. The AMO does not check compliance with this rule.
	HWYBDL	d	Highway Bündel Die HG 3500 / STMI2/4/STMIX/STMIY Baugruppe unterstützt die Wideband Technologie. Deshalb muss der Baugruppe entweder das Highway Bündel A (default) oder F zugewiesen werden.
	HWYBDL	e	Highway Bundle The HG 3500 / STMI2/4/STMIX/STMIY board supports wideband technology. Thus either highway bundle A (default) or F must be assigned to this board.
	TYPE=IPGW	d	Baugruppentyp IP Gateway = Common Gateway
	MTYPE=IPGW	e	board hardware type IP gateway = common GATEWAY

10.2.4 Subscriber, CO/Tie Trunk Circuits in Access Points

In an IP distributed access point, all subscriber line and CO/tie trunk modules can be used, with a few exceptions which are described in the OpenScape 4000 Technical Upgrade Plan

When using analog access modules which also require a ring generator, the following must be taken into consideration:

In the 19“ access point AP 3500 IP and the AP 3505 IP expansion box, only RGM type ring generator modules (S30807-Q6141-X or S30122-K5929-X) can be used, not RG modules. The AP 3505 IP expansion box requires its own RGM independently of the AP 3500 IP basic box, if analog access modules are to be operated in it.

IMPORTANT: Trunk connections between access points in the same system or between a central system and its access points are not permitted.

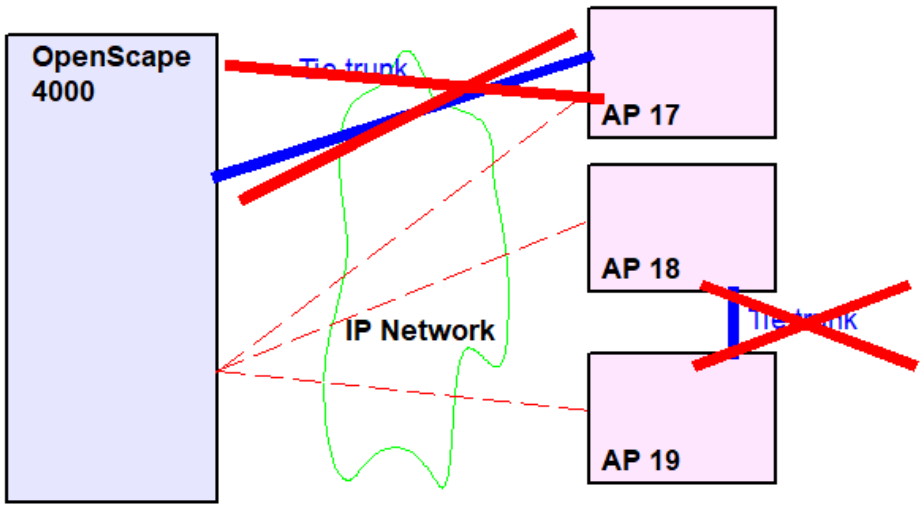


Figure 184: Tie connections are not permitted within a system

With the configuration in an IP distributed access point, all circuits are given additional parameters to govern their handling of Voice over IP. These IPDA classmarks are:

Table 41: IPDA classmarks

Classmark	Sprache/ Language	Beschreibung/ Description
EC	d	Echo Cancellation
EC	e	Echo Cancellation
G711	d	Codec Typ G.711
G711	e	Codec Type G.711
G729	d	Codec Typ G.729A
G729	e	Codec Type G.729A
G729OPT	d	Codec Typ G.729A - optional
G729OPT	e	Codec Type G.729A - optional
INIT	d	stellt Default-Einstellung wieder her
INIT	e	restores default setting
KEINE	d	schaltet alle Classmarks aus
NONE	e	turns all Classmarks off

Classmark	Sprache/ Language	Beschreibung/ Description
ML	d	Multiple Listener - Ansage wird auf einer Verbindung übertragen und im Access Point an meherere Sätze geschaltet. *) nur für Ansagegeräte/MOH
ML	e	Multiple Listener - Announcement is transmitted on a single connection and switched to multiple ports in the Access Point. *) only for Announcement Devices/MOH
VAD	d	Voice Activity Detection
VAD	e	Voice Activity Detection
VIAHHS	d	Payload über Zentralsystem *) nur für Ansagegeräte/MOH
VIAHHS	e	Payload via central system *) only for Announcement Devices/MOH

Details of the procedures that are switched with classmarks can be found in:

- Voice Compression - Section 4.2 on page 4-79 in the document “Gateways HG 3500 and HG 3575”
- Voice Activity Detection (VAD) - Section 4.3 on page 4-81 in the document “Gateways HG 3500 and HG 3575”
- Echo Cancellation- Section 4.5 on page 4-82 in the document “Gateways HG 3500 and HG 3575”
- Codec Standards - Section 1.3 on page 1-34 in the document “Gateways HG 3500 and HG 3575”

Handling the classmarks for a call

If a call is to be established between Subscriber A and Subscriber B, the classmarks of both subscribers, or of the subscriber and the CO/tie trunk circuit via which the subscriber is reached, are assessed.

Echo cancellation or voice activity detection is only activated if both circuits have set the corresponding classmark.

Connections with announcement devices configured with the AMOs SSC, RCSU or TSCSU are an exception to this rule. Here, the announcement device setting is always adopted.

Table 42: Classmark handling for EC or VAD

EC or VAD		Circuit B			**EC or VAD**		**Announcement Device** (RCSU)	
		NO	YES				NO	YES
Circuit A	NO	NO	NO		Circuit A	NO	NO	**YES**

	YES	NO	**YES**		YES	NO	**YES**

In the case of codec types, only one type which supports both is selected.

In contrast to version 1, compression is now available for announcement devices and conferences. As far as codec classmarks are concerned, conference trunk circuits are assigned either G711 (default) or G711 & G729OPT when selecting the codec type.

Table 43: Classmark handling for codec type

Circuit A			Circuit B			Codec type used
G711	G729	G729OPT	G711	G729	G729OPT	
NO	NO	NO	-	-	-	NONE
NO	NO	YES	-	NO	YES	G.711
NO	YES	-	YES	NO	-	G.711
NO	YES	-	-	NO	YES	G.729
NO	YES	-	-	YES	-	G.729
YES	NO	NO	YES	-	-	G.711
YES	NO	YES	YES	NO	YES	G.711
YES	NO	YES	YES	YES	-	G.729
YES	NO	-	NO	YES	-	G.711
YES	YES	-	YES	NO	YES	G.729
YES	YES	-	YES	YES	-	G.729
YES	-	-	YES	NO	NO	G.711
-	NO	YES	NO	NO	YES	G.711
-	NO	YES	NO	YES	-	G.729
-	YES	-	NO	YES	-	G.729
-	-	-	NO	NO	NO	NONE
- Applies regardless of whether YES or NO is set						

Generating the classmarks

The default setting is always **EC&G711&G729OPT**.

IMPORTANT: The classmark setting in the CHANGE branches of the AMOs overwrites the setting that existed prior to the AMO call. Therefore, if an additional classmark is to be set, the

existing setting must be displayed beforehand and specified again with CHANGE.

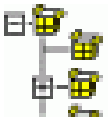
If a setting is to be reset to its default value, the value INIT must be specified.

If all classmarks are to be deactivated, the value NONE must be used.

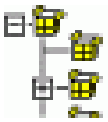
If only some classmarks are to be deactivated, the classmark to be retained must be specified again with CHANGE. All others are automatically deleted.

Examples:

Subscriber:

	**Configuration Management > Station > Station** Click **SEARCH** and select the subscriber. Set or delete the required classmarks on the **Basic 2** tab under **IPDA**, **IP Connection Features** and **Save**.
	`CHANGE-SDAT:STNO=54321,TYPE=DATA1,CLASSMRK=NONE;` Deactivates all classmarks as required for digital data terminal devices.
	`CHA-SDAT:STNO=54321,TYPE=DATA1,CLASSMRK=EC&G711&G729;` Sets the EC, G711 and G729 classmarks. Use of the G.729 codec is forced if the partner has set G729 or G729OPT.
	`CHANGE-SDAT:STNO=54321,TYPE=DATA1,CLASSMRK=EC&G711&G729&G729OPT&VAD;` Sets the classmarks for EC, G711, G729, G729OPT and VAD (in other words, all).

Attendant console:

	Administration of the attendant console can only be executed in expert mode. **Expert Mode > Expert Access > Open ...**<IP> with AMO (see AMO command)
	`CHANGE-ACSU:ATNDNO=65432,CLASSMRK=EC&G711;` Sets the EC and G711 classmarks. Calls are always switched without compression and the echo is suppressed.

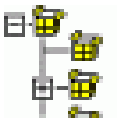
Announcement devices:

The default setting for AMO SSC and AMO RCSU is always **G711&G729OPT&VIAHHS&ML**.

The default setting for AMO TSCSU is **EC&G711&G729OPT&VIAHHS&ML**.

IMPORTANT: The option of setting **G729OPT** or even **G729** for announcement devices should only be used after careful consideration. G.729 specifies a codec for **voice** compression. The codec is totally unsuitable for music compression. Music

playback is extremely distorted with G.729. In some cases it may be necessary to disable **G729OPT** particularly if you want to avoid distortions and if circuits have been configured with codec **G729**.

	**Configuration Management > Station > Special Stations** Click **Search** and select the special station (**Station Type**: **EXTANS**). Set or delete the required classmarks on the **Features** tab and **Save**.

	`ADD-SSC:PEN=1-2-37-10,TYPE=EXTANS,CPCALL=HOLD,CLASSMRK=G711&VIAHHS&ML;`
	or
	`CHANGE-RCSU:PEN=1-2-37-5,CLASSMRK=G711&VIAHHS&ML;`
	Disables G729OPT and sets the G711 classmark. Echo cancellation is not required at announcement devices because the path from the subscriber to the announcement device is not switched.

IMPORTANT: The classmarks **VIAHHS** and **ML** are **enabled** by default. They may only be disabled in exceptional cases. In the case of `CHANGE`, do not forget to specify both classmarks if they were previously set.

If **VIAHHS** is not set, announcements and/or music on hold are no longer distributed via the OpenScape 4000 host system. Instead they are transferred directly from the HG 3575 which hosts the source to all other HG 3575 systems that require the announcement.

If **ML** is not set, an individual connection is established from the source HG 3575 for each circuit in an access point that requires an announcement or music on hold.

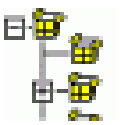
For further information on announcements or music on hold, refer to Section 2.12, “External Music on Hold”.

Conference:

A central configuration switch is used system-wide to set whether or not compressed connections can be connected to conference units.

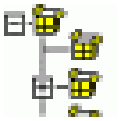
By default, only uncompressed RTO connections are supported with conference units. In other words, the codec classmarks associated with the conference units are set to G711.

You can use the AMO ZAND to change the setting to G711 & G729OPT.

	Administration of central system data can only be executed in expert mode. **Expert Mode > Expert Access > Open ...**<IP> with AMO (see AMO command)
	`CHANGE-ZAND:TYPE=ALLDATA3,IPDAVCCF=YES;` This AMO permits compressed connections with the conference unit.

The change becomes effective immediately, that is, the next time an IP connection is connected to a conference unit.

CO/tie trunks:

	**Configuration Management > System Data > Trunk > Trunk** Click **Search** and select the circuit. Set or delete the classmarks for **IP connections** on the **Basic Data** tab and **Save**.
	`CHANGE-TACSU:PEN=1-1-91-1,CLASSMRK=EC&G711;` Sets the EC and G711 classmarks. (G729OPT has effectively been deactivated in contrast to the default setting.)
	`CHANGE-TDCSU:PEN=1-1-91-1,CLASSMRK=G711;` Sets the G711 classmark.

IMPORTANT: If the classmark setting "**NONE**" is temporarily required for an outbound call (e.g. for privacy module), this can be done using an access code: AMO WABE: **NOEC**. This code can only be used as the prefix.

Example

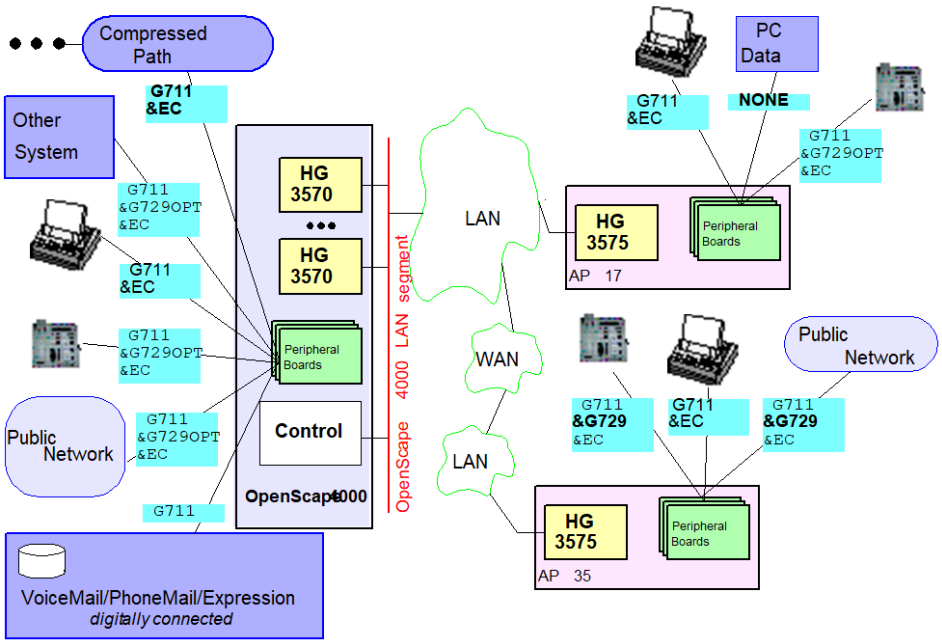


Figure 185: Classmarks

The example in Figure 20 "Classmarks" shows how classmarks are set for different circuits.

The default is G711&G729OPT&EC.

In the central system, there are three exceptions: the fax which does not tolerate signal compression, the compressed tie trunk path and the digital VoiceMail/PhoneMail/Expression server connected. Fax devices can also be configured with the default classmarks if STMI2/4/STMIX/STMIY and NCUI2/4 boards are used exclusively. A sequence of compressions and expansions should be avoided. The selected G711&EC setting in the example ensures that calls from the compressed tie trunk path cannot be compressed a second time. Digital announcement/voice recording devices connected generate absolutely no echo - and save voice in compressed form. Consequently, compression is disabled and EC is deactivated.

The data terminal device on the AP 17 is set to NONE, as it tolerates neither compression nor echo cancellation or attenuation/amplification. When the ISDN service is signaled correctly in the bearer capabilities, transmission is always performed with the NONE classmark, irrespective of the classmark setting.

The AP 35 is connected to the central system via WAN. Bandwidth is therefore a precious commodity and voice compression should always be used if possible. The setting G711&G729&EC for telephones and the CO line ensures that calls with telephone subscribers in the central system and AP 17 are compressed, as are calls from telephones in the central system or AP 17 via the local CO line in AP 35.

10.2.5 Special Routes

The usual demands made on the routing between access points and HG 3500 modules in the central OpenScape 4000 switch are fully met by the administration described above. A default router (AMO SIPCO, parameter **DEFRT**) serves the HiPath 3500 processors as an access to the IP world beyond the OpenScape 4000 LAN segment. One default router per LAN segment in which access points are located serves the access points as a bridge to other network segments.

However, additional demands may be imposed by the specific network architecture of the customer.

A distinction is to be made between 2 basic scenarios in this context:

- Links between LAN segments containing access points which do not lead to the respective LAN segments via the default router.
- Links from the OpenScape 4000 LAN segment to LAN segments containing access points which do not lead to the OpenScape 4000 LAN segment via the default router.

The difference is that, in the first case, only HG 3575 routing tables are affected, while in the second case, the routing tables of all HG 3500 modules, as well as the CC computer and the OpenScape 4000 Assistant, are also affected.

The routing tables of the HG 3500 and HG 3575 allow the configuration of 8 routes (in addition to default routes which do not appear in the routing table). These are configured by specifying a target (IP) address, the netmask of the target network and the IP address of the router port to be accessed by the source module.

It must be ensured that:

- no duplicate routes are entered, e.g.

192.168.23.99	,	255.255.255.0	,	192.168.22.2
192.168.23.98	,	255.255.255.0	,	192.168.22.2

1) The first entry already leads the route into the entire network segment 192.168.23.X via the router port 192.168.22.2. The second entry would achieve precisely the same and, therefore, must be suppressed.

- the configuration of the route from A to B remains in place without influencing the route from B to A. In other words, a route back to the source must generally also be configured in the target module, e.g.

192.168.22.43	,	255.255.255.0	,	192.168.23.2

10.2.5.1 Special Routes Between Access Points

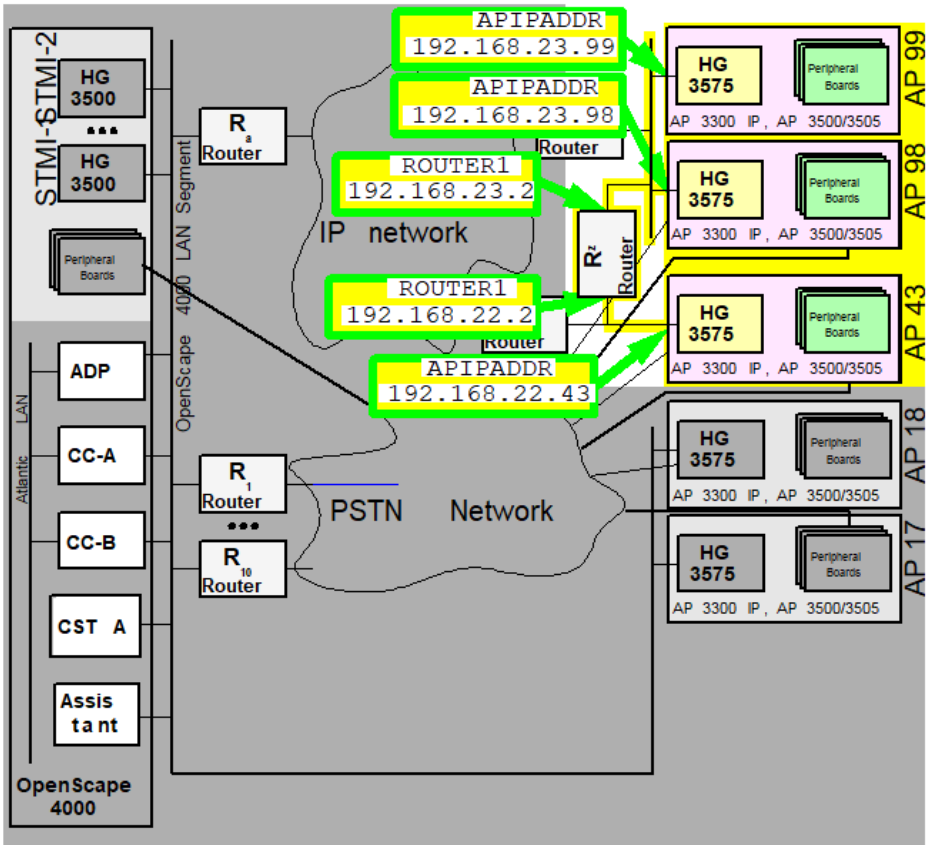
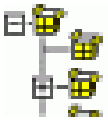


Figure 186: Special routes between access points

Generation

The configuration of special routes in HG 3575 (NCUI2/4S) is realized with the AMO APRT in the **ROUTTBL** branch.

Configuring the scenario illustrated in Figure 21 “Special routes between access points”:

	**Configuration Management > System Data > IPDA > HG3575 Additional Routing** Click **New** if there are no existing entries. Enter **LTU**. Enter the IP addresses of the destinations and routers, enter the network masks in the routing table and **Save**.

	`CHANGE-APRT:TYPE=ROUTTBL,MTYPE=NCUI,LTU=99, DSTADDR1=192.168.22.43,DSTMSK1=255.255.255.0, ROUTER1=192.168.23.2;`
	Sets the route from AP99 to AP43 via Router Rz.
	`CHANGE-APRT:TYPE=ROUTTBL,MTYPE=NCUI,LTU=98, DSTADDR1=192.168.22.43,DSTMSK1=255.255.255.0, ROUTER1=192.168.23.2;`
	Sets the route from AP98 to AP43 via Router Rz.
	`CHANGE-APRT:TYPE=ROUTTBL,MTYPE=NCUI,LTU=43, DSTADDR1=192.168.23.99,DSTMSK1=255.255.255.0, ROUTER1=192.168.22.2;`
	Sets the route from AP43 to AP99 - **and AP98** - via Router Rz.

In this example, the first of the 8 routing table entries was used in all 3 modules. Of course, this presupposes that these entries have not yet been used.

If the first 2 entries had already been used in AP43, the following would need to be done:

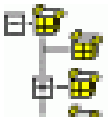
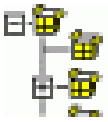
	**Configuration Management > System Data > IPDA > HG3575 Additional Routing** Click **Search** and select **LTU**. Enter the IP addresses in line 3 of the routing table and **Save**.
	`CHANGE-APRT:TYPE=ROUTTBL,MTYPE=NCUI,LTU=43, DSTADDR3=192.168.23.99,DSTMSK3=255.255.255.0, ROUTER3=192.168.22.2;`

Table 16 “AMO APRT parameters in CHANGE branch under TYPE=ROUTTBL” provides a precise description of the parameters.

If a **ROUTTBL** entry is to be deleted (e.g. the second entry in AP43), this is realized as follows:

	**Configuration Management > System Data > IPDA > HG3575 Additional Routing** Click **Search** and select **LTU**. Delete the IP addresses in the second line of the routing table and **Save**. **Configuration Management > System Data > IPDA > IPDA System Data** Click **Search** and select the access point. Click **Execute** on the **Action** pull-down menu and select the mode of action **Update AP**, confirm with **OK**.

	`DELETE-APRT:TYPE=ROUTTBL,MTYPE=NCUI,LTU=43,INDEX=2;`
	In order for these changes to become effective in the access point, this has to be restarted with
	`EXEC-USSU:MODE=UPDATAP,LTU=xx;`

IMPORTANT: Connections are cleared down without further warning. Prior to the `EXEC-USSU:UPDATAP`, the configuration must be updated on the system hard disk.

10.2.5.2 Special Routes between Access Point and OpenScape 4000 LAN Segment

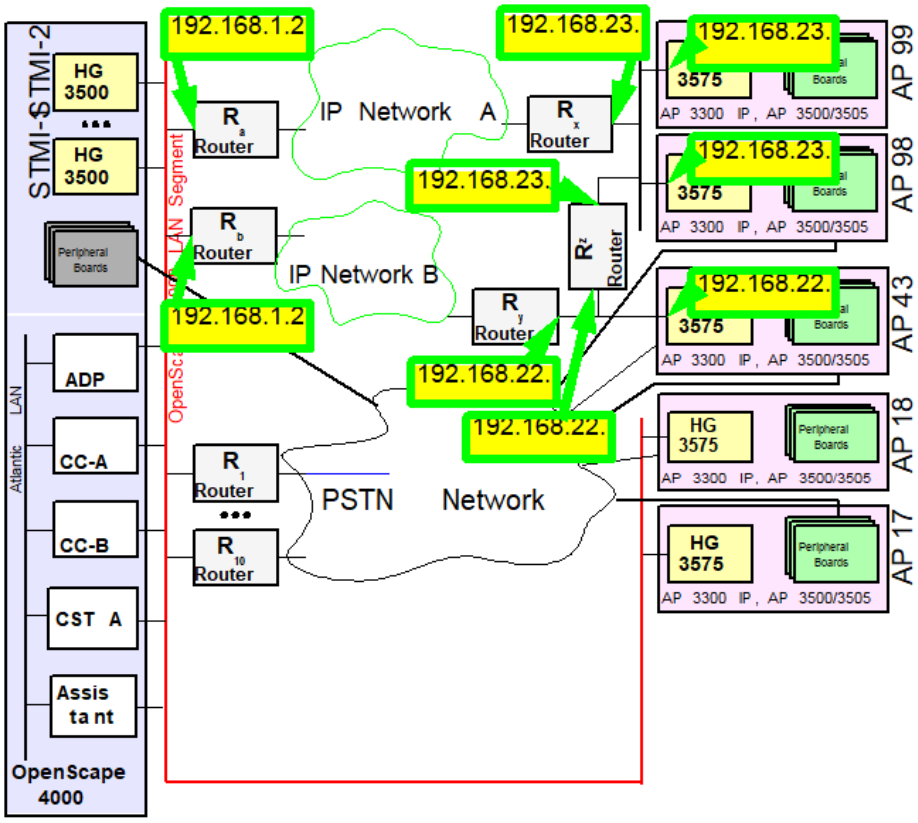


Figure 187: Special routes between access point and OpenScape 4000 LAN segment

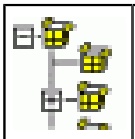
This complicated scenario is based on the simple case of the special route between 2 access points. In addition, the IP network of the customer in this case is broken down into 2 sub-networks which are not, or only, linked to one another via the OpenScape 4000 LAN segment.

This scenario assumes that the routers a, x and y are the default routers (for OpenScape 4000 components) in the respective networks.

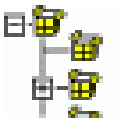
Without additional routes, neither the HG 3500, nor the “direct link“ access points AP17 and AP18 can reach access point AP 43.

The configuration for the entire scenario is realized according to the following steps:

- Configure Router Ra as the default router for all HG 3500 modules

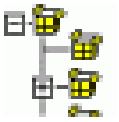
	**Configuration Management > System Data > IPDA > IPDA System Data** Click **Search** and enter the default router address, then **Save**.
	`ADD-SIPCO: ... DEFRT=192.168.1.254 ...;`

- Configure Router Ra as the default router for AP17 and AP18

	**Configuration Management > System Data > IPDA > IPDA Access Point** Click **Search** and select the access point. Enter the router address on the **IP Interface (DL)** tab, then **Save**.

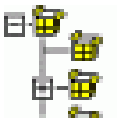
	`ADD-UCSU:UNIT=AP,LTU=17, ...`
	`APRTADDR=192.168.1.254 ...;`
	and
	`ADD-UCSU:UNIT=AP,LTU=18, ...`
	`APRTADDR=192.168.1.254 ...;`

- Configure Router Rx as the default router for AP98 and AP99 and specify Router Ra as the route for the signaling messages of the CC-A and CC-B, respectively

	**Configuration Management > System Data > IPDA > IPDA Access Point** Click **Search** and select the access point. Enter the router addresses on the **IP Interface (NW)** tab, then **Save**.

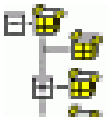
	`CHANGE-UCSU:UNIT=AP,LTU=98, ...`
	`LSRTADDR=192.168.1.254,APRTADDR=192.168.23.1 ...;`
	and
	`ADD-UCSU:UNIT=AP,LTU=99, ...`
	`LSRTADDR=192.168.1.254,APRTADDR=192.168.23.1 ...;`

- Configure Router Ry as the default router for AP43 and specify Router Rb as the route for the signaling messages of the CC-A and CC-B, respectively

	**Configuration Management > System Data > IPDA > IPDA Access Point** Click **Search** and select the access point. Enter the router addresses on the **IP Interface (NW)** tab, then **Save**.
	`ADD-UCSU:UNIT=AP,LTU=43, ...` `LSRTADDR=192.168.1.253,APRTADDR=192.168.22.1 ...;`

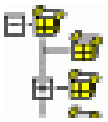
The payload between AP43 and AP98/AP99 would now be routed via Router Ry -> Router Rb -> Router Ra -> Router Rx. The shortcut via Router Rz is configured as in the previous example with:

- Set the routes from AP43 to AP98/AP99 via Router Rz

	**Configuration Management > System Data > IPDA > HG3575 Additional** **Routing** Click **Search**, select the access point, enter or change IP addresses, then click **Save**.
	`CHANGE-APRT:TYPE=ROUTTBL,MTYPE=NCUI,LTU=43, DSTADDR1=192.168.23.99,DSTMSK1=255.255.255.0, ROUTER1=192.168.22.2;`

For the payload route from AP98/AP99 to AP43, special routes likewise have to be configured:

- Set the routes from AP98/AP99 to AP43 via Router Rz

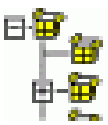
	**Configuration Management > System Data > IPDA > HG3575 Additional** **Routing** Click **Search**, select the access point, enter or change IP addresses, then click **Save**.
	`CHANGE-APRT:TYPE=ROUTTBL,MTYPE=NCUI,LTU=98, DSTADDR1=192.168.22.43,DSTMSK1=255.255.255.0, ROUTER1=192.168.23.2;` `CHANGE-APRT:TYPE=ROUTTBL,MTYPE=NCUI,LTU=99, DSTADDR1=192.168.22.43,DSTMSK1=255.255.255.0, ROUTER1=192.168.23.2;`

The payload from the HG 3500 to AP98/AP99 is routed via the default router, Ra. The route is already specified with ADD-SIPCO.

The payload from AP98/AP99 to the HG 3500 is routed via the default router, Rx. The route is already specified with ADD-UCSU.

However, for the payload transport from the HG 3500 to AP43, the route is still missing. In this case, a special route has to be configured for all HG 3500s (STMI2/4/STMIX/STMIY) via Router Rb:

- Set the route from the HG 3500 to AP43 via Router Rb

	**Configuration Management > System Data > IPDA > HG3570 Additional** **Routing** Click **Search**, enter or change network mask, destination and router addresses, then click **Save**.
	`CHANGE-APRT:TYPE=ROUTTBL,MTYPE=STMI, DSTADDR1=192.168.22.43,DSTMSK1=255.255.255.0, ROUTER1=192.168.1.253;`

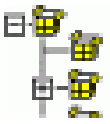
The payload from AP43 to the HG 3500 is routed via the default router, Ry. The route is already specified with ADD-UCSU.

The payload between the HG 3500 and the “direct link“ access points AP17/AP18 and back remains within the OpenScape 4000 LAN segment and requires no additional routes.

The payload between the “direct link” access points AP17/AP18 and AP98/AP99 and back is routed via the route specified with ADD-UCSU. (Ra, Rx)

However, for the payload transport from the “direct link“ access points AP17/AP18 and AP43, the route is still missing. In this case, a special route has to be configured via Router Rb:

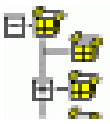
- Set the routes from AP17/AP18 to AP43 via Router Rb

	**Configuration Management > System Data > IPDA > HG3575 Additional** **Routing** Click **Search**, select the access point, enter or change network mask, destination and router addresses, then click **Save**.

	`CHANGE-APRT:TYPE=ROUTTBL,MTYPE=NCUI,LTU=17,`
	`DSTADDR1=192.168.22.43,DSTMSK1=255.255.255.0,`
	`ROUTER1=192.168.1.253;`
	`CHANGE-APRT:TYPE=ROUTTBL,MTYPE=NCUI,LTU=18,`
	`DSTADDR1=192.168.22.43,DSTMSK1=255.255.255.0,`
	`ROUTER1=192.168.1.253;`

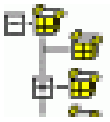
The payload from AP43 to AP17/AP18 is routed via the default router, Ry, and no additional routes need to be configured.

In order for these changes to become effective in the access points, these have to be restarted.

	**Configuration Management > System Data > IPDA > IPDA System Data** Click **Search** and select the access point. Click **Execute** on the **Action** pull-down menu and select the mode of action **Update AP**, confirm with **OK**.
	`EXEC-USSU:MODE=UPDATAP,LTU=xx;`

IMPORTANT: Connections are cleared down without further warning. Prior to the `EXEC-USSU:UPDATAP`, the configuration must be updated on the system hard disk.

In order for these changes to become effective in the HG 3500, **all** HG 3500 modules have to be restarted.

	**Configuration Management > System Data > Maintenance > Board Maintenance** Click **Search** and select **STMI**. Click **Execute** on the **Action** pull-down menu, select **Restart** and confirm with **OK**.
	`RESTART-BSSU:ADDRTYPE=PARTNO,PARTNO=Q2316-X,FCTID=1;`

IMPORTANT: Connections are cleared down without further warning.

In order to maintain an overview in these somewhat more complex scenarios, the creation of a communications matrix is recommended:

Table 44: Communication matrix for special routes between access point and OpenScape 4000 LAN segment”

to from	CC-A	CC-B	HG 3500	AP 17	AP 18	AP 43	AP 98	AP 99
CC-A	-	-	-	direct	direct	Rb	Ra	Ra
CC-B	-	-	-	direct	direct	Rb	Ra	Ra
HG 3500	-	-	-	direct	direct	Rb	Ra	Ra
AP 17	direct	direct	direct	-	direct	Rb	Ra	Ra
AP 18	direct	direct	direct	direct	-	Rb	Ra	Ra
AP 43	Ry	Ry	Ry	Ry	Ry	-	Rz	Rz
AP 98	Rx	Rx	Rx	Rx	Rx	Rz	-	direct
AP 99	Rx	Rx	Rx	Rx	Rx	Rz	direct	-

Table 45: AMO APRT parameters in CHANGE branch under TYPE=ROUTTBL

AMO	Parameter	Sprache/ Language	Beschreibung/Description
APRT	MTYP	d	Modul Typ Hier wird zwischen STMI2/4/STMIX/ STMIY (HG 3500) und NCUI2/4 (HG 3575) unterschieden. MTYP=STMI: Diese Routing Table gilt für alle STMI2/4/ STMIX/STMIY im System gleichermaßen. DSTADRx darf nicht zum OpenScape 4000 LAN Segment gehören. ROUTERx muss zum OpenScape 4000 LAN Segment gehören. (siehe NETADR im AMO SIPCO, Table 1 “AMO SIPCO parameters in ADD branch or for CHANGE unde MTYP=NCUI: Diese Routing Tabelle gilt nur für die durch LTU angegebene NCUI2/4. Bei Routen zwischen 2 NCUI2/4 müssen bei beiden NCUI2/4 die entsprechenden Einträge gemacht werden!
	MTYPE	e	Modul Type This is to distinguish between STMI2/4/ STMIX/STMIY (HG 3500) and NCUI2/4 (HG 3575). MTYPE=STMI: This routing table is common to all the STMIs in the system. DSTADRx must not belong to the OpenScape 4000 LAN Segment. ROUTERx must belong to the OpenScape 4000 LAN Segment. (see NETADDR in AMO SIPCO, Table 1 “AMO SIPCO parameters in ADD branch or for CHANGE unde MTYPE=NCUI: This routing table is valid only for the NCUI2/4 assigned by LTU. For routes between 2 NCUI2/4 entries must be made for both NCUI2/4 respectively!

AMO	Parameter	Sprache/ Language	Beschreibung/Description
	DSTADR1	d	Zieladresse der 1. Route. Legt die Adresse fest, die über die im 1. Eintrag spezifizierte Route erreicht werden soll. Das kann eine Host- oder auch eine Netzadresse sein. Die DSTMSK1 erlaubt die Interpretation.
	DSTADDR1	e	Destination Address for the 1st Route. Assigns the address to be reached using the route defined in the 1. entry. It may be a host or a network address. DSTMSK1 allows the interpretation.
	DSTMSK1	d	Netzmaske des Netzes, dem DSTADR1 angehört
	DSTMSK1	e	Netmask of the network which DSTADDR1 is part of
	ROUTER1	d	IP-Adresse des Routers, über den Pakete an DSTADR1 gesendet werden sollen. Diese IP-Adresse muss zum OpenScape 4000 LAN Segment gehören (siehe NETADR im AMO SIPCO, Table 1 “AMO SIPCO parameters in ADD branch or for CHANGE
	ROUTER1	e	IP Address of the Router via which Packets to DSTADDR1 are to be sent. This IP address must belong to the OpenScape 4000 LAN Segment (see NETADDR in AMO SIPCO, Table 1 “AMO SIPCO parameters in ADD branch or for CHANGE
	DSTADR2	d	Zieladresse der 2. Route.
	DSTADDR2	e	Destination Address for the 2nd Route.
	DSTMSK2	d	Netzmaske des Netzes, dem DSTADR2 angehört
	DSTMSK2	e	Netmask of the network which DSTADDR2 is part of
	ROUTER2	d	IP-Adresse des Routers, über den Pakete an DSTADR2 gesendet werden sollen.
	ROUTER2	e	IP Address of the Router via which Packets to DSTADDR2 are to be sent.
	DSTADR3	d	Zieladresse der 3. Route.
	DSTADDR3	e	Destination Address for the 3rd Route.

AMO	Parameter	Sprache/ Language	Beschreibung/Description
	DSTMSK3	d	Netzmaske des Netzes, dem DSTADR3 angehört
	DSTMSK3	e	Netmask of the network which DSTADDR3 is part of
	ROUTER3	d	IP-Adresse des Routers, über den Pakete an DSTADR3 gesendet werden sollen.
	ROUTER3	e	IP Address of the Router via which Packets to DSTADDR3 are to be sent.
	DSTADR4	d	Zieladresse der 4. Route.
	DSTADDR4	e	Destination Address for the 4th Route.
	DSTMSK4	d	Netzmaske des Netzes, dem DSTADR4 angehört
	DSTMSK4	e	Netmask of the network which DSTADDR4 is part of
	ROUTER4	d	IP-Adresse des Routers, über den Pakete an DSTADR4 gesendet werden sollen.
	ROUTER4	e	IP Address of the Router via which Packets to DSTADDR4 are to be sent.
	DSTADR5	d	Zieladresse der 5. Route.
	DSTADDR5	e	Destination Address for the 5th Route.
	DSTMSK5	d	Netzmaske des Netzes, dem DSTADR5 angehört
	DSTMSK5	e	Netmask of the network which DSTADDR5 is part of
	ROUTER5	d	IP-Adresse des Routers, über den Pakete an DSTADR5 gesendet werden sollen.
	ROUTER5	e	IP Address of the Router via which Packets to DSTADDR5 are to be sent.
	DSTADR6	d	Zieladresse der 6. Route.
	DSTADDR6	e	Destination Address for the 6thRoute.
	DSTMSK6	d	Netzmaske des Netzes, dem DSTADR6 angehört
	DSTMSK6	e	Netmask of the network which DSTADDR6 is part of

AMO	Parameter	Sprache/ Language	Beschreibung/Description
	ROUTER6	d	IP-Adresse des Routers, über den Pakete an DSTADR6 gesendet werden sollen.
	ROUTER6	e	IP Address of the Router via which Packets to DSTADDR6 are to be sent.
	DSTADR7	d	Zieladresse der 7. Route.
	DSTADDR7	e	Destination Address for the 7th Route.
	DSTMSK7	d	Netzmaske des Netzes, dem DSTADR7 angehört
	DSTMSK7	e	Netmask of the network which DSTADDR7 is part of
	ROUTER7	d	IP-Adresse des Routers, über den Pakete an DSTADR7 gesendet werden sollen.
	ROUTER7	e	IP Address of the Router via which Packets to DSTADDR7 are to be sent.
	DSTADR8	d	Zieladresse der 8. Route.
	DSTADDR8	e	Destination Address for the 8th Route.
	DSTMSK8	d	Netzmaske des Netzes, dem DSTADR8 angehört
	DSTMSK8	e	Netmask of the network which DSTADDR8 is part of
	ROUTER8	d	IP-Adresse des Routers, über den Pakete an DSTADR8 gesendet werden sollen.
	ROUTER8	e	IP Address of the Router via which Packets to DSTADDR8 are to be sent.

10.2.6 Signaling Survivability

Signaling Survivability has been moved to an own section within the IP Solutions:

1) Signaling Survivability

10.2.7 Quality Monitoring for the Signaling Connection over IP

As already described in the section Signaling Survivability, you cannot operate an access point unless the signaling connection is working properly.

The concept for monitoring the signaling connection uses the additional monitoring connection to verify if communication is basically possible between

CC and an access point. The main advantage of this is that you can respond very quickly and activate signaling survivability in the event of a crash on the IP connection between CC and the access point.

The IP connection between the CC and access point is sometimes not completely severed, “just“ severely restricted. This can have an extremely negative impact on the signaling function without this malfunction being detected by the separate monitoring connection.

To eliminate this restriction, we have introduced a new mechanism for monitoring the actual signaling connection to complement the mechanism already described and based on a separate monitoring connection.

This additional functionality is split into five components:

- Restriction of the Available Signaling Bandwidth (Traffic Shaping)
- Monitoring the Runtime for Signaling Messages (Round Trip Delay)
- Monitoring Message Throughput
- Advanced Criteria for Signaling Survivability
- Output of Statistical Information on the Signaling Connection

10.2.7.1 Restriction of the Available Signaling Bandwidth (Traffic Shaping)

The signaling bandwidth for controlling an access points is not particularly large and fluctuates very heavily. A flat rate of 64 Kbps is required for the signaling connection, although in some configurations a lower bandwidth (e.g. 32 Kbps) would be sufficient for normal business hours, i.e. to control the call processing/ access point.

Bandwidth requirements spike briefly when a call processing action triggers numerous parallel follow-up actions in the peripherals. Several large packets containing signaling information can be sent to an access point in a short period of time.

During startup/installation of an access point there is also more bandwidth needed (e.g. FTP loadwre transfer for NCUI board and other peripheral boards) and as a consequence there must be a minimum bandwidth of 64 Kbps for TCP signaling available/guaranteed (same bandwidth available via ISDN modem, i.e. signaling survivability).

For a WAN router with a very low available bandwidth for this signaling connection (e.g. 64 Kbps), this means that while the first packet from this burst is being sent, another is being received. The router may not have enough buffer space to buffer the packets. As a result, packets from this “burst“ are rejected by the router and have to be resent later by the CC.

Restricting the signaling bandwidth to an access point in the CC prevents a burst from occurring when packets are immediately sent one after the other from the CC. This is done by staggering the packets so that they are sent at intervals that prevent buffer overflow in the router.

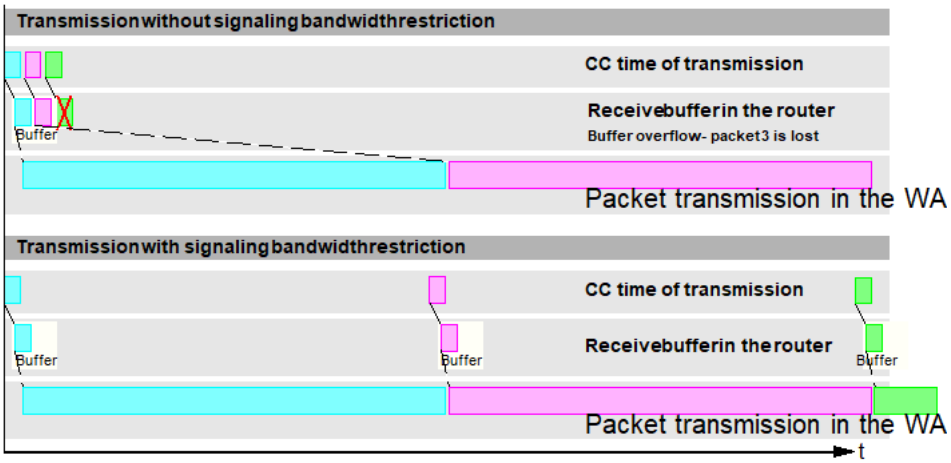


Figure 188: Signaling connection with/without bandwidth restriction

---

IMPORTANT: If there is only a bandwidth of between 64 and 250 Kbps available for signaling to an access point in the IP network, then signaling bandwidth restriction must be activated (AMO STMIB, parameter **SIGQOS**) in the CC and set to the value available in the network.

The signaling bandwidth restriction delays signaling messages in the CC and sometimes results in a backlog of several messages. If a backlog of this kind persists for several seconds, the signaling bandwidth configured is too low. The system issues the error message F8292 (see Table 16 “F8292 - Bandwidth Requirement Exceeds Limit”) that marks the beginning of backlog. The publication of a message status can also be a criteria for changing from the signaling path to the signaling survivability path (see Section 2.7.4, “Advanced Criteria for Signaling Survivability”).

The message F8293 is output to signal that the backlog has cleared (see Section 2.7.6.5, “F8293 - Bandwidth Required Back Below Limit”).

The restriction of the signaling bandwidth only affects the signaling path over LAN. The modem connection is not affected in the case of signaling survivability.

IMPORTANT: Under-dimensioning the signaling bandwidth can lead to a message buffer deficit which results in a access point reset. All connections are then cleared down. The system outputs the error message F8292 as soon as under-dimensioning is detected during live operation (see Section 2.7.6.4, “F8292 - Bandwidth Requirement Exceeds Limit”). The actual available signaling bandwidth in the customer network **must** be increased in response to this message. Ignoring these early warning signals can result in the mentioned access point reset or other major issues. Furthermore a restriction of the bandwidth in the TCP can cause long delays during loading the loadware and setting up the shelf/system!

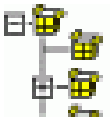
Procedure

At the start of each second, a transmission credit with the value of the signaling bandwidth configured is made available for use. If the setting is 64 Kbps, for example, 8000 bytes may be transmitted every second. For every packet to be sent, the credit is now reduced by the packet size. If there is not enough credit left, the packet is delayed until sufficient credit is available.

When the second expires, the remaining transmission credit is cancelled. The next second then starts again with a new credit for the value of the signaling bandwidth configured, for example, 8000 bytes. Returned packets can now be sent.

The transmission bandwidth is restricted at “application level“, in other words, over the TCP/IP stack.

Generation

	**Configuration Management > System Data > IPDA > Access point** Click **Search** and enter or change the bandwidth on the **Quality of Service** tab in the **Signaling Quality of Service** section, then **Save**.
	`CHANGE-STMIB:MTYPE=NCUI2,TYPE=SIGQOS,LTU=99,BANDW=64;`

The signaling bandwidth is expressed in kilobits per second (Kbps). The value `BANDW=0` disables signaling bandwidth restriction (default configuration). The setting becomes effective immediately.

10.2.7.2 Monitoring the Runtime for Signaling Messages (Round Trip Delay)

If a malfunction occurs in the IP network, the effective bandwidth available drops and the time between the dispatch of a message and receipt acknowledgement rises.

A maximum permissible message runtime can be defined for the signaling connection for every access point. This runtime includes the entire time from sending the message to receiving the acknowledgement, in other words, the “Round Trip Delay“. The runtime is evaluated with every signaling message. Measurement is therefore independent of the signaling load.

If the runtime exceeds the limit set, the system outputs the error message F8290 (see Section 2.7.6.2, “F8290 - Net Weakness Begin”). The exceeding of the maximum message runtime can also be a criteria for changing from the signaling path to the signaling survivability path (see Section 2.7.4, “Advanced Criteria for Signaling Survivability”).

The message F8291 is output to signal a return by the runtime to permitted values (see Section 2.7.6.3, “F8291 - Net Weakness End”).

Monitoring the maximum message runtime is only active on the signaling path over LAN. The modem connection is not affected in the case of signaling survivability.

Procedure

An average runtime value is calculated and stored every three seconds for all messages acknowledged in this interval.

The three-second average values are used to generate further average values over a short (15 seconds: SHORT) and long monitoring time (60 seconds: LONG).

The error message is generated whenever either of the two values (SHORT/LONG) exceeds the limit configured.

The limit is set for the long monitoring duration (LONG). The limit for the short duration (SHORT) is set to factor 2 times the value.

The SHORT interval makes sense with a higher limit because if the network quality jumps, the system can respond faster, that is, within 15 seconds. This interval would be 60 seconds in the case of exact measurement.

The measurement is made at “application level“, in other words, over the TCP/IP stack. On account of stack dynamics, measured values cannot be compared directly with values that are measured directly on the network.

The runtime includes:

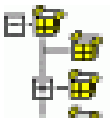
1) Sender of packet from TCP level in the OpenScape 4000 central system

- Transmission of packet in the network
- Receipt of packet on HG 3575 up to TCP
- Creation and sending of acknowledgement on the HG 3575
- Transmission of acknowledgement in the network
- Receipt of acknowledgement in the OpenScape 4000 central system

Since TCP can delay the acknowledgement of a packet in order to combine the acknowledgement with that of another packet, values under 400 ms are impractical.

Keep alive packets are not included in the measurement. If no packets are sent or acknowledged within a 3-second interval, a long-term mean value is used that is determined by the TCP.

Generation

	**Configuration Management > System Data > IPDA > Access point** Click **Search** and enter or change the maximum runtime on the **Quality of Service** tab in the **Signaling Quality of Service** section, then **Save**.
	`CHA-STMIB:MTYPE=NCUI2,TYPE=SIGQOS,LTU=99,MAXRTD=500;`

The message runtime is expressed here in milliseconds. The value `MAXRTD=0` disables message runtime monitoring. The setting becomes effective immediately.

IMPORTANT: Measurements are performed at 10-ms intervals. As a result, it only makes sense to set values divisible by 10 (without remainder), for example, 400, 410, 420, etc.

10.2.7.3 Monitoring Message Throughput

A minimum necessary message throughput can be defined for the signaling connection for every access point. The throughput measurement includes the volume of all messages sent by the CC.

The undershooting of the minimum necessary message throughput only takes account of the times when the specified load at least was used. An undershooting of the minimum message throughput is ignored because the number of messages available for transmission is not sufficient.

If the throughput falls short of the threshold value set, the system outputs the error message F8290 (see Section 2.7.6.2, “Message Throughput Undershot”). The undershooting of the minimum message throughput can also be a criteria for changing from the signaling path to the signaling survivability path (see Section 2.7.4, “Advanced Criteria for Signaling Survivability”).

The message F8291 is output to signal a return by the message throughput to permitted values (see Section 2.7.6.3, “F8291 - Net Weakness End”).

Monitoring the minimum message throughput is only active on the signaling path over LAN. The modem connection is not affected in the case of signaling survivability.

Procedure

Every three seconds the system calculates the number of bytes sent during this interval. The result is then used to calculate the throughput in Kbps. *(Bytes sent * 8/3)*

The three-second values are used to generate average values over a short (15 seconds: SHORT) and long monitoring time (60 seconds: LONG).

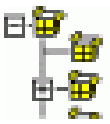
The error message is generated whenever either of the two values (SHORT/LONG) exceeds the limit configured.

The limit is set for the long monitoring duration (LONG). The limit for the short duration (SHORT) is set to 2/3 of the LONG value.

The SHORT interval makes sense with a lower limit because if the network quality jumps, the system can respond faster, that is, within 15 seconds. This interval would be 60 seconds in the case of exact measurement.

The measurement is made at “application level“, in other words, over the TCP/IP stack. On account of stack dynamics, measured values cannot be compared directly with values that are measured directly on the network.

Generation

	**Configuration Management > System Data > IPDA > Access point** Click **Search** and enter or change the minimum message throughput on the **Quality of Service** tab in the **Signaling Quality of Service** section, then **Save**.
	`CHA-STMIB:MTYPE=NCUI2,TYPE=SIGQOS,LTU=99,MINTHRPT=32;`

The minimum message throughput is expressed here in Kbps. The value `MINTHRPT=0` disables message throughput monitoring. The setting becomes effective immediately.

10.2.7.4 Advanced Criteria for Signaling Survivability

The restriction and monitoring functions described in Section 2.7.1, “Restriction of the Available Signaling Bandwidth (Traffic Shaping)” to Section 2.7.3, “Monitoring Message Throughput” can trigger the signaling path switchover from LAN to modem.

The events that should activate signaling survivability are set for each access point in the course of configuration.

The following options are available:

- Switching over the signaling path to modem in the event of loss of monitoring connection - [STD] In STanDard mode, the signaling path is switched back to LAN as soon as stability returns to the monitoring connection.
- Switching over the signaling path to modem in the event of loss of the monitoring connection or violation of the criteria from monitoring the quality of the signaling connection - [EXTENDED] In EXTENDED mode, the signaling path is switched back to LAN as soon as stability returns to the monitoring connection and the quality criteria are satisfied. To measure the quality criteria, a load is periodically generated on the monitoring connection which must at least be able to transport the signaling connection after reverting to LAN.

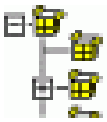
  IMPORTANT: When using EXTENDED mode, the bandwidth available must be taken into consideration on the signaling path over modem. There is no point in switching to a 28.8-Kbps modem connection because the minimum throughput for the LAN connection falls short of 64 Kbps.

- Exclusive use of the signaling path on modem - [SURVONLY] SURVONLY mode permits the administrative switchover of the signaling path to modem irrespective of behavior on the LAN connection. This can be used for stable switchover when performing planned maintenance in the LAN/WAN environment for the duration of the maintenance work. Switching back is then performed in STanDard or EXTENDED mode

  IMPORTANT: Even in the case of administrative activation of signaling survivability for an access point, the establishment of

new payload connections is blocked in the OpenScape 4000 CC (to all HG 3500s).

Generation

	**Configuration Management > System Data > IPDA > Access point** Click **Search** and select the switchover mode for signaling survivability on the **Quality of Service** tab in the **Signaling Quality of Service** section, then **Save**.
	`CHA-STMIB:MTYPE=NCUI2,TYPE=SIGQOS,LTU=99,SIGPTHSW=EXTENDED;`

The setting becomes effective immediately.

10.2.7.5 Output of Statistical Information on the Signaling Connection

If monitoring is active for the message runtime or the message throughput, the system only signals the results of measurements if limits are breached.

It is therefore very difficult to say if the limits configured were set too low or even much too high.

For this reason, the cyclical output of measurement data can be set at the operating terminal.

You can set whether or not measurement data should be output cyclically for every access point.

Data is only output, however, if

- monitoring is active for the message runtime or the message throughput
- output is generally enabled with the AMO-DIAGS (CC/HSR option S00)

The measurement data are output with the message F8289

IMPORTANT: The cyclical query and output of measurement data generates a high load in the system. There is also a danger that important error messages will be overlooked in the surge of measurement data. As a result, the output of measurement data may only be selectively used for a limited number of access points simultaneously. The output release should only be used for a manageable period of time.

For further information (e.g. on generation) please refer to **Gateways HG 3500 and HG 3575 >** Section 11.11, “TYPE SIGQOS - Quality Monitoring for the Signaling Connection over IP”**.**

10.2.7.6 Error Messages from Quality Monitoring for the Signaling Connection over IP

10.2.7.6.1 F8289 - Output of Statistics Data

IMPORTANT: The displayed values are decimal values in kbit/s. The target is to have high values: displayed value >= short value => good displayed value < short value => bad

Round Trip Delay

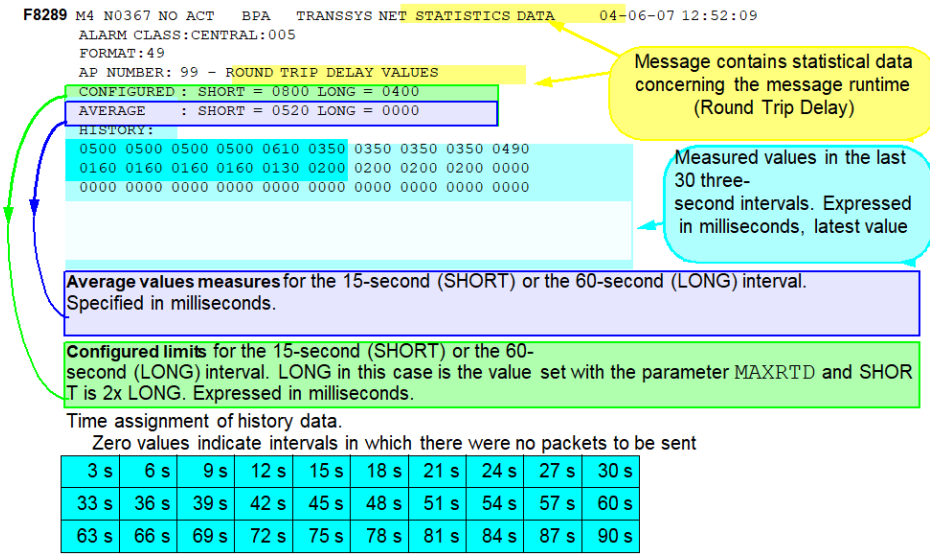


Figure 189: F8289 - Output of statistics data concerning message runtime (round trip delay)

Message Throughput

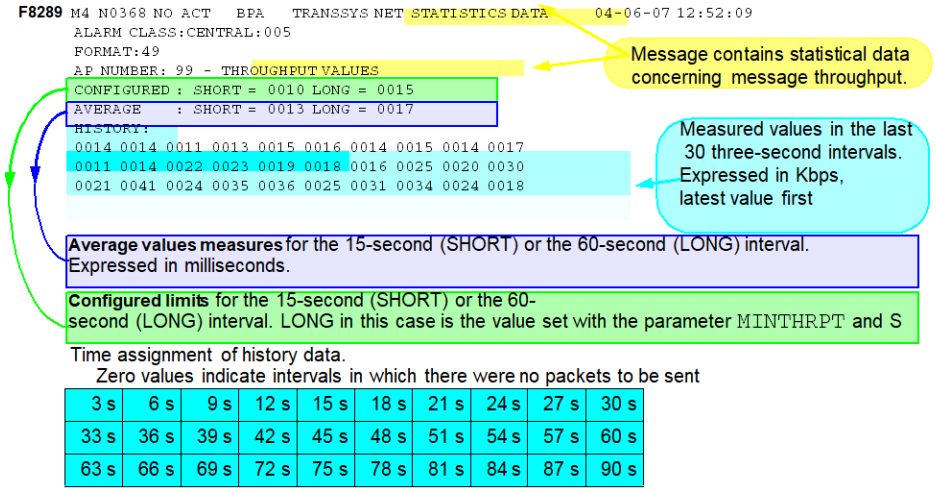


Figure 190: F8289 - Output of statistics data concerning message throughput

10.2.7.6.2 F8290 - Net Weakness Begin

IMPORTANT: The displayed values are decimal values in kbit/s. The target is to have high values: displayed value >= short value => good displayed value < short value => bad

Message Runtime Exceeded

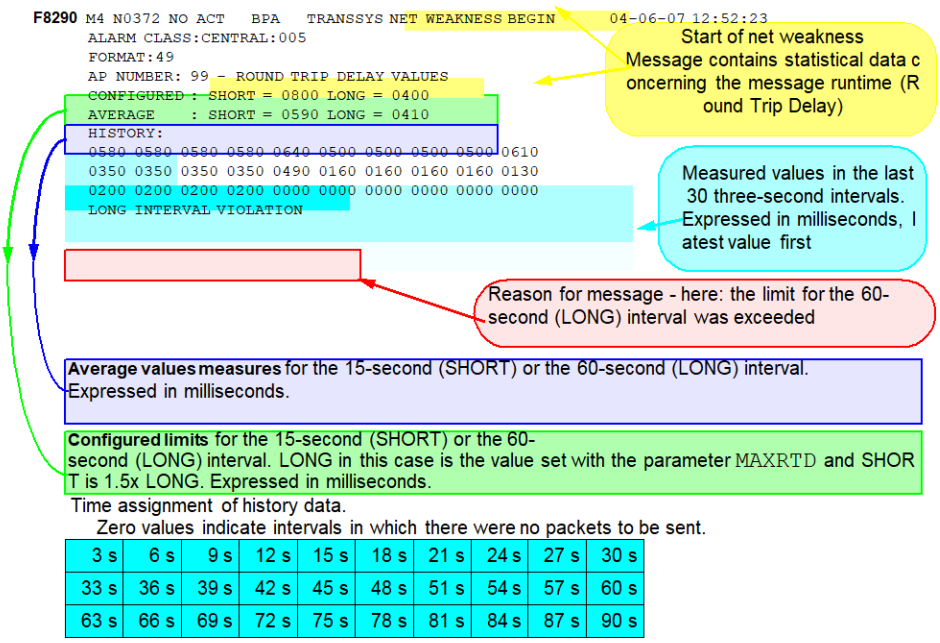


Figure 191: F8290 - Start of net weakness (statistical data concerning message runtime (round trip delay))

Message Throughput Undershot

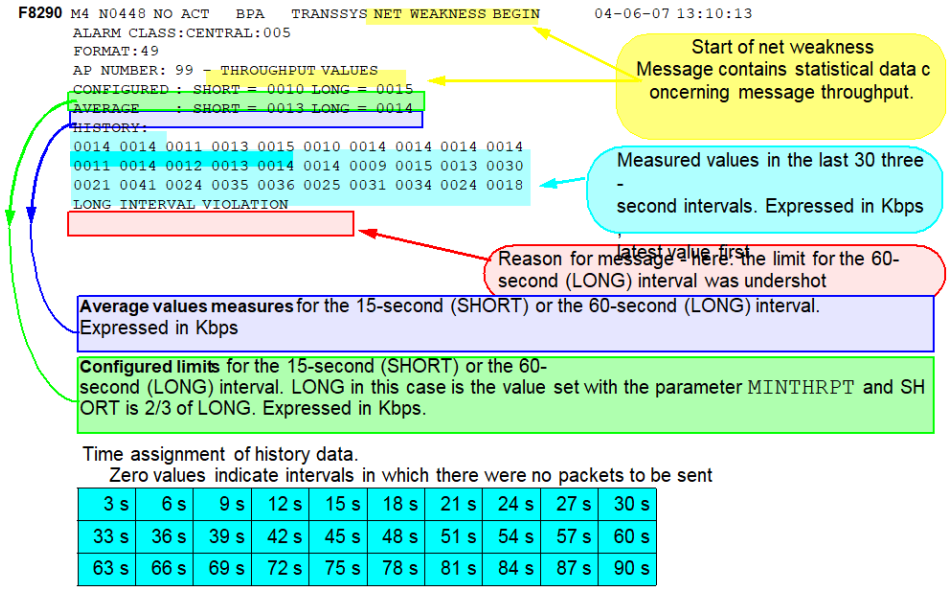


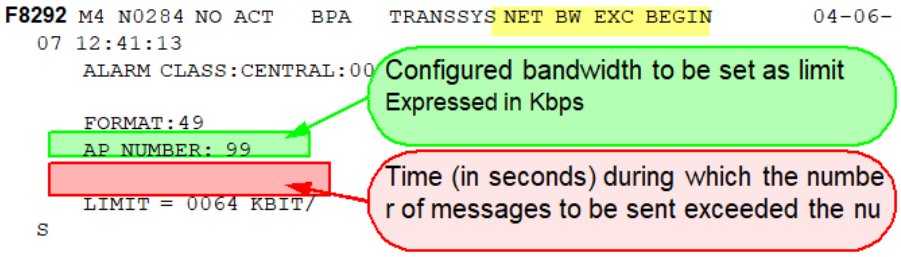
Figure 192: F8290 - Start of net weakness (statistical data concerning message throughput

10.2.7.6.3 F8291 - Net Weakness End

```
F8291 M4 N0380 NO ACT   BPA   TRANSSYS NET WEAKNESS END        04-06-
  07 13:04:05
      ALARM CLASS:CENTRAL:005

      FORMAT:49
```

10.2.7.6.4 F8292 - Bandwidth Requirement Exceeds Limit



10.2.7.6.5 F8293 - Bandwidth Required Back Below Limit

```
F8293 M4 N0366 NO ACT   BPA   TRANSSYS NET BW EXC END          04-06-
  07 12:49:45
           ALARM CLASS:CENTRAL:005

      FORMAT:49
```

10.2.8 Source Dependent Routing

With IP distributed architecture, it is possible to position parts of a OpenScape 4000 system in different local networks. In this way, the OpenScape 4000 CC could be located in Munich, with linked access points in Berlin and Frankfurt.

Now, if all calls were to be subject to uniform routing, this would result in a call from the Frankfurt access point being routed into the Frankfurt local network - with LCR from the point of view of the CC in Munich - via IP to Munich and from there back to Frankfurt as a long-distance call. This would not be particularly cost-effective.

If a subscriber at the access point in Berlin were to call the fire service, the call would arrive at the fire service in Munich, which would not only be prohibited, but also dangerous.

The solution to this problem is to assign the access points in Berlin and Frankfurt a connection to the respective local network and to route them on a subscriber-dependent basis.

This “source dependency“ always applies to multiple subscriber lines, CO circuits or tie trunk circuits. In order to identify a group requiring the same routing behavior, the source group ID is introduced. Every access point must be assigned to a source group. If the subscriber line, CO or tie trunk circuits are configured with source group ID “0“ (default value), they adopt the settings of the access point. If necessary, a source group ID which deviates from the access point can be assigned to individual subscriber lines, CO circuits or tie trunk circuits.

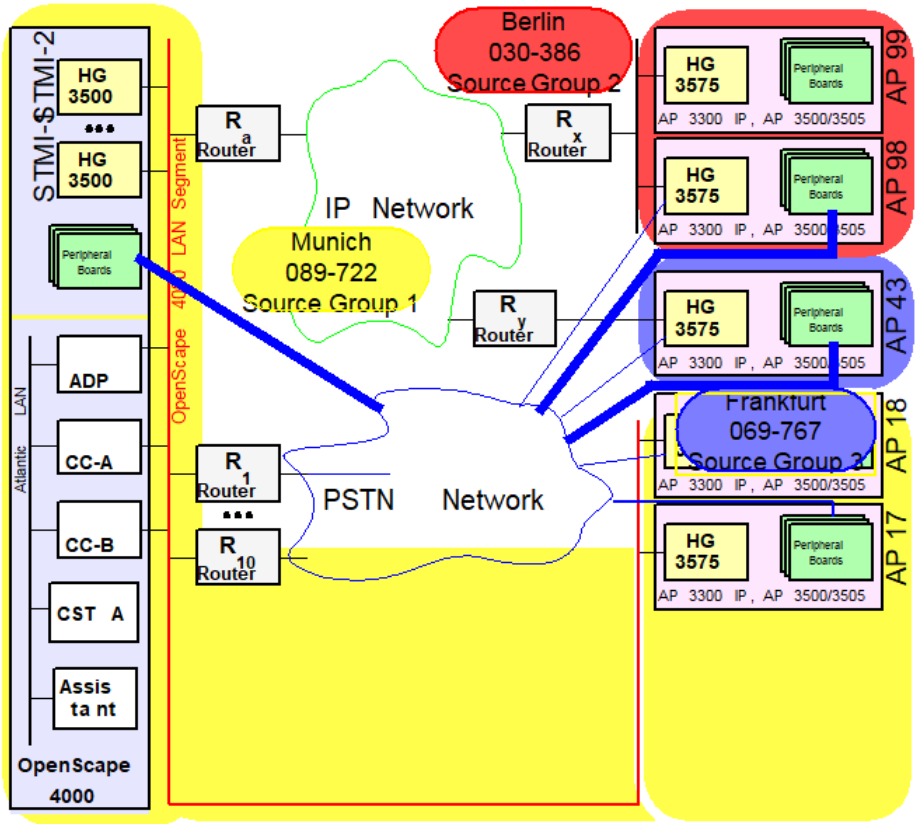


Figure 193: Source-dependent routing

In the example, access points AP 17 and AP 18 in Munich have been assigned to Source Group 1, which is also always the default setting for all LTUs (1..15) of the central OpenScape 4000 system. The two access points in Berlin (AP 98 and AP 99) have been assigned to Source Group 2. The Frankfurt access point AP 43 has Source Group 3.

The number of the source group is specified as the source group index with ADD-UCSU (see parameter SRCGRP in Table 6 “APNW: AMO UCSU parameters in ADD branch under TYPE=AP”).

In order to realize source dependent routing, LCR had to be extended.

While routing numbers (LROUTE) have previously been assigned in the digit pattern plan with the AMO LDPLN for one digit pattern, taking into account DPLN groups, class of service etc., source dependent routing requires that the index of an LCR profile (PROFIDX) be specified instead of the LROUTE. In the LCR profile, an LROUTE can be branched to as a function of the source group index. LCR profiles are configured with the AMO LPROF.

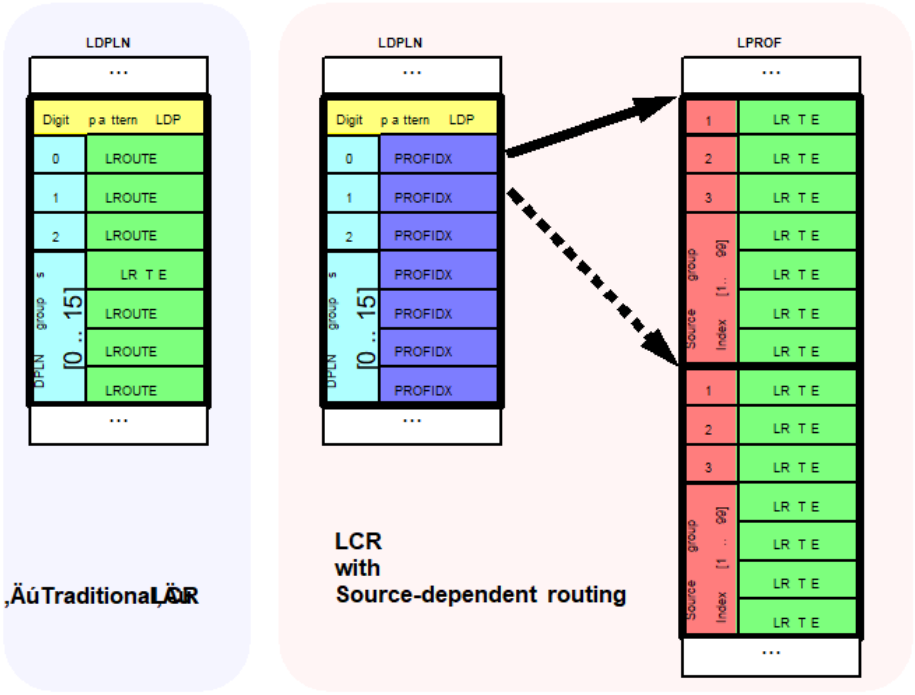
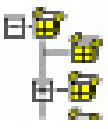


Figure 194: Interaction between LDPLN and LPROF

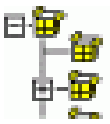
As PROFIDX indicates an LCR profile in the digit pattern plan, this must be configured first.

An LCR profile for emergency calls to the fire service is to be generated. In Munich, LRTE 722 leads to the CO; in Berlin, LRTE 386 and in Frankfurt, LRTE 767.

	**Configuration Management > Least Cost Routing > LCR Profiles** Click **New**, enter the **Profile Name**, **Source Group**, and **LCR Route** and **Save**. The profile index is calculated and returned.

	`ADD-LPROF:PROFNAME=FEUERWEHR,SRCGRP=1,LRTE=722;`
	The AMO returns the profile index, provided it is 12.
	Additional source groups can be supplemented with:
	`CHANGE-LPROF:PROFIDX=12,SRCGRP=2,LRTE=386;`
	`CHANGE-LPROF:PROFIDX=12,SRCGRP=3,LRTE=767;`

Next, an entry can be made in the digit pattern plan for emergency calls to the fire service, indicating the LCR profile number 12 just configured.

	**Configuration Management > Least Cost Routing > Digit Pattern** Click **New**, enter **112** for **Digit Pattern**. On the **Data** tab, enter the **LCR Profile Number** configured above under profile index and SAVE.
	`ADD-LDPLN:LDP=112,PROFIDX=12, ...;`

Additional functions of the AMO LPROF:

	`DELETE-LPROF:PROFIDX=12,SRCGRP=3;`

Deletes the entry for a source group from the specified LCR profile. If no source group is specified, the entire profile is deleted.

	`DISPLAY-` `LPROF:PROFIDX=1&&33,INFOPAT=FEUER,FORMAT=K;`

All parameters are optional. A specific index or range can be specified for **PROFIDX**. **INFOPAT** allows a search pattern to be specified. If the pattern is found in a profile name, the profile is output. **FORMAT** is used to choose between short or long output format.

Notes:

- Every subscriber line, CO circuit or tie trunk circuit is automatically assigned the source group index 0 upon configuration. This means that the LTU source group index is used. However, it can be changed individually. A maximum of 99 source groups are available.
- The source group index used for a subscriber is output when the AMO SDAT is called up. The output `SRCGRP =(1)`means that the subscriber uses the LTU source group index. The subscriber is configured with `SRCGRP=0`. If the subscriber moves in an LTU that is assigned to another source group, it is assigned this source group.

- The output `SRCGRP = 1` means that the subscriber uses the value 1 independent of the LTU source group index. The subscriber is configured with `SRCGRP=1`. The user-specific source group that is set thus remains the same if the subscriber moves to another LTU. Check if this allocation is still useful.

Table 46: AMO LPROF parameters

AMO	Parameter	Sprache/ Language	Beschreibung/ Description
LPROF	FORMAT	d	Abhängig vom Parameter Format werden die Profile in einem gekürzten Format angezeigt (nur die Service Information) oder in einem langen Format (alle für LCR Profile relevanten Informationen) K Ausgabe LCR Profile, Service Information - Kurz L Ausgabe LCR Profile Einträge - Lang.
	FORMAT	e	According to the parameter format, the profiles are displayed in a short format (only the Service Information) or a long format (all LCR profile releated info). S Display LCR Profile, Service information - Short L Display of LCR Profile related info - Long
	INFOMUS	d	Bestimmt das Muster nach dem das Profil angezeigt wird. Wenn das im Parameter INFOMUS angegebene Muster im Profil Namen gefunden wird, wird das folgende Profil angezeigt.
	INFOPAT	e	Specifies the pattern according to which profiles will be displayed.If the pattern given in the INFOPAT parameter is found in the profile name, the following profile is displayed.
	LRTG	d	LCR Richtung
	LRTE	e	LCR route
	PROFIDX	d	LCR Profil-Index
	PROFIDX	e	LCR profile index
	PROFNAME	d	LCR Profilname
	PROFNAME	e	LCR profile name
	SRCGRP	d	Source Group Index
	SRCGRP	e	Source Group Index

10.2.9 Payload Survivability

In principle, the IP distributed architecture is dependent on the availability of the IP network. If the IP connection fails between two access points or between the central OpenScape 4000 switch and an access point, no payload connections are possible via IP.

Also, separation of signaling and payload streams is required very often by customers in the following scenario:

- signaling from branch to HQ should go over the IP Customer Network (WAN)
- payload should go over the traditional PSTN network using ISDN flatrate

The aspect of signaling between the CO and the access point is covered in Section 2.6, “Signaling Survivability”.

If control of the access point is safeguarded through signaling survivability, calls can be made within the access point in all cases. External calls via trunks or tie trunks in other systems are possible if the corresponding connection modules are located in this access point.

Payload survivability uses existing trunks in order to establish payload connections with other access points or with the OpenScape 4000 central system independently of the IP network. In this context, the system calls itself via the trunk.

The procedure followed for payload survivability between a local subscriber and a CO/tie trunk circuit is route-specific.

If the call comes in via the CO/tie trunk circuit, a trunk call is established between the source group into which the call comes and the source group to which the subscriber belongs.

If, on the other hand, the OpenScape 4000 subscriber establishes the call, the call is routed out of the system via the CO using LCR. A CO/tie trunk from the central system cannot be used in this case.

Payload survivability is destination-oriented and is restricted to one OpenScape 4000 system. I. e, hardware gateways NCUI and STMI2/STMI4, and vNCUI (for SoftGate and Enterprise GW) and STMIX/STMIY boards are affected. If other systems are connected to the OpenScape 4000, the networking LCR must be extended. Details can be found in Section 2.9.3, “Payload Survivability in OpenScape 4000 Networks”.

10.2.9.1 When is Payload Survivability Used?

There are the following reasons to handle connections to access points via trunk traffic instead of via IP:

If the quality of the existing connections in the IP network is bad

The capacity of the IP link is exhausted

If a subscriber specifies via access code that he does not wish to use IP

Payload Survivability when signaling survivability is active

If in AMO UCSU parameter BCHLCNT is set to „0“.

If the quality of the existing connections in the IP network is bad

The quality of the active payload connections via the IP network is permanently monitored.

If the packet delay or the packet loss rate exceeds the predefined or upper limits, the connection is labeled as „Bad Quality“. If these variables drop below the likewise predefined lower limits, the connection is relabeled as „Good Quality“. The limit values are set in the **PLQUAL** branch in AMO SIPCO (see Section 2.1, “Payload Quality (PLQUAL)”).

Figure 30 “Blocks the IP connection for payload due to „Bad Quality“” indicates the sequences:

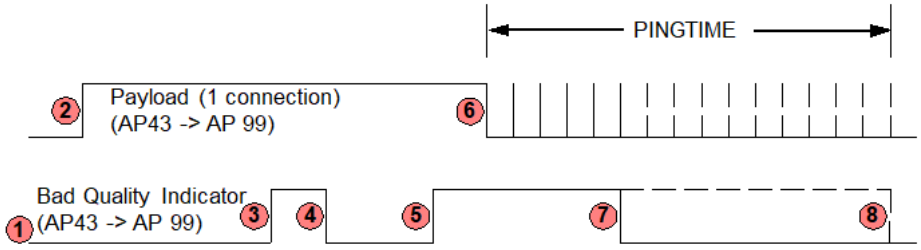


Figure 195: Blocks the IP connection for payload due to „Bad Quality“

	At the start of appraisal, the IP connection quality of AP 43 to AP 99 is labeled as good.
	A payload connection is established via IP.
	The constant monitoring of the connection quality reports “Bad Quality“ From this time on, no further payload connections are established between AP 43 and AP 99 via IP. If available, an alternative route via payload survivability is used. Otherwise, the connection request is rejected. The existing payload connection is not disconnected, despite “Bad Quality“.
	The constant monitoring of the connection quality reports a return to “Good Quality“ The establishment of payload connections between AP 43 and AP 99 over IP resumes from this time on.
	as per 3
	The subscriber terminates the payload connection At this time, the connection is labeled as “Bad Quality“. As a result of the preceding payload connection, “UDP ping“ messages are now transmitted every 5 seconds, in order to further monitor the behavior of the IP connection.

	The test with “UDP ping“ messages shows that the connection quality has been restored. The “Bad Quality indicator“ is reset. From this time on, payload connections are again established between AP 43 and AP 99 via IP.
	If the tests with “UDP ping“ messages are unsuccessful, the “bad quality indicator“ is reset after expiry of **PINGTIME**. **PINGTIME** is configured in the TIMING branch of the AMO SIPCO. The value range is between 0 and 3600 seconds. Important • It is recommended to change the parameter **PINGTIME** in AMO SIPCO from the default value 60 to the maximum value of 3600. • The actual status of the Payload Matrix can be displayed from AMO SIPCO with the command `DIS-SIPCO:PLMATRIX;` • Additionally to help follow the status of the Payload Matrix, the following F5915/F5750 error messages can also be activated by aid of a DIAGS switch `CHA-DIAGS:,NMC,,ON;` • REASON:01H IP GOOD QUALITY REASON:02H IP QUALITY TEST TIMER EXPIRED

If several payload connections are running in parallel between 2 access points or between an access point and HG 3500, these may provide differing quality statements. In all events, the „Bad Quality“ status of a connection is always prioritized over any number of „Good Quality“ connections.

In other words, if 10 connections report „Good Quality“ and 1 reports „Bad Quality“, no further IP connections are established until the connection with the status of „Bad Quality“ has returned to a status of „Good Quality“. For information on possible sequences, see Figure 30 “Blocks the IP connection for payload due to „Bad Quality“”.

All payload routes between the central system (all HG 3500 modules) and an access point are labeled „Bad Quality“ as soon as signaling survivability is activated for the access point. In this case it is assumed that a fault affecting the route between the central system and access point is having the same effect on the payload connections.

If the blocking of the availability of subscriber lines in an access point without payload survivability due to poor IP connections is to be prevented („Bad Quality“), payload quality handling can be deactivated for the access point in the AMO UCSU with the parameter **PLCHECK**. This means that every call is switched regardless of the quality of the IP connection. In the worst case scenario, this can result in the call being signaled, but the voice link remaining dead because no packets with payload are received.

The capacity of the IP link is exhausted

The transport capacity for payload connections between an access point and the IP network is limited by the maximum number of simultaneous connections possible (30/60/120 connections depending on the hardware) and the maximum bandwidth configured in the Resource Manager. If the full transport capacity is used, the payload survivability route is automatically used for further calls within the OpenScape 4000 system. The path selection makes no distinction as

to whether there is no path available because of a failure in the IP network or because all available routes from the access point are already occupied.

Because of the restrictions with regard to payload survivability, the system must be configured so that this spillover route is only used in cases of exceptional overload.

If a subscriber specifies via access code that he does not wish to use IP

In OpenScape 4000 system, the WABE code **FRCALTRT** can be used to force the survivability route. The access code **FRCALTRT** can be used by anyone and is not subject to any class of service requirements. The same payload survivability restrictions apply for these calls.

Payload Survivability when signaling survivability is active

If a OpenScape 4000 SoftGate is in signaling survivability mode, then the connections to all other APs which are in a different source group than the designated OpenScape 4000 SoftGate, will be established over the alternative route.

Connection to all APs which share the same source group with the designated OpenScape 4000 SoftGate will be established over LAN if possible. If this is not possible, then no connection is possible.

As for IPDA traditional shelves, the functionality is controlled by the parameter **NPLMSURV** in AMO Zande > **ALLDATA**. If this parameter is set to **NO** then we have the same functionality as in versions prior to HiPath 4000 V5. This means all payload routes between the host system (all HG 3500 modules) and an access point are labeled as „Bad Quality“ as soon as signaling survivability is activated for the access point. In case of alternative routing (signaling survivability is active) the payload matrix between HHS and the corresponding AP will be blocked. All available routes from HHS to AP are marked as BAD IP.

If **NPLMSURV** is set to **YES** then the traditional IPDA shelves will have an enhanced behavior similar to the OpenScape 4000 SoftGate behavior mentioned above.

I.e. an IPDA shelf in signaling survivability mode will connect to OpenScape 4000 host system. All other APs which are in a different source groups will connect over the alternative route.

On the other hand connection to all APs which share the same source group with the designated OpenScape 4000 SoftGate will be established over LAN if possible, and if not, then no connection is possible.

IMPORTANT: Parameter **NPLMSURV** has no effect on a OpenScape 4000 SoftGate which is in Signaling Survivability mode. OpenScape 4000 SoftGate always follow the enhanced behavior.

IMPORTANT: Parameter **PLMSGSRV** in AMO ZANDE > **ALLDATA** has no effect.

10.2.9.2 How is Payload Survivability Configured?

10.2.9.2.1 Overview

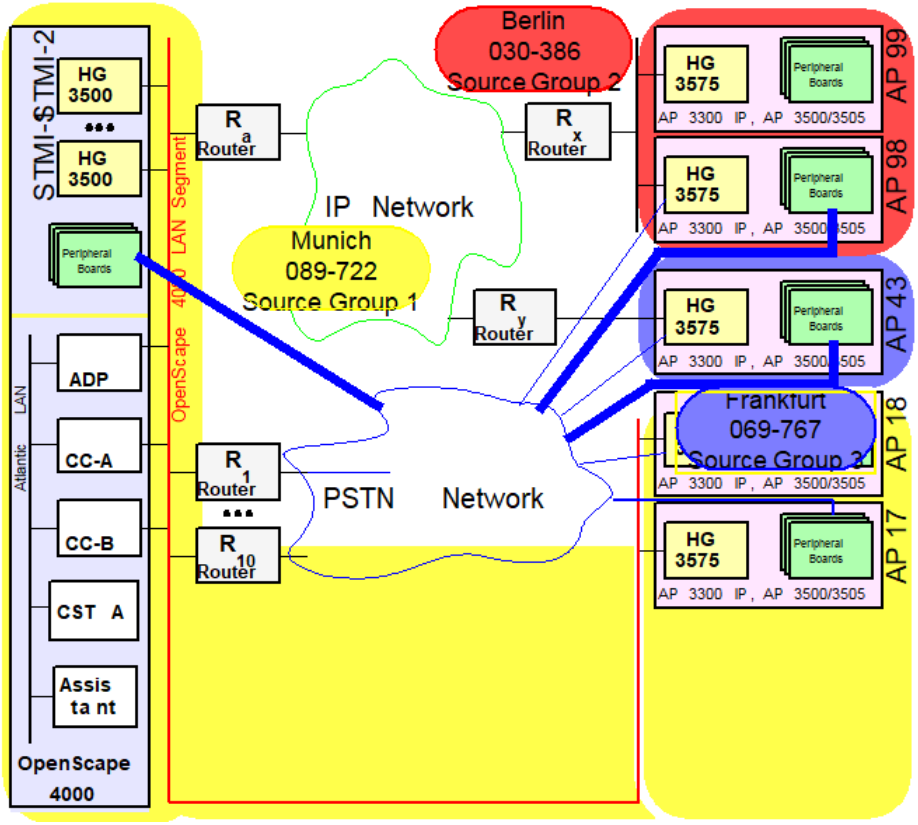


Figure 196: Payload survivability - source dependent routing configuration

Payload survivability requires CO lines at access points, in order to switch alternative routes. If, in example Figure 31 “Payload survivability - source dependent routing configuration”, the IP connection between Berlin and Frankfurt fails, all existing calls will be interrupted. No new calls can be set up until “Good Quality“ has been determined again.

As both an access point in Berlin and the access point in Frankfurt have a local CO line, calls between subscribers in Berlin and Frankfurt can alternatively be switched via the trunk. Of particular note here is that, in the case of IPDA, a OpenScape 4000 system now calls itself via trunk, in order to connect its own subscribers.

The alternative routes are defined as a function of the source group. Thus, in the example, it is unnecessary for AP 99 to have its own trunk access. It can be reached via the trunk access of its source group in AP 98.

10.2.9.2.2 Variants of Payload Survivability

There are 3 variants of payload survivability, which depend on the type of trunk switching and have different advantages and disadvantages. ALR should be used as standard.

ALR with single number	Functions with any kind of trunk switching, even analog. • A separate phone number must be assigned to each channel of the trunk switching • Therefore requires many individual phone numbers and many entries in the **ALTROUT** table • When the payload survivability route is used, party A sees the “Alternate Routing Number“ used for the call in addition to the dialed internal number • When the payload survivability route is used, party B hears the “external call ring“ despite the fact that it is an internal call, but sees the internal phone number of party A.
ALR via multichannel trunk	Only functions with multichannel ISDN CO lines. • Only one phone number for all of the channels of a circuit • Only one entry per circuit in the **ALTROUT** table • Use of the “Artificial Calling Number“ requires agreement with the PSTN network carrier that the transmitted calling party number will not be checked, as it does not correspond to the actual phone number for the circuit (USER PROVIDED SCREENED). The same must be agreed for all source groups. The source group for which ALR is configured with **ARTCNR** must be available in this way from all other source groups. • The entire carrier network must guarantee transmission of the Artificial Calling Number from all source groups without corruption. (No modification of the phone number) • Call charges for using the payload survivability route cannot be uniquely assigned to the calling party • When the payload survivability route is used, party A sees the “Alternate Routing Number“ used for the call in addition to the dialed internal number • When the payload survivability route is used, party B hears the “external call ring“ despite the fact that it is an internal call, but sees the internal phone number of party A.
PUBDID	If **PUBDID** numbers are already configured for subscribers of an access point, these can also be used for payload survivability. • Relatively high level of administration effort involved, as the **PUBDID** number has to be configured individually for each subscriber. • 1 entry in the **ALTROUT** table for the entire source group • The **PUBDID** number is retained in the event of a relocation • In the case of payload survivability, the **PUBDID** number is displayed for the other party • Call charges for using the payload survivability route can be uniquely assigned to the calling party

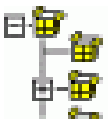
ALR with single number

At the CO line which is (also) to be used for the payload survivability of a source group, certain call numbers are configured for payload survivability.

Let us assume that the numbers 069-767-97, 069-767-98 and 069-767-99 have been reserved in Frankfurt for payload survivability. Up to 3 calls can then reach source group 3 simultaneously via alternative routes.

The INCALTRT digit analysis result must be configured in WABE for every access code.

This is configured through

	**Configuration Management > System Data > IPDA > IPDA Payload Survivability** Click **New**, enter **Index**, **Routing Position**, **Phone Number** and **Access Code** on the **Basic Data** tab and **Save**. **Configuration Management > Tables > Dial Plan > Dial Codes** Click **New**, select **Delete Mask** on the **Edit** pull-down menu. Enter the **Dial Code** and **Code Type** and **Save**.

	`ADD-APRT:TYPE=ALTROUT,SRCGRP=3,POS=1,ALRTYPE=ALR, ALTRTNR=006976797,ACCODE=97; ADD-WABE:CD=97,DAR=INCALTRT;`
	`ADD-APRT:TYPE=ALTROUT,SRCGRP=3,POS=2,ALRTYPE=ALR, ALTRTNR=006976798,ACCODE=98; ADD-WABE:CD=98,DAR=INCALTRT;`
	`ADD-APRT:TYPE=ALTROUT,SRCGRP=3,POS=3,ALRTYPE=ALR, ALTRTNR=006976799,ACCODE=99; ADD-WABE:CD=99,DAR=INCALTRT;`
	This insertion sequence means that ACCODE 97 is at the top of the list and is occupied first.

Note regarding ALTRTNR

Specific rules must be observed for the Alternate Routing Number **ALTRTNR**:

- **ALTRTNR** must contain the access code for CO breakout.
- If the source groups are distributed across different local networks, the local network access codes must also be specified (see example).
- The access code setting for CO breakout must be identical in all source groups. The destination number must be accessible in the same way from all other source groups.
- **ALTRTNR** cannot be modified throughout the entire network with LCR (no REROUTE-INTERN).
- **ALTRTNR** must be routed in each source group on a “source-dependent“ basis.

Note regarding AMO parameter POS (AMO APRT:ALTROUT)

The AMO parameter POS is optional. If this parameter is not specified, the entry is inserted at the end. The table is always kept compact starting at POS=1. If a specific POS value is specified, the table entry is only entered at this position if this position is already occupied or if it is the first free position. If this position is

not free, the entries following POS are shifted back. If this position is not free, the entries following POS are shifted back. If an entry is deleted, all subsequent entries are shifted forwarded by one position. POS is important when multiple entries are made for a source group. Assignment of the specified alternative routes is in ascending order according to the POS value.

ALR via multichannel trunk circuit under one call number

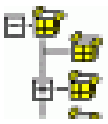
At the CO line, 30 channels are available, for example, to a source group for payload survivability, all of which can be reached via the same call number. In Munich, for example, this could be the number 089-722-9000.

The INCALTRT digit analysis result must be configured in WABE for the access code 9000.

Furthermore, up to 30 calls, for example, can reach source group 1 simultaneously via alternative routes. However, as all calls are routed to the same call number (ACCODE, AMO APRT:ALTROUT), the call processing is faced with the problem of correctly assigning the alternative route calls. To this end, an identification number has to be transmitted with each call. This is realized by replacing the Calling Party Number. Precisely which numbers will be available to this end is configured via the parameters ARTCNR (Artificial Calling Number) and ARTCNRG (Artificial Calling Number Range).

The Artificial Calling Number is configured on a target-dependent basis with the information on a specific source group. However, this number is used at the source, i.e. at the trunk access which leads into the alternative route. The value is ultimately used as the Calling Party Number. As carriers do not allow freely selectable Calling Party Numbers, an agreement must be made with the carrier concerning the use of the Artificial Calling Numbers). The carrier must deactivate checking of the Calling Party Number (CLIPNOSCREEN).

Configuration example:

	**Configuration Management > System Data > IPDA > IPDA Payload Survivability** Click **New**, fill in all fields for alternative routing on the **Basic Data** tab and **Save**. **Configuration Management > Tables > Dial Plan > Dial Codes** Click **New**, select **Delete Mask** on the **Edit** pull-down menu. Enter the **Dial Code** and **Code Type** and **Save**.
	`ADD-APRT:TYPE=ALTROUT,SRCGRP=1,ALRTYPE=ALR, ALTRTNR=00897229000,ACCODE=9000,ARTCNR=1000, ARTCNRNG=30;` `ADD-WABE:CD=9000,DAR=INCALTRT;`

Note regarding ARTCNR

Specific rules must be observed for the Artificial Calling Number ARTCNR:

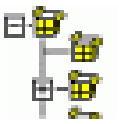
- The ARTCNR ranges for different circuits and source groups must not overlap.
- The ranges must be big enough to allow the desired maximum number of calls via the payload survivability route on a circuit.
- This ARTCNR range must **NOT** be reserved in WABE.

- The entire carrier network must guarantee transmission of the ARTCNR range from all source groups without corruption. (No modification of the phone number)

PUBDID

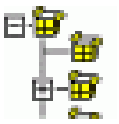
Subscribers of a source group have a Public DID number in the local CO. In other words, Berlin-based subscribers can be reached directly both via the central OpenScape 4000 switch's Munich dial-in and via their Berlin dial-in number. For example: a subscriber could be reached not only via 089-722-**12345**, but also via 030-386-**789** (different extension numbers/branch concept.

Setting the PUBDID number: *[TON: Type Of Number - NPI: Numbering Plan Identifier]*

	**Configuration Management > Station > Station** Click **Search** and go to subscriber. Enter the **Sation No.**, **Numbering Plan Identifier** and **Type of Number (TON)** on the **Basic 3** tab under **Primary Rate Interface** and **Save**.
	CHANGE- SDAT:STNO=12345,TYPE=DATA1,PUBNUM=30386789, TON=NATIONAL,NPI=ISDN;

Other settings made using the AMOs DNIT and DIDCR are required.

If this mechanism for payload survivability is to be used, it is activated as follows:

	**Configuration Management > System Data > IPDA > IPDA Payload Survivability** Click **New**, enter the **Position** and **Type Of Routing** on the **Basic Data** tab and **Save**.
	ADD- APRT:TYPE=ALTROUT,SRCGRP=2,POS=1,ALRTYPE=PUBDID;

However, it is also possible to configure one of the ALR procedures for payload survivability for source groups.

Table 47: AMO APRT parameters in ADD branch under TYPE=ALTROUT

AMO	Parameter	Sprache/ Language	Beschreibung/ Description
APRT	SRCGRP	d	Source Group Index Zuordnung des Access Points in eine Source Group. Die Access Points einer Source Group sind für Payload Survivability über einen bestimmten Amtsanschluss erreichbar.

AMO	Parameter	Sprache/ Language	Beschreibung/ Description
	SRCGRP	e	Source Group Index Assignment of the Access Point to a Source Group. The Access Points of one Source Group are reachable via a distinct CO trunk for Payload Survivability.
	POS	d	Position Index des Eintrags in der Alternate Routing Tabelle. [1 .. 500] Siehe auch: Section 2.9.2.2, **“Note regarding AMO parameter POS (AMO APRT:A**
	POS	e	Position Index of the entry in the Alternate Routing Table. [1 .. 500] See also: Section 2.9.2.2, **“Note regarding AMO parameter POS (AMO APRT:A**
	ALRTYP	d	Alternate Routing Typ des Eintrags. 3 Typen sind möglich: ALR: Alternate Routing über eine DID, DIT oder PRI Nummer. NOALR: Kein Alternate Routing Pfad PUBDID: Alternate Routing über Public DID Nummer, d.h. Teilnehmer haben eine zweite Nummer, unter der sie über den Amtsanschluss für die angegebene Source Group aus dem öffentlichen Netz erreichbar sind.
	ALRTYPE	e	Alternate Routing Type of the Entry 3 types are possible: ALR: Alternate Routing via a DID, DIT or PRI number. NOALR: No Alternate Routing PUBDID: Alternate Routing using a public DID number. Subscribers are reachable by a second number via the CO access for the specified Source Group.
	ALTRTNR	d	Rufnummer für Alternate Routing Vollständige Rufnummer des Alternate Routing Anschlusses Siehe auch: Section 2.9.2.2, “Note regarding ALTRTNR”

AMO	Parameter	Sprache/ Language	Beschreibung/ Description
	ALTRTNR	e	Alternate Routing Number. Complete number of the Alternate Routing access See also: Section 2.9.2.2, “Note regarding ALTRTNR”
	ACCODE	d	Access Code Nebenstellennummer des Alternate Routing Anschlusses, d.h. ALTRTNR ohne Vorwahl und Amtsnummer. Maximal 6-stellig.
	ACCODE	e	Access Code Extension Number of the ALternate Routing Access. ALTRTNR without Area and Office Code. Maximum 6 digits.
	ARTCNR	d	Artificial Calling Number Maximal 6-stellige Nummer, welche zur Identifikation des Rufes als “Nummer des Rufenden” übertragen wird. Diese Nummer ist die erste eines Bereichs (siehe ARTCNRNG), der für diese Zwecke genutzt wird. Siehe auch: Section 2.9.2.2, “Note regarding ARTCNR”
	ARTCNR	e	Artificial Calling Number. A number with a maximum of 6 digits. Is given als “Calling Party Number” to identify the call. This number is the first of a range (see ARTCNRNG) used for that purpose. See also: Section 2.9.2.2, “Note regarding ARTCNR”
	ARTCNRNG	d	Artificial Calling Number Bereich Gibt an, wieviele Artificial Calling Numbers einschließlich ARTCNR zur Verfügung stehen [1 .. 99999].
	ARTCNRNG	e	Artificial Calling Number Range Specifies, how many Artificial Calling Numbers including ARTCNR are available [1 .. 99999].

10.2.9.3 Payload Survivability in OpenScape 4000 Networks

Payload survivability is destination-oriented and is restricted to **one** OpenScape 4000 system. If other systems are connected to the OpenScape 4000 via ECMAV2 trunks (closed numbering), the networking LCR (NWLCR) must be extended. Otherwise, AP subscribers cannot access the relevant network subscribers when payload survivability is active.

The procedure followed for payload survivability between a local subscriber and a CO/tie trunk circuit is route-specific.

If the call comes in via the CO/tie trunk circuit, a trunk call is established between the source group into which the call comes and the source group to which the subscriber belongs.

If, on the other hand, the OpenScape 4000 subscriber establishes the call, the call is routed out of the system via the CO using LCR. A tie trunk from the central system cannot be used in this case.

Figure 32 “Payload survivability and networking - normal route A calls B or B calls A”, Figure 33 “Payload survivability and networking - survivability route A calls B” and Figure 34 “Payload survivability and networking - survivability route B calls A” show the different routes.

To handle call A -> B with payload survivability (Figure 33 “Payload survivability and networking - survivability route A calls B”), an extension must be added to the NWLCR of system 1 for the route to DESTNO 2. This extension contains an overflow entry to the local CO of AP 17 (trunk group 17), which ensures that routing to destination system 2 takes place via CO in the case of payload survivability.

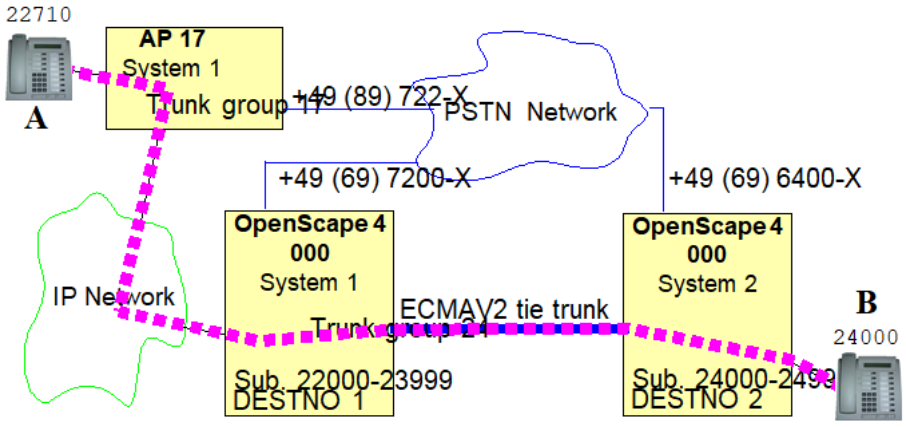


Figure 197: Payload survivability and networking - normal route A calls B or B calls A

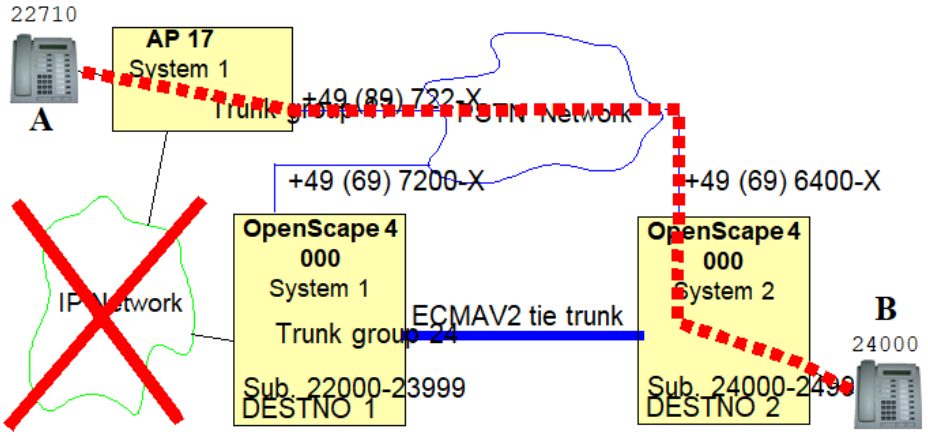


Figure 198: Payload survivability and networking - survivability route A calls B

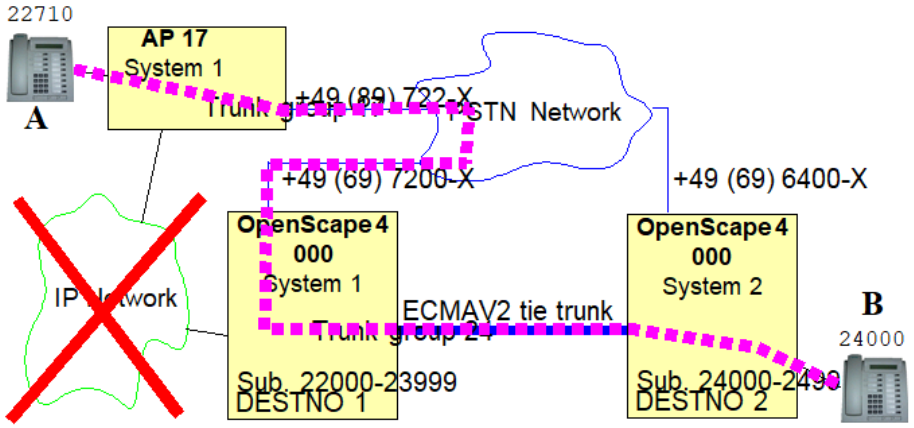


Figure 199: Payload survivability and networking - survivability route B calls A

NWLCR extension for AP 17 to system 2 with payload survivability (Figure 33 “Payload survivability and networking - survivability route A calls B”**)**

```
+-------------------------------------------------------------------------+
| LRTE = 124              NAME = SYSTEM 2                  SERVICE = ALL  |
| TYPE = NWLCR                                  DIDNO-ROUTE = 1 -2 -400   |
| SERVICE INFO =                                                          |
+-------+-----+-----+-----+------+----------+------------+----------+------+
|       |     |     |     |      | SCHEDULE | CARRIER    |          |      |
|LRTGEL |LVAL |TRUNO|  LWR| LBER | ABCDEFGH |       ZONE |    LATTR | LDSRT|
+-------+-----+-----+-----+------+----------+------------+----------+------+
|     1 |    1|   24|    1|    1 | ******** | 1     EMPTY |    NONE  |      |
|    2  |  1| 17| 17|   17|      |******** | 1     EMPTY |    NONE  |      |
+-------+-----+-----+-----+------+----------+------------+----------+------+
+-----------------------------------------------------+
| LWR      LWRELPOS  LWREL       PARAMETER            |
+--------+--------------------------------------------+
|   1    |      1    ECHO    1                        |
|        |      2    END                              |
+--------+--------------------------------------------+
```

```
|INFO:STANDARD NWLCR FOR SYSTEM 2                          |
+----------------------------------------------------------+
+----------------------------------------------------------+
| LWR      LWRELPOS  LWREL       PARAMETER                 |
+--------+----------------------------------------------+
|   17   |      1    OUTPULSE    696400                    |
|   2    |      1    ECHO    1                             |
|        |      3    NPI         ISDN                      |
|        |      4    TON         NATIONAL                  |
|        |      5    END                                   |
+--------+----------------------------------------------+
|INFO:OVERFLOW CO FOR SYSTEM 2 (SURVIVABILITY)             |
+--------+----------------------------------------------+
```

10.2.9.4 Restrictions

Display problems on VNR systems when Payload Survivability is activated

Please note that in case of a VNR system, for calls that have to be sent over the payload survivability route, the displayed called numbers will change to the numbers used for the external routing via the public network.

10.2.10 Signaling and Payload Separation (SPS)

IMPORTANT: Signaling and Payload Separation (SPS) is released for standalone systems only! In networked environment a project specific release (PSR) is required and only basic call is possible!

Signaling and payload separation is a feature which enables OpenScape 4000 in an IPDA environment to split the path of the network traffic in the meaning of

1) signaling from Hostsystem (call control) to access point is routed over the IP Customer Network (Enterprise WAN)

- payload is routed over the PSTN Network using payload survivability connections (e.g. calls from host system to an access point is automatically routed via CO).

IMPORTANT: SPS connectivity and features are only supported for IP Access Points and host shelves (LTUs) that are controlled by the central communication server (host system). If an IP Access Point goes in AP Emergency survivability mode, then SPS connectivity and features are no longer possible/supported. For IP Access Points in AP Emergency mode all calls to other IP Access Points and host shelves will be routed over PSTN based on the

AP Emergency LCR routing configuration with basic call functionality.

Signaling and payload separation based on existing survivability solution and therefore the signaling path is routed in the same way as today.

Signaling and payload separation can be configured in a way that

- payload separation is always active (static signaling and payload separation)
- payload separation is used in case of limited WAN- bandwidth managed by the resource manager or overflow scenarios when then maximum of bandwidth is reached (payload overflow)
- payload separation is used in case of network failure (emergency routing)
- If a subscriber specifies via access code that he does not wish to use IP. In this case payload separation with all access points configured in different source groups can be used

In this situation all access points have to be assigned in different source groups and CO access will be mandatory for all access points.

All calls between access points and between access points and host system will be made over ISDN lines.

10.2.10.1 General Restrictions and Limitations

- SPS trunk groups must be configured for payload separation without intercept parameters.
- Transfer busy is not possible over SPS.
- Route optimization is not possible.
- Direct tie trunk access if the trunk is located in a different shelf is not possible. Workaround: Use AMO TWABE or activate the Block Dial feature.
- Attendant scenarios are not supported.
- Only ComAssistant basic scenarios are supported. Other applications using ACL (through CAP/CA4000) are not supported.
- Payload survivability ALR with single number and PUBDID are not supported.
- Virtual Numbering (VNR) is not supported.
- US specific scenarios are not supported.
- Direct station selection (DSS)
- Override/Intercept
- Camp on
- Only local announcements are supported; announcements are not routed via ISDN (due to CO resource usage).
- MLPP is not suported - MLPP calls over payload separation are not possible.
- Chese - Secretary and Executive must be located on the same branch.
- Broadcast, Speaker Call - One-Way - All party's must be located on the same branch.
- ACD agents must be located on the same branch.
- PARK - Must not be used on different branches
- SIP Phones are not supported.
- Hunt group Master which is also a UC member cannot be reached via ALR path.

- ISDN, ANATE - only basic call is supported.
- UC and UnifyPhone applications not supported with SPS

10.2.10.2 Effects on Features with SPS

- Basic call
  - Direct calls from one shelf to another will be routed through central office (e.g. calls from the host system to an access point will be automatically routed via the CO).
  - Name and number display: Incoming and outgoing calls - When the payload survivability route is used:
    - The calling party will see for basic call the called number and name on the first line.
    - The called party will see for basic call the calling number and name on the first display line.
  - When the payload survivability route is used, called party hears the "external call ring" despite the fact that it is an internal call.
  - If CO connection will breakdown during a call between different shelfs, the call will have no payload and will be disconnected after 90s.
  - The name is not shown on TIE calls.

IMPORTANT: Signaling and Payload Separation (SPS) is released for standalone systems only! In networked environment a project specific release (PSR) is required and only basic call is possible!

- Hunt Group
  - Parallel hunt group is not supported.
  - Hunt group specific functionality is covered - linear/cyclic, master/pilot, activate/deactivate hunt, overflow.
  - Hunt group members must be located on the same branch.
  - Hunting group stations are reached over LAN if calling party and hunt group member are in the same shelf. In case that calling party and hunt

group member are in a different shelf hunting group station is reached over Central Office.

– Charging:

The calling party will be charged if a hunting group station that is located on a different shelf will answer. For external (CO) calls the paying party is a default virtual route code destination and the destination is the ALR number.

– Incoming calls to hunt group - When the payload survivability route is used:
  – The calling party will see the name and number of the hunting group on the first line and the alerting hunt group member number and name on second the line.
  – The connected party will see the hunt group member number and name on the first line.
  – The alerting hunt group member will seethe calling number and name on the first display line and the name and number of the hunting group on the second line of the display.
  – The connected hunt group member will see the connected number and name on the first display line.

Overflow scenario:

– The calling party will see the name and number of the hunting group on the first line and the last alerting hunt group member name and number on the second line.
– The connected party will see the hunt group member number and name on the first line.
– Forwarding for hunt group members is not supported (**LVAFTEXT =N**)*
– Announcement with hunting group call queue is not supported due CO resource limitations.
– Execute call forwarding from hunt group parameter **EXECCFW** will be ignored if the calling party and hunting group station with activated call forward are located on different shelves.

• Call Pick Up
  – Pick up specific functionality is covered (display of the calling user (**DISTNO**), delayed notification ring (**NOTRNG**).
  – Call pick up members must be located on the same branch.
  – A station/user can pick up calls which belong to the pickup group.

  For call scenarios where the calling party is located on a different shelf than the called and picking party the CO route will be used. The calling party will be charged.

  For external (CO) calls the paying party is a default virtual route code destination and the destination is the ALR number.

  – Display The picking party will see on the display the name and number of the calling partner.
  – When the payload survivability route is used, the called party hears the "external call ring" despite the fact that it is an internal call.
  – Directed call pickup is not supported.
  – Networkwide call pickup groups are not supported.
• Call Back

- A station user can set a call back request to a party located on a different shelf.
  - Callback busy/no answer/free/mailbox is possible for calls between different branches over CO.
  - When callback is initiated (called party become free), calling party hears the "internal call ring" despite the fact that it is an internal call.
  - When callback is executed, called party hears the "external call ring" despite the fact that it is an internal call.
  - Callback from/to network partner is not possible - "Callback" menu will not be offered
- Call Forwarding
- The user can forward calls to a party located on a different shelf.
  - Call forwarding busy/no answer is possible in the same system. To stations located on different branches the call will be routed over CO.
  - Call forwarding to Xpressions is possible independent of shelf location when a TIE trunk to Xpressions is configured.
  - For Call forward scenarios no CO resources will be used if the calling party and forward destination station are located on the same shelf.
  - Charging

  The calling party will be charged if the forward destination is located on a different branch.

  - Display

  Forward Unconditional/Busy - The forward destination is located on a different branch than the calling party

  1) The calling party will see the called name and number on the first line display.

  - Diverted-to party will see the calling party name and number on the first line.

  Forward no reply - If forward destination is located on a different branch than the calling party:

  - The calling party will see the called name and number on the first line display and diverted-to party name and number on the second line display.
  - Diverted-to party will see the calling party name and number on the first line.

  - Call forwarding indication at diverted-to party is not shown on the display.

- Transfer and Toggle
  - The user can transfer calls to a party located on a different shelf.

  Transfer of incoming and outgoing external calls is possible to stations located on a different shelf. In this case the call will be routed over CO.

  - Display

  The calling party will see after transfer the called party name and number and the transfered to party will see the calling party name and number on the first line display.

  - Ring

  If the calling party and transferring party are located on different shelves the transferred party hears the "external call ring" independent of the location of the transferred party (local, network).
- Conference
  - The user can initiate a conference or be a conference member.
  - Display

  If all members of a conference are located on the same branch as the conference master the display will show the correct information.

  - The members of a conference which are located in another branch as the conference master will see on the display only one connection to the conference master.
  - ALR route name will be shown instead of party name for members of a conference which are located in another branch as the conference master.
- Keyset
  - All Keysets can be reached via the main station number and can initiate calls using primary line.
  - Primary, Secondary and phantom line must be located in the same source group.
- Name and number display
- One Number Service (ONS)
  - An ONS member can pick up calls which belong to the ONS group.
  - ONS group members must be located on the same branch.
  - For call scenarios where the calling party, ONS master and picking party are on the same shelf no CO route will be used.
  - For call scenarios where the calling party is located on a different shelf than the ONS master and ONS slave the CO route will be used. the calling party will be charged.
  - Tones
    - The RING TYPE applied to ONS members is the same as the one of the ONS master.
    - When the payload survivability route is used, the called party hears the "external call ring" despite the fact that it is an internal call.
- Fax-Modem
- Call Waiting
- Call Log
- OpenScape Xpressions basic scenarios
- ComAssistant basic scenarios

10.2.10.3 Configuration

General activation of the SPS feature:

CHANGE-ZANDE:TYPE=ALLDATA,SPS=YES;

For more information on the configuration please refer to Section 2.9.2, “How is Payload Survivability Configured?”.

Configuration Example

- Describe how source group (1) is reached with alternate routing table

ADD-
APRT:TYPE=ALTROUT,SRCGRP=1,ALRTYPE=ALR,ALTRTNR=00897229000,
ACCODE=9000,ARTCNR=1000,ARTCNRNG=30;

- Describe how source group (19) is reached with alternate routing table

ADD-
APRT:TYPE=ALTROUT,SRCGRP=19,ALRTYPE=ALR,ALTRTNR=00897229000,
ACCODE=9000,ARTCNR=1000,ARTCNRNG=30;

- Define code for incoming alternate route

ADD-WABE:CD=9000,DAR=INCALTRT;

- Source group needs to be configured in AMO TDCSU for all involved trunks

CHANGE-TDCSU:PEN=x-x-x-x,SRCGRP=1;

CHANGE-TDCSU:PEN=x-x-x-x,SRCGRP=19;

- AMO TWABE will be used for direct call to Xpression access numbers

ADD-TWABE:STNO=64,LEN=5;

1) ..where 64 (TIE code to XPR, max. 3), 5 is total length of the number (TIE code + length of the direct access number)

It should be noted that TWABE has no DPLN groups. The usage of block dial feature might be used as alternative solution to AMO TWABE.

- Configuring code for force alternate route

ADD-WABE:xxx,,,FRCALTRT,N,,,,,,,,;

- Configuring station autorization
- Stn COSSU must have autorization TTT (Transfer Trunk to Trunk) to allow transfer over SPS

  CHANGE-COSSU:TYPE=COS,COS=xx,AVCE=TTT;

IMPORTANT: The carrier must deactivate checking of the Calling Party Number (**CLIPNOSCREEN**).

10.2.11 Divert Call in Survivability Mode to another Access Point

When Single StepTransfer is invoked for a DIGITE or an ANATE in talk state and no path is available between source and destination, then the alternate path for payload survivability is used if properly configured.

10.2.11.1 Prerequisites

- Each access point needs access to the PSTN over CO trunk and corresponding alternate routes and numbers must be configured.
- Payload survivability or signaling and payload separation (see Section 2.10, “Signaling and Payload Separation (SPS)”) must be configured.
- OpenScape Contact Center (OSCC) at least V8.

10.2.11.2 User Scenarios

Scenario 1

Call arrives on a trunk at IPDA in **Location B** (labeled #1 in the figure below). OpenSape Contact Center requests that the call routes to an agent extension which is located on the IPDA at **Location C**, which routes via PSTN due to payload survivability (labeled #2 and #3).

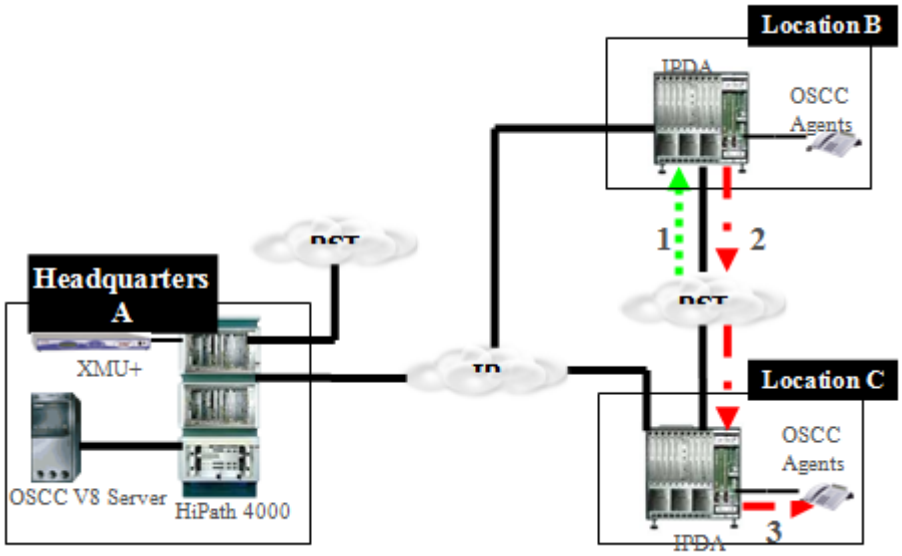


Figure 200: Divert call in survivability mode - User scenario 1

Scenario 2

Call arrives on a trunk at the IPDA in **Location B** (labeled #1 in the figure below). The call routes to the main OpenScape 4000 in **Headquarters A** via PSTN due to payload survivability to play a Call Director message (labeled #2 and #3). This call may be subsequently routed to an agent extension at the IPDA in **Location C** either via payload survivability or over the WAN (labeled #4 and #5).

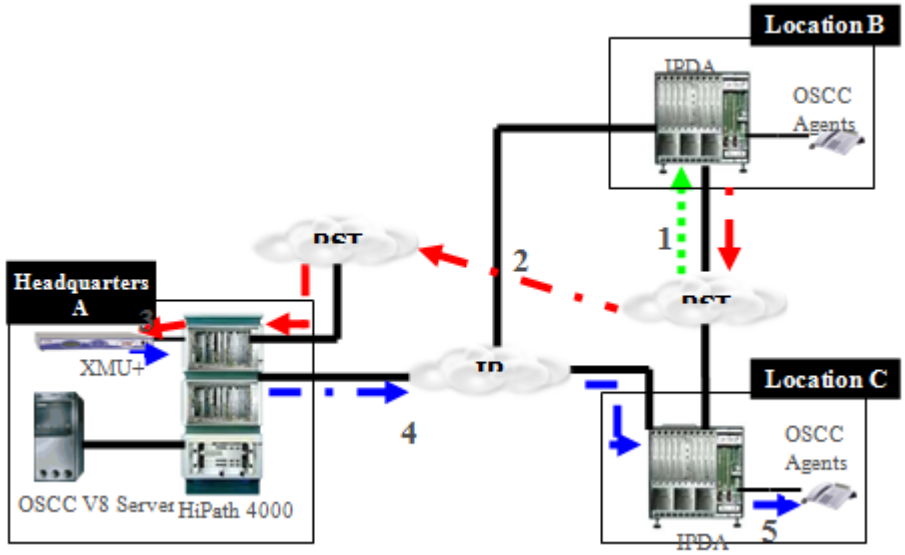


Figure 201: Divert call in survivability mode - User scenario 2

Scenario 3

Call arrives at the IPDA in **Location B** and routes to an agent extension (labeled #1). This agent then consults, conferences, or transfers with an agent on the IPDA in **Location C** (labeled #2), which routes via PSTN due to payload survivability.

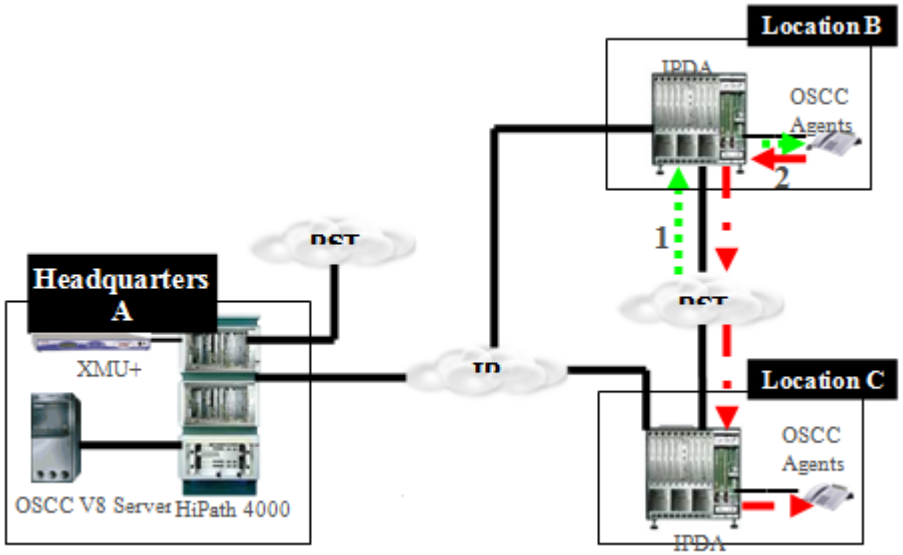


Figure 202: Divert call in survivability mode - User scenario 3

Scenario 4

Call arrives on a trunk at the main OpenScape 4000 at **Headquarters A** (labeled #1), and is routed to an agent extension on an IPDA at **Location C** (labeled #2 and #3) via PSTN due to payload survivability.

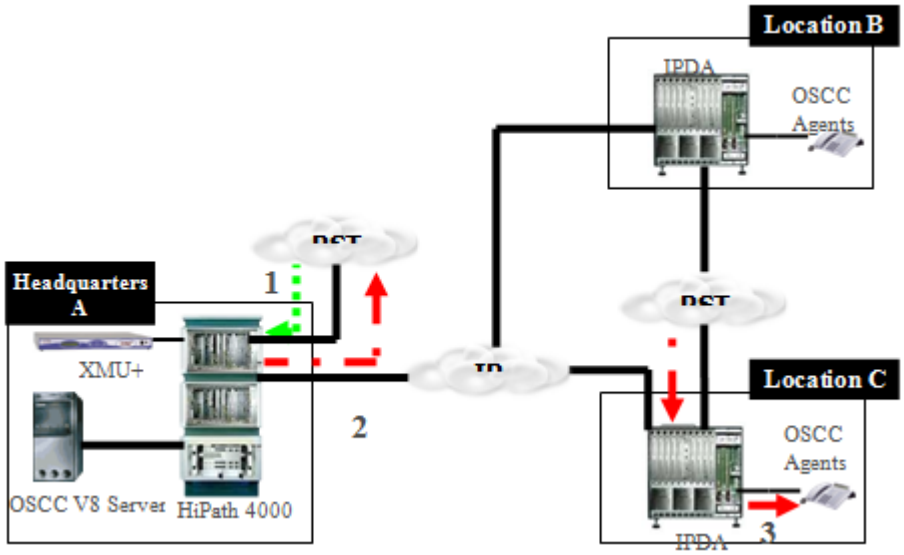


Figure 203: Divert call in survivability mode - User scenario 4

10.2.11.3 Use Cases

1) Basic call

- ACD incoming call on AP x is routed directly to an agent on AP y.

Details:

a) incoming call using CO trunk located on AP x

- call enters ACD queue
- agent available and OpenScape Contact Center routes the call to agent on AP y using CSTA_DEFLECT_CALL_REQUEST

- ACD incoming call on OpenScape 4000 host system is routed directly to an agent on AP x.

Details:

a) incoming call using CO trunk located on OpenScape 4000 host system

- call enters ACD queue
- agent available and OpenScape Contact Center routes the call to agent on AP x using CSTA_DEFLECT_CALL_REQUEST

- ACD incoming call on AP x is routed directly to an agent on OpenScape 4000 host system.

Details:

a) incoming call using CO trunk located on AP x

- call enters ACD queue
- agent available and OpenScape Contact Center routes the call to agent on OpenScape 4000 host system using CSTA_DEFLECT_CALL_REQUEST

2) Scenarios with XMU (AMO RCSU) ports

- ACD incoming call on AP x is routed to XMU (OpenScape 4000 host system) and then redirected to an agent at AP x.

Details:

a) incoming call using CO trunk located on AP x.

- call enters ACD queue and is connected to ACD music/announcement port (check Note 2)
- agent available and OpenScape Contact Center routes the call to agent on AP x using CSTA_DEFLECT_CALL_REQUEST

- ACD incoming call on AP x is routed to XMU (OpenScape 4000 host system) and then redirected to an agent at AP y.

Details:

a) incoming call using CO trunk located on AP x

- call enters ACD queue and is connected to ACD music/announcement port (check Note 2)
- agent available and OpenScape Contact Center routes the call to agent on AP y using CSTA_DEFLECT_CALL_REQUEST

- ACD incoming call on AP x is routed to XMU (OpenScape 4000 host system) and then redirected to an agent at OpenScape 4000 host system

Details:

a) incoming call using CO trunk located on AP x

- call enters ACD queue and is connected to ACD music/announcement port (check Note 2)
- agent available and OpenScape Contact Center routes the call to agent on OpenScape 4000 host system using CSTA_DEFLECT_CALL_REQUEST

- ACD incoming call on OpenScape 4000 host system is routed to XMU (OpenScape 4000 host system) and then redirected to an agent at AP x

Details:

a) incoming call using CO trunk located on OpenScape 4000 host system

- call enters ACD queue and is connected to ACD music/announcement port (check Note 2)
- agent available and OpenScape Contact Center routes the call to agent on AP x using CSTA_DEFLECT_CALL_REQUEST

NOTICE: In case that no agent becomes available during announcement, the ACD call is routed back to RCG/DNIT via CSTA_DEFLECT_CALL_REQUEST and then a new agent search begins. I.e. use case 2 works for 2 cases: a. an agent gets available during announcement b. no agent gets available during announcement and a new search begins.

NOTICE: If ACD music/announcements (XMU configured as RCSU ports) are used, ACD only switches paths, connecting caller TSL with XMU TSL.

If no payload possible, there is no mechanism to use alternate path to listen to these ports. The call is still in ACD queue and can be routed anytime to any agent using CSTA_DEFLECT_CALL_REQUEST as described in Note 1 above. As alternative to RCSU ports, Call Directors can be used (see use case **Scenarios with Call Director (AMO SCSU) ports (analog device)**).

3) Scenarios with Call Director (AMO SCSU) ports (analog device)

- ACD incoming call on AP x is routed to Call Director (OpenScape 4000 host system) and then redirected to an agent at AP x

Details:

a) incoming call using CO trunk located on AP x

- call enters ACD queue
- OpenScape Contact Center routes the call to Call Director on OpenScape 4000 host system using CSTA_DEFLECT_CALL_REQUEST and caller is connected with Call Director
- OpenScape Contact Center routes the call back in ACD queue using CSTA_SINGLE_STEP_XFER_CALL_REQUEST, an agent becomes available and OpenScape Contact Center routes the call to the agent on APx using CSTA_DEFLECT_CALL_REQUEST or
- OpenScape Contact Center routes the call to an agent on AP x using CSTA_SINGLE_STEP_XFER_CALL_REQUEST

- ACD incoming call on AP x is routed to Call Director (OpenScape 4000 host system) and then redirected to an agent at AP y

Details:

a) incoming call using CO trunk located on AP x

- call enters ACD queue
- OpenScape Contact Center routes the call to Call Director on OpenScape 4000 host system using CSTA_DEFLECT_CALL_REQUEST and caller is connected with Call Director
- OpenScape Contact Center routes the call back in ACD queue using CSTA_SINGLE_STEP_XFER_CALL_REQUEST, an agent becomes available and OSCC routes the call to the agent on AP y using CSTA_DEFLECT_CALL_REQUEST or
- OpenScape Contact Center routes the call to agent on AP y using CSTA_SINGLE_STEP_XFER_CALL_REQUEST

- ACD incoming call on AP x is routed to Call Director (OpenScape 4000 host system) and then redirected to an agent at OpenScape 4000 host system

Details:

a) incoming call using CO trunk located on AP x

- call enters ACD queue
- OpenScape Contact Center routes the call to Call Director on OpenScape 4000 host system using

CSTA_DEFLECT_CALL_REQUEST and caller is connected with Call Director
- OpenScape Contact Center routes the call back in ACD queue using CSTA_SINGLE_STEP_XFER_CALL_REQUEST, an agent becomes available and OpenScape Contact Center routes the call to agent on OpenScape 4000 host system using CSTA_DEFLECT_CALL_REQUEST or
- OpenScape Contact Center routes the call to agent on OpenScape 4000 host system using CSTA_SINGLE_STEP_XFER_CALL_REQUEST

- ACD incoming call on OpenScape 4000 host system is routed to Call Director (OpenScape 4000 host system) and then redirected to an agent at AP x

Details:

a) incoming call using CO trunk located on OpenScape 4000 host system

- call enters ACD queue
- OpenScape Contact Center routes the call to Call Director on OpenScape 4000 host system using CSTA_DEFLECT_CALL_REQUEST and caller is connected with Call Director
- OpenScape Contact Center routes the call back in ACD queue using CSTA_SINGLE_STEP_XFER_CALL_REQUEST, an agent becomes available and OpenScape Contact Center routes the call to the agent on AP x using CSTA_DEFLECT_CALL_REQUEST or
- OpenScape Contact Center routes the call to agent on A Px using CSTA_SINGLE_STEP_XFER_CALL_REQUEST

NOTICE: In case that no agent gets available during announcement, the ACD call is routed back to RCG/DNIT via CSTA_SINGLE_STEP_XFER_CALL_REQUEST and then a new agent search begins. I.e. use case 3 works for 2 cases: a. an agent gets available during announcement b. no agent gets available during announcement and a new search begins.

NOTICE: This use case works if Call Director is located on AP x.

NOTICE: This use case works if Call Director is replaced by a DIGITE.

---

4) Consultation, call transfer scenarios

5) In principle it could be that an agent wants to transfer a call to another agent who can be located on the same or in another location where maybe no IP resources are available. The call transfer can occur after every above mentioned scenario.

NOTICE: Update of numbers on the phone display after transfer via alternate routing is not possible.

---

6) **Ring No Answer - which can occur after every above mentioned scenario**
7) The ACD call is already ringing, i.e. the destination agent is already seized but not answering the call. After timeout the OpenScape Contact Center/ACD takes the call back and routes it back to the RCG/DNIT via CSTA_DEFLECT_CALL_REQUEST and starts with a new search for agents. This scenario works regardless where the originator trunk is located (OpenScape 4000 host sytsem/AP x or A Py) or where the old/new agent is located.

10.2.11.4 Generation

No special AMO configuration is necessary.

Payload Survivability must be configured properly. The only supported configuration is ALR via multichannel trunk circuit under one call number.

OpenScape Contact Center timer for ring no answer must be lower than no call transfer parameter **NOCALLTR** in OpenScape 4000.

Both timers (in OpenScape 4000 and OpenScape Contact Center) have the default value equal with 30. This leads to the following behavior: When the call comes back from ISDN it is transferred to attendant console and it is not routed to Call Director.

In OpenScape 4000 the parameter can be changed using the following AMO command:

e.g. `CHANGE-CTIME:TYPESWU=TRK,NOCALLTR=35;`

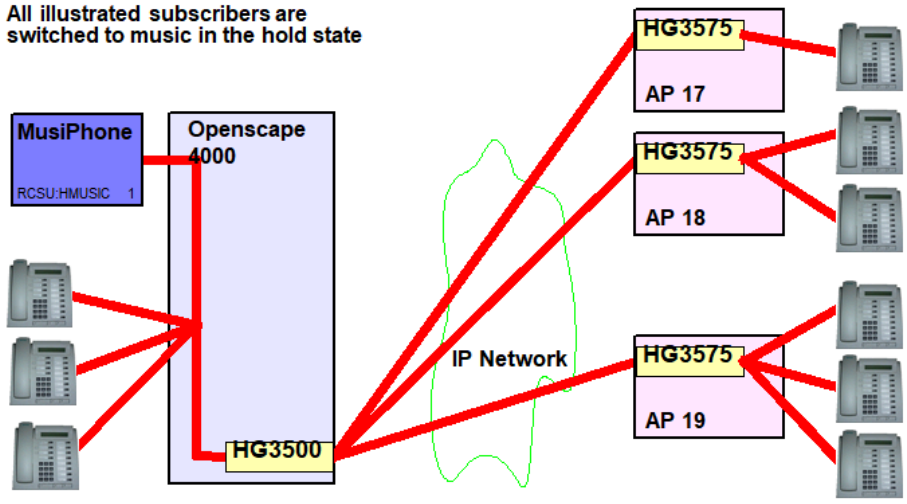
The instruction to change the timer in OpenScape Contact Center can be found in **OpenScape Contact Center Enterprise V8 R2, Manager Administration Guide, Administrator Documentation > Section 8.3.2**.

10.2.12 External Music on Hold

If an internal sound type (SIU) is replaced by an external sound source (e.g. music on hold), this new sound type is applied throughout the system.

In the example below (Figure 39 “Routes for music on hold: Supply in the central system”) an external MusiPhone is configured in the central system, as is most commonly the case.

IP payload connections to the central system are then required for all circuits in IPDA access points that are switched to external MOH. If multiple circuits/ subscribers in one access point are connected to the same MOH, only one payload connection (B channel) is connected for transmission of music between the central system and the access point, and all relevant circuits of the AP cut in to this.

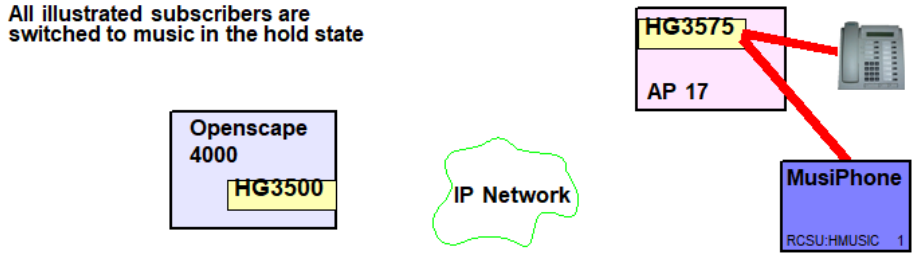


Routes for music on hold: Supply in the central system

IMPORTANT: If a circuit is switched to MOH, e.g. as a result of consultation hold, the original payload connection remains active. In other words, the connection of MOH uses an additional payload connection.

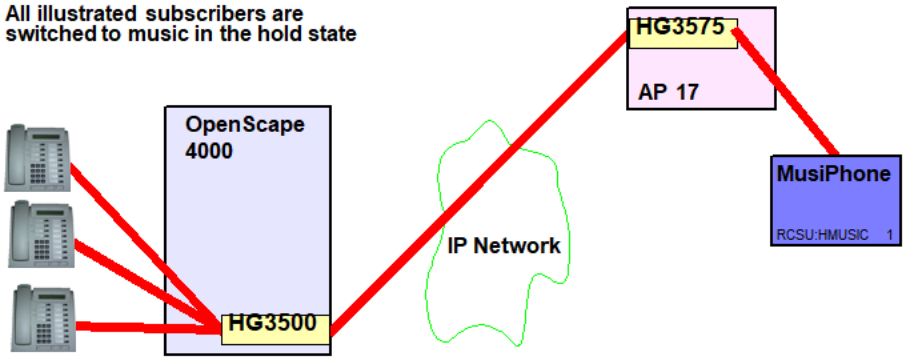
If the external MOH is supplied in an access point rather than on the central system, the connections continue to be handled as explained below.

Circuits within the access point in which the MOH is supplied are switched to MOH via the internal AP memory time switch. In other words, no additional payload connections over IP are required.



Routes for music on hold: Supply in access point 17 - local subscriber

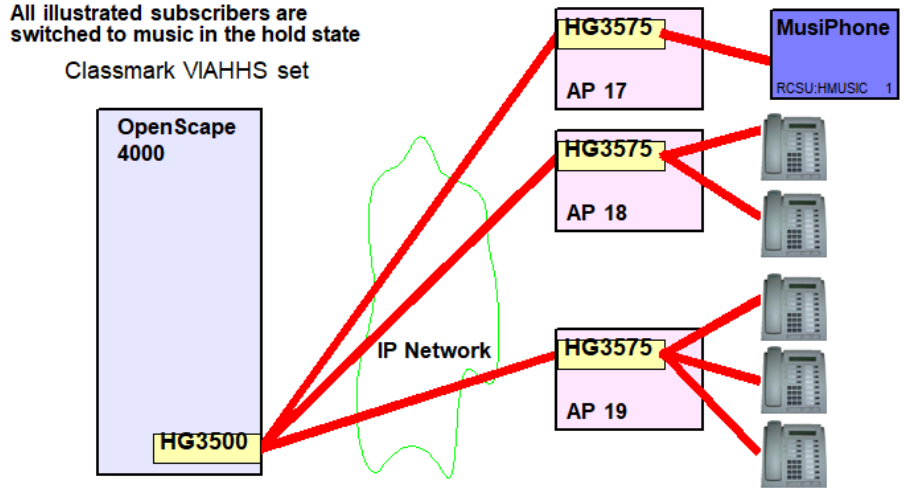
If circuits in the central system are switched to MOH, a payload connection between the access point with the MOH source and the central system is switched, from which all circuits of the central system are then operated.



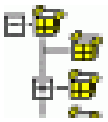
Routes for music on hold: Supply in access point 17 - central subscriber

If circuits of other access points are switched to MOH, a separate payload connection to the central system is switched for these access points. The central system is connected to the access point with the MOH source via a second payload connection. MOH connections between access points are therefore always switched via the central system.

There is no alternative routing via access point <-> access point connections if there are not enough or no resources available for the route via the central system.

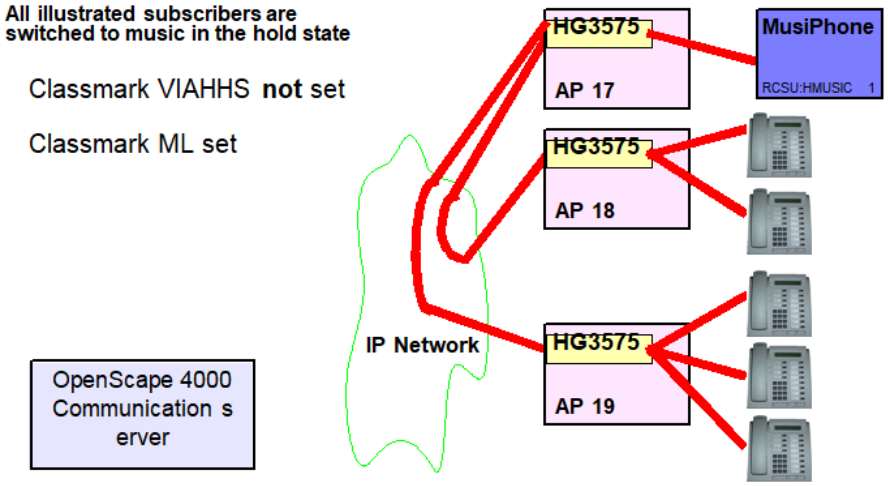


Routes for music on hold: Supply in access point 17 - subscriber in different AP

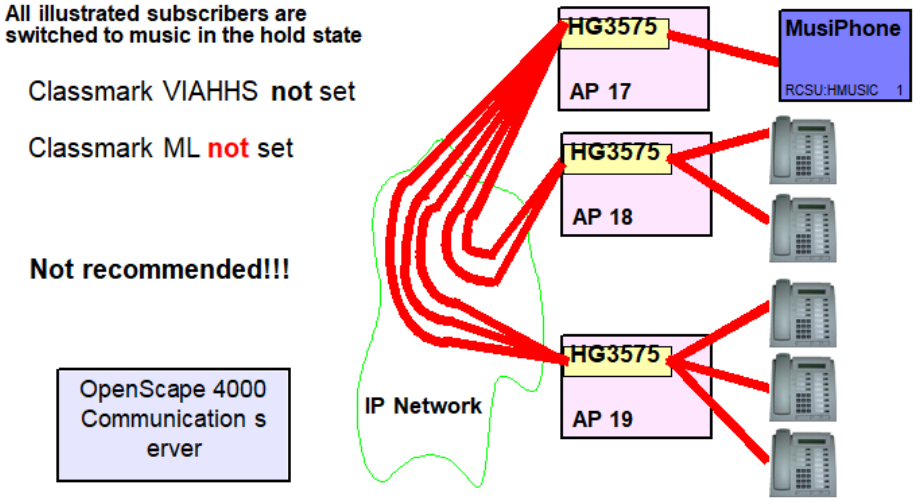
	**Configuration Management > Station > Special Stations** Click **Search** and select the special station (**Station Type**: **EXTANS**). Set or delete the required classmarks on the **Features** tab and **Save**.

	`ADD-SSC:PEN=1-2-37-10,TYPE=EXTANS,CPCALL=HOLD, CLASSMRK=G711&ML;`
	or
	`CHANGE-RCSU:PEN=1-2-37-5,CLASSMRK=G711&&ML;`

IMPORTANT: With CHANGE, please note that you must specify all classmarks that are to be set. Classmarks that were set prior to the changes will not be taken over. Always specify the classmark **ML**, otherwise an individual payload connection to the source HG 3575 will be set up for each circuit on a HG 3575 that requires active MOH. As a result, considerable bandwidth and B channel resources are consumed.



Routes for music on hold: Supply in access point 17 - subscriber in different AP



Routes for music on hold: Supply in access point 17 - subscriber in different AP

Multiple Music on Hold

With IPDA-based branch concepts, a requirement exists for the setting of different music on hold for different branches.

With the aid of flex routing, up to 150 different announcements can be used in the system. The announcements are assigned on a subscriber basis.

If all subscribers of an access point are assigned the same MOH and this MOH is supplied locally in the access point, no payload connections over IP are required for MOH. If, however, a subscriber is assigned MOH that is supplied

in a different access point, two payload connections over IP are switched - one from the MOH source to the central system and one from the central system to the AP of the subscriber.

10.2.13 Information on CMI

Please refer to the project planning guideline of OpenScape Cordless E in TI-Online.

https://ti-online.global-intra.net/produktiv/en/z3-hp4-70a.pdf

Home page TI - Online:

https://ti-online.global-intra.net/index.html

10.2.14 IP Address Changes

Unfortunately, the correct configuration of the IP addresses of all IPDA components at the time of installation is not all that is required. Restructuring of the IP network of the customer, which also affects the addressing of the IPDA components, is part of day-to-day business.

Whenever an IP address has to be changed, there is no avoiding a brief interruption in operation. In order to minimize the effects for the users of the OpenScape 4000 system, the procedure for changing addresses must be planned meticulously.

In the following scenarios, it is always assumed that the changes involved are changes that affect the entire LAN segment to which the IPDA components are connected, and not just the address of an individual component.

A distinction is made between three cases in this context:

- Change of Address in a Network Segment to which Access Points are Connected
- Changing the Address of the Survivability Network
- Changes in the OpenScape 4000 LAN Segment

10.2.14.1 Change of Address in a Network Segment to which Access Points are Connected

Let us use the configuration of Access Point AP99 as an example:

- It is to be reached from the OpenScape 4000 LAN segment via Router Ra (192.168.1.254).
- It is to reach other networks via Router Rx (192.168.23.1).
- Its own IP address is 192.168.23.99.
- The IP address for the TAP is 192.168.23.199.
- The netmask of the network in which the access point is located is 255.255.255.0

As this involves a change of the entire network segment, AP 98 is also affected with **APIPADDR=192.168.23.98**.

We receive the following information from the customer’s network administrator:

Table 48: Change of address in “networked“ access points

Name	NEW address	OLD address
Netmask	255.255.255.224	255.255.255.0
Router Rx	10.123.87.222	192.168.23.1
AP 98 APIPADDR	10.123.87.198	192.168.23.98
AP 99 APIPADDR	10.123.87.199	192.168.23.99

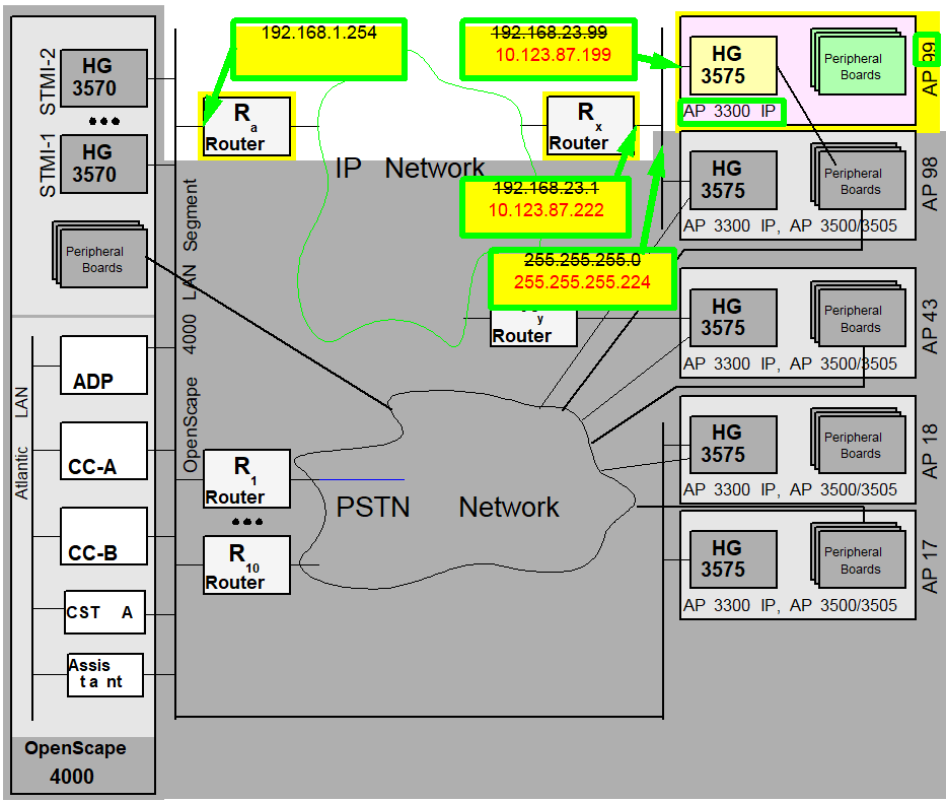


Figure 204: Change of address in “networked“ access points

The time of the address change in the access points is critical.

If parallel operation of both network addressing cannot be configured in the customer network during the transition period, the address change must be oriented to the time of transition of Router Rx and the change in routing in the customer network.

The address change must be performed prior to the reconfiguration of Router Rx and started on the access point via EXEC-USSU:UPDATAP. Existing links are disconnected. After reconfiguring the router, we would no longer be able to reach the access point and would only be able to implement the address change locally at the access point.

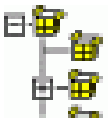
IMPORTANT: Prior to the EXEC-USSU:UPDATAP, the configuration must be updated on the system hard disk. Otherwise, the data on the system would conflict with the data on the HG 3575 when the system is reloaded and could

only be synchronized again with EXEC-USSU:UPDATAP,LTU number,UL.

As soon as the access point has restarted with the new address, the OpenScape 4000 central switch can no longer reach it via the signaling survivability route (if configured), or can only reach it via this route. This applies until the routing in the customer network has likewise been changed.

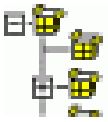
IMPORTANT: If special routes are used in the configuration of the IPDA system (in access points or for HG 3500 modules), these must all be checked and, if necessary, modified. (CHANGE-APRT:TYPE=ROUTTBL ...)

Generation

	**Configuration Management > System Data > IPDA > IPDA Access Point** Click **Search** and select the access point. Change the addresses on the **IP Interface** tab and **Save**. **Configuration Management > System Data > IPDA > IPDA System Data** Click **Search** and select the access point. Click **Execute** on the **Action** pull-down menu and select the mode of action **Update AP,** confirm with **OK**.
	CHANGE- APRT:TYPE=APNET,LTU=98,APIPADDR=10.123.87.198, NETMASK=255.255.255.224; EXEC-USSU:MODE=UPDATAP,LTU=98; CHANGE- APRT:TYPE=APNET,LTU=99,APIPADDR=10.123.87.199, NETMASK=255.255.255.224; EXEC-USSU:MODE=UPDATAP,LTU=99;

10.2.14.2 Changing the Address of the Survivability Network

This case scenario, while unlikely, is simple to realize in the OpenScape 4000 switch. All addresses in the survivability network are fixed addresses derived from the network address.

	**Configuration Management > System Data > IPDA > IPDA System Data** Click **Search**, change the survivability network address on the **System Data** tab and **Save**. **Configuration Management > System Data > IPDA > IPDA System Data** Click **Search** and select the access point. Click **Execute** on the **Action** pull-down menu and select the mode of action **Update AP**, confirm with **OK**.

	`CHANGE-SIPCO:TYPE=LSNET,SURVNET=192.168.123.0;`
	The change within the access points becomes effective after
	`EXEC-USSU:MODE=UPDATAP,LTU=xx;`
	for all affected access points.

IMPORTANT: Connections are cleared down without further warning. Prior to the `EXEC-USSU:UPDATAP`, the configuration must be updated on the system hard disk.

IMPORTANT: As ports of the survivability router are also affected by the address change, the routers also have to be reconfigured. However, this may not be performed until after conversion of the access points.

10.2.14.3 Changes in the OpenScape 4000 LAN Segment

This is the most complicated change of all, and the one which harbors the greatest risk, which is why address changes in the OpenScape 4000 LAN segment should be avoided whenever possible.

The reason is the security concept of IPDA. An access point may only be controlled by CC-A or CC-B. To this end, the IP addresses of the two processors are configured in the access point. If these addresses change, the access point can no longer be controlled and would have to be reconfigured locally.

This potentially risky task was improved in HiPath 4000 V6 R2. Since this version there is a possibility to connect to the access point from arbitrary IP address if there is no active HSR connection. So it is possible to open a new connection and transfer the configuration data to the access point or OpenScape 4000 SoftGate and establish the regular control connection. After this step the original security mechanism , that means the remote CC-A, CC-B address check, is activated again.

Furthermore, if the control connection to an access point can not be open, there is a possibility to start an SSH session to its control IP address and perform the configuration changes manually.

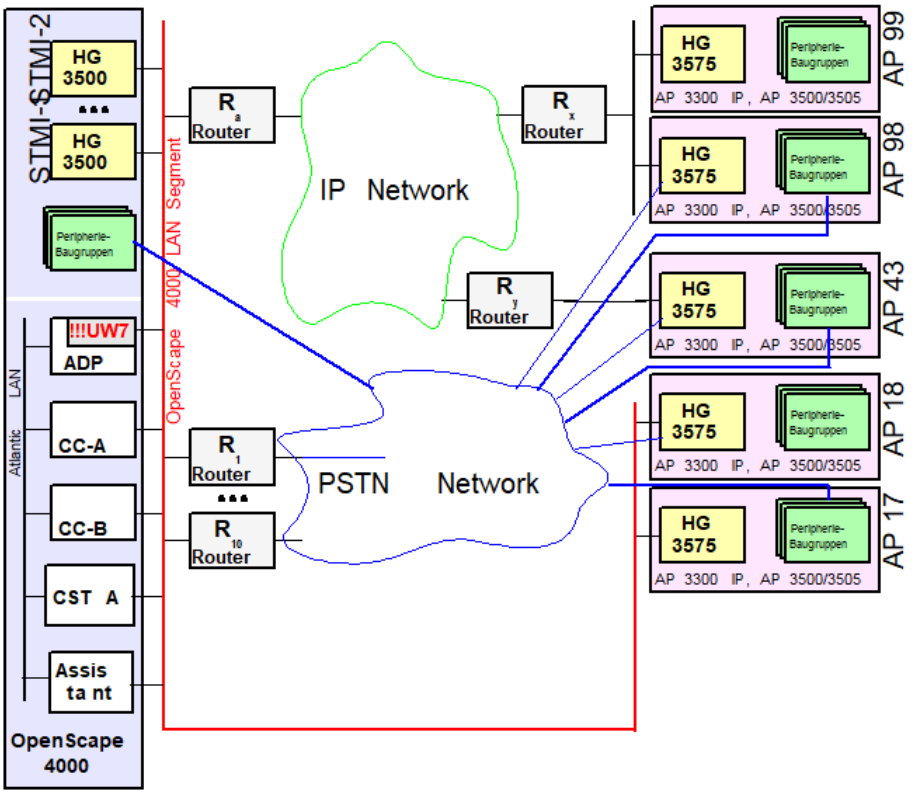


Figure 205: Installation example

We receive the following information from the customer's network administrator:

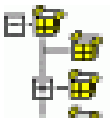
Table 49: Address change in OpenScape 4000 LAN segment

Name	NEW address	OLD address
Netmask	255.255.255.224	255.255.255.0
Network address	10.123.1.64	192.168.1.0
CC-A	10.123.1.65	192.168.1.1
CC-B	10.123.1.66	192.168.1.2
ADP	10.123.1.67	192.168.1.3
Router Ra	10.123.1.94	192.168.1.254
Router R1	10.123.1.83	192.168.1.101
Router R10	10.123.1.93	192.168.1.102
AP 17	10.123.1.77	192.168.1.17
AP 18	10.123.1.78	192.168.1.18
STMI-1	10.123.1.68	192.168.1.10
STMI-2	10.123.1.69	192.168.1.11

The following procedure avoids local reconfiguration of the access points.

Step 1

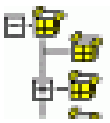
Change the IP addresses in the OpenScape 4000 LAN segment.

	**Configuration Management > System Data > IPDA > IPDA System Data** Click **Search**, change the IP addresses and, if required, **Network Mask** on the **System Data** tab and **Save**.
	`CHANGE-SIPCO:TYPE=LSNET,NETADDR=10.123.1.64, NETMASK=255.255.255.224,DEFRT=10.123.1.94, CCAADDR=10.123.1.65,CCBADDR=10.123.1.66;`

This results in the addresses being changed. However, the change is not effective until the system has been restarted, which must be the last step performed in this sequence.

Step 2

The CC-A and CC-B address changes implicitly for “networked“ access points. `LSRTADDR` must be explicitly modified as well as the address of the router on the OpenScape 4000 LAN segment (Router Ra) used for configuring the signaling connection.

	**Configuration Management > System Data > IPDA > IPDA Access Point** Click **Search** and select the access point. Change the address of the router in the network on the **IP Interface (NW)** tab and **Save**. **Configuration Management > System Data > IPDA > IPDA System Data** Click **Search** and select the access point. Click **Execute** on the **Action** pull-down menu and select the mode of action **Update AP**, confirm with **OK**.

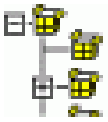
	`CHANGE-UCSU:UNIT=AP,LTU=xx,LSRTADDR=10.123.1.94;`
	`EXEC-USSU:MODE=UPDATAP,LTU=xx;`
	for **every** “networked“ AP, i.e. in this example 43, 98 and 99.

This puts the access points out of operation until both the CC address change in the system is effective and the routing in the customer network has been changed. Existing **links are disconnected.**

Step 3

Change the OpenScape 4000 LAN addresses of the “direct link“ access points.

It is assumed in this context that the addressing in the internal network of the “direct link“ access points is not changed.

	**Configuration Management > System Data > IPDA > IPDA Access Point** Click **Search** and select the access point. Change the address of the router in the network on the **IP Interface (DL)** tab and **Save**. **Configuration Management > System Data > IPDA > IPDA System Data** Click **Search** and select the access point. Click **Execute** on the **Action** pull-down menu and select the mode of action **Update AP**, confirm with **OK**.

	`CHANGE-UCSU:UNIT=AP,LTU=17,LSRTADDR=10.123.1.77;`
	`EXEC-USSU:UPDATAP,17;`
	`CHANGE-UCSU:UNIT=AP,LTU=18,LSRTADDR=10.123.1.78;`
	`EXEC-USSU:UPDATAP,18;`

This puts the access points out of operation until the CC address change in the system is effective. Existing **links are disconnected.**

Step 4

Change the survivability router addresses at the OpenScape 4000 LAN segment.

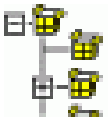
In the example, this involves Routers R1 and R10. In order to change their addresses in the OpenScape 4000 LAN segment, they must be deleted from the configuration and re-entered.

Unfortunately, a survivability router cannot be deleted until no more access points are configured on this router.

In this example, these are the access points 18, 43 and 98 which are configured for signaling survivability. Here, too, the configuration must be deleted and re-entered again.

The address configuration of the survivability routers (e.g. WAML) must, of course, be modified as well.

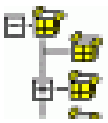
The overall procedure is as follows:

	**Configuration Management > System Data > IPDA > IPDA Access Point** Click **Search** and select the access point. Delete the router number on the **General** tab under **Signaling Survivability** and **Save**. **Configuration Management > System Data > IPDA > IPDA Signaling Survivability Router** Click **Search** and select router > **Delete**. Click **New**, enter router with modified data and **Save**. **Configuration Management > System Data > IPDA > IPDA Access Point** Click **Search** and select the access point. Enter the router number on the **General** tab under **Signaling Survivability** and **Save**.

	`DELETE-APRT:TYPE=SURV,CONF=AP,LTU=43;`
	`DELETE-APRT:TYPE=SURV,CONF=AP,LTU=98;`
	`DELETE-APRT:TYPE=SURV,CONF=ROUTER,ROUTERNO=1;`
	`ADD-APRT:TYPE=SURV,CONF=ROUTER,ROUTERNO=1, LSADDR=10.123.1.83;`
	`ADD-APRT:TYPE=SURV,CONF=AP,LTU=43,ROUTERNO=1;`
	`ADD-APRT:TYPE=SURV,CONF=AP,LTU=98,ROUTERNO=1;`
	`DELETE-APRT:TYPE=SURV,CONF=AP,LTU=18;`
	`DELETE-APRT:TYPE=SURV,CONF=ROUTER,ROUTERNO=10;`
	`ADD-APRT:TYPE=SURV,CONF=ROUTER,ROUTERNO=10, LSADDR=10.123.1.93;`
	`ADD-APRT:TYPE=SURV,CONF=AP,LTU=18,ROUTERNO=10;`

Step 5

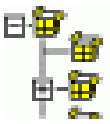
Change the addresses of the HG 3500 modules:

	**Configuration Management > System Data > Board > Board** Click **Search** and select **STMI**. Change the address on the **STMI Board Data** tab under **IP Gateway** and **Save**.
	`CHA-BCSU:TYPE=IPGW,LTU=5,SLOT=85,IPADDR=10.123.1.68;` `CHA-BCSU:TYPE=IPGW,LTU=5,SLOT=91,IPADDR=10.123.1.69;`

IMPORTANT: If special routes are used in the configuration of the IPDA system (between access points and HG 3500), these

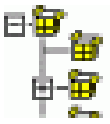
must all be checked and, if necessary, modified. (`CHANGE-APRT:TYPE=ROUTTBL ...`)

Subsequently, the changed addresses have to be loaded on the HG 3500 modules via:

	**Configuration Management > System Data > Maintenance > Board Maintenance** Click **Search** and select **STMI**. Click **Execute** on the **Action** pull-down menu, select **Restart** and confirm with **OK**.
	`RESTART-BSSU:ADDRTYPE=PARTNO,PARTNO=Q2316-X,FCTID=1;`

Step 6

To complete the procedure, the OpenScape 4000 switch now has to be reset in order for the addresses configured with SIPCO to become effective.

	The restart can only be initiated in expert mode. **Expert Mode > Expert Access > Open ...**<IP> with AMO (see AMO command)
	`EXEC-REST:UNIT,BP,SOFT;`

Contact with the “networked“ access points cannot be re-established until the routing in the customer network has also been changed.

10.2.15 A-Law/µ-Law Conversion in AP Shelf

10.2.15.1 Feature Description

It is possible to connect telephones in AP shelves that work with companding algorithms different to the host system (e.g. host system in Germany (A-law), access point in the USA (µ-law)).

10.2.15.2 Service Information

Conversion is supported for

- SIP and H323 trunk and
- HFA, SIP, TDM and analog subscribers.

10.2.15.3 Generation (Example)

CHANGE-UCSU:UNIT=AP,LTU=17,**CONVLAW=YES**;

It is necessary to reset the NCUI board in order to activate the functionality. From this moment AP shelf works in a different law against host system. The NCUI represents a G711 law conversion point.

10.2.16 Different Announcements, Tones and DTMF DialTone Receivers per Access Point

It is possible to configure different languages/countries for each access point with AMO UCSU. Therefore different access points can have the same or different SIU-Init-Data files.

10.2.16.1 Feature Description

This feature enables you to set tones and announcements for each access point on a country and language-specific basis. This means that stations will hear suitable tones and announcements for the set country/language. These are created by the SIU part of the NCUI board. Individual tones can also be assigned varying SIU functions on an access point-specific basis. In addition, the country code can also be set specific to the access point.

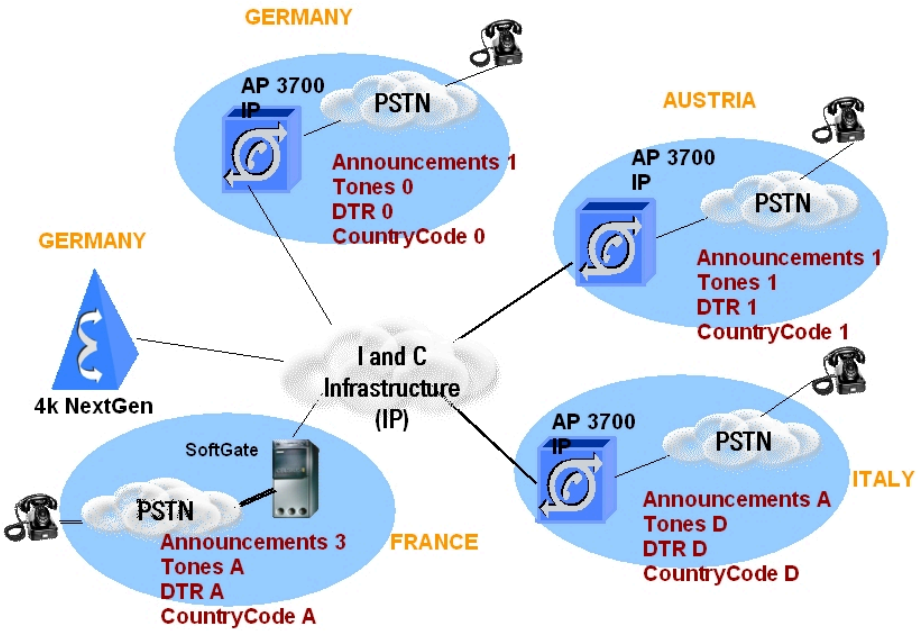


Figure 206: Feature overview

All known subscriber types (analog, digital, IP) can be used.

Analog subscriber boards can be configured per access point on a country-specific basis (this may be necessary, for example, to set the correct companding algorithm).

The dial tone receiver of the SIU part of the NCUI can also be configured on a country-specific basis.

External announcement devices (configurable via AMO SSC) can be assigned to all host and AP shelves or to individual shelves only (all host shelves certain AP shelves).

The feature is valid for classic access points and for soft APs.

10.2.16.2 Service Information

If the same country and language settings as the host system are applied to all access points, configuration can be performed as in HiPath 4000 V5 and earlier systems. Please note, however, that system-wide settings (via AMO ZAND) must be performed before the access points are configured. If system-wide settings are subsequently changed, these apply only to host shelves. If they should also apply to access points, you must set them individually for each affected access point.

The following system-wide settings (via AMO ZAND) can also be access point-specific:

Table 50: Access point-specific configuration

	AMO ZAND D1 = typ, D2 = parameter (Deutsch) E1 = typ, E2 = param (English)			
	(D1) DATENALL (D2) SIUSPKZ	(D1) DATENALL (D2) LANDKZ	(D1) TOENE (D2) SIU	(D1) TOENE (D2) HZE
	(E1) ALLDATA (E2) SIUANN	(E1) ALLDATA (E2) CNTRYCD	(E1) TN (E2) SIUC	(E1) TN (E2) DTR
Funktion / function	SIU Ansagen / SIU announcements	Länderkennzeichen für Steuerung Baugruppenloadware SLMA / Country code to control board loadware SLMA	SIU Töne / SIU tones	Hörzeichenempfänger / dial tone receiver

Access point-specific settings are performed with AMO UCSU. The parameter names in AMO ZAND are used as they are for the new parameters in AMO UCSU.

If one of these settings is changed while the access point is in operation (via CHANGE-UCSU), the ACDR or tone parameter must be loaded manually. This is done via the `EXEC-USSU:NCUILOAD;` command.

The change only takes effect when the affected NCUI board is reset. This is done via the `EXEC-USSU:UPDATAP;`.

If these system-wide settings are subsequently changed, these changes apply only to host shelves. If they should also apply to access points, the changes must also be performed on an access point-specific basis.

Special behavior for the setting for the USA:

In the USA, the companding algorithm µ-law is used (in all other countries, A-law is used).

It is possible to connect telephones in AP shelves that work with companding algorithms different to the host system (e.g. host system in Germany, AP in the USA). There was the restriction that no analog telephones may be connected in these AP shelves. With the feature "Different Announcements per Access Point", this restriction is lifted and even if the companding algorithms in the access point and host system are different, analog telephones may still be connected in the AP shelves. See also Section 2.15, “A-Law/µ-Law Conversion in AP Shelf”.

Restrictions

- The functions of peripheral SIU (SIU type 2 and 3, SIU TDS) are not access point specific configurable, i.e. the system wide setting is valid for all access points (in OpenScape 4000 SoftGate access point there is no peripheral SIU possible at all).
- Music on hold (MOH) Even though music on hold (MOH) is language/country independent it is still not configurable per access point.
- Other country-specific features like MFC variants, loadware variant for SLMA2 / SLMAR, country specific tones and attenuation for conference board of compact hardware and SCC board, etc are only supported system wide.

10.2.16.3 Generation Example

The following examples only list the AMOs/parameters that can be set on an access point-specific basis and thus only illustrate part of the total configuration.

10.2.16.3.1 Access Point in a different Country to the Host System

First, the parameters must be set for the host system (e.g. Germany):

```
CHANGE-ZAND:TYPE=ALLDATA,CNTRYCD=0,SIUANN=1;
CHANGE-ZAND:TYPE=TN,SIUC=0,DTR=0,RDS=0,CONFC=0;
```

Now the tones/announcements for another country (e.g.: Italy) can be set for an access point:

```
ADD-UCSU:UNIT=AP,LTG=1,LTU=17,LTPARTNO="Q2323-X
 ",SRCGRP=17,FRMTYPE=L80XF,CONNTYPE=APDL,LSRTADDR=198.16.16.63,
APRTADDR=198.16.16.150,LOCID=017,LOCATION="LOCATION",PHONE=3140,
FAX=3141,PLCHECK=YES,BCHLCNT=60,CONVLAW=NO,TCLASS=0,ALARMNO=0,
SIUANN=A,SIU=D,DTR=D,CNTRYCD=D;
```

10.2.16.3.2 Access Point with different Companding Algorithm

First, the parameters must be set for the host system (e.g. Germany):

```
CHANGE-ZAND:TYPE=ALLDATA,CNTRYCD=0,SIUANN=1;
CHANGE-ZAND:TYPE=TN,SIUC=0,DTR=0,RDS=0,CONFC=0;
```

Now tones/announcements can be set for an access point for a country with a different companding algorithm (USA):

```
ADD-UCSU:UNIT=AP,LTG=1,LTU=17,LTPARTNO="Q2323-X ",SRCGRP=17,FRMTYPE=L80XF,
CONNTYPE=APDL,LSRTADDR=198.16.16.63,APRTADDR=198.16.16.150,LOCID=017,
LOCATION="LOCATION",PHONE=3140,FAX=3141,PLCHECK=YES,BCHLCNT=60,CONVLAW=YES,
TCLASS=0,ALARMNO=0,SIUANN=D,SIU=K,DTR=K,CNTRYCD=K;
```

If the companding algorithm is changed while the access point is already in operation (via CHANGE-UCSU), the access point must first be deactivated (via DEACTIVATE-USSU). Only when you have completed this action will the **CONVLAW** parameter be considered when changing. Finally, you should reactivate the access point (via ACTIVATE-UCSU).

10.2.16.3.3 Access Point with individual CP Tone <-> SIU Function Assignment

When setting system-wide tones (via AMO ZAND), the standard assignment of CP tones to SIU functions is also set for the system. This assignment can be adapted system-wide via AMO ZAND (**TYPE=TONES**, parameter **CPCALL** and **SIU**).

When setting access point-specific tones (via AMO UCSU), the standard assignment of CP tones to SIU functions for the corresponding access point is also set. This assignment can be adapted via AMO UCSU (parameter **CPCALL** and **SIU**) to as specific access point.

Example: assign the CP tone "Not possible" to the SIU function 0:

CHANGE-UCSU:UNIT=AP,LTG=1,LTU=17,**CPCALL=NOPO**,**SIU=0**;

10.2.16.3.4 External Announcement Devices

CP tones can also be assigned to external announcement devices that can be configured via AMO SSC to an analog board. External announcement device assignment to CP tone can be configured on a system-wide or individual basis

- for all host shelves only, or
- for all host shelves and x access points, or
- for x access points only.

(x stands for one or all APs)

If the AMO SSC is configured for announcement devices, this means that the setting applies to all shelves (host and AP). If the announcement devices is to be configured individually for certain shelves, the parameter **LTU** should be entered. This means that entering a host shelf applies the setting to all host shelves and entering an AP shelf (or AP shelf area) applies the setting to the AP shelf (or to the corresponding AP shelves).

You can configure up to 300 different external announcement devices.

1) Setting external announcement devices system-wide:

ADD-SSC:PEN=1-18-1-0,TYPE=EXTANN,CPCALL=INTDTN;

1) Setting external announcement devices for all host shelves only:

ADD-SSC:1-18-1-0,EXTANN,INTDTN,**LTU=1**;

1) Setting external announcement devices for all host shelves and an AP shelf:

ADD-SSC:PEN=1-18-1-0,TYPE=EXTANN,CPCALL=INTDTN,**LTU=1**; ADD-SSC:PEN=1-18-1-0,TYPE=EXTANN,CPCALL=INTDTN,**LTU=17**;

1) Setting external announcement devices for multiple AP shelves:

ADD-SSC:PEN=1-18-1-0,TYPE=EXTANN,CPCALL=INTDTN,**LTU=17**; ADD-SSC:PEN=1-18-1-0,TYPE=EXTANN,CPCALL=INTDTN,**LTU=20**;

10.2.16.4 Relevant AMOs

AMO	Parameter	Sprache/ Language	Beschreibung/ Description
SSC	TYP=EXTANS	d	Externe Ansage

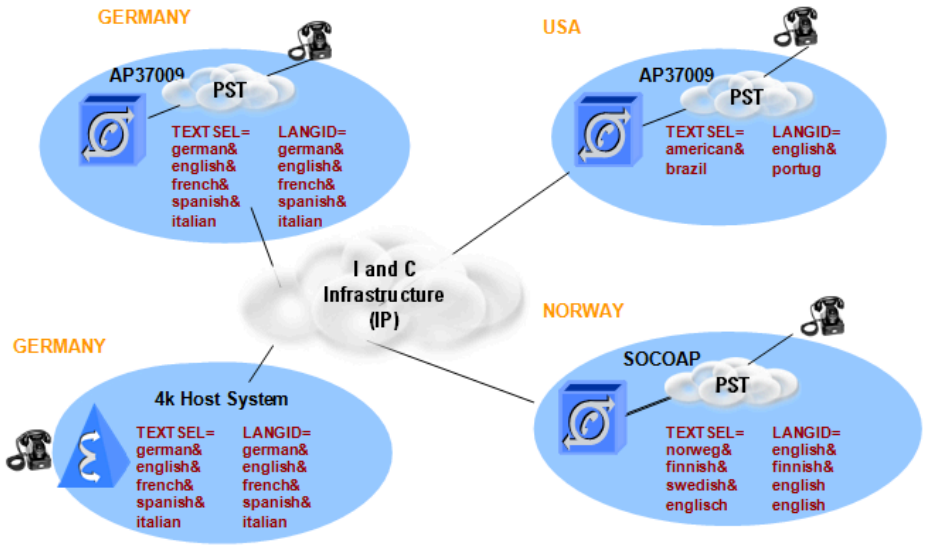
AMO	Parameter	Sprache/ Language	Beschreibung/ Description
	TYPE=EXTANN	e	External announcement
	LTU	d	LTU-Nummer
	LTU	e	LTU Number
UCSU	CPTON	d	Vermittlungstechnischer Ton
	CP	e	Call processing tone
	HZE	d	Auswahl der länderspezifischen Hörzeichenempfängertabelle
	DTR	e	Selection of country-specific dial tone receiver table
	KONVLAW	d	A-Law/Mu-Law Konvertierung auf der NCUIx-Baugruppe
	CONVLAW	e	A-Law/Mu-Law conversion on NCUIx board
	LANDKZ	d	Loadwarevariante für SLMA2 / SLMAR
	CNTRYCD	e	Loadware variant for SLMA2 / SLMAR
	SIU	d	Auswahl der länderspezifischen SIU-Tontabelle
	SIUC	e	Selection of country-specific SIU tone table
	SIUSPKZ	d	Sprachkennzeichen für SIU-Texte
	SIUANN	e	Set options for SIU announcement texts
	SIUTON	d	Zugeordneter Ton der SIU
	SIU	e	Assigned siu tones
ZAND	HZE	d	Auswahl der länderspezifischen Hörzeichenempfängertabelle
	DTR	e	Selection of country-specific dial tone receiver table
	LANDKZ	d	Loadwarevariante für SLMA2 / SLMAR
	CNTRYCD	e	Loadware variant for SLMA2 / SLMAR
	SIU	d	Auswahl der länderspezifischen SIU-Tontabelle

AMO	Parameter	Sprache/ Language	Beschreibung/ Description
	SIUC	e	Selection of country-specific SIU tone table
	SIUSPKZ	d	Sprachkennzeichen für SIU-Texte und SWU-Displaytexte
	SIUANN	e	Set options for SIU announcement texts
	TYP=TONTBL	d	Zuordnungstabelle CP-Ton -> SIU-Ton
	TYPE=TONES	e	Tone table, assignment of CP tones to SIU tones
	CPTON	d	Vermittlungstechnischer Ton
	CP	e	Call processing tone
	SIUTON	d	Zugeordneter Ton der SIU
	SIU	e	Assigned siu tones

10.2.17 Different Languages/National Character Sets for Displaying Text for Individual Access Points

Different language pairs/national character sets can be configured individually for each Access Point for displaying text on terminals. Furthermore, the settings may also differ from the host system. This means that the display languages available on a terminal connected to an Access Point may differ from those on a terminal connected to the host system.

10.2.17.1 Feature Description



Languages/national character sets for displaying text for individual Access Points

This feature allows five languages to be configured individually for each Access Point. This can be carried out with AMO UCSU, Parameter **TEXTSEL**. The languages can either be the same as in the host system or may differ. Furthermore, the same languages can be configured for all Access Points/ OpenScape 4000 SoftGates or different languages can be configured individually for each Access Point.

Since individual languages can be configured for Access Points/OpenScape 4000 SoftGates, the relevant national character sets (AMO UCSU, Parameter **LANGID**) can also be configured specifically per Access Point. Five character sets (the same for all host shelves) can also be configured for the host system (AMO ZAND, Parameter **LANGID**).

As with the host system (AMO ZAND, Parameter **TEXTSEL**), it is also the case for Access Points/OpenScape 4000 SoftGates that the first language configured with AMO UCSU, Parameter **TEXTSEL**, is taken as the default language for the relevant Access Point.

All terminals connected to the host system use the default language of the host system as the preferred language. Terminals connected to an Access Point use the default language of the corresponding Access Point/OpenScape 4000 SoftGate as the preferred language.

The preferred language of a terminal can also be changed individually with AMO SBCSU or SCSU. However, only the languages that are valid for the shelf (on which the terminal is configured) are possible.

10.2.17.2 Service Information

General information

- This feature is supported from OpenScape 4000 V7 R0.

- The languages for displaying text can be configured independently of other language-specific settings (e.g. announcements or tones).
- The feature is valid both for traditional Access Points and for Soft Access Points (e.g. OpenScape 4000 SoftGate, OpenScape Access/Branch).
- The values used for **TEXTSEL** and **LANGID** have to match.
- It is also possible to transfer the language setting for the "PIN mobile" feature. This means the home station is used following identification of the preferred language. The prerequisite for this however is that the home station language is also configured for the shelf to which the visitor station is connected. If this is not the case, the first language of the visited shelf is set.
- The same applies for the "Mobile HFA" feature. The preferred language of the home station is used following the mobile login. The prerequisite for this likewise is that the home station language is also configured for the shelf to which the visitor station is connected. If this is not the case, the first language of the visited shelf is set.
- Language selection on the terminal is possible as usual, in other words the language can be changed by means of the language selection key. The languages that are configured for the shelf to which the terminal is connected can be selected.
- It is still possible to change the language for an individual terminal (using AMO SBCSU or AMO SCSU).
- If the changes are made with CHANGE-UCSU on an Access Point that is already in operation, then the texts have to be loaded or the character set defined. Only then will the change be effective. This is done by

  – resetting the Access Point:

  RESTART-USSU:RESTYPE=LTU,LTU=<LTU number>;

  – Hard restart with resetting of peripherals

  CHANGE-ZANDE:TYPE=LOADBHV,PIT=HRBHV,LOAD=LWLOAD;

  and

  EXEC-REST:TYPE=UNIT,UNIT=BP,RSLEVEL=RELOAD;

  or

  – Reload

  EXEC-REST:TYPE=UNIT,UNIT=BP,RSLEVEL=RELOAD;

Restriction

A default system language can no longer be configured once this feature is introduced.

If a default language is still to be configured for the entire system, then either:

- No individual languages can be set for Access Points with AMO UCSU. The languages configured in the host system with AMO ZAND then apply in this case.

or

- The first language for host shelves and all Access Points must be the same (Parameter **TEXTSEL** for the first language in AMO ZAND and in AMO UCSU).

- Example:

  In the case of CMI terminals, the language for menu texts (e.g. SAVED NUMBER REDIAL) is set identically for all CMI terminals on the system using CATool. The default system language is used for this purpose.

  The service menu texts (e.g. "Please select") are shown in the language that is configured for the respective CMI terminal (using AMO SBCSU). This language can be selected from the languages configured for the host shelves or AP shelves (depending on whether the CMI terminal is configured on a host or AP shelf). If the language for the service menu texts is to be the same as the language for the menu texts for all CMI terminals, then the first language with ZAND and UCSU must be the same as the language for menu texts; this then corresponds to the default system language.

10.2.17.3 Generation (Example)

If all Access Points are assigned the same language settings as the host system, the configuration can be performed in the same way as the previous variant. Please note, however, that system-wide settings (via AMO ZAND) must be performed first before the Access Points are configured. If system-wide settings are subsequently changed, these apply only to host shelves. If they are also to apply to Access Points, they have to be configured individually for each affected Access Point.

10.2.17.3.1 Access Point with the same Settings as the Host System

The parameters are first configured for the host system (e.g. German, English, French, Spanish and Italian):

```
CHANGE-ZAND:TYPE=ALLDATA2,TEXTSEL=GERMAN&ENGLISH&FRENCH&SPANISH&ITALIAN;
CHANGE-ZAND:TYPE=OPTISET,LANGID=GERMAN&ENGLISH&FRENCH&SPANISH&ITALIAN;
```

The same texts/character sets as for the host system can now be used for an Access Point:

If the **TEXTSEL** and **SPRACHID** parameters are not specified, they will be taken automatically from the central settings:

```
ADD-UCSU:UNIT=AP,LTG=1,LTU=17,LTPARTNO="Q2324-X ",SRCGRP=17,FRMTYPE=AP37009,
CONNTYPE=APDL,LSRTADDR=198.16.16.63,APRTADDR=198.16.16.150,LOCID=017,LOCATION="LOCATION",
PHONE=3140,FAX=3141,PLCHECK=YES,BCHLCNT=60,CONVLAW=NO,TCLASS=0,ALARMNO=0,SIUANN=1,SIUC=0,
DTR=0,CNTRYCD=0;
```

The **TEXTSEL** and **SPRACHID** parameters can also be specified with the same values however:

```
ADD-UCSU:UNIT=AP,LTG=1,LTU=17,LTPARTNO="Q2324-X ",SRCGRP=17,FRMTYPE=AP37009,
CONNTYPE=APDL,LSRTADDR=198.16.16.63,APRTADDR=198.16.16.150,LOCID=017,LOCATION="LOCATION",
PHONE=3140,FAX=3141,PLCHECK=YES,BCHLCNT=60,CONVLAW=NO,TCLASS=0,ALARMNO=0,SIUANN=1,SIUC=0,
DTR=0,CNTRYCD=0,TEXTSEL=GERMAN&ENGLISH&FRENCH&SPANISH&ITALIAN,
LANGID=GERMAN&ENGLISH&FRENCH&SPANISH&ITALIAN;
```

10.2.17.3.2 Access Point with different Settings to the Host System

The parameters are first configured for the host system (e.g. German, English, French, Spanish and Italian):

```
CHANGE-ZAND:TYPE=ALLDATA2,TEXTSEL=GERMAN&ENGLISH&FRENCH&SPANISH&ITALIAN;
CHANGE-ZAND:TYPE=OPTISET,LANGID=GERMAN&ENGLISH&FRENCH&SPANISH&ITALIAN;
```

The texts/character sets can now be configured with different values for an Access Point (e.g. American and Brazilian):

```
ADD-UCSU:UNIT=AP,LTG=1,LTU=20,LTPARTNO="Q2329-X ",SRCGRP=20,
```

```
FRMTYPE=SOCOAP,CONNTYPE=APDL,LSRTADDR=198.16.16.20,APRTADDR=198.16.16.150,
LOCID=020,LOCATION="LOCATION",PHONE=3140,FAX=3141,PLCHECK=YES,BCHLCNT=60,
CONVLAW=YES,TCLASS=0,ALARMNO=0,SIUANN=D,SIUC=K,DTR=K,CNTRYCD=K,
TEXTSEL=AMERICAN&BRAZIL,LANGID=ENGLISH&PORTUG;
```

10.2.17.4 Relevant AMOs

AMO	Parameter	Sprache/ Language	Beschreibung/ Description
UCSU	TEXTSEL	d	Grundeinstellungen für die teilnehmerindividuelle Einstellung der Sprache der Ausgabetexte im Display pro Access Point. Jede Sprache kann nur einmal eingegeben werden. Doppeleinträge werden nach Meldung H14 ignoriert. Die Sprachen werden nacheinander eingetragen, wobei der erste Eintrag als Standardwert im Shelf verwendet wird. Werden weniger als 5 Sprachen eingegeben, werden die restlichen Felder mit "Leerzeichen" belegt. Außerdem wird überprüft, ob zur einzutragenden Sprache das Textsubsystem auf Hard Disk vorhanden ist. Falls nicht, wird die Sprache nach Meldung F34 ignoriert.
	TEXTSEL	e	General settings for individual language setting of display texts. None of the languages may be stated more than once. The multiple entries will be ignored and the advisory message H14 will be displayed. All languages are entered one after the other, whereby the first language is used as default value for the shelf. If less than 5 languages are entered, the remaining places of the table are filled with blank. There is an additional check if the corresponding text subsystems are available on the hard disk. If not, the language will be ignored and the message F34 will be displayed.
	SPRACHID	d	Festlegen des nationalen Zeichensatzes für das Display
	LANGID	e	National character set for display

10.3 Load Calculation

The following bit rate calculations only take one direction into account. The route back in the opposite direction requires the same bit rate.

If a “shared medium“ is used for both directions, i.e. both directions are routed via the same line, then both directions also have to be included in the calculation. This is the case with 10Base5, 10Base2 and 10BaseT or 100BaseT half-duplex.

The Ethernet Media Access Layer (MAC) is realized pursuant to the IEEE 802.3 / DIX Ethernet II Standard with MAC-Type 0800 (IP) in the case of the IPDA components. The alternative pursuant to IEEE 802.3 and 802.2 LLC/ SNAP is not customary and would require greater bandwidth.

The calculations have been performed with active VLAN Tagging pursuant to IEEE 802.1q. This yields the higher network load. Without VLAN Tagging, the packet size is reduced by 4 octets (bytes).

IMPORTANT: The bit rate calculation used in this manual differs from that used in previous versions. By popular demand, the bit rate is no longer specified on the Physical Layer (PHY), but instead on the Media Access Layer (MAC). The 8 bytes for the preamble are no longer included in the calculation.

Payload transport with RTP (Realtime Transmission Protocol)

Table 51: Load calculation for an RTP connection (VoIP)

Codec type	Sample size [ms]	Payload [Octets]	Ethernet packet size [Octets]	Ratio Overhead / Payload	Ethernet load No preamble [kbps]	Ratio RTP / ISDN bit rate
G.711	20	160	222	39%	88.8	139%
G.711	**30**	**240**	**302**	**26%**	**80.5**	**126%**
G.711	60	480	542	13%	72.3	113%
G.729A	**20**	**20**	**82**	**310%**	**32.8**	**51%**
G.729A	40	40	102	155%	20.4	32%
G.729A	60	60	122	103%	16.3	25%

The G.711 codec generates a sample every 125 µs. The G.729A codec generates a 10-octet frame every 10 ms.

The overhead calculation is based on the following:

Table 52: Overhead with RTP connections

Protocol	Overhead
RTP	12

Protocol	Overhead
UDP	8
IP	20
IEEE 802.1Q VLAN Tagging	4
Ethernet MAC (DA,SA,TYPE,FCS - no preamble)	18
Total	**62**

The transmission bit rate depends not only on the codec type used and the sample size, but also on the stack layer on which the bit rate is calculated. Details on configuring the RTP payload can be found in Section 3.3, “Calculation Basis - Configuring Payload Packets”.

In this document, the “worst case“ on the physical layer is always considered, i.e. the Ethernet MAC frame including FCS with activated VLAN tagging. The bit rates on higher stack layers are also important when calculating the load following implementation on other media. The table below provides an overview. The values are specified in Kbps and apply to an RTP connection in one direction:

Table 53: Load for an RTP connection [Kbps]- by stack layer

Stack layer (Protocol)	Codec type / Sample size					
	G.711			G.729		
	20 ms	30 ms	60 ms	20 ms	30 ms	60 ms
RTP	68.8	67.2	65.6	12.8	10.4	9.6
UDP	72.0	69.3	66.7	16.0	12.0	10.7
IP	80.0	74.7	69.3	24.0	16.0	13.3
Ethernet No preamble No VLAN TAG	84.0	79.5	71.7	31.2	19.6	15.7
Ethernet No preamble With VLAN TAG	85.6	80.5	72.3	32.8	20.4	16.3
Ethernet With preamble No VLAN TAG	87.2	81.6	72.8	34.4	21.2	16.8
Ethernet With preamble With VLAN TAG	88.8	82.7	73.3	36.0	22.0	17.3

RTP load during inactivity of VAD or DMC master connections

If “idle“ is detected when Voice Activity Detection has been enabled, audio signals will not be transmitted temporarily. Nonetheless, the load on the RTP connection does not drop completely to zero because data continues to be transmitted on the RTP connection to check the connection and (depending on the codec) to transmit the background noise. This data is referred to as SID frames (**S**ilence **I**nsertion **D**escriptor). The RTCP connection is not affected by VAD.

Table 54: Load on an RTP connection [kbps] with VAD during inactivity

Stack Layer (Protocol)	Codec Type	
	G.711	G.729
RTP	1.8	1.1
UDP	2.5	1.8
IP	4.1	3.4
Ethernet, No preamble, No VLAN TAG	4.9	4.2
Ethernet, No preamble, With VLAN TAG	5.2	4.5
Ethernet, With preamble, No VLAN TAG	5.5	4.8
Ethernet, With preamble, With VLAN TAG	5.8	5.1

The payload connection is controlled via the parallel RTCP connection (Realtime Transmission Control Protocol)

A **Sender Report** message is sent by each relevant connection partner every five seconds for every RTP connection. No Receiver Reports are sent. This produces a load of 0.2 Kbps in each direction. The packet size was once again calculated with VLAN tag and preamble.

Table 55: Load calculation for an RTCP connection

Report type	Report interval [s]	Average Ethernet packet size [Octets]	Ethernet load excl. preamble [Kbps]
Sender report	5	130	**0.2**

10.3.1 Load Calculation for Access Points

IMPORTANT: The estimated bandwidth of 32kBit/s (minimum bandwidth) or 64kBit/s for TCP signaling is sufficient for call processing operation. Initial operation and loading of the boards in an AP shelf (sometimes with large loadware volumes) are also controlled via TCP this can result in very long initial operation times!

Calculation of the high-priority load for an individual access point

Table 56: High-priority load of an access point (G.711/20 ms sample size)

Protocol	Data type	Maximum bit rate/ port [Kbps]	Total bit rate [Kbps] with N payload ports		
			N=30	N=60	N=120
RTP	VoIP	88.8	2,664	5,328	10,656
RTCP	VoIP	0.2	6	12	25
TCP/IP	Signaling	64.0	64	64	64
TCP/IP	Supervisory (only if signaling supervisory is configured)	0.1	4	8	15
Total load			**2,738**	**5,412**	**10,760**

The requisite bit rate for a supervisory connection depends on the configuration of the keep-alive timer for this connection. The parameter to this end is SUPVTIME in the TIMING branch of the AMO SIPCO. The maximum values are specified in the table.

The load which is generated through signaling and control between the OpenScape 4000 central system and an access point - which is also a high-priority load - has been specified globally as 64 Kbps.

However, the actual load depends on the number of subscriber lines, CO and tie trunks and the actual telephone usage behavior in the access point.

If, however, modules are reloaded, additional load is generated which, in the case of limited bandwidth, can delay the signaling.

The absolute minimum of signaling bandwidth required is 32 kbps. If less than 64 kbps signaling bandwidth is available, traffic shaping must be enabled and set to the actual bandwidth available. See Section 2.7.1, “Restriction of the Available Signaling Bandwidth (Traffic Shaping)”.

In addition to high-priority load, low-priority load portions may also arise in certain situations for the following:

1) SNMP queries via network management

- TAP/Service PC access at the access point
- FTP-loading of a new HG 3575 loadware as a background task

High-priority load of an access point as a function of codec type and sample size

Table 57: High-priority load of an AP as a function of codec and sample size

Codec type	Sample size	RTP load [Kbps] with N payload ports			Total Ethernet load [Kbps] with N payload ports		
		N=30	N=60	N=120	N=30	N=60	N=120
G.711	20	2,664	5,328	10,656	2,738	5,412	10,760
G.711	**30**	**2,416**	**4,832**	**9,664**	**2,490**	**4,916**	**9,768**
G.711	60	2,168	4,336	8,672	2,242	4,420	8,776
G.729A	**20**	**984**	**1,968**	**3,936**	**1,058**	**2,052**	**4,040**
G.729A	40	612	1,224	2,448	686	1,308	2,552
G.729A	60	488	976	1,952	562	1,060	2,056

Note

This appraisal must be treated with caution, as the utility of the G.729A codec is limited by various factors:

1) The call is transferred uncompressed if one of the subscribers/circuits involved prevents compression

- Connections with fax, modem and data terminal devices are only transferred uncompressed
- External music and announcements are mostly transferred uncompressed (depends on the configuration (RCSU-CLASSMRK))
- Connections to a conference unit are mostly switched without compression (depends on the configuration (ZAND-IPDAVCCF))

In all of these cases, either G.711 is used, or no codec at all.

The bit rates for G.711 thus apply.

In order to guarantee that bottlenecks are never encountered in the available bandwidth, the access point link must be designed for the G.711 bit rate.

By means of statistical appraisals, taking the actual configuration into account (how many fax/data devices are actually deployed, how many compression licenses are available, are all possible subscriber/access circuits configured for compression, how frequently are conferences used), a mixed calculation can be performed.

The load as a function of a sample size can only be used if it is ensured that all IPDA components are configured exclusively for this sample size. Otherwise, the worst value for the respective codec type would have to be used for reasons of reliability.

High-priority load of an access point as a function of the maximum number of B-channels

Table 58: High-priority load of an AP as a function of the permissible B-channels

Maximum permissible number of B-channels	Total Ethernet load at G.711/20ms [Kbps]	Total Ethernet load at G.711/30ms [Kbps]	Total Ethernet load at G.711/60ms [Kbps]
1	153	145	137
2	242	226	209
3	331	306	282
4	420	387	354
5	509	468	427
6	598	549	499
7	687	629	571
8	776	710	644
9	865	791	716
10	954	872	789
11	1,043	952	861
12	1,132	1,033	934
13	1,221	1,114	1,006
14	1,310	1,195	1,079
15	1,399	1,275	1,151
16	1,488	1,356	1,224
17	1,577	1,437	1,296
18	1,666	1,517	1,369
19	1,755	1,598	1,441
20	1,844	1,679	1,514
21	1,933	1,760	1,586
22	2,022	1,840	1,659
23	2,111	1,921	1,731
24	2,200	2,002	1,804

Maximum permissible number of B-channels	Total Ethernet load at G.711/20ms [Kbps]	Total Ethernet load at G.711/30ms [Kbps]	Total Ethernet load at G.711/60ms [Kbps]
25	2,289	2,083	1,876
26	2,378	2,163	1,948
27	2,467	2,244	2,021
28	2,556	2,325	2,093
29	2,645	2,406	2,166
30	2,734	2,486	2,238
31	2,823	2,567	2,311
32	2,912	2,648	2,383
33	3,001	2,729	2,456
34	3,090	2,809	2,528
35	3,179	2,890	2,601
36	3,268	2,971	2,673
37	3,357	3,052	2,746
38	3,446	3,132	2,818
39	3,535	3,213	2,891
40	3,624	3,294	2,963
41	3,713	3,375	3,036
42	3,802	3,455	3,108
43	3,891	3,536	3,181
44	3,980	3,617	3,253
45	4,069	3,697	3,325
46	4,158	3,778	3,398
47	4,248	3,859	3,470
48	4,337	3,940	3,543
49	4,426	4,020	3,615
50	4,515	4,101	3,688
51	4,604	4,182	3,760

Maximum permissible number of B-channels	Total Ethernet load at G.711/20ms [Kbps]	Total Ethernet load at G.711/30ms [Kbps]	Total Ethernet load at G.711/60ms [Kbps]
52	4,693	4,263	3,833
53	4,782	4,343	3,905
54	4,871	4,424	3,978
55	4,960	4,505	4,050
56	5,049	4,586	4,123
57	5,138	4,666	4,195
58	5,227	4,747	4,268
59	5,316	4,828	4,340
60	5,405	4,909	4,413
61	5,494	4,989	4,485
62	5,583	5,070	4,558
63	5,672	5,151	4,630
64	5,761	5,232	4,703
65	5,850	5,312	4,775
66	5,939	5,393	4,847
67	6,028	5,474	4,920
68	6,117	5,555	4,992
69	6,206	5,635	5,065
70	6,295	5,716	5,137
71	6,384	5,797	5,210
72	6,473	5,878	5,282
73	6,562	5,958	5,355
74	6,651	6,039	5,427
75	6,740	6,120	5,500
76	6,829	6,200	5,572
77	6,918	6,281	5,645
78	7,007	6,362	5,717

Maximum permissible number of B-channels	Total Ethernet load at G.711/20ms [Kbps]	Total Ethernet load at G.711/30ms [Kbps]	Total Ethernet load at G.711/60ms [Kbps]
79	7,096	6,443	5,790
80	7,185	6,523	5,862
81	7,274	6,604	5,935
82	7,363	6,685	6,007
83	7,452	6,766	6,080
84	7,541	6,846	6,152
85	7,630	6,927	6,224
86	7,719	7,008	6,297
87	7,808	7,089	6,369
88	7,897	7,169	6,442
89	7,986	7,250	6,514
90	8,075	7,331	6,587
91	8,164	7,412	6,659
92	8,253	7,492	6,732
93	8,342	7,573	6,804
94	8,431	7,654	6,877
95	8,520	7,735	6,949
96	8,609	7,815	7,022
97	8,698	7,896	7,094
98	8,787	7,977	7,167
99	8,876	8,058	7,239
100	8,965	8,138	7,312
101	9,054	8,219	7,384
102	9,143	8,300	7,457
103	9,232	8,380	7,529
104	9,321	8,461	7,601
105	9,410	8,542	7,674

Maximum permissible number of B-channels	Total Ethernet load at G.711/20ms [Kbps]	Total Ethernet load at G.711/30ms [Kbps]	Total Ethernet load at G.711/60ms [Kbps]
106	9,499	8,623	7,746
107	9,588	8,703	7,819
108	9,677	8,784	7,891
109	9,766	8,865	7,964
110	9,855	8,946	8,036
111	9,944	9,026	8,109
112	10,033	9,107	8,181
113	10,122	9,188	8,254
114	10,211	9,269	8,326
115	10,300	9,349	8,399
116	10,389	9,430	8,471
117	10,478	9,511	8,544
118	10,567	9,592	8,616
119	10,656	9,672	8,689
120	10,745	9,753	8,761

10.3.2 Load Calculation for a HG 3500

Calculation of the high-priority load for a HG 3500

Table 59: High-priority load of a HG 3500 (G.711/20 ms sample size)

Protocol	Data type	Maximum bit rate/ port [Kbps]	Total bit rate [Kbps] with N payload ports		
			N=30	N=60	N=120
RTP	VoIP	88.8	2,664	5,328	10,656
RTCP	VoIP	0.2	6	12	25
Total load			**2,670**	**5,340**	**10,681**

In addition to high-priority load, low-priority load portions may also arise in certain situations for the following:

1) SNMP queries via network management

- TAP/Service PC access at the access point
- FTP-loading of a new HG 3575 loadware as a background task

High-priority load of a HG 3500 as a function of codec type and sample size

Table 60: High-priority load of a HG 3500 as a function of codec and sample size

Codec type	Sample size	RTP load [Kbps] with N payload ports			Total Ethernet load [Kbps] with N payload ports		
		N=30	N=60	N=120	N=30	N=60	N=120
G.711	20	2,664	5,328	10,656	2,670	5,412	10,760
G.711	**30**	**2,416**	**4,832**	**9,664**	**2,490**	**4,916**	**9,768**
G.711	60	2,168	4,336	8,672	2,242	4,420	8,776
G.729A	**20**	**984**	**1,968**	**3,936**	**1,058**	**2,052**	**4,040**
G.729A	40	612	1,224	2,448	686	1,308	2,552
G.729A	60	488	976	1,952	562	1,060	2,056

Note

This appraisal must be treated with caution, as the utility of the G.729A codec is limited by various factors:

1) The call is transferred uncompressed if one of the subscribers/circuits involved prevents compression

- Connections with fax, modem and data terminal devices are only transferred uncompressed
- External music and announcements are mostly transferred uncompressed (depends on the configuration (RCSU-CLASSMRK))
- Connections to a conference unit are mostly switched without compression (depends on the configuration (ZAND-IPDAVCCF))

In all of these cases, either G.711 is used, or no codec at all.

The bit rates for G.711 thus apply.

In order to guarantee that bandwidth bottlenecks are never encountered, the access point link must be designed for the G.711 bit rate.

By means of statistical appraisals, taking the actual configuration into account (how many fax/data devices are actually deployed, how many compression licenses are available, are all possible subscriber/access circuits configured for compression, how frequently are conferences used), a mixed calculation can be performed.

The load as a function of a sample size can only be used if it is ensured that all IPDA components are configured exclusively for this sample size. Otherwise,

the worst value for the respective codec type would have to be used for reasons of reliability.

High-priority load of a HG 3500 as a function of the maximum number of B-channels

Table 61: High-priority load of a HG 3500 as a function of the permissible number of B-channels

Maximum permissible number of B-channels	Total Ethernet load at G.711/20ms [Kbps]	Total Ethernet load at G.711/30ms [Kbps]	Total Ethernet load at G.711/60ms [Kbps]
1	89	81	72
2	178	161	145
3	267	242	217
4	356	323	290
5	445	404	362
6	534	484	435
7	623	565	507
8	712	646	580
9	801	727	652
10	890	807	725
11	979	888	797
12	1,068	969	870
13	1,157	1,050	942
14	1,246	1,130	1,015
15	1,335	1,211	1,087
16	1,424	1,292	1,160
17	1,513	1,373	1,232
18	1,602	1,453	1,305
19	1,691	1,534	1,377
20	1,780	1,615	1,449
21	1,869	1,696	1,522
22	1,958	1,776	1,594
23	2,047	1,857	1,667

Maximum permissible number of B-channels	Total Ethernet load at G.711/20ms [Kbps]	Total Ethernet load at G.711/30ms [Kbps]	Total Ethernet load at G.711/60ms [Kbps]
24	2,136	1,938	1,739
25	2,225	2,019	1,812
26	2,314	2,099	1,884
27	2,403	2,180	1,957
28	2,492	2,261	2,029
29	2,581	2,341	2,102
30	2,670	2,422	2,174
31	2,759	2,503	2,247
32	2,848	2,584	2,319
33	2,937	2,664	2,392
34	3,026	2,745	2,464
35	3,115	2,826	2,537
36	3,204	2,907	2,609
37	3,293	2,987	2,682
38	3,382	3,068	2,754
39	3,471	3,149	2,827
40	3,560	3,230	2,899
41	3,649	3,310	2,971
42	3,738	3,391	3,044
43	3,827	3,472	3,116
44	3,916	3,553	3,189
45	4,005	3,633	3,261
46	4,094	3,714	3,334
47	4,183	3,795	3,406
48	4,272	3,876	3,479
49	4,361	3,956	3,551
50	4,450	4,037	3,624
51	4,539	4,118	3,696

Maximum permissible number of B-channels	Total Ethernet load at G.711/20ms [Kbps]	Total Ethernet load at G.711/30ms [Kbps]	Total Ethernet load at G.711/60ms [Kbps]
52	4,628	4,199	3,769
53	4,717	4,279	3,841
54	4,806	4,360	3,914
55	4,895	4,441	3,986
56	4,984	4,522	4,059
57	5,073	4,602	4,131
58	5,162	4,683	4,204
59	5,251	4,764	4,276
60	5,340	4,844	4,348
61	5,429	4,925	4,421
62	5,518	5,006	4,493
63	5,608	5,087	4,566
64	5,697	5,167	4,638
65	5,786	5,248	4,711
66	5,875	5,329	4,783
67	5,964	5,410	4,856
68	6,053	5,490	4,928
69	6,142	5,571	5,001
70	6,231	5,652	5,073
71	6,320	5,733	5,146
72	6,409	5,813	5,218
73	6,498	5,894	5,291
74	6,587	5,975	5,363
75	6,676	6,056	5,436
76	6,765	6,136	5,508
77	6,854	6,217	5,581
78	6,943	6,298	5,653
79	7,032	6,379	5,725

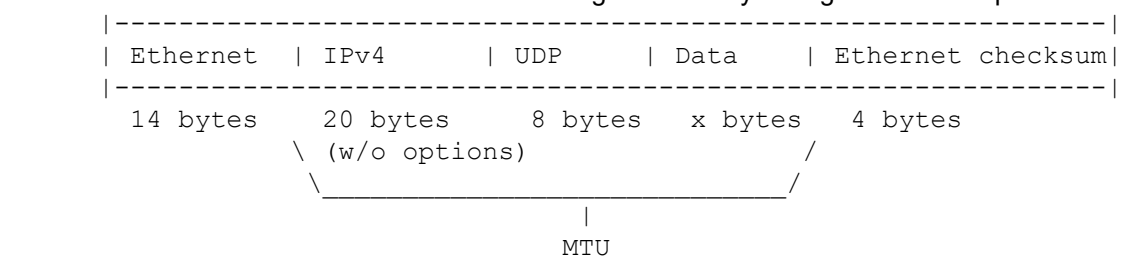
Maximum permissible number of B-channels	Total Ethernet load at G.711/20ms [Kbps]	Total Ethernet load at G.711/30ms [Kbps]	Total Ethernet load at G.711/60ms [Kbps]
80	7,121	6,459	5,798
81	7,210	6,540	5,870
82	7,299	6,621	5,943
83	7,388	6,702	6,015
84	7,477	6,782	6,088
85	7,566	6,863	6,160
86	7,655	6,944	6,233
87	7,744	7,024	6,305
88	7,833	7,105	6,378
89	7,922	7,186	6,450
90	8,011	7,267	6,523
91	8,100	7,347	6,595
92	8,189	7,428	6,668
93	8,278	7,509	6,740
94	8,367	7,590	6,813
95	8,456	7,670	6,885
96	8,545	7,751	6,958
97	8,634	7,832	7,030
98	8,723	7,913	7,103
99	8,812	7,993	7,175
100	8,901	8,074	7,247
101	8,990	8,155	7,320
102	9,079	8,236	7,392
103	9,168	8,316	7,465
104	9,257	8,397	7,537
105	9,346	8,478	7,610
106	9,435	8,559	7,682
107	9,524	8,639	7,755

Maximum permissible number of B-channels	Total Ethernet load at G.711/20ms [Kbps]	Total Ethernet load at G.711/30ms [Kbps]	Total Ethernet load at G.711/60ms [Kbps]
108	9,613	8,720	7,827
109	9,702	8,801	7,900
110	9,791	8,882	7,972
111	9,880	8,962	8,045
112	9,969	9,043	8,117
113	10,058	9,124	8,190
114	10,147	9,205	8,262
115	10,236	9,285	8,335
116	10,325	9,366	8,407
117	10,414	9,447	8,480
118	10,503	9,527	8,552
119	10,592	9,608	8,624
120	10,681	9,689	8,697

10.3.3 Calculation Basis - Configuring Payload Packets

10.3.3.1 MTU Packet

We work with an MTU size of 1500 bytes as standard. An overview is provided below for greater clarity as regards how the packet is assembled:




```
Represented differently:
  1472 bytes payload of ICMP protocol (transport layer)
+    8 bytes ICMP header (transport layer)
+   20 bytes IPv4 header (network layer)
-------------
= 1500 bytes (Ethernet payload) /* for us this is the defined MTU value
+   14 bytes (data link layer header)
+    4 bytes (frame check sequence)
```

```
-------------
= 1518 bytes (complete Ethernet frame)
```

If the MTU size is not permitted to exceed 1500, the OpenScape 4000 can only send a maximum of 1472 bytes as payload for UDP.

In case of a protocol other than UDP (8 bytes), e.g. TCP (20 bytes), the size of the header changes and consequently the resulting size of the payload.

It is therefore okay if a packet length of 1510 bytes, for example, is displayed in a Wireshark Trace. It must then be calculated what the actual length (less overhead) is.

NOTICE: The MSS Clamping procedure can also be used for changing the MTU packet size. MSS Clamping is used in the WAN and automatically adapts the TCP packet size in dialog between the router and the OpenScape 4000 host or access point.

10.3.3.2 Configuring Ethernet MAC Frames

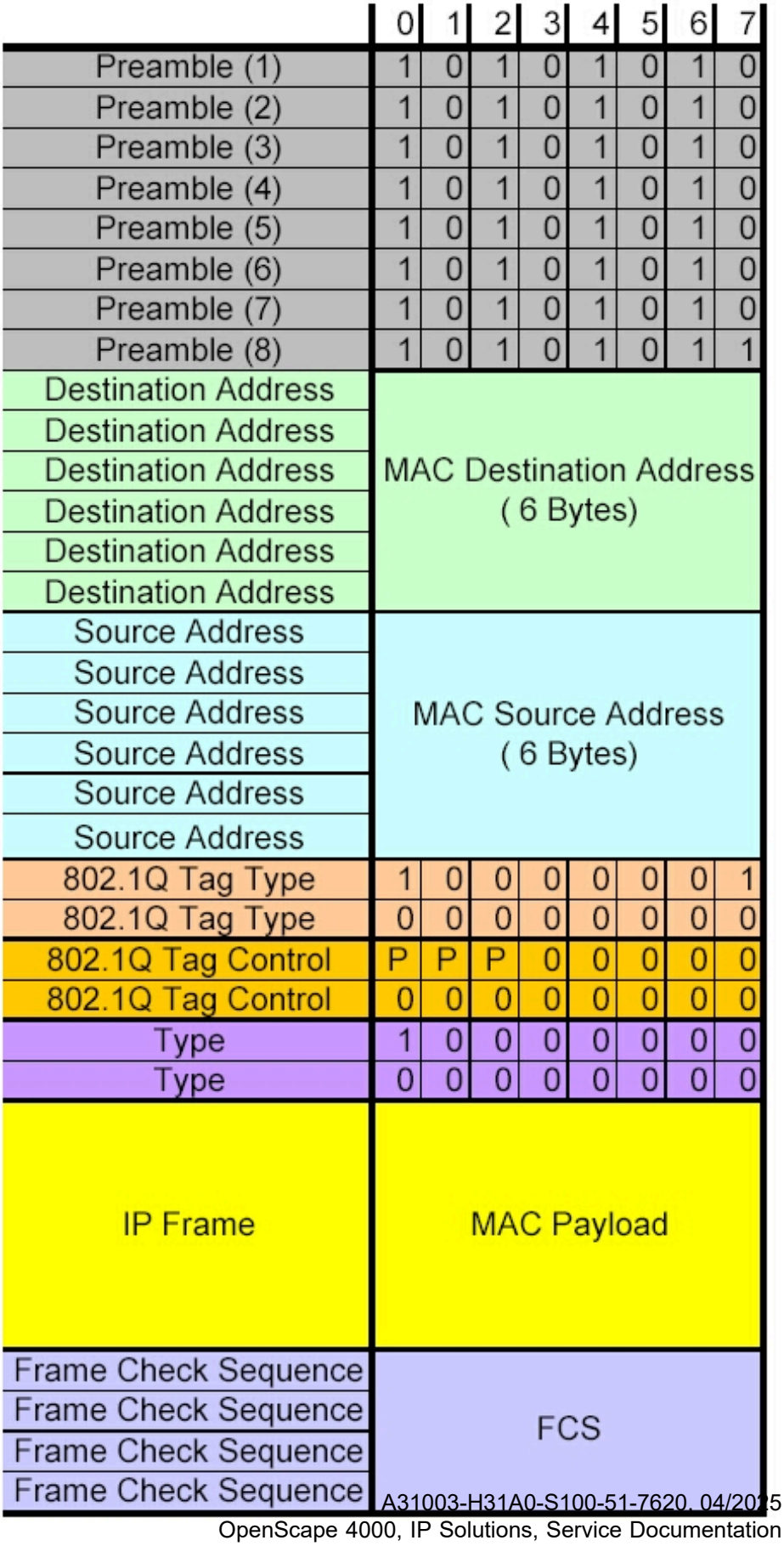
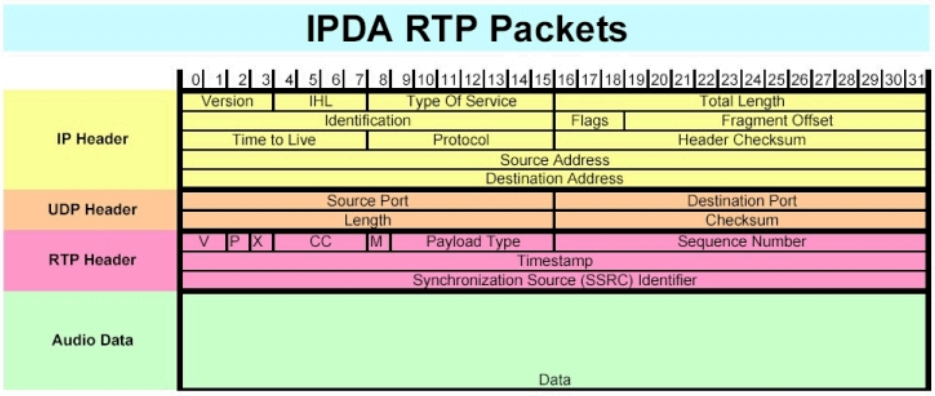


Table 62: Configuring Ethernet MAC frames for IPDA payload

10.3.3.3 Configuring IP Frames



Version	Version of Internet Header	4
IHL	Internet Header Length	20
Type Of Service	Type of Service / Packet Handling Behavior Class acc. To DiffServ - Administrated Value	
Total Length	Length of IP datagram including header	160/280/400/520 for G.711 with 15/30/45/60 msec Audio 60/80/100 for G.729 with 20/40/60 msec Audio
Identification	ID to assemble fragments of datagram	
Flags	set to May fragment, Last fragment	0
Fragment Offset	sent unfragmented -> no offset	0
Time to Live	decremented by each instance the datagram passes	
Protocol	UDP	17
Header Checksum	Checksum on IP Header only	
Source Address	IP Address	
Destination Address	IP Address	
Source Port		
Destination Port		
Length	Length of UDP datagram including UDP header	140/260/380/500 for G.711 with 15/30/45/60 msec Audio 40/60/80 for G.729 with 20/40/60 msec Audio
Checksum	Checksum over IP Header, UDP Header und UDP Data	
V	Version of RTP	2
P	Padding	0
X	Extension	0
CC	Contributing Source (CSRC) identifiers	0
M	Marker	0
Payload Type	Payload Type (G.711 µ-law = PCMU = 0 / G.711 A-law = PCMA = 8 / G.729A = ???)	0/8/18
Sequence Number	Incremented by 1 with each RTP packet - initial value is random	
Timestamp	Timestamp for 1st sample in packet - incremented by 1 for each sampling period - every 125 µsec	
Synchronization Source (SSRC) Identifier	chosen randomly, valid only per session	

Table 63: Configuring IP frames for IPDA payload

10.4 Local Access Point Administration at CLI via Terminal

If an LCT/service PC running “Expert Access“ is not available for the local configuration of an access point, the administration may also be performed directly via a terminal or terminal emulation, if necessary.

The RS 232 / V.24 interface at the 3575 is labeled with “Service“ and is set to 38400 Baud, 8 Bit, no Parity.

The Command Line Interface issues the following message after you press

=:

Please log in.

Username:

Login data

1) new board (before installation)

2) Login: HP4K-DEVEL

Password: 4K-admin

3) after installation (OpenScape 4000 steuert NCUI4)

4) Login: TRM

Password: HICOM

If the module was already in operation and if the WBM login and password were changed, then the values set apply.

The following is displayed after successful login:

Welcome to the HG 3575 V4.0 <currently loaded LW-version> Command Line Interpreter.

vxTarget>

After the prompt, the necessary parameters can now be entered.

A list of available commands can be now requested via the local help function which is available via the `help` command.

The CLI does not distinguish between “direct link“ and “networked“ access points. The designation of the parameters reflects the programming name of the loadware. As already mentioned, direct operation of the CLI without the “Expert Access“ application is only an emergency solution.

The following tables are intended to assist in finding the correct content for the parameters. The tables list the requisite CLI parameters and arrange them in relationship to the AMO parameters from which the values have to be derived:

10.4.1 Networked access point

IMPORTANT: In order to be able to carry out the following commands, you will need ADMIN rights in CLI.

Table 64: CLI parameter for “networked“ access point

CLI parameter name	Parameter meaning	AMO - Branch - Parameter
ip_addr_eth	IP address of the access point	APRT TYPE=APNET - APIPADDR
netmask_eth	Netmask in the network of the access point	APRT TYPE=APNET - NETMASK
default_gateway	IP address of the default router in the network of the access point	UCSU UNIT=AP - APRTADDR

CLI parameter name	Parameter meaning	AMO - Branch - Parameter
ip_addr_signaling	IP address of the access point	APRT TYPE=APNET - APIPADDR
netmask_signaling	Netmask in the network of the access point	APRT TYPE=APNET - NETMASK
ip_addr_CC_A	IP address of the CC-A	SIPCO TYPE=LSNET - CCAADDR
ip_addr_CC_B	IP address of the CC-B	SIPCO TYPE=LSNET - CCBADDR
netmask_hhs	OpenScape 4000 LAN segment netmask	SIPCO TYPE=LSNET - NETMASK
vlan_tag	VLAN tagging on/off [0 = OFF,1 = ON]	STMIB: MTYPE=NCUI2, TYPE=IFDATA - VLAN
vlan_id	VLAN ID [0.. 4095]	STMIB: MTYPE=NCUI2, TYPE=IFDATA - VLANID
eth_link_mode	Ethernet interface operating mode 0 : Autonegotiation 21 : 10 Mbps half duplex 22 : 10 Mbps full duplex 23 : 100 Mbps half duplex 24 : 100 Mbps full duplex	STMIB: MTYPE=NCUI2, TYPE=IFDATA - BITRATE AUTONEG: Autonegotiate 10MBHD: 10 Mbps, half duplex 10MBFD: 10 Mbps, full duplex 100MBHD: 100 Mbps, half duplex 100MBFD: 100 Mbps, full duplex

Note

For “networked“ access points

1) ip_addr_signaling = ip_addr_eth

and

1) netmask_signaling = netmask_eth

must be set!

The command syntax is

1) `set ip address` *Parameter name Value* or `set id` *Parameter name Value*

   For Access Point 99 from the configuration examples (see Figure 12 “OpenScape 4000 LAN segment” and Figure 14 “Configuring a “networked“ access point”), the following command syntax is yielded:

   ```
   get write access set ip address ip_addr_eth
   192.168.23.99 set ip address netmask_eth 255.255.255.0
   set ip address default_gateway 192.168.23.1 set
   ip address ip_addr_signaling 192.168.23.99 set ip
   address netmask_signaling 255.255.255.0 set ip address
   ip_addr_CC_A 192.168.1.1 set ip address ip_addr_CC_B
   192.168.1.1 set ip address netmask_hhs 255.255.255.0 set
   id vlan_tag 0 set id vlan_id 0 set id eth_link_mode 0
   finish
   ```

   IMPORTANT: No other commands (e.g. `show`) may be transmitted between the `set` commands and the `finish` command, which transfers the data to the Flash memory.

10.4.2 Direct link access point

IMPORTANT: In order to be able to execute the following commands, you will need ADMIN rights in CLI.

Table 65: CLI parameters for “direct link“ access point

CLI parameter name	Parameter	AMO - Branch - Parameter
ip_addr_eth	IP address of the access point in the OpenScape 4000 LAN segment	UCSU UNIT=AP - LSRTADDR
netmask_eth	OpenScape 4000 LAN segment network mask	SIPCO TYPE=LSNET - NETMASK
default_gateway	IP address of the default router in the OpenScape 4000 LAN segment	UCSU UNIT=AP - APRTADDR
ip_addr_signaling	IP address of the access point in the internal AP network segment	APRT TYPE=APNET - APIPADDR
netmask_signaling	Netmask of the internal AP network segment	APRT TYPE=APNET - NETMASK
ip_addr_CC_A	IP address of the CC-A	SIPCO TYPE=LSNET - CCAADDR

CLI parameter name	Parameter	AMO - Branch - Parameter
ip_addr_CC_B	IP address of the CC-B	SIPCO TYPE=LSNET - CCBADDR
netmask_hhs	OpenScape 4000 LAN segment network mask	SIPCO TYPE=LSNET - NETMASK
vlan_tag	VLAN tagging on/off [0 = OFF,1 = ON]	STMIB: MTYPE=NCUI2, TYPE=IFDATA - VLAN
vlan_id	VLAN ID [0.. 4095]	STMIB: MTYPE=NCUI2, TYPE=IFDATA - VLANID
eth_link_mode	Ethernet interface operating mode 0 : Autonegotiation 21 : 10 Mbps half duplex 22 : 10 Mbps full duplex 23 : 100 Mbps half duplex 24 : 100 Mbps full duplex	STMIB: MTYPE=NCUI2, TYPE=IFDATA - BITRATE AUTONEG: Autonegotiate 10MBHD: 10 Mbps, half duplex 10MBFD: 10 Mbps, full duplex 100MBHD: 100 Mbps, half duplex 100MBFD: 100 Mbps, full duplex

The command syntax is

1) `set ip address` *Parameter name Value* or `set id` *Parameter name Value*

For Access Point 17 from the configuration examples (see Figure 12 “OpenScape 4000 LAN segment” and Figure 15 “Configuring a “Direct Link“ access point”), the following command syntax is yielded:

```
get write access set ip address ip_addr_eth 192.168.1.17
set ip address netmask_eth 255.255.255.0 set ip
address default_gateway 192.168.1.254 set ip address
ip_addr_signaling 192.168.200.1 set ip address
netmask_signaling 255.255.255.252 set ip address
ip_addr_CC_A 192.168.1.1 set ip address ip_addr_CC_B
192.168.1.2 set ip address netmask_hhs 255.255.255.0 set
id vlan_tag 0 set id vlan_id 0 set id eth_link_mode 0
finish
```

IMPORTANT: No other commands (e.g. `show`) may be transmitted between the `set` commands and the `finish` command, which transfers the data to the Flash memory.

10.4.3 Assignment of parameter names in LW-CLI to the AMO parameters

Finally, the following table provides an overview of all CLI parameters and their assignment to AMO parameters.

Table 66: Assignment of parameter names in LW-CLI to the AMO parameters

Parameter name in LW-CLI		Parameter name	AMO	Branch
ip_addr_eth	*	APDL: LSRTADDR APNW: APIPADDR	UCSU APRT	UNIT=AP TYPE=APNET
netmask_eth	*	APDL: NETMASK APNW: NETMASK	SIPCO APRT	TYPE=LSNET TYPE=APNET
default_gateway	*1	APRTADDR	UCSU	UNIT=AP
ip_addr_signaling	*	APIPADR	APRT	TYPE=APNET
netmask_signaling	*	NETMASK	APRT	TYPE=APNET
ip_addr_survivability	*2	SURVNET (last byte identical to LTU - UCSU)	SIPCO	TYPE=LSNET
netmask_survivability	*2	fix: 255.255.255.0	-	-
gateway_survivability	*2	SURVNET (last byte identical to ROUTERNO - TYPE=SURV -APRT)	SIPCO	TYPE=LSNET
netmask_hhs	*	NETMASK	SIPCO	TYPE=LSNET
ip_addr_CC_A	*	CCAADDR	SIPCO	TYPE=LSNET
ip_addr_CC_B	*3	CCBADDR	SIPCO	TYPE=LSNET
vlan_tag		VLAN	STMIB	MTYPE=NCUI2 TYPE=IFDATA
vlan_id		VLANID	STMIB	MTYPE=NCUI2 TYPE=IFDATA
eth_link_mode		BITRATE	STMIB	MTYPE=NCUI2 TYPE=IFDATA
debug_details		DEBUGDET	STMIB	MTYPE=NCUI2 TYPE=DEBUG
file_access_mode		FACCMODE	STMIB	MTYPE=NCUI2 TYPE=DEBUG
server_port_signaling		fix: 4000	-	-

Parameter name in LW-CLI		Parameter name	AMO	Branch
keep_alive_time_signal		ALVTIME	SIPCO	TYPE=TIMING
reset_timer_sign_loss		RESTIME	SIPCO	TYPE=TIMING
server_port_supervisory		fix: 4001	-	-
tos_lan		TOSLAN	STMIB	MTYPE=NCUI2 TYPE=IFDATA
tos_modem		TOSMODEM	STMIB	MTYPE=NCUI2 TYPE=IFDATA
survivability_enable	*2	derived from ip_addr_survivability > 0.0.0.0	-	-

*	Requisite parameters for first-time initialization of NCUI2/4
***1**	Requisite parameters for first-time initialization of NCUI2/4 *for "networked" access points*
***2**	Requisite parameters for first-time initialization of NCUI2/4 *with signaling survivability*
***3**	Requisite parameters for first-time initialization of NCUI2/4 at *duplex systems*

In the case of some parameters, a distinction must be made according to the type of connection configured CONNTYPE - UNIT=AP - UCSU. In this case, different assignments are required for APDL and APNW.

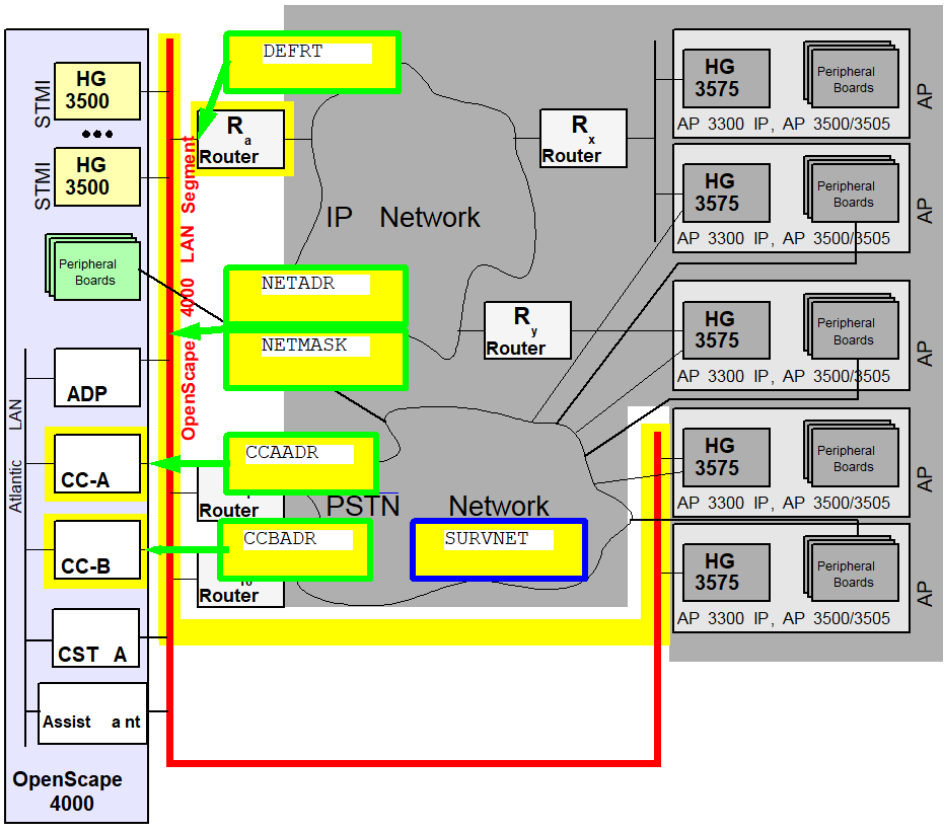
10.5 Spreadsheets - IPDA Configuration

The following spreadsheets are designed to help you perform an IPDA configuration. Each of the sheets has a configuration diagram and a blank AMO template on one side, and the completed example from the Service Manual on the other.

The following spreadsheets (with example) are available:

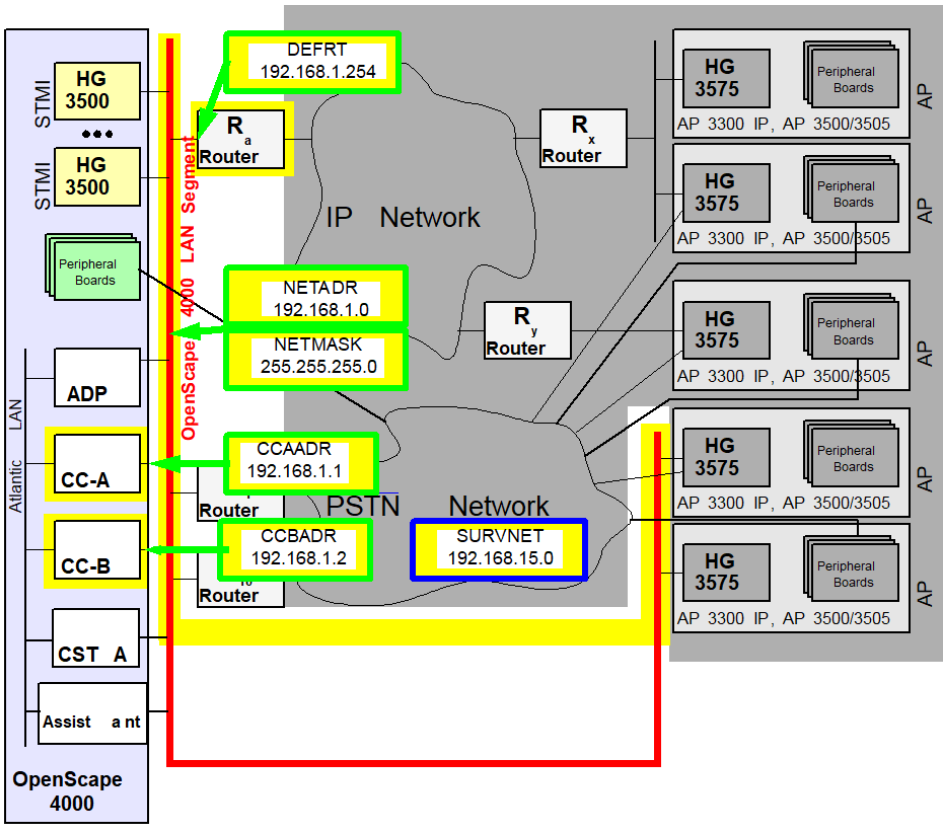
- Spreadsheet: Configuring the OpenScape 4000 LAN segment
- Spreadsheet: Configuring a "networked" access point
- Spreadsheet: Configuring a "direct link" access point
- Spreadsheet: Configuring HG 3500 as HG3570 in the OpenScape 4000 system

Spreadsheet: Configuring the OpenScape 4000 LAN segment



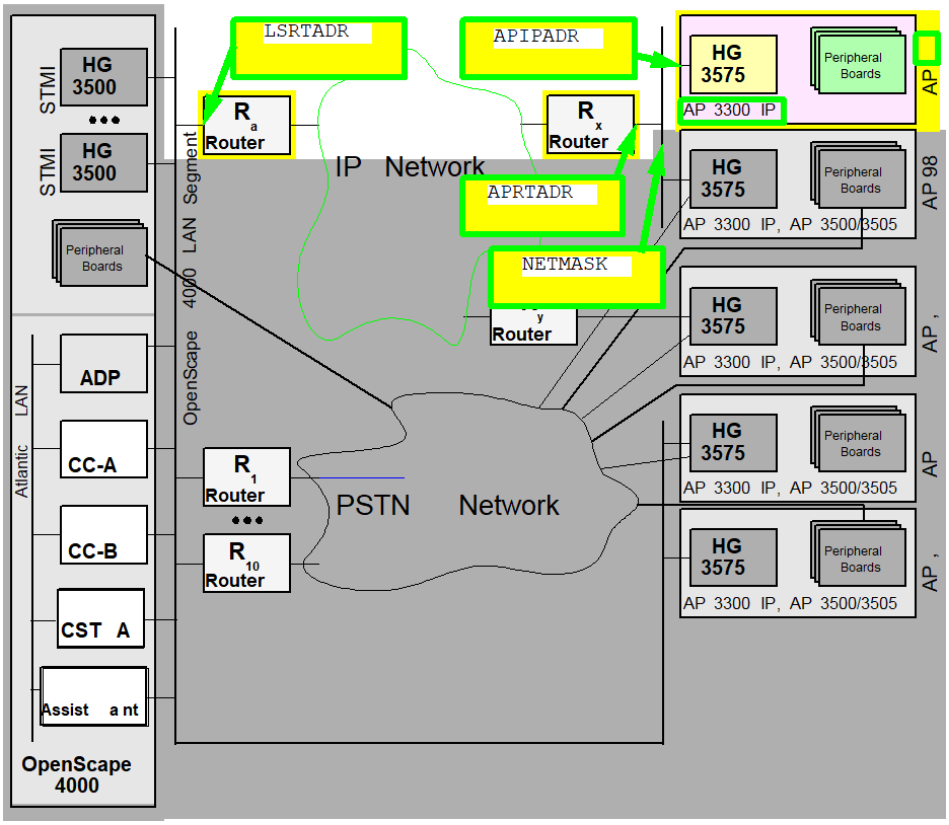
ADD-SIPCO:	NETADDR= . . . ,	NETMASK= . . . ,
	DEFRT= . . . ,	CCAADDR= . . . ,
	CCBADDR= . . . ,	SURVNET= . . .0;

Sample Sheet: Configuring the OpenScape 4000 LAN segment



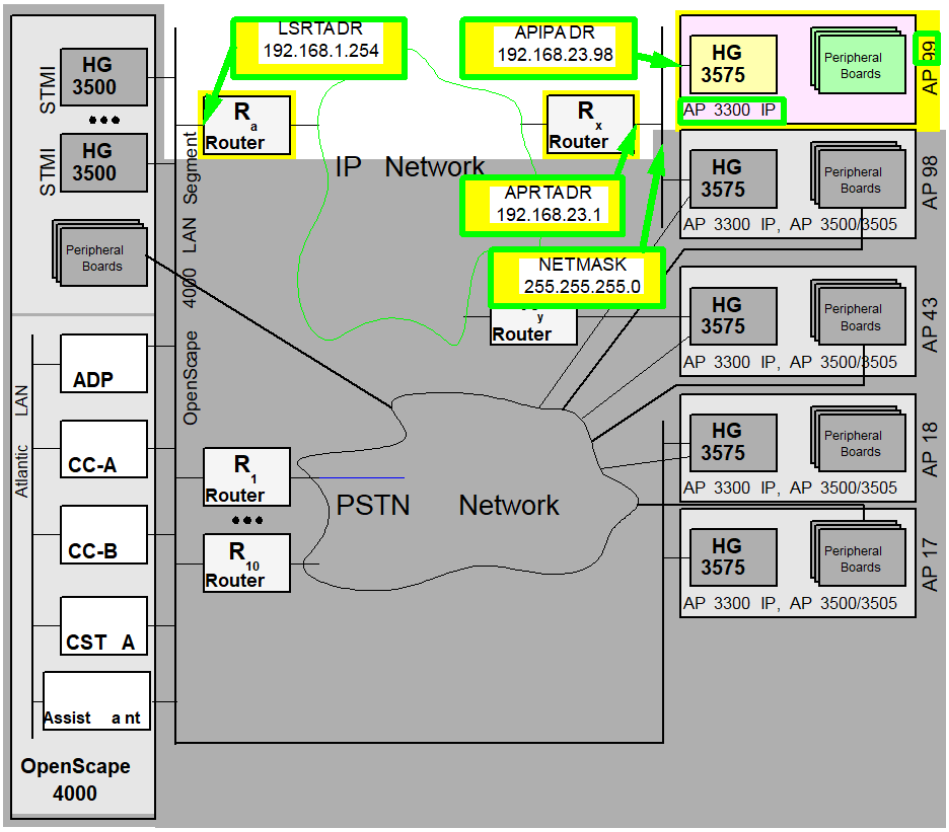
ADD-SIPCO:	NETADDR=192.168.1.0,	NETMASK=255.255.255.0,
	DEFRT=192.168.1.254,	CCAADDR=192.168.1.1,
	CCBADDR=192.168.1.2,	SURVNET=192.168.15.0;

Spreadsheet: Configuring a “networked“ access point



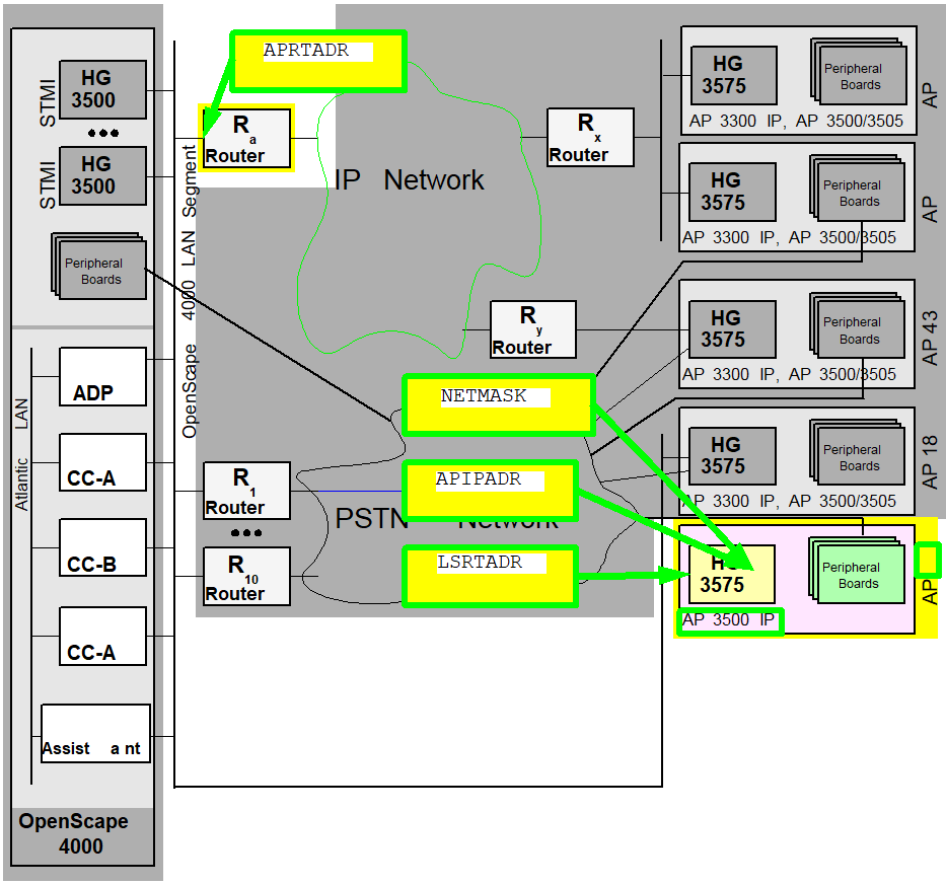
ADD-UCSU:	UNIT=AP,	LTU= ,
	LTPARTNO=Q23 -X ,	SRCGRP= ,
	FRMTYPE= ,	CONNTYPE=APNW,
	LSRTADDR= . . . ,	APRTADDR= . . . ,
	LOCID= ,	LOCATION=“ “,
	PHONE= ,	FAX= ,
	PLCHECK= ,	BCHLCNT= ,
	CONVLAW= ;	
ADD-APRT:	TYPE=APNET,	LTU= ,
	APIPADDR= . . . ,	NETMASK= . . . ;

Sample Sheet: Configuring a “networked“ access point



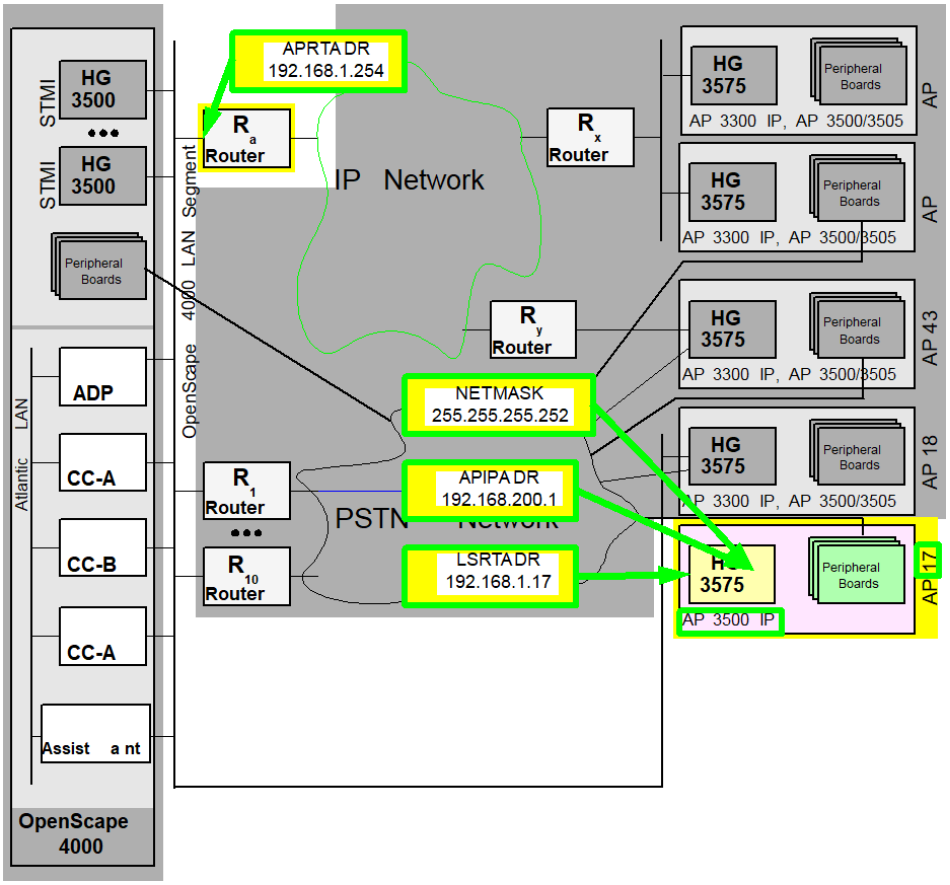
ADD-UCSU:	UNIT=AP,	LTU=99,
	LTPARTNO=Q2305-X35,	SRCGRP=2,
	FRMTYPE=AP 9837009,	CONNTYPE=APNW,
	LSRTADDR=192.168.1.254,	APRTADDR=192.168.23.1,
	LOCID=2,	LOCATION=“BLN ROHRDAMM 85. GEB. 30-222“,
	PHONE=03038612345,	FAX=03038654321,
	PLCHECK=YES,	BCHLCNT=40,
	CONVLAW=NO;	
ADD-APRT:	TYPE=APNET,	LTU=99,
	APIPADDR=192.168.23.99,	NETMASK=255.255.255.0;

Spreadsheet: Configuring a “direct link“ access point



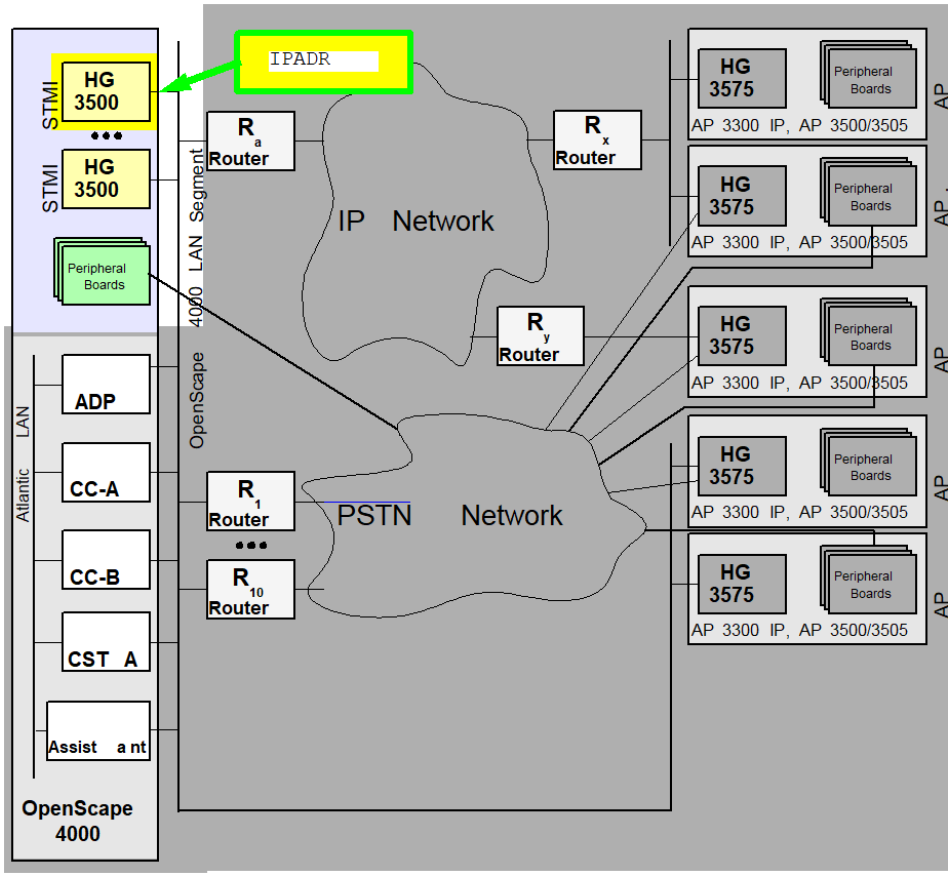
ADD-UCSU:	UNIT=AP,	LTU= ,
	LTPARTNO=Q23 -X ,	SRCGRP= ,
	FRMTYPE= ,	CONNTYPE=APDL,
	LSRTADDR= . . . ,	APRTADDR= . . . ,
	LOCID= ,	LOCATION=“ “,
	PHONE= ,	FAX= ,
	PLCHECK= ,	BCHLCNT= ,
	CONVLAW= ;	
ADD-APRT:	TYPE=APNET,	LTU= ,
	APIPADDR= . . . ,	NETMASK= . . . ;

Sample Sheet: Configuring a “direct link“ access point



ADD-UCSU:	UNIT=AP,	LTU=17,
	LTPARTNO=Q2302-X10,	SRCGRP=1,
	FRMTYPE=INCH19,	CONNTYPE=APDL,
	LSRTADDR=192.168.1.17,	APRTADDR=192.168.1.254,
	LOCID=1,	LOCATION=“MCH MACHTLFINGERSTR.1 GEB. 7202-111“,
	PHONE=08972223456,	FAX=08972265432,
	PLCHECK=YES,	BCHLCNT=20,
	CONVLAW=NO;	
ADD-APRT:	TYPE=APNET,	LTU=17,
	APIPADDR=192.168.200.1,	NETMASK=255.255.255.252;

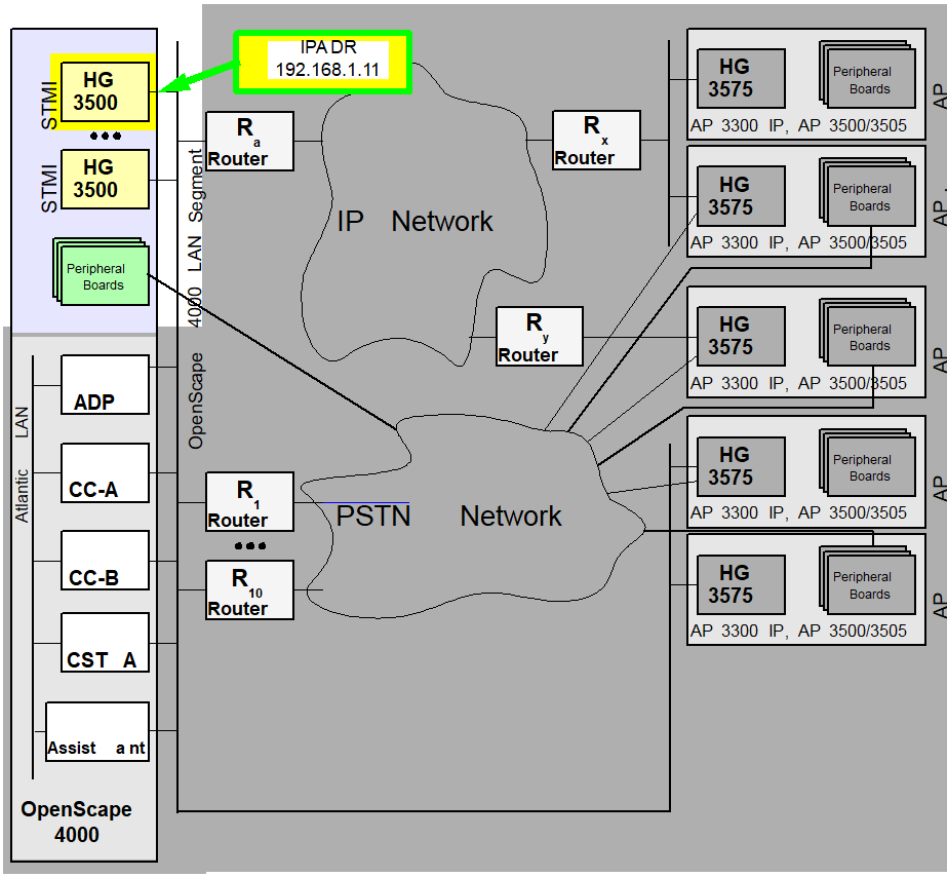
Spreadsheet: Configuring HG 3500 as HG3570 in the OpenScape 4000 system



ADD-BFDAT:	FCTBLK= ,	FUNCTION=HG3570,
	BRDBCHL= ;	
CHANGE-BFDAT:	CONFIG=CONT,	FCTBLK= ,
	FUNCTION= ,	BCHLCNT= ;
CHANGE-BFDAT:	CONFIG=OK,	FCTBLK= ,
	ANSW= ;	
ADD-BCSU:	MTYPE=IPGW,	LTU= ,
	SLOT= ,	PARTNO=Q23 -X ,
	FCTID= ,	FCTBLK= ,
	IPADR= . . . ,	BCHL3570= ;
CHANGE-BCSU:	TYPE=HWYBDL,	LTU= ,
	SLOT= ,	PARTNO=Q23 -X ,

	HWYBDL=A;	

Sample Sheet: Configuring HG 3500 as HG3570 in the OpenScape 4000 system



ADD-BFDAT:	FCTBLK=1,	FUNCTION=HG3570,
	BRDBCHL=BCHL60&BCHL120;	
CHANGE-BFDAT:	CONFIG=CONT,	FCTBLK=1,
	FUNCTION=HG3570,	BCHLCNT=40;
CHANGE-BFDAT:	CONFIG=OK,	FCTBLK=1,
	ANSW=YES;	
ADD-BCSU:	MTYPE=IPGW,	LTU=5,
	SLOT=91,	PARTNO=Q2316-X,
	FCTID=1,	FCTBLK=1,
	IPADR=192.168.1.11,	BCHL3570=40;
CHANGE-BCSU:	TYPE=HWYBDL,	LTU=5,

	SLOT=91,	PARTNO=Q2316-X,
	HWYBDL=A;	

10.6 Information for network administrators

10.6.1 Central Processor

Every central processor receives an additional LAN interface for controlling access points when an IPDA system is installed.

PHY	1GBit - autosensing or can be permanently set
MAC address	Permanently programmed on the interface card, ->sticker
IP address	Configured in the OpenScape 4000 system, can be set
IEEE 802.1 p/q VLAN tagging	Configurable; priority bits are always set when active. See Table 3 “TOS values” in document “Gateways HG 3500 and HG 3575”. The VLAN ID can be set. Configuration in the OpenScape 4000 system.
TOS/DiffServ	The six highest bits in the TOS byte can be set. See Table 3 “TOS values” in document “Gateways HG 3500 and HG 3575”. Configuration in the OpenScape 4000 system.
Protocols/ports	See Chapter 20, “IP Ports” in the document “Gateways HG 3500 and HG 3575”.
Routing	A host route that is configured in the OpenScape 4000 system is used to every access point. No default route.
Firewall	The central processor only allows connections to addresses that it knows, i.e. access points or assigned service PCs.
Number of connections	Up to 166 TCP/IP connections (two per access point)

In large systems, two redundant central processors are installed, one of which is always active. Every processor has its own IP network connection with its own IP and MAC address. PHY is active in the processor. However, the processor does not receive and send packets.

10.6.2 HG 3500 Voice Gateway

IMPORTANT: IP packets with the used ports (hard-coded and configured using AMOs) must be routed transparently in the IP network, i.e. the packets must not be manipulated, e.g. by a firewall). Functional problems can be the result of non-transparent routing!

These boards are installed in the OpenScape 4000 central system. A maximum of 83 HG 3500 boards can be configured in a system.

PHY	10/100 Base T - autosensing or can be permanently set
MAC address	Permanently programmed on the board, ->sticker
IP address	Configured in the 4000 system, can be set. It must be in the same network segment as the central processor. The address is assigned to the slot in the system. When a board is exchanged, the new one automatically adopts the IP address.
IEEE 802.1 p/q VLAN tagging	Configurable; priority bits are always set when active. See Table 3 “TOS values” in document “Gateways HG 3500 and HG 3575”. The VLAN ID can be set. Configuration in the OpenScape 4000 system.
TOS/DiffServ	The six highest bits in the TOS byte can be set. See Table 3 “TOS values” in document “Gateways HG 3500 and HG 3575”. Configuration in the OpenScape 4000 system.
Protocols/ports	See Chapter 20, “IP Ports” in the document “Gateways HG 3500 and HG 3575”.
Routing	Routing table configured in the OpenScape 4000 system with a default route and up to eight additional routes. Routing is identical for all HG 3500s in the system.
Number of connections	Up to 30/60/120 RTP and RTCP connections to any access points, depending on the hardware used. Connection setup controlled completely from OpenScape 4000. H.323 Fast Connect for direct media connections outside the IPDA gateway network, no gatekeeper necessary. See Section 3.2, “Load Calculation for a HG 3500” for connection bandwidths.

10.6.3 Access Points with HG 3575

An HG 3575 is used as the central board for each access point. Access points are only connected to the central system via IP. A maximum of 83 access points can be configured in a system.

As regards addresses, a distinction must be made between “networked“ and “direct link“ access points.

“Networked“ access points are in a different network segment to the central system and can therefore only be reached via a router.

“Direct Link“ access points are connected in the same network segment as the central system.

The OpenScape 4000 system is used for configuring addresses and the port settings. The access point is stored locally. The parameters must be set locally for initial startup.

PHY	10/100 Base T - autosensing or can be permanently set
MAC address	Permanently programmed on the board, ->sticker
IP addresses	See below
IEEE 802.1 p/q VLAN tagging	Configurable; priority bits are always set when active. See Table 3 “TOS values” in document “Gateways HG 3500 and HG 3575”. The VLAN ID can be set. Configuration in the OpenScape 4000 system.
TOS/DiffServ	The six highest bits in the TOS byte can be set. See Table 3 “TOS values” in document “Gateways HG 3500 and HG 3575”. Configuration in the OpenScape 4000 system.
Protocols/ports	See Chapter 20, “IP Ports” in the document “Gateways HG 3500 and HG 3575”.
Routing	Routing table configured in the OpenScape 4000 system with a default route and up to eight additional routes. Routing can be individually set for the access point.

Number of connections	Up to 30/60/120 RTP and RTCP connections to any HG 3500 or access points. Connection setup controlled completely from OpenScape 4000. H.323 Fast Connect for direct media connections outside the IPDA gateway network, no gatekeeper necessary. Up to two TCP/IP connections to the central processor. When using AP Emergency features and a TCP/IP connection to the survivability unit. See Section 3.1, “Load Calculation for Access Points” for connection bandwidths.

IP addresses for “networked“ access points:

IP address of the access point	For signaling, payload, SNMP, FTP, Telnet. See Figure 13 “Difference between “networked“ and “direct link“ access point” Address must be routed in the network.
IP address for signaling survivability	This address remains invisible in the LAN as it is only used for the PPP connection between the survivability router and modem connection of the access point. This address is assigned indirectly by configuring the network address for the virtual survivability network (PPP via ISDN). Only a “private“ address such as 192.168.x.0 should be used here.

IP address for “direct link“ access points:

IP address of the access point	For payload, SNMP, FTP, Telnet, however not for signaling. See Figure 13 “Difference between “networked“ and “direct link“ access point” . Address must be in the same network segment as the central processor. Address must be routed in the network.

IP address for signaling	The signaling connection between the central processor and the access point must pass via a router. See Figure 13 “Difference between “networked“ and “direct link“ access point” . If the LAN connection fails, the current TCP connection is rerouted for signaling survivability. This can only be performed by changing the router whereas the destination address remains the same. An internal router which routes between the access point IP address and the internal address of the signaling instance is therefore used for “direct link“ access points. The IP address for signaling must be in a separate “private“ network segment. It is visible in the LAN (using a sniffer) as the destination address of the signaling packet. However, as signaling packets are routed exclusively from the central processor to the access point IP address via the host route, no router needs to/must route this address in the LAN. Only a “private“ address such as 192.168.x.0 should be used here.
IP address for signaling survivability	This address remains invisible in the LAN as it is only used for the PPP connection between the survivability router and modem connection of the access point. This address is assigned indirectly by configuring the network address for the virtual survivability network (PPP via ISDN). Only a “private“ address such as 192.168.x.0 should be used here.

10.6.4 Redundant LAN Interface

IMPORTANT: Only possible if HG 3500 is configured without WAML function!

Feature requirement

For increased resilience, HG 3500 and HG 3575 boards should be connected with two LAN cables to different switches.

Feature functionality

- Board is starting up:

- If both LAN cables are connected and the HG board is starting up, LAN port 1 will always be activated.

  LAN port 2 will be on , only layer 1 is active (higher protocol layers are down).

  If only one LAN port is connected when the board is starting up (LAN1 or LAN2), that port will be used.
- If the active LAN port is disconnected/disabled by peer or equipment (when both LAN ports are connected):
  - The boards activate the LAN port.
  - The “new” port sends a GRATUITOUS ARP with the same MAC and IP addresses as the “old” port (the second MAC address will only be used if also another feature is configured at the interface (WAML/PPP router)).
  - When the board switches ports, the payload will be lost for < 2 sec – all active connections will be saved and NOT disconnected.
  - The port switch will be logged via OpenScape-4000-F message in HISTA.
  - If the “old” port comes up again, no port switchback will be performed.

Restriction

If the board is configured with FUNCTION=WAML in the AMO BFDAT, LAN port 1 is unable to switch over to LAN port 2 in the event of a fault.

This is because the feature WAML2/WAML Replacement is used for signaling survivability. This prevents the STMI board used from even operating redundant LAN interfaces.

Notes

- The boards only have one IP and MAC address.
- Only one port is active at a time.
- When the board starts up with two connected ports, LAN1 will be activated.
- No port switchback will be performed.
- No configuration in OpenScape 4000 / HG boards is necessary to activate the feature.
- After installation of redundant LAN feature it is recommended to verify the functionality. The test can be performed by unplug the active LAN cable for at least 5 seconds and observe the switchover. The reason for the test is to verify the correct behavior of HG3500 in interaction with redundant IT/LAN infrastructure (e.g. L2 Switches/Router).
- Even if a separate management LAN is configured, LAN redundancy can still be used on STMIX/STMIY if VLANs are used

10.7 IPDA Wizard

The IPDA Wizard provides a step-by-step user interface to help you with IPDA and OpenScape 4000 SoftGate configuration.

You will find the wizard under:

	**Configuration Management > IPDA Wizard**

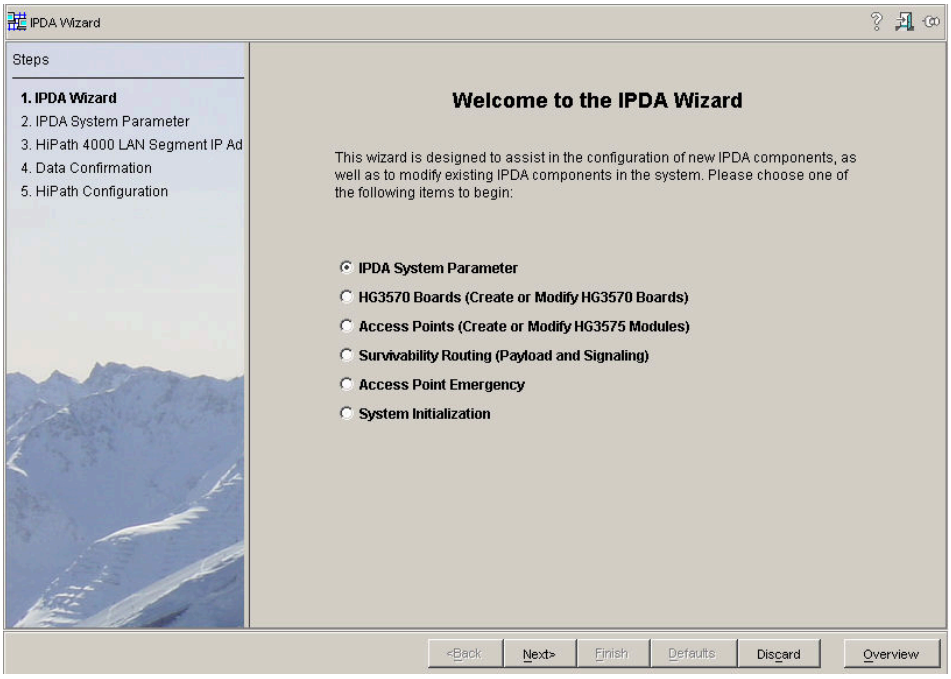


Figure 207: IPDA Wizard - Start page

10.7.1 Functions

You can add or change the following IPDA components:

- **IPDA System Parameter**
- The following functions are available:

  – Configure System IP Addresses

  IP addresses of the OpenScape 4000 LAN segment, central processors, and the default router of the OpenScape 4000 LAN segment.

  – Configure Network Parameters

  Parameters used for transmission bitrate, VLAN tagging and quality of service parameters are configured here.

  – Configure Payload Quality Thresholds

  Configure thresholds (e.g. timers) used to monitor transmissin quality on a connection.
- **HG 3570 Boards (Create or Modify HG 3570 Boards)**
- **Access Points (Create or Modify HG 3575 Modules)**
- With this function you can configure new access points/OpenScape 4000 SoftGates or modify existing access points/OpenScape 4000 SoftGates. It is also possible to configure a new access point/OpenScape 4000 SoftGate by using an already existing access point/OpenScape 4000 SoftGate as template.

  Result Access Point:

  – AMO batch

  - CLI batch (for configuring the NCUI board in the AP)

  Result OpenScape 4000 SoftGate:

  - AMO batch
  - xml file (for configuring the OpenScape 4000 SoftGate)

- **Survivability Routing (Payload and Signaling)**
- Here you can configure alternate routes for the Signaling and payload connections to be used in case the IP network fails.
- **Access Point Emergency**
- With Access Point Emergency, additional control processors at access points (CC-AP) are deployed, which can take over control of a group of access points when these access points have lost connection to the host control processors (CC-A, CC-B) due to network failure or failure oft he host system itself.

  The following functions are available:

  - Configure a local CC for an access point
  - Configure a control processor located in an access point, which will be used in emergency situations.
  - Configure an emergency group

  Configure emergency group specific data, i.e. criteria for switching to emergency mode resp. back and the control processor to be used.

  - Assign an access point to an emergency group

  Here you can assign an individual access point to the emergency groups defined before or change the influence of this AP for switching the group to emergency mode.

  - Configure alternate routing for emergency

  Configure an alternate CO route per source group, which will be used in emergency situations.

- **System Initialization**
- You can perform the following under System Initialization

  - Reset of Boards

  Reload of HG3570 boards and/or access points.

  - Loadware and SIU Files onto Access Points

  Load new loadware onto access points.

  - System Restarts

  Execute Soft- or System-Restart on the OpenScape 4000 Switch.

  - Switch Systemmode

  Switch a system unit to emergency or normal mode.

Button “Overview”

Additionally the assistant provides a graphical overview of the current IPDA configuration.

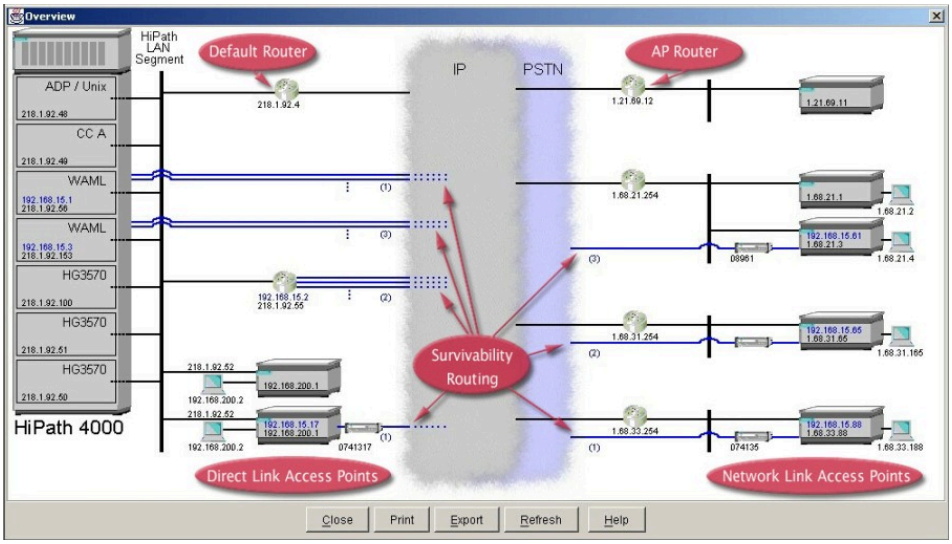


Figure 208: IPDA Wizard - Graphical overview of the current IPDA configuration

10.8 FAQs - Frequently Asked Questions

1) **Question:** Do I actually need a HG 3500 board in the central system for every AP 3300 IP or AP 3500 IP access point?
2) **Answer:** NO, definitely not. It is always assumed that there must be a fixed relationship between a HG 3575 and a HG 3500 to transfer signaling data. However, signaling data comes directly from the central processor (via the SL 200 or SL 100 module). The HG 3500 is only responsible for payload transport. The number of HG 3500s required in the system depends solely on the traffic volume between the access points (total for all APs) and the central system.
3) **Question:** How can I ensure that a HG 3500 crash does not automatically affect associated access points?
4) **Answer:** HG 3500s are not allocated to any specific access points. If there are several HG 3500s in the system, then they share the overall traffic volume. HG 3500 seizure is performed cyclically in the system, i.e. the first connection is routed via the first HG 3500, the next via the second and so on. If an HG 3500 fails, all active calls over this board are interrupted. The board is then no longer seized for new calls. These new calls are then routed via the other HG 3500s, as capacity allows.
5) **Question:** Why are IPDA components not allowed to be connected via hubs?
6) **Answer:** Hubs work in Ethernet’s classic “shared medium“ mode. All connected units share the total bandwidth. Jeder kann alles mithören. Nur einer kann zu einem Zeitpunkt senden. Voice communication is bidirectional. The data flow from A to B is the same size (expect using VAD) as the dataflow from B to A. As transmission is only possible from one unit at a time in shared medium mode, the send and receive direction each occupy the same share of the total bandwidth available. The use of layer 2 switches, which are nowadays often cheaper than hubs, decouples the connection media of the individual units. All units can simultaneously send and receive. The bandwidth (now available for each unit) can be used more efficiently.

7) **Question:** Why are the LAN ports on the IPDA components set by default to *Autonegotiate*? There are many reports that this can lead to problems.
8) **Answer:** The default setting should ensure that initial startup runs relatively smoothly. However, on account of the recurring problems encountered with autonegotiation, we strongly urge you to enter a **fixed** setting for **both** interface partners. It is essential to configure both interfaces - with the same values - at the same time. When using an autonegotiate interface with one that is fixed, the autonegotiate interface often fails to “negotiate“ to the fixed interface’s setting. Please also refer to the Note on page 652.
9) **Question:** Is it necessary to enter the network address for the OpenScape 4000 LAN segment in the AMO SIPCO? Does every OpenScape 4000 need a separate LAN segment or can I operate multiple OpenScape 4000 systems in the same LAN segment?
10) **Answer:** You can operate multiple OpenScape 4000 systems in the same network. In this case, the components’ IP addresses must not be used more than once and the capacity of the router or WAN connection must suffice for the entire bandwidth requirement.
11) **Question:** The effect of default setting recommended by popular router manufacturers and the TOS byte default values documented for IPDA, that is, the pre-defined DiffServ CodePoints (DSCP) is exactly the opposite of the intended effect. The packets we marked as high priority are rejected straightaway by the router. What is this nonsense about?
12) **Answer:** The default values used for IPDA come from an internal standard that was implemented in all HG 35xx gateways. The interoperability problem has since come to light with the result that the company standard will be modified shortly. The default values can be modified at any time and modified in line with actual conditions in the customer network.
13) **Question:** Does IPDA support VLANs?
14) **Answer:** Yes but only in conjunction with priority tagging. In accordance with IEEE 802.1 p/q, tagging was introduced for IPDA to support priority tagging. If tagging is activated then the permanently preset priority bits of the various types of traffic are always set (see the last column of Table 3 “TOS values” in document “Gateways HG 3500 and HG 3575”). If tagging is active, the VLAN ID can also be set (default value is zero). VLAN ID is not supported without the set priority bits.
15) **Question:** Does IPDA support subnetting (RFC 950)?
16) **Answer:** Yes. When the network mask is entered, a check is performed to determine whether the block of ones that has been set meets the minimum length required for the class of the address, i.e. 8 ones for Class A, 16 for B and 24 for C. If the number of ones is greater than the number required for the class, subnetting is activated.
17) **Question:** Does IPDA support supernetting (RFC 1338)?
18) **Answer:** No.
19) **Question:** Can an access point be operated such that signaling is only routed via IP? Voice can be routed as a dial-up connection via ISDN as in the case of payload survivability.
20) **Answer:** Payload survivability is designed as an emergency solution in the event of an IP network crash/malfunction. Only basic call functionality can be guaranteed. You must also take into consideration that signaling via IP must offer Quality of Service which is often not supported when

using external narrowband WAN links together with data communication in existing installations.

Follow-up question: It cannot be that difficult for an ISDN PABX to route voice connections via a carrier network.

Answer: The systems are designed for it. However, in the case described above, the system must call itself via the CO and negotiate this as an internal call with the complete range of features - and this in itself is not an easy task.

21) **Question:** Why does the “direct link“ access point need additional IP addresses? It must be easier to route a call in the same LAN segment than in multiple LAN segments with routers.

22) **Answer:** The reason for the internal router and the additional address is due to signaling survivability. For signaling survivability, TCP layer packets which can no longer be transported via LAN must be delivered on another route, that is, the survivability path, before the supervision timer in the TCP expires. The IP destination addresses must remain the same for this, only the router involved can be switched. In the case of a “networked“ access point, the (default) LAN router is switched to the survivability router. This LAN router is not available in the case of a “direct link“ access point, as CC and AP are in the same LAN segment. You cannot switch from *no* router to a survivability router. Consequently, signaling survivability could not be offered for “direct link“. The only practical solution is to integrate the LAN router in the access point. Two IP addresses are therefore provided for a “direct link“ access point: the router port IP address at the OpenScape 4000 LAN segment and the signaling instance IP address in the AP “internal network“.

23) **Question:** Is it possible to operate the IPDA components in a network that does not support Quality of Service?

24) **Answer:** If the entire network is ideally dimensioned, if there is no packet loss and no significant packet propagation time during long-term measurements and if the network load (including the IPDA load) is moderate on all paths, then an IPDA system will also function in this network without QoS measures. Malfunctions will occur if these conditions are violated, for example, through load displacement or something similar. Constant, highly developed network monitoring is essential in this case to recognize bottlenecks developing in the network and to remove them immediately. If narrowband WAN connections which are also used for data connections and have a high load are utilized in the network used for IPDA, then malfunctions are guaranteed in networks without a QoS functionality for prioritizing IPDA traffic.

25) **Question:** A remote access point is connected via WAN. Transmission capacity is only 800 Kbps. Major interferences occur during peak traffic and the access point sometimes performs restarts. The traffic from/to the access point is prioritized higher compared to parallel, active data traffic. Can the bandwidth seized by OpenScape 4000 on the WAN link be limited to 800 Kbps?

26) **Answer:** The bit rate required by the access point can be limited by the Resource Manager. Table 29 “High-priority load of an AP as a function of the permissible B-channels” provides an overview of the capacity required as a function of the number of connections simultaneously active. The basis for this assumption is calls using the G.711 codec. The signaling load was set to 64 Kbps.

With a sample size of 30 ms (default), nine connections could be used simultaneously to remain under 800 Kbps (792).

Follow-up question: Table 28 “High-priority load of an AP as a function of codec and sample size” shows me that I can transport significantly more B-channels with the available bandwidth if I use the G.729 codec.

Answer: The 800 Kbps available could theoretically transport over 30 B channels if the sample size were set to 40 ms in G.729. However, please note that in this case, all the trunks in the entire system involved in calls must be configured to support G.729 (classmark G729OPT). This is the default setting. All trunks in the access point must also be configured with classmark G729 which necessitates the use of the G.729 codec. This also applies to the conference connection and music-on-hold. However, we advise against configuring the conference unit with G.729 if you want to guarantee the best voice comprehension levels possible for conferences. It should also be noted that the **melody** played back when music-on-hold is active is distorted by the voice compression. In addition, please note that fax machines, modems and ISDN data terminals must not operate with G.729 compression. If these devices are active, 81 Kbps will be seized (30 ms - in this example - with G.711 and 40 ms with G.729) instead of the anticipated 21 Kbps. In other words, the number of B channels in this example must not be set to 30 even with the maximum possible use of G.729. The correct value is between 9 and 30. It depends on how many G.711 connections are still required. If the number of B channels is set too high, **ALL** connections will be affected when the capacity of the WAN link is exceeded. The signaling connection can also be affected and can, depending on the level of interference, cause a switchover to signaling survivability or an access point restart.

27) **Question:** I’d like to dispatch an access point over ISDN. Given that NCUI only provides a LAN connection, I’d like to use a router with an S0 interface. This offers me a bandwidth of 128 Kbps, which is enough for 7 B channels. I estimate the signaling volume to be very low. Should I expect any problems?

28) **Answer:** Yes, you should stay well clear of this configuration. Although 7 B channels require only 114 Kbps with G.729 compression and a sample size of 60 ms, there is good reason for always keeping around 64 Kbps free for signaling. This leaves only around 64 Kbps for payload. That is not sufficient, even if only one call cannot be compressed (fax, modem, ISDN data). See also Question 13.

29) **Question:** I’d like to use a PCM30 router between an access point and OpenScape 4000 LAN segment, thus with a maximum of 2 Mbps of bandwidth available. However, because the customer wants to use dial-up lines through the public telephone network instead of dedicated circuits, the actual bandwidth should be kept as small as possible and only adapted/increased as required. As a minimum, we would provide one channel for the required 64 Kbps signaling. Should I expect any problems?

30) **Answer:** Yes, having “dynamic“ WAN bandwidth will cause problems that can only be resolved with fixed bandwidth. The reason for this is very simple. Let’s assume that the amount of bandwidth currently available is exactly right. Now a call comes through. There is therefore no longer enough bandwidth available. What does the router do? Firstly, it blocks the packets that it can no longer get rid of due to the lack of bandwidth, which affects all connections equally. If the backlog is not cleared within a specific time, it establishes a second 64 Kbps connection in the telephone network.

Once connection setup has been completed, there is once again enough bandwidth available. (If not, a further 64 Kbps are set up.) This requires only a few seconds. During this time, all payload connections are affected as is - if not protected by means of prioritization - the signaling connection.

31) **Question:** How can I check the actual Quality of Service available at an access point? The network operator says that everything is in order. The telephone subscribers complain about sporadic low voice comprehension.

32) **Answer:** The QoS values recorded with the real-time transmission protocol can be checked via SNMP at all HG 3575 and HG 3500 boards. See Chapter 19, “SNMP Support HG 3500 / HG 3575” in the document “Gateways HG 3500 and HG 3575”. OpenScape 4000 Assistant also features an option for recording, evaluating and displaying QoS parameters on a call-by-call basis. See OpenScape 4000 Assistant -> Diagnose -> IPDA Service Access -> Call Quality Recording Viewer, MIB Viewer or QoS Viewer

Follow-up question: According to the network operator, not a single IP packet was lost during the period when there were problems with voice communication. Is there another possible cause for poor voice quality?

Answer: If the network operator delivers packets with a delay greater than the size of the jitter buffer, they are not available for the codec when they are needed. This means that although the packets are being delivered correctly from the network operator’s point of view, they are lost in the real time context of voice transmission.

33) **Question:** Fax and data via Voice over IP connections are very critical. How well does this really work?

34) **Answer:** There are three factors that are relevant here: packet loss, jitter and delay. Modern voice codecs provide acceptable voice quality even with a packet loss of 5% through procedures such as “packet loss concealment“. The packet loss cannot, however, be disguised in the case of fax, modem or ISDN data connections. The throughput declines here due to the number of retransmissions necessary. If packet loss is too high, the connection is cleared down by the terminals. Jitter causes indirect packet loss. Jitter buffer dimensioning is important here. This should be dimensioned as small as possible to keep delays short. However, packets whose deviation from “normal“delays can no longer be compensated for in the jitter buffer are lost. The total number of packets lost in the network or due to high jitter levels should be significantly higher for voice then for fax, modem and data. To satisfy the various traffic type requirements in terms of jitter-specific packet loss (voice < 5%, fax, modem data ~0%), the jitter buffer value set for fax, modem or data connections is increased by 30 ms in the OpenScape 4000 components HG 3500 and HG 3575. The delay on the connection can - depending on the data transfer protocol used - also be critical. If transmission is subject to acknowledgment, the acknowledgment is delayed by the transmission delay which reduces the throughput in contrast to connections that are not delayed. The signal processors evaluate the signaling tones from the connected fax or modem devices when setting up a connection. A distinction is made here between high- and low-speed devices and transmission is optimized accordingly.

35) **Question:** What bit rates are guaranteed by IPDA for fax devices or modems?

36) **Answer:** IPDA is unable to guarantee bit rates higher than those ensured by the OpenScape 4000 central system. That is 14.4 Kbps. Higher bit rates lead to dependencies on the attenuation plan, the attenuation set at the T

reference point, etc. Bit rates above 14.4 Kbps are technically possible in particular constellations but cannot be guaranteed.

37) **Question:** The customer uses an all-in-one device (printer/scanner/modem combo) as a fax machine. Fax connections to conventional fax devices work perfectly. Faxes from identical devices within the IPDA system, however, cause problems.

38) **Answer:** Problem are caused by all-in-one devices that want to improve the transmission speed above and beyond the fax standard. These devices enter the negotiation phase at the start of the fax connection as “normal“ Group 3 fax devices. If they both determine that they both support a proprietary - and faster - transmission method, then they use it. The IPDA gateway problem is like the problem that occurs on remote links. The transmission path is optimized on the basis of the signaling tones that indicate a low bit-rate connection. But the devices decide to use a transmission method with a high bit rate during negotiation. And that causes problems with the path optimized for low bit-rate transmission.

39) **Question:** The Service Manual makes repeated references to the pinging of IP addresses for the IPDA components. I’m now doing it, and it only works sometimes or not at all.

40) **Answer:** There are three factors that influence a successful ping

    - The ping request must reach the destination in order to obtain a response.

    For this to happen, the routing from the port of the computer that sends the ping to the destination must be safeguarded. It is therefore important that ping requests come from known IPDA components (AMO SIPCO, parameter **LSNET** und AMO AART, parameter **APNET**) and not from any other unknown network address segments/devices (e.g. service PC on different network).

    - The ping request must not be rejected by a firewall at the destination.

    The control processors CC-A/CC-B protect themselves from floods of ping requests by allowing only a specific volume of requests per unit of time. The filter is set up so that a standard ping command with approximately 5 requests in intervals of about one second can be responded to without any problems. However, requests that are more frequent or at shorter intervals are rejected. Both CC-A and CC-B will reply.

    - The ping response must come back to the requester to be analyzed.

    For this to happen, the routing from the pinged IPDA component to the computer that sent the ping must be safeguarded. The control processors CC-A/CC-B use specific host routes to the configured devices (in other words, no default route exists to unknown networks on which other devices are connected). AMO SIPCO, parameter **DEFRT** is therefore only used for those specific routes and is not a classic default router.

41) **Question:** I have, on a number of occasions and in different error scenarios, exchanged the NCUI boards “cross-wise“. The error is always repeated. This can’t be right, can it?

42) **Answer:** With the NCUI, cross-wise exchange is very problematic because the local configuration data needs to be changed. If you just exchange the modules without reconfiguring them, you take the LTU number and the entire configuration of the shelf as well. The central system accesses LTU 17 with the configured IP address. If the NCUI module with this address now actually sits in another shelf, this is now LTU 17. You should therefore follow the instructions in Section 2.2.9,

"Information on Exchanging HG 3575 Boards" of the Service Manual when exchanging modules. Cross-wise exchange is also a module exchange. This involves applying the local configuration (with "Expert Access") in exactly the same way as `EXEC-USSU:UPDATAP,LTU Number,UL;`

43) **Question:** From the customer's perspective, an IPDA access point is a device that features both IP and TDM ports. The use of devices of this kind in the customer network is prohibited for security reasons.

44) **Answer:** There is a widespread and logical ban on the operation of PCs that have simultaneous network access to another networks (that cannot be controlled and is not protected by a firewall, etc.) on the LAN. Devices of this kind could be used as "private" gateways in order, for example, to offer a secure dial-in connection to the LAN.

    An IPDA access point used as a gateway for voice connections from TDM <-> IP must have access both to the LAN and to TDM ports.

    The design of the HG 3575 guarantees a distinct separation between the payload functionality and the signaling functionality.

    In the payload part, random TDM <-> TDM or TDM <-> IP <-> TDM connections are set up at the request of the OpenScape 4000 central system. The network consisting of the OpenScape 4000 central system and the IPDA access points provides a TDM operation that, from the outside, appears closed and features an internal IP network for networking the access points.

    If HG 3575 were misused, additional IP connections would be routed from the NCUI, for example via PPP, to TDM connections.

    This is not possible because

    a) the IP stack only responds to a limited number of ports (see Chapter 20, "IP Ports" in the document "Gateways HG 3500 and HG 3575").

    - the signaling unit can access the TDM payload

    The HG 3575 supports PPP but only for a signaling connection over an **external** modem connected using a serial V.24 interface in the case of signaling survivability.

45) **Question:** We measured the mouth-to-ear delay in a voice connection between the OpenScape 4000 central system and an IPDA access point. The delay clearly exhibits a very slow sawtooth pattern. In other words, it falls steadily until it reaches a minimum threshold value and then jumps back to a maximum value and then immediately starts to fall again. What causes this sawtooth process and what can be done about it?

46) **Answer:** You have no digital trunk interfaces in the access point or do not use these for clocking the HG 3575. Without synchronization over digital trunk interfaces in the access point, the clock generators in the OpenScape 4000 central system and the access point become asynchronous, despite the extremely high precision of the free-running clock generator on the HG 3575 (ISO 11 573 class III, TIA stratum 4, CTR4 and CTR12/13). Nevertheless, the unsynchronized clock generators start to diverge over time. In the scenario you measured, the receiver works with a slightly higher clock frequency than the sender. The IP connection starts with the predefined jitter buffer value. As more data is read than sent, the jitter buffer slowly runs idle. This explains the steadily falling mouth-to-ear delay. When the minimum jitter buffer fill level is reached, time is "inserted" at the receive end during which the jitter buffer fills up again. This explains the jump to the maximum value. The converse effect can be observed in the

opposite direction. The mouth-to-ear delay climbs steadily until the upper limit of the jitter buffer is exceeded. Time is then “removed“ and the jitter buffer is reset to the target value.

You can observe this effect in all devices that transfer data at a constant rate over a long period of time without transfer clock synchronization. A solution for the IPDA access points involves synchronizing the central system and all HG 3575 ASCs with a common exchange clock.

47) **Question:** Why are calls from the IPDA to the central VoiceMail server routed over the CO in the case of payload survivability? This doesn’t make any sense. Can this be prevented?

48) **Answer:** VoiceMail systems are not affected by payload survivability. This is explicitly specified as an exception in the sales release for OpenScape 4000 (1st supplement). In this case, calls are not routed over the survivability path (that is the CO).

49) **Question:** Is NAT supported with IPDA?

50) **Answer:** NO.

51) **Question:** Which resources are available per access point (NCUI2+/ NCUI4/OpenScape 4000 SoftGate)?

52) **Answer:**

- 64 TSLs for conference
- 4 receivers for DTMF signaling (CR) - 32 receivers for OpenScape 4000 SoftGate
- 4 sender for DTMF signaling (CS) - 32 sender for OpenScape 4000 SoftGate
- 2 continuous-tone dial tone receivers (DTR-DT)
- 2 cadenced-tone dial tone receivers (DTR-TT)
- 2 test receivers (TESTR)
- 1 test sender (TESTS)
- up to 18 different tones
- 6 different announcements
- 1 music on hold
- 1 TDS port

53) **Question:** I want to change IP addresses during next major version upgrade session (e.g. HiPath 4000 V6 -> OpenScape 4000 V8) on my host system, is there any easy way to achieve this?

54) **Answer:** From HiPath 4000 V6 R2 loadware lines, access points will accept HSR connections from any IP address, so long as there is not one already active (i.e. the IPDA must be in NOT READY status for this to work). This means you can simply change the CCA/CCB address in AMO SIPCO (also NCUI/OpenScape 4000 SoftGate) and the access point will accept the new HSR connection upon next startup. The alternative method listed under Section 2.14, “IP Address Changes”, can still be used for running systems with active HSR connections.

11 Access Point Emergency (APE)

11.1 Access Point Emergency Feature Description

The Access Point Emergency feature lets you maintain operation of Access Points/OpenScape 4000 SoftGates irrespective of whether or not the central system is available.

Options for operating access points/OpenScape 4000 SoftGates from additional, physically separable control systems are provided for this purpose. These additional control systems (survivability units) can be mounted in each AP 3700 IP access point.

In principle, you can control all access points/OpenScape 4000 SoftGates associated with a OpenScape 4000 system from a single survivability unit (depending on the survivability unit’s processor performance). Most of these scenarios avoid the use of “classic“ shelves with a TDM connection and only use IPDA access points or OpenScape 4000 SoftGates.

In the case of the "Survivable OpenScape 4000 SoftGate" feature, the survivability unit is implemented as software on the OpenScape 4000 SoftGates hosts. The survivability unit takes over the operation of its own OpenScape 4000 SoftGate if the central controller fails (e.g. through loss of the IP connection to the central control unit).

We have the following environment:

OpenScape 4000 platform, which is the host for the follwoing virtual machines (VM):

- VM ADP, CCA, CCB, CCAP (RMX)
- VM Assistant
- VM CSTA

11.1.1 Access Point Emergency Implementation Scenarios

11.1.1.1 LAN Scenario

The central control unit - the communication server - is often housed in the main computer center while the access points/OpenScape 4000 SoftGates with the survivability unit is located in the computer center. The access points/ OpenScape 4000 SoftGates are distributed on the campus and networked over a high-availability IP infrastructure. If the communication server in the main computer center is not available, the survivability unit takes over the entire system operation.

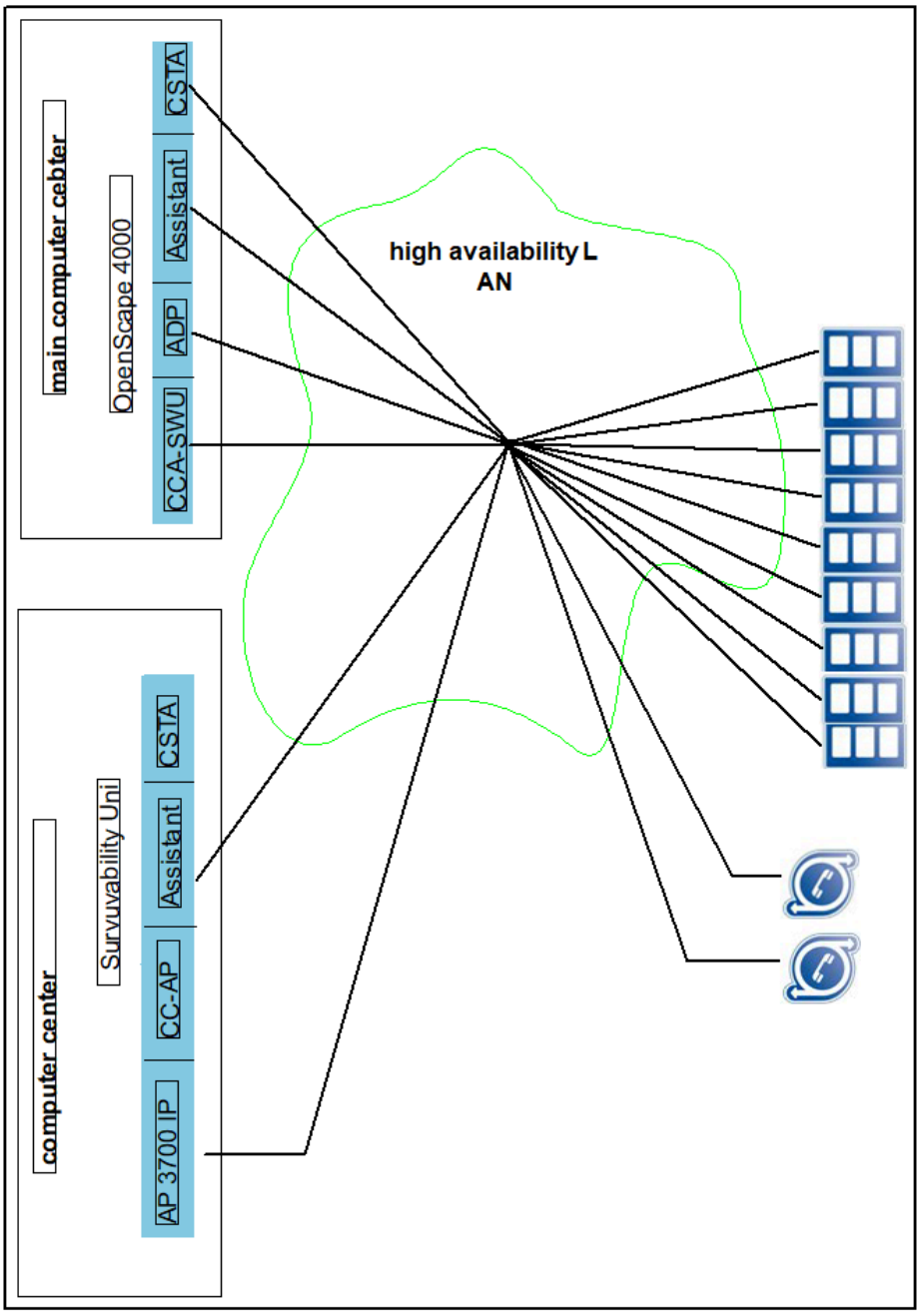


Figure 209: LAN scenario

The survivability unit is indicated by the abbreviation CC-AP in all the following figures and on all operational user interfaces. This is based on the logic used for naming the control processors (CCA-SWU and ADP). Of course not only does the CC-AP run on the survivability unit, rather also - as in the host system - OpenScape 4000 Assistant and OpenScape 4000 CSTA.

11.1.1.2 LAN/WAN Scenario

If the network features WAN routes that connect sites with several IPDA access points/OpenScape 4000 SoftGates, for example, we recommend installing an

individual survivability unit on each of these LAN islands. The access points/ OpenScape 4000 SoftGates can then be operated autonomously not only in the event of a central control unit failure but also if the WAN connection fails.

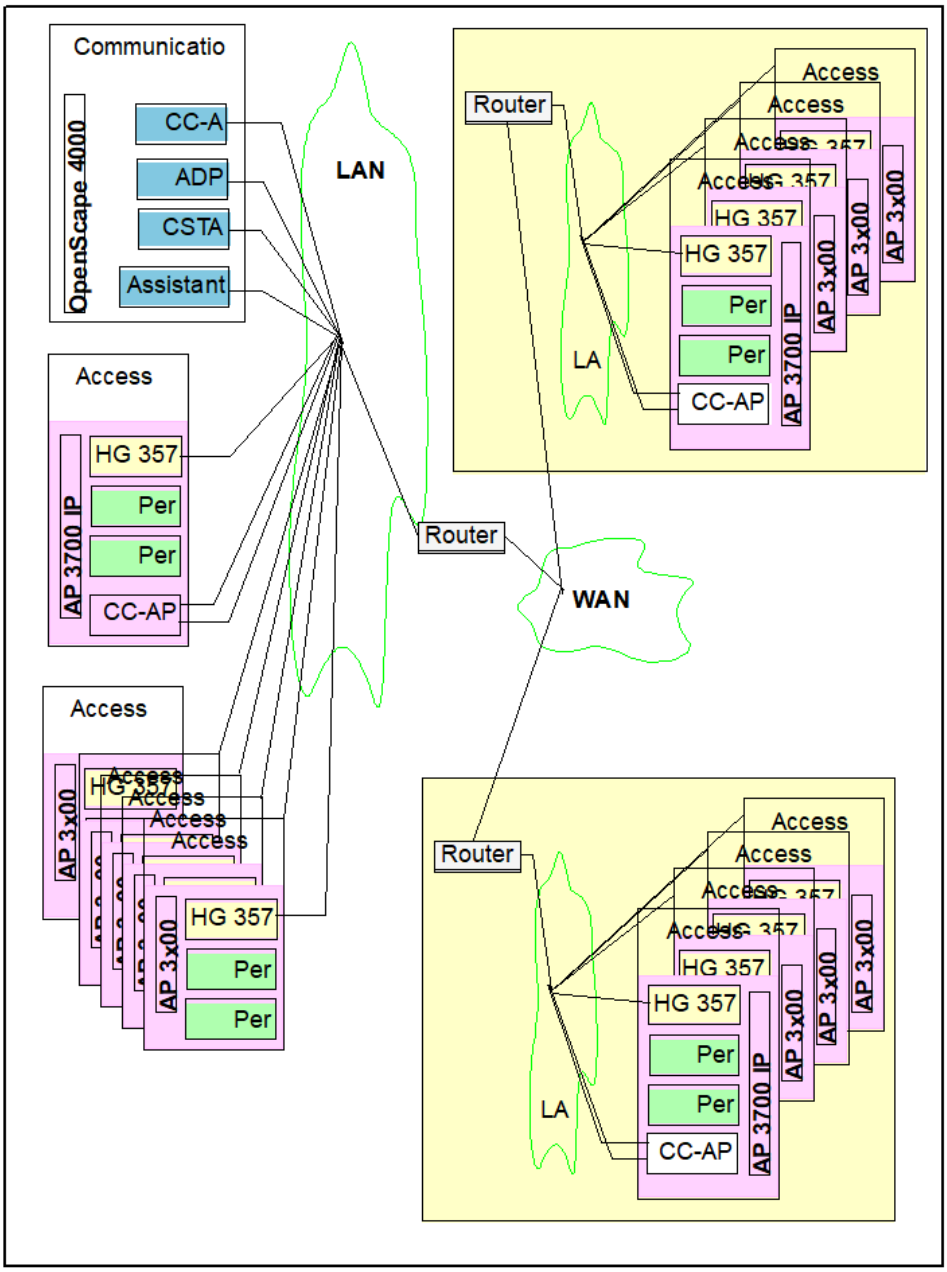


Figure 210: LAN/WAN scenario

11.1.1.3 Branch (WAN) Scenario

In the classic branch structure, numerous relatively small but broadly distributed branches are connected via precisely dimensioned WAN routes to the company's host system. In this scenario, we recommend providing a survivability unit for the IPDA access point/OpenScape 4000 SoftGate in each individual branch. In this way, you can ensure autonomous branch operation in the event of failure of the central control unit or WAN connection.

11.1.2 Access Point Emergency and Signaling Survivability

The AP Emergency feature and the signaling survivability feature are not alternatives. Instead, they complement each other. A reliable layer concept for system stability can be implemented in all scenarios containing WAN routes.

1) Signaling survivability guarantees access point/OpenScape 4000 SoftGate operation over the central control unit in the event of a WAN malfunction. The signaling survivability path is switched over without interruption.
2) AP Emergency takes over access point/OpenScape 4000 SoftGate operation if the central control unit fails.

Notes:

- The HSR signaling connection from the APE to the Access Point/ OpenScape 4000 SoftGate is always only a pure TCP/IP connection as opposed to a "HSR over UDP" connection (regardless of the SIGMODE configuration in AMO UCSU).
- There is always only a single HSR signaling connection over a defined path between the APE and Access Point/OpenScape 4000 SoftGate and no alternative survivability path.

Figure 53 “AP Emergency scenario” illustrates a mixed scenario that will be referred to throughout the manual. In this figure, the broken blue lines represent the communication paths between the central control unit and the access points/OpenScape 4000 SoftGates and the red dotted lines represent communication between the survivability units and the access points/ OpenScape 4000 SoftGates allocated to them.

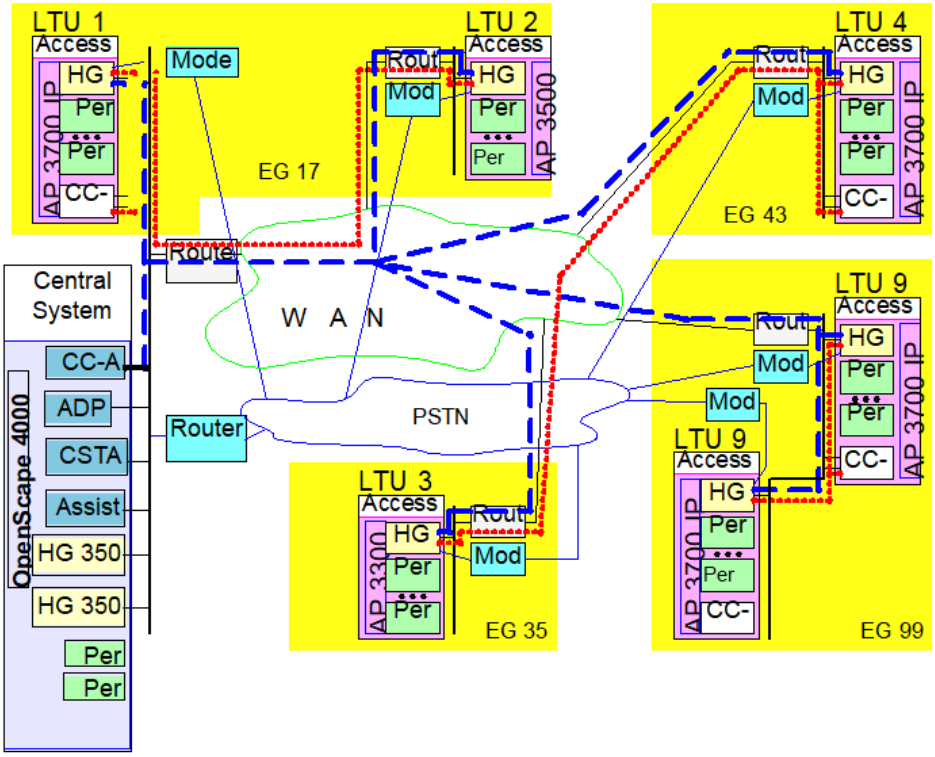


Figure 211: AP Emergency scenario

11.1.3 Survivability Unit in AP 3700 IP

The survivability unit can only be used in AP 3700 IP access points. However, it can control all possible IPDA access point models (AP 3300 IP, AP 3500 IP, AP 3700 IP) and OpenScape 4000 SoftGates. Access points are controlled regardless of whether the access point features NCUI2+ or NCUI4.

The survivability unit consists of a cassette with cPCI backplane, DSCXL2 processor, power supply and redundant fan trays.

Depending on the power supply module, it can be powered with 110/230 V alternating current or 48 V direct current. In AP 3700 IP, there is no electrical connection between the access point and the survivability unit.

Communication between the survivability unit and the NCUI2+/4 on the same access point/OpenScape 4000 SoftGate only runs via the IP network.

11.1.4 Survivability unit on OpenScape 4000 SoftGate

In the case of the "Survivable OpenScape 4000 SoftGate" feature, the survivability unit is implemented as software on the OpenScape 4000 SoftGate host.

11.1.5 Allocating Access Points/OpenScape 4000 SoftGates to a Survivability Unit

Access points/OpenScape 4000 SoftGates are not directly allocated to a survivability unit. Instead, they are allocated to an emergency group. The group defines which access points/OpenScape 4000 SoftGates are to be treated the same.

For example, it does not make sense to switch control of an individual access point/OpenScape 4000 SoftGate without trunk access from the host system to a survivability unit. It makes more sense to switch an entire group in one go that also contains an access point/OpenScape 4000 SoftGate with trunk access. Switchover regulations are defined per access point/OpenScape 4000 SoftGate and group.

By introducing the abstract emergency groups, you can control several groups independently of a shared survivability unit.

The hierarchical assignment is simple:

1) An access point/OpenScape 4000 SoftGate can belong to exactly one emergency group.

- An emergency group can be controlled by exactly one survivability unit.

All combinations with 1 to 83 access points/OpenScape 4000 SoftGates in 1 to 83 emergency groups on 1 to 83 survivability units are possible. A single APE entity can control all 83 access points.

There are two kinds of access points/OpenScape 4000 SoftGates, depending on the type of connection; these are “Direct Link” (APDL) and

“Networked Link” (APNW). For details, see “IP Distributed Architecture”, Section 2.2, “Access Point”.

IMPORTANT: A survivability unit in an **APNW** access point/ OpenScape 4000 SoftGate cannot control any **APDL** access points/OpenScape 4000 SoftGates. However, a survivability unit in an **APDL** access point/OpenScape 4000 SoftGate can control both **APDL** and **APNW** access points/OpenScape 4000 SoftGates.

11.1.6 Switchover in Emergency Mode

When a HG 3575/virtual HG 3575 discovers an interruption of the signaling connection to the central control unit, it reports this event to the allocated survivability unit.

Emergency mode, that is, when access point/OpenScape 4000 SoftGate is controlled by a survivability unit, is the one escalation level higher than signaling survivability. If signaling survivability is configured when the connection is lost, signaling survivability first attempts to control the access points/OpenScape 4000 SoftGates via modem. Emergency mode is initiated if this fails (for example, because central control unit is not available).

The survivability unit uses preconfigured rules to decide whether it should take over access point/OpenScape 4000 SoftGate control or not.

1) Each access point/OpenScape 4000 SoftGate is assigned a weight.

- If the total weight of all access points/OpenScape 4000 SoftGates in an emergency group that has lost its connection to the central control unit is greater than the limit specified, the survivability unit assumes control of all access points/OpenScape 4000 SoftGates assigned to this group
- However, access points/OpenScape 4000 SoftGates can also be configured so that they can always be individually controlled by the survivability unit regardless of their weighting.
- In addition, you can switch control of
  - individual access points/OpenScape 4000 SoftGates
  - all access points/OpenScape 4000 SoftGates in an emergency group
  - all access points/OpenScape 4000 SoftGates in all emergency groups in a survivability unit or
  - all access points/OpenScape 4000 SoftGates in the entire OpenScape 4000 system

  to the assigned survivability unit(s) at any time.

  The survivability unit takes over control of the access point/OpenScape 4000 SoftGate by instructing the HG 3575/virtual HG 3575 to initiate a restart and then start up with the survivability unit. The HG 3575/virtual HG 3575 restart triggers a restart in all peripheral boards on the access point/OpenScape 4000 SoftGate.
- All calls are cleared down.
- Features with active logon, e.g. mobile subscribers (PIN, mobile HFA), are logged off.
- Features that can be configured by the user, such as key layout for (name keys, DSS keys), forwarding key, reminder key, etc., are set up in the

state that they were in when the data was incorporated from the host system (see also Section 1.8, “Configuration Data”).

11.1.7 Reverting to Normal Operation

When a HG 3575/virtual HG 3575 discovers that the signaling connection to the central control unit has been restored, it reports this event to the allocated survivability unit.

The survivability unit uses preconfigured rules to decide whether or not it should hand back access point/OpenScape 4000 SoftGate control to the host system.

1) Every access point/OpenScape 4000 SoftGate in an emergency group must have a stable connection to the host system for a minimum set time

- Automatic reversion is only permitted during a set interval during the day. The interval can be set to 24 hours so that automatic reversion is possible at any time.
- Automatic reversion can be deactivated.
- You can also switch back control of
  - individual access points/OpenScape 4000 SoftGates,
  - all access points/OpenScape 4000 SoftGates in an emergency group,
  - all access points/OpenScape 4000 SoftGates in all emergency groups in a survivability unit or
  - all access points/OpenScape 4000 SoftGates in the entire OpenScape 4000 system

  to the central control unit at any time.

  The survivability unit returns access point/OpenScape 4000 SoftGate control to the central control unit by instructing the HG 3575/virtual HG 3575 to initiate a restart and then start up with the central control unit. The HG 3575/virtual HG 3575 restart triggers a restart in all peripheral boards on the access point/OpenScape 4000 SoftGate.
- All calls are cleared down.
- Features with active logon, e.g. mobile subscribers (PIN, mobile HFA), are logged off.
- Features that can be configured by the user, such as key layout (name keys, DSS keys), forwarding key, reminder key, etc., are set up in the state which is active in the host system - i.e. generally as it was prior to switchover.

11.1.8 Configuration Data

The entire OpenScape 4000 system including all its access points/OpenScape 4000 SoftGates and survivability units is only configured in the host system.

Local administration of the feature is not possible at the survivability unit with the exception of OpenScape 4000 Assistant, Backup and Restore.

A special backup of the OpenScape 4000 system database (OpenScape 4000 Assistant > Backup and Restore in the host system) is performed at set intervals (usually once a day).

The survivability units perform continuous checks (every 10 minutes) to see if a new OpenScape 4000 database backup is available. If this unit is not actively controlling an access point/OpenScape 4000 SoftGate (emergency mode), it downloads the saved data and incorporates it by means of a reload (OpenScape 4000 Assistant > Backup and Restore on the survivability unit).

The backup data is stored on a file server. This file server may be located in the customer's computer center. You can also use the OpenScape 4000 Manager platform as a file server.

The daily backup is configured on the file server in such a way that it always contains the complete system with database, patches and software.

However, transmission from the host system to the file server and from the file server to the survivability unit is optimized. Only different data is actually transferred.

For more information on the "Backup and Restore" application please refer to the online help.

11.1.9 Transferring new System Releases and Patches

OpenScape 4000 system complexity is considerably increased by survivability units. To keep operation and maintenance costs low, system releases and patches are automatically distributed to the survivability units.

In addition, new system releases and patches are incorporated in the backup/restore process for the database (see Section 1.8, "Configuration Data").

11.1.10 Connection Between Subsystems (Islands)

If an OpenScape 4000 system breaks down in emergency mode into several autonomous islands, how can the islands then communicate with each other? An autonomous island is defined as a survivability unit and all the access points/OpenScape 4000 SoftGates over which the unit currently has active control.

Everything else remains the same within each individual island:

- Calls between subscribers in the same access point/OpenScape 4000 SoftGate are switched within the access point/OpenScape 4000 SoftGate.
- Calls between subscribers in different access points/OpenScape 4000 SoftGates of an island are switched via IP connections between the access points/OpenScape 4000 SoftGates.
- Incoming/outgoing trunk calls are conducted via the island's trunk interfaces.
- Incoming/outgoing calls in networked systems are conducted via the island's tie trunk interfaces.

What happens to calls for subscribers on another island?

All survivability units have the same complete host system database. Therefore, every island knows every subscriber in the entire configuration, including all subscribers on other islands. Access points/OpenScape 4000 SoftGates outside the island are configured but cannot be reached. All boards and their subscribers, trunks and tie trunks are therefore known and belong to a set hierarchy (UNACH).

Although the IP infrastructure between some islands may still be intact, no inter-island calls between access points/OpenScape 4000 SoftGates are switched via IP.

Trunk interfaces can still be used for inter-island communication. It is therefore still possible to reach a subscriber who is known but not directly available in another island over CO. The “Alternate Routing on Error“ feature supports rule-based call number modification in emergency mode.

This feature guarantees Basic Call connectivity for traffic between the islands.

For this feature to work, the trunks on the islands must use different access codes. If all trunks use the same access code, directed routing must be performed by the carrier using the complete number dialed (**CENTREX**).

If the islands are integrated in an extensive OpenScape 4000 network with QSig trunks, the LCR configuration must include normal and emergency mode because the system has only one configuration. Even in this scenario, Basic Call connectivity is guaranteed for incoming, system-wide traffic to an access point/OpenScape 4000 SoftGate which results in a transit connection. In order to support network-wide features, the islands should be configured as virtual nodes.

Payload survivability does not work in emergency mode as the islands involved no longer have a shared control unit.

11.1.11 Time Synchronization

An exact time is required for many OpenScape 4000 functions (call detail recording, time-dependent channels, night service, etc.). All clocks in the system (up to 84) have to operate synchronously.

There are two ways of synchronizing the time:

1) The IP network has a time server, which supports time synchronization of all OpenScape 4000 processors (the central processor and all survivability units) using the Network Time Protocol.

2) A time server is **not** available in the IP network. The OpenScape 4000 platform then makes its local time available over the network for synchronizing all survivability units.

11.1.12 Feature Licensing

A license is necessary for operating a survivability unit in a OpenScape 4000 system.

All host system licenses are also used on the survivability units in emergency mode. The survivability units are operated without licenses. As a result, a 30-day grace period for license management begins once a restore has been performed. All SWU features are disabled at the end of this 30-day period.

It is advisable that an APE Backup is scheduled at least once per month on the central system. This will not only ensure an APE restore on the survivability unit that would reset the 30-day grace period, but also that the database of every survivability unit is kept consistent with the central/host system, to reflect any configuration changes.

NOTICE: If the 30-day license management grace period was already active on the central system and only 10 days of unrestricted operation remain, then this restriction also applies to all survivability units after a restore.

11.1.13 Application Support in Emergency Mode

The OpenScape CSTA is supported on the AP Emergency feature so that a number of applications can function on both the host system and the survivability unit.

The prerequisites for this are:

- the application must have a functioning IP connection to the CSTA of the survivability unit
- the application can only monitor/ handle resources that are controlled by one and the same survivability unit.

11.2 Configuring the APE Feature (Access Point Emergency)

To configure the AP Emergency feature, you must have a good understanding of the functioning of this feature. This overview is found in Chapter 1, “Access Point Emergency Feature Description”

IMPORTANT: For emergency mode, configuration of the feature “Alternate Routing on Error“ is mostly required so that subscribers of different “emergency islands“ can contact one another. This is described in the service manual „Section 3 - Feature Usage Examples > Alternate Routing on Error“. In some installations trunk and tie-line circuits have to be configured in order to access a HiPath 400/OpenScape 4000 network or the public network from the “islands“. Conclude this part of the configuration **before** configuring the AP Emergency feature. You can prevent APE from taking effect if a fault occurs in the network for example. If, however, the above requirements have not been fulfilled, the communication capability of an “emergency island“ may be restricted and it may no longer be possible to make emergency calls.

The feature configuration is divided into the following steps:

- Activities on OpenScape 4000 host system
  - Configuring or Modifying a CC-AP/ Survivable OpenScape 4000 SoftGate in OpenScape 4000
  - Configuring or Modifying an Emergency Group
  - Configuring Access Points/ OpenScape 4000 SoftGates for AP Emergency
  - Configuring the Display for AP Emergency on the Terminal
  - Defining the Switchover Delay
  - Time Synchronization Between the Host System and CC-AP/ Survivable OpenScape 4000 SoftGate

- Activities on the survivability unit - CC-AP/Survivable OpenScape 4000 SoftGate
  - Initial Startup of the CC-AP/Survivable OpenScape 4000 SoftGate
  - Verification and Acceptance of the AP Emergency Configuration

11.2.1 Configuring or Modifying a CC-AP/Survivable OpenScape 4000 SoftGate in OpenScape 4000

The CC-AP/Survivable OpenScape 4000 SoftGate is always addressed with the LTU number of the access point/OpenScape 4000 SoftGate in which it is integrated.

Only the IP address for the IPDA LAN connection of the CC-AP/Survivable OpenScape 4000 SoftGate and the operating mode of the Ethernet interface are required as configuration data. All other parameters necessary for IP communication are taken from the CBM configuration of HG 3575 of the access point/OpenScape 4000 SoftGate.

Table 67: Configuration parameters derived for the CC-AP/Survivable OpenScape 4000 SoftGate

Parameter	“Network Link“ Access Point/OpenScape 4000 SoftGate	“Direct Link“ Access Point/ OpenScape 4000 SoftGate
IP address	Directly configured	
Netmask	HG 3575 network mask APRT: TYPE=APNET - NETMASK	OpenScape 4000 LAN segment network mask SIPCO: TYPE=LSNET - NETMASK
Default router	Default router in the network of the access point/OpenScape 4000 SoftGate UCSU: UNIT=AP - APRTADDR	Default router in the network of the access point/OpenScape 4000 SoftGate UCSU: UNIT=AP - APRTADDR that is usually the default router of the OpenScape 4000 LAN segment SIPCO: TYPE=LSNET - DEFRT
VLAN tagging	STMIB: MTYPE=NCUI2 - TYPE=IFDATA - VLAN	
VLAN ID	STMIB: MTYPE=NCUI2 - TYPE=IFDATA - VLANID	

Parameter	“Network Link“ Access Point/OpenScape 4000 SoftGate	“Direct Link“ Access Point/ OpenScape 4000 SoftGate
TOS byte for the signaling connection	STMIB: MTYPE=NCUI2 - TYPE=IFDATA - TOSLAN	

The Ethernet interface setting **must** be **identical** for both connected interface partners (CC-AP/Survivable OpenScape 4000 SoftGate or LAN switches or routers)!

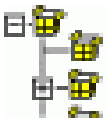
IMPORTANT: The setting of a fixed interface partner leads to problems with the “Autonegotiate“ setting of the other partner.

IMPORTANT: Incorrect settings cannot normally be detected by the system and therefore go unreported. If one device is operating in full duplex and the other in half duplex mode, this is not immediately noticeable. Where there is a high payload, the device set to half duplex will report a higher number of late collisions and the packet delay will increase sharply.

IMPORTANT: If the LAN port to which the CC-AP/Survivable OpenScape 4000 SoftGate is connected does not support auto-negotiation, or if it does not function reliably, the CC-AP/ Survivable OpenScape 4000 SoftGate Ethernet interface must be set to fixed values.

In the example, the CC-AP/Survivable OpenScape 4000 SoftGate is configured or modified in access point/OpenScape 4000 SoftGate 99.

The IP address is 192.168.23.199, the Ethernet interface is set to 10 Mbps, half duplex.

	**Configuration Management > System Data > IPDA > IPDA CC Access Point** Click **Search** and select CC-AP/Survivable OpenScape 4000 SoftGate or create a **New** one. Set the **IP Address** and the Ethernet interface transmission speed (**Speed**) and mode and **Save**.

	`ADD-APESU:DATA=CCAP,CCAPNO=99,IPADDR=192.168.23.199;`
	or
	`CHANGE-APESU:DATA=CCAP,CCAPNO=99,IPADDR=192.168.23.199;`

The modified data does not take effect until after you have used OpenScape 4000 Assistant Backup & Restore to copy the database to the CC-AP/

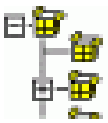
Survivable OpenScape 4000 SoftGate, and the CC-AP/Survivable OpenScape 4000 SoftGate has accepted it.

Table 68: AMO APESU parameters in ADD or CHANGE branch under DATA=CCAP

AMO	Parameter	Sprache/ Language	Beschreibung/ Description
APESU	CCAPNUM	d	LTU-Nummer des Access Points/ OpenScape 4000 SoftGates, in welchem der CC-AP/das Survivable OpenScape 4000 SoftGate eingebaut ist.
	CCAPNO	e	Line/Trunk Unit Number of the access point/ OpenScape 4000 SoftGate, where the CC-AP/Survivable OpenScape 4000 SoftGate is installed.
	IPADR	d	IP Adresse des CC-AP/Survivable OpenScape 4000 SoftGate.
	IPADDR	e	IP Address of the CC-AP/Survivable OpenScape 4000 SoftGate

11.2.2 Deleting a CC-AP/Survivable OpenScape 4000 SoftGate in OpenScape 4000

When you delete a CC-AP/Survivable OpenScape 4000 SoftGate, all emergency groups allocated to it and the AP Emergency configuration of the allocated access points/OpenScape 4000 SoftGates are also automatically deleted. If you want to keep the emergency groups, you must first allocate them to a different CC-AP/Survivable OpenScape 4000 SoftGate (`CHANGE-APESU:DATA=APEGRP,EGRPNO=xx,CCAPNO=yy;`).

	**Configuration Management > System Data > IPDA > IPDA CC Access Point** Click **Search** and select the CC-AP/Survivable OpenScape 4000 SoftGate, then click **Delete**.
	`DELETE-APESU:CCAPNO=99;`

The modified data does not take effect until after you have used OpenScape 4000 Assistant Backup & Restore to copy the database to the CC-AP/ Survivable OpenScape 4000 SoftGate, and the CC-AP/Survivable OpenScape 4000 SoftGate has accepted it.

11.2.3 Configuring or Modifying an Emergency Group

The emergency group is the logical connecting link between the access point/ OpenScape 4000 SoftGate and CC-AP/Survivable OpenScape 4000 SoftGate.

An access point/OpenScape 4000 SoftGate is a member of exactly one emergency group. An emergency group is served by exactly one CC-AP/ Survivable OpenScape 4000 SoftGate.

The emergency group was introduced for transferring complete groups of access points/OpenScape 4000 SoftGates, together and at the same time, to and from the host system control to the CC-AP/Survivable OpenScape 4000 SoftGate control.

While the primary function of the AP Emergency feature is handling the total breakdown of the central control, the difficulty lies in appropriate handling of partial breakdowns that may arise in the IP communication.

An emergency group typically combines access points/OpenScape 4000 SoftGates that together form a survivable unit. For example, this could be external location connected via WAN.

Faults in the routing can result in only some of a group's access points/ OpenScape 4000 SoftGates losing contact with the central control. In this case it would be possible to transfer only the affected access points/OpenScape 4000 SoftGates to the CC-AP/Survivable OpenScape 4000 SoftGate control. This interrupts communication among the group's access points/OpenScape 4000 SoftGates, however. Calls would then only be possible via the trunk. But does each access point/OpenScape 4000 SoftGate have its own trunk line? Where are the central resources, such as recorded announcements, servers, etc.?

This is why it often makes sense to switch a group only as a whole. In this way all access point/sOpenScape 4000 SoftGates remain under **one** control, and communication among the access points/OpenScape 4000 SoftGates runs via IP. All access points/OpenScape 4000 SoftGates can communicate with the rest of the system via a common trunk line. In such cases, the access points/ OpenScape 4000 SoftGates of **one** emergency group will also belong to **one** source group for source-dependent routing (see "IP Distributed Architecture", Section 2.8, "Source Dependent Routing").

An emergency group is identified by a freely selectable number. Depending on the installation, it may be advantageous to base the emergency group number on the numbering of the associated source group or the CC-AP/Survivable OpenScape 4000 SoftGate number.

Because plain text says more than any number, no matter how cleverly selected, you can give each emergency group a name.

Each configured emergency group must be assigned to a CC-AP/Survivable OpenScape 4000 SoftGate. The assignment can be changed.

Weighting determines whether all of an emergency group's access points/ OpenScape 4000 SoftGates switch to the CC-AP/Survivable OpenScape 4000 SoftGate. A weighting is assigned to each access point/OpenScape 4000 SoftGate. The access point/OpenScape 4000 SoftGate contributes this weighting to the switching evaluation in the event of a breakdown in its connection to the central control. A limiting value can be defined for the group. When this value is exceeded, a switchover is carried out.

Because they have higher weightings, access points/OpenScape 4000 SoftGates with trunk lines, central resources or VIP users are more likely to trigger a switchover than access points/OpenScape 4000 SoftGates with “standard features“.

When assigning the weightings, you must make sure that the weighting of all access points/OpenScape 4000 SoftGates that are assigned to an emergency group is sufficient in order to reach the group’s limiting value. This is easy to overlook, particularly when you are changing the configuration.

If the IP connections to central control are available again for all access points/OpenScape 4000 SoftGates, switchback to central control must be organized. There will be customers who require immediate switchback to the central control, even though this means disconnecting calls. Often, however, switchback is prohibited at certain times. It may also be the case that only administrative switchovers are permitted.

AP Emergency enables the activation of either automatic switchback, or of only manual switchback. The parameters for automatic switchback are based on the level of the emergency groups.

For the group - and therefore for all access points/OpenScape 4000 SoftGates in the group - you can stipulate how long the connection between each access point/OpenScape 4000 SoftGate and the central control must be stable without interruptions, before a switchback will be considered.

Once the connection has been stable for the specified length of time, a check is made as to whether a switchback is allowed at the time. Intervals during which a switchback is permitted are set up for this purpose. The interval starts with the specified hour (of the day) and ends at another specified hour. It is customary to set up a time offset in order to shift the network load of scheduled activities away from the exact hour. This allows you to specify how many minutes after the hour the switchback interval is opened or closed. For example, if the switchback start is at 8pm, the switchback end at 6am, and the offset is 13, this means that the switchback can automatically take place during the time from 8:13pm and 6:13am. If there was a network fault in this configuration that interrupted the IP connection between the central control and the access points/OpenScape 4000 SoftGates from 9:05am until 9:15am, the automatic switchback would take place at 8:13pm. If the fault occurs during the switchback interval, the switchback takes place immediately once the IP connections between the central control and access points/OpenScape 4000 SoftGates have been stable again for the minimum time.

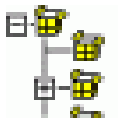
A manual switchback is possible at any time. The administrator must ensure here that the boundary conditions are correct (is switchback required? - are all access points/OpenScape 4000 SoftGates connected to the central control unit again?).

If a CC-AP/Survivable OpenScape 4000 SoftGate fails while it is actively controlling access points/OpenScape 4000 SoftGates, the following behavior results:

- If the host system is available and if it has contact with an affected access point/OpenScape 4000 SoftGate, the host system takes control of the access point/OpenScape 4000 SoftGate again without taking the stability time and the set switchover time into consideration.
  - This only applies if automatic switchback has been configured.
  - If manual switchback has been configured, an access point/OpenScape 4000 SoftGate is **not** automatically taken over by the host system if the

CC-AP/Survivable OpenScape 4000 SoftGate fails during emergency mode.

- If the host system is not available, control is no longer available for the access point/OpenScape 4000 SoftGate. It resets itself within the configured time period and waits until a control makes contact with it.

	**Configuration Management > System Data > IPDA > AP Emergency Group** Click **Search** and select an emergency group or create a **New** one. Set configuration parameters and **Save**.

	`ADD-APESU:DATA=APEGRP,EGRPNO=2,CCAPNO=99,THRSHLD=100,SB-MODE=,NAME="BERLIN",STABLE=10,SBBEGIN=20,SBEND=6,RSOFFSET=13;`
	or
	`CHANGE-APESU:DATA=APEGRP,EGRPNO=2,CCAPNO=99,THRSHLD=100,SBMODE=AU-TO,NAME="BERLIN",STABLE=10,SBBEGIN=20,SBEND=6,RSOFFSET=13;`

The modified data does not take effect until after you have used OpenScape 4000 Assistant Backup & Restore to copy the database to the CC-AP/ Survivable OpenScape 4000 SoftGate, and the CC-AP/Survivable OpenScape 4000 SoftGate has accepted it.

Table 69: AMO APESU parameters in ADD or CHANGE branch under DATA=APEGRP

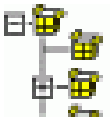
AMO	Parameter	Sprache/ Language	Beschreibung/ Description
APESU	EGRPNUM	d	Identifikations-Nummer der Emergency Gruppe. Wertebereich [1 .. 99]
	EGRPNO	e	Identification number of the Emergency Group. Range [1 .. 99]
	CCAPNUM	d	Nummer des CC-AP/Survivable OpenScape 4000 SoftGate, dem die Emergency Gruppe zugeordnet ist.
	CCAPNO	e	Number of the CC-AP/Survivable OpenScape 4000 SoftGate, to which the Emergency Group is assigned.
	SCHWELLE	d	Grenzwert für den Gewichtungsalgorithmus. Bei Erreichen bzw. Überschreiten werden die Access Points/OpenScape 4000 SoftGates der Emergency Gruppe in die Steuerung des CC-AP/Survivable OpenScape 4000 SoftGate umgeschaltet. Wertebereich [0 .. 1000]

AMO	Parameter	Sprache/ Language	Beschreibung/ Description
	THRSHLD	e	Threshold for the weighing alogrithm. When reached or exceeded, the access points/OpenScape 4000 SoftGates of the Emergency Group are switched over into control of the CC-AP/Survivable OpenScape 4000 SoftGate. Range [0 .. 1000]
	RSMODE	d	Rückschaltemodus Bestimmt, ob die Access Points/OpenScape 4000 SoftGates der Emergency Gruppe automatisch, oder ausschließlich manuell zur zentralen Steuerung zurückgeschaltet werden dürfen. Werte: AUTO: Automatische Rückschaltung MAN: Manuelle Rückschaltung
	SBMODE	e	Switch-Back Mode Specifies if the access points/OpenScape 4000 SoftGates of the Emergency Group may be switched back to the central control automatically or only manually. Values: AUTO: Automatical Switch-Back MAN: Manual Switch-Back
	NAME	d	Name der Emergency Gruppe (maximal 22 Zeichen)
	NAME	e	Name of the Emergency Group (maximum 22 characters)
	STABIL	d	Stabilitätszeit Minimale Zeitdauer, über welche alle Access Points/OpenScape 4000 SoftGates der Emergency Gruppe eine stabile Verbindung zur zentralen Steuerung haben müssen, bevor automatisch rückgeschaltet werden darf. Wertebereich [0 .. 255] Minuten

AMO	Parameter	Sprache/ Language	Beschreibung/ Description
	STABLE	e	Stability time Minimum amount of time, during which all access points/OpenScape 4000 SoftGates of the Emergency Group must have a stable connection to central control, before they may be switched back. Range [0 .. 255] Minutes
	RSBEGIN	d	Beginn des täglichen Zeitintervalls für die automatische Rückschaltung. Die Rückschaltung ist erlaubt in der Zeit zwischen RSBEGIN:RSOFFSET und RSENDE:RSOFFSET.
	SBBEGIN	e	Begin of the daily time interval for the automatic switch-back. Switch-back is allowed during the time between SBBEGIN:SBOFFEST and SBEND:SBOFFEST.
	RSENDE	d	Ende des täglichen Zeitintervalls für die automatische Rückschaltung. Ist RSENDE gleich RSBEGIN gesetzt, darf jederzeit automatisch rückgeschaltet werden.
	SBEND	e	End of the daily time interval for the automatic switch-back. If SBEND is set identically to SBBEGIN, automatic switch-back is allowed at any time.
	RSOFFEST	d	Offsetwert [in Minuten] zum täglichen Zeitintervall für die automatische Rückschaltung.
	RSOFFSET	e	Offset value [in minutes] to the daily time interval for the automatic switch-back.

11.2.4 Deleting an Emergency Group

When you delete an emergency group, the AP Emergency configuration of the access points/OpenScape 4000 SoftGates allocated to it are also automatically deleted. If you want to keep the configuration of the access points/OpenScape 4000 SoftGates, you must first allocate these to a different emergency group (`CHANGE-APESU:DATA=AP,APNO=xx,EGRPNO=yy;`),

	**Configuration Management > System Data > IPDA > AP Emergency Group** Click **Search** select the CC-AP/Survivable OpenScape 4000 SoftGate and **Delete**.
	`DELETE-APESU:EGRPNO=99;`

The modified data does not take effect until after you have used OpenScape 4000 Assistant Backup & Restore to copy the database to the CC-AP/ Survivable OpenScape 4000 SoftGate, and the CC-AP/Survivable OpenScape 4000 SoftGate has accepted it.

11.2.5 Configuring Access Points/OpenScape 4000 SoftGates for AP Emergency

To configure an access point/OpenScape 4000 SoftGate for the AP Emergency feature, it must be assigned to an already existing emergency group. Most of the configuration specific to AP Emergency is performed at the level of the emergency group.

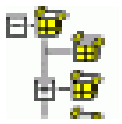
Access points/OpenScape 4000 SoftGates with the “direct link“ connection type (APDL) - see “IP Distributed Architecture”, Section 2.2, “Access Point” - can only be assigned to emergency groups for which the CC-AP/Survivable OpenScape 4000 SoftGate is in an access point/OpenScape 4000 SoftGate with link type **APDL**. For access points/OpenScape 4000 SoftGates with the “networked“ connection type (**APNW**) there is no restriction for the connection type of the access point/OpenScape 4000 SoftGate containing the CC-AP/ Survivable OpenScape 4000 SoftGate.

You must stipulate the emergency group to which an access point/OpenScape 4000 SoftGate belongs as well as the “weight“ of the access point/OpenScape 4000 SoftGate in question, i.e. its contribution to the weighting algorithm for the switchover.

Regardless of the weighting in the emergency group, you can also specify that an access point/OpenScape 4000 SoftGate be immediately included in the control of the CC-AP/Survivable OpenScape 4000 SoftGate allocated to the emergency group when the connection to the central control is lost. This exception to the group behavior can for example be useful when an access point/OpenScape 4000 SoftGate with VIP users is equipped in such a way that it has its own trunk access and is therefore independent of the availability of the other group members.

IMPORTANT: Access points/OpenScape 4000 SoftGates that are switched over to the CC-AP/Survivable OpenScape 4000 SoftGate independently of the group and that do not have their own trunk or tie line only allow access point/OpenScape 4000 SoftGate internal communication. **This prevents emergency calls from being forwarded over the trunk, for example.**

This exception only applies when the limiting value for the weighting within the emergency group has not been reached. The weighting contribution of an access point/OpenScape 4000 SoftGate with separate switching is always taken into consideration for the weighting of the group behavior. The access point/OpenScape 4000 SoftGate is always included in the switchover when required by the weighting for the emergency group. The switchback also takes place along with the group.

	**Configuration Management > System Data > IPDA > IPDA Access Point** Click **Search** and select the access point/OpenScape 4000 SoftGate. Set the configuration parameters in the **AP Emergency** tab and **Save**.

	`ADD-APESU:DATA=AP,APNO=99,EGRPNO=2,WEIGHT=70,SWMODE=GROUG;`
	or
	`CHA-APESU:DATA=AP,APNO=99,EGRPNO=2,WEIGHT=70,SWMODE=GROUP;`

The modified data does not take effect until after you have used OpenScape 4000 Assistant Backup & Restore to copy the database to the CC-AP/ Survivable OpenScape 4000 SoftGate, and the CC-AP/Survivable OpenScape 4000 SoftGate has accepted it.

Table 70: AMO APESU parameters in ADD or CHNAGE branch under DATA=AP

AMO	Parameter	Sprache/ Language	Beschreibung/ Description
APESU	APNUM	d	LTU-Nummer des Access Points/OpenScape 4000 SoftGates
	APNO	e	Line/Trunk Unit Number of the access point/ OpenScape 4000 SoftGate
	EGRPNUM	d	Identifikations-Nummer der Emergency Gruppe.
	EGRPNO	e	Identification number of the Emergency Group.
	GEWICHT	d	Gewichtsbeitrag des Access Points/ OpenScape 4000 SoftGates für den Gewichtungsalgorithmus. Verliert der Access Point/OpenScape 4000 SoftGate die Verbindung zur zentralen Steuerung, so wird sein Gewichtsbeitrag in die Gewichtung der Emergency Gruppe eingebracht. Wertebereich [0 .. 1000]

AMO	Parameter	Sprache/ Language	Beschreibung/ Description
	WEIGHT	e	Weight share of the access point/ OpenScape 4000 SoftGate to the weighing alogrithm. When the access point/OpenScape 4000 SoftGate loses the connection with the central control, it's weight share is brought into the weighing of the Emergency Group. Range [0 .. 1000]
	UMSCHALT	d	Umschaltemodus Bestimmt, ob ein Access Point/OpenScape 4000 SoftGate ausschließlich zusammen mit der gesamten Emergency Gruppe umgeschaltet wird, oder ob er auch unabhängig von der Gewichtung sofort vom CC-AP/Survivable OpenScape 4000 SoftGate übernommen wird, wenn er die Verbindung zur zentralen Steuerung verloren hat. Werte: GRUPPE: Umschaltung nur mit gesamter Gruppe EINZEL: Einzelbehandlung bei der Umschaltung
	SWMODE	e	Switch-Over Mode Specifies if the access point/OpenScape 4000 SoftGate may be switched over only together with the complete Emergency Group, or if it may be taken over by the CC-AP/Survivable OpenScape 4000 SoftGate independently to the weighing, as soon as it loses connection with central control. Values: GROUP: Switch-Over only together with Group SINGLE: Individual handling at Switch-Over

11.2.6 Examples for Determination of Weights

The combined use of access point/OpenScape 4000 SoftGate weighting, threshold settings for group switchover and, if necessary, exemption from the group rule through individual switchover, form a powerful instrument for configuring automatic switchover to the emergency mode. The following two examples should help you to understand the calculations.

- Basic IP system (with no shelves in slots 1-15) with the communication server located at the computer center and 30 access points/OpenScape 4000 SoftGates, 1 CC-AP/Survivable OpenScape 4000 SoftGate at the backup computer center, and multiple trunk connections with the same code distributed on four access points/OpenScape 4000 SoftGates.
- Sample configuration 1 (Emergency mode in the case of complete failure of the communication server only, i.e. the connection from **all** access points/ OpenScape 4000 SoftGates to the server has been lost)

  – 1 emergency group, threshold = 300
  – Weight of each of the 30 access points/OpenScape 4000 SoftGates = 10

  Disadvantage: If only one access point/OpenScape 4000 SoftGate is not available, for example as a result of a power failure, it is excluded from the calculation since it does not have any contact with the CC-AP/Survivable OpenScape 4000 SoftGate. In such a scenario, the threshold **cannot** be reached.

  Sample configuration 2 (If the connection between the communication server and more than half of the access points/OpenScape 4000 SoftGates is lost, the system switches to emergency mode. This also applies if the same occurs with more than half of the trunk connections).

  – 1 emergency group, threshold = 150
  – Access points/OpenScape 4000 SoftGates without a trunk connection: Weight = 10
  – Access points/OpenScape 4000 SoftGates with a trunk connection: Weight = 75
- Conventional system at main location, branch 1 with 3 access points/ OpenScape 4000 SoftGates one of which has a trunk connection; branch 2 with 6 access points/OpenScape 4000 SoftGates, two of which have a trunk connection; branch 3 with 1 access point/OpenScape 4000 SoftGate, which also has a trunk connection; branch 4 has 4 access points/OpenScape 4000 SoftGates, one of which has a general trunk connection and another which contains the ports for the executive management with a separate trunk connection. Connectivity via a local trunk connection is very important for the branches. If a single access point/OpenScape 4000 SoftGate without a trunk connection “fails“, this should not lead to a change of group. If, however, two or more access points/OpenScape 4000 SoftGates fail, the group must be changed. Each location has an individual access point/OpenScape 4000 SoftGate equipped with CC-AP/Survivable OpenScape 4000 SoftGate.

- Sample configuration Branch 1 (3 access points/OpenScape 4000 SoftGates)
  - 1 emergency group, threshold = 200
  - Access points/OpenScape 4000 SoftGates without a trunk connection: Weight = 100
  - Access point/OpenScape 4000 SoftGate with a trunk connection: Weight = 200

  Branch 2 (6 access points/OpenScape 4000 SoftGates)
  - 1 emergency group, threshold = 200
  - Access points/OpenScape 4000 SoftGates without a trunk connection: Weight = 100
  - Access points/OpenScape 4000 SoftGates with a trunk connection: Weight = 100

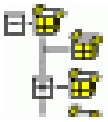
  Branch 3
  - 1 emergency group, threshold = 100
  - Access points/OpenScape 4000 SoftGates: Weight = 100

  Branch 4
  - 1 emergency group, threshold = 200
  - Access points/OpenScape 4000 SoftGates without a trunk connection: Weight = 100
  - access point/OpenScape 4000 SoftGate with a trunk connection: Weight = 200
  - Executive access point/OpenScape 4000 SoftGate: Weight = 100, individual switchover active The CC-AP/Survivable OpenScape 4000 SoftGate should be integrated in this access point/OpenScape 4000 SoftGate.

11.2.7 Removing Access Points/OpenScape 4000 SoftGates from the AP Emergency Configuration

You can remove an access point/OpenScape 4000 SoftGate from the AP Emergency configuration at any time.

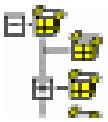
IMPORTANT: When you delete an access point/OpenScape 4000 SoftGate from the AP Emergency configuration, its possible weighting contribution to the weighting algorithm of the emergency group to which it belonged is also deleted. Verify whether the emergency group's limiting value "THRSHLD" is still a valid number.

	**Configuration Management > System Data > IPDA > IPDA Access Point** Click **Search** and select the access point/OpenScape 4000 SoftGate. Delete the **Emergency Group Number** on the **AP Emergency** tab and **Save**.
	`DELETE-APESU:APNO=99;`

The modified data does not take effect until after you have used OpenScape 4000 Assistant Backup & Restore to copy the database to the CC-AP/ Survivable OpenScape 4000 SoftGate, and the CC-AP/Survivable OpenScape 4000 SoftGate has accepted it.

11.2.8 Deleting the entire AP Emergency Configuration

If the entire AP Emergency configuration of a OpenScape 4000 system is to be deleted, this can be performed easily at system level. All CC-APs, all emergency groups and the AP Emergency configuration of all access points/ OpenScape 4000 SoftGates are completely removed.

	**Configuration Management > System Data > IPDA > IPDA CC Access Point** Click **Search** and select the **Object list** view. Select all (CC-AP/Survivable OpenScape 4000 SoftGate) objects and **Delete**.
	`DELETE-APESU;`

The modified data does not take effect until after you have used OpenScape 4000 Assistant Backup & Restore to copy the database to the CC-AP/ Survivable OpenScape 4000 SoftGate, and the CC-AP/Survivable OpenScape 4000 SoftGate has accepted it.

11.2.9 Configuring the Display for AP Emergency on the Terminal

If an access point/OpenScape 4000 SoftGate is actively controlled by a survivability unit, i.e. a CC-AP/Survivable OpenScape 4000 SoftGate, there are changes that the user needs to know about.

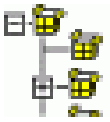
This information is output on the second line of the terminals' idle display. **The text to be output must be agreed upon with the customer.**

The output text replaces the LOGO information that can be output during normal operation.

The maximum text length is 22 characters and may comprise numbers and letters in upper and lower case.

IMPORTANT: Insert blank spaces for all positions in the second display line where information is output in idle mode, and leave enough room to allow the information to be read. For example, if the telephone's number is shown in the first 5 spaces of the idle display, you must start the AP Emergency information text with at least 6 blank spaces.

Use the AMO ZANDE for this setting.

	You must be in expert mode to make this setting with the AMO ZANDE. **Expert Mode > Expert Access > Open** ...<IP> with AMO (see AMO command)

	`CHANGE-ZANDE:TYPE=ALLDATA,APEDTXT="`
	` Emergency operation ";`
	The text should be exactly 22 characters long.

The modified data does not take effect until after you have used OpenScape 4000 Assistant Backup & Restore to copy the database to the CC-AP/ Survivable OpenScape 4000 SoftGate, and the CC-AP/Survivable OpenScape 4000 SoftGate has accepted it.

11.2.10 Defining the Switchover Delay

If a breakdown has been detected in the OpenScape 4000 host system or the IP network, and if a CC-IP has decided based on its configured rules that access points/OpenScape 4000 SoftGates should be switched over, there is another point to be considered:

How should the overall system react if the OpenScape 4000 host system carries out a RELOAD?

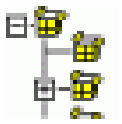
There are two possibilities:

1) React as quickly as possible, i.e. perform immediate switchover. In the case of a RELOAD, switchover to emergency operation is then **always** performed.
2) Delay the switchover long enough to **prevent** a RELOAD leading to emergency operation.

In line with this decision, you must set the AP Emergency switchover delay either

1) to zero (switch immediately) or

- to the length of time that the OpenScape 4000 system needs to execute a complete RELOAD.

	**Configuration Management > System Data > IPDA > IPDA System Data** Click **Search**, enter the switchover delay for AP Emergency in the **System data** and **Timing** tabs and then click **Save**.
	`CHANGE-SIPCO:TYPE=TIMING,APESWDLY=5;` Sets the switchover delay to 5 minutes ->i.e. the system RELOAD takes 5 minutes; wait for the corresponding length of time.

The modified data does not take effect until after you have used OpenScape 4000 Assistant Backup & Restore to copy the database to the CC-AP/Survivable OpenScape 4000 SoftGate, and the CC-AP/Survivable OpenScape 4000 SoftGate has accepted it.

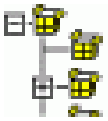
Table 71: The AP Emergency-specific parameter APESWDLY of the AMO SIPCO in CHANGE branch under TYPE=TIMING

AMO	Parameter	Sprache/ Language	Beschreibung/ Description
SIPCO	APESWDLY	d	APE Umschalteverzögerung Das Umschalten eines Access Points/ OpenScape 4000 SoftGates in den Emergency Mode kann um eine konfigurierbare Zeit verzögert werden. Der Wert wird in Minuten angegeben. Wertebereich [0 .. 99]. "0" sollte nicht konfiguriert werden, weil damit würde der APE auch im Falle eines RMX Restarts des Hostsystems (CCA/CCB) übernehmen. Konfigurationsempfehlung und AMO Defaultwert: 5 (Minuten)

AMO	Parameter	Sprache/ Language	Beschreibung/ Description
	APESWDLY	e	APE Switch Over Delay The switch-over of an Access Point/ OpenScape 4000 SoftGate to Emergency Mode can be delayed for a configurable amount of time. The value is entered in minutes. Range [0 .. 99]. "0" should not be configured because then a switch over to the APE is performed even in case of a restart of the RMX of the host system (CCA/CCB). Recommendation configuration and AMO default: 5 (minutes)

11.2.11 Querying the Connection Data

11.2.11.1 Querying the Connection Data via Configuration Management

	Configuration Management > System Data > Maintenance > IPDA - CC Access Point Maintenance Click SEARCH and select CC-AP/Survivable OpenScape 4000 SoftGate. The table that this generates shows the connection status for all access points/OpenScape 4000 SoftGates that belong to the emergency groups of the selected CC-AP/Survivable OpenScape 4000 SoftGate.

11.2.11.2 Querying the Connection Data via AMO



A query for the AP Emergency configuration also includes output of the current connection status. The amount of data output and the information it contains depend on the logical level at which the query is running - and whether it is performed in the OpenScape 4000 host system or on a CC-AP/Survivable OpenScape 4000 SoftGate.

DISPLAY-APESU;

1) on OpenScape 4000 host system

a) all CC-APs

- all emergency groups
- all access points/OpenScape 4000 SoftGates

- locally on a CC-AP/Survivable OpenScape 4000 SoftGate
  - local CC-AP/Survivable OpenScape 4000 SoftGate
  - all of the CC-AP/Survivable OpenScape 4000 SoftGate Emergency groups
  - all access points/OpenScape 4000 SoftGates of the CC-AP/Survivable OpenScape 4000 SoftGate Emergency groups

  DISPLAY-APESU:CCAPNO=xx; **or** DISPLAY-APESU:xx;
- on OpenScape 4000 host system
  - selected CC-AP/Survivable OpenScape 4000 SoftGate
  - all of the selected CC-AP/Survivable OpenScape 4000 SoftGate Emergency groups
  - all access points/OpenScape 4000 SoftGates of the selected CC-AP/Survivable OpenScape 4000 SoftGate Emergency groups
- locally on a CC-AP/Survivable OpenScape 4000 SoftGate

if the local CC-AP/Survivable OpenScape 4000 SoftGate is selected

a) local CC-AP/Survivable OpenScape 4000 SoftGate

- all of the CC-AP/Survivable OpenScape 4000 SoftGate Emergency groups
- all access points/OpenScape 4000 SoftGates of the CC-AP/Survivable OpenScape 4000 SoftGate Emergency groups

if the local CC-AP/Survivable OpenScape 4000 SoftGate is not selected: system message

DISPLAY-APESU:EGRPNO=xx; **or** DISPLAY-APESU:,xx;

- OpenScape 4000 host system
  - selected emergency group
  - all access points/OpenScape 4000 SoftGates in the selected emergency group
- locally on a CC-AP/Survivable OpenScape 4000 SoftGate

if an emergency group in the local CC-AP/Survivable OpenScape 4000 SoftGate is selected

a) selected emergency group

- all access points/OpenScape 4000 SoftGates in the selected emergency group

otherwise: system message

DISPLAY-APESU:APNO=xx; **or** DISPLAY-APESU:,,xx;

- OpenScape 4000 host system
  - selected access point/OpenScape 4000 SoftGate
- locally on a CC-AP/Survivable OpenScape 4000 SoftGate

if an access point/OpenScape 4000 SoftGate of an emergency group in the local CC-AP/Survivable OpenScape 4000 SoftGate is selected

a) selected access point/OpenScape 4000 SoftGate

otherwise: system message

CC-AP/Survivable OpenScape 4000 SoftGate-specific block:

```
 +-------------------------------------------------------------------
+
          | CC-AP: 99                                        IP
 ADDRESS:192.168.23 .199        |
          |SPEED/WORK MODE(IPDA): 100MBFD
                                |

 +-------------------------------------------------------------------
+
```

Emergency group-specific block:

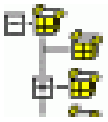
```
+-------------------------------------------------------------------
+
| AP EMERGENCY GROUP: 2    CC-AP: 99
 NAME: BERLIN          |
| THRSHLD: 100         SBMODE: AUTO
                      |
| STABLE: 10 MIN         SBBEGIN: 20 H    SBEND: 6 H
 SBOFFSET: 13 MIN       |
+-------------------------------------------------------------------
+
```

Access Point/OpenScape 4000 SoftGate-specific block:

```
+-------------------------------------------------------------------
+
| AP: 99 AP EMERGENCY GROUP: 2    CC-AP: 99    WEIGHT: 70
   SWMODE: GROUP    |
| CONTROL UNIT: HOST-CC          SIGNAL PATH: LAN
                     |
| LAST RECORDED CONNECTION STATUS CHANGE:
                     |
|
                     |
|      HOST-CC:   CONNECTED: yes       CONNECTED SINCE:
 08-06-2004 18:20       |
|      CC-AP:     CONNECTED: yes       CONNECTED SINCE:
 18-06-2004 23:01       |
+-------------------------------------------------------------------
+
```

11.2.12 Administration Switchover of Access Points/OpenScape 4000 SoftGates

11.2.12.1 Administration Switchover of Access Points/OpenScape 4000 SoftGates via Configuration Management



Configuration Management > System Data > Maintenance > IPDA - CC Access Point Maintenance

Click **Search** and select CC-AP/Survivable OpenScape 4000 SoftGate.

In the main menu, select -> **Action** -> **Execute**.

In the mask that this generates, you can set

- whether the switchover should be to normal or emergency mode,
- whether a particular access point/OpenScape 4000 SoftGate, all access points/OpenScape 4000 SoftGates of a particular emergency group, all access points/OpenScape 4000 SoftGates of all emergency groups in the selected CC-AP/Survivable OpenScape 4000 SoftGate, or the entire system should be switched over.

11.2.12.2 Administrator Switchover of Access Points/OpenScape 4000 SoftGates via AMO

Administrative switchover of access points/OpenScape 4000 SoftGates to and from the central control to CC-AP/Survivable OpenScape 4000 SoftGate is possible at any time.

The task is forwarded to the OpenScape 4000 host system via AMO. From there, it is sent to the affected CC-AP/Survivable OpenScape 4000 SoftGate via an affected access point/OpenScape 4000 SoftGate. Finally, the CC-AP/Survivable OpenScape 4000 SoftGate instructs the HG 3575 of the affected access points/OpenScape 4000 SoftGates to start up with the requested control (central control (host) or CC-AP/Survivable OpenScape 4000 SoftGate). If more than one CC-AP/Survivable OpenScape 4000 SoftGate is affected, this process is repeated for each CC-AP/Survivable OpenScape 4000 SoftGate.

Communication from the OpenScape 4000 host system to the CC-AP/Survivable OpenScape 4000 SoftGate via access points/OpenScape 4000 SoftGates requires that at least one access point/OpenScape 4000 SoftGate has a connection to both the central control and the CC-AP/Survivable OpenScape 4000 SoftGate. If this is not the case, switchover cannot be initiated.

The switchover can take place at various levels:

- all access points/OpenScape 4000 SoftGates of all emergency groups of all CC-APs in the system
- `EXEC-APESU:SYSMODE=EMERG,LEVEL=SYSTEM;` switches to the CC-AP/Survivable OpenScape 4000 SoftGate `EXEC-APESU:SYSMODE=NORMAL,LEVEL=SYSTEM;` switches to the central control
- all access points/OpenScape 4000 SoftGates of all emergency groups of one CC-AP/Survivable OpenScape 4000 SoftGate

- `EXEC-APESU:SYSMODE=EMERG,LEVEL=CCAP,NO=99;` switches to the CC-AP/Survivable OpenScape 4000 SoftGate `EXEC-APESU:SYSMODE=NORMAL,LEVEL=CCAP,NO=99;` switches to the central control
- all access points/OpenScape 4000 SoftGates of one emergency group (of one CC-AP/Survivable OpenScape 4000 SoftGate)
- `EXEC-APESU:SYSMODE=EMERG,LEVEL=APEGRP,NO=2;` switches to the CC-AP/Survivable OpenScape 4000 SoftGate `EXEC-APESU:SYSMODE=NORMAL,LEVEL=APEGRP,NO=2;` switches to the central control
- one access point/OpenScape 4000 SoftGate (of one emergency group (of one CC-AP/Survivable OpenScape 4000 SoftGate))
- `EXEC-APESU:SYSMODE=EMERG,LEVEL=AP,NO=99;` switches to CC-AP/Survivable OpenScape 4000 SoftGate `EXEC-APESU:SYSMODE=NORMAL,LEVEL=AP,NO=99;` switches to the central control

---

IMPORTANT: The switchover is always performed for all selected access points/OpenScape 4000 SoftGates that have contact with the requested control, regardless of group rules. If some access points/OpenScape 4000 SoftGates in a selection (SYSTEM, CC-AP/Survivable OpenScape 4000 SoftGate, APEGRP) do not have contact with the requested control, these are **not** switched over. The AMO then issues the message “partially performed“. Following a partial switchover, resources important for operation (such as trunk lines) may not be available for a group! For this reason, the connection status **must** be queried and verified before a manual switchover. See Section 2.11, “Querying the Connection Data”.

IMPORTANT: Access points/OpenScape 4000 SoftGates that are switched over independently of the group and that do not have their own trunk or tie line only allow access point/OpenScape 4000 SoftGate internal communication. **This prevents emergency calls from being forwarded over the trunk, for example.**

Table 72: AMO APESU parameter in the EXEC branch

AMO	Parameter	Sprache/ Language	Beschreibung/ Description
APESU	SYSMODE	d	Gibt an, welche Steuerung übernehmen soll. Werte: NORMAL: zentrale Steuerung (Host) EMERG: Emergency Steuerung (CC-AP/ Survivable OpenScape 4000 SoftGate)

AMO	Parameter	Sprache/ Language	Beschreibung/ Description
	SYSMODE	e	Identifies, which control shall take over. Values: NORMAL: Central Control (Host) EMERG: Emergency Control (CC-AP/ Survivable OpenScape 4000 SoftGate)
	LEVEL	d	Gibt an, auf welcher System-Ebene umgeschaltet werden soll. Werte: SYSTEM: gesamtes System (alle Access Points/OpenScape 4000 SoftGates, APEGRPs, CC-APs) CCAP: ein CC-AP/Survivable OpenScape 4000 SoftGate (alle Access Points/ OpenScape 4000 SoftGates, APEGRPs) APEGRP: eine Emergency Gruppe (alle Access Points/OpenScape 4000 SoftGates) AP: ein Access Point/OpenScape 4000 SoftGate
	LEVEL	e	Identifies on which system level the switch over shall be executed. Values: SYSTEM: complete system (all access points/OpenScape 4000 SoftGates, APEGRPs, CC-APs) CCAP: one CC-AP/Survivable OpenScape 4000 SoftGate (all access points/ OpenScape 4000 SoftGates, APEGRPs) APEGRP: one Emergency Group (all access points/OpenScape 4000 SoftGates) AP: one Access Point/OpenScape 4000 SoftGate
	NUMMER	d	Gibt die Nummer des betroffenen CC-AP/ Survivable OpenScape 4000 SoftGate, der Emergency Gruppe oder des Access Points/ OpenScape 4000 SoftGates an.
	NO	e	Identifies the number of the affected CC-AP/Survivable OpenScape 4000 SoftGate, Emergency Group or Access Point/ OpenScape 4000 SoftGate

11.2.13 Time Synchronization Between the Host System and CC-AP/ Survivable OpenScape 4000 SoftGate

An exact time is required for many OpenScape 4000 functions (call detail recording, time-dependent channels, night service, etc.). All clocks in the system (up to 84) have to operate synchronously.

There are two ways of synchronizing the time:

1) A time server is available in the IP network, which supports time synchronization of all OpenScape 4000 processors (the central processor and all survivability units) using the Network Time Protocol.

2) A time server is **not** available in the IP network. The OpenScape 4000 platform then makes its local time available over the network for synchronizing all survivability units.

For more information on date/time settings and time synchronisation please refer to Section 1.11, “Time Synchronization”.

11.2.14 Initial Startup of the CC-AP/Survivable OpenScape 4000 SoftGate

11.2.14.1 Preparation

During the initial installation, you must make sure that the same APS version that is currently running on the host system is also running on the CC-AP/ Survivabel OpenScape 4000 SoftGate hard disk.



DISPLAY-APS;

This display on the OpenScape 4000 host system outputs the part numbers of the loaded program system. Of interest here is the part number of the **Y0**-APS.

PROGRAM SYSTEM	: Y0-EN0YC
VERSION NUMBER	:10
CORRECTION VERSION NUMBER	: 001
PART NUMBER	: **P30252x**xxxxxxxxxx
PROGRAM SYSTEM WITH CODE SUBSYSTEMS	
INTERFACE VERSION:	
PROGRAM SYSTEM CONTAINS NO INTERFACE VERSION	

11.2.14.2 C-AP

Please refer to the appropriate How To in the Release Note for OpenScape 4000.

11.2.14.3 Survivable OpenScape 4000 SoftGate

Please refer to the appropriate How To in the Release Note for OpenScape 4000.

11.2.15 Verification and Acceptance of the AP Emergency Configuration

The customer uses the AP Emergency feature to facilitate telephone calls during emergency situations where the central control and/or essential components of the IP infrastructure are not available.

As a rule, this emergency situation occurs only very rarely. For this reason it is particularly crucial that the emergency measures function as intended, should they actually be needed at some point.

It is essential that the function of the AP Emergency configuration be verified by an acceptance test after the initial startup and after substantial modifications.

To this end, each emergency group must be switched over once to the CC-AP/Survivable OpenScape 4000 SoftGate for administration. In emergency operation, it must then be verified that emergency calls, communication to the trunk and other systems in the network, and communication between emergency groups at different CC-APs function as planned. Where applicable, also include installed applications that support emergency operation in the test.

Also verify the communications capability of access points/OpenScape 4000 SoftGates that can be switched to the CC-AP/Survivable OpenScape 4000 SoftGate independently of the emergency group when the group is running in normal operation.

You can conduct the tests when the system load is low.

11.3 Backup & Restore

11.3.1 OpenScape 4000 Assistant Backup & Restore on OpenScape 4000 Host System

To support the backup and restore processes for the AP Emergency feature, the OpenScape 4000 Assistant Backup & Restore application replicates the software and the configuration data from the host system to the CC-APs/ Survivable OpenScape 4000 SoftGates.

It must be differentiated between HOST and APE:

- HOST
- OpenScape 4000 Platform with the virtual machines ADP/CCA, OpenScape 4000 Assistant and OpenScape 4000 CSTA.
- APE

- OpenScape 4000 Platform with the virtual machines CCAP, OpenScape 4000 Assistant and OpenScape 4000 CSTA.

  Therefore, there are four possible systems that have to be synchronized. But at the moment only CC-AP on APE is synchronized with ADP/CCA on host. This is provided by OpenScape 4000 Assistant Backup & Restore.

  For more information please refer to the online help of Backup & Restore.

Basic conditions regarding timing

A backup can only be carried out when the AP backup server is free, i.e. not currently blocked by restore processes. You can set the number of simultaneous restore processes allowed, in order to limit the load on the server or network.

The interval between two scheduled backups must therefore be sufficient to allow the backup and restore processes of all CC-APs in the system to be carried out.

If the number of CC-APs is larger than the number of restore operations supported simultaneously, some CC-APs must wait until the capacity on the AP backup server is free before performing restore procedures. This leads to an increase in the required restore time that must be considered in the process as a whole.

The time required is determined by the data volume to be transported and the available transmission bandwidth. The maximum data volume (in the case of a system maintenance release) is estimated at 100 MB. The average size will be less than 10% of the maximum.

If the restore process on the CC-AP/Survivable OpenScape 4000 SoftGate requires a great deal of time (available transmission bandwidth is limited), you must ensure that all CC-APs can be restored at the same time.

The start time for the backup also determines indirectly the content of the database. For example, if the customer usually activates fixed call forwarding on the telephone and if the backup is performed outside business hours, the saved database will contain the activated call forwarding settings. But if a problem arises during the day, which initiates emergency mode, it will be initiated with the saved call forwarding settings.

11.3.1.1 Configuring an AP Backup Server with OpenScape 4000 Assistant Backup & Restore

In the first configuration step, you define where the OpenScape 4000 backup data should be stored. To do this, you must specify the computer that should act as the file server (AP backup server), the directory where the data should be stored, and the login data for access. Configuration on the file server (create the directory, define the user ID) should be completed before the configuration as part of OpenScape 4000 Assistant Backup & Restore.

- Use the Web browser to display the OpenScape 4000 Assistant start page and log in with the user ID “`rsta`“.
- In the left menu bar, select the function area **Software Management**.
- Select the application **Backup & Restore** provided as a submenu option under **Software Management**.

- In the Backup & Restore user interface, select the function **AP Backup Server** under **Administration**.

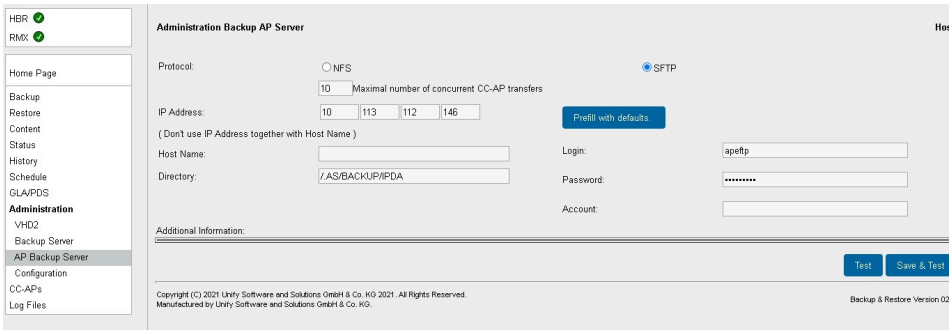


Figure 212: OpenScape 4000 Assistant Backup & Restore: configuring an AP backup server

1) The following fields must be now be completed:

- Select the **Protocol** (**SFTP** or **NFS**) - typically: **SFTP**

If you want to configure the AP backup server on the OpenScape 4000 host system, you must select **SFTP** as the protocol.

- **Maximum number of concurrent CC-AP/Survivable OpenScape 4000 SoftGate transfers**

In the maximum configuration, 83 CC-APs may want to sign on to the AP backup server and download the latest backup set simultaneously. If the server does not support this large number of simultaneously logged-in systems, or if you want to reduce possible load peaks on the server, you can adjust the maximum number of simultaneously logged-in CC-APs accordingly. Dependencies are shown in “Section 3.1, “Basic conditions regarding timing”“.

- Enter the **IP Address** or **Host Name** of the AP backup server

You can only enter a host name if either it is configured directly in UBA or if the name resolution is configured with DNS.

- Enter the **Directory** on the AP backup server that should be used for the backup and restore

If you want to configure the AP backup server on the OpenScape 4000 host system, you must select the directory already provided for this purpose (“`/.AS/BACKUP/IPDA`“).

The directory must be able to hold approximately 100 MB of data.

- If you selected **SFTP** as the protocol, you still need to configure the **Login** name and the **Password** for accessing the AP backup server (SFTP server). If the SFTP server requires an **Account**, this also needs to be entered.

If you want to run the AP backup server on the OpenScape 4000 host system, for security reasons you should configure the login under `apeftp`. You do not need to configure an account in this case.

IMPORTANT: Remember that the login password for the AP backup server must be maintained, both on the backup server and in the OpenScape 4000 Assistant Backup &

Restore configuration of the OpenScape 4000 host system and the CC-APs.

Complete the AP backup server configuration with

- **Save & Test** - Save the configuration and test the access to the AP backup server.

  You should always use this option if the file server is already available when it is configured in the network.
- **Test** - Test the configuration without saving it. Input will revert after the test.

  Use this option only for diagnostic purpose, when you do not want to clear a previously saved setting.

  In this way, the memory is configured for backup.

11.3.1.2 Creating a Schedule for the Backup

In the second configuration step, you must now define when OpenScape 4000 Assistant Backup & Restore should carry out a backup on the configured AP backup server. Typically, a backup is performed daily at a time when there is not much activity.

When you select a start time for the backup, keep in mind that this also indirectly defines the start time for the restore on the CC-APs. The restore on the CC-AP/Survivable OpenScape 4000 SoftGate starts as soon as the CC-AP/Survivable OpenScape 4000 SoftGate detects availability of new completed backup. Dependencies are shown in the section “Section 3.1, “Basic conditions regarding timing”“.

Prerequisite:

- Logged on to the OpenScape 4000 Assistant via a Web browser under the ID “`rsta`“.
- **Software Management** -> **Backup & Restore** has been started.
- In the OpenScape 4000 Assistant Backup & Restore user interface, select the function **Schedule**.

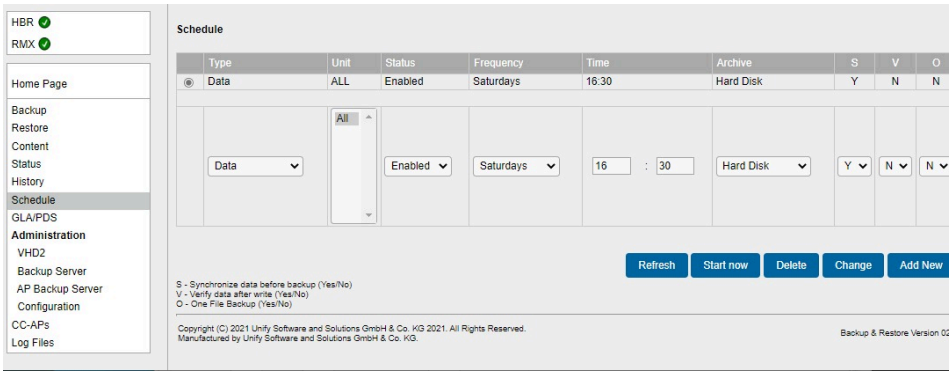


Figure 213: OpenScape 4000 Assistant Backup & Restore: Creating a schedule for the backup

The following fields must be now be completed:

Table 73: Input fields in the OpenScape 4000 Assistant Backup & Restore schedule

Field name	Value	Explanation
Type	AP Emergency	Only this value is permitted
Unit	All	Only this value is permitted
Status	Activated	This is where a configured schedule can be activated or deactivated.
Frequency	Daily (weekdays, Mondays, Tuesdays, Wednesdays, ...)	Typically, a backup should be carried out daily.
Time	Hour: Minute	Time of day at which the backup should start
Archive	AP backup server	Only this value is permitted - AP backup server must already have been configured.
S	**Yes**	Synchronize before backup, i.e. perform UPDATE. Must be set to **Yes** so that the latest version of the database is saved.
V	Yes/**No**	Backup data verification
O	Yes/**No**	One File Backup
I	Yes/**No**	Include installation partition

To perform more than one backup a day, enter additional daily backups in the schedule, for example, one backup at 12 noon and an additional one at 6pm.

Complete the AP backup server configuration with

- **Add New**- The new entry is saved in the timetable. A backup is performed according to the configuration.

This completes configuration on the OpenScape 4000 host system.

The time required for a backup procedure depends heavily on the amount of data to be transferred and the transmission bandwidth available between the host system and the AP backup server. The procedure takes at least one hour.

11.3.1.3 Performing the First Backup

So that as little time as possible is lost before the CC-APs can collect the data, it may be useful to initiate a backup immediately, i.e. outside of the configured schedule.

Do this by selecting a schedule for AP Emergency and clicking **Start now**.

The first system backup takes the longest, because all saved data (approximately 100 MB) must be transferred to the AP backup server for the first time. The time required is also heavily dependent on the available bandwidth in the IP network between the OpenScape 4000 host system and the AP backup server.

11.3.1.4 Using OpenScape 4000 Assistant Backup & Restore for more extensive Changes in the System

If you need to make extensive changes to the system, or if you are importing a new system version, the following requirements could arise:

- Larger configuration changes should be distributed to all CC-APs as quickly as possible
  - After completing the changes, you should initiate an “unscheduled“ backup. However, make sure that you verify that there is sufficient transmission bandwidth available in the network at this time to complete the backup and the subsequent restore operations of the CC-APs. Remember that you cannot cancel backup and restore procedures that are active. It may be useful to deactivate the backup process before making the changes. -> See the second point. In the OpenScape 4000 Assistant Backup & Restore, go to the schedule for the backup type “AP Emergency“ and click **Start now**. It is not advisable to use “Backup“ for this. If you do, you must remember to run an EXEC-UPDAT beforehand.
- You should verify new SW (regardless of whether it is a pre-revision bug fix of an LW or a new system version) on the host system first, before distributing it to all CC-APs.
  - *Before importing new SW:* In the OpenScape 4000 Assistant Backup & Restore, go to the schedule for the backup type “AP Emergency“ and change the status from “**activated**“ to “**deactivated**“. If there are several entries in the schedule for the backup type “AP Emergency“, you must deactivate all entries that could apply during the planned interval.
  - *After successful verification of the SW:* In the OpenScape 4000 Assistant Backup & Restore, go to the schedule for the backup type “AP Emergency“ and change the status from “**deactivated**“ back to “**activated**“. If there are several entries in the schedule for the backup type “AP Emergency“, you must activate all entries that you previously deactivated. If the network allows it, it may be useful to initiate an unscheduled backup. -> See the first point.

11.3.1.5 Checking the Regular Activities of OpenScape 4000 Assistant Backup & Restore

In addition to the “usual“ methods (log files etc.), there is an option for communication with the backup server to query when and which processor was last in contact with the AP backup server.

Prerequisite:

- Logged on to the OpenScape 4000 Assistant via a Web browser under the ID “`rsta`“.
- **Software Management** -> **Backup & Restore** has been started.
- In the Backup & Restore user interface, select the function Log Files.

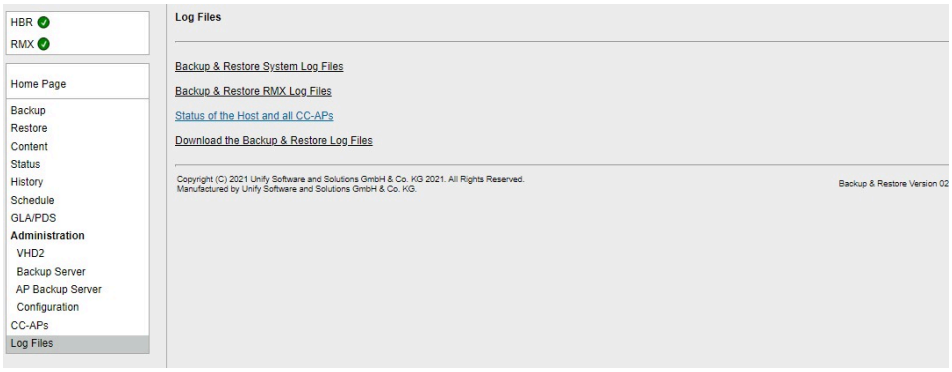


Figure 214: OpenScape 4000 Assistant Backup & Restore - Select “Log Files“

- Select “Status of Host and All CC-APs“ from the list

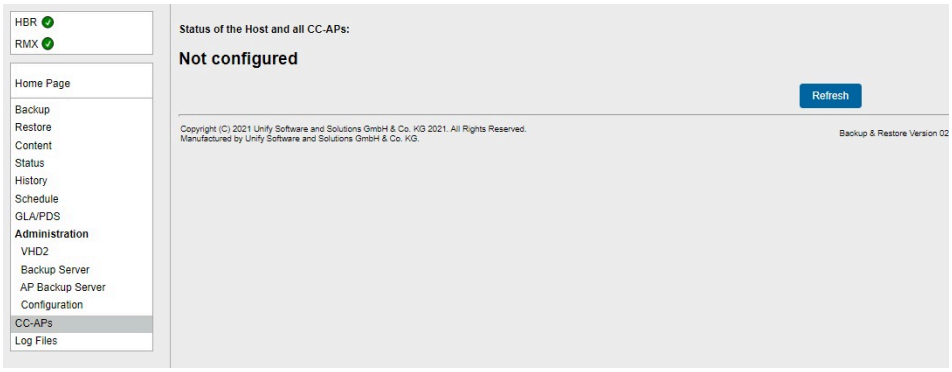


Figure 215: OpenScape 4000 Assistant Backup & Restore - Status of Host and CC-APs

The date and time data must be interpreted as follows:

Host:	Conclusion of last backup procedure
CC-AP/Survivable OpenScape 4000 SoftGate:	Time of last query on AP backup server (normally queries once every 10 minutes)

11.3.2 OpenScape 4000 Assistant Backup & Restore Configuration on the CC-AP/Survivable OpenScape 4000 SoftGate

11.3.2.1 Configuring the AP Backup Server on the CC-AP/Survivable OpenScape 4000 SoftGate

For the automatic restore of the saved data, you must stipulate where the OpenScape 4000 backup data should be retrieved. This requires that you set up the computer, directory and login data exactly as they were for the AP backup server on the OpenScape 4000 host system (see Section 3.1.1, “Configuring an AP Backup Server with OpenScape 4000 Assistant Backup & Restore”).

- In the Backup & Restore user interface, select the function **AP Backup Server** under **Administration**.

You must now complete the following fields with the same settings as the OpenScape 4000 host system:

- **Protocol** (**SFTP** or **NFS**) - typically: **SFTP**
- **IP Address** or **Host Name** of the AP backup server.
- **Directories** on the AP backup server.
- If you selected **SFTP** as the protocol, you still need to configure the **Login** name and the **Password** for accessing the AP backup server (SFTP server). If the SFTP server requires an **Account**, this also needs to be entered.

IMPORTANT: If you want to use as backup directory **/.AS/BACKUP/IPDA** for security reasons you should use as ftp login „apeftp“.

- By activating **Automatic restore disabled**, you can deactivate the restore process. Activate this switch only temporarily and never forget to deactivate the switch for routine operation.

Complete the AP backup server configuration with:

- **Save and test** - Save the configuration and test the access to the AP backup server.

  This option tests whether the installation works, i.e.:

  – Whether the connection to the AP backup server can be established.
  – Login with the configured data is possible.
  – Access to the configured directory is possible.
- **Test** - Test the configuration without saving it. Input will revert after the test.

  Use this option only for diagnostic purpose, when do not want to clear a previously saved setting.

Access to the AP backup server has now been configured. The OpenScape 4000 Assistant Backup & Restore application on the CC-AP/Survivable OpenScape 4000 SoftGate will now immediately start to contact the AP backup server every 10 minutes, check whether a new, completed backup set is available, and download and activate the modified sections of the backup set.

IMPORTANT: Before the first restore, OpenScape 4000 Assistant Backup & Restore performs a complete backup on the hard disk. This backup is used as a reference for determining modified files that must be retrieved from the AP backup server when the system is restored. You do have to initiate the backup manually. In addition, you cannot prevent it. This procedure takes approximately one hour.

The time required for the restore procedure depends heavily on the amount of data to be transferred and the transmission bandwidth available between the AP backup server and the CC-AP/Survivable OpenScape 4000 SoftGate. The procedure takes at least a half hour.

11.3.2.2 Configuring a Routine Configuration Data Backup to Hard Disk

While the CC-AP/Survivable OpenScape 4000 SoftGate draws the essential configuration data from the host system using restore, a regular backup of the specific local CC-AP/Survivable OpenScape 4000 SoftGate configuration is still worthwhile. Because changes to the local configuration are rather rare, a weekly backup is sufficient. When defining the starting time, make sure that this backup should run at an appropriate time, i.e. after the host system backup and subsequent restore on the CC-AP/Survivable OpenScape 4000 SoftGate.

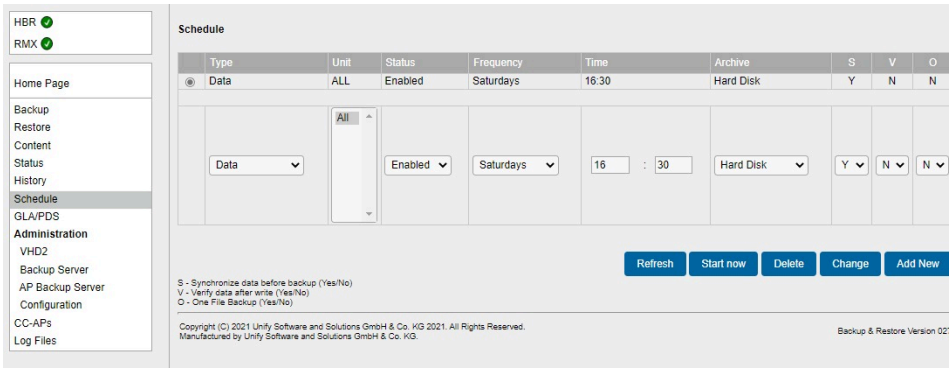
The example is based on the following plan:

1) Start backup of the host system: daily at 10:05pm

- Completion of the CC-AP/Survivable OpenScape 4000 SoftGate restore: by 6:30am, at the latest
- Local backup to hard disk: Sundays at 12:05pm

Prerequisite for the configuration:

- Logged on to the OpenScape 4000 Assistant via a Web browser under the ID “`rsta`“.
- **Software Management** -> **Backup & Restore** has been started.
- In the Backup & Restore user interface, select the function **Schedule**.



OpenScape 4000 Assistant Backup & Restore: Creating a schedule for the configuration data backup

The following fields must be completed:

Table 74: Schedule input fields for the configuration data backup

Field name	Value	Explanation
Type	Data	Only this value is permitted
Unit	All	Only this value is permitted
status	Activated	This is where a configured schedule can be activated or deactivated.
Frequency	for example, Sundays	Typically, a backup should be carried out weekly, for example, on Sundays.
Time	Hour: Minute	Time of day at which the backup should start
Archive	Hard disk	Only this value is permitted
S	Yes/**No**	Synchronize before backup, i.e. perform UPDATE. - Is not necessary in this case.
V	Yes/**No**	Backup data verification

Complete setup of the configuration data backup with

- **Add New** - The new entry is saved in the schedule. A backup is performed according to the configuration.

A backup procedure takes approx. 10 minutes.

11.4 Service Scenarios

11.4.1 Upgrading the AP Emergency Server (New Fix Release/Minor Release)

Procedure

The AP emergency computer regularly checks its backup sector for updated software packages. If there is a new software package there, it is copied to the AP emergency computer.

Notes

- Upgrade performed via Software Transfer/Software Activation. This will deliver the patches and upgrade all systems (OpenScape 4000 Platform, ADP/CCA/CCB, OpenScape 4000 Assistant, OpenScape 4000 CSTA). In such case the patches are transferred by OpenScape 4000 Backup & Restore to APE and applied there by OpenScape 4000 Software Activation.
- If an RMX upgrade was performed by replacing the HD within the context of the same major release, then the APE integrates both the RMX software and the OpenScape 4000 Assistant software. For this to function a backup is required including the install partition files. This can be selected under **OpenScape 4000 Assistant > Software Management > Backup &**

Restore > Schedule (Backup schedule for AP Emergency) with **I=Y** in the last column. This function is not guaranteed for a software upgrade to a future major release.

- If an RMX upgrade was performed by replacing the HD within the context of the same major release, then the APE integrates both the RMX software and the UW7 software (for this to function a backup is required including the new install partition files, this can be selected under HBR backup schedule for AP Emergency with I=Y in the last column). This function is not guaranteed for a software upgrade to a future major release.
- If an RMX upgrade was performed by replacing the HD (major release switch), then the procedure is the same as a new installation and the APE integrates only the RMX software. The OpenScape 4000 Assistant software is not upgraded.
- **The APE functionality is not dependent on the OpenScape 4000 Assistant version and therefore guaranteed accordingly.**

11.4.2 Replacing the DSCXL2 in the AP Emergency Server

Proceed as follows if there is a fault with the DSCXL2:

1) Remove the defective DSCXL2.
2) Install the new DSCXL2.
3) Reinstall the software (see How Tos for APE installation)

IMPORTANT: Please ensure that the software version installed on the AP emergency server corresponds to the software version of the host system (same minor or fix release).

---

1) Load the restore with the assistance of OpenScape 4000 Assistant "Backup & Restore".

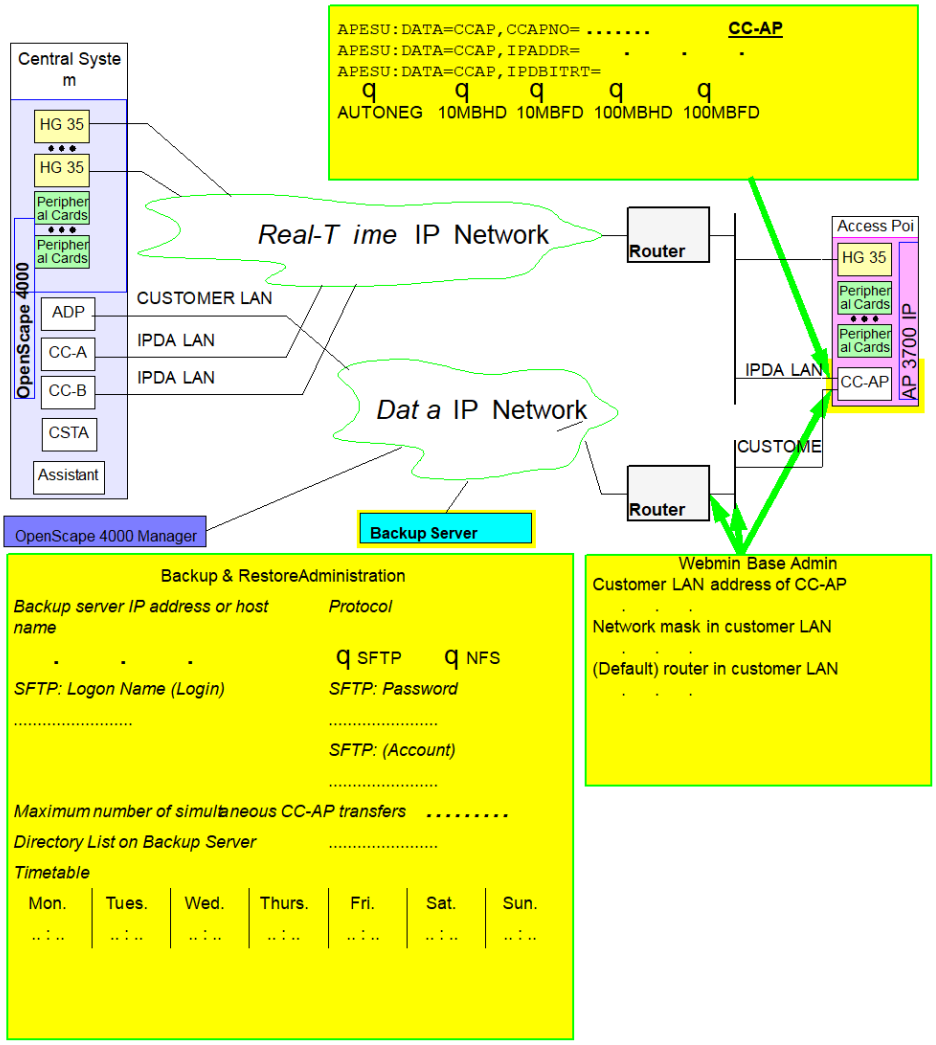
11.5 Spreadsheets - APE Configuration

The following spreadsheets are designed to help you perform an Access Point Emergency configuration. Each of the sheets has a configuration diagram and a blank AMO template on one side, and the completed example from the Service Manual on the other.

The following spreadsheets (with example) are available:

- AP Emergency spreadsheet: configuring a CC-AP
- AP Emergency spreadsheet: emergency group

AP Emergency spreadsheet: configuring a CC-AP



Two separate networks are shown in the spreadsheet for real-time or data communication. If one network is used for both communication types, both routers are identical.

AP Emergency spreadsheet: emergency group

Spreadsheet: Emergency Group								
	EGRPNO		Name					CCAPNO
Number		Name					CC-AP	
Switch to emergency mode					**Assigned access points**			
		THRSHLD			LTU	**Weight**	**SWMODE**	
Weighting threshold value					APNO		**SINGLE**	**GROUP**
							q	q
Reverting to normal mode							q	q

	SBMODE	**AUTO**matic	**MAN**ual				q	q
Revert mode		q	q				q	q
		STABLE					q	q
Stability time			[Minutes]				q	q
							q	q
Time frame for automatic switchover							q	q
	Hour	Minute (offset)					q	q
Start							q	q
End							q	q
	SBBEGIN	SBOFFSET					q	q
	SBEND						q	q
							q	q
							q	q
							q	q
							q	q
							q	q
							q	q
							q	q
							q	q
							q	q
		Total weight						

11.6 Information for network administrators

11.6.1 Survivability Unit for AP Emergency

The survivability unit integrates a control processor in an access point. A maximum of 83 survivability units can be integrated in the system with the maximum 83 access points per system.

The survivability unit processor requires 2 LAN connections in the IP network.

Detailed information can be found in “Section 2 - System Components (Harwdare & Software) > OpenScape 4000 in the Customer LAN > AP 3700 IP/ OpenScape 4000 SoftGate with Survivability Unit in the Customer LAN”.

An “IPDA“ interface is required for the signaling connection with the allocated access points.

PHY	10/100 Base T - autosensing or can be permanently set
MAC address	Permanently programmed ->sticker (the higher of the two addresses)
IP address	Configured in the OpenScape 4000 system, can be set
IEEE 802.1 p/q VLAN tagging	Configurable; priority bits are always set when active. See Table 3 “TOS values” in document “Gateways HG 3500 and HG 3575”. The VLAN ID can be set. Configuration in the OpenScape 4000 system.
TOS/DiffServ	The six highest bits in the TOS byte can be set. See Table 3 “TOS values” in document “Gateways HG 3500 and HG 3575”. Configuration in the OpenScape 4000 system.
Protocols/ports	See Chapter 20, “IP Ports” in the document “Gateways HG 3500 and HG 3575”.
Routing	The default host route, which is configured for HG 3575 in the same shelf, is used for the access point.
Firewall	The central processor only allows connections to addresses that it knows, i.e. access points or assigned service PCs.
Number of connections	Up to 83 TCP/IP connections (one per allocated access point)

An additional “CUSTOMER“ interface is required for remote access by OpenScape 4000 Manager and for accessing the file server, which distributes OpenScape 4000 central system software and data.

PHY	10/100 Base T - autosensing
MAC address	Permanently programmed on the board, ->sticker (lower of the two addresses)
IP address	Can be configured in the OpenScape 4000 Assistant
Routing	Configurable
Number of connections	TCP/IP connection to file server if required. Administration via OpenScape 4000 Assistant
Security	The same as for OpenScape 4000 Assisatnt

11.7 Quick Guide to Setting up an AP Emergency (IPDA)

11.7.1 Introduction

This chapter illustrates an AP Emergency configuration example and its generation by means of AMOs and OpenScape 4000 Assistant. An existing IPDA configuration is used.

Case distinction:

A distinction is made with an AP Emergency between a direct link and a networked configuration.

Direct Link means that the AP Emergency and OpenScape 4000 host system are in the same network segment (OpenScape 4000 LAN Segment).

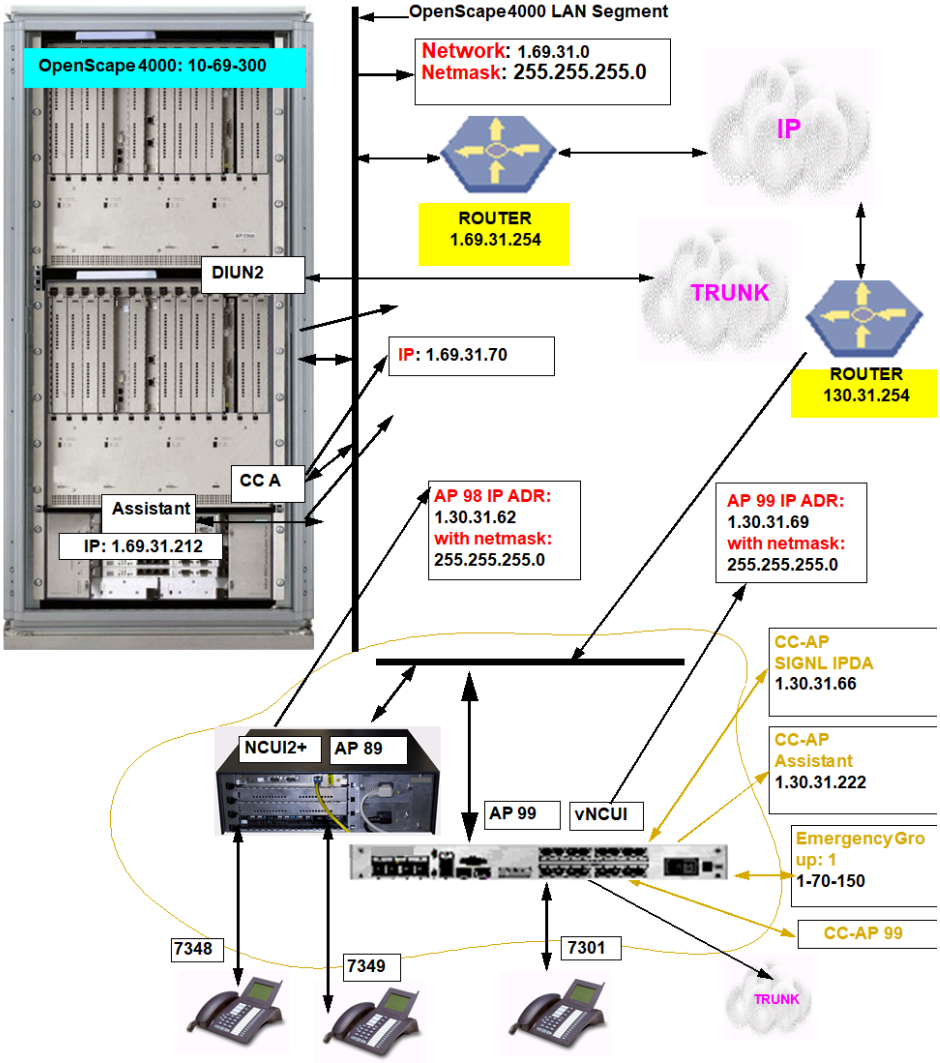
Networked Configuration means that the AP Emergency and OpenScape 4000 host system are in different network segments.

The following should be noted here:

- If the IPDA shelves in an emergency group are activated via a direct link, their associated emergency processor must likewise be activated via a direct link.
- If IPDA shelves are activated via a networked configuration, the associated emergency processor can be activated either via a direct link or networked configuration.

The configuration of a direct link emergency processor differs only marginally from that of a networked configuration. It must simply be noted in the case of a networked configuration that the respective router entries correspond in the OpenScape 4000 Assistants for host and APE.

The following generation example corresponds to the following configuration and IP situation:



11.7.2 Requirement

The IPDA feature is already installed. The relevant parameters are:

OpenScape LAN Segment	1.69.31.0, netmask 255.255.255.0
CC-A	1.69.31.70
CC-B	Not available
HG3575 - AP98	1.30.31.62, 255.255.255.0
vHG3575 - AP99	1.30.31.69, 255.255.255.0
Assistant - Customer LAN	1.69.31.212
Default Router - HHS	1.69.31.254
Default Router - AP-LAN	1.30.31.254

New IP addresses are required for the Access Point Emergency feature:

eth0 - SLES	1.30.31.220
Portal Access 500	1.30.31.221
Assistant Customer APE	1.30.31.222
CC-C (IPDA Signaling)	1.30.31.66

Licenses must be available in the code word to use AP Emergency.

IMPORTANT: Survivability and AP Emergency must be purchased in order to use it.

DISPLAY-CODEW;

```
-------------------------------------------+--------+------+-------+-------+ |
UNIT | PUR- | USED | FREE | BL- | | | CHASED | | | OCKED |
+-------------------------------------------+--------+------+-------+-------+ |
OPENSCAPE 4000 V6 FLEX | 12000 | 89 | 11911 | | | SIGNALING
SURVIVABILITY | 83 | 0 | 83 | | | CC-AP FOR AP EMERGENCY | 83 | 1 | 82 | |
+-------------------------------------------+--------+------+-------+-------+
```

11.7.3 Configuration Steps in OpenScape 4000

Step 1: Select the signaling IP address of the CC-AP

Requirement: `ADD-DIMSU:TYPE=SYSTEM,CCAP=xx;`

`ADD-APESU:DATA=CCAP,CCAPNO=99,IPADDR=1.30.31.66;`

IMPORTANT: The CC-AP number must be one of the AP (LTU) numbers that are configured in the system (usually the AP number, in which the CC-AP is incorporated).

Step 2: Configure AP Emergency Group

Requirement: `EINRICHTEN-DIMSU:TYP=SYSTEM,APEGRP=xx;`

```
ADD-
APESU:DATA=APEGRP,EGRPNO=1,CCAPNO=99,THRSHLD=0,SBMODE=AUTO,NAME="
MUC",STABLE=10,SBBEGIN=20,SBEND=6,SBOFFSET=15;
```

Parameter	Description
CCAPNO	Number of the CC-AP that controls the emergency group
NAME	Name of emergency group
SBMODE	Switchback mode: Manual or automatic (the switching interval is irrelevant with a manual switchback)
SBBEGIN	Switching interval: Start (hour) for automatic switchback
SBEND	Switching interval: End (hour) for automatic switchback

Parameter	Description
SBOFFSET	Switching interval: Minutes for RSBEGIN and RSENDE
STABLE	Stabilization time of LAN connection in minutes
THRSHLD	Threshold value for weighting algorithm Every AP is assigned a "weight" with AMO APESU. If the threshold value in the emergency group is exceeded, a switchover is made to this group's CC-AP.

Step 3: Configure AP 98 and 99 for AP Emergency

```
ADD-APESU:DATA=AP,APNO=98,EGRPNO=1,WEIGHT=0,SWMODE=GROUP;
```

```
ADD-APESU:DATA=AP,APNO=99,EGRPNO=1,WEIGHT=0,SWMODE=GROUP;
```

Step 4: Configure display readout in emergency mode on system telephone

```
CHANGE-ZANDE:TYPE=ALLDATA,APEDTXT="AP EMERGENCY";
```

Step 5: Define switching delay

e.g. : if a (OpenScape 4000) system RELOAD does not initiate emergency mode, a switching delay (in minutes) can be configured.

```
DISPLAY-SIPCO:TYPE=TIMING;
```

```
H500: AMO SIPCO GESTARTET
```

```
TIMING :
-----------------------------------------------------------------
PINGTIME ( UEBERW.-ZEIT FUER PAYLOAD PATH QUALITY ) : 60
SEK RESTIME ( RESET ZEIT BEI SIGNALING VERB. VERLUST ) :
60 SEK SUPVTIME ( UEBERW.-ZEIT FUER SUPERVISORY VERB. ) : 4
SEK APESWDLY ( APE UMSCHALTEVERZOEGERUNG. ) : 0 MIN ALVTIME
( UEBERW.-ZEIT FUER SIGNALING VERBINDUNG ) : 60 SEK
```

```
CHANGE-SIPCO:TYPE=TIMING,APESWDLY=<minutes>;
```

Step 6: Display AP Emergency configuration

```
DISPLAY-APESU:;
+-------------------------------------------------------------------
+
| AKTUELLE SYSTEMZEIT : 22-06-2012 09:35:47
                       |
+-------------------------------------------------------------------
+
+-------------------------------------------------------------------
+
| CC-AP: 99 IP ADRESSE: 1 .30 .31 .66
                       |
+-------------------------------------------------------------------
+
+-------------------------------------------------------------------
+
```

```
| AP EMERGENCY GRUPPE: 1 CC-AP: 99 NAME: HPA MUC
                        |
| SCHWELLE: 0 RSMODE: AUTO
                        |
| STABIL: 10 MIN RSBEGIN: 20 H RSENDE: 6 H RSOFFSET: 15 MIN
                        |
+-------------------------------------------------------------------
+
| AP: 98 AP EMERGENCY GRUPPE: 1 CC-AP: 99 GEWICHT: 0
 UMSCHALT: GRUPPE            |
| KONTROLL-EINHEIT: UNBEKANNT SIGNAL-PFAD: KEIN
                        |
| LETZTE AUFGEZEICHNETE VERBINDUNGS-STATUS-AENDERUNG:
                        |
|
                        |
| HOST-CC: VERBUNDEN: NEIN GETRENNT SEIT: 00-00-0000 00:00
                        |
| CC-AP: VERBUNDEN: NEIN GETRENNT SEIT: 00-00-0000 00:00
                        |
+-------------------------------------------------------------------
+
| AP: 99 AP EMERGENCY GRUPPE: 1 CC-AP: 99 GEWICHT: 0
 UMSCHALT: GRUPPE            |
| KONTROLL-EINHEIT: UNBEKANNT SIGNAL-PFAD: KEIN
                        |
| LETZTE AUFGEZEICHNETE VERBINDUNGS-STATUS-AENDERUNG:
                        |
|
                        |
| HOST-CC: VERBUNDEN: NEIN GETRENNT SEIT: 00-00-0000 00:00
                        |
| CC-AP: VERBUNDEN: NEIN GETRENNT SEIT: 00-00-0000 00:00
                        |
+-------------------------------------------------------------------
+
```

Step 7: Update the BP database and synchronize local HG3575 database

```
EXEC-USSU:MODE=UPDATAP,LTU=98;

EXEC-USSU:MODE=UPDATAP,LTU=99;

EXEC-UPDAT:UNIT=BP,SUSY=ALL;
```

Step 8: Check synchronicity of configuration management

After the setup is finished with AMO APESU, connect to the OpenScape 4000 Assistant in the host (e.g. http://1.30.11.212). Verify here first that the configuration management is in sync with the RMX system. If this is not the case, an upload must be performed.

To do this, go to **Configuration Management > Network > System**, click **Search** on the displayed page and start the upload if necessary with **Action**/ **Upload**.

Step 9: Configure the time server in the host

An exact time is required for many OpenScape 4000 functions. The OpenScape 4000 should therefore be connected to a time server. The procedure here is as follows:

1) Set up an ssl connection to the SLES (e.g. with putty), in this case to 1.30.31.210.
2) Log in with root/hicom and call yast.
3) Go to System / Date and Time in yast.
4) Set the Region (e.g. Europe) and Time Zone (e.g. Germany). Activate **Hardware Clock Set To UTC** and then go to the **Change Date and Time** page with **Change**. Enter the IP address of the time server here under **Synchronize with NTP Server** (in this case 1.50.100.2). Tick **Save NTP Configuration** and go to **Configure**.
5) Activate **Advanced NTP Configuration > Now and on Boot**. The NTP service restarts after pressing **Ok** and yast can be exited again.
6) The RMS time is updated with AENDERN-DATE:;

Step 10: Configure the system ID apeftp

Instead of a conventional system ID, the special system identifier apeftp should be used for transporting the APE backup set. To use apeftp, it has to be released explicitly. To do this, go to **Access Management > System Account Administration** in OpenScape 4000 Assistant and unlock the apeftp user and assign a password.

The same must also be done later in the OpenScape 4000 Assistant of the APE processor because the IDs and passwords are not synchronized via the APE backup.

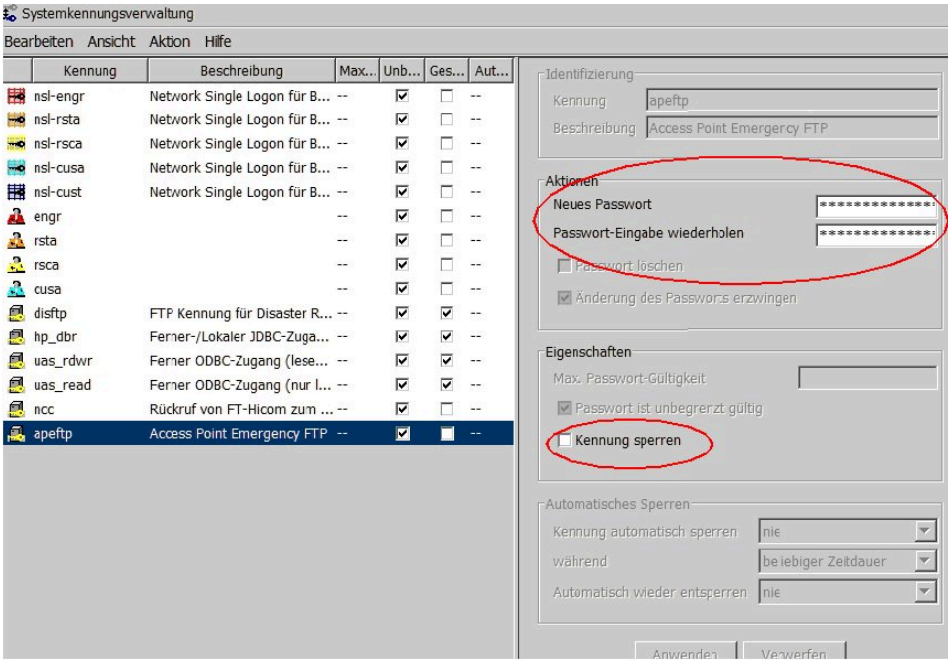


Figure 216: Configuring the system ID apeftp in the host

Step 11: Configure the AP backup server

OpenScape 4000 Assistant:

Software Management > Backup & Restore > AP Backup Server

The OpenScape 4000 is itself the backup server in this example. The directory /.AS/BACKUP/IPDA is provided in the system. Now select Test (also includes configuration).

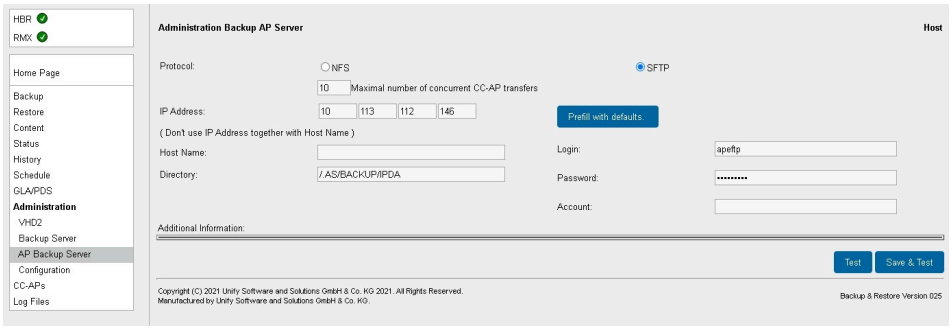


Figure 217: Configuring the AP backup server in the host

By setting the schedule for the backup, the transfer time to the CC-APs is defined indirectly. After a maximum of 10 minutes (not controllable) following the backup, the CC-APs recognize that a more recent backup set is available and automatically fetch the delta.

The first backup has to be started manually (step 2) with the initial installation in order to set up the feature fully.

Check the status after the manual backup:

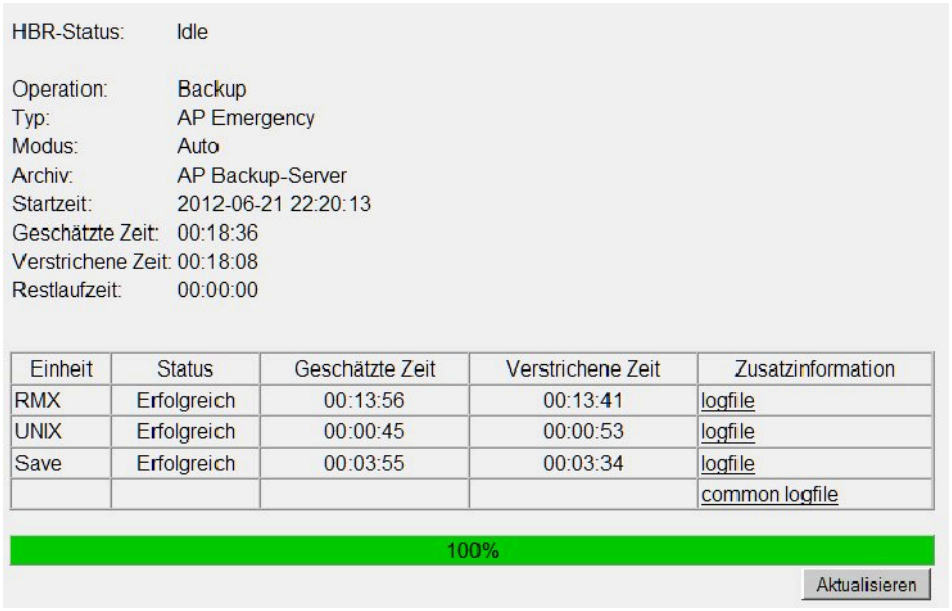


Figure 218: Checking the backup status

11.7.4 Configuration Steps in the CC-AP

Step 1: Install AP Emergency on DSCXL2 or OpenScape 4000 SoftGate/ OpenScape Access 500

1) USB installation of DSCXL2s (Deployment AP Emergency) or OpenScape 4000 SoftGate / OpenScape Access/Branch 500 (Deployment Survivable SoftGate).
2) Connect the monitor/keyboard or connect to the system using a standard IP address (192.168.0.2). Change the password for root (hicom). Set the IP address for SLES (default 192.168.0.2) in YaST, set the time server in the same way as in the host, switch the keyboard from English to German if appropriate (owing to special characters in the password).
3) Set up the connection to the OpenScape 4000 Platform Administration Portal via YaST. Launch the LAN wizard. The LAN wizard contains the initial config file for IPDA:

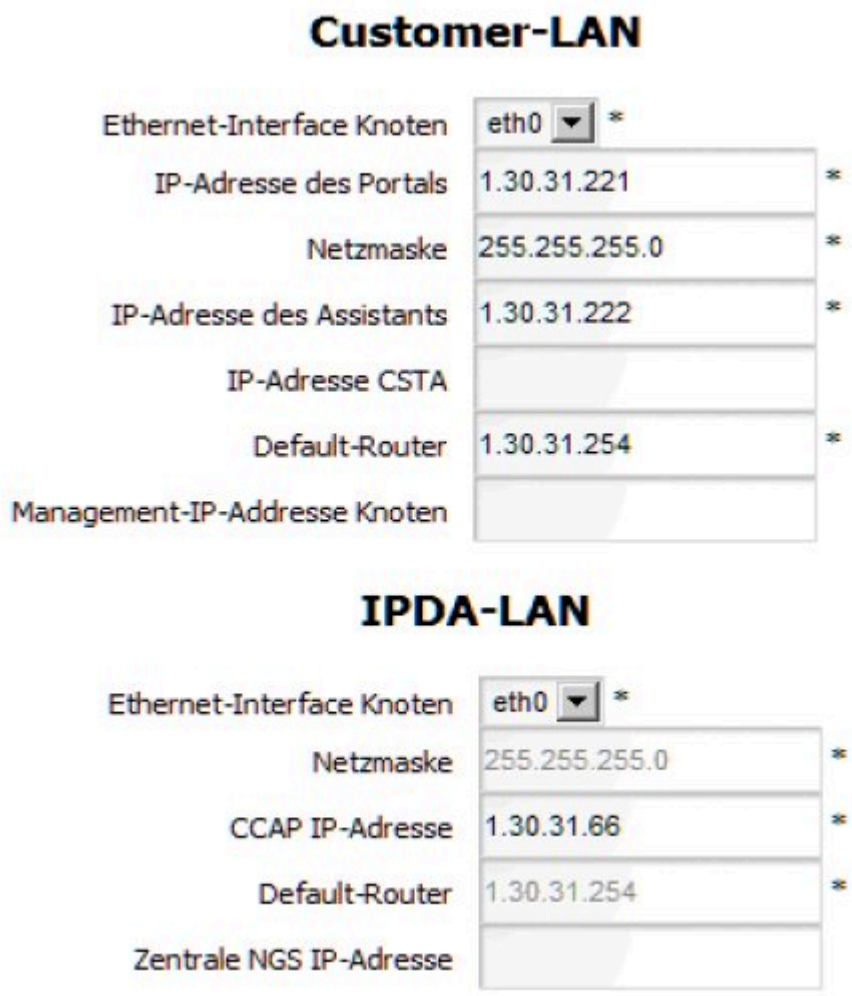


Figure 219: LAN wizard - Selecting the deployment for AP Emergency installation

Configure the IP address of the portal and the OpenScape 4000 Assistant in the LAN wizard. Please note here that this is about APE addresses and not host addresses.

If necessary configure the default router.

The IP address of the APE is entered under IPDA-LAN.



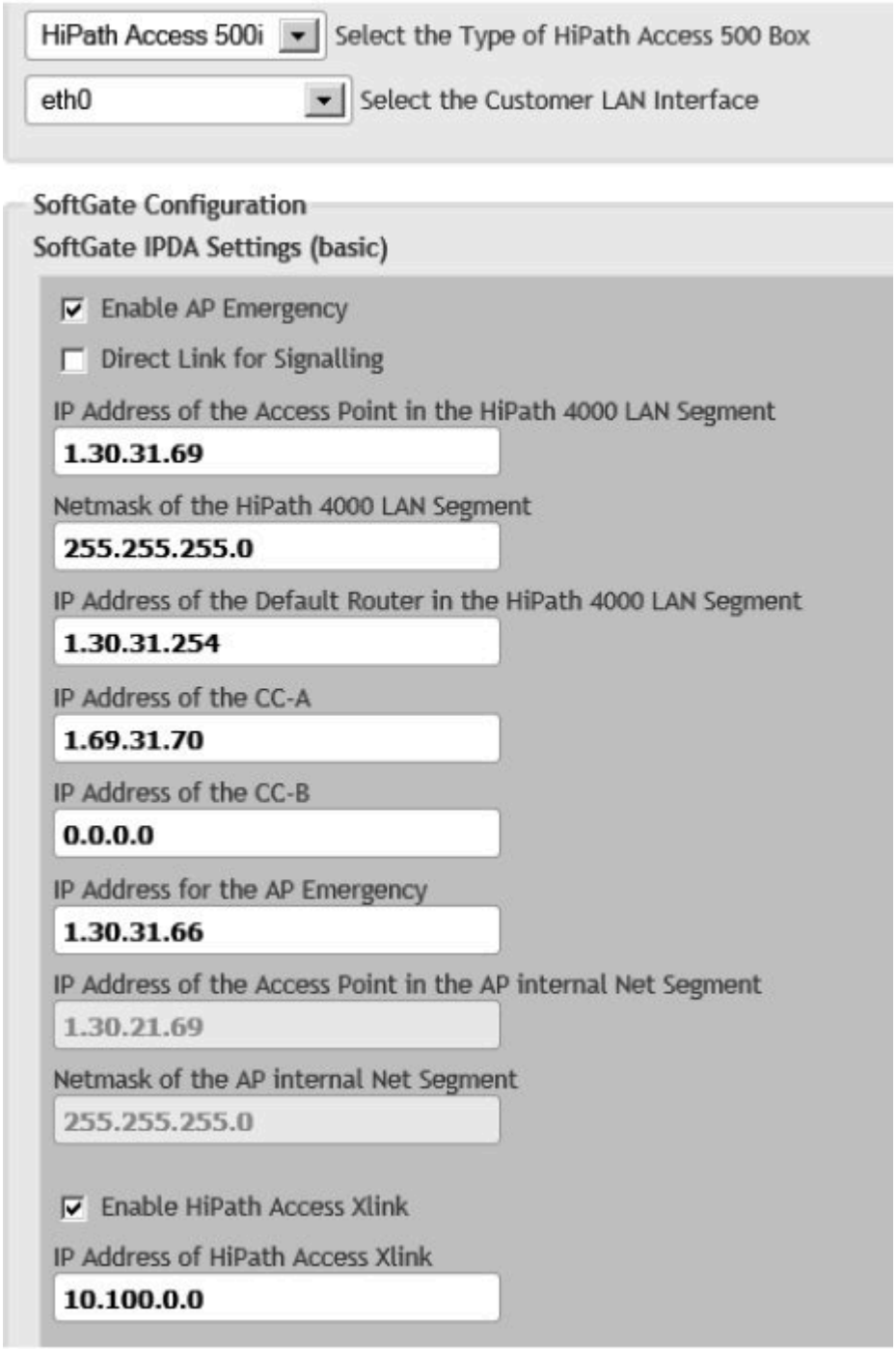
LAN wizard - Entering the customer LAN and IPDA LAN addresses

Make sure that the checkbox **Send AMO initialization commands** is activated in the **Internal LAN** section. The RMS configuration AMOs are configured automatically as a result.



Figure 220: LAN wizard - Send AMO initialization commands

Now configure the IPDA shelf (in this case as OpenScape 4000 SoftGate in Access 500/Branch).



Configuring the IPDA shelf

Step 2: Configure the user ID of the FTP user (apeftp)

The user for the FTP transport (apeftp) must also be activated in the CC-AP and configured with the same password as in the host.

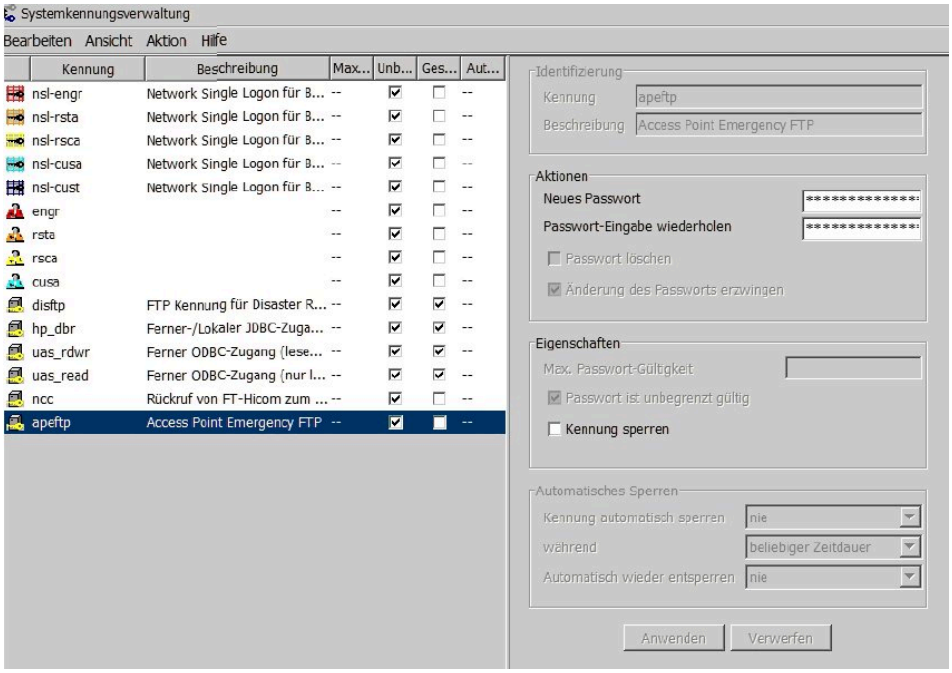


Figure 221: Configuring the apeftp system ID in the CC-AP

Step 3: Configure the FTP backup for APE in the CC-AP

Configure the FTP server for the APE backup in the OpenScape 4000 Assistant for the CC-AP. The entries are the same as in the host.

Synchronization of the CC-AP is started immediately with **Save & Test**.

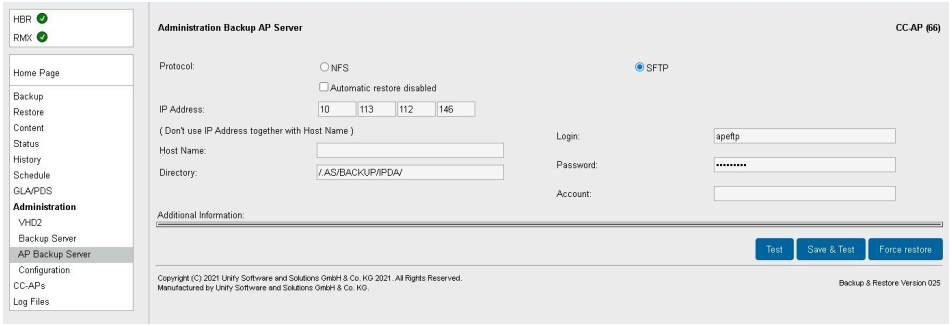
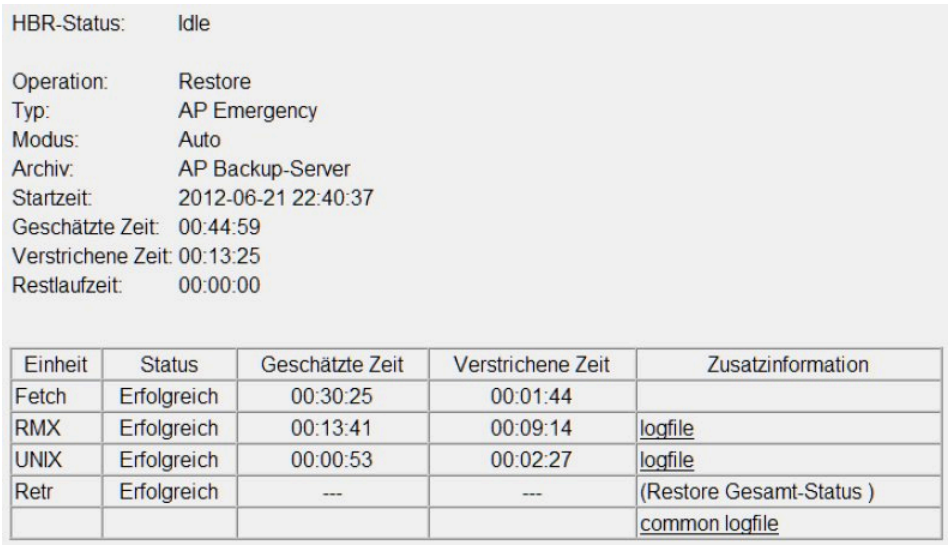


Figure 222: Configuring the AP backup server in the CC-AP

Step 4: Query the status

The progress can be seen on the HBR status page. With the initial installation, the CC-AP starts with a backup so that it has a comparison with the host backup. Immediately afterwards, the CC-AP starts with a restore, which is concluded with a reload. The CC-AP then starts up automatically. The CC-AP only performs restores in normal operation. To this end, the CC-AP contacts the AP backup server every 10 minutes and checks whether a new, complete backup set is available so as to then download and activate the modified sections of the backup set.

The time required for the restore procedure depends to a large extent on the amount of data to be transferred and the transmission bandwidth available between the AP backup server and the CC-AP. The process takes about half an hour, but may be shorter if only changes were made to the RMX.



HBR-Status: Idle

Operation: Restore
Typ: AP Emergency
Modus: Auto
Archiv: AP Backup-Server
Startzeit: 2012-06-21 22:40:37
Geschätzte Zeit: 00:44:59
Verstrichene Zeit: 00:13:25
Restlaufzeit: 00:00:00

Einheit	Status	Geschätzte Zeit	Verstrichene Zeit	Zusatzinformation
Fetch	Erfolgreich	00:30:25	00:01:44	
RMX	Erfolgreich	00:13:41	00:09:14	logfile
UNIX	Erfolgreich	00:00:53	00:02:27	logfile
Retr	Erfolgreich	---	---	(Restore Gesamt-Status)
				common logfile

Figure 223: Checking the backup status

Step 5: Output the APE status

DISPLAY-APESU;

H500: AMO APESU GESTARTET

```
+------------------------------------------------------------------------------+
| AKTUELLE SYSTEMZEIT  : 22-06-2012 10:38:14                                   |
+------------------------------------------------------------------------------+

+------------------------------------------------------------------------------+
| CC-AP: 99                          IP ADRESSE: 1  .30 .31 .66                |
+------------------------------------------------------------------------------+

+------------------------------------------------------------------------------+
| AP EMERGENCY GRUPPE: 1    CC-AP: 99          NAME: HPA MUC                   |
| SCHWELLE: 0         RSMODE: AUTO                                             |
| STABIL: 5   MIN     RSBEGIN: 20 H     RSENDE: 6  H     RSOFFSET: 15 MIN      |
+------------------------------------------------------------------------------+
| AP: 98  AP EMERGENCY GRUPPE: 1   CC-AP: 99  GEWICHT: 0     UMSCHALT: GRUPPE  |
| KONTROLL-EINHEIT: HOST-CC     SIGNAL-PFAD: LAN                               |
| LETZTE AUFGEZEICHNETE VERBINDUNGS-STATUS-AENDERUNG:                          |
|                                                                              |
|     HOST-CC:  VERBUNDEN: JA        VERBUNDEN SEIT: 22-06-2012  10:07         |
|     CC-AP:    VERBUNDEN: JA        VERBUNDEN SEIT: 22-06-2012  10:07         |
+------------------------------------------------------------------------------+
| AP: 99  AP EMERGENCY GRUPPE: 1   CC-AP: 99  GEWICHT: 0     UMSCHALT: GRUPPE  |
| KONTROLL-EINHEIT: HOST-CC     SIGNAL-PFAD: LAN                               |
| LETZTE AUFGEZEICHNETE VERBINDUNGS-STATUS-AENDERUNG:                          |
|                                                                              |
|     HOST-CC:  VERBUNDEN: JA        VERBUNDEN SEIT: 22-06-2012  10:08         |
|     CC-AP:    VERBUNDEN: JA        VERBUNDEN SEIT: 22-06-2012  10:08         |
+------------------------------------------------------------------------------+
```

11.7.5 Verification and Acceptance of the AP Emergency Configuration

It is essential that the function of the AP Emergency configuration be verified by an acceptance test after the initial startup and after substantial modifications.

To this end, each emergency group must be switched over once to the CC-AP for administration. In emergency mode, it must then be verified that communication with the trunk and with other systems in the network as well as among emergency groups at different CC-APs functions as planned. Where applicable, installed applications that support emergency operation should also be included in the test.

Also verify the communications capability of access points that can be switched to the CC-AP independently of the emergency group when the group is running in normal mode.

You can conduct the tests when the system load is low.

The following manual switching options are available:

- all access points of all emergency groups of all CC-APs in the system
- `EXEC-APESU:SYSMODE=EMERG,LEVEL=SYST;` switches to CC-AP

  `EXEC-APESU:SYSMODE=NORMAL,LEVEL=SYST;` switches to central control
- all access points of all emergency groups of one CC-AP
- `EXEC-APESU:SYSMODE=EMERG,LEVEL=CCAP,NUMMER=17;` switches to CC-AP

  `EXEC-APESU:SYSMODE=NORMAL,LEVEL=CCAP,NUMMER=17;` switches to central control
- all access points of one emergency group (of one CC-AP)
- `EXEC-APESU:SYSMODE=EMERG,LEVEL=APEGRP,NUMMER=1;` switches to CC-AP

  `EXEC-APESU:SYSMODE=NORMAL,LEVEL=APEGRP,NUMMER=1;` switches to central control
- one access point (of one emergency group (of one CC-AP))
- `EXEC-APESU:SYSMODE=EMERG,LEVEL=AP,NUMMER=17;` switches to CC-AP

  `EXEC-APESU:SYSMODE=NORMAL,LEVEL=AP,NUMMER=17;` switches to central control

11.8 FAQs - Frequently Asked Questions

1) **Question:** When the central system breaks down, an OpenScape 4000 system with IPDA and AP Emergency is divided into 5 islands. Each island is controlled by a survivability unit. Can islands communicate via IP insofar as this is permitted by the IP network?
2) **Answer:** No. Each island represents an individual system in emergency mode. These systems only communicate via CO or tie trunks.

   Follow-up question: If I configure IP trunking between the islands, will it work then?

   Answer: In principle yes, however, you cannot only configure IP trunking for emergencies. It must be configured in the central system and is then also available during normal operation. You must pay particular attention

here that you are dealing with tie trunks in normal operation within a system, something that is very difficult to manage in terms of LCR. Therefore, we would strongly advise against such scenarios.

3) **Question**: Is the Survivable OpenScape 4000 SoftGate (OpenScape Access/Branch 500 a/i/) able to take over the control (survival mode) for the local OpenScape 4000 SoftGate machine in case of a local LAN failure (L1/ eth0 down)?
4) **Answer**: Yes. On a OpenScape Access/Branch 500 hardware the signaling routing (HSR) can be handled on internal path (backplane), i.e. no external LAN needed. If there are OpenScape Access modules connected over Xlink they will continue to work also.
5) **Question**: Can Minor/Fixed Release upgrades be made via hard disk exchange with APEs and Survivable OpenScape 4000 SoftGates?
6) **Answer**: Please note when upgrading a system in the main system via hard disk exchange, the OpenScape 4000 Platform Administration (Portal), OpenScape 4000 CSTA and OpenScape 4000 Assistant[4] on APEs and Survivable OpenScape 4000 SoftGates will not be automatically upgraded.

   Under such circumstances there are two possible courses of action to ensure the APEs and Survivable OpenScape 4000 SoftGates receive the correct software afterwards:

   a) The new host system hard disk for the customer upgrade should be prepared in the lab with the identical version as the existing customer software level and then upgraded to the version the customer requires via SWA/SWT. In this way the upgrade history exists on the new hard disk and with the next HBR for the APE/Survivable OpenScape 4000 SoftGate the correct packages will be transferred and an automatic update performed to the correct OpenScape 4000 Platform Administration (Portal), OpenScape 4000 CSTA and OpenScape 4000 Assistant[4] versions.

   After installation of the new hard disk with a newer version made with First Installation, RMX would only upgrade on the APEs/Survivable OpenScape 4000 SoftGates, but OpenScape 4000 Platform Administration (Portal), OpenScape 4000 CSTA and OpenScape 4000 Assistant 1 versions will not be updated due to the missing upgrade history. Once the Fix Release/ Maintenance Release is transferred and activated individually on each APE/ Survivable OpenScape 4000 SoftGate via SWT/SWA, any subsequent Hot Fixes will be activated automatically with the next HBR.

IMPORTANT: Linux host OpenScape 4000 Platform Administration (Portal) (PLT) and OpenScape 4000 CSTA are not included in this backup. Therefore if host system is updated by replacing system hard disk, then each connected APE/Survivable OpenScape 4000 SoftGate has to be either installed anew or updated with RLC of the same version as the new host hard disk.

IMPORTANT: This handling of course does not apply for upgrades where a new installation is needed. After installing

[4] Note: OpenScape 4000 Assistant Upgrade can be forced via Option I in HBR, however this is not recommend as standard and would not upgrade the OpenScape 4000 Platform Administration (Portal) or OpenScape 4000 CSTA as already commented in the Service Manual.

the central host with OpenScape 4000 software, only RMX would replicate to APEs/Survivable OpenScape 4000 SoftGates, but OpenScape 4000 Platform Administration (Portal), OpenScape 4000 Assistant and OpenScape 4000 CSTA will not be updated. Therefore the APEs/Survivable OpenScape 4000 SoftGates must be newly installed and then synchronized with the central host.

7) **Question**: Should Activation of Hot Fixes on APEs and Survivable OpenScape 4000 SoftGates be made?
8) **Answer**: As per SWA graphical user interface activation hints:

   ATTENTION: Activation of Hotfixes and FR/MR should not be made directly on APE Nodes !!!

   Software updates should be activated directly on the Host system and will be mirrored to the APE nodes during the next APE restore process.

   Direct activation on APE should only be used in rare instances of first installation or manual upgrade.

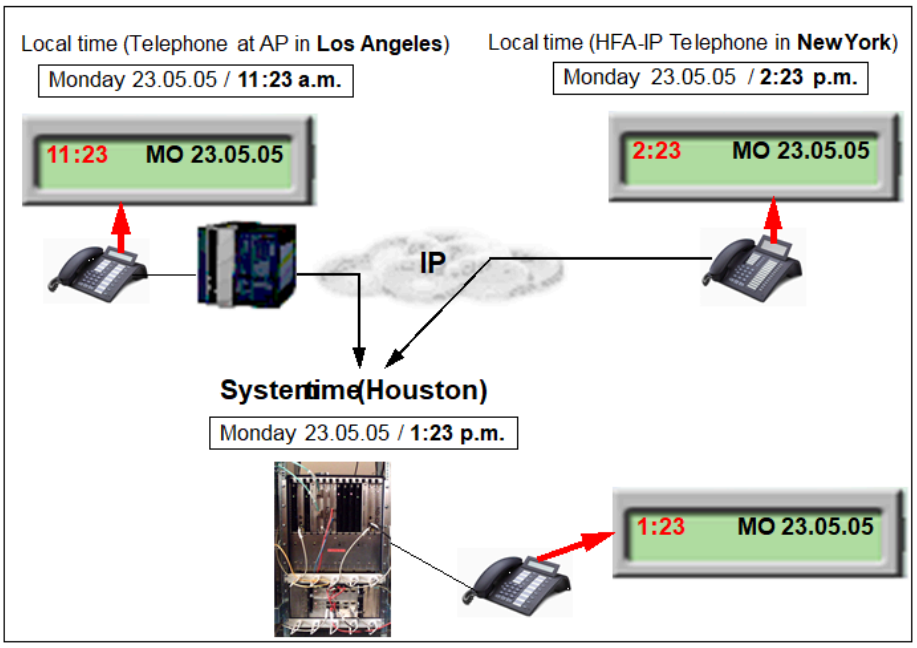
12 Different Time Zones (DTZ)

12.1 Feature Description

The “IPDA Different Time Zones (DTZ)” feature is used in situations when an IPDA shelf or access point (AP-IP) or HFA IP telephones are located in different time zones than the host system. In these cases, the local time of day should be shown instead of the system time on the display of the digital telephones that are connected to the remote AP or on the display of the HFA IP telephones.

Example for the local time display:

An OpenScape 4000 system in Houston (Texas) has one remote AP in Los Angeles (California) and one HFA IP telephone in New York (New York). All phones should display the local time.



Example: OpenScape 4000 system in Houston with external telephones in Los Angeles and New York

The local time is supported for the following functions:

1) Date and time of day in the idle display

- Daylight savings time and standard time
- Call list
- Callbacks
- Date/time button
- Date change at midnight

12.2 Service Information

In the OpenScape 4000, you can set up as many as 50 time classes using the AMO SIPCO. Local times have a fixed offset (in minutes: west or east) to the system time.

You can assign a time class to an IPDA shelf with the AMO UCSU. In this way, all Digits that have a display and that are configured on this shelf use this time class.

You can assign a time class to an HFA station with the AMO SDAT. If an HFA station that is configured on an IPDA shelf has no time class configured, the time class of the IPDA shelf is used. As soon as this HFA station is given a time class with the AMO SDAT, the time class of the IPDA shelf is ignored for this station.

The net must be also defined in AMO SIPCO, if only HFA subscribers are configured in a differed time zone.

- Using the IPDA wizard in the OpenScape 4000 Assistant, the time zones must be configured before in menu: Configuration Management -> System data -> IPDA -> IPDA data
- The time class (TCLASS) in AMO SDAT can only be changed for HFA subscribers.

Restrictions

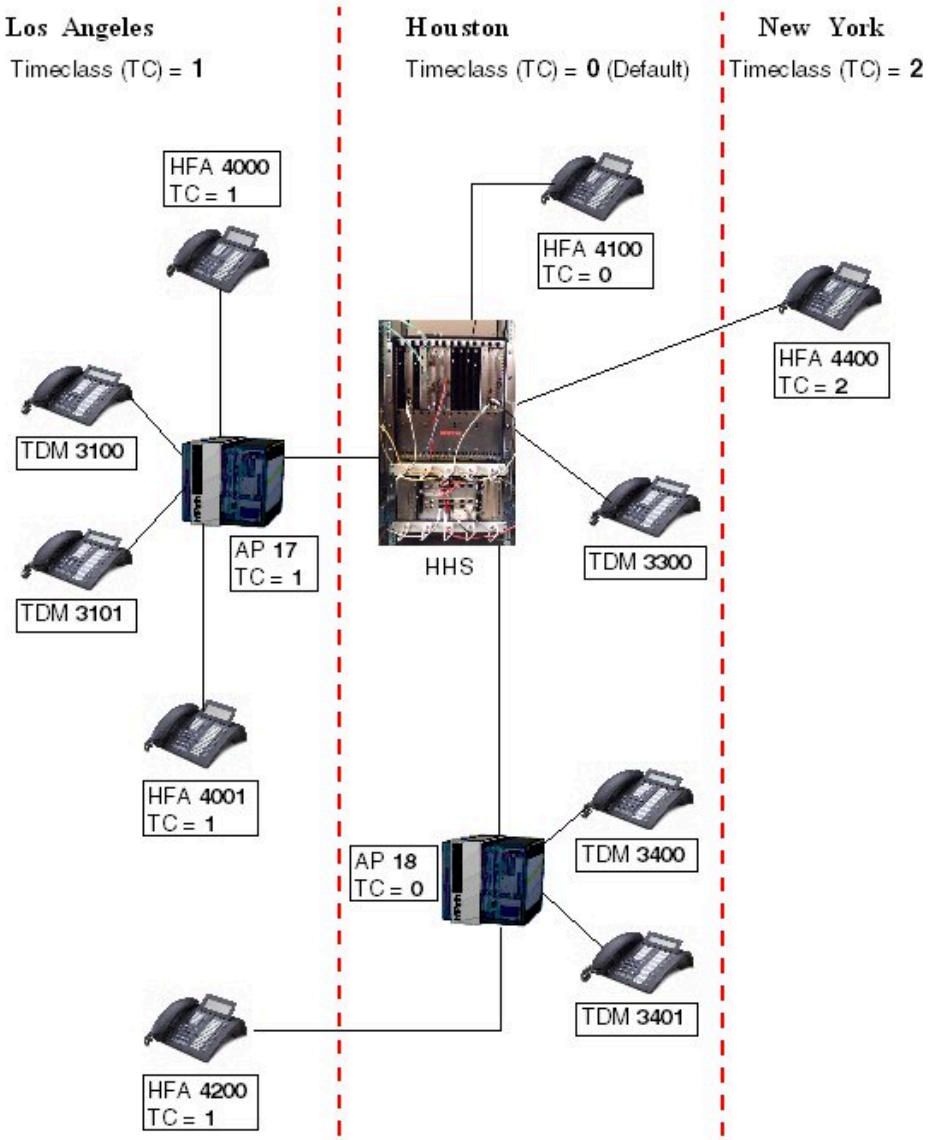
- “HFA Mobile User” is not supported. A user’s display shows the time that has been configured for his or her phone, even if he or she has logged in a different time zone.
- Timed reminders are not supported. The timed reminder function is blocked if a telephone has a local time class configured.
- Call detail recording is done in the system time.
- Error messages are output with the system time.
- In the case of an APE (CCAP) taking over control, it will function in place of the computer in the host system (CCA/CCB) with a copy of the database from HHS. If the "Different Time Zones (DTZ)" function (AMO TCLASS) is configured or if HHS and access points are distributed across multiple timezones, the APE (CCAP) must be configured to the same time as the HHS (CCA/CCB/ADP), to ensure correct time display in case of an APE emergency (CC-AP has taken over control).

12.3 Generation Example

- The following example covers different DTZ configuration possibilities:
  - The HHS is in Houston, Texas and has two AP shelves configured. HFA stations 4000 and 4001 are in AP shelf 17, which is located in Los Angeles and assigned time class 1. Because of the different time zones, AP shelf 17 is given the time class 1, which provides for a time difference of two hours to the west.
  - HFA station 4100 is located in Houston station, 4100 is configured directly on the HHS. The AP shelf 18 is also located in Houston (Direct link). Neither AP shelf 18 nor the station configured directly on the HHS requires a special time class - the default settings are entirely sufficient.

- Although the HFA station 4400 is configured in the HHS in Houston, it is physically located in New York. This station is given the time class 2, which means a time difference of one hour in the easterly direction.
- Another configuration option involves the HFA station 4200 that is configured in AP 18 but that is physically located in Los Angeles. Therefore the HFA station 4200 has to be assigned to time class 1. If the station would be located in New York, the time class 2 has to be assigned to this station.
- All TDM stations get the time class depending on their locations. Stations 3100, 3101, 3400 and 3401 get the time class of the AP shelf configuration (AMO UCSU). Station 3300 gets the system time.
- Furthermore, an HFA station could also be configured in AP 17 (in Los Angeles), but be physically located in New York. Then time class 2 would have to be configured for this station in the AMO SDAT. This configuration is not pursued any further in this example.

• Overview diagram for the following configuration possibilities:

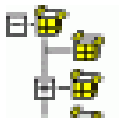


12.3.1 Configuring the Time Classes

- The time classes needed for the example are configured in the AMO SIPCO.
- Time class 1, Los Angeles with automatic switch to standard time, minus 2 hours relative to Houston (system time).

  This class supports changes from standard time to daylight savings time and back; these take place automatically on the last Sunday in March at 2:30 a.m. and on the last Sunday in October at 3:30 a.m.

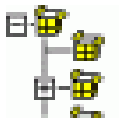
  The time class and the automatic switches for daylight savings time are configured as follows:

	Configuration Management -> System Data -> IPDA -> IPDA System Data
	CHANGE- SIPCO:TYPE=TCLASS,TCLASS=1,OFFSET=120,DIRECT=WEST, TEXT=”TIME ZONE: -2H L.A.”,DSTSW=AUTO,MONTHDST=3, WKDAYDST=SU,DAYNODST=LAST,HOURDST=2,MINDST=30, MONTHDST=10,WKDAYST=SUN,DAYNODST=LAST, HOURNT=3,MINNT=30;

Time class 2, New York, with manual switch to standard time, plus 1 hour relative to Houston (system time).

This class supports changes from standard time to daylight savings time and back; these take place on March 27th at 2:00 a.m. and on October 30th at 3:00 a.m.

The time class and the manual switches for daylight savings time are configured as follows:

	Configuration Management -> System Data -> IPDA -> IPDA System Data
	CHANGE-SIPCO:TYPE=TCLASS,TCLASS=2,OFFSET=60,DIRECT=EAST, TEXT=”TIME ZONE: +1H N.Y.”,DSTSW=MAN,MONTHNT=3, DAYDST=27,HOURDST=2,MINDST=0,MONTHNT=10,DAYNT=30, HOURNT=3,MINNT=0;

- The time class configuration now looks as follows:

DISPLAY-SIPCO:TYPE=TCLASS;

TIME CLASS DATE:

```
-------------------------------------------------------------
+------+-----------+-----------+-------------------+--------+
```

```
|INDEX |   OFFSET   |    DIRECT  |        TEXT         | DSTSW  |
+------+------------+------------+---------------------+--------+
|   1  |     120    |    WEST    |TIME ZONE: -2H L.A.  | AUTO   |
+------+------------+------------+---------------------+--------+
|   2  |      60    |    EAST    |TIME ZONE: +1H N.Y.  |  MAN   |
+------+------------+------------+---------------------+--------+

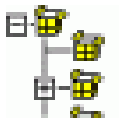
+------+-----+-------+-----------+-----------+--------+--------+
|INDEX |     | MONTH | WEEKDAY   | DAYNUMBER | HOUR   | MINUTE |
+------+-----+-------+-----------+-----------+--------+--------+
|   1  |DST: |   3   |    SU     |  LAST     |    2   |   30   |
|   1  |NT:  |  10   |    SU     |  LAST     |    3   |   30   |
+------+-----+-------+-----------+-----------+--------+--------+

+------+-----+-----------+------------+------------+-----------+
|INDEX |     |   MONTH   | DAYOFMONTH |   HOUR     |  MINUTE   |
+------+-----+-----------+------------+------------+-----------+
|   2  |DST: |     3     |     27     |      2     |     0     |
|   2  |NT:  |    10     |     30     |      3     |     0     |
+------+-----+-----------+------------+------------+-----------+
```

12.3.2 Assigning the Time Classes to an AP Shelf

- The AP shelf 17 configured in the example needs a time class because there is a station configured on it that draws its time class from the AP shelf.
- **Assign time class 1 to AP shelf 17.**

  The time class is configured with the new parameter TCLASS in AMO UCSU:

	Configuration Management -> System Data -> IPDA -> IPDA Access Point
	ADD-UCSU:UNIT=AP,LTG=1,LTU=17, LTPARTNO=”Q2305-X40 “,SRCGRP=17,FRMTYPE=INCH19, CONNTYPE=APDL,LSRTADDR=198.16.16.63, APRTADDR=198.16.16.150,LOCID=017, LOCATION=”LOS ANGELES”,PHONE=3140,FAX=3141,PLCHECK=Y, BCHLCNT=120,CONVLAW=N,TCLASS=1;

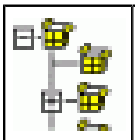
- The AP 18 is not assigned a time class of its own so that the TCLASS parameter is not specified. Consequently, AP 18 works with the default time class 0 (no additional calculation of the display with regard to time zones and daylight savings time).

IMPORTANT: If the shelf's time class has to be changed, the shelf must first be deactivated with the AMO USSU and then reactivated after the change has been made.

12.3.3 Assigning the Time Classes to an HFA Station

- A time class must be assigned to HFA stations 4200 and 4400 configured in the example.
- Assigning a time class for HFA stations with AMO SDAT.

  After the HFA stations have been configured by means of the AMO SBCSU (OPTIIP), the time class is configured with the new TCLASS parameter in AMO SDAT:

	Configuration Management -> Station -> Station
	CHANGE- SDAT:STNO=4400,TYPE=DATA1,NNO=1-1-100,TCLASS=2; CHANGE- SDAT:STNO=4200,TYPE=DATA1,NNO=1-1-100,TCLASS=1;

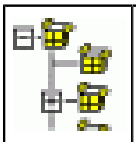
- HFA stations 4000, 4001 and 4100 are not assigned a time class with AMO SDAT.
  - For HFA station 4000, the calculation is controlled by the time class of the AP shelf in where the station is currently logged on (here AP 17, and therefore time class 1).
  - HFA station 4100 is directly logged on to the HHS and therefore does not need a time class. The display is always adapted to the HHS time.
- HFA subscriber 4200 is configured in AP shelf 18 (system time). Station 4200 is in time class 1, which was assigned to the station with AMO SDAT.
- The HFA subscriber 4400 is configured in Host and is assigned to the Time Class 2 (TC=2) with AMO SDAT.
- The configured time classes are always shown at station level by the AMOs SDAT and SBCSU.
- Only an HFA subscriber can be assigned a time class with AMO SDAT. If an HFA subscriber is assigned time class 0 with AMO SDAT, then the AP shelf's time class applies for this subscriber.

12.3.4 Deleting a Time Class

- You can delete a time class by setting the time offset and direction to the initialization values.

- Delete time class 1.

  Reset the offset and direction to delete the time class:

	Configuration Management -> System Data -> IPDA -> IPDA - System Data
	CHANGE- SIPCO:TYPE=TCLASS,TCLASS=1,OFFSET=0,DIRECT=NONE;

IMPORTANT: All stations with time class 1 are now using system time!

- The time class configuration now looks as follows:

DISPLAY-SIPCO:TYPE=TCLASS;

TIME CLASS DATE:

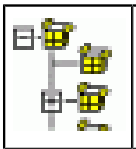
```
-------------------------------------------------------------------
+------+------------+------------+--------------------+--------+
|INDEX |   OFFSET   |    DIRECT  |        TEXT        | DSTSW  |
+------+------------+------------+--------------------+--------+
|   2  |      60    |     EAST   |TIME ZONE: +1H N.Y. |  MAN   |
+------+------------+------------+--------------------+--------+

+------+-----+-----------+------------+------------+-----------+
|INDEX |     |   MONTH   | DAYOFMONTH |   HOUR     |  MINUTE   |
+------+-----+-----------+------------+------------+-----------+
|   2  |DST: |     3     |     27     |      2     |     0     |
|   2  |NT:  |    10     |     30     |      3     |     0     |
+------+-----+-----------+------------+------------+-----------+
```

12.3.5 Deleting the Daylight Savings Time Changeover

- You can deactivate the consideration of daylight savings time in the time class with an AMO parameter.
- Deactivate the daylight savings time calculation in time class 2.

  Reset the offset and direction to delete the time class.

	Configuration Management -> System Data -> IPDA -> IPDA - System Data
	CHANGE-SIPCO:TYPE=TCLASS,TCLASS=2,DSTSW=OFF;

- The time class configuration now looks as follows:

DISPLAY-SIPCO:TYPE=TCLASS;

TIME CLASS DATE:

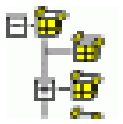
```
------------------------------------------------------------

+------+------------+------------+--------------------+--------+
|INDEX |   OFFSET   |    DIRECT  |        TEXT        | DSTSW  |
+------+------------+------------+--------------------+--------+
|   2  |      60    |     EAST   |TIME ZONE: +1H N.Y. |  OFF   |
+------+------------+------------+--------------------+--------+
```

12.3.6 Changing the System Date/Time with AMO DATE

IMPORTANT: The MODE parameter (DST/ NT) must be specified for DTZ, otherwise the telephones may display the wrong time.

Changing the system date/time

	Base Administration -> Unix Base Administration -> Date/Time Comment: At present, the MODE parameter can only be entered via RMX.
	CHA- DATE:YEAR=2005,MONTH=7,DAY=20,HOUR=14,MINUTE=30,MODE=DST;

- Displaying the system date/time:

DISPLAY-DATE;

```
+-----------------------------+
| WEDNESDAY                   |
| DATE:            TIME:      |
| 2005-07-20        14:30:34  |
|                             |
| DAY OF YEAR: 201            |
| DAYLIGHT SAVING             |
| GMTDIR:       TIMEOFFS:0    |
+-----------------------------+
```

12.4 Relevant AMOs

AMO	Parameter	Sprache/ Language	Beschreibung/Description
DATE	MODE	d	Zeit-Modus
	MODE	e	Mode of time
	SZ	d	Sommerzeit
	DST	e	Daylight Saving Time

AMO	Parameter	Sprache/ Language	Beschreibung/Description
	NZ	d	Normalzeit
	NT	e	Normal Time
UCSU	TCLASS	d	Zeitklasse des AP-Shelfs
	TCLASS	e	Time class of the AP shelf
SDAT	TCLASS	d	Zeitklasse des Teilnehmers
	TCLASS	e	Time class of the subscriber
SIPCO	TCLASS	d	Zeitklasse
	TCLASS	e	Time class
	OFFSET	d	Zeit-Offset (Minuten)
	OFFSET	e	Time offset (minutes)
	RICHT	d	Richtung (WEST/OST/KEINE)
	DIRECT	e	Direction (WEST/EAST/NONE)
	TEXT	d	Beschreibung der Zeitklasse
	TEXT	e	Time class description
	SONUS	d	Sommer-/Normalzeit-Umschaltung (AUTO/MAN/AUS)
	DSTSW	e	Daylight savings time switching (AUTO/MAN/OFF)
	MONATSZ	d	Monat der Sommerzeitumschaltung
	MONTHDST	e	Month of switching to daylight savings time
	WOTAGSZ	d	Wochentag der Sommerzeitumschaltung
	WKDAYDST	e	Weekday of switching to daylight savings time
	TAGNRSZ	d	Tagesnummer der Sommerzeitumschaltung
	DAYNODST	e	Day number of switching to daylight savings time
	STUNDESZ	d	Stunde der Sommerzeitumschaltung
	HOURDST	e	Hour of switching to daylight savings time

AMO	Parameter	Sprache/ Language	Beschreibung/Description
	MINSZ	d	Minute der Sommerzeitumschaltung
	MINDST	e	Minute of switching to daylight savings time
	MONATNZ	d	Monat der Normalzeitumschaltung
	MONTHNT	e	Month of switching to normal time
	WOTAGNZ	d	Wochentag der Normalzeitumschaltung
	WKDAYNT	e	Weekday of switching to normal time
	TAGNRNZ	d	Tagesnummer der Normalzeitumschaltung
	DAYNONT	e	Day number of switching to normal time
	STUNDENZ	d	Stunde der Normalzeitumschaltung
	HOURNT	e	Hour of switching to normal time
	MINNZ	d	Minute der Normalzeitumschaltung
	MINNT	e	Minute of switching to normal time
	TAGSZ	d	Tag der Sommerzeitumschaltung
	DAYDST	e	Day of switching to daylight savings time
	TAGNZ	d	Tag der Normalzeitumschaltung
	DAYNT	e	Day of switching to normal time

13 Signaling Survivability

13.1 Feature Description

IP Distributed Architecture is an architecture with a central system and numerous “unintelligent” peripheral modules. An access point/OpenScape 4000 SoftGate is essentially “remotely controlled” by the central system. If the control link fails, the access point/OpenScape 4000 SoftGate cannot survive autonomously. It must forward signaling messages from the peripheral modules to the central system. It cannot process these itself. Therefore, in the event of a failure in the control link with the central system, the access point/OpenScape 4000 SoftGate has no option other than to reset itself and wait until the central system restores it to operational status.

Thus, if the control link between the central system and an access point/ OpenScape 4000 SoftGate fails, the access point/OpenScape 4000 SoftGate can no longer place telephone calls.

On account of these very severe consequences of a failure in the control link between the OpenScape 4000 central system and the access point/OpenScape 4000 SoftGate, a possibility of “surviving” such failures has been created. In the event of a fault, signaling survivability switches the control link from the IP network to an alternative route. The signaling path is switched over without interruption.

However, signaling survivability does not help against a central system failure. If a central system is no longer available to control the access points/OpenScape 4000 SoftGates, a signaling path via CO or alternative LAN is no help either. In such cases, the entire communication system (including all access points/ OpenScape 4000 SoftGates) fails.

Calls possible with signaling survivability:

- Calls within the access point/OpenScape 4000 SoftGate
- Full scope of features
- Trunk calls from subscribers in the access point/OpenScape 4000 SoftGate via local trunks
- Full scope of features (for trunk calls)
- Calls with subscribers in other access points/OpenScape 4000 SoftGates to which an IP connection can still be established for the payload
- Full scope of features

  Calls with subscribers in the central system and calls with subscribers in access points/OpenScape 4000 SoftGates to which no IP connection can be established for the payload are only possible if the “Payload Survivability”

feature is configured for the relevant components. However, even if “Payload Survivability” is configured, only “Basic Call” functionality can be guaranteed.

Please refer IP Distributed Architecture > Section 2.9, “Payload Survivability”.

Signaling survivability is sold as a performance feature and is configured individually for each access point/OpenScape 4000 SoftGate.

Two alternatives are available for the Signaling Survivability feature for each Access Point/OpenScape 4000 SoftGate (see also Section 1.2, “What is Used as an Alternative Route for Signaling?”):

– Signaling Survivability via PSTN network
– Signaling Survivability via alternative LAN

IMPORTANT: For OpenScape 4000 SoftGates it is recommended to use Signalling Survivability over Alternate LAN.

IMPORTANT: In this context please pay attention to the use of the feature “HSR via UDP” (see Section 1.3, “HSR via UDP”).

13.1.1 How is the Fault Detected?

The control link (-> signaling link) between the CC and access point/OpenScape 4000 SoftGate is a TCP connection. Alternatively, it also can be a connection using UDP packages (feature “HSR via UDP”, see Section 1.3, “HSR via UDP”). The original TCP packages are part of these UDP packages. Therefore in this case both connection types can be considered as a TCP connection.

TCP connections (thus also the control link between CC and access point/OpenScape 4000 SoftGate) are generally subject to permanent monitoring of their functionality. Transmitted packets are acknowledged. If the acknowledgment does not arrive within a certain time, the packet is repeated. In the case a packet cannot be sent regardless of TCP retransmissions (i.e. no acknowledgment during defined time frame) the sender must assume packet loss. Even if no packets are currently being transmitted, TCP checks that the connection is functional. To this end, so-called “Keep Alive” messages are sent at predetermined intervals, which have to be answered.

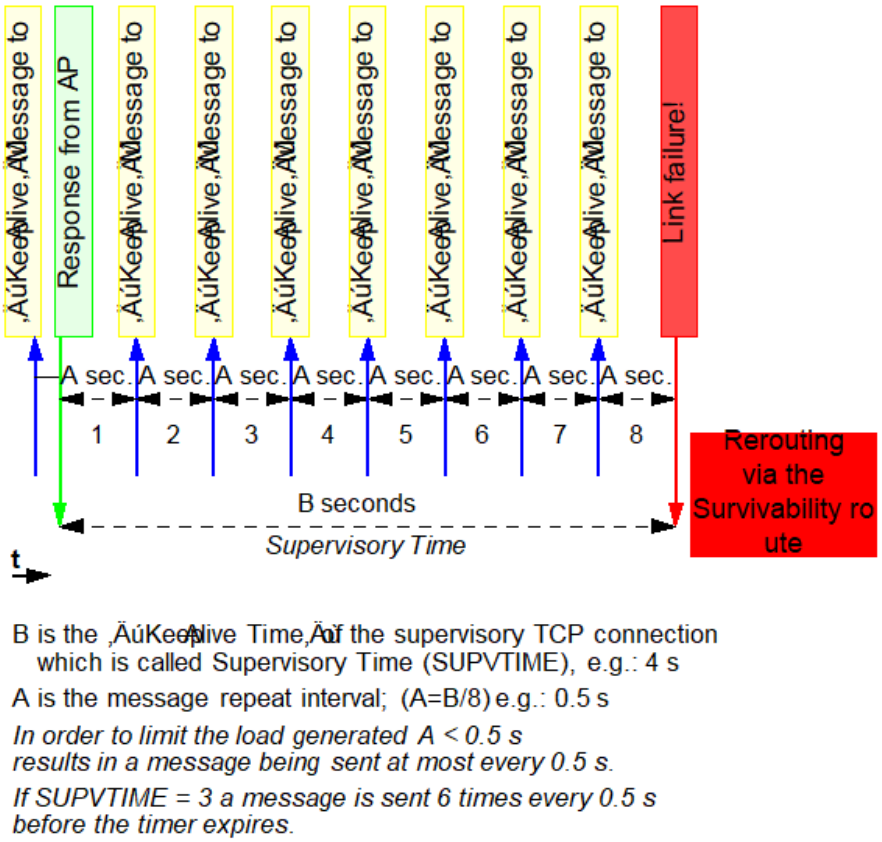
When a fault is reported on a signaling link, a relatively long period (e.g. more than 30 seconds) has already passed since the first indication. If it is assumed that signaling messages for a OpenScape 4000 switch have to be delivered within a specified time (e.g. 60 seconds), the difference between these two times is available to find and establish an alternative route and re-transmit the messages.

The time can be shortened by drastically reducing the time between the error index and the message.

Therefore, a supervisory link is always established in OpenScape 4000 between the CC and the access point/OpenScape 4000 SoftGate parallel to the signaling link as soon as signaling survivability is configured for the access point/OpenScape 4000 SoftGate.

This supervisory link is used exclusively to exchange “Keep Alive” messages at very short intervals (e.g. every second).

If the CC fails to receive a response to a “Keep Alive” message within a definable time interval (supervisory time), it switches the routing of the signaling messages to this access point/OpenScape 4000 SoftGate from the IP router to the survivability router.



B is the „Keep Alive Time“ of the supervisory TCP connection which is called Supervisory Time (SUPVTIME), e.g.: 4 s

A is the message repeat interval; (A=B/8) e.g.: 0.5 s

In order to limit the load generated A < 0.5 s results in a message being sent at most every 0.5 s.

If SUPVTIME = 3 a message is sent 6 times every 0.5 s before the timer expires.

Figure 224: Supervisory message flow for signaling survivability in the CC

An escalation strategy is also triggered in the access point/OpenScape 4000 SoftGate.

An interface fault is reported if, irrespective of the supervisory link, messages do not reach the access point/OpenScape 4000 SoftGate on the signaling link within the set time interval (**ALVTIME**), either via the IP network or the alternative route.

After the interface fault report (**ALVTIME**) the access point/OpenScape 4000 SoftGate is taken out of attendant list and will be reset within a definable time interval (**RESTIME**). It then waits for a renewed contact through the OpenScape 4000 CC.

Up to end of **ALVTIME**, all signaling messages queued in the CC and in the access point/OpenScape 4000 SoftGate for transmission are buffered. If the alive time (**ALVTIME**) expires, it can be assumed that the stored messages are outdated and may no longer be delivered. However, this means that the message flow between the CC and the access point/OpenScape 4000 SoftGate is no longer consistent.

The time constants can be changed with the AMO SIPCO in the **TIMING** branch. (see IP Distributed Architecture > Section 2.1, “OpenScape 4000 LAN Segment” > System timing (TIMING))

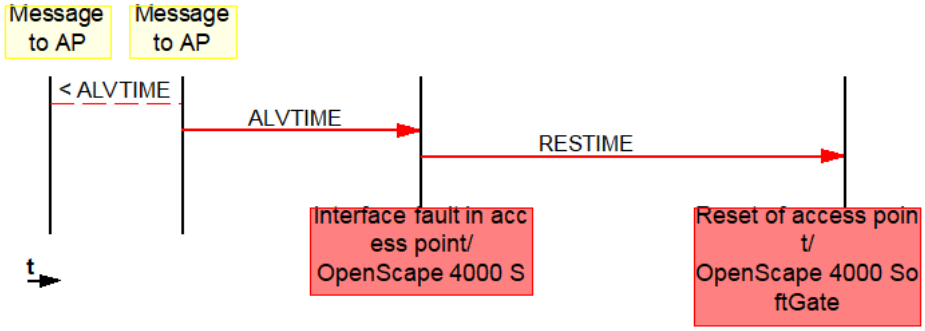


Figure 225: Message flow for signaling survivability in the access point/ OpenScape 4000 SoftGate

13.1.2 What is Used as an Alternative Route for Signaling?

If the IP link of an access point/OpenScape 4000 SoftGate fails, an alternative route in a network is required that is not affected by the failure.

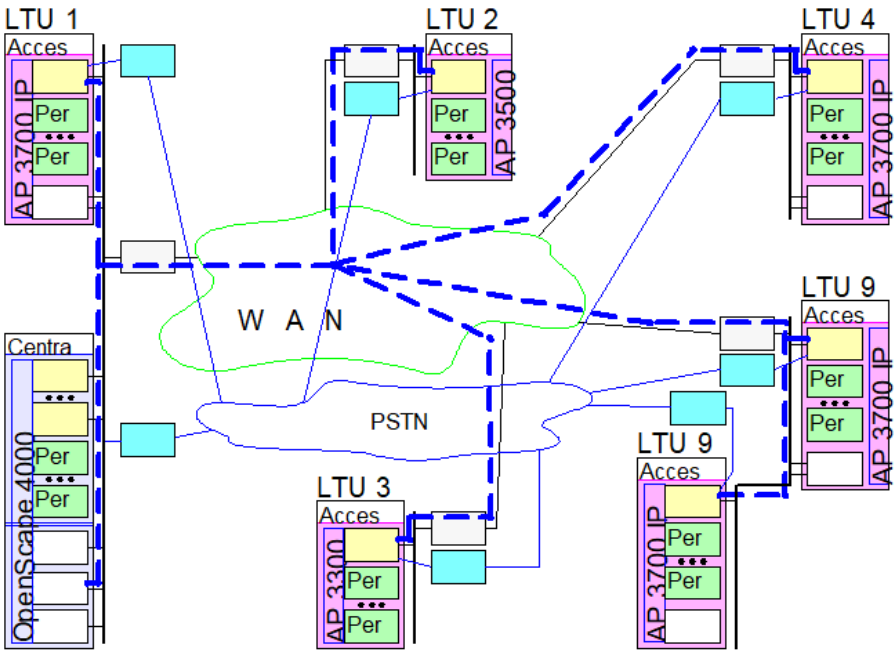
The basic demand on the network for the alternative route is simple:

- It must be independent of the IP network whose fault is to be bypassed via the alternative route.
- A connection device for the access point/OpenScape 4000 SoftGate is required, which acts as a modem. It must be actively callable and provide the access point/OpenScape 4000 SoftGate with “Ring Indication“.
- The central system must be supported by a corresponding router on an STMI2/4 with WAML function.

There are two different ways for signaling survivability:

- Signaling Survivability via PSTN Network
- Signaling Survivability via Alternate LAN

13.1.2.1 Signaling Survivability via PSTN Network



IPDA with signaling survivability

With signaling survivability via the PSTN network, an *alternative route* for signaling via the ISDN network (PSTN) is set up as soon as a fault in the IP path is detected. The messages are then routed via a PSTN router to the central system (for example, router with IP > S2 or STMI2/4 board with WAML function) and an ISDN modem on the access point/OpenScape 4000 SoftGate. The signaling messages are sent via this alternative path once it is established (approx. 30 ... 60 seconds). This ensures that none of the messages that may be in a backlog are lost.

As a rule, an access point/OpenScape 4000 SoftGate with signaling survivability generally requires a telephone connection for this purpose. The connection should be in the public PSTN network. Alternatively, it may be in a private network, insofar as the connection is not routed via the (IP) network whose fault is to be bypassed via the alternative route.

IMPORTANT: The modem may **not** access the public network via the access point/OpenScape 4000 SoftGate. It requires a separate connection independent of the access point/ OpenScape 4000 SoftGate. If the LAN connection fails, the access point/OpenScape 4000 SoftGate can no longer be controlled. If the alternative route to the modem is routed via the access point/OpenScape 4000 SoftGate, it cannot be switched before the alternative route is activated. However, the alternate route cannot be activated before being switched in the access point/OpenScape 4000 SoftGate.

The access point/OpenScape 4000 SoftGate is equipped with an RS 232/ V.24 interface on the HG 3575 module in order to connect a modem, via which the alternative signaling route into the telephone network is routed.

The counterpart to this modem is a special router at the OpenScape 4000 LAN segment, referred to here as the survivability router. This router also requires access to the telephone network.

If the LAN/WAN-based connection to the access point fails, a modem connection is established via CO. The access point is controlled via this connection until the LAN/WAN connection is reestablished.

If every access point features an individual modem (and the central system has reserved enough router connections via CO (PSTN)), signaling survivability can cover even the total failure of the WAN infrastructure. The only critical factor here are the connection between the active CC and the survivability router(s) in the OpenScape 4000 LAN segment and the independence of (failed) WAN from the PSTN used for survivability.

Details on the transmission methods between router and modem:

The transmission methods between the router and the modem must be compatible. Whenever possible, a digital link between the router and the modem should be used (ISDN modem), as analog modems require a long time to measure the route and agree on a transmission method. If the supervisory timer of the CC or access point/OpenScape 4000 SoftGate expires during the link establishment time, there is a danger of messages being lost. The access point/OpenScape 4000 SoftGate then resets itself. In addition, transmissions rates are substantially lower with analog modems than via ISDN. This can lead to delays with signaling messages and to the supervision timer expiring during bottleneck situations, in which case the access point/OpenScape 4000 SoftGate resets itself in the end.

Approximately 64 Kbps are generally considered to be sufficient for the maximum transmission capacity required in the signaling path. The transmission rate offered by ISDN modems comes sufficiently close to this value. In the case of analog modems, at most half of the transmission bandwidth can be achieved. This can lead to the limitations described. A transmission bandwidth of at least 28.8 Kbps must be guaranteed. A path is considered unsuitable for survivability if a lower bit rate is used for modem connects due to low-quality links.

13.1.2.2 Signaling Survivability via Alternate LAN

With signaling survivability via alternate LAN, an alternative route for signaling via a second LAN path is set up as soon as a fault in the IP path is detected. Therefore, a survivability router on the central system and a second LAN infrastructure on the access point/OpenScape 4000 SoftGate must be available. Then an alternate path is set up via the survivability router on the central system and the second LAN on the access point/OpenScape 4000 SoftGate. The signaling messages are sent via this alternative path once it is established. This ensures that none of the messages that may be in a backlog are lost.

There are two possible scenarios for signaling survivability via alternate LAN:

- Using L2 Redundancy at access point/OpenScape 4000 SoftGate for input of alternative router

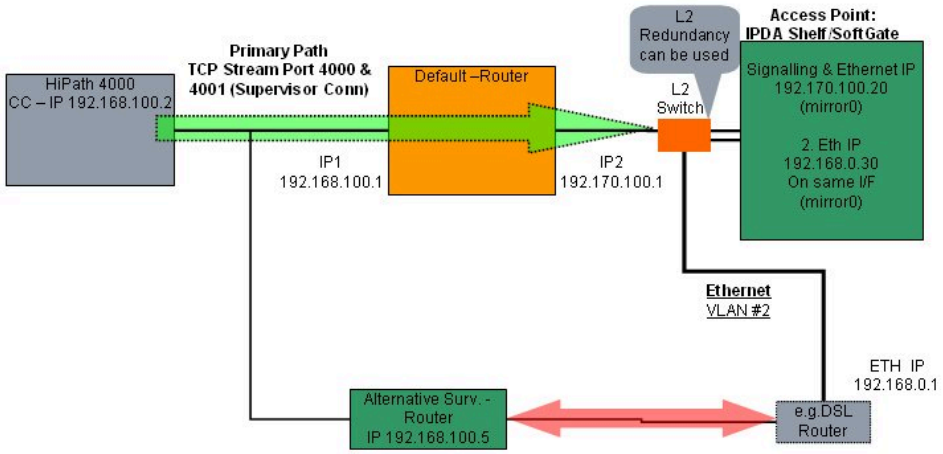


Figure 226: Signaling Survivability about alternatives LAN and L2 Redundancy

- Using 2nd ethernet interface of access point/OpenScape 4000 SoftGate for input of alternative router

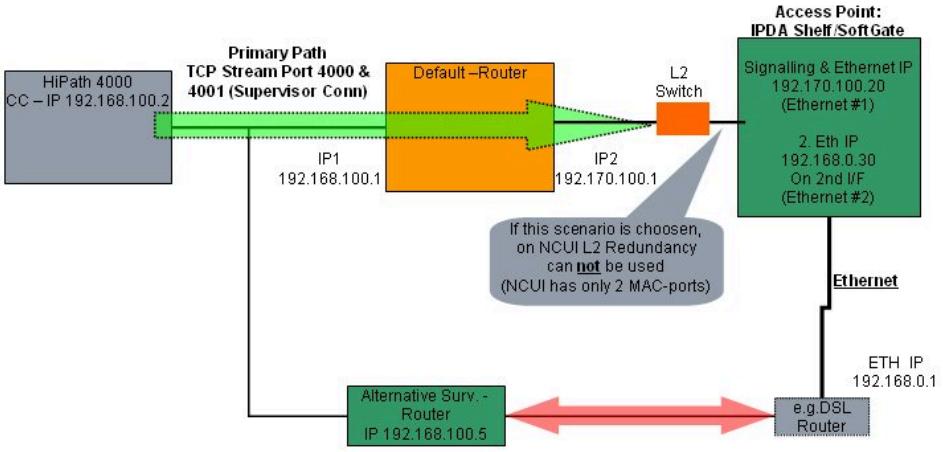


Figure 227: Signaling Survivability about alternatives LAN and second Ethernet interface

If every access point/OpenScape 4000 SoftGate features an individual survivability router, signaling survivability can cover even the total failure of the WAN infrastructure. The only critical factor here are the connection between the active CC and the survivability router(s) in the OpenScape 4000 LAN segment and the independence of (failed) WAN from the LAN used for survivability.

13.1.3 HSR via UDP

The "HSR (HiPath Signaling Router) over UDP" feature

- concerns the signaling connection between the host system and Access Point/OpenScape 4000 SoftGate. The signaling connection between APE and Access Point/OpenScape 4000 SoftGate is not affected. The latter is always only a pure TCP/IP connection regardless of the configuration of the **SIGMODE** parameter in AMO UCSU.

- can/may be activated additionally for "Signaling Survivability via the public CO" in order to bypass firewalls.
- must be activated for using the "Signaling Survivability over alternative LAN" feature.
- can/must be activated/deactivated individually for each Access Point/ OpenScape 4000 SoftGate (AMO UCSU, **SIGMODE=HSRUDP**).

IMPORTANT: The customer IP network (firewall) must not block the UDP 4000 and 4050 ports.

13.2 Service Information

- The feature “Signaling Survivability” is released for access points, OpenScape 4000 SoftGate and OpenScape Access/Branch.
- Up to 10 survivability routers can be configured in the system.
- Signaling survivability via PSTN network (modem) with OpenScape 4000 SoftGate (vNCUI) is supported for SoftGate 50 and SoftGate 500.
- **Only valid for signaling survivability via PSTN network:** Depending on the connection capacity, a survivability router can operate up to 30 access points/OpenScape 4000 SoftGates (router with S2 connection). As it cannot be foreseen precisely where in the IP network a fault will occur, the router capacity must be designed for the worst case scenario, i.e. failure of the link from the OpenScape 4000 LAN segment to the IP network of the customer. In such a case, alternative signaling routes will be needed immediately for all access points/OpenScape 4000 SoftGates with signaling survivability.
- **Only valid for signaling survivability via PSTN network:** If the modem connection goes over the public network, connection charges will accrue. The link to an access point/OpenScape 4000 SoftGate is used as long as the access point/OpenScape 4000 SoftGate is not accessible via the IP network. The configuration of the survivability router contains a setting for the period of “non-use“ after which this link is disconnected. This “hold-time” does not form part of the IPDA configuration. Accessibility of the access point/OpenScape 4000 SoftGate via the modem connection is checked on a cyclical basis (RTO). The check can also be started directly using the AMO TSU. In these cases too, charges for the link will accrue in the PSTN.
- The connection from the active processor (CC-A or CC-B) to the survivability router runs via the OpenScape 4000 LAN segment, just like the connection to the normal LAN router. If this LAN segment fails, for instance because a central L2 switch is faulty, the signaling survivability function will also fail. This “single point of failure” can be somewhat mitigated if CC-A and CC-B are connected to different L2 switches and, for example, half the survivability routers and half the HG 3500 are each connected to the relevant switches. This ensures that at least half of the system will still be available should one of the two L2 switches fail.
- The TCP stream (tcp.port=4000) has to be routed fully transparently through the customer's IP network (i.e. no manipulation of the SequenceNumber etc.), otherwise the "Signaling Survivability" will not work. Furthermore, any available firewalls have to be configured accordingly so that no SequenceNo and SYN check takes place for the tcp.port=4000. It this cannot be guaranteed, the "HSR over UDP" feature should be activated alternatively.

- Signaling survivability via PSTN network (modem) with OpenScape 4000 SoftGate (vNCUI) is tested and supported with OpenScape 4000 SoftGate 50 & OpenScape 4000 SoftGate 500. Both startup and basic scenarios with high load are tested (480 subscribers with > BHCA 6000) via modem, however the use of any large group Signaling features (e.g. AUN) may lead to Signaling delays. The delays are not one of the feature itself, however an issue of Bandwidth Limitation of the PPP connection (64kbit/s) that can lead to TCP Retransmission. If large groups with Signaling are in use, **or** OpenScape 4000 SoftGate 1000 is used, it is recommended to use "Signaling Survivability via alternate LAN" where there are lesser bandwidth concerns (i.e. ADSL access has much higher available bandwidth for Signaling). Other survivable options like APE, Survivable OpenScape 4000 SoftGate and BPOOL functions are also available, but not without interruption to telephony.
- Please also note:

  To assure signaling survivability at the OpenScape 40000 SoftGate a certain USB cable is necessary (Part number: C39195-Z7705-A3). If you are unsure, the correct type of cable will display "New USB device found, idVendor=067b, idProduct=2303" in \var\log\messages under Linux. An alternative cable from ATEN is known to cause problems. This has the vendor id "New USB device found, idVendor=0557, idProduct=2008".

  For signaling survivability at the OpenScape 40000 SoftGate functions with an external ISDN router, the ISDN modem must have a minimum firmware version of V7.019 to understand the AT**ACCM command. For further details, please see MSC24547 in G-DMS.
- Signaling Survivability with WAML-Replacement is only released for Common Gateway Boards (HG 3500). Thus, the WAML function can only be configured in a host shelf or in IPDA shelf (“direct link”), i.e. the functionality at an OpenScape 4000 SoftGate / OpenScape Access/Branch is not supported.
- Using L2 redundancy at access point for input of alternative router is only possible with OpenScape 4000 SoftGate.
- In case of signaling survivability via alternate LAN (AMO APRT, parameter **SURVLAN**) HSR over UDP must be configured.
- Restrictions and information with the deployment “Simply with integrated SoftGate” (OpenScape 4000 SoftGate on same computer as host system):
  - The integrated OpenScape 4000 SoftGate doesn’t support HSR over UDP.
  - The integrated OpenScape 4000 SoftGate doesn’t support Signaling Survivability function for HSR connection.
  - The integrated OpenScape 4000 SoftGate is allowed to accept a HSR Connection from an AP-CC (feature APE).
- Restrictions and information with the deployment “Survivable SoftGate” (OpenScape 4000 SoftGate and APE on the same computer):
  - APE doesn’t support Signaling Survivability function for HSR connection.
  - OpenScape 4000 SoftGate supports HSR over UDP to the host system.
  - OpenScape 4000 SoftGate supports Signaling Survivability function for HSR connection to the host system.
- The golden load loadware of the NCUI board doesn’t support UDP functionality which is necessary for signaling survivability via alternate LAN. Thus, follow the instructions in Section 3.2.4,

"Replacement of a defect NCUI Board with a new NCUI Board" when replacing a board.

13.3 Generation (Example)

13.3.1 Signaling Survivability via PSTN Network

13.3.1.1 Configuring the OpenScape 4000

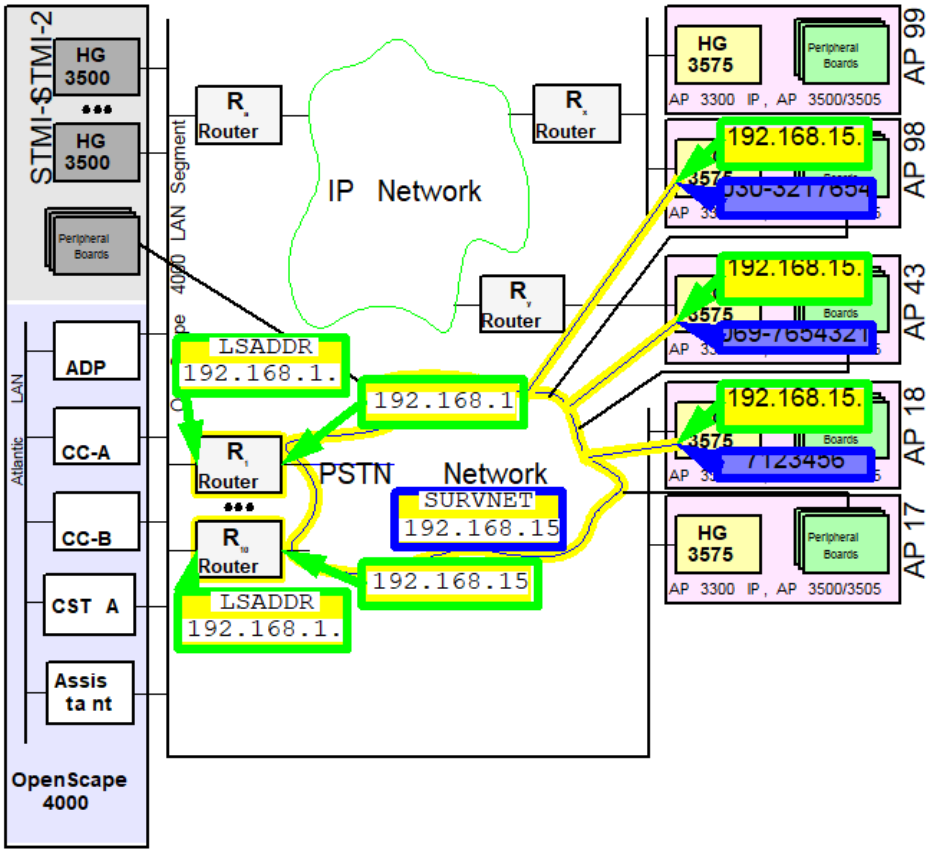


Figure 228: Signaling survivability via Modem

The access connections of the survivability routers and modems into the PSTN telephone network form a virtual IP network, the survivability network. Every access to this virtual network requires an IP address in this network. In order to keep the administrative effort for this network to a minimum, a number of stipulations have been agreed on:

- The survivability network has the netmask 255.255.255.0.
- A maximum of 10 survivability routers are supported between the OpenScape 4000 LAN segment and the survivability network; these are numbered consecutively from 1 to 10. The fourth digit in the IP address of

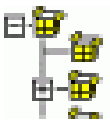
routers in the survivability network is the consecutive number of the router, i.e. 1-10.

- The address of an access point in the survivability network is likewise specified. The fourth section of the IP address is set to be identical to the LTU number of the access point.

Thus, only one parameter essentially remains to be configured in the survivability network: the network address.

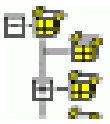
This is configured with the AMO SIPCO and must already be specified during ADD-SIPCO if the customer has purchased signaling survivability licenses (see IP Distributed Architecture > Section 2.1, “OpenScape 4000 LAN Segment”).

If the licenses for signaling survivability are not purchased until later or if the zero address 0.0.0.0 was specified during initial installation, this address must be set now.

	**Configuration Management > System Data > IPDA > IPDA System Data** Click **Search**, enter or change the survivability network address on the **System Data** tab, then **Save**.
	`CHANGE-SIPCO:TYPE=LSNET,SURVNET=192.168.15.0;`

IMPORTANT: The last digit of the SURVNET address must always be ZERO. Otherwise, it would not be a network address, together with the specified netmask 255.255.255.0.

The licenses for signaling survivability can be queried as follows:

	**Configuration Management > HiPath Inventory Management > HIM System Data > Feature > Marketing Units** Click **Search** > **Sales Features** tab > **Signaling Survivability** entry
	`DISP-CODEW;` “SIGNALING SURVIVABILITY“ entry

Although this network is only used when needed and the communication partners are fixed, the address for this network must be agreed on with the customer network administrator.

Thought now has to be given to the assignment of access points to survivability routers. Every survivability router can be described through the following data, which must also be configured in the router itself:

- Consecutive number of the router [1..10]
- IP address of the router in the OpenScape 4000 LAN segment
- IP address of the router in the survivability network

- Access points to be operated via this router, including:
  - LTU number and, derived from that number, its IP address for survivability
  - Telephone number of the modem connection
- Signaling survivability type = MODEM

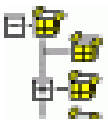
Ultimately, the router is to be configured in such a way that, upon receipt of a packet with a target address identical to that of the survivability address of an access point, it establishes a dial-up connection to the modem of that access point and subsequently transmits the packet. If the connection is not used for an extended period (e.g. 30 seconds), the access point can be reached again via LAN and the link to the modem can be disconnected.

An STMI2/4 module with WAML function in the OpenScape 4000 CC can also be used as a survivability router.

IMPORTANT: If a survivability router is to access the ISDN network via the OpenScape 4000, there must be sufficient connection capacity in the trunk access of the OpenScape 4000. If, for example, 83 access points on a system are equipped with signaling survivability, 83 B-channels to the CO must be made available immediately in the central area around the OpenScape 4000 system in the event of an IP network failure. If this capacity is not reserved, it may not be possible to reach all access points. Access points that are not reached via signaling survivability perform a restart and can only operate again if they are accessed by CC via LAN or modem.

The configuration in the OpenScape 4000 switch is realized as follows:

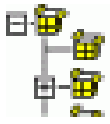
- Announce the survivability routers in the system

	**Configuration Management > System Data > IPDA > IPDA Signaling Survivability Router** Click **Search**, enter or change the router number and address on the Router Data tab, then **Save**.

	`ADD-APRT:TYPE=SURV,CONF=ROUTER,ROUTERNO=1,`
	`LSADDR=192.168.1.101;`
	`ADD-APRT:TYPE=SURV,CONF=ROUTER,ROUTERNO=10,`
	`LSADDR=192.168.1.110;`

Routers 1 and 10 from the example in Figure 6 “Signaling survivability via Modem” are thus configured.

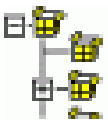
- Assign the access points to the survivability routers

	**Configuration Management > System Data > IPDA > IPDA Access Point** Click **Search**, set the desired router number on the **General** tab under signaling survivability and **Save**.

	`ADD-APRT:TYPE=SURV,CONF=AP,LTU=98,ROUTERNO=1,SURVTYPE=MODEM;`
	`ADD-APRT:TYPE=SURV,CONF=AP,LTU=43,ROUTERNO=1,SURVTYPE=MODEM;`
	`ADD-APRT:TYPE=SURV,CONF=AP,LTU=18,ROUTERNO=1,SURVTYPE=MODEM;`

Thus, all access points with signaling survivability in the example in Figure 6 “Signaling survivability via Modem” are assigned to a router. Finally, when assigning the access points to a router, signaling survivability for the respective access point is configured. This command checks whether a license for signaling survivability is available. If so, the use is booked; if not, the configuration is rejected.

If the assignment of an AP to a survivability router is changed, e.g. if AP 43 should in future be operated by Router 10 instead of Router 1, the following action is required:

	**Configuration Management > System Data > IPDA > IPDA Access Point** Click **Search**, set the desired router number on the **General** tab under signaling survivability and **Save**. **Configuration Management > System Data > IPDA > IPDA System Data** Click **Search** and select the access point. Click **Execute** on the **Action** pull-down menu and select the mode of action **Update AP**, confirm with **OK**.

	A CHANGE of the configuration for signaling survivability with APRT is not possible. In order to change the configuration, the corresponding assignment is simply deleted and subsequently re-configured.
	`DELETE-APRT:TYPE=SURV,CONF=AP,LTU=43;`
	`ADD-APRT:TYPE=SURV,CONF=AP,LTU=43,ROUTERNO=10,SURVTYPE=MODEM;`
	In order for this change to become effective, AP 43 has to be restarted.
	`EXEC-USSU:MODE=UPDATAP,LTU=43;`

IMPORTANT: Connections are cleared down without further warning. Prior to the `EXEC-USSU:UPDATAP`, the configuration must be updated on the system hard disk.

13.3.1.2 Configuring the Modem

In order to be able to make the configuration settings, the modem must be connected to a PC and a terminal emulation program (HyperTerminal) must be started on the PC.

IMPORTANT: The **Pocket ISDN TA** modem from *INSYS Microelectronics, S30122-X7551-X AYA422* is recommended for use as an IPDA survivability modem with ISDN interface.

The following must be set if they were not already set by default:

- The baud rate at the modem’s serial interface must be set to 115200 bauds which is mostly covered via the auto-detect mode. **Modems that do not support the 115200 baud rate at the serial interface are unsuitable for use with IPDA.**
- Auto-Answer must be switched **off**.
- The local echo must be switched **off**.

- The modem response to commands must be shown in plain text (in long form), i.e. as text “RING“, “CONNECT“, etc.
- Neither error correction nor compression must be activated in the modem. This is performed by the PPP itself.
- The software handshake (XON/XOFF) must be deactivated.
- *For ISDN modems*: the B-channel protocol: HDLC - PPP protocol (“Async to sync” conversion, asynchronous PPP, single link PPP)
- *For analog modems*: set the line bit rate permanently on both modems to save negotiation time. In response to the modem’s “RING“ message, the HG 3575 sends the “ATA” command to the modem which must report “CONNECT“ within 60 seconds.

First the factory defaults must be restored

AT&F

The parameters specified above must then be set

For modem **Pocket ISDN TA**

- Auto-Answer must be switched off:

`ATS0=0`

- The local echo must be switched off:
- `ATE` or generally `ATE0`

At least the configuration must be saved:

AT&W

13.3.1.3 Configuring the Router

Overview

- Signaling Flow Survivability for “Networked“ Access Points
- Signaling Flow Survivability for “Direct Link“ Access Points
- Signaling Survivability with WAML Replacement
- External ISDN Router as the Survivability Router

13.3.1.3.1 Signaling Flow Survivability for “Networked“ Access Points

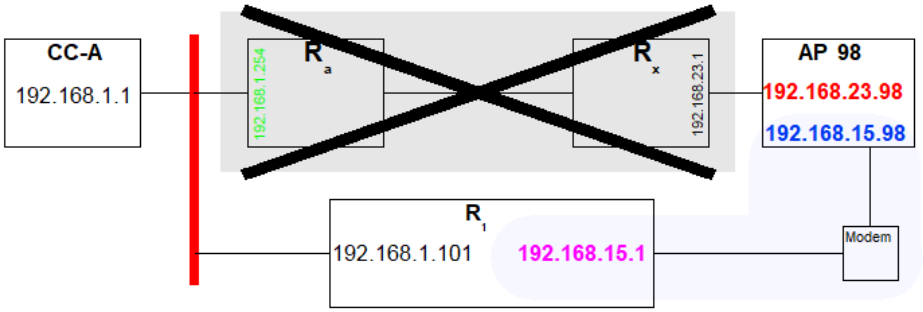


Figure 229: Survivability router configuration

The following process must be taken into consideration when configuring the survivability router.

Normal operation (without survivability):

1) CC-A generates packet at AP 98 with destination 192.168.23.98 and source 192.168.1.1 and transfers it to the Ra router (192.168.1.254).

   This may send the packet via another router to Rx which delivers the packet to AP 98.

   Survivability:

   CC-A generates packet at AP 98 with destination 192.168.23.98 and source 192.168.1.1 and transfers it to the router R1 under 192.168.1.101.

IMPORTANT: The complete **IP frame**, including addresses, remains identical to the frame in normal operation. With survivability, only the accessed router changes (in the OpenScape 4000 LAN segment). This change takes the form of a different destination address at Ethernet level (MAC-DA). The IP address of Router R1 in the OpenScape 4000 LAN segment is not accessed visibly. It is needed to determine the MAC address of the router port with ARP.

13.3.1.3.2 Signaling Flow Survivability for “Direct Link“ Access Points

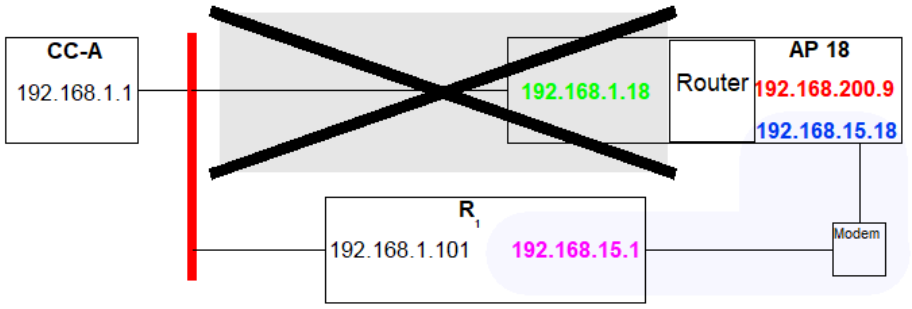


Figure 230: Survivability router configuration

The following process must be taken into consideration when configuring the survivability router.

Normal operation (without survivability):

1) CC-A generates packet at signaling unit AP 18 with destination 192.168.200.9 and source 192.168.1.1 and transfers it to the internal signaling router associated with AP 18 (192.168.1.18).

   This sends the packet to the signaling unit AP 18 (192.168.200.9).

   Survivability:

   CC-A generates packet at AP 18 with destination 192.168.200.9 and source 192.168.1.1 and transfers it to the router R1 under 192.168.1.101.

IMPORTANT: The complete **IP frame**, including addresses, remains identical to the frame in normal operation. With survivability, only the accessed router changes (in the OpenScape 4000 LAN segment). This change takes the form of a different destination address at Ethernet level (MAC-DA). The IP address of Router R1 in the OpenScape 4000 LAN

segment is not accessed visibly. It is needed to determine the MAC address of the router port with ARP.

R1 sends the packet to the next hop router 192.168.15.18 and creates the modem link for the PPP connection between 192.168.15.1 and 192.168.15.18 or uses the existing connection.

The packet is sent from the PPP instance 192.168.15.18 to the destination 192.168.200.9 in AP 98.

For this, the route for **192.168.200.9** must be configured via 192.168.15.18 in the survivability router R1 and the dial-up connection for the destination 192.168.15.18.

The PPP instance in R1 must be configured with the address 192.168.15.1 so that packets from AP 18 can be transported back to CC-A.

13.3.1.3.3 Signaling Survivability with WAML Replacement

For the feature “Signaling Survivability with WAML Replacement “ a common gateway board (HG 3500) must be configured in the AMO BFDAT using **FUNCTION=WAML**. Either a separate board or a board that supports multiple functions can be used for this purpose.

IMPORTANT: If this feature is configured (STMI board with WAML function), then the redundant LAN interfaces function does not work. See also Section 6.4, “Redundant LAN Interface”.

Hardware:

- STMI (HG 3500) with WAML functionality is used as a router. It **must** be configured in the host system in order to communicate with CCA/ CCB (within the same network).
- S0 connection has to be configured.
- Modem ISDN connected with V.24 (modem) at NCUI (HG 3575).

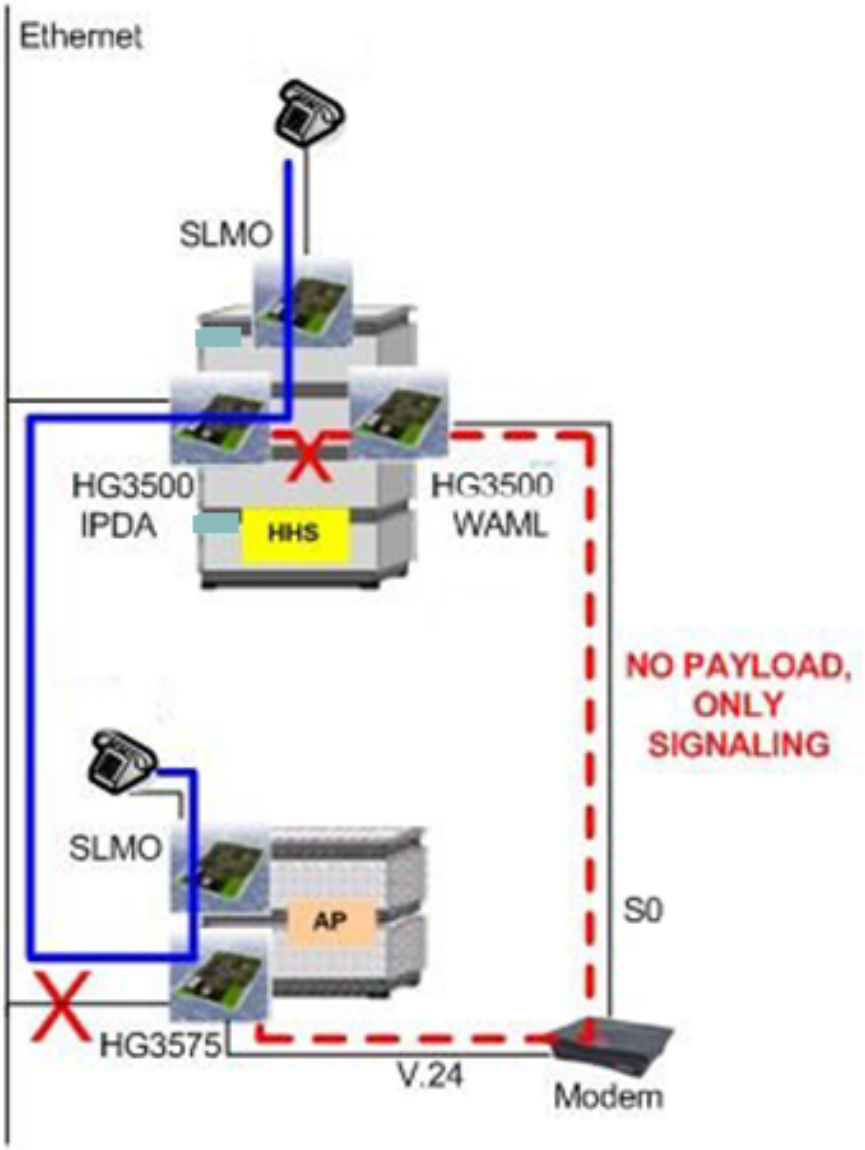


Figure 231: Signaling survivability withWAML replacement

The configuration consists of 3 parts:

1. IPDA

```
ADD-
SIPCO:NETADDR=172.28.145.0,NETMASK=255.255.255.0,IPMODE=IPV4,DEFRT=172.28.145.25
4,CCAADDR=172.28.145.150,CCBADDR=0.0.0.0,SURVNET=192.168.15.0;
ADD-UCSU:UNIT=AP,LTG=1,LTU=18,LTPARTNO=Q2305-X40,SRCGRP=1,FRMTYPE=L80XF,CONN►
TYPE=APDL,LSRTADDR=172.28.145.155,APRTADDR=172.28.145.254,LOCID=012,LOCATION="IP
DA17WEAS",PLCHECK=YES,BCHLCNT=30,CONVLAW=NO,TCLASS=0,ALARMNO=0;
ADD-APRT:TYPE=APNET,LTU=18,APIPADDR=172.28.0.57,NETMASK=255.255.255.255,TAIPAD►
DR=0.0.0.0;
```

/* HG3575 Configuration data

ip_addr_eth is	*	172.28.145.155

netmask_eth is	*	255.255.255.0
default_gateway is	*1	172.28.145.254
ip_addr_signaling is	*	172.28.0.57
netmask_signaling is	*	255.255.255.255
ip_addr_survivability is	*2	192.168.15.18
netmask_survivability is	*2	255.255.255.0
gateway_survivability is	*2	192.168.15.1
netmask_hhs is	*	255.255.255.0
ip_addr_CC_A is	*	172.28.145.150
ip_addr_CC_B is	*3	0.0.0.0
ip_addr_CC_C is		0.0.0.0

2. Signaling Survivability with WAML

/* **WAML**

```
ADD-BFDAT:FCTBLK=5,FUNCTION=WAML,BRDBCHL=BCHL60&BCHL120;

CHANGE-BFDAT:CONFIG=CONT,FCTBLK=5,FUNCTION=WAML,BCHLCNT=1;

CHANGE-BFDAT:CONFIG=OK,FCTBLK=5,ANSW=YES;
ADD-BCSU:MTYPE=IPGW,LTG=1,LTU=1,SLOT=85,PARTNO="Q2316-X10",FCTID=1,LW►
VAR="0",FCTBLK=5,BCHLWAML=10;
ADD-CGWB:LTU=1,SLOT=85,SMODE=NORMAL,IPADR=172.28.145.156,NETMASK=255.255.255.0;
```

/* **Direction to the router and call number of the router**

```
ADD-BUEND:TGRP=111,NAME="WAML",NO=30;
ADD-COT:COTNO=222,PAR=ANS&LWNC&DFNN&NTON&NLCR&NLRD,INFO=FUER_WAML;
ADD-COP:COPNO=222,PAR=SFRM,TRK=TA,TOLL=TA,DEV=LAN,INFO=COP_FUER_WAML;
ADD-COSSU:NEWCOS=222,AVCE=TA&TNOTCR;
ADD-WABE:CD=446,DAR=TIE,CHECK=N;
ADD-TDCSU:OPT=NEW,PEN=1-1-85-0,COTNO=222,COP►
NO=222,COS=222,LCOSV=1,LCOSD=1,CCT=WAMLREPLACED,DESTNO=0,PROTVAR=ECMAV2,SEG►
MENT=8,NNO=1-1-318,TGRP=111,DEV=HG3550LA,BCHAN=1&&10;
ADD-RICHT:MODE=LRTENEW,LRTE=223,LSVC=ALL,NAME=WAML,TGRP=111,DNNO=1-1-118;
ADD-LODR:ODR=11,CMD=ECHO,FIELD=1;

ADD-LODR:ODR=11,CMD=END;

ADD-LODR:ODR=11;
ADD-LDAT:LROUTE=223,LSVC=ALL,LVAL=1,TGRP=111,ODR=11,LAUTH=1;
ADD-LDPLN:LCRCONF=LCRPATT,DIPLNUM=0,LDP=446,LROUTE=223,LAUTH=1;
/* IP address of the router (IP address of the physical router - WAML)
ADD-APRT:TYPE=SURV,CONF=ROUTER,ROUTERNO=1,LSADDR=172.28.145.156;
/* Assign access point to the survivability router
ADD-APRT:TYPE=SURV,CONF=AP,LTU=18,ROUTERNO=1;
```

3. WAML (HG 3500/STMI) configuration with WBM

WAML and LAN Redundancy

If WAML functionality is configured there is no LAN redundancy at all despite the configuration of the LAN2 active or not.

Therefore select during initial setup (Wizard > Initial Setup) Not configured or deactivated.



WAML replacement - Second LAN

Router Call Number

Configuration > Routing > PSTN > (right mouse click) Edit Global PSTN Data -> Router Call Number “446” as configured in AMO LDPLN.

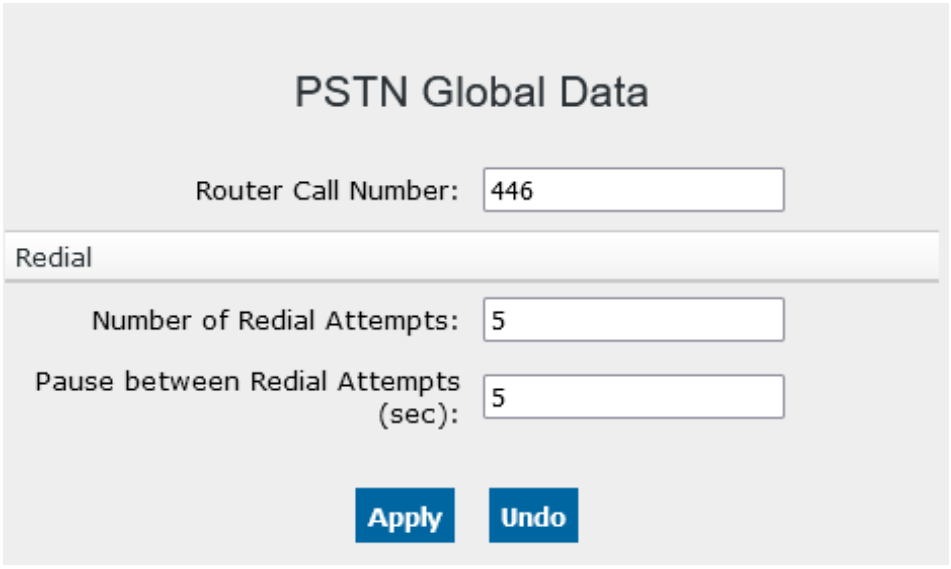


Figure 232: WAML replacement - PSTN global data

You can check the result with **Configuration > Routing > PSTN > Display Global PSTN Data**.

PSTN Peer

The PSTN Peer (PSTN-Partner) is the survivability-modem with its IP-Address coming from AMO SIPCO, parameter SURVNET + access point number, here 192.165.15.18.

The PSTN-interface is the PPP side of the WAML, i.e. AMO SIPCO, parameter SURVNET + router number, here 192.168.15.1.

Configuration > Routing > PSTN > PSTN Partner > (1) WAML18

NOTICE: Activate **Short Hold** and set the **Short Hold Time** to 180 seconds.

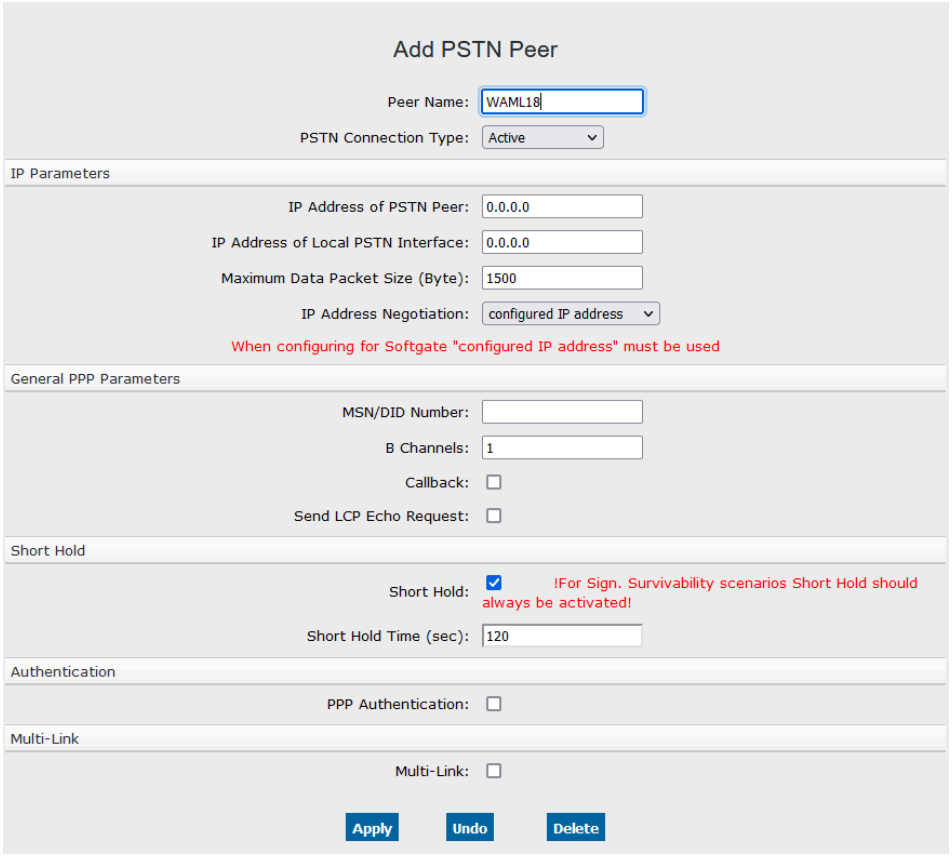


Figure 233: WAML replacement - PSTN peer

PSTN Station Number

With this number the WAML reaches the survivability modem. The number is configured on the S0 trunk with the extension 3277. Change Direction to Incoming and Outgoing.

Configuration > Routing > PSTN > PSTN Peers > (1) WAML18 > Add Station Number

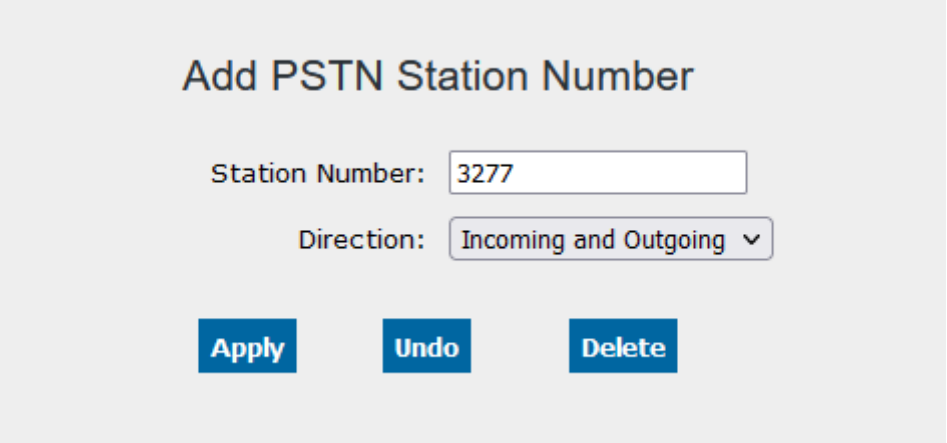


Figure 234: WAML replacement - PSTN station number

You can check the result with Configuration > Routing > PSTN > PSTN Peers > WAML18 > Display Station Number.

Static Route

Destination is the signaling IP address of the HG 3575 (NCUI), as configured as APIPADDR in AMO APRT (172.28.0.57)

The Route Gateway is the ISDN IP address of the modem (AMO SIPCO, parameter SURVNET+AP no.): 192.168.15.18

The Destination Netmask must be set to 255.255.255.255 for tunneling. Therefore the netmask entry is hard coded to 255.255.255.255 and read-only for STMI boards with WAML function.

Configuration > Routing > IP-Routing > Static Routes> WAML18

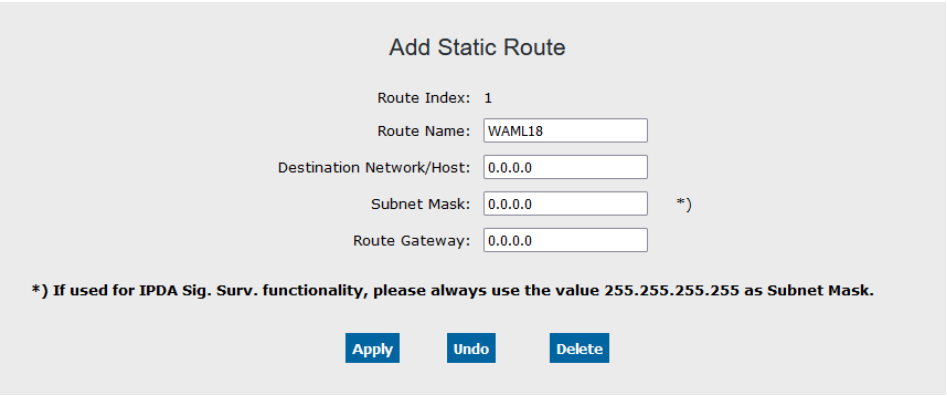


Figure 235: WAML replacement - Static route

Save all the changes (disk icon) and reboot the board. Then the changes become effective.

13.3.1.3.4 External ISDN Router as the Survivability Router

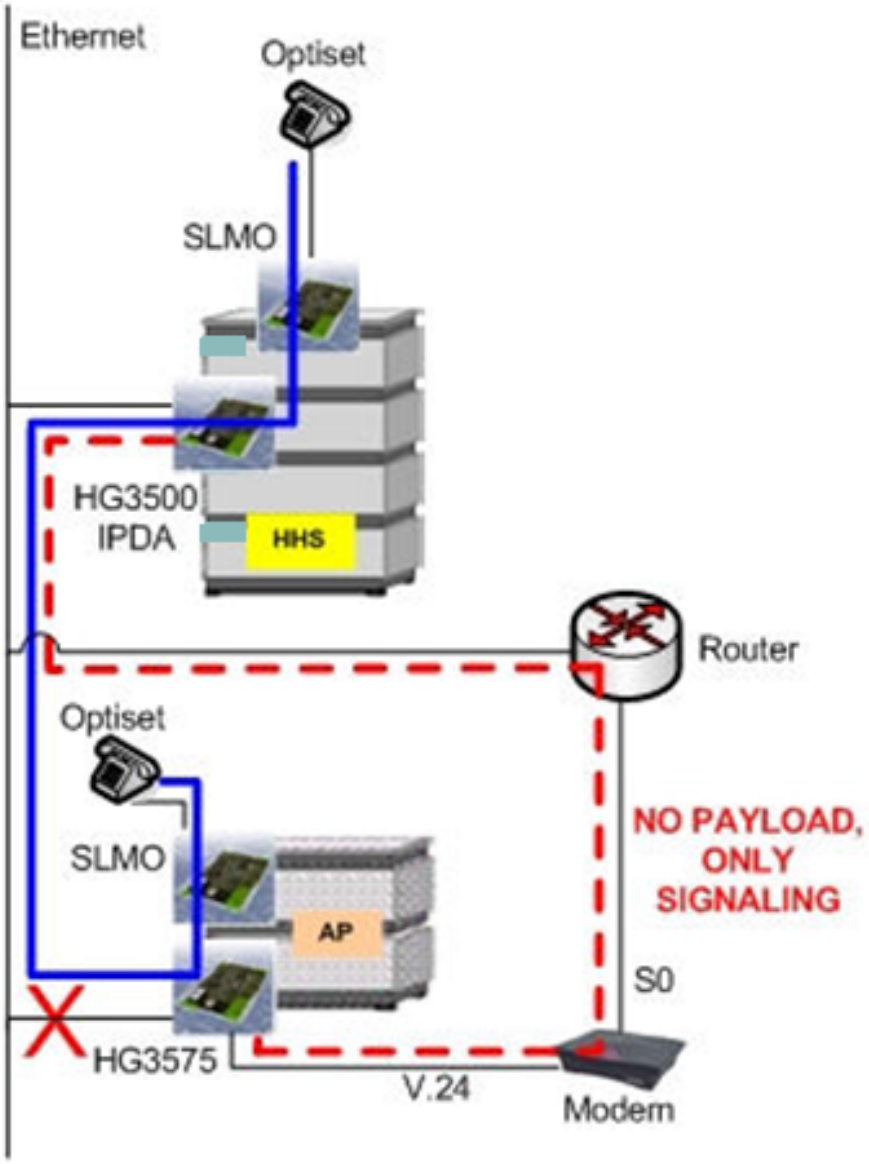
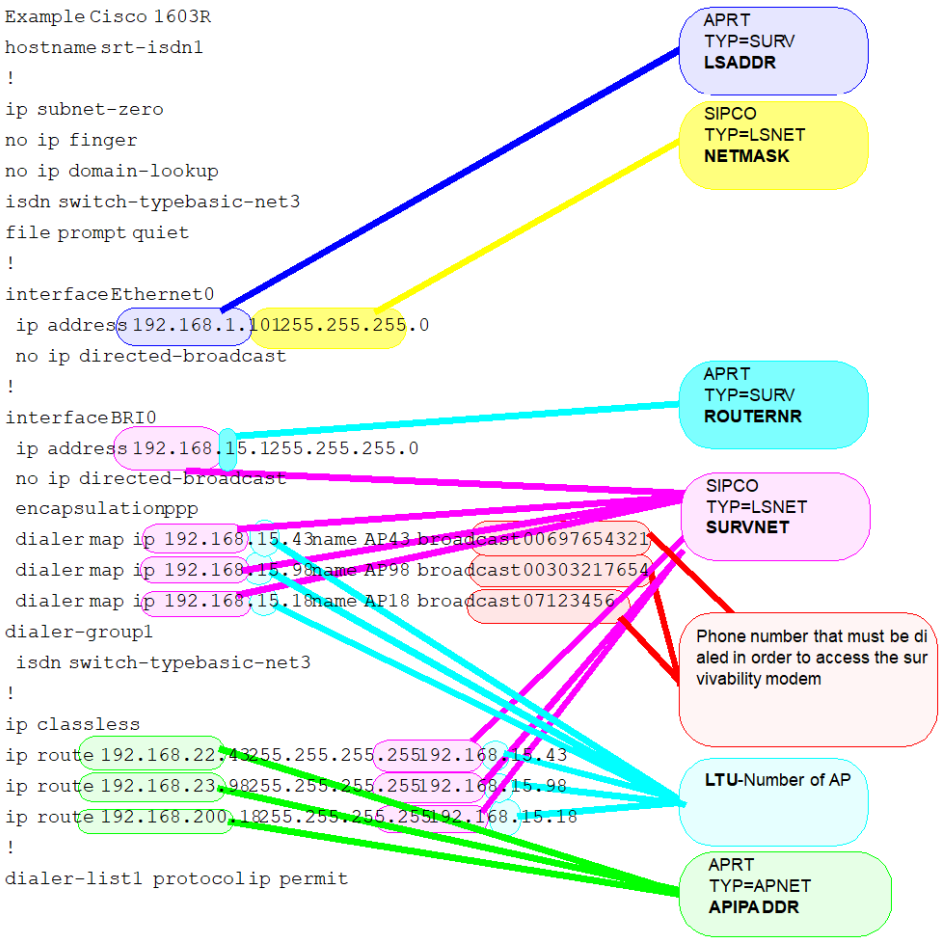


Figure 236: Signaling survivability without WAML replacement but with a router

By way of example, the settings for an external *Cisco 1603R* router are displayed.

IMPORTANT: The setting for this router is merely provided as an example and is only intended to illustrate how to use the parameters in a router configuration. The router selected in this case is not a special recommendation and its availability cannot be guaranteed. Routers from other product lines and manufacturers can also be used.



13.3.2 Signaling Survivability via alternate LAN

13.3.2.1 Configuring the OpenScape 4000

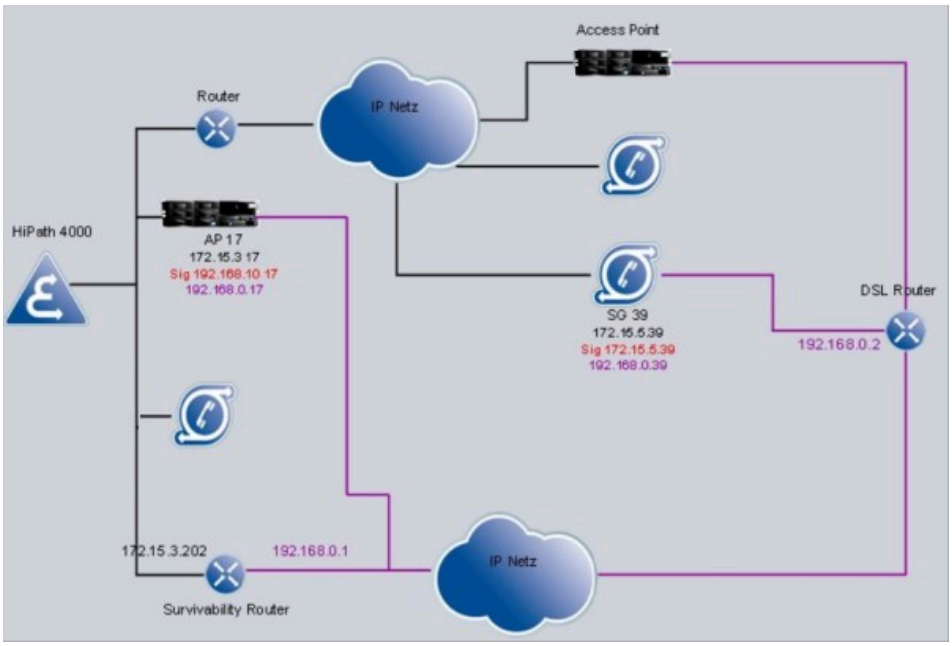


Figure 237: Signaling Survivability via alternate LAN

The configuration in the OpenScape 4000 switch is realized as follows:

- If signaling survivability via alternate LAN will be used, UDP must be configured for HSR signaling for the access point/OpenScape 4000 SoftGate.

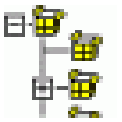
Access Point (direct link):

```
ADD-UCSU:UNIT=AP,LTG=1,LTU=17,LTPARTNO="Q2324-X10 ",SRCGRP=1,FRM►
TYPE=AP37009,CONNTYPE=APDL,LSRTADDR=172.15.3.17,APRTAD-
DR=172.15.3.1,LOCID=722,LOCATION="722
",PHONE=722,PLCHECK=YES,BCHLCNT=120,CONVLAW=YES,TCLASS=0,ALARMNO=0,
IPMODE=IPV4,DHCPV4=NO,DHCPV6=NO,SIUANN=1,SIUC=0,DTR=0,CNTRY-
CD=0,SIGMODE=HSRUDP;
OpenScape 4000 SoftGate (networked link):
ADD-UCSU:UNIT=AP,LTG=1,LTU=39,LTPARTNO="Q2329-X   ",SRCGRP=1,FRM►
TYPE=SOCOAP,CONNTYPE=APNW,LSRTADDR=172.15.3.1,APRTAD-
DR=172.15.5.1,LOCID=722,LOCATION="SG39
",PHONE=722,PLCHECK=YES,BCHLCNT=250,CONVLAW=NO,TCLASS=0,ALARMNO=0,S
OCOTYPE=SOCO500,IPMODE=IPV4,DHCPV4=NO,DHCPV6=NO,SIUANN=1,SI-
UC=0,DTR=0,CNTRYCD=0,SIGMODE=HSRUDP;
```

IMPORTANT: When switching from **HSRTCP** to **HSRUDP** or vice versa an `EXEC-USSU:TYPE=UPDATAP,LTU=<number>;` must be executed. Existing connections are cleared down without further warning!

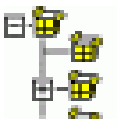
NOTICE: SIPCO parameter SURVNET has no effect on the feature Signaling Survivability via alternate LAN, however AMO APRT requires an entry to allow it to add a router.

- Announce the survivability routers in the system

	**Configuration Management > System Data > IPDA > IPDA Signaling Survivability Router** Click **Search**, enter or change the router number and address on the Router Data tab, then **Save**.
	`ADD-APRT:TYPE=SURV,CONF=ROUTER,ROUTERNO=1,LSADDR=172.15.3.202;`

Router 1 from the example in Figure 16 "Signaling Survivability via alternate LAN" is thus configured.

- Assign the access points to the survivability routers

	**Configuration Management > System Data > IPDA > IPDA Access Point** Click **Search**, set the desired router number on the **General** tab under signaling survivability and **Save**.
	`APRT:TYPE=SURV,CONF=AP,`**`LTU=17`**`,ROUTERNO=1,`**`SURVTYPE=SURVLAN`**`,SURVIP=192.168.0.17,SURVNETM=255.255.255.0,SURVRT=192.168.0.1,VLAN-TAG=NO,VLANID=0;` `ADD-APRT:TYPE=SURV,CONF=AP,`**`LTU=39`**`,ROUTERNO=1,`**`SURVTYPE=SURVLAN`**`,SURVIP=192.168.0.39,SURVNETM=255.255.255.0,SURVRT=192.168.0.2,VLAN-TAG=NO,VLANID=0;`

13.3.2.2 Configuring the LAN Interface

Additionally to the configuration with the AMOs the LAN interface of the vHG 3575 in the OpenScape 4000 SoftGate which is used for signaling survivability must be assigned.

WBM > Configuration > Signaling Survivability Interface

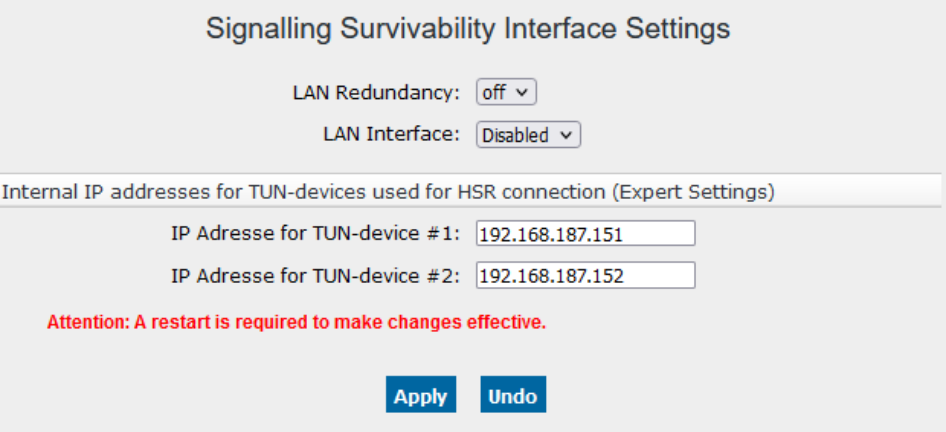


Figure 238: Signaling Survivability LAN interfaces

13.3.2.3 Configuring the Router

Example for a router configuration

```
interface FastEthernet0/0
/*IP address and netmask of the survivability LAN
  ip address 192.168.0.1 255.255.255.0
 duplex auto
 speed auto
!
interface FastEthernet0/1
/*IP address and netmask of the OpenScape 4000 LAN
 ip address 172.15.3.202 255.255.255.0
 duplex auto
 speed auto
!
ip route 0.0.0.0 0.0.0.0 172.15.3.1
ip route 172.15.5.37 255.255.255.255 192.168.0.37
/*Routing for SoftGate 39
ip route 172.15.5.39 255.255.255.255 192.168.0.39
/*Routing for AP 17
ip route 192.168.10.17 255.255.255.255 192.168.0.17
```

13.3.2.4 Replacement of a defect NCUI Board with a new NCUI Board

The golden load loadware of the NCUI board doesn't support UDP functionality which is necessary for signaling survivability via alternate LAN. Thus the following steps have to be performed when replacing the board.

There are two possibilities:

Possibility 1:

1) Copy the latest NCUI loadware to the new board before going in service with the board.
2) Perform the board replacement as usual (see also "Gateways HG 3500 and HG 3575" > Section 3.2.2, "Exchanging Boards").

Possibility 2:

1) Delete the assignment of the concerned access point/OpenScape 4000 SoftGate to the survivability routers.

DELTE-APRT:TYPE=SURF,KONF=AP,LTU=<number>;

1) Change signaling mode to **HSRTCP**.

CHANGE-UCSU:TYPE=AP,LTU=<number>,**SIGMODE=HSRTCP**;

1) In order for this change to become effective, the access point/OpenScape 4000 SoftGate has to be restarted.

EXEC-USSU:TYPE=UPDATAP,LTU=<number>;

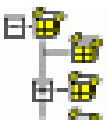
IMPORTANT: Existing connections are cleared down without further warning!

1) Put the new NCUI board in service (see “Gateways HG 3500 and HG 3575” > Section 3.2.2, “Exchanging Boards”).
2) Change back to **HSRUDP** as signaling mode (see Section 3.1.1, “Configuring the OpenScape 4000”).
3) Reconfigure the assignment of the survivability routers (see Section 3.1.1, “Configuring the OpenScape 4000”).

13.3.3 Is Signaling Survivability Currently Active? (DIS-UCSU)

When a system is operating with signaling survivability, it is often necessary - without analyzing any error messages - to query whether an access point is currently being controlled normally via LAN or whether it is being controlled via modem with signaling survivability.

This query is executed with the AMO UCSU.

	The query with the AMO UCSU can only be executed in expert mode. **Expert Mode > Expert Access > Open ...**<IP> with AMO (see AMO command)
	`DISPLAY-UCSU:AP,1,;` The AMO returns an overview of all configured access points, containing not just configured parameters, but also current operating states.

```
+---------+------------------+---------+-------------+----------+--------+
|ADDRESS  |EXPECTED CONFIGUR. |STATE    |LTUC MODULE   |LTU-TYPE  |FRMTYPE |
|         +------------------+---------+-------------+----------+--------+
|         |CONNTYPE  LOCATIONID LOCATION                            SRCGRP |
|         |PHONE:                          FAX:                            |
|         |LSRTADDR         APRTADDR       BCHL BCHLCNT PLCHECK  SIGNAL.  |
|         |IP MODE   DHCP V4  DHCP V6      AP REDUNDANCY TO APXY STATUS   |
|         |CONVLAW   CONTROL UNIT          TCLASS       ALARMNO           |
|         |CNTRYCD   SIGMODE                                               |
|         +----------------------------------------------------------------+
```

```
|         |SIGNAL. ENCRYPTION ACTIVE [ ]     PAYLOAD ENCRYPTION ACTIVE [ ] |
|         |SECURE STATE : SEE DESCRIPTION AT BOTTOM                        |
+---------+-------------------+---------+--------------+----------+--------+
|AP   1.17|ADDED              |READY    |Q2324-X10     |AP37009   |AP37009 |
|         +-------------------+---------+--------------+----------+--------+
|         |APDL      722 722                                           1 |
|         |PHONE:  722                        FAX:                         |
|         |172.015.003.017  172.015.003.001   120   100      YES   SURVLAN |
|         |    IPV4    NO       NO           AP REDUNDANCY TO AP           |
|         | YES        HOST-CC               0                0            |
|         |0           HSRUDP                                             |
+---------+-------------------+---------+--------------+----------+--------+
|         |SIUANN : 1   SIUC : 00   DTR : 00                               |
|         +----------------------------------------------------------------+
|         |CPTON / SIUTON :  NO DIFFERENCE TO ZAND                         |
+---------+-------------------+---------+--------------+----------+--------+
|AP   1.18|ADDED              |READY    |Q2329-X       |AP37009   |SOCOAP  |
|         +-------------------+---------+--------------+----------+--------+
|SOCOTYPE |APDL      722 722                                           1 |
|SOCO1000 |PHONE:  722                        FAX:                         |
|         |172.015.003.018  172.015.003.001   250   250       NO     MODEM |
|         |    IPV4    NO       NO           AP REDUNDANCY TO AP           |
|         |  NO        HOST-CC               0                0            |
|         |K           HSRTCP                                             |
+---------+-------------------+---------+--------------+----------+--------+
|         |SIUANN : D   SIUC : 0K   DTR : 0K                               |
|         +----------------------------------------------------------------+
|         |CPTON / SIUTON :  NO DIFFERENCE TO ZAND                         |
+---------+-------------------+---------+--------------+----------+--------+
|AP   1.19|ADDED              |READY    |Q2329-X       |AP37009   |SOCOAP  |
|         +-------------------+---------+--------------+----------+--------+
|SOCOTYPE |APDL      722 722                                           1 |
|SOCO500  |PHONE:  722                        FAX:                         |
|         |172.015.003.019  172.015.003.001   250   250      YES       LAN |
|         |    IPV4    NO       NO           AP REDUNDANCY TO AP           |
|         | YES        HOST-CC               0                0            |
|         |0           HSRUDP                                             |
+---------+-------------------+---------+--------------+----------+--------+
|         |SIUANN : 1   SIUC : 00   DTR : 00                               |
|         +----------------------------------------------------------------+
|         |CPTON / SIUTON :  NO DIFFERENCE TO ZAND                         |
+---------+-------------------+---------+--------------+----------+--------+
|AP   1.26|ADDED              |READY    |Q2305-X35     |AP37009   |AP37009 |
|         +-------------------+---------+--------------+----------+--------+
|         |APDL      722 722                                           1 |
|         |PHONE:  722                        FAX:                         |
|         |172.015.003.026  172.015.003.001    60    60       NO       LAN |
|         |    IPV4    NO       NO           AP REDUNDANCY TO AP           |
|         | YES        HOST-CC               0                0            |
|         |0           HSRTCP                                             |
+---------+-------------------+---------+--------------+----------+--------+
|         |SIUANN : 1   SIUC : 00   DTR : 00                               |
|         +----------------------------------------------------------------+
|         |CPTON / SIUTON :  NO DIFFERENCE TO ZAND                         |
+---------+-------------------+---------+--------------+----------+--------+
|AP   1.27|ADDED              |READY    |Q2305-X35     |AP37009   |AP37009 |
```

```
|         +------------------+---------+--------------+----------+---------+
|         |APDL      722 722                                          1 |
|         |PHONE:  722                       FAX:                        |
|         |172.015.003.027  172.015.003.001    60    60      YES       LAN |
|         |    IPV4    NO       NO           AP REDUNDANCY TO AP          |
|         | YES        HOST-CC               0                0          |
|         |0           HSRTCP                                            |
+---------+------------------+---------+--------------+----------+---------+
|         |SIUANN : 1   SIUC : 00   DTR : 00                             |
|         +--------------------------------------------------------------+
|         |CPTON / SIUTON :  NO DIFFERENCE TO ZAND                       |
+---------+------------------+---------+--------------+----------+---------+
|AP   1.36|ADDED             |READY    |Q2305-X35     |INCH19    |INCH19   |
|         +------------------+---------+--------------+----------+---------+
|         |APNW      722 722                                          1 |
|         |PHONE:  722                       FAX:                        |
|         |172.015.003.001  172.015.005.001    60    60      YES     MODEM |
|         |    IPV4    NO       NO           AP REDUNDANCY TO AP          |
|         |  NO        HOST-CC               0                0          |
|         |0           HSRTCP                                            |
+---------+------------------+---------+--------------+----------+---------+
|         |SIUANN : D   SIUC : 00   DTR : 00                             |
|         +--------------------------------------------------------------+
|         |CPTON / SIUTON :  NO DIFFERENCE TO ZAND                       |
+---------+------------------+---------+--------------+----------+---------+
|AP   1.37|ADDED             |READY    |Q2305-X35     |AP37009   |AP37009  |
|         +------------------+---------+--------------+----------+---------+
|         |APNW      722 722                                          1 |
|         |PHONE:  722                       FAX:                        |
|         |172.015.003.001  172.015.005.001    60    60       NO       LAN |
|         |    IPV4    NO       NO           AP REDUNDANCY TO AP          |
|         |  NO        HOST-CC               0                0          |
|         |0           HSRUDP                                            |
+---------+------------------+---------+--------------+----------+---------+
|         |SIUANN : 1   SIUC : 00   DTR : 00                             |
|         +--------------------------------------------------------------+
|         |CPTON / SIUTON :  NO DIFFERENCE TO ZAND                       |
+---------+------------------+---------+--------------+----------+---------+
|AP   1.38|ADDED             |READY    |Q2329-X       |AP37009   |SOCOAP   |
|         +------------------+---------+--------------+----------+---------+
|SOCOTYPE |APNW      722 SG38                                         1 |
|SOCO500  |PHONE:  722                       FAX:                        |
|         |172.015.003.001  172.015.005.001   250   250      YES     MODEM |
|         |    IPV4    NO       NO           AP REDUNDANCY TO AP          |
|         |  NO        HOST-CC               0                0          |
|         |0           HSRTCP                                            |
+---------+------------------+---------+--------------+----------+---------+
|         |SIUANN : 1   SIUC : 00   DTR : 00                             |
|         +--------------------------------------------------------------+
|         |CPTON / SIUTON :  NO DIFFERENCE TO ZAND                       |
+---------+------------------+---------+--------------+----------+---------+
|AP   1.39|ADDED             |READY    |Q2329-X       |AP37009   |SOCOAP   |
|         +------------------+---------+--------------+----------+---------+
|SOCOTYPE |APNW      722 SG39                                         1 |
|SOCO50   |PHONE:  722                       FAX:                        |
|         |172.015.003.001  172.015.005.001   250   250      YES       LAN |
```

```
|          |    IPV4    NO       NO           AP REDUNDANCY TO AP           |
|          |  NO        HOST-CC                0                0          |
|          |0           HSRUDP                                             |
+---------+------------------+---------+--------------+----------+--------+
|          |SIUANN : 1   SIUC : 00   DTR : 00                               |
|          +----------------------------------------------------------------+
|          |CPTON / SIUTON :  NO DIFFERENCE TO ZAND                         |
+---------+------------------+---------+--------------+----------+--------+
|AP   1.41|ADDED              |READY    |Q2329-X       |AP37009   |SOCOAP  |
|          +------------------+---------+--------------+----------+--------+
|SOCOTYPE |APDL      722 722                                           1 |
|SOCO500  |PHONE:  722                        FAX:                         |
|          |172.015.003.041  172.015.003.001   250   250      YES       LAN |
|          |    IPV4    NO       NO           AP REDUNDANCY TO AP           |
|          | YES        HOST-CC                0                0          |
|          |0           HSRUDP                                             |
+---------+------------------+---------+--------------+----------+--------+
|          |SIUANN : 1   SIUC : 00   DTR : 00                               |
|          +----------------------------------------------------------------+
|          |CPTON / SIUTON :  NO DIFFERENCE TO ZAND                         |
+---------+------------------+---------+--------------+----------+--------+
|AP   1.50|ADDED              |READY    |Q2329-X       |AP37009   |SOCOAP  |
|          +------------------+---------+--------------+----------+--------+
|SOCOTYPE |APNW      722 SG50                                          1 |
|SOCO500  |PHONE:  722                        FAX:                         |
|          |172.015.003.001  172.015.005.001   250   250      YES   SURVLAN |
|          |    IPV4    NO       NO           AP REDUNDANCY TO AP           |
|          |  NO        HOST-CC                0                0          |
|          |0           HSRUDP                                             |
+---------+------------------+---------+--------------+----------+--------+
|          |SIUANN : 1   SIUC : 00   DTR : 00                               |
|          +----------------------------------------------------------------+
|          |CPTON / SIUTON :  NO DIFFERENCE TO ZAND                         |
+---------+------------------+---------+--------------+----------+--------+
```

13.4 Relevant AMOs

Table 75: AMO APRT parameters in ADD branch under TYPE=SURV, CONF=ROUTER

AMO	Parameter	Sprache/ Language	Beschreibung/ Description
APRT	ROUTERNR	d	Nummer des Routers für Signaling Survivability. IPDA unterstützt bis zu 10 Survivability Router, welche von 1..10 durchnummeriert und über diesen Index verwaltet werden.

AMO	Parameter	Sprache/ Language	Beschreibung/ Description
	ROUTERNO	e	Number of the Router for Signaling Survivability. IPDA supports up to 10 survivability routers, numbered 1..10 which are administered using this index.
	LSADR	d	IP-Adresse eines Routers für Signaling Survivability im OpenScape 4000 LAN Segment. Diese IP-Adresse muss zum OpenScape 4000 LAN Segment gehören (siehe IP Distributed Architecture > Parameter **NETADR** im AMO SIPCO, Table 1 “AMO SIPCO parameters in ADD branch or for CHANGE unc
	LSADDR	e	IP Address of a Router for Signaling Survivability in the OpenScape 4000 LAN Segment. This IP address must belong to the OpenScape 4000 LAN Segment (see IP Distributed Architecture > parameter **NETADDR** in AMO SIPCO, Table 1 “AMO SIPCO parameters in ADD branch or for CHANGE unc

Table 76: AMO APRT parameters in ADD branch under TYPE=SURV, CONF=AP

AMO	Parameter	Sprache/ Language	Beschreibung/Description
APRT	ROUTERNR	d	Nummer des Routers für Signaling Survivability. Bestimmt einen der bis zu 10 Survivability Router, über den dieser Access Point erreicht werden soll.
	ROUTERNR	e	Number of the Router for Signaling Survivability. Selects one of the up to 10 survivability routers, via which this Access Point shall be reached.
	SURVTYP	d	MODEM = Signaling Survivability über Modem SURVLAN = Signaling Survivability über alternatives LAN

AMO	Parameter	Sprache/ Language	Beschreibung/Description
	SURVTYPE	e	MODEM = Signaling survivability via Modem SURVLAN = Signaling survivability via alternate LAN

Table 77: AMO UCSU parameter in ADD/CHANGE branch under UNIT=AP

AMO	Parameter	Sprache/ Language	Beschreibung/Description
UCSU	SIGMODE	d	HSRTCP: HSR über TCP-Verbindung HSRUDP: HSR über UDP-Verbindung
	SIGMODE	e	HSRTCP: HSR via TCP connection HSRUDP: HSR via UDP connection

14 SIP Connectivity

14.1 Overview

The following SIP interfaces are available for OpenScape 4000:

- SIP subscriber
- UFIP Devices
- SIP trunking

14.1.1 Interfaces

14.1.1.1 SIP Subscriber

The feature "SIP Subscriber for OpenScape 4000" encompasses the operation of SIP endpoints, which can be run on a OpenScape 4000 system using a gateway (virtual HG 3500 or HG 3500).

14.1.1.2 UFIP Devices

UFIP (Universal Feature access IP) is a new SIP device interface with enhanced CSTA support.

The UFIP interface provides Circuit connectivity.

UFIP is the preferred SIP device interface.

14.1.1.3 SIP Trunking

OpenScape 4000 supports:

1) SIP-Q trunking (e.g. for the connection to OpenScape Voice)

- native SIP trunking (e.g. for the connection to SIP service provider)

14.1.2 Supported RFCs (Request for Comments) for SIP Interfaces

Table 78: Supported RFCs (Request for Comments) for SIP interfaces

RFC-Number	Title	Interfaces:		
		Subscriber	Native Trunk	SIP-Q
RFC 2198	RTP Payload for Redundant Audio Data	Yes	Yes	Yes

RFC-Number	Title	Interfaces:		
		Subscriber	Native Trunk	SIP-Q
RFC 2246	The TLS Protocol Version 1.0	Yes	Yes	Yes
RFC 2327	SDP: Session Description Protocol (obsoleted by RFC4566)	Yes	Yes	Yes
RFC 2396	Uniform Resource Identifiers (URI): Generic Syntax	Yes	Yes	Yes
RFC 2617	HTTP Authentication: Basic and Digest Access Authentication	Yes	Yes	Yes
RFC 2782	DNS RR for specifying the location of services (DNS SRV)	No	Yes	Yes
RFC 2833	RTP Payload for DTMF Digits, Telephony Tones and Telephony Signals	Yes	Yes	Yes
RFC 2976	The SIP INFO Method	No	No	Yes
RFC 3204	MIME media types for ISUP and QSIG Objects	Yes	Yes	Yes
RFC 3261	SIP: Session Initiation Protocol	Yes	Yes	Yes
RFC 3262	Provisional Response Acknowledgment (PRACK) Early Media	Yes	Yes	Yes
RFC 3263	SIP Locating Servers	No	Yes	Yes
RFC 3264	An Offer/Answer Model with SDP	Yes	Yes	Yes
RFC 3265	Session Initiation Protocol (SIP)-Specific Event Notification	Yes	No	No
RFC 3310	HTTP Digest Authentication	Yes	Yes	Yes
RFC 3311	Session Initiation Protocol (SIP) UPDATE Method	Yes	Yes	Yes

RFC-Number	Title	Interfaces:		
		Subscriber	Native Trunk	SIP-Q
RFC 3323	A Privacy Mechanism for the Session Initiation Protocol (SIP)	Yes	Yes	No
RFC 3324	Short Term Requirements for Network Asserted Identity	Yes	Yes	Yes (but no use case)
RFC 3325	Private Extensions to the Session Initiation Protocol (SIP) for Asserted Identity within Trusted Networks	Yes	Yes	No
RFC 3326	The Reason Header Field for the Session Initiation Protocol (SIP)	No	No	Yes
RFC 3484	Default Address Selection for Internet Protocol version 6 (IPv6)	Yes	Yes	Yes
RFC 3515	The Session Initiation Protocol (SIP) Refer Method[5]	Yes	Yes	No
RFC 3550	RTP: Transport Protocol for Real-Time Applications	Yes	Yes	Yes
RFC 3551	RTP Profile for Audio and Video Conferences with Minimal Control	Yes	Yes	Yes
RFC 3581	An Extension to the Session Initiation Protocol (SIP) for Symmetric Response Routing	No	Yes	No
RFC 3711	The Secure Real-time Transport Protocol (SRTP)	Yes	Yes	Yes

5 Refer is only supported I/C for SIP subscribers and native SIP Trunks (configurable in WBM > SIP Trunk Profiles) - (NOT RECOMMENDED FOR SIP Service Providers due to accounting, billing, permissions etc.)

RFC-Number	Title	Interfaces:		
		Subscriber	Native Trunk	SIP-Q
RFC 3725	Best Current Practices for Third Party Call Control (3pcc) in the Session Initiation Protocol (SIP)	Yes	No	Yes
RFC 3830	MIKEY: Multimedia Internet KEYing	No	Yes	Yes
RFC 3842 (partly)[6]	Message Waiting Indication Event Package	Yes	Yes	No
RFC 3891	The Session Initiation Protocol (SIP) Replaces Header	Yes	Yes	No
RFC 3892	The Session Initiation Protocol (SIP) Referred-By Mechanism [7]	Yes	Yes	No
RFC 4028	Session Timers in the Session Initiation Protocol (SIP)	Yes	Yes	Yes
RFC 4119	A Presence-based GEOPRIV Location Object Format	No	Yes	Yes
RFC 4291	IP Version 6 Addressing Architecture	Yes	Yes	Yes
RFC 4568	Session Description Protocol (SDP) Security Descriptions for Media Streams	Yes	Yes	Yes
RFC 4733	RTP Payload for DTMF Digits, Telephony Tones and Telephony Signals	Yes	Yes	Yes

6 "partly" means that only the static subscription at Voice Mail Server is supported (in outgoing direction). OpenScape 4000 doesn't support dynamic subscription in outgoing direction, i.e. no SUBSCRIBE message is sent. Static subscription is typical for PBXes (like OpenScape 4000) and dynamic subscription is typical for SIP clients. In incoming direction (e.g. from a SIP client to OpenScape 4000), both static and dynamic subscription is supported.

7 Refer is only supported I/C for SIP subscribers and native SIP Trunks (configurable in WBM > SIP Trunk Profiles) - (NOT RECOMMENDED FOR SIP Service Providers due to accounting, billing, permissions etc.)

RFC-Number	Title	Interfaces:		
		Subscriber	Native Trunk	SIP-Q
RFC 5009	Private Header (P-Header) Extension to the SIP for Authorization of Early Media	No	Yes	No
RFC 5139	Revised Civic Location Format for Presence Information Data Format Location Object (PIDF-LO)	No	Yes	Yes
RFC 5246	Transport Layer Security (TLS) Protocol Version 1.2	Yes	Yes	Yes
RFC 5491	GEOPRIV Presence Information Data Format Location Object (PIDF-LO) Usage Clarification, Considerations and Recommendations	No	Yes	Yes
RFC 5746	Transport Layer Security (TLS) Renegotiation Indication Extension	Yes	Yes	Yes
RFC 5806	Diversion Indication in SIP	Yes	Yes	No
RFC 5923	Connection Reuse in the Session Initiation Protocol (SIP)	Yes	Yes	Yes
RFC 6140	Registration for Multiple Phone Numbers in the Session Initiation Protocol (SIP)[8]	No	Yes	Yes
RFC 6716	Definition of the Opus Audio Codec	Yes	Yes	Yes
RFC 7433	A Mechanism for Transporting User-to-User Call Control Information in SIP	No	Yes	Yes

[8] Only possible if SIP trunk profile is used.

RFC-Number	Title	Interfaces:		
		Subscriber	Native Trunk	SIP-Q
RFC 7852	Additional Data Related to an Emergency Call	No	Yes	Yes
RFC 7044	An Extension to the Session Initiation Protocol (SIP) for Request History Information	No	Yes	Yes
RFC 8446	Transport Layer Security (TLS) Protocol Version 1.3	No	Yes	Yes

14.1.3 Boards Used

The common gateway board HG 3500 and the virtual HG 3500 in OpenScape 4000 SoftGate support SIP connectivity. For details, see "Gateways HG 3500 and HG 3575", Chapter 3, “Supported Gateways” and the documentation for "OpenScape 4000 SoftGate".

14.1.4 Gateway Port Configuration

- UDP
- UDP as transport protocol is allowed on SIP subscriber and native SIP trunk interface. Symmetric UDP ports are used. The listening UDP port is configured with AMO parameter SIPTCPP.
- TCP/TLS
- Ephemeral ports are used as source ports. The RFC 5923: Connection Reuse in the Session Initiation Protocol (SIP) is supported for TCP and TLS connections.

  The listening TCP port is configured with AMO parameter SIPTCPP, the listening TLS port with AMO parameter SIPTLSP.

14.2 SIP Subscriber

From OpenScape 4000 V8 the preferred method for configuring SIP Subscribers is UFIP. Should any feature discrepancy be noticed to prior S0PP configuration then it should be reported via customer ticket.

Up to 240 native SIP subscribers can be configured on the common gateway HG 3500 and the virtual HG 3500. The total number of 240 IP subscribers per common gateway (CGW) refers to HFA and SIP subscribers (e.g. 200 HFA and 40 SIP subscribers).

SIP subscriber can also be connected over the Internet - see Chapter 14, “Secure Remote Subscriber”.

14.2.1 SIP Endpoints

For the list of supported certified SIP clients please check the Common Compatibility Matrix, the "Unify Ready" certifications and the following links:

- https://unify.com/en/solutions/phones-and-clients
- https://wiki.unify.com/wiki/Devices

3rd Party Native SIP Clients can generally be connected to the OpenScape 4000 Gateway without any Project Specific Release (PSR).

The list of RFCs supported by OpenScape 4000 can be found in the SIP Connectivity chapter.

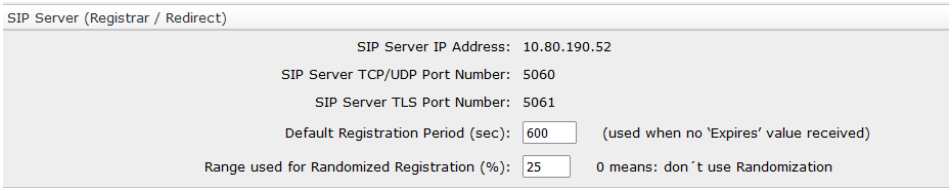
In case the OpenScape 4000 Gateway do not conform to any of the published RFCs, any encountered issue can be addressed via a Service Ticket and will be further evaluated.

14.2.2 Service Information

- RFC 2833 (DTMF via RTP) and RFC 2198 (Support of Redundant Audio Data) are supported.
- The following table shows the combinations of the parameters **SECZONE**, **USERID** and **PASSWD** in AMO SBCSU to make secure registration possible.

Parameter			
SECZONE	USERID	PASSWD	Possible
Set	Set	Set	Yes
Not Set	Set	Set	Yes
Set	Not Set	Set	Yes
Not Set	Not Set	Set	Yes
Set	Not Set	Not Set	No
Not Set	Set	Not Set	No
Set	Set	Not Set	No
Not Set	Not Set	Not Set	Yes

- As an additional security measure, configuring SUBIPADD parameter restricts client registration to only the defined IP address, preventing multiple client (multiple IPs) registration under the same subscriber.
- Any Register "expires" value offered by a partner will be honored with a default randomization value of 25% (to avoid load peaks). If no value is provided, then a default of 600 seconds (10 minutes) will be used. Both Randomization Timer (0% will deactivate randomization) and default time (when none received) will be configurable. The range 120-3600 is allowed for **Default Registration Period**. The new configuration parameters replace the old ones and can be found under **WBM > Configuration > Voice Gateway > SIP Parameters**.



1) With this range a random timer will be taken from between this range for further re-registrations after the initial SIP REGISTER message.

   The usual minimum time allowed for SIP registration is hard coded as 120 seconds. Should more than 60 subscribers be configured, then the minimum time is then 120 + number of SIP subscribers over 60 e.g. for 65 stations, the minimum allowed time is then 125, for 70 subscribers 130 seconds etc.

   NOTICE: It is recommended not to exceed 20 SIP Registration messages per second.

14.2.3 Features

Table 79: UFIP SIP Features overview

Feature	UFIP SIP
CLIP/CLIR	☑
COLP/COLR	☑
Name display	☑
Call forwarding (no reply, busy, unconditional)?	☑
Hold / Retrieve / Toggle	☑
Direct call park	☑
Attended call transfer	☑
Semi attended call transfer	☑
Local 3-party conference (if supported from the SIP terminal)	☑
Message Waiting Indication (MWI) (for more information, please refer to Section 2.5.7,"Message Waiting Indication (MWI)")	☑
Do-not-disturb	☑
CSTA/ACL monitoring of SIP subscriber	☑
Hunt group with SIP subscriber as slave	☑

Feature	UFIP SIP
T.38 fax connections with Mediatrix 41xx	☑
DTMF signaling (Inband and RFC2833 compliant)	☑
SIP session timer RFC4028 compliant (more information can be found in Section 2.4,“Restrictions”)	☑
Digest Authentication	☑
Number Identification	☑
Call waiting (take, reject or forward the call)	☑
Second call (forward the second call, hold)	☑
SIP Subscriber as Member/Master of an ONS Group (see OpenScape 4000 documentation, **Section 3 - Feature Usage Examples > Parallel Ringing - One Number Service (ONS)**)	☑
SIP Subscriber as DSS Key on a Desktop Phone	☑
SIP Peer Filtering	☑
Supported RFCs (see Section 1.2,“Supported RFCs (Request for Comments) for SIP Interfaces”).	☑
Programming of central call forwarding (CFU, CFNR, CFB)	☑
Remote call forwarding activation	☑
Number suppression	☑
Blind transfer	☑
Recall after transfer ringing	☑
Override and Emergency Release/Intrusion (only Invocation. UFIP devices can’t be intruded / Forced released)	☑
Pickup group	☑
Call back on ‘busy’ with WL3/WL4 phones. For configuration, please see Chapter 8, “OpenStage WL3/WL4 Configuration”.	☑
Display suppression via access code (DISUON/DISUOFF)	☑
Private call via access code + PIN	☑
Up to five subscribers registered with the same number	☑

Feature	UFIP SIP
Support of registration with E.164 number (with and without leading +) and extension-number only	☑
ACL/CSTA Services: Make call/ Defect/ SST etc.	☑
ACL/CSTA: Monitor Set	☑
ACL/CSTA: Monitor Cancel	☑
ACL/CSTA: Device Type Check	☑
ACL/CSTA: Get Switching Function Devices	☑
ACL/CSTA: Snapshot Call	☑
ACL/CSTA: Answer Call	☑
ACL/CSTA: Snapshot Monitor	☑
ACL/CSTA: Divert Call	☑
ACL/CSTA: Continue Call	☑
ACL/CSTA: Make Predictive Call	☑
ACL/CSTA: Reject Call	☑
Busy override, emergency intrusion and emergency disconnect	☑
Get Logical Device Information	☑
Switching function devices	☑
Change monitor filter	☑
Alternate Call - Consultation Call must have been initiated via Consultation Call Service	☑
Conference Call - Consultation Call must have been initiated via Consultation Call Service	☑
Make Call - Client must support procedure 9.18.1.1 defined in OSCAR SIP client spec. https://sp2013.myatos.net/org/usp/_layouts/DocIdRedir.aspx?ID=5SMA7FHWUQFR-1472063257-248304 HINT: Unify phones require having **Configuration > Incoming Calls > CTI Calls > Allow auto-answer** to be activated to allow the function.	☑

Feature	UFIP SIP
Reconnect Call - Consultation Call must have been initiated via Consultation Call Service	☑
Transfer Call - Consultation Call must have been initiated via Consultation Call Service	☑
Get Do Not Disturb - Get System Do Not Disturb	☑
Get Forwarding - Get System Call Forwarding Status	☑
Set Do Not Disturb - Set System Do not Disturb	☑
Set Forwarding - Set System Call Forwarding	☑
Answer Call Service - Client must support procedure 9.18.1.1 defined in OSCAR SIP client spec. https://sp2013.myatos.net/org/usp/_layouts/DocIdRedir.aspx?ID=5SMA7FHWUQFR-1472063257-248304 HINT: Unify phones require having **Configuration > Incoming Calls > CTI Calls > Allow auto-answer** to be activated to allow the function.	☑
SIP Subscribers support Remote Subscriber with OS-SBC Restriction: OS-SBC does not support Cluster Server assignment for Remote Subscribers, like for ATC in Remote Endpoints. Thus resulting in a limitation of 240 registered SIP subscribers per Gateway. Only Clustered Mode with Routing Prefix usage is supported which could extend the limitation.	☑

IMPORTANT: All other features that are offered by the SIP subscribers but require board support do not work.

SIP phones have a different behavior compared to HFA or digital phones (e.g. OpenStage HFA/T). Because of the different behavior for SIP phones, ACL monitoring will show in some call scenarios other monitoring flows compared to ACL monitoring of digital extensions.

HiPath CAP V3.0 R9 (or higher) is needed for the corresponding CSTA services. These are

- CSTA Monitor Start/Stop
- CSTA Snapshot Device/Call
- CSTA Get Device Type
- CSTA Get Switching Function Devices

The BLF WIN application R15.4.0 (busy lamp field) supports this new CSTA/ACL monitoring feature and is able to display the device status in the busy lamp field of the attendant consoles.

Passive Features

The following features cannot be activated by the SIP subscriber itself, but the SIP subscriber can be integrated:

- (S0PP & UFIP*) Call back on busy/no reply (A callback can be entered on a SIP terminal if free / busy, but the SIP terminal itself cannot enter a callback).
- *CCBS is supported for WL3/WL4 devices as an active feature.
- (S0PP) SIP subscriber can’t dial the code for call pickup but it can be a passive member of the pickup group. That means other subscribers of the pickup group can pick up the calls whose destination number is the number of the SIP subscriber.

UFIP WABE DARs

The following WABE DARs are available from an UFIP device:

- RA
- KNOVR
- PU
- ACDLOGON
- ACDLOGOF
- ACDNAV
- ACDWORK
- OWNNODE
- RELEASE
- EOVR
- FLTRACE
- TIE
- TIEATND
- SPDC1
- SPDC2
- ATND
- FRCALTRT
- SCONSCO
- SCONSI
- CO
- HUNT
- AHTVCE
- DHTVCE
- NOEC
- STN
- STNREL
- ATNDDID
- ATNDIND
- APIN
- DPIN
- DISUON
- DISUOFF
- CCMS
- CCMSURG
- CCMANS
- AFWDEXIN

- AFWDNA
- AFWDB
- DFWDVCE
- AFWDVCE
- AFFWDVCE
- DFFWDVCE
- NOPT

Support of uaCSTA

OpenScape 4000 only supports uaCSTA for CSTA requests, and not for CSTA events. Please see Appendix D of CSTA Connectivity Adapter - Application Developer's Guide (ADG) for a list of supported requests.

14.2.4 Restrictions

14.2.4.1 Restrictions of System Features

The following system features cannot be used by SIP terminals:

- Exec. / Secr. - SIP terminals cannot be configured as Chese members.
- Keyset functionality - SIP terminals cannot be configured as keysets.
- ACD (automatic callback (CCBS / CCNR))
- Witness Facility - An SIP terminal can only be the passive subscriber for the witness facility.
- Malicious Call Identification/Tracing - A SIP terminal can be traced, but cannot trace a connection itself.
- UFIP devices access system features sending the entire digit string at once. Currently this string is limited at 22 digits. For example, in order to enable “remote call forwarding”, the UFIP user has to dial: <AFWDREM_WABE_CD><src_STNO_#><PIN_src_STNO#><dest_STNO_#> - entire string cannot exceed 22 digits.
- For activating a PIN from an UFIP device, PINNKEY has to be set to **YES** in the coresponding PERSI/COPIN.
- In case of a feature activation from a SIP device (configured as UFIP subscriber) there is no confirmation on the device display that the feature has been activated.
- No DMC in UFIP-UFIP, in the recording cases.

14.2.4.2 Restrictions of Terminal Features

The following entries must be deactivated on SIP terminals (either in the DLS “Feature Availability” menu or on the terminal directly), as these features are **not** supported by the OpenScape 4000:

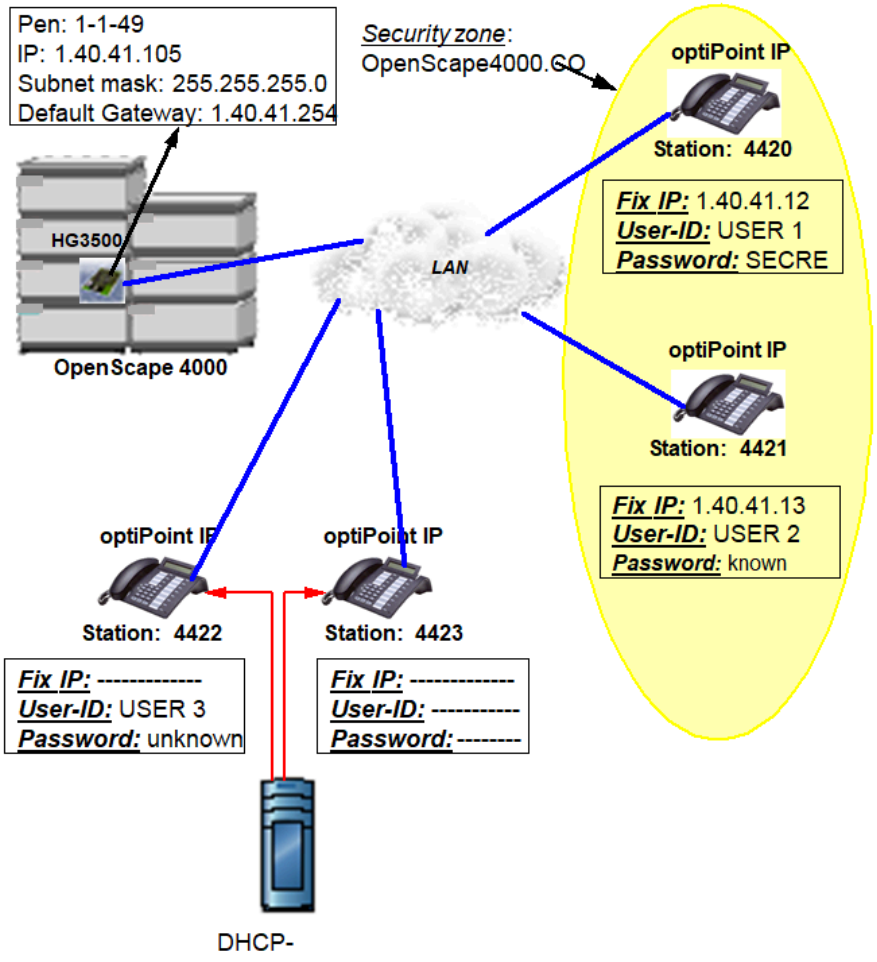
- Log forwarded calls
- Call display name
- Music on Hold
- Message waiting
- Auto. reconnect

- Park
- Call park pickup
- Call back on busy (supported only with WL3/WL4 phones)
- Call back on no reply

14.2.4.3 General restrictions

Parallel registration is released generally only for the usage with UnifyPhone and OpenScape Mobile Clients. The endpoint which invoked features like call deflection are not supported when multiple registration is active for any other type of SIP client.

14.2.5 Configuration



14.2.5.1 STMI2/4 and STMIX/STMIY Board Configuration

	**Configuration Management > System Data > Board > CGW Function Block** Click **New**, enter data and click **Save**. **Configuration Management > System Data > Board > Board** Click **New**, enter data (header information, **General Board Data** tab, **STMI2-IGW Board Data** tab, **CGW Functionalities** tab) and **Save**.

	`ADD-BFDAT:FCTBLK=1,FUNCTION=SIP,BRDBCHL=BCHL60;`
	
	`CHANGE-BFDAT:CONFIG=CONT,FCTBLK=1,FUNCTION=SIP,LINECNT=10,BCHLCNT=10;`
	
	`CHANGE-BFDAT:CONFIG=OK,FCTBLK=1,ANSW=YES;`
	`ADD-BCSU:MTYPE=IPGW,LTG=1,LTU=1,SLOT=49,PARTNO="Q2316-X ",FCTID=1,FCT▶`
	`BLK=1;`
	`ADD-CGWB:LTU=1,SLOT=49,SMODE=NORMAL,IPADR=1.40.41.105,NET▶`
	`MASK=255.255.255.0,DEFRT=1.40.41.254;`
	The Parameter **GWAUTREQ** and **SIPREG** must be set to NO,in situations where the board is used for SIP Subscriber.
	`CHANGE-CGWB:MTYPE=CGW,LTG=1,LTU=1,SLOT=49,TYPE=SIPTRERH,GWAUTREQ=NO;`
	`CHANGE-CGWB:MTYPE=CGW,LTG=1,LTU=1,SLOT=49,TYPE=SIPTRSSA,SIPREG=NO;`

14.2.5.2 Configuring a SIP Subscriber

IMPORTANT: Configuration of HG 3500 (CGW) board is prerequisite for SIP subscriber support (see Section 2.5.1, “STMI2/4 and STMIX/STMIY Board Configuration”).

IMPORTANT: If the parameters **SECZONE**, **USERID** and **PASSWD** are used for a secure registration in the AMO SBCSU, the parameter **AUTHERF** is set to **YES** and the security data must be set also in the SIP terminal!

IMPORTANT: The parameter **MBCHL** in AMO SDAT should be set for all SIP subscribers. If this parameter is not set, features which need a second B channel are not possible (e.g. conference, second call).

IMPORTANT: For all types of SIP phones settings like volume or ring type are not controlled by the system, so values set via AMO ACTDA/AMO KCSU for such devices are not used.

UFIP Interface configuration

UFIP subscribers can be configured, on IP gateways (STMI or vHG) with SIP functionality (BFDAT). UnifyPhone app functionality is provided only via vHG (SoftGate).

In general, “regular” SIP endpoints and UnifyPhone clients can be configured in parallel on the same gateway.

AMO:

ADD-SBCSU:STNO=<UFIP_STN>,OPT=OPTI,CONN=IP2,PEN=<X-Y-Z-T>,DVCFIG=UFIP;

For Digest Authentication parameters IPPASW, USER ID and SECZONE have to be configured.

The client supports registration with E.164 number (with and without leading +) and extension-number only.

Registration can be checked via vHG WBM: Configuration > Voice Gateway > Clients > UFIP SIP.

Actual SIP devices do not require any specific loadware or configuration changes.

14.2.5.3 Removing a SIP Subscriber

	**Configuration Management > Station > Station** Click **Search**. Select subscriber you want to delete. Click **Delete**.
	`DELETE-SBCSU:STNO=4420,SVC=ALL;`

14.2.5.4 Changing a SIP Subscriber

The SIP endpoint data is changed under branch “OPT=FPP”

	**Configuration Management > Station > Station** Click **Search**. Select subscriber you want to change. Change data. Click **Save**.
	`CHA-SBCSU:STNO=4220,OPT=OPTI,SUBIPADD=1.40.41.15;`

14.2.5.5 Enabling/Disabling DMC

DMC is enabled for station 4420 and disabled for station 4422 and 4423.

	Configuration Management > Station > Station Click **Search**. Select subscriber you want to change the DMC settings. Acivate/deactivate check box **DMC allowed** on **Basic 3** tab sheet.
	`CHANGE-SDAT:STNO=4420,TYPE=ATTRIBUT,AATTR=DMCALLWD;`

NOTICE: Changing this attribute only takes effect after deactivation and re-activation of the corresponding circuit via RES-DSSU.

14.2.5.6 SIP Session Timer

The "SIP Session Timer" provides a "keep alive" system for SIP sessions. If this feature is activated, reINVITE or UPDATE messages are sent periodically during an established connection. If the partner answers, the session is extended by a period of time previously arranged between the partners. If the partner does not answer, the session is released. This verifies whether the connection is still established.

The marginal values for the duration of the extension can be set in the WBM of the gateway:

1) WBM -> Configuration -> Voice Gateway -> SIP Parameters

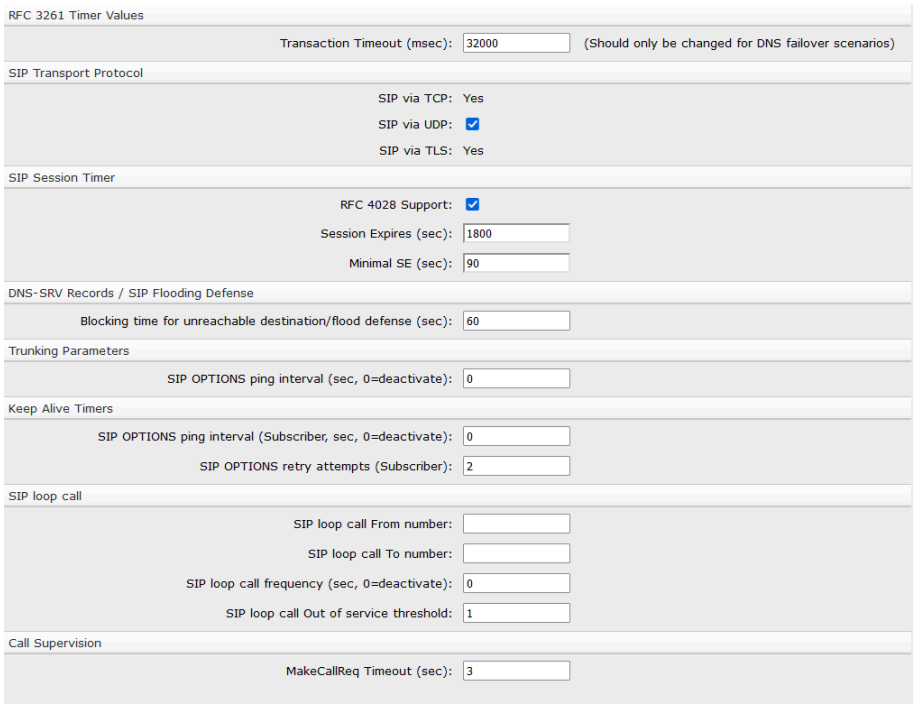


Figure 239: SIP session timer

- The SIP session timer is activated by the **Use RFC4028** checkbox.
- **Session Expires**: Determines the maximum time by which a session can be extended.

- **Minimal SE**: Determines the minimum time by which a session can be extended.

The actual duration of the extension also depends on the partner's settings but is within the configured interval. A session is renewed as soon as half the duration has expired.

IMPORTANT: Please note that very short intervals lead to increased message traffic!

14.2.5.7 Subscriber Parameters

Starting with V10R1 OpenScape 4000 supports Subscriber Parameters for UFIP clients based on SIP OPTIONS messages.

If a station does not respond in a certain amount of time to these messages, the station is de-registered.

WBM Implementation

Subscriber Parameters are displayed in the WBM of the HG board, at Configuration - Voice Gateway - SIP Options.

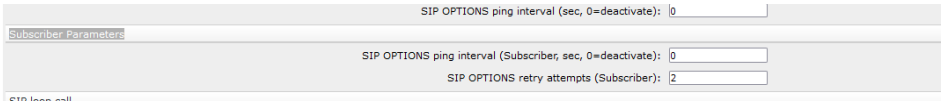


Figure 240: Subscriber Parameters

SIP OPTIONS ping interval:

- The timer is started by setting a value not equal to 0, but in the range of 30 - 3600 seconds.
- The value represents the time interval after which an OPTIONS message will be sent to a station.

SIP OPTIONS retry attempts:

- It represents the number of sent messages for which no answer (200 OK) is received, before the station is de-registered.
- The value should be in the range of 1 - 5.

14.2.5.8 Message Waiting Indication (MWI)

The Message Waiting Indication MWI feature is activated/deactivated on each SIP subscriber by setting the **PMIDX** parameter in AMO SBCSU and using authorization **MB** in COS of the subscriber.

The feature is realized both for OpenScape 4000 SoftGate and common gateway HG 3500.

MWI feature activation:

- Use AMO RICHT for **MODE=PM** to create a new IDX for phone mail access:

ADD-RICHT:MODE=PM,IDX=1,SAN=0894711,NAME=XPRESSION;

MODE=PM	Address mode of the route is Phone Mail (PM)
IDX	Index of service access number
SAN	Service access number
NAME	Name of the route

- **PMIDX=1** must be set for SIP subscribers in AMO SBCSU.
- Set **AVCE=MB** (mail box (authorization to receive mail)) with AMO COSSU in the subscriber COS.

MWI feature deactivation:

- **PMIDX=0** must be set for SIP subscribers in AMO SBCSU.
- Set **DVCE=MB** to remove/deactivate authorization to receive mail in the subscriber COS with AMO COSSU.

14.2.5.9 SIP Subscriber as DSS Key on a Desktop Phone

Feature Description

It is possible to configure a SIP subscriber as a DSS key (DSS destination) on a desktop phone with AMO ZIEL.

Scenarios

The busy condition of the SIP subscriber is displayed via a LED on the monitoring extension's DSS key LED.

- LED off: SIP subscriber is free to get a call.
- LED on: SIP subscriber is busy.

If SIP subscriber is member of an ONS group

- If the SIP subscriber is the master of the ONS group, the DSS LED shows the status of the ONS group.
- If the SIP subscriber is the slave and the slave number is monitored, the DSS LED shows the status of the slave.

SIP subscriber is called if free (LED off) when the DSS key is pressed on monitoring extensions.

Remarks

- The ringing state of the SIP subscriber is considered as busy, therefore the DSS LED does not flash and call pickup is not possible.
- Local features activated on a SIP subscriber cannot be monitored by the system. Call forwarding locally activated on the SIP subscriber will be executed when the DSS key configured with the SIP subscriber as destination is pressed.

Generation (example)

Digit: 3412, SIP: 3434

```
ADD-ZIEL:TYPE=DSS,SRCNO=3412,KYNO=12,DESTNOD=3434;
DIS-ZIEL:DSS,3412;
H500:  AMO ZIEL STARTED
```

```
DSS
 SOURCE       | DEVICE |  KEY    | DEST.         | SLKTYPE   | SLKTEXT

-------------+--------+--------+--------------+----------+-------------

3412          |   BD   | 12      | 3434          | SLKSTNO   |
AMO-ZIEL -111       DESTINATIONS FOR VARIOUS STATION FEATURES
DISPLAY COMPLETED;
```

14.2.5.10 SIP Peer Filtering

The feature **SIP Peer Filtering** is released for HG 3500 and vHG 3500 SIP.

To avoid hacker attacks (scanning) via SIP trunks, only SIP requests from "known" peers (partners) are answered, all other requests are ignored. "Known" peers are IP addresses or FQDNs from an enabled SIP Trunk Profile and/or registered SIP clients.

There are two operation modes:

- Gateway/HG configured (B channels) for SIP clients **and** SIP trunks.

  Only incoming REGISTER messages from "known" peers will be answered, all other requests from "unknown" peers will be ignored.
- Gateway/HG configured as trunking gateway only (there are only configured SIP trunk B channels)

  Only requests from "known" peers will be answered; all requests from "unknown" peers will be ignored.

  Typical use case where this feature should be activated is SIP trunk gateway connected to SIP provider via WAN/Internet without additional security tools like firewall usage.

  The feature can be activated in the **SIP Trunk Profile Parameter** menu via the checkbox **Enable SIP Peer Filtering**. After activation/deactivation of the feature the gateways be restarted.

  WBM > Configuration > Voice Gateway > SIP Trunk Profile Parameter

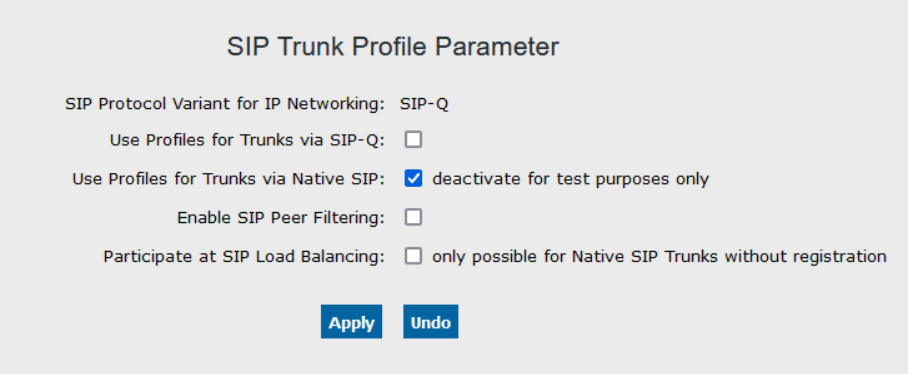


Figure 241: SIP Peer Filtering

14.2.5.11 Call Forwarding

3 kinds of call forwarding are possible:

- CFU - Call Forwarding Unconditional

ADD-ACTDA:TYPE=STN,STNO=<station number>,FEATCD=FWD,CFVAR=<call forwarding variant>,**DTYPE=CFU**,SI=VCE;

- CFNR - Call Forwarding No Reply

ADD-ACTDA:TYPE=STN,STNO=<station number>,FEATCD=FWD,CFVAR=<call forwarding variant>,**DTYPE=CFNR**,SI=VCE;

- CFB - Call Forwarding Busy

ADD-ACTDA:TYPE=STN,STNO=<station number>,FEATCD=FWD,CFVAR=<call forwarding variant>,**DTYPE=CFB**,SI=VCE;

NOTICE: For legacy SIP devices with S0PP, SI=SPCH must be used.

14.2.5.12 Display of the SIP Subscribers

Registered and unregistered SIP subscribers can be displayed via the **HG 35xx Web Based Management** in the OpenScape 4000 Assistant.

In the OpenScape 4000 Assistant:

1) Expert mode -> Gateway Dashboard -> HG 35xx Web Based Management

In the HG35xx Web Based Management:

Configuration -> Voice Gateway

Configuration -> Voice Gateway - Clients - UFIP SIP

Registered clients are written in bold.

14.2.5.13 Busy override, emergency intrusion and emergency disconnect for SIP (UFIP) subscribers

Busy override, emergency intrusion and emergency disconnect are implemented for SIP (UFIP) subscriber in version V8R1 with specific SIP interface restrictions/limitations:

Busy override, emergency intrusion and emergency disconnect against SIP subscriber:

1) The Display at SIP level will not be updated

- At CP level the SIP subscriber is considered busy if at least one transaction is busy when override, emergency intrusion or emergency

disconnect are invoked (activation of “second call” feature at device level has to be taken into account).

Busy override, emergency intrusion and emergency disconnect invoked from a SIP subscriber:

- Currently, only WL3/WL4 (UFIP) devices support the feature.
- The system supports the feature for any kind of SIP (UFIP) device but at device level the interface must be implemented to support specific menu options for busy override, emergency intrusion and emergency disconnect
- The features can be invoked from any SIP (UFIP) by dialing specific WABE codes (KNOVR, EOVR, RELEASE) followed by the station number.

Feature activation via AMO commands:

CHANGE-FEASU:TYPE=A,CM=OVR&EMOVR&EMRLS;

CHANGE-ZAND:TYPE=ALLDATA,OVRMST=YES;

SDAT attributes for intruding station:

CHANGE-SDAT:STNO=13203,TYPE=ATTRIBUT,AATTR=EOVR&KNOVR;

ADD-WABE:*56,,,KNOVR,N,,,,,,,;

ADD-WABE:*57,,,EOVR,N,,,,,,,;

ADD-WABE:*58,,,RELEASE,N,,,,,,,;

For more details please consult the feature description documentation.

In case of WL3/WL4 (UFIP) device, the feature activation and the activation codes must also be configured in phone WBM.

14.2.5.14 UFIP in Pickup Group

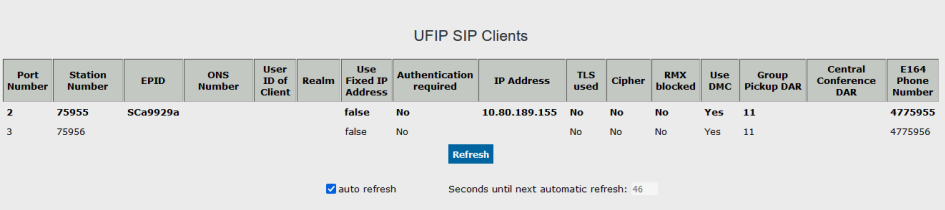
Starting with V8, the chronologically first and only the first WABE PU code configured in the system will be marked and used also for UFIP devices.

```
DISPLAY-WABE:TYPE=GEN,DAR=PU;
H500:  AMO WABE  STARTED
  ------------------------------------------------------------------------------
  | DIGIT INTERPRETATION                    VALID FOR ALL DIAL PLANS           |
  ------------------------------------------------------------------------------
  |                 |    CALL PROGRESS STATE     |NODE/DIGIT| RESERVED/CONVERT |
  |      CODE       |            1 11111 11112 22| ANALYSIS | DNI/ADD-INFO/UFIP|
  |                 |0 12345 67890 12345 67890 12|  RESULT  | *=OWN NODE       |
  ------------------------------------------------------------------------------
  | *19             |. ....* ..... ..... ..... ..| PU       |                  |
  | *70             |. ....* ..... ..... ..... ..| PU       |   UFIP           |
  | *90             |. ....* ..... ..... ..... ..| PU       |                  |
  ------------------------------------------------------------------------------

AMO-WABE -111       DIALLING PLANS, FEATURE ACCESS CODES
DISPLAY COMPLETED;
  <
```

Once the UFIP PU code is configured, it can be changed only via CHANGE-WABE command. Deleting it is not allowed.

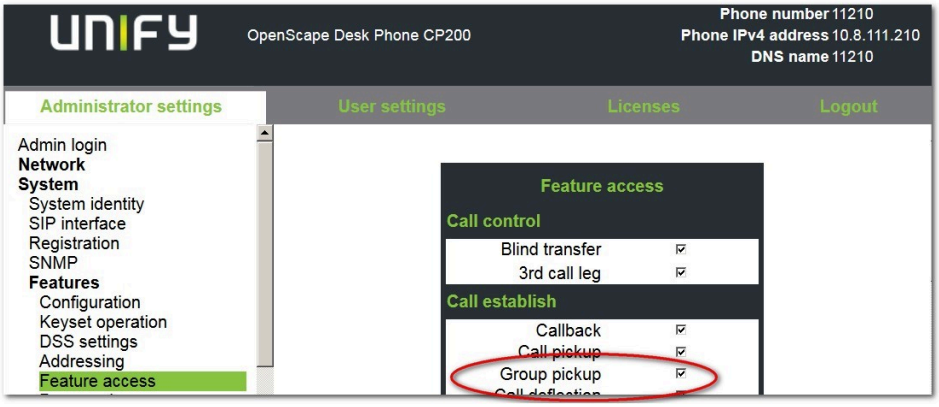
UFIP gateways must be restarted to load the new UFIP PU code, which can be checked in WBM: Configuration -> Voice Gateway -> Clients -> UFIP SIP: “Group Pickup DAR” column



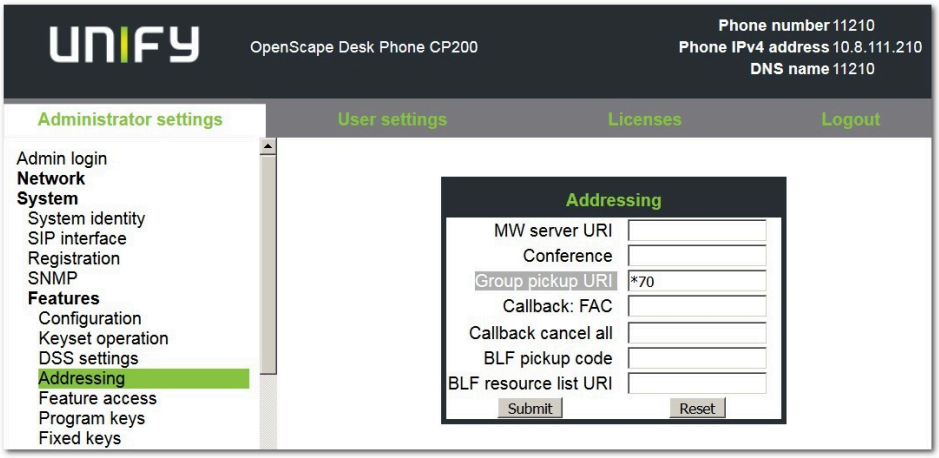
Restrictions: only one PU code at a time can be used for UFIP clients. Since REGENERATE-WABE will return the codes in numerical order, after new generation of the system (including upgrades via Auto-GENDB) manual adaption maybe needed to change the order of configured codes.

Following the system AUN configuration, for each UFIP device:

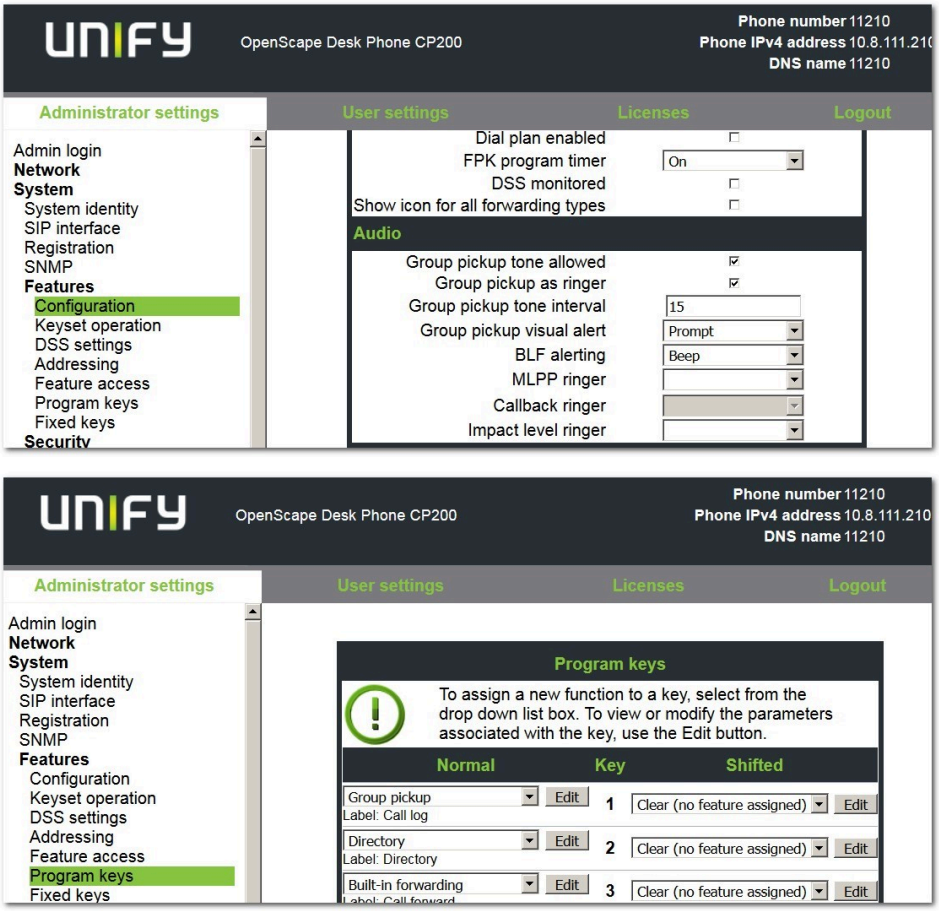
- “Group pickup” feature must be enabled:



- WABE UFIP PU code must be configured:



- Optional device pickup call behavior customization and key configuration:



For details, please check phone documentation.

14.2.5.15 Relevant AMOs

AMO	Parameter	Sprache/ Language	Beschreibung/ Description
ACTDA	UART	d	CFB: Anrufumleitung bei besetzt CFNR: Anrufumleitung bei nicht melden CFU: ständige Anrufumleitung
	DTYPE	e	CFB: call forwarding busy CFNR: call forwarding no reply CFU: Call forwarding unconditional
BCSU	ALARMNR	d	Alarm Nummer
	ALARMNO	e	Alarm number
	ART=HWYBDL	d	Highway-Bündel
	TYPE=HWYBDL	e	Highway bundle

AMO	Parameter	Sprache/ Language	Beschreibung/ Description
	BKANSIP	d	Anzahl der B-Kanaele fuer die SIP-Subscriber Funktion
	BCHLSIP	e	Number of b channels for sip subscriber function
	FCTID	d	Function Id (wird immer auf 1 gesetzt)
	FCTID	e	Function id (is always set to 1)
	FCTBLK	d	Funktionsblock-Index (einen beliebigen freien Funktionsblock zwischen 1-20 wählen)
	FCTBLK	e	Function block index
	LWVAR	d	Index auf Loadware Block der T1 Baugruppe
		e	Loadware variant
	SACHNR	d	Baugruppensachnummer (2. und 3. Block) Q2316-X, Q2316-X10, Q2324-X500, Q2324-X510
	PARTNO	e	Part numver (2nd and 3rd bloc) Q2316-X, Q2316-X10, Q2324-X500, Q2324-X510
	TYP=IPGW	d	IP Gateway (Common Gateway Baugruppe)
	MTYPE=IPGW	e	IP Gateway (Common gateway board)
BFDAT	ANZSATZ	d	Anzahl der funktionsbezogenen Saetze. Mögliche Werte: 1-240
	LINECNT	e	Defines the number of lines related to the selected function.
	BGBKAN	d	Block fuer Baugruppe mit 60 und/oder 120 B-Kanaelen
	BRDBCHL	e	dedicates the block for boards with 60 and/or 120 b-channels
	CONFIG=WEITER	d	Weitere Block-Konfiguration ermöglichen
	CONFIG=CONT	e	Continue block configuration
	CONFIG=OK	d	Block-Konfiguration abschließen

AMO	Parameter	Sprache/ Language	Beschreibung/ Description
	CONFIG=OK	e	Finish block configuration
	FCTBLK	d	Dieser Index beschreibt den Funktionsblock welcher auf dem Common Gateway konfiguriert werden soll. Anhand des Funktionsblocks wird die Konfiguration der benötigten pyhsikalischen Lines (Sätze der Baugruppe) festgelegt.
	FCTBLK	e	This index describes the function block which should be configured on the common gateway board. With that index the amount of needed physical lines (board circuits) is calculated.
	FUNCTION	d	Dieser Parameter legt das Konfigurationsprofile des Common Gateways fest. Dabei muss die eventuell benötigte HG 3570 Funktion als erste angeführt werden. Falls ein bestimmter Line-Bereich für die Funktionen HG 3530 oder HG 3550 vorreserviert werden soll, muss die entsprechende Funktion am Ende stehen und mit dem Wert HG35xxR abgeschlossen sein. Die Funktion kann nur als Einzel-Funktion konfiguriert werden. FUNCTION=SIP: SIP Subscriber Funktion
	FUNCTION	e	This parameter defines the configuration profile of the common gateway board. If HG3570 functionality is used, it must be configured at first position. If a prereservation of a certain line range of functions HG3530 or HG3550 is desired, this function must be at the end of the profile just suffixed by the according HG35xxR value. The function can only be configured as single function. FUNCTION=SIP:SIP subscriber function

AMO	Parameter	Sprache/ Language	Beschreibung/ Description
CGWB	DEFRT		IP-Adresse des Default Routers innerhalb des LAN-Segmentes. Der Default Router übernimmt die Weiterleitung der Pakete, die eine Zieladresse außerhalb des eigenen LAN-Segmentes haben. 0.0.0.0 bedeutet, daß kein Default Router konfiguriert ist.
	DEFRT	e	IP address of the default router within the LAN segment. The default router takes care of routing forward all packets with a destination address with a network part different from the own LAN segment. 0.0.0.0 means that no default router is configured.
	IPADR	d	IP Adresse der Common Gateway Baugruppe (Source Adresse)
	IPADR	e	IP address of common gateway board (source address)
	MTYP=INITCGWB	d	Zurücksetzen der Konfigurationsdaten der Common Gateway Baugruppe auf die Standardwerte
	MTYPE=INITCGWB	e	Reset configuration data of common gateway board to default values
	NETMASK	d	IP-Netzmaske des LAN-Segmentes. Die IP-Netzmaske bestimmt die Grenze zwischen Netz- und Host-Teil in der IP-Adresse. Alle IP-Adressen am LAN-Segment müssen bezüglich des Netzanteils der IP-Adresse gleich und bezüglich des Host-Teils unterschiedlich sein (auch der Default Router muss dieser Bedingung entsprechen).
	NETMASK	e	IP net mask of LAN segment The IP net mask determines the network and the host partition of an IP address. All IP addresses of a LAN segment must contain the identical network address part but different host address parts (also the Default Router must fulfill this requirement).

AMO	Parameter	Sprache/ Language	Beschreibung/ Description
	SMODE=NORMAL	d	Mode oder Normal Mode Eine Baugruppe im Normal Mode hat gültige Baugruppendaten und normalerweise auch OPTIIPs konfiguriert. Eine Baugruppe im Ready Mode hat keine gültigen Baugruppendaten, auf diese Baugruppe können OPTIIPs umgeschaltet werden, falls eine andere Baugruppe aus demselben Baugruppen-Pool (AMO BPOOL) defekt wurde. Eine Baugruppe im Defekt Mode hat ebenfalls keine gültigen Baugruppendaten, diese Baugruppe hat aufgrund eines Defekts seine OPTIIPs und seine Baugruppendaten abgegeben.
	SMODE=NORMAL	e	Mode or Normal Mode A board in Normal Mode has valid board data and normally also OPTIIPs assigned to it. A board in Ready Mode has no valid board data, to this board OPTIIPs can be switched over if another board of the same board reconfiguration pool (AMO BPOOL) becomes defective. A board in Defect Mode has also no valid board data, this board has lost its OPTIIPs and its board data to another board because it's gone defective.
SBCSU	ART=FPP	d	Hauptrufnummer des S0-/S2-Punkt zu Punkt Anschlusses
	OPT=FPP	e	Functional point-to-point connection
	ANSCHL=SIP	d	Anschlussart=SIP
	CONN=SIP	e	Kind of connection=SIP
	GERKON=S0PP	d	S0-Punkt zu Punkt Anschluss
	DVCFIG=S0PP	e	S0-point-to-point
	PROT=SBDSS1	d	Protokollvariante DSS1
	PROT=SBDSS1	e	Protocol variant DSS1
	OPT=10	d	Optiontabellenindex 10
	OPTIDX=10	e	Option table index 10

AMO	Parameter	Sprache/ Language	Beschreibung/ Description
	IPADR	d	IP-Adresse
	IPADDR	e	IP address
	PASSWD	d	Passwort
	PASSWD	e	Password
	KENNUNG	d	Benutzerkennung
	USERID	e	User ID
	SECBER	d	Security-Bereich (Art Domäne)
	SECZONE	e	Security zone (kind of a Domain)
	FESTEIP	d	Feste IP-Adresse
	FIXEDIP	e	Fixed IP address
	AUTHERF	d	Authentifizierung erforderlich
	AUTHREQ	e	Authentification required
	SMGTLN	d	SMG Teilnehmer; Für Survivability-Lösung mit der H8k;
	SMGSUB	e	SMG subscriber For survivability solution with H8k;
SDAT	EMERK	d	Teinehmermerkmal einfügen
	AATTR	e	Add attribute
	AMERK	d	Teinehmermerkmal ausfügen
	DATTR	e	Delete attribute

14.3 SIP Trunking

14.3.1 SIP-Q Trunking

SIP-Q: CorNet-NQ tunneling over SIP. SIP-Q is the preferred protocol for Interworking to other Unify systems.

14.3.1.1 Features

IMPORTANT: All CorNet-NQ- features can only be supported for networking with SIP-Q. From HiPath 4000 V4 the preferred

method of networking HiPath 4000 and OpenScape 4000 systems is SIPQ. SIPQ v2 is supported starting with HiPath 4000 V4.

14.3.1.1.1 Connectivity to OpenScape Voice

For connectivity with OpenScape Voice only the protocol SIP-Q V2 is supported. SIP-Q V2 supports TLS (Transport Layer Security for signaling) and SRTP (secure RTP for the payload).

SIP-Q is also used for the connectivity with OpenExchange providing a very powerful and scalable IP LCR.

For SIP-Q connectivity towards OpenScape Voice the block-dial mode in OpenScape 4000 LCR and for the subscribers must be configured. Two block-dial modes are supported:

- like a SIP Phone in an OpenScape Voice solution.
- like the existing OpenScape 4000 bock-dial mode (as known up to OpenScape 4000 V4).

IMPORTANT: For the OpenStage 60 and 80 HFA the block dial mode has been released with OpenStage HFA **V2**.

Features with SIP-Q V2 between HiPath 4000/OpenScape 4000 and OpenScape Voice

- Call identification
  - CLIP/CLIR
  - COLP/COLR
  - CNIP/CNIR
  - CNOP/CNOR
- Call transfer
- Call hold / retrieve / toggle
- Call Forwarding
  - CFU (call forwarding unconditional)
  - CFB (call forwarding on busy)
  - CFNR (call forwarding no reply)
- Callback on busy subscriber / no reply
- Message Waiting Indication (MWI)
- Release links (also called route optimization or path replacement)
- Transmission of "CorNet-NQ" messages
- IPv6 (see "OpenScape 4000 SoftGate" > Chapter 12, “IPv6”)
- Signaling (TLS) and payload encryption (SRTP) (see "Signaling and Payload Encryption (SPE)")
- Call data recording
- T.38 fax connections (e.g. for SIP-Q trunking in common gateway HG 3500 towards OpenScape Voice V4/V5)

14.3.1.1.2 Codecs per Destination Gateway for SIP-Q Trunking

Feature Description

OpenScape 4000 can be configured such that a codec is chosen depending on the destination gateway. This means that the voice codec settings

are dependent on the IP address of the destination gateway. Any other configuration options (e.g.: fax settings) are not considered for this feature.

In order to specify the direction of the call, the following options can be used:

- Configure single IP addresses
- Configure a range of IP addresses
- Configure a subnet mask

Service Information

- This feature is supported for common gateway HG 3500 and vHG 35000 OpenScape 4000 SoftGate.
- This feature is only supported for OpenScape 4000 internal SIP-Q networking that uses fixed IP addresses.
- If FQDNs (fully qualified domain names) are used (e.g.: towards OpenScape Voice) then this feature cannot be used.
- The specific voice codec settings should be evaluated for incoming and outgoing calls (from a gateway perspective). The destination specific codecs can be changed dynamically without any reboot (both for SIP-Q in common gateway and OpenScape 4000 SoftGate).

14.3.1.1.3 SIP Peer Filtering

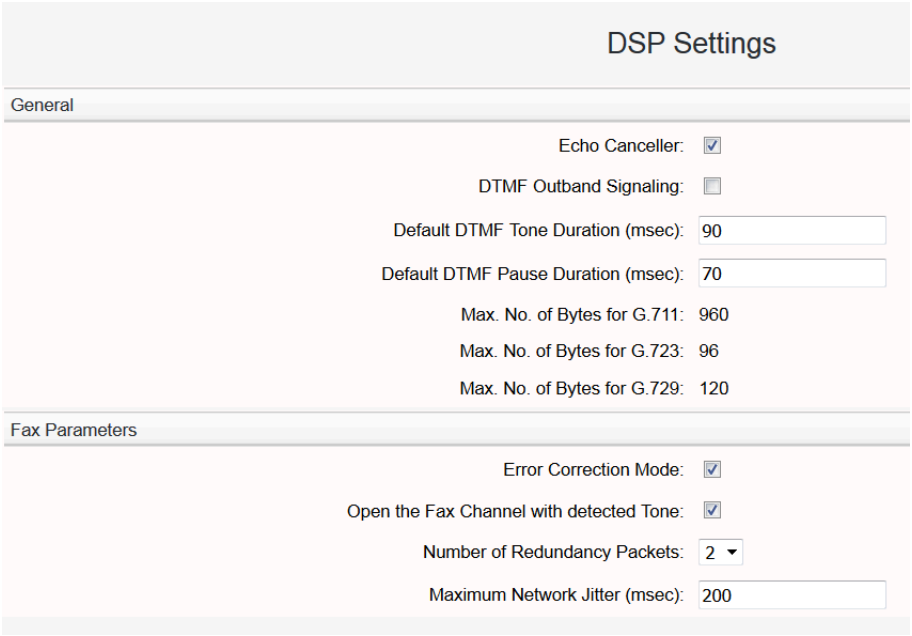
SIP Peer Filtering is released with HG 3500 and vHG 3500 SIP.

For more information please refer to Section 2.5.9, “SIP Peer Filtering”.

14.3.1.2 Restrictions

- Outband signaling is not supported.
- The function must be deactivated via WBM:

  WBM > Configuration > Voice Gateway > Payload > HW Modules > DSP Settings



- Trunking between HiPath 3000 and OpenScape 4000

- SIP registration of the HG 1500 board at the Large Enterprise Gatekeeper (LEGK) is not supported.
- SIP-Q V2 connectivity between HiPath 4000/OpenScape 4000 and OpenScape Voice
- Call detail recording is not supported.

14.3.1.3 Configuration

see Chapter 6, “Configuration of SIP-Q-Trunking / Native SIP Trunking”.

14.3.2 Native SIP Trunking

Native SIP trunks can be used to connect SIP service provider (see Section 3.2.3.1, “SIP Service Provider”) or 3rd party SIP products (e.g. OpenScape Xpressions, Section 3.2.3.3, “Applications”).

3rd Party Native SIP connections can be connected to OpenScape 4000 Gateway using the standard delivered profiles of the Gateway without any Project Specific Release (PSR).

The list of Supported RFCs can be found in the SIP Connectivity chapter of this document. Should the OpenScape 4000 Gateway not conform to any of the published RFCs, then any found issue can be addressed via a Service Ticket.

It is not supported to change the fixed parameters of existing profiles. The recommended profile for 3rd Party SIP applications is “NatTrkEnterprise”, which includes support for SIP Refer. There are dedicated profiles for the 3rd party products MS Teams and Cisco UCM.

The process to request new board profiles, which is mandatory for SIP Service Provider (SSP), can be found here: https://wiki.unify.com/wiki/Collaboration_with_VoIP_Providers_on_Enterprise_Platforms#OpenScape_4000

14.3.2.1 Features

IMPORTANT: The availability of the following functionalities depends on the SIP partner and must be tested individually!

- Basic Call in accordance with RFC3261 SIP (for supported RFCs please refer to Section 1.2, “Supported RFCs (Request for Comments) for SIP Interfaces”)
- CLIP/CLIR
- COLP/COLR
- Sending and receiving E.164 explicit international telephone numbers with a leading “+” (e.g. +498972237729) or implicit telephone numbers with prefixes (e.g. 00498972237729)
- Name display (e.g. for OpenScape Xpressions V6 connectivity)
- Call hold / retrieve / toggle
- Call transfer (attended call transfer / semi-attended call transfer / blind call transfer)
- Call forwarding ("forward switching" method)

- Diversion header
- Early media (183 Call Progress with SDP)

IMPORTANT: Call forwarding via “Call rerouting method” is not supported. Instead diversion header is supported (sending of call forwarding information; required for call forwarding scenarios to SIP service provider).

- Conferencing (3 party conference)
- Message Waiting Indication MWI
- This feature can be used for SIP connectivity towards service providers offering hosted Unified Messaging services.
- DNS SRV - Locating and addressing SIP servers/proxies using fully qualified domain names
- SIP proxy failover and recovery
- Registration to SIP service provider (registration **to** OpenScape 4000 **from** other vendors is not supported).
- Session border controller connectivity
- SIP session timer RFC4028 (more information can be found in Section 2.4, “Restrictions”)
- Digest authentication
- L2 and L3 QoS for signaling and payload
- T.38 fax connections (towards SIP service providers, e.g. T-Systems)
- DTMF signaling (Inband and RFC2833 compliant)
- Voice codecs G.729 and G.711
- Silence suppression
- Inband / outband proxy configuration
- SIP trunking profiles (enable easy SIP service provider integrations and administration)
- UDP/TCP transport
- IPv6 (see "OpenScape 4000 SoftGate" > Chapter 12, “IPv6”)
- Signaling (TLS) and payload encryption (SRTP) (see "Signaling and Payload Encryption (SPE)")
- Location-ID in the SIP-Header - GeoPriv PIDF-LO

NOTICE: Emergency call behavior (including PANI and GeoPriv) corresponding in each SIP Profile to certified SIP partner requirements.

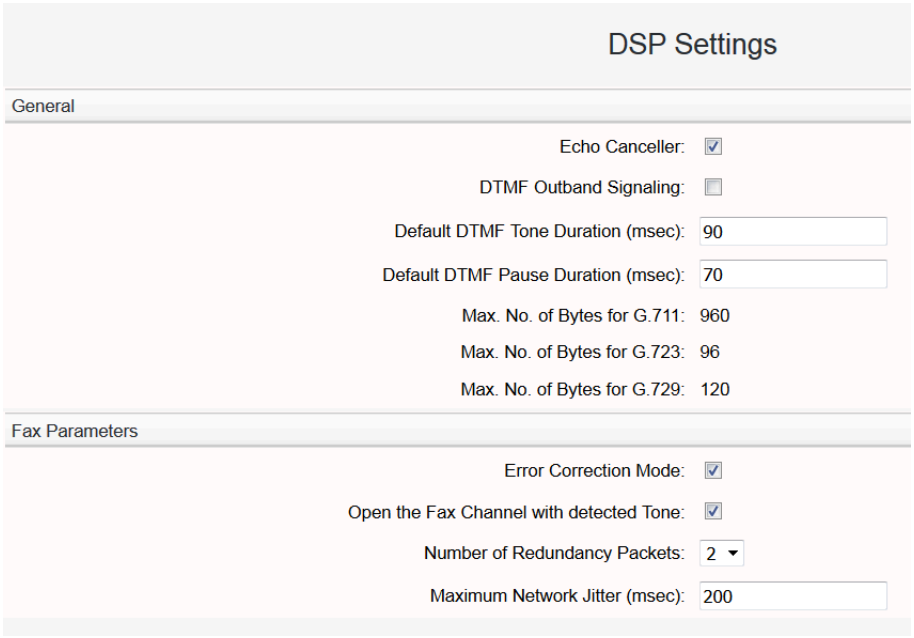
OpenScape 4000 and OpenScapeVoice systems are normally networked via SIP-Q (see Section 3.1, “SIP-Q Trunking”).

14.3.2.2 Restrictions

- Common Gateway HG 3500: SRTP is not supported for native SIP trunking.
- Outband signaling is not supported.

- The function must be deactivated via WBM:

  WBM > Configuration > Voice Gateway > Payload > HW Modules



- Trunking between HiPath 3000 and OpenScape 4000
- SIP registration of the HG 3500 board at the Large Enterprise Gatekeeper (LEGK) is not supported.

14.3.2.3 Use Cases

14.3.2.3.1 SIP Service Provider

Native SIP trunking is mainly used for connections to SIP service providers.

> **IMPORTANT:** For a connection to a non-released SIP service provider a change request has to be written!

The SIP providers and SIP trunking partners released in the OpenScape 4000 are listed in the OpenScape 4000 Release Notes. They will be updated with every new minor or fix release.

For more information please refer to Chapter 5, “Configuration of SIP Service Provider / SIP Carrier”.

14.3.2.3.2 Remote Agent Server Connectivity

Remote agent server enables remote connectivity of agents via mobile phones or home phones or any phone with DTMF. This connectivity is established via a native SIP trunk interface.

For more information please refer to the Remote Agent Server Solution documentation.

14.3.2.3.3 Applications

Native SIP trunking is also used however for connectivity with other proprietary applications, such as OpenScape Xpressions.

14.3.2.4 Configuration

14.3.2.4.1 General Configuration

see Chapter 6, “Configuration of SIP-Q-Trunking / Native SIP Trunking” or Chapter 5, “Configuration of SIP Service Provider / SIP Carrier”.

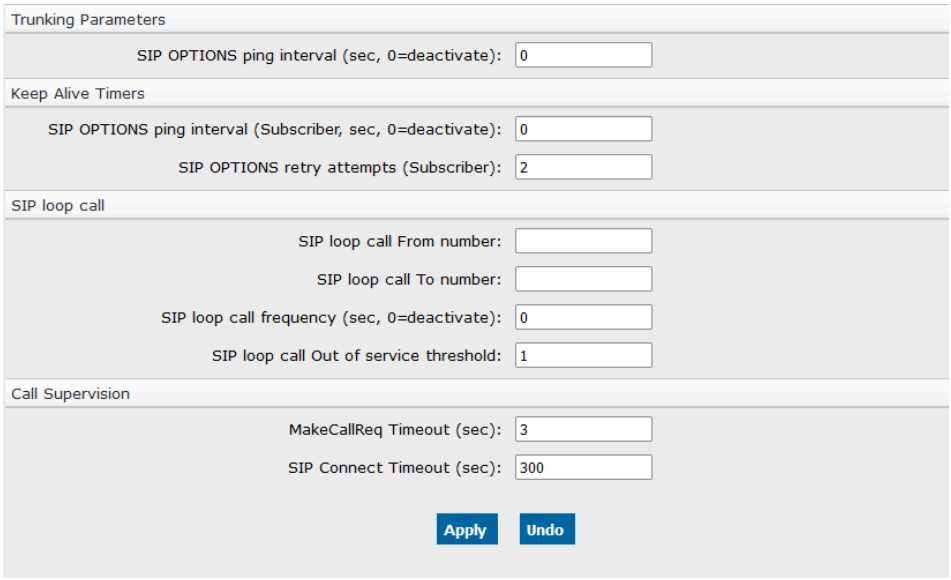
14.3.2.4.1.1 Monitoring availability of SIP Trunks

There a two possibilities to monitor SIP trunk connectivity, either SIP OPTION pings or SIP loop calls. SIP OPTIONs give no guaranty about the reachability of the provider, because they are only exchanged between the PBX and the Carrier Ethernet Router (CER). Also, the CER router acts as an SBC, but it doesn’t pass the SIP OPTIONs from one side to the other side. The only way to monitor a native SIP trunk (similar to the predecessor PRA trunks) is to use loop calls generated by the PBX and routed through the SSP back to the PBX.

The configuration of a native SIP trunk is the following: **Configuration -> Voice Gateway -> SIP Parameters -> Trunking Parameters**

- SIP loop call frequency (sec, 0=deactivate): 0
- SIP loop call To number: empty string by default
- SIP loop call From number: empty string by default
- SIP loop call Out of service threshold: default=1

Figure 242: Configuration of a native SIP trunk



HINT: Since the complete configuration for this feature is in the HG, it is recommended to ensure the DDI number is reserved also in the system to avoid it being used for anything else e.g. create a SCSU FLOAT with a PERSI entry of "SIP LOOP CALL" to ensure the number is reserved.

A HISTA L1 Error is generated, if the Loop-Call fails:

```
F5749 E8 N8265 NO ACT BPA BOARD LW REQUEST 20-04-07 11:42:32
 ALARM CLASS:CENTRAL:002
 ** :LTG1 :LTU30:009: 0 : 0 Q2330-X vHG3500 BST:01 PLS:-07
 FORMAT:43
 REASON:00H ONLY SIGNALING
 SIP loop call failed
```

```
F5412 E8 N8266 OUT SERV BPA CIRCUIT L1 ERROR 20-04-07 11:42:32
 ALARM CLASS:SWU-PER:001
 ** :LTG1 :LTU30:009: 0 : 0 Q2330-X vHG3500 BST:01 PLS:-07
 REASON:03H LOST FRAME (RED) (LOCAL ALARM)
 FORMAT:36 DEVICE NAME: HG3550IP

F5749 E8 N8267 NO ACT BPA BOARD LW REQUEST 20-04-07 11:47:03
 ALARM CLASS:CENTRAL:002
 ** :LTG1 :LTU30:009: 0 : 0 Q2330-X vHG3500 BST:01 PLS:-07
 FORMAT:43
 REASON:00H ONLY SIGNALING
 SIP loop call resumed

F5418 E8 N8268 IN SERV BPA CIRCUIT LX ACTIVE 20-04-07 11:47:03
 ALARM CLASS:SWU-PER:001
 ** :LTG1 :LTU30:009: 0 : 0 Q2330-X vHG3500 BST:01 PLS:-07
 REASON:07H LAYER 1 ACTIVE (GREEN)
 FORMAT:36 DEVICE NAME: HG3550IP

F5418 E8 N8269 IN SERV BPA CIRCUIT LX ACTIVE 20-04-07 11:47:03
 ALARM CLASS:SWU-PER:001
 ** :LTG1 :LTU30:009: 0 : 0 Q2330-X vHG3500 BST:01 PLS:-07
 REASON:09H LAYER 3 ACTIVE
```

There is no de-registration after a L1 error - registration will be handled via standard timeouts.

SNMP-traps will be generated if an outage is detected.
MSG_SIP_TRUNK_ERROR if the monitoring fails and **MSG_SIP_TRUNK_OK** if trunk connectivity is possible again.

14.3.2.4.2 Codec Configuration

OpenScape Xpressions supports the following codecs:

- G711-A,
- G711-µ
- G729AB.

Codec configuration is performed via CHANGE-CGWB or via WBM:

```
CHANGE-
CGWB:MTYPE=CGW,LTU=<LTU>,SLOT=<SLOT>,TYPE=ASC,PRIO=PRIO1,CODEC=<CODEC>,RTP=<RTP>;
```

14.3.3 SIP Trunk Profiles

SIP trunk profiles are required for native SIP trunking connections and can be configured in WBM.

It is also possible to configure SIP-Q trunking connections (e.g. to OpenScape Voice) via the WBM with SIP trunk profiles.

Information about available SIP trunk profiles you can find in Section 3.3.2, “Default Profiles”.

14.3.3.1 General Information

- Secure
- If Proxy and/or Registrar, Inbound proxy and/or Outbound proxy are configured via the WBM, each incoming call is checked if the partner address is configured. If not, the call is rejected (with 403 Forbidden).

  Hint: when not using profiles for native SIP Trunk there is no checking against the partner IP making the gateway vulnerable to SIP calls being spoofed. It must be then ensured the gateway is protected in other ways e.g. using VLAN separation from client network etc.
- The right profile for the right partner
- Trunk profiles are already tailored to the specific needs of a SIP trunk partner, e.g. if in an outgoing FROM header account or call number should be sent.

  Generic Profiles are available where a partner is not certified.
- DNS SRV support
- DNS SRV propagates via DNS which IP-based services (e.g. SIP) in a domain (e.g. SIP provider domain) are provided. More than one partner IP address can be configured using DNS/ SRV

  DNS SRV timeout is influenced by two factors:

  Transaction timeout configured in:

  – RFC 3261 Timer Values
  – WBM-Voice Gateway-SIP Parameters-RFC 3261 Timer Values-Transaction timeout

  Blocking timeout

  – DNS-SRV Records / SIP Flooding Defense
  – WBM-Voice Gateway-SIP Parameters-Blocking time for unreachable destination/flood defense

  For example, if DNS SRV contains two partners IP addresses, IP1 and IP2, when there is no answer at an Invite to IP1, for UDP only the GW retransmits the request, until timeout. First after 500ms, then doubles the interval after each retransmission. Then, after transaction timeout, IP2 is contacted, for current and next transactions, for the period of "blocking timeout" and IP1 is banned.

  Notes:
- Only one profile can be activated.
- Trunk profiles “Use Profiles for Trunks via Native SIP” may only be deactivated for test purposes.
- The outbound proxy must be configured if a Session Border Controller (SBC) is used for LAN/WAN Nat-Traversal.

14.3.3.2 Default Profiles

Besides specific profiles for SIP trunk partners there are standard SIP trunk profiles for native SIP and SIP-Q:

For example:

- Native SIP Trunking
  - Profiles for SIP Service Provider
  - OpenScapeUC
  - NATTrkEnterprise (recommended Profile for 3rd Party SIP Applications using REFER)
  - NatTrkWithoutRegistration

    Use this profile for an external native SIP trunk partner without registration.
  - NatTrkWithRegistration

    Use this profile for an external native SIP trunk partner with registration.
- SIP-Q Trunking
  - SIPQTrkWithoutRegistration

    Use this profile for an internal SIP-Q trunk partner without registration.
  - SIPQTrkWithRegistration

    Use this profile for an internal SIP-Q trunk partner with registration

  The profiles for SIP specific provider have been tested and are (see also ReleaseNote) released. The list profiles may be extended with minor releases / hotfixes.

14.3.3.3 Activating the SIP Trunk Profiles

Before activating a profile it must be configured.

14.3.3.3.1 Native SIP Trunk Profiles

1) SIP protocol variant for IP networking must be set to native SIP in AMO CGWB (parameter **TRPRSIP**).
2) The use of SIP trunk profiles for native SIP trunking must be activated (default value) in the WBM.
3) Call up:

   WBM > Configuration > Voice Gateway > SIP Trunk Profile Parameter > "Use Profiles for Trunks via Native SIP"



Figure 243: Activating SIP trunk profiles

If the usage of profiles is enabled the menu **SIP Trunk Profiles** is visible in the WBM under voice gateway (see Section 3.3.4, “"SIP Trunk Profiles" menu”).

14.3.3.3.2 SIP-Q Trunk Profiles

1) SIP protocol variant for IP networking must be set to SIP-Q in AMO CGWB (parameter **TRPRSIPQ**).
2) By default, the SIP trunk profiles for SIP-Q are deactivated in the WBM. The use of SIP-Q trunk profiles must be activated in the WBM:
3) **WBM > Configuration > Voice Gateway > SIP Trunk Profile Parameter >** Activate checkbox **"Use Profiles for Trunks via SIP-Q"**

   If the usage of profiles is enabled the menu **SIP Trunk Profiles** is visible in the WBM under voice gateway (see Section 3.3.4, “"SIP Trunk Profiles" menu”).

14.3.3.4 "SIP Trunk Profiles" menu

IMPORTANT: the usage of profiles must be activated to see the **SIP Trunk Profile Parameter** menu, (see Section 3.3.3, “Activating the SIP Trunk Profiles”).

Several SIP trunk profiles are available (see Section 3.3.2, “Default Profiles”)

1) **WBM > Configuration > Voice Gateway > SIP Trunk Profiles**

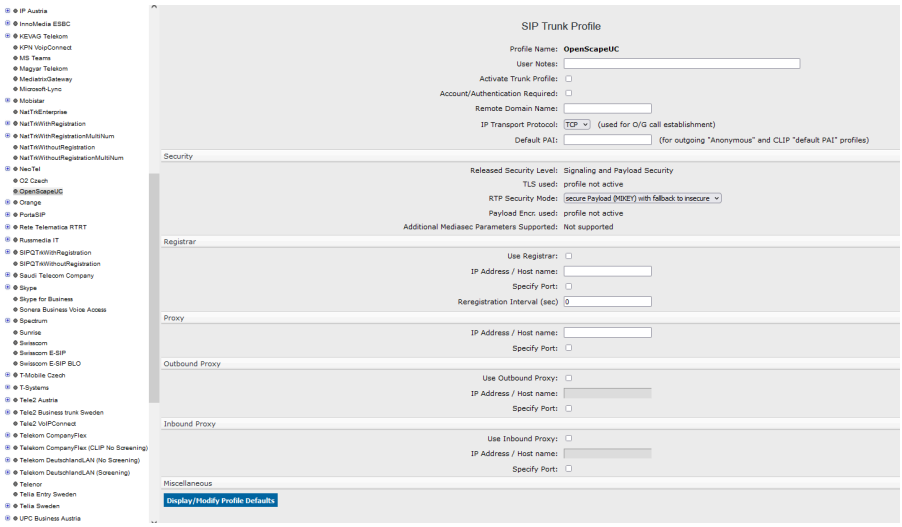


Figure 244: Example of a standard profile:

14.3.3.4.1 Change

The following SIP trunk parameters can be configured.

- **Account/authentication required** (see Section 3.3.4.2, “Authentication”)
- **Remote Domain Name**
- **SIP Transport Protocol**
- **Registrar, IP address/host name** and/or **port**
- Proxy
- Inbound proxy
- Outbound proxy
- **Security** (see Section 3.3.4.3, “Security”)

If DNS names instead of IP addresses are configured for Registrar, Proxy, Inbound Proxy or Outbound Proxy in the SIP trunk profile, DNS SRV is used for resolution.

Expert mode parameters for SIP Trunk Profiles can be displayed and modified (only for a non-activated profile) via the "Display/Modify Profile Defaults" button.



Figure 245: Display/Modify Profile Defaults for SIP Trunk Profiles

A modified profile is displayed as shown in the figure below:

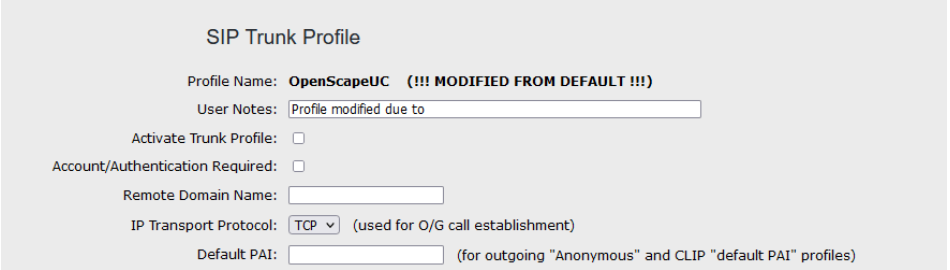


Figure 246: Display of a modified profile

"Reset Profile Defaults" button will reset only the “expert mode parameters” to default:

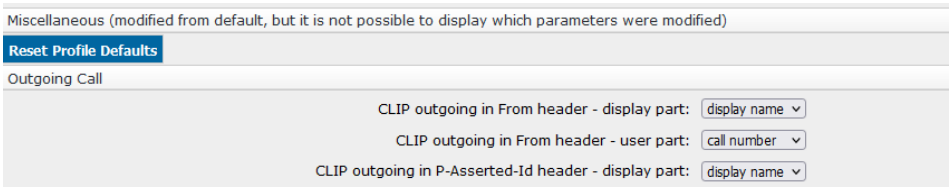


Figure 247: Reset Profile Defaults

After changing the parameters, the "Apply" button needs to be pressed.

It is recommended to use the default profile parameters and change them only after GVS consultation. Support for modified profiles is limited, since the profiles are no longer compliant to the certified standard. The right is reserved to refuse software enhancements for modified profiles.

Issues identified with current software builds, requiring a profile modification to work correctly with a certified SIP partner, should be reported to investigate and address any certificate discrepancies.

14.3.3.4.2 Authentication

If the trunk partner requires "Authentication" this must be configured in the profile. The authentication data (login and password) is provided by the trunking partner.

IMPORTANT: Authentication must be configured prior to activating the SIP trunk profile.

Procedure:

1) In the SIP trunk profile menu activate the **Account/Authentication required** checkbox.
2) Click **Add Account/Authentication** from the menu and enter the data provided by the trunking partner.

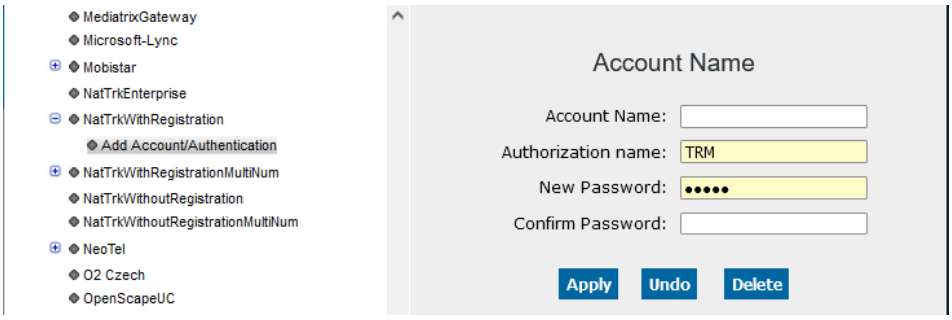


Figure 248: Add Account/Authentication (Example)

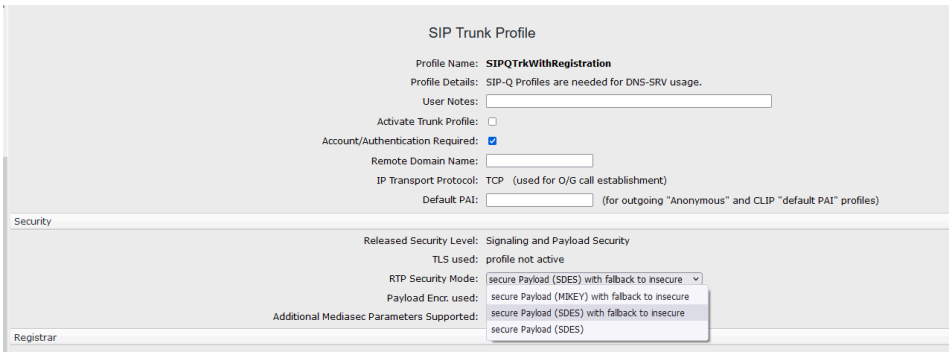
1) Activate the profile (see Section 3.3.4.4, “Activate”).

14.3.3.4.3 Security

The security parameters are different for native SIP trunk profiles and SIP-Q trunk profiles.

RTP security mode for SIP-Q trunk profiles

RTP security mode can be configured for SIP-Q trunk profiles. The common gateway board does not support SDES, thus this menu is not offered. If all conditions for SRTP are fulfilled, the payload is encrypted in accordance with the configuration.



Security configuration for SIP-Q trunk profiles

Security mode for native SIP trunking

For native SIP trunk the security mode is displayed. The security mode is defined by the AMO TDCSU and the released security level of the selected SIP trunk partner.

The common gateway board does not support payload security on the native SIP trunk. If all conditions for security, signaling and/or payload will be encrypted. The payload is encrypted with the tested and released SDES mode.

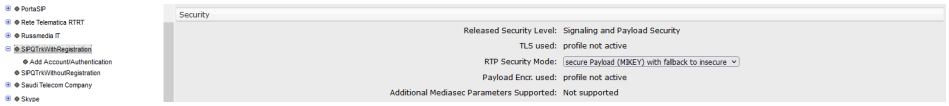


Figure 249: Security configuration for SIP-Q trunk profiles

14.3.3.4.4 Activate

Before activating a profile it must be configured.

Procedure:

1) Mark a SIP trunk profile.
2) Select **Activate** from the menu.

> **IMPORTANT:** If "Account/Authentication required" is activated in the configured profile, an account with authentication data has to be added **before** the profile is activated (see Section 3.3.4.2, “Authentication”).

14.3.3.4.5 Deactivate

Procedure:

1) Mark a SIP trunk profile.
2) Select **Deactivate** from the menu.

Once the profile is successfully deactivated, the green coloring is removed.

14.3.3.4.6 Delete

Before a SIP trunk profile can be deleted, all accounts must be deleted first.

Procedure:

1) Mark a SIP trunk profile.
2) Select (right-click) Delete from the menu.

The selected profile is deleted.

14.3.3.5 Configuration of SIP Trunks with Registration

The prerequisites for using the SIP trunk profiles must be fulfilled (see Section 3.3.3, “Activating the SIP Trunk Profiles”).

14.3.3.5.1 Native SIP Trunks

1) Change the profile

2) Use the "NatTrkWithRegistration" profile for native SIP trunk configurations with registration. Configure the account name and authentication

Configuration > Voice Gateway > SIP Trunk Profile > NatTrkWithRegistration > Modify > Activate checkbox **Add Account/ Authentication**

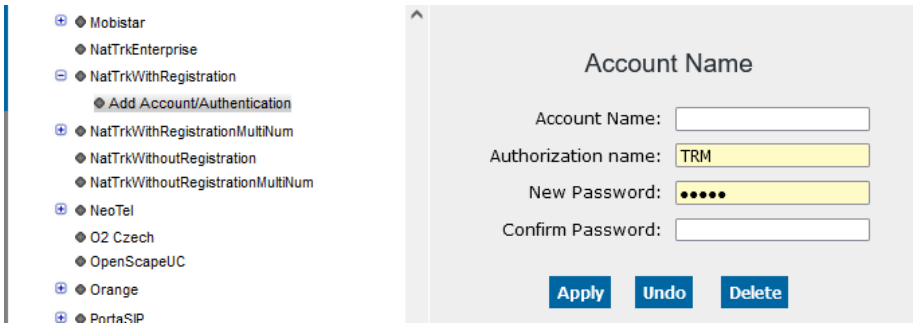


Figure 250: Account/authentication data

3) Configure the IP address/host name and domain name

4) The **IP address/host name** (e.g. DNS name = provider.com) of the SIP trunk partner is configured in the **Registrar** section and in the **Proxy** section. The remote **domain name** usually has the same value as the **IP address/ host name** (see Sections **Registrar** or **Proxy**) and is used as a host part in the URL of the SIP messages.

Configuration > Voice Gateway > SIP Trunk Profile > NatTrkWithRegistration > Modify

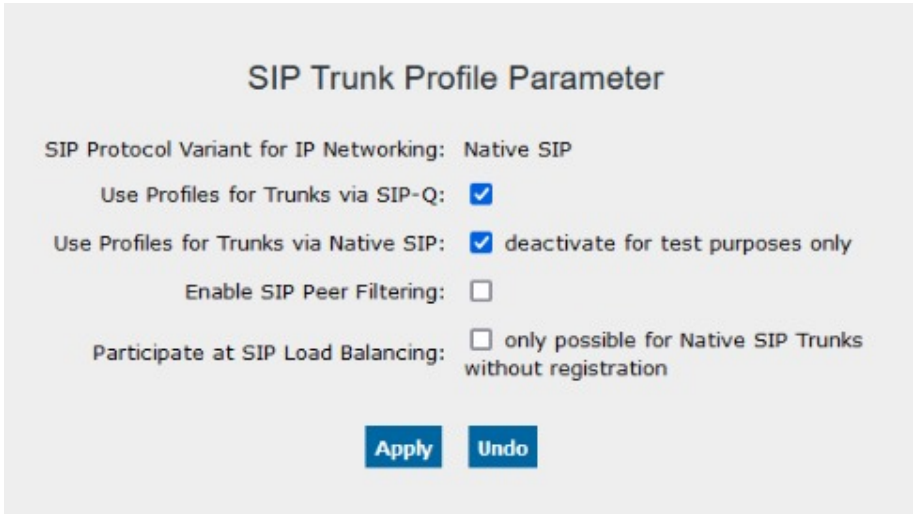


Figure 251: SIP trunk profile of a provider with registration

5) Activate the profile

6) After the profile has been configured activate it. If the profile was activated successfully, it turns green.

Configuration > Voice Gateway > SIP Trunk Profile > NatTrkWithRegistration > Activate

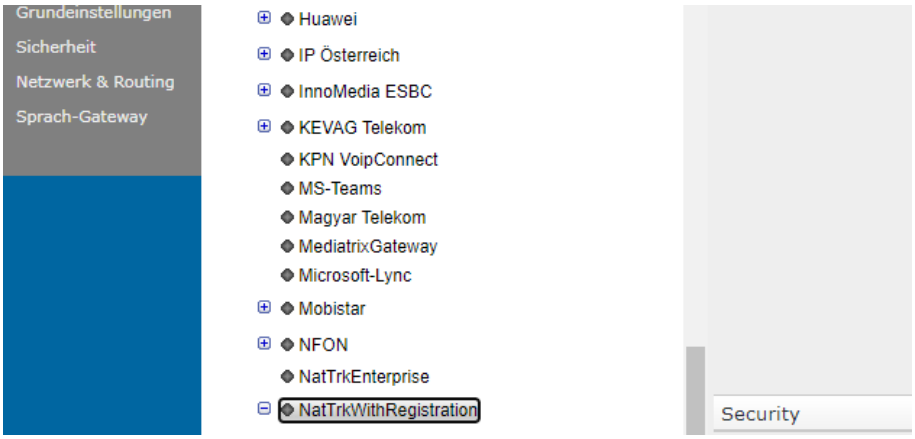


Figure 252: Activated SIP trunk profile (with registration)

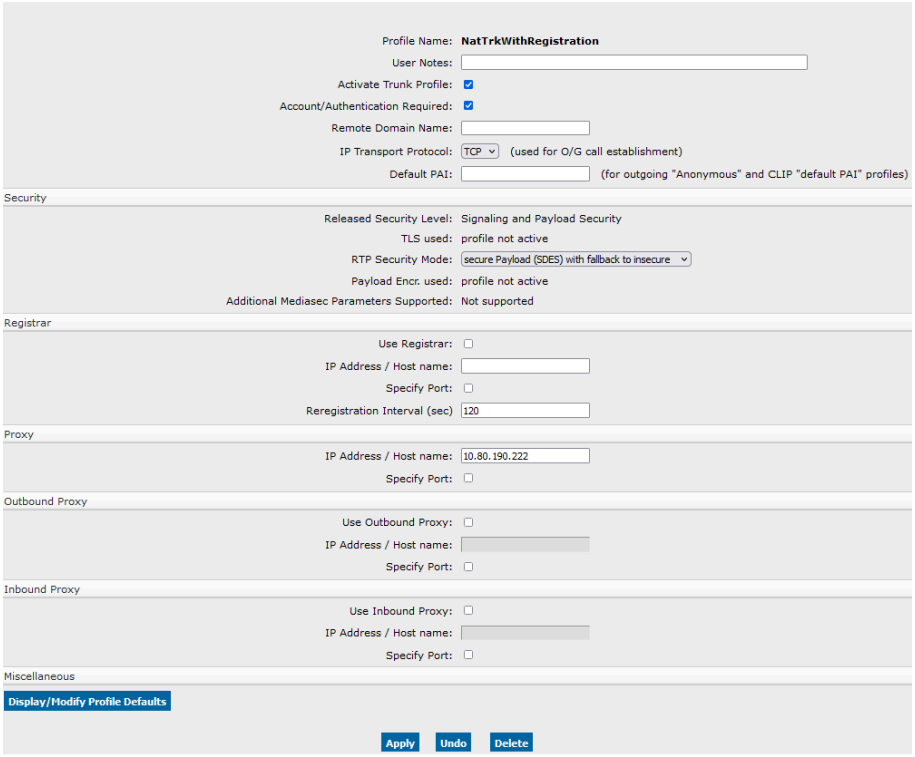


Figure 253: Activated SIP trunk profile (with registration)

14.3.3.5.2 SIP-Q Trunks

1) Change the profile
2) The "SIPQTrkWithRegistration" profile offered can be used for trunk configurations with registration. The account name and authentication data (if required) can be configured.

Configuration > Voice Gateway > SIP Trunk Profile > SIPQTrkWithRegistration > Modify > Activate checkbox **Add Account/Authentication**

3) Configure the IP address/host name and domain name
4) Configure **IP address/host name** (e.g. DNS name = provider.com) of the SIP trunk partner in the **Registrar** section and in the **Proxy** section. The **domain name** usually has the same value as the **IP address/host name** (see Sections **Registrar** or **Proxy**) and will be used as a host part in the URI of the SIP messages.

Configuration > Voice Gateway > SIP Trunk Profile > SIPQTrkWithRegistration > Modify

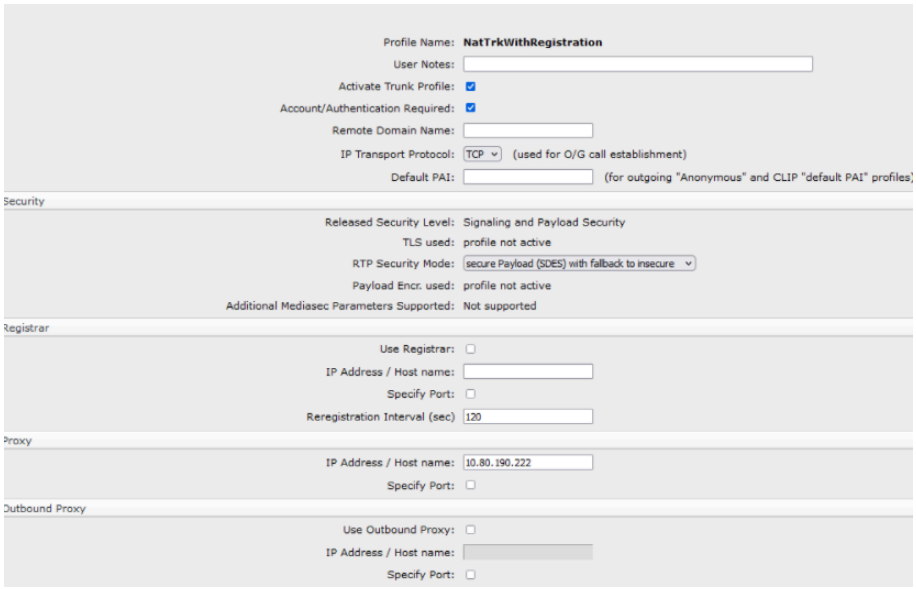
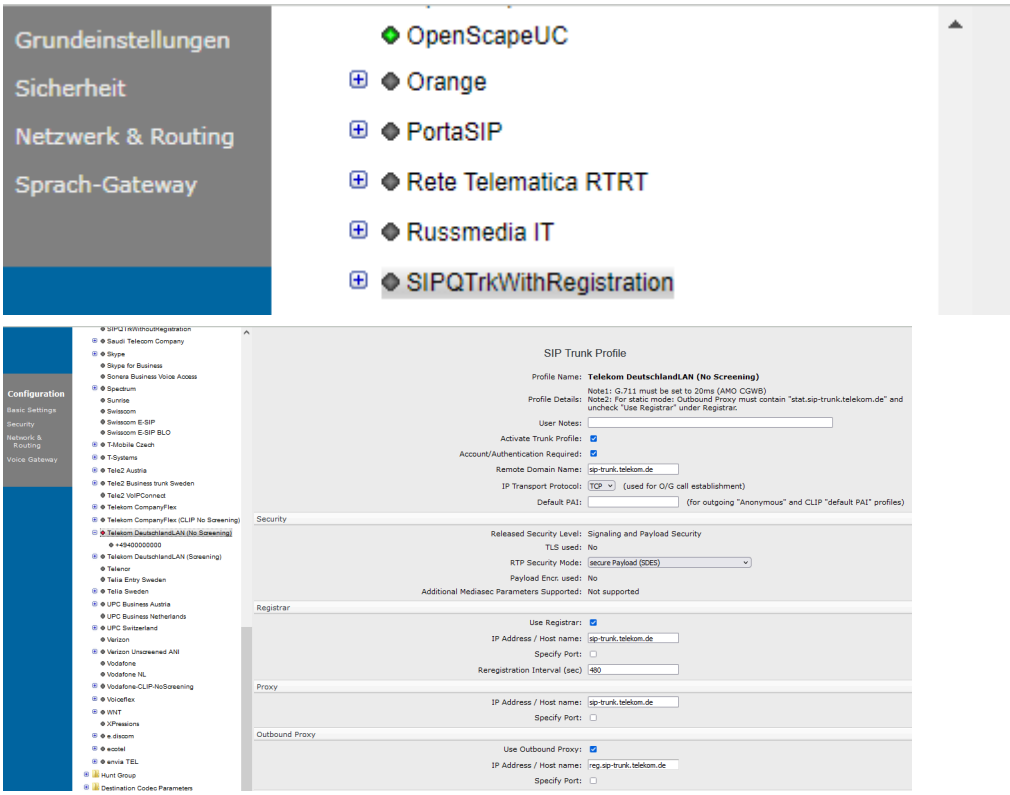


Figure 254: SIP-Q trunk profile with registration

5) Activate the profile

6) After the profile has been configured activate it. If the profile was activated successfully, it turns green.

Configuration > Voice Gateway > SIP Trunk Profile > SIPQTrkWithRegistration > Activate



Activated SIP-Q trunk profile with registration

DNS SRV switchback functionality for SIP-Q Trunking

FQDNs (without port setting) can be used for Registrar, Proxy and Outbound-Proxy (if used).

SIP registration procedure:

- Before starting a SIP-Q registration, the Registrars FQDN is resolved using DNS SRV procedure.
-
- Then a TCP/TLS connection is established with the highest priority IP address that is reachable.
- A SIP OPTIONS message is sent to check if partner is SIP capable.
- Then a REGISTER message will be sent.
- Afterwards calls are sent to this partner IP address.

  If the current target is no longer reachable anymore (e.g. lost TCP/TLS connection or no response to outgoing REGISTER or INVITE request), the next (in order of priority) IP address will be contacted using the same SIP registration procedure as described above.

  The default value of the polling period is a 60 seconds configurable in WBM under **Configuration > Voice Gateway > SIP Parameters > DNS-SRV**), which is also taken for the black listing period for unreachable IP addresses. As soon as an IP address with a higher priority is reachable (again), the SIP

registration procedure is repeated using the same procedure as described above.

PAI for anonymous

Default name/number, which will be used instead of Anonymous to prevent GW adding SIP PAI header with ***anonymous@host***.

14.4 Built-in SBC

The upcoming chapters will describe how OpenScape 4000 covers general Session Border Controller specifications.

The first chapter presents general Session Border Controller specifications gathered via Wikipedia as source information.

The Built-in SBC Function chapter is referring to these general Session Border Controller requirements and describes how these are realized in OpenScape 4000 Gateways (Classical HG Boards such as STMIX, STMIY, STMI4, STMI2 and SoftGates virtual HGs).

14.4.1 General SBC specifications (Source Wikipedia)

A Session Border Controller (SBC) is a network component for safe coupling of different computer networks or computer networks with different security requirements. SBC are mainly used in IP telephony networks (VoIP) to connect external (insecure) data networks with internal (secure) IT structures or to implement so-called sessions.

An SBC enables control and monitoring of signaling and media streaming as well as setup, execution and termination of telephone conversations or other interactive media that are involved in a communication.

An SBC is, as the name implies, used at network boundaries and couples internal and external networks. The SBC analyzes the various data streams (sessions) and acts on the different data streams (here: media data or signaling data) depending on the configuration. Within the telecommunications area (VoIP) signaling data and voice / video data are transmitted separately.

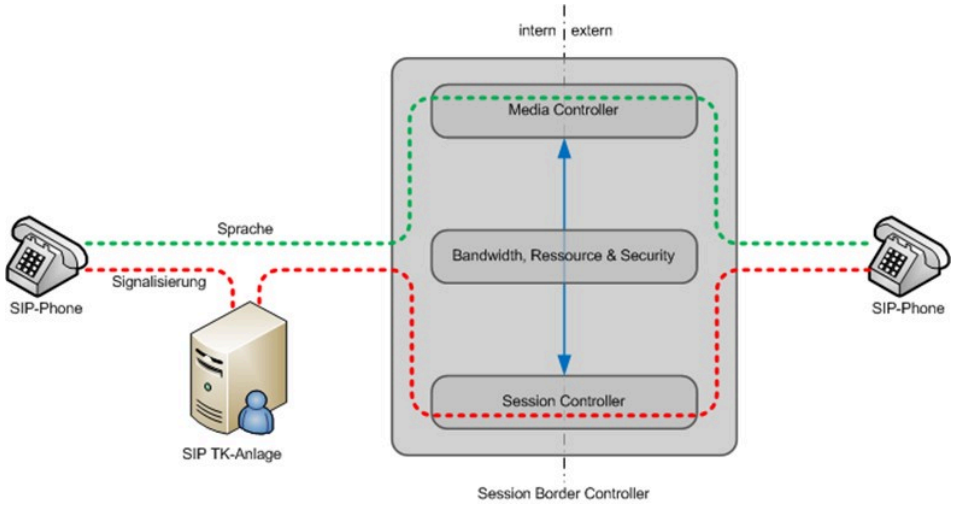


Figure 255: Operating principle of the Session Border Controller in VoIP environment

In general a SIP-based phone sends the signaling data to the telephone system, while the voice data is usually transmitted via the shortest route directly from phone to phone. By decoupling of signaling and voice data on the one hand the advantages of IP-based data networks can be used but on the other hand, the transmission of voice (media) data cannot be affected by the telephone system.

- **Security Offloading** Support of encryption techniques (TLS, SRTP)
- **Media Pinholing** Specific activation of UDP / TCP ports for the transmission of media data
- **Transcoding** Transcoding of different voice / video codecs such as G.711 to G.729
- **Protocol Translation** Conversion and adjustments of various signaling protocols such as SIP to SIP-Q (QSIG over SIP)
- **Header Manipulation** Adaptation of SIP and SDP header in order to convert e.g. phone number formats (E.164) or IP addresses
- **Media Anchoring** Coupling of voice data of SIP terminals that can only be reached via Network Address Translation. Secured coupling of voice / video data.

14.4.2 Built-in SBC Function

There are several SBC solution concepts in an OpenScape 4000 environment, e. g. usage of OpenScape SBC, Hosted OpenScape SBC (hSBC) or other 3rd-Party SBC. Independent of that the OpenScape 4000 components (Gateways) provide a “**Built-in SBC**” function that is always automatically active when VoIP connections have to be transmitted via an Internet telephony service provider (ITSP). This Built-in SBC functionality is not related to the *Hosted OpenScape SBC (hSBC)* Feature of OS4K V8. The Hosted OpenScape SBC Feature must be activated separately, when needed. The activation of the appropriate built-in SBC function is done automatically and is always active within OpenScape 4000. An explicit configuration is not necessary and therefore not provided in the Administration Portals (WBM).

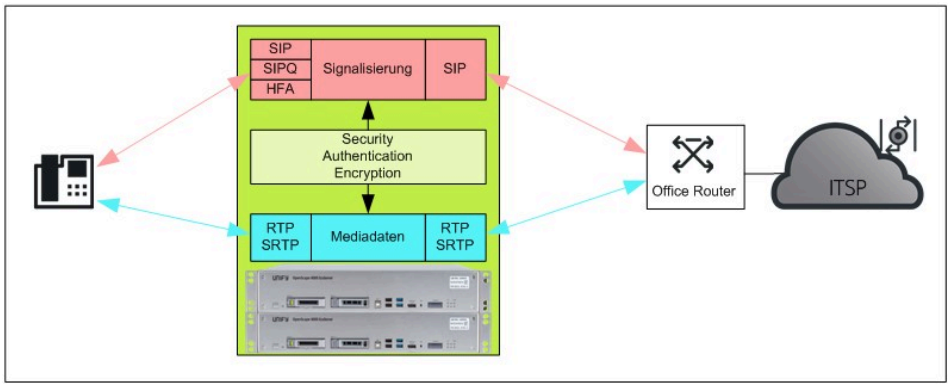


Figure 256: OpenScape 4000 built-in SBC function

The Built-in SBC function is also activated in case of:

- Secure Remote Subscriber HFA/SIP (@Home)

OpenScape 4000 does not necessarily require the connection of a dedicated external SBC. Nevertheless the OpenScape 4000 V8 has been extended with the new feature of a Hosted OpenScape SBC (hSBC), which can of course be used in addition to the Built-in SBC.

In case of usage with more than 120 ITSP connections/channels, the use of an OpenScape SBC for Load Balancing between OS4K Gateways (max. 120 b-channels) or even between several OS4K locations will be necessary.

NOTICE: OpenScape 4000 ITSP certifications are primarily done using the Built-in SBC function. In some cases – e. g. Telekom DeutschlandLAN SIP-Trunk – the certification has been invoked in addition also with an OpenScape SBC.

- **Security Offloading**
- In OpenScape 4000 the transport protocols UDP, TCP and TLS are supported. For the media transport RTP and SRTP is supported. For SRTP the transcoding function is applied as described within the paragraph **Transcoding**.

  As default UDP / TCP and RTP are used. In case that the TLS transport protocol is offered by an ITSP, the ITSP configuration can be used together with the Signaling- and Payload Encryption (SPE) of OpenScape 4000.

  The built-in SBC function provides additional security features such as:

  – Network overload protection
  – Address filtering with Whitelisting and Registration Blacklist

  The address filter settings are derived from the configuration data for stations and ITSP connection details (i. a. Inbound Proxy of SIP Provider Profile). There are no other specific configurations required.
- **Media Pinholing**
- The built-in SBC function ensures enabling of UDP ports in the Internet router for transmitting media data. For this purpose, no specific configuration is necessary.
- **Transcoding**

- The built-in SBC function is implemented as a "Routing Engine". Therefore the IP addresses and UDP ports are adjusted in the RTP packets accordingly, but the RTP data itself remains unchanged.

  If requested, the RTP transcoding is provided by different gateway configurations within OpenScape 4000. For this purpose the different gateway codecs need to be configured per gateway.

  All available OpenScape 4000 codecs are supported if transcoding is used:

  – G711
  – G729A
  – G729AB
  – G722
  – OPUS
  –

- **Protocol Translation**
- OpenScape 4000 supports the connection of IP devices with different protocols (HFA, SIP, etc.) and various IP lines with SIPQ and / or native SIP protocol. The built-in SBC function automatically performs all the necessary conversions of the protocols for a seamless data flow between the different interfaces.
- **Header Manipulation**
- The built-in SBC function adjusts all the necessary protocol elements such as IP addresses in SIP and SDP and the number formats in all SIP header fields.

  All ITSP specific header parameters are stored in profiles, which are defined in the certification of the respective provider. Deviating configurations are possible by means of profile changes.
- **Media Anchoring**
- The built-in SBC function terminates all media streams of the ITSP. Doing so allows connections to internal endpoints via Network Address Translation. Only one RTP stream is supported per connection. Therefore, video connections are not supported via the built-in SBC function.

  The port range for the RTP stream is preset but can be changed if necessary.

14.5 Configuration of SIP Service Provider / SIP Carrier

IMPORTANT: A list with certified SIP Service Providers (ITSP) can be found in G-DMS document INF-13-000534. The Wiki from Unify can also be used as reference that contains some of the information provided by the Service INF: https://wiki.unify.com/wiki/Collaboration_with_VoIP_Providers_on_Enterprise_Platforms

NOTICE: In case a hardware exchange is considered, please refer to Chapter 3, “Board Replacement”

14.5.1 Motivation

Almost all providers/ carriers now offer a direct, IP-based network interface, on which Session Initiation Protocol (SIP) is used between the IP-PBX and SIP provider. This IP-based network interface can be used instead of or in addition to the existing ISDN system connections.

The following figure shows an example of this type of network interface:

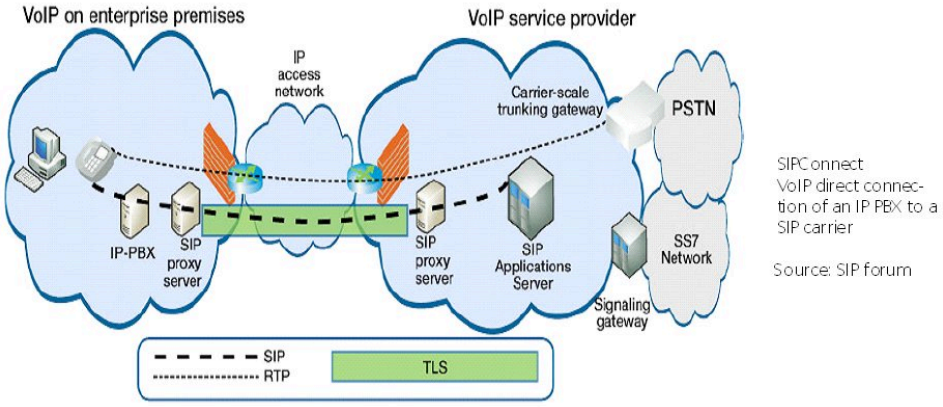


Figure 257: SIPconnect reference architecture

Native SIP enables IP-based, direct connection between a OpenScape 4000 system and a SIP provider. In an OpenScape 4000 system, the SIP provider connection can, of course, be configured in addition to the traditional ISDN connections.

14.5.2 Configuration Basics

14.5.2.1 Configuration

The feature is configured in two or three steps, depending on the initial situation.

- Without Session Border Controller
- If no session border controller is present, the feature is configured via AMOs and via WBM. In this case, the (v)HG 3500 receives an IP address from the WAN. This IP address is permanently allocated by the service provider.
- With Session Border Controller
- If a session border controller is being used, it must also be configured. In this case, the (v)HG 3500 has an IP address in the customer LAN, while the session border controller has two IP addresses - one from the customer LAN, and the other from the service provider WAN. The session border controller operates as a router for the (v)HG 3500 in the WAN.
- DNS
- As you are using Internet telephony and the Internet operates based on names, it is always advisable to use DNS.

14.5.2.2 Notes

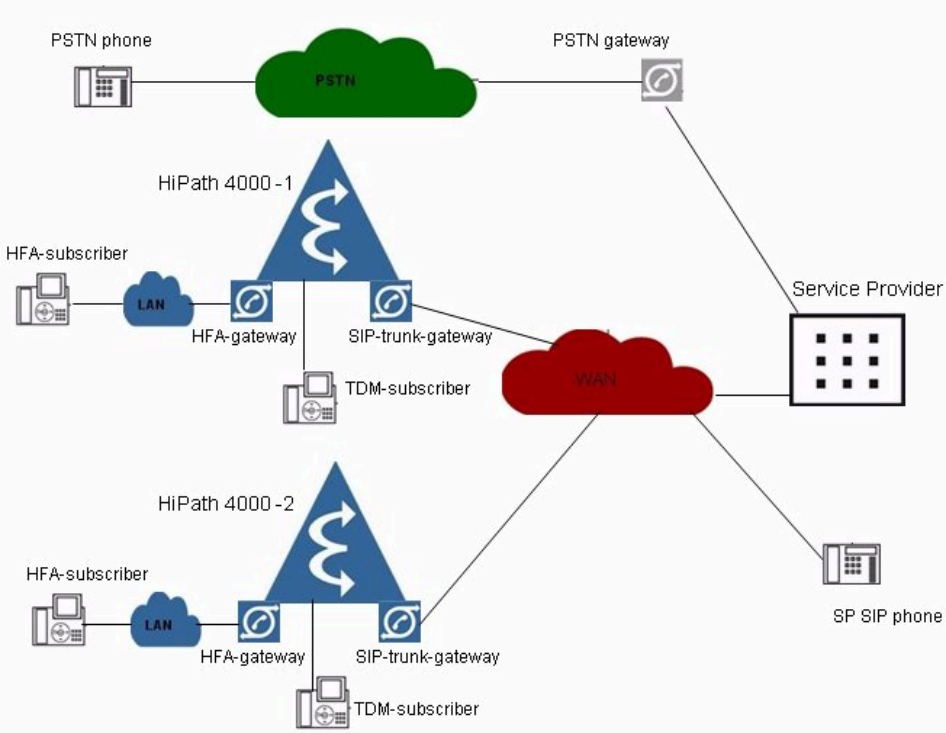
- OpenScape 4000 SoftGate
- In the following example, a HG 3500 is used as an SIP trunking gateway. You could also use a virtual HG 3500 in an OpenScape 4000 SoftGate as an SIP trunking gateway. To do this, the AMO batch must be adapted to reflect the part number (AMO BCSU) and device type (AMO TDCSU).
- Features of SIP carriers
- This application scenario shows the connection to the SIP carrier. The service technician will use a standardized test plan with the support of system development to determine which features are possible using the respective SIP carrier.

14.5.3 Scenario 1: Gateway direct to SIP Carrier

14.5.3.1 Initial Situation

Key parameters:

Endpoint/Description	DN name/Phone number	IP address
SIP registrar / proxy	sip.iandc.training.com	2.3.3.124
DNS - service provider	iandc.training.com (domain name)	2.3.3.123
STNO carrier connection / HG 3500-1	+49180130100	3.3.3.11
STNO carrier connection / HG 3500-2	+49180130200	3.3.3.22



HG 3500 direct to SIP carrier

Subsequently, the following case should be configured. The HG 3500 of OpenScape 4000-1 should be set up as a native SIP gateway and register at the service provider. Registration should be performed using the phone number of the SIP system connection (+49180130100).

Another OpenScape 4000-2 from another customer has registered on the service provider. This system has the system number +49180130200 and a four-digit extension range. This system should be the dialing destination for the OpenScape 4000-1 node in this scenario. Thus only one specific phone number is routed via the SIP carrier connection instead of all phone numbers.

This section only explains configuration in the OpenScape 4000-1 system. Configuration of the OpenScape 4000-2 system is almost identical, so this is not described.

14.5.3.2 AMO Configuration

14.5.3.2.1 Configuration with ISDN Numbering Plan (recommended)

Using ISDN International Format is the easiest and recommended way for SIP numbering configuration. The format will then result in + being prefixed before the numbers in SIP. Using + is also preferred format for receiving numbers from any SIP Provider.

In AMO BFDAT a function block must be preset for HG 3550:

```
ADD-BFDAT:FCTBLK=3,FUNCTION=HG3550,BRDBCHL=BCHL60&BCHL120;

CHANGE-BFDAT:CONFIG=CONT,FCTBLK=3,FUNCTION=HG3550,LINECNT=2,UNITS=3;

CHANGE-BFDAT:CONFIG=OK,FCTBLK=3,ANSW=YES;
```

HG 3550 is configured with function ID 1 and the functional block 3 described above:

```
ADD-BCSU:MTYPE=IPGW,LTG=1,LTU=1,SLOT=10,PARTNO="Q2324-X500",FCTID=1,LW►
VAR="0",FCTBLK=3,BCHL3550=60,ALARMNO=0;
```

The HG 3550 IP address is entered in the AMO CGWB. In this case, it is an address from the WAN allocated by the service provider. The DNS whose address is also entered here as DNSIPADR, is also in the service provider area:

```
ADD-CGWB:LTU=1,SLOT=10,SMODE=NORMAL,IPADR=3.3.3.11, NETMASK=255.255.255.0,BI►
TRATE="AUTONEG",TRPRSIP=60,DNSIPADR=2.3.3.123;
```

In the AMO CGWB, LEGKDATA section, the number of gateways is entered (GWNO):

```
CHANGE-CGWB:MTYPE=CGW,LTU=1,SLOT=10,TYPE=LEGKDATA,GWNO=1,REGEXTGK=NO;
```

In the AMO CGWB, external registration and digest authentication remain deactivated:

```
CHANGE-CGWB:MTYPE=CGW,LTU=1,SLOT=10,TYPE=SIPTRERH,GWAUTREQ=NO;

CHANGE-CGWB:MTYPE=CGW,LTU=1,SLOT=10,TYPE=SIPTRSSA,SIPREG=NO;
```

You can configure a bundle for the SIP carrier application:

```
ADD-BUEND:TGRP:=55,NAME="SIP CARRIER",NO=60;
```

The following COT/COP classes are recommended:

```
ADD-COT:COTNO=55,PAR=ANS&CEBC&BSHT&BLOC&LWNC&NLCR&TSCS&NOFT&NTON;
ADD-COP:COPNO=55,TOLL=TA,TRK=TA;
ADD-TDCSU:OPT=NEW,PEN=1-01-010-0,COTNO=55,COPNO=55,DPLN=0,VBZ=0,
COS=1,LCOSV=1,LCOSD=1,CCT="SIP CARRIER ", DESTNO=0,PROTVAR="ECMAV2",SEG►
MENT=8,ATNTYP=CO,ISDNIP=00,ISDNNP=0,TRACOUNT=31,SATCOUNT=MANY,NNO=1-40-
155,ALARMNR=2,FIDX=1, COTX=55,FWDX=1,UUSCCX=16,UUSCCY=8,FNIDX=1, CLASSM►
RK=EC&G711&G729AOPT,TGRP=55,SRCHMODE=DSC,INS=Y,SECLEVEL=TRADITIO,DEV=HG3550►
CO,BCHAN=1&&30,BCNEG=N,BCGR=1,LWPAR=0;
```

If more than 30 B channels are required, the set 1-1-10-1 can be identical.

A RICHT is required for the LCR:

```
ADD-RICHT:MODE=LRTENEW,LRTE=55,LSVC=ALL,TGRP=55,DNNO=1-40-155;
```

You also need an outdial rule:

```
ADD-LODR:ODR=56,CMD=ECHO,FIELD=4;

ADD-LODR:ODR=56,CMD=ECHO,FIELD=5;

ADD-LODR:ODR=56,CMD=ECHO,FIELD=6;

ADD-LODR:ODR=56,CMD=ECHO,FIELD=7;

ADD-LODR:ODR=56,CMD=NPI,NPI=ISDN,TON=INTERNAT;

ADD-LODR:ODR=56,CMD=END;
```

and an LDAT.

```
ADD-LDAT:LROUTE=55,LAUTH=1,LSVC=ALL,LVAL=1,TGRP=55,ODR=56;
```

In the numbering plan, a digit pattern is configured according to regulations, which is to be routed via the SIP carrier connection.

```
ADD-LDPLN:LCRCONF=LCRPATT,DIPLNUM=0,LDP="0"-"W"-"00"-"49"-"1801"-"30200"-"XXXX",
LRTE=55,LAUTH=1;
```

NOTICE: SIP Providers expect all digits en-bloc and do not support overlap dialing. Thereby an alternative possibility to using -X in LDPLN is to use -Z with corresponding time out (LCREOD in AMO CTIME, branch CP1).

The following GKREG entry is not necessary and is only used for completeness, as the LEGK does not resolve addresses:

```
ADD-GKREG:GWNO=1,GWATTR=INTGW&HG3550V2&SIP,DIPLNUM=0,DPLN=0,LAUTH=1;
```

The KNDEF entry cancels out the system part of the incoming phone number:

```
ADD-KNDEF:NNO=1-40-155,TYPE=OWN,ISDNCC=49,ISDNAC=1801,ISDNLC=30100,ISDNSK=5;
```

14.5.3.2.2 Configuration with Unknown Numbering Plan

In AMO BFDAT a function block must be preset for HG 3550:

```
ADD-BFDAT:FCTBLK=3,FUNCTION=HG3550,BRDBCHL=BCHL60&BCHL120;

CHANGE-BFDAT:CONFIG=CONT,FCTBLK=3,FUNCTION=HG3550,LINECNT=2,UNITS=3;

CHANGE-BFDAT:CONFIG=OK,FCTBLK=3,ANSW=YES;
```

HG 3550 is configured with function ID 1 and the functional block 3 described above:

```
ADD-BCSU:MTYPE=IPGW,LTG=1,LTU=1,SLOT=10,PARTNO="Q2324-X500",FCTID=1,LW►
VAR="0",FCTBLK=3,BCHL3550=60,ALARMNO=0;
```

The HG 3550 IP address is entered in the AMO CGWB. In this case, it is an address from the WAN allocated by the service provider. The DNS whose address is also entered here as DNSIPADR, is also in the service provider area:

```
ADD-CGWB:LTU=1,SLOT=10,SMODE=NORMAL,IPADR=3.3.3.11, NETMASK=255.255.255.0,BI►
TRATE="AUTONEG",TRPRSIP=60,DNSIPADR=2.3.3.123;
```

In the AMO CGWB, LEGKDATA section, the number of gateways is entered (GWNO):

```
CHANGE-CGWB:MTYPE=CGW,LTU=1,SLOT=10,TYPE=LEGKDATA,GWNO=1,REGEXTGK=NO;
```

In the AMO CGWB, external registration and digest authentication remain deactivated:

```
CHANGE-CGWB:MTYPE=CGW,LTU=1,SLOT=10,TYPE=SIPTRERH,GWAUTREQ=NO;

CHANGE-CGWB:MTYPE=CGW,LTU=1,SLOT=10,TYPE=SIPTRSSA,SIPREG=NO;
```

You can configure a bundle for the SIP carrier application:

```
ADD-BUEND:TGRP:=55,NAME="SIP CARRIER",NO=60;
```

The following COT/COP classes are recommended:

```
ADD-COT:COTNO=55,PAR=ANS&CEBC&BSHT&BLOC&LWNC&NLCR&TSCS&LINC&NOFT&NTON;
ADD-COP:COPNO=55,PAR=IMEX,TOLL=TA,TRK=TA;
```

You can then configure the AMO TDCSU. The ISDNIP and ISDNNP parameters are linked to the IMEX parameter. This allows an implicit number to be changed into an explicit number. In this case, it is configured that an incoming number in the format "Unknown" is transformed to an ISDN INTERNATIONAL phone number if it begins with two zeros (ISDNIP=00). If the incoming number only begins with one zero, it is changed into an ISDN National (ISDNNP=0):

```
ADD-TDCSU:OPT=NEW,PEN=1-20-010-
0,COTNO=55,COPNO=55,DPLN=0,COS=1,LCOSV=6,LCOSD=1,CCT="SIP_CARRIER",DESTNO=0,PROT
VAR=ECMAV2,SEGMENT=8,ATNTYP=CO,ISDNIP=00,ISDNNP=0,TRACOUNT=31,SATCOUNT=MA►
NY,NNO=1-40-
155,FIDX=1,COTX=55,FWDX=1,UUSCCX=16,UUSCCY=8,FNIDX=1,CLASSMRK=EC&G711&G729AOPT,T
```

```
GRP=55,SRCHMODE=DSC,INS=Y,SECLEVEL=TRADITIO,DEV=HG3550CO,BCHAN=1&&20,BCNEG=N,BC►
GR=1,LWPAR=0;
```

If more than 30 B channels are required, the set 1-1-10-1 can be identical.

A RICHT is required for the LCR:

```
ADD-RICHT:MODE=LRTENEW,LRTE=55,LSVC=ALL,TGRP=55,DNNO=1-40-155;
```

You also need an outdial rule:

```
ADD-LODR:ODR=56,CMD=ECHO,FIELD=3;

ADD-LODR:ODR=56,CMD=ECHO,FIELD=4;

ADD-LODR:ODR=56,CMD=ECHO,FIELD=5;

ADD-LODR:ODR=56,CMD=ECHO,FIELD=6;

ADD-LODR:ODR=56,CMD=ECHO,FIELD=7;

ADD-LODR:ODR=56,CMD=NPI,NPI=UNKNOWN,TON=UNKNOWN;

ADD-LODR:ODR=56,CMD=END;
```

and an LDAT.

```
ADD-LDAT:LROUTE=55,LAUTH=1,LSVC=ALL,LVAL=1,TGRP=55,ODR=56;
```

In the numbering plan, a digit pattern is configured according to regulations, which is to be routed via the SIP carrier connection.

```
ADD-LDPLN:LCRCONF=LCRPATT,DIPLNUM=0,LDP="0"-"W"-"00"-"49"-"1801"-"30200"-"XXXX",
LRTE=55,LAUTH=1;
```

The following GKREG entry is not necessary and is only used for completeness, as the LEGK does not resolve addresses:

```
ADD-GKREG:GWNO=1,GWATTR=INTGW&HG3550V2&SIP,DIPLNUM=0,DPLN=0,LAUTH=1;
```

The KNDEF entry cancels out the system part of the incoming phone number:

```
ADD-KNDEF:NNO=1-40-155,TYPE=OWN,ISDNCC=49,ISDNAC=180,ISDNLC=130100,ISDNSK=6;
```

14.5.3.3 Gateway Configuration in WBM

In the HG 3500 WBM under **Configuration** > **Voice Gateway**, you will find the menu item **SIP Trunk Profile**. Here you will find preset profiles for the released service providers. For a simulation, we use a general profile with registration.

The following settings are configured under this profile (**NatTrkWithRegistration**):

- **Domain name**: supplied by the provider (here: iandc.training.com).
- **IP address/hostname** of the registrar: supplied by the provider (here DNS name: sip.iandc.training.com).
- **IP address/hostname** of the proxy: supplied by the provider (here DNS name: sip.iandc.training.com).

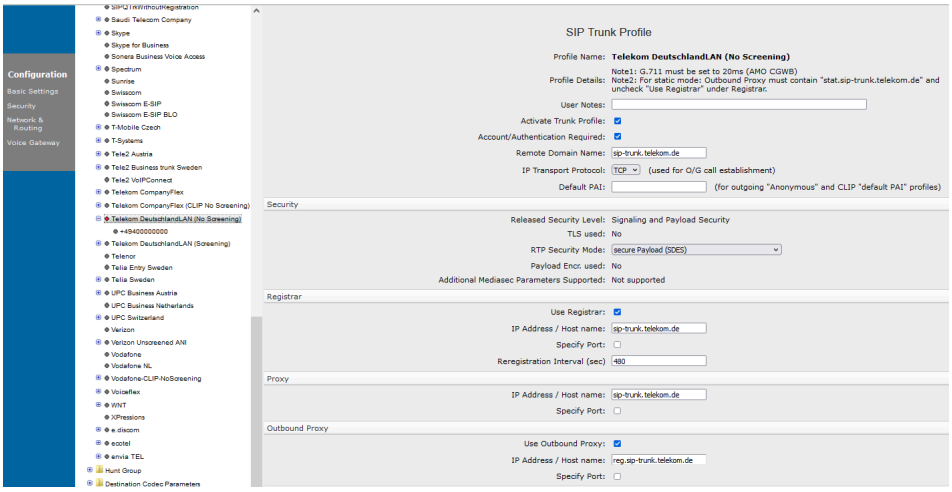


Figure 258: SIP service profiles in HG 3500 WBM (scenario 1)

Finally, enter the **Account Name** (click the menu item **NatTrkWithRegistration**). In this example, you are registering under the system number assigned to the connection by your provider.

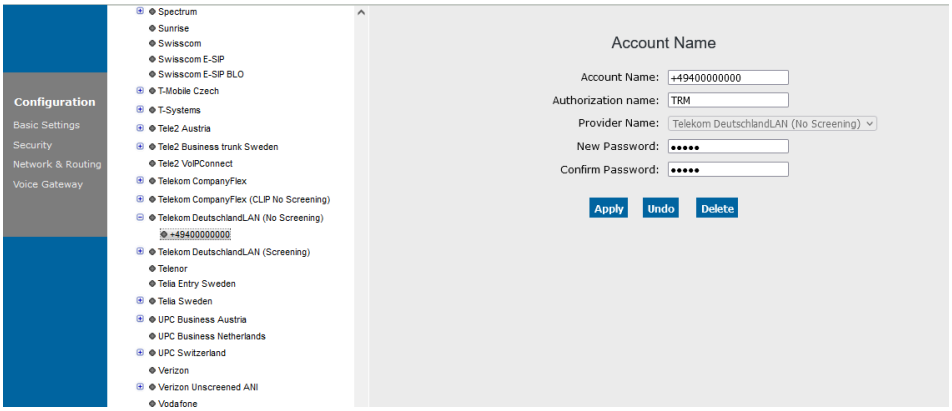


Figure 259: SIP service profiles in HG 3500 WBM (scenario 1)

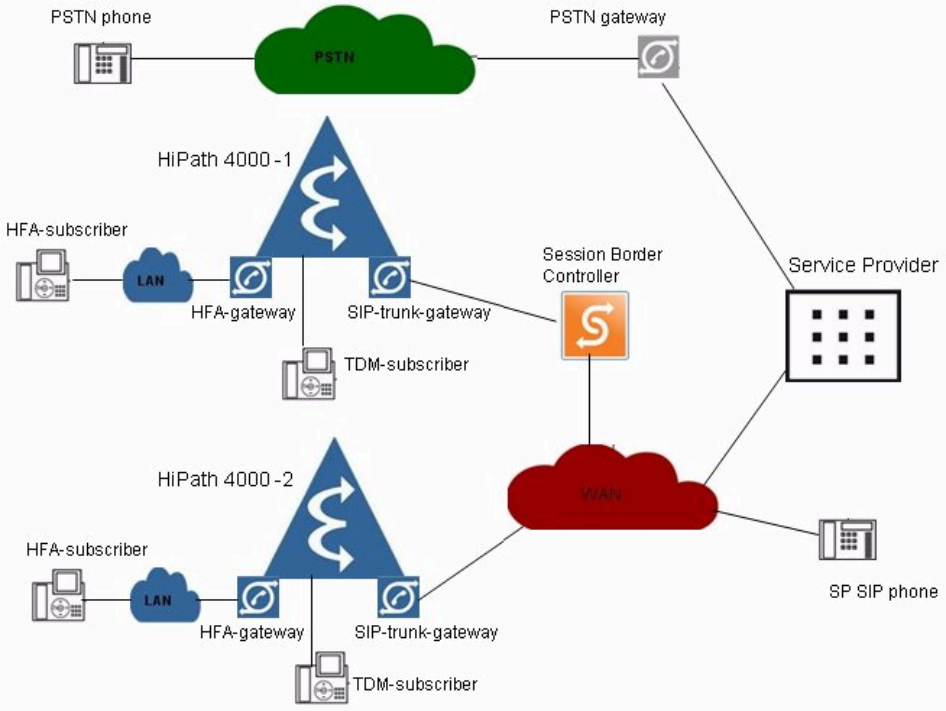
14.5.4 Scenario 2: Gateway via Session Border Controller to SIP Carrier

14.5.4.1 Initial Situation

Key parameters:

Endpoint/Description	DN name/Phone number	IP address
DNS - service provider	iandc.training.com (domain name)	2.3.3.123
SIP registrar / proxy	sip.iandc.training.com	2.3.3.124

STNO carrier connection / SBC-WAN-1	+49180130100	3.3.3.1
STNO carrier connection / HG 3500-2	+49180130200	3.3.3.2
HG 3500 -1 (LAN)		1.40.11.82
SBC -1 (LAN)		1.40.11.89



HG 3500 via session border controller to SIP carrier

In this example, the scenario has changed as only one session border controller (SBC) is switched between the SIP trunk gateway (HG 3500) and service provider on the OpenScape 4000 -1 system. The SIP trunk gateway is now configured with an IP address from the customer LAN (1.40.11.82). The session border controller has two IP addresses, 1.40.11.89 in the customer LAN and 3.3.3.1 in the service provider LAN.

A session border controller is recommended when using OpenScape 4000 SoftGates, to increase security. It has Network Address Translation (NAT) and firewall functionality.

In case of AMO configuration in the OpenScape 4000-1, only the HG 3500 changes. In the HG 3500 WBM, the session border controller is configured as the interface to the service provider (Outbound-Proxy). Of course, the session border controller must also be configured.

The OpenScape 4000-1 system can be called from the OpenScape 4000-2 system using the digit pattern 0049180130100-xxxx.

14.5.4.2 AMO Configuration

Configuration is identical to scenario 1. Gateway direct to SIP Carrier (Chapter 5, “Scenario 1: Gateway direct to SIP Carrier”), except for CGWB AMO.

The HG 3550 IP address is entered in the AMO CGWB. In this case, it is an address from the customer LAN:

```
ADD-CGWB:LTU=1,SLOT=10,SMODE=NORMAL,IPADR=1.40.11.82, NETMASK=255.255.255.0,BI►
TRATE="AUTONEG",TRPRSIP=60,DNSIPADR=2.3.3.123;
```

14.5.4.3 HG 3500 Configuration in WBM

HG 3500 configuration in WBM corresponds almost exactly to scenario 1 : Gateway direct to SIP Carrier. In a suitable SIP trunk profile (in this case: **NatTrkWithRegistration**) enter:

- **Domain name**: supplied by the provider (here: iandc.training.com).
- **IP address/hostname** of the registrar: supplied by the provider (here DNS name: sip.iandc.training.com).
- **IP address/hostname** of the proxy: supplied by the provider (here DNS name: sip.iandc.training.com).
- Outbound proxy: Different to scenario 1! Here, activate the checkbox under **Use outbound proxy** and enter the IP address of the session border controller in the LAN (**IP address/hostname**: 1.40.11.89). All calls are routed to the SIP carrier from the HG 3500 via OpenScape SBC. The HG 3500 also only permits incoming calls routed via OpenScape SBC.
- **Inbound proxy**: Not activated here! You can enter a proxy here, which will be used especially for incoming calls.

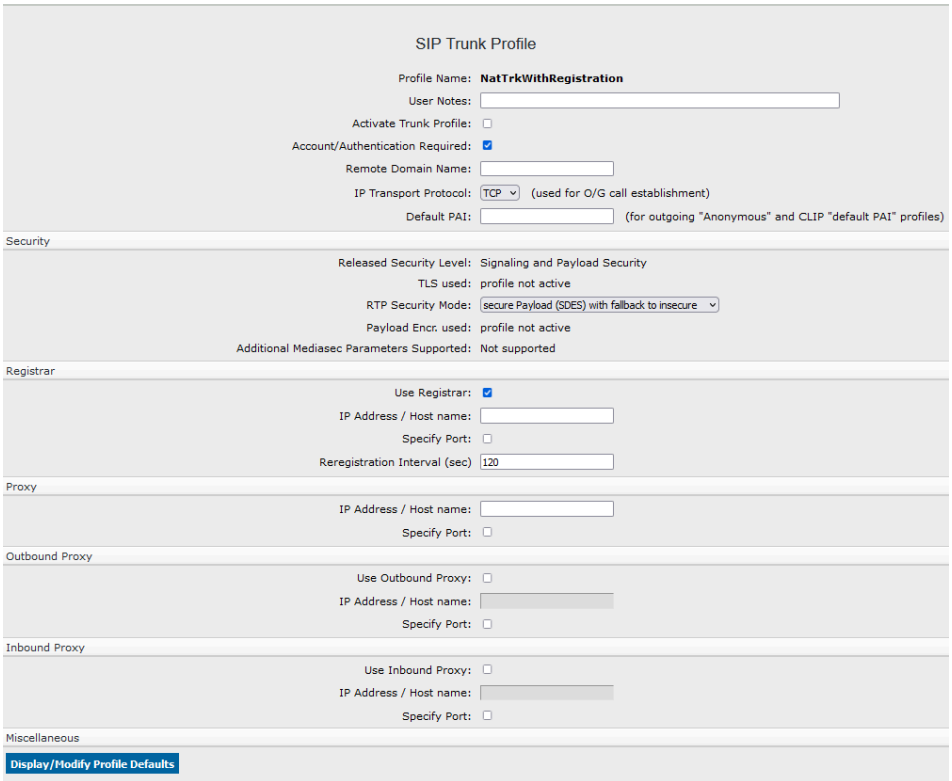


Figure 260: SIP service profiles in HG 3500 WBM (scenario 2)

As in scenario 1, you can right-click *the profile name* in the Explorer bar to add registration data to the account. The registration name is the system number in our example.

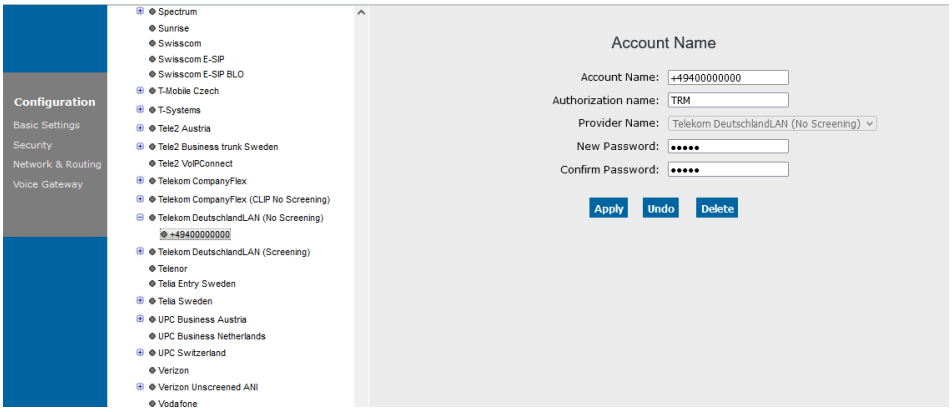


Figure 261: SIP service profiles in HG 3500 WBM (scenario 2)

14.5.4.4 Configuration in the Session Border Controller

You might have to configure the following parameters in the session border controller:

- Time settings
- External IP address for the WAN interface (allocate by the service provider)
- Internal IP address for the LAN1 interface
- DNS
- Firewall settings
- IP address of the SIP service provider
- SIP settings
- Configure the HG 3500 IP address as gateway

Please refer to the appropriate and used SBC.

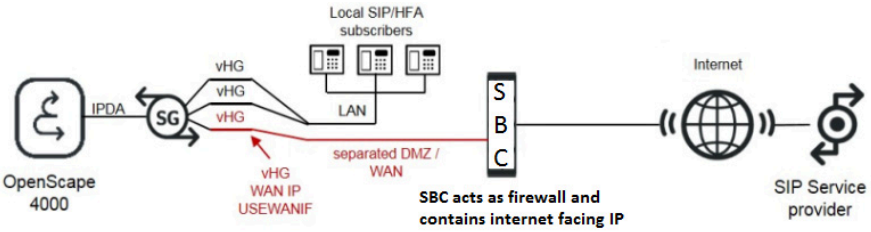
In case an OpenScape SBC is used, please refer to the OpenScape SBC Configuration Guide, chapter 3.6 SBC using OpenScape 4000 as SIP Server

14.5.4.5 SG vHG direct connectivity (USEWANIF)

In some cases, the SSP provides its own SBC/Router and a dedicated interface and network address is preferred. This is done by activating USEWANIF in AMO CGWB.

The external SBC contains the Internet facing IP (and will often suffice instead for a firewall), thus no additional configuration is needed to standard SSP configuration.

SPE in the direction of SSP is controlled via TDCSU SECLEVEL. TLS signaling connection with payload encryption is possible if having the correct security certificates, profile configuration and SECLEVEL=SECURE.



14.5.5 SIP Provider Telekom Deutschland GmbH

Telekom Deutschland GmbH now also offers a change of the ISDN PABX connections to SIP telephony in the modernization of traditional TDM technology to IP-based communications. This conversion (often under the pseudonym title "ALL-IP") involves the exchange of ISDN multiplexers (S2M) / ISDN NTBA (S0) with certified IP routers e.g. Telekom. These routers provide the connectivity to the Internet used for in- and outcoming connections by the OpenScape 4000 SIP trunking to the Central Office (CO).

An alternative is the so-called “DeutschlandLAN SIP-Trunk Pure” by Telekom. This includes no access (xDSL/FTTH) by Telekom and can be used with any Internet connection (bandwidth dependent) where Telekom Sales should be contacted for more details. For guaranteed speech quality (Quality of Service) by Telecom a DeutschlandLAN SIP trunk with access service provided by Telekom is required (e.g. xDSL, FTTH).

For OpenScape 4000 perspective this means the connection must be moved from a classical ISDN Board to a SIP-compatible Board in terms of both board and LCR Routing configuration.

On OpenScape 4000 side these changes are supported with existing virtual HG boards (SoftGate) as well as the SIP-compatible STMIX/STMIY and STMI boards.

14.5.5.1 Service Information

Supported OS4K Gateways:

- SoftGate with virtual HG (vHG) (e. g. OpenScape 4000 Branch, OpenScape Access 500 or VMware SoftGate)
- **STMIX/STMIY**
- STMI (Only TCP/UDP & RTP support)

Supported Connections:

- Direct Connection OS4K Gateway
- OS4K Gateways connected via Hosted OpenScape SBC / OpenScape SBC

Telekom implemented a logic for their SIP-Trunks DeutschlandLAN and CompanyFlex which makes it possible to operate an IP-PBX behind a certified Telekom Router, although IP Network Address Translation is used. The Telekom checks in their Central Office (Backend) whether the received SIP messages originally arrived from a private network (Class A, B or C). If this is the case

the communication will be realized with NAT traversal which sends the payload streams on basis of the received RTP packets to the correct ports.

In contrast to direct SIP provider connections; this method is advantageous that the OS4K Gateway must not be served with a dedicated Public IP. The used OS4k gateway is therefore not directly be accessible from the Internet in the NAT scenario. It is enough to route the OS4K gateway into the local network of the certified router. (For a pictorial view refer to Section 5.5.4, “Connection Examples”: Gateway (HG/vHG) in the local network of the Telekom Router (NAT scenario))

All business routers which are certified by the Telekom (LANCOM, AudioCodes, etc.) include a stateful firewall and/or network address translation. These routers will pass through only packets from the WAN side towards the LAN if the used port has already made an outbound connection towards the WAN/ Internet (and is counted as active). Everything else is dropped. The used OS4K gateways are therefore “not on the Internet". Connectivity can be compared to a usual Home PC behind a commercial DSL router where a permanent port forwarding and open connection is not necessary. The used port on the WAN interface is set by the router randomly using network address port translation (NAPT) for the SIP communications. Depending on the used router, NAPT can be guaranteed only if the SIP interface on the OS4K is used with port 5060/5061. A modification to a higher port range from the LAN to the WAN interface of the router cannot be excluded (normal NAT).

Furthermore the OS4K Gateways are designed to terminate each SIP and Media session at the gateway itself. Nevertheless in all supported connection scenarios it is possible to connect a session border controller and/or to integrate the scenario into a DMZ.

Connection Scenarios:

Direct Connection OS4K Gateway:

- Gateway (HG/vHG) in the local network of the Telekom Router (NAT-Scenario)
- Gateway (HG/vHG) with dedicated Internet/Public IP (WAN-Scenario)

OS4K Gateways connected via Hosted OpenScape SBC / OpenScape SBC:

- Gateway (HG/vHG) via Hosted OpenScape SBC (z. B. OpenScape 4000 Branch)/OpenScape SBC in the local network of the Telekom Router (NAT-Scenario)
- Gateway (HG/vHG) via Hosted OpenScape SBC (z. B. OpenScape 4000 Branch)/OpenScape SBC with dedicated Internet/Public IP (WAN-Scenario)

Refer to chapter Section 5.5.4, “Connection Examples”

See also https://hilfe.companyflex.de/de/einrichtung/anschalteszenarien

Please check also the corresponding hints regarding Emergency Call Routing.

14.5.5.2 Restrictions

The DeutschlandLAN SIP trunk Telekom supports encryption only when both signaling and payload encryption (TLS and SRTP) are active together. Should one of these be sent unencrypted then the connection is terminated.

On the part of the Telekom only SDES is supported for voice encryption (SRTP). For configuration and relevant support of SDES, please see sub-chapter “1.5.

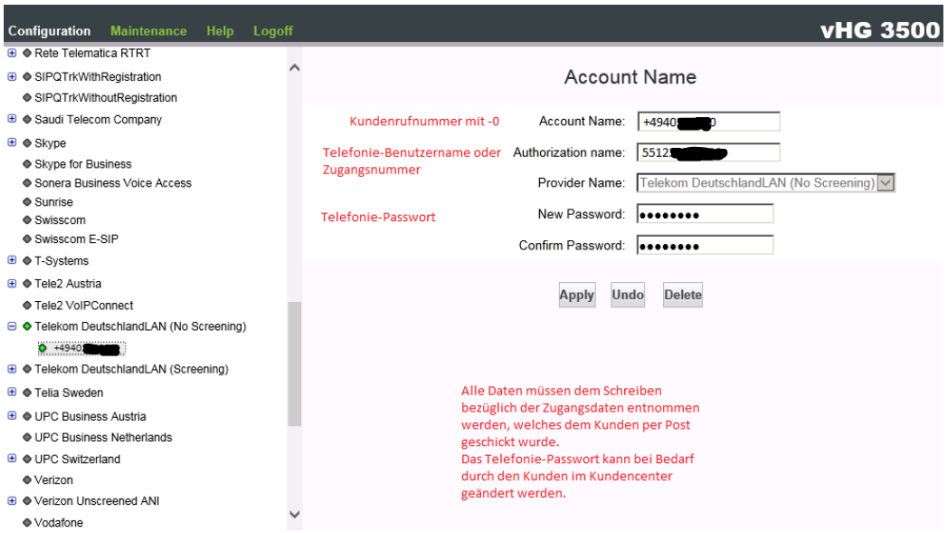
Session Description (SDES) Protocol” under “Signaling and Payload Encryption (SPE)” from IP Solutions.

IPv6 support is still in certification phase by Telekom.

14.5.5.3 Configuration

The HG/vHG Loadware contains SIP-Provider Profiles for the SIP trunks "Telekom DeutschlandLAN” and “CompanyFlex”. Only these profiles must be used for connectivity.

The profiles require a correct input of the Telekom account data, e. g in case of **DeutschlandLAN**:

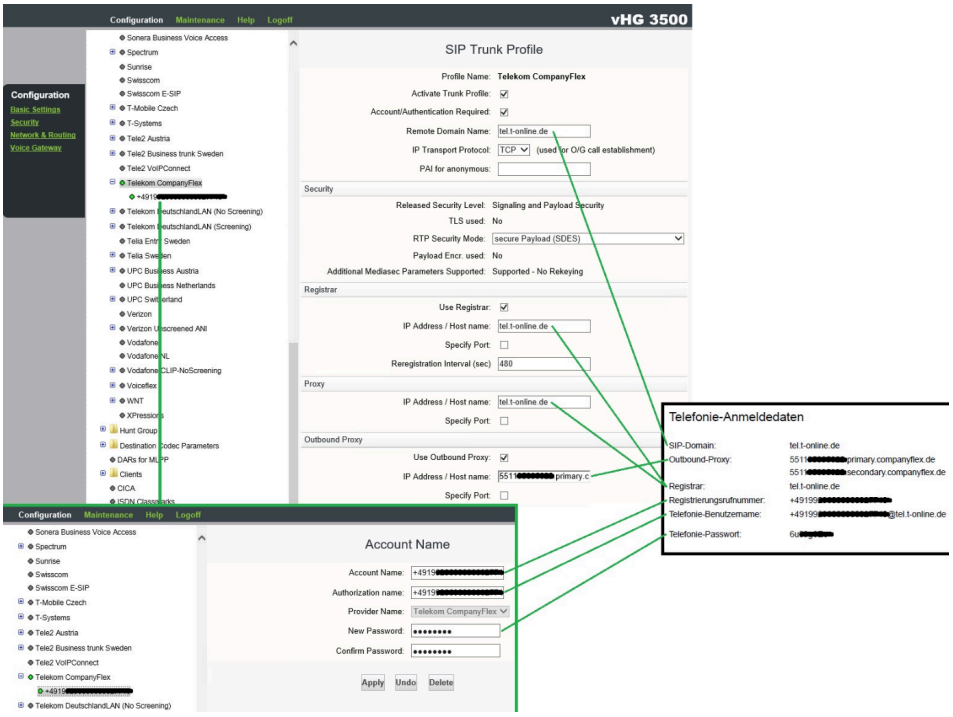


Like conventional SIP providers the Telekom offers two different modes: Registration and Static mode. Telekom prefers, the default “Registration” mode. The static mode can be enabled via the Telekom customer service if necessary.

Static Mode is no longer supported with CompanyFlex.

OpenScape 4000 also uses as default the registration mode in the SIP Provider Profile preset (Outbound Proxy). If required this can be changed manually (Outbound Proxy: stat.sip-trunk.telekom.de) in case of "Telekom DeutschlandLAN”.

There are separate profiles for CompanyFlex:



For CLIPnoScreening (if PUBNUM is not used) a different profile has to be used for CompanyFlex **“CompanyFlex (CLIP No Screening)”** and the parameter ***Default PAI*** needs to be configured.



The PUBNUM entries in SDAT and ACSU have to be configured in the format ISDN INTERNAT.

Due to the use of host names and DNS SRV the OS4K Gateway must be provided with a reachable DNS server. The DNS server must be able to resolve the Telekom addresses (see above). AMO CGWB is used to configure the DNS server.

To separate the customer LAN from the SIP trunk CompanyFlex/ DeutschlandLAN, the trunk can be connected via a separate interface i.e. eth1. The build-in SBC function of the vSTMI is active automatically. The CGWB path MANLANIF has to be used to configure the administration connectivity.

Example:

```
DIS-CGWB:21,16,GLOBIF;
```

```
H500:  AMO CGWB   STARTED
-------------------------------------------------------------------|
CGW BOARD DATA
-------------------------------------------------------------------|
HG3550
-------------------------------------------------------------------|
LTU = 21 SLOT = 16 SMODE = NORMAL POOLNO: 0
-------------------------------------------------------------------
GLOBAL DATA AND ETHERNET INTERFACE DATA - CONFIGURABLE VALUES:
-----------------------------------------------------
IPADR     = 88 .217.251.213        TCPP   =       (4060)
NETMASK   = 255.255.255.240        VLAN   = NEIN  (NEIN)
DEFRT     = 88 .217.251.209        (0.0.0.0 = NICHT KONFIGURIERT)
BITRATE   =         (SIEHE OS)     VLANID = 0     (0)
MUSTER    = 213 (213)              TLSP      = 4061  (4061)
TRPRSIP   = 1   (0)                TRPRH323  = 0  (0)
TRPRSIPQ  = 0   (0)                TPRH323A  = 0   (0)
DNSIPADR  = 212.18 .0  .5          SIPTCPP   = 5060 (5060)
DNSIPADR2 = 212.18 .3  .5          SIPTLSP   = 5061 (5061)
USEWANIF  = JA  (NEIN)
WPUBIP    = 0  .0  .0 .0
```

The OpenScape 4000 default values for RTP packet length and Type Of Service for signaling (TOSSIGNL) must be manually changed with AMO CGWB in the branch ASC to match Telekom requirements. RTP for G711 must be changed to 20ms and TOSSIGNL to 104. The TOS payload does not need to be changed.

HINT: The QoS settings are taken over by the routers in the Telekom-Portfolio for the WAN-Interface. At this point correct QoS marking is particularly important as here exists the bottle neck of the connection.

Configuration example:

```
ADD-CGWB:LTU=[LTU],EBT=[EBT],SMODE=NORMAL,IPADR=[IP-address],NETMASK=[netmask];

CHA-CGWB:MTYP=CGW,LTU=[LTU],EBT=[EBT],TYPE=GLOBIF,DEFRT=[IP-
address],TRPRSIP=[number of parallel calls],DNSIPADR=[DNS IP-
address],USEWANIF=YES;

CHANGE-CGWB:MTYPE=CGW,LTU=[LTU],
SLOT=[EBT],TYPE,TYPE=ASC,TOSSIGNL=192,PRIO=PRIO1,CODEC=G711A,VAD=NEIN,RTP=20;

CHANGE-CGWB:MTYPE=CGW,LTU=[LTU],SLOT=[EBT],TYPE=MANLANIF,
MIPADR=[IP-address administration LAN],MNETMASK=[netmask],MDEFRT=[Default Router
 administration LAN];
```

Example:

```
DIS-CGWB:21,16,ASC;
H500:  AMO CGWB  STARTED
-------------------------------------------------------------------
|  CGW BOARD DATA
-------------------------------------------------------------------
|   HG3550 |
-------------------------------------------------------------------
|  LTU = 21      SLOT = 16     SMODE = NORMAL           POOLNO: 0 |
-------------------------------------------------------------------
 ASC DATA - CONFIGURABLE VALUES:
---------------------------------
```

```
TOSPL    = 184   (184)    TOSSIGNL = 192   (104)
UDPPRTLO = 29100 (29100)  UDPPRTHI = 30099 (30099)
T38FAX   = YES   (YES)    REDRFCTN = YES   (YES)
RFCFMOIP = NO    (NO)     RFCDTMF  = YES   (YES)
PRIO1 :  CODEC = G711A   VAD = NO     RTP-SIZE = 20
```

In general connections to SIP providers should use international format an dialed national telephone number (e.g. mobile) must be sent to the CO in international format (NPI = ISDN, TON = INTERNAT).

Configuration Example international numbers:

```
ADD-LDPLN:LCRCONF=LCRPATT,DIPLNUM=0,LDP="0"-"W"-"00"-"X"-"Z",LAUTH=[LBER];
ADD-LODR:ODR=[LODR NUMMER],CMD=NPI,NPI=ISDN,TON=INTERNAT;
```

National numbers:

```
ADD-LDPLN:LCRCONF=LCRPATT,DIPLNUM=0,LDP="0"-"W"-"0"-"X"-"Z",LAUTH=[LBER];
ADD-LODR:ODR=[LODR NUMMER],CMD=OUTPULSE,DGTS=[LANDESVORWAHL DES ANSCHLUSSES];
ADD-LODR:ODR=[LODR NUMMER],CMD=NPI,NPI=ISDN,TON=INTERNAT;
```

Reference chapter: Section 5.3.2.1, “Configuration with ISDN Numbering Plan (recommended)”.

LCR has to be configured in international format and the reachability of special rate numbers with prefix codes has to be considered .

COT and COP in TDCSU have to be configured in a suitable way.

```
ADD-COT:COTNO=[COT number],
PAR=ANS&CEBC&BSHT&BLOC&LWNC&NLCR&TSCS&DFNN&NLRD&NOFT&NTON;
CHANGE-COP:COPNO=[COP NUMMER],COPTYPE=COPADD,PAR=T311,TRK=TA,TOLL=TA;
```

In case of CLIP No Screening the parameter PDL2 has to be set:

```
CHANGE-COT:COTNO=[COT NUMMER],PAR=PDL2;
```

Example TDCSU:

```
ADD-TDCSU:OPT=NEW,PEN=1-2-3,COTNO=[COT number],COPNO=[COP number],
CCT="COMPANYFLEX",PROTVAR=ECMAV2,SEGMENT=8,TRTBL=GDTR,FWDX=5,CLASSMRK=EC&G711&G729AOPT,
TGRP=1,SRCHMODE=DSC,INS=Y,SECLEVEL=SECURE,DEV=HG3550CO,BCGR=1;
```

Local numbers dialed without area code.

```
ADD-LDPLN:LCRCONF=LCRPATT,DIPLNUM=0,LDP="0"-"W"-"X"-"Z",LAUTH=[LBER];
ADD-LODR:ODR=[LODR number],CMD=OUTPULSE,DGTS=[country code + area code];
ADD-LODR:ODR=[LODR NUMMER],CMD=NPI,NPI=ISDN,TON=INTERNAT;
```

Call-by-Call 010

```
ADD-LDPLN:LCRCONF=LCRPATT,DIPLNUM=0,LDP="0"-"W"-"010"-"Z",LAUTH=[LBER];
ADD-LODR:ODR=[LODR NUMMER],CMD=NPI,NPI=ISDN,TON=NATIONAL;
```

In Telekom DeutschlandLAN SIP-trunk case there are special rate numbers with prefix codes which (not in E. 164-format) must be sent to the Telekom. These (nine) special rate numbers/-pre selection codes are:

```
110, 112, 115, 116-X, 118-X, 010-X, 0137-X, 0138-X and 0900-X
```

Example for special numbers:

```
ADD-LDPLN:LCRCONF=LCRPATT,DIPLNUM=0,LDP="0"-"W"-"11"-"0",LAUTH=[LBER];
ADD-LDPLN:LCRCONF=LCRPATT,DIPLNUM=0,LDP="0"-"W"-"11"-"2",LAUTH=[LBER];
ADD-LDPLN:LCRCONF=LCRPATT,DIPLNUM=0,LDP="0"-"W"-"11"-"5",LAUTH=[LBER];
ADD-LDPLN:LCRCONF=LCRPATT,DIPLNUM=0,LDP="0"-"W"-"116"-"Z",LAUTH=[LBER];
ADD-LDPLN:LCRCONF=LCRPATT,DIPLNUM=0,LDP="0"-"W"-"118"-"Z",LAUTH=[LBER];
ADD-LODR:ODR=[LODR NUMMER],CMD=NPI,NPI=ISDN,TON=SUBSCR;
```

Please consider also the corresponding hints regarding emergency routing published from the German Telekom:

https://hilfe.companyflex.de/de/einrichtung/anschalteszenarien

To use Signaling and Payload Encryption (SPE) activate following the chapter from the service documentation IP Solutions - Signaling and Payload Encryption (SPE).

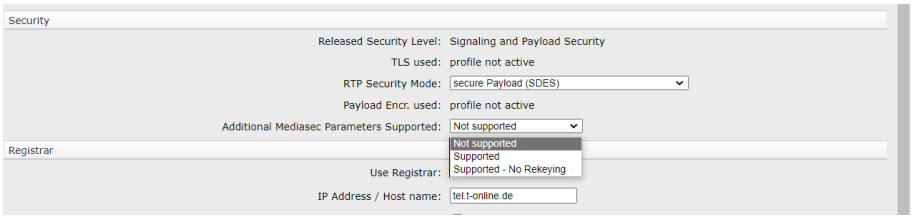
Telekom provides their own certificates (CA) for DeutschlandLAN SIP-Trunk. The provided Telekom CA certificates must be imported on the OS4K Gateway. Due to the OS4K SPE design, the Gateway also requires an "own server" certificate (e. g. *.p12) in addition to these CA certificates to activate SPE (TLS). For this purpose any private server certificate can be created (for example using OS4K Assistant) which then must be imported to the OS4K Gateway. The entered data in the server's certificate is irrelevant.

SIP Providers expect all digits en-bloc and do not support overlap dialing.

LCREOD should be changed on demand to a higher value:
`CHANGE-CTIME:TYPESWU=CP1,LCREOD=5;`

If Media-Security is used between OS-SBC and OS4K-GW as well, the following configuration needs to be changed in the SIP provider Profile for CompanyFlex:

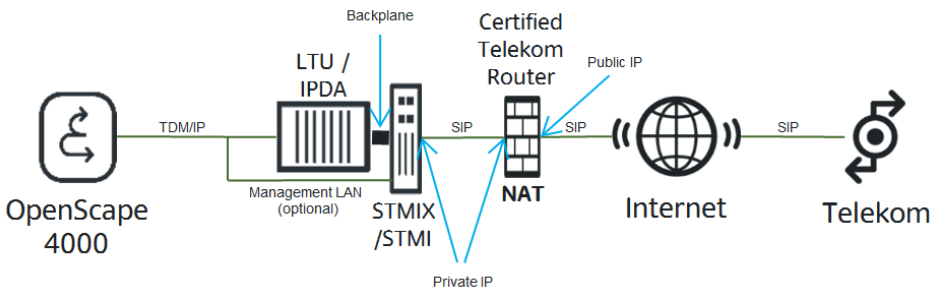
- Set **Additional Mediasec Parameters Supported** to "Not supported".

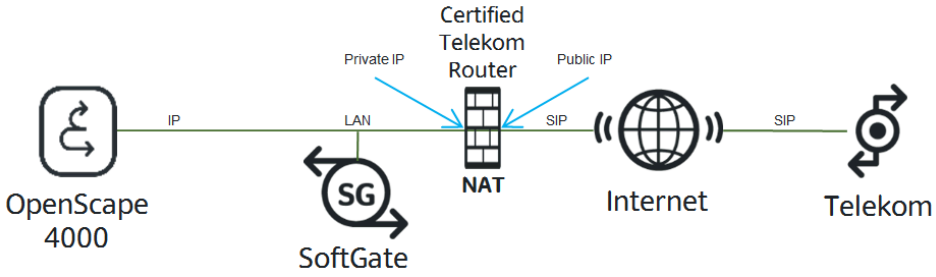


NOTICE: This parameter needs to be set to "Supported - No Rekeying" in case of direct connectivity between OS4K and SSP (default).

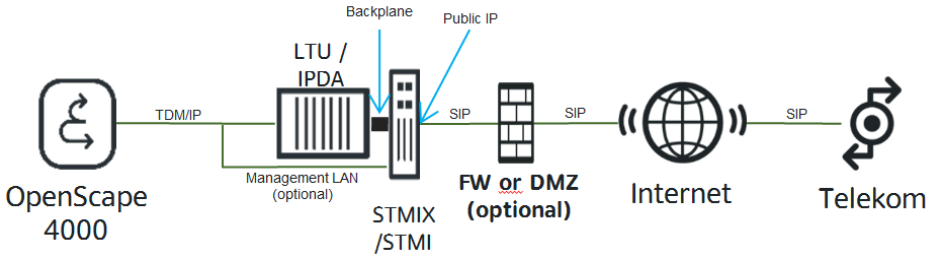
14.5.5.4 Connection Examples

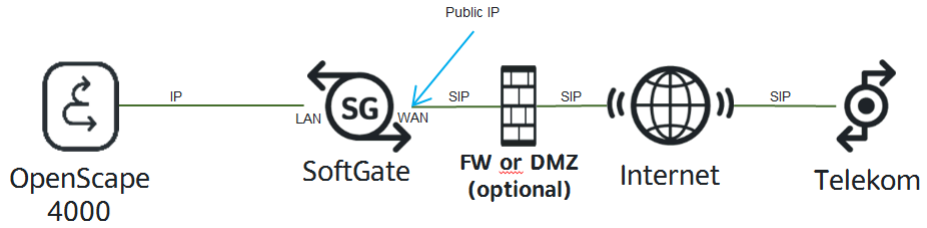
Gateway (HG/vHG) in the local network of the Telekom Router (NAT-Scenario):



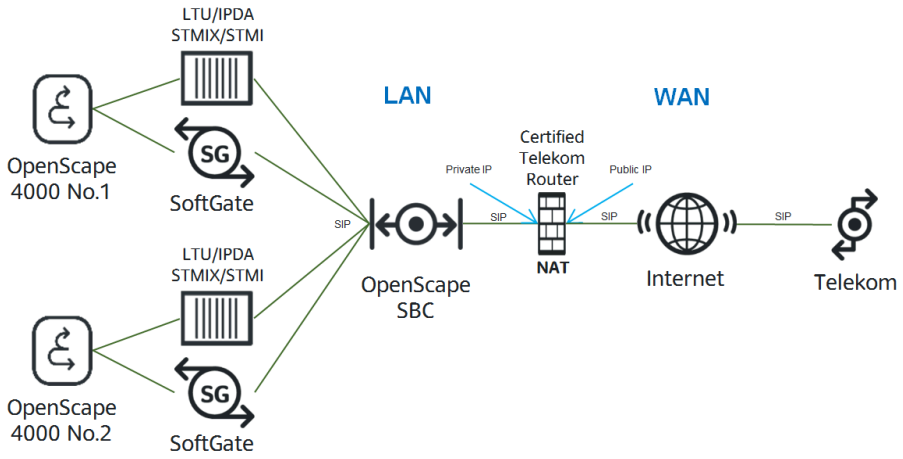


Gateway (HG/vHG) with dedicated Internet/Public IP (WAN-Scenario):

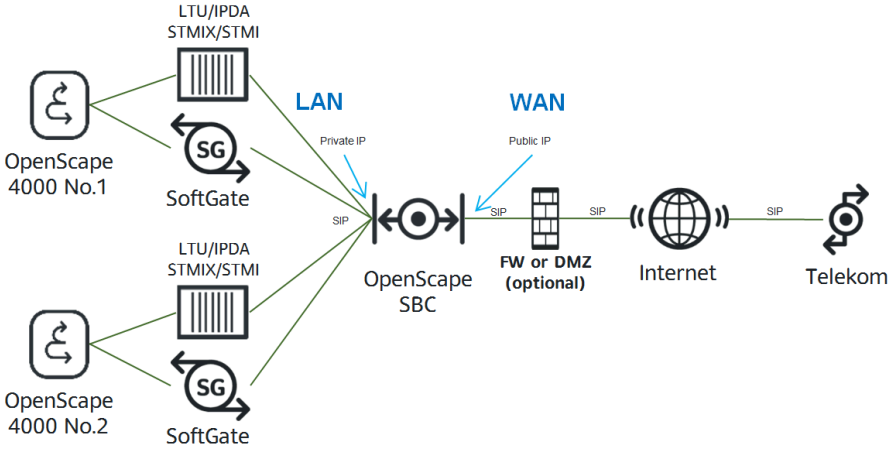




Gateway (HG/vHG) via Hosted OpenScape SBC (z. B. OpenScape 4000 Branch)/OpenScape SBC in the local network of the Telekom Router (NAT-Scenario):



Gateway (HG/vHG) via Hosted OpenScape SBC (z. B. OpenScape 4000 Branch)/OpenScape SBC with dedicated Internet/Public IP (WAN-Scenario):



14.5.5.5 Configuration Example OpenScape SBC

In this chapter an example configuration for the OpenScape SBC with the Telekom Deutschland GmbH (TDG) - DeutschlandLAN SIP-Trunk is described. In this case the OpenScape SBC registers itself to the DeutschlandLAN SIP-Trunk instead of the OS4K gateway.

Further OpenScape SBC documentation (e. g. configuration of “Clustered Mode” for connecting multiple Gateways and/or multiple OS4Ks), please refer to the official OpenScape SBC Configuration Guide (such as OpenScape SBC, Configuration Guide, Administrator Documentation).

The configuration data needs to be taken from the Telekom letter:



ERLEBEN, WAS VERBINDET.

TELEKOM DEUTSCHLAND GMBH

P

DV03 18 1,45 Deutsche Post

Telekom Deutschland GmbH

Landgrabenweg 151
53227 Bonn

ZUGANGSDATEN

Vertraulich, bitte aufbewahren!

Datum	01. März 2016
Ortsvorwahl	0228
Durchwahlnr.	12345
Abfragestelle	0
Registrierungsrufnummer	+49 228 123450
Rufnummernblock	von 000 bis 299

Sehr geehrte Damen und Herren,

hier sind die Zugangsdaten für Ihren neuen Telekom Anschluss. Sie gelten ab dem Tag der Bereitstellung, das genaue Datum sehen Sie in Ihrer Auftragsbestätigung.

Wie Sie Ihren Anschluss in einfachen Schritten einrichten, erfahren Sie in der beiliegenden Inbetriebnahme-Anleitung. Verwenden Sie für die darin beschriebene Einrichtung folgende Zugangsdaten:

2 Internet-Zugang einrichten

Anschlusskennung:	002529106948
Zugangsnummer: (vormals T-Online Nummer)	5511295012345
Mitbenutzernummer:	0001
Persönliches Kennwort:	25170493

3 Telefonie einrichten

Telefonie-Benutzername:	5511295012345
Telefonie-Passwort:	Yni2Fi84
Outbound-Proxy:	reg.sip-trunk.telekom.de
Registrar:	sip-trunk.telekom.de

Ein Wort in Sachen Sicherheit.
Halten Sie Ihre persönlichen Zugangsdaten vor anderen Personen geheim. Bitte geben Sie bei Fragen hierzu immer nur die Zugangsnummer an.

Wenn Sie Fragen haben, rufen Sie uns einfach an. Sie erreichen uns **kostenfrei unter 0800 33 02524.**

Freundliche Grüße
Ihre Telekom

TELEKOM DEUTSCHLAND GMBH, GESCHÄFTSKUNDENSERVICE

Postanschrift: 53171 Bonn | Internet: www.telekom.de
Aufsichtsrat: Timotheus Höttges (Vorsitzender) | Geschäftsführung: Dr. Dirk Wössner (Sprecher), Dr. Ferri Abolhassan, Walter Goldenits, Michael Hagspihl, Hagen Rickmann, Simone Thöner, Klaus Wiener
Handelsregister: Amtsgericht Bonn, HRB 9919, Sitz der Gesellschaft Bonn, USt-IdNr. DE 122653127, WEEE-Reg.-Nr. DE 60930328

Figure 262: Deutsche Telekom letter

1. DNS

It must be configured a DNS server which can resolve the Telekom DNS records configured in the Remote Endpoints:

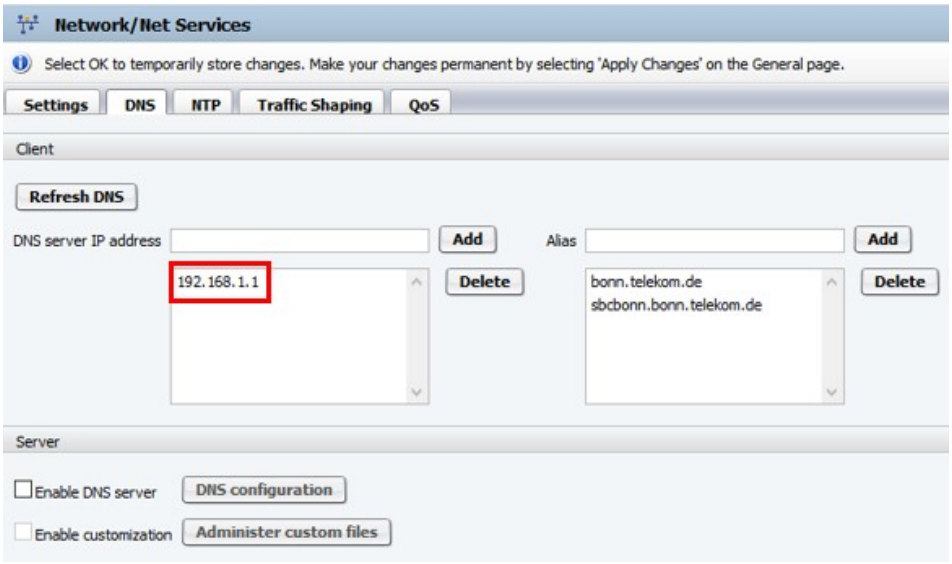


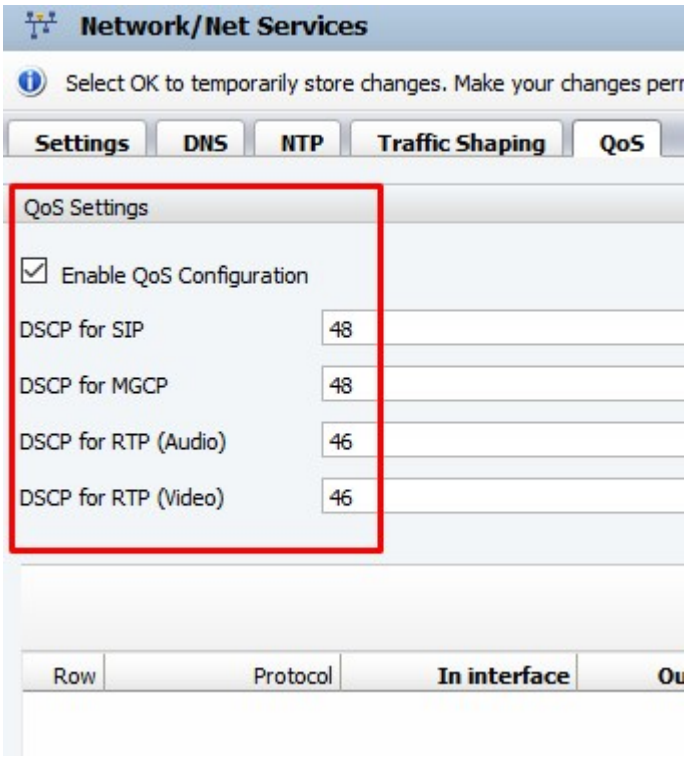
Figure 263: 2. Quality of Service (QoS)

Telekom has specified in their 1TR114 document QoS requirements which must be applied on OpenScape SBC:

8.4.2 Traffic Classes in Layer 3

The UE uses the following traffic classes at Layer 3 (according to the Architecture of T-Home)

- Voice Control Class 6 (DSCP 110 000)
- Voice Bearer Class 5 (DSCP 101 110)



3. Media Profile

Depending on whether the SIP trunk is encrypted via TLS or not, one of the two example Media Profiles in the screenshot need to be used:

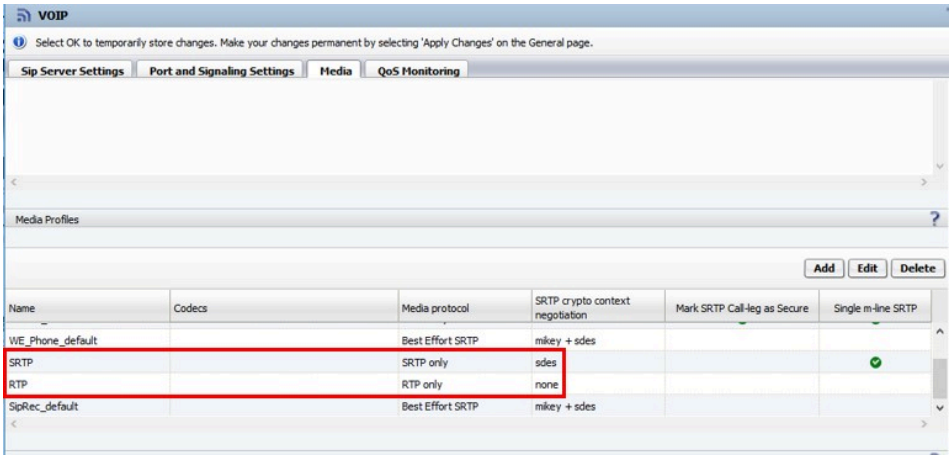
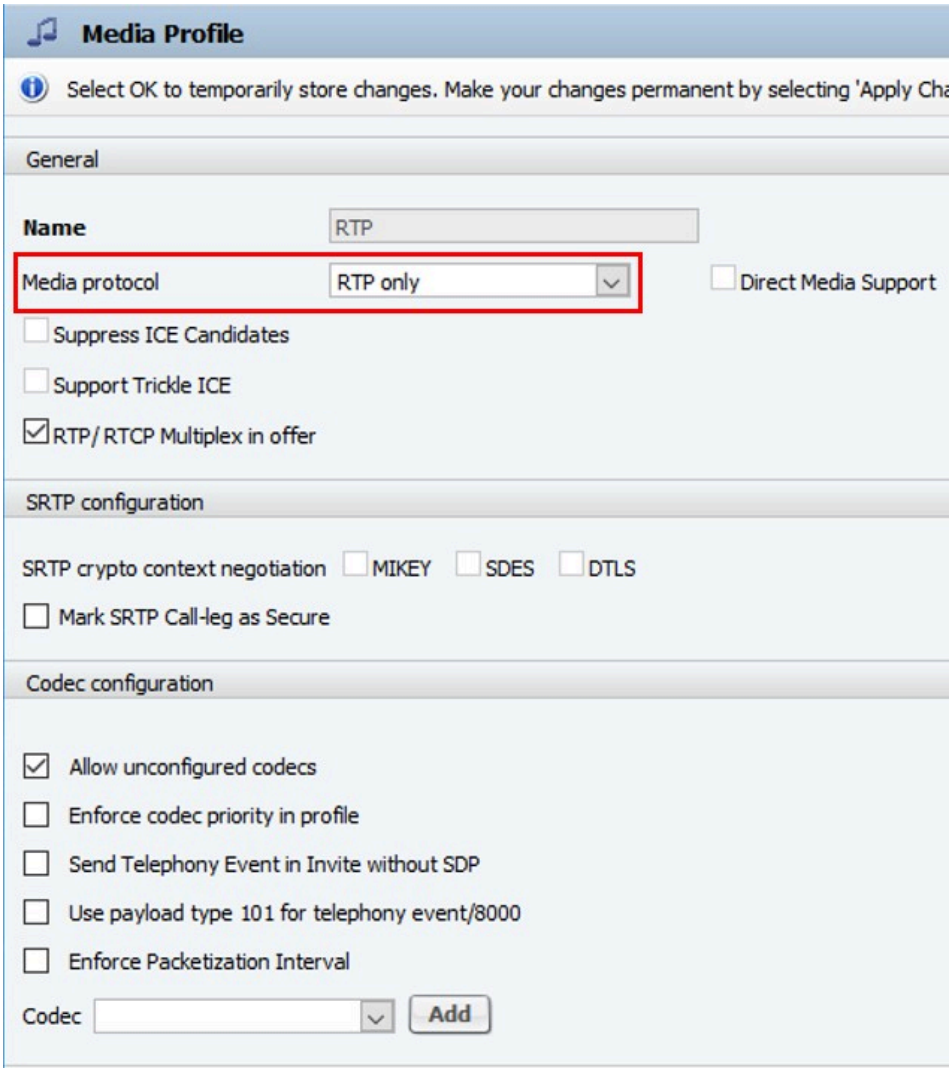
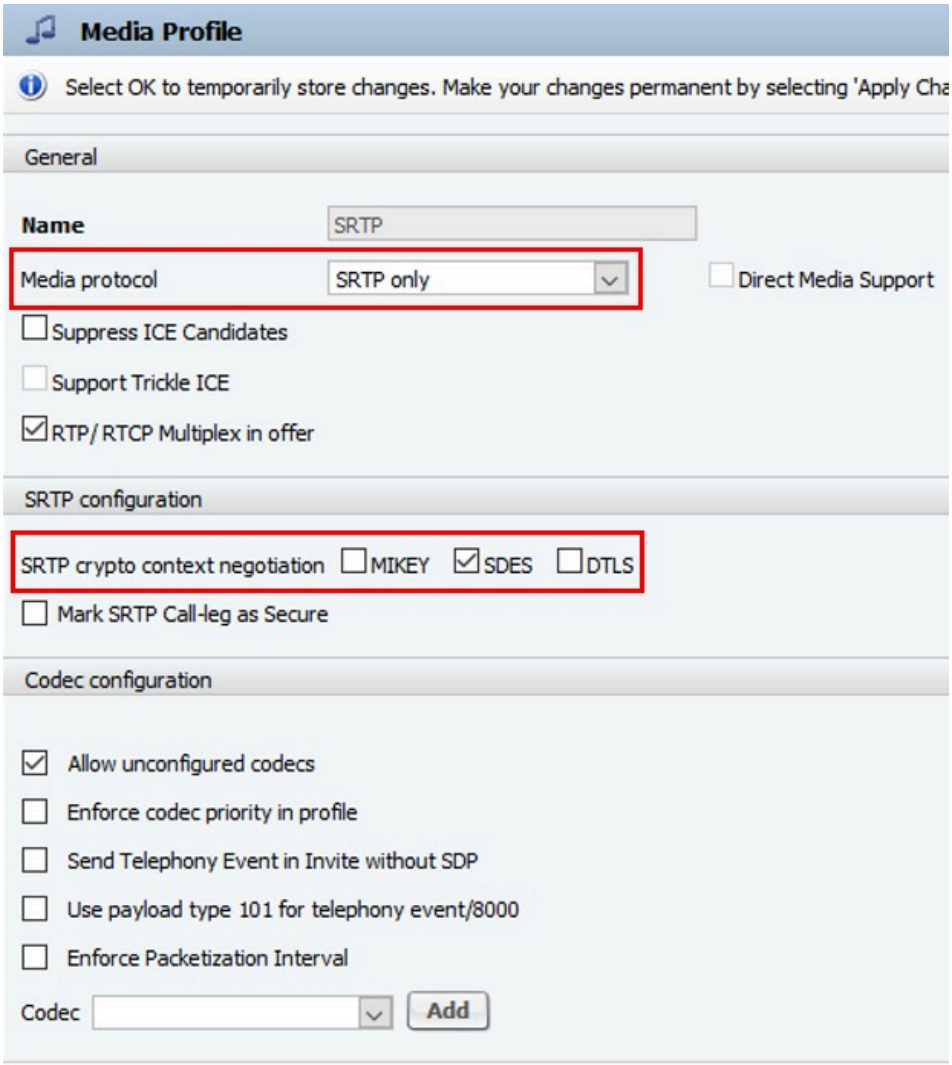


Figure 264: For an unencrypted SIP trunk the Media Protocol RTP was used:



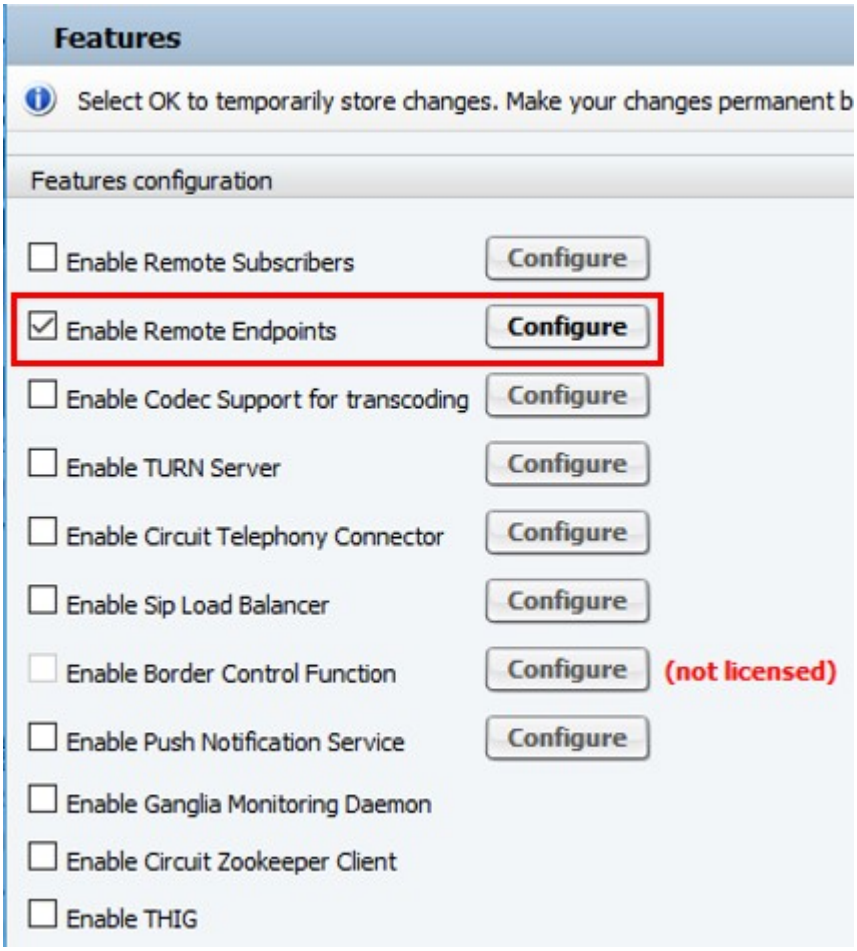
For an encrypted SIP trunk the Media Protocol SRTP and SDES to negotiate the cryptographic parameters was used. MIKEY may not be enabled because it's not supported by Telekom.



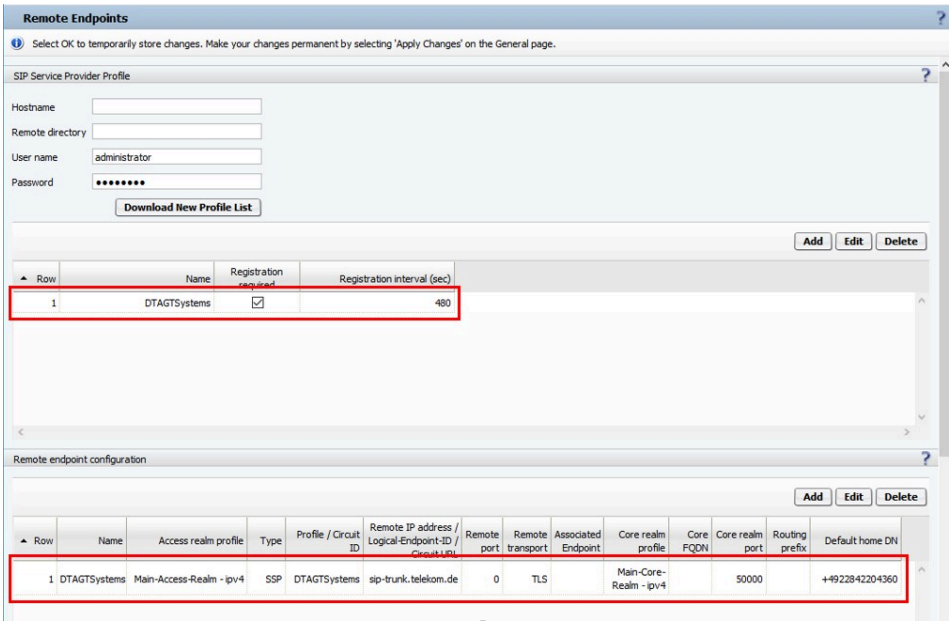
How to activate the defined Media Profile for the SIP trunk is described in the section Remote Endpoint below.

4. Remote Endpoint

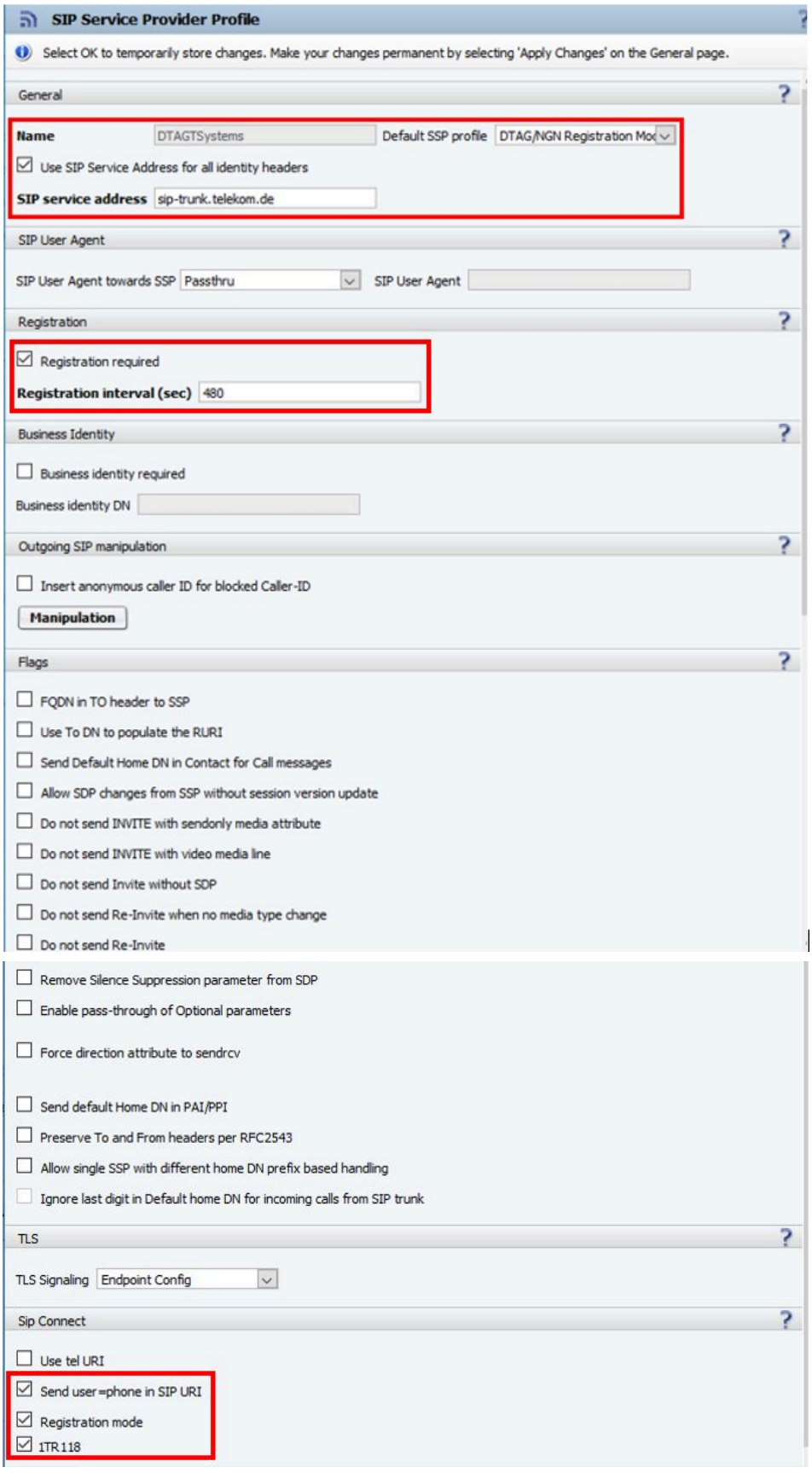
On the OpenScape SBC must be activated Enable Remote Endpoints:



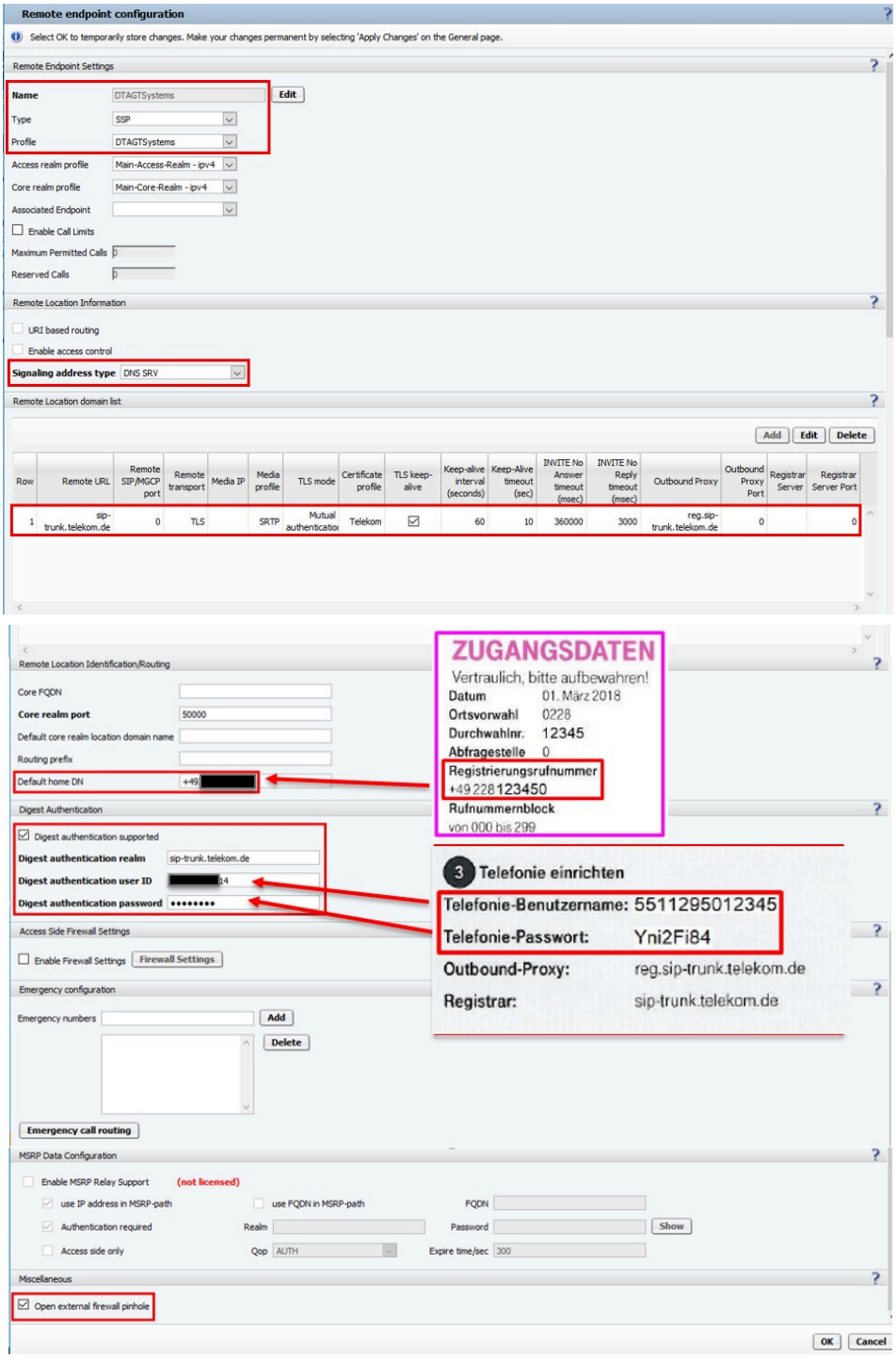
When opening the Remote Endpoints window the SIP Service Provider Profile and the Remote Endpoint has to be configured:



In the SIP Service Provider Profile window must be selected as default SSP profile DTAG/NGN Registration Mode. The registration interval has to be set to 480 seconds:

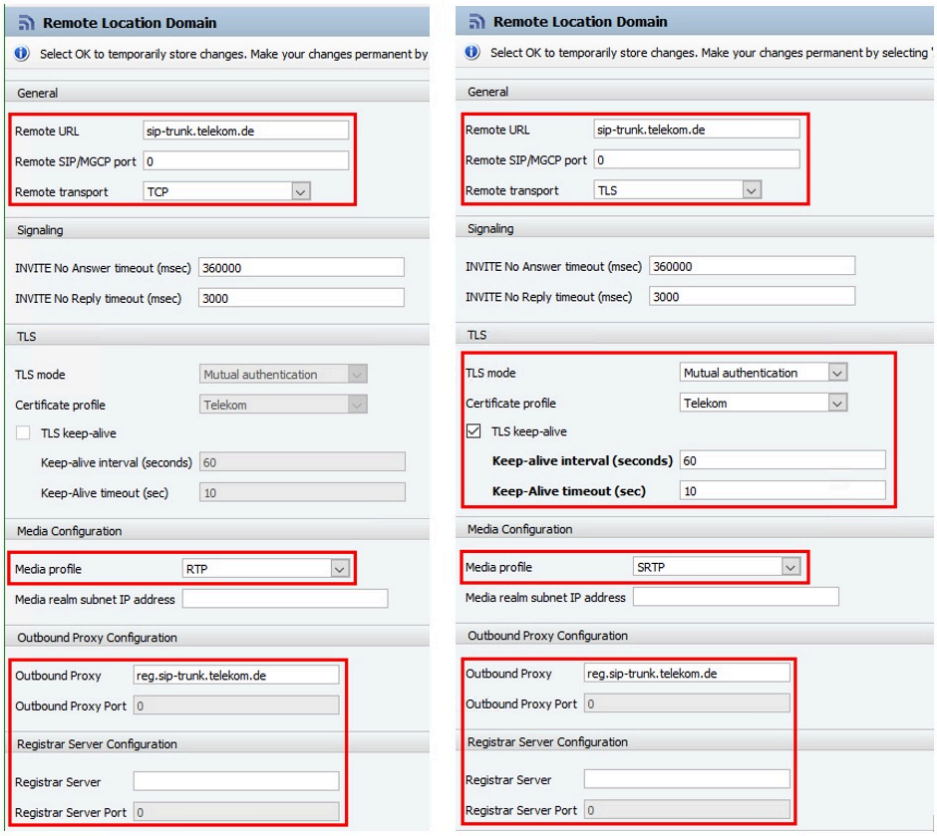

SIP Service Provider Profile
Select OK to temporarily store changes. Make your changes permanent by selecting 'Apply Changes' on the General page.
General
Name
DTAGTSystems
Default SSP profile
DTAG/NGN Registration Mo
Use SIP Service Address for all identity headers
SIP service address
sip-trunk.telekom.de
SIP User Agent
SIP User Agent towards SSP
Passthru
SIP User Agent
Registration
Registration required
Registration interval (sec)
480
Business Identity
Business identity required
Business identity DN
Outgoing SIP manipulation
Insert anonymous caller ID for blocked Caller-ID
Manipulation
Flags
FQDN in TO header to SSP
Use To DN to populate the RURI
Send Default Home DN in Contact for Call messages
Allow SDP changes from SSP without session version update
Do not send INVITE with sendonly media attribute
Do not send INVITE with video media line
Do not send Invite without SDP
Do not send Re-Invite when no media type change
Do not send Re-Invite
Remove Silence Suppression parameter from SDP
Enable pass-through of Optional parameters
Force direction attribute to sendrcv
Send default Home DN in PAI/PPI
Preserve To and From headers per RFC2543
Allow single SSP with different home DN prefix based handling
Ignore last digit in Default home DN for incoming calls from SIP trunk
TLS
TLS Signaling
Endpoint Config
Sip Connect
Use tel URI
Send user=phone in SIP URI
Registration mode
1TR118

In the Remote Endpoint Configuration window the SIP Service Provider Profile shown above has to be selected:



If a NAT router is in between SBC and SIP Trunk Open external firewall pinhole must be enabled so OpenScape SBC will open the RTP port on the NAT router by sending UDP packets to let the NAT router pass RTP packets from a PSTN phone.

The figures below show the Remote Location Domain window for an unencrypted SIP trunk using TCP and RTP on the left and for an encrypted SIP trunk using TLS and SRTP on the right:



5. Preparing and Installing TLS Certificates

For using TLS and SRTP over the SIP trunk uploading and configuration of the TLS certificates on OpenScape SBC is required:

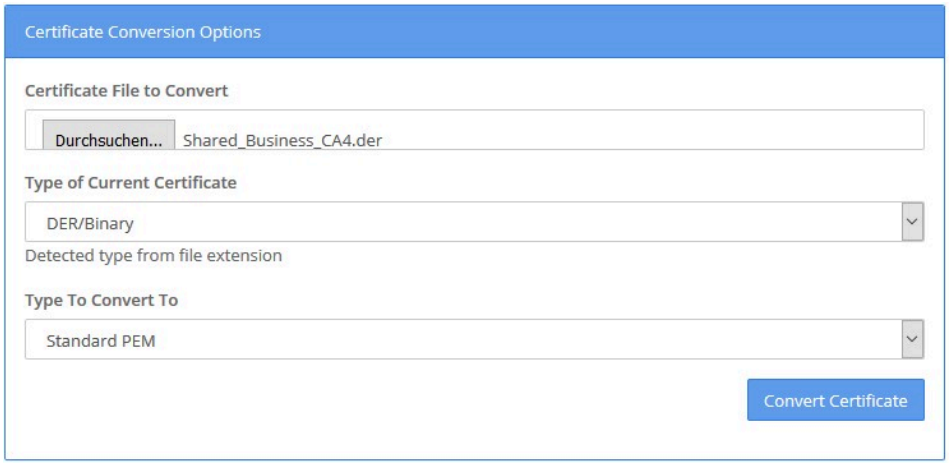
- Download the Telekom *Root-CA-Certificate* **T-TeleSec GlobalRoot Class 2** from URL:
- https://www.telesec.de/assets/downloads/PKI-Repository/T-TeleSec_GlobalRoot_Class_2.cer

---

NOTICE: Please make sure that the certificates are still valid. In case they are expired or not available anymore, please contact Telekom Deutschland GmbH or use the ones from the public websites.

Because the OpenScape SBC supports only certificates in pem format the Telekom *‚Shared Business CA'* certificate Shared_Business_CA4.der has to be converted

- via Linux shell e.g. on the OpenScape SBC via command
- openssl x509 -inform der -in Shared_Business_CA4.der -out Shared_Business_CA4.pem
- or via e.g. online converter https://www.sslshopper.com/ssl-converter.html



Click on *Convert Certificate* and save the converted certificate with file extension .pem.

Create in the next step a chained certificate based on the certificates Deutsche Telekom Root CA 1 and Shared Business CA named e.g. dt-chain-ca.pem and copy the content of this certificate files into it in the following order:

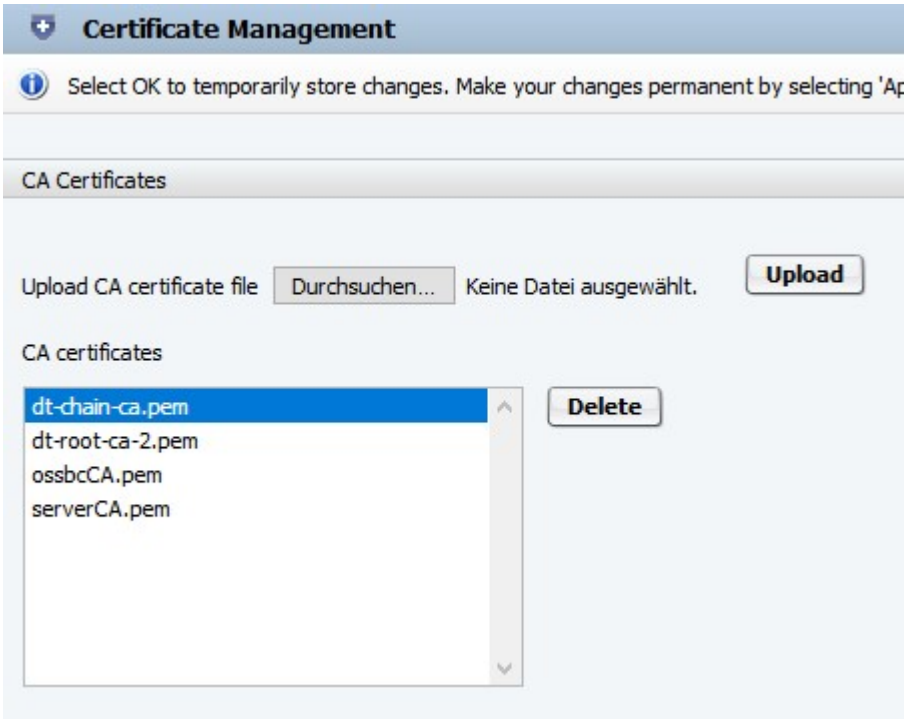
Because the OpenScape SBC supports only certificates in pem format, the Telekom "Shared Business CA" certificate T-TeleSec_GlobalRoot_Class_2.cer has to be converted via Linux shell. For example, on the OpenScape SBC run the command:

openssl x509 -inform der -in T-TeleSec_GlobalRoot_Class_2.cer -out T-TeleSec_GlobalRoot_Class_2.cer.pem

---

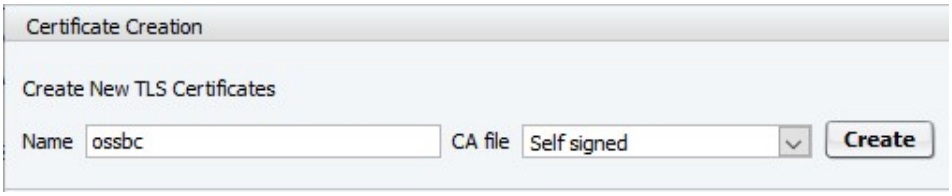
NOTICE: For more information, please refer to the OpenScape SBC V10 Configuration Guide.

Then upload this certificate via GUI at Security -> General -> Certificate Management into OpenScape SBC in the in section CA Certificates by selecting this certificate and clicking on Upload. Then the certificate appears in the CA certificates list:



To replace the OpenScape SBC default certificates provided by installation execute the following steps:

In Certificate Creation section enter e.g. ossbc in the Name field an click on *Create* leaving Self signed as CA file unchanged:



In the *CA certificates*, *X.509 Certificates* and *Key files* windows appears now the new certificates:

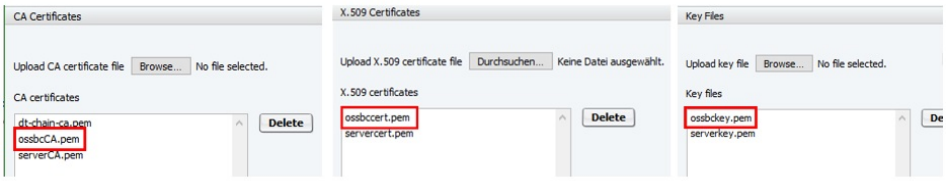


Figure 265: In the *Certificate Profiles* section click on *Add*:

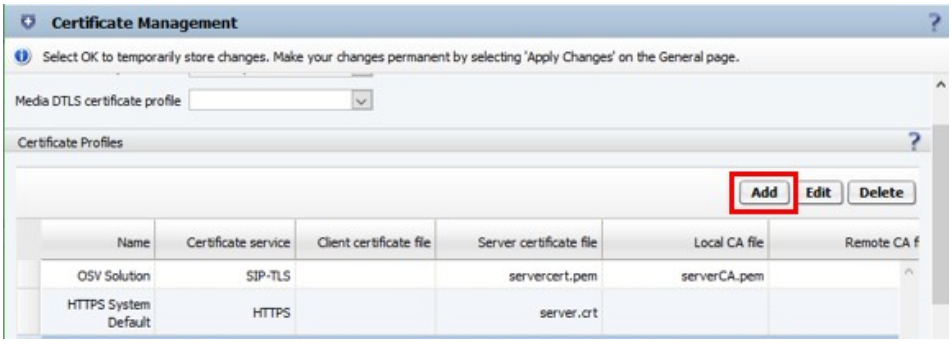
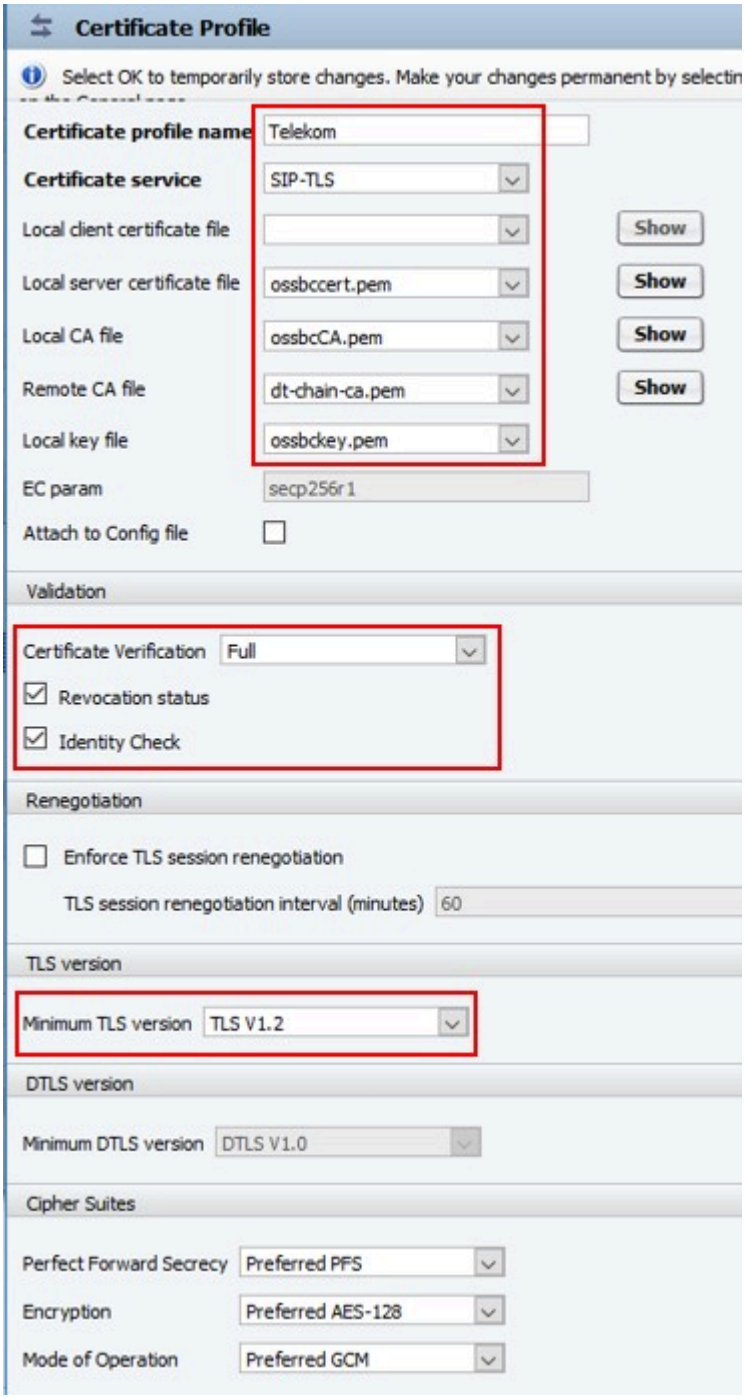


Figure 266: Create a new Certificate Profile selecting the certificates created before:



Finally the created Certificate Profile has to be configured in the *Remote Location Domain* window:

6.Configuration of VOIP Settings towards OS4K

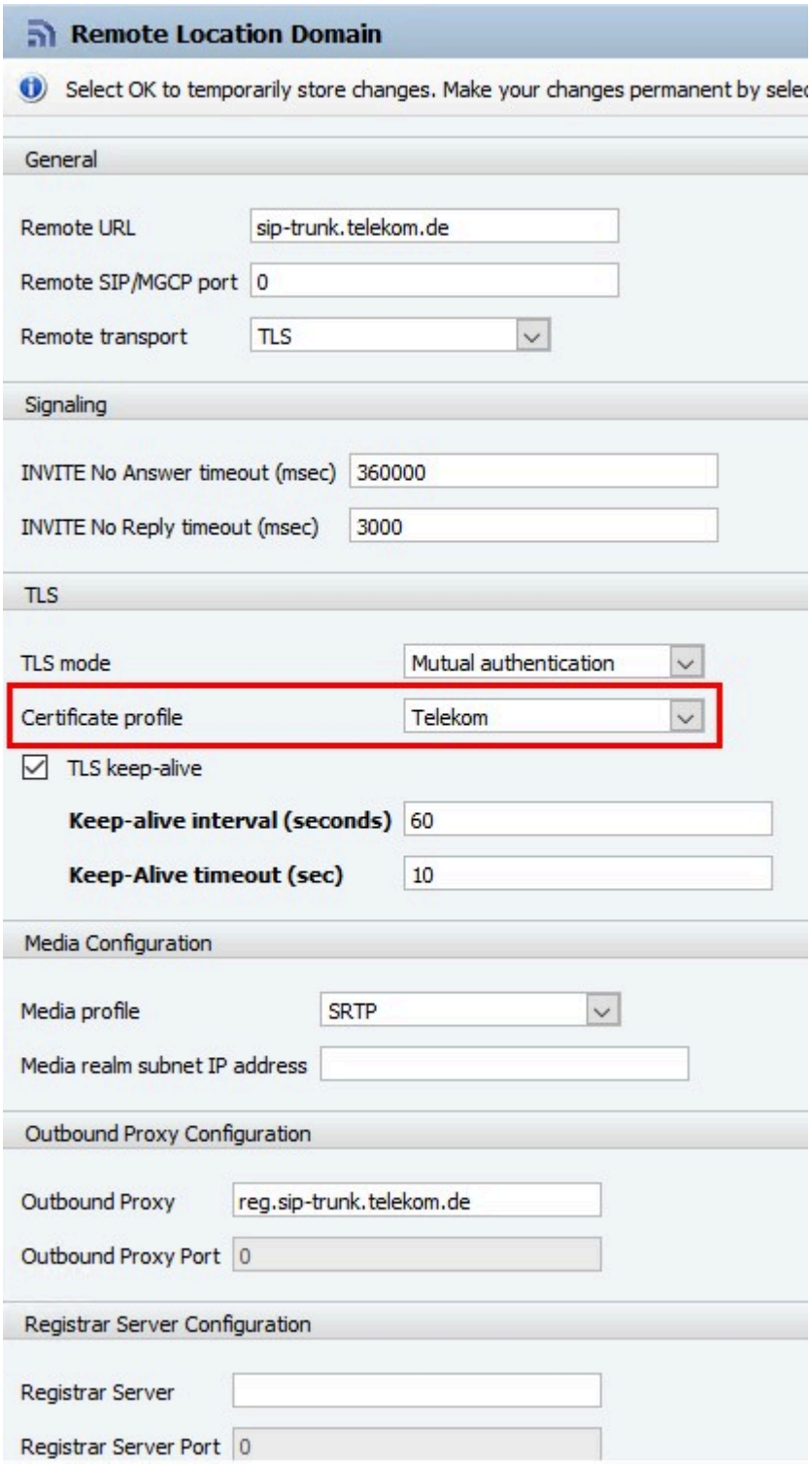
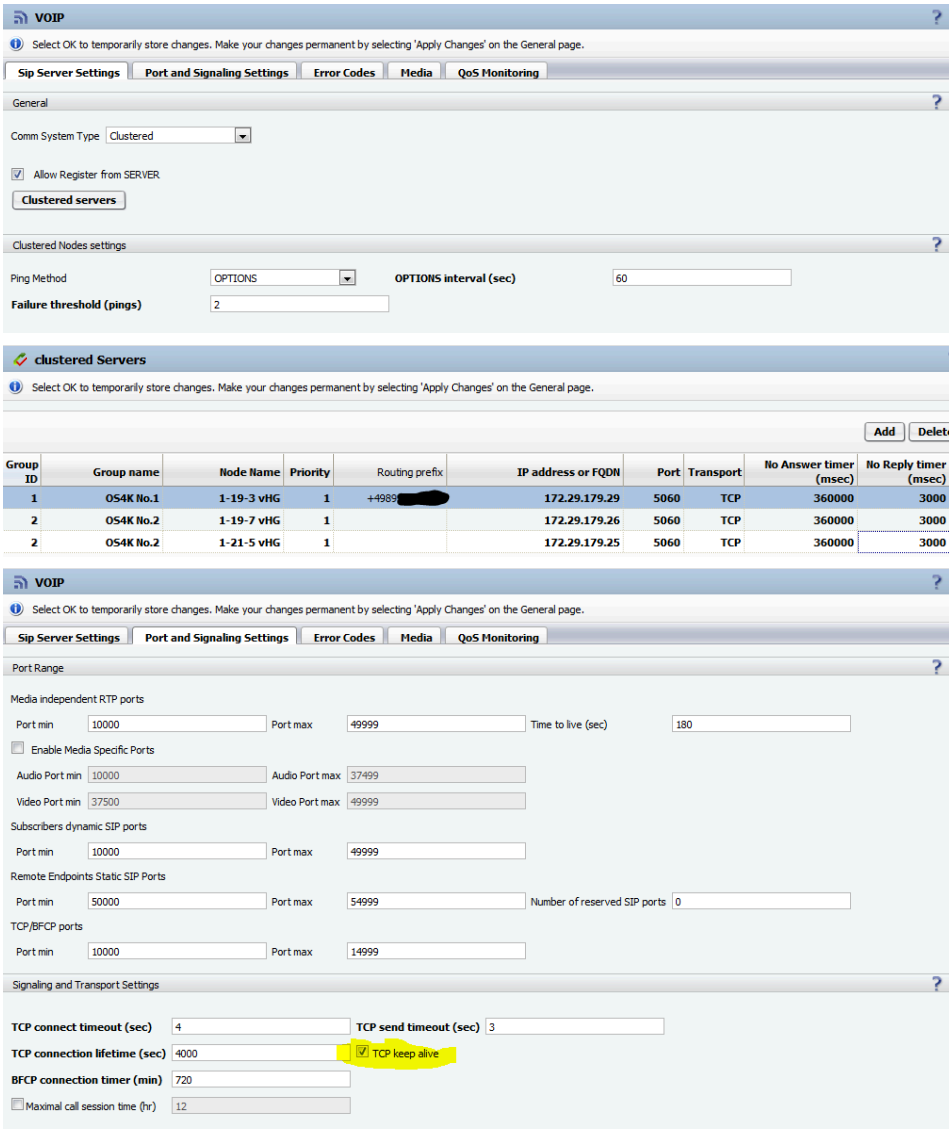
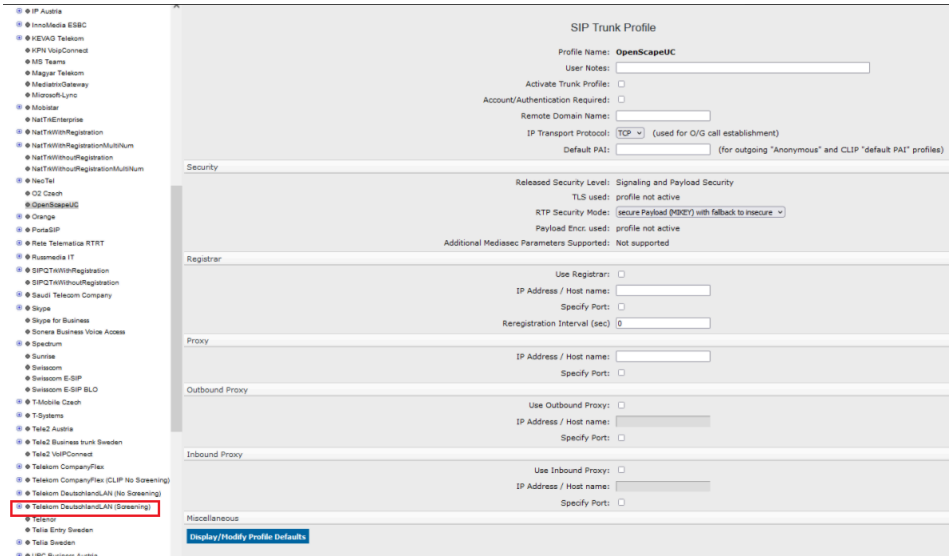


Figure 267: Configuration of VOIP Settings towards OS4K

(Example is using Non-Secure TCP, in case of Secure TLS please adapt accordingly e. g. 5061)



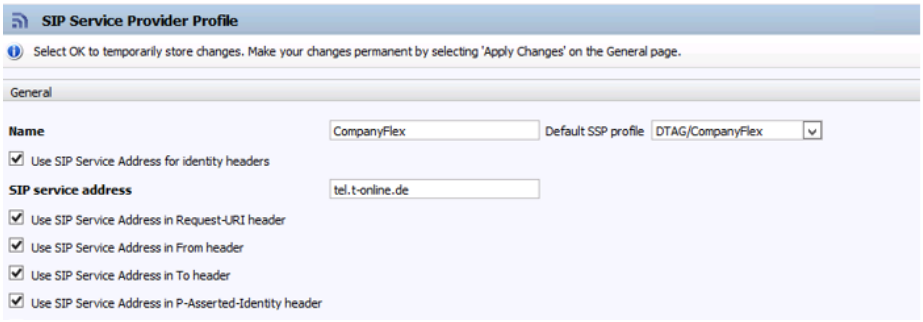
7. OS4K Gateway configuration (OpenScape SBC Core IP = 172.29.179.80)
(Example is using Non-Secure TCP, in case of Secure TLS please adapt accordingly to use TLS Ports etc)



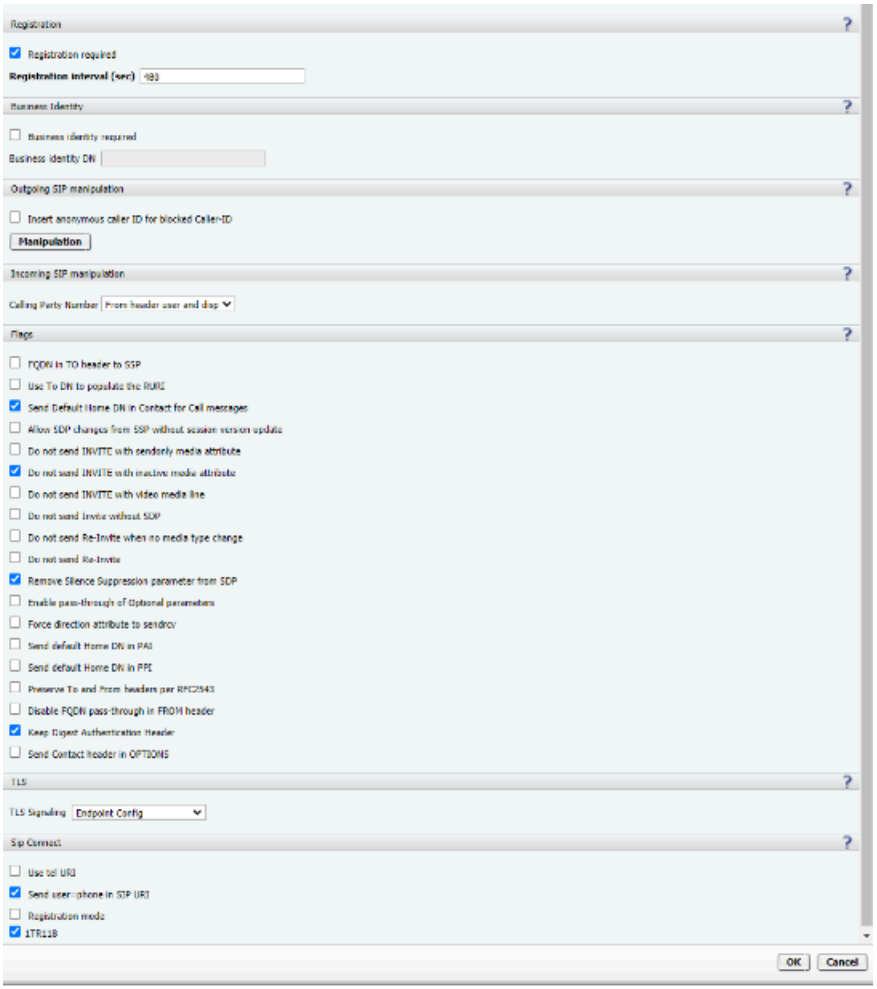
14.5.5.6 Configuration Example OpenScape SBC (CompanyFlex)

The SBC is similar to the configuration of the DeutschlandLAN SIP trunk.

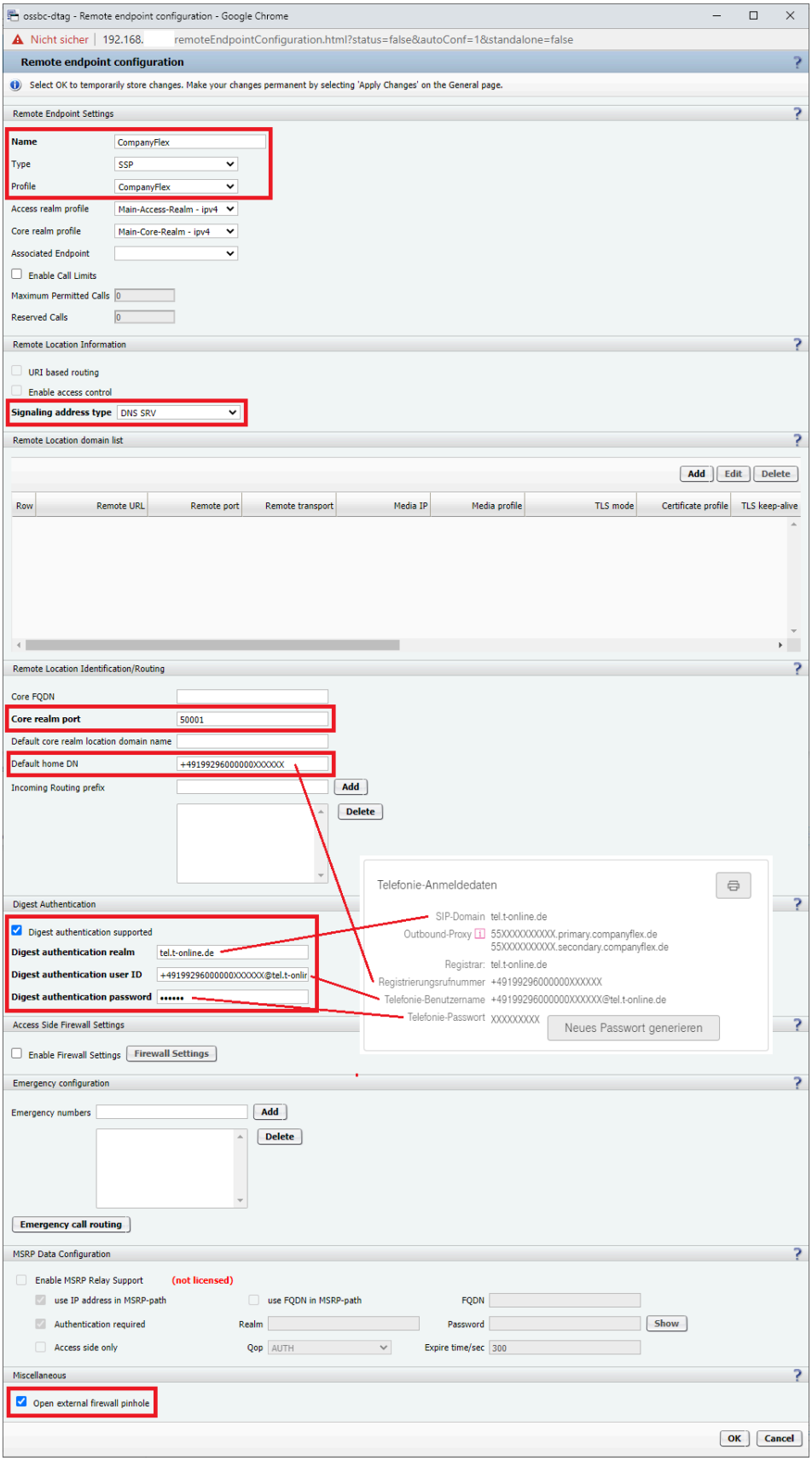
There is an own profile for CompanyFlex:

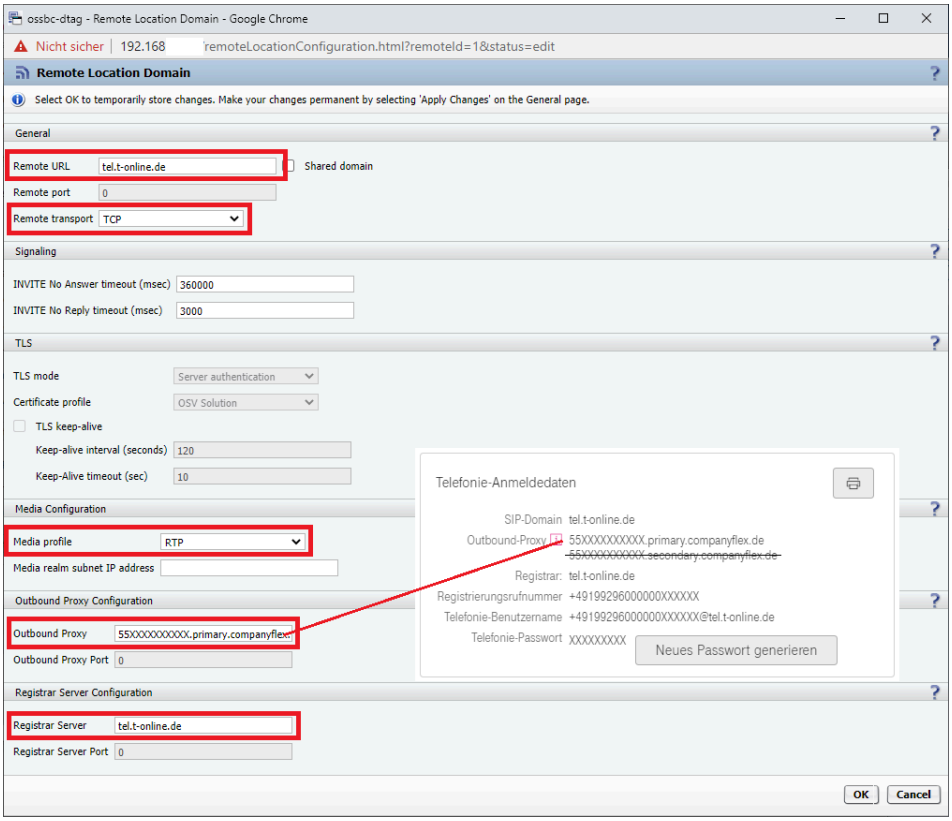


„Use SIP Service Address for identity headers“ has to be set manually.



Example „Remote Endpoint Configuration” and „Remote Location Domain“ configuration (unencrypted communication TCP/RTP):


ossbc-dtag - Remote endpoint configuration - Google Chrome
Nicht sicher | 192.168. remoteEndpointConfiguration.html?status=false&autoConf=1&standalone=false
Remote endpoint configuration
Select OK to temporarily store changes. Make your changes permanent by selecting 'Apply Changes' on the General page.
Remote Endpoint Settings
Name CompanyFlex
Type SSP
Profile CompanyFlex
Access realm profile Main-Access-Realm - ipv4
Core realm profile Main-Core-Realm - ipv4
Associated Endpoint
Enable Call Limits
Maximum Permitted Calls 0
Reserved Calls 0
Remote Location Information
URI based routing
Enable access control
Signaling address type DNS SRV
Remote Location domain list
Add Edit Delete
Row Remote URL Remote port Remote transport Media IP Media profile TLS mode Certificate profile TLS keep-alive
Remote Location Identification/Routing
Core FQDN
Core realm port 50001
Default core realm location domain name
Default home DN +4919929600000XXXXXX
Incoming Routing prefix
Add
Delete
Telefonie-Anmeldedaten
SIP-Domain tel.t-online.de
Outbound-Proxy 55XXXXXXXXX.primary.companyflex.de
55XXXXXXXXX.secondary.companyflex.de
Registrar: tel.t-online.de
Registrierungsrufnummer +4919929600000XXXXXX
Telefonie-Benutzername +4919929600000XXXXXX@tel.t-online.de
Telefonie-Passwort XXXXXXXXX
Neues Passwort generieren
Digest Authentication
Digest authentication supported
Digest authentication realm tel.t-online.de
Digest authentication user ID +4919929600000XXXXXX@tel.t-onlir
Digest authentication password
Access Side Firewall Settings
Enable Firewall Settings Firewall Settings
Emergency configuration
Emergency numbers
Add
Delete
Emergency call routing
MSRP Data Configuration
Enable MSRP Relay Support (not licensed)
use IP address in MSRP-path
use FQDN in MSRP-path
FQDN
Authentication required
Realm
Password
Show
Access side only
Qop AUTH
Expire time/sec 300
Miscellaneous
Open external firewall pinhole
OK Cancel



14.5.5.7 FAQ

Telekom Deutschland GmbH (TDG) - DeutschlandLAN SIP-Trunk

Q: Which setups are supported and preferred by TDG? A: All Setups listed in above documentation are supported. For OS4K versions <V7R2 a TDM solution is provided by TDG. The TDG Router registers via SIP to TDG, but connects to the OS4K using S2M/S0. Preferred setup from TDG is to connect an STMIX/ STMIY/STMI or SoftGate directly with the Certified TDG Routers => Drive the “ALL IP” Rollout

Q: Is NAT supported or DMZ mandatory? A: Both setups are supported with TDG. Due to a special logic the TDG backend/CO is checking if a NAT IP address is used. If yes, then the TDG backend/CO recognizes and sends the payload accordingly.

Q: Is there a special configuration necessary for DeutschlandLAN SIP-Trunk? A: Yes, beside the predefined SIP Profile which needs to be used, also some special rate numbers must be explicitly configured in LCR of OS4K. These must be sent in Subscriber & National type of number format e. g. 110 or 112. Further some default payload settings need to be changed. Please refer to chapter 4.5.3 “Configuration” for a detailed description.

Q: Are secure calls (TLS) supported for DeutschlandLAN SIP-Trunk? A: Yes, supported for STMIX/STMIY and SoftGate. TDG supports SDES Only. STMI supports TCP/UDP & RTP.

Q: Which is the preferred connectivity mode – registration or static? A: In the end it comes down to the network or your needs. Both modes have pros

& cons. In case of easiness and NAT, the registration mode might have advantages. In case of fixed host/ip the static mode might be practical.

14.5.6 Near-end NAT support for SG vHG boards

Near-end NAT support can be activated per SG vHG SIP board using AMO-CGWB: WPUBIP parameter:

- WPUBIP = 0.0.0.0 indicates that near-end NAT support is not active
- WPUBIP = <valid IPv4 internet address> activates near-end NAT support for the specified vHG board

Near-end NAT support can be combined with separated WAN/DMZ network configuration:

- USEWANIF=YES indicates that vHG board is connected to the DMZ firewall via separated WAN/DMZ network
- USEWANIF=NO indicates that shared LAN/DMZ network is used.

Near-end NAT feature supports both TRADITIO as well as SECURE SIP trunks.

SG vHG board can be configured to host SIP SRS (Secure Remote Subscriber) functionality together with Near-end NAT SIP trunk if USEWANIF=YES is active.

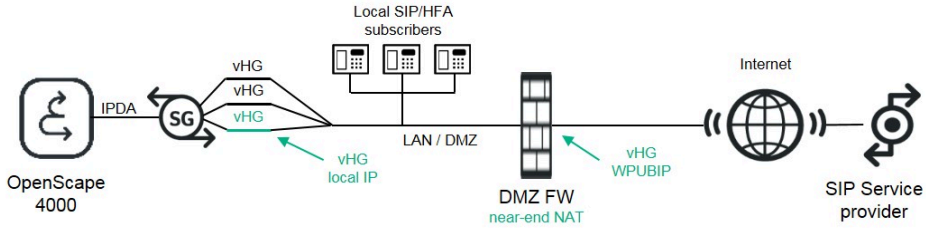


Figure 268: Dedicated SG vHG SIP trunk board with configured near-end NAT - common LAN/DMZ between vHG and DMZ firewall

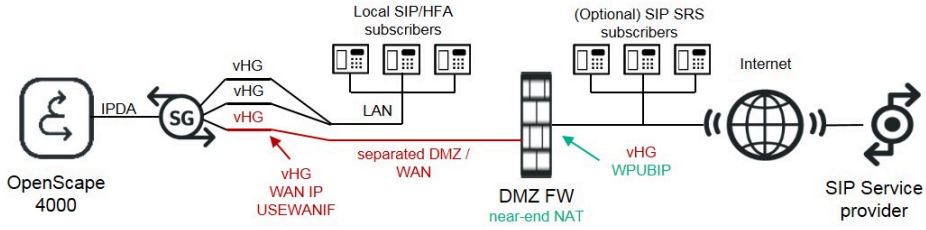


Figure 269: Dedicated SG vHG SIP trunk board with configured near-end NAT and WANIF (optionally combined with SIP SRS subscriber functionality)

14.5.6.1 AMO-CGWB configurations

1) Dedicated SG vHG SIP trunk board with configured near-end NAT - common LAN/DMZ between vHG and DMZ firewall

```
ADD-CGWB:LTU=<ltu>,SLOT=<vHG_slot>,SMODE=NORMAL,IPADR=<local_vHG_IP>,NET►
MASK=<netmask>,USEWANIF=NO;
CHANGE-CGWB:MTYPE=CGW,LTU=<ltu>,SLOT=<vHG_slot>,TYPE=GLOBIF,WPUBIP=<external_in►
ternet_IP_address>;
```

It is additionally recommended to de-activate DMC and SMP on the board:

```
CHANGE-CGWB:MTYPE=CGW,LTU=<ltu>,SLOT=<vHG_slot>,TYPE=DMCDATA,DMCCO▶
NN=0,SMP=NO,SMP4OSV=NO;
```

1) Dedicated SG vHG SIP trunk board with configured near-end NAT and WANIF (optionally combined with SIP SRS subscriber functionality)

```
ADD-CGWB:LTU=<ltu>,SLOT=<vHG_slot>,SMODE=NORMAL,IPADR=<WAN_vHG_IP>,NETMASK=<net▶
mask>,USEWANIF=YES;
CHANGE-CGWB:MTYPE=CGW,LTU=<ltu>,SLOT=<vHG_slot>,TYPE=GLOBIF,WPUBIP=<external_in▶
ternet_IP_address>;
```

It is additionally recommended to de-activate DMC and SMP on the board:

```
CHANGE-CGWB:MTYPE=CGW,LTU=<ltu>,SLOT=<vHG_slot>,TYPE=DMCDATA,DMCCO▶
NN=0,SMP=NO,SMP4OSV=NO;
```

And also management IP address from the LAN:

```
CHANGE-CGWB:MTYPE=CGW,LTU=<ltu>,SLOT=<vHG_slot>,TYPE=MANLANIF,MIPADR=<local_vH▶
G_mngmt_IP>,
;
```

14.5.7 SIP trunks with near-end destination NAT (STMIX/STMIY)

14.5.7.1 Important Information

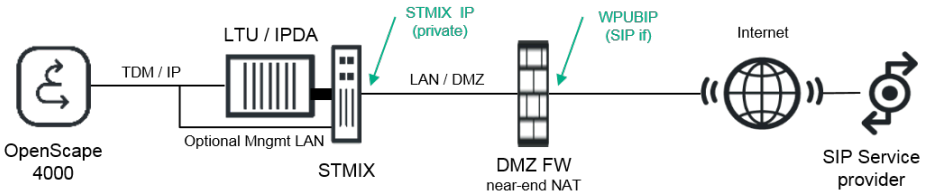
Originally there was no possibility to use “WAN Public IP” on STMIX/STMIY as there was no option to define a dedicated WAN interface. Therefore WPUBIP and USEWANIF parameters of CGWB AMO commands were dependent on each other. Splitting the functionality into two independent parameters brought us a benefit of employing Near-end NAT on STMIX/STMIY board (with limited number of interfaces or as multiple-feature with local HFA subscribers and SIP trunk) or on SoftGate. Near-end NAT is mainly requested in scenarios with SIP trunk between OpenScape 4000 and PSTN provider.

WPUBIP is detached local IP address used for SIP protocol and local media (= near-end destination NAT support).

USEWANIF activates additional firewall security (relevant for Softgate only), enforcing subscriber security (CIPHER) and activating support for far-end (home based) NAT bypass (SIP@Home subscribers)

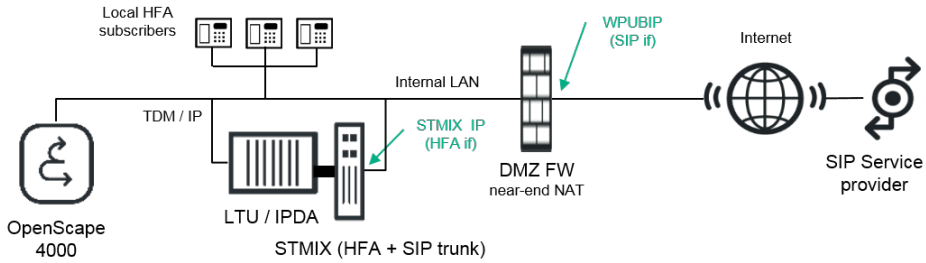
Supported configurations:

- Dedicated STMIX/STMIY for SIP trunk connectivity to PSTN provider placed in local network or DMZ with (optional) near-end NAT to the internet. I. e. WPUBIP is (optionally) configured to public IP address visible from internet.



- MFS STMIX/STMIY configuration supporting SIP trunk connectivity to PSTN provider over (optional) DMZ firewall with near-end NAT and locally connected HFA subscribers. I.e. WPUBIP is configured. The STMIX/STMIY

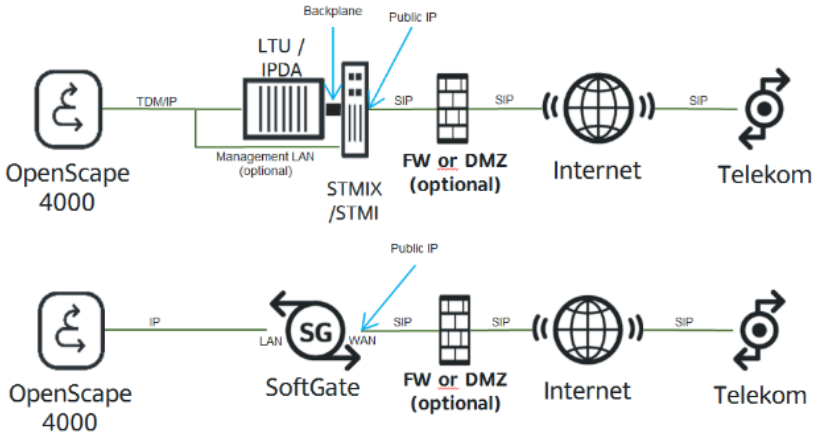
cannot support local SIP/UFIP subscribers and SIP trunk using Near-end NAT in parallel way because there is just one SIP interface bound to external public IP address.



- SIP@Home subscribers connected to STMIX/STMIY are NOT supported because USEWANIF=YES or NO is without any effect on STMIX/STMIY. Therefore additional security as well a far-end home base NAT support cannot be activated on STMIX/STMIY.

The feature does not define any new security requirements and does not require any changes in supported LAN configuration on STMIX/STMIY. AMO commands and interface between RMX and GW are not affected.

Original STMIX/STMIY/STMI/SoftGate configuration - Public IP is either in local network or in DMZ:



14.5.7.2 Configuration options

The two parameters should be set via AMO CGWB:

- AMO CGWB: TYPE=GLOBIF, **WPUBIP**=<near-end NAT public IP address>
- AMO CGWB: TYPE=GLOBIF, **USEWANIF**=<YES/NO> (optionally configurable to support far-end home base NAT for SIP@Home subscribers)
-

  NOTICE: This AMO command is relevant for SoftGate only, resp. vHG3500 board in SoftGate. For real GWs - i.e. STMI, STMIX/STMIY - this parameter is not allowed to be changed by AMO command. Its default value is "NO".

14.5.8 Multisite emergency calls via centralized SIP trunk

It is possible to install SIP trunks only at the main site and route all calls from the branch offices through the main sites SIP trunks. In order to route emergency calls to the correct PSAP, the SIP carrier must know the origin of the emergency call.

Some SIP providers (e.g.Vodafone) require to register at least one SIP trunk per branch office. This allows the carrier to determine the origin of the emergency calls.

OpenScape 4000 must route emergency calls originating in branch offices to the SIP trunk assigned to the branch office.

The OpenScape SBC solution is used to connect to the SIP carrier, which allows to administrate multiple SIP trunks to the carrier, e.g. one trunk per branch office.

These native SIP trunks are linked to core ports at the SIP interface towards the OpenScape 4000 SIP Gateways.

Example:

SIP trunk 1 is assigned to branch office A. SIP trunk 2 is assigned to branch office B.

Core port 50000 of the SBC is linked to Central Office trunk 1. Core port 50001 of the SBC is linked to Central Office trunk 2.

OpenScape 4000 routes emergency calls originating in branch office A to the SBC core port 50000. OpenScape 4000 routes emergency calls originating in branch office B to the SBC core port 50001.

OpenScape 4000 with its LCR Routing capabilities provides this functionality.

The corresponding core ports need to be set in AMO GKREG. See an example below.

```
ADD-
GKREG:GWNO=99,GWATTR=EXTGW&HG3550V2&SIP,GWIPADDR=10.140.102.208,
GWDIRNO=701,DIPLNUM=0,DPLN=0,LAUTH=1,INFO="TRUNK_MULTI",
SECLEVEL=TRADITIO,PORT=50000;
ADD-
GKREG:GWNO=100,GWATTR=EXTGW&HG3550V2&SIP,GWIPADDR=10.140.102.208,
GWDIRNO=702,DIPLNUM=0,DPLN=0,LAUTH=1,INFO="TRUNK_MULTI",
SECLEVEL=TRADITIO,PORT=50001;
```

14.5.9 Emergency Calls

In case of emergency calls, the SIP PAI header and Call Geolocation information (received via Native SIP or system generated with AMO LIN) are handled via the **SIP Provider** profile (Modify Profile Defaults), by changing the **Emergency Call Behaviour** and/or **Call Geolocation (RFC 6442)** parameter from "No modification"/ "Do not send location information for any call" to one of the values displayed in the figures below.

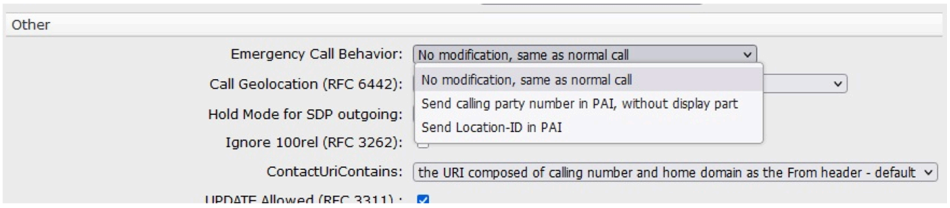


Figure 270: Change of the Emergency Call Behavior parameter

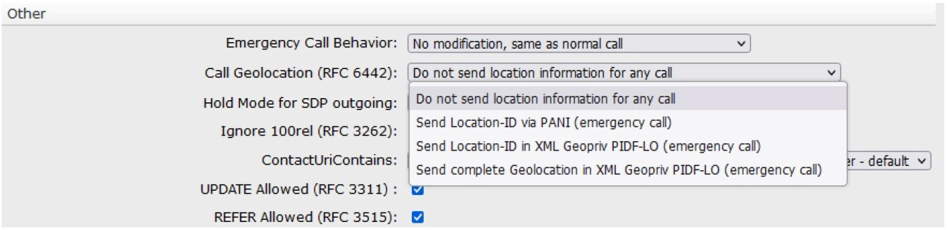


Figure 271: Change of the Call Geolocation (RFC 6442) parameter

In case of Native SIP transit calls, the incoming SIP GW **Emergency Call Behavior/ Call Geolocation (RFC 6442)** settings should match the source system settings to allow forwarding, filtering or modifying all received information on the outgoing transit GW.

In case of transit Native SIP trunking with SMP active, the **EMCYRTT** (emergency route) RICHT parameter is ignored.

It is not possible to automatically determine the number type sent in the PAI header (whether it is a phone number or Location ID). In case of Native SIP transit calls, where the source system sends the Location ID in PAI, the removal is possible by changing the SIP profile of the OpenScape 4000 incoming transit Gateway. This way, the received PAI is replaced with the number received in the **FROM** header.

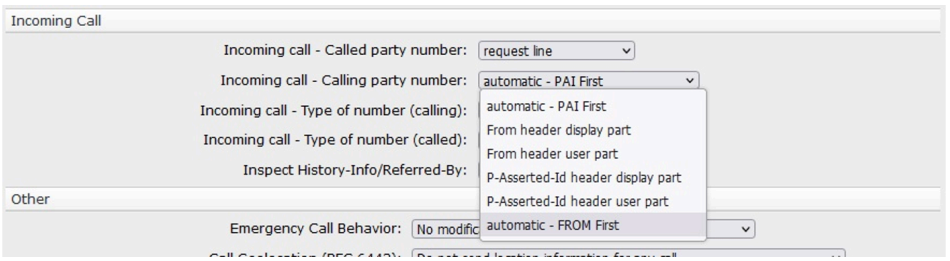


Figure 272: Change of Incoming call - Calling party number

14.6 Configuration of SIP-Q-Trunking / Native SIP Trunking

14.6.1 Configuration using AMOs

IMPORTANT: In addition to the AMO configuration, the trunking partner **must** be configured for a **native SIP trunk** or **can** be configured for a **SIP-Q trunk** in WBM using the SIP trunk profiles (see Section 3.3, “SIP Trunk Profiles”).

14.6.1.1 Trunking Protocol

The same protocols must always be set in the AMO CGWB and AMO GKREG.

Table 80: Protocols in the AMOs CGWB and GKREG

AMO CGWB	AMO GKREG	Protocol
TRPRSIP	SIP	native SIP
TPRSIPQ	SIPQ	SIP-Q V2

14.6.1.2 Configuring a HG 3500 as a Local Gateway

The following diagram shows a HG 3500 scenario for a fictitious customer in Frankfurt. It shows node 10-69-100 (Frankfurt-Bockenheim) and node 10-69-200 (Frankfurt-Sachsenhausen). Both systems have a common gateway board that should be configured as HG 3500. LEGK should be active on both systems (two local gateways). This constellation is relatively easy to explain because both nodes can be configured more or less symmetrically. The figure shows all necessary parameters. Node 10-69-100 is located in IP network 1.69.11.0/24 and node 10-69-200 is located in IP network 1.69.21.0/24. The networks reach each other over the routers Ra and Rb.

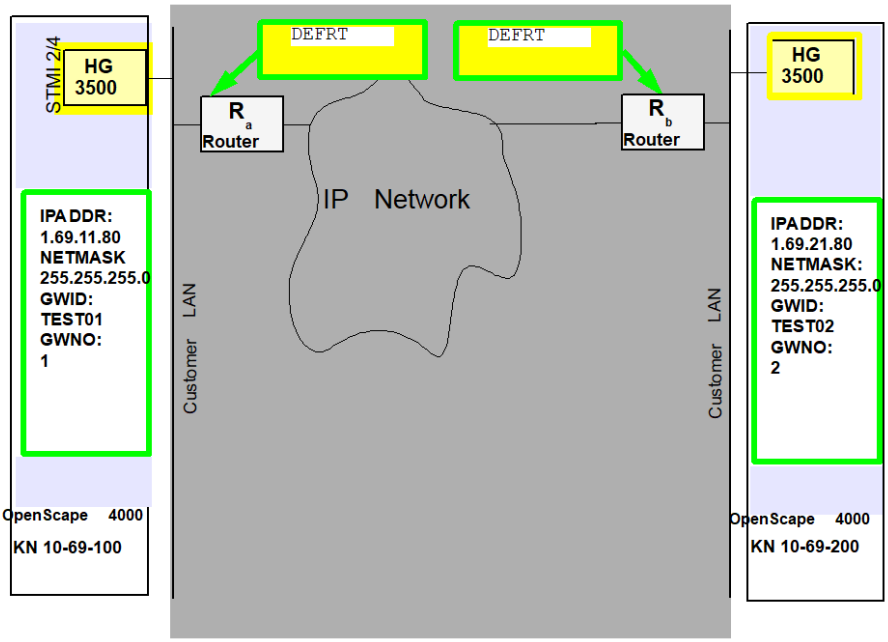


Figure 273: Configuration example: both nodes are LEGK

14.6.1.2.1 Configuration in Node 10-69-100

Start by configuring the board as HG 3500 in node 100. To avoid repeated restarts, do not insert the board until configuration is complete.

Step 0:

Configure LEGK in node 10-69-100.

```
CHANGE-ZANDE:TYPE=ALLDATA,GATEKPR=YES;
```

Step 1:

The Common Gateway Board Q2316-X is configured as HG 3500. Q2316-X is the version with 60 B channels. You can configure the board as a pure IP trunking board or in mixed operation with IP trunking and LAN connectivity (WAML) and many other features.

Configuration of the board for IP trunking only:

```
ADD-BFDAT:FCTBLK=1,FUNCTION=HG3550,BRDBCHL=BCHAN60&BCHAN120;
CHANGE-BFDAT:CONFIG=CONT,FCTBLK=1,FUNCTION=HG3550,LINECNT=1,UNITS=3; /* 30 B
channels for HG3550 functionality (H323 trunking, SIP trunking, SIP subscriber)
CHANGE-BFDAT:CONFIG=OK,FCTBLK=1,ANSW=YES; /* Close the configuration
ADD-BCSU:MTYPE=IPGW,LN=1,LTU=1,SLOT=37,PARTNO="Q2316-X",FCTID=1,LWVAR="0",FCT►
BLK=1,BCHL3550=30,ALARMNO=0;
```

or

IP Trunking & WAML:

```
ADD-BFDAT:FCTBLK=1,FUNCTION=HG3550&WAML,BRDBCHL=BCHAN60&BCHAN120;
CHANGE-BFDAT:CONFIG=CONT,FCTBLK=1,FUNCTION=HG3550,LINECNT=1,UNITS=3; /* 30 B
channels for HG3550 functionality (IP trunking, SIP trunking, SIP subscriber)
CHANGE-BFDAT:CONFIG=CONT,FCTBLK=1,FUNCTION=WAML,UNITS,LINECNT=1; /* Board will
be configured with one circuit, i.e. 10 B channels for WAML
CHANGE-BFDAT:CONFIG=OK,FCTBLK=1,ANSW=YES; /* Close the configuration
ADD-BCSU:MTYPE=IPGW,LN=1,LTU=1,SLOT=37,PARTNO="Q2316-X   ",FCTID=1,LWVAR="0",FCT►
BLK=1,BCHL3550=30,BCHLWAML=10,ALARMNO=0;
```

Step 2:

The AMO CGWB allows the board to receive the IP address in the customer LAN (LAN1), the subnet mask and the protocol variant (H323A / SIP-Q / NONE (board is only configured for SIP subscribers).

IMPORTANT: Only one trunking protocol may be configured for each board! There are no restrictions on interworking with other functions!

```
ADD-CGWB:LTU=1,SLOT=37,SMODE=NORMAL,IPADDR=1.69.11.80,NETMASK=255.255.255.0,TR►
PRHSIPQ=10;/*10 B channels for SIP-Q trunking
```

or

```
ADD-CGWB:LTU=1,SLOT=37,SMODE=NORMAL,IPADDR=1.69.11.80,NETMASK=255.255.255.0,TR►
PRHSIP=10; /*10 B channels for native SIP trunking
```

=> 20 B channels remain for other functions

Step 3:

The default router is now set in the customer LAN:

```
CHANGE-CGWB:MTYPE=CGW,LTU=1,SLOT=37,TYPE=GLOBIF,DEFRT=1.69.11.254;
```

Step 4:

The HG 3500 boards are administered using one gateway number (**GWNO**). This number must also be unique.

```
CHANGE-CGWB:MTYPE=CGW,LTU=1,SLOT=37,TYPE=LEGKDATA,GWNO=1;
```

Step 5:

Configuration without authentication and without registration (default values in AMO CGWB.

```
CHANGE-CGWB:MTYPE=CGW,LTU=1,SLOT=37,TYPE=LEGKDATA,GWNO=1, REGEXTGK=NO;
```

SSA:

```
CHANGE-CGWB:MTYPE=CGW,LTU=1,SLOT=37,TYPE=SIPTRSSA,SIPREG=NO;
```

ERH:

```
CHANGE-CGWB:MTYPE=CGW,LTU=1,SLOT=37,TYPE=SIPTRERH,GWAUTREQ=NO;
```

IMPORTANT: The **SIPREG** and **REGEXTGK** parameters must always have the same value.

Step 6:

IMPORTANT: Multiple boards are permitted in one trunk group!

This step consists of several configuration commands. We need to set up the trunk group and circuit, via which the B channels between gateway and OpenScape 4000 are switched.

First you need a trunk group:

```
ADD-BUEND:TGRP=50,NAME="IP TRUNK GWID 1   ",NO=30,TRACENO=0, ACDTHRH=*, PRIO►
NO=2, TDDRFLAG=ON, GDTRRULE=0, ACDPMGRP=0, CHARCON=NEUTRAL;
```

A digital trunk is then required (AMO TDCSU). The device type is **HG3550IP** (for H323/H323A and native SIP/SIP-Q trunking). If you want to permit DMC, set **DMCALLWD=Y**. This is only possible when the partner system supports DMC.

```
ADD-TDCSU:OPT=NEW,PEN=1-01-037-0,COTNO=36,

COPNO=32,DPLN=0,ITR=0, COS=2,LCOSV=1,LCOSD=1,

CCTN="CIRCUIT from GW2",PROTVAR="ECMAV2",SEGMENT=8, ISDNIP=00,ISDN►
NP=0,TRACOUNT=31,SATCOUNT=MANY,

NNO=1-69-499,ALARMNO=12, COTX=36,CCHDL=SIDEA,CLASSMRK=EC&G711,

TCCID="IP RS",TGRP=50,SRCHMODE=DSC,INS=Y,DEV=HG3550IP,

BCHANNEL=1&&30,BCNEG=N,BCGR=1,LWPAR=0,DMCALLWD=YES;
```

If DMC has been activated for the native SIP-/SIP-Q trunking path, Voice Activity Detection should also be activated. Otherwise the same bandwidth is required for the master connection as for the slave connection!

```
CHANGE-CGWB:MTYPE=CGW,LTU=<ltu>,SLOT=<slot>,TYP=ASC,

PRIO=PRIO1,VAD=YES;
```

Otherwise the same bandwidth is required for the master connection as for the slave connection.

IMPORTANT: It is recommended to reset the board: `RESET-BSSU:ADDRTYPE=PEN,LTG=1,LTU=1,SLOT=37;`

IMPORTANT: The command CHANGE-FUNSU can prevent the complete reloading of the STMI board. Reloading is only necessary in the case of loadware changes. `CHANGE-FUNSU:PIT=FLASH,PARTNO="Q2316-X ",FCTID=2, ACTION=RESET;`

Step 7:

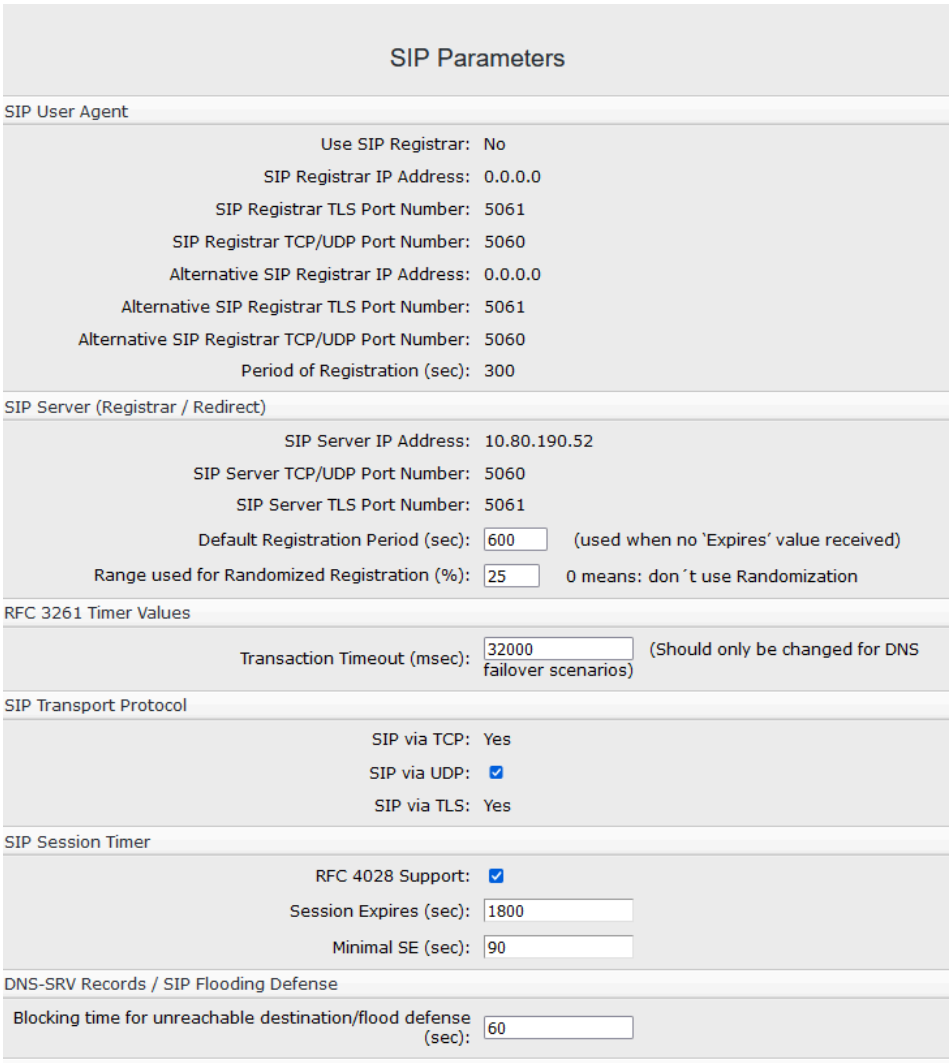
The LEGK must now still be informed about the existence of the HG 3500 gateway in the AMO GKREG. The **GWNO** must match the entry from the AMO CGWB. In the case of a local gateway, the AMO GKREG automatically loads the IP address (**IPADR**) from the AMO CGWB. You must also set the attributes **INTGW** (internal -local- gateway) and **HG3550V2** (version ID). The parameter **REGGW** is not necessary because the gateway does not have to register at another gateway.

`ADD-GKREG:GWNO=1,GWATTR=INTGW&HG3550V2&SIPQ or SIP,NUM=0,DPLN=0,LAUTH=1;`

If a local gateway is configured, **REGISTERED=NO** is always displayed with `DISPLAY-GKREG;`.

Step 8:

The same transport protocol (TCP, UDP) must be configured in all systems. The transport protocol used can be set with WBM under **Configuration** > **Voice Gateway** > **SIP Parameters**.



The HG 3500 board in node 10-60-100 is now configured properly and is communicating with the LEGK. However, the gateway is still missing in the partner node.

14.6.1.2.2 Configuration in Node 10-69-200

An LEGK should also be active in node 10-69-200. As the configuration procedures for nodes 10-69-200 and 10-69-100 are identical, this section only lists the appropriate AMO commands for the steps described above.

Step 0:

```
CHANGE-ZANDE:TYPE=ALLDATA,GATEKPR=YES;
```

Step 1:

```
ADD-BFDAT:FCTBLK=1,FUNCTION=HG3550,BRDBCHL=BCHAN60&BCHAN120;
CHANGE-BFDAT:CONFIG=CONT,FCTBLK=1,FUNCTION=HG3550,LINECNT=1,

UNITS=3; /* 30 B channels for HG3550 functionality (IP trunking, SIP trunking,
SIP subscriber)
CHANGE-BFDAT:CONFIG=OK,FCTBLK=1,ANSW=YES; /* Close the configuration
ADD-BCSU:MTYPE=IPGW,LN=1,LTU=2,SLOT=49,PARTNO="Q2316-X   ",
```

```
FCTID=1,LWVAR="0",FCTBLK=1,BCHL3550=30,ALARMNO=0;
```

Step 2:

```
ADD-CGWB:LTU=2,SLOT=49,SMODE=NORMAL,

IPADDR=1.69.21.80,NETMASK=255.255.255.0,TRPRHSIPQ=10;
ADD-CGWB:LTU=2,SLOT=49,SMODE=NORMAL,

IPADDR=1.69.21.80,NETMASK=255.255.255.0,TRPRHSIP=10;
```

Step 3:

```
CHANGE-CGWB:MTYPE=CGW,LTU=2,SLOT=49,TYPE=GLOBIF,DEFRT=1.69.21.254;
```

Step 4:

```
CHANGE-CGWB:MTYPE=CGW,LTU=2,SLOT=49,TYPE=LEGKDATA,GWNO=2;
```

Step 5:

```
CHANGE-CGWB:MTYPE=CGW,LTU=2,SLOT=49,TYPE=LEGKDATA,

GWNO=2,REGEXTGK=NO;
```

SSA:

```
CHANGE-CGWB:MTYPE=CGW,LTU=1,SLOT=49,TYPE=SIPTRSSA,SIPREG=NO;
```

ERH:

```
CHANGE-CGWB:MTYPE=CGW,LTU=2,SLOT=49,TYPE=SIPTRERH,GWAUTREQ=NO;
```

IMPORTANT: The **SIPREG** and **REGEXTGK** parameters must always have the same value.

Step 6:

```
ADD-BUEND:TGRP=50,NAME="IP TRUNK GWID 2 ",NO=30;
ADD-TDCSU:OPT=NEW,PEN=1-02-049-0,COTNO=36,

COPNO=32,DPLN=0,ITR=0, COS=2,LCOSV=1,LCOSD=1,

CCTN="CIRCUIT from GW2",PROTVAR="ECMAV2",SEGMENT=8,ISDNIP=00,

ISDNNP=0,TRACOUNT=31,SATCOUNT=MANY,NNO=1-69-499,

ALARMNO=12, COTX=36,CCHDL=SIDEA,CLASSMRK=EC&G711,TCCID="IP RS",

TGRP=50,SRCHMODE=DSC,INS=Y,DEV=HG3550IP,BCHANNEL=1&&30,BCNEG=N,BCGR=1,LW►
PAR=0(=Master),DMCALLWD=YES;
CHANGE-CGWB:MTYPE=CGW,LTU=<ltu>,SLOT=<slot>,TYP=ASC,PRIO=PRIO1,

VAD=YES;
```

Step 7:

The GKREG contains the configuration for both HG 3500 boards. Here, **GWNO=2** is now the local gateway in node 10-69-200 with the attributes **INTGW** and **HG3550V2** and **SIPQ/SIP**, while **GWNO=1** (the partner gateway

in node 10-69-100) contains the attributes **EXTGW**, **HG3550V2** and **SIPQ/SIP** in this system. The parameter **REGGW** is not necessary because the gateway does not have to register at another gateway.

```
ADD-GKREG:GWNO=1,GWATTR=EXTGW&HG3550V2&SIPQ or SIP,GWIPAD►
DR=1.69.11.80,DIPLNUM=0,DPLN=0,LAUTH=1;
ADD-GKREG:GWNO=2,GWATTR=INTGW&HG3550V2&SIPQ or SIP,DIPLNUM=0,DPLN=0,LAUTH=1;
```

14.6.1.2.3 Extension in Node 10-69-100

The HG 3500 in node 10-69-200 must be retrofitted in node 10-69-100 for LEGK (AMO GKREG). For node 10-69-100, this HG 3500 (**GWNO=2**) is an external gateway (attributes **EXTGW&HG3550V2&SIPQ/SIP**) and is not registered in node 10-69-100.

```
ADD-GKREG:GWNO=2,GWATTR=EXTGW&HG3550V2&SIPQ or SIP,GWIPAD►
DR=1.69.21.80,DIPLNUM=0,DPLN=0,LAUTH=1;
```

14.6.1.2.4 Call from Node 10-69-100 to Node 10-69-200

LCR should now be configured for node 10-69-100 in our example so that a station using open numbering (**UNKNOWN**) in this node can reach a station in node 10-69-200 over the IP trunk. Closed numbering or ISDN numbering plans are also supported and configured in the same way.

A station in node 10-69-100 reaches node 10-69-200 over the tie number 902.

```
ADD-WABE:CD=902,DAR=TIE;
```

LRTE 520 should route to node 10-69-200 and use trunk group 50 (see above):

```
ADD-RICHT:MODE=LRTENEW,LRTE= 520,LSVC=ALL,

NAME="IP TO KN 69 200",TGRP=50,DNNO=1-69-499;
```

The following is a simple outdial rule:

```
ADD-LODR:ODR=520,CMD=ECHO,FIELD=2;

ADD-LODR:ODR=520,CMD=END;

ADD-LODR:ODR=520,INFO="TIE TO GW2";
```

Enter **GW1=2-0** in LRTE 520 now. The **2** refers to the parameter **GWNO** in AMO GKREG (section Section 6.1.2.3, “Extension in Node 10-69-100”). In AMO GKREG for node 10-69-100, the HG 3500 with **GWNO=2** is the IP address 1.69.21.80. The **0** stands for the sector path number. Sector path 0 means there is unlimited bandwidth for this path. If the destination gateway is not reachable, you can use the parameters **GW2** to **GW5** to configure an alternative route.

```
ADD-LDAT:LRTE=520,LSVC=ALL,LVAL=1,TGRP=50,ODR=520,

LAUTH=1,GW1=2-0;
```

IMPORTANT: In contrast to S0/S2 connections (point-to-point), an IP connection is a point-to-multipoint connection and therefore the same trunk number is used to the different destination gateways (**GW1-GW5**) in the AMO LDAT!

The tie number is entered in the AMO LDPLN. The directory number is entered in the default dial plan with **DIPLNUM=0**. A profile index can also be used instead of LRTE (AMO-LPROF):

```
ADD-LDPLN:LCRCONF=LCRPATT,DIPLNUM=0,LDP="902"-"X",

LRTE=520,LAUTH=1;
```

If you want to be able to reach node 10-69-100 from node 10-69-200, perform the following configuration. You then point to the **GWNO=1** in AMO LDAT.

14.6.1.3 Backup & Restore of the WBM Configuration Data

All configuration data configured via the WBM of the board must be backed up using the backup server. Otherwise all configuration data will be lost after a board replacement, a reset of the board or loadware upgrade and the native SIP-/SIP-Q trunking connection cannot be automatically reestablished. This is done with the OpenScape 4000 Assistant > Backup & Restore.

It is important to ensure that the backup server can be reached. If the backup server is not available, the configuration data can also be saved in the flash memory of the board and then can be retrieved from there.

OpenScape 4000 Assistant > Backup & Restore

Configuration of a connection to backup server and OpenScape 4000 Assistant.

```
CHANGE-CGWB:MTYPE=CGW,LTU=1,SLOT=37,TYPE=MGNTDATA,

MGNTIP=<ip_address_assistant>,MGNTPN=<port_no_assistant>,

BUSIP=<ip_address_backup_server>,BUSPN=<port_no_backup_server>};
```

Note: The values for **MGNTPN** and **BUSPN** will not be restored after a reset of the board. They have to be configured again manually.

Local Flash

IMPORTANT: It is recommended to additionally use the local flash as a backup media. If the connection to the backup server is broken the configuration data will be automatically restored from the local flash.

WBM > Maintenance > Actions > (double-click) Automatic Actions > Saving Local Configuration for Upgrade

For more information please refer to "Gateways HG 3500 and HG 3575", Chapter 6, “Save Configuration Data in Local Flash ((local Backup & Restore)”.

IMPORTANT: If the restore is necessary (e.g. after an upgrade of the loadware) and the backup server cannot be reached during the startup phase, the board is loaded and put into operation with the default configuration. If the HBR server is then reachable, the restore is carried out afterwards and a reboot with the new configuration is triggered! An additional reboot is also triggered during the startup phase if configurations/data required for operation are restored (e.g. SPE certificates).

IMPORTANT: To avoid problems during upgrading/loadware swapping, a backup should be initialized after exchanging the board because the backup is associated with the MAC address.

14.6.1.4 Displaying Link Status

The link status of the LAN interface (link signal Ethernet, LAN speed, and LAN interface) can be displayed at each level with the AMO SDSU using the usual commands (**PERI1**, **PERI2,** and **PERI3**):

```
DISPLAY-SDSU:TYPE=PEN,LEVEL=PERI1,LTG=1,LTU=<ltu no>,

SLOT=<slot no>;
```

14.6.1.5 Procedure for Adding Supplementary HG 3500 Boards to the Network

Additional LEGKs can be configured in the same way as node 10-69-100. The AMO BFDAT, AMO BCSU, AMO CGWB, AMO GKREG and AMO LDAT are then in a single node.

IMPORTANT: The GKREG must recognize all HG 3500 boards in the network.

14.6.1.6 Relevant AMOs

AMO	Parameter	Sprache/ Language	Beschreibung/Description
BCSU	TYP=IPGW	d	CGW einrichten
	TYPE=IPGW	e	Configure CGW
	BKAN3550	d	Anzahl der B-Kanäle für IP-Trunking
	BCHL3550	e	Number of b channels for IP trunking
BFDAT	FUNCTION=HG3550	d	CGW mit IP-Trunking
	FUNCTION=HG3550	e	CGW with IP trunking
	BGBKAN	d	Maximale Anzahl der verfügbaren B-Kanäle der Baugruppe (entweder 60 oder 120)
	BRDBCHL	e	Maximum number of available b channels (60 or 120)
	ANZSATZ	d	Anzahl der Sätze für IP-trunking
	LINECNT	e	Number of lines for IP trunking
	ANZEINH	d	Anzahl der vordefinierten Blöcke mit ausgewählter Funktion pro Satz.
	UNITS	e	Defines the number of predefined blocks with the selected function per line.

AMO	Parameter	Sprache/ Language	Beschreibung/Description
CGWB	DEFRT	d	IP-Adresse des Default Routers
	DEFRT	e	IP address of the default router
	GWAUTREQ	d	Ziffern-Authentifizierung wird benötigt
	GWAUTREQ	e	Digest authentication is required
	GWREALM	d	Security Zone of the gateway
	GWREALM	e	Security Zone of the gateway
	GWRNR	d	Gateway Rufnummer
	GWDIRNO	e	Gateway Directory Number
	GWSECRET	d	Passwort des Gateways
	GWSECRET	e	Password of the gateway
	GWUSERID	d	User Identifizierung des Gateways
	GWUSERID	e	User identification of the gateway
	REGIP1	d	IP-Addresse des primären SIP Registrars
	REGIP1	e	IP address of the primary SIP registrar
	REGIP2	d	IP-Addresse des sekundären SIP Registrars
	REGIP2	e	IP address of the secondary SIP registrar
	PORTTCP1	d	Port Nummer für die primäre SIP Registrierung über TCP/UDP
	PORTTCP1	e	Port number of the primary SIP registration via TCP/UDP
	PORTTCP2	d	Port Nummer für die sekundäre SIP Registrierung über TCP/UDP
	PORTTCP2	e	Port number of the secondary SIP registration via TCP/UDP
	REGTIME	d	Zeit in Sekunden wie lange die SIP-Registrierung gültig ist
	REGTIME	e	Time in seconds the SIP registration is valid

AMO	Parameter	Sprache/ Language	Beschreibung/Description
	SIPREG	d	Gateway an einem SIP Registrar registrieren
	SIPREG	e	Register gateway at a SIP registrar
	TRPRSIP	d	Anzahl der B-Kanäke für Trunking-Protokoll SIP
	TRPRSIP	e	Number of b channels for trunking protocol SIP
	TRPRSIPQ	d	Anzahl der B-Kanäke für Trunking-Protokoll SIP-Q
	TRPRSIPQ	e	Number of b channels for trunking protocol SIP-Q
	TYP=SIPTRSSA	d	SIP Trunking Daten für SSA (SIP Stack Agent)
	TYPE=SIPTRSSA	e	SIP trunking data for SSA (SIP Stack Agent)
	TYP=SIPTRERH	d	SIP Trunking Daten für ERH (Endpoint Registration Handler)
	TYPE=SIPTRERH	e	SIP trunking data for ERH (Endpoint Regustration Handler)
	VAD	d	Voice Activity Detection
	VAD	e	Voice Activity Detection
GKREG	GWATTR	d	Gateway Attribut
	GWATTR	e	Gateway attribute
	GWNR	d	Gateway ID (muss dem Eintrag im AMO CGWB entsprechen)
	GWNO	e	Gateway ID (must correspond to the value in AMO CGWB)
TDCSU	DMCERL=NEIN	d	DMC wird verhindert
	DMCALLWD=NO	e	DMC not allowed
ZANDE	GATEKPR=JA	d	PBX mit Gatekeeper
	GATEKPR=YES	e	PBX with gatekeeper

14.6.2 Configuration with OpenScape 4000 Assistant

14.6.2.1 Configure Common Gateway HG 3500

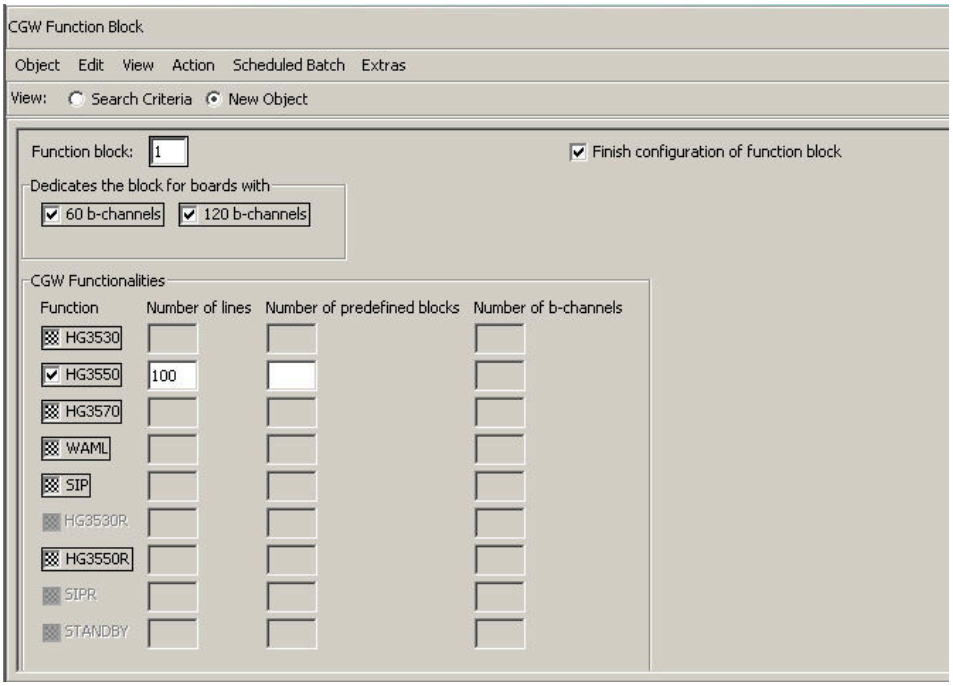
In order to configure a CGW board, you have to do the following:

- Step 1: Create function block
- Step 2: Search for a free slot
- Step 3: Open Board configuration menu in OpenScape 4000 Assistant
- Step 4: Add new board
- Step 5: Fill in the mask
- Step 6: Open STMI2-IGW Board Data dialog and fill mandatory fields

Step 1: Create function block

Start CM > System Data > Board > CGW Function Block

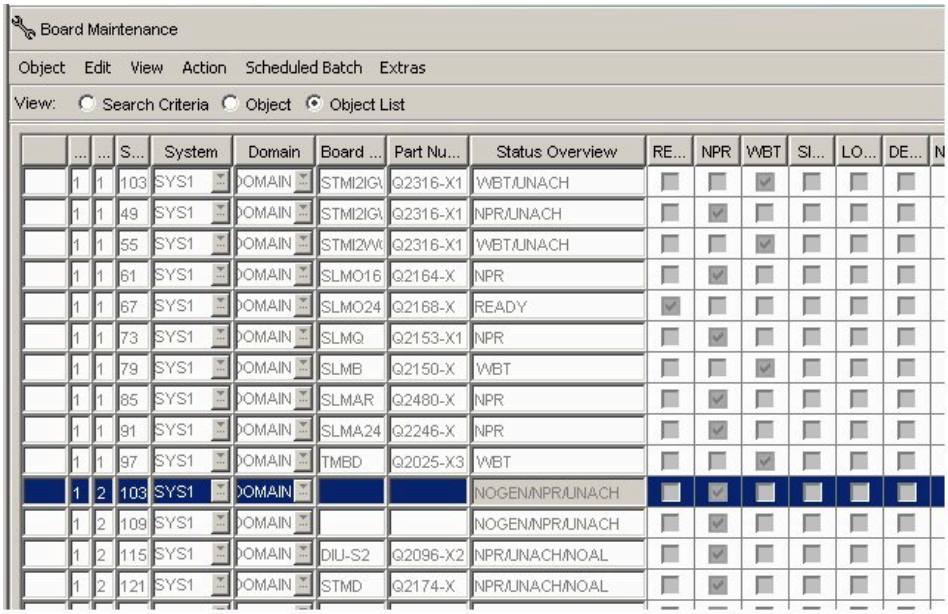
Click **Search** for searching for a free function block number. Click **New** for adding a new function block. Enter the required data and click **Save**.



Step 2: Search for a free slot

Before entering the LTU and SLOT number it is recommended to check if the desired SLOT is free. To do this call: **CM > System Data > Maintenance> Board Maintenance**.

Following the search in the object list view, free LTUs and SLOTs are marked with **NOGEN/NPR/UNACH** in the **Status Overview** column.



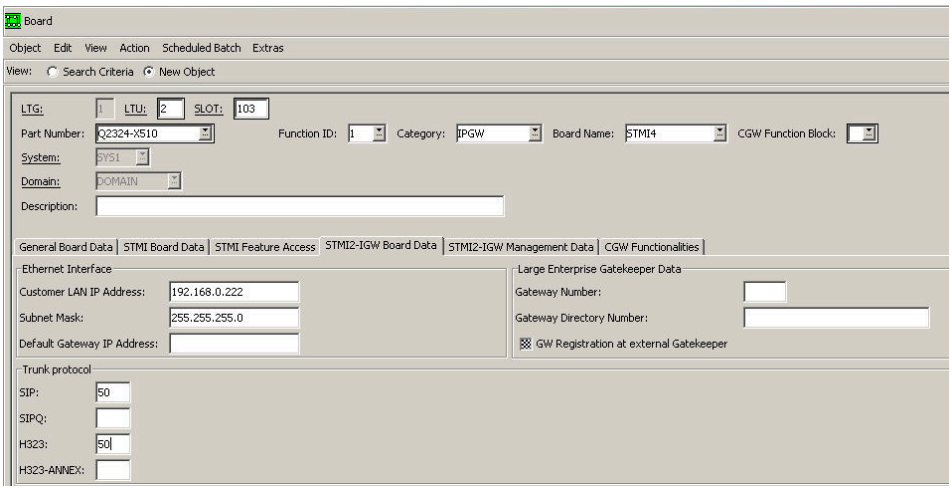
Step 3: Open Board configuration menu in OpenScape 4000 Assistant

CM > System Data > Board > Board

Step 4: Add new board

Press **New** button in order to add a new board.

Step 5: Fill in the mask



- **Part Number**: Q2316-X or Q2316-X10 or Q2324-X500 or Q2324-X510
- **Function ID**: is always 1
- **Category**: IPGW
- **Board Name**: STMI2, STMI4, STMIX or STMIY
- **CGW Function Block**: enter previously created function block for trunking (see Step 1: Create function block)
- **LTU** and **SLOT**: select a free slot (see Step 2: Search for a free slot)

Step 6: Open STMI2-IGW Board Data dialog and fill mandatory fields

Customer LAN IP Address and **Subnet Mask**.

Trunk Protocol: number of b-channels per protocol (e.g. **SIP/SIPQ**: 50).

IMPORTANT: Only one trunk protocol per board is supported! A combination of different trunking protocols on one board is not possible!

After all required data has been entered in the relevant fields, press the **Save** button.

The board is now added and can be found in **Board Dialog** or in **Board Maintenance**.

14.6.2.2 Delete IPGW

To delete an IPGW board, proceed as follows:

- Step 1: Open Board configuration menu in OpenScape 4000 Assistant
- Step 2: Search for IPGW
- Step 3: Select IPGW and delete it

Step 1: Open Board configuration menu in OpenScape 4000 Assistant

CM > System Data > Board > Board

Step 2: Search for IPGW

Search Criteria > Category: IPGW

Step 3: Select IPGW and delete it

Choose the board that has to be deleted from the list and click **Delete**. After pressing the **Delete** button, a message appears confirming deletion of the board from the system.

14.6.2.3 Modify Board Data of IPGW

In order to modify board data, follow these steps:

- Step 1: Open Board configuration menu in OpenScape 4000 Assistant
- Step 2: Select IPGW
- Step 3: Carry out desired changes
- Step 4: Check the changes

Step 1: Open Board configuration menu in OpenScape 4000 Assistant

CM > System Data > Board > Board

Step 2: Select IPGW

Select **IPGW** in the **Category** list and press the **Search** button.

Step 3: Carry out desired changes

Perform the necessary changes in the board dialog (e.g. IP address) and save the changes with the **Save** button.

After saving the changes, a dialog confirming the successful action pops up.

Step 4: Check the changes

Make a new board search in order to check if new data has been accepted.

14.6.3 Configuration using SIP Trunk Profiles in WBM

see Section 3.3.5, “Configuration of SIP Trunks with Registration”.

14.6.4 SIP-Q Trunking between OpenScape 4000 and OpenScape Voice

A connection between OpenScape 4000 and OpenScape Voice can be established using SIP-Q V2 trunks.

OpenScape Voice provides only a limited range of features over this connection. For details, please refer to the OpenScape Voice documentation.

The phone numbers between OpenScape 4000 and OpenScape Voice must be in **INTERNATIONAL** format.

14.6.4.1 Restrictions

- Dialing with overlapping digits is not supported in OpenScape Voice (overlapping reception is supported).
- With a OpenScape 4000 - OpenScape Voice (Transit) - OpenScape 4000 scenario, the message waiting display is not routed via OpenScape Voice.
- HG 3500 does not support digit authentication.
- The payload partners can be defined with DMC in a HiPath 400/OpenScape 4000 network. A OpenScape 4000 cannot however send the payload directly to or receive it directly from OpenScape Voice partners. A hop always results on the HG 3500 module.
- If there are more than two partners configured for the HG 3500 (e.g. Proxy) and **REGIP1** fails, **REGIP2** remains registered until **REGIP2** is no longer available. Automatic switchback to **REGIP1** is not possible.

14.6.4.2 OpenScape 4000 Configuration

See also "Section 6.1, “Configuration using AMOs”.

The following settings must be configured differently from the configuration given above:

- **Configure the IP address**
- The IP address (IPADR), which is configured with the AMO CGWB, is the IP address of the OpenScape 4000. The IP address must be the same as the alias name in OpenScape Voice.
- **Configure the gateway phone number**

- To set up a SIP-Q trunking connection to an OpenScape Voice system, the parameter **GWRNO** must be configured. This value of **GWRNO** must correspond to the alias name in OpenScape Voice.

```
CHANGE-CGWB:MTYPE=CGW,LTU=1,SLOT=37,TYPE=LEGKDATA,GWNO=1,

GWDIRNO=816901;
```

- **Configure the external registrar**
- In case of a trunking connection to OpenScape Voice, the OpenScape 4000 has to register dynamically with the OpenScape Voice partner system. An external registrar has to be set up for this purpose.

  The external registrar is configured with the AMO CGWB.

  – Operation at an external registrar (**SIPREG=YES**) must be activated.
  – The duration of the registration validity must be entered in **REGTIME**. The partner system registrar data must be entered in the fields **REGIP** (OpenScape Voice address or proxy address) and **REGPORT**.

```
CHANGE-CGWB:MTYPE=CGW,LTU=<ltu>,SLOT=<slot>,TYPE=SIPTRSSA,

SIPREG=YES, REGIP1=127.28.45.54,PORTTCP1=5060,

REGTIME=<Seconds>,REGIP2=0.0.0.0,PORTTCP2=5060;
```

  OpenScape Voice does not accept values less than 300 seconds in the **REGTIME** parameter.

  – The parameter **REGEXTGK** must be set to YES in AMO CGWB.

```
CHANGE-CGWB:MTYPE=CGW,LTU=1,SLOT=37,TYPE=LEGKDATA,GWNO=1,

GWDIRNO=816901REGEXTGK=YES;
```

> **NOTICE:** REGEXTGK can also be set to NO, however a GWNO will then need to be added.

- **Configure authentication**
- If authentication is activated in the partner system, the authentication data (SIP UserId in the field **GWUSERID**, password in the field **GWSECRET** and **realm** in the field **GWREALM**) must be configured for registration on the partner system. The transmission of authentication data can be activated and deactivated using the parameter **GWAUTREQ**.

```
CHANGE-CGWB:MTYPE=CGW,LTU=<ltu>,SLOT=<slot>,TYPE=SIPTRERH,

GWAUTREQ=YES,GWSECRET=<string>,GWUSERID=<string>,

GWREALM=<string>;
```

- **AMO TDCSU**

  – **DESTNO** must not be set to 0 (the value 0 deactivates loop detection).
  – Set the parameter **TRACOUNT** to the number of hops permitted in your network.

```
ADD-TDCSU:TYPE=NEW,PEN=1-01-037-0,COTNO=36,COPNO=32,

DPLN=0,ITR=0, COS=2,LCOSV=1,LCOSD=1,CCT="CIRCUIT from GW2", DESTNO=81,PROT►
VAR="ECMAV2",SEGMENT=8, ISDNIP=00,ISDNNP=0, TRACOUNT=10,SATCOUNT=MANY,NNO=1-69-
1499,ALARMNO=12, COTX=36,CCHDL=ASIDE,CLASSMRK=EC&G711,TCCID="IP RS",

TGRP=50,SRCHMODE=AB, INS=Y,DEV=HG3550IP,BCHAN=1&&30, BCNEG=N,BCGR=1,LWPAR=0,DM►
```

```
CALLWD=Y;
```

- **AMO COP**

```
ADD-COP:COPNO=36,TOLL=TA,TRK=TA;
CHANGE-COP:COPNO=36,COPTYPE=COPADD,DEV=INDEP,

INFO="36: S0/2 TIE ECMA2 AB V3.0";
```

- **AMO COT**
- Also check whether the COT parameter **TRCA** is set.

```
ADD-COT:COTNO=200,

PAR=RCL&XFER&MELD&KNOR&CEBC&TIE&CBBN&CBFN&COTN&ANHT&BLOC&LWNC&NLCR&ATRS&TSCS&DFN
N&NLHT&NLRD&VCMN&SNBE&IICB&NCDR&NOFT&VNCO&NOTO&NOSD&NPIS&PGEP&IBBA&PRNI&NTON&OS►
CV&FWDN&FNAN;
CHANGE-COT:COTNO=200,COTTYPE=COTADD,DEV=INDEP,INFO="HP8K";
```

Notes:

– If the entire network uses E.164 numbering, the COT parameter **NPIS** must be set for all digital trunks. If the dial plan **UNKNOWN/UNKNOWN** is used, the parameter **NPIS** should **NOT** be set!

– The COT parameters **FWDN** and **FWAN** may cause problems if a consistent dial plan is not used throughout the entire network.

– The COT parameter **OSCV** must be set.

- **Configure block dialing**
- Block dialing must be set up for the trunking connection to OpenScape Voice.
- **Note for national and local calls**
- Dialing with national numbers makes sense also for OpenScape 4000 users. Example: The extension +49(89)722-31256 can be reached under the following numbers:

31256	If closed numbering is configured
000498972231256	Always
0-722-31256	Local call
0-089-722-31256	National call

If local or national dialing is desired by OpenScape 4000 users, a number of other special LCR configurations have to be performed. This configuration

is outside the scope of the current description because it is not relevant for OpenScape Voice.

Example of closed numbering:

The LCR must also be configured for closed numbering.

This is an example of the destination number **31256**.

DN **31256** remains for +49(89)722-31256

Use the E.164 numbering scheme for OpenScape 4000 / OpenScape Voice interworking. The called subscriber's extension should also use E.164 with the dial plan ID ISDN in the internal ISDN messages.

Station number type: INTERNATIONAL

Missing digits must be filled with AMO LODR ##out pulse (e.g. 4989722).

AMO WABE defines the code

Example for:

```
DN 31256 NETRTE=224.
ADD-WABE:CD=224,DAR=NETRTE;
ADD-WABE:CD=31256,DAR=STN,CHECK=N;
CHANGE-WABE:CD=31256,DESTNO=218;
```

AMO RICHT sets up the bundle

Example for:

```
CD=224 (defined with AMO WABE) LRTE=224 (used later with AMO LDAT) TGRP=240
 (preconfigured with AMO BUEND)
ADD-RICHT:MODE=CD,LRTE= 224,CD=224,CPS=0,LSVC=ALL, NAME="HP 8K
 MEDIATRIX",TGRP1=240,
DESTNO=240,DNNO=218, PDNNO=1-1-218,ZEICHUM=NEUTRAL,KPRCAUL=NO,CLNAMEDL=NO;
ADD-RICHT:MODE=CD,CD=224,CPS=0,SRVC=VCE,TYPE=DTMF,M FVCONF=FIX,DTMFPULS=PP300;
```

AMO LODR defines the outdial rule

Example for:

```
ODR=240 (use for AMO LDAT)
ADD-LODR:ODR=240,CMD=OUTPULSE,DGTS=4989722; ADD-LODR:ODR=240,CMD=ECHO,FIELD=1;
 ADD-LODR:ODR=240,CMD=NPI,NPI=ISDN,
TON=INTERNAT; ADD-LODR:ODR=240,CMD=END; ADD-LODR:ODR=240,INFO="HP8K";
```

AMO LDAT defines LCR data

Example for:

```
TRRP240 (defined with AMO BUEND) ODR=240 (defined with AMO LODR) LRTE=224 (defined
 with AMO RICHT)
ADD-LDAT:LRTE=224,LSVC=ALL,LVAL=1,TGRP=240,ORD=240, LAUTH=16,CARRIER=1,
ZONE=EMPTY,LATTR=DMCEND,VCCYC=4;
```

14.6.4.3 OpenScape Voice Configuration

OpenScape Voice is configured with the OpenScape Voice Assistant.

Equivalent parameters must be configured in OpenScape Voice. The following data must be correctly configured:

Configuration of endpoint profile

The **endpoint profile** must be created before the **endpoints**.

Open the list of **endpoint profiles** in OpenScape Voice Assistant with **OpenScape Voice > Business Group > Available Private Numbering Plan = NP_Gateways > Profiles > Endpoint Profile**.

Choose the relevant endpoint profile from the list (e.g. HP4K) or create a new profile.

Tab **General**:

- Endpoint Profile:
  - Name: HP4K
  - Remark: <optional>
  - Numbering Plan: NP_Gateways
- Management Information
  - Class of Service: international
  - Routing Area: H4K_Network
  - Calling Location: <optional>
  - Time Zone: LOCAL
  - SIP Privacy Support: FULL
  - Failed Call Intercept Treatment: Enabled

  Tab **Endpoints**:

  This tab contains a list of endpoints assigned to the current profile.

  Tab **Services**:
- Message Waiting: Yes
- Call Transfer: Yes
- Call Forward Invalid Destination: No
- Toll and Call restrictions: No

Endpoint data that describes the connection to OpenScape 4000

OpenScape Voice > Business Group > Members > Endpoints > Name

Tab **General**:

Definition of connection data for an endpoint. Define the **name** and the **profile** here.

The **Registered** checkbox is activated automatically if the CGW has the status **registered**.

Tab **SIP**:

Configuration of IP address and CGW port and general configuration for SIP-Q.

- Choose the option button **SIP-Q Signaling**.
- **Enter** (**Static**, **Dynamic**):
  - If **Static** is entered here, HG 3500 (SIP) registration is not required.
  - If **Dynamic** is entered, HG 3500 (SIP) registration is required.
- **Signaling Binding Address**: IP address of CGW (this parameter must correspond with the parameter **IPADDR** in the AMO CGWB)
- **Port**: (this parameter must correspond with the parameter **PORTTCP2** in the AMO CGWB)
- **Transport protocol**: TCP

Tab **Attributes**:

Set **Support of Best Effort SRTP** to **Enabled (MIKEY, SDES, Automatic)** and activate the checkbox next to **Enable Session Timer**.

Tab **Aliases**:

When configuring the endpoint displayed by OpenScape 4000 (i.e. HG 3500), the following parameters must correspond with the data configured in the AMO CGWB:

- **Name**: This parameter must correspond with the parameter **GWID1**.
- **IP Address** of CGW: This parameter must correspond with the parameter **IPADDR**.
- **Aliases**:
- The ID of the gateway is used for dynamic registration. This is entered in the AMO CGWB in the branch **LEGKDATA** in the parameter **GWDIRNO**.

  Set the IP address of OpenScape 4000 to "trusted".

  OpenScape Voice > Administration > Signaling Management > Digest Authentication > Realms > Add

  Activate the checkbox **Trusted Entry**, enter the IP address of the CGW in the field **Signaling Primary** and select **All Ports**.

  Signaling and registration parameters that describe the OpenScape Voice registration data (IP address, port, login)

  The data entered here must correspond with the data entered in the AMO CGWB for ERH or SSA.

  The listening IP address must be entered in the IP address of the external registrar.

  The TCP/UDP port must be set in the field **TCP/UDP Port**.

  The data set for authentication (**UserID**, **Password**, **Realm**) must correspond with the data entered in the AMO CGWB in the data branch for SSA.

  Aliases:

  The ID of the gateway is used for dynamic registration. This is entered in the AMO CGWB in the branch **LEGKDATA** in the parameter **GWDIRNO**.

IMPORTANT: You will find more detailed information on the OpenScape Voice configuration in the relevant OpenScape Voice documentation.

14.6.5 Number management between OpenScape 4000 and OpenScape Voice for Italy

Because the phone number format for Italian mobile phones is different, the phone numbers in the OpenScape Voice direction are modified incorrectly if the following configuration information is not observed.

Scenario:

1. System A - OpenScape 4000
2. System B - OpenScape Voice

Incoming trunk call to OpenScape 4000 to an OpenScape Voice subscriber.

Requirements:

The phone numbers sent to OpenScape Voice must be in **ISDN/ INTERNATIONAL** format.

The OpenScape 4000 must be configured as an Italian system.

Generation (example)

Configure DAR=TIE in the central office direction:

```
ADD-WABE:CD=901,DAR=TIE;
```

Set up a separate direction to the central office for the Italian mobile phone numbers:

```
ADD-RICHT:MODE=LRTENEW,LRTE=393,LSVC=ALL,

NAME=ITALIANMOBILE,TGRP=XX,DNNO=1-1-393,ROUTOPT=NO,REROUT=NO,DESTNO=193,FWD►
SWTCH=YES;
ADD-LODR:ODR=393,CMD=ECHO,FIELD=3;
ADD-LODR:ODR=393,CMD=NPI,NPI=ISDN,TON=UNKNOWN;
ADD-LODR:ODR=393,CMD=END;
ADD-LDAT:LRTE=393,LSVC=ALL,TGRP=XX,ORD=393,LAUTH=1;
ADD-LDPLN:LCRCONF=LCRPATT,DIPLNUM=0,LDP=0-W-3,LRTE=393,

LAUTH=1;
```

Set up a separate direction to the central office for the Italian mobile phone numbers (if the phone number is dialed with a country code):

```
ADD-RICHT:MODE=LRTENEW,LRTE=394,LSVC=ALL,

NAME=ITALIANMOBILE,TGRP=XX,DNNO=1-1-393,ROUTOPT=NO,REROUT=NO,DESTNO=193,FWD►
SWTCH=YES;
ADD-LODR:ODR=394,CMD=ECHO,FIELD=4;
ADD-LODR:ODR=394,CMD=NPI,NPI=ISDN,TON=UNKNOWN;
ADD-LODR:ODR=394,CMD=END;
ADD-LDAT:LRTE=394,LSVC=ALL,TGRP=xx,ORD=394,LAUTH=1;
ADD-LDPLN:LCRCONF=LCRPATT,DIPLNUM=0,LDP=0-W-0039-3,LRTE=394,

LAUTH=1;
```

Create a KNDEF entry with **TYPE=FOREIGN** for the Italian mobile phone numbers:

```
ADD-KNDEF:NNO=1-1-393,TYPE=FOREIGN,ISDNCC=39;
```

Add the COT parameter DCCO to allow a node number to be derived:

```
CHA-COT:COTNO=YY,COTTYPE=COTADD,COTPAR=DCCO;
```

14.7 Configuration Guide for OpenScape 4000 / OpenScape Voice Networking

14.7.1 General

This document describes how to configure OpenScape 4000 and OpenScape Voice in order to establish the networking.

For a detailed description of specific settings, please refer to the OpenScape 4000 installation instructions/service documentation respectively OpenScape Voice documentation.

14.7.2 Introduction and Overview

- The module HG 3500 is part of an OpenScape 4000 system. It's the peripheral gateway module with LAN interface toward the OpenScape Voice system.
- In the OpenScape 4000 system there is a customer database. This database contains the configuration about trunks, stations and features.
- The HG 3500 can be configured with different parameters. The HG 3500 configuration should match the configuration on the OpenScape Voice system.
- For configuration in the OpenScape 4000 there is an interface for AMO commands.
- This documentation should help the OpenScape 4000 system engineer to find a working configuration.
- For details please refer to the service documentation of the OpenScape 4000.

14.7.3 Requirements and Released Combinations

OpenScape 4000

- Supported versions
- HiPath 4000/OpenScape 4000 must support SIP-Q V2 meaning HiPath 4000 V4 onwards.
- Trunking modules

Trunking modules

Type	Part number
STMI2	Q2316-X or Q2316-X10
STMI4[9]	Q2324-X500 or Q2324-X510 or Q2324-X511
vhg3500	Q2300-X
STMIX	Q2343-X
STMIY	Q2361-X

OpenScape Voice

- Supported versions

[9] Hint: On STMI4 boards the SENTA version must be 12 or higher

- OpenScape Voice V5.0 and higher.

Released Combinations

Please check “Sales Information - Common Compatibility Matrix” for exact released version combinations. This document can be found on the Unify Partner Portal.

14.7.4 Configuration on OpenScape 4000

14.7.4.1 Settings for STMI2/STMI4/STMIX/STMIY

14.7.4.1.1 Central settings in OpenScape 4000

- **GATEKPR=YES** from **CHANGE-ZANDE:TYPE=ALLDATA** is used in this document. If set to **GATEKPR=NO** the AMO CGWB looks slightly different. Either configuration of this parameter is fine.
- In a HiPath 4000/OpenScape 4000, HiPath 3000 network we suggest to use the E.164 numbering for the complete network. Then please add the COT parameter **NPIS** to every digital trunk.
- Settings for module in OpenScape 4000
- For this example the trunking module is installed in location 1-2-4 (means LTG=1, LTU=2, SLOT=4).

14.7.4.1.2 AMO Configurations

AMO BFDAT

```
DIS-BFDAT:4;
H500:  AMO BFDAT STARTED

-------------------------------------------------------------------------------

| FCTBLK =  4    BRDBCHL : BCHL120              STATUS=      OK                |

-------------------------------------------------------------------------------

|  1. FUNCT : HG3550       4 LINES    UNITS  3  BCHLCNT  30  TOTAL BCHAN 120   |

-------------------------------------------------------------------------------

AMO-BFDAT-111       CONFIGURATION OF FUNCTIONAL BLOCKS FOR CGW BOARDS
ADD-BFDAT:FCTBLK=4,FUNCTION=HG3550,BRDBCHL=BCHL120;
CHANGE-BFDAT:CONFIG=CONT,FCTBLK=4,FUNCTION=HG3550,LINECNT=4,UNITS=3;
CHANGE-BFDAT:CONFIG=OK,FCTBLK=4,ANSW=YES;
```

AMO BCSU

```
DIS-BCSU:TBL,1,2,4;
H500:  AMO BCSU  STARTED


 LTG  1  LTU 2   SRCGRP 1   ALARMNO-LTU 0

-----+----------+--------+---+-+-+---+-+-----------+-----------+-----------
```

```
     |           |        |   |S|H|AL-| |             |            |
     | ASSIGNED  | MODULE |FCT|E|W|ARM| | INSERTED    |    HW-     | MODULE
 PEN | MODULE    | TYPE   |ID |C|Y|NO | | MODULE      |STATE INFO  | STATUS
-----+-----------+--------+---+-+-+---+-+-------------+------------+------------
   4 | Q2324-X510 STMI4      1   A   0| | Q2324-X510 |  1  -12 -  | READY
     +----------------------------------+-+------------+------------+------------
     | IP ADDRESS : 172. 29.136.200         B-CHANNELS : 120    BCHLCNT : 120
     | BLOCK NO   :   4                     PRERESERVED LINES ASSIGNED :   NO
     |  1. FUNCT  : HG3550        4 LINES   B-CHANNELS : 120    BCHLCNT : 120
     +----------------------------------+-+------------+------------+------------


+----+----+----------------------------+-+------------+------------+--------+
| NO SECURITY STATUS AVAILABLE, SINCE FEATURE SPE IS NOT ACTIVATED          |
+---------+-------------------------------------------------------------------+

AMO-BCSU -111       BOARD CONFIGURATION, SWITCHING UNIT

DISPLAY COMPLETED;
ADD-BCSU:MTYPE=IPGW,LTG=1,LTU=2,SLOT=4,PARTNO="Q2324-X510",FCTID=1,LW►
VAR="0",FCTBLK=4,BCHL3550=120,ALARMNO=0;
AMO TDCSU
DIS-TDCSU:1-02-004-0;

H500:  AMO TDCSU STARTED

  +------------------------ DIGITAL TRUNK (FORMAT=L) -------------------------+
  | DEV      = HG3550IP      PEN      =  1-02-004-0   TGRP     = 281          |
  |-----------------------------------------------------------------------------|
  | PROTVAR  = ECMAV2        INS      = Y             SRCHMODE = DSC          |
  | COTNO    = 200           COPNO    = 36            DPLN     = 0            |
  | ITR      = 0             COS      = 1             LCOSV    = 3            |
  | LCOSD    = 8             CCT      = OSV KN281     DESTNO   = 81           |
  | SEGMENT  = 8             DEDSCC   =               DEDSVC   = NONE         |
  | FACILITY =               DITIDX   =               SRTIDX   =              |
```

```
  | TRTBL    = GDTR          SIDANI   = N             ATNTYP   = TIE          |
  | CBMATTR  = NONE          NWMUXTIM = 10            TCHARG   = N            |
  | SUPPRESS = 0             DGTPR    =               CHIMAP   = N            |
  | ISDNIP   =               ISDNNP   =                                       |
  | PNPL2P   =               PNPL1P   =               PNPAC    =              |
  | TRACOUNT = 10            SATCOUNT = MANY          NNO      = 281          |
  | ALARMNO  = 0             FIDX     = 1             CARRIER  = 1            |
  | ZONE     = EMPTY         COTX     = 200           FWDX     = 10           |
  | DOMTYPE  =               DOMAINNO =               TPROFNO  =              |
  | INIGHT   =                                        CCHDL    =              |
  | UUSCCX   = 16            UUSCCY   = 8             FNIDX    = 1            |
  | CLASSMRK = EC      & G711    & G729AOPT           SRCGRP   = 1            |
  | TCCID    =                                        SECLEVEL = TRADITIO     |
  |-------------------------------------------------------------------------|
  | BCNEG    = N             BCGR     = 1             LWPAR    = 0            |
  | LWPP     = 0             LWLT     = 0             LWPS     = 0            |
  | LWR1     = 0             LWR2     = 0                                     |
  | DMCALLWD = Y             VNNO     =                                       |
  | SVCDOM   =                                                               |
  | BCHAN    =  1 && 30                                                      |
  |                                                                          |
  +-------------------------------------------------------------------------+
  AMOUNT OF B-CHANNELS IN THIS DISPLAY-OUTPUT: 30


AMO-TDCSU-111       DIGITAL TRUNKS

DISPLAY COMPLETED;
ADD-TDCSU:OPT=NEW,PEN=1-02-004-0,COTNO=200,COP►
NO=36,DPLN=0,ITR=0,COS=1,LCOSV=3,LCOSD=8,CCT="O KN281  ",DESTNO=81,PROTVAR="EC►
MAV2",SEGMENT=8,DEDSVC=NONE,TRTBL=GDTR,SIDANI=N,ATNTYP=TIE,CBMATTR=NONE,TCHARG=N
,SUPPRESS=0,TRACOUNT=10,SATCOUNT=MANY,NNO=281,ALARMNO=0,FIDX=1,CARRIER=1,ZONE=EM
PTY,COTX=200,FWDX=10,CHIMAP=N,UUSCCX=16,UUSCCY=8,FNIDX=1,NWMUXTIM=10,SRCGRP=1,CL
```

```
ASSMRK=EC&G711&G729AOPT,TGRP=281,SRCHMODE=DSC,INS=Y,SECLEVEL=TRADITIO,DEV=HG3550
IP,BCHAN=1&&30,BCNEG=N,BCGR=1,LWPP=0,LWLT=0,LWPS=0,LWR1=0,LWR2=0,DMCALLWD=Y;
```

Hints:

- Make sure the **DESTNO** differs from 0 (the value 0 will deactivate the loop detection).
- Please set the parameter **TRACOUNT** to the amount of hops which are valid in your network. Please also check if the COT Parameter **ATRS** is set (see also Section 7.10, “OpenScape Voice Loop detection” below).

AMO BUEND

```
DIS-BUEND:281;

H500:  AMO BUEND STARTED


+------------------------------ FORMAT = L ----------------------------------+
|  TGRP NUMBER :   281   TGRP NAME   : OSV IFS           MAXIMUM NO.   :  120 |
|                        CHARCON     : NEUTRAL                               |
|  SUBGROUP NO.:    10   DEVICE TYPE : HG3550IP          TRACENO       :    0 |
|  SEARCH MODE : DESCENDING                              ACD THRESHOLD :    * |
|  NUMBER OF ASSOCIATED ROUTES       : 10                PRIORITY      :    2 |
|  TDDRFLAG    :    ON  TDDRTHRESHOLD: 5                SOURCEGROUPIDX :    1 |
|  GDTRRULE    :     0      ACDPMGRP : 0                                      |
|  THE FOLLOWING TRUNKS (LTG-LTU-SLOT-CCT) HAVE BEEN ALLOCATED:                |
+------------------------------------------------------------------------------+
|   1- 2-  4-0           1 |  1- 2-  4-0           2 |  1- 2-  4-0           3 |
|   1- 2-  4-0           4 |  1- 2-  4-0           5 |  1- 2-  4-0           6 |
|   1- 2-  4-0           7 |  1- 2-  4-0           8 |  1- 2-  4-0           9 |
|   1- 2-  4-0          10 |  1- 2-  4-0          11 |  1- 2-  4-0          12 |
|   1- 2-  4-0          13 |  1- 2-  4-0          14 |  1- 2-  4-0          15 |
|   1- 2-  4-0          16 |  1- 2-  4-0          17 |  1- 2-  4-0          18 |
|   1- 2-  4-0          19 |  1- 2-  4-0          20 |  1- 2-  4-0          21 |
|   1- 2-  4-0          22 |  1- 2-  4-0          23 |  1- 2-  4-0          24 |
|   1- 2-  4-0          25 |  1- 2-  4-0          26 |  1- 2-  4-0          27 |
|   1- 2-  4-0          28 |  1- 2-  4-0          29 |  1- 2-  4-0          30 |
```

1- 2- 4-1	1	1- 2- 4-1	2	1- 2- 4-1	3
1- 2- 4-1	4	1- 2- 4-1	5	1- 2- 4-1	6
1- 2- 4-1	7	1- 2- 4-1	8	1- 2- 4-1	9
1- 2- 4-1	10	1- 2- 4-1	11	1- 2- 4-1	12
1- 2- 4-1	13	1- 2- 4-1	14	1- 2- 4-1	15
1- 2- 4-1	16	1- 2- 4-1	17	1- 2- 4-1	18
1- 2- 4-1	19	1- 2- 4-1	20	1- 2- 4-1	21
1- 2- 4-1	22	1- 2- 4-1	23	1- 2- 4-1	24
1- 2- 4-1	25	1- 2- 4-1	26	1- 2- 4-1	27
1- 2- 4-1	28	1- 2- 4-1	29	1- 2- 4-1	30
1- 2- 4-2	1	1- 2- 4-2	2	1- 2- 4-2	3
1- 2- 4-2	4	1- 2- 4-2	5	1- 2- 4-2	6
1- 2- 4-2	7	1- 2- 4-2	8	1- 2- 4-2	9
1- 2- 4-2	10	1- 2- 4-2	11	1- 2- 4-2	12
1- 2- 4-2	13	1- 2- 4-2	14	1- 2- 4-2	15
1- 2- 4-2	16	1- 2- 4-2	17	1- 2- 4-2	18
1- 2- 4-2	19	1- 2- 4-2	20	1- 2- 4-2	21
1- 2- 4-2	22	1- 2- 4-2	23	1- 2- 4-2	24
1- 2- 4-2	25	1- 2- 4-2	26	1- 2- 4-2	27
1- 2- 4-2	28	1- 2- 4-2	29	1- 2- 4-2	30
1- 2- 4-3	1	1- 2- 4-3	2	1- 2- 4-3	3
1- 2- 4-3	4	1- 2- 4-3	5	1- 2- 4-3	6
1- 2- 4-3	7	1- 2- 4-3	8	1- 2- 4-3	9
1- 2- 4-3	10	1- 2- 4-3	11	1- 2- 4-3	12
1- 2- 4-3	13	1- 2- 4-3	14	1- 2- 4-3	15
1- 2- 4-3	16	1- 2- 4-3	17	1- 2- 4-3	18
1- 2- 4-3	19	1- 2- 4-3	20	1- 2- 4-3	21
1- 2- 4-3	22	1- 2- 4-3	23	1- 2- 4-3	24

```
|   1- 2-  4-3          25 |  1- 2-  4-3          26 |  1- 2-  4-3          27 |

|   1- 2-  4-3          28 |  1- 2-  4-3          29 |  1- 2-  4-3          30 |

+--------------------------------------------------------------------------+

AMO-BUEND-111       TRUNK GROUP

DISPLAY COMPLETED;
ADD-BUEND:TGRP=281,NAME="OSV IFS           ",NO=120,TRACENO=0,ACDTHRH=*,PRIO►
NO=2,TDDRFLAG=ON,GDTRRULE=0,ACDPMGRP=0,CHARCON=NEUTRAL;
```

AMO COP

```
DIS-COP:36;
   COP:  36  INFO: 36: S0/2 QUER ECMA2 AB V3.0

   DEVICE: S2CONN       SOURCE: DB

   PARAMETER:


CO TRUNK ACCESS:

TRUNK ACCESS                                                    TA

TOLL ACCESS:

TRUNK ACCESS                                                    TA


ADD-COP:COPNO=36,TRK=TA,TOLL=TA;
CHANGE-COP:COPNO=36,COPTYPE=COPADD,DEV=S2CONN,INFO="36: S0/2 QUER ECMA2 AB
V3.0";
```

AMO COT

The following COT parameters were tested and are recommended.

```
DIS-COT:200;
H500:  AMO COT   STARTED



COT: 200  INFO: OSV STANDARD COT

DEVICE: INDEP        SOURCE: DB

PARAMETER:


RECALL IF USER HANGS UP IN CONSULTATION CALL                     RCL

TRUNK CALL TRANSFER                                             XFER

TRUNK SIGNALING ANSWER                                          ANS

KNOCKING OVERRIDE POSSIBLE                                      KNOR
```

```
CALL EXTEND FOR BUSY, RING OR CALL STATE                          CEBC

NETWORKWIDE AUTOMATIC CALLBACK ON BUSY                            CBBN

NETWORKWIDE AUTOMATIC CALLBACK ON FREE                            CBFN

NETWORKWIDE CALL FORWARDING PERMITTED                             FWDN (*1)

NETWORKWIDE FORWARDING NO-ANSWER                                  FNAN (*1)

REGENERATED CO DIALTONE ON OUTGOING SEIZURE                       COTN

DON'T RELEASE CALL TO BUSY HUNT GROUP                             BSHT

CAMP-ON DID CALLS                                                 KNDI (*2)

END-OF-DIAL FOR BLOCK IS SET                                      BLOC

SEND NO NODE NUMBER TO PARTNER                                    LWNC

ACTIVATE TRANSIT COUNTER ADMINISTRATION FOR S0/S2 LINE            ATRS

CONNECTION TO ROUTE OPTIMIZATION NODE                             ROPT

TSC-SIGNALING FOR NETWORKWIDE FEATURES (MANDATORY)                TSCS

USE DEFAULT NODE NUMBER OF TRUNK                                  DFNN (*3)

NO LOCAL HOLDTONE, HOLDTONE FROM REMOTE SYSTEM                    NLHT

SEND NO BILLINGELEMENTS                                           SNBE

IGNORE INCOMING BILLING                                           IICB

SUPPRESS SIGNALING OF CDR-E SPECIFIC MESSAGES                     NCDR

NO FLAG TRACE                                                     NOFT

SEND VIRTUAL SUBSCRIBER NUMBER TO CO                              VNCO

NO SIMPLE DIALOG AVAILABLE                                        NOSD

NPI ISDN, OUTGOING CALL                                           NPIS (*4)

SEND DIGITS VIA IN.BAND DTMF BEFORE ANSWER                        IBBA

PREVENT NODE INFORMATION                                          PRNI

OPENSCAPE VOICE INTERWORKING                                      OSCV

NO TONE                                                           NTON
AMO-COT  -111       CLASS OF TRUNK FOR CALL PROCESSING

DISPLAY COMPLETED;
ADD-
```

```
COT:COTNO=200,PAR=RCL&XFER&ANS&KNOR&CEBC&CBBN&CBFN&COTN&BSHT&BLOC&LWNC&ATRS&ROPT
&TSCS&DFNN&NLHT&SNBE&IICB&NCDR&NOFT&VNCO&NOSD&NPIS&IBBA&PRNI&NTON&FWDN&OS►
CV&FNAN;
CHANGE-COT:COTNO=200, COTTYPE=COTADD, DEV=INDEP, INFO="OSV STANDARD COT";
```

Hints:

- (*1) COT Parameters **FWDN**&**FWAN** may cause problems when not using a consistent numbering plan throughout the network.
- (*2) **KNDI** to allow network calls to automatically camp on to station when calling from DDI.
- (*3) **DFNN** is not necessarily needed. Without the parameter, node information is derived from the calling number via LCR. If no route is configured, then the node (**NNO**) is taken from AMO TDCSU. **DFNN** is often set by technicians so the AMO TDCSU **NNO** is always taken.
- (*4) If the whole network (HiPath 4000/OpenScape 4000, HiPath 3000, OpenScape Voice) uses E.164 numbering and the COT parameter **NPIS** is set on every digital trunk. If using **UNKNOWN/UNKNOWN** numbering plan, **NPIS** should **NOT** be set.
- COT parameter **NOTO** should not be set. From OpenScape Voice V5, tones are heard from the OpenScape 4000 even with Progress messages (delayed disconnect procedure).
- Set the parameter **TRACOUNT** (with AMO TDCSU) to the amount of hops which are valid in your network (see section AMO TDCSU)!
- **SECO** may also need to be set in USA configurations to allow correct E911 working.
- For further details, please reference:

  https://gsikm-productive.unify.com/rkm/viewdoc.jsp?doc=209494

  AMO CGWB

```
DIS-CGWB:2,4;

H500:  AMO CGWB  STARTED

------------------------------------------------------------------------------

|  CGW BOARD DATA                                                            |

------------------------------------------------------------------------------

|   HG3550                                                                   |

------------------------------------------------------------------------------

|  LTU = 2       SLOT = 4      SMODE = NORMAL           POOLNO: 0            |

------------------------------------------------------------------------------


  GLOBAL DATA AND ETHERNET INTERFACE DATA - CONFIGURABLE VALUES:

  ------------------------------------------------------------

  IPADR     = 10.237.88.122       // own address
```

```
                                  // config OSV -> Endpoint-> alias
                                      TCPP   =        (4060)
  NETMASK   = 255.255.255.192         VLAN   = NO     (NO)
  DEFRT     = 172.29 .136.193         (0.0.0.0 = NOT CONFIGURED)
  BITRATE   =         (CHECK OS)      VLANID = 0      (0)
  PATTERN   = 213 (213)
  TRPRSIP   = 0   (0)
  TRPRSIPQ  = 120 (0)                  // Number of available SIPQ Trunks
  TRPRH323  = 0   (0)                 // channels, dependant on DMC capability
  TPRH323A = 0   (0)
  TLSP   = 4060  (4061)

  GLOBAL DATA - CONSTANT VALUES:
  ------------------------------
  AMO INTERFACE VERSION: 0      OPMODE: 1   DATA_VALID: YES

  DNSIPADR  = 10.237.1.3
  DNSIPADR2  = 0.0.0.0

  SERVICE INTERFACE
  -----------------
  LOGINTRM = "TRM" (TRM)
  PASSW    = *****

  ASC DATA - CONFIGURABLE VALUES:
  -------------------------------
  TOSPL    = 184   (184)     TOSSIGNL = 104   (104)
  UDPPRTLO = 29100 (29100)  UDPPRTHI = 30099 (30099)
```

```
T38FAX   = YES   (YES)    REDRFCTN = YES   (YES)

RFCFMOIP = YES   (YES)    RFCDTMF  = YES   (YES)


PRIO1 :  CODEC = G711A   VAD = NO   RTP-SIZE = 20  // RTP-SIZE 20

                // if Feature DECT-IP or OSCMC exist somewhere in the network

PRIO2 :  CODEC = G711U   VAD = NO   RTP-SIZE = 20

PRIO3 :  CODEC = G729A   VAD = NO   RTP-SIZE = 20

PRIO4 :  CODEC = G723    VAD = NO   RTP-SIZE = 30

PRIO5 :  CODEC = NONE    VAD = NO   RTP-SIZE = 20

PRIO6 :  CODEC = NONE    VAD = NO   RTP-SIZE = 20

PRIO7 :  CODEC = G729AB  VAD = YES     RTP-SIZE = 20


DSP CONFIGURATION DATA

----------------------

JITBUFD  = 60   (60) (PAREMERTER IS NOT USED ANYMORE)


MANAGEMENT STATION AND BACK-UP SERVER

--------------------------------------

MGNTIP    = 10.237.80.50 (0.0.0.0)    // Address from OpenScape 4000 Assistant

MGNTPN    = 8000 (8000)

BUSIP     = 10.237.80.50 (0.0.0.0)    // Address from OpenScape 4000 Assistant

BUSPN     = 443 (443)

UIMODE    = CLASSIC (CLASSIC


DMC DATA

--------

DMCCONN   = 90 (0)           // Maximum value for DMC
```

```
  WBM LOGIN DATA

  --------------

  LOGINWBM  = HP4K-DEVEL   ROLE  = ENGR (ADMIN)

  LOGINWBM  = HP4K-SU      ROLE  = SU (ADMIN)

  LOGINWBM  = HP4K-ADMIN   ROLE  = ADMIN (ADMIN)

  LOGINWBM  = HP4K-READER  ROLE  = READONLY (ADMIN)


  GATEWAY DATA

  ------------

  GWID1     = GW1

  GWID2     =


  H.235 SECURITY DATA

  -------------------

  GLOBID1   = Gateway2003

              (Gateway2003)

  GLOBID2   =

  TIMEWIN   = 100  (100)

  SECSUBS   = YES   (NO)                // YES if SECURE NO for TCP

  SECTRNK   = YES   (NO)                // YES if SECURE NO for TCP

  GLOBPW    = 242-191-30-119-188-83-173-161-43-0-70-36-218-74-169-221-78-102-
174-170


  LEGK DATA

  ------------------

  GWNO      =  (0)

  GWDIRNO   = 166                        // configuration OSV-> Endpoint-> alias

  REGEXTGK  = YES (NO)                  // Yes for Registration, NO for DNS-SRV
```

```
SIP TRUNKING DATA FOR  ERH

---------------------------

GWAUTREQ    = NO (NO)

GWSECRET    = *****

GWUSERID    =

GWREALM     =


SIP TRUNKING DATA FOR  SSA

---------------------------

SIPREG      = YES   (NO)               // YES for Registration, NO for DNS-SRV

REGIP1      = 10.237.81.104 (0.0.0.0)     // OSV Node-1 or Proxy Address

                                        // sipsm1 OSV (if TCP)

                                       // sipsm3 OSV cluster (if TLS)

PORTTCP1    = 5060 (5060)

PORTTLS1    = 5061  (5061)

REGIP2      = 10.237.84.104 (0.0.0.0)       // OSV Node-2 if geo-separated

                                            // OSV Node-1 if Proxy configured

                                            // sipsm2 OSV (if TCP)

                                            // sipsm4 OSV cluster (if TLS)

PORTTCP2    = 5060 (5060)

PORTTLS2    = 5061 (5061)

REGTIME     = 300  (120)                // Value >= 300


DLS DATA

-------------------------------------

DLSIPADR  = 0.0.0.0

DLSPORT   = 18443
```

```
  DLSACPAS  = NO


  JB DATA - CONFIGURABLE VALUES:

  ------------------------------

  JBMODE    = 2

  AVGDLYV   = 40  (40)

  MAXDLYV   = 120 (120) MINDLYV = 20  (20)

  PACKLOSS  = 4   (4)

  AVGDLYD   = 60  (60)  MAXDLYD = 200 (200)


IP CONFIGURATION

  -------------------------------------

  IPMODE    = IPV4 (IPV4)

  DHCPV4    = NO (NO)

  DHCPV6    = NO (NO)


  MANAGEMENT LAN INTERFACE DATA - CONFIGURABLE VALUES:

  ------------------------------------------------------------

  MIPADR    = 0  .0  .0  .0          MNETMASK   = 0  .0  .0  .0

  MVLAN     = NO     (NO)            MVLANID    = 0      (0)

  MDEFRT    = 0  .0  .0  .0          (0.0.0.0 = NOT CONFIGURED)


AMO-CGWB -111       CONFIGURATION OF HG3500 BOARD

DISPLAY COMPLETED;
  <
ADD-CGWB:LTU=2,SLOT=4,SMODE=NORMAL,IPADR=172.29.136.200,NETMASK=255.255.255.192;
CHANGE-CGWB:MTYPE=CGW,LTU=2,SLOT=4,TYPE=GLOBIF,PATTERN=213,VLAN=NO,VLANID=0,DE►
FRT
=172.29.136.193,BITRATE="AUTONEG",TRPRSIP=0,TRPRSIPQ=120,TR►
PRH323=0,TPRH323A=0,TLSP=4061,DNSIPADR=0.0.0.0,DNSIPAD2=0.0.0.0;
CHANGE-CGWB:MTYPE=CGW,LTU=2,SLOT=4,TYPE=SERVIF,LOGINTRM="TRM";
CHANGE-CGWB:MTYPE=CGW,LTU=2,SLOT=4,TYPE=ASC,UDPPRTLO=29100,UDPPRTHI=30099,TO►
SPL="
```

```
184",TOSSIGNL="104",T38FAX=NO,RFCFMOIP=YES,RFC►
DTMF=YES,REDRFCTN=YES,PRIO=PRIO1,CODEC=G711A,VAD=NO,RTP="20";
CHANGE-CGWB:MTYPE=CGW,LTU=2,SLOT=4,TYPE=ASC,PRIO=PRIO2,CO►
DEC=G711U,VAD=NO,RTP="20";
CHANGE-CGWB:MTYPE=CGW,LTU=2,SLOT=4,TYPE=ASC,PRIO=PRIO3,CO►
DEC=G729A,VAD=NO,RTP="20";
CHANGE-CGWB:MTYPE=CGW,LTU=2,SLOT=4,TYPE=ASC,PRIO=PRIO4,CO►
DEC=G723,VAD=NO,RTP="30";
CHANGE-CGWB:MTYPE=CGW,LTU=2,SLOT=4,TYPE=ASC,PRIO=PRIO5,CO►
DEC=NONE,VAD=NO,RTP="20";
CHANGE-CGWB:MTYPE=CGW,LTU=2,SLOT=4,TYPE=ASC,PRIO=PRIO6,CO►
DEC=NONE,VAD=NO,RTP="20";
CHANGE-CGWB:MTYPE=CGW,LTU=2,SLOT=4,TYPE=ASC,PRIO=PRIO7,CO►
DEC=G729AB,VAD=YES,RTP="20";
CHANGE-CGWB:MTYPE=CGW,LTU=2,SLOT=4,TYPE=DSP,JITBUFD="60";
CHANGE-
CGWB:MTYPE=CGW,LTU=2,SLOT=4,TYPE=GKDATA,PRIGKPN=1719,PRIGKID1="PRIMARYRASMANAGER
ID",SECGKPN=1719,SECGKID1="SECONDARYRASMANAGERID",TIMTLIVE=120;
CHANGE-CGWB:MTYPE=CGW,LTU=2,SLOT=4,TYPE=MGNTDATA,MGNTIP=172.29.136.242,MGNT►
PN=8000,BUSIP=172.29.136.242,BUSPN=443;
CHANGE-CGWB:MTYPE=CGW,LTU=2,SLOT=4,TYPE=DMCDATA,DMCCONN=90;
CHANGE-CGWB:MTYPE=CGW,LTU=2,SLOT=4,TYPE=WBMDATA,LOGINWBM="HP4K-DEVEL",ROLE=ENGR;
CHANGE-CGWB:MTYPE=CGW,LTU=2,SLOT=4,TYPE=WBMDATA,LOGINWBM="HP4K-SU",ROLE=SU;
CHANGE-CGWB:MTYPE=CGW,LTU=2,SLOT=4,TYPE=WBMDATA,LOGINWBM="HP4K-ADMIN",ROLE=AD►
MIN;
CHANGE-CGWB:MTYPE=CGW,LTU=2,SLOT=4,TYPE=WBMDATA,LOGINWBM="HP4K-READ►
ER",ROLE=READONLY;
CHANGE-CGWB:MTYPE=CGW,LTU=2,SLOT=4,TYPE=H235DATA,SECSUBS=NO,SECTRNK=NO,GLO►
BID1="Gateway2003",TIMEWIN=100,GLOBPW=242-191-30-119-188-83-173-161-43-0-70-36-
218-74-169-221-78-102-174-170;
CHANGE-CGWB:MTYPE=CGW,LTU=2,SLOT=4,TYPE=LEGKDATA,GWDIRNO=166,REGEXTGK=YES;
CHANGE-CGWB:MTYPE=CGW,LTU=2,SLOT=4,TYPE=SIPTRERH,GWAUTREQ=NO,GWUSERID="sipq",GW►
REALM="mchh";
CHANGE-
CGWB:MTYPE=CGW,LTU=2,SLOT=4,TYPE=SIPTRSSA,SIPREG=YES,REGIP1=172.29.132.152,PORTT
CP1=5060,PORTTLS1=5061,REGTIME=300,REGIP2=0.0.0.0,PORTTCP2=5060,PORTTLS2=5061;
CHANGE-CGWB:MTYPE=CGW,LTU=2,SLOT=4,TYPE=DLSDATA,DLSIPADR=172.29.128.156,DL►
SPORT=18443,DLSACPAS=NO;
CHANGE-CGWB:MTYPE=CGW,LTU=2,SLOT=4,TYPE=JB,AVGDLYV=40,MAXDLYV=120,MIND►
LYV=20,PACKLOSS=4,AVGDLYD=60,MAXDLYD=200,JBMODE=2;
```

14.7.4.1.3 Routing to the OpenScape Voice System

The numbering between OpenScape 4000 and OpenScape Voice should be international dialing.

For routing configuration on OpenScape 4000 please refer to *OpenScape 4000, Volume 3: Feature Usage Examples* service documentation.

14.7.4.1.4 Hint for National and Local Dialling

For OpenScape 4000 users it makes sense to dial with national numbering, too.

E.g. station +49(89)722-31256 can be reached with dialing

31256	// If closed numbering is configured
000498972231256	// always
0-722-31256	// local dialing

0-089-722-31256	// national dialing

If this local or national dialing is requested from OpenScape 4000 users, some special additional LCR-configuration must be done. This configuration is not part of this description because there is no need from the OpenScape Voice side. Please refer to **OpenScape 4000, Volume 3: Feature Usage Examples** service documentation.

Example closed numbering

Also for closed numbering the LCR for international dialing must be configured (see Section 7.9, “OpenScape Voice Routing for International Dialing - Extend Dialed Numbers to International N

This is an example for destination number DN=31256. DN=31256 stays for +49(89)722-31256

Use the E.164 numbering scheme for OpenScape 4000 and OpenScape Voice interworking.

In internal ISDN messages even the called number should use E.164 with

1) Numbering plan identifier: ISDN

and

1) Type of number: INTERNATIONAL.

Make sure to outpulse missing digits with AMO LODR (e.g. `ADD-LODR=xxx,CMD=OUTPULSE,DGTS=4989722;`). AMO WABE defines the access code.

Example for AMO WABE with destination number 31256 and **NETRTE=224**:

```
ADD-WABE:CD=224,DAR=NETRTE;
DIS-WABE:TYPE=GEN,CD=224;
H500:  AMO WABE  STARTED

  ------------------------------------------------------------------------

  | DIGIT INTERPRETATION                  VALID FOR ALL DIAL PLANS          |

  ------------------------------------------------------------------------

  |                 |    CALL PROGRESS STATE     |NODE/DIGIT| RESERVED/CONVERT |

  |      CODE       |            1 11111 11112 22| ANALYSIS | DNI/ADD-INFO     |

  |                 |0 12345 67890 12345 67890 12|  RESULT  | *=OWN NODE       |

  ------------------------------------------------------------------------

  | 224             |* ..... ..... ..... ..... ..| NETRTE   |                  |

  ------------------------------------------------------------------------


AMO-WABE -111       DIALLING PLANS, FEATURE ACCESS CODES
```

```
DISPLAY COMPLETED;
ADD-WABE:CD=31256,DAR=STN,CHECK=N;
CHANGE-WABE:CD=31256,DESTNO=218;
DIS-WABE:TYPE=GEN,CD=31256;
H500:  AMO WABE  STARTED

  ------------------------------------------------------------------------------

  | DIGIT INTERPRETATION                    VALID FOR ALL DIAL PLANS            |

  ------------------------------------------------------------------------------

  |                 |    CALL PROGRESS STATE     |  DIGIT   | RESERVED/CONVERT |

  |      CODE       |            1 11111 11112 22| ANALYSIS | DNI/ADD-INFO     |

  |                 |0 12345 67890 12345 67890 12|  RESULT  | *=OWN NODE       |

  ------------------------------------------------------------------------------

  | 31256           |. .**** ***** **... ..... .*| STN      |                  |

  |                 |                            |          |DESTNO 218        |

  |                 |                            |          |DNNO    0-  0-218 |

  |                 |                            |          |PDNNO   1-  1-218 |

  ------------------------------------------------------------------------------


AMO-WABE -111       DIALLING PLANS, FEATURE ACCESS CODES

DISPLAY COMPLETED;
```

AMO RICHT is used to prepare trunk groups.

Example for AMO RICHT with **CD=224** (defined with AMO WABE), **LRTE=224** (used later with AMO LDAT) and **TGRP=240** (pre-configured with AMO BUEND)

```
ADD-RICHT:MODE=CD,LRTE=224,CD=224,CPS=0,SVC=ALL,NAME="OSV & MEDIA►
TRIX",TGRP1=240,DESTNO=240,DNNO=218,PDNNO=1-1-218,CHARCON=NEUTRAL,NOPRCF►
WD=NO,CLNAMEDL=NO;
CHANGE-RICHT:MODE=CD,CD=224,CPS=0,SVC=VCE,TYPE=DTMF,DTMFCNV=FIX,DTMFPULS=PP300;
DIS-RICHT:MODE=CD,CD=224,CPS=0;
H500:  AMO RICHT STARTED

+------------------------------------------------------------------------------+

| ROUTES FOR ALL DPLN                                              SVC = VCE |

|                                                                              |

+-------+------------------+----+-+-------------------------------+-----+----+--+

|CODE   |NAME, CQMAX,      |TGRP|P|          DTMF                 | LRTE|CPAR| F|
```

```
|       |DESTNO AND CPS    |CCNO|L+---+---+---------------+-----+     |     | W|
|       |          1 111112|    |B|CNV|DSP|      TEXT      |PULS |     |     | D|
|       |12345 67890 123452|    | |   |   |                |PAUSE|     |     | B|
+-------+------------------+----+-+---+---+----------------------+-----+----+--+
|224    |..... ..... ......| 240| | F | W |                |PP300|  224|     |  |
|NEUTRAL|OSV & MEDIATRIX   |    | |   |   |                |     |     |     |  |
|       |DNNO:         218 |    | |   |   |                |     |     |     |  |
|       |PDNNO: 1 -1  -218 |    | |   |   |                |     |     |     |  |
|       |DESTNO   :240     |    | |   |   |                |     |     |     |  |
|       |ROUTOPT  :YES     |    | |   |   |                |     |     |     |  |
|       |REROUT   :YES     |    | |   |   |                |     |     |     |  |
+-------+------------------+----+-+---+---+----------------+-----+-----+----+--+
+-------------------------------------------------------------------------------+
| ROUTES FOR ALL DPLN                                                SVC = FAX  |
|                                                                               |
+-------+------------------+----+-+-------------------------------+-----+----+--+
|CODE   |NAME, CQMAX,      |TGRP|P|          DTMF                 | LRTE|CPAR| F|
|       |DESTNO AND CPS    |CCNO|L+---+---+---------------+-----+     |     | W|
|       |          1 111112|    |B|CNV|DSP|      TEXT      |PULS |     |     | D|
|       |12345 67890 123452|    | |   |   |                |PAUSE|     |     | B|
+-------+------------------+----+-+---+---+----------------------+-----+----+--+
|224    |..... ..... ......| 240| |   |   |                |     |  224|     |  |
|NEUTRAL|OSV & MEDIATRIX   |    | |   |   |                |     |     |     |  |
|       |DNNO:         218 |    | |   |   |                |     |     |     |  |
|       |PDNNO: 1 -1  -218 |    | |   |   |                |     |     |     |  |
|       |DESTNO   :240     |    | |   |   |                |     |     |     |  |
|       |ROUTOPT  :YES     |    | |   |   |                |     |     |     |  |
|       |REROUT   :YES     |    | |   |   |                |     |     |     |  |
```

```
+-------+-----------------+----+-+---+---+--------------+-----+-----+----+--+
+-------------------------------------------------------------------------+
| ROUTES FOR ALL DPLN                                              SVC = DTE |
|                                                                         |
+-------+-----------------+----+-+-----------------------------+-----+----+--+
|CODE   |NAME, CQMAX,     |TGRP|P|          DTMF               | LRTE|CPAR| F|
|       |DESTNO AND CPS   |CCNO|L+---+---+----------------+-----+     |    | W|
|       |          1 111112|    |B|CNV|DSP|      TEXT      |PULS |     |    | D|
|       |12345 67890 123452|    | |   |   |                |PAUSE|     |    | B|
+-------+-----------------+----+-+---+---+----------------------+-----+----+--+
|224    |..... ..... ......| 240| |   |   |                |     |  224|    |  |
|NEUTRAL|OSV & MEDIATRIX   |    | |   |   |                |     |     |    |  |
|       |DNNO:         218 |    | |   |   |                |     |     |    |  |
|       |PDNNO: 1 -1  -218 |    | |   |   |                |     |     |    |  |
|       |DESTNO   :240     |    | |   |   |                |     |     |    |  |
|       |ROUTOPT  :YES     |    | |   |   |                |     |     |    |  |
|       |REROUT   :YES     |    | |   |   |                |     |     |    |  |
+-------+-----------------+----+-+---+---+----------------+-----+-----+----+--+
AMO-RICHT-111       TRUNK ROUTING
DISPLAY COMPLETED;
```

AMO LODR defines the outdial rule.

Example for AMO LODR with **ODR=240** (use for AMO LDAT).

```
ADD-LODR:ODR=240,CMD=OUTPULSE,DGTS=4989722;
ADD-LODR:ODR=240,CMD=ECHO,FIELD=1;
ADD-LODR:ODR=240,CMD=NPI,NPI=ISDN,TON=INTERNAT;
ADD-LODR:ODR=240,CMD=END;
ADD-LODR:ODR=240,INFO="OSV";
DIS-LODR:ODR=240;
H500:  AMO LODR  STARTED
   +-----------------------------------------------------+
   |  ODR     POSITION  CMD         PARAMETER            |
   +--------+--------------------------------------------+
```

```
   |  240   |      1    OUTPULSE    4989722               |
   |        |      2    ECHO        1                     |
   |        |      3    NPI         ISDN                  |
   |        |      4    TON         INTERNAT              |
   |        |      5    END                               |
   +--------+-----------------------------------------------+
   |INFO:OSV                                              |
   +------------------------------------------------------+
H03: THE NEXT FREE ODR IS 2


AMO-LODR -111       ADMINISTRATION OF LCR OUTDIAL RULES

DISPLAY COMPLETED;
```

AMO LDAT defines the least cost routing data.

Example for AMO LDAT with **TGRP=240** (defined with AMO BUEND), **ODR=240** (defined with AMO LODR) and **LROUTE=224** (defined with AMO RICHT)

```
ADD-LDAT:LROUTE=224,LSVC=ALL,LVAL=1,TGRP=240,ODR=240,LAUTH=16,CARRI►
ER=1,ZONE=EMPTY,VCCYC=4;
DIS-LDAT:TYPE=ALL,LROUTE=224;
H500:  AMO LDAT  STARTED

+-------------------------------------------------------------------------------+
| LROUTE = 224                NAME = OSV & MEDIATRIX           SERVICE =  ALL |
| TYPE = NWLCR                                  DNNO OF ROUTE  =        218    |
| SERVICE INFO =                                                               |
+------+-----+-----+----+-----+----------+-----------+----------+------+-------+
|      |     |     |    |     | SCHEDULE | CARRIER   |          |      |       |
|LRTEL | LVAL|TGRP | ODR|LAUTH| ABCDEFGH |       ZONE|    LATTR | LDSRT|COTIDX |
+------+-----+-----+----+-----+----------+-----------+----------+------+-------+
|     1|    1|  240| 240|16   | ******** | 1    EMPTY|          |      | 0     |
+-------------------------------------------------------------------------------+
```

```
AMO-LDAT -111        LCR-DIRECTIONS

DISPLAY COMPLETED;
```

14.7.5 Configuration on OpenScape Voice

The following sections show the trunking configuration toward the OpenScape 4000 on OpenScape Voice side.

14.7.5.1 OpenScape Voice Endpoint Profile

Common Management Platform > OpenScape Voice > Business Group > Profiles > Endpoint Profile

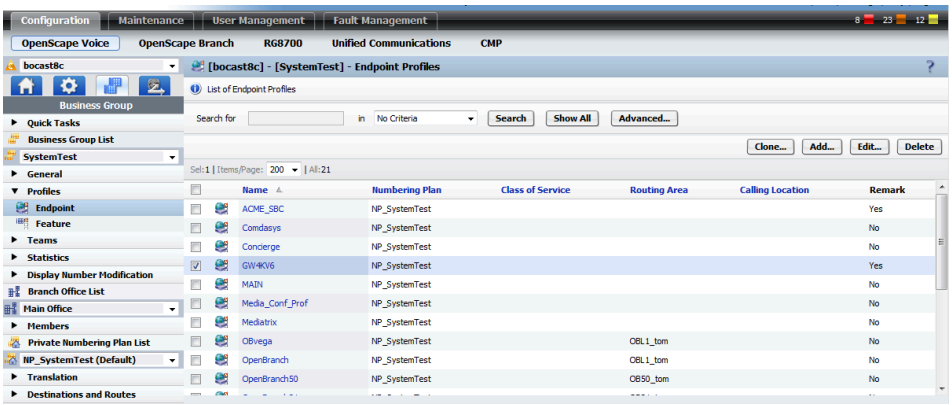


Figure 274: OpenScape Voice: Endpoint profile configuration

Endpoint profile folder **General**:

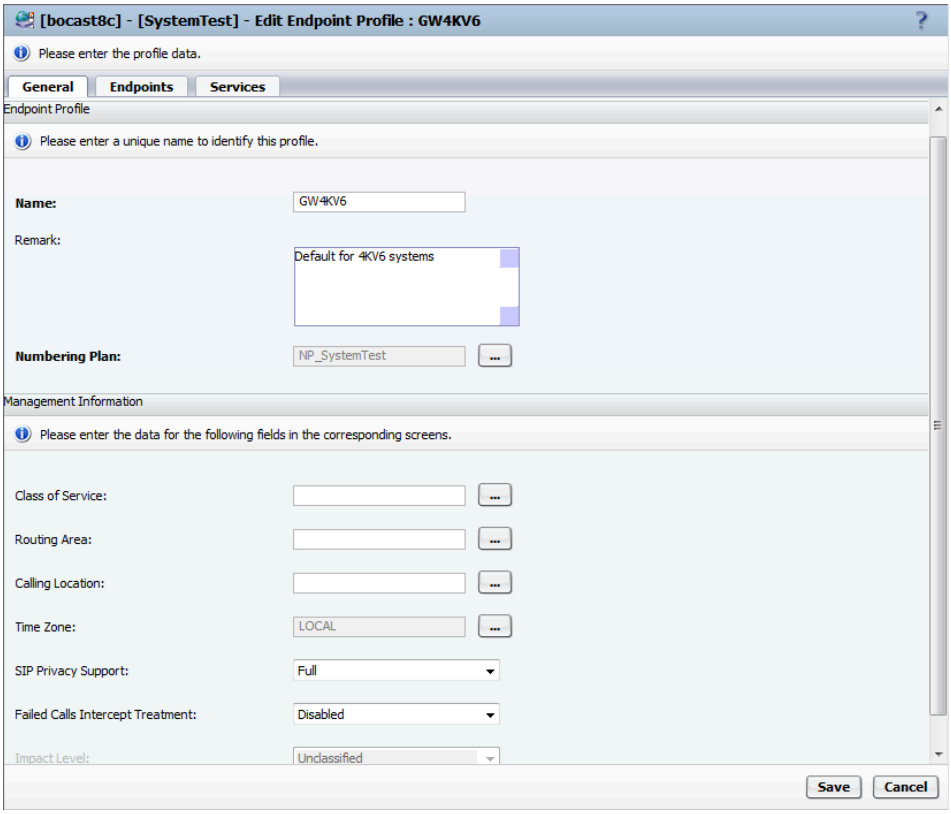


Figure 275: OpenScape Voice: Endpoint folder “General”

Endpoint profile folder **Services**:

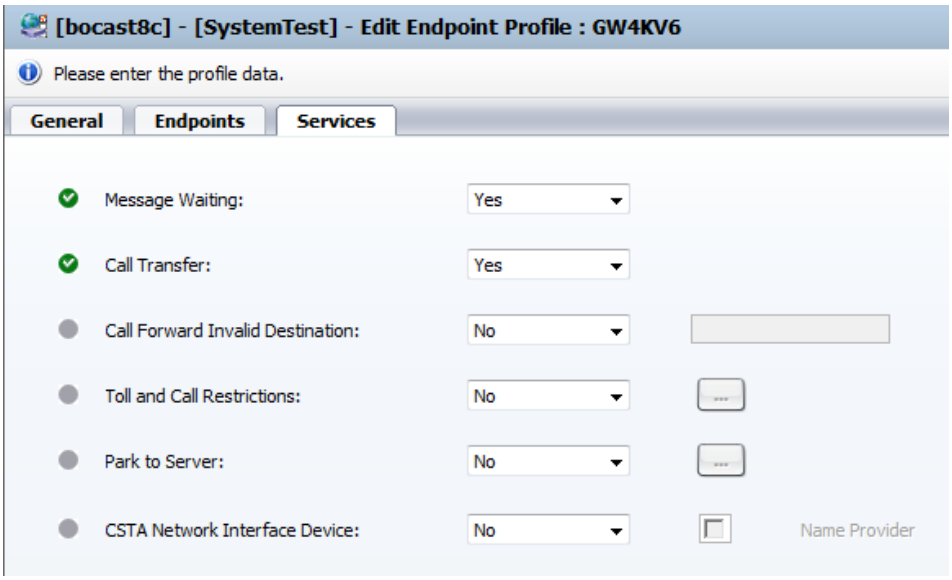


Figure 276: OpenScape Voice: Endpoint folder “Services”

14.7.5.2 OpenScape Voice Endpoint

Common Management Portal > OpenScape Voice > Business Group > Main Office > Members > Endpoints > Name (e.g 4kv6IPDA)

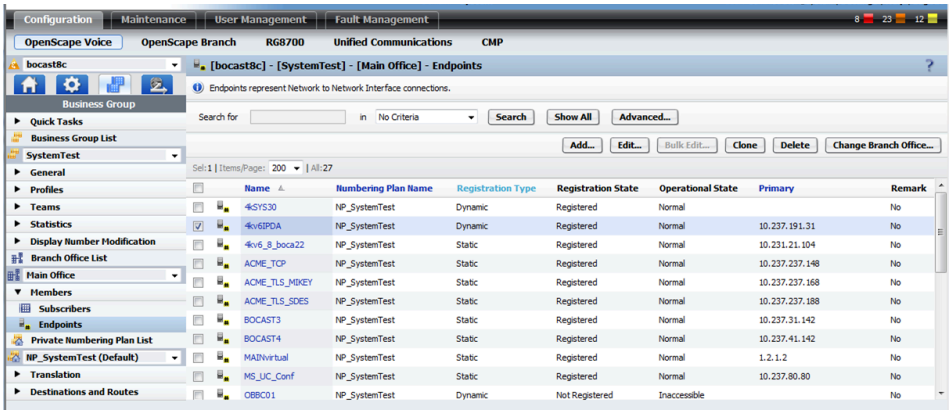


Figure 277: OpenScape Voice: Endpoint configuration

Endpoint toward the OpenScape 4000 folder “General”:

Name definition and profile:

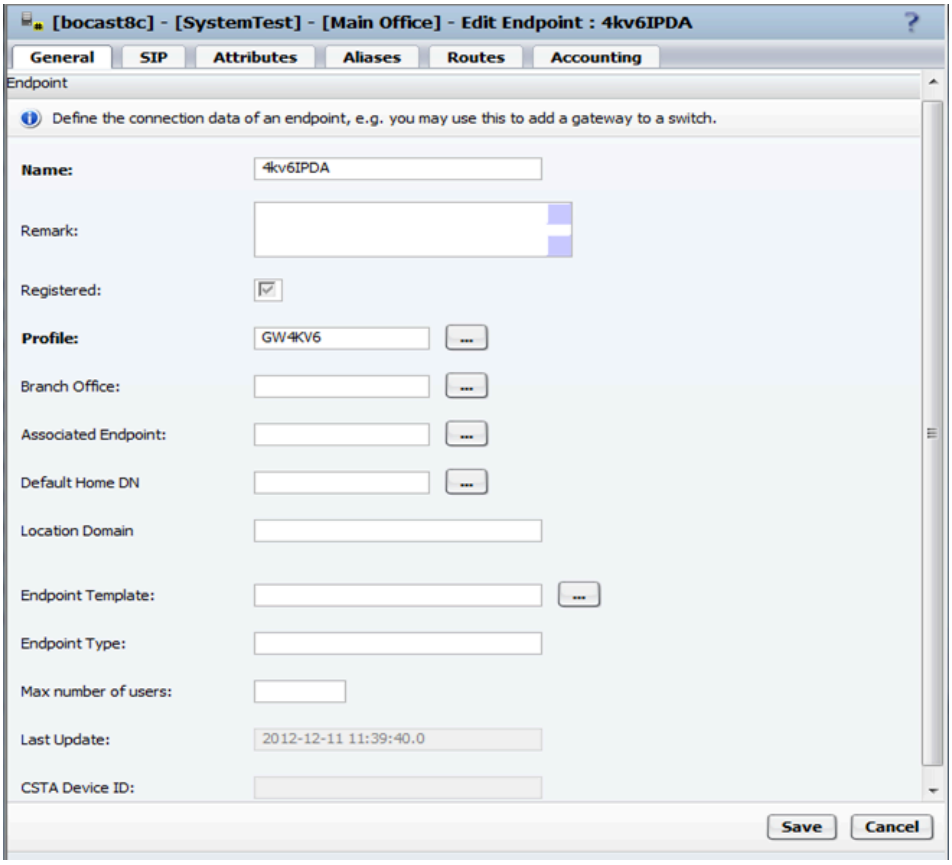


Figure 278: OpenScape Voice: Endpoint toward OpenScape 4000 folder “General”

The check box **Registered** appears automatically when the HG 35xx is defined as **Dynamic** and is in state **Registered**.

Endpoint toward the OpenScape 4000 folder “SIP” requirements:

- **SIP-Q Signaling** (activate with radio button)
- IP-Address for HG 35xx (**Endpoint Address**)

- **Transport protocol** (TCP)

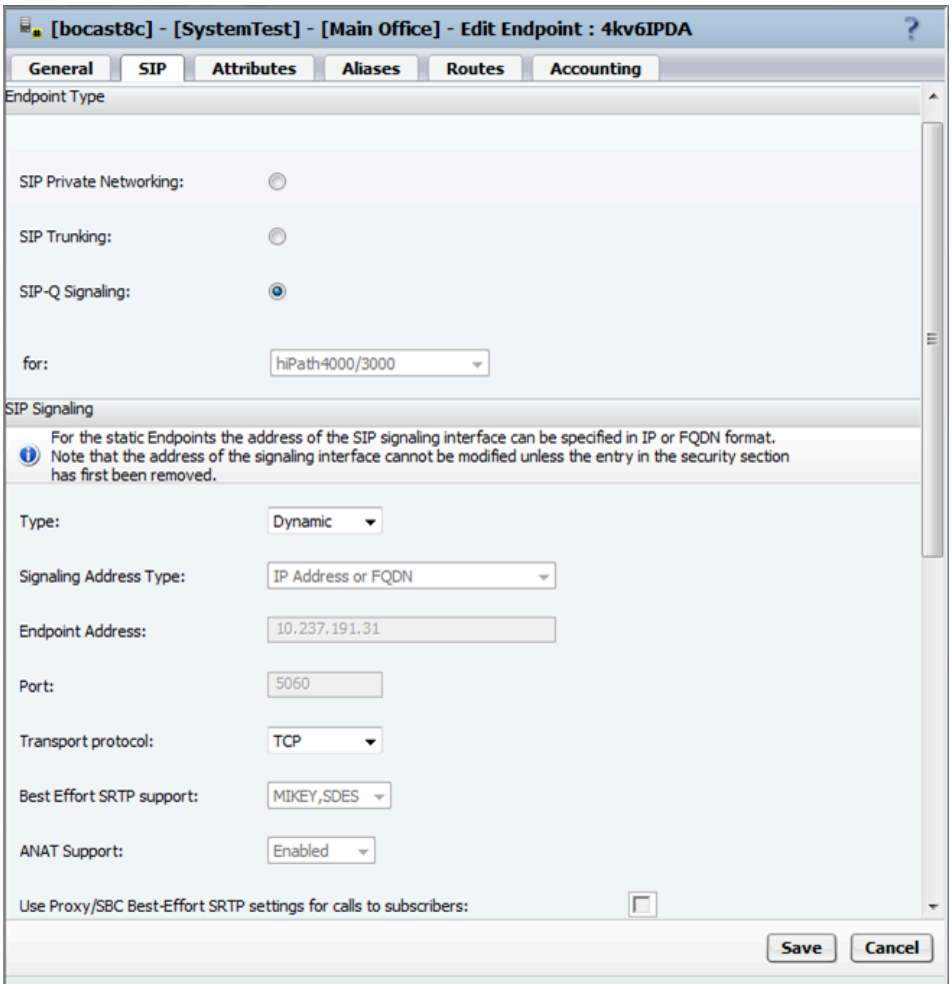


Figure 279: OpenScape Voice: Endpoint toward OpenScape 4000 folder “SIP”

Endpoint toward the OpenScape 4000 folder “Attributes”:

Only **Enable Session Timer** is required.

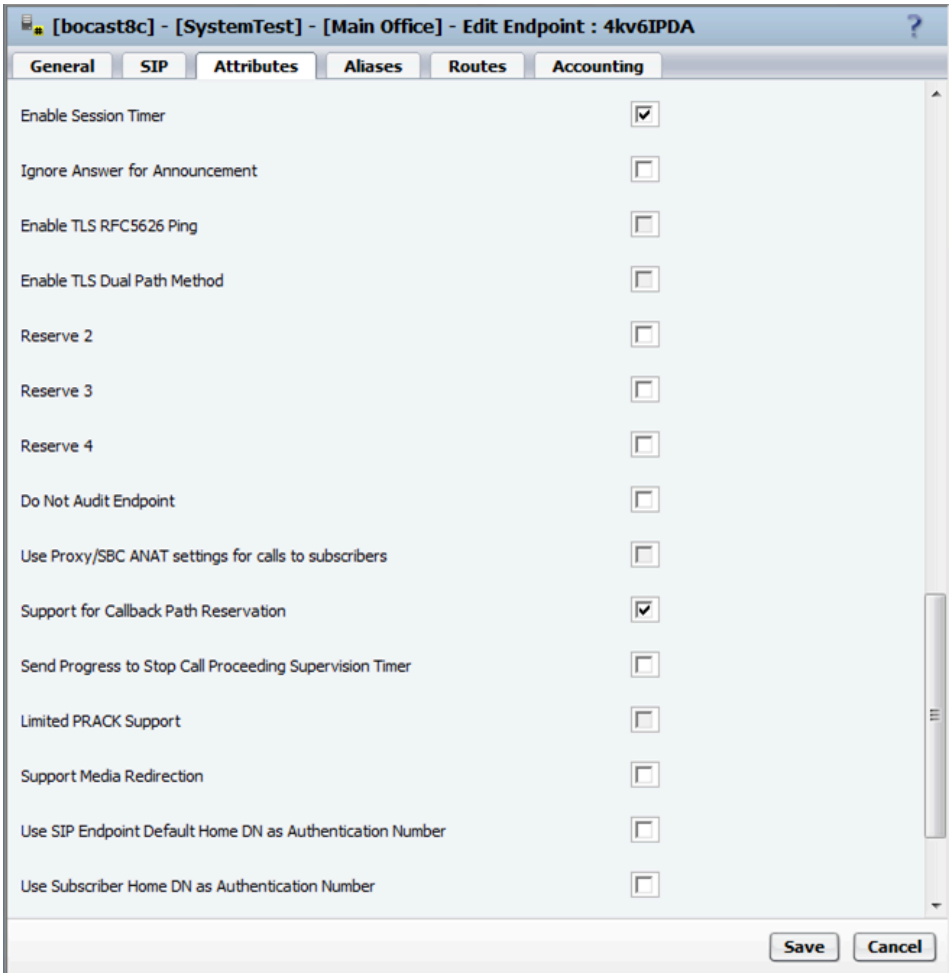


Figure 280: OpenScape Voice: Endpoint toward OpenScape 4000 folder "Attributes"

IMPORTANT: Support for **Callback Path Reservation** is especially important for Unified Communication!

Endpoint toward the OpenScape 4000 folder "Aliases":

Insert the IP address of HG 35xx from OpenScape 4000, e.g:

1) 10.237.191.31 (check with AMO CGWB on OpenScape 4000 side).

   Insert the **GWDIRNO** from OpenScape 4000, e.g:

   166 (check with AMO CGWB on OpenScape 4000 side).

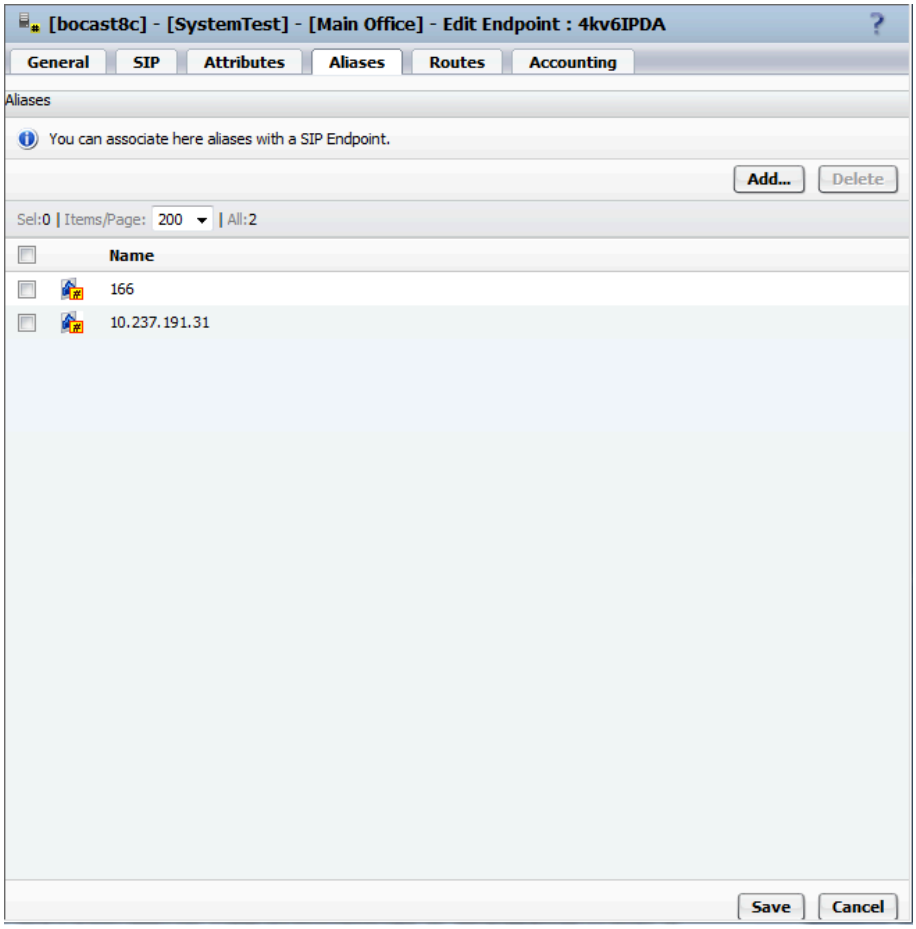


Figure 281: OpenScape Voice: Endpoint toward OpenScape 4000 folder "Aliases"

All these names are defined in OpenScape4000 with AMO CGWB.

IP address of HG 35xx:

```
ADD-CGWB:LTU=22,SLOT=2,SMODE=NORMAL,IPADR=10.237.191.31,NETMASK=255.255.255.0;
```

HG 3550 LEGKDATA for **GWDIRNO** and **REGEXTGK**:

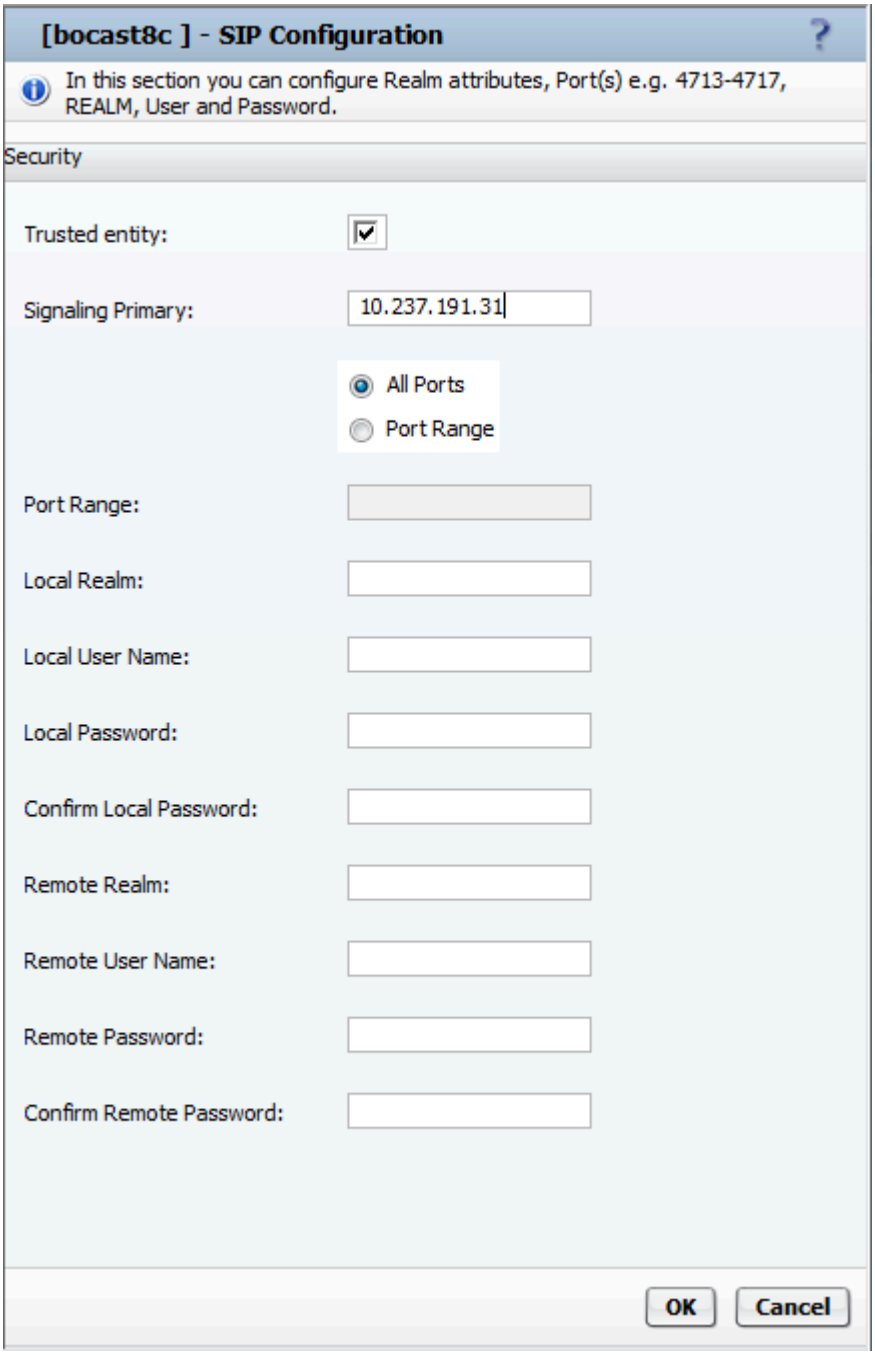
```
CHANGE-CGWB:MTYPE=CGW,LTU=22,SLOT=2,TYPE=LEGKDATA,GWDIRNO=166,REGEXTGK=YES;
```

NOTICE: REGEXTGK can also be set to NO, however a GWNO will then need to be added.

14.7.5.3 Set IP-Address for OpenScape 4000 to trusted in case of Digest Authentication

Common Management Portal > OpenScape Voice > Administration > Signaling Management > Digest Authentication > Realms > Add

Activate the **Trusted Entity** checkbox and enter the IP address for **Signaling Primary** (e.g: 10.237.191.31 (HG 35xx of OpenScape 4000))



OpenScape Voice: Set IP address for OpenScape 4000 to trusted

14.7.6 DNS-SRV for HG 3500

AMO CGWB requires the following items:

Configure the IP address of the DNS-SRV server (**DNSIPADR**) in **TYPE=GLOBIF**.

```
CHANGE-CGWB:MTYPE=CGW,LTU=22,SLOT=5,TYPE=GLOBIF,DNSIPADR=10.237.1.3;
```

Configure the **GWDIRNO** in **TYPE=LEGKDATA** which is also used for the **Account Name** in the SIP Trunk Profile.

```
CHANGE-CGWB:MTYPE=CGW,LTU=22,SLOT=5,TYPE=LEGKDATA,GWDIRNO=166,REGEXTGK=YES;
```

NOTICE: REGEXTGK can also be set to NO, however a GWNO will then need to be added.

Configure **SIPREG=NO** in **TYPE=SIPTRSSA** to use SIP Trunk Profile.

```
CHANGE-CGWB:MTYPE=CGW,LTU=22,SLOT=5,TYPE=SIPTRSSA,SIPREG=NO;
```

IMPORTANT: For DNS-SRV the SIP Trunk Profile **SIPQTrkWithRegistration** found in the Web GUI of the gateway has to be used.

14.7.6.1 Example of Web-GUI for Geo-Separated OpenScape Voice with TLS Configuration

WBM > Configuration > Voice Gateway > SIP Trunk Profile Parameter

Use Profiles for Trunks via SIP-Q must be enabled/set to **Yes**.

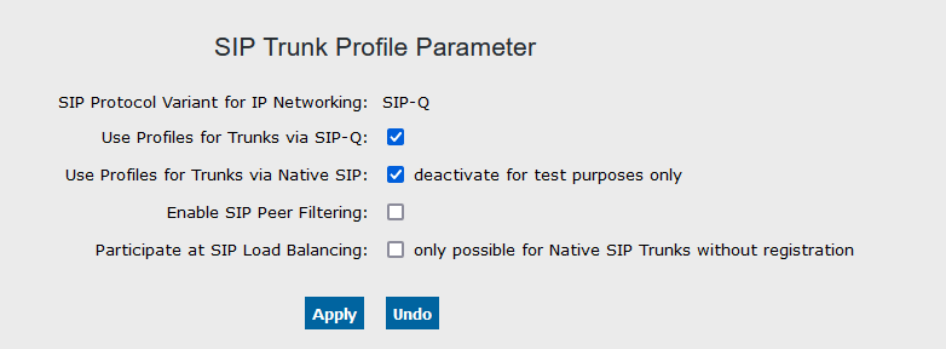


Figure 282: OpenScape 4000: Use profiles for SIP trunks

DNS-SVR records:

nd08a.st.lz.com leads to

sipsm3 on node1

sipsm4 on node2.

WBM > Configuration > Voice Gateway > SIP Trunk Profiles

Use DNS-SRV-host-names for Registrar and Proxy addresses, set Port=0.

The **SIP Transport Protocol** is not configurable. The **Security** section is at the bottom of the pull down section and is used to set MIKEY or SDES parameters if SPE is to be used.

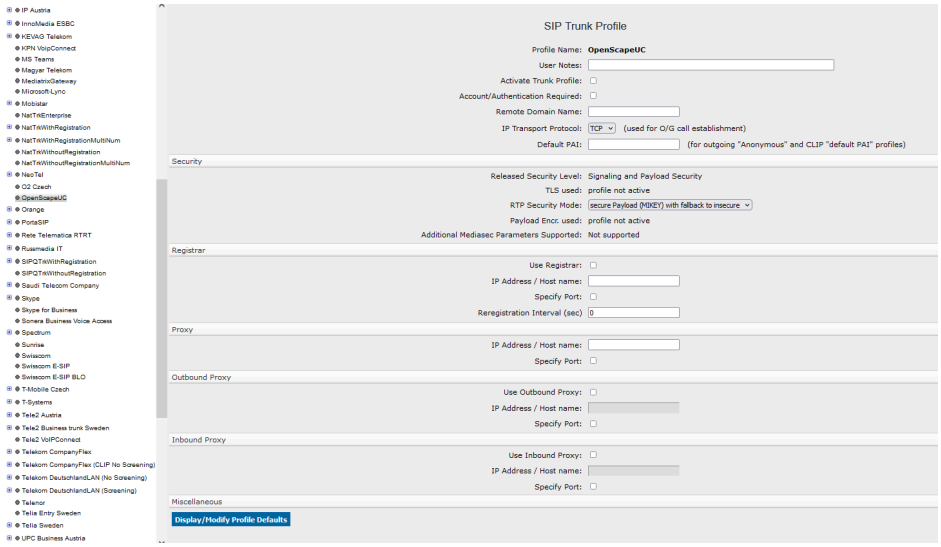


Figure 283: OpenScape 4000: Properties of SIP trunk profile "SIPQTrkWithRegistration"

WBM > Configuration > Voice Gateway > SIP Trunk Profiles > SIPQTrkWith Registration

Edit the **Account Name** (same as in AMO CGWB parameter **GWDIRNO**) and apply.

Now you must activate the profile with right click on **SIPQTrkWithRegistration**. The folder shows RED if not registered with OpenScape Voice or OpenScape Branch. It shows GREEN  when registration is successful.

14.7.6.2 Branch Example with Geo-Separated OpenScape Voice and TLS

In branch scenarios (with Survivability-Proxy, e.g. OpenScape Branch or Comdasys) you can have two DNS server entries, one for the local branch-proxy and a central one. Specify the DNS servers in AMO CGWB under parameters **DNSIPADR** and **DNSIPADR2**. In this example the network only has one DNS server.

DNS-SVR-records:

br08a2.st.lz.com leads to:

Branch-proxy

Sipsm3 on node1

Sipsm4 on node2.

nd08a.st.lz.com leads to:

Sipsm3 on node1

Sipsm4 on node2.

WBM > Configuration > Voice Gateway > SIP Trunk Profiles > SIPQTrkWith Registration

Section **Outbound Proxy**:

Activate the checkbox **Use Outbound Proxy** and insert the DNS-SRV-host-name/IP address (**IP Address / Host name** (e.g.: br08a2.st.lz.com)) for OpenScape Branch.

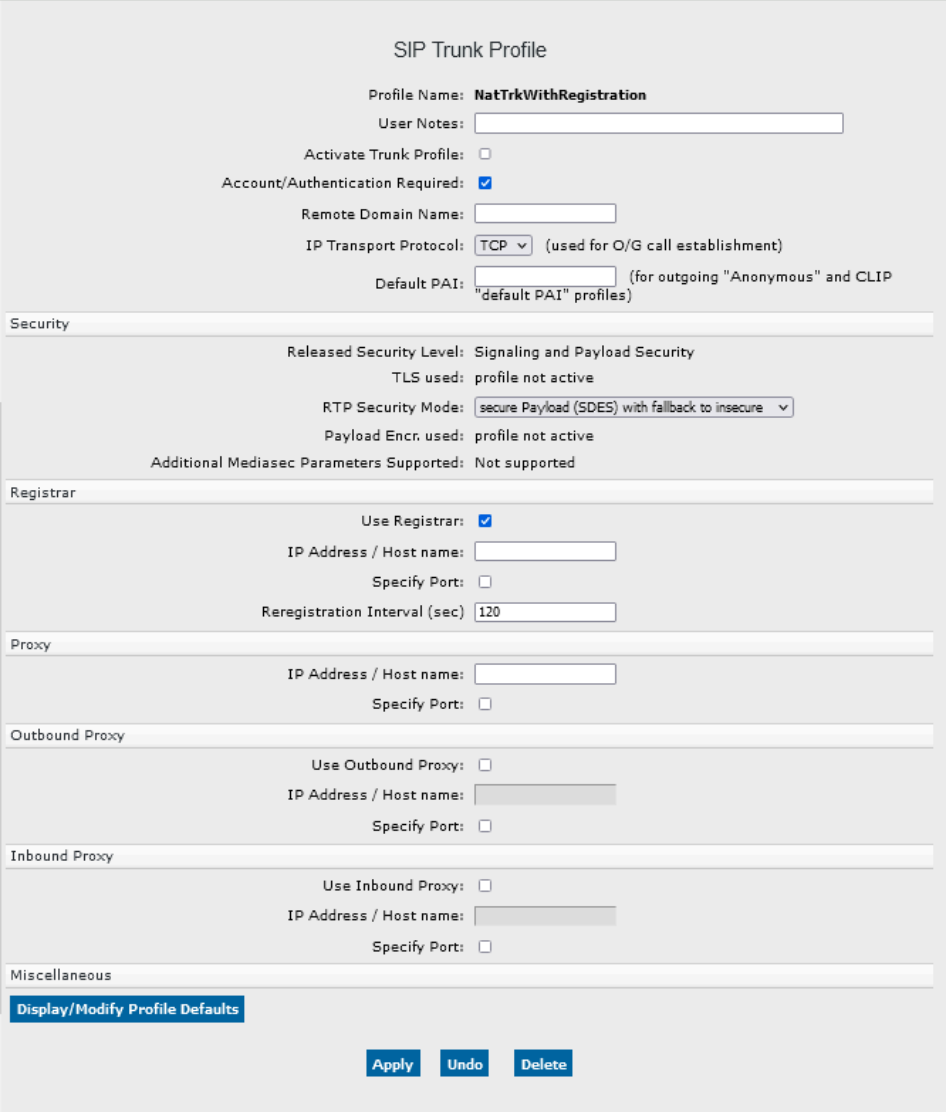


Figure 284: OpenScape 4000: IP address/host name of OpenScape Branch

14.7.7 Signaling and Payload Encryption (SPE)

IMPORTANT: The virtual HG 3500 gateways can be configured to offer either MIKEY or SDES operation but not **both** at the same time. The HG 3500 gateways can be configured for MIKEY only.

NOTICE: The following steps are the minimum required settings to enable secure calls using MIKEY or SDES encryption over a HG 3500 gateway configured directly between OpenScape 4000 and OpenScape Voice systems.

NOTICE: SDES is supported only by virtual HG 3500 gateways on OpenScape 4000 SoftGate.

IMPORTANT: All OpenScape Voice and OpenScape 4000 systems must be timed accurately using an NTP time server. **Over** 60 seconds difference and registration and security will not be possible.

1) Copy the system default security certificates from the OpenScape Voice to your work station. These certificates are located in the `/usr/local/ssl/certs` for the `client.pem` and in the `/usr/local/ssl/private` directory for the `root.pem`.
2) There are dedicated TLS ports on the OpenScape Voice. They can be displayed by logging on as SRX user and executing the following command from the SRX directory:

   $ startup/srxqry <cr/enter>
3) This provides a long output for each node but look for the entry that shows:

   SIP TLS Auth Vip: 10.237.84.104 Up ....for IPV4 address

   SIP TLS Auth Vip: fd00:10:237:84::104 Up ....for IPV6 address

4) OpenScape Voice configuration: Add or modify an Endpoint. Required here is **SIP-Q Signaling** with the **Port** set to **5061** and the **Transport protocol** is set to **MTLS**.

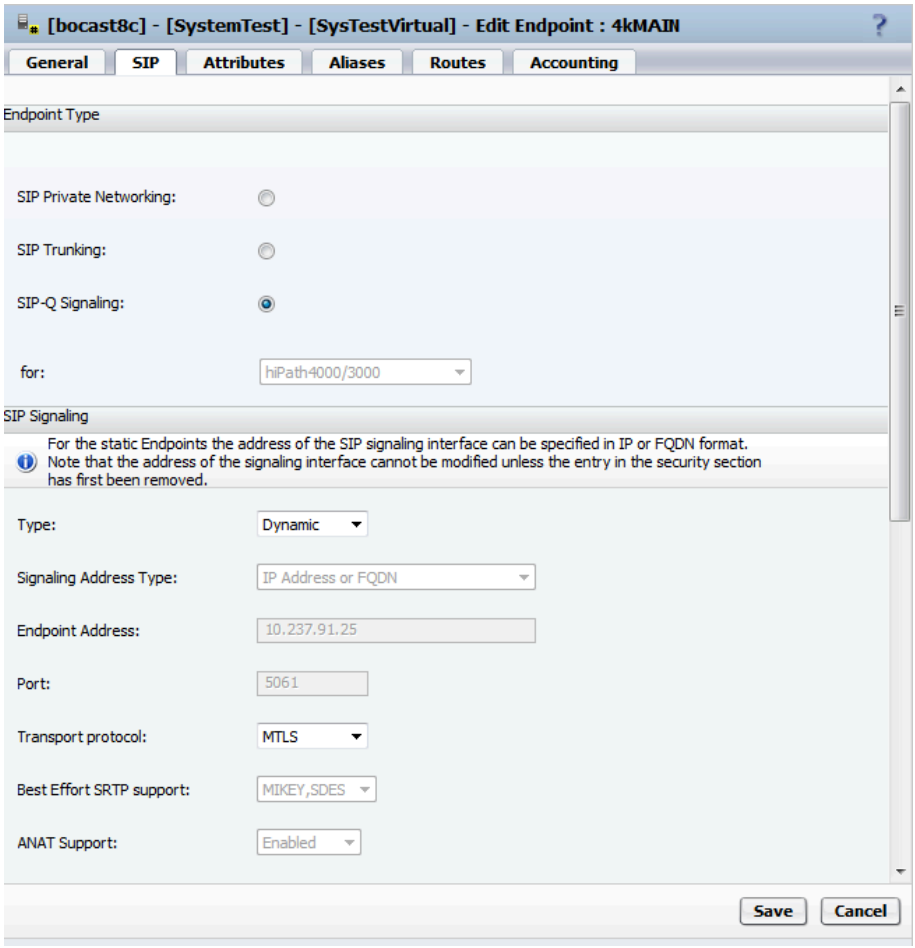


Figure 285: OpenScape Voice: Signaling and Payload Encryption: Endpoint configuration

On OpenScape 400

1) AMO ZANDE for **TYPE=SECURITY** must have **SPESUPP=YES**, **SECIPSB=SECURE** and **SECIPTR=SECURE**.
2) AMO TDCSU must have **SECLEVEL=SECURE**.
3) AMO CGWB for both HFA and trunk configuration must have **SECSUBS=YES** and **SECTRNK=YES**. The **REGIP1** and **REGIP2** parameters should use the OpenScape Voice TLS port IDs (if the OpenScape Voice is a duplex) as determined from *step 2*.
4) The certificates are now copied to the HG 35xx board by logging on to the WBM.

5) Select **Configuration > Security > Signaling and Payload Encryption (SPE) > Import SPE certificate..**



Figure 286: OpenScape 4000: Signaling and Payload Encryption: Load SPE CA certificate

It is advised to install the certificates in the following order:

First load the SPE CA Certificate using the **root.pem**. Right 'click' on **SPE CA Certificate** to **Import trusted CA Certificate**. This will now open a new session of the browser titled **Load a SPE CA Certificate via HTTP**. Use the **Browse** button to locate and select the `root.pem` file on your workstation. Now select **View Fingerprint of Certificate**. After verification of the fingerprint select **OK. Now Import Certificate from File** can be selected.

Do the same process for the SPE Certificate and the `client.pem` file.

Now the gateway registers on the OpenScape Voice using TLS as transport protocol. For payload SRTP with MIKEY encryption is offered.

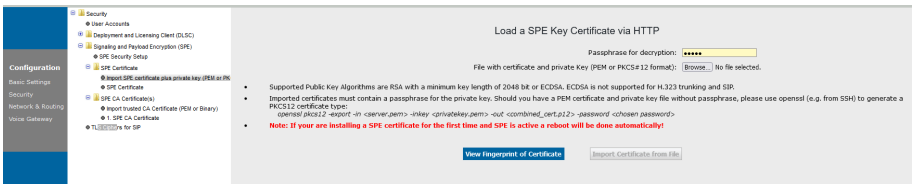


Figure 287: OpenScape 4000: Signaling and Payload Encryption: Load SPE certificate

SDES security is available only with SIP Trunk Profile configuration. No changes on the OpenScape Voice settings are required. Changes are only required only in the OpenScape 4000:

In AMO CGWB **SIPREG** must be set to **NO**:

```
CHANGE-CGWB:MTYPE=CGW,LTU=22,SLOT=2,TYPE=SIPTRSSA,SIPREG=NO;
```

This allows the SIP Trunk Profiles to manage registration from the gateway WBM. These profiles are found and activated by logging on to the WBM,

selecting **Configuration > Voice Gateway > SIP Trunk Profile Parameter**. Right click and select **Edit**.

Use Profiles for Trunks via SIPQ must be enabled/checked and confirm with **Apply**.

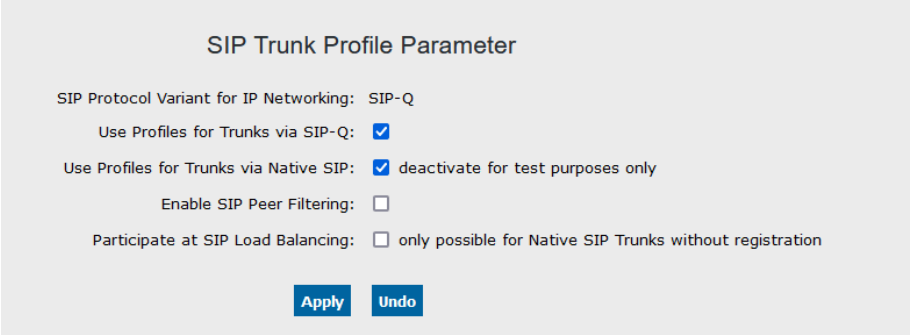


Figure 288: OpenScape 4000: Enable use of profiles for SIP-Q trunks

Now a folder with available for SIP Trunk Profiles is shown. Open this folder, scroll down and select **SIPQTrkWithRegistration**.

Enter the necessary data for the Registrar. The **IP Address / Host name** should be a DNS-SRV entry and the **Registration Interval** cannot be set lower than **300** seconds. The Proxy must also be configured with the same information as the Registrar. **Outbound Proxy** is used to connect to

OpenScape Branch or to another Branch/Proxy device. Scroll down to the bottom of this screen and select **SDES security with Fallback to Insecure**.

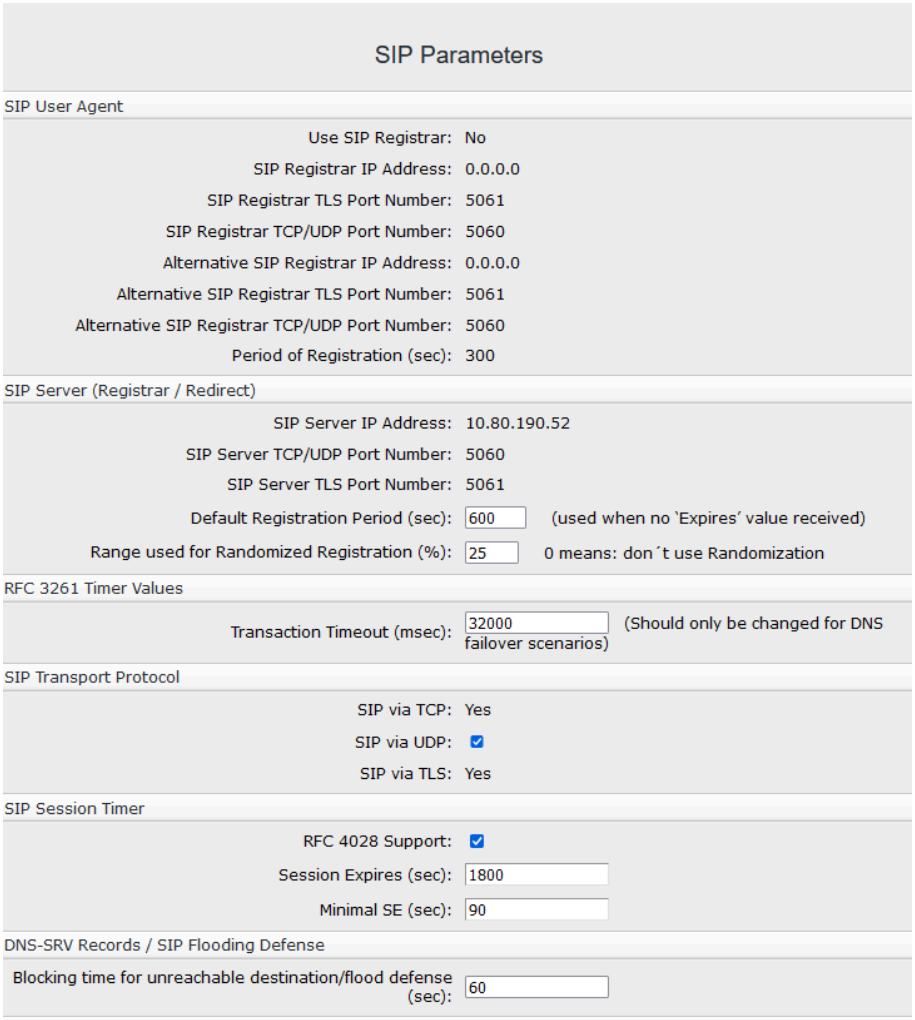


Figure 289: OpenScape 4000: Settings for SIP Trunk Profile

Here you can see how it should look after configuration:

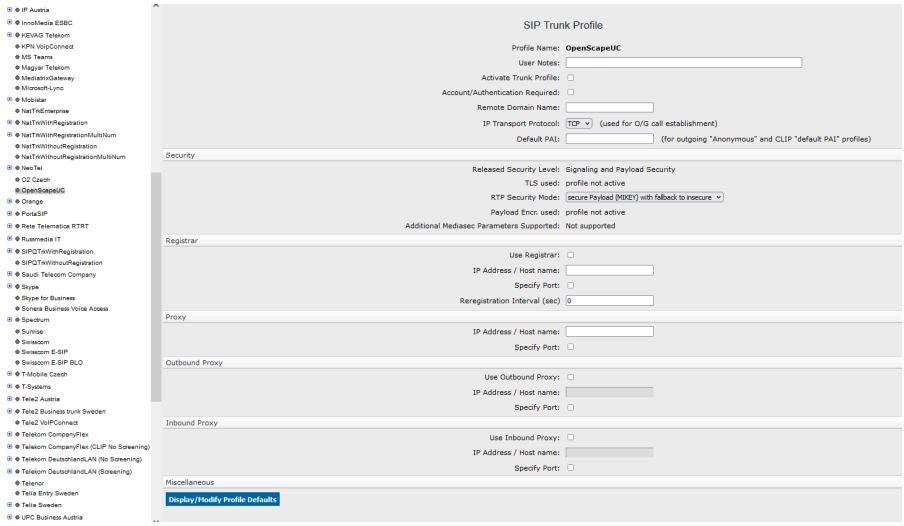


Figure 290: OpenScape 4000: SIP Trunk Profile - Part 1

Select the **RTP Security Mode**:

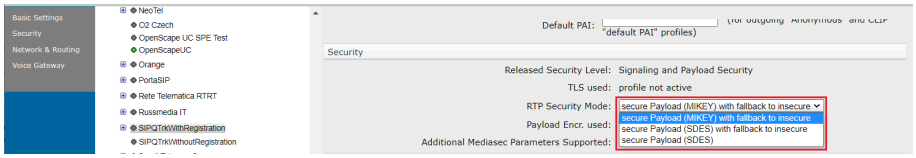


Figure 291: OpenScape 4000: SIP Trunk Profile - Part 2

Now a sub-menu appears to configure the **Account Name**. You can edit the account name by right click. The **Account Name** must be identical with the **GWDIRNO** configured in AMO CGWB, **TYPE=LEGKDATA**.

```
CHANGE-CGWB:MTYPE=CGW,LTU=22,SLOT=2,TYPE=LEGKDATA,GWDIRNO=166,REGEXTGK=NO;
```

Now activate the profile with right click on SIPQTrkWithRegistration.

Save the configuration.

The folder is RED if the gateway is not registered successfully on the

OpenScape Voice and OpenScape Branch. It turns GREEN  when registration was successful.

6) End-to-end secure calling

The OpenScape 4000 and its SIP gateway are now configured to support Signaling and payload security (SPE) on the SIP-Q trunk to the OpenScape Voice. To have end-to-end secure calls which is displayed on the phones, the devices must be configured secure, too. Configure the SIP phones in the same way as the gateway by importing proper OpenScape Voice security

certificates. After the certificates are installed a secure connection icon is displayed on the phones.

IMPORTANT: On the OpenScape Voice both optiPoint and OpenStage devices can be MIKEY, but only OpenStage devices support SDES.

Check the **SIP transport** protocol (should be TLS) for the OpenStage devices and make sure that the **Connectivity check timer** has a value greater than **0** (in this example 100).

OpenStage IP Admin > System > SIP Interface

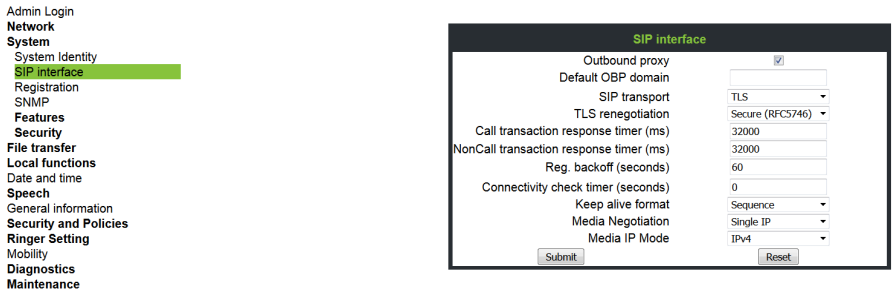


Figure 292: OpenStage: SIP interface settings

Then move to the **Security** section. Select **System** and enable **Use secure calls** and select an **SRTP type**. In case of OpenStage you can choose between **MIKEY** and **SDES**.

OpenStage IP Admin > Security > System

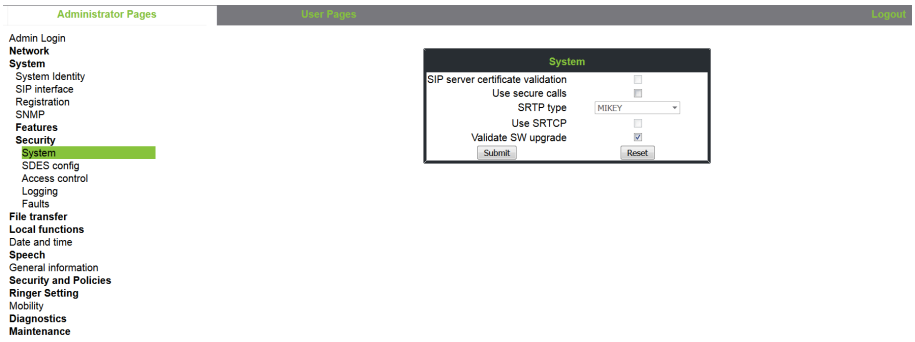


Figure 293: OpenStage: Security settings

Then there is a SDES configuration selection that allows you to change SDP negotiation (by default it is SRTP and RTP) and the priority of the SDES

SHA1-80 or SHA1-32 methods. These can also be left at the defaults which has the SHA1-80 as the highest priority.

For subscribers on the OpenScape Voice the configuration must have **Transport Protocol** set to **TLS** and the **Port** set to **5061**.

Common Management Portal > OpenScape Voice > Business Group > Main Office > Members > Subscribers

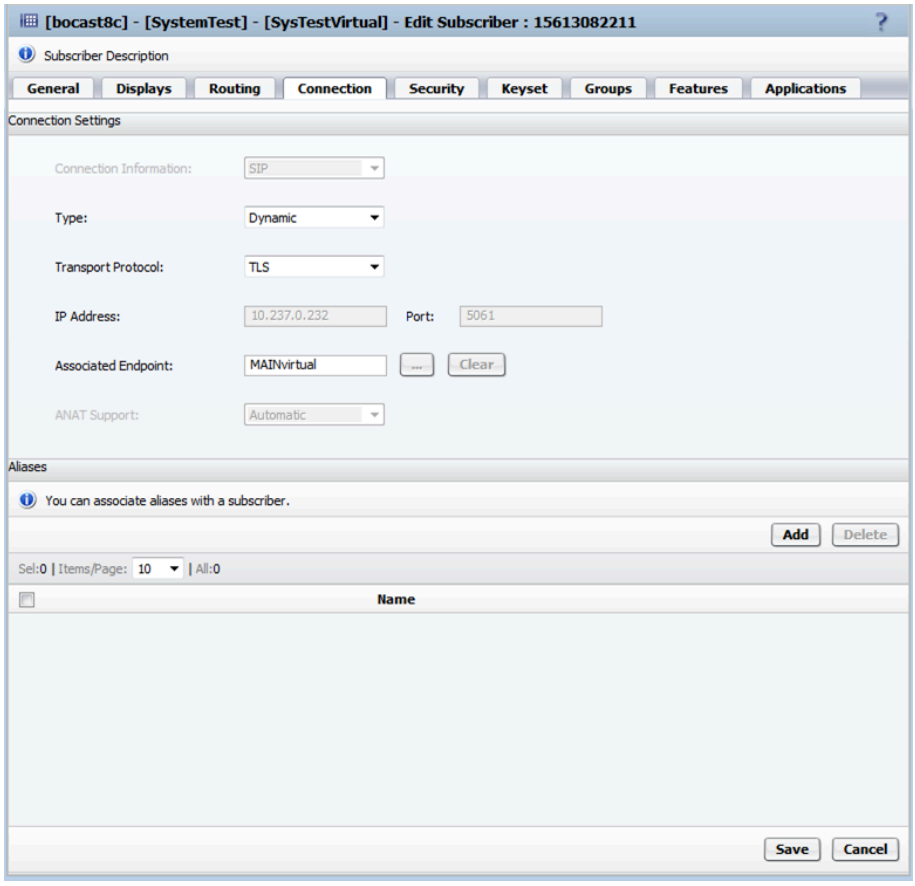


Figure 294: OpenScape Voice: Subscriber configuration > Tab "Connection"

Under the **Security** tab, the **Secure RTP** can be left at its default of **MIKEY, SDES**.

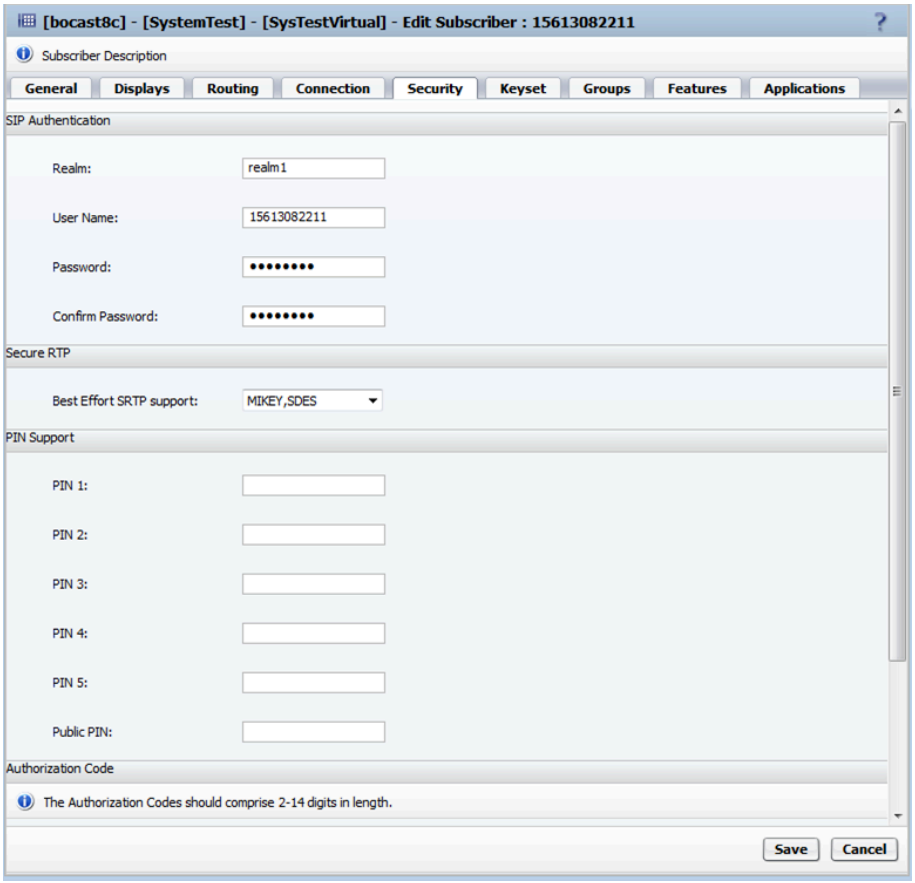


Figure 295: OpenScape Voice: Subscriber configuration > Tab "Security"

NOTICE: The SIP authentication fields are for Digest Authorization and are not required for SPE operation.

14.7.8 OpenScape Voice Route to OpenScape 4000

To access the endpoint a destination and route must be configured.

Common Management Platform > OpenScape Voice > Business Group > Destinations and Routes > Destinations > Add

Navigate to the **Destinations** folder and select **Add**. A new folder opens on the **General** tab.

Create a name for the Destination table (e.g.: 4kv6IPDA) and don't activate the checkbox **is a media server**. Confirm with **Save**.

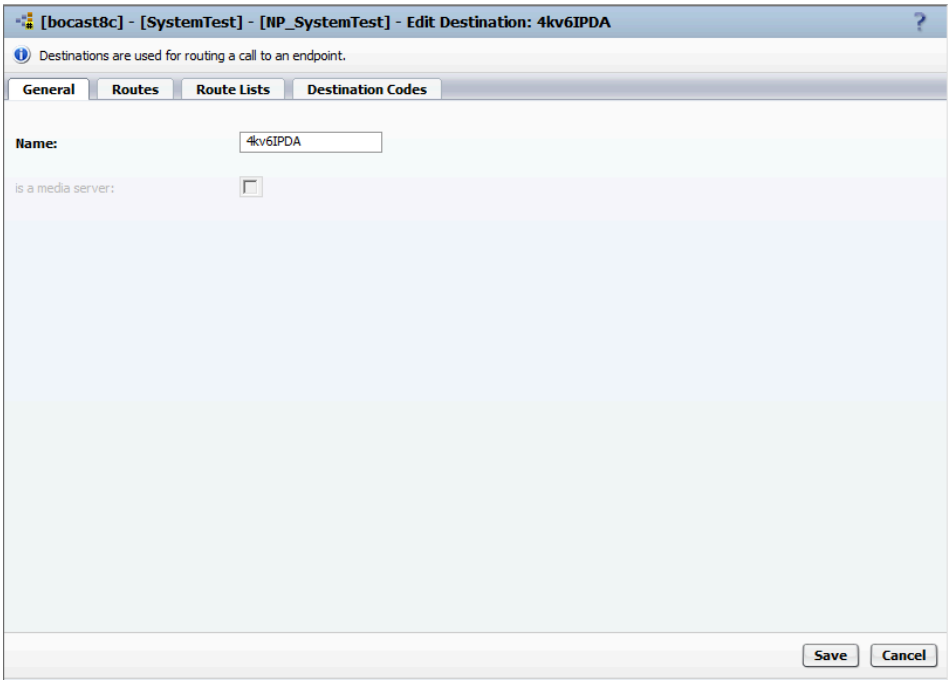


Figure 296: OpenScape Voice: Destination and route configuration

Return to the **Destinations** folder for **4KV6IPDA** and navigate to the tab **Routes** and select **Add**.

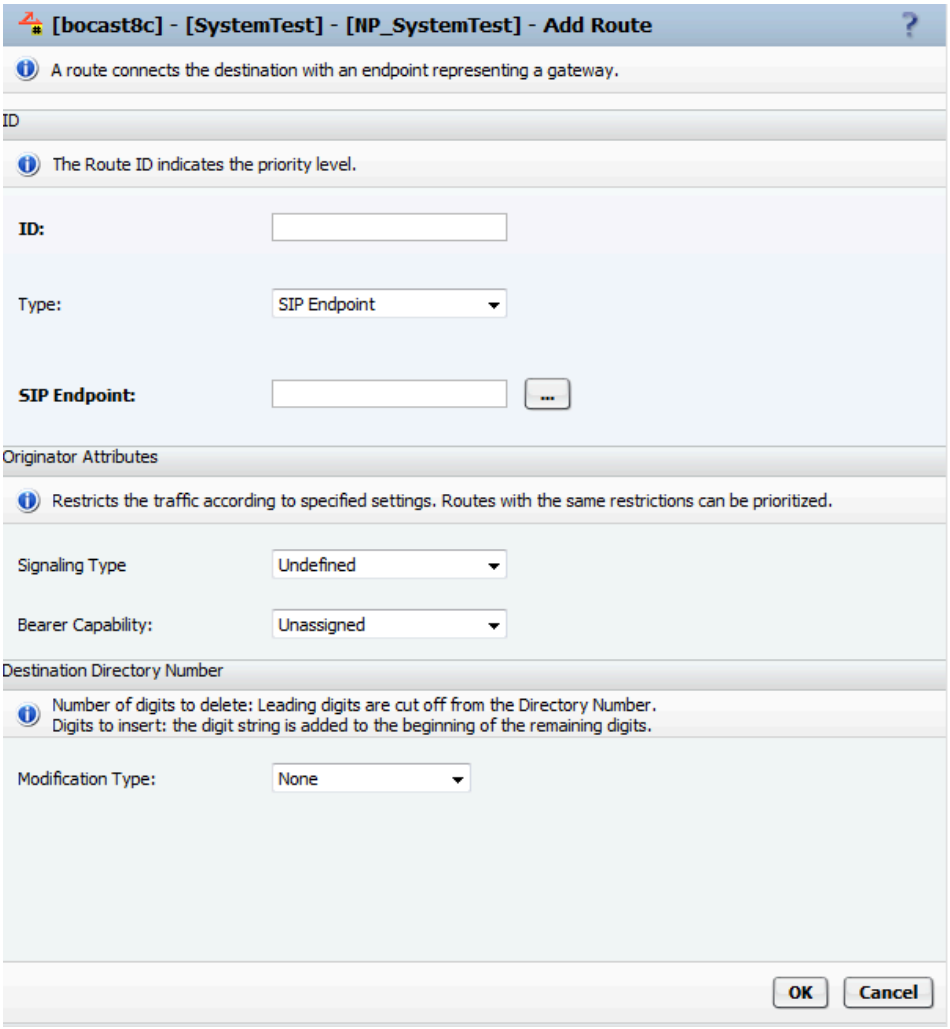


Figure 297: OpenScape Voice: Destination and route configuration

ID: Any number can be used. But typically if it is the first route then use "1". The number of the route ID also indicates the priority level if more than 1 route is configured.

Type: Default is **SIP Endpoint**. Don’t change.

SIP Endpoint: Use menu to select your endpoint, e.g. 4KV6IPDA

Signaling Type: leave the default

Bearer Capability: leave the default

Modification Type: leave the default

Now select **OK** at the bottom of the tab.

14.7.9 OpenScape Voice Routing for International Dialing - Extend Dialed Numbers to International Number

In this configuration we use 5 and 6 digit dialing for internal destination numbers and for external destination numbers toward the OpenScape Voice.

We use E.164 numbering, too.

The destination numbers for the closed numbering are in the range from 31000 to 31249.

For all dialed **Prefix Access Codes** the number is converted to an international E.164 number.

After this number conversion, all useful dialed numbers are existing only one time as E.164 number.

This entry is sent to **BG Common Destination** where the analysis for international E.164 numbers is done.

Common Management Platform > OpenScape Voice > Business Group > Available Private Numbering Plan = "NP_FT_7007" **> Translation > Prefix Access Codes**

14.7.9.1 For 5 or 6 Digit Extension Dialing

Common Management Platform > OpenScape Voice > Business Group > BG_Common > Translation > Prefix Access Codes > Add

- **Prefix Access Code**: 3
- **Minimum Length**: 5
- **Maximum Length**: 6
- **Digits to insert**: 49897007
- **Destination Type**: BG Common Destination
- **Destination Name**: NP_COMMON

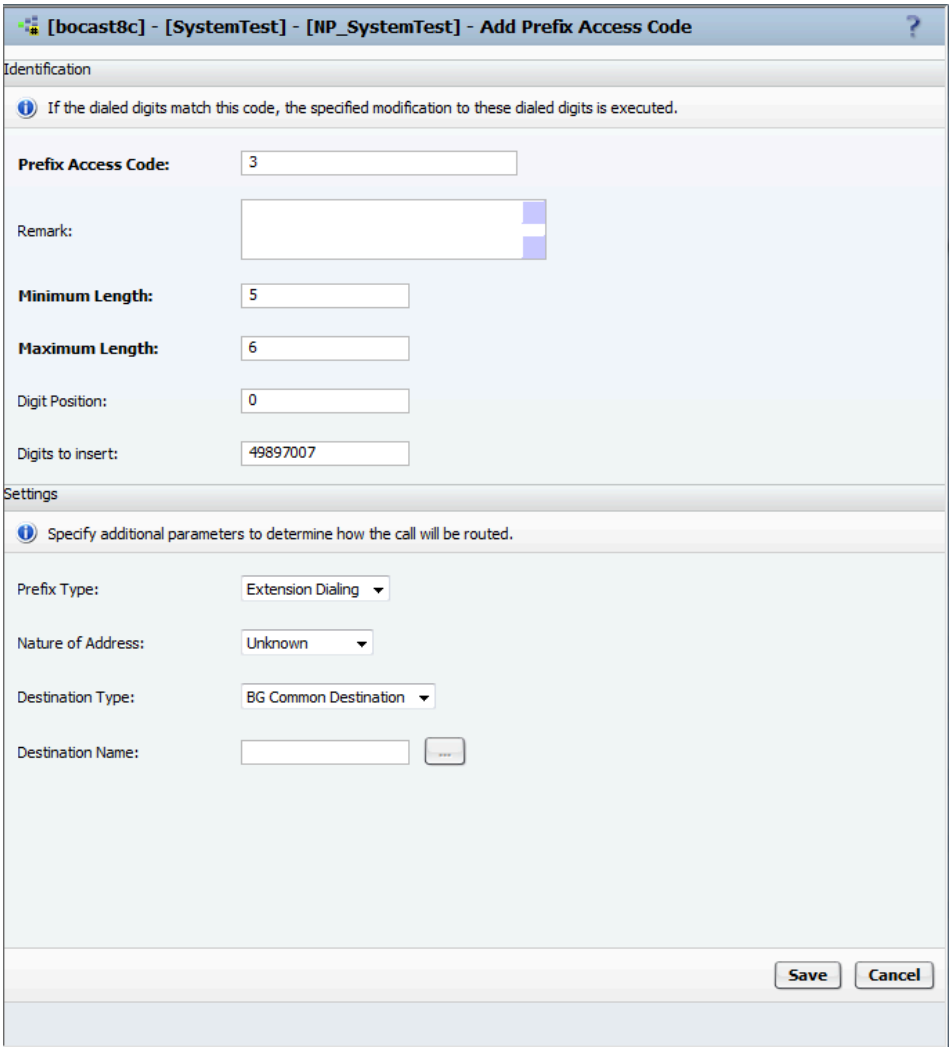


Figure 298: OpenScape Voice: Extend dialed number to international number

14.7.9.2 Dialing with Local Code

Common Management Platform > OpenScape Voice > Business Group > BG_COMMON > Translation > Prefix Access Codes > Add

E.g. 0-7007-3xxxx

- **Prefix Access Code**: 0
- **Minimum Length**: 4
- **Maximum Length**: 30
- **Digit Position**: 1
- **Digits to insert**: 4989 (adds 4989 to dialed string)
- **Destination Name**: NP_COMMON (destination where the number is sent to)

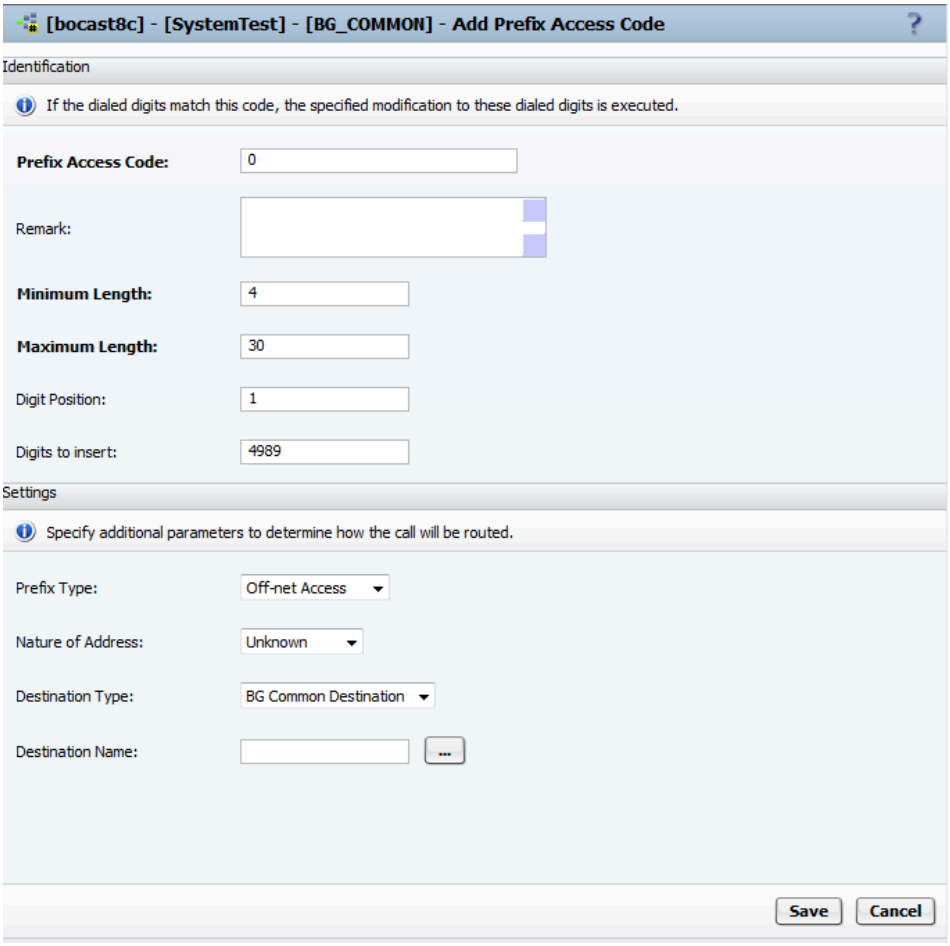


Figure 299: OpenScape Voice: Dialing with local code

14.7.9.3 Dialing with Local Code (Closed Numbering)

Common Management Platform > OpenScape Voice > Business Group > BG_COMMON > Translation > Prefix Access Codes > Add

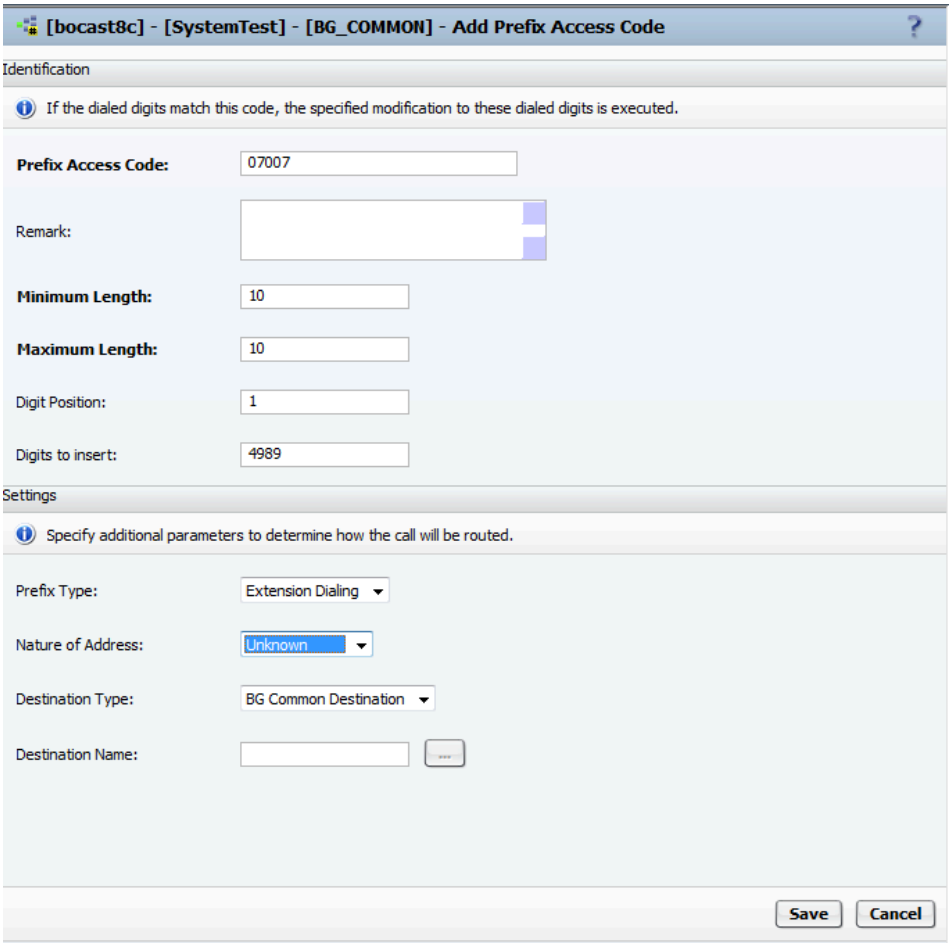


Figure 300: OpenScape Voice: Closed numbering

14.7.9.4 Dialing with National Code

Common Management Platform > OpenScape Voice > Business Group > BG_COMMON > Translation > Prefix Access Codes > Add

E.g. 0-0897007-3xxxx

- **Prefix Access Code**: 00
- **Minimum Length**: 8
- **Maximum Length**: 30
- **Digit Position**: 2 (delete the first 00)
- **Digits to insert**: 49 (adds 49 to dialed string)
- **Destination Name**: NP_COMMON (destination where the number is sent to)

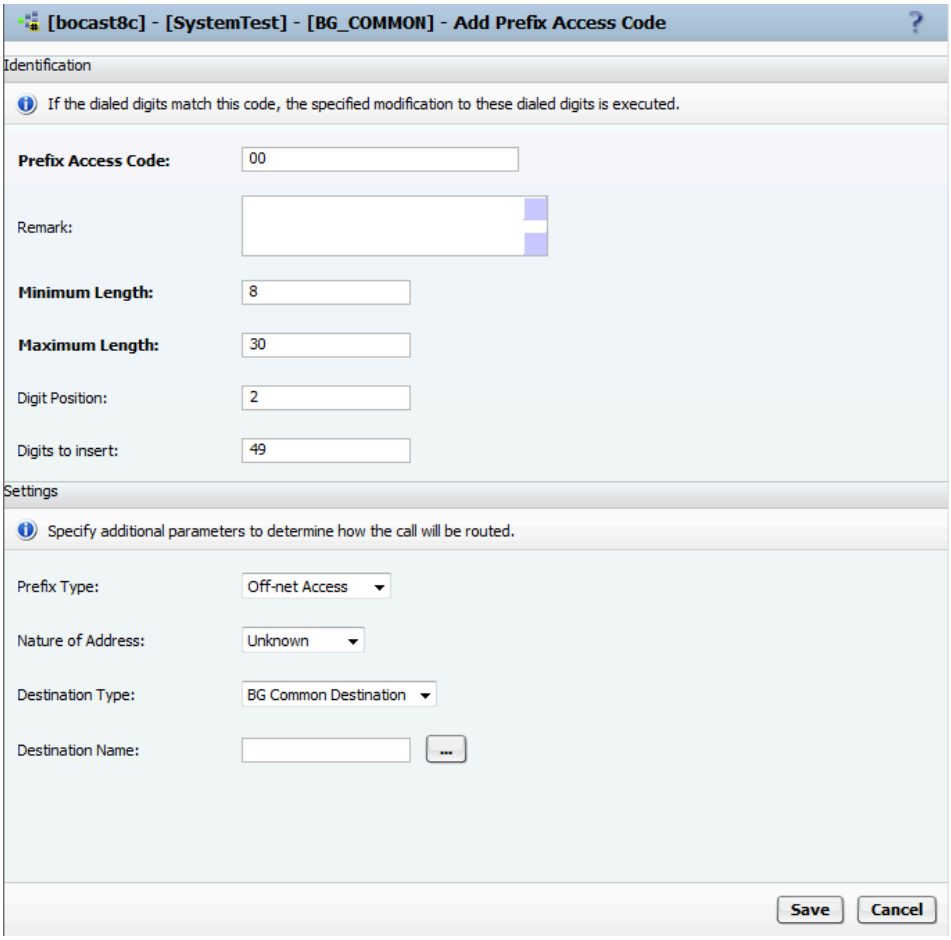


Figure 301: OpenScape Voice: Dialing with national code

14.7.9.5 Dialing with National Code (Closed Numbering)

Common Management Platform > OpenScape Voice > Business Group > BG_COMMON > Translation > Prefix Access Codes > Add

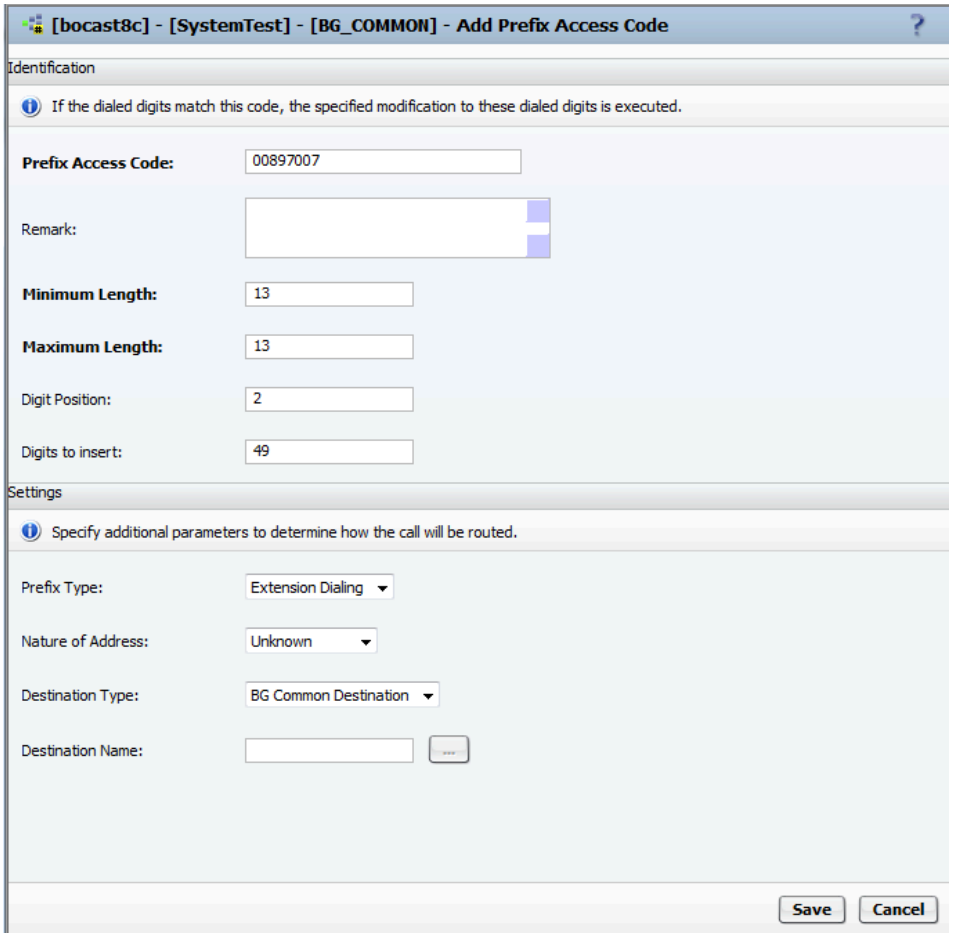


Figure 302: OpenScape Voice: Dialing with national code (closed numbering)

14.7.9.6 Dialing with International Code

Common Management Platform > OpenScape Voice > Business Group > BG_COMMON > Translation > Prefix Access Codes > Add

E.g. 0-0049897007-3xxxx

- Prefix Access Code: 000
- Minimum Length: 16
- Maximum Length: 16
- **Digit Position**: 3 (delete the first 000)
- **Destination Name**: NP_COMMON (destination where the number is sent to)

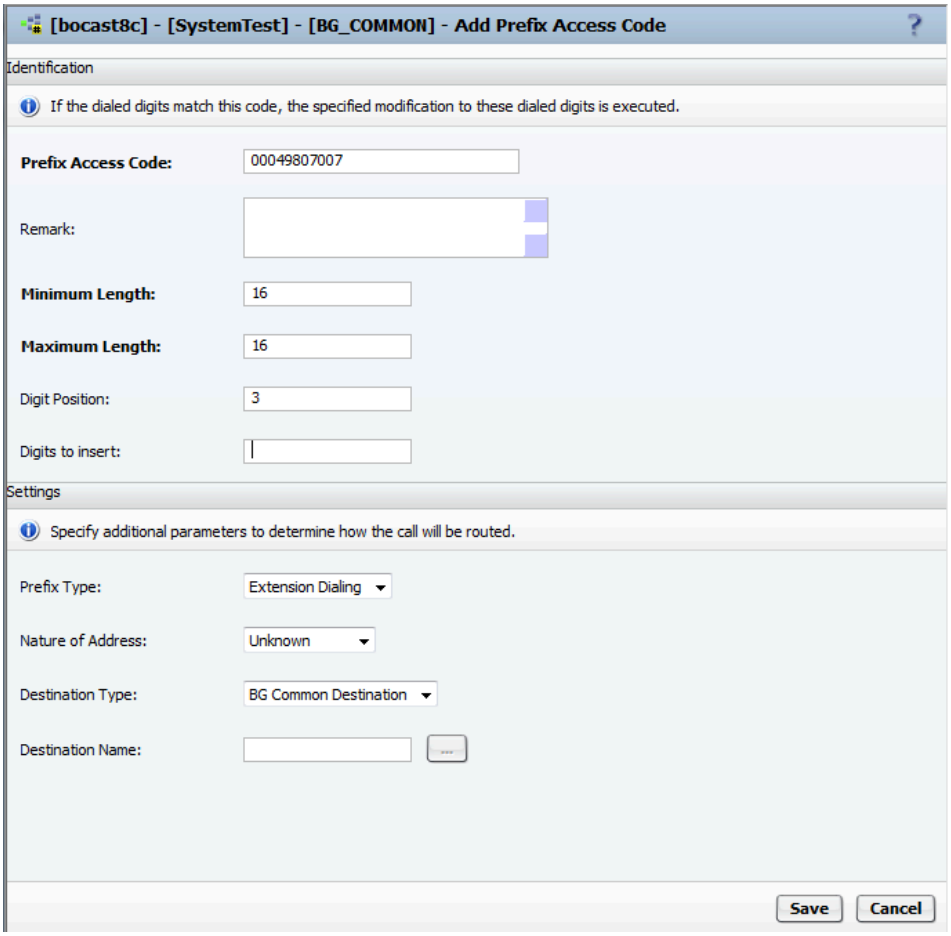


Figure 303: OpenScape Voice: Dialing with national code

14.7.9.7 Dialing with International Code (Closed Numbering)

Common Management Platform > OpenScape Voice > Business Group > BG_COMMON > Translation > Prefix Access Codes > Add

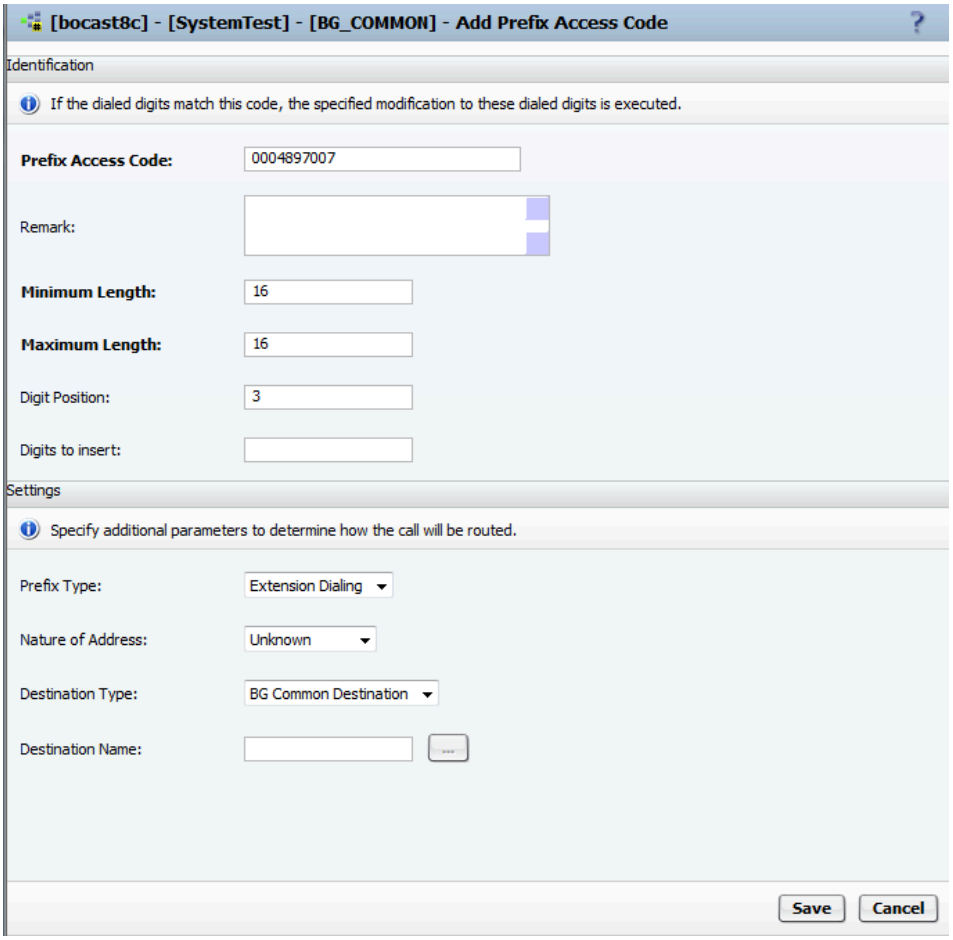


Figure 304: OpenScape Voice: Dialing with national code (closed numbering)

14.7.9.8 Change Type of Number to “International”

Common Management Portal > OpenScape Voice > Business Group > BG_COMMON > Translation > Prefix Access Codes

Set **Nature of Address** to **International**.

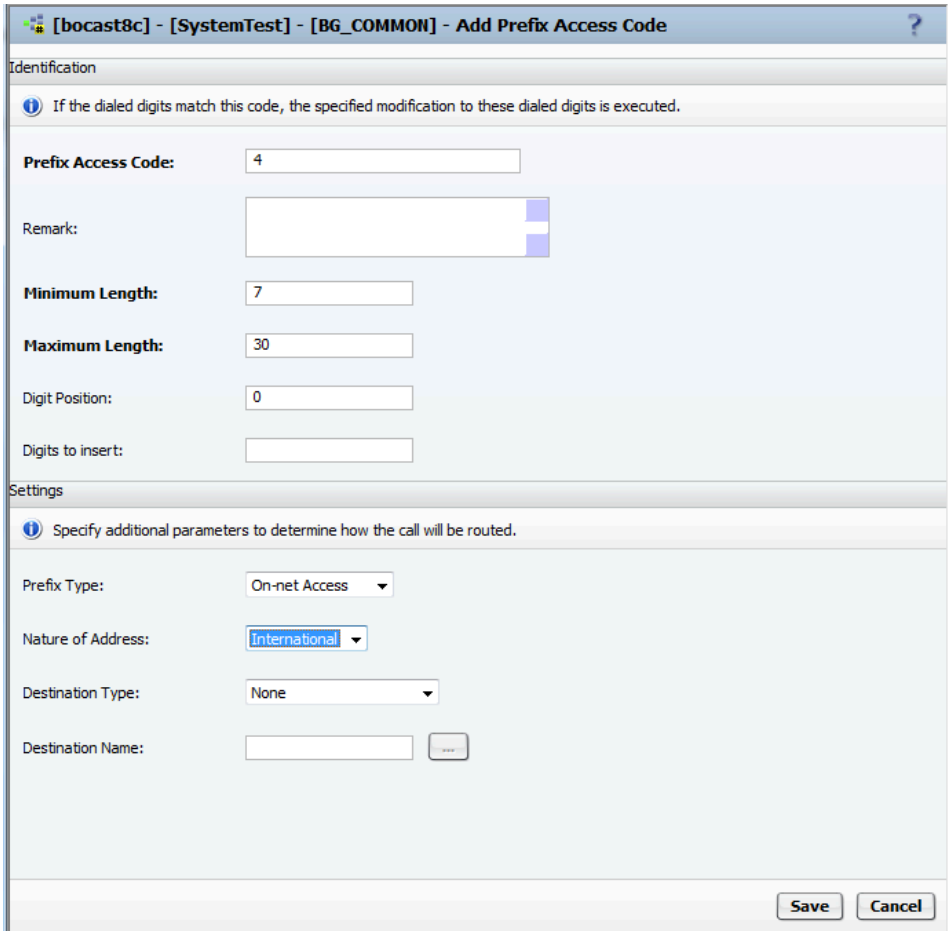


Figure 305: OpenScape Voice: Change type of number to international

14.7.9.9 Match International Number for “HOME DN”

Common Management > OpenScape Voice > Business Group > BG_COMMON > Translation > Destination Code > Add

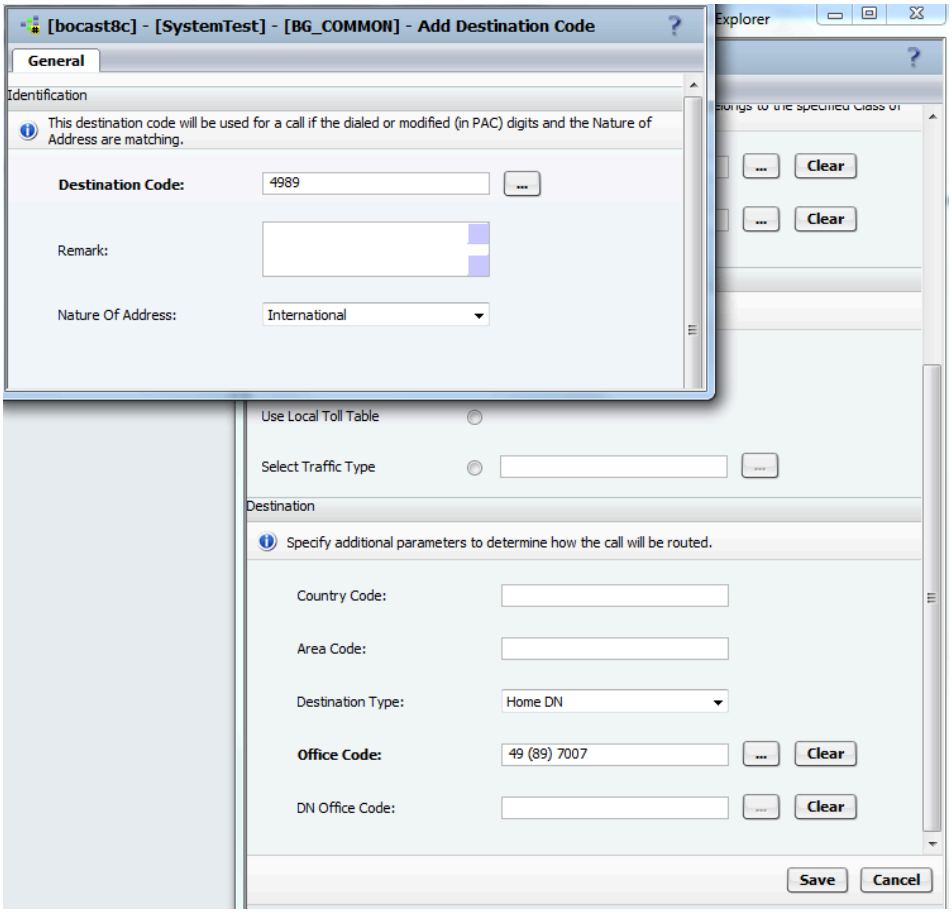


Figure 306: OpenScape Voice: Match international number for "HOME DN"

14.7.9.10 Configuration of Default Route if Number did not Match in “HOME DN”

In Figure 64 above the dialed number 49897007-xxxxx was sent for a check if there exists an entry in the OpenScape Voice system. If there is no match, dialed numbers are checked against this entry.

As default, you should configure the partner OpenScape 4000 system. But in this example we used as default a different OpenScape Voice system.

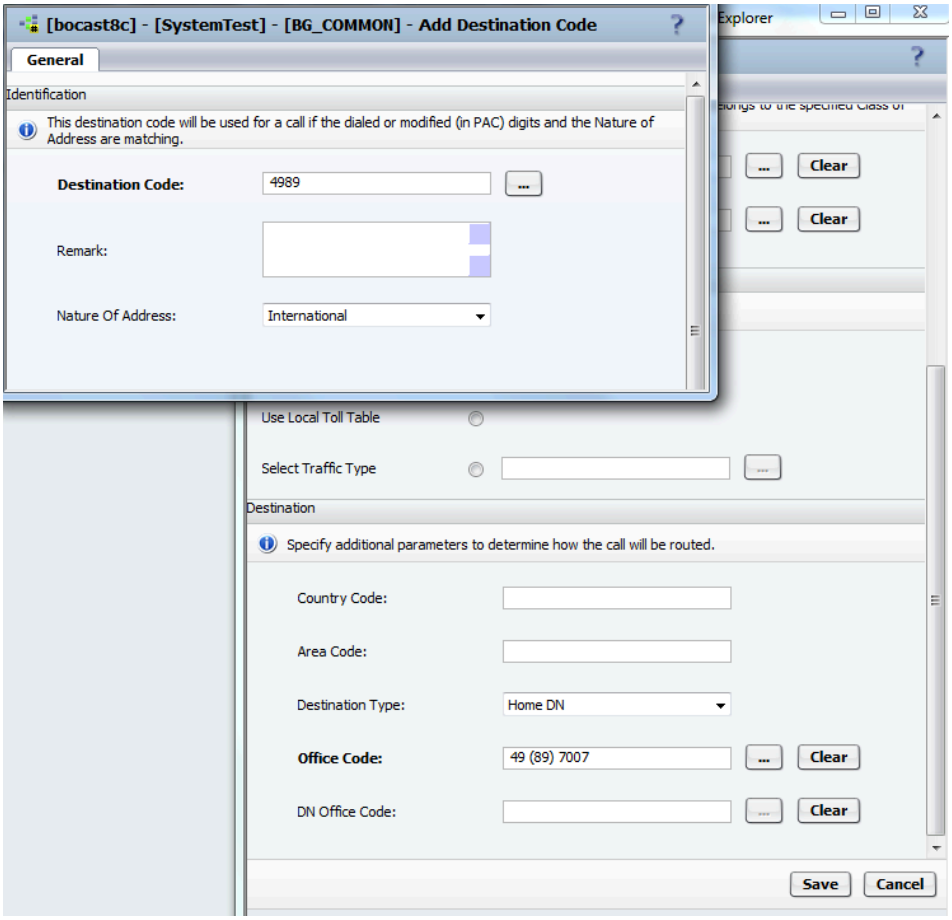


Figure 307: OpenScape Voice: Configuration of default route

14.7.9.11 Complete International Number Selection for single external Destination Number

In this example we have more than one partner system.

Therefore we have to send each international number which is not in our own system and not in the default partner system directly to the destination route.

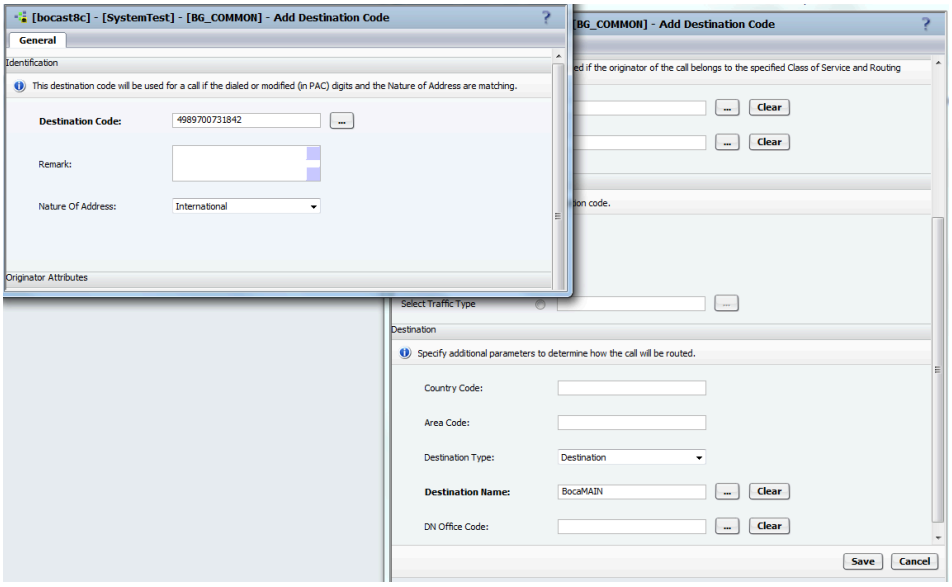


Figure 308: OpenScape Voice: Complete international number selection

14.7.10 OpenScape Voice Loop detection

OpenScape Voice supports:

- Setting and incrementing the Q.931 Transit Counter. This mechanism only provides protection for calls that loop within the enterprise network (e.g. with OpenScape 4000).
- On OpenScape 4000 the COT parameter **ATRS** and the AMO TDCSU parameter **TRACOUNT** are used for configuration.
- OpenScape Voice has a loop detection service that also protects against calls that loop through the public network. The service can be enabled with the parameters:

Srx/Service/CFLoopPrevention

Srx/Service/CFLoopMaxCount

1) This service limits the number of concurrent unanswered trunk to trunk calls that have the same calling and called party number. The service applies to tandem calls (e.g. direct trunk to trunk routing) as well as diversion scenarios (e.g. trunk call is forwarded by a subscriber to a trunk). In case of diversion: the "diverted to" number is used.

- The SIP Max-Forwads hop counter as per RFC 3261.
- The scenario can be addressed with the Q.931 Transit counter configured on OpenScape 4000 or the loop detection service in OpenScape Voice.

14.7.11 Restrictions

- The HG 3500 only sends digest credentials for Register and Invite requests if a challenge is made. Such user name and password configuration is made in the SIP-Q trunk profile. OpenScape 4000 challenge Digest Authentication only for Registration requests for SIP subscribers.

- In a HiPath 4000/OpenScape 4000 network the payload partners can be set with DMC. But a HiPath 4000/OpenScape 4000 phone can not send / receive the payload direct to the OpenScape Voice partner. There always is a hop on the HG 3500 module.
- If the HG 3500 has more than two partners configured (e.g. proxy) and the **REGIP1** fails, the **REGIP2** remains registered until **REGIP2** is no longer available.

IMPORTANT: It will not switch back automatically to **REGIP1**.

1)

NOTICE: From HiPath 4000 V6 DNS SRV can be used with SIPQ Trunk Profiles.

- Please be aware that the number of usable B-channels that can be assigned for SIP-Q calls vary dependent on which features (DMC/SPE/ QOS collection) are activated and also which type of hardware (STMI2/ STMI4/STMIX/STMIY) on OpenScape 4000 is in use. AMOs will make some automatic adjustments, however please reference the *OpenScape 4000, Volume 4: IP Solution* service documentation for more specific information.

14.8 Interworking with Microsoft Lync Communication Server 2010/2013

14.8.1 Important Information

IMPORTANT: This feature is released for vHG3500 (OpenScape 4000 Softgate) connectivity on project-specific basis only!

14.8.2 Feature Description

Interworking is supported between OpenScape 4000 and the Microsoft Lync Communication Server 2010/2013 which is the successor of Microsoft Office Communications Sever 2007. This interworking provides the capability to interconnect the Microsoft Lync Communication Server 2010/2013 with the OpenScape 4000 enterprise network via the Mediation Server. Therefore calls to/from Lync Communication Server 2010/2013 are possible over OpenScape 4000 SoftGate via native SIP trunks.

Microsoft Lync Communication Server 2010/2013 connectivity works with native SIP trunks located on OpenScape 4000 SoftGate (direct SIP).

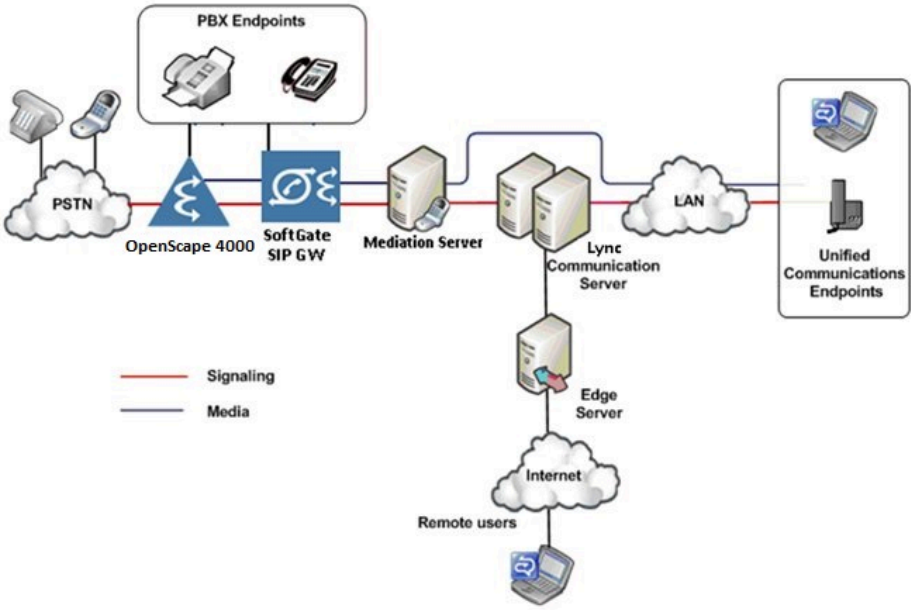


Figure 309: Interworking with Microsoft Lync Communications Server 2010/2013 over Mediation Server

14.8.3 Realization

Only native SIP trunks located on OpenScape 4000 SoftGate are considered for connectivity to Microsoft Lync Communication Server 2010/2013 (direct SIP).

14.8.4 Service Information

14.8.4.1 Restrictions

General restrictions

- Refer is not supported
- => Disable REFER on Lync Mediation Server
- OpenScape 4000 SoftGate doesn't support comfort noise.

Feature restrictions

- Dual forking
- Media bypass
- E911
- DNS load balancing is not supported by OpenScape 4000
- No tones on Lync Communications Server client after OpenScape 4000 station makes transfer ringing.
- For restrictions on feature basis see Section 8.4.2, “Available Features” (detailed description for every feature in each section).

14.8.4.2 Available Features

14.8.4.2.1 Basic Call

Name and number display

- Incoming calls to OpenScape 4000:
  - Calling party (Lync Communications Server) will see for basic call dialed number.
  - Called party (OpenScape 4000) will see for basic call calling number and name on first display line.
  - Connected party on OpenScape 4000 will see for basic call calling number and name.
  - Connected party on Lync Communications Server will see for basic call dialed number but no name.
- Outgoing calls to Lync Communications Server:
  - Calling party (OpenScape 4000) will see for basic call dialed number and SIP trunk name.
  - Called party (Lync Communications Server) will see for basic call calling number and name.[10]
  - Connected party on OpenScape 4000 will see for basic call dialed number and SIP trunk name.
  - Connected party on Lync Communications Server will see for basic call calling number and name.[11]
- CLIP/CLIR features - Calling Party Name and Number delivery (Allowed and Restricted).
- **Restriction (name and number display)**: Missed call notification doesn't include Display Name information associated with the calling party.
- Special note: Used numbering plan is E.164 (ISDN/International).

Codecs

- G.711a-Law, ptime=20msec preferred codec G.711 u -Law
- G.729 is not supported by Lync Communications Server
- G.723 is not supported by OpenScape 4000 Softgate and Lync Communications Server
- Silence suppression for G711 is not possible while different signaling is used.
  - Lync Communications Server uses Comfort Noise PT (13)
  - vHG 35xx / OpenScape 4000 uses attribute: silenceSupp:on - not supported by Lync Communications Server.
- Restrictions:
  - G.729, G.723 is not supported
  - Silence suppression is not supported

14.8.4.2.2 Call Transfer (blind, semi-attended, attended)

The OpenScape 4000 user can transfer calls to a Lync Communications Server party. Attended, Semi attended[12] and blind[13] transfer are possible.

10 Exception: If calling/connected number is found in Global Catalog (Active Directory) then the name from AD is shown for calling/connected party.

11 Exception: If calling/connected number is found in Global Catalog (Active Directory) then the name from AD is shown for calling/connected party.

12 only on OpenScape 4000 side

- Transfer Talking (Attended transfer)
- Display - no display update for any device - CO behavior:

  Calling party will see after transfer called party name and number and transfered to party will see calling party name and number on first line display.
- Transfer Ringing (Semi attended transfer)

  IMPORTANT: Offered at OpenScape 4000 side; not at Lync Communications Server side.

1) Display - no display update for any device - CO behavior.

Calling party will see after transfer called party name and number and transfered to party will see calling party name and number on first line display

- Blind transfer

  IMPORTANT: Offered at Lync Communications Server side; not at OpenScape 4000 side.

1) Display - transferred party's display is not updated:

Calling party will see after transfer called party name and number and transfered to party will see calling party name and number on first line display

14.8.4.2.3 Call Forwarding

The OpenScape 4000 user can forward calls to a Lync Communications Server party.

CFA (Call Forward All), CFA (Call Forward Busy) and CFNA (Call Forward No Answer) are possible.

- Display forward unconditionally/busy - independent of forward destination
  - Calling party will see called name and number on first line display.
  - Diverted-to party will see calling party name and number on first line.
  - No visible indication that a call forwarding happened on any display.
- Display forward no reply - independent of forward destination
  - Calling party will see called name and number on first line display.
  - Diverted-to party will see calling party name and number on first line.
  - No visible indication that a call forwarding happened on any display.

Special Note

- Forward switching is done on both sides.

Restrictions and Limitations

- Party A doesn't get forward information.
- Call forward busy not supported on Lync Communications Server side.
- PBX is not aware of call forwarding.
- Voice mail scenarios on OpenScape 4000 side are not possible.

[13] only on Lync Communications Server side

14.8.4.2.4 Hold and Retrieve

This scenario is possible on both sides, OpenScape 4000 and Lync Communications Server side. It works with the attribute “inactive in both direction”. Local MOH (Music on Hold) is used on both sides.

14.8.4.2.5 Three-Way Conferencing

Conference scenarios are possible - CO behavior.

Display - On conference all parties located on OpenScape 4000 will show correct display info for OpenScape 4000 conference members. Lync Communications Server parties will be displayed as external parties.

Display won’t be updated on OpenScape 4000 if new members are added at Lync Communications Server side.

Special Note:

Lync Communications Server side: Party C/OpenScape 4000 is added to conference before party C is connected and invite/from is different to basic call.

Display party C/OpenScape 4000 shows the configured (OpenScape 4000 system) trunk name.

OpenScape 4000 side: no message is sent towards Lync Communications Server with "Conference" display update.

14.8.4.2.6 DTMF

Works with 0-15.

14.8.4.2.7 SDES Support

Secure SIP trunking via SDES to the Microsoft Lync Communication Server is supported. To use the feature you have to select the appropriate SIP trunk profile and select the desired **SIP Trunk Security Mode**.

14.8.5 Configuration Example

14.8.5.1 OpenScape 4000

OpenScape 4000 routing configuration

Trunk and route configuration as described in SIP Connectivity > Chapter 5, “Configuration of SIP Service Provider / SIP Carrier” or find here a configuration example.

- Trunk configuration
- AMO TDCSU - DEV=HG3550IP

  Besides AMO BFDAT, AMO BCSU, AMO BUEND, AMOTDCSU (ECMAV2 protocol) AMO COT and AMO COP is of interest:

```
ADD-COT:COTNO=80,PAR=ANS&CEBC&BSHT&BLOC&LWNC&NLCR&TSCS&DFNN&NLRD&NOFT&NTON;
ADD-COP:COPNO=80,TRK=TA,TOLL=TA;
```

  Routing and numbering plan specific issues see below (AMO TDCSU, AMO COT, AMO COP).
- Common gateway board configuration

- AMO CGWB (in the following example with **IPADR=192.168.125.44**) is used to configure, the used trunk protocol (native SIP), DNS/SRV server (used by profile) and the codec list (example has **VAD=NO**)

  The gateway is configured as local gateway with AMO GKREG. **RFCFMOIP** is set to **NO**.

```
ADD-CGWB:LTU=77,SLOT=10,SMODE=NORMAL,IPADR=192.168.125.44,NETMASK=255.255.255.0;
CHANGE-
CGWB:MTYPE=CGW,LTU=77,SLOT=10,TYPE=GLOBIF,PATTERN=213,VLAN=NO,VLANID=0,DEFRT=192
.168.125.234,BITRATE="AUTONEG",TRPRSIP=4,TRPRSIPQ=0,TRPRH323=0,TPRH323A=0,TL▶
SP=4061,DNSIPADR=0.0.0.0;
CHANGE-CGWB:MTYPE=CGW,LTU=77,SLOT=10,TYPE=SERVIF,LOGINTRM="TRM";
CHANGE-
CGWB:MTYPE=CGW,LTU=77,SLOT=10,TYPE=ASC,UDPPRTLO=29100,TOSPL="184",TOSSIGNL="104"
,T38FAX=YES,RFCFMOIP=NO,RFCDTMF=YES,REDRFCTN=YES,PRIO=PRIO1,CO▶
DEC=G711A,VAD=YES,RTP="20";
CHANGE-CGWB:MTYPE=CGW,LTU=77,SLOT=10,TYPE=ASC,PRIO=PRIO2,CO▶
DEC=G729A,VAD=NO,RTP="20";
CHANGE-CGWB:MTYPE=CGW,LTU=77,SLOT=10,TYPE=ASC,PRIO=PRIO3,CO▶
DEC=G711U,VAD=NO,RTP="20";
CHANGE-CGWB:MTYPE=CGW,LTU=77,SLOT=10,TYPE=DMCDATA,DMCCONN=0;
ADD-GKREG:GWNO=11,GWATTR=INTGW&HG3550V2&SIP,DIPLNUM=0,DPLN=0,LAUTH=1,INFO="Di▶
rect SIP to OCS";
ADD-LDAT:LROUTE=300,LSVC=ALL,LVAL=1,TGRP=1,ODR=300,LAUTH=1;
```

- Routing and numbering plan configuration
- For outgoing calls block dialing has to be configured for native SIP trunk, dialing pattern has to end with e.g. '-Z'.

  ADD-
  LDPLN:LCRCONF=LCRPATT,DIPLNUM=0,LDP="0"-"Z",LROUTE=1,LAUTH=1;

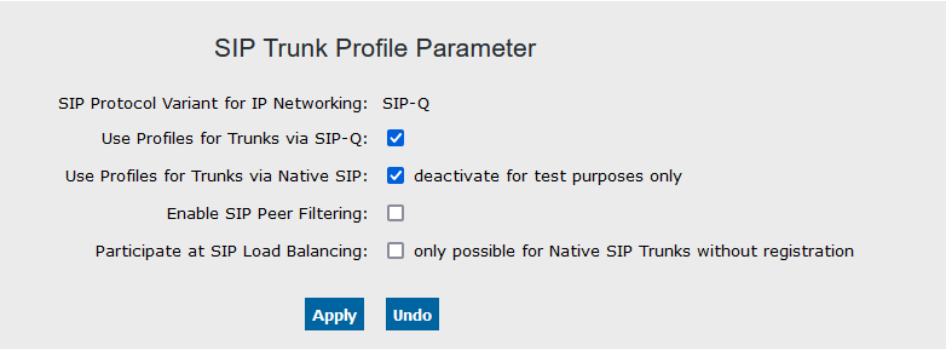
  LCR configuration rules depend on the numbering plan, that is used between OpenScape 4000 and Mediation Server.

  The recommended numbering plan is **NPI= ISDN**, **TON= INTERNATIONAL** (explicit format).

vHG 3500 configuration

Verify that **SIP Protocol Variant for IP Networking** is set to **Native SIP** (AMO CGWB) and **Use Profiles for Trunks via Native SIP** flag is set:

WBM > Configuration > Voice Gateway > SIP Trunk Profile Parameter

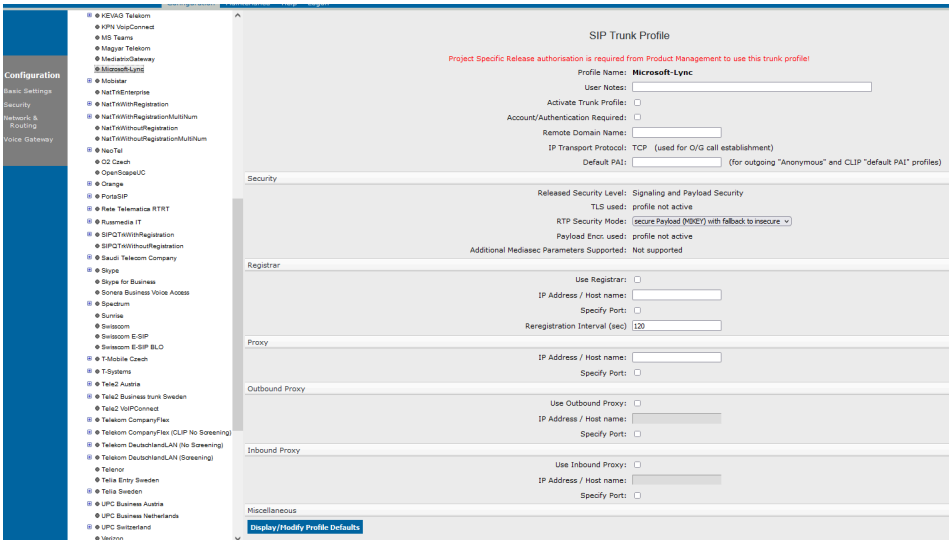


Microsoft-Lync - SIP trunk profile parameter for vHG 3500

As SIP trunk profile Microsoft-*Lync* must be activated on OpenScape 4000 SoftGate on the SIP Trunk profile page and IP address of Mediation Server has to be configured on **IP Address / Host name** field from **Proxy** tab.

If you want to use secure SIP trunk connections, the **SIP Trunk Security Mode** is automatically derived from the AMO values in TDCSU and GKREG. It no longer needs to be set in the WBM.

WBM > Configuation> Voice Gateway> SIP Trunk Profile > Microsoft-Lync



Microsoft-Lync - SIP trunk profile configuration for vHG 3500

DMC end must be configured with AMO LDAT (e.g. `CHANGE-LDAT:LROUTE=x,LRTEL=1,LATTR=DMCEND;`).

14.8.5.2 Microsoft Lync Server/Mediation Server

To complete the Direct SIP configuration with OpenScape 4000, perform the following steps:

1) Add OpenScape 4000 vSTMI as a Gateway to the Lync Server Topology
2) Define dial plan by configuring normalization rules.
3) Create a voice policy.
4) Define a trunk configuration.
5) Assign the voice policy that you created to Lync users.

14.8.5.2.1 Add OpenScape 4000 vSTMI as a Gateway to the Lync Server Topology

1) Start Topology Builder: **Start > All Programs > Microsoft Lync Server 2010/2013 > Lync Server Topology Builder**
2) Select **PSTN Gateway** and define a new gateway:

3) Right click **PSTN Gateways** and select **New IP/PSTN Gateway**

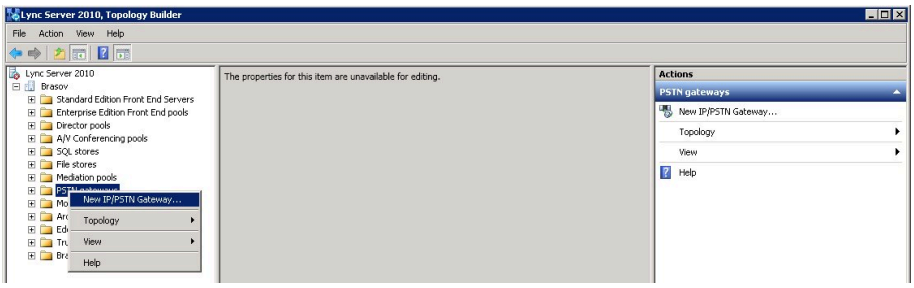


Figure 310: Microsoft Lync Server - Define new IP/PSTN gateway

4) **Define New IP/PSTN Gateway** dialog:

- **Gateway FQDN or IP Address**: specify the IP address of the OpenScape 4000
- **Listening port for IP/PSTN gateway**: enter 5060
- Select **TCP** as **Sip Transport Protocol**.

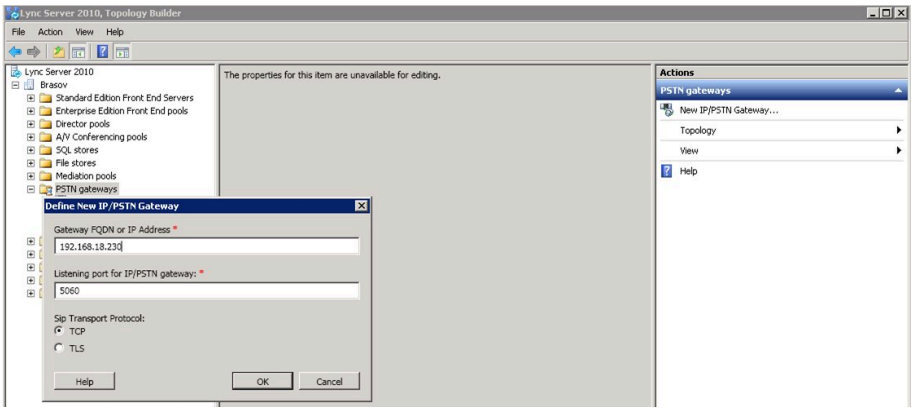


Figure 311: Microsoft Lync Server - Properties for new IP/PSTN gateway

5) Select **Mediation pools**.

6) Right click **Mediation pool**, select **Edit Properties** and click **OK** and then click **OK** again.

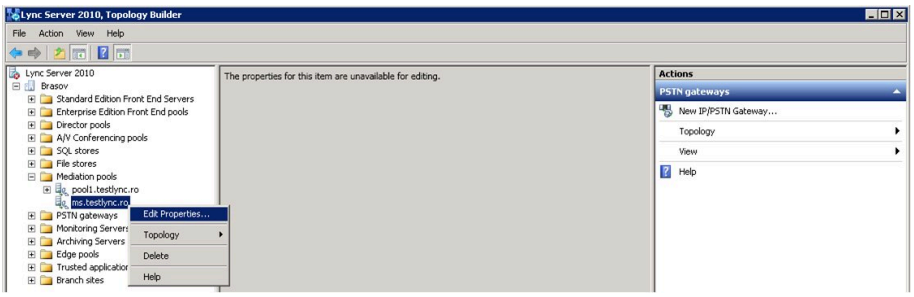


Figure 312: Microsoft Lync Server - Mediation pool properties

7) Select **Gateway on PSTN gateway** tab and click **Add**.

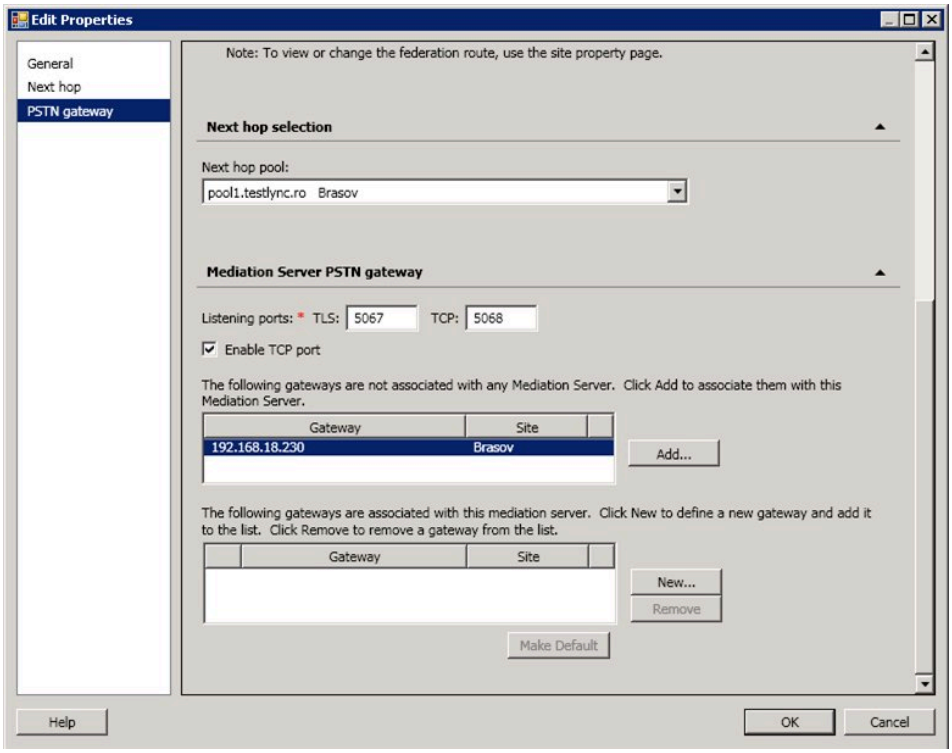


Figure 313: Microsoft Lync Server - PSTN gateway properties

1) Gateway has been assigned to Mediation Server. Click **OK**.

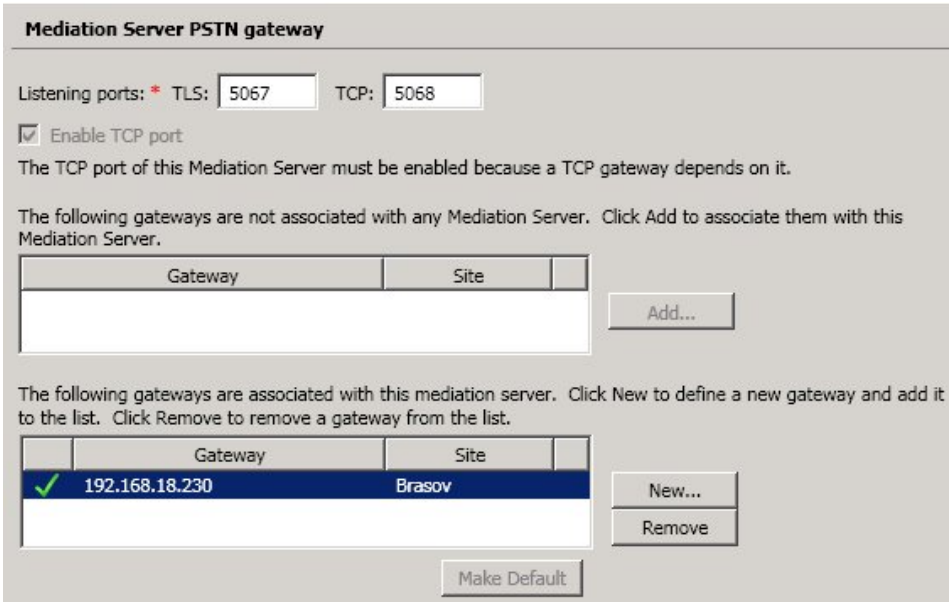


Figure 314: Microsoft Lync Server - Assign gateway to Mediation Server

1) Publish your changes to the Lync Server topology:

2) Actions panel of the Topology Builder > Topology > Publish

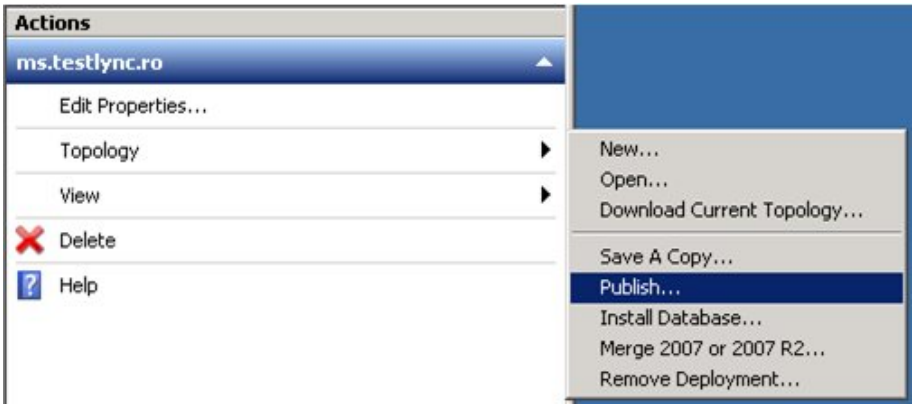


Figure 315: Microsoft Lync Server - Publish the changes to the Micorosft Lync Server topology

14.8.5.2.2 Define Dial Plan Rules

Define the dial plan rules in Lync Server Control Panel.

1) Start Lync Server Control Panel
2) **Voice Routing > Dial Plan** tab
3) Create normalization rules which permit Lync users to be able to dial OpenScape 4000 phone numbers and the PSTN.
4) To commit your changes click **Commit** and then **Commit all**.

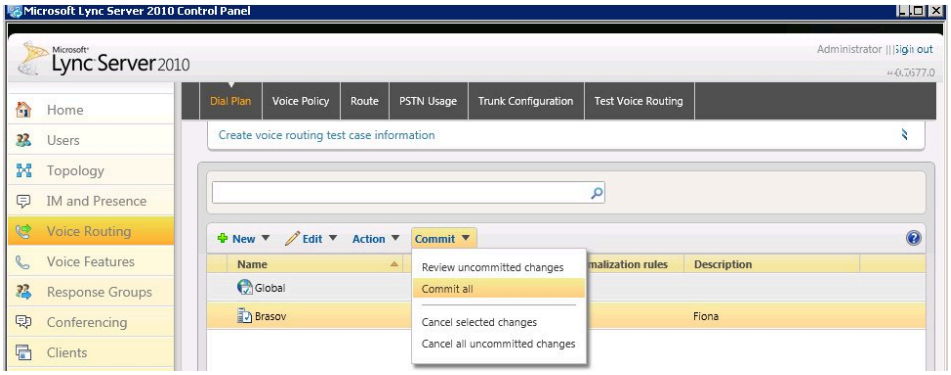


Figure 316: Microsoft Lync Server - Define dial plan rules

14.8.5.2.3 Create Voice Policy

Users assigned to specific voice policy will be able to dial out through the Direct SIP connection to the OpenScape 4000 system.

1) **Voice Routing > Voice Policy** tab
2) Click **New**. Depending on the scope of the policy you want to create click **Site Policy** or **User Policy**.

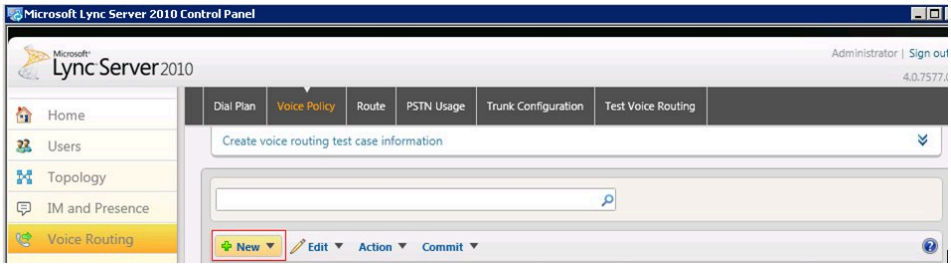


Figure 317: MicrosoftLync Server - Create voice policy

1) Specify a unique name for this voice policy and provide a description.
2) To create a new PSTN usage for this policy click **New**.

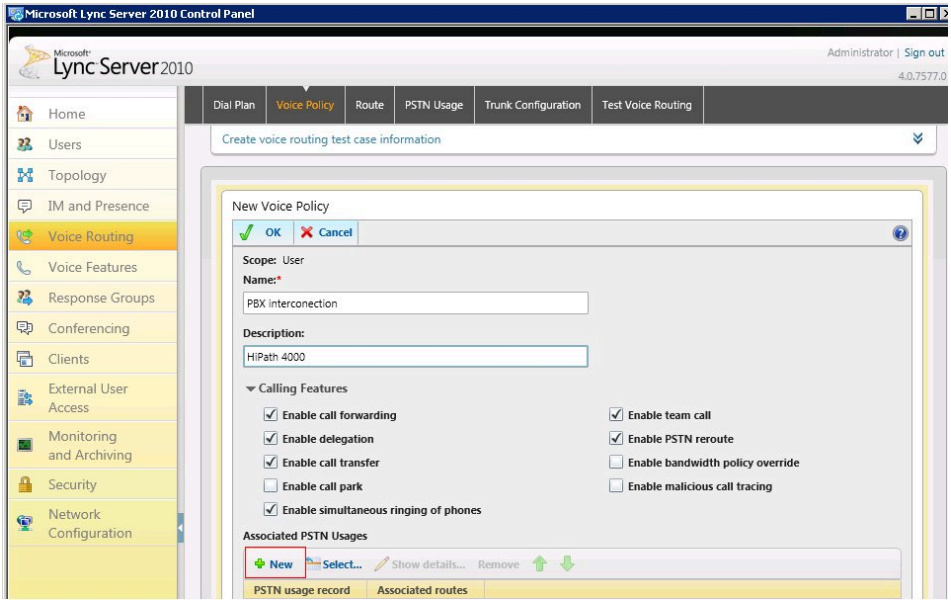


Figure 318: Microsoft Lync Server - Create new PSTN usage

1) Specify a name for the new PSTN usage record. The name must be unique to this specific voice policy. Also, provide a detailed description of the PSTN usage record.
2) To assign a route to this PSTN usage click **New**.

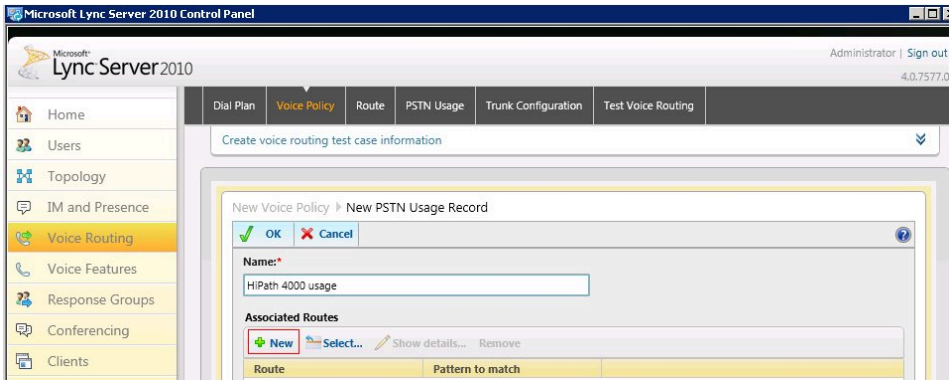


Figure 319: Microsoft Lync Server - Assign a route to the PSTN usage

1) Specify a name for this route, and provide a meaningful description.
2) To assign the OpenScape 4000 gateway to this new route click **Add**.

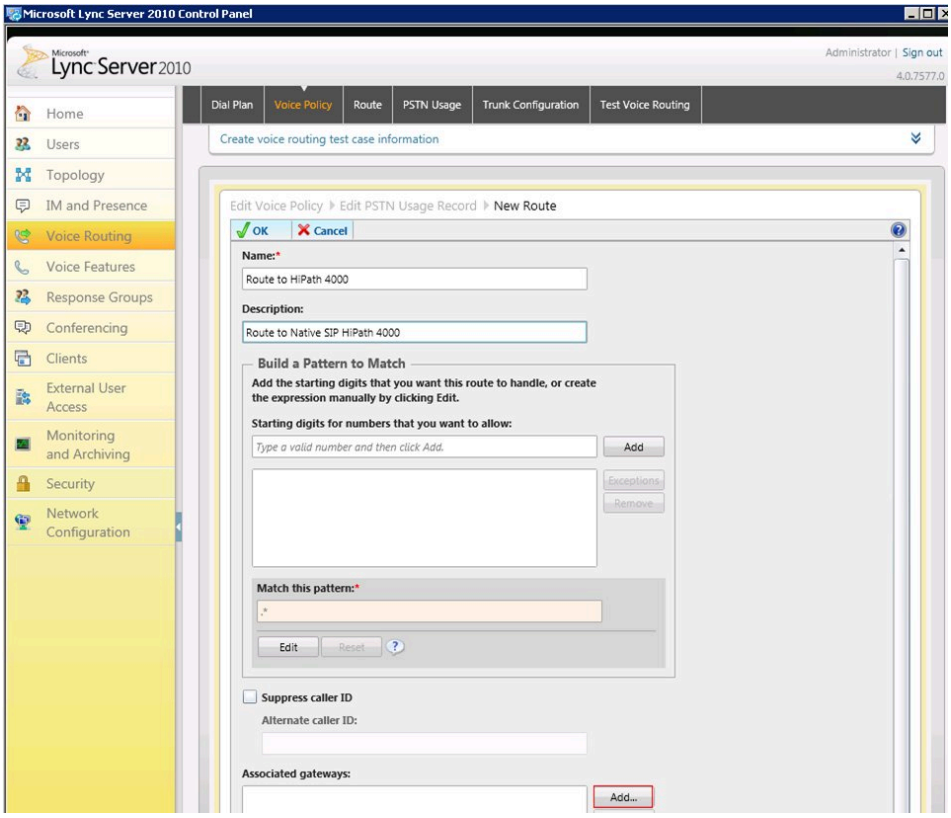


Figure 320: Microsoft Lync Server - Assign the OpenScape 4000 gateway to the route

1) Select the OpenScape 4000 gateway you created earlier.
2) Click **OK** in all different dialog boxes to complete the creation of the voice policy.
3) To commit your changes click **Commit** and then **Commit all**.

14.8.5.2.4 Define Trunk Configuration

The next step is to assign the OpenScape 4000 gateway to a trunk associated with a pool or a site as follows:

1) **Lync Server Control Panel > Voice Routing > Trunk Configuration** tab
2) Click **New**. Depending on the scope of the policy you want to create click **Site Configuration** or **Pool Configuration**.

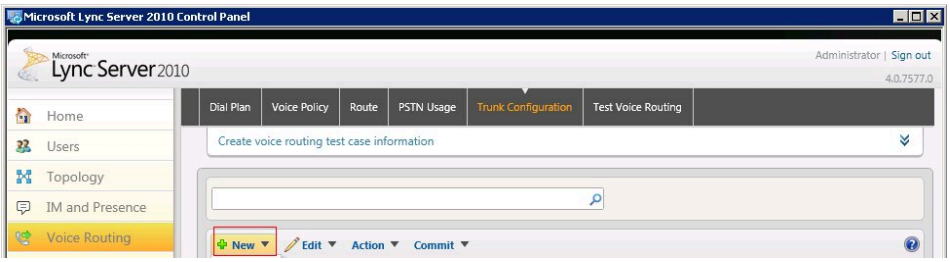


Figure 321: Microsoft Lync Server - Define the trunk configuration

1) Select a pool or site for this trunk configuration.
2) In the **New Trunk Configuration** dialog box click **OK**.
3) To commit your changes click **Commit** and then **Commit all**.

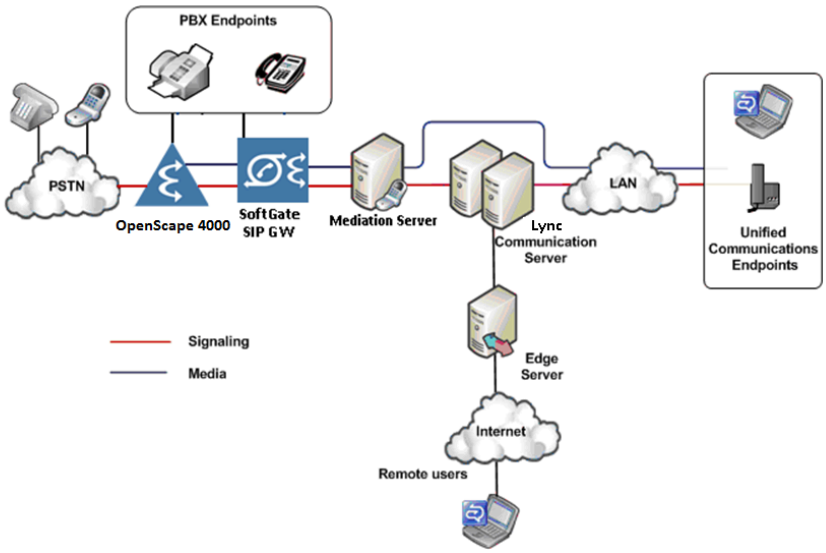
IMPORTANT: Make sure that **Enable Media bypass** and **Enable refer support** check boxes are disabled.

14.9 Skype for Business

14.9.1 Feature Overview

Native SIP trunks located on SoftGate/STMIX/STMIY are considered for interoperability between OpenScape 4000 and Microsoft Skype for Business over Mediation Server.

TLS and SRTP connection between OpenScape 4000 and Microsoft Skype for Business over Mediation Server is optional and can be used.



14.9.1.1 Features available (Overview):

- Basic call
- CLIP/CLIR features - Calling Party Name and Number delivery (Allowed and Restricted)
- Call Transfer (Blind, semi-attended, Attended)
- Call Forwarding (CFA - Call Forward All, CFB - Call Forward Busy, CFNA - Call Forward No Answer)
- Hold and Retrieve
- Three-way conferencing
- DTMF
- Security

14.9.1.2 Feature detailed description

14.9.1.2.1 Basic call

Functionality

- Incoming calls to OpenScape 4000

- calling party on Skype for Business will see for basic call dialed number - called party on OS4K will see for basic call calling number and name on first display line - connected party on OS4K will see for basic call calling number and name. - connected party on Skype for Business will see for basic call dialed number but no name.

Outgoing calls to Skype for Business

- calling party on OS4K will see for basic call dialed number and SIP trunk name. - called party on Skype for Business will see for basic call calling number and name*. - connected party on OS4K will see for basic call dialed number and SIP trunk name. - connected party on Skype for Business will see for basic call calling number and name*

IMPORTANT: if calling/connected number is found in Global Catalog (Active Directory) then the name from AD is shown for calling/connected party.

CLIP/CLIR features - Calling Party Name and Number delivery (Allowed and Restricted)

Restrictions

-Missed call notification doesn’t include Display Name information associated with the calling party -Call not encrypted shown on display in case that security is enabled

Special Note:

- Used numbering plan is E.164 (ISDN/International)

14.9.1.2.2 Call Transfer

- Transfer Talking (Attended transfer): no display update for any device;

- Transfer Ringing (Semi attended transfer): offered at OS4K side; not at Skype for Business side no display update for any device;

- Blind transfer: offered at Skype for Business side; not at OS4K side Original Skype for Business call partner does not get a display update. Transferred-To party gets Original Skype for Business partner's name/number from Skype for Business in the initial call setup.

Functionality

The OS4K user can transfer calls to a Skype for Business party, Attended, Semi attended (only on OS4K side) and blind (only on Skype for Business side) transfer possible.

Attended transfer Display – no display update for any device – CO behavior; Calling party will see after transfer called party name and number and transfered to party will see calling party name and number on first line display.

Semi attended transfer (only on OS4K side) Display – no display update for any device – CO behavior; Calling party will see after transfer called party name and number and transfered to party will see calling party name and number on first line display

Blind transfer (only on Skype for Business side) Display – Transferred pty's display is not updated; Calling party will see after transfer called party name and number and transfered to party will see calling party name and number on first line display

14.9.1.2.3 Call Forwarding

Functionality

The OS4K user can forward calls to an Skype for Business FOR BUSINESS party. CFA - Call Forward All, CFB (only on OS4K side) - Call Forward Busy, CFNA - Call Forward No Answer – possible, CO behavior;

- Display Forward Unconditional/Busy – Independent of forward destination

- Calling party will see called name and number on first line display. - diverted-to party will see calling party name and number on first line. - no visible indication that a call forwarding happened on any display.

- Display Forward no reply – Independent of forward destination

- Calling party will see called name and number on first line display. - diverted-to party will see calling party name and number on first line. - no visible indication that a call forwarding happened on any display.

Forward switching is done on both sides.

Restrictions and limitation

Party A doesn’t get forward information. Call forward busy not supported on Skype for Business side. PBX is not aware of call forwarding. Voice mail scenarios on OpenScape 4000 side are not possible. Call forward via rerouting not possible, e.g.call forward from OS4K to Skype for Business in case of incoming call from Skype for Business will not free resources.

14.9.1.2.4 Hold and Retrieve

Scenario possible on both sides OS4K and Skype for Business works w/ attribute=inactive in both direction -> local Moh is used on both sides

14.9.1.2.5 Three-way conferencing

Functionality

Conference scenarios possible – CO behavior Display – On conference all parties located on OS4K members will show correct display info for OS4K conference members, Skype for Business parties will be displayed as external parties. Display not update on OS4K if new members are added in Skype for Business side.

Special Note:

Skype for Business side: Pty C/OS4K is added to conference before Pty C is connected and invite/from is different to BC. Display Pty C/OS4K shows the configured (OS4K system) trunk name.

OS4K side: no message is sent towards OSC w/ "Conference" display update

Restrictions and limitation

No name or number shown on OS4K user if OS4K is invited to the conference. OS4K participants to Skype for Business conference are not disconnected after conference end. OS4K users must manually close the conference call.

14.9.2 Restrictions

- General restrictions

Refer not supported - Disable REFER on Skype for Business Mediation Server - OS4K REFER is disabled in profile and no manual action needed SoftGate doesn’t support comfort noise.

- Feature restrictions

- Dual forking - Simultaneously ring - Video call - Media bypass - E911 - DNS load balancing is not supported by OpenScape 4000 - No tones on Skype for Business client after OpenScape 4000 stn make transfer ringing - Call not encrypted shown on display in case that security is enabled - Call transfer initiated from OS4K to Skype for Business if caller is Skype for Business if security enabled - Call forward via rerouting not possible

- SIP trunk connected to Skype for Business can be configured only on vSTMI or on STMIX/STMIY.

See above restrictions on feature basis.

- Call Forward is available only on Skype for Business full Client comparison below

https://technet.microsoft.com/en-us/library/dn933896.aspx?f=255&MSPPError=-2147217396

Codecs:

- G.711a-Law, ptime=20msec preferred codec G.711 a -Law - G.729 is not supported by Skype for Business - G.723 is not supported by the Softgate or Skype for Business - silence suppression for g711 not possible while different signalling - Skype for Business uses Comfort Noise PT (13); not supported by Softgate - vHG/OS4K uses attribute: silenceSupp:on ;not not supported by Skype for Business -DTMF for RFC2833 is supported for tones 0-15

14.9.3 Specific configuration

See Service Manual – SIP Trunk Provider chapter for general configuration

The following specific configuration steps should be performed additional to configure SIP trunk between OpenScape 4000 and Skype for Bussiness:

1) Configure OpenScape 4000 routing – please see Service Manual – SIP Trunk Provider chapter
2) Configure vHG 3500 – please see Service Manual – SIP Trunk Provider chapter
3) Configure Skype for Business Server 2015.

14.9.3.1 OpenScape 4000 routing

- DMC end must be configured on LDAT e.g. `CHANGE-LDAT:LROUTE=x,LRTEL=1,LATTR=DMCEND;`
- Routing and numbering plan configuration

For outgoing calls block dialing has to be configured for native SIP trunk, dialing pattern has to end with e.g. '-Z'.

```
ADD-LDPLN:LCRCONF=LCRPATT,DIPLNUM=0,LDP="0"-"Z",LROUTE=1,LAUTH=1;
```

End of Dial timer can be changed via the parameter LCREOD in AMO CTIME under branch CP1 if wanted;

LCR configuration rules depend on the numbering plan, that is used between OpenScape 4000 and Mediation Server. The recommended numbering plan is `NPI= ISDN, TON= INTERNATIONAL` (explicit format).

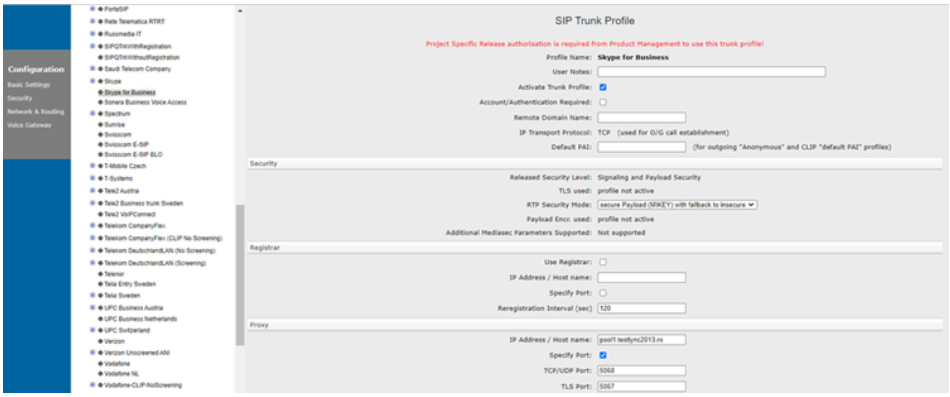
14.9.3.2 vHG 3500 WBM configuration

Verify that SIP Protocol Variant for IP Networking is set to Native SIP (AMO CGWB) and Use Profiles for Trunks via Native SIP flag is set: WBM > Configuration > Voice Gateway > SIP Trunk Profile Parameter



14.9.3.2.1 Configure vHG 3500

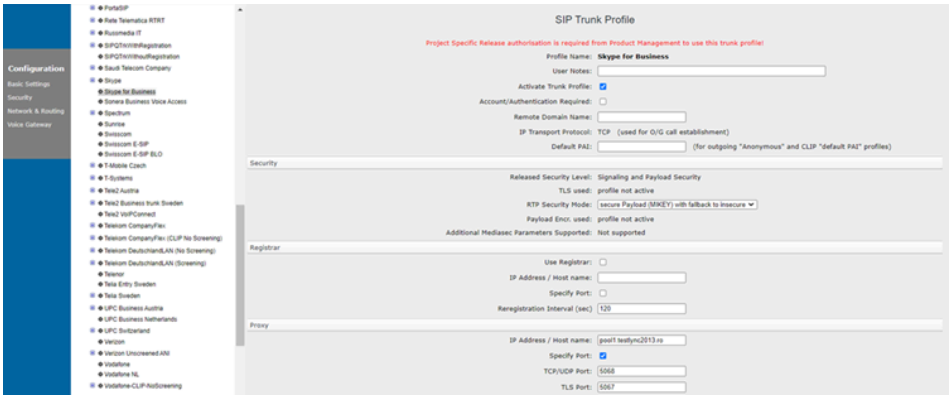
Skype for Business profile must be activated, and IP address or DNS name of Mediation Server has to be configured on IP address / Host name field from Proxy tab.



14.9.3.2.2 Configure vHG 3500 Security enabled (specific configuration)

Skype for Business profile must be activated, and IP address or DNS name of Mediation Server has to be configured on IP address / Host name field from Proxy tab.To enable security on gateway SECLEVEL field from AMO TDCSU should be set as SECURE, than Gateway security tab Signaling and Payload Security will show TLS used YES.

NOTICE: Signaling and Payload Security is optional.



14.9.3.3 Configure Skype for Business Server 2015

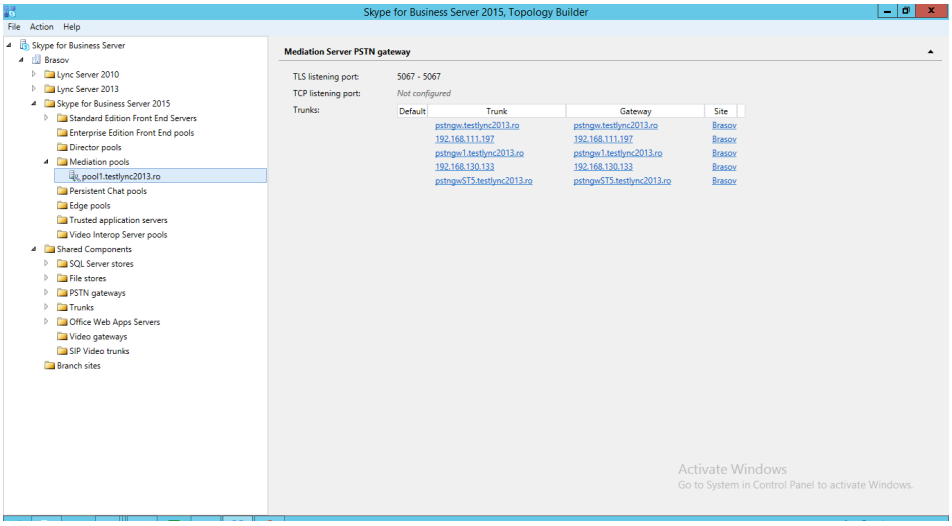
To complete the Direct SIP configuration with OpenScape 4000, perform the following steps:

1) Add OpenScape 4000 vSTMI (vHG3500) as a gateway to the Skype for Business Server 2015 topology.
2) Define dial plan by configuring normalization rules.
3) Create a voice policy.
4) Define a trunk configuration.
5) Assign the voice policy that you created to Skype for Business users.

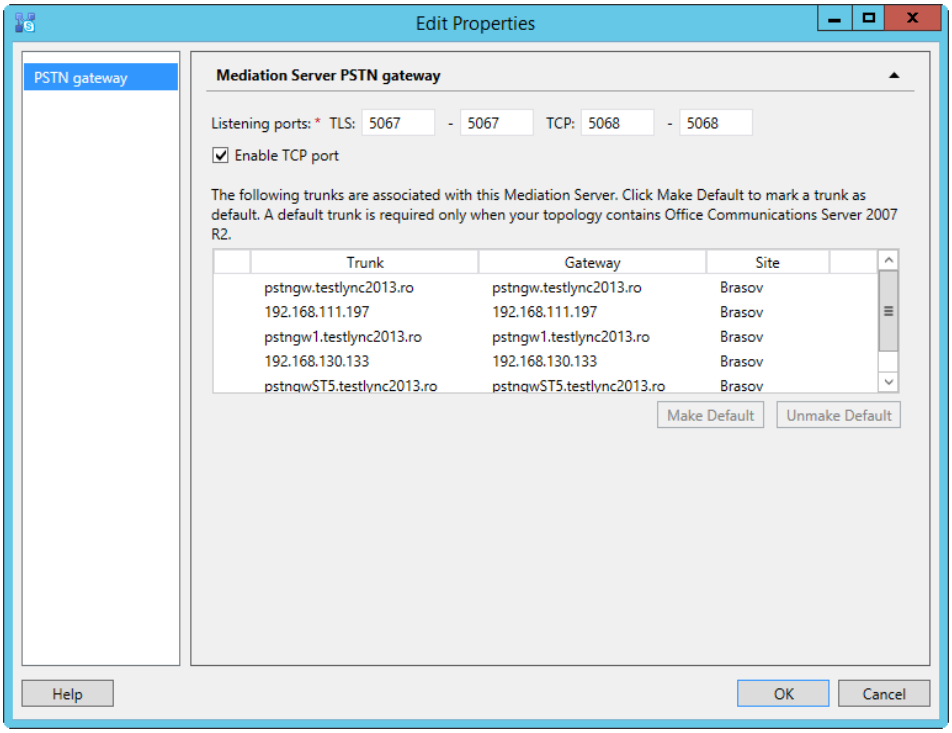
NOTICE: On OpenScape4000V8 DIRECT STP can be configured on vSTMI or STMIX/STMIY.

14.9.3.4 Adding OpenScape 4000 vSTMI as a gateway to the Skype for Business Server 2015 Topology

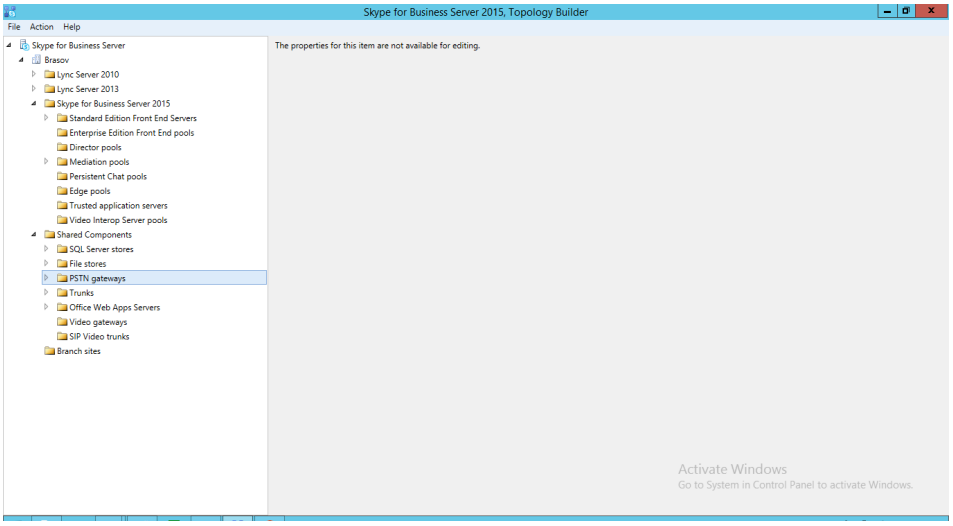
1) Start Topology Builder: Click Start, click All Programs, click Microsoft Skype for Business Server 2015, and then click Skype for Business Server 2015 Topology Builder.
2) Expand the Mediation pools node.
3) Right-click the Mediation pool, and then click Edit Properties.



1) In Mediation Server PSTN gateway check Enable TCP port and set as Listening ports 5067 – 5067 for TLS and 5068 - 5068 for TCP. Once a new gateway will be defined, it will appear here.

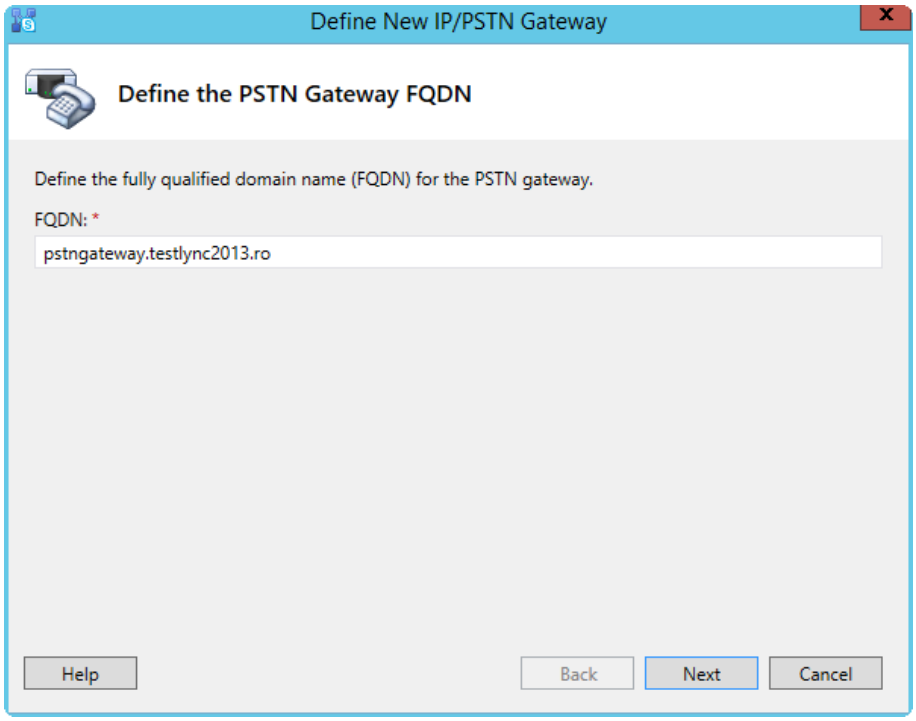


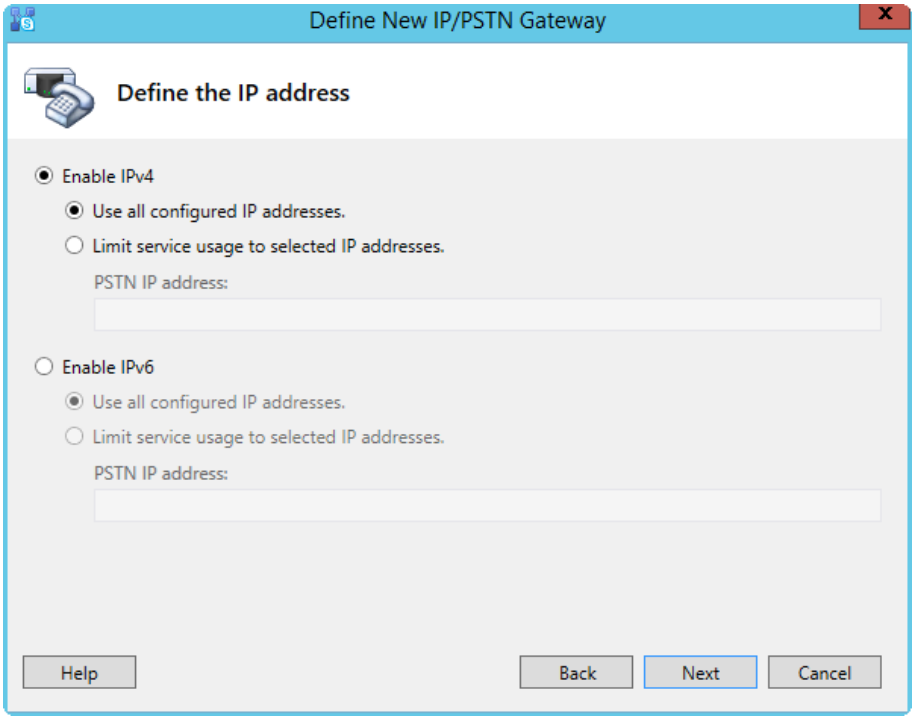
1) In the PSTN Gateway box, do the following: Right click on PSTN Gateways and select New IP/PSTN Gateway

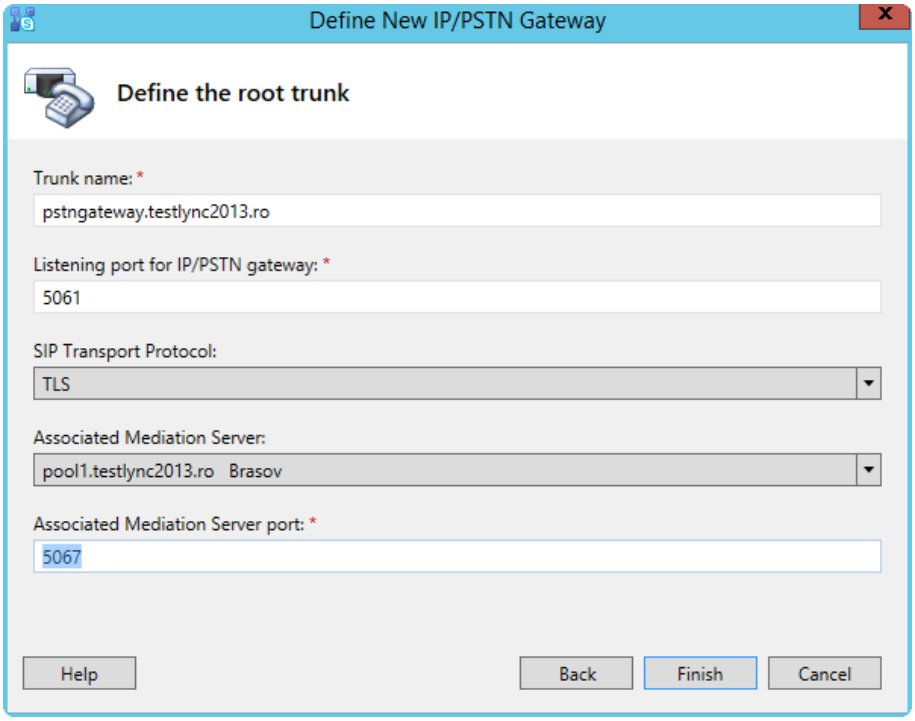

Skype for Business Server 2015, Topology Builder
File Action Help
Skype for Business Server
Brasov
Lync Server 2010
Lync Server 2013
Skype for Business Server 2015
Standard Edition Front End Servers
Enterprise Edition Front End pools
Director pools
Mediation pools
Persistent Chat pools
Edge pools
Trusted application servers
Video Interop Server pools
Shared Components
SQL Server stores
File stores
PSTN gateways
Trunks
Office Web Apps Servers
Video gateways
SIP Video trunks
Branch sites
The properties for this item are not available for editing.
Activate Windows
Go to System in Control Panel to activate Windows.

1) In the Define New IP/PSTN Gateway dialog box, do the following:

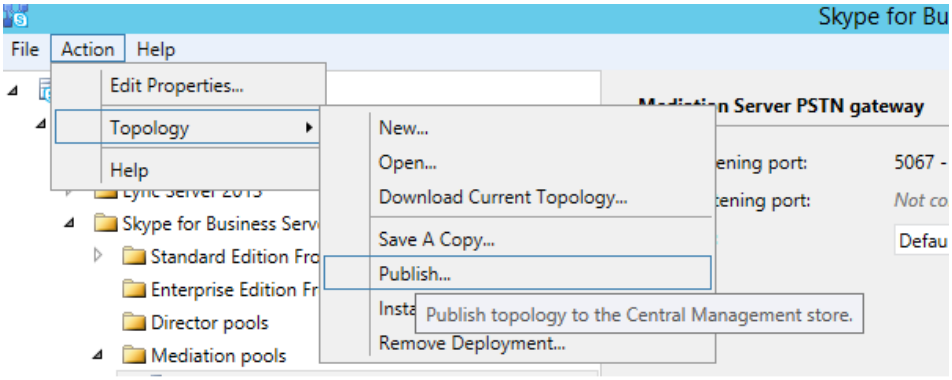
- In Define the PSTN Gateway FQDN specify the IP address or FQDN of the OpenScape 4000.
- In Define the IP address select Use all configured IP addresses if the gateway is defined in DNS, or Limit service usage to selected IP addresses to set the IP manually.
- In Define the root trunk, at Listening port for IP/PSTN gateway set the port to 5060 for TCP connection, or 5061 for TLS connection.
- Under Sip Transport Protocol, click TCP for unsecure connection, or TLS for secure connection.
- In Associated Mediation Server select the mediation server.
- In Associated Mediation Server port select 5068 for TCP connection, or 5067 for TLS connection.







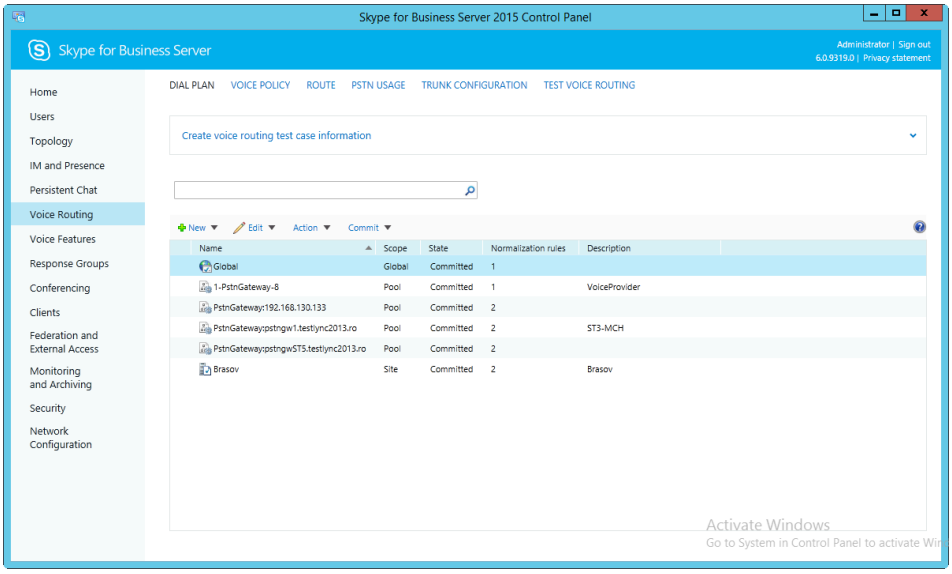
2) To publish your change to the Skype for Business Server 2015 topology, in the Action panel of the Topology Builder, point to Topology, and then click Publish.



14.9.3.5 Define Dial Plan

Define dial plan rules in Skype for Business Server 2015 Control Panel.

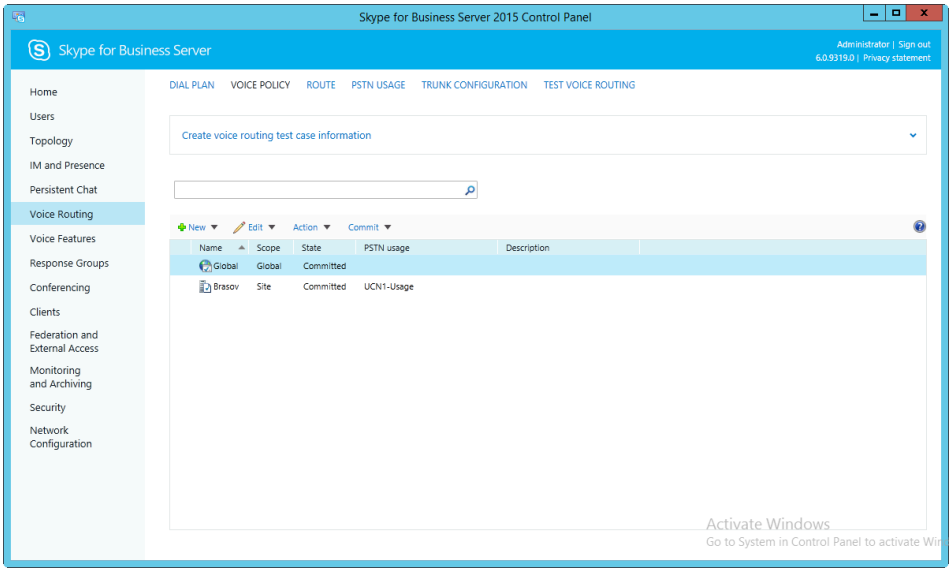
1) Start Skype for Business Server 2015 Control Panel
2) Click Voice Routing, and then click the Dial Plan tab.
3) Create normalization rules which permit Skype for Business users to dial OpenScape 4000 phones and the PSTN.
4) To commit your changes, click Commit, and then click Commit all.



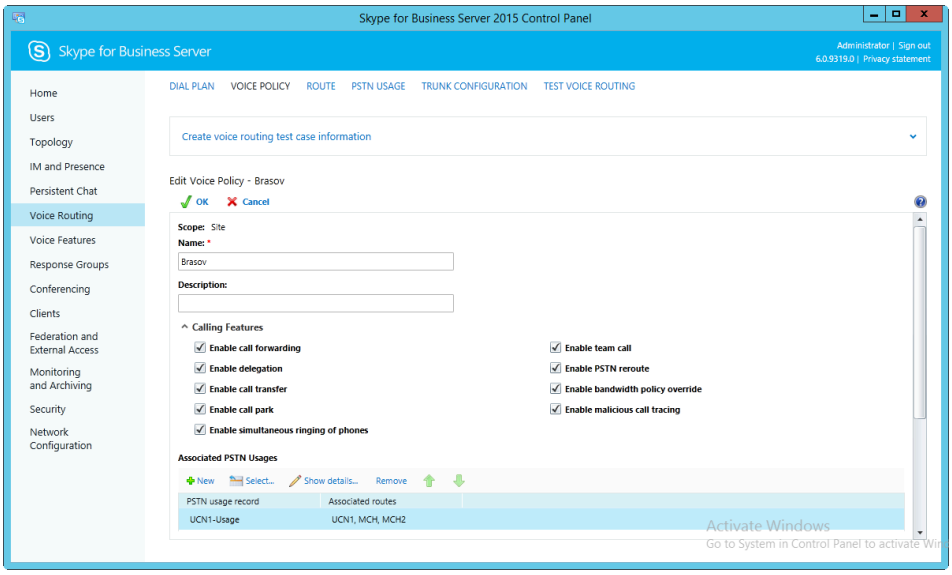
14.9.3.6 Create Voice Policy

Users assigned to specific voice policy will be able to dial out through the Direct SIP connection to the OpenScape 4000 system.

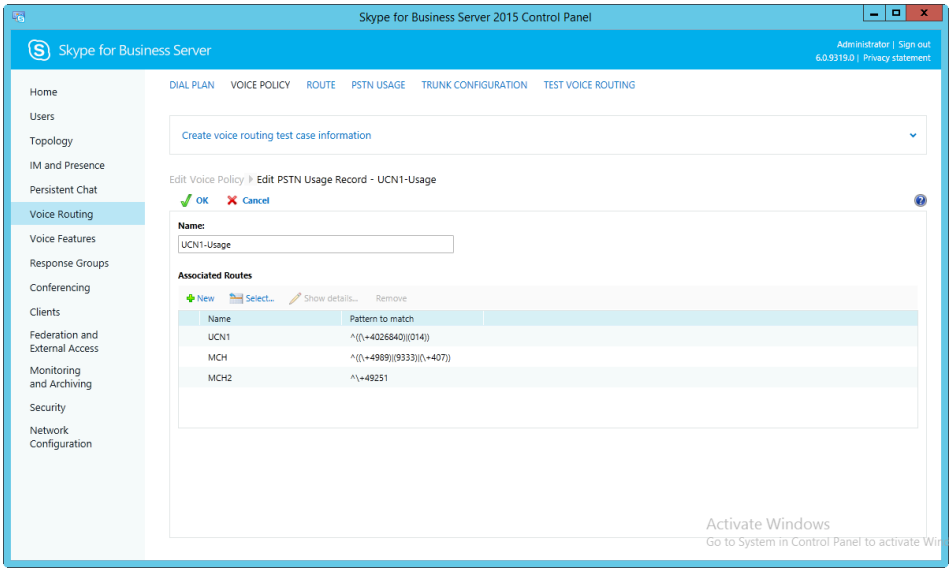
1) Click Voice Routing, and then click the Voice Policy tab.
2) Click New, and depending on the scope of the policy you want to create, click Site Policy or User Policy.



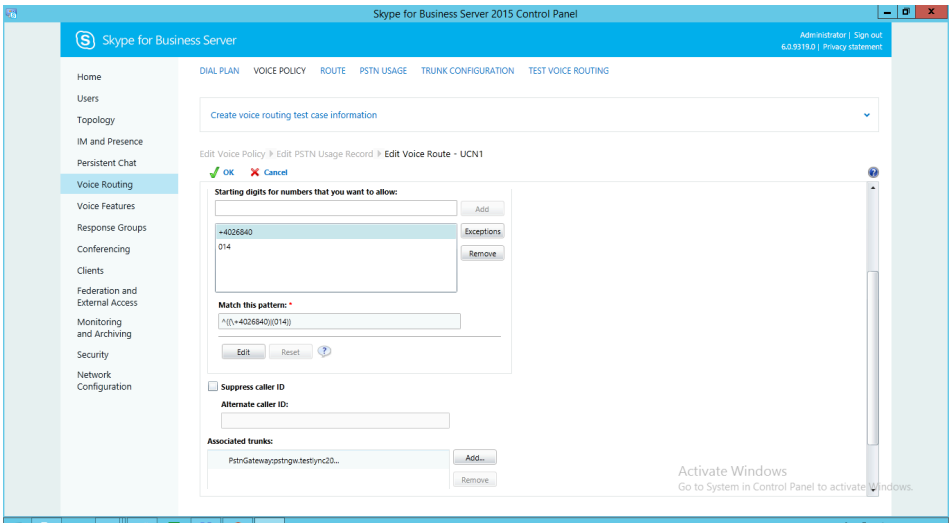
1) Specify a unique name for this voice policy, and provide a description (optional).
2) Create a new PSTN usage for this policy, click New.



1) Specify a name for the new PSTN usage record. The name must be unique to this specific voice policy. Also, provide a detailed description of the PSTN usage record.
2) To associate a route with this PSTN usage, click New.



1) Specify a name for this route, and provide a meaningful description.
2) To associate the OpenScape 4000 gateway with this new route, click Add.

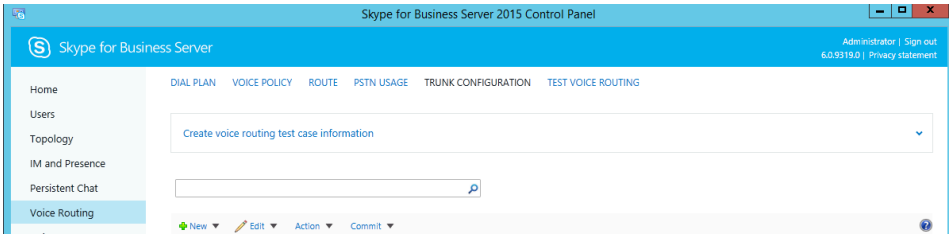


1) Select the OpenScape 4000 gateway that you created earlier.
2) Click OK in all different dialog boxes to complete the creation of the voice policy.
3) To commit your changes, click Commit, and then click Commit all.

14.9.3.7 Define Trunk Configuration

The next step is to assign the OpenScape 4000 gateway to a trunk associated with a pool or a site as follows:

1) On Skype for Business Server 2015 Control Panel click Voice Routing, and then click the Trunk Configuration tab.
2) Click New, and depending on the scope of the policy you want to create, click Site Configuration or Pool Configuration.

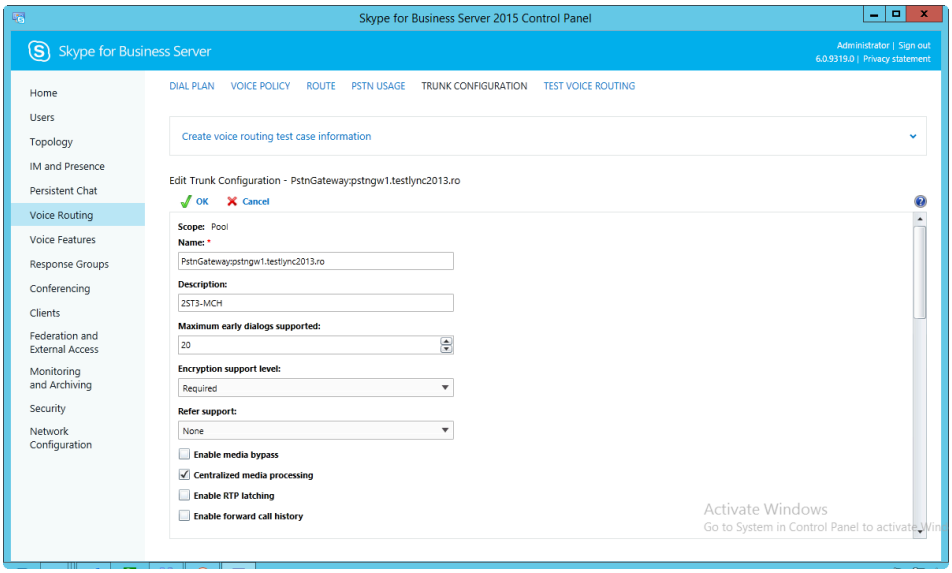


1) Select a pool or site for this trunk configuration.
2) In the New Trunk Configuration dialog box, click OK.
3) To commit your changes, click Commit, and then click Commit all.

NOTICE: make sure that Enable Media bypass is disabled and Enable refer support is set to “None”.

---

1) To enable encryption select Required on Encryption support level drop down.

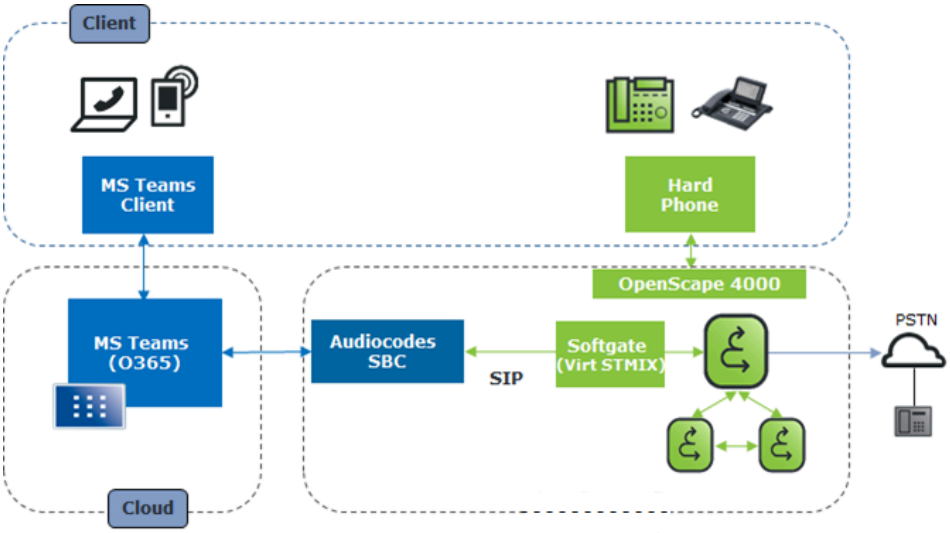


1) To commit your changes, click Commit, and then click Commit all.

14.10 MS Teams DR with Audio Codes SBC

14.10.1 Feature Overview

Native SIP trunks located on SoftGate/STMIX/STMIY are considered for interoperability between OpenScape 4000 and MS Teams via Audiocodes SBC.



14.10.1.1 Features available (Overview):

- Basic call
- CLIP/CLIR features - Calling Party Name and Number delivery (Allowed and Restricted)
- Call Transfer (Blind, semi-attended, Attended)
- Call Forwarding (CFA - Call Forward All, CFB - Call Forward Busy, CFNA - Call Forward No Answer)
- Hold and Retrieve
- Three-way conferencing
- DTMF
- Security

14.10.2 Restrictions and Hints

- General restrictions

Refer not supported

- Feature restrictions

Display Information: Phone Number

Hold indication: MOH (no display information)

No display update after call forwarding

14.10.3 Configuration

See Chapter Native SIP Trunking on page 829 for general configuration.

SIP trunking profile: MS Teams

14.11 MS Teams Direct Routing with OpenScape SBC

OpenScape 4000 connected to Microsoft Teams Direct Routing via Atos-Unify OpenScape SBC.

14.11.1 Network Topology

The block diagram below shows the Teams Direct Routing connection topology, Teams Phone System is directly connected to OpenScape SBC.

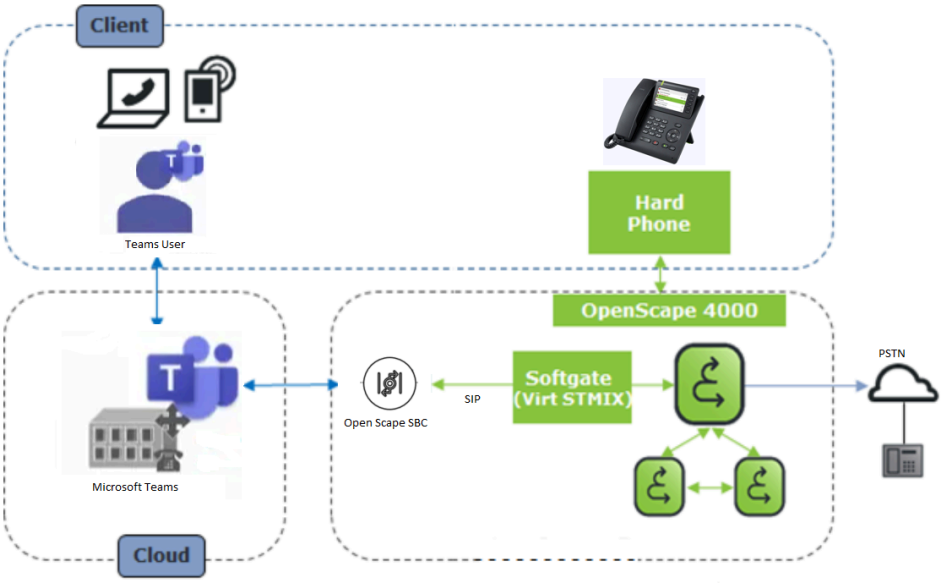


Figure 322: Teams Direct Routing connection

Native SIP trunks located on the SoftGate/STMIX/STMIY are considered for interoperability between OpenScape 4000 and MS Teams via OpenScape SBC.

14.11.2 OpenScape 4000 Configuration

14.11.2.1 AMO Configuration

OpenScape 4000 interworking with OS SBC and MS Teams supports two setups with:

- Three SIP trunks (Native SIP trunks located on the SoftGate/STMIX/STMIY) connected to SBC via Clustered Mode.
- Only one SIP trunk.

To configure the OpenScape 4000 routing, see Native SIP Trunking on page 829 for the general configuration steps.

14.11.2.2 STMIX/STMIY/vHG WBM configuration

This chapter presents the configuration for the STMIX/STMIY/vHG WBM side. MS Teams trunk profile need to be configured and enabled.

Perform the following steps:

1) Go to **vHG WBM > Configuration > Voice Gateway**, extend **SIP Trunk Profiles** and click on **MS Teams**.

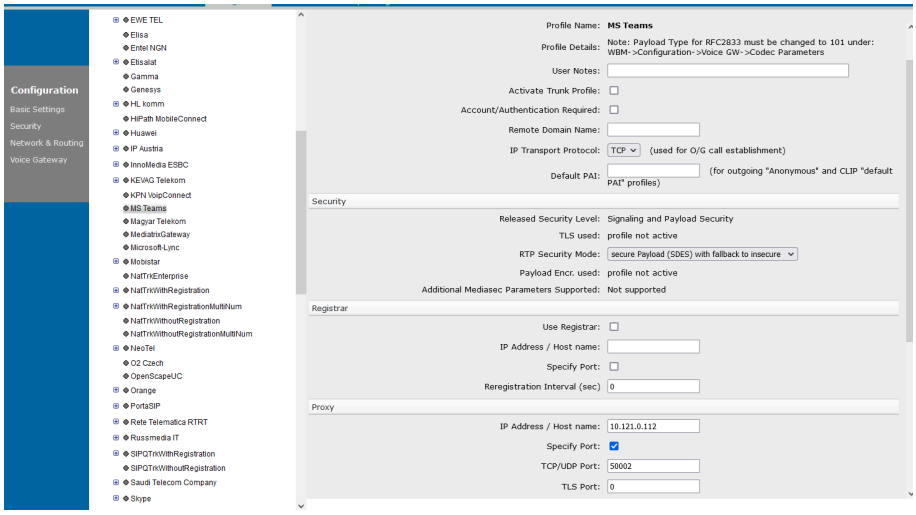


Figure 323: MS Teams

2) Under **Proxy** settings, enable the **Specify port** check box and enter the following:

   - **IP Address /Host name:** SBC LAN IP.

     NOTICE: SBC LAN IP is the core side IP of the SBC used for direct routing to MS Teams.

   - **TCP/UDP Port:** 50002.

   Click the Apply button.

   Click the OK button.

3) After the above configuration is done, the trunk profile must be activated:

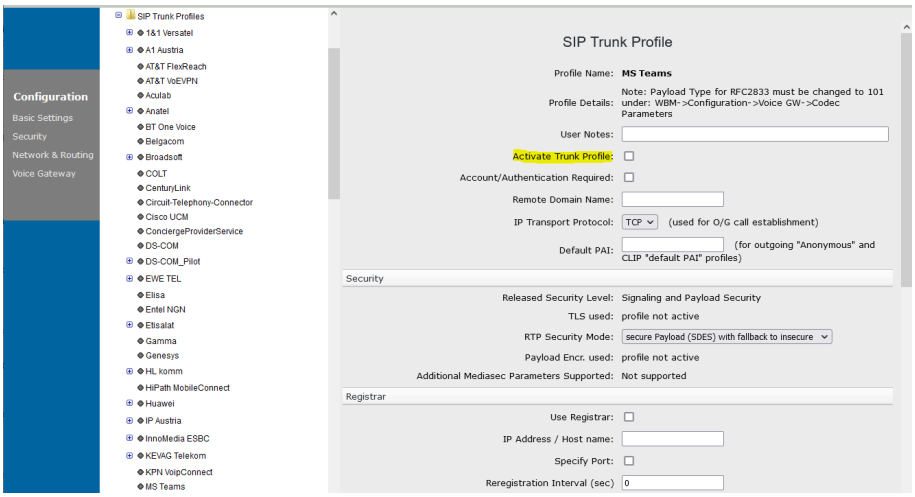


Figure 324: Activate Trunk Profile

Check the **Activate Trunk Profile** box.

Click the Apply button.

Click the OK button.

4) Enable **SIP OPTIONS** for Keep Alive communication with MS Teams:

Go to **vHG WBM > Configuration > Voice Gateway > SIP Parameters**.

The default value for **Trunking Parameters > SIP OPTIONS ping interval** is **0**. It needs to be set to a higher value.

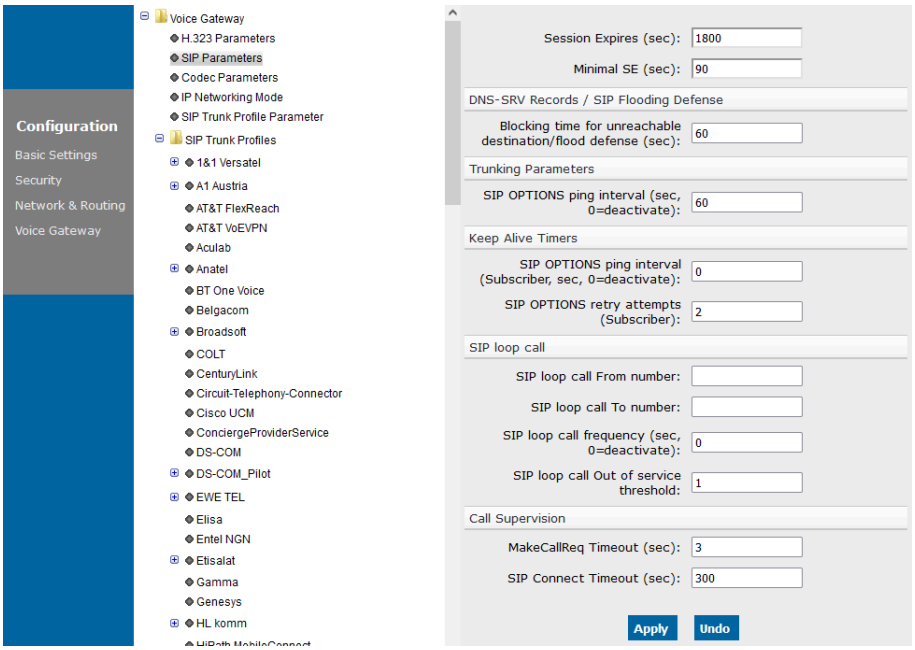


Figure 325: SIP OPTIONS ping interval

Click the Apply button.

Click the OK button.

5) Repeat the procedure for the rest of the vHGs (if the desired configuration uses four vHGs).

14.11.3 OpenScape SBC Configuration

This chapter outlines the configuration of OpenScape SBC for interworking with Teams Direct Routing. The OpenScape SBC will be configured with the connection to OpenScape 4000 and Teams Phone System (remote) endpoints.

14.11.3.1 Core Realm Interface

Use the TCP port number for the connection of OpenScape SBCs eth0 (core) interface to OpenScape 4000.

Go to **OS SBC Management Portal > Network/Net Services**.

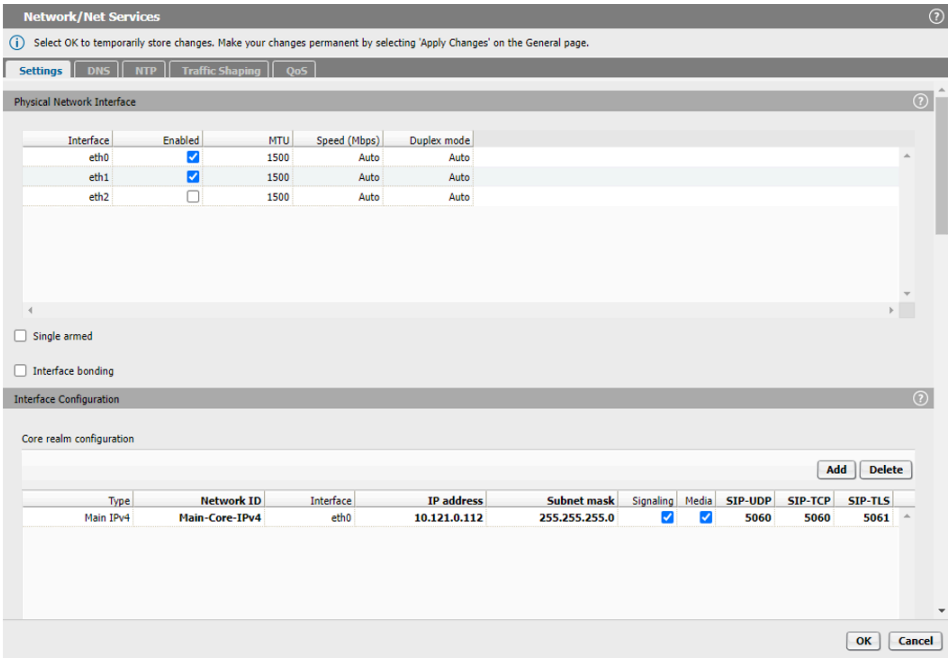


Figure 326: Network/Net Services

On **Settings** tab, in the **Core realm configuration** area, ensure that for the **eth0** interface, the value of the **SIP-TCP** filed is 5060.

Click the OK button.

On the SBC main page, click the Apply Changes button.

14.11.3.2 SIP Server

There are two possible setups:

- Simplex Mode, with one vHG configured.
- Cluster Mode, with more than one vHGs configured

The SIP connectivity to OpenScape 4000 is configured in **OS SBC Management Portal > VOIP > Sip Server Settings** window.

Simple Mode

The following parameters must be entered in the **Sip Server Settings** window:

- **Comm System Type**: Simplex
- **Target Type**: Binding
- **Primary Server:** 10.121.121.138 (vHG address)
- **Transport:** TCP
- **Port:** 5060 (listening port for the vHG)

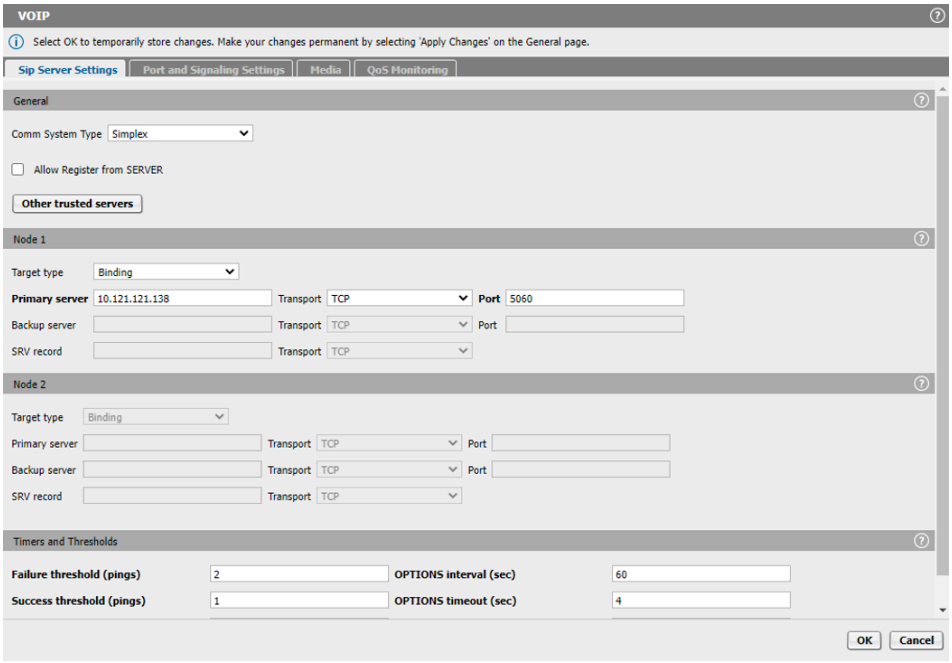


Figure 327: Simplex configuration

Once the above parameters are set, click the OK button. Next, on the main OS SBC page, click the Apply Changes button.

Clustered Mode

In the Sip Server Settings window, for the Comm System Type select the Clustered option.

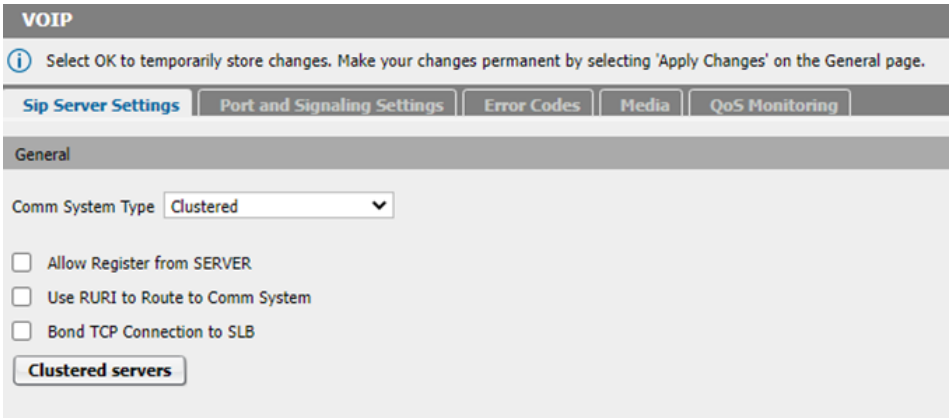


Figure 328: Clustered Mode

Next, click the **Clustered servers** button and add all the vHGs configured under chapter 14.11.2.2. Click the Add button to select each vHG and enter the following parameters:

- **Group Name:** MS_TEAMS (friendly name)
- **Node Name:** Teams_SP1 (friendly name)
- **Priority:** 1
- **IP address or FQDN:** 10.121.121.138 (vHG address)
- **Port:** 5060 (listening port for vHG)
- **Transport:** TCP

Once the above parameters are set, click the OK button twice. In the OS SBC main page, click the Apply Changes button.

The **Clustered servers** window should look like the figure below:

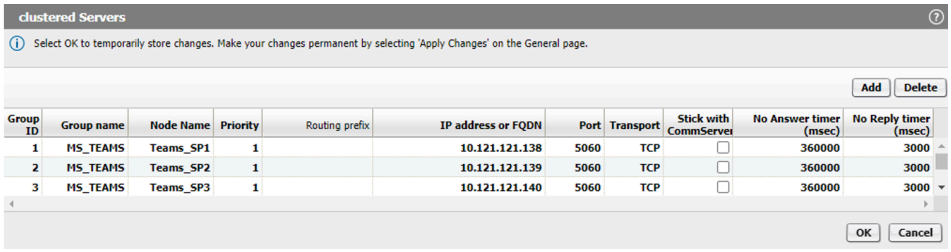


Figure 329: Clustered servers

Navigate to **OS SBC Management Portal > VOIP > Error Codes** and make sure the option **Enable routing for all codes** is checked.

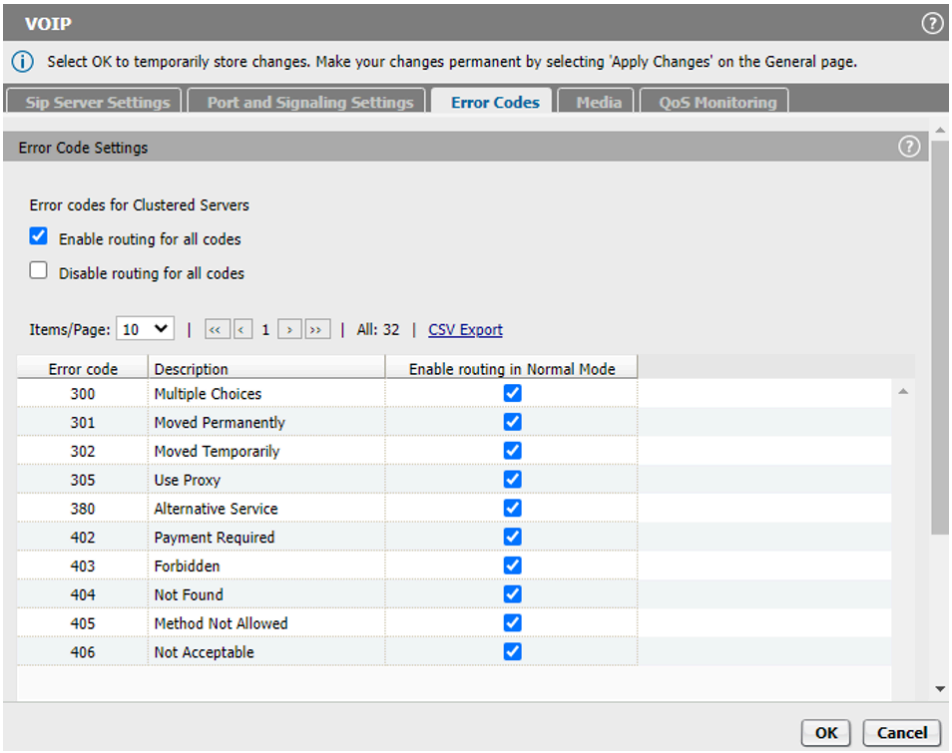


Figure 330: Enable routing for all codes

Once the **Enable routing for all codes** option is enabled, click the OK button. In the OS SBC main page click the Apply Changes button.

14.11.3.3 Certificates

Microsoft Phone System Direct Routing interface allows only TLS connections for SIP traffic from the SBCs with a certificate signed by one of Microsoft's trusted Certification Authorities.

The certificate needs to have the SBC FQDN as the common name (CN) in the subject field. Certificates with a wild card in the certificate Subject Alternate Name field conforming to RFC2818 are also supported.

For more information about the certificate and current Microsoft supported Certification Authorities, refer to Microsoft site:

https://docs.microsoft.com/en-us/microsoftteams/direct-routing-plan#public-trusted-certificate-for-the-sbc.

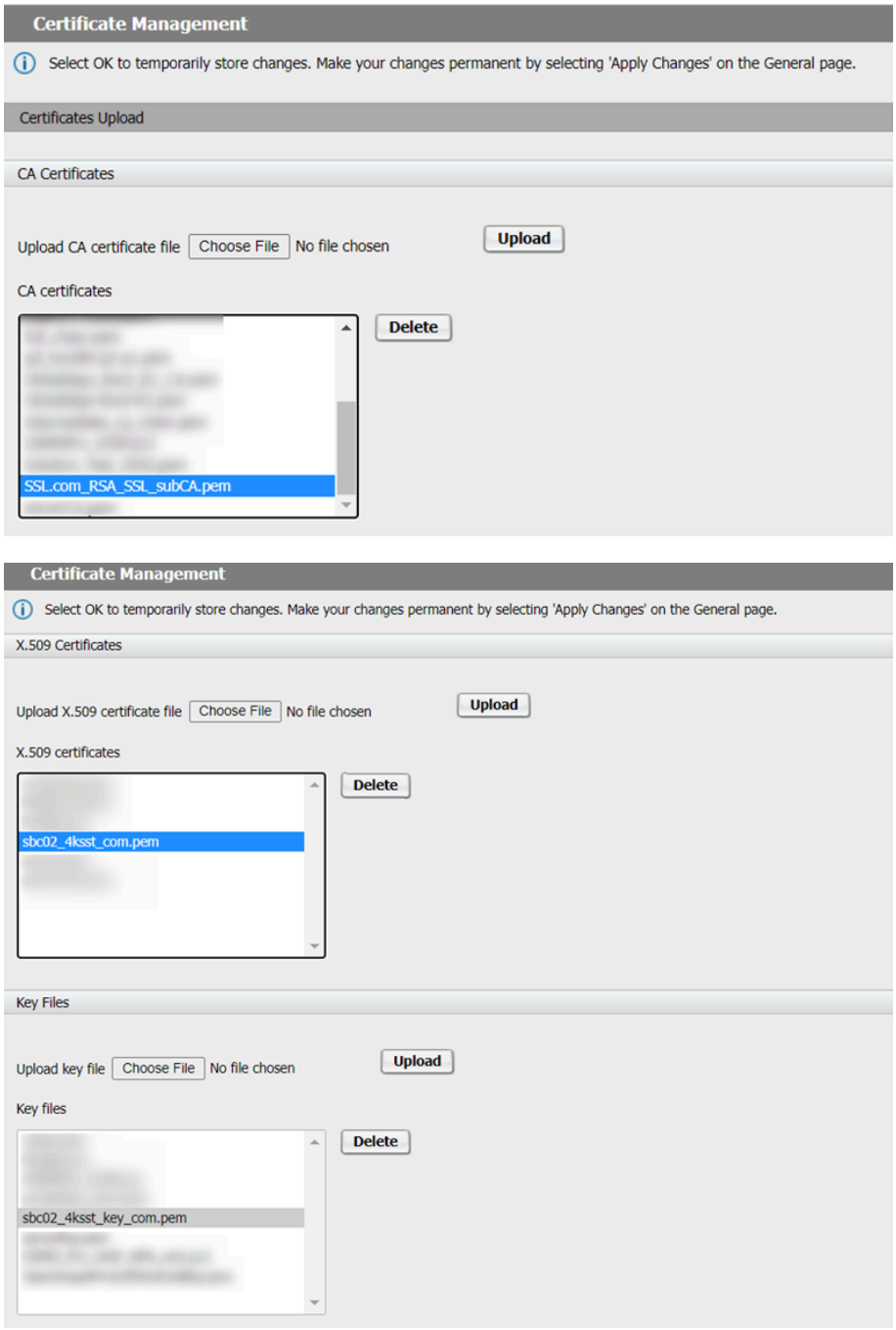
For the OpenScape SBC TLS interconnection to Microsoft Phone System, 3 files in pem format are required from the Certification Authority:

- CA certificate (e.g. ca_chain.pem)
- Server certificate for OS SBC (e.g. certificate.pem)
- OS SBC server certificate private key used for the CSR to CA (e.g. privatekey.pem)

The above files must be uploaded to OS SBC and used for the TLS connection with the Microsoft Phone System interface. For this, follow the below procedure:

1) Navigate to **OS SBC Management Portal > Security > General** and click on **Certificate Management**

2) Upload the **SSL.com_RSA_SSL_subCA.pem** file to **CA Certificates**, the **sbc02_4ksst_com.pem** file to **X.509** and the **sbc02_4ksst_key_com.pem** file to **Key Files**, as shown in the figures below:



3) In the same window, click the Add button to create the certificate profiles.

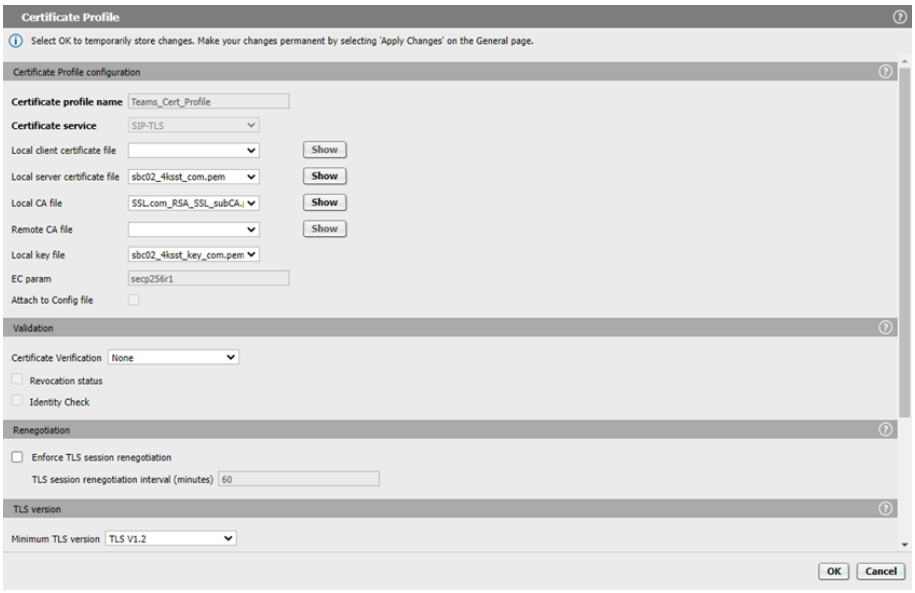


Figure 331: Certificate Profile

4) In the Certificate Profile window, enter the following parameters:
   - **Certificate profile name:** Teams_Cert_Profile (friendly name)
   - **Certificate service:** SIP-TLS
   - **Local server certificate file:** certificate.pem
   - **Local CA file:** ca_chain.pem
   - **Local key file:** privatekey.pem
   - **Minimum TLS version:** TLS V1.2
5) Click the OK button.
6) In the **Certificate Management** window, click the OK button.
7) In the **Security** window, click the OK button.
8) In the OS SBC main page, click the Apply Changes button.

14.11.3.4 Teams Media Profile

The communication between Teams Phone System is secure with secure audio (SRTP).

To configure the Teams Media Profile, proceed as follows:

1) Go to **OS SBC Management Portal > VOIP > Media**.

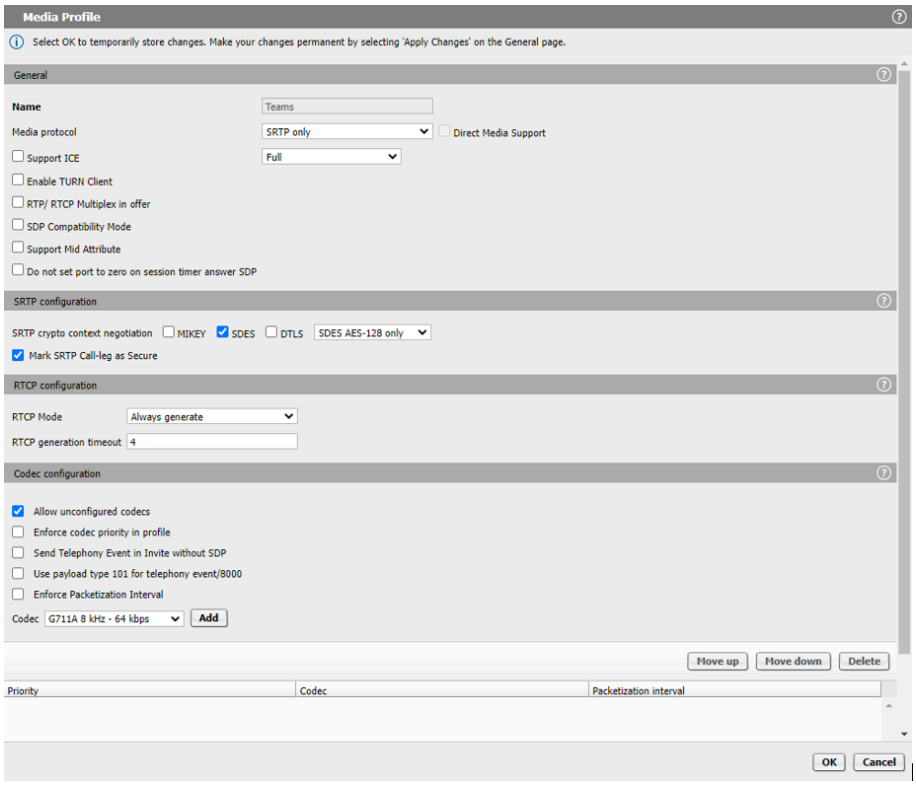


Figure 332: Media Profiles

2) In the Media Profiles area, click the Add button to create the media profile for OS SBC - Teams connections. The following parameters must be entered:
   - **Name:** Teams (friendly name)
   - **Media protocol:** SRTP only
   - **Support ICE:** Unchecked (for MB = OFF case)
   - **SRTP crypto context negotiation:** SDES
   - **Mark SRTP Call-legasSecure:** Checked
   - **rtcpMode:** Bypass or Always Generate
   - **Allow unconfigured codecs:** Checked
3) In the **Media** window, click the OK button.
4) In the **VOIP** window, click the OK button.
5) In the main OS SBC page, click the Apply Changes button.

14.11.3.5 OpenScape 4000 Media Profile

To configure the OpenScape 4000 Media Profile, proceed as follows:

1) Go to **OS SBC Management Portal > VOIP > Media.**

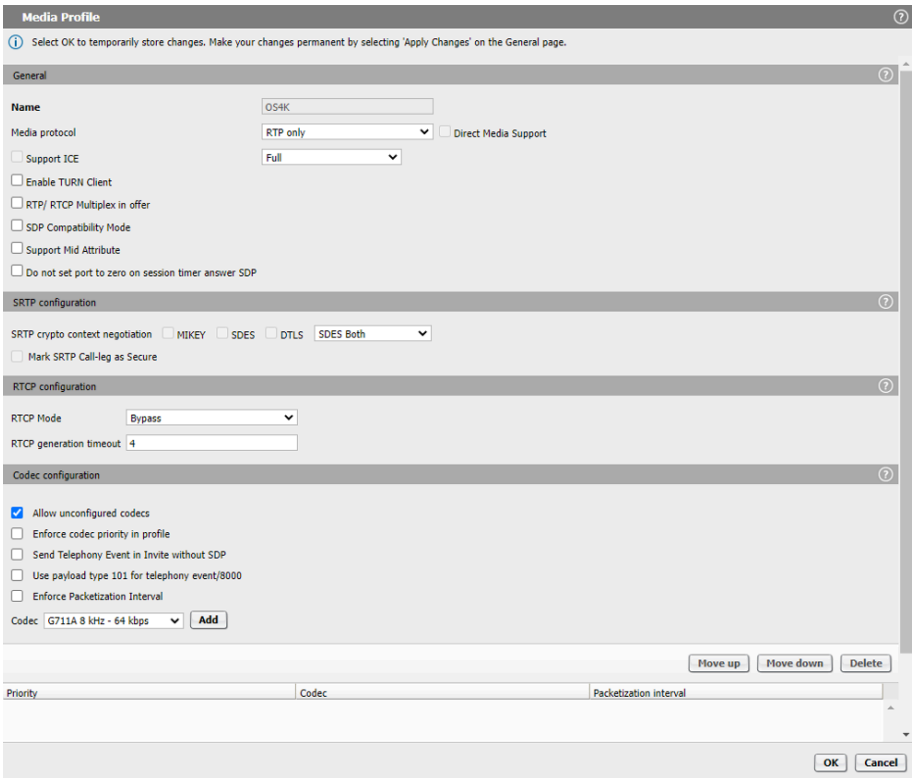


Figure 333: Media profile

2) In **Media Profiles** area, click the **Add** button to create the media profile for OS SBC – OpenScape 4000 connection. The following parameters must be configured:
   - **Name:** OS4K (friendly name)
   - **Media protocol:** RTP only
   - **RTP/RTCP Multiplex in offer:** Unchecked
   - **Allow unconfigured codecs:** Checked
3) In the **Media** window, click the OK button.
4) In the **VOIP** window, click the OK button.
5) In the main OS SBC page, click the Apply Changes button.

14.11.3.6 General Media Settings

After creating the media profiles, the general media setting must be configured. To do so, the below procedure must be followed:

1) Go to **OS SBC Management Portal > VOIP** > **Media** window.

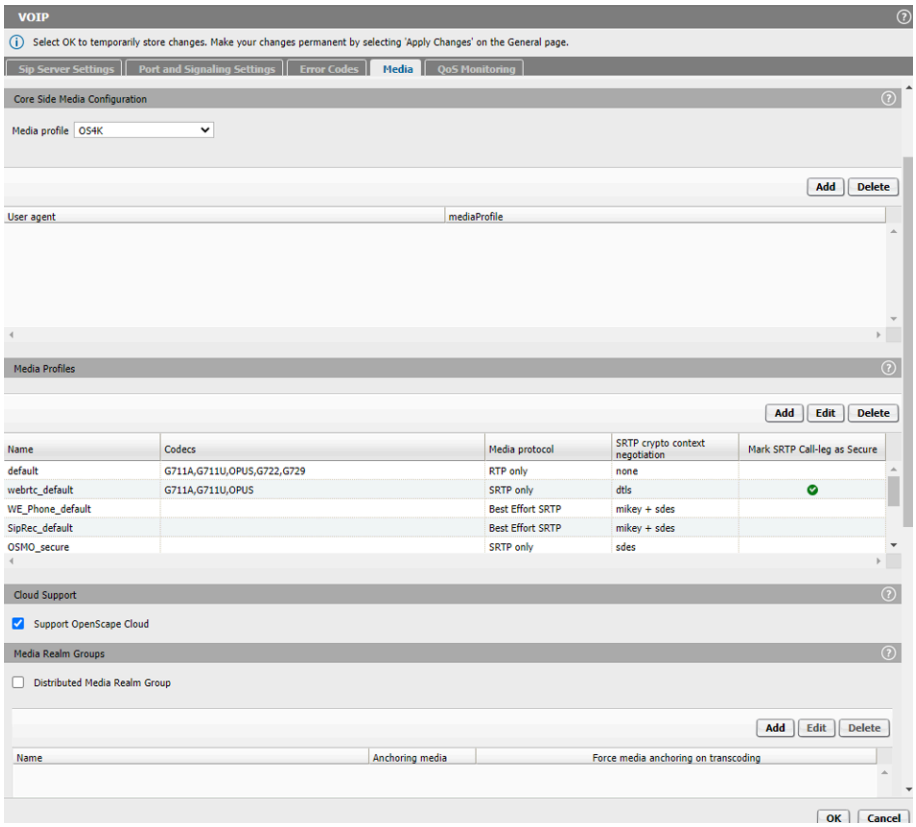


Figure 334: VOIP window

2) Under **Core Side Media Configuration** chose from the drop down list the corresponding media profile added in section OpenScape 4000 Media Profile on page 1000.
   - **Media profile:** OS4K
3) Click the OK button.
4) In the main OS SBC page, click the Apply Changes button.

14.11.3.7 Remote Endpoints

The **Remote Endpoint** configuration for OS SBC with Teams Phone System is set up.

To be able to set MS Teams profile in SIP Service Provider Profile, a license is required.

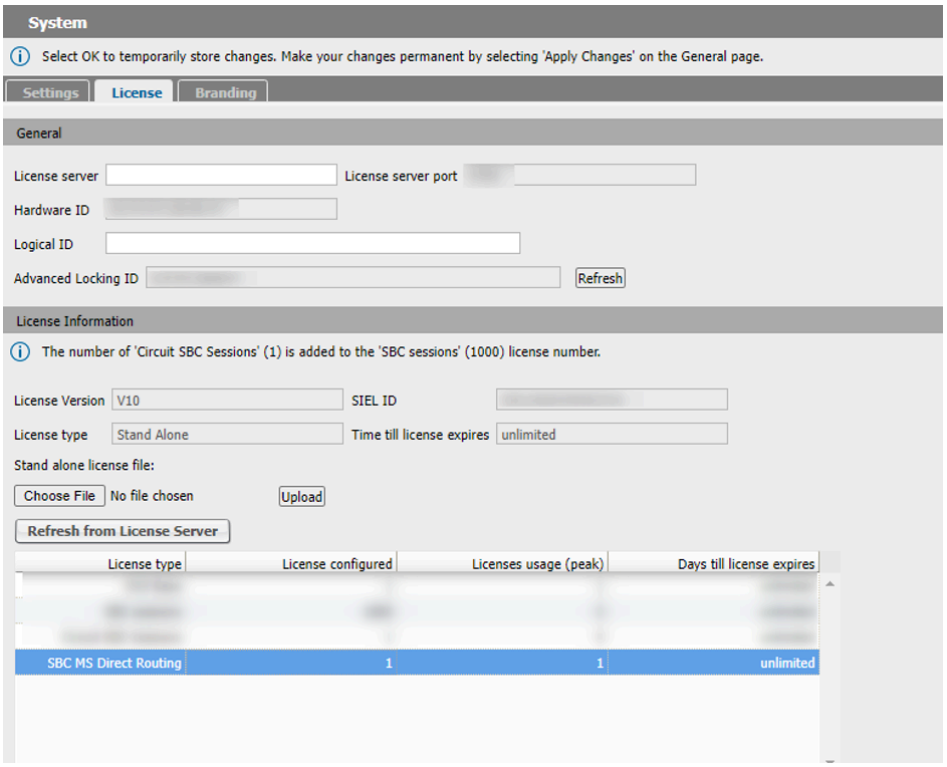


Figure 335: SIP Service Profile license

Navigate to **OS SBC Management Portal > Features** window, to check and configure the **Enable Remote Endpoints** option.

On the **Remote Endpoints** window, click the **Add** button in **SIP Service Provider Profile** area to add the endpoint profile for the OS SBC – Teams Phone System endpoint.

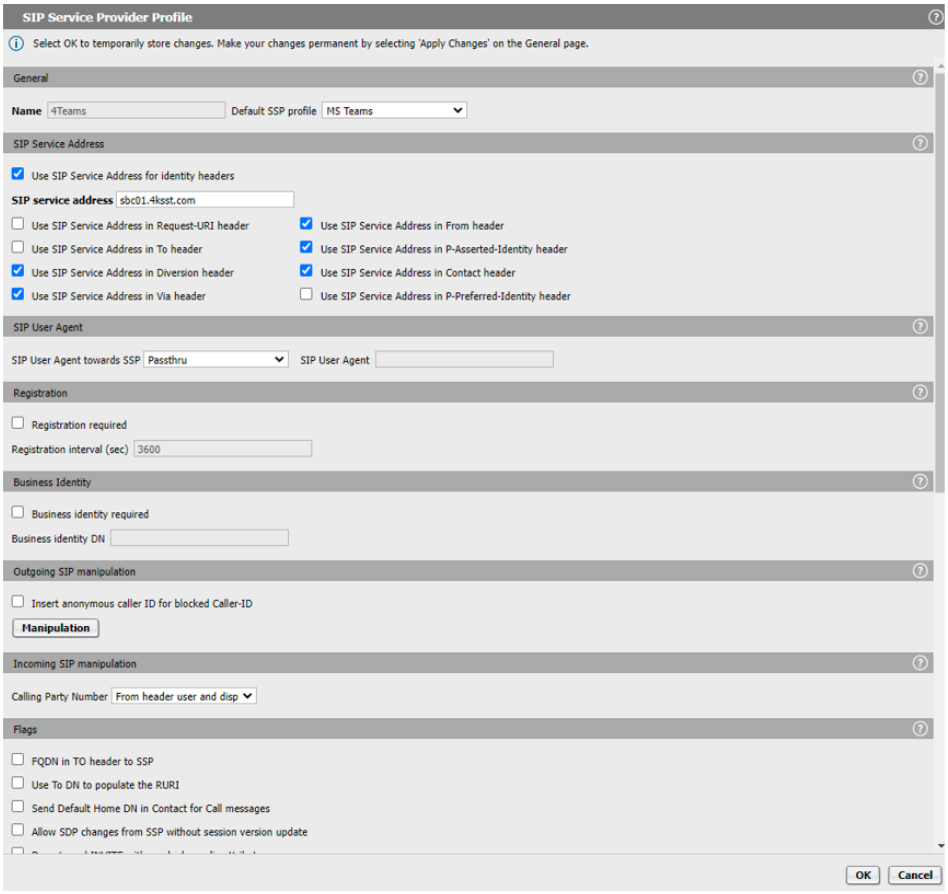


Figure 336: SIP Service Provider Profile

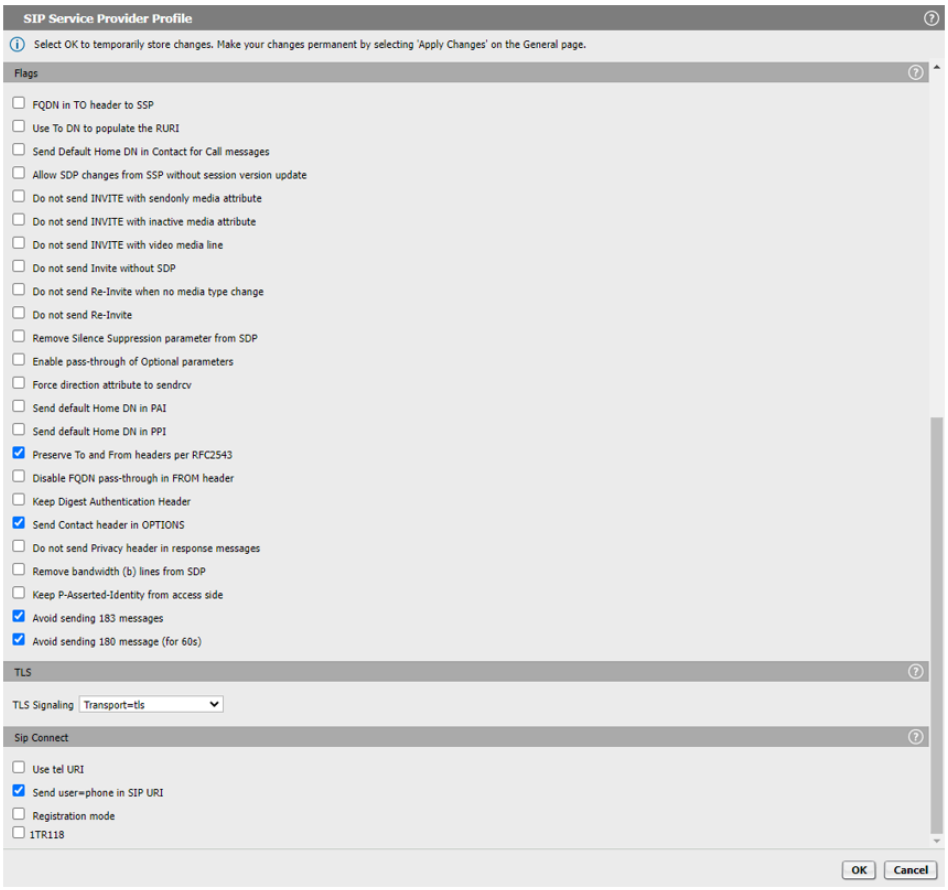


Figure 337: SIP Service Provider Profile

On the **SIP Service Provider** window, the following parameters must be configured:

- **Name:** 4Teams (friendly name)
- **Default SSP Profile:** MS Teams
- **SIP service address:** sbc01.4ksst.com (SBC public FQDN)

Click the **OK** button to return to the **Remote Endpoints** window.

In the **Remote endpoint configuration** area, click the **Add** button.

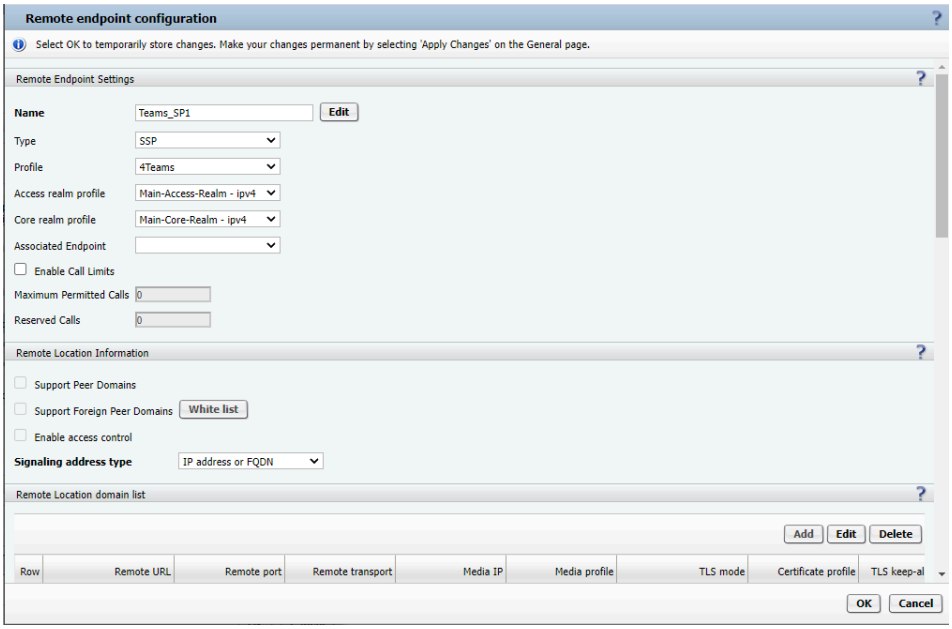


Figure 338: Remote endpoint configuration

In the **Remote endpoint configuration** window, the following parameters must be configured:

- **Name:** Teams_SP1 (friendly name)
- **Type:** SSP
- **Profile:** 4Teams

Click the **Add** button in the **Remote Location domain list** area.

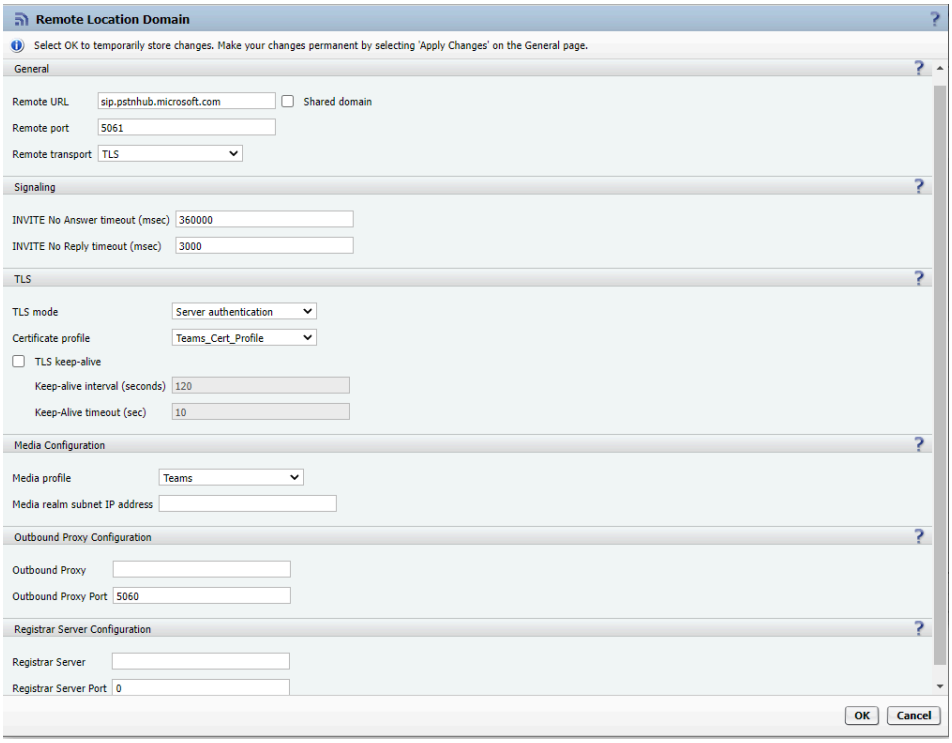


Figure 339: Remote Location Domain

In the **Remote Location Domain** window, the following parameters must be configured.

- **Remote URL:** sip.pstnhub.microsoft.com (Teams FQDN 1)
- **Remote port:** 5061
- **Remote transport:** TLS
- **TLS mode:** Server authentication
- **Certificate profile:** Teams_Cert_Profile (see section SIP Server)
- **Media profile:** Teams (see section Certificates)

Click on the **OK** button to return to **Remote endpoint configuration.**

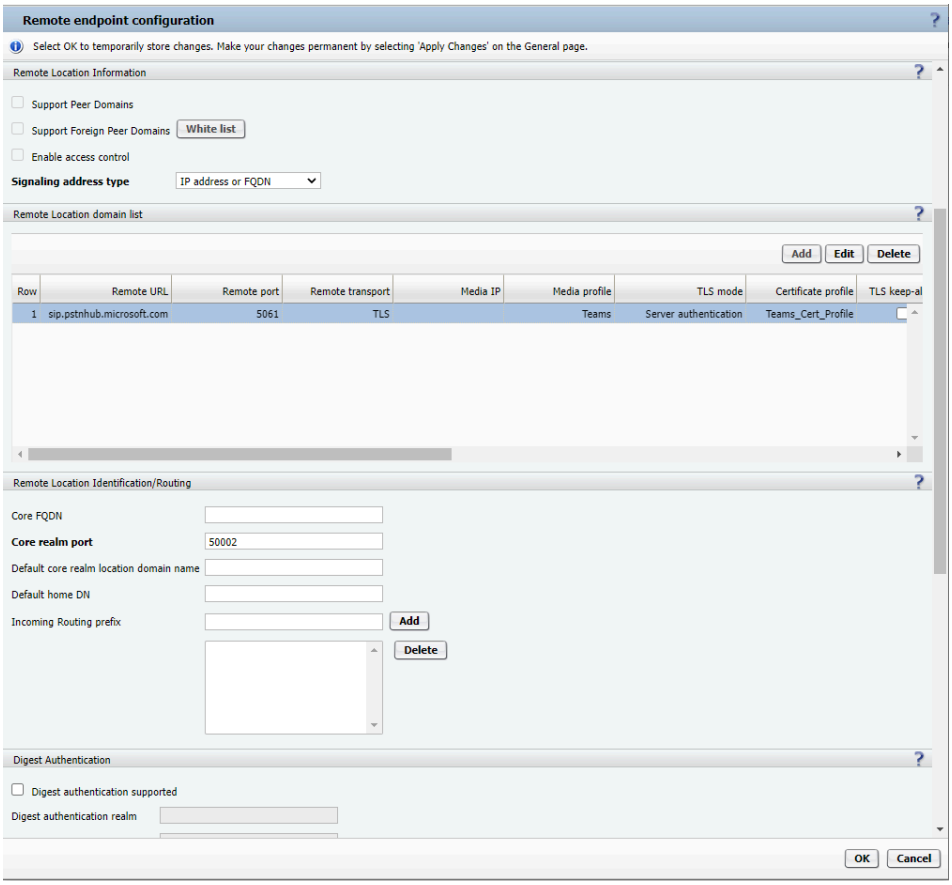


Figure 340: Remote endpoint configuration

In the **Remote endpoint configuration** window, the following parameters must be configured:

- **Signaling address type:** IP address or FQDN
- **Core realm port:** 50002 (configured under vHG MS Teams SIP trunk profile)

Click the **OK** button to return to the **Remote Endpoints** window.

Repeat the procedure for the rest of the Teams FQDNs (i.e. sip2.pstnhub.microsoft.com, sip3.pstnhub.microsoft.com).

The **Remote Endpoints** window should look like the figure below:

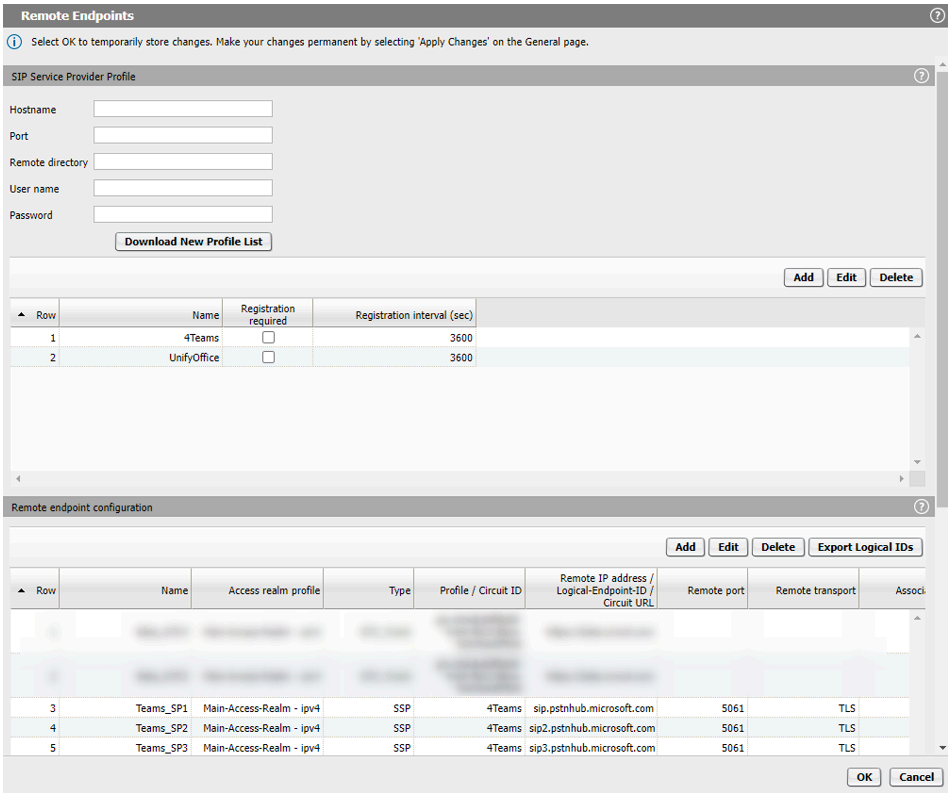


Figure 341: Remote Endpoints

Click the OK button on all opened windows.

Click the Apply button on the main OS SBC page.

14.11.4 MS Teams Direct Routing Configuration

This document describes how to connect the Unify OpenScape SBC (with OpenScape 4000) to Microsoft Teams Direct Routing configuration. Microsoft Teams Direct Routing configuration is not included in current document and may be found under https://docs.microsoft.com/en-us/microsoftteams/direct-routing-configure.

NOTICE:

Make sure the SBC is added with **Forward P-Asserted-Identity (PAI) header** set to **Off**.

Using the Microsoft Teams admin center, in the left navigation panel, go to **Voice > Direct Routing**, then click the **SBCs tab**.

Select the already configured SBC (based on Microsoft official documentation provided above) and click the **Edit** button. Next, set the **Forward P-Asserted-Identity (PAI) header** to off and click the Save button.

NOTICE:

You need to open ports in your firewall for the IP address ranges to allow incoming and outgoing traffic to and from the addresses for signaling purposes. For more information, refer to the Microsoft documentation: https://learn.microsoft.com/en-us/microsoftteams/direct-routing-plan

14.11.5 Features Available (Overview)

- Basic Call
- CLIP/CLIR features - Calling Party Name and Number delivery (Allowed and Restricted)
- Hold / Retrieve
- Toggle after consultation
- Transfer (attended/blind)
- Conference
- Call forwarding
- Send / Receive DTMF tones
- Park / Unpark
- Parallel ringing

14.11.6 General Restrictions and Limitations

MS Teams Media Bypass Mode OFF is currently supported.

MS Teams P-Asserted-Identity (PAI) header is currently not supported by OS4K and must be disabled from MS Teams SBC Direct routing configuration.

There is no phone display update after transfer (and forward scenarios) as Teams does not send PAI in the 200OK event (even if ForwardPAI is activated on tenant). Additionally, it also neglects the PAI received from the other side. Teams reads the display information from the “FROM” header.

History-info header is not yet supported by OpenScape 4000. (affects forward, parallel ringing scenarios)

In a conference call, the display is not updated which is a limitation of native SIP trunk.

NOTICE: DMC can not be used on the SIP trunk interface to MS Teams.

14.12 SIP URI Dialing

For internal video calls with OpenScape 4000, OpenScape SBC and OpenScape UC, there are currently two possibilities:

- Video calls between OpenScape 4000/ OpenScape UC endpoints;
- Video conferences held by OpenScape UC conference bridge for OpenScape 4000/ OpenScape UC endpoints.

For video calls and video conferences with other companies, OpenScape 4000 supports the following two use cases:

- **Video dial out**: OpenScape UC clients type in a SIP URI string and join video conferences from other companies (routed through internet).
- **Video dial in**: users from other companies type in a SIP URI string and join the video OpenScape UC conference as unknown users.

The functionality is achieved with the following video components:

- Call Control: OpenScape 4000
- Video gateway: OpenScape SBC
- Video MCU: video conference server
- Video Clients: OS UC Clients: Fusion, WebRTC client
- Video Room Systems from Poly: e.g Group series, Group 7500

14.12.1 Video Dial Out

For the video dial out method, the UC clients type in a SIP URI string and are able to join video conferences from other companies (routed through internet).

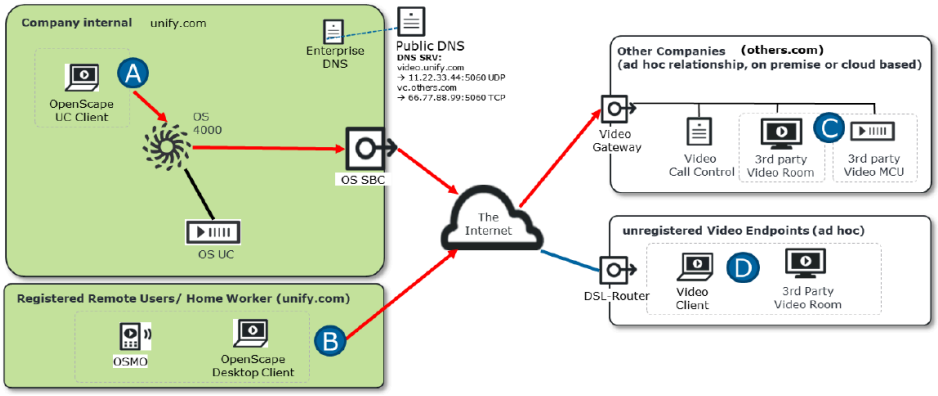


Figure 342: Video Dial Out

Table 81: D1 and D2 are connected

Product	Dial out scenario: Task/ Responsability
OpenScape UC client OpenScape UC	• Type in SIP URI address • Forward to OpenScape 4000 (via CSTA) OpenScape 4000
OpenScape 4000	• Analyze SIP URI • Route call to SBC (wildcard based or domain based defined in SBC)
OpenScape SBC	• Resolve SIP URI to IP address • Send call to internet

14.12.1.1 Call Routing of external alphanumeric SIP URIs

OpenScape 4000 must route video calls using an external SIP URI address to the defined SBC (if more than one SBC is installed). External means the dialed SIP-URI is not assigned to an OpenScape 4000 subscriber or is within the own or a trusted domain.

OpenScape 4000 must forward/ route SIP URI calls without modifying the dialed alphanumeric SIP-URI. This allows the next SIP peer to route the call to the correct destination without the loss of important parameters (e.g. port)

OpenScape 4000 must route SIP URI Invites with an unknown domain to a predefined SBC (e.g. SBC1), using wildcard routing.

Additionally OpenScape 4000 must route SIP URI Invites with specific domains to predefined SBCs (domain based routing to the trunk towards SBC, e.g. domain “customer1.com” should be routed to SBC2, domain “customer2.com” should be routed to SBC3).

14.12.1.2 SIP URI dialing via CSTA interface

The UC clients represent the video clients within the OpenScape 4000 solution.

The UC clients are registered to OpenScape 4000. The calls from UC clients will be initiated via CSTA to OpenScape 4000.

Therefore, OpenScape 4000 must interpret and resolve SIP URI dialing within CSTA accordingly.

OpenScape 4000 must accept and route SIP URI calls received from the UC Clients or the OpenScape UC media server.

14.12.1.3 SIP-Q Support

SIP-Q does not support the transport of alphanumeric SIP URIs.

The UC clients are registered to OpenScape 4000. The calls from UC clients will be initiated via CSTA to OpenScape 4000.

Any route in translation that leads to an alphanumeric SIP URI to be sent as called party to a SIP-Q endpoint shall be treated as ‘Route not Available’ by translation.

14.12.2 Video Dial In

Users from other companies dial SIP URI string and join the video conference of the OpenScape UC conference server as unknown users.

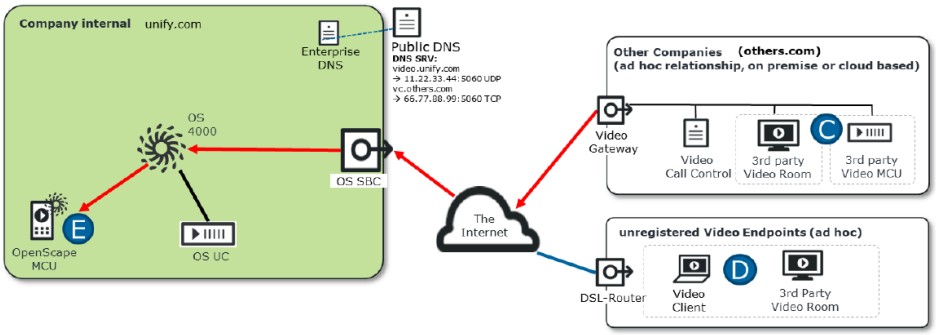


Figure 343: Video Dial In

Table 82: D1 and D2 are connected

Product	Dial in scenario: Task/Responsability
Other Company	• Dial SIP URI address of OpenScape UC conference server, e.g video10@unify.com • Call will be routed through the internet to OpenScape SBC
OpenScape SBC	• Entry in company network • Verify incoming call (e.g white lists) • Forward call to OpenScape 4000 • Reject/ignore call
OpenScape 4000	• Route call to OpenScape UC MediaServer / MCU
OpenScape UC MS/ MCU	• Proof PIN at conference portal/ welcome screen • Route to conference • Terminate call

The UC clients are registered to OpenScape 4000. The calls from UC clients will be initiated via CSTA to OpenScape 4000.

Any route in translation that leads to an alphanumeric SIP URI to be sent as called party to a SIP-Q endpoint shall be treated as "Route not Available' by translation.

14.12.2.1 Call Processing - Invites from OS-SBC (Internet)

Dial-In Calls to SIP URI which are routed to OpenScape UC MCU are accepted.

14.12.2.2 URI Mapping Service

A new URI Mapping Service handles the mapping of SIP URIs Domains to numbers (preconfigured trunk access codes).

The mapping table is configurable via AMO CLIMA.

14.12.3 SIP URI format for video dial out

OpenScape 4000 must route the following SUP URI formats, which are used for video calls:

SIP URI format sip:<user>@<domain>

- The user part cannot be empty.
- The domain part can be:
  - FQDN
- Examples:

  4989700712345@unify.com

  Erika.Mustermann@polycom.com

The definition above is a reduced approach which includes the most common SIP URI formats (SIP URI Definition RFC 3261).

14.12.4 Configuration

Calls to a Domain will be routed to a specific trunk based on the configuration via AMO CLIMA.

With AMO CLIMA, a mapping table can be configured with a DOMAIN-NUMBER, where NUMBER represents a preconfigured trunk access code.

Considering CLIMA is now the priority lookup, anyone using DNS names must differentiate internal SIP functions from URI domain dialing.

AMO LDPLN

- For the new DOMAIN table, a DOMAIN NUMBERING PLAN has to be configured.
- The 790 numbering plan in the LCR pool 8 will be reserved for the DOMAIN table.

```
ADD-LDPLN:LCRADM,790,8,20,"DOMAIN PATTERN PLAN";
```

NOTICE: The 790 numbering plan in the LCR pool 8 is reserved for the DOMAIN table, therefore it must not be included by UPLOL in LDPLNS and LDPLN objects.

AMO CLIMA

- A new TABLE named DOMAIN has been added for domain mapping.
- The domain is mapped to a number which is a preconfigured trunk access code.
- The calls to a specific domain will be routed to the configured trunk according to the DOMAIN-NUMBER pair configured with AMO CLIMA.

```
ADD-CLIMA:DOMAIN,ATOS.NET,101;
// the Domain ATOS.NET will be routed to preconfigured trunk access code 101
   <ADD-CLIMA
TABLE = ?
```

```
TABLE           : TABLE TYPE
CHARACTERISTIC  : REQUIRED CONDITIONAL
POSS. VALUES    : DDI          DDI TABLE
                  CLI          CLI TABLE
                  DOMAIN       DOMAIN TABLE

TABLE = DOMAIN

DOMAIN = ?
DOMAIN          : DOMAIN; ALLOWED: 0..9,A-Z,A-Z,_,.,
CHARACTERISTIC  : REQUIRED
POSSIBLE VALUES : MAX. OF 63 POSITIONS

DOMAIN = ATOS.NET

NUMBER = ?
NUMBER          : TRUNK ACCESS CODE
CHARACTERISTIC  : REQUIRED
POSSIBLE VALUES : MAX. OF 22 POSITIONS
NUMBER = 101;
ADD-CLIMA:DOMAIN,ATOS.NET,101;
H500: AMO CLIMA STARTED
H04: DOMAIN HAS BEEN ADDED FOR DOMAINNO 6.

AMO-CLIMA-111 CLI MANIPULATION
ADD COMPLETED;



DIS-CLIMA:DOMAIN;
H500: AMO CLIMA STARTED
-------------------------------------------------------------------------
| DOMAIN TABLE                                                          |
-------------------------------------------------------------------------
| DOMAINNO : 1                                                          |
| DOMAIN   : ABA.COM                                                    |
| NUMBER   : 100                                                        |
-------------------------------------------------------------------------
| DOMAINNO : 6                                                          |
| DOMAIN   : ATOS.NET                                                   |
| NUMBER   : 101                                                        |
-------------------------------------------------------------------------
| DOMAINNO : 7                                                          |
| DOMAIN   : SIEMENS.COM                                                |
| NUMBER   : 102                                                        |
-------------------------------------------------------------------------

AMO-CLIMA-111 CLI MANIPULATION
DISPLAY COMPLETED
```

NOTICE: For more information regarding the configuration of SIP URI, please see *OpenScape Solution Set V10, OpenScape SIP URI Configuration Guide, Administrator Documentation*.

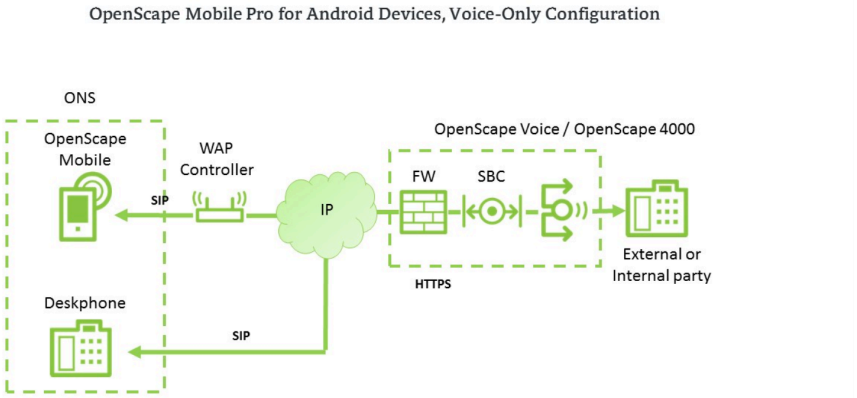
15 OpenScape Mobile Pro Client

15.1 Overview

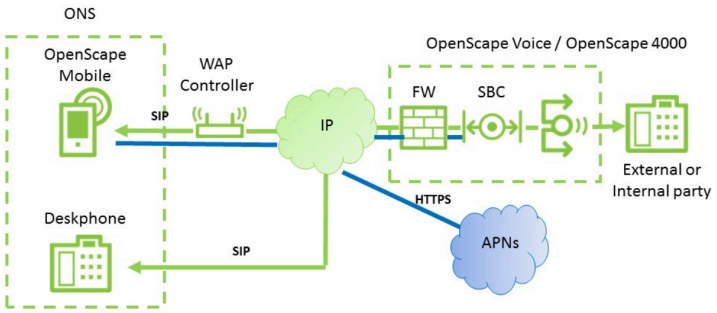
OpenScape 4000 V8R2 and higher support OSMO Pro only.

OSMO Pro at the OpenScape 4000 uses the same behavior like the OSV – the so called Auto Pilot Routing. It can be compared with a hunt group. As soon as the OSMO Pro is logged in the Auto Pilot Routing is activated. Incoming calls are routed always in this sequence: First the OSMO Pro rings and after a system-wide configured time (Default=15 sec) the call is routed to the Deskphone (Info: Feature can also be used without dedicated Deskphone). From then on the normal 4k call processing (No Answer Advance ANSADV / Rufweiterschaltung RWEITER) is executed. If the OSMO Pro client has a cell number configured and route call to cell is active in the OSMO Pro settings then an incoming call is routed to the cell number in case the client is logged off. Incoming calls to an OSMO Pro / Desk Phone combination will be signaled with a busy signal on the third caller in case of Voice-Only Mode (e.g. as long as auto-pilot routing finds a free device it will route the call to that device). In Combined Mode it is possible to set the Preferred Device to a dedicated device and then it will have busy-on-busy on the second call.

Voice-Only Configuration Example:

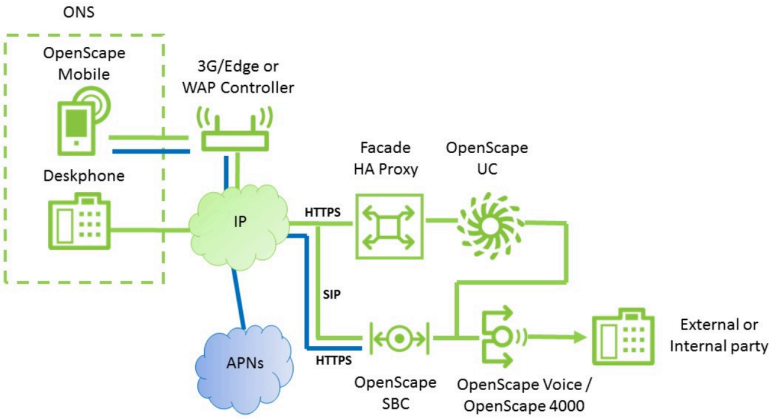


OpenScape Mobile Pro for Apple Devices, Voice-Only Configuration

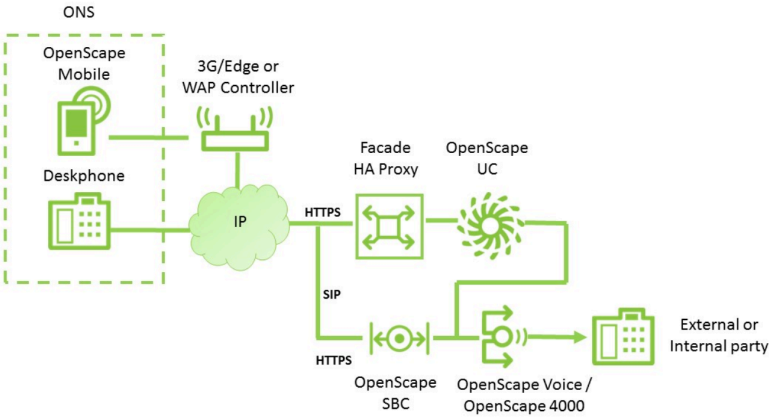


Combined-Mode (Integrated) Configuration example:

OpenScape Mobile Pro for Apple Devices, Integrated Configuration



OpenScape Mobile Pro for Android Devices, Integrated Configuration



For detailed description please refer to OpenScape Mobile Pro, Administrator Documentation.

NOTICE: Hand-over between the two topologies is not possible.

15.1.1 General Restrictions and Limitations

The following restrictions apply

- It is not supported that a user utilizes OMO Pro, Circuit-ATC, OSCC, C4B phone etc. in parallel.
- OSMO Pro is supported with STMIX/STMIY or SoftGate; classic STMI is not supported
- Video Calls are not supported by the OSMO Pro client.
- DMC is not supported for the OSMO Pro client.
- Emergency Release and Override are not supported for the OSMO Pro client.
- Answering calls from the OpenScape Mobile Pro Client is not possible in the following cases:
  - Recall on DESK phone
  - OpenScape Mobile Pro Client ONS is HG member: HG was called, call ringing at DESK phone

  Same restriction applies when call is in OpenScape Mobile Pro Client and OSMO Pro user chooses to answer from desk phone or alternative number using OpenScape Mobile Pro Client.
- Callback and Pick-Up group (with OpenScape Mobile Pro Client):
  - Callback to a client-desk configuration is executed only when this configuration is completely idle.Callback is not executed when OpenScape Mobile client calls a station which is member of the same pick-up group.
- Network Pick-Up group (OpenScape Mobile Pro Client):
  - Not supported
- CHESE group (Executive / Secretary):
  - Not supported
- Parallel ringing (Classic ONS group):
  - Not supported
- ACD / AGENT feature:
  - Not supported
- Personal Device group (Twinning):
  - Not supported – OpenScape Mobile Pro Client and twinning are mutual exclusive
- COM groups
  - Not supported
- SPS (Signaling and payload separation)
  - Not supported
- Speaker Call - One-Way
  - Not supported
- DSS key not supported with OpenScape Mobile Pro Client. Example: OpenScape 4000 subscriber has DSS key configured in AMO ZIEL with

number of the OpenScape Mobile Pro Client/Desk configuration as target. When OpenScape Mobile Pro Client has an incoming call in OpenScape Mobile Pro Client, then DSS key does not flash. The key starts flashing when the call is forwarded to the deskphone (after FWDDESK expiry).

- OpenScape Mobile Pro Client CA4000 Connectivity Adapter must not be shared with other applications which are not using full E164 Number formats.

15.1.1.1 OSMO Pro Combined Mode Restrictions

- The OS4K Assistant supports TLS1.2 only starting with UCV9R4.10. Please use TLS1.2 with fallback to TLS 1.0
- OSMO Pro in combined mode requires the calling party number to be sent in E164 international format. The KNFOR entry of the node hosting the OSMO Pro clients must have set TONIN to INTERPRE. In case international format is not wanted for non OSMO Pro devices a separate node id must be used for the OSMO Pro clients.
- If the work phone (desk phone) is set as preferred device and the work phone has call forwarding activated then an incoming call will not follow the call forwarding and ring the desk phone.
- Please check also the UC planing guide and the UC release note for general OSMO Pro combined mode restrictions.
- Seamless handover performed with OSMO application is not correctly handled by UC. Therefore, handover options in UC interface are not updated after move actions made in OSMO. Call control window is missing in UC when the calling party moves the call from OSMO to work phone (desk phone).

15.1.1.2 Notes for SIP device as OpenScape Mobile Pro Client Deskphone

1. DTMF on SIP is possible via CSTA_GENERATE_DIGITS_REQUEST

2. HOLD from OpenScape Mobile Pro Client when call is on the desk phone

SIP-UFIP as DESK feature: CSTA HOLD implemented for SIP-UFIP as DESK

1) CSTA HOLD is an exclusive RMX-CP feature (it is not a device feature)

- If CSTA HOLD is invoked, then only CSTA RETRIEVE is allowed to reconnect
- If SIP HOLD is invoked, then only SIP RETRIEVE is allowed to reconnect
- If CSTA HOLD is invoked, then SIP phone is not notified (device itself is not aware that its partner is in HOLD). In this case SIP phone, has HOLD option in phone menu, but if user selects this option it is rejected. The

same happens for NEW CALL and TRANSFER options which use HOLD as first step

3. RETRIEVE from OpenScape Mobile Pro Client when call is on the deskphone SIP-UFIP as DESK feature: CSTA RETRIEVE implemented for SIP-UFIP as DESK

- CSTA RETRIEVE is an exclusive RMX-CP feature (it is not a device feature)
- If CSTA HOLD is invoked, then only CSTA RETRIEVE is allowed to reconnect
- If SIP HOLD is invoked, then only SIP RETRIEVE is allowed to reconnect

4. Message waiting call back is not supported for SIP devices.

5. Move call to OOS UFIP deskphone Move call to desktop appears when OOS status of SIP-UFIP deskphone is not visible in the system (check AMO SDSU). The system relies on a mechanism implemented in the gateway which reports OOS status of SIP. This mechanism does not present this status in real time, therefore there are cases where the SIP phone is OOS but the systen is not aware of this.

IMPORTANT: Actions initiated from OpenScape Mobile Pro Client (via CSTA) should not be mixed with actions initiated from SIP-UFIP phone, or the other way around. It is recommended to use only OpenScape Mobile Pro Client actions (via CSTA) or only physical actions from SIP-UFIP phone.

15.1.2 Configuration

OpenScape Mobile Pro Clients must be configured in an OpenScape 4000 system as UFIP SIP device. There is one UFIP SIP device per OpenScape Mobile Pro Client user. This UFIP SIP device acts as a proxy for all of the user's OpenScape Mobile Pro Clients.The UFIP SIP is an auxiliary device therefore it's number is not presented on any phone display and known only by the system administrator.

OSMO Pro licenses are required to configure OSMO Pro clients. A OSMO Pro user needs one flexlicense for the deskphone and one OSMO Pro license for the clients. (if a user wants to run the client on multiple smartphones/tablets in parallel only one OSMO Pro license is needed).

Direct calls to UFIP SIP devices are not possible. The OpenScape Mobile Pro Clients are reachable with the user's OpenScape 4000 Deskphone number. The users Deskphone ONS number is linked to the auxiliary UFIP SIP device via AMO SBCSU (see below for configuration example).

"Regular" SIP endpoints and UFIP OpenScape Mobile Pro Clients can be configured in parallel on a gateway board.

NOTICE: Background architecture information of a OpenScape Mobile Pro Client registration process: the OpenScape Mobile Pro Client uses the ONS deskphone phone number for a dummy registration as soon as the OpenScape Mobile Pro Client logs in to its OpenScape Mobile Pro Client application. The data

needed to register the client with the gateway (auxiliary UFIP SIP phone number etc) are sent to the Client via CSTA over SIP. Once the Client has received all this data it registers as a SIP client with the GW . After successful registration the Client is in service.

NOTICE: For UFIP SIP Clients capabilities see Section , “SIP Subscriber”.

The Clients must also be linked to the user’s desktop phone via administration. (AMO SBCSU, parameter CLNTDESK).

The clients must be configured as OSMO Pro clients (AMO SBCSU parameter OSMO = YES)

For Mobile Pro clients the user’s mobile phone number can be assigned to the client as a configurable option (AMO ZIEL).

Additional parameters for OSMO Pro are configured with AMO ZANDE branch OSMO. These parameters are sent to the OSMO Pro client when the user logs on.

- SERVMAIL Email address for customer service
- OSVTLS Level of Certificate Security Check Gateway (0=no check, 1=check)
- SBCSTLS SBC Level of Certificate check (0=no check, 1=check)
- QOSVIDEO Quality of service for video (0..254)
- DSCPTOS enable/disable DSCPTOS (yes, no)
- WMM enable/disable wireless multi media (yes, no)
- SECOSV Media security mode gateway (rtp, srtp, best effort)
- SECOSBC Media security mode SBC (rtp, srtp, best effort)
- FEATLIST OSMO Pro feature list. Please use Parameter ALL to set all of them. In case there are problems with certain features like the MOVE Button then delete feature SST from the list and the MOVE button is greyed out.
  - Call Forwarding CF
  - Single Step Transfer SST
  - TransferONHold TOH
  - HandoverFrom HF
  - Sip Over Data Connection SIP
  - Seamless Handover SEHO
  - Extended Alerting XA
  - Consultation Call CSC
  - Snooze DnD SDND
- VCPRIO1 preferred Video Codec (VP8 or H264)
- VCPRIO2 alternative Video Codec (VP8 or H264)
- SBCFQDN1-5 SBC Fully qualified domain name
- SBCADDR1-5 SBC IP address
- PORT1-5 SBC PORT

15.1.3 Configuration Example

15.1.3.1 Configuration on OpenScape 4000

The OpenScape Mobile Pro clients connect to OpenScape 4000 via SoftGate (vHG-SIP) or STMIX/STMIY. Besides the regular SoftGate/STMIX/STMIY configuration, vHG/SG – CICA (application hosted by CSTA) link has to be considered.

The CSTA/CICA IP address is delivered to the SoftGate/STMIX/STMIY via board data (AMO-SIPCO).

NOTICE: A valid KNDEF entry is mandatory with defined CC, AC and LC for E164 UFIP registration to OpenScape Mobile Pro Client. For countries not using KNDEF codes, a KNDEF KNOWNET entry must be created instead and linked with AMO SDAT to OpenScape Mobile Pro Client devices.

When changing KNDEF, following steps must be executed:

1. Configure all existing OpenScape Mobile Pro Clients with the new E164 numbers.

2. Change KNDEF.

3. Restart all gateways used for OpenScape Mobile Pro Client connectivity.

CSTA configuration

CICA in CSTA can be seen as an own application.

By default it uses port 1040 to connect to the CA4000_default.

The used port/CA4000 must have “E164 number format” support and “ONS monitoring” enabled.

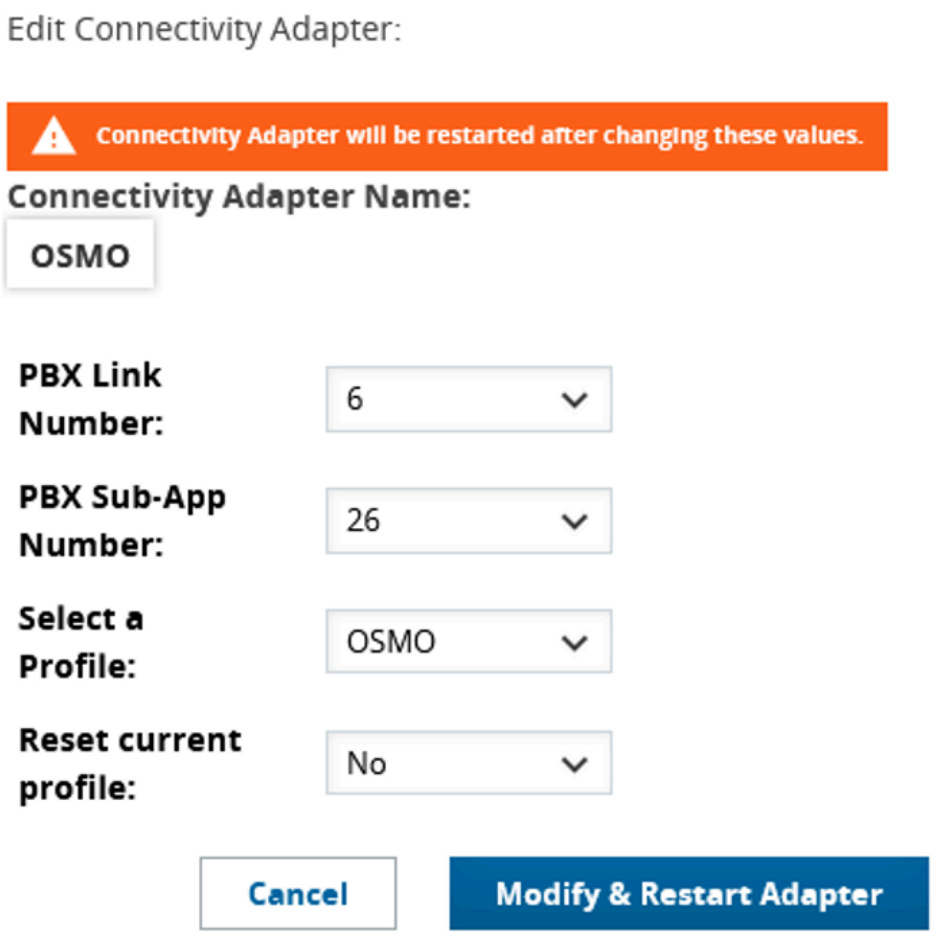


Figure 344: CA4000 Default Configuration

CICA application has to be configured with the correct port number and then started by checking the option “Auto start” and clicking “Start”:

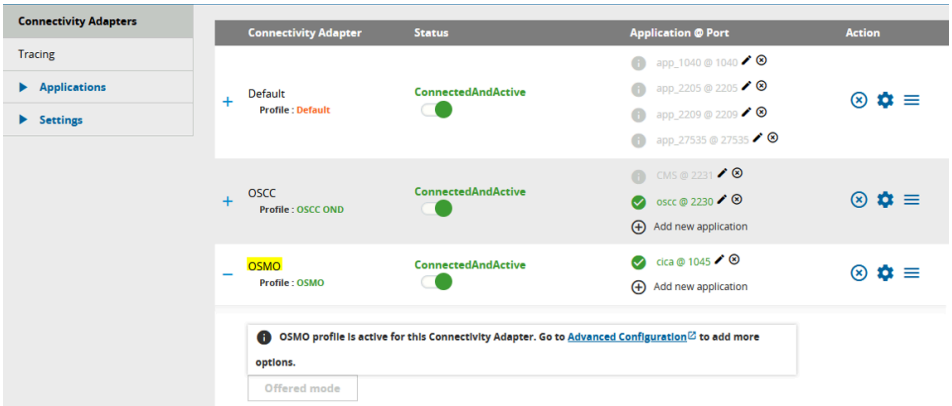


Figure 345: CICA Configuration

If needed, the default configuration can be changed: a new/different port/ application can be configured.

After configuring the NGS IP address and confirming that CSTA CICA application is started with the correct configuration, its status can be checked in the WBM of the vHG (SIP) board. The vHG where the OpenScape Mobile Pro

Clients will register to the OpenScape 4000) must show under the tab “CICA Connection Status” the status “Registration at CICA successful”:

The default configuration should look like in the following figure:

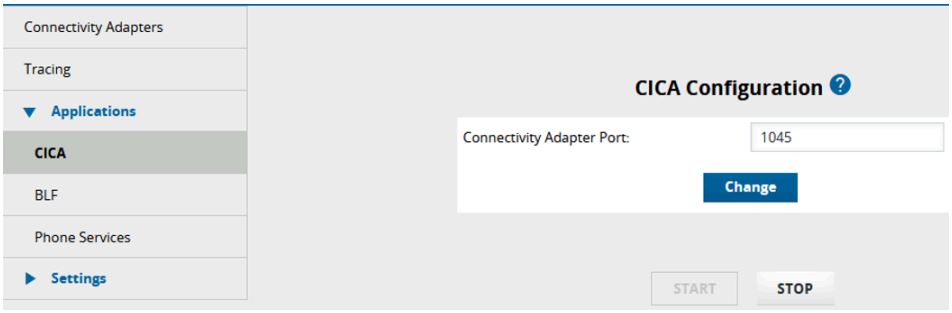


Figure 346: vHG WBM CICA Status Page

User Configuration in OpenScape 4000

Each OpenScape Mobile Pro Client will register in the OpenScape 4000 as an UFIP SIP device. The client must be linked to an actual desktop phone via parameter CLNTDESK and marked as OSMO Pro client via Parameter OSMO=YES

```
ADD-SBCSU:STNO=<UFIP_STN>,OPT=OPTI,CONN=IP2,PEN=<X-Y-Z-T>,DVCFIG=UFIP,
 CLNTDESK=<DSKTP_PHN_STN>,OSMO=YES
```

It is not necessary that the desktop phone is in service. If the desktop phone is out of service, logged off, or if there is no phone HW connected at all then autopilot routing skips the routing step to the deskphone. Desk Phones must require a Port Equipment Number (PEN aka. LAGE) and therefore TDM Phones cannot be used in Signed–Off state.

Correct linkage can be checked:

DIS-SBCSU for UFIP STN will show:

DESK=<DSKTP_PHN_STN>

DIS-SBCSU for Desktop Phone STN will show:

CLIENT=<UFIP_STN>

Parameters CLNTDESK and OSMO cannot be changed via CHANGE-SBCSU. In order to change them , the UFIP SIP client has to be deleted and reconfigured with the new CLNTDESK /OSMO value. The OSMO Pro UFIP SIP client consumes one OSMO license.

OSMO Pro combined mode only:

- The node hosting the OSMO Pro UFIP SIP devices must have KNFOR parameter TONIN set to INTERPRE.

After configuration of the SBCSU linkage between Deskphone and Client the configuration can be verified on the SIP HG WBM under Configuration -> Voice Gateway -> Clients -> UFIP SIP (Figure 7). Further it can be verified if everything is correctly configured and the linkage fits to the ONS number which will be used for client registration. Also after a successful registration the entry will be displayed in bold font.

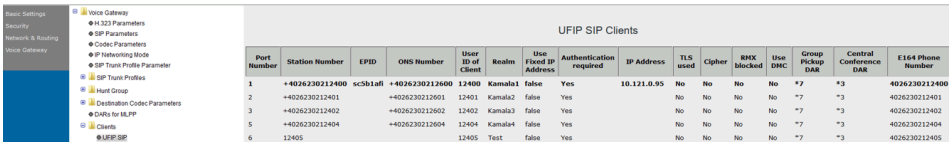


Figure 347: Client Configuration

Timer Configuration

The timers control the Routing steps of Autopilot Routing for OSMO users. Routing steps are: OSMO Client, deskphone and eventualy Voicemail (if configured).

The Client rings until FWDDESK timer expires. The call is moved from OpenScape Mobile Pro Client to deskphone and another timer FWDVM is started. The incoming call is still signaled at the Client. FWDDESK timer is configurable with the following AMO command:
`CHANGE-CTIME:TYPESWU=CP2,FWDDESK=xx;`

Upon expiry of FWDVM forward to Voice Mail the call is forwarded to the deskphones No Answer Destination (Voicemail for many users). FWDVM timer is configurable with the following AMO command:
`CHANGE-CTIME:TYPESWU=CP2,FWDVM=xx;`

The timers listed above can also be administered per user with AMO ACTDA (VARRING)

Call reach cellular number only if user meets the following 3 conditions:

1) OSMO client has configured the cell number
2) "Route calls To Cell" is enabled
3) OSMO client is signed out (not registered)

In this case routing will be deskphone then cell (and voicemail if configured)

ZANDE:OSMO Configuration

Additional parameters like SBC address etc are configured with AMO ZANDE branch OSMO.

```
CHANGE-ZANDE:TYPE=OSMO,SERVMAIL=”helpdesp@unify.com”,OSVTLS=0,
SBCTLS=0,QOSVIDEO=0,DSCPTOS=NO,WMM=YES,SECOSV=BESTEFRT,SECOSBC=BESTEFRT;
CHANGE-ZANDE:TYPE=OSMO,FEATLIST=ALL; /* ALL sets all available features */
CHANGE-ZANDE:TYPE=OSMO,VCPRIO1=H264,VCPRIO2=VP8;
CHANGE-ZANDE:TYPE=OSMO,SBCFQDN1=”os4kosmo.unify.com”,SBCADDR1=0,0,0,0,PORT1=0,
SBCADDR2=210.1.234.56,PORT2=65061;
CHANGE-ZANDE:TYPE=OSMO,SBCADDR3=192.168.0.55,PORT3=5061;
```

Enter 0.0.0.0 to delete a SBC IP address from ZANDE:OSMO.

In the example above the FQDN “os4kosmo.unify.com” represents a hostname which resolves into a Public IP e.g.. 210.1.234.56 of the OpenScape SBC (Public Internet Access Side). The other IP addresses are examples of local WIFI IP addresses, which can be configured additionally at the Access Side of the OpenScape SBC, e.g. Non-VLAN IP. Depending on the customer setup this may look totally different, e.g OpenScape SBC behind a NAT Router where the Access Side has an internal IP and the OpenScape SBC utilizes his “External Firewall IP” field.

Please refer to the OpenScape SBC Service Documents for all available setup options.

Requirements

- OpenScape Mobile Pro UFIP-SIP subscribers must be configured on SoftGate vHG or STMIX boards with SIP functionality (BFDAT)
- The desktop phone must be a TDM, HFA or UFIP SIP device. Analog devices are not supported.

15.1.3.2 CICA Connectivity to OS4K

The CSTA protocol used by OpenScape Mobile Pro Client is a plaintext protocol that does not support encryption. The Integrated VPN feature is a security enhancement, which creates a Virtual Private Network to encrypt network traffic and provides connectivity between remote components of an OpenScape 4000 (OS4K) system.

NOTICE: For detailed information how to setup the Integrated VPN service, please refer to OpenScape 4000 V8 - Platform Administration (Portal), Administrator Documentation, chapter Integrated VPN Service.

If enabled this feature will set-up a VPN network between OS4K Host system and SoftGates, which encrypts any traffic between the vHG boards and CSTA. This includes the CICA connectivity traffic.

If the Integrated VPN feature setup fails, the CICA traffic is routed via IPDA LAN directly (in plaintext).

15.1.3.3 OpenScape Mobile Pro Client Configuration

In OpenScape Mobile Pro application go to Settings > Account and add the required parameters:

Voice only mode

Subscriber number: <The ONS number of the 4K Deskphone e. g. +4989700731000 >

Server address: <IP/Host address of OS-SBC:port > (Default port is TLS port 5061) or <FQDN of the OS-SBC>

Password: <SBCSU password from UFIP configuration>

Mobile number: <e. g. +4916098947000>

Combined mode

Subscriber number: <UC user e.g 3100@system>

Server address: <HTTPS://IP/Host address of Facade sever:port> (Default Port is 8443)

Password: <UC password>

Mobile number: <e.g +4916098947000>

For detailed configuration please refer to the OpenScape Mobile Pro application Service Documentation: **OpenScape Mobile Pro User Guide**.

15.1.3.4 OpenScape SBC Configuration Example

OpenScape SBC usage is mandatory

Feature Remote Subscriber in OpenScape SBC must be enabled and used to register the OSMO Pro Clients through the OpenScape SBC to the OS4K Gateway which hosts the UFIP proxy devices. For detailed configuration of OpenScape SBC please refer to the OpenScape SBC Configuration Guide.

For detailed configuration of the connection to the Apple push notification server please refer to the OpenScape Mobile Pro administrator documentation.

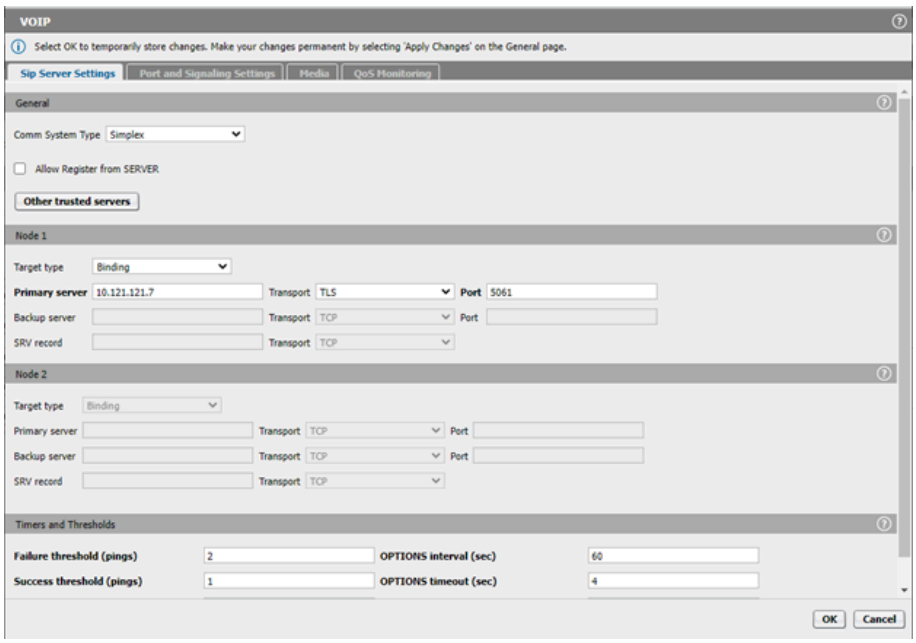
Following a brief example of an OpenScape SBC configuration for OSMO Pro:

VoIP

Sip Server Settings

4K Gateway's (SIP Subscriber Gateway > SoftGate/STMIX/STMIY e.g.10.121.121.7) are configured via TCP on 5060 or TLS on 5061 (for secure connection between OS-SBC and 4K) in two modes:

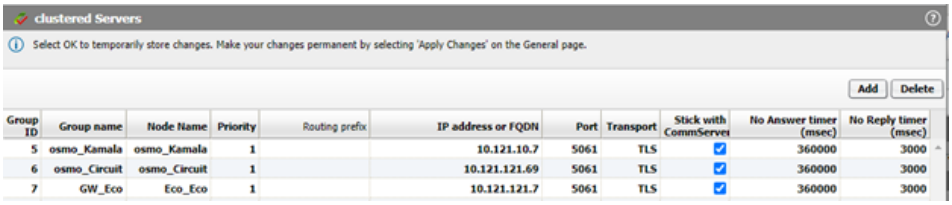
1) **Simplex mode** (one single 4K GW is used):



2) **Clustered Mode** (more 4K GW's are configured on the same OS-SBC => more than 240 OSMO users):

Switch from Simplex mode to Clustered mode and add the OS4K Gateways with "Priority 1".

Go to **VoIP> Sip Server Settings>Comm System Type** and choose **Clustered**.



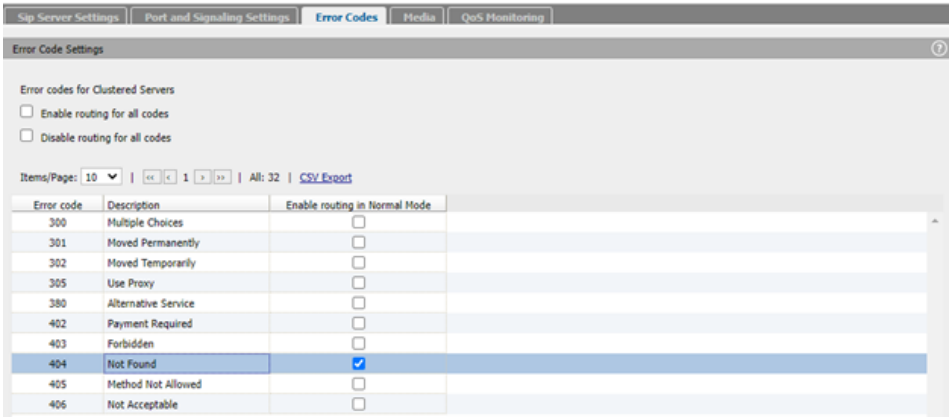
Next, add the Clustered servers.

IMPORTANT: Stick with CommServer must be checked! This is a dedicated setting for OSMO-OS4K and SBC.

Enable error code for 404 (SBC will reroute a message if it receives a 404 Not Found)

At first, OSMO client registration SBC will send the REGISTER message to each GW until it will receive a positive answer (100 Trying/200 OK), from the other GWs it will receive a 404 Not Found.

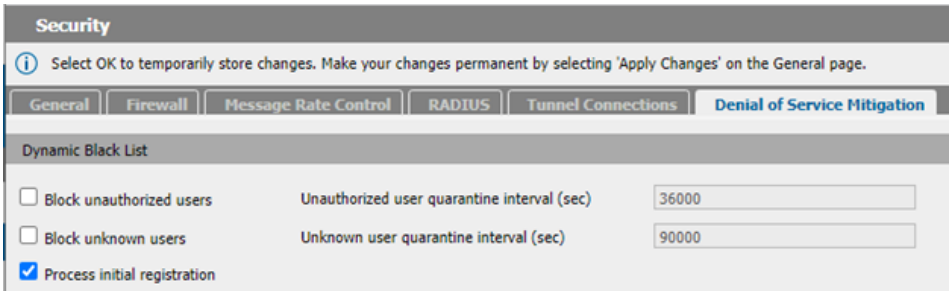
Go to **VoIP**>**Error Codes** and select the checkbox **Enable routing for error codes** for the 404 error code.



NOTICE: All error codes can be enabled for rerouting simultaneously by selecting **Enable routing for all codes**.

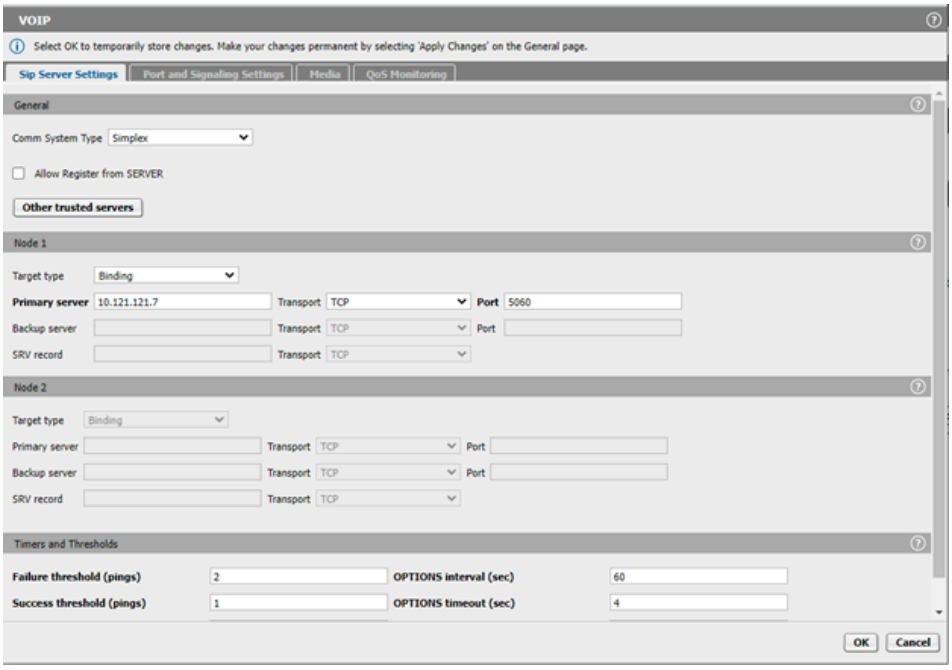
Enable **Process initial registration** flag in order to facilitate the registration process (otherwise OSMO registration process will take more than 50 seconds).

Go to **Security**> **Denial of Service** and select the checkbox **Process initial registration** to enable it.

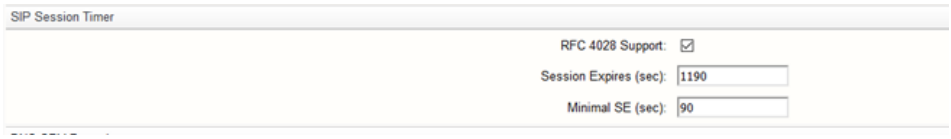


Port and Signaling Settings

Per default the OS-SBC uses for payload (e. g. voice) a UDP port range configured with “Media Independent RTP Ports”. In this example these ports were reduced from “Port min” 35500 to “Port max” 35600:



TCP Connection Lifetime must have a value greater than Session refresh timer in the 4K-GW (SIP Session Timer Session Expires (sec)). For example, set SBC TCP connection lifetime to maximum allowed (**1200 s**) and the 4K GW one to **1190 s.**



Media

OSMO media mode

Possible configurations:

OS4K (AMO ZANDE:OSMO)	...	**OS-SBC**
RTP	>	RTP Only
SRTP	>	SRTP Only **or** Best Effort SRTP
BESTEFRT	>	SRTP Only **or** Best Effort SRTP

For **RTP** configured in ZANDE:OSMO, this changes must be done:

```
DISP-ZANDE:OSMO;
H500:  AMO ZANDE STARTED
   SERVMAIL  = test@unify.net
   OSVTLS    = 0
   SBCSTLS   = 0
   QOSVIDEO  = 0
   DSCPTOS   = NO
   WMM       = YES
   SECOSV    = RTP
   SECOSBC   = RTP
   FEATLIST  = CF&SST&TOH&HF&SIP&SEHO&XA&SDND&CSC&FC1&GPC
   +----------------------------------------+
   |     VIDEO CODEC LIST                   |
   +----------------------------------------+
   | PRIO1 :  CODEC = H264                  |
   | PRIO2 :  CODEC = VP8                   |
   +----------------------------------------+

 +-------------------------------------------------------------------
+
   |                         LIST OF IP ADDRESSES OR FULLY
                    |
   |                      QUALIFIED DOMAN NAMES FOR SBC
 GATEWAYS                  |

 +-------------------------------------------------------------------
+
   |SBCADDR1 = x.x.x.x.       PORT1 = 5061
    |
   |SBCADDR2 = x.x.x.x        PORT2 = 5061
    |
   |SBCFQDN3 =
                    |
   |SBCFQDN4 =
                    |
   |SBCFQDN5 =
                    |

 +-------------------------------------------------------------------
+

AMO-ZANDE-111       SYSTEM DATA - EXTENDED
DISPLAY COMPLETED;
```

For SRTP or BestEffort SRTP configured in ZANDE:OSMO, this changes must be done:

SRTP:

```
DISP-ZANDE:OSMO;
H500:  AMO ZANDE STARTED
   SERVMAIL  = test@unify.net
   OSVTLS    = 0
   SBCSTLS   = 0
   QOSVIDEO  = 0
   DSCPTOS   = NO
   WMM       = YES
   SECOSV    = SRTP
   SECOSBC   = SRTP
   FEATLIST  = CF&SST&TOH&HF&SIP&SEHO&XA&SDND&CSC&FC1&GPC
   +----------------------------------------+
   |     VIDEO CODEC LIST                   |
   +----------------------------------------+
   | PRIO1 :  CODEC = H264                  |
   | PRIO2 :  CODEC = VP8                   |
   +----------------------------------------+

 +-------------------------------------------------------------------
+
   |                         LIST OF IP ADDRESSES OR FULLY
                    |
   |                      QUALIFIED DOMAN NAMES FOR SBC
 GATEWAYS                  |

 +-------------------------------------------------------------------
+
   |SBCADDR1 = x.x.x.x.       PORT1 = 5061
    |
   |SBCADDR2 = x.x.x.x        PORT2 = 5061
    |
   |SBCFQDN3 =
                    |
   |SBCFQDN4 =
                    |
   |SBCFQDN5 =
                    |

 +-------------------------------------------------------------------
+

AMO-ZANDE-111       SYSTEM DATA - EXTENDED
DISPLAY COMPLETED;
```

Best Effort SRTP:

```
DISP-ZANDE:OSMO;
H500:  AMO ZANDE STARTED
   SERVMAIL  = test@unify.net
   OSVTLS    = 0
   SBCSTLS   = 0
   QOSVIDEO  = 0
   DSCPTOS   = NO
   WMM       = YES
   SECOSV    = BESTEFRT
   SECOSBC   = BESTEFRT
   FEATLIST  = CF&SST&TOH&HF&SIP&SEHO&XA&SDND&CSC&FC1&GPC
   +----------------------------------------+
   |     VIDEO CODEC LIST                   |
   +----------------------------------------+
   | PRIO1 :  CODEC = H264                 |
   | PRIO2 :  CODEC = VP8                   |
   +----------------------------------------+

 +-------------------------------------------------------------------
+
   |                         LIST OF IP ADDRESSES OR FULLY
                    |
   |                      QUALIFIED DOMAN NAMES FOR SBC
 GATEWAYS                  |

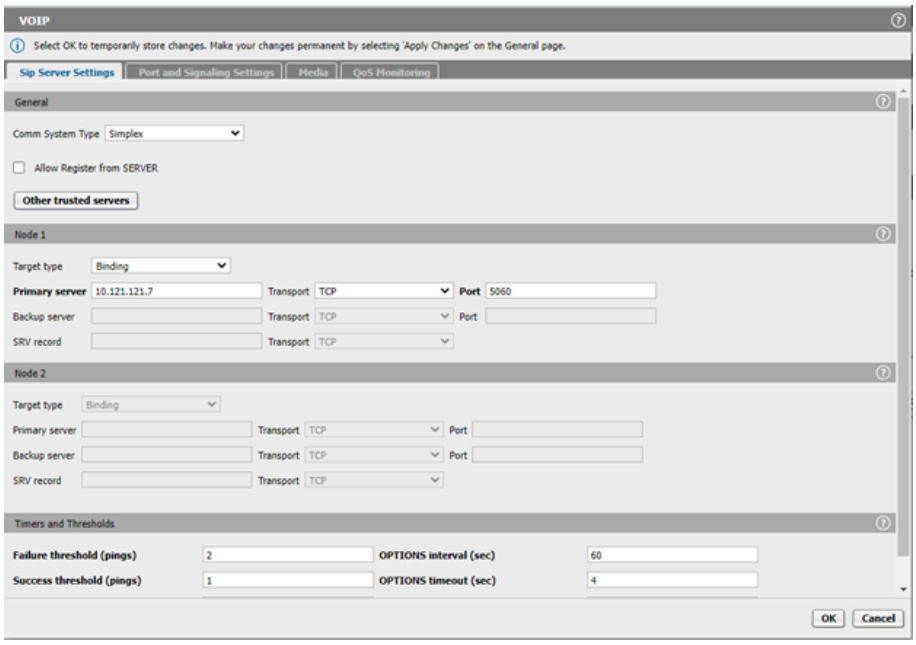
 +-------------------------------------------------------------------
+
   |SBCADDR1 = x.x.x.x.       PORT1 = 5061
    |
   |SBCADDR2 = x.x.x.x        PORT2 = 5061
    |
   |SBCFQDN3 =
                    |
   |SBCFQDN4 =
                    |
   |SBCFQDN5 =
                    |

 +-------------------------------------------------------------------
+

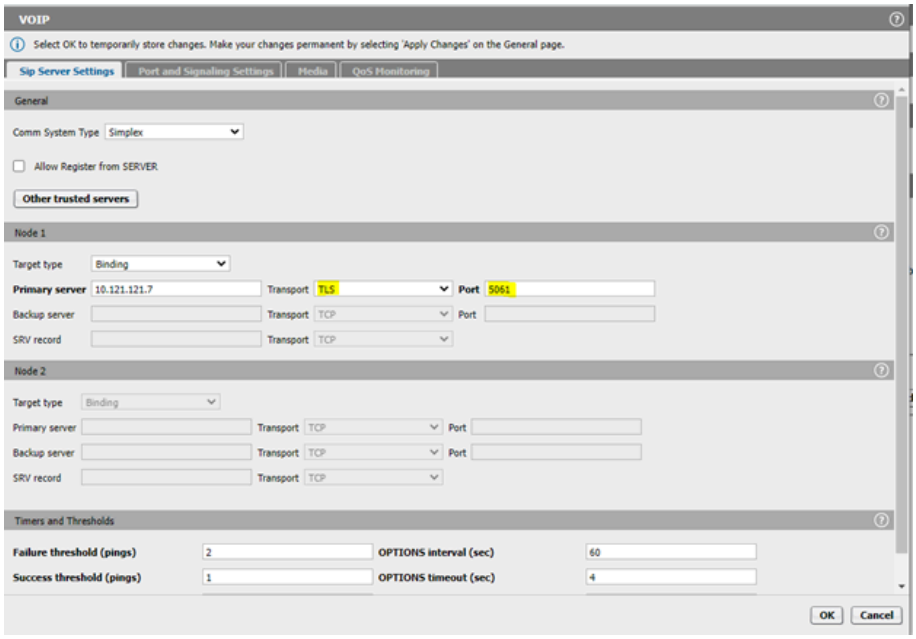
AMO-ZANDE-111       SYSTEM DATA - EXTENDED
DISPLAY COMPLETED;
```

1) In case **TLS** together with **SRTP** or **Best Effort SRTP** towards the 4K wants to be used, then first **SPE (Signalling and Payload Encryption)** must be activated on 4K side (SPE must not be activated for **TCP** and usage of **RTP**)

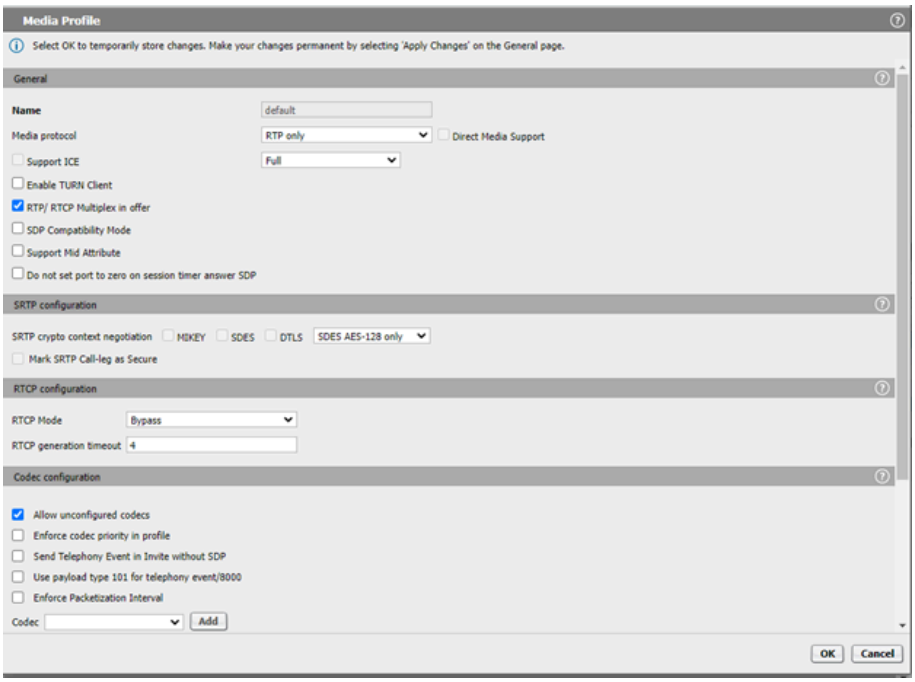
2) OS-SBC: VoIP > Sip Server Settings, switch Transport for 4K GW as: over TCP and 5060 if **RTP** is used



over TLS and 5061 if **SRTP** or **Best Effort SRTP** is used:

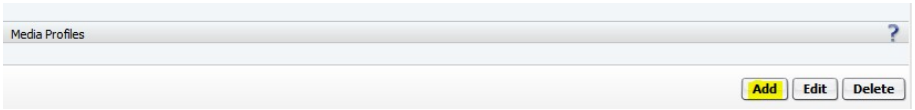


3) Dedicated Media profiles need to be created for OSMO:

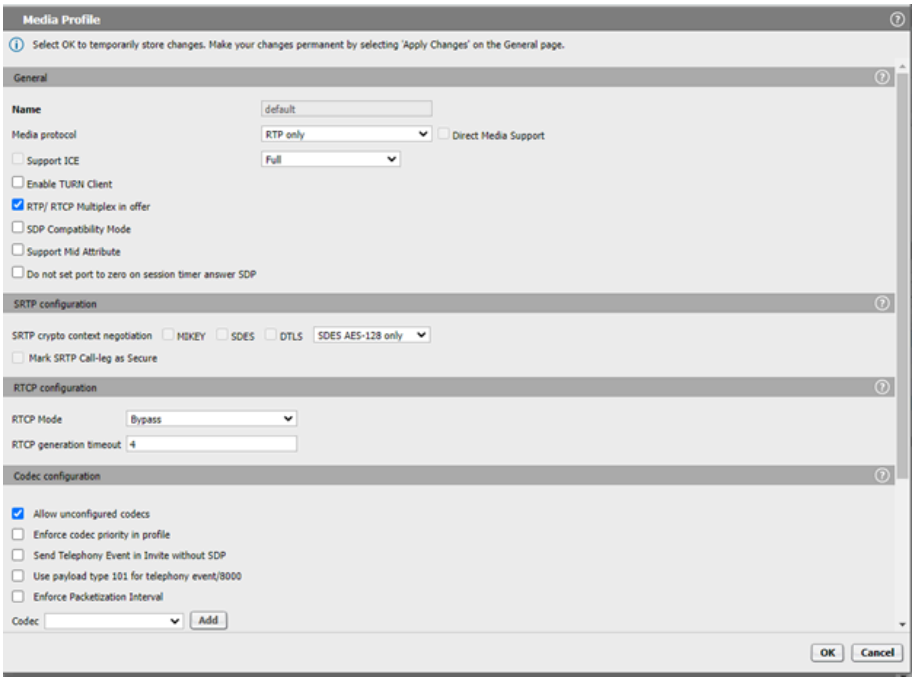


VoIP > Media > Add new **Media Profile:**

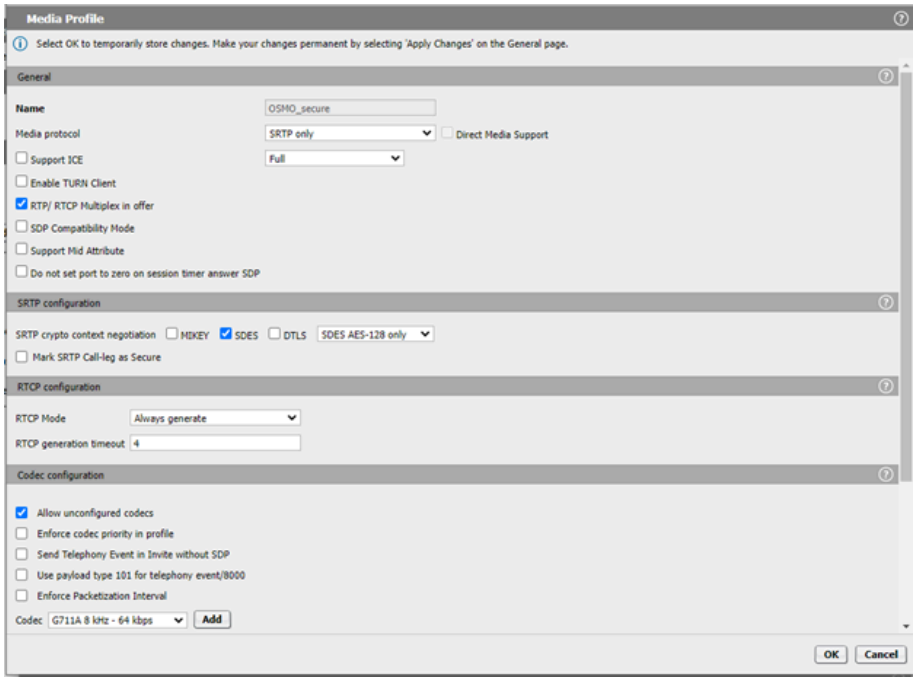
RTP:

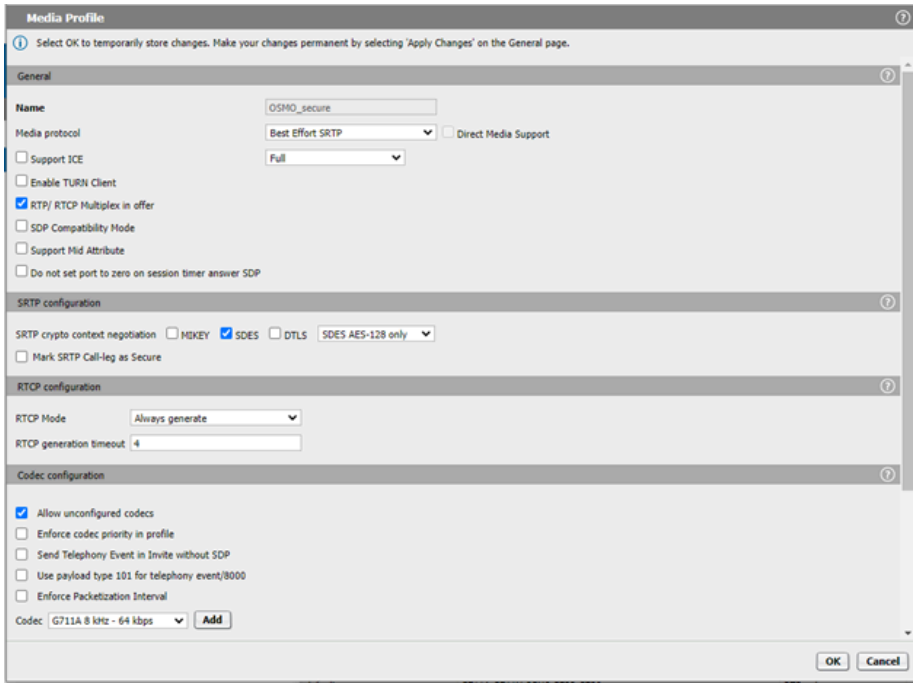


SRTP (Use only with SDES):

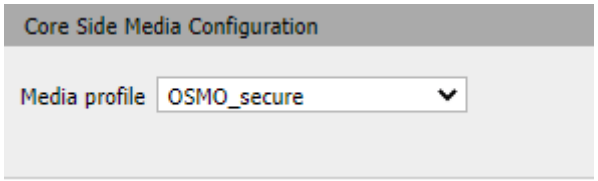


Best Effort SRTP (Use only with SDES)





4) Then select the needed profile as “Core Side Media Configuration” accordant with your configuration (RTP, SRTP or BEST Effort SRTP)



Keep in mind that you need to save all the time the configuration, don’t forget to Apply Changes (on the main page):



5) Go to Features > and enable Enable Remote Subscribers

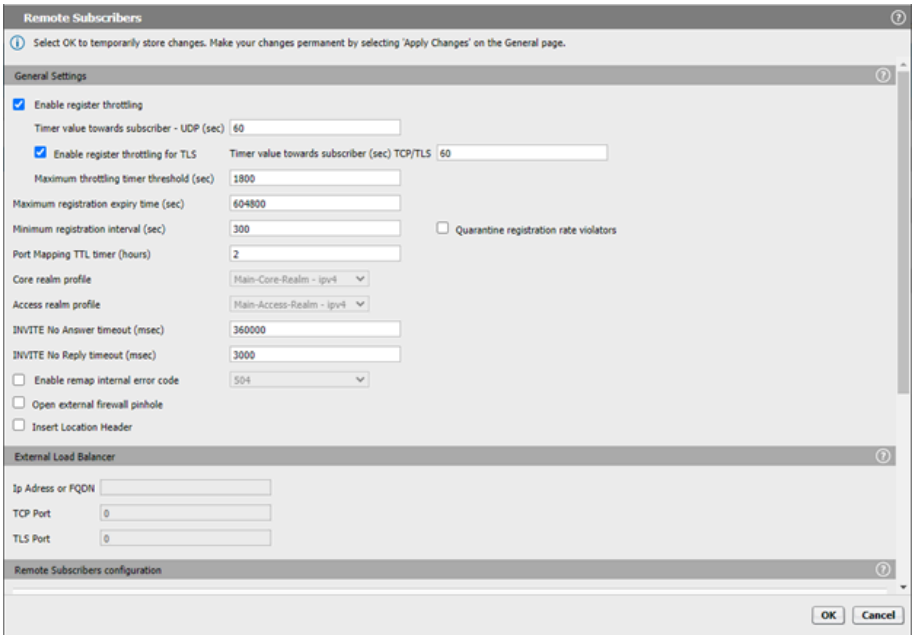


Next steps (6,7,8) are just for SRTP or Best Effort SRTP, if RTP is used, then ignore steps 6,7,8.

6) Press Configure:



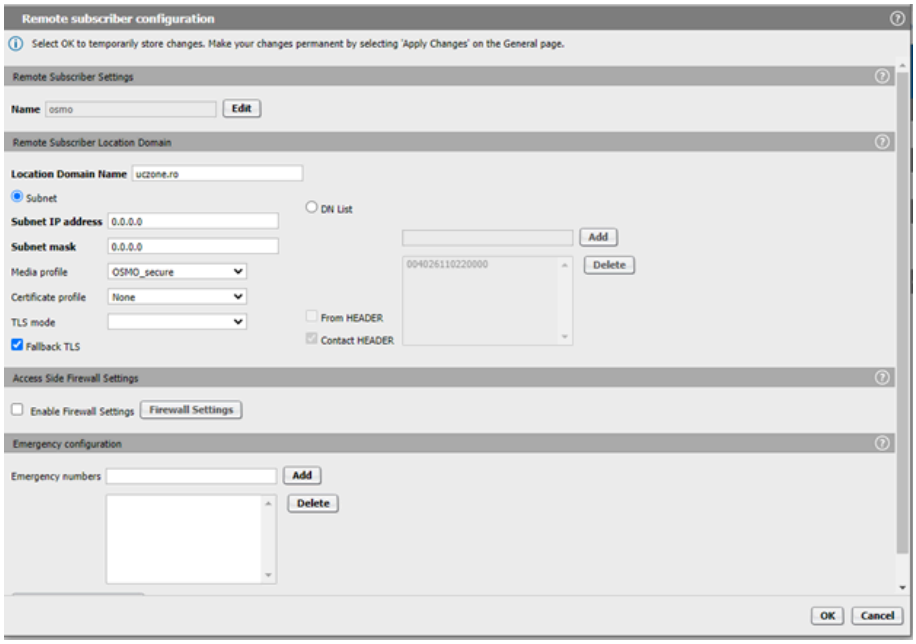
7) Configure parameters as described below:



8) Add new Remote Subscribers configuration



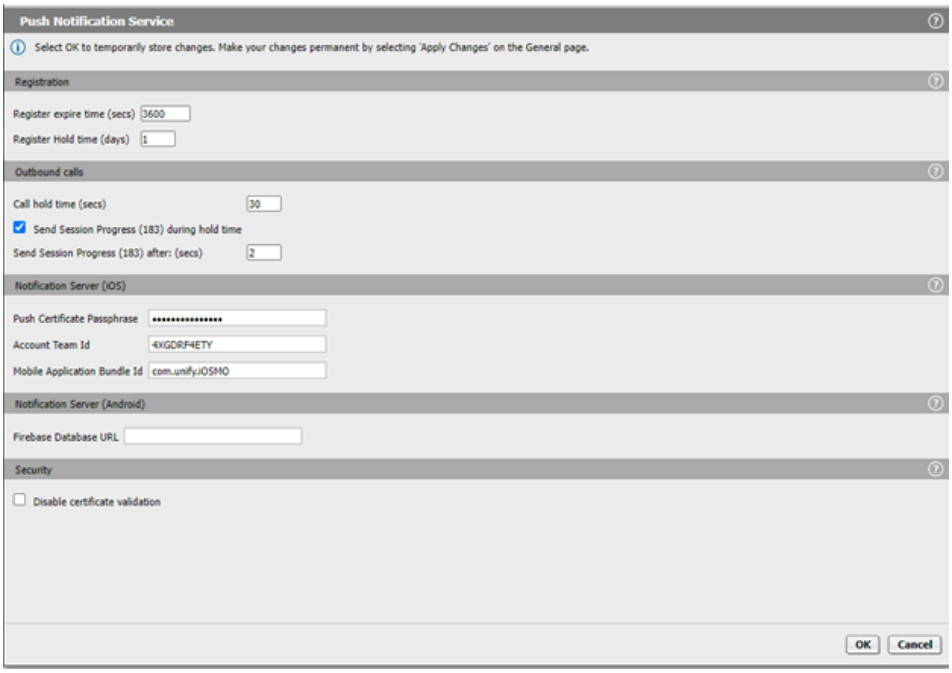
Add as Media profile the one used at step 4:



OpenScape Mobile Pro iOS is using APN's (Apple Push Notification), it needs to be activated in OS-SBC:

Features > and enable Enable Push Notification Service

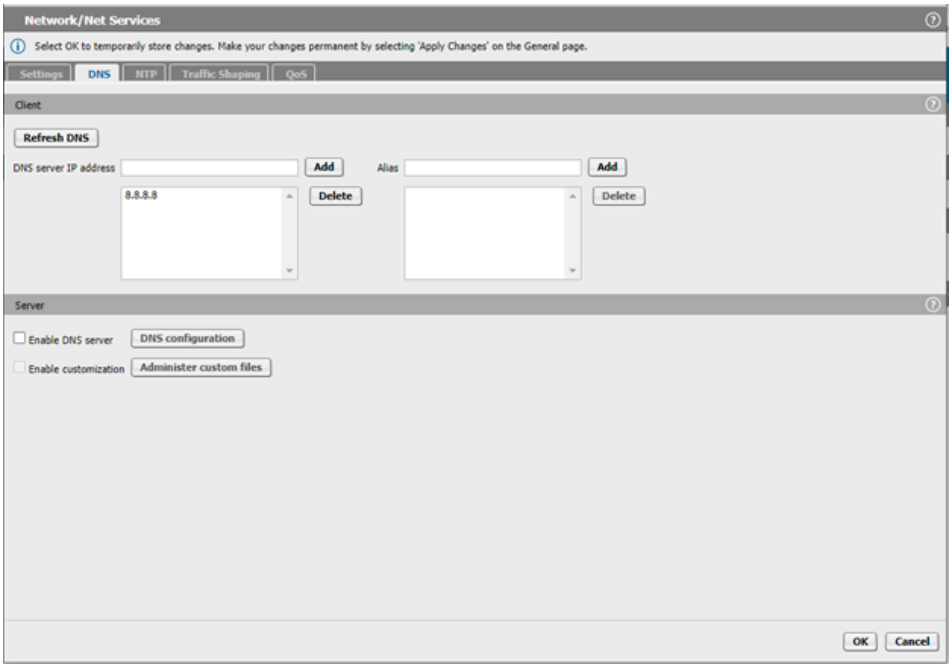




If the configuration of the Notification Server e. g. Push Certificate Passphrase, Account Team Id or Mobile Application Bundle Id is not set, then please refer to the OpenScape Mobile Pro Administration Documentation.

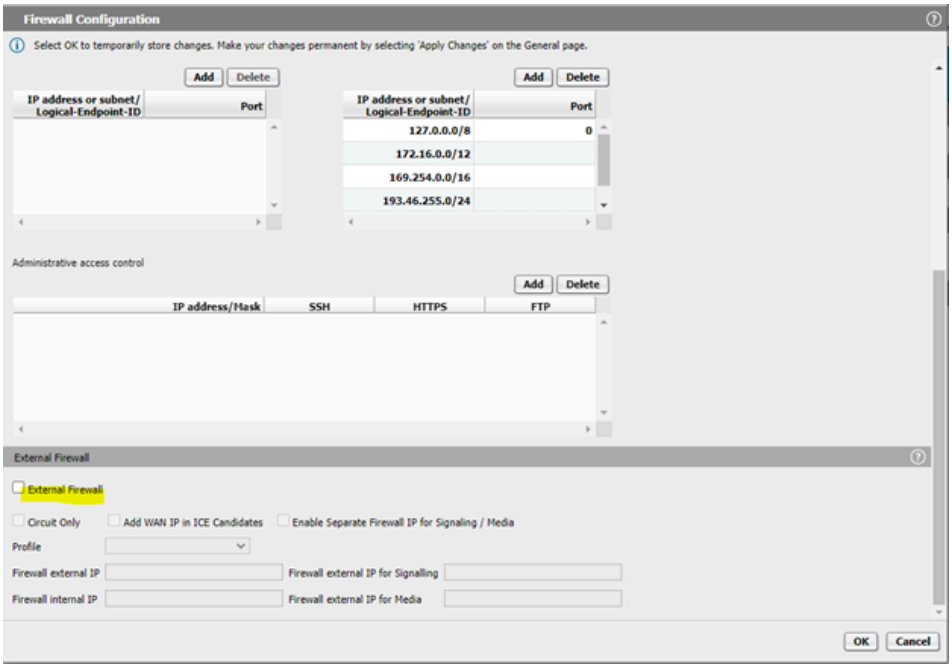
Network/Net Services > DNS

The OS-SBC needs to resolve the hostname of the Apple Push Notification Service, therefore he needs a connection a DNS server, e. g.



Security > Firewall

In case the Access Side of the OS-SBC is located in NAT behind an external Firewall, then please configure the External Firewall IP address accordingly:



15.1.3.4.1 OpenScape SBC Redundancy Mode

Please see OpenScape SBC V10 Configuration Guide, chapter 3.4.3.9.3OS-SBC -Collocated Redundancy.

The only specific configuration that needs to be done for OpenScape 4000 - SBC connection is to change the SBC public IP in AMO ZANDE:OSMO. Here needs to be the **Virtual WAN IP** (configured above).

15.1.3.5 Facade and UC configuration

Please see UC documentation for installation and configuration

OpenScape UC Application V9, Installation and Upgrade, Installation Guide

OpenScape UC Application V9 Configuration and Administration Guide

16 Unify Phone Connectivity

16.1 Overview

Unify Phone is a telephony connector for Unify Video. It acts as a bridge between OpenScape 4000 and Unify Video, enabling users to make and receive phone calls on their business phone number using the Unify Phone clients.

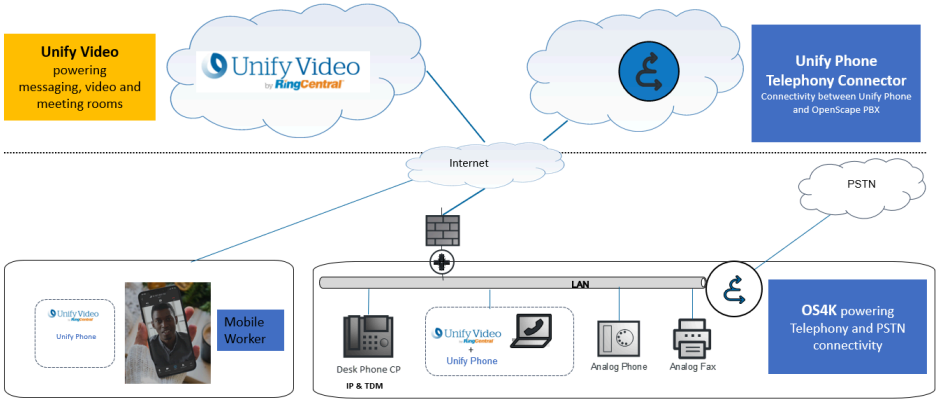


Figure 348: Unify Phone Overview

16.1.1 Features

Unify Phone supports the following features:

- Make call
- Answer, decline or drop a call
- Send DTMF commands in a call
- Hold and retrieve
- Mute/ Unmute
- Transfer call
- Pull call from other Unify Phone clients, desk phone or alternative device
- Push call to desk phone or alternative device, in case an alternative device is configured
- Make or answer a second call
- Swap calls (alternate)
- Merge two calls into a conference
- Call forwarding
- Alternative number (One Number Service)
- Call routing
- Voicemail
- Cross-launch from Unify Video
- Pickup Group (supported only for web clients)

16.1.2 Architecture

Each Unify Phone user must be configured in an OpenScape 4000 system as UFIP SIP device. This client device requires a Unify Phone license but it will not use a Flex license (similar to OSMO). Nevertheless, the desk device of a Unify Phone user requires a Flex license even if the desk phone does not exist physical. The UFIP SIP is an auxiliary device, therefore, direct calls are not possible and its number will not be presented on any phone displays. The Unify Phone clients are reachable over the user's OpenScape 4000 desk phone number. However the physical desk phone is not mandatory, it can be out of service or unplugged but the Signed–Off stations are not supported as desk phones.

The OpenScape 4000 Assistant will synchronize the user data with the Unify Phone Telephony Connector. Therefore, the Assistant must be able to access the Telephony Connector via the Internet (either directly or via HTTPS proxy). The OpenScape 4000 Assistant will retrieve all Unify Phone users which are configured in Unify Video from the Telephony Connector. When the Assistant finds a matching Unify Phone configuration for a user (based on the email address), it will upload the needed connection data to the Unify Phone Connector.

Unify Phone Web and Mobile clients are connected to OpenScape 4000 via SBC. The cluster mode allows to distribute the UFIP SIP devices over several Gateways (GWY) on SoftGates or STMIX/STMIY. Unify Phone Clients can make direct calls to all other OpenScape 4000 stations, external calls (via trunks) and vice versa. Multiple registrations for the same Unify Phone user are possible. All registered Unify Phone Clients and the desk phones will be alerted for incoming calls simultaneously if the Unify Phone user has configured "Default routing". If a second call is signaled or receives busy, the routing depends on the "Busy settings" of the Unify Phone user.

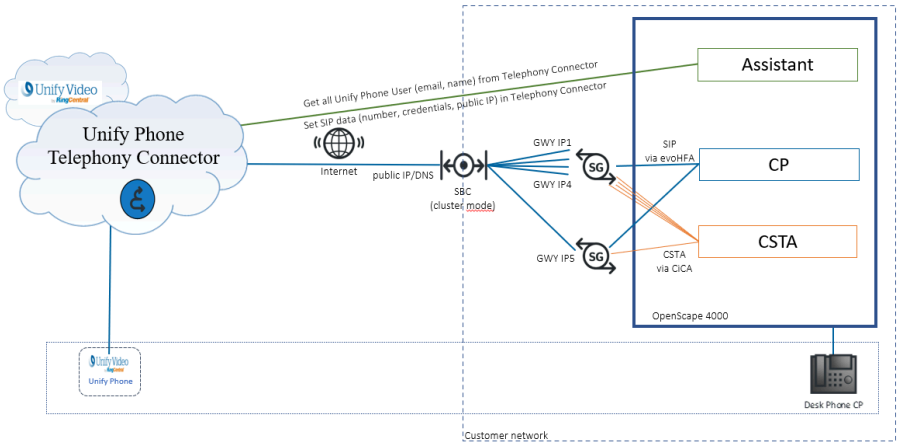


Figure 349: Unify Phone Architecture

16.2 Feature interaction and restrictions

The auxiliary devices for Unify Phone (e.g. OSMO) must be configured on a SoftGate or STMIX/STMIY (STMI2/STMI4 are not supported). The auxiliary device is linked to a desk phone which defines the E.164 number of the Unify Phone user.

The TDM, HFA, DECT (classic and IP) and UFIP SIP devices can be used as desk devices (Classic SIP and analogue devices are not supported). The desk devices can be out of service or unplugged. It is currently not possible to change the linkage of an auxiliary device after configuration, but you can change the type of the auxiliary device via the CLNTTYPE parameter in AMO-SBCSU. To change the linkage, the auxiliary device has to be deleted and reconfigured and a new value for the CLNTDESK parameter must be added in AMO-SBCSU.

It is possible to configure Unify Phone, OSMO on the same SBC as OpenScape 4000, but a Unify Phone user must not be configured for parallel usage of Unify Phone and other applications (e. g. UC, OSCC, C4B Xphone, OSMO etc).

Since the CICA component is shared between Unify Phone, OSMO, the UnifyPhone CSTA profile must be used. Using this profile for OSMO clients in SIP only mode will cause a short call setup delay of 2s. The CSTA Connectivity Adapter which is used for CICA must not be shared with other applications which are not using E.164 number format.

It is recommended to use G.711 as preferred codec because DTMF over OPUS codec is not functional yet.

It is not possible to answer a call from Unify Phone when the desk phone is a hunt group member and a call to the hunt group is ringing on the desk phone.

The following OpenScape 4000 features are not supported together with Unify Phone:

- CHESE group (Executive/ Secretary);
- DSS keys configured via AMO ZIEL with the desk phone number of a Unify Phone user will not signal an incoming call until it is forwarded to the desk phone;
- Parallel Ringing (Classic ONS group);
- Personal Device Group (Twinning);
- Hunt groups;
- Multi-line support;
- COM groups and one way speaker calls.
- Secret Numbers (SSTNO = Y in AMO SBCSU) [14]
- When DECT phone is switched off, auto-pilot routing is not executed (e.g. routing to Alternative number or Voicemail are not executed)
- DECT phone auto-answer is not supported (outgoing calls made from application using deskphone option, must be answered from a physical DECT phone)

NOTICE:

If the F5 key is pressed on a Web Client during an active call, the call will be dropped.

F5 can be pressed to eliminate display issues that occur only in idle state.

[14] This is a temporary restriction.

16.3 Configuration

For the initial configuration, the connectivity between OpenScape 4000, SBC and Unify Phone Telephony Connector must be set. For more information, refer to Connector configuration.

After the initial configuration, new Unify Phone users can be configured from OpenScape 4000. For more information, refer to User configuration.

16.3.1 Connector configuration

16.3.1.1 Configure Unify Phone Telephony Connector

Register your Unify Video tenant in Unify Phone Telephony Connector via https://phoneapp.unify.com/tenant/. To authenticate, you need a Unify Video account with "Super Admin" role.

For more information, refer to Unify Phone Administration.

16.3.1.2 Configure OpenScape 4000

Configure access to Unify Phone Telephony Connector

1) Open the OpenScape 4000 Assistant and navigate to **Configuration Management** > **Unify Phone** to configure the connectivity to the Unify Phone Telephony Connector.
2) Check the status of **Unify Phone Cloud** in the upper left corner of the window:
   - **Unify Phone Cloud not reachable** means that you might need to configure a proxy to reach the Internet.
   - **No or wrong API key** means that the connector is reachable but you have not entered the API Key of your tenant.

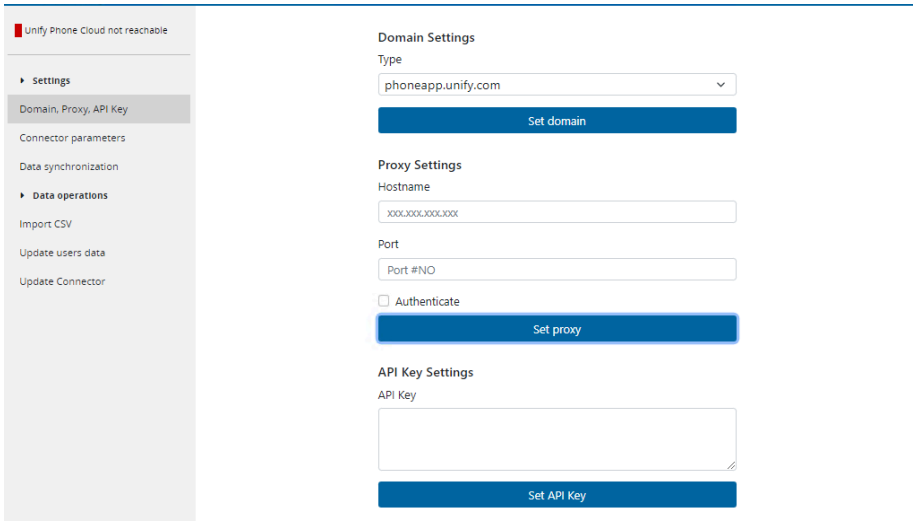


Figure 350: Unify Phone Cloud status

3) Login to the Unify Phone Telephony Connector via https://phoneapp.unify.com/tenant/ with a super admin account.

   From the **Telephony connector** tab, you can copy the API key, then paste it into the API key field and click **Set API Key**.

   If the API key is correct, the status will change to green **Unify Phone Cloud reachable**. After setting the API key, the input will disappear for security reasons.

Configure CICA

Unify Phone requires an active CICA connection for all Gateways where auxiliary devices are configured to forward CSTA messages between client and CSTA. Without an active CICA connection, Unify Phone cannot register and will display **Telephony is down**. The Gateways connect to CICA service port 31101 via VPN for security reasons. For more information, refer to the "Integrated VPN Service" chapter in the OpenScape 4000 V10, Platform Administration (Portal) document.

The status can be checked in the WBM area of the Gateways:

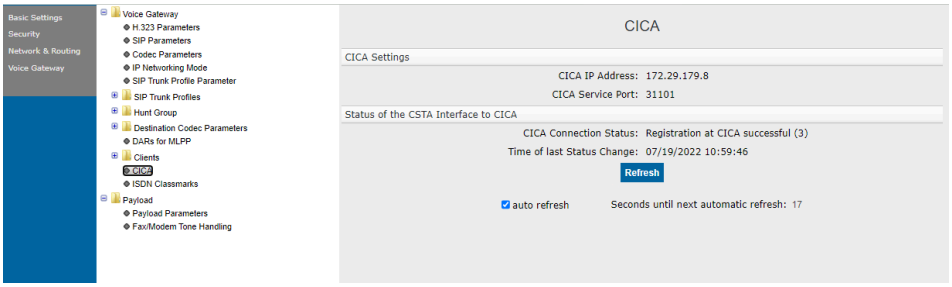


Figure 351: Configure CICA

CICA is a special application in CSTA. By default it uses port 1040 of the Default Connectivity Adapter, but Unify Phone requires the **Circuit** profile. (E164_NUMBER_FORMAT=1, OFFERED_MODE_NEEDED=1, ONS_MONITORING=1).

If the Default Connectivity Adapter is used for other applications, it is recommended to create a dedicated Connectivity Adapter with the Circuit profile on another port. For this, follow the steps below:

1) Navigate to **Expert Mode** > **CSTA** and click on **Add Connectivity Adapter**.

2) Select an available **PBX Link Number** (e.g. 7) and **PBX Sub-App Number** (e.g. 27), then select the **Circuit** profile, as displayed in the figure below.

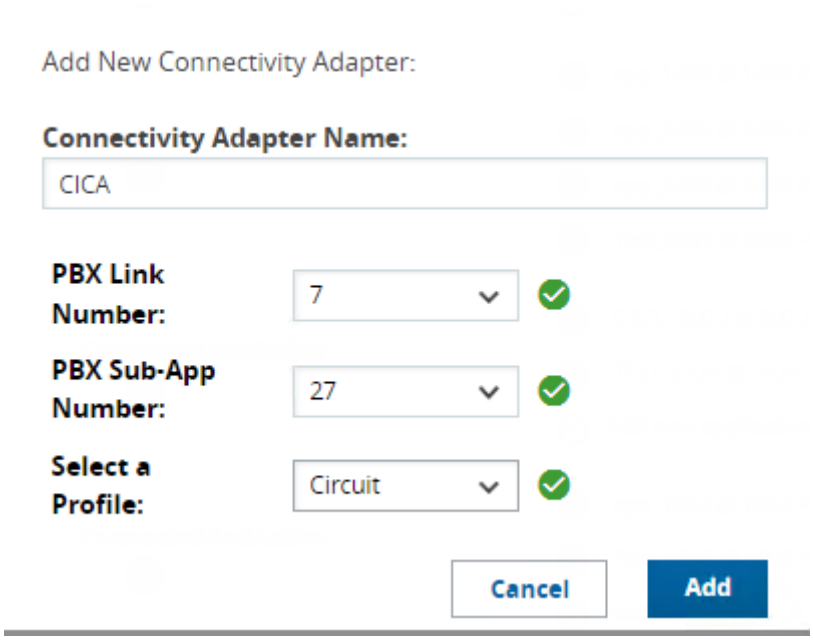


Figure 352: Connectivity Adapter Name

Click **Add**.

3) In **CSTA Administration** > **Connectivity Adapters**, click the **Add a new application** button, next to the Connectivity Adapter created in the previous step.

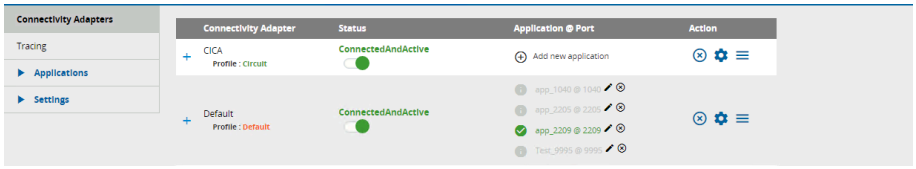


Figure 353: Add a new application in CSTA Administration

4) Define a port (e.g. port 1041) for CICA and configure the same port on the CICA Configuration page.

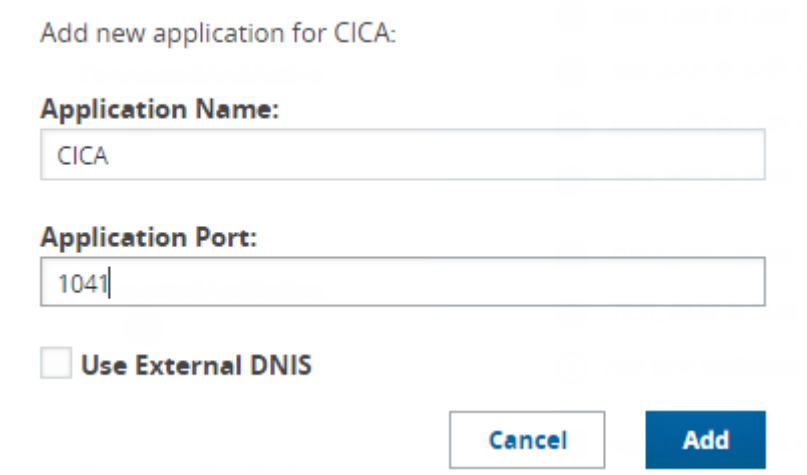


Figure 354: Define the CICA port

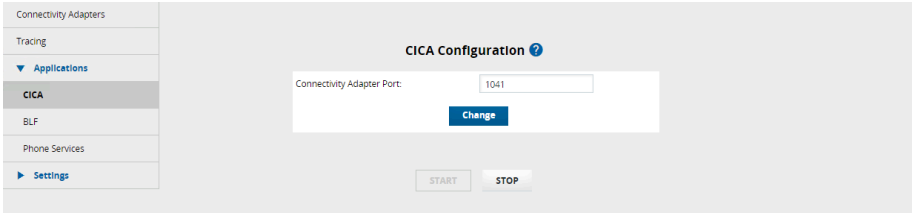


Figure 355: CICA Configuration port

Configure an external SBC address

Unify Phone will always be securely configured (TLS) by OpenScape 4000. The external IP of the SBC (in case of NAT, it is the Firewall external IP) and the SIP TLS port must be configured in OpenScape 4000 Assistant (similar to OSMO) in AMO-ZANDE, on the OSMO branch. Only IP address 1 will be used for Unify Phone.

You can configure either an FQDN name or an IP address using:

- The AMO-ZANDE command:
  ```
  CHANGE-ZANDE:TYPE=OSMO, SBCFQDN1="os4k.unify.com",
   SBCADDR1=0.0.0.0, PORT1=5061;
  ```

- The OpenScape 4000 Assistant or Manager, by navigating to **Configuration Management** > **Network** > **System**, as displayed in the figure below.

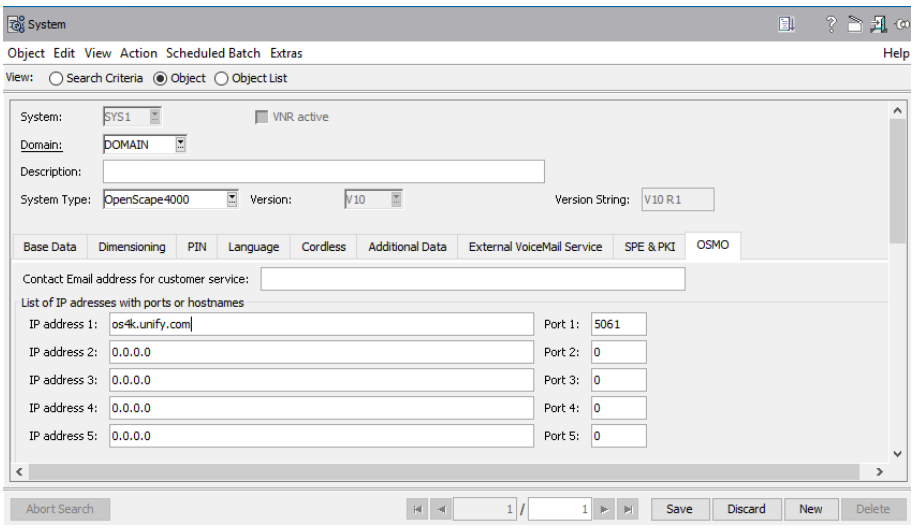


Figure 356: Configure IP Address 1 in the Configuration Management

Configure the feature list

To use the OpenScape 4000 features in Unify Phone, configure the AMO ZANDE branch OSMO FEATLIST using the following command: `CHANGE-ZANDE:TYPE=OSMO,FEATLIST=CF&SST&HF&SIP&SEHO&SDND&CSC&FC1&GPC;`

The feature list contains the following:

- Call Forwarding CF
- Single Step Transfer SST
- Handover from HF
- Sip Over Data Connection SIP
- Seamless Handover SEHO
- Snooze DnD SDND
- Consultation Call CSC
- Call Forwarding Circuit1 FC1
- Group Call GPC

16.3.1.3 Configure OpenScape SBC

The usage of OpenScape SBC is mandatory for the Unify Phone configuration.

The **Remote Subscriber** feature in OpenScape SBC must be enabled. Unify Phone Clients will register via OpenScape SBC in the OpenScape 4000 Gateways that host the UFIP auxiliary devices. For more information about the OpenScape SBC configuration, refer to the OpenScape SBC Configuration Guide.

Follow the steps below to activate the cluster mode:

1) Navigate to **VoIP > Sip Server Settings**.
2) Select **Clustered** as Comm System Type.

3) Click the **Clustered Servers** button and add all the gateways that will host UFIP auxiliary devices for Unify Phone or OSMO.

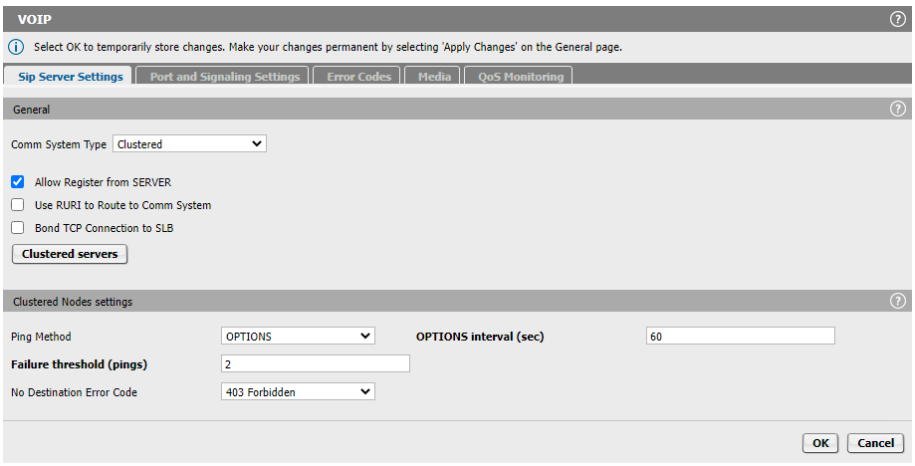


Figure 357: Sip Server Settings

Each gateway must have priority **1** and the **Stick with CommServer** option enabled, as displayed in the figure below.

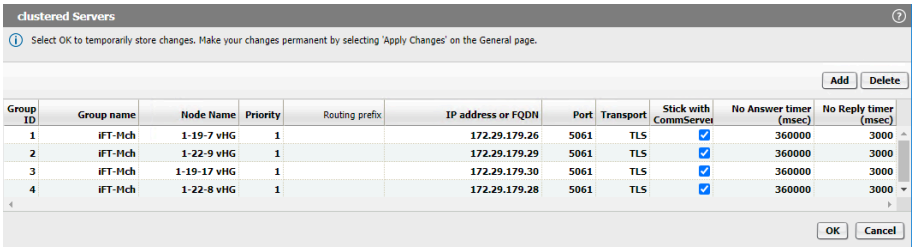


Figure 358: Clustered Servers

4) Navigate to **VoIP > Error Codes** and activate **404 Not Found**, as displayed in the figure below.

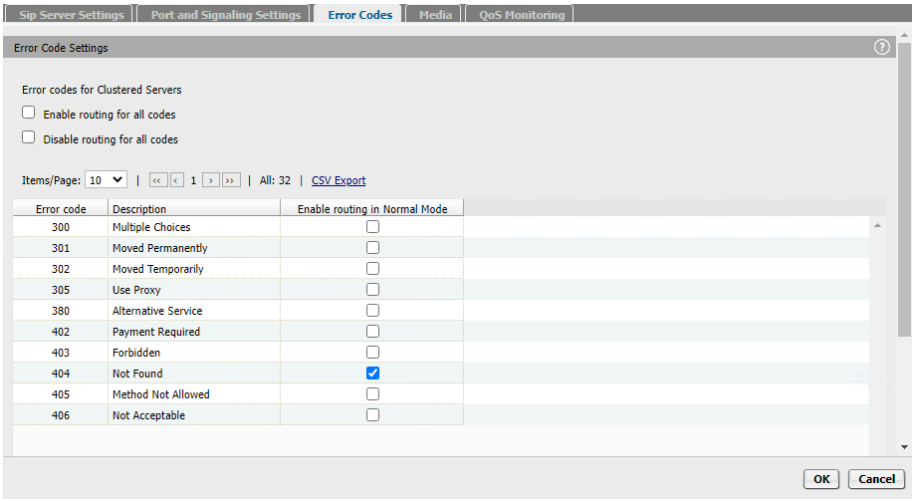


Figure 359: Error Codes

When the SBC receives the first SIP registration, it will send REGISTER to each configured gateway until it receives an answer which is not "404 Not Found". Only the gateway where the device is configured will answer with

200 OK. After the first message, the SBC will send further SIP messages only to the GWY where the device is configured.

5) Navigate to **VoIP > Media** and add the **Unify_Phone_default** Media Profile to the **OpenScape Mobile Client - WebRTC NGTC** user agent.

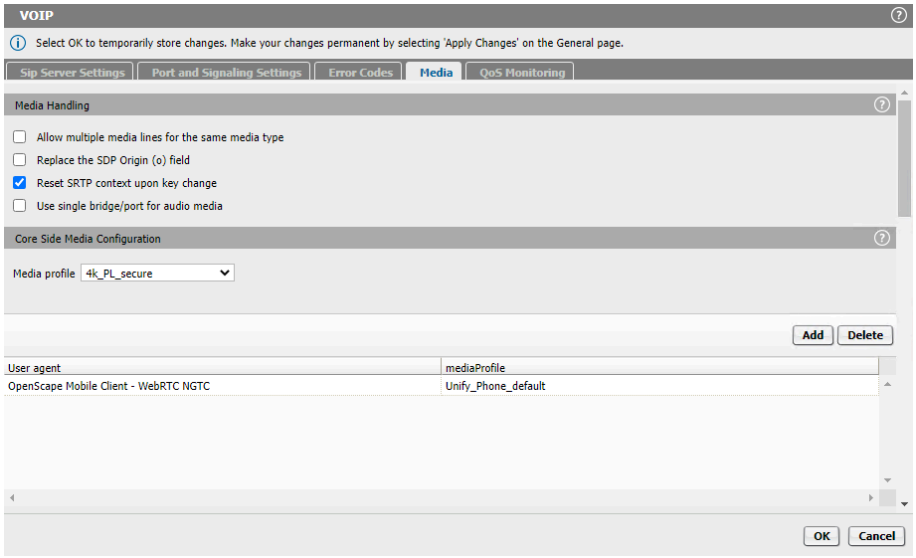


Figure 360: Media profile

6) Navigate to **Features** and enable the checkboxes for **Enable Remote Subscribers** and **Enable Codec Support for transcoding**.

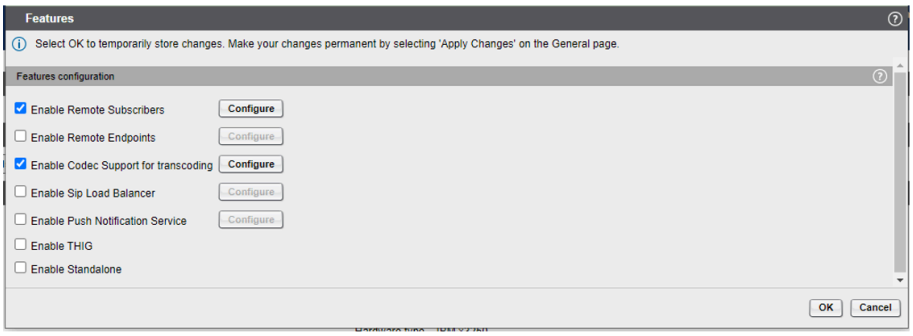


Figure 361: Features

No input is required in the **Enable Remote Subscribers** configuration tab.

In the **Enable Codec Support for transcoding** the following codecs can be enabled:

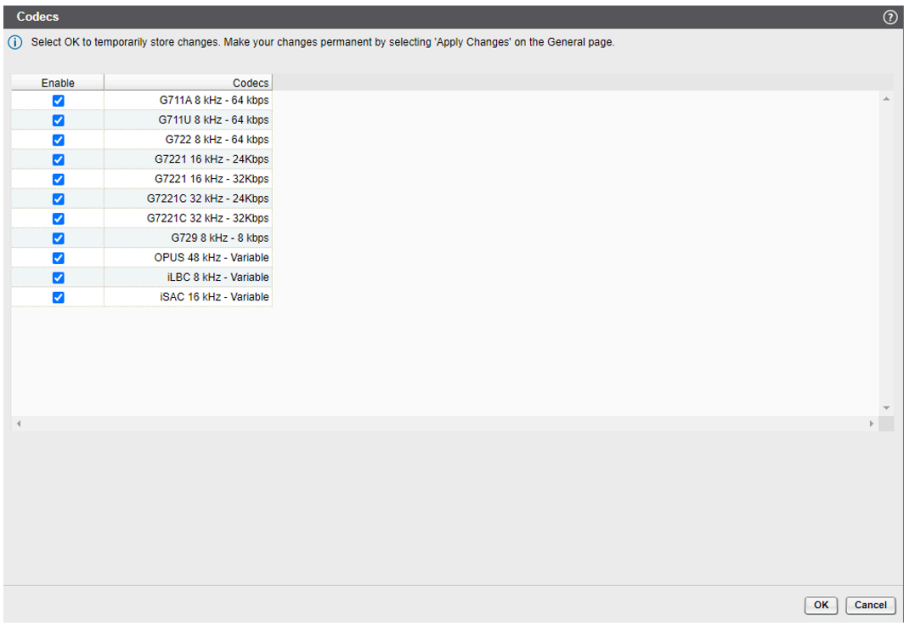


Figure 362: Codecs

16.3.2 User configuration

16.3.2.1 Configure Unify Video

Each Unify Phone user must have a Unify Video account with **Video Pro+** license and activated Cross-Launch functionality. For more information, please refer to Unify Phone Administration.

Follow the steps below to configure Unify Video:

1) Login to https://service.unifyoffice.com with an **Super Admin** or **User Admin** account.

2) To assign licenses to users, select the user you want to configure, under **Users > User List**, and click **Assign Licenses**.
3) To enable the Cross-Launch functionality, select the users under **More > Account Settings > Cross-Launch** and click **Turn on Cross-Launch**.

Under **Users > User List**, you can also add new accounts by clicking **Add User** or **Bulk Upload Users**. Each new user will get an email invitation in the configured email address. This email address will be used to map the Unify Video account to a Unify Phone station in OpenScape 4000.

16.3.2.2 Configure OpenScape 4000

Configure the email address

An Unify Phone client will register in the OpenScape 4000 system as an UFIP SIP device that is further linked to a desk device. This desk device defines the E164 number of the Unify Phone user but it is not mandatory that the desk device is in service.

The email address of the Unify Phone user must be configured in OpenScape 4000 (at the desk device) in the Configuration Management. Currently, this configuration is not possible via AMO.

To configure the email address, navigate to **Configuration Management > Station** and add the email address in the **Basic 3** tab.

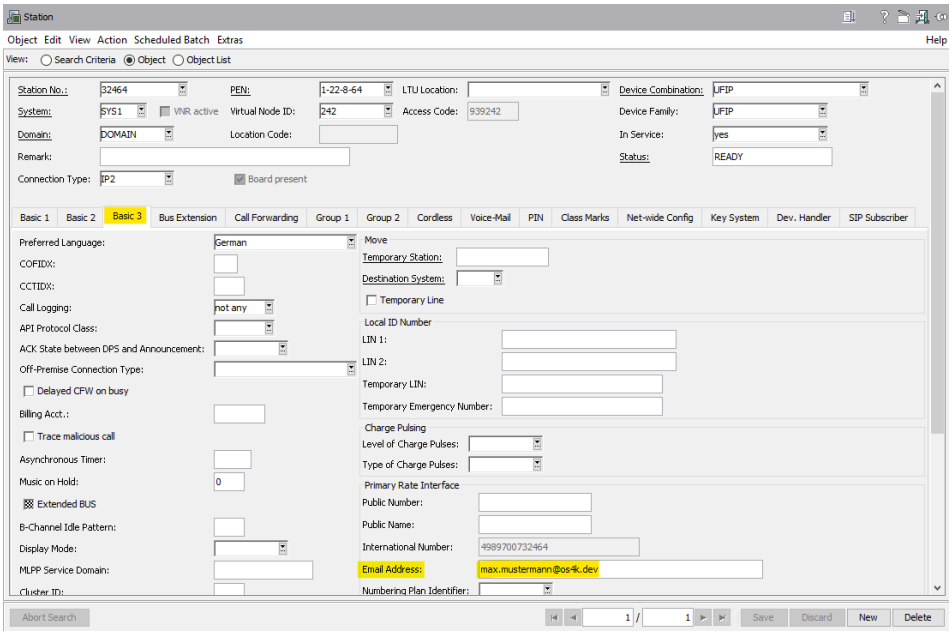


Figure 363: Add the email address

NOTICE:

If multiple email addresses need to be configured, use the Circuit mass migration csv import. For more information, refer to Mass migration from Circuit.

Configure an auxiliary device

Each Unify Phone client (e.g. OSMO and Circuit clients) will register in OpenScape 4000 as an UFIP SIP device. This auxiliary device must be linked to user's desk device via the CLNTDESK parameter. Additionally, it must be marked as an Unify Phone device via the CLNTTYPE=UNIPHONE parameter.

Auxiliary devices configured with CLNTTYPE=UNIPHONE must have a Unify Phone license. Without such a license, any registration from the Unify Phone client will be rejected.

The auxiliary device can be configured using:

- The AMO-SBCSU command:
  `ADD-SBCSU:STNO=<UFIP_STN>, OPT=OPTI, CONN=IP2, PEN=<X-Y-Z-T>, DVCFIG=UFIP, IPPASSW=..., USERID=..., SECZONE=..., CLNTDESK=<DESK_STN>, CLNTTYPE=UNIPHONE;`
- The OpenScape 4000 Assistant or Manager, by navigating to **Configuration Management** > **Station** > **Bus Extension** tab and configuring the **Universal Feature Access** section, as displayed in the image below:

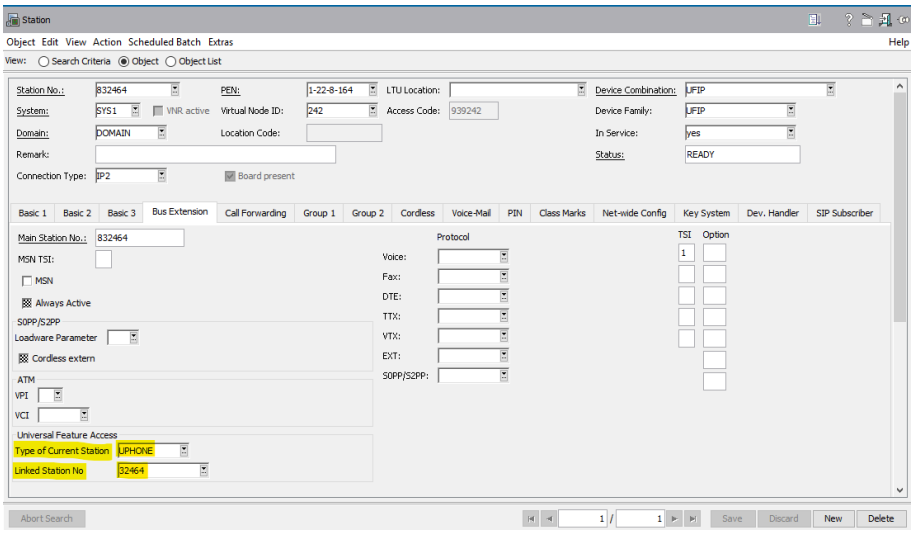


Figure 364: Bus Extension

To check the linkage, use **DIS-SBCSU**:

- DIS-SBCSU for UFIP_STN will show DESK=<DESK_STN>
- DIS-SBCSU for DESK_STN will show CLIENT=<UFIP_STN>

or

- The WBM of the Gateway, where UFIP_STN is configured under **Configuration > Voice Gateway > Clients > UFIP SIP**:
  - The **Station Number** column will show <UFIP_STN>.
  - The **ONS Number** column will show DESK_STN.

Synchronize data between Unify Phone Telephony Connector and OpenScape 4000

The configuration in OpenScape 4000 can be synchronized with Unify Phone Telephony Connector periodically (e.g. every 5h). During the synchronization process, the OpenScape 4000 will retrieve changes from the Unify Video side (e.g. new users) and upload the configuration data (e.g. phone number and SIP credentials) to Unify Phone Telephony Connector. When you have configured

some new Unify Phone users in OpenScape 4000, you can also start the synchronization process immediately.

To synchronize the configuration, navigate to **Configuration Management > Unify Phone**, select **Data synchronization** frequency and click **Synchronize Data**

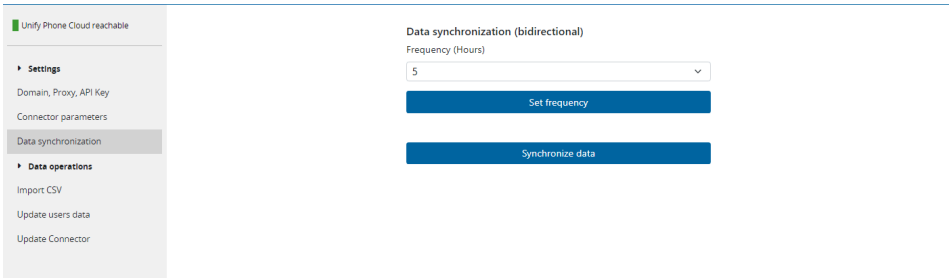


Figure 365: Data synchronization

You can check the configuration under the **Update users data** section, as displayed in the figure below.

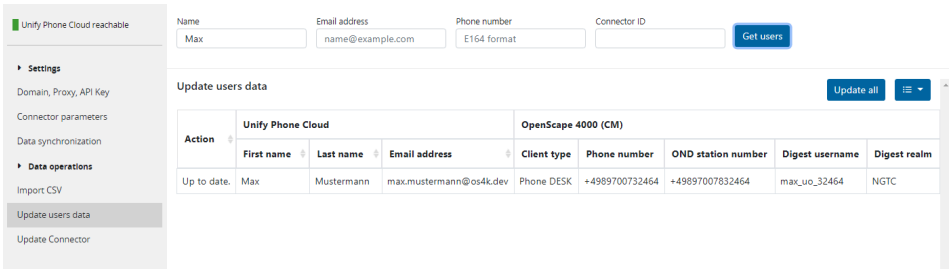


Figure 366: Update users data

The **Action** column displays the current state of the configuration and synchronization.

- **Up to date**: the data is already synchronized with Unify Phone Telephony Connector.
- **Update**: the changes were made on OpenScape 4000 and are not synchronized yet. You can press the update button to synchronize them now.
- **E-Mail not configured in OS4K**: the Unify Video user has no corresponding email address configured in OpenScape 4000.

  NOTICE: This message is also displayed when the user is configured on another PBX.

- **Unify Phone not configured in OS4K**: The Unify Video user has an email address configured in OpenScape 4000, but the auxiliary device is not configured or it has the wrong Client type assigned.

16.3.3 Mass migration from Circuit

In the first step, all Circuit users must be added to Unify Video. This can be done via the **Bulk Upload Users** of Unify Video or using the **Unify Migration Tool**. After you have uploaded the OpenScape license with sufficient Unify

Phone licenses, the Client type of all auxiliary devices used by Circuit can be changed from **OTHER** to **UNIPHONE** using the following AMO Command:
`CHA-SBCSU:STNO=<UFIP_STN>, OPT=OPTI, CLNTTYPE=UNIPHONE;`

This can be done even if the user is still using Circuit. The registration of a Circuit client will not be rejected when the auxiliary device is already switched to UNIPHONE, but the registration of a Unify Phone client will be rejected if the CLNTTYPE is OTHER.

It is possible to export all users of the Circuit tenant using a CSV file. This CSV file can be directly imported in OpenScape 4000 and will have the following format:

```
Name,First name,Last name,Location,Role,Status,Created
 on,First login,Last login,Data usage,Phone number,Package
 name
max.mustermann@os4k.dev,Max,Mustermann,,,,,,,,4989700732464,
somewhere.else@os4k.dev,Not,Here,,,,,,,,4989700799999,
...
```

Follow the steps below to import the CSV file:

1) Navigate to **Configuration Management > Unify Phone**.
2) Click **Choose file** under **Import CSV**, select your csv file and click **Import**.

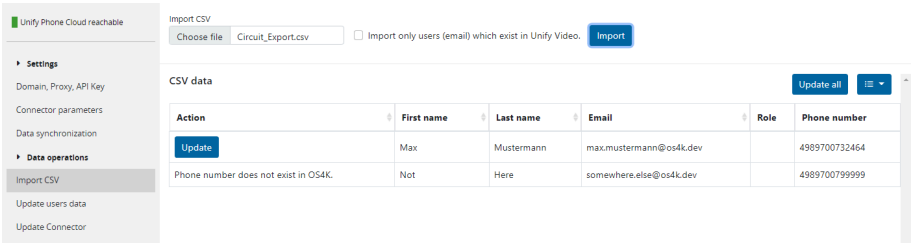


Figure 367: Import a CSV file

3) Click **Update all** or selective **Update** to configure the email address based on the **Phone number** column. If a phone number (International Number in Basic 3) does not exist (or exist in another PBX), then the corresponding row will contain the message **Phone number does not exist in OS4K**.

NOTICE:

This method can also be used if the email addresses need to be configured for many desk devices.

---

4) After Data synchronization with the Unify Phone Telephony Connector, the clients can be used.

17 H323 / H323 Annex Connectivity

17.1 Overview

IMPORTANT: As of OpenScape 4000 V8 H323 trunking is only supported for connections to OpenScape XPressions.

Features

- CLIP / CLIR / COLP / COLR
- Name Display
- Hold / Retrieve / Toggle
- Transfer (blind, unattended, attended)
- Call forwarding
- Callback on busy subscriber / Callback no reply
- Message waiting indication
- Route optimization
- OpenScape 4000 as survivability media gateway
- Signaling and payload encryption (TLS / SRTP)
- T.38

Boards Used

- The common gateway board HG 3500 is used. For details, see “Gateways HG 3500 and HG 3575”, Chapter 3, “Supported Gateways”.
- H323 trunk protocol to OpenScape Xpressions is supported on STMIX/ STMIY board and SoftGate (vHG3500 board).

17.2 DTMF Outband Signaling

To activate the “DTMF Outband Signaling”, the following steps have to be made:

1) Deactivate RFC 2833 via AMO CGWB:

```
CHA-CGWB:MTYP=CGW,LTU=<ltu>,SLOT=<slot>,TYPE=ASC,RFCDTMF=NO;
```

1) To activate H.323 DTMF Outband Signaling, transmission of DTMF tones according to RFC 2833 has to be deactivated. Against a widely held belief transmission of DTMF tones according to RFC 2833 is not a DTMF Outband Signaling, but an Inband Signaling using special codecs.

To deactivate it parameter **RFCDTMF** in AMO CGWB path **ASC** has to be set to **NO on both sides**.

2) Activate “DTMF Outband Signaling” via WBM (Parameter **DTMF Outband Signaling**)

3) WBM: **Configuration > Payload > HW Modules**

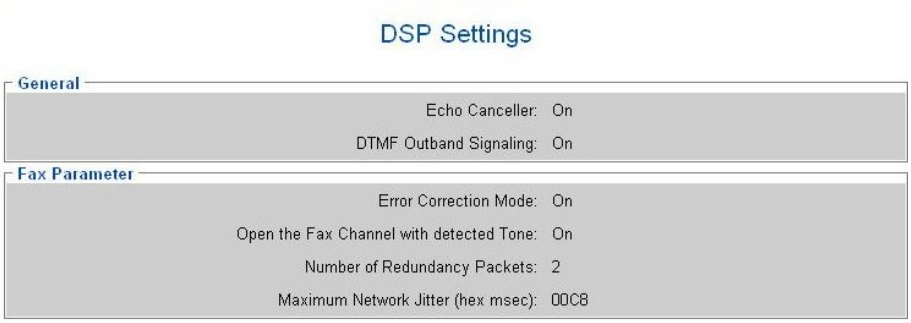


Figure 368: Activation of DTMF outband signaling

17.3 Configuration Example

17.3.1 Configuration using AMOs

17.3.1.1 Trunking Protocol

The same protocols must always be set in the AMO CGWB and AMO GKREG.

Table 83: Protocols in the AMOs CGWB and GKREG

AMO CGWB	AMO GKREG	Protocol
TRPRH323	H323	native H323
TPRH323A	H323ANN	H323 Annex

If H323 Annex is set in the AMO CGWB/AMO GKREG, this protocol is only used if it was also set in the peer or if the peer can use this protocol.

17.3.1.2 Configuring a HG 3500 as a Local Gateway

The following diagram shows a HG 3500 scenario for a fictitious customer in Frankfurt. It shows node 10-69-100 (Frankfurt-Bockenheim) and node 10-69-200 (Frankfurt-Sachsenhausen). Both systems have a common gateway board that should be configured as HG 3500. LEGK should be active on both systems (two local gateways). This constellation is relatively easy to explain because both nodes can be configured more or less symmetrically. The figure shows all necessary parameters. Node 10-69-100 is located in IP network 1.69.11.0/24 and node 10-69-200 is located in IP network 1.69.21.0/24. The networks reach each other over the routers Ra and Rb.

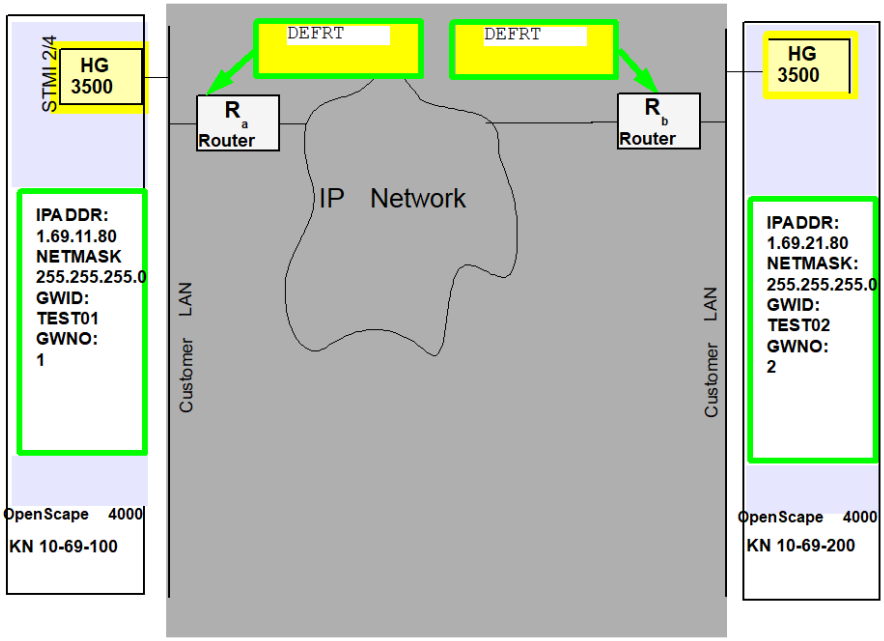


Figure 369: Configuration example: both nodes are LEGK

17.3.1.2.1 Configuration in Node 10-69-100

Start by configuring the board as HG 3500 in node 100. To avoid repeated restarts, do not insert the board until configuration is complete.

Step 0:

Configure LEGK in node 10-69-100.

```
CHANGE-ZANDE:TYPE=ALLDATA,GATEKPR=YES;
```

Step 1:

The Common Gateway Board Q2316-X is configured as HG 3500. Q2316-X is the version with 60 B channels. You can configure the board as a pure IP trunking board or in mixed operation with IP trunking and LAN connectivity (WAML) and many other features.

Configuration of the board for IP trunking only:

```
ADD-BFDAT:FCTBLK=1,FUNCTION=HG3550,BRDBCHL=BCHAN60&BCHAN120;
CHANGE-BFDAT:CONFIG=CONT,FCTBLK=1,FUNCTION=HG3550,LINECNT=1,

UNITS=3; /* 30 B channels for HG3550 functionality (H323 trunking,

SIP trunking, SIP subscriber)
CHANGE-BFDAT:CONFIG=OK,FCTBLK=1,ANSW=YES; /* Close the configuration
ADD-BCSU:TYPE=IPGW,LN=1,LTU=1,SLOT=37,PARTNO="Q2316-X",

FCTID=1,LWVAR="0",FCTBLK=1,BCHL3550=30,ALARMNO=0;
```

or

IP Trunking & WAML:

```
ADD-BFDAT:FCTBLK=1,FUNCTION=HG3550&WAML,

BRDBCHL=BCHAN60&BCHAN120;
CHANGE-BFDAT:CONFIG=CONT,FCTBLK=1,FUNCTION=HG3550,LINECNT=1,
```

```
UNITS=3; /* 30 B channels for HG3550 functionality (IP trunking, SIP trunking,
SIP subscriber)
CHANGE-BFDAT:CONFIG=CONT,FCTBLK=1,FUNCTION=WAML,UNITS,LINECNT=1; /* Board will
be configured with one circuit, i.e. 10 B channels for WAML
CHANGE-BFDAT:CONFIG=OK,FCTBLK=1,ANSW=YES; /* Close the configuration
ADD-BCSU:TYPE=IPGW,LN=1,LTU=1,SLOT=37,PARTNO="Q2316-X   ",FCTID=1,LWVAR="0",FCT►
BLK=1,BCHL3550=30,BCHLWAML=10,ALARMNO=0;
```

Step 2:

The AMO CGWB allows the board to receive the IP address in the customer LAN (LAN1), the subnet mask and the protocol variant (H323A / SIP-Q / NONE (board is only configured for SIP subscribers).

IMPORTANT: Only one trunking protocol may be configured for each board! There are no restrictions on interworking with other functions!

```
ADD-CGWB:LTU=1,SLOT=37,SMODE=NORMAL,IPADDR=1.69.11.80,NET►
MASK=255.255.255.0,TPRH323A=10;/*10 B channels for H323A trunking
```

or

```
ADD-CGWB:LTU=1,SLOT=37,SMODE=NORMAL,IPADDR=1.69.11.80,NETMASK=255.255.255.0,TR►
PRH323=10;/*10 B channels for H323A trunking
```

=> 20 B channels remain for other functions

Step 3:

The default router is now set in the customer LAN:

```
CHANGE-CGWB:MTYPE=CGW,LTU=1,SLOT=37,TYPE=GLOBIF,DEFRT=1.69.11.254;
```

Step 4:

The HG 3500 requires an ID that is unique in the network. This is the parameter **GWID** in AMO CGWB:

CHANGE-
CGWB:MTYPE=CGW,LTU=1,SLOT=37,TYPE=GWDATA,GWID1="TEST01";

GWID1 and **GWID2** together form a contiguous value consisting of 128 characters. Entries are case-sensitive.

Step 5:

The HG 3500 boards are administered using one gateway number (**GWNO**). This number must also be unique.

```
CHANGE-CGWB:MTYPE=CGW,LTU=1,SLOT=37,TYPE=LEGKDATA,GWNO=1;
```

Step 6:

IMPORTANT: Multiple boards are permitted in one trunk group!

This step consists of several configuration commands. We need to set up the trunk group and circuit, via which the B channels between gateway and OpenScape 4000 are switched.

First you need a trunk group:

```
ADD-BUEND:TGRP=50,NAME="IP TRUNK GWID 1   ",NO=30,TRACENO=0, ACDTHRH=*, PRIO►
NO=2, TDDRFLAG=ON, GDTRRULE=0, ACDPMGRP=0, CHARCON=NEUTRAL;
```

A digital trunk is then required (AMO TDCSU). The device type is **HG3550IP** (for H323/H323A and native SIP/SIP-Q trunking). If you want to permit DMC, set **DMCALLWD=Y**. This is only possible when the partner system supports DMC.

```
ADD-TDCSU:TYPE=NEW,PEN=1-01-037-0,COTNO=36,

COPNO=32,DPLN=0,ITR=0, COS=2,LCOSV=1,LCOSD=1,

CCTN="CIRCUIT from GW2",PROTVAR="ECMAV2",SEGMENT=8, ISDNIP=00,ISDN►
NP=0,TRACOUNT=31,SATCOUNT=MANY,

NNO=1-69-499,ALARMNO=12, COTX=36,CCHDL=SIDEA,CLASSMRK=EC&G711,

TCCID="IP RS",TGRP=50,SRCHMODE=DSC,INS=Y,DEV=HG3550IP,

BCHANNEL=1&&30,BCNEG=N,BCGR=1,LWPAR=0,DMCALLWD=YES;
```

If DMC has been activated for the H323-/H323A trunking path, Voice Activity Detection should also be activated. Otherwise the same bandwidth is required for the master connection as for the slave connection!

```
CHANGE-CGWB:MTYPE=CGW,LTU=<ltu>,SLOT=<slot>,TYP=ASC,

PRIO=PRIO1,VAD=YES;
```

Otherwise the same bandwidth is required for the master connection as for the slave connection.

IMPORTANT: It is recommended to reset the board: `RESET-BSSU:ADDRTYPE=PEN,LTG=1,LTU=1,SLOT=37;`

IMPORTANT: The command CHANGE-FUNSU can prevent the complete reloading of the STMI board. Reloading is only necessary in the case of loadware changes. `CHANGE-FUNSU:PIT=FLASH,PARTNO="Q2316-X ",FCTID=2, ACTION=RESET;`

Step 7:

The LEGK must now still be informed about the existence of the HG 3500 gateway in the AMO GKREG. The **GWNO** must match the entry from the AMO CGWB. In the case of a local gateway, the AMO GKREG automatically loads the IP address (**IPADR**) from the AMO CGWB. You must also set the attributes **INTGW** (internal -local- gateway) and **HG3550V2** (version ID). The parameter **REGGW** is not necessary because the gateway does not have to register at another gateway.

```
ADD-GKREG:GWNO=1,GWATTR=INTGW&HG3550V2&H323ANN or H323,NUM=0,DPLN=0,LAUTH=1;
```

If a local gateway is configured, **REGISTERED=NO** is always displayed with `DISPLAY-GKREG;`.

The HG 3500 board in node 10-60-100 is now configured properly and is communicating with the LEGK. However, the gateway is still missing in the partner node.

17.3.1.2.2 Configuration in Node 10-69-200

An LEGK should also be active in node 10-69-200. As the configuration procedures for nodes 10-69-200 and 10-69-100 are identical, this section only lists the appropriate AMO commands for the steps described above.

Step 0:

```
CHANGE-ZANDE:TYPE=ALLDATA,GATEKPR=YES;
```

Step 1:

```
ADD-BFDAT:FCTBLK=1,FUNCTION=HG3550,BRDBCHL=BCHAN60&BCHAN120;
CHANGE-BFDAT:CONFIG=CONT,FCTBLK=1,FUNCTION=HG3550,LINECNT=1,

UNITS=3; /* 30 B channels for HG3550 functionality (IP trunking, SIP trunking,
SIP subscriber)
CHANGE-BFDAT:CONFIG=OK,FCTBLK=1,ANSW=YES; /* Close the configuration
ADD-BCSU:TYPE=IPGW,LN=1,LTU=2,SLOT=49,PARTNO="Q2316-X   ",

FCTID=1,LWVAR="0",FCTBLK=1,BCHL3550=30,ALARMNO=0;
```

Step 2:

```
ADD-CGWB:LTU=2,SLOT=49,SMODE=NORMAL,IPADDR=1.69.21.80,NETMASK=255.255.255.0,
TPRH323A=10;
```

or

```
ADD-CGWB:LTU=2,SLOT=49,SMODE=NORMAL,IPADDR=1.69.21.80,NETMASK=255.255.255.0, TR►
PRH323=10;
```

Step 3:

```
CHANGE-CGWB:MTYPE=CGW,LTU=2,SLOT=49,TYPE=GLOBIF,DEFRT=1.69.21.254;
```

Step 4:

```
CHANGE-CGWB:MTYPE=CGW,LTU=2,SLOT=49,TYPE=GWDATA,GWID1="TEST02";
```

Step 5:

```
CHANGE-CGWB:MTYPE=CGW,LTU=2,SLOT=49,TYPE=LEGKDATA,GWNO=2;
```

Step 6:

```
ADD-BUEND:TGRP=50,NAME="IP TRUNK GWID 2 ",NO=30;
ADD-TDCSU:TYPE=NEW,PEN=1-02-049-0,COTNO=36,

COPNO=32,DPLN=0,ITR=0, COS=2,LCOSV=1,LCOSD=1,

CCTN="CIRCUIT from GW2",PROTVAR="ECMAV2",SEGMENT=8,ISDNIP=00,

ISDNNP=0,TRACOUNT=31,SATCOUNT=MANY,NNO=1-69-499,

ALARMNO=12, COTX=36,CCHDL=SIDEA,CLASSMRK=EC&G711,TCCID="IP RS",

TGRP=50,SRCHMODE=DSC,INS=Y,DEV=HG3550IP,BCHANNEL=1&&30,BCNEG=N,BCGR=1,LW►
PAR=0(=Master),DMCALLWD=YES;
CHANGE-CGWB:MTYPE=CGW,LTU=<ltu>,SLOT=<slot>,TYP=ASC,PRIO=PRIO1,
```

```
VAD=YES;
```

Step 7:

The GKREG contains the configuration for both HG 3500 boards. Here, **GWNO=2** is now the local gateway in node 10-69-200 with the attributes **INTGW** and **HG3550V2** and **H323ANN or H323**, while **GWNO=1** (the partner gateway in node 10-69-100) contains the attributes **EXTGW**, **HG3550V2** and **H323ANN or H323** in this system. The parameter **REGGW** is not necessary because the gateway does not have to register at another gateway.

```
ADD-GKREG:GWNO=1,GWATTR=EXTGW&HG3550V2&H323ANN or H323,GWIPAD►
DR=1.69.11.80,DIPLNUM=0,DPLN=0,LAUTH=1;
ADD-GKREG:GWNO=2,GWATTR=INTGW&HG3550V2&H323ANN or H323,DIPLNUM=0,DPLN=0,LAUTH=1;
```

17.3.1.2.3 Extension in Node 10-69-100

The HG 3500 in node 10-69-200 must be retrofitted in node 10-69-100 for LEGK (AMO GKREG). For node 10-69-100, this HG 3500 (**GWNO=2**) is an external gateway (attributes **EXTGW&HG3550V2&H323ANN or H323**) and is not registered in node 10-69-100.

ADD-GKREG:**GWNO=2**,GWATTR=**EXTGW**&HG3550V2&**H323ANN or H323**,GWIPADDR=1.69.21.80,DIPLNUM=0,DPLN=0,LAUTH=1;

17.3.1.2.4 Call from Node 10-69-100 to Node 10-69-200

LCR should now be configured for node 10-69-100 in our example so that a station using open numbering (**UNKNOWN**) in this node can reach a station in node 10-69-200 over the IP trunk. Closed numbering or ISDN numbering plans are also supported and configured in the same way.

A station in node 10-69-100 reaches node 10-69-200 over the tie number 902.

```
ADD-WABE:CD=902,DAR=TIE;
```

LRTE 520 should route to node 10-69-200 and use trunk group 50 (see above):

```
ADD-RICHT:MODE=LRTENEW,LRTE= 520,LSVC=ALL,

NAME="IP TO KN 69 200",TGRP=50,DNNO=1-69-499;
```

The following is a simple outdial rule:

```
ADD-LODR:ODR=520,CMD=ECHO,FIELD=2;

ADD-LODR:ODR=520,CMD=END;

ADD-LODR:ODR=520,INFO="TIE TO GW2";
```

Enter **GW1=2-0** in LRTE 520 now. The **2** refers to the parameter **GWNO** in AMO GKREG (section Section 3.1.2.3, “Extension in Node 10-69-100”). In AMO GKREG for node 10-69-100, the HG 3500 with **GWNO=2** is the IP address 1.69.21.80. The **0** stands for the sector path number. Sector path 0 means there is unlimited bandwidth for this path. If the destination gateway is not reachable, you can use the parameters **GW2** to **GW5** to configure an alternative route.

```
ADD-LDAT:LRTE=520,LSVC=ALL,LVAL=1,TGRP=50,ODR=520,

LAUTH=1,GW1=2-0;
```

IMPORTANT: In contrast to S0/S2 connections (point-to-point), an IP connection is a point-to-multipoint connection and therefore the same trunk number is used to the different destination gateways (**GW1-GW5**) in the AMO LDAT!

The tie number is entered in the AMO LDPLN. The directory number is entered in the default dial plan with **DIPLNUM=0**. A profile index can also be used instead of LRTE (AMO-LPROF):

```
ADD-LDPLN:LCRCONF=LCRPATT,DIPLNUM=0,LDP="902"-"X",

LRTE=520,LAUTH=1;
```

If you want to be able to reach node 10-69-100 from node 10-69-200, perform the following configuration. You then point to the **GWNO=1** in AMO LDAT.

17.3.1.3 Backup & Restore of the WBM Configuration Data

All configuration data configured via the WBM of the board must be backed up using the backup server. Otherwise all configuration data will be lost after a board replacement, a reset of the board or loadware upgrade and the H323-/H323A trunking connection cannot be automatically reestablished. This is done with the OpenScape 4000 Assistant > Backup & Restore.

It is important to ensure that the backup server can be reached. If the backup server is not available, the configuration data can also be saved in the flash memory of the board and then can be retrieved from there.

OpenScape 4000 Assistant > Backup & Restore

Configuration of a connection to backup server and OpenScape 4000 Assistant.

```
CHANGE-CGWB:MTYPE=CGW,LTU=1,SLOT=37,TYPE=MGNTDATA,

MGNTIP=<ip_address_assistant>,MGNTPN=<port_no_assistant>,

BUSIP=<ip_address_backup_server>,BUSPN=<port_no_backup_server>};
```

IMPORTANT: Note: The values for **MGNTPN** und **BUSPN** will not be restored after a reset of the board. They have to be configured again manually.

Local Flash

IMPORTANT: It is recommended to additionally use the local flash as a backup media. If the connection to the backup server is broken the configuration data will be automatically restored from the local flash.

WBM > Maintenance > Actions > (double-click) Automatic Actions > Saving Local Configuration for Upgrade

For more information please refer to "Gateways HG 3500 and HG 3575", Chapter 6, “Save Configuration Data in Local Flash ((local Backup & Restore)”.

IMPORTANT: If the restore is necessary (e.g. after an upgrade of the loadware) and the backup server cannot be reached during the startup phase, the board is loaded and put into operation with the default configuration. If the HBR server is then reachable, the restore is carried out afterwards and a reboot with the new configuration is triggered! An additional reboot is also

triggered during the startup phase if configurations/data required for operation are restored (e.g. SPE certificates).

IMPORTANT: To avoid problems during upgrading/loadware swapping, a backup should be initialized after exchanging the board because the backup is associated with the MAC address.

17.3.1.4 Displaying Link Status

The link status of the LAN interface (link signal Ethernet, LAN speed, and LAN interface) can be displayed at each level with the AMO SDSU using the usual commands (**PERI1**, **PERI2,** and **PERI3**):

```
DISPLAY-SDSU:TYPE=PEN,LEVEL=PERI1,LTG=1,LTU=<ltu no>,

SLOT=<slot no>;
```

17.3.1.5 Procedure for Adding Supplementary HG 3500 Boards to the Network

Additional LEGKs can be configured in the same way as node 10-69-100. The AMO BFDAT, AMO BCSU, AMO CGWB, AMO GKREG and AMO LDAT are then in a single node.

IMPORTANT: The GKREG must recognize all HG 3500 boards in the network.

17.3.1.6 Relevant AMOs

AMO	Parameter	Sprache/ Language	Beschreibung/Description
BCSU	TYP=IPGW	d	CGW einrichten
	TYPE=IPGW	e	Configure CGW
	BKAN3550	d	Anzahl der B-Kanäle für IP-Trunking
	BCHAN3550	e	Number of b channels for IP trunking
BFDAT	FUNCTION=HG3550	d	CGW mit IP-Trunking
	FUNCTION=HG3550	e	CGW with IP trunking
	BGBKAN	d	Maximale Anzahl der verfügbaren B-Kanäle der Baugruppe (entweder 60 oder 120)
	BRDBCHL	e	Maximum number of available b channels (60 or 120)
	ANZSATZ	d	Anzahl der Sätze für IP-trunking

AMO	Parameter	Sprache/ Language	Beschreibung/Description
	LINECNT	e	Number of lines for IP trunking
	ANZEINH	d	Anzahl der vordefinierten Blöcke mit ausgewählter Funktion pro Satz.
	UNITS	e	Defines the number of predefined blocks with the selected function per line.
CGWB	DEFRT	d	IP-Adresse des Default Routers
	DEFRT	e	IP address of the default router
	GWID1	d	Gateway ID
	GWID1	e	Gateway ID
	VAD	d	Voice Activity Detection
	VAD	e	Voice Activity Detection
GKREG	GWATTR	d	Gateway Attribut
	GWATTR	e	Gateway attribute
	GWNR	d	Gateway ID (muss dem Eintrag im AMO CGWB entsprechen)
	GWNO	e	Gateway ID (must correspond to the value in AMO CGWB)
TDCSU	DMCERL=NEIN	d	DMC wird verhindert
	DMCALLWD=NO	e	DMC not allowed
ZANDE	GATEKPR=JA	d	PBX mit Gatekeeper
	GATEKPR=YES	e	PBX with gatekeeper

17.3.2 Configuration with OpenScape 4000 Assistant

17.3.2.1 Configure Common Gateway HG 3500

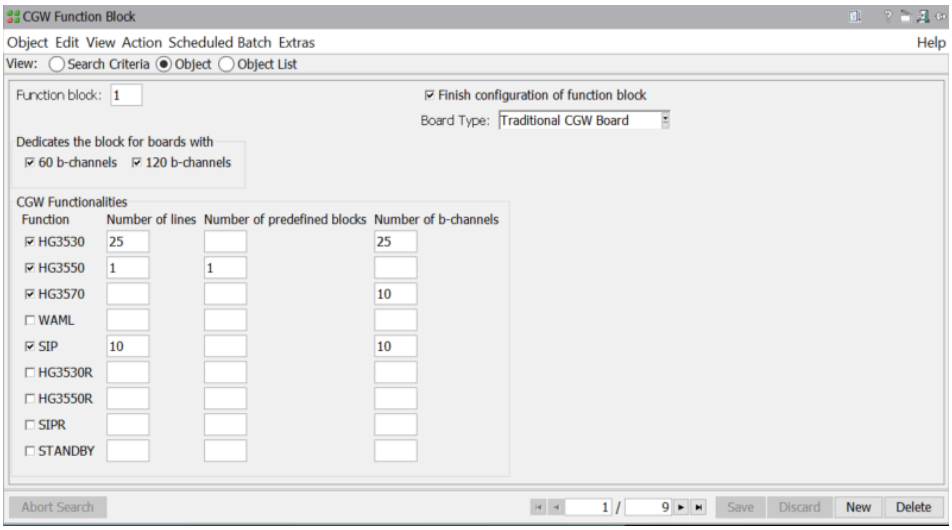
In order to configure a CGW board, you have to do the following:

- Step 1: Create function block
- Step 2: Search for a free slot
- Step 3: Open Board configuration menu in OpenScape 4000 Assistant
- Step 4: Add new board
- Step 5: Fill in the mask
- Step 6: Open STMI2-IGW Board Data dialog and fill mandatory fields

Step 1: Create function block

Start **CM > System Data > Board > CGW Function Block**

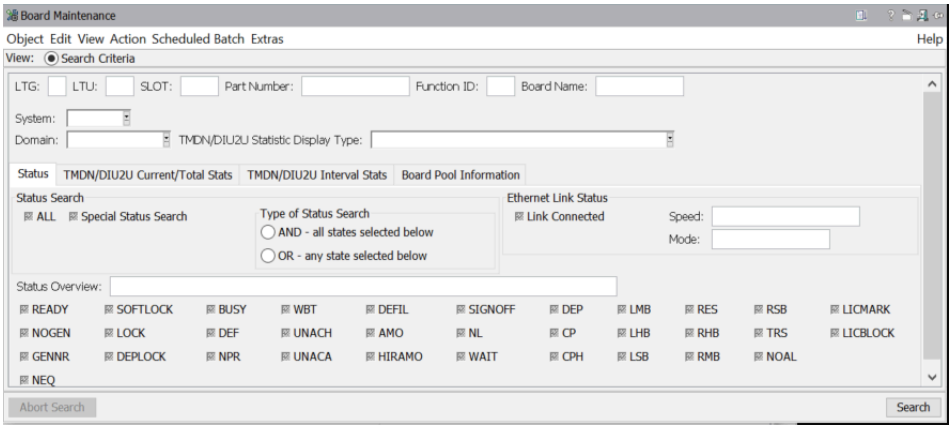
Click **Search** for searching for a free function block number. Click **New** for adding a new function block. Enter the required data and click **Save**.



Step 2: Search for a free slot

Before entering the LTU and SLOT number it is recommended to check if the desired SLOT is free. To do this call: **CM > System Data > Maintenance> Board Maintenance**.

Following the search in the object list view, free LTUs and SLOTs are marked with **NOGEN/NPR/UNACH** in the **Status Overview** column.



Step 3: Open Board configuration menu in OpenScape 4000 Assistant

CM > System Data > Board > Board

Step 4: Add new board

Press **New** button in order to add new board.

Step 5: Fill in the mask

- **Part Number**: Q2316-X or Q2316-X10 or Q2324-X500 or Q2324-X510
- **Function ID**: is always 1
- **Category**: IPGW

- **Board Name**: STMI2, STMI4 or STMIX/STMIY
- **CGW Function Block**: enter previously created function block for trunking (see Step 1: Create function block)
- **LTU** and **SLOT**: select a free slot (see Step 2: Search for a free slot)

Step 6: Open STMI2-IGW Board Data dialog and fill mandatory fields

Customer LAN IP Address and **Subnet Mask**.

Trunk Protocol: number of b-channels per protocol (e.g. **H323/H323-Annex**: 50).

IMPORTANT: Only one trunk protocol per board is supported! A combination of different trunking protocols on one board is not possible!

After all required data has been entered in the relevant fields, press the **Save** button.

The board is now added and can be found in **Board Dialog** or in **Board Maintenance**.

17.3.2.2 Delete IPGW

To delete an IPGW board, proceed as follows:

- Step 1: Open Board configuration menu in OpenScape 4000 Assistant
- Step 2: Search for IPGW
- Step 3: Select IPGW and delete it

Step 1: Open Board configuration menu in OpenScape 4000 Assistant

CM > System Data > Board > Board

Step 2: Search for IPGW

Search Criteria > Category: IPGW

Step 3: Select IPGW and delete it

Choose the board that has to be deleted from the list and click **Delete**. After pressing the **Delete** button, a message appears confirming deletion of the board from the system.

17.3.2.3 Modify Board Data of IPGW

In order to modify board data, follow these steps:

Step 1: Open Board configuration menu in OpenScape 400 Assistant

CM > System Data > Board > Board

Step 2: Select IPGW

Select IPGW in the Category list and press the Search button.

Step 3: Carry out desired changes

Perform the necessary changes in the board dialog (e.g. IP address) and save the changes with the Save button.

After saving the changes, a dialog confirming the successful action pops up.

Step4: Check the changes

Make a new board search in order to check if new data has been accepted.

18 Signaling and Payload Encryption (SPE)

18.1 Feature Description

The "Signaling and Payload Encryption" feature encompasses the encryption of payload data and signaling data within OpenScape 4000 systems or between such systems and the associated endpoints. Additionally, calls in networks with HiPath 3000 V7 (and higher) and OpenScape Voice V3.1 R2 (and higher) are transferred encrypted.

A PKI (Pubic Key Infrastructure) is needed to use signaling and payload encryption. For more information, see Section 1.3.1, “PKI (Public Key Infrastructure)”.

IMPORTANT: T38 fax streams are not supported for SPE.

18.1.1 Encrypted Signaling and Payload Connections

Security for **all** signaling and payload streams passed through an IP network by means of encryption is supported.

Table 84: Signaling and payload encryption (IP environment)

OpenScape 4000	STMI board	OpenScape 4000 SoftGate/vHG 3500/ STMIX/STMIY
Native SIP Trunk	TLS	TLS + SDES
SIP-Q Trunk	TLS + MIKEY	TLS + MIKEY or SDES
HFA subscriber	TLS + MIKEY	TLS + MIKEY
SIP subscriber	TLS	TLS + SDES

NOTICE: SIP devices are supported for SPE (TLS and SRTP) on STMIX/STMIY and SoftGate, however for devices that don’t support MTLS (e.g. Mediatrix) MFS functionality with SIPQ Trunks is not possible and a dedicated SIP Subscriber board is recommended. The issue is the activation of SIPQ will force MTLS and thereby SIP stations using TLS won’t work.

18.1.2 Scenarios - Overview

Signaling and payload encryption is supported in the following scenarios:

- IP trunking (see Section 3.3.2, “SPE for IP Trunking”)
- SIP subscriber (see Section 3.4.2, “SPE for IP Subscribers”)
- HFA subscribers (see Section 3.4.2, “SPE for IP Subscribers”)
- IPDA (see Section 3.5, “Activation / Deactivation of SPE for Access Points”)

- OpenScape 4000 SoftGate (see Section 3.6, “OpenScape 4000 SoftGate SPE Activation / Deactivation”)
- Analog and TDM terminals (see Section 3.4.1, “SPE for Analog/ TDM Endpoints”)
- Analog and TDM trunking connections (see Section 3.3.1, “SPE for Analog / TDM Trunks”)

18.1.3 Solution Concepts

18.1.3.1 PKI (Public Key Infrastructure)

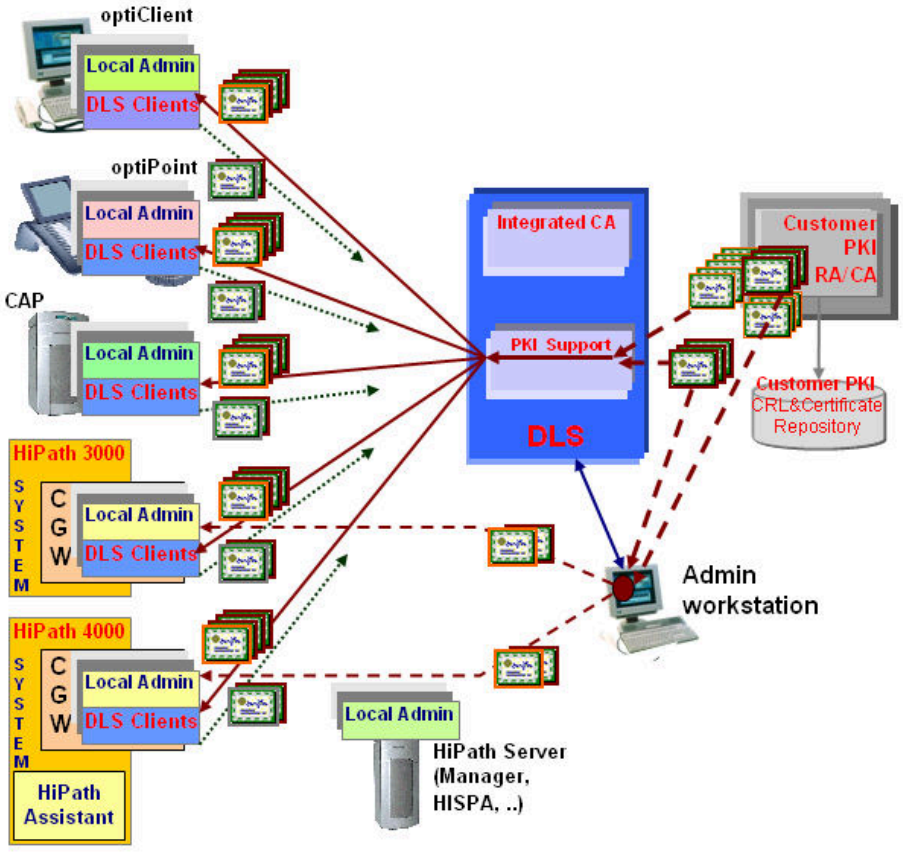


Figure 370: Public Key Infrastructure (PKI) using the example of common gateways

A Public Key Infrastructure (PKI) is needed to use the "Signaling and Payload Encryption" feature. You can either use an existing customer PKI for this or apply a new PKI using Deployment Service DLS (DLS V3 and V7 R1.11.2).

The necessary certificates are centrally deployed to all OpenScape 4000 gateways and subscribers via DLS.

The PKI for OpenScape 4000 included in DLS

- features a basic PKI solution for customers who do not have a PKI (certificate creation),

- supports the integration of an existing PKI (certificate provision for customer PKI),
- performs automatic certificate deployment.

Customer with PKI

If the customer already has a PKI, the following factors must be considered:

- The existing certificate must be allowed for encryption and signing.
- The existing certificate is an RSA or ECDSA certificate.
- For RSA certificates, the length of the private key must be at least 512 bits.
- For RSA, certificate key lengths up to 4096 bits are supported. For STMI2/4, the maximum key length is 2048 bits.
- The existing certificate is in PEM or PKCS #12 format.

Customer without PKI

If the customer does not have a PKI, the necessary certificates can be created with DLS. The **Automatic SPE Configuration** function in the **Administration** menu is used for this.

Detailed information on DLS

For more information on importing and distributing certificates, see Chapter 7, “Distribution of Certificates using Deployment Service (DLS)”.

18.1.3.2 Signaling encryption

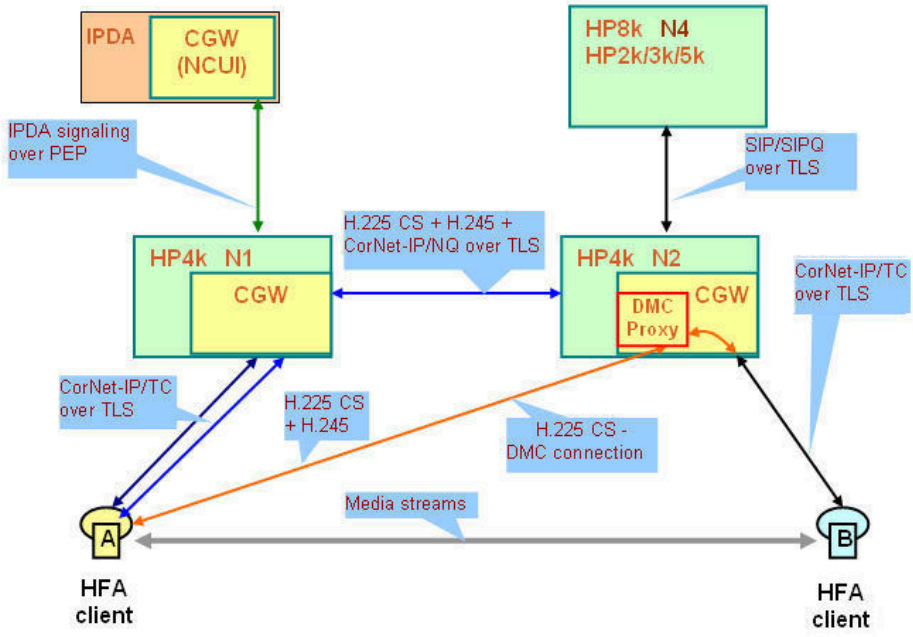


Figure 371: Signaling encryption

The PEP (Proprietary Encryption Protocol) is based on the Master Encryption Key (MEK). PEP is used to protect signaling for connections between a host system and access points (IPDA and OpenScape 4000 SoftGate).

For all other signaling connections, the TLS (Transport Layer Security) protocol is used (e.g. HFA/ SIP phones, IP trunking (H.323/SIP)).

In the case of VoIP signaling paths in a HiPath 4000/OpenScape 4000 network or to partner systems (such as OpenScape Voice), every connection is individually and independently encrypted. TLS/SSL encryptions (SIP/H.323/ HFA) and AES encryption based on pre-shared secrets (IPDA/DMC) is used for this. End-to-end encryption is based on an unbroken encrypted chain of partial signaling links.

- SIP/ HFA/ H.323 connections
- Signaling is secured by TLS connection.
- DMC connections
- Signaling (H.225 is secured with H.235.1(authentication and integrity) for the DMC connections. The "shared-secret" (key) needed is generated by the OpenScape 4000 for every call and distributed to the DMC endpoints. This means that DMC connections are not encrypted, they are only authenticated.

18.1.3.3 TLS Version

Protocols TLSv1.2 and higher are supported. SSLv2, SSLv3 and TLSv1.0 are not permitted due to security issues.

The TLS version can be configured for each interface (HFA/ SIP/ HTTPS) separately in WBM menu:

Configuration > Security > single-click on TLS Ciphers for HFA or SIP or HTTPS

The TLS version, the key agreement method for HFA and SIP in case of TLSv1.2, the encryption algorithm as well as the AES operation mode can be configured. For more information about TLSv1.2, see https://www.ietf.org/rfc/rfc5246.txt.

IMPORTANT: After changing and saving TLS HFA settings, the gateway must be rebooted for the changes to take effect.

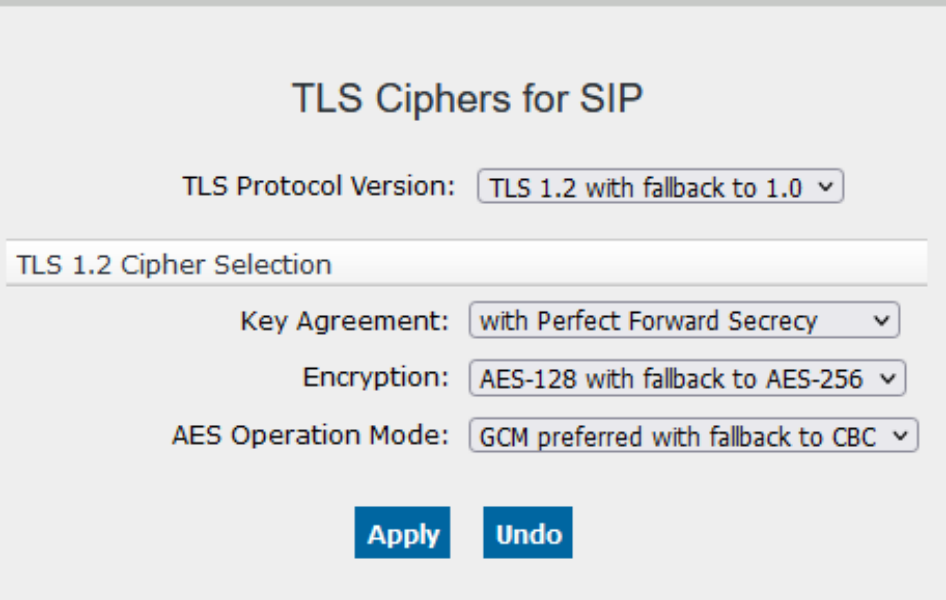


Figure 372: SPE configuration TLS version

Starting with V11R0, TLS version 1.3 is supported on the VoIP Interfaces (HFA and SIP).

NOTICE: TLS1.3 ciphers cannot be configured (fix settings).

18.1.3.4 Certificate Verification Level

During session setup of TLS (Transport Layer Security) the product needs to check the presented identity (certificate) of the opposite side of the communication channel. This checking needs to be done on client side of the TLS session regarding the identity of the server side or on both the client and server side if MTLS (Mutual TLS) is being used.

IMPORTANT: If on the TLS server side Trusted or Full is configured, the certificate from the TLS client is requested (Mutual TLS). If on the gateway subscribers are configure which do not have a certificate, then select on the gateway (which is on this interface TLS server) as Certificate Verification Level None, but on the subscribers (which are TLS clients) Trusted or Full to check the received certificate from the TLS server.

IMPORTANT: For SIP-Q trunks the Certificate Verification Level None is not allowed, because Mutual TLS is mandatory.

IMPORTANT: If for native SIP trunks the gateway has a certificate, the Certificate Verification Level should not be None in order to check the received certificate.

IMPORTANT: For all SIP interfaces on a gateway the Certificate Verification Level is the same. Thus it is not possible to have on one gateway SIP-Q trunking and SIP subscribers without certificates configured.

For the certificate verification three different levels are defined which can be selected:

Configuration > Security > Signaling and Payload Encryption (SPE) > SPE Security Setup > SIP TLS Parameters > Certificate Verification Level.

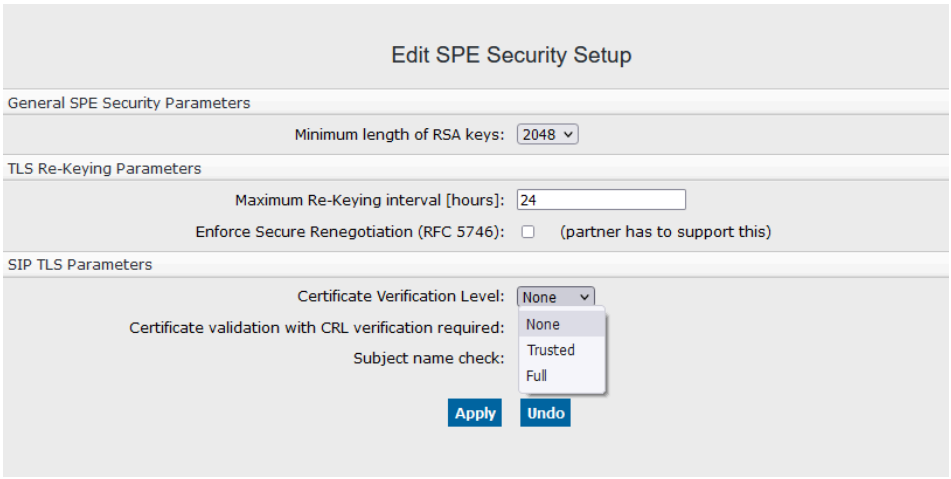


Figure 373: SPE security setup - certificate verification level

- None - no authentication of the remote entity performed.

  The certificate of remote entity is not requested and not checked.
- Trusted - the certificate (including certificate chain) provided by the remote entity is requested and checked for integrity.

  This means that the chain of trust for the digital signature provided by the remote entity ends up in one of the (root) CA-certificates, which are preconfigured for that interface on the product. And that all certificates in the chain are not expired (i.e. current date/time is within the certificate's given validity period).
- Full - the certificate (including certificate chain) provided by the remote entity is requested and checked against the same criteria as in Trusted mode, plus:

  the correct use of all critical extensions is checked (e.g. Basic constraints, Key Usage, Extended Key Usage). If an extension is marked critical and is not recognized, the certificate must be rejected. And the correct use of known extensions not marked as critical is checked (e.g. Basic constraints, Key Usage, Extended Key Usage).

  There are optional checks:

  In level Trusted and Full:

- Certification validation with CRL verification required:

  Check that none certificate in the chain is revoked. This behavior can be changed by checkbox:

  Configuration > Security > Signaling and Payload Encryption (SPE) > SPE Security Setup > SIP TLS Parameters > Certification validation with CRL verification required.

  In level Full:
- Subject name check:

  The end entity’s identity is verified. This behavior can be changed by checkbox:

  Configuration > Security > Signaling and Payload Encryption (SPE) > SPE Security Setup > SIP TLS Parameters > Subject name check.

18.1.3.5 Minimum Length of RSA Keys

Define the minimum length of RSA keys from the remote entity.

The minimum length of RSA keys can be set in the WBM:

WBM > Configuration > Security > Signaling and Payload Encryption (SPE) > SPE Security Setup > General SPE Security Parameters > Minimum length of RSA keys

In case the certificates used for SPE are generated with RSA Signature Algorithm (also known as "RSA certificates"), you must define the minimum length of RSA keys from the remote entity.

18.1.3.6 ECDSA certificates

Starting with OpenScape 4000 V11, you can use SPE certificates generated with ECDSA Signature Algorithm (also known as "ECDSA certificates") for OpenScape 4000 SoftGate and STMIX/STMIY, for SIP and HFA TLS signalling.

For H.323 trunking on OpenScape 4000 SoftGate and STMIX/STMIY, ECDSA certificates are not supported. In this case, traditional RSA certificates must be used.

HG3500 STMI2/4 boards do not support ECDSA certificates. In this case, traditional RSA certificates must be used.

ECDSA has the following advantages over RSA:

- ECDSA provides a significantly lower output length for the same security level as RSA. For example, a 3072-bit RSA signature provides the same level of security as a 256-bit ECDSA signature.
- ECDSA runs faster than RSA.
- ECDSA requires significantly less memory than RSA.

However, you must ensure that the communication partner (e.g. the connected HFA or SIP phones, or a trunking partner like OpenScape Voice or OpenScape SBC) supports ECDSA certificates.

For more information, please refer to the Release Note.

18.1.3.7 Maximum Re-Keying Interval

The TLS/SSL connections remain permanently active and are renewed at regular intervals. The time interval for renegotiation is set in the WBM:

1) WBM > Configuration > Security > Signaling and Payload Encryption (SPE) > SPE Security Setup > TLS Re-Keying Parameters > Maximum Re-Keying interval [hours]

18.1.3.8 Enforce Secure Renegotiation (RFC 5746)

If all remote entities which are connected over TLS support secure renegotiation (RFC 5746), then enable to enforce it. If a remote entity does not support the RFC the renegotiation in some scenarios even the establishment will fail and the connection is released.

This behavior can be changed by checkbox:

1) Configuration > Security > Signaling and Payload Encryption (SPE) > SPE Security Setup > TLS Re-Keying Parameters > Enforce Secure Renegotiation (RFC 5746)

18.1.3.9 Voice Encryption

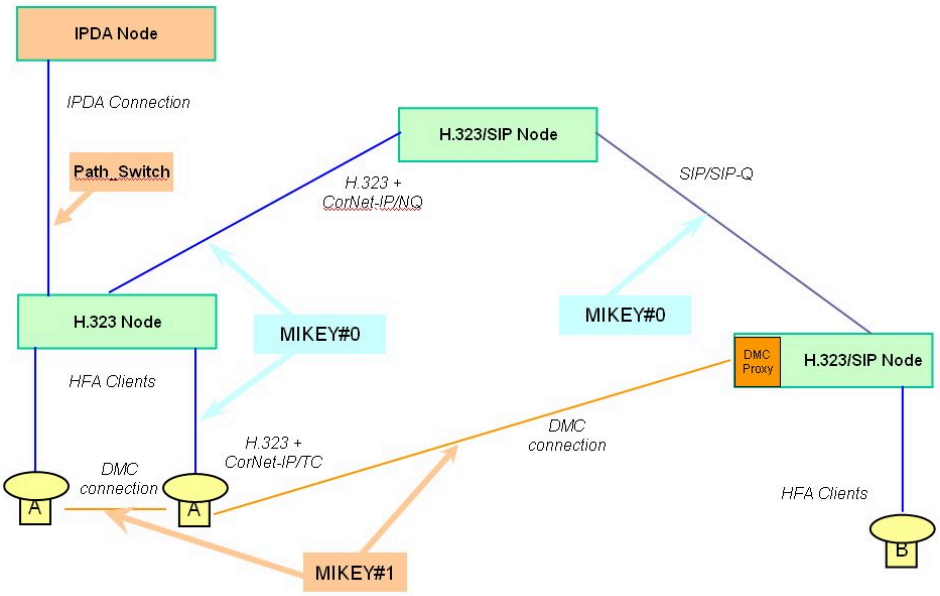


Figure 374: Voice Encryption

SRTP is used for all connections (HFA, SIP, IPDA) for payload encryption. SRTP is based on the Advanced Encryption Standard (AES). Depending on the connection type MIKEY, SDES or MEK is used for encryption.

For this purpose, the endpoints generate (cryptographically) random 128-bit long keys. The key exchange between the participating communication partners takes place in the framework of signaling (see Section 1.3.2, “Signaling encryption”). Depending on the connection type, MIKEY, SDES or

internal OpenScape 4000 mechanisms are used for generating or exchanging keys.

All keys are essentially only used once, i.e. they apply exclusively for the duration of the relevant voice connection. Stations are shown a message as to whether the call is end-to-end encrypted.

IPDA

Because there are no signaling connections for IPDA media streams the usage of MIKEY for key agreement is not possible. Instead following concept will be implemented:

- A database routing (DNIL) generates a call specific SRTP master encryption key and some other SRTP parameters e.g. key length, salt key.
- CallProcessing (CP) conveys this SRTP parameters within the path switching message (PATH_SWITCH) to the involved parties.
- The corresponding IP gateway (STMIx/NCUIx) uses the newly added parameters to generate the same SRTP parameter set as provided by MIKEY and uses it for the payload encryption.

18.1.4 MIKEY (Multimedia Internet KEYing)

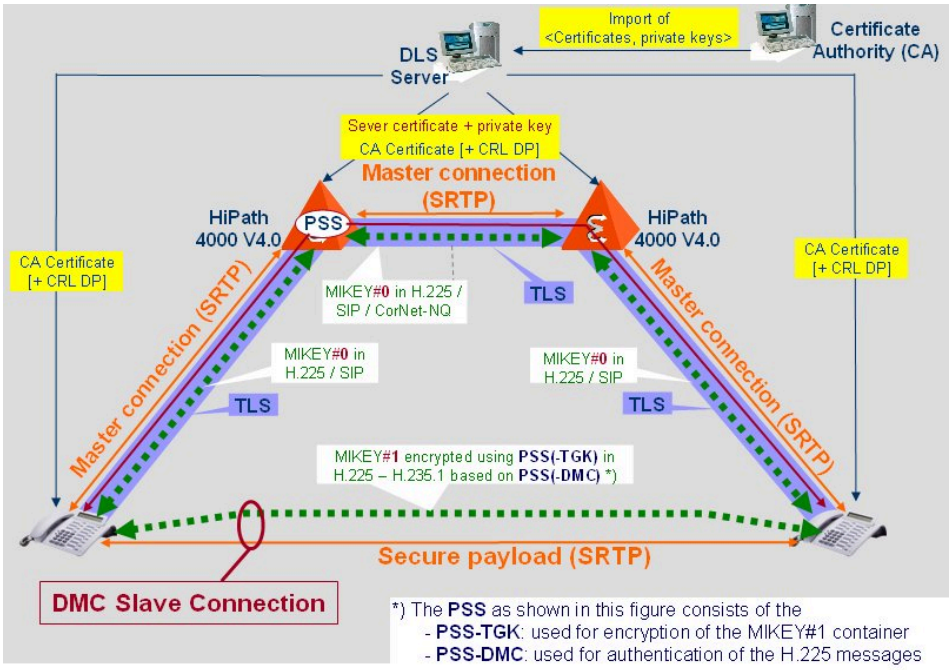


Figure 375: MIKEY

MIKEY is a form of key management for realtime multimedia communication and facilitates the exchange of keys and other security parameters between stations. In VoIP, MIKEY can be used to exchange the master key and other security parameters to ensure secure SRTP transmission between subscribers. MIKEY is described in RFC 3830 “MIKEY: Multimedia Internet KEYing".

18.1.4.1 MIKEY Option 0

MIKEY Option 0 is used if the signaling connection is secured via TLS (Hop-by-Hop). This is ensured for all end-to-end payload streams for the (DMC) master connection of an OpenScape 4000 node in which all sections support signaling encryption.

Thus, no certificates are needed for MIKEY Option 0 itself but the OpenScape 4000 systems or their gateways need an own (server) certificate plus private key for TLS purposes.

All involved entities need the certificate of that/these CAs that issue the certificates for the OpenScape 4000 systems / gateways.

If **CRL** (**C**ertificate **R**evocation **L**ist) checks are required by the configuration, the **CRL DP** (**CRL D**istribution **P**oint - HTTP/LDAP-URL) is required by every endpoint and must therefore also be distributed.

18.1.4.2 MIKEY Option 1

MIKEY Option1 is used for DMC slave connections only as these cannot be secured via TLS.

The required symmetric encryption key needed therefore is generated on a per call basis by the OpenScape 4000 system and distributed to the DMC endpoints via secured network links.

IMPORTANT: No certificates are required by MIKEY Option 1 itself.

18.1.5 Session Description (SDES) Protocol

The "Advanced Encryption Standard (AES)" encryption system can be used for payload encryption on the vHG3500 for SIP connections along with SDES as the encryption attribute. SDES is described in RFC 4568 "Session Description Protocol (SDP) Security Descriptions for Media Streams".

The vHG 3500/STMIX/STMIY supports crypto suites with 80-bit authentication and 32-bit authentication and SRTP with optional m lines.

IMPORTANT: SDES is not supported on the STMI2 or STMI4 boards.

18.1.6 Master Encryption Key (MEK)

The **MEK** (**M**aster **E**ncryption **K**ey) is used for OpenScape Access/Branch/ OpenScape 4000 SoftGate signaling connections.

18.1.7 Secure SIP Connections

Restrictions:

- Payload encryption with SDES is not supported on the STMI board.
- Payload encryption with MIKEY is only supported on SIP-Q trunks.

The security settings that are possible depending on the connection type and gateway type. They are listed in the next table:

Table 85: Possible encryption depending on the connection type and gateway

Security	STMI board	vHG 3500/ STMIX/STMIY
SIP Subscriber		
Signaling encryption	---	---
TLS	ok	ok
Payload encryption	---	---
SRTP with MIKEY - Key Management	---	---
SRTP with SDES - Key Exchange	---	ok
SIP-Q Trunk		
Signaling encryption		
TLS	ok	ok
Payload encryption		
SRTP with MIKEY - Key Management	ok	ok
SRTP with SDES - Key Exchange	---	ok
Native SIP Trunk		
Signaling encryption		
TLS	ok	ok
Payload encryption		
SRTP with MIKEY - Key Management	---	---
SRTP with SDES - Key Exchange	---	ok

18.1.7.1 SIP-Q Trunking

If all requirements for SPE are fulfilled in an OpenScape 4000 system (see Chapter 3, “Configuration”), the gateway will try to set up a secure SIP-Q connection to the partner gateway.

If no SIP-Q profile is activated (see "SIP-Connectivity > Section 3.3, “SIP Trunk Profiles”"), then the payload is encrypted with MIKEY.

If a SIP-Q profile is activated, then payload encryption can be configured on the vHG3500.

WBM > Configuration > Voice Gateway > SIP Trunk Profiles > Select suitable SIP-Q trunk profile > Edit

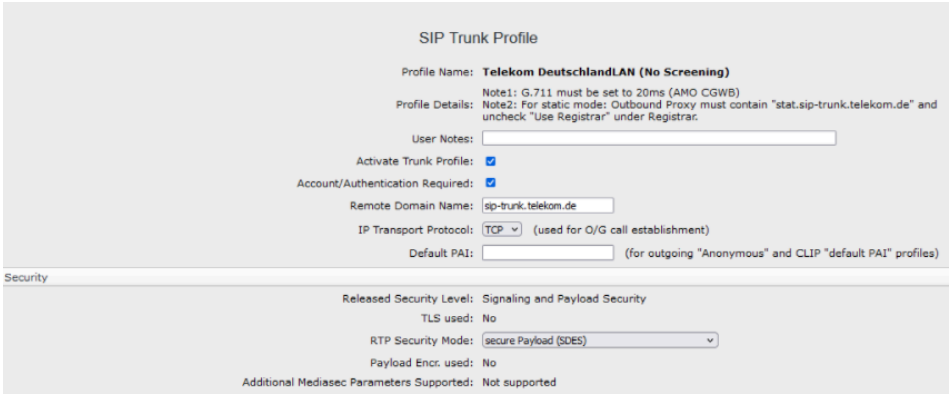


Figure 376: RTP security mode on the vHG3500 for a SIP-Q trunk

18.1.7.2 Native SIP trunking

If an OpenScape 4000 system fulfills all requirements for SPE (see Chapter 3, “Configuration”), the gateway will try to set up a secure SIP connection to the partner gateway if this is configured in the SIP trunk profile (see SIP Connectivity > Section 3.3, “SIP Trunk Profiles”).

For native SIP trunks only SDES as payload encryption mode is supported, if payload encryption is released for the trunk partner. The payload encryption mode cannot be configured.

If an OpenScape 4000 system fulfills all requirements for SPE (see Chapter 3, “Configuration”) and if security is released for the activated SIP trunk partner, then the gateway will try to set up a secure connection to the partner gateway.

NOTICE:

Starting with Software Version V11R0, it is possible to run native SIP trunks with SPE enabled without the need to activate SPE on the full OpenScape 4000 system (ZAND and SIPCO).

For this, SPE needs to be enabled via AMO TDCSU and the corresponding security configuration needs to be done via the WBM.

18.1.7.3 SIP Subscriber

If an OpenScape 4000 system fulfills all requirements for SPE and a configured SIP subscriber registers over TLS at the gateway then payload security is possible, if supported by both sides. For SIP subscribers only SDES as payload encryption mode is supported.

If a SIP subscriber is configured as Cipher with AMO SDAT, then B?

see Section 3.4.2, “SPE for IP Subscribers”.

18.2 Service Information

18.2.1 Restrictions

- The CSTA traffic is clear text protocol and should operate in trusted network environment. If not possible use the Integrated VPN Service of the OS4K Platform / Portal - please see OpenScape 4000 V8, Platform Administration (Portal), Administrator Documentation, chapter 2.5 Integrated VPN Service.
- This feature is **not** compatible with "Signaling and Payload Encryption" in HiPath 4000 V3.0, i.e. encrypted signaling and payload cannot be transmitted in a network with HiPath 4000 V3.0. In a network with HiPath 4000 V3.0, it is not possible to encrypt the trunking path between the two systems. HiPath 4000 V3.0's internal encryption can be activated, however, within HiPath 4000 V3.0.
- If encryption has been activated on an STMI2/NCUI2+ board, the number of configured channels must be 33% less than when encryption is deactivated.
- For the exact number of B channels, see "Gateways HG 3500 and HG 3575", Section 2.6, “B Channels”.
- Up to 240 HFA and SIP subscribers (native or UFIP) can be configured on the common gateway HG 3500 on STMI4 using SPE.
- Up to 120 HFA subscribers can be configured on STMI2 using SPE.
- SPE is not supported on STMI2 for SIP subscriber functionality (native or UFIP).
- T.38 fax streams are not supported for SPE

Table 86: Payload encryption

Feature	STMI2	STMI4	SoftGate/STMIX/ STMIY
Native SIP Trunk	☑*	☑*	☑
SIP-Q Trunk	☑	☑	☑
SIP subscriber - classic	☒	☒	☒
SIP subscriber - UFIP	☒	☑*	☑
Circuit Connectivity (UFIP)	☒	☒	☑

Feature	STMI2	STMI4	SoftGate/STMIX/ STMIY
HFA subscriber	☑**	☑	☑
H323 Trunk	☒	☒	☒
* Only signaling encryption supported. SDES is supported on SoftGate/STMIX/STMIY only.			
** Maximum of 120 SPE subscribers supported on STMI2 boards.			

IMPORTANT: Starting with V10R0 the support for STMI2 will not be offered anymore. The replacement for STMI2 is STMIX/ STMIY.

18.2.2 Generation of a Certificate

With the function **Automatic SPE Configuration** of the DLS it is possible to generate a certificate and to distribute it to the gateways and endpoints. This is especially useful when there is no client PKI. For more information please refer to Chapter 8, “AutoSPE Configuration (DLS)”.

Alternatively, a certificate can be generated on a common gateway board.

For manually generated certificates (PKCS#12 file) in case of STMI4/STMIX/ STMIY/NCUI4 boards, the signature algorithm SHA-1 or SHA-2 (recommended) can be used.

Term SHA-2 (SHA2) means the whole family of SHA-2 algorithms, i.e. SHA-256, SHA-384, SHA-512 and SHA-224

IMPORTANT: Supported Key Length is 4096 bit, but for STMI2/4 boards is Maximum Key Length 2048 bit.

18.2.3 Supported Certificates

The following certificates (X.509v3) can be imported:

- CA certificates (*.crt, *.cer) from the certification authority
- Certificates in the format **P**ublic **K**ey **C**ryptography **S**tandards #12 (PKCS #12) (*.p12)
- Certificates in the format X.509 PEM

An expired certificate should not be reloaded. If a certificate expires in the course of implementation, a HISTA message is issued along with an error message (F5881 with Error Cause: CERTIFICATE EXPIRED). The system may no longer function in secure mode with certification verification level Trusted or Full. Phones may not register to boards, trunks may not work. Security may be deactivated until the certificates will be renewed (see Section 2.4, “Renew a Certificate”).

IMPORTANT: Certificates should be replaced when their validity expires.

Certificate chaining is supported. CA certificate chains can either be imported as separate files (one by one), or a CA certificate chain can be imported directly, with up to 3 CA certificates in PEM format. The order of the CA certificate chain import or in the PEM file does not have any effect.

18.2.4 Renew a Certificate

Expired certificates should be renewed.

If exchanging SPE certificates to OSV, please refer to the INF-14-000180 MOP (Method of Procedure) to updated used certificates:

https://www.g-dms.com/livelink/livelink.exe/view/INF-14-000180

18.2.5 Board Replacement

If certificates are lost (for example, when loading a board following board replacement), they can be reloaded by means of the customary "Backup&Restore" mechanism (logical DATA Backup). The same applies to the MEKs during access point/OpenScape 4000 SoftGate encryption.

IMPORTANT: Only a valid certificate should be loaded on the gateway.

18.2.6 STMI Board

STMI board is supported in SPE. It applies if a backup was made by means of the customary Backup&Restore mechanism (logical DATA Backup). This ensures that the board will take the same certificates and configuration like the active board.

Restriction

Secure connections that are configured using the SIP trunk profiles are not supported.

18.2.7 Activating/Deactivating SPE for Subfunctions in the System

SPE subfunctions can be deactivated - and in some cases even reactivated - without a restart. This allows service personnel to deactivate specific SPE sub functions in problem situations, on the one hand, to verify if the problem is caused by SPE and, on the other hand, to pinpoint the cause of the fault. For more information please refer to the following sections:

- Section 3.2, “Activation / Deactivation of SPE for Gateways with AMO CGWB”
- Section 3.3, “Trunk SPE Activation / Deactivation”

- Section 3.4, “Subscriber SPE Activation / Deactivation”
- Section 3.5, “Activation / Deactivation of SPE for Access Points”
- Section 3.6, “OpenScape 4000 SoftGate SPE Activation / Deactivation”

18.2.8 Connecting Gateway

There are several options for connecting a gateway.

Table 87: Connecting Gateways

Connection to gateway via ...	STMI	vHG 3500
V24 connection: With this connection it is possible to collect data and communicate with the board before startup is complete.	yes	no
SSH: With a SSH client (as TeraTerm, Putty) it is possible to connect when the IP communication is available.	yes	no
SSH via HiPath 4000 Assistant under **Expert Mode > HG 35xx Telnet / SSH** on an active board, if HiPath 4000 Assistant has IP routing access.	yes	no
WBM connection on an active board if IP routing access is possible.	yes	yes

IMPORTANT: With the first three (1-3) connections it is possible to "reset bootstrapping" on the active STMI boards.

18.2.9 SPE in Connection with Mobile HFA

18.2.9.1 Terminology used

SPEcapable client:	A client actually logged in as TRADITIONAL client but that is SPE capable and provided with all credential and configurations for connecting as **SECURE** or **CIPHER** client.
TRADITIONAL client:	A client actually logged in as TRADITIONAL client and **NOT SPE** capable at all (e.g. optiPoint 500).

	**SECURE** and **CIPHER** client
	**TRADITIONAL** client
	SPEcapable client

18.2.9.2 Prerequisite

The **same protocol** (TCP or TLS) must be used for the connection to the gateway **for** the **VISITED and HOME station** in order to avoid that a VISITED station using TCP can disconnect a HOME station using TLS (Dos attacks).

A HOME station connected via TCP that is disconnected by a VISITED station connected via TLS is unable to disconnect the VISTED station and therefore cannot reconnect to its gateway again.

18.2.9.3 Scenarios with Homogenous HiPath 4000/OpenScape 4000 Network with SPE Enabled

IMPORTANT: Valid as of HiPath 4000 V4!



	Visted		
Home	Secure/Cipher	Traditional	SPEcapable
Secure/Cipher		does not work	critical[15] [16]
Traditional	no problems[17]	no problems	no problems
SPEcapable	no problems[18]	no problems	no problems

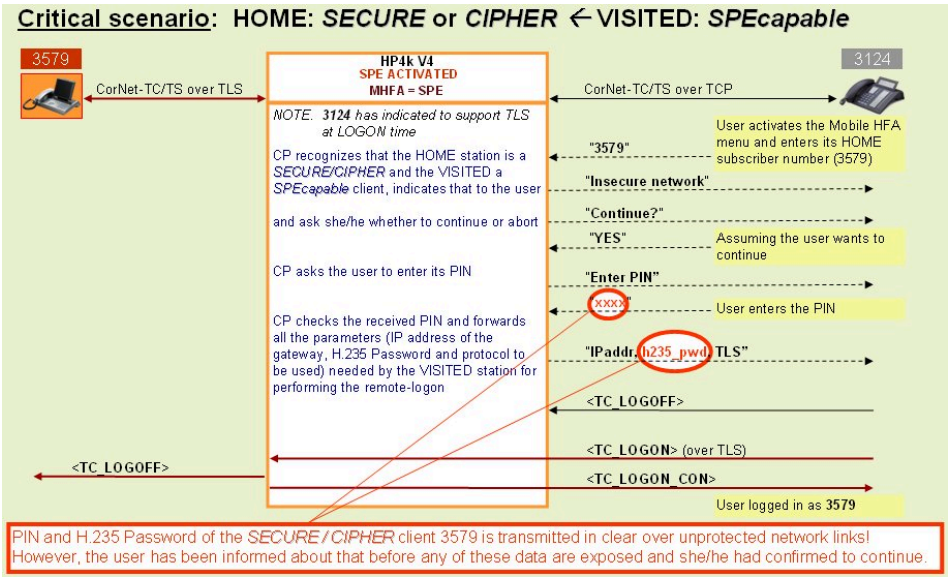
IMPORTANT: The VISITED station already gets the protocol to be used for connecting to the HOME gateway from the SPE Mobile HFA call flows.

15 SPEcapable clients have to use TLS when acting as VISITED stations for a SECURE / CIPHER client.

16 This scenario is critical due to **PIN and H.235 password transfer over insecure network links**.

17 Secure/Cipher clients have to use TCP when acting as visited stations for a traditional client.

18 Secure/Cipher clients have to use TCP when acting as visited stations for a SPEcapable client.



18.2.9.4 Scenarios within a Network with SPE activated Nodes and SPE deactivated Nodes

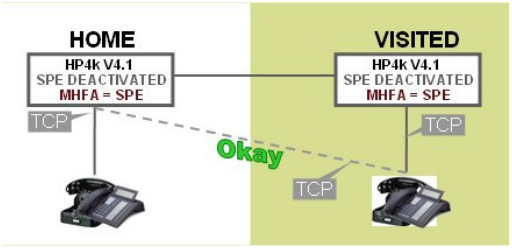
HOME and VISITED: SPE deactivated and TRADITIONAL/SPEcapable

HOME:

- SPE deactivated
- phones: TRADITIONAL/SPEcapable

VISITED:

- SPE deactivated
- phones: TRADITIONAL/SPEcapable



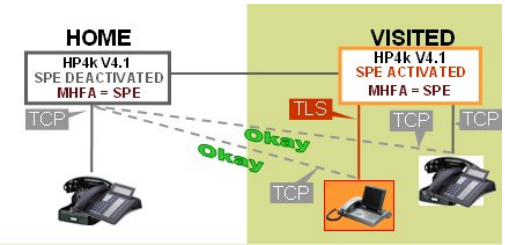
HOME: SPE deactivated and TRADITIONAL/SPEcapable, VISITED: SPE activated and TRADITIONAL/SPEcapable and SECURE/CIPHER

HOME:

- SPE deactivated
- phones: TRADITIONAL/SPEcapable

VISITED:

- SPE activated
- phones: TRADITIONAL/SPEcapable and SECURE/CIPHER



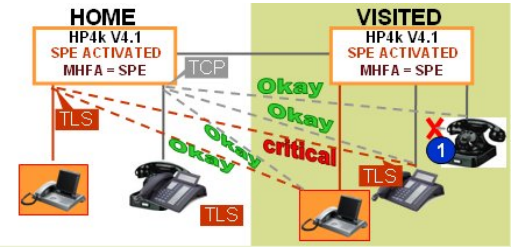
HOME: SPE activated and TRADITIONAL/SPEcapable and SECURE/CIPHER, VISITED: SPE activated and TRADITIONAL and SPEcapable and SECURE/CIPHER

HOME:

- SPE activated
- phones: TRADITIONAL/SPEcapable and SECURE/CIPHER

VISITED:

- SPE activated
- phones: TRADITIONAL and SPEcapable and SECURE/CIPHER



1	A **TRADITIONAL** client (without SPE support) is never accepted as a VISITED station for a **SECURE** or **CIPHER** client. Call processing on the VISITED switch is aware of this and rejects the remote login attempt with "Remote Login not possible" (before asking the user to enter his/her PIN).

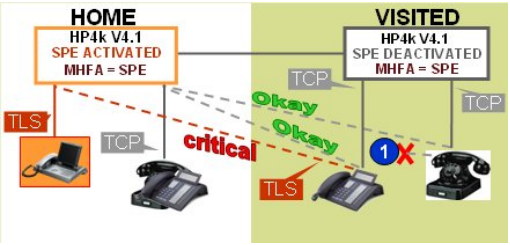
HOME: SPE activated and TRADITIONAL/SPEcapable and SECURE/CIPHER, VISITED: SPE activated and TRADITIONAL and SPEcapable

HOME:

- SPE activated
- phones: TRADITIONAL/SPEcapable and SECURE/CIPHER

VISITED:

- SPE activated
- phones: TRADITIONAL and SPEcapable



1	A **TRADITIONAL** client (without SPE support) is never accepted as a VISITED station for a **SECURE** or **CIPHER** client. Call processing on the VISITED switch is aware of this and rejects the remote login attempt with "Remote Login not possible" (before asking the user to enter his/her PIN).

18.2.9.5 Network Wide Usage of Mobile HFA

If **TRADITIONAL** clients are accepted both as HOME and VISITED stations on a HiPath 4000 with SPE activated, this offers significant improvements in the usage of the Mobile HFA feature within homogenous HiPath 4000[19]/OpenScape 4000 (with or without SPE activated) networks.

IMPORTANT: Mobile HFA **cannot** be used in networks between HiPath 4000 (as of version 4)/OpenScape 4000 systems with SPE activated and HiPath 4000 V2.0 / V3.0.

18.3 Configuration

Before configuring the **Signaling and Payload Encryption (SPE)** feature in an OpenScape 4000 system, make sure that all prerequisites are met (see Section 3.1, “Prerequisites”Once this has been assured, you can configure the individual functions as required.

Short overview of the necessary steps for activation / deactivation of the SPE feature on an OpenScape 4000 system.

1) Activation / deactivation of SPE for subscriber gateways

2) Activation of this feature will encrypt the signaling / payload between endpoints (subscriber gateways, vHG 3500, HFA/ SIP subscriber, etc.) with TLS/SRTP. This is configured with the PKI (**P**ublic **K**ey **I**nfrastructure) process. Activation / deactivation in the system is performed with AMO ZANDE. Make sure to use the correct secure port: TLSP (for HFA and H323) / PORTTLS1 (for SIP) parameter from AMO CGWB. The default values are 4061 / 5061. For more information, please refer to Section 3.2, “Activation / Deactivation of SPE for Gateways with AMO CGWB”.

IMPORTANT: The key material for trunking and HFA is exchanged for gateways in an Access Point/OpenScape 4000 SoftGate via the HSR connection. If the HSR connection is not secure then the key material is exposed in clear text. SPE must therefore also be activated for OpenScape 4000 SoftGate/IPDA Access Points (see Section 3.5, “Activation / Deactivation of SPE for Access Points”).

3) Activation / deactivation of SPE for trunks

[19] As of HiPath 4000 V4

4) Activation of this feature will encrypt the signaling / payload on the trunk.

   Activation / deactivation is performed by changing the security mode in AMO TDCSU, AMO GKREG. For more information, please refer to Section 3.3, “Trunk SPE Activation / Deactivation”.
5) Activation / deactivation of SPE for subscribers
6) Activation of this feature will encrypt the signaling / payload between subscribers and the gateways. Activation / deactivation is performed by changing the security mode of the subscribers with AMO SDAT / WBM. For more information, please refer to Section 3.4, “Subscriber SPE Activation / Deactivation”.
7) Activation / deactivation of SPE for access points
8) Activation will encrypt the signaling / payload between established HSR connections with PEP (**P**roprietary **E**ncryption **P**rotocol) / SRTP. This feature is configured by the SPE administration client process. Activation / deactivation in the system is performed with AMO SIPCO. For more information, see Section 3.5, “Activation / Deactivation of SPE for Access Points”.
9) Activation / deactivation of SPE for OpenScape 4000 SoftGate
10) Activation will encrypt the signaling / payload between established HSR connections with PEP (**P**roprietary **E**ncryption **P**rotocol) / SRTP. This feature is configured by the MEK administration client process. For more information please see Section 3.6, “OpenScape 4000 SoftGate SPE Activation / Deactivation”.

18.3.1 Prerequisites

System

The following prerequisites must be met before you can activate **SPE** in a system:

- Depending on the certificate verification level and all (v)HG 3500 gateways in this system may be assigned SPE certificates and/ or at least one CA certificate (see Section 1.3.4, “Certificate Verification Level”).
- All NCUI2 boards must be replaced by NCUI2+ or NCUI4.
- All (v)NCUI boards must have Master Encryption Keys (MEKs) configured.
- All components must be synchronized via the NTP server.

IMPORTANT: Do not use Assistant as an NTP server for IP phones, as it is not supported. It has a limited number of buffers which makes it unreliable in large deployments.

18.3.2 Activation / Deactivation of SPE for Gateways with AMO CGWB

Activation of SPE on the gateways will encrypt communication between the endpoints with TLS / SRTP. For information on certificate distribution / activation on the /gateways, please see Chapter 6, “Distribution of Certificates with the WBM of the Gateway”.

IMPORTANT: The key material for trunking and HFA is exchanged for gateways in an Access Point/OpenScape 4000

SoftGate via the HSR connection. If the HSR connection is not encrypted, the key material will be displayed in plain text. SPE must therefore also be activated for Access Points/OpenScape 4000 SoftGate (see Section 3.5, “Activation / Deactivation of SPE for Access Points” or Section 3.6, “OpenScape 4000 SoftGate SPE Activation / Deactivation”).

All components should be time synchronized otherwise activation of SPE between components may fail.

For better protection against errors in case of losing certificates, a backup server should be configured for each board and also a backup should be made for every new certificate that is installed on the board by means of the customary "Backup&Restore" mechanism (logical DATA Backup).

The following steps have to be performed for activating SPE on a gateway:

1) Deploy certificates for each board that need to be secure. Bootstrapping should be made (in case DLS is used for deployment of certificates) before the distribution of the certificates. For more information, please refer to Chapter 7, “Distribution of Certificates to Gateways” For information on connection options with gateways, please refer to Section 2.8, “Connecting Gateway”.

- Activation of SPE for trunks and IP subscribers. For more information, please refer to Chapter 3, “Trunk SPE Activation / Deactivation” and Chapter 3, “Subscriber SPE Activation / Deactivation”.
- Activation of SPE for gateways with AMO ZANDE.

Activation / deactivation of SPE for gateways:

```
CHANGE-ZANDE:TYPE=SECURITY,SPESUPP=YES;
```

If parameter **SPESUPP** is set to **YES**, SPE is enabled!

Parameters:

SPESUPP (YES/ NO):	Activates SPE for this system.

IMPORTANT: You must perform a hard restart on the system after you have activated SPE. Do not forget to make an update of the system before the restart EXEC-UPDAT:UNIT=BP,SUSY=ALL;. If you have a duplex system you have to perform the following command on both processors simultaneously (at the same time). This means all LTUs and APs will restart! `EXEC-REST:TYPE=UNIT,UNIT=BP,RSLEVEL=HARD;`

A default security level that is used when configuring new trunks or stations can be defined with AMO ZANDE:

```
CHA-ZANDE:TYPE=SECURITY,SECTDMSB=<sec_level_subs_TDM>,

SECTDMTR=<sec_level_trunks TDM>,SECIPSB=<sec_level_ip_subs>,
```

SECIPTR=<sec_level_IP_trunks>;

Parameters:

SECTDMSB (TRADITIO/SECURE):	Security level for TDM subscribers. Default value : **TRADITIO**
SECTDMTR (TRADITIO/EXTSECUR):	Security level for TDM trunks Default value : **TRADITIO**
SECIPSB (STANDARD/SECURE/CIPHER):	Security level for IP subscribers Default value : **SECURE**:
SECIPTR (TRADITIO/STANDARD/SECURE/ EXTSECUR):	Security level for IP trunks Default value : **SECURE**:
SECLVDSP **YES / NO**	Security terminal display Default value : **N**

18.3.3 Trunk SPE Activation / Deactivation

18.3.3.1 SPE for Analog / TDM Trunks

IMPORTANT: Activation / Deactivation of SPE for analog / TDM trunks requires a restart of the board.

IMPORTANT: The configuration of analog and TDM trunks has no effect on their behavior. The only purpose of this configuration is the determination of end-to-end encryption points. The connection is then treated by call processing as if encrypted but it isn't really encrypted. The other side of the trunk must also be an OpenScape 4000 configured as EXTSECUR. Note that SPE activation on CO trunks (both digital and analog) is not possible.

CHANGE-TDCSU:PEN=<port equipment number>, SECLEVEL=<security_level>;

The security level (**SECLEVEL**) can feature the following values:

TRADITIO:	Nonsecure trunk Default value for TDM trunks

EXTSECUR :	This trunk is encrypted by a mechanism (such as VPN) that is different from this feature. This trunk is therefore treated by call processing as "fully encrypted" but not encrypted by OpenScape 4000. The other side of the trunk must also be an OpenScape 4000 configured as EXTSECUR.

18.3.3.2 SPE for IP Trunking

IMPORTANT: Depending on the gateway and the trunk type, various payload encryptions are possible for IP trunking (see Table 1, “Signaling and payload encryption (IP environment)”).

IMPORTANT: Activation / Deactivation of SPE for IP trunking requires a restart of the board.

The following steps have to be performed:

1) **Configuring the trunk**
2) The AMO TDCSU is used for basic trunk configuration:

   CHANGE-TDCSU:PEN=<port equipment number>,**SECLEVEL**=<security_level>;

   Security level (**SECLEVEL**) can feature the following values:

TRADITIO:	Nonsecure trunk Default value for TDM trunks
STANDARD	SRTP (payload encryption) is not supported, only signaling encryption (TLS-secured)
SECURE	Full encryption (SRTP + TLS-secured) Default value for IP trunks
EXTSECUR :	This trunk is encrypted by a mechanism (such as VPN) that is different from this feature. This trunk is therefore treated by call processing as "fully encrypted" but not encrypted by OpenScape 4000. The other side of the trunk must also be an OpenScape 4000 configured as EXTSECUR.

IMPORTANT: The same security level will be set for all trunks associated with a board.

3) **Configuring the gateway**

a) Configuring the remote gateway (**EXTGW**)

CHANGE-GKREG:GWNO:=<gateway_number>,**SECLEVEL=<SECURITY_level>**;

Configuring the internal (local) gateway (**INTGW**)

The security level of the internal gateway is set via AMO TDCSU (with the command `CHANGE-TDCSU`). With AMO GKREG you can only display the actual security level but can't modify it. To modify the security level use AMO TDCSU.

If the security level configured with the AMO TDCSU is not displayed for the internal gateway in AMO GKREG, this could be because:

a) SPE is not active (check with AMO ZANDE) or

- certificates are not available, faulty or expired (for more information, refer to the WBM/DLS and AMO HISTA, AMO BCSU, AMO SDSU).

AMO BCSU

Detailed information can be found in AMO BCSU with the command `DISPLAY-BCSU:TYPE=TBL,LTG=<ltg>,LTU=<ltu>,SLOT=<slot>;` in the **SECURITY STATUS** section.

AMO SDSU

Detailed information can be found in AMO SDSU with the command `DISP-SDSU;`. Refer to **SECURITY LEVEL** in the output.

```
<DISPLAY-SDSU:STATUS=ALL,TYPE=PEN,LEVEL=PER3,LTG=1,LTU=1,SLOT=14;
DISPLAY-SDSU:STATUS=ALL,TYPE=PEN,LEVEL=PER3,LTG=1,LTU=1,SLOT=14;
H500:  AMO SDSU  STARTED
  LTG1  (PERIPHERY)
  ------
  MOUNTING LOCATION    MODULE NAME     BDL BD(#=ACT)  STATUS
  -------------------  LTG    1 ---------------------- READY
  -AP370013-----SG  1  LTU    1 ---------------------- READY
  **  .LTG 1.LTU 1.014 STMI4           A   Q2324-X510 READY
                       LAN CONN.   .   . . . . . . . .  READY
                       LINK SIGNAL ETHERNET  . . . .      PRESENT
                       LAN SPEED   . . . . . . . . .  100 MBIT/S
                       LAN INTERFACE . . . . . . . .  FDX (FULL DUPLEX)
                       CCT          FUNCTION BLOCK
                       0            HG3570_2
                       1   - 2      HG3550_2
                       3   - 12     HG3530_2
                       13  - 22     HG3540_2
              CCT  LINE         STNO  SI BUS TYPE
              001  2401                 PP NW         READY
                MULTLINE 10 . . . . . . . . . . . . . .READY
                000 NO CONN
                001 NETWORK SUBUNIT . TMD CONN ISDN  READY
                (ALT_ROUT: N)       (HG3550IP)
                  LINE: 2401 STNO:              SI:
                    001 . . . . . . . . TMD CONN ISDN  READY
                002 NETWORK SUBUNIT . TMD CONN ISDN  READY
                (ALT_ROUT: N)       (HG3550IP)
                  LINE: 2401 STNO:              SI:
```

```
      001 . . . . . . . . TMD CONN ISDN  READY
  003 NETWORK SUBUNIT . TMD CONN ISDN  READY
  (ALT_ROUT: N)       (HG3550IP)
    LINE: 2401 STNO:              SI:
      001 . . . . . . . . TMD CONN ISDN  READY
  004 NETWORK SUBUNIT . TMD CONN ISDN  READY
  (ALT_ROUT: N)       (HG3550IP)
    LINE: 2401 STNO:              SI:
      001 . . . . . . . . TMD CONN ISDN  READY
  005 NETWORK SUBUNIT . TMD CONN ISDN  READY
  (ALT_ROUT: N)       (HG3550IP)
    LINE: 2401 STNO:              SI:
      001 . . . . . . . . TMD CONN ISDN  READY
  006 NETWORK SUBUNIT . TMD CONN ISDN  READY
  (ALT_ROUT: N)       (HG3550IP)
    LINE: 2401 STNO:              SI:
      001 . . . . . . . . TMD CONN ISDN  READY
  007 NETWORK SUBUNIT . TMD CONN ISDN  READY
  (ALT_ROUT: N)       (HG3550IP)
    LINE: 2401 STNO:              SI:
      001 . . . . . . . . TMD CONN ISDN  READY
  008 NETWORK SUBUNIT . TMD CONN ISDN  READY
  (ALT_ROUT: N)       (HG3550IP)
    LINE: 2401 STNO:              SI:
      001 . . . . . . . . TMD CONN ISDN  READY
  009 NETWORK SUBUNIT . TMD CONN ISDN  READY
  (ALT_ROUT: N)       (HG3550IP)
    LINE: 2401 STNO:              SI:
      001 . . . . . . . . TMD CONN ISDN  READY
  010 NETWORK SUBUNIT . TMD CONN ISDN  READY
  (ALT_ROUT: N)       (HG3550IP)
    LINE: 2401 STNO:              SI:
      001 . . . . . . . . TMD CONN ISDN  READY
  011 NO CONN
  012 NO CONN
  013 NO CONN
  014 NO CONN
  015 NO CONN
  016 NO CONN
  017 NO CONN
  018 NO CONN
  019 NO CONN
  020 NO CONN
  021 NO CONN
  022 NO CONN
  023 NO CONN
  024 NO CONN
  025 NO CONN
  026 NO CONN
  027 NO CONN
  028 NO CONN
  029 NO CONN
  030 NO CONN
  SECURITY LEVEL  . . . . . . . (CONF.)  "SECURE"
                                (ACT.)   "SECURE"
CCT  LINE         STNO  SI BUS TYPE
```

```
002  2402                                NOGEN
003  2403                 OPTI ONLY      READY
  MULTLINE 8. . . . . . . . . . . . . .READY
  000 NO CONN
  001 SUBUNIT . . . . . DIGITE MAIN      READY
  (ALT_ROUT: N)       (OPTIIP  )
    LINE: 2470 STNO: 24054         SI:VCE
      001 . . . . . . . . DIGITE SUB A   READY
      002 . . . . . . . . DIGITE SUB A   READY
      003 . . . . . . . . DIGITE SUB C   READY
  002 NO CONN
  003 NO CONN
  004 NO CONN
  005 NO CONN
  006 NO CONN
  007 NO CONN
  008 NO CONN
  SECURITY LEVEL  . . . . . . . (CONF.)  "SECURE"
                                (ACT.)   "TRADITIO"
CCT  LINE         STNO  SI BUS TYPE
004  2404                 OPTI ONLY      READY
  MULTLINE 8. . . . . . . . . . . . . .READY
  000 NO CONN
  001 SUBUNIT . . . . . DIGITE MAIN      READY
  (ALT_ROUT: N)       (OPTIIP  )
    LINE: 2471 STNO: 24055         SI:VCE
      001 . . . . . . . . DIGITE SUB A   READY
      002 . . . . . . . . DIGITE SUB A   READY
      003 . . . . . . . . DIGITE SUB C   READY
  002 NO CONN
  003 NO CONN
  004 NO CONN
  005 NO CONN
  006 NO CONN
  007 NO CONN
  008 NO CONN
  SECURITY LEVEL  . . . . . . . (CONF.)  "CIPHER"
                                (ACT.)   "CIPHER"
CCT  LINE         STNO  SI BUS TYPE
005  2405                 OPTI ONLY      READY
  MULTLINE 8. . . . . . . . . . . . . .READY
  000 NO CONN
  001 SUBUNIT . . . . . DIGITE MAIN      READY
  (ALT_ROUT: N)       (OPTIIP  )
    LINE: 2472 STNO: 24056         SI:VCE
      001 . . . . . . . . DIGITE SUB A   READY
      002 . . . . . . . . DIGITE SUB A   READY
      003 . . . . . . . . DIGITE SUB C   READY
  002 NO CONN
  003 NO CONN
  004 NO CONN
  005 NO CONN
  006 NO CONN
  007 NO CONN
  008 NO CONN
  SECURITY LEVEL  . . . . . . . (CONF.)  "SECURE"
```

```
                                (ACT.)   "SECURE"
CCT  LINE         STNO  SI BUS TYPE
006  2406                 OPTI ONLY     READY
  MULTLINE 8. . . . . . . . . . . . . .READY
  000 NO CONN
  001 SUBUNIT . . . . . DIGITE MAIN      TRS
  (ALT_ROUT: N)       (OPTIIP  )
    LINE: 2193 STNO: 24057         SI:VCE
      001 . . . . . . . . DIGITE SUB A   UNACH
      002 . . . . . . . . DIGITE SUB A   UNACH
      003 . . . . . . . . DIGITE SUB C   UNACH
  002 NO CONN
  003 NO CONN
  004 NO CONN
  005 NO CONN
  006 NO CONN
  007 NO CONN
  008 NO CONN
  SECURITY LEVEL  . . . . . . . (CONF.)  "SECURE"
                                (ACT.)   "UNKNOWN"
CCT  LINE         STNO  SI BUS TYPE
007  2407                 OPTI ONLY     READY
  MULTLINE 8. . . . . . . . . . . . . .READY
  000 NO CONN
  001 SUBUNIT . . . . . DIGITE MAIN      TRS
  (ALT_ROUT: N)       (OPTIIP  )
    LINE: 2436 STNO: 24058         SI:VCE
      001 . . . . . . . . DIGITE SUB A   UNACH
      002 . . . . . . . . DIGITE SUB A   UNACH
      003 . . . . . . . . DIGITE SUB C   UNACH
  002 NO CONN
  003 NO CONN
  004 NO CONN
  005 NO CONN
  006 NO CONN
  007 NO CONN
  008 NO CONN
  SECURITY LEVEL  . . . . . . . (CONF.)  "SECURE"
                                (ACT.)   "UNKNOWN"
CCT  LINE         STNO  SI BUS TYPE
008  2408                                NOGEN
009  2409                                NOGEN
010  2410                                NOGEN
011  2411                                NOGEN
012  2412                                NOGEN
013  2413                 PP S0          READY
  ELEM DEV. . . . . . SB FCT TERM        READY
  (ALT_ROUT: N)       (S0PP    )
    LINE: 2413 STNO: 24060         SI:VCE
  SECURITY LEVEL  . . . . . . . (CONF.)  "SECURE"
                                (ACT.)   "TRADITIO"
CCT  LINE         STNO  SI BUS TYPE
014  2414                 PP S0          READY
  ELEM DEV. . . . . . SB FCT TERM        READY
  (ALT_ROUT: N)       (S0PP    )
    LINE: 2414 STNO: 24061         SI:VCE
```

```
  SECURITY LEVEL  . . . . . (CONF.)   "SECURE"
                            (ACT.)    "UNKNOWN"
CCT  LINE         STNO  SI BUS TYPE
015  2415                             NOGEN
016  2416                             NOGEN
017  2417                             NOGEN
018  2418                             NOGEN
019  2419                             NOGEN
020  2420                PP S0        READY
  ELEM DEV. . . . . SB FCT TERM       READY
  (ALT_ROUT: N)       (S0PP    )
    LINE: 2420 STNO: 24067         SI:VCE
  SECURITY LEVEL  . . . . . (CONF.)   "SECURE"
                            (ACT.)    "UNKNOWN"
CCT  LINE         STNO  SI BUS TYPE
021  2421                PP S0        READY
  ELEM DEV. . . . . SB FCT TERM       READY
  (ALT_ROUT: N)       (S0PP    )
    LINE: 2421 STNO: 24068         SI:VCE
  SECURITY LEVEL  . . . . . (CONF.)   "SECURE"
                            (ACT.)    "UNKNOWN"
CCT  LINE         STNO  SI BUS TYPE
022  2422                             NOGEN
```

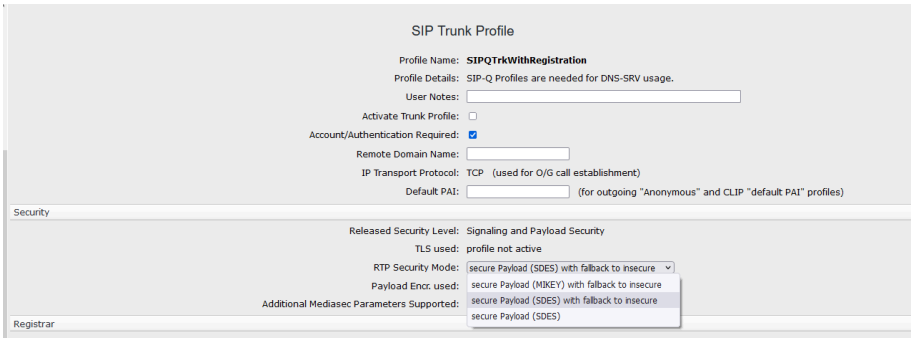
4) Security parameters of SIP trunk profile

A SIP trunk profile can be activated for SIP-Q trunks and must be activated for native SIP trunks (see “SIP Connectivity > Section 3.3, “SIP Trunk Profiles””).

- SIP-Q trunk profile
- If a SIP-Q trunk profile is used, **RTP security mode** can be configured in vHG 3500.

  WBM > Configuration > Voice Gateway > SIP Trunk Profiles > Select Profile > Edit

  The default value is secure Payload (MIKEY) with fallback to insecure.



SIP trunk profile, SIP-Q, security parameters

- Native SIP trunk profile
- For native SIP trunks only SDES as payload encryption mode is supported, if payload encryption is released for the trunk partner. The payload encryption mode cannot be configured. Because SDES is not supported on STMI boards, no payload encryption is possible.

18.3.3.3 Deactivation of SPE for SIP-Q / Native SIP Trunking

Deactivating SPE

IMPORTANT: SPE can be deactivated without reboot.

The reduction of the security level from **SECURE** to **TRADITIO** for a partner gateway (**AMO GKREG**, parameter **SECLEVEL**) means that all subsequent calls are set up via TCP or UDP. SPE is therefore deactivated for all subsequent calls to the relevant partner gateway.

The ongoing calls are maintained on TLS just as the TLS connection is maintained, even if all associated calls are ended. gateway itself also remains in secure mode.

IMPORTANT: If you want to deactivate SPE for incoming calls from this partner gateway, you must also reconfigure the AMO GKREG at the partner system (parameter **SECLEVEL=TRADITIO**).

Activating SPE

SPE can be activated without reboot.

As for deactivation, again with the AMO-GKREG.

IMPORTANT: gateway must already be in secure mode. Do not overlook possible changes in the partner system when performing activation (AMO GKREG, **SECLEVEL=SECURE**).

18.3.4 Subscriber SPE Activation / Deactivation

Both the HFA/ SIP subscribers and the OpenScape 4000 system have to be configured for signaling and payload encryption.

18.3.4.1 SPE for Analog/TDM Endpoints

IMPORTANT: The configuration of analog and TDM endpoints has no effect on their behavior. The only purpose of this configuration is the determination of end-to-end encryption. The connection is then treated by call processing as if encrypted but it isn't really encrypted.

```
CHA-SDAT:STNO=<station number>,TYPE=DATA1,CLASSSEC=<security_level>;
```

The security level (**CLASSSEC**) can feature the following values:

TRADITIO:	Nonsecure endpoint Default value.

SECURE	Full encryption (SRTP + TLS-secured) The phone is secured by external means but not encrypted by OpenScape 4000. Call processing will consider this phone as a fully secure phone.

18.3.4.2 SPE for IP Subscribers

IMPORTANT: For SIP stations to continue to work once SPE is activated (via AMO ZANDE and/or AMO SIPCO) a Hard Restart must be performed. On a duplex system two hard restarts are required after each other to ensure all gateways are loaded new with the new SPE configuration.

IMPORTANT: For SIP subscribers only SDES as payload encryption mode is supported, Because SDES is not supported on STMI boards, no payload encryption is possible.

A list of the subscribers which support SPE is available in the ReleaseNote/ compatibility matrix.

18.3.4.3 Configuration

1) Configuring the IP subscriber.

The AMO SDAT is used for basic subscriber configuration:

CHANGE-SDAT:STNO=<station number>,TYPE=DATA1,**CLASSSEC=<security_level>**;

The security level (**CLASSSEC**) can feature the following values:

SECURE:	These subscribers are allowed to connect to the HFA/ SIP gateway with TLS or TCP depending on the subscriber settings (WBM/DLS). That means that this subscriber can be fully secure (SRTP+TLS) or traditionally non-secure, i.e. no signaling or payload encryption. This can be set via WBM/DLS for the subscriber. The AMO SDAT configuration stays **SECURE** in both cases (setting of the subscriber secure or non-secure). Default value.

CIPHER:	These subscribers allow only fully encrypted direct connections. This means that the connection to the system logged on and each DMC connection must be encrypted. This setting provides the highest security but may lead to a lower connection quality. This setting is not applicable for SIP subscribers on STMI boards.

IMPORTANT: For HFA subscribers there is no separation between payload and signaling encryption: either both are active or not active.

IMPORTANT: HFA/ SIP subscribers can only be configured as SECURE or CIPHER in AMO SDAT. Other values are available in the AMO but cannot be used for HFA/ SIP subscribers.

2) Configuring SPE at the HFA subscriber

SPE settings are performed at the HFA subscriber either with DLS/WBM or via the subscriber itself. Signaling and display settings can also be performed at the subscriber.

OpenStage WBM

(Tab sheet) **Administrator Pages > System > Security**

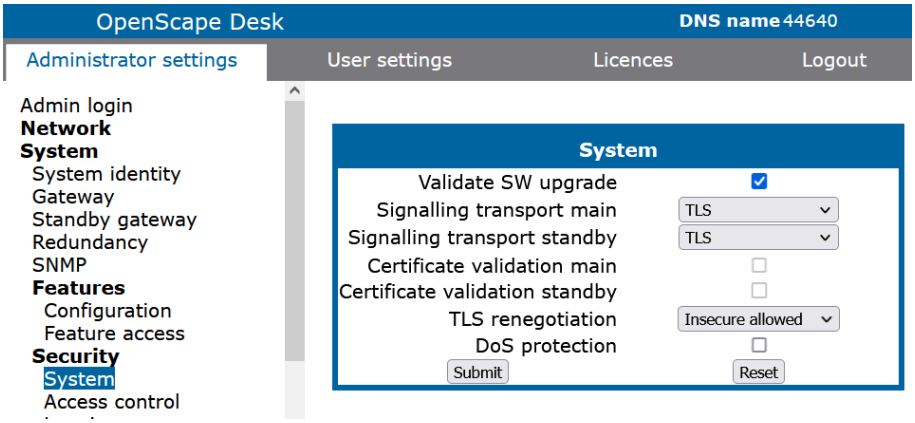
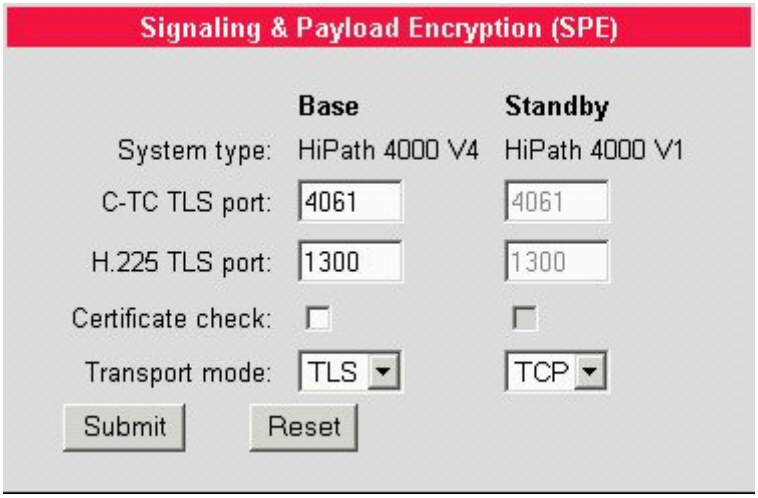


Figure 377: OpenScape Desk Phone

It can be specified in this menu whether the **transport mode** TLS or TCP is used. Additionally, it can be defined that the SPE certificate will be checked by the CA certificate (check box **Certificate check**).

Admin > System > Signaling & Payload Encryption (SPE)



DLS

IP Devices > IP Phone Configuration > Signaling and Payload Encryption (SPE)

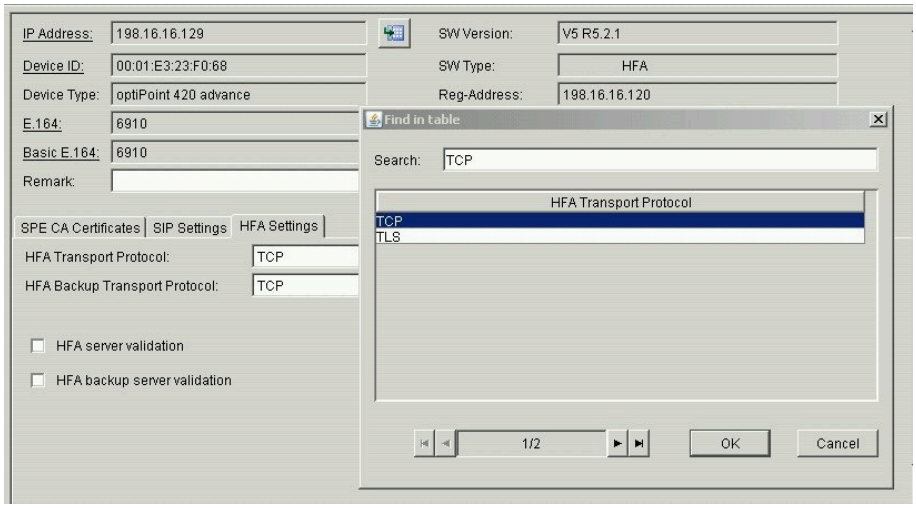


Figure 378: Detailed Information / Documentation

For more information please refer to the relevant documentation:

Deployment Service

http://apps.g-dms.com:8081/edoku/jsp/searchresult_v2.jsp?edokutype=&search_mode=product&product=OpenScape%20Deployment%20Service&product_version_main=&product_version_sub=&search_term_type=all&term=

OpenStage HFA Subscribers

- OpenStage HFA

http://apps.g-dms.com:8081/edoku/jsp/searchresult_v2.jsp?edokutype=&search_mode=product&product=OpenStage%20HFA&product_version_main=&product_version_sub=&search_term_type=all&term=&s

optiPoint 410

- optiPoint 410 advance

http://apps.g-dms.com:8081/techdoc/en/P31003H8400B413017619/index.htm

- optiPoint 410 economy/standard

http://apps.g-dms.com:8081/techdoc/en/P31003H8400B412017619/index.htm

- optiPoint 410 entry

http://apps.g-dms.com:8081/techdoc/en/P31003H8400B411017619/index.htm

optiPoint 420 Operating Manual

- optiPoint 420 advance

http://apps.g-dms.com:8081/techdoc/en/P31003H8400B423017619/index.htm

- optiPoint 420 economy/standard

http://apps.g-dms.com:8081/techdoc/en/P31003H8400B422017619/index.htm

optiPoint 410/420 Administrator Manual

- optiPoint 410/420 Administrator Manual

http://apps.g-dms.com:8081/techdoc/en/P31003A2056B4150176A9/index.htm

3) Activating SPE

4) The configurations described above take effect if SPE is activated for this system:

CHANGE-ZANDE:TYPE=SECURITY,**SPESUPP=YES**;

Parameters:

SPESUPP (YES/NO):	Activates/Deactivates SPE for this system.

For more information please refer to Chapter 3, “Activation / Deactivation of SPE for Gateways with AMO CGWB”

IMPORTANT: You must perform a hard restart on the system after you have activated SPE. If you have a duplex system you have to perform the following command on both processors simultaneously (at the same time). This means all LTUs and APs will restart! `EXEC-REST:TYPE=UNIT,UNIT=BP,RSLEVEL=HARD;`

18.3.4.4 Signaling at the Display

A connection is displayed as "encrypted" if all sections (signaling & payload) and the DMC path (signaling & payload) between all subscribers involved in this call are encrypted.

18.3.4.4.1 Display in Call State

If you want to indicate on the display of a subscriber if a call is encrypted, you must first enable the parameter **SECLVDSP** in the AMO ZANDE for the entire system.

CHANGE-ZANDE:TYPE=SECURITY,**SECLVDSP=YES**;

The **SECLVDSP** attribute must also be activated in AMO SDAT on the subscribers where the display is to appear.

CHA-SDAT:STNO=<station number>,TYPE=ATTRIBUTE,**AATTR=SECLVDSP**;

IMPORTANT: If you want a display to appear, the parameter **SECLVDSP** must be activated in both AMO ZANDE and AMO SDAT. If the parameter is activated for the first time in ZANDE, a RES-DSSU:PEN,
must be performed manually for each subscriber (if parameter CONT is set to yes, the phone restart will be executed automatically for each relevant subscriber).

You can use AMO SDAT, parameter **AATTR=SECLVTON** to ensure that the secure station also receives an advisory tone if the call is not encrypted.

CHANGE-SDAT:STNO=<station number>,TYPE=ATTRIBUTE,AATTR=**SECLVTON**;

18.3.4.4.2 Display in Idle State

The display of a subscriber in idle state (with no active call) does not indicate if the station is secure or not.

Display via key

You can configure a key in AMO TAPRO to display the status of the station:

Example: `CHANGE-TAPRO:STNO=<station number>,KY09=SECURE;`

Please note that the first eight keys are preprogrammed in OpenStage subscribers.

Display via SPE entry in menu

You can also check the security status of the subscribers in idle call state using the subscribers menu.

- **Voice encryption not enabled**
  - The subscriber is connected to the switch via TLS but SPE is not activated for this subscribers or
  - The subscriber is connected to the switch via TCP. In this case subscribers configuration at the switch is not relevant.

  In this case encryption is always disabled (**Voice encryption not enabled**).
- **Voice encryption enabled**
- The subscriber is connected to the switch via TLS and the subscriber is configured as a **SECURE** client.

  In this case encryption is enabled (**Voice encryption enabled**).
- **Voice encryption always active**
- The subscriber is connected to the switch via TLS and the subscriber is configured as a **CIPHER** client.
  - Logon via TCP not possible.
  - All media streams are encrypted (at least to the gateway).

  In this case encryption is always active (**Voice encryption always active**).

18.3.4.4.3 Scenarios

- Client A - Standard client
- The subscriber is connected to the switch via TLS but SPE is not activated for this subscriber or the subscriber is connected to the switch via TCP (subscriber configuration at the switch is not relevant).
- Client B - Secure client
- The subscriber is connected to the switch via TLS and the subscriber is configured in the system as a **SECURE** client.
- Client C - Cipher client
- The subscriber is connected to the switch via TLS and the subscriber is configured in the system as a **CIPHER** client.

Secure call: B calls C

Both subscribers have a secure connection to the gateway. Therefore the DMC connection is also secure. The displays of both subscribers show **encrypted call**. During the call both subscribers are able to check the security status in their menus.

Insecure Call: A calls B

The connection from A to the gateway is insecure. Only the connection from the gateway to client B is secure. Therefore the DMC connection is insecure. The displays of both subscribers show **call not encrypted**. During the call both subscribers are able to check the security status in their menus.

Insecure Call: A calls C

The connection from A to the gateway is insecure. Only the connection from the gateway to client C is secure. If a DMC connection if it is established it is insecure. The DMC connection ends in the OpenScape 4000 because all connections to client c (CIPHER) must be secure. The display of both subscribers show **call not encrypted**. During the call both subscribers are able to check the security status in their menus.

18.3.4.5 Deactivating SPE for Subscribers

DLS/WBM can be used to deactivate SPE for all HFA/ SIP subscribers. This causes all subscribers to log off and then log on via TCP.

The gateways themselves remain in secure mode, but **no** encryption methods are used as long as all clients are connected via TCP.

CIPHER clients will not work correctly unless they are modified in AMO SDAT to **SECURE**.

Activating SPE

As for deactivation, again using DLS/WBM.

Subscribers will log off and log on when SPE is activated or deactivated.

IMPORTANT: The gateways must already be in secure mode when the clients log on over TLS.

18.3.5 Activation / Deactivation of SPE for Access Points

Activation

The following steps have to be performed for activating SPE for access points.

1) Distribute **M**aster **E**ncryption **K**ey (**MEK**) via OpenScape 4000 Assistant to **all** APs configured in the system (states **Ready**, **NPR** (not present) and **UNACH** (hierarchically blocked)).

   This will

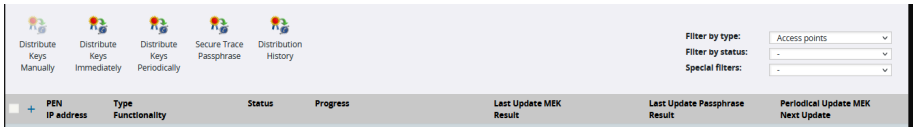
   - configure the MEK in the RMX for all access points regardless of their state and
   - transmit the MEK to all access points in **Ready** state.

   The **M**aster **E**ncryption **K**ey (MEK) is used to encrypt the signaling data between the host system and an IPDA access point.

   The MEK must be configured first on the NCUI boards for new access points and then on the host system. For more information, please refer to Section 3.5.1, “New Access Point in an Active SPE System”.

   The MEK is configured via OpenScape 4000 Assistant:

   Expert Mode > Gateway Manager > SPE



2) Check the Progress to see if something has failed.
3) **Expert Mode > Gateway Manager > SPE**
4) For access points with the status **NPR** and **UNACH**, you need to enter the MEK manually via CLI on the access point using the `Set new MEK XXXXXXXXXXXXXXXX` command.
5) Once MEKs have been successfully configured for all access points, SPE can be activated.
6) The access point encryption is activated with AMO SIPCO, parameter **IPDAENCR**:

   CHANGE-SIPCO:TYPE=SECURITY,**IPDAENCR=YES**;

IPDAENCR (YES/ NO):	Signaling and payload encryption for IPDA connections.

   SPE activation for the access points fails if MEKs are not configured for all access points (see points 1 to 3).
7) Following activation of security in AMO SIPCO, a hard system restart is required.

IMPORTANT: If you have a duplex system you have to perform the hard restart command on both processors simultaneously (at the same time). This means all LTUs and APs will restart! `EXEC-REST:TYPE=UNIT,UNIT=BP,RSLEVEL=HARD;`

---

1) **Exception**

   A soft restart is enough, if

   - no common gateways exist in the access point
   - no HFA subscribers exist in the access point
   - only TDM terminals exist in the access point
   - common gateways in the access point need no encryption
   - HFA subscribers in the access point need no encryption

   Example: Soft restart of the active BP

   EXEC-REST:TYPE=UNIT,UNIT=BP,RSLEVEL=SOFT;

2) If you have common gateway boards and HFA subscribers in the access point and if these are to be used in secure mode, you have to perform all steps that would be necessary if the common gateway board and the HFA subscribers were in the host system (activate SPE with AMO ZANDE parameter **SPESUPP**, import certificates and so on).
3) Related topics:

   - Trunk SPE Activation / Deactivation
   - Subscriber SPE Activation / Deactivation
   - Distribution of Certificates to Gateways
   - Distribution of Certificates with the WBM of the Gateway
   - Distribution of Certificates to Subscribers

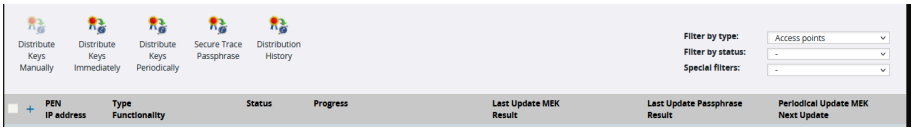
Deactivation

If a customer would like to deactivate SPE completely for the access points and the associated common gateways, a hard restart must be performed for this.

18.3.5.1 New Access Point in an Active SPE System

If you need to add a new access point while access point encryption is already active, you need to do the following:

- Configure the access point in the system as usual with AMO UCSU, AMO APRT.
- Don't connect the access point yet because it will fail.
- Use **SPE Administration** in OpenScape 4000 Assistant and update the board list to see if your new access point has been added.
- **Expert Mode > Gateway Manager > SPE**



  – Configure a MEK manually for this access point. This will transmit the MEK to the RMX.
  – Use the CLI to configure the same MEK on the NCUI.
  – Now you can connect the access point to the LAN and activate the connection to the system via `EXEC-USSU:MODE=CONFAP,LTU=<ltu_number>;`.

18.3.5.2 Deactivating SPE for Access Points with Soft Restart

Access point encryption (signaling and payload) is deactivated with the AMO SIPCO followed by a soft restart. In a duplex system, you also only have to perform **one** soft restart on the active CC.

IMPORTANT: Deactivation of the access point encryption causes every call and the associated DMC connections with access point reference (subscriber or trunk in AP shelf) to be executed and signaled as non-secure calls from an end-to-end perspective. The connections between the STMI board in the AP shelf and the HFA subscribers or the partner gateway, however, remain encrypted, i.e. TLS subscribers will still run on TLS in AP shelves and trunking gateways which have already established a TLS connection will continue using TLS connections.

Activating SPE

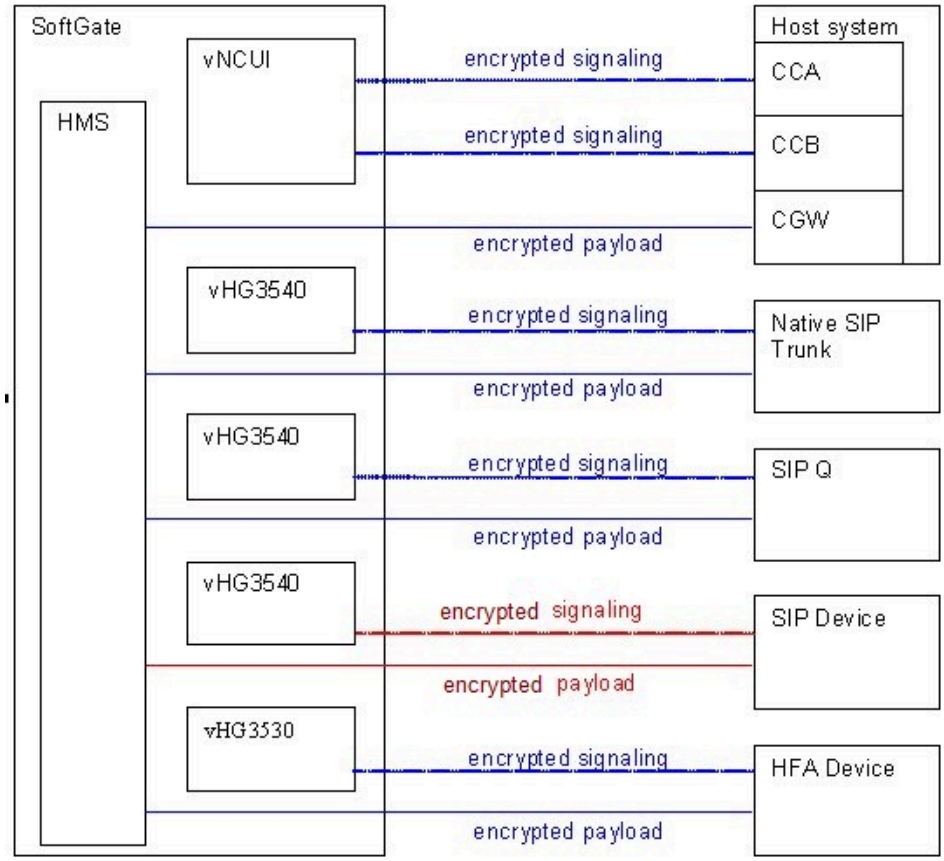
Like deactivation, with the AMO SIPCO and soft restart.

Caution

AMO SIPCO prompts the administrator to perform a hard restart after activating/ deactivating SPE. This advisory is not modified for the following reasons:

- When SPE is already activated on the system for HFA subscribers and IP trunking and access point encryption is activated for the first time, a hard restart must be performed before the feature works correctly.
- If a customer would like to deactivate SPE completely for an access point and the associated common gateways, a hard restart must be performed for this.

18.3.6 OpenScape 4000 SoftGate SPE Activation / Deactivation



OpenScape 4000 SoftGate and SPE - Overview

18.3.6.1 Features

- The signaling connection between OpenScape 4000 SoftGate and common control in host system is encrypted.
- Payload connections from OpenScape 4000 SoftGate to HG 3570 in the host system or to another OpenScape 4000 SoftGate or to AP shelves are encrypted.
- A Signaling and payload encryption is also supported for SIP trunking and HFA/ SIP subscribers.

18.3.6.2 Restrictions

- If SPE is activated in the host system and no default MEK is assigned to the OpenScape 4000 SoftGate, the OpenScape 4000 SoftGate will not start.
- HFA signaling cannot be traced at the OpenScape 4000 SoftGate!

18.3.6.3 Configuration

To use signaling and payload encryption (**SPE**) for OpenScape 4000 SoftGate, the **M**aster **E**ncryption **K**ey (**MEK**) has to be configured as for a normal access point (AP). For a normal access point, this is done with the **C**ommand **L**ine **I**nterface (**CLI**). As the OpenScape 4000 SoftGate does not have a CLI, the process is a little different.

18.3.6.3.1 Scenario 1: Activate a OpenScape 4000 SoftGate on a host system that already has SPE activated

---

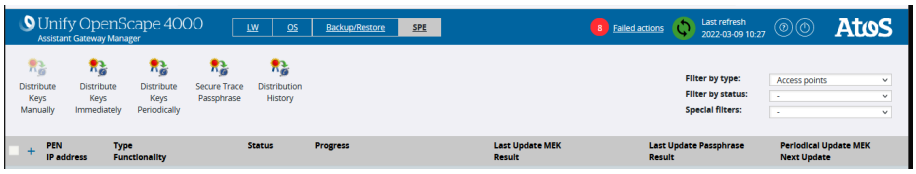
IMPORTANT: Please note the sequence!

IMPORTANT: Don't start the OpenScape 4000 SoftGate because it will fail!

---

1) Use the SPE administration in OpenScape 4000 Assistant and update the board list to see your new OpenScape 4000 SoftGate.

   Expert Mode > Gateway Manager > SPE



2) Configure a MEK **manually** for this OpenScape 4000 SoftGate. This will transmit the MEK to the RMX.

   Expert Mode > Gateway Manager > SPE

3) Use the “OpenScape 4000 Platform Administration (Portal)” to configure the MEK.

IMPORTANT: Since SPE is active in the system, the OpenScape 4000 SofGate will not be able to connect unless it has the correct MEK. WBM (for the distribution of a MEK) can’t be used till the OpenScape 4000 SofGate connects successfully to the host system.

---

4) Now you can start up the OpenScape 4000 SoftGate.

18.3.6.3.2 Scenario 2: SPE is neither activated on OpenScape 4000 SoftGate nor at host system

The following steps have to be performed for activating SPE for OpenScape 4000 SoftGate.

IMPORTANT: Please note the sequence!

---

1) Please note the sequence! Switch on the host system and all OpenScape 4000 SoftGates configured in the system.

2) Distribute **M**aster **E**ncryption **K**ey (**MEK**) via OpenScape 4000 Assistant to **all** OpenScape 4000 SoftGates. This will

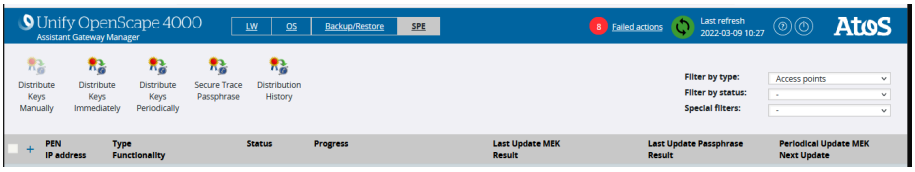
   This will

   - configure the MEK in RMX for all OpenScape 4000 SoftGates and
   - transmit the MEK to all OpenScape 4000 SoftGate.

   The MEK must be set first on the vNCUI boards and then on the host system.

   The MEK is configured via OpenScape 4000 Assistant:

   Expert Mode > Gateway Manager > SPE



3) Check the Progress to see if something has failed.

   Expert Mode > Gateway Manager > SPE

4) Once MEKs have been successfully configured for all OpenScape 4000 SoftGates, SPE can be activated.

   The IPDA encryption is activated with AMO SIPCO, parameter **IPDAENCR**:

   CHANGE-SIPCO:TYPE=SECURITY,**IPDAENCR=YES**;

IPDAENCR (YES/ NO):	Signaling and payload encryption for IPDA connections.

IMPORTANT: SPE activation for OpenScape 4000 SoftGate fails when MEKs are not configured for all OpenScape 4000 SoftGate (refer to point 1 to 3).

18.4 Generation SPE Certificates with OpenScape 4000 Assistant

The SPE TLS/ SSL Certificate Management area in OpenScape 4000 Assistant comprises the features for administering SSL security certificates for the feature Signaling and Payload Encryption (SPE). It provides the tools for the generation of SSL root certificate (CA) and for the generation of PKCS#12 certificate which is signed by root certificate suitable for the SPE feature.

To start the application select in the OpenScape 4000 Assistant **Expert Mode > Signaling & Payload Encryption**.

18.4.1 SPE Root Certificate

This feature allows you to create your own root certificate which is used to sign all SPE certificates generated by SPE Certificate feature and to download it directly from the user interface.

The goal of this feature is to have all SPE certificates within a HiPath 4000/ OpenScape network signed by just one root certificate (CA).

A root certificate is a special type of self signed certificate.

The main difference is that a root certificate is a CA certificate and therefore may be used to sign other certificates.

18.4.1.1 Open the SPE Root Certificate Dialog

Navigate in the OpenScape 4000 Assistant start page to **Expert Mode > Signaling and Payload Encryption > SPE Root Certificate**. The SPE Root Certificate dialog opens.

Two cases are possible:

- Root certificate does not exist yet.
- If no root certificate has been created yet, the empty root certificate dialog will open.
- Root certificate already exists.
- If a root certificate has already been created on this server, the data of the existing certificate will be displayed together with a corresponding note in the root certificate dialog in the browser.

18.4.1.2 Creating a New Root Certificate

Navigate in the OpenScape 4000 Assistant start page to **Expert Mode > Signaling and Payload Encryption > SPE Root Certificate**. The SPE Root Certificate dialog opens.

There are two cases which have to be distinguished:

- No SPE root certificate exists
- If no SPE root certificate is created yet, the dialog for creating a SPE root certificate is displayed with empty fields.

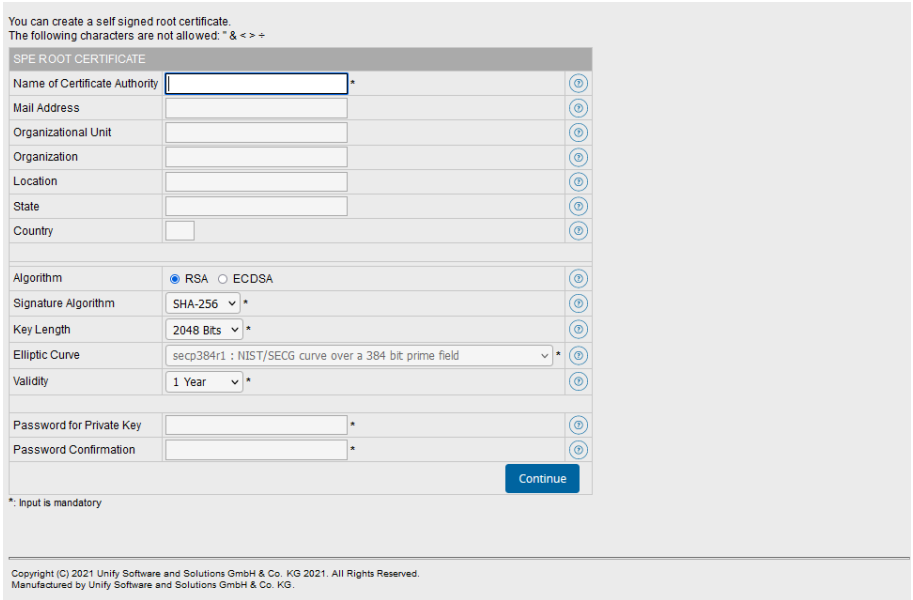


Figure 379: SPE root certificate generation (no SPE root certificate exists)

- A SPE root certificate already exists

- If a SPE root certificate is already created, click the **New Root Certificate** button for creating a new SPE root certificate. A new dialog opens. The data of the existing SPE root certificate are displayed in the entry fields and can modified accordingly for the new SPE root certificate.

  IMPORTANT: If you create a new SPE root certificate although a SPE root certificate already exists for this server, the existing SPE root certificate will be overwritten.

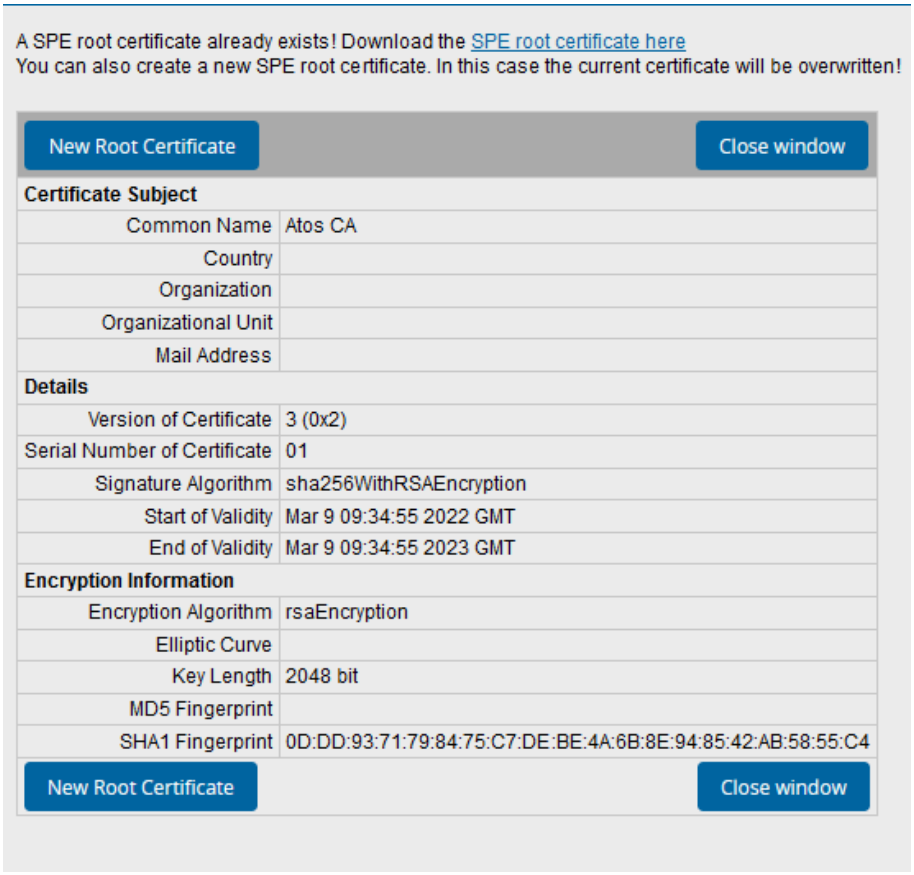


Figure 380: SPE root certificate generation with existing SPE root certificate

Procedure

1) Enter all required data. Mandatory fields are flagged with a red asterisk (*). The following characters are not allowed in the entry fields: " & < > ÷ as well as accented and special characters.
2) To get additional context information related to the individual entry fields, click on the **?** icon to the right of each entry field. The context-specific information related to the respective field is displayed as a tooltip in the browser.
3) Click on **Continue**. The SPE root certificate will be generated. After the creation of the certificate it is displayed and can be downloaded via a link.
4) When creating a SPE certificate based on the ECDSA Signature Algorithm, please ensure that all endpoints support ECDSA.

   For example, HG3500 and STMI2/4 boards do not support them.

18.4.1.3 Displaying/Downloading the newly Created SPE Root Certificate

Navigate in the OpenScape 4000 Assistant start page to **Expert Mode > Signaling and Payload Encryption > SPE Root Certificate**. The SPE Root Certificate dialog opens.

If a SPE root certificate already exists it will be displayed and you may download the SPE root certificate by clicking the **SPE Root Certificate here** link.

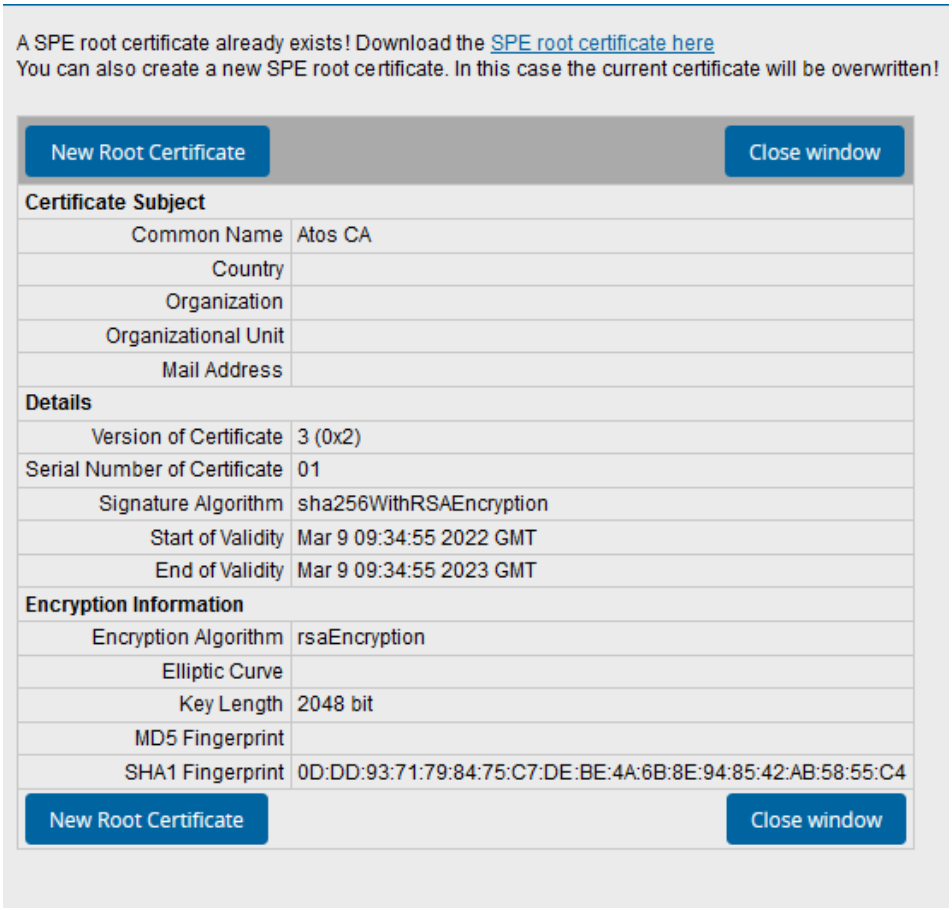


Figure 381: Download of SPE root certificate

18.4.2 SPE Certificate

The **SPE Certificate** feature provides the method of creating a new SSL certificate and having it signed by SPE root certificate. Certificates created by this function is always signed by SPE root certificate created in **SPE Root Certificate** dialog (see Section 5.1, “SPE Root Certificate”).

18.4.2.1 Open the SPE Certificate Dialog

Navigate in the OpenScape 4000 Assistant start page to **Expert Mode > Signaling and Payload Encryption > SPE Certificate**. The SPE Certificate dialog opens.

Three cases are possible:

- Certificate does not exist yet.
- If no certificate has been created yet, the empty certificate dialog opens.
- Certificate already exists.
- If a certificate has already been created in this server, the data of the existing certificate will be displayed together with a corresponding note in the certificate dialog in the browser.
- Root certificate does not exist yet.
- If no root certificate has been created yet, user is informed to create root certificate first

18.4.2.2 Creating a new SPE Certificate

Navigate in the OpenScape 4000 Assistant start page to **Expert Mode > Signaling and Payload Encryption > SPE Certificate**. The SPE Certificate dialog opens.

There are two cases which have to be distinguished:

- No SPE certificate exists.
- If no SPE certificate is created yet, the dialog for creating a SPE certificate is displayed with empty fields.

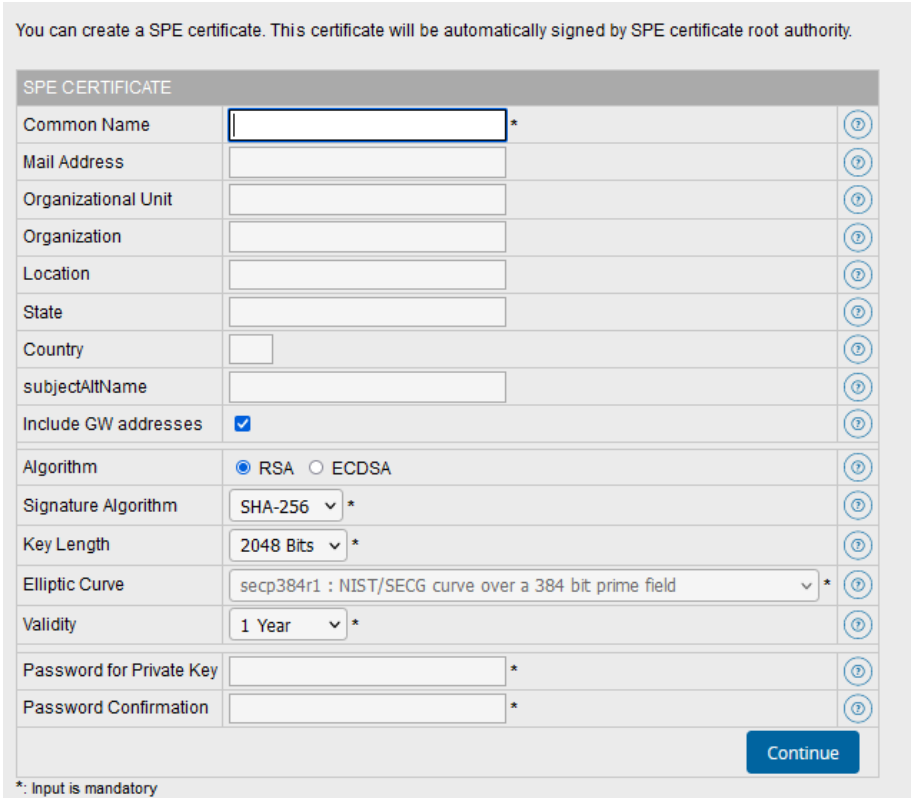


Figure 382: SPE certificate generation (no SPE certificate exists)

- A SPE certificate already exists
- If a SPE certificate is already created, click the **New SPE Certificate** button for creating a new SPE certificate. A new dialog opens. The data of the

existing SPE certificate are displayed in the entry fields and can modified accordingly for the new SPE certificate.

IMPORTANT: If you create a new SPE certificate although a SPE certificate already exists for this server, the existing SPE certificate will be overwritten.

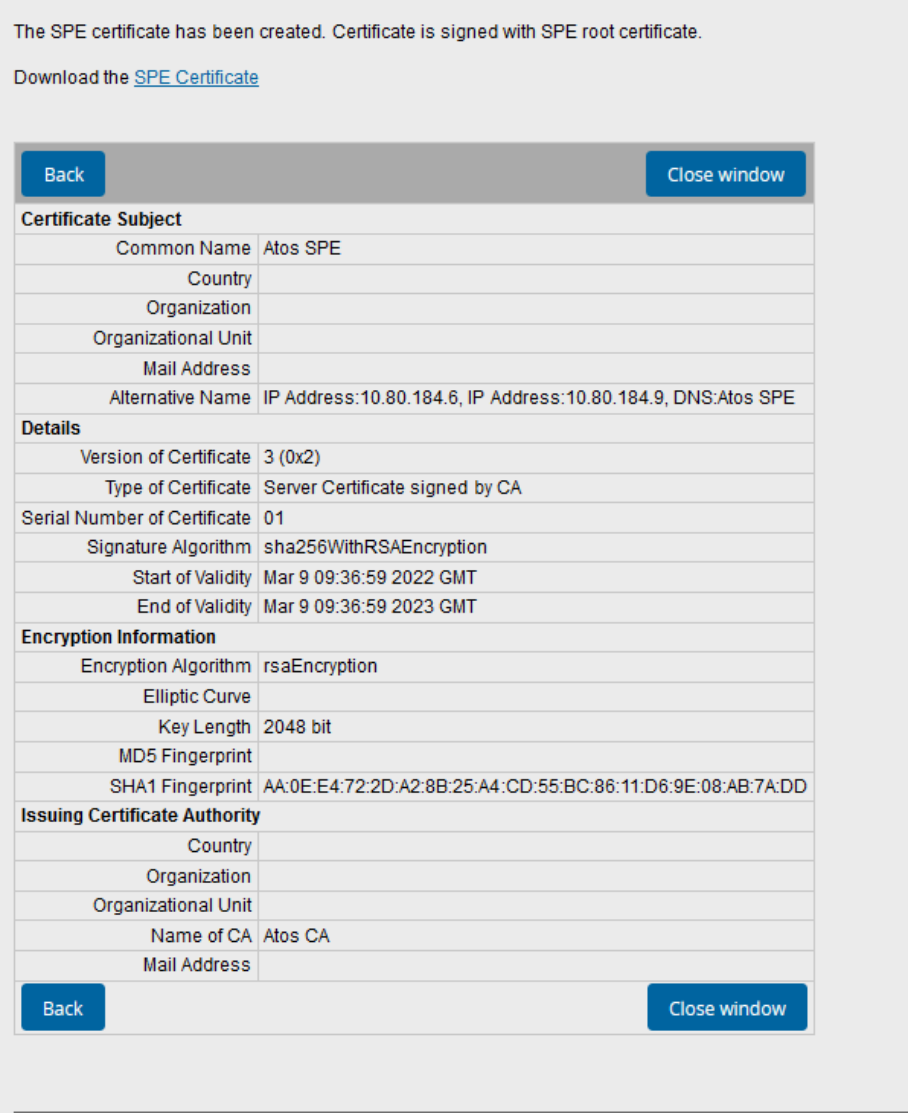


Figure 383: SPE certificate generation with existing SPE certificate

Procedure

1) Enter all required data. Mandatory fields are flagged with a red asterisk (*). The following characters are not allowed in the entry fields: " & < > ÷ as well as accented and special characters.
2) To get additional context information related to the individual entry fields, click on the "?" icon to the right of each entry field. The context-specific information related to the respective field is displayed as a tooltip in the browser.

3) Click on **Continue**. The SPE certificate will be generated. After the creation of the certificate it is displayed and can be downloaded via a link.

18.4.2.3 Displaying/Downloading the newly created SPE Certificate

Navigate in the OpenScape 4000 Assistant start page to **Expert Mode > Signaling and Payload Encryption > SPE Certificate**. The SPE Certificate dialog opens.

If a SPE certificate already exists it will be displayed and you may download the SPE certificate by clicking the **SPE Certificate** link.

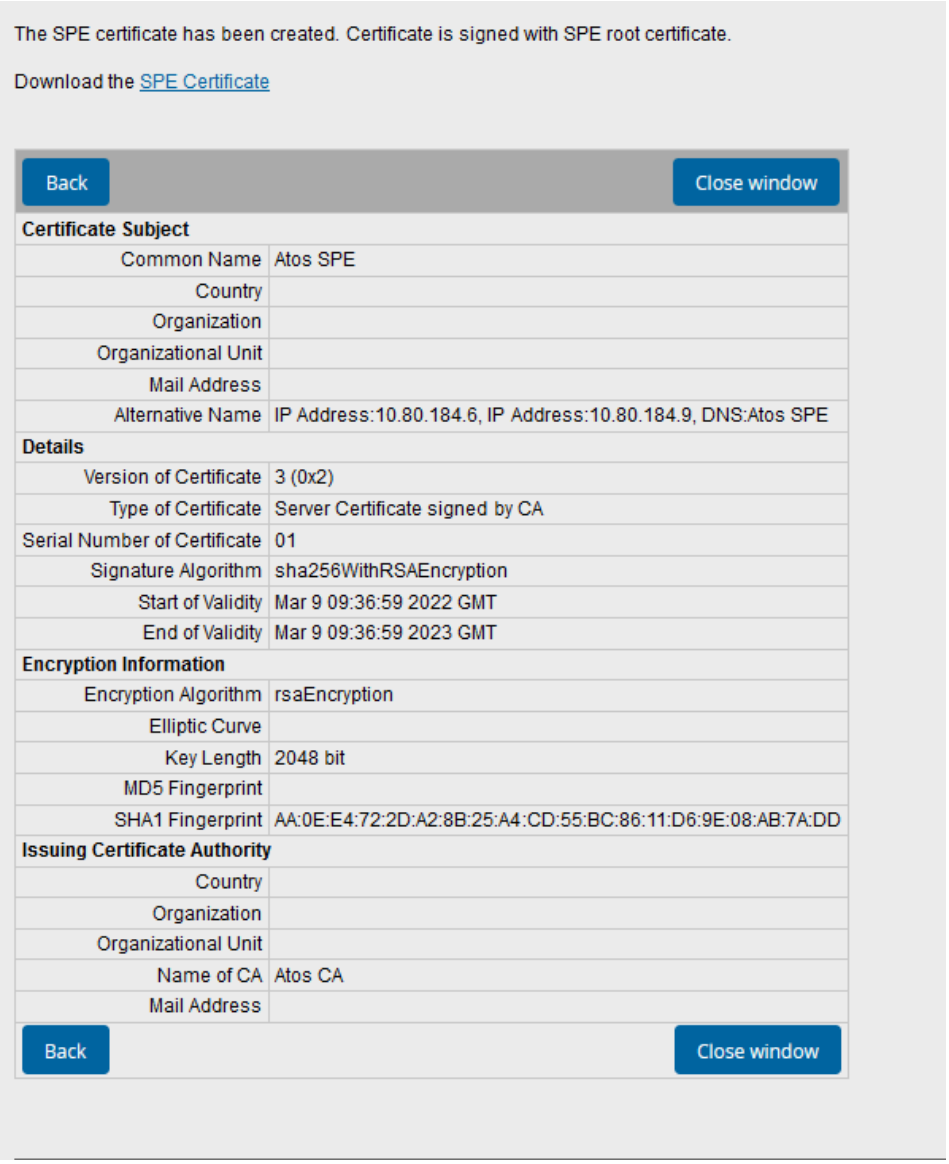


Figure 384: Displaying/Downloading of SPE certificate

18.5 Distribution of Certificates with the WBM of the Gateway

This chapter is only intended as a brief overview of the necessary steps in WBM.

For a detailed description, refer to the administrator manual of the WBM.

- HG 3500 (&HG3575)
- http://apps.g-dms.com:8081/techdoc/en/P31003H3180M1000176A9/index.htm
- vHG 3500 HFA (for HFA subscriber)
- http://apps.g-dms.com:8081/techdoc/en/P31003H3180M1020176A9/index.htm
- vHG 3500 SIP (for SIP trunking and SIP subscribers)
- http://apps.g-dms.com:8081/techdoc/en/P31003H3180M1030176A9/index.htm
- vHG 3575
- http://apps.g-dms.com:8081/techdoc/en/P31003H3180M1030176A9/index.htm
- HG 3500 on STMIX/STMIY
- http://apps.g-dms.com:8081/techdoc/en/P31003H3180M1050176A9/index.htm

  Certificates can be imported directly via WBM (Web-Based Management) on the gateway in any case, even if DLS is not available in the customer network.

  You can access the WBM via HiPath 4000 Assistant: **Expert Mode > Gateway Dashboard**

18.5.1 Importing SPE CA Certificate on a Gateway

Configuration > **Security** > **Signaling and Payload Encryption (SPE) > SPE CA Certificate(s)** > **Import trusted CA Certificate (PEM or Binary)**

The **Load a SPE CA Certificate via HTTP** screen is displayed. Browse for the certificate. Click **View Fingerprint of Certificate**. Now import the certificate with the **Import Certificate from File** button.

An appropriate message is output if the import operation was successful.



Figure 385: Importing a SPE CA certificate on a gateway

18.5.2 Importing a SPE Certificate on a Gateway

IMPORTANT: For a vHG3500 HFA see Section 6.3, “Importing a SPE Certificate on a vHG3500 HFA”**.**

Configuration > Security > Signaling and Payload Encryption (SPE) > SPE Certificate(s) > Import trusted SPE Certificate (PEM or PKCS#12)

The **Load a SPE Key Certificate via HTPP** screen is displayed. Enter the passphrase ("confidential password" (see Section 4.3, “Configuration”)) and then browse for the certificate. Click **View Fingerprint of Certificate**. Now import the certificate with the **Import Certificate from File** button.



Figure 386: Importing a SPE certificate on a gateway

18.5.3 Importing a SPE Certificate on a vHG3500 HFA

IMPORTANT: Only possible for vHG 3500 HFA!

Configuration > SIP Load Balancer > SPE > Import Keycert

The **Load a SPE Key Certificate via HTTP** screen is displayed.



Importing a SPE certificate for HFA subscriber at vHG 3500

A SPE key certificate can be imported in this dialog by entering the decryption password and the file name. The file containing the certificate originates in a customer PKI certification authority (RA/CA) or the DLS server's internal certification authority (CA) and must be available in PEM or PKCS#12 format.

18.5.4 Certificates and Security on vHFA and WAN Interfaces

vHFA

SPE certificate configured on vHFA WBM is used for TLS connection to its IP address.

- TLS ports on vHFA are opened only if SPE is enabled and certificates are loaded (all on vHFA works as before WAN introducing)
- SPE certificate on vHFA is used just for "local" connection.
- SPE certificate on vHFA is not necessary if SPE is disabled or TLS is not required for local connections.

WAN Interface

SPE certificate configured on OpenScape 4000 SoftGate WBM is used for TLS connection to WAN IP address.

- SRTP is always used on WAN regardless of security settings
- TLS ports on WAN are opened if certificate is configured regardless SPE is enabled or disabled.
- WAN interface requires SPE certificate because only TLS is allowed on WAN.
- WAN interface always uses TLS and SRTP regardless of SPE settings.
- If SPE is enabled the phone on WAN is reported to system as secure using TLS.
- If SPE is disabled the phone on WAN is reported to system as insecure using TCP (regardless it uses TLS).
- If SPE is disabled then mobile HFA between WAN and local interfaces works with TCP on local and TLS on WAN connections.
- if SPE is enabled and mobile HFA is required for some subscriber than this subscriber have to use TLS also on local connection (otherwise mobile HFA from WAN can not be canceled on local phone because TCP can not override TLS)

18.6 Distribution of Certificates using Deployment Service (DLS)

IMPORTANT: This chapter is only intended as a brief overview of the necessary steps in the Deployment Service (DLS). For a detailed description, refer to the appropriate DLS administrator manual.

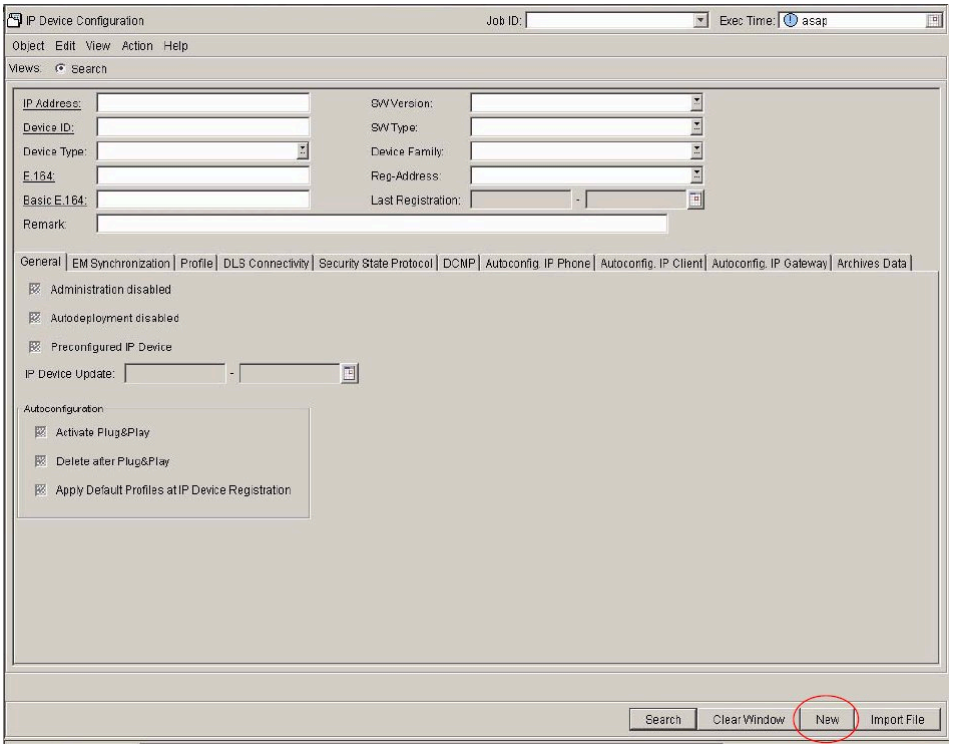
IMPORTANT: If a board has a separate Management LAN interface configured, DLS bootstrapping will use the MAN IP address instead of the VOIP IP address.

18.6.1 Distribution of Certificates to Gateways

18.6.1.1 Creating a Virtual IP Device

IP Devices > IP Device Management > IP Device Configuration

Press button **New** to create a new virtual IP device.



In the general data area enter the **Device ID** (IP address of the gateway) and select from the drop-down list **IP Gateway** as **Device Family.**

Choose now the tab **DLS Connectivity**.

In the section **DLS Connectivity** enter the **DLS Server Address** (IP address of the DLS) and the **DLS Port** (18443).

These data must be the same as the data configured in the system.

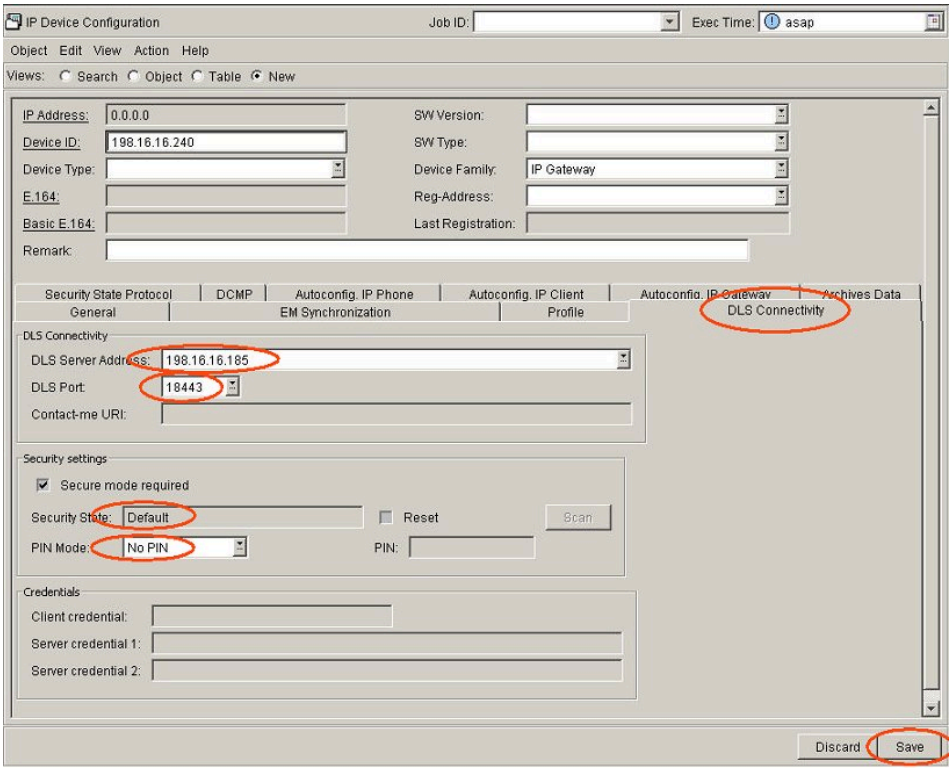
Please make sure the DLS port and IP address are configured correctly in the system:

```
CHANGE-ZANDE:TYPE=DLS,DLSIPADR=198.16.16.185,DLSPORT=18443;
```

Also make sure that AMO CGWB for the individual gateways is configured correctly:

```
CHANGE-CGWB:MTYPE=CGW,LTU=1,SLOT=4,TYPE=DLSDATA,DLSIPADR=198.16.16.185,DL▶
SPORT=18443;
```

In the section **Security Settings** the checkbox Secure mode required must be activated. The **Security State** is at the moment **Default**.



Communication between DLS and the IP devices (gateways) is a secure TLS connection using default certificates that are the same for every DLS and gateway.

In the drop down menu **Pin Mode** you can choose between different security settings:

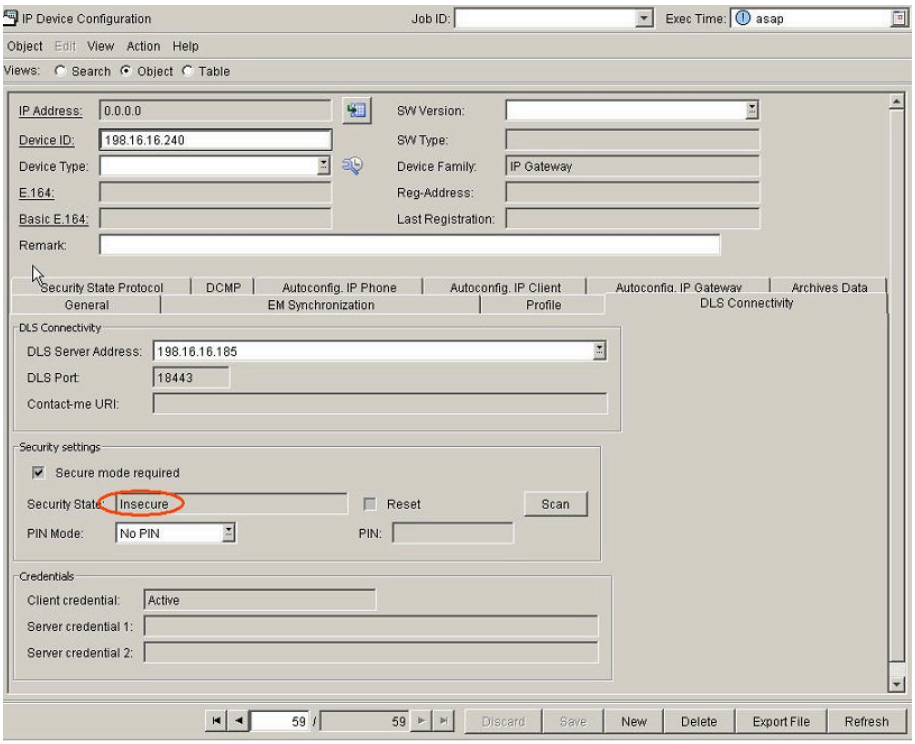
1) No PIN

2) Access data is sent encrypted to the IP Device using a hardcoded passphrase.

   This mode can only be used if the parameter **DLSACPAS = NO** is set. Please check with AMO CGWB and change it if necessary.

   CHANGE-
   CGWB:MTYPE=CGW,LTU=1,SLOT=14,TYPE=DLSDATA,**DLSACPAS=NO**;

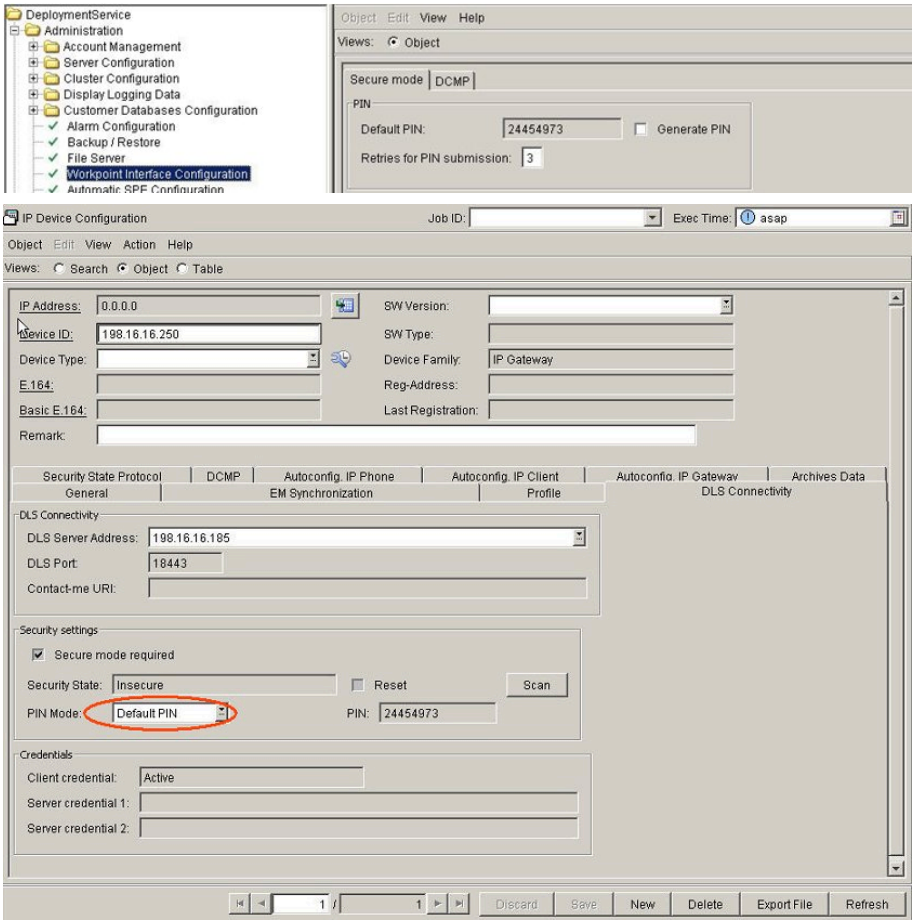
   After saving the settings the **Security State** changes from **Default** to **Insecure**.



3) **Default PIN**
4) In order to make this TLS connection more secure we can additionally encrypt the content of the TLS communication with a PIN.

   Default PIN will use the same PIN for every gateway. You can view an already randomly generated PIN in the **Secure Mode** tab under

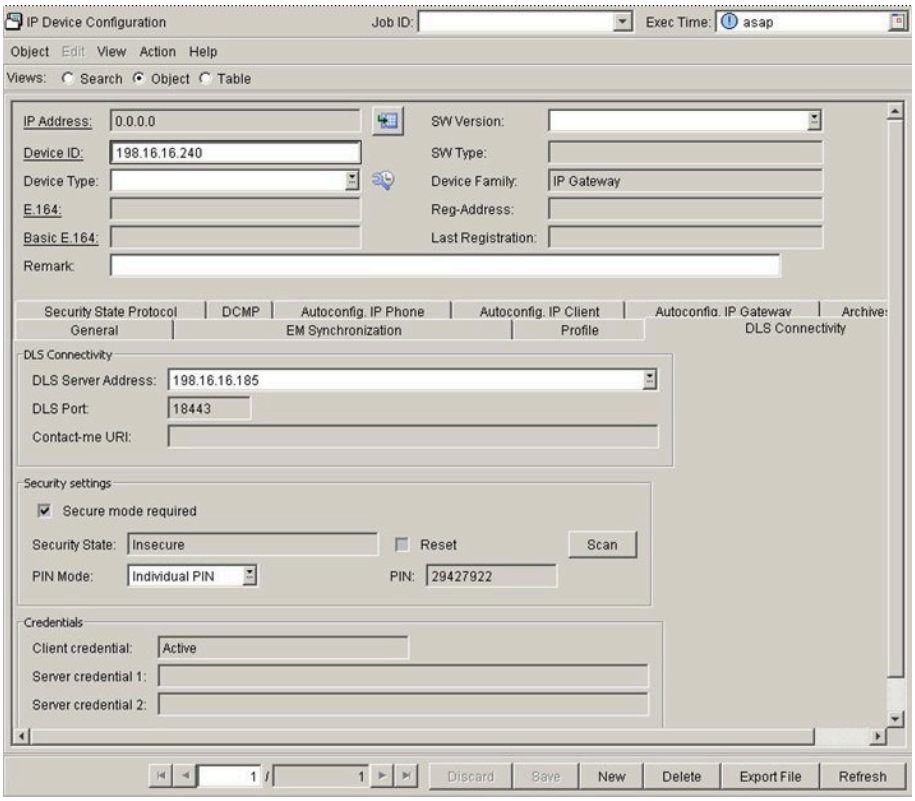
Administration > Workpoint Interface Configuration and also generate a new random PIN.



After pressing the **Save** button you can see the default PIN.

5) **Individual PIN**

6) Individual PIN will use different PINs for every gateway.



DLS generates the PINs randomly and automatically when you press the **Save** button.

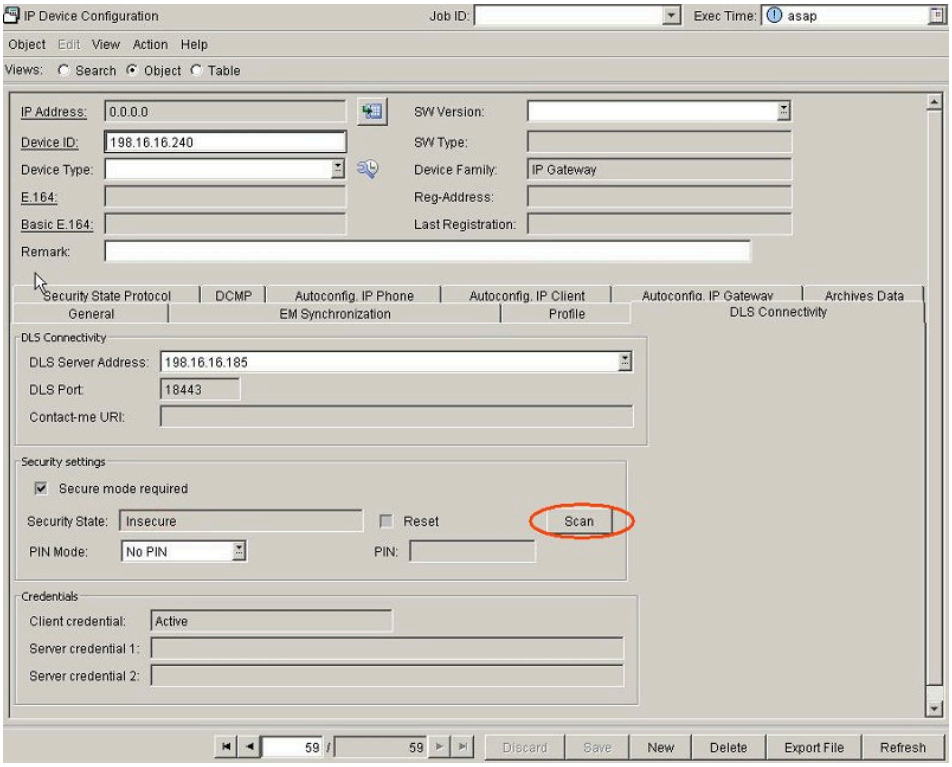
18.6.1.2 Scanning the IP Devices (IP Gateways)

Bootstrapping: By scanning the IP devices (gateways), the DLS sends a certificate to the gateway to prepare a secure connection for importing the customer certificates (CA and certificate).

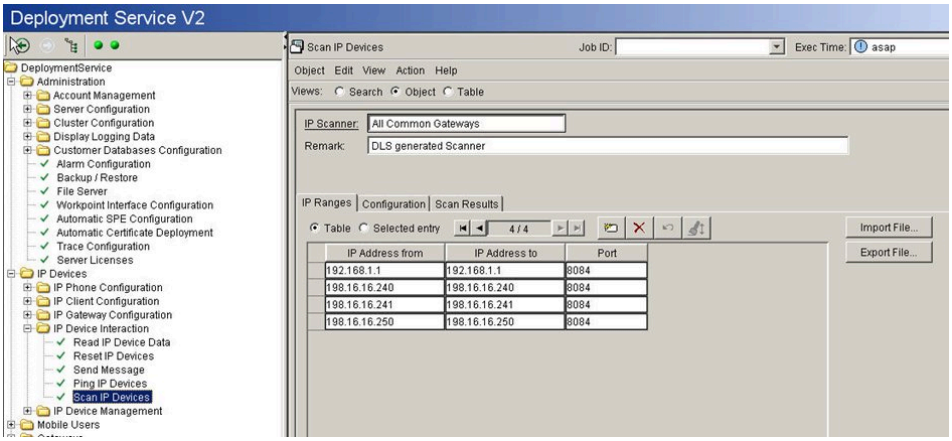
The scanning action is the same regardless of which mode is being used (No PIN, Default PIN or Individual PIN).

There are 2 possibilities to do the SCAN.

1) Scanning individual gateways one by one



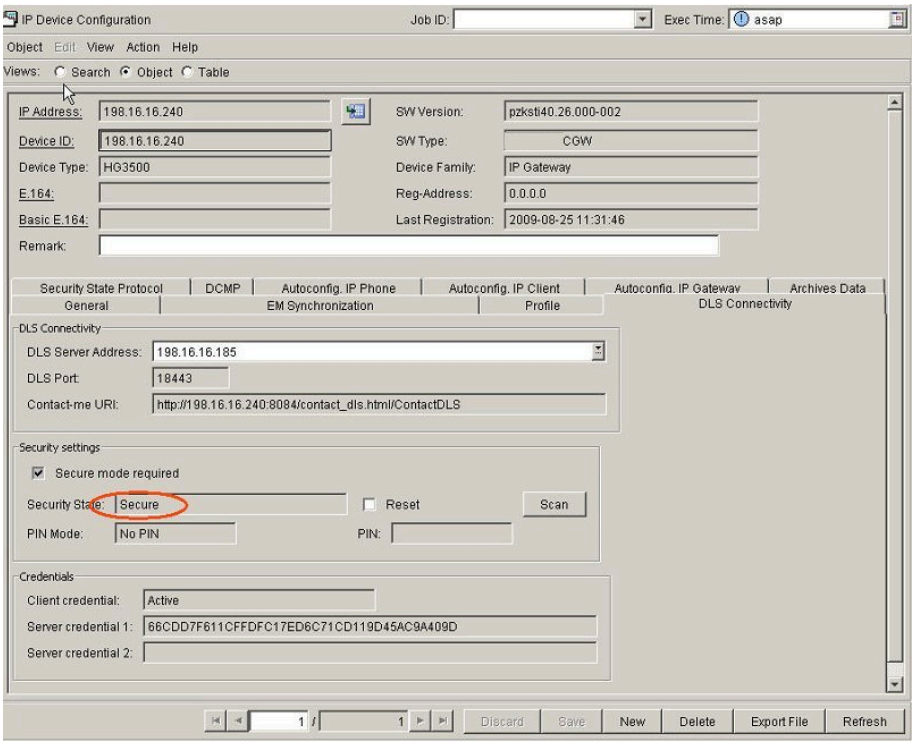
1) After pressing the Save button to save the configuration, you can press the **Scan** button and the configured gateway will be scanned right away.
2) **Group scanning of gateways in one run**



1) After the scanning has been done, the next step will depend on the security mode used:

   a) When **NO PIN** mode is used, **IP Device Configuration** > **DLS Connectivity** > **Security State** will show **Secure**. Now bootstrapping for this mode is finished and you can proceed with the distribution of SPE CA certificate and SPE certificates (see Section 7.1.3,

"Distribution of the SPE CA Certificate" and Section 7.1.4, "Distribution of the SPE Certificate").



When Default PIN or Individual PIN security mode is used, the **Security State Pending** is shown after scanning.

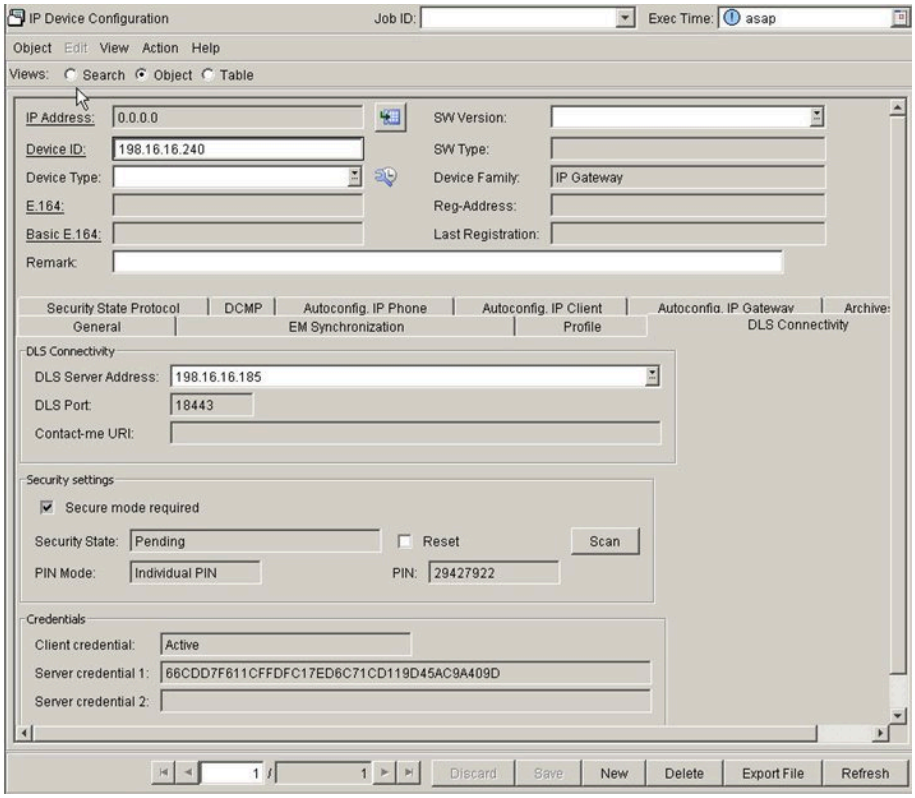


Figure 387: The PIN must be entered on the gateway via CLI.

CLI command:

vxTarget> activate dls pin 29427922

activate dls pin - args: 29427922.

Bootstrapping succeeded.

OK

vxTarget>

There is no CLI with virtual gateways. The PIN must therefore be entered in a WBM screen.

If you now go back to DLS DLS Connectivity > **Security State**, the gateway will show **Secure**. Bootstrapping is now finished and you can proceed with the distribution of CA and SPE certificates (see Section

7.1.3, “Distribution of the SPE CA Certificate” and Section 7.1.4, “Distribution of the SPE Certificate”).

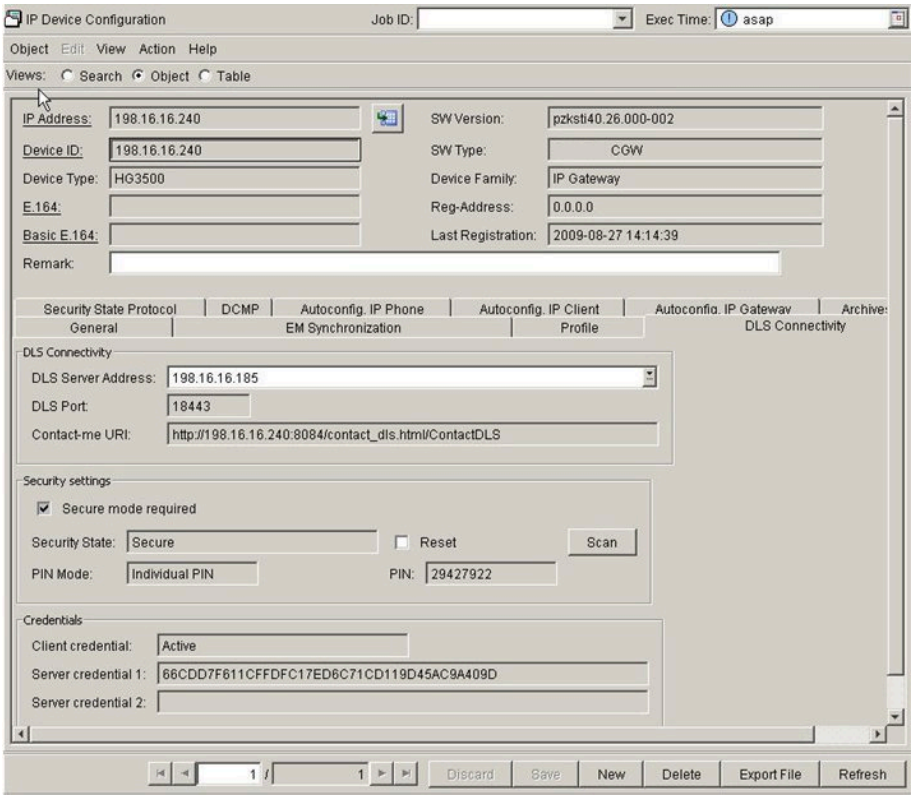


Figure 388: Bootstrapping final verification in gateway WBM:

You can use the WBM application in HG 3500/3575 V4 and newer to check if the import operations worked properly and the certificates were activated. Access is possible with the HiPath 4000 Assistant.

Menu: Menu: **Expert Access** > HiPath **4000** > **HG35xx Web Based Management**

In the WBM you can view the certificates in the following directory:

Configuration > **Security** > **Deployment and Licensing Client (DLSC)**

There should be two entries:

a) DLSC Client Certificate

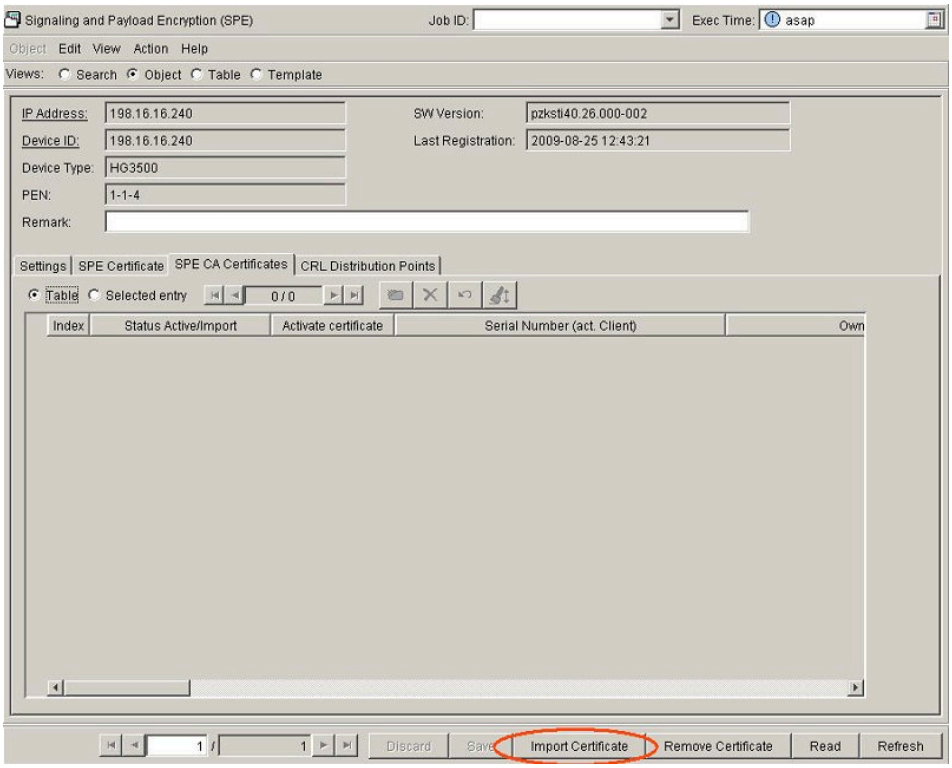
- DLSC CA Certificate

18.6.1.3 Distribution of the SPE CA Certificate

Import CA certificate: **IP Devices** > **IP Gateway Configuration** >**Signaling and Payload Encryption (SPE)**

All successfully bootstrapped boards (see Section 7.1.2, “Scanning the IP Devices (IP Gateways)”) will be shown using the radio button **Search**.

Press the button **Import Certificate**.



A new window now appears where you can browse for the CA certificate. Up to 16 CA certificates can be imported. The importing and activation of CA certificates can be combined in one step.

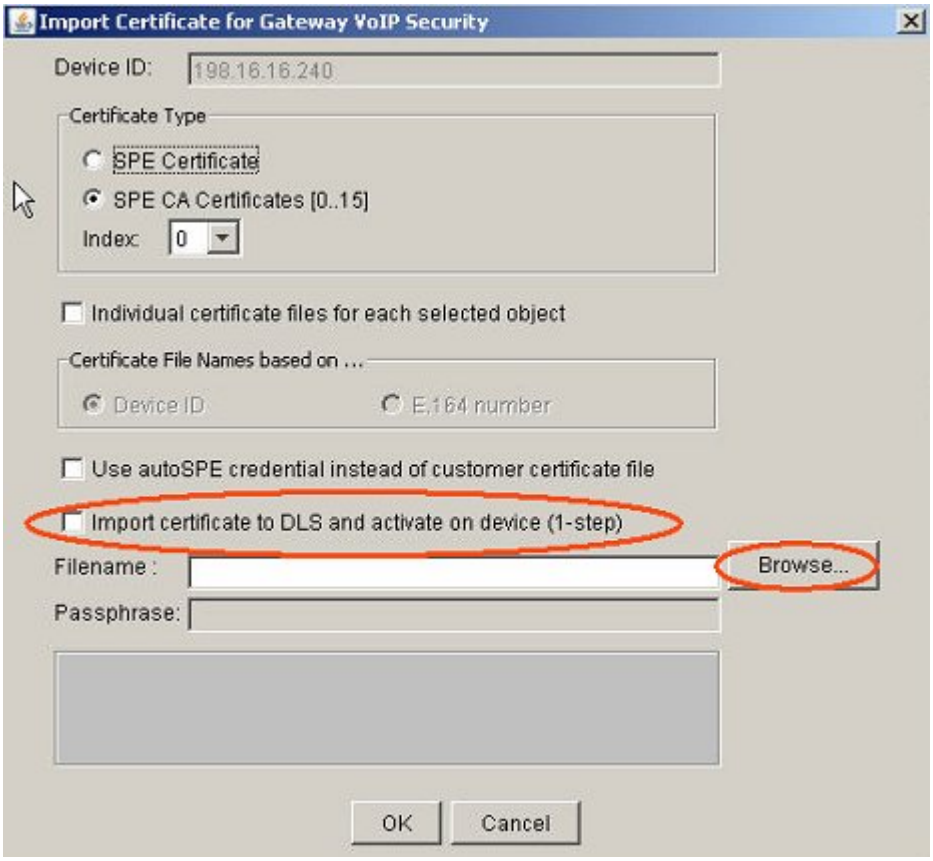


Figure 389: Select CA certificate

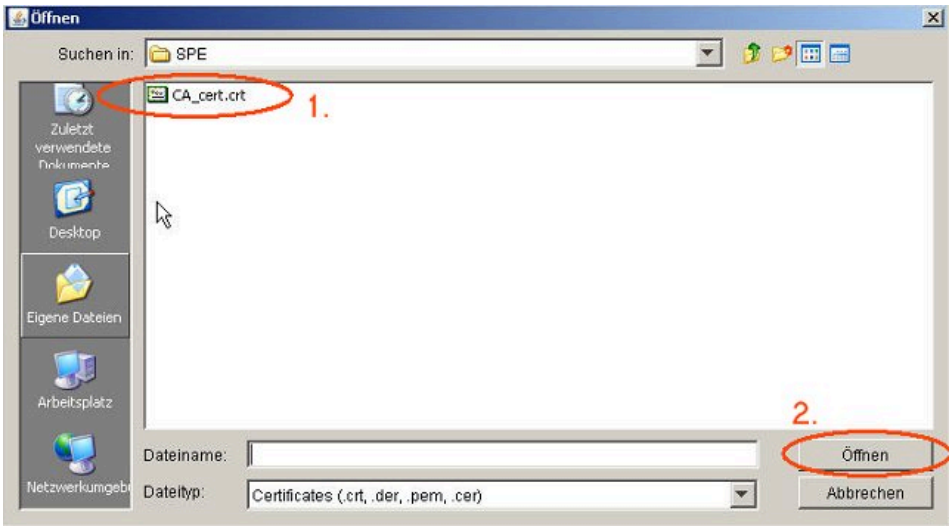


Figure 390: Confirm your selection.

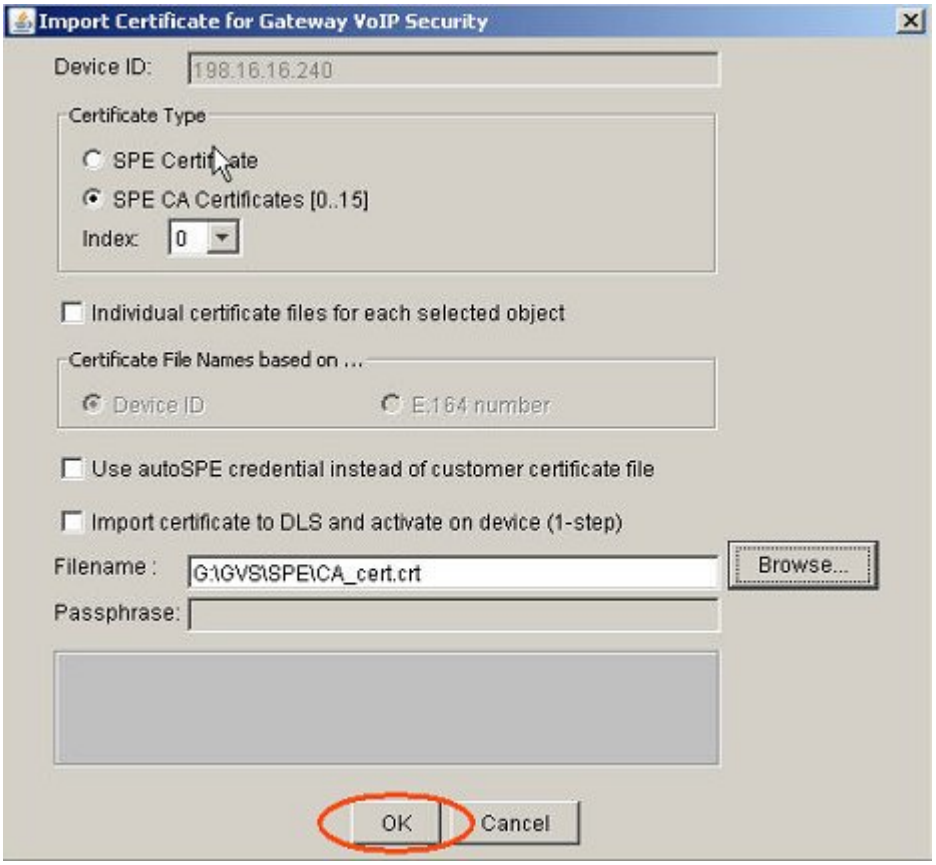
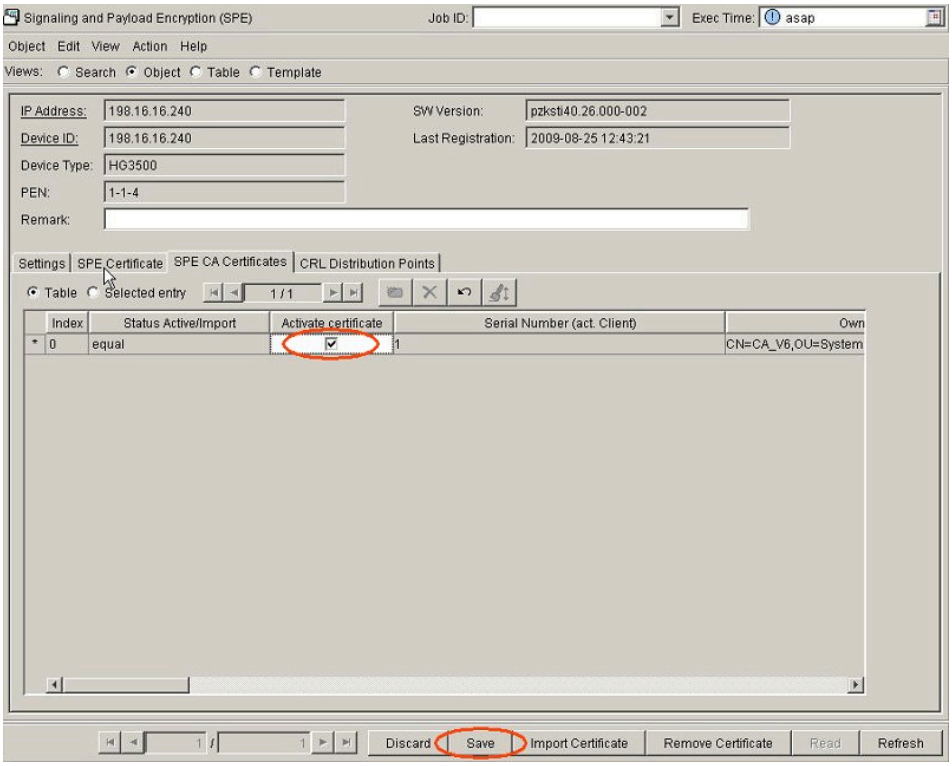


Figure 391: Activate CA certificate.

Activate the checkbox **Activate certificate** and click **Save** to activate the certificate. The status of the imported certificate will change from **no active certificate** to **equal** if the certificate is valid. Additionally some data will be read by the DLS, e.g. CN, OU.



18.6.1.4 Distribution of the SPE Certificate

Import SPE certificate: **IP Devices** > **IP Gateway Configuration** > **VoIP Security** > tab **Credentials**

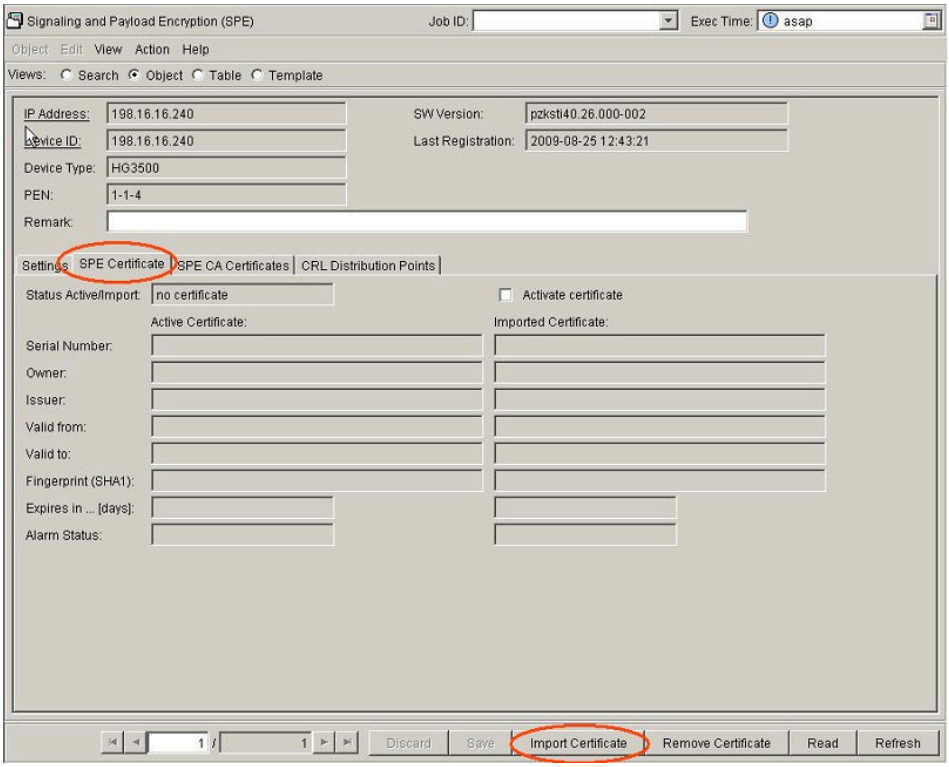


Figure 392: Browse for the certificate.

The importing and activation of the certificate can be combined in one step.

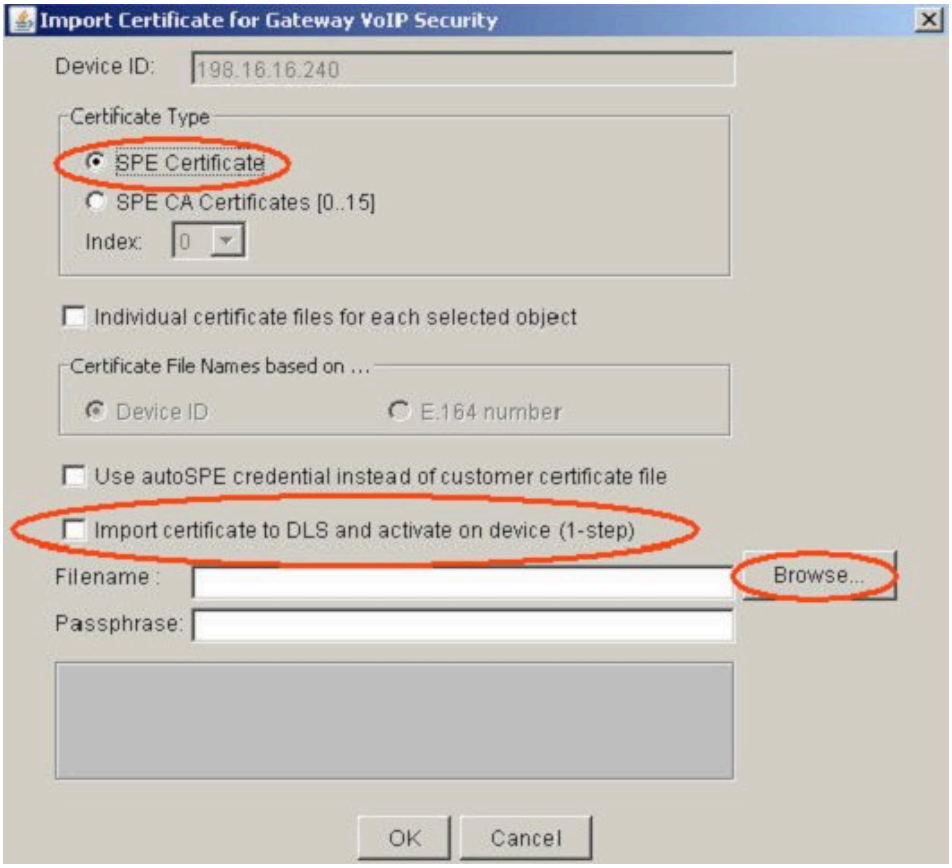
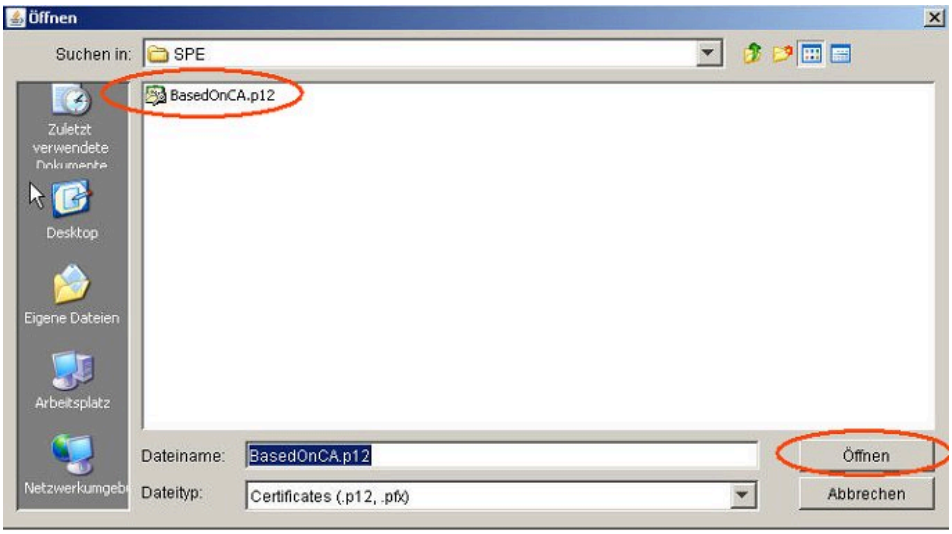


Figure 393: Select the certificate.



Passphrase is the password which is used to encrypt the content of the p12 file. It is created when the p12 file was created.

IMPORTANT: Don't confuse this passphrase with the passphrase configured in Assistant and used to activate Secure Trace. These two passphrases have nothing to do with each other.

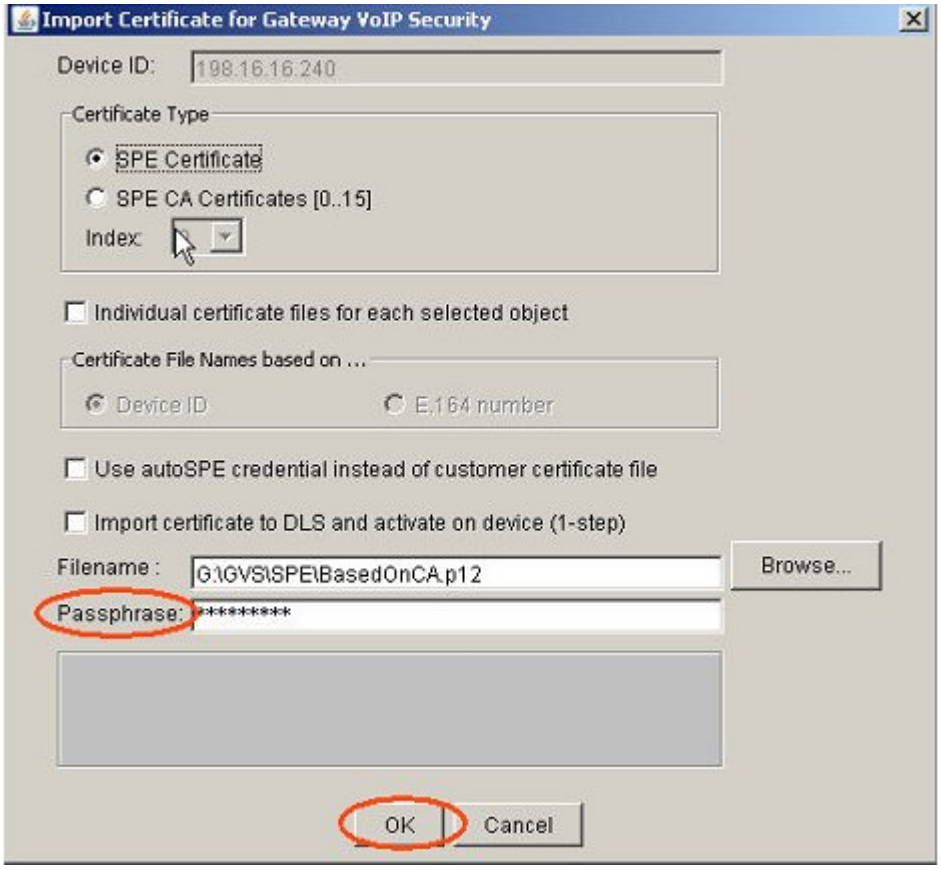


Figure 394: The certificate has been successfully imported.



Figure 395: Activate the certificate.

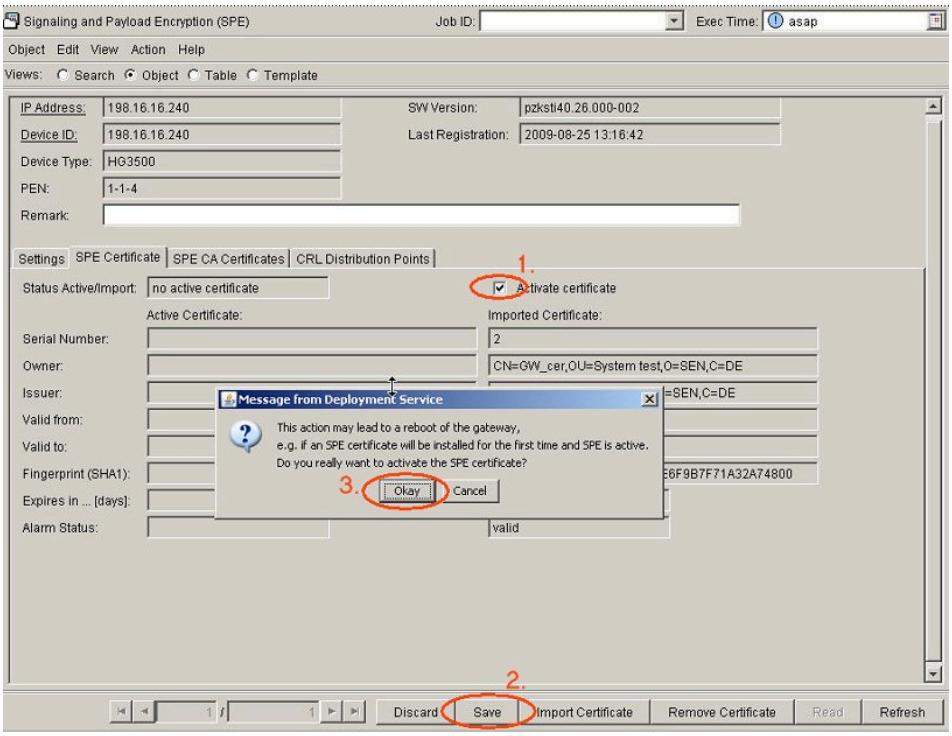
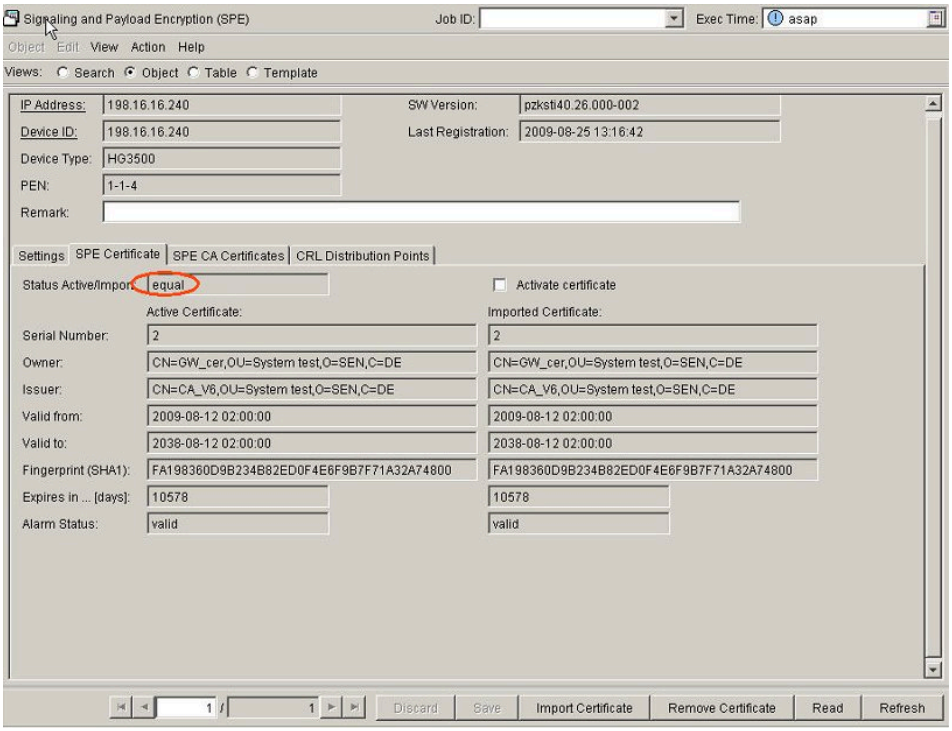


Figure 396: Certificate is active. Status (Status active/Import) is equal.



You can use the WBM application in HG 3500/3575 V4 and newer to check if the import operations worked properly and the certificates were activated. Access is possible with the HiPath 4000 Assistant.

Menu: Menu: **Expert Access** > HiPath **4000** > **HG35xx Web Based Management**

In the WBM you can view the certificates in the following directory:

1) **Configuration** > **Security** > **Signaling and Payload Encryption (SPE)**

There should be two entries:

- SPE Certificate
- SPE CA Certificate(s)



18.6.1.5 Resetting Bootstrapping

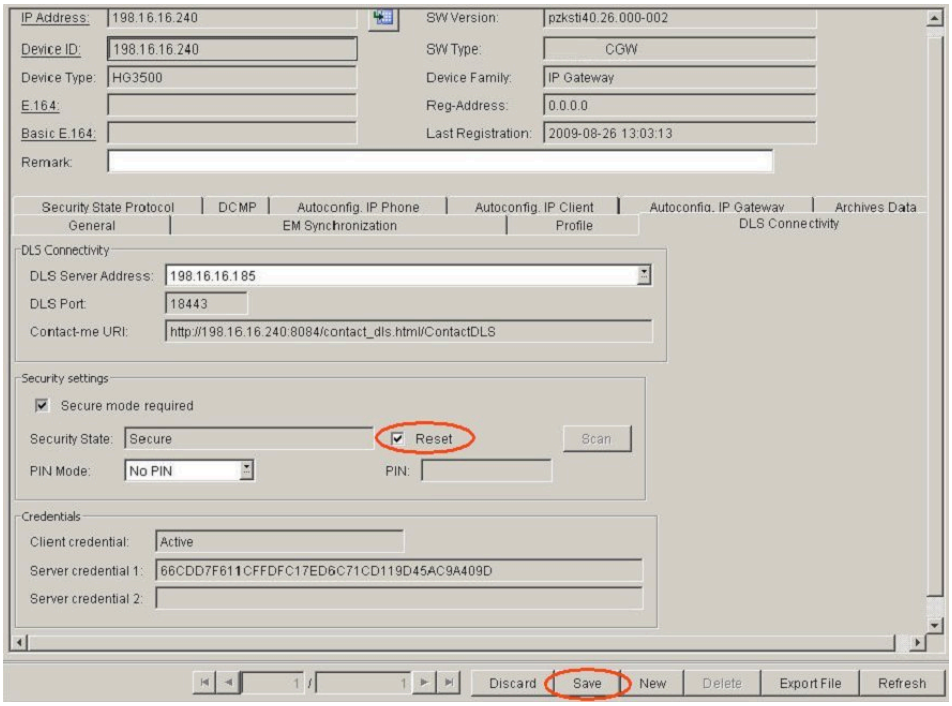
Should it happen that the DLS and the gateway can no longer communicate with one another, the bootstrapping between the DLS and the gateway must be reset.

18.6.1.5.1 DLS Bootstrapping Reset

Reset button functionality:

If this checkbox is activated, the security mode can be reset to "Insecure" by clicking Save.

The DLS must then send a new security configuration to the IP device, i.e. the bootstrap operation must be repeated.



18.6.1.5.2 Gateway Bootstrapping Reset

CLI command:

reset dls bootstrapping

IMPORTANT: There is no CLI with virtual gateways. Reset bootstrapping should be performed in that case with WBM.

18.6.2 Distribution of Certificates to Subscribers

18.6.2.1 Distribution of a CA Certificate

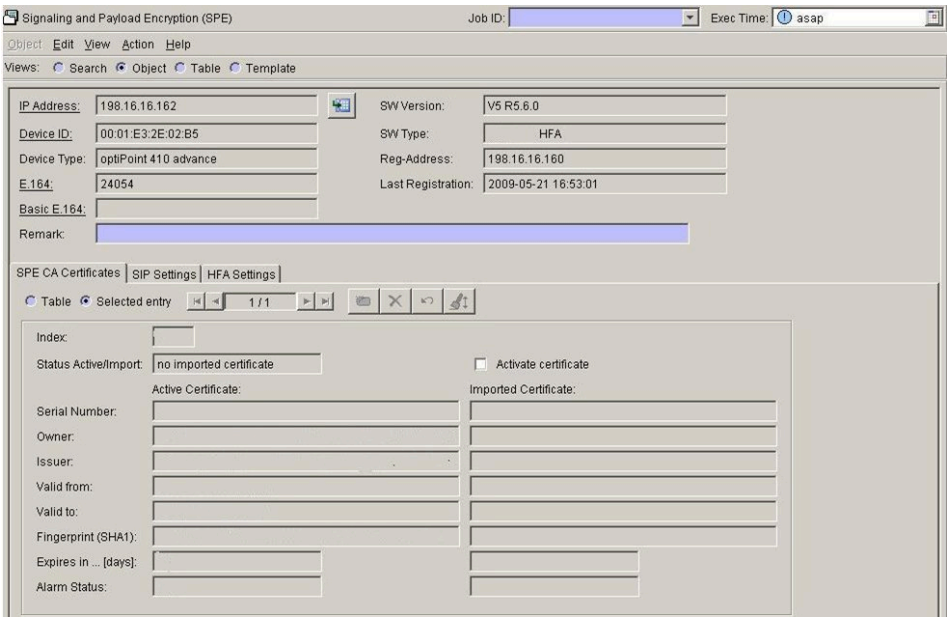
In the subscriber the transport protocol can be set to TCP or TLS (via menu, WBM of the subscriber or DLS). If **encryption** is used the protocol **TLS** must be used for the subscriber.

An IP subscriber only gets a CA certificate. The SPE certificate will be sent directly from the gateway to the IP subscriber, if the subscriber is working with the TLS protocol.

The CA certificate can be distributed to the phone only via the DLS. A manual distribution as for the gateways is not possible.

Distribution of the certificate to the subscriber via DLS.

IP Devices > **IP Phone Configuration** > **Signaling and Payload Encryption (SPE)** > tab **SPE CA Certificate**



Select the CA certificate by using the button **Import Certificate** and **Browse**.

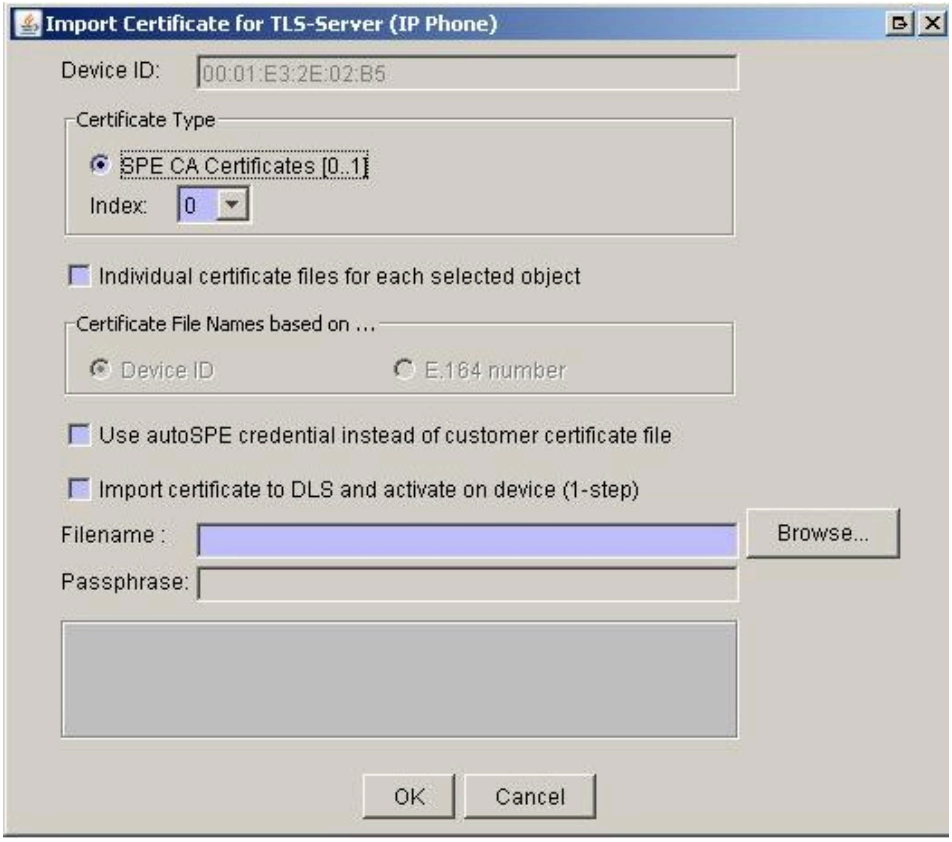


Figure 397: If the import of the certificate was successful a message is displayed.

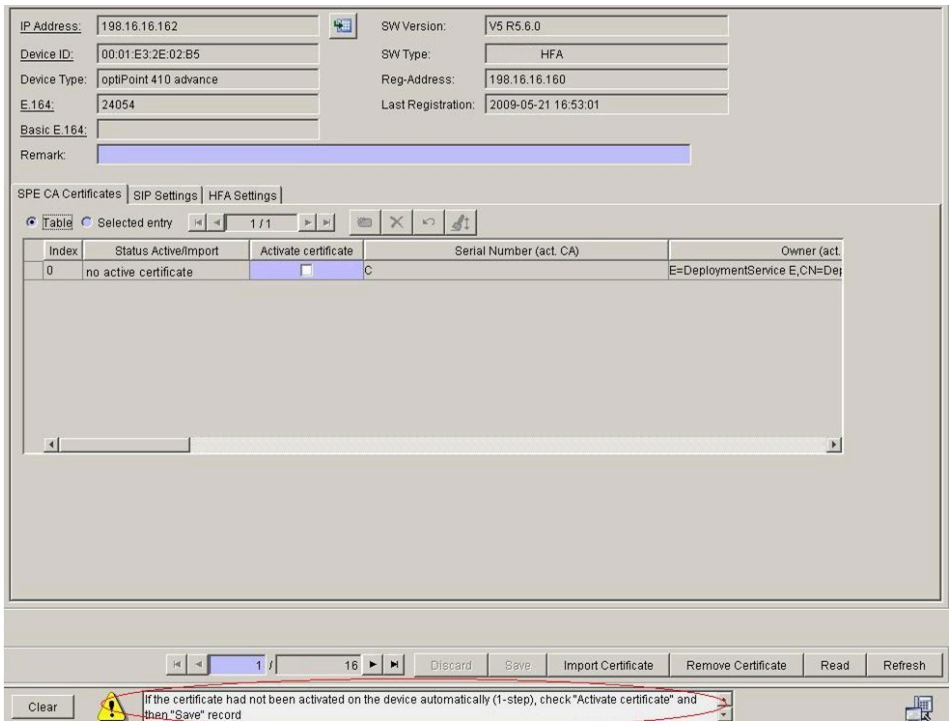
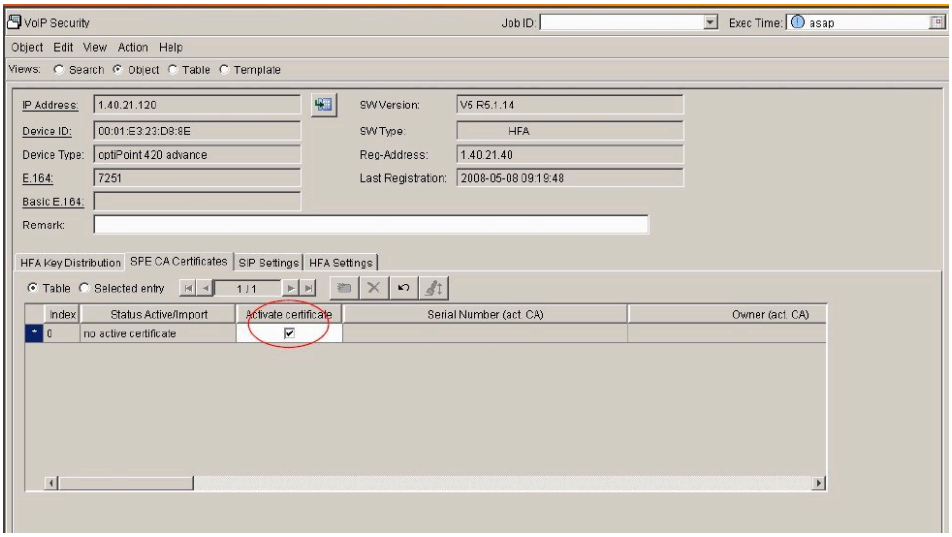
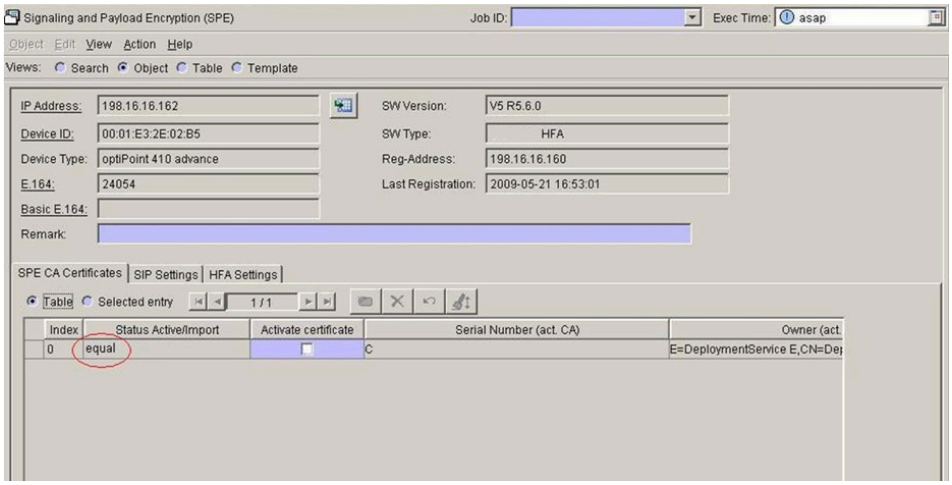


Figure 398: Activation of the certificate.



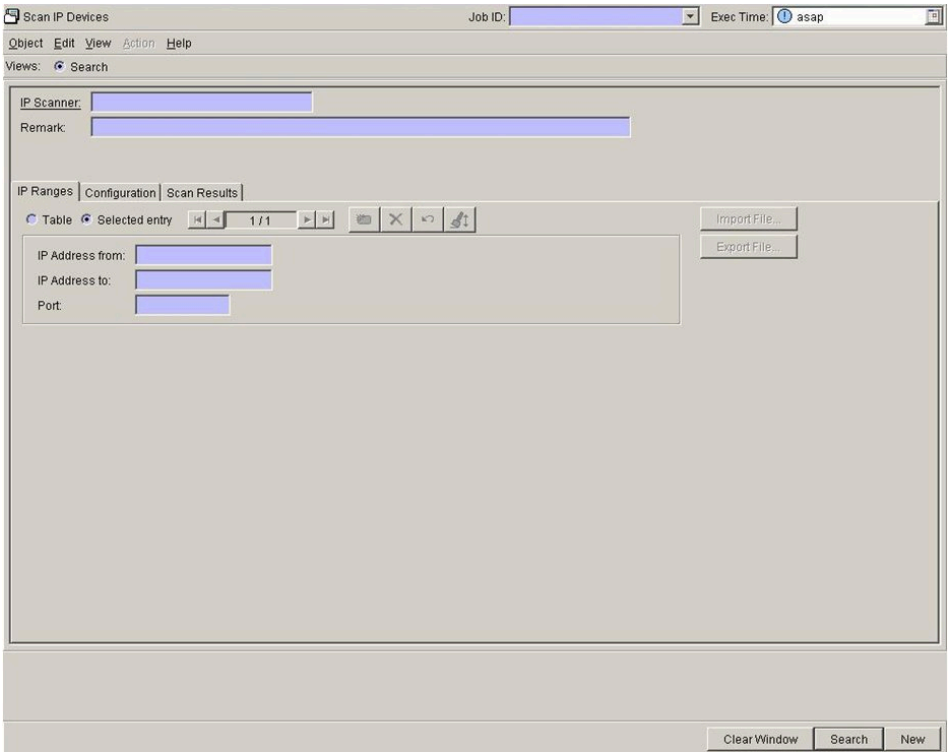
If the activation was successful the status (**Status Active/Import**) will change from **no active certificate** to **equal**.



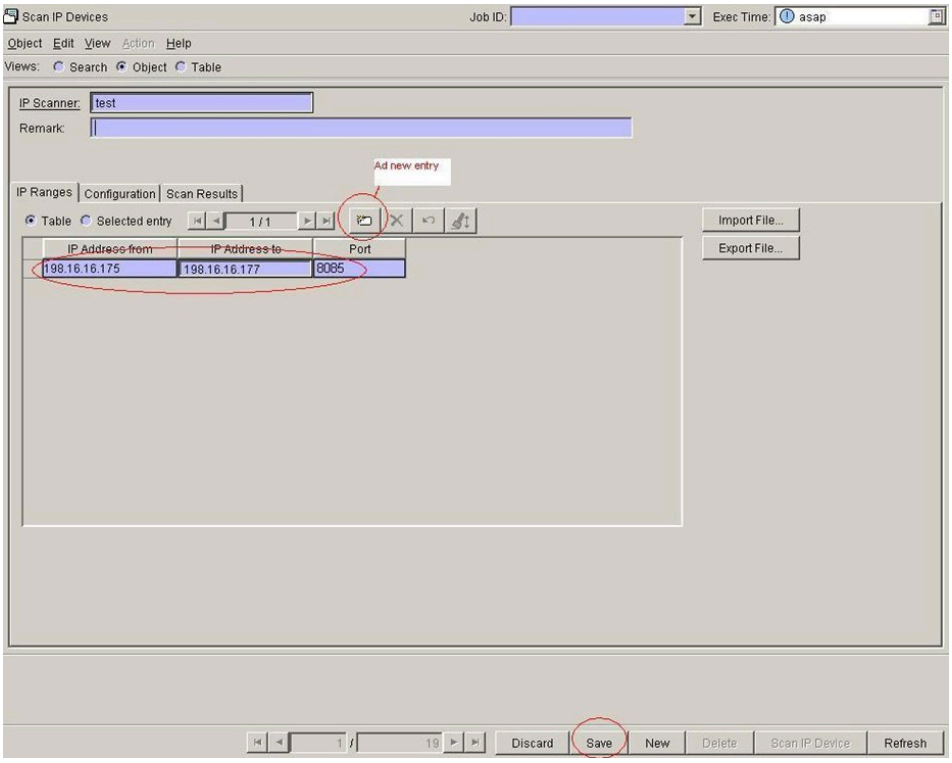
18.6.2.2 Scanning the IP Devices

To add the IP subscribers in the DLS it is needed to scan the IP range from where the subscribers belong.

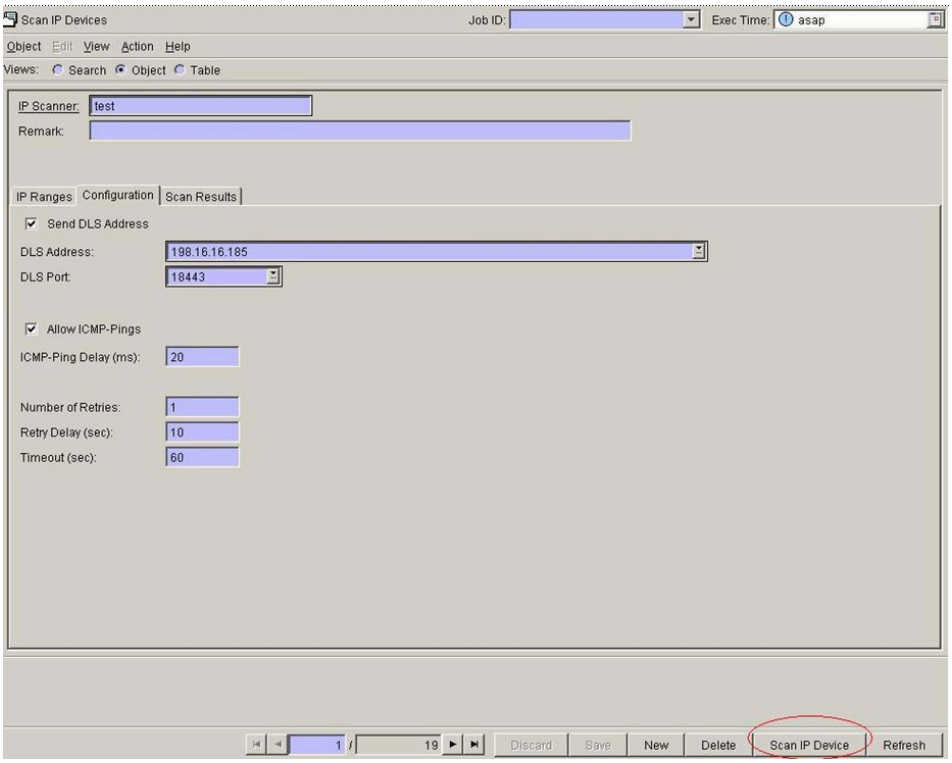
IP Device > **IP Device Interaction** > **Scan IP Device**



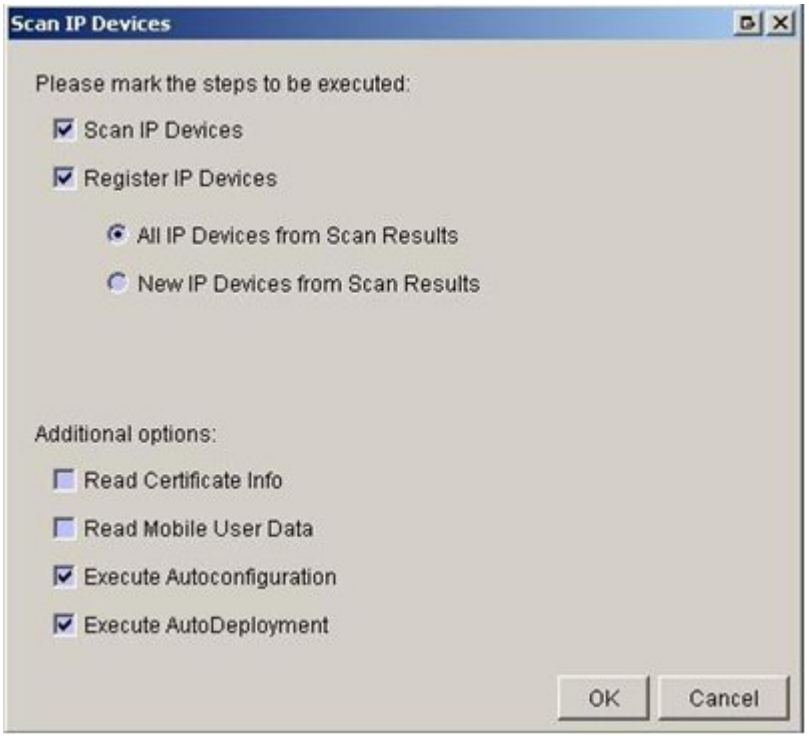
IP Ranges tab: Set name for the **IP Scanner**, IP address range (**IP Address from, IP Address to**) and **Port 8085**.



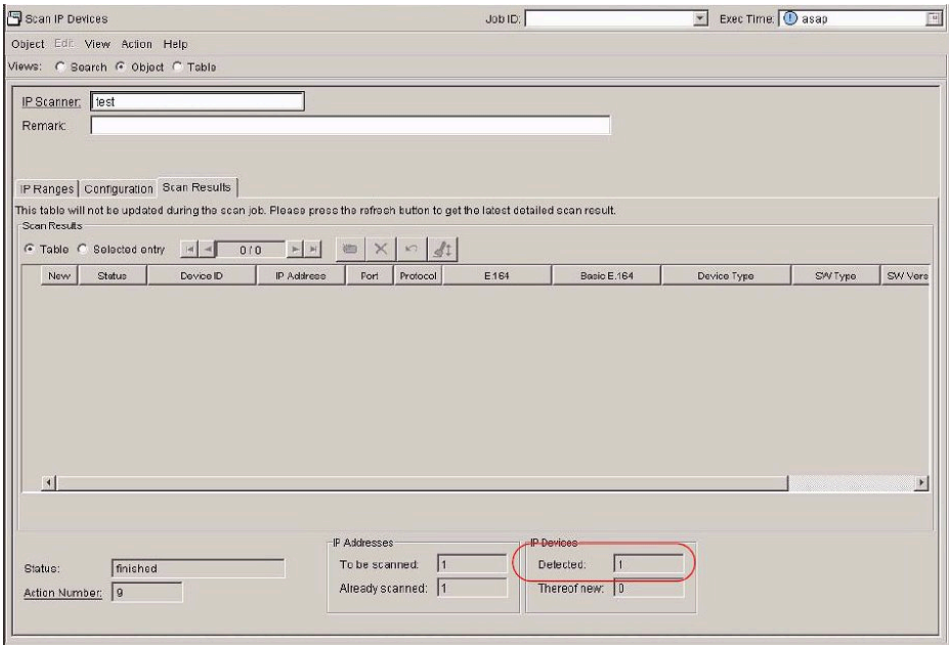
Configuration tab: Set IP Address of DLS (**DLS Address**) and **DLS Port** and select check box **Send DLS Address**. Start the scan with the button **Scan IP Devices**.



Select **Scan IP Devices**, **Register IP Devices** and **All IP Devices from Scan** and then select **OK**.



Scan Results tab: Number of detected gateways (**IP Devices > Detected**) will be shown.



18.7 AutoSPE Configuration (DLS)

IMPORTANT: This chapter is only intended as a brief overview of the necessary steps in the Deployment Service (DLS). For a detailed description, refer to the DLS Administrator Manual.

IMPORTANT: If a board has a separate Management LAN interface configured, DLS bootstrapping will use the MAN IP address instead of the VOIP IP address.

IMPORTANT: Starting with OpenScape 4000 V7 R1.8 Secure Hash Algorithm SHA2 (SHA224, SHA256, SHA384, SHA512) is supported. Prior to OpenScape 4000 V7 R1.8 Auto SPE needs to be explicitly configured for SHA128 on DLS side via a function available from DLS V7 R1.11.2. Please refer to section 16.5.6 “SHA1 Configuration for AutoSPE” from documentation “OpenScape Deployment Service V7, Administrator Documentation”.

The area of automatic SPE configuration in DLS enables automatic configuration of PKI-based Signaling and Payload Encryption (SPE) for users. This is especially useful when there is no client PKI.

DLS supports the generation and deployment of SPE CA certificates (CA= Certificate Authority) for administered IP devices (gateways and subscribers). When activating an SPE CA certificate, a SPE CA certificate is generated and deployed for each administered gateway.

Via export and import, it is possible to migrate CA certificates from one DLS to another.

With automatic SPE configuration via DLS, all subscribers that are known in DLS also receive the CA certificate (independently of the gateway) generated by the AutoSPE configuration. The validity of this certificate can be checked in the security settings of the subscriber (DLS: HFA Server Validation, Phone: Certificate Check).

18.7.1 OpenScape 4000

Requirements for SPE

IMPORTANT: SPE certificates can be configured at the gateways even if SPE is deactivated.

1) An NTP server must be configured for time synchronization.
2) The following must be set in AMO ZANDE SPESUPP=YES: CHANGE-ZANDE:TYPE=SECURITY,SPESUPP=YES; In case AP shelves or SoftGate are configured also following command should be executed: CHANGE-SIPCO:TYPE=SECURITY,IPDAENCR=Y;
3) In case of duplex configuration, the standby node should be restarted as well:

EX-REST:TYPE=UNIT,UNIT=BPS,RSLEVEL=HARD; EX-REST:TYPE=UNIT,UNIT=BP,RSLEVEL=HARD;

1) Following subscriber settings must be verified: The parameter CLASSEC=SECURE must be set in AMO SDAT for each SPE subscriber:

CHANGE-SDAT:TYPE=DATA1,CLASSEC=SECURE;

1) You have to check in AMO CGWB for HFA stations if the value in the parameter branch **TYP=GLOBIF** is **TLSP=4061**.

18.7.2 Deployment Service (DLS)

18.7.2.1 DLS Time Server

For example: Freeware tool "Nettime"

IMPORTANT: The Windows Time Service must be ended.

18.7.2.2 Preparing DLS

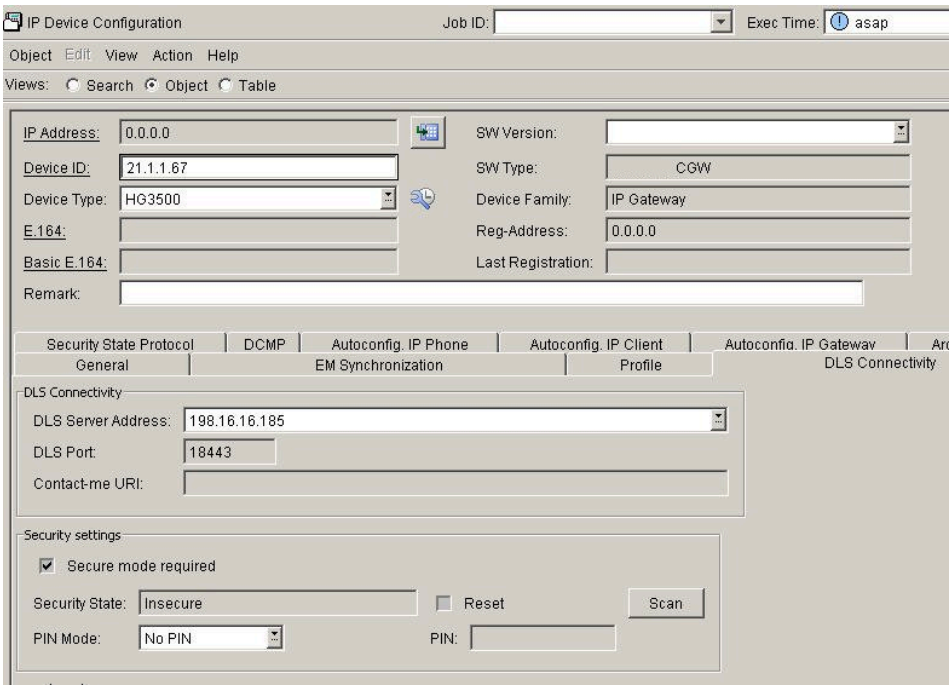


Figure 399: Creating a Virtual Device / IP Gateway

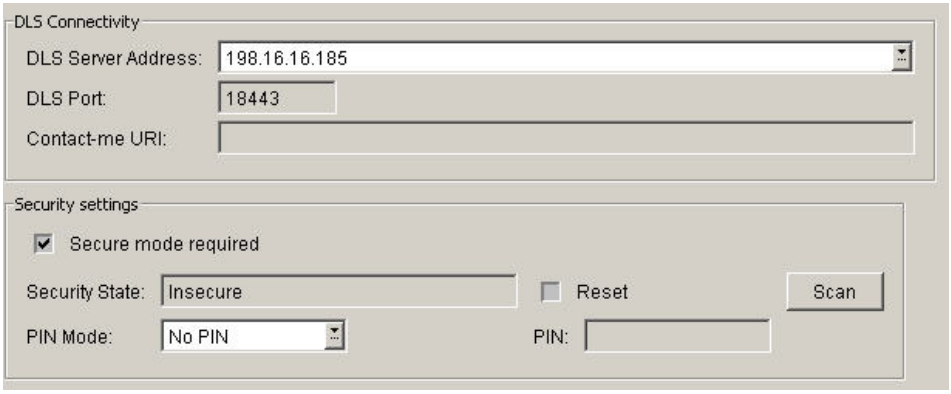


Figure 400: Scanning an IP Gateway

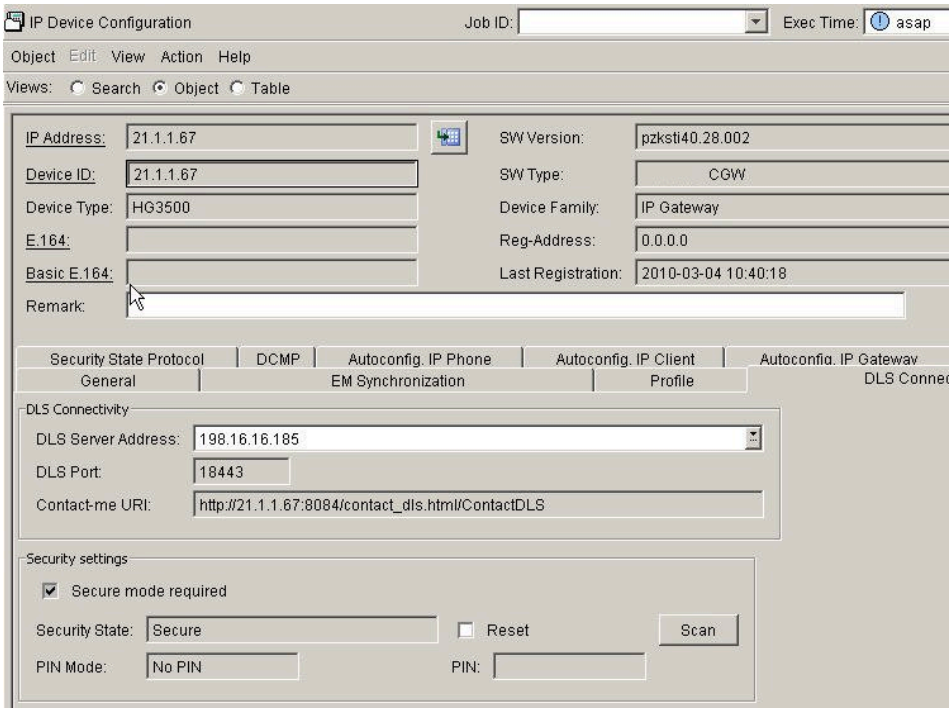


Figure 401: IP Gateway "scanned"

18.7.3 Device Configuration

18.7.3.1 Preparations

IMPORTANT: The value for H.225.0 TLS must be 1300.

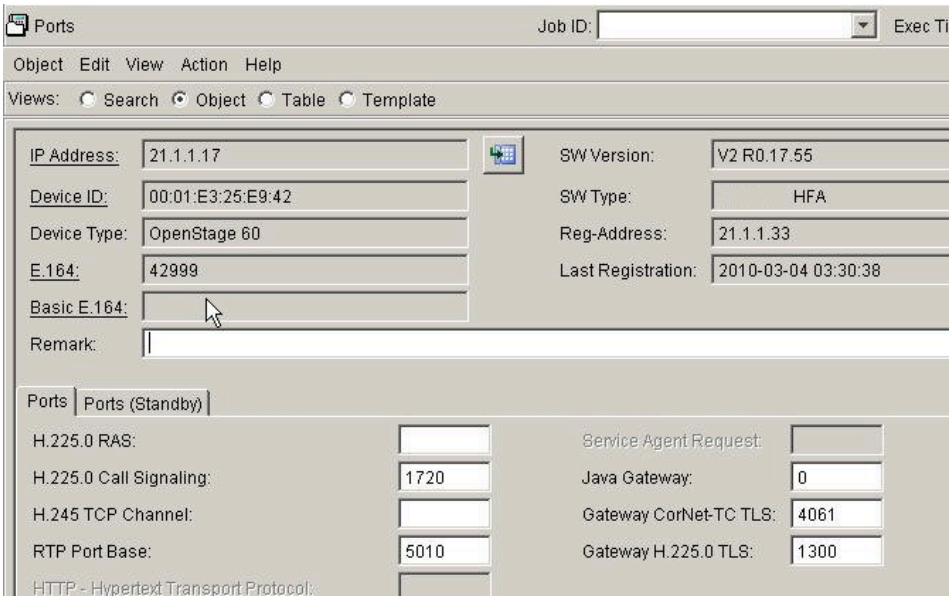


Figure 402: Preparing Devices

The display and trace time can be set to "SNTP".

18.7.3.2 Time Server

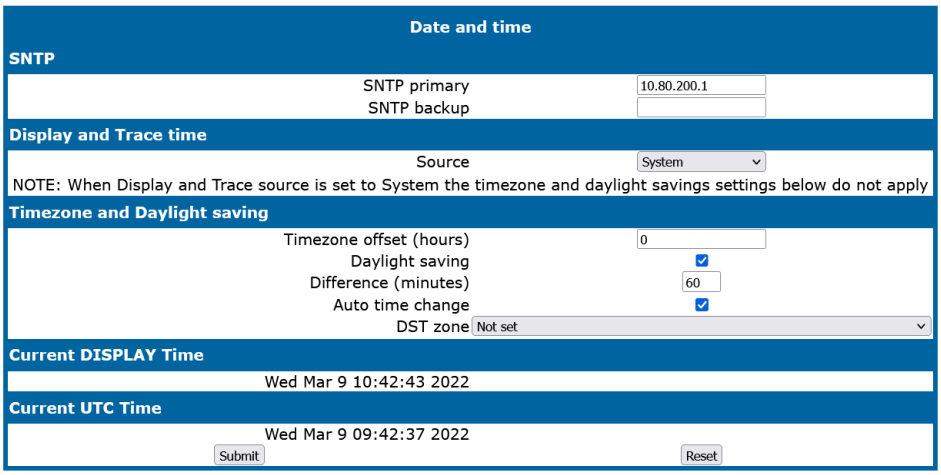


Figure 403: Time Server Devices

18.7.4 Automatic Certificate Creation

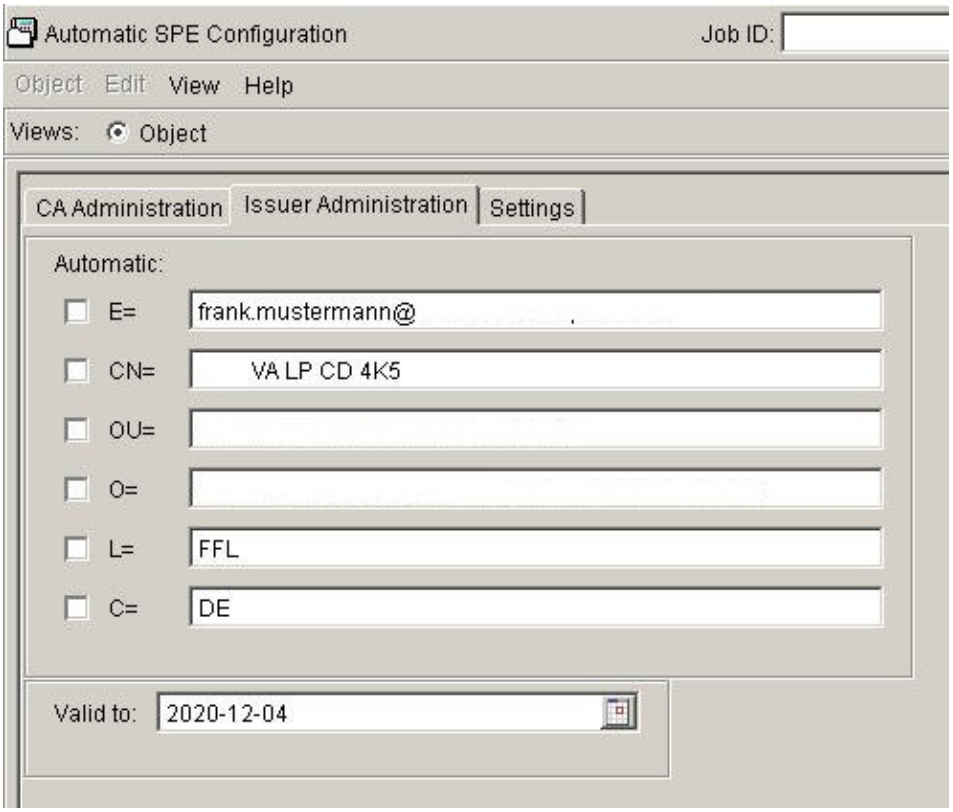


Figure 404: Issuer: Administration

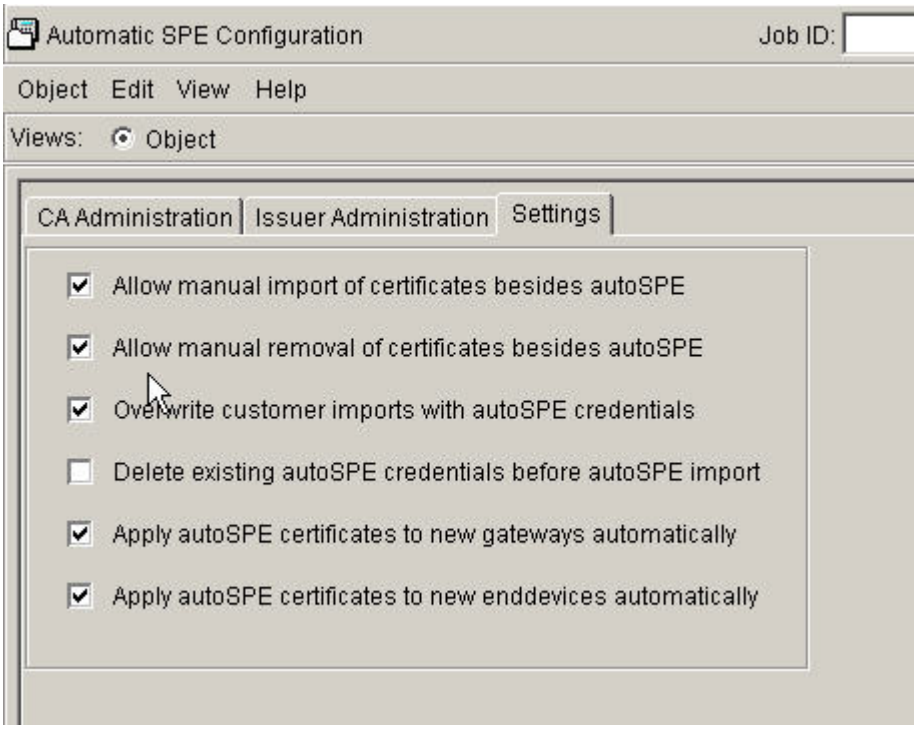


Figure 405: Issuer: Administration > Settings

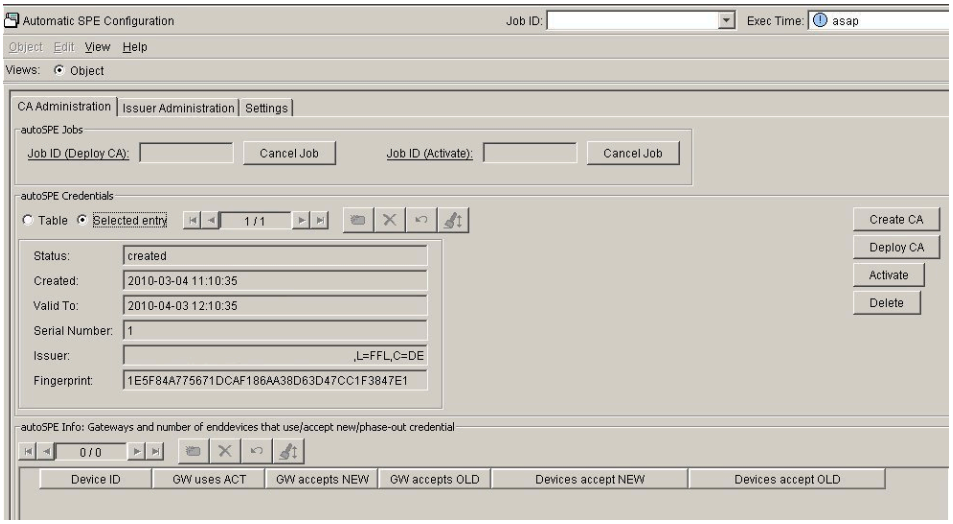


Figure 406: CA Administration

In the case of CA administration, a certificate must first be created, then distributed, and finally activated. This can be displayed in the status.

The lower table shows how many subscribers have received certificates.

18.7.5 Activate Voice Encryption

To activate voice encryption from SPE, the transport protocol must be switched to "TLS":

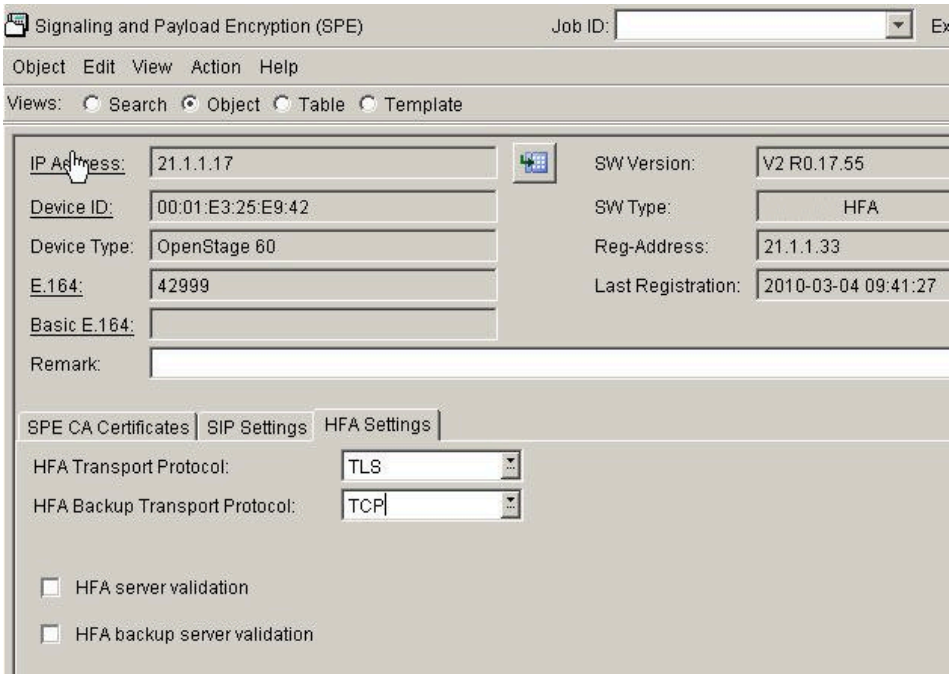


Figure 407: Activate Voice Encryption

18.7.6 Check Certificates

Display the current certificate on the subscriber: SPE CA certificate(s)

Display the current certificate on the gateway: SPE CA certificate(s)

IMPORTANT: Both certificates must always be identical.

18.7.7 Display of SPE Status

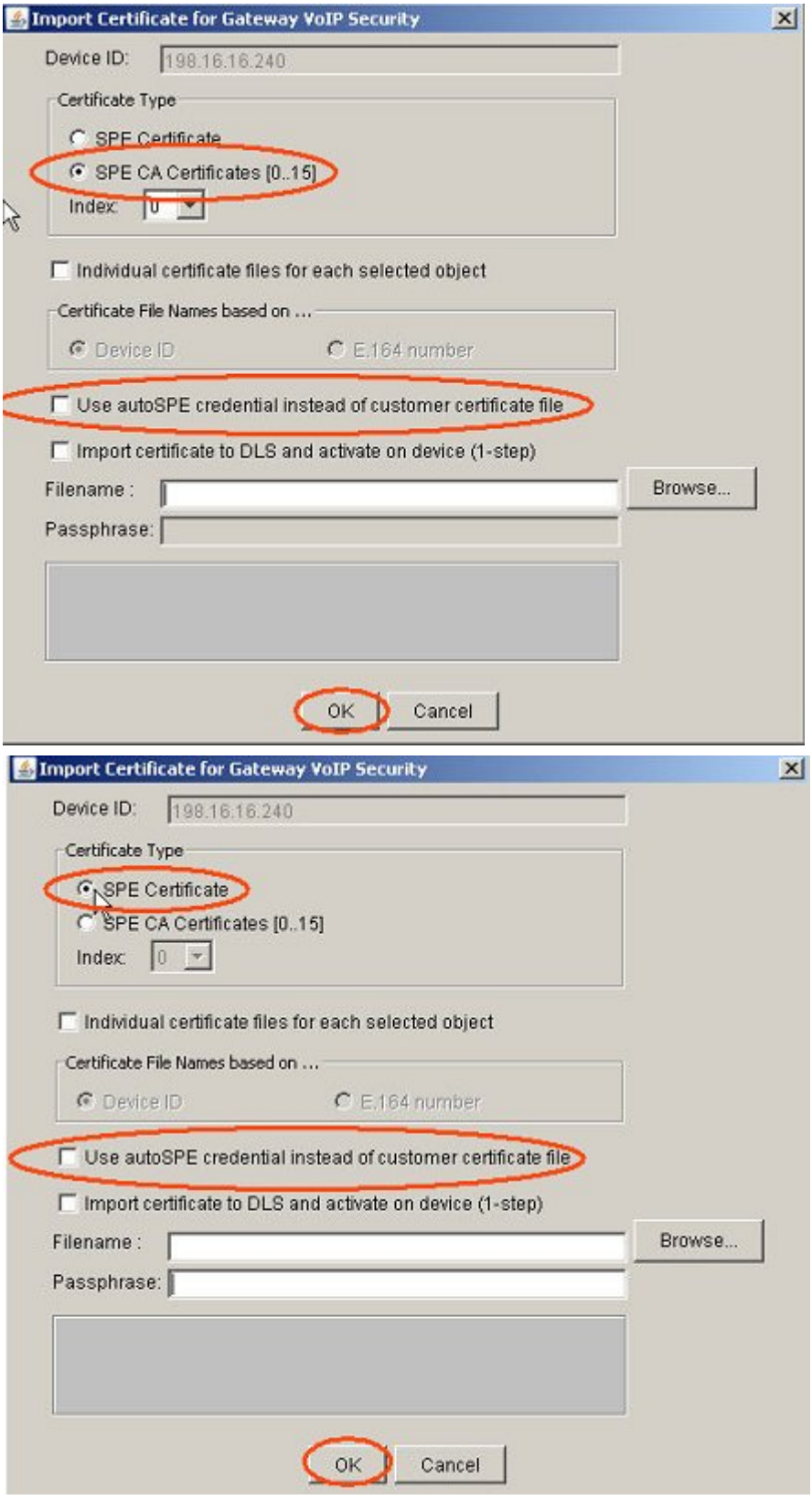
A key can be configured in AMO TAPRO to display the SPE status of the subscriber (see Section 3.4.4, “Signaling at the Display”).

18.7.8 Adding new Gateways after AutoSPE Activation

The board has to be added in DLS as a virtual device, bootstrapped and scanned as explained in Chapter 7, “Distribution of Certificates to Gateways”).

You will then be able to see the board in the board list under AutoSPE configuration, also under **IP Devices** > **IP Gateway Configuration** > **Signaling and Payload Encryption (SPE)**.

In order to send the already generated AutoSPE CA and SPE certificates to the new gateway, you have to go to **IP Devices** > **IP Gateway Configuration** > **Signaling and Payload Encryption (SPE)**. From there you can manually import the certificates onto the new gateway.



18.8 MTLS Implementation on CGW and SG

18.8.1 System Setting

System configuration is identical to normal SPE, please see Chapter 8, “OpenScape 4000”.

18.8.2 Enabling Enforce Secure TLS Renegotiation (RFC 5746)

You can use secure renegotiation for HFA devices (not OptiPoint). Possible values are from 0 to 167 hours, 0 disables renegotiation.

1) Activation/Deactivation on CGW:

STMI WBM > Configuration > Security > Signaling & Payload encryption (SPE) > click on **SPE Security Setup > Edit Security Setup > Enforce Secure Renegotiation (RFC 5746)**

1) Re-keying interval on CGW:

STMI WBM > Configuration > Security > Signaling & Payload encryption (SPE) > click on **SPE Security Setup > Edit Security Setup > Maximum Re-Keying interval**

1) Activation/Deactivation on SG:

NCUI WBM > Configuration > Security > Security Options > Enforce Secure TLS Renegotiation (RFC 5746)

1) Re-keying interval on SG:

STMI WBM > Configuration > SPE > SPE Security Setup > Maximum Re-Keying interval

18.8.3 Device Setting

18.8.3.1 OpenStage Phones

WBM> Administrator Pages > System > Security > System

For SPE choose from **Signaling transport main** and **Signaling transport** select box **TLS** protocol.

In order to validate GW certificate on phone side fill **Certificate validation main** and **Certificate validation** check boxes.

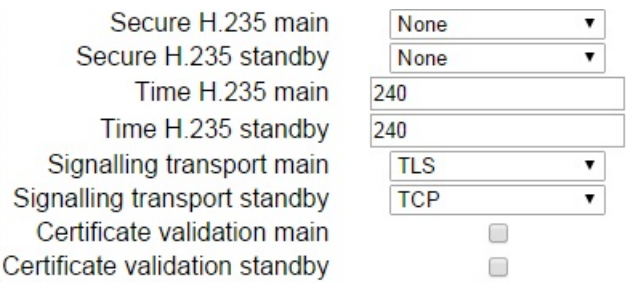


Figure 408: OpenStage SPE Enable

18.8.3.2 OpenScape Desk Phones

OptiPoint phone support SPE but not mutual TLS. GW certificate verification is possible only.

WBM> Administration > System > Signaling & Payload Encryption (SPE)

For SPE choose from **Transport mode** select box **TLS** protocol for **Base** and .

In order to validate GW certificate on phone side fill **both Certificate check** boxes.

18.8.4 DLS Device Setting

18.8.4.1 Protocol Setting

For device protocol setting is possible to use also Deployment service server. This option is located in the menu: **Deployment service > IP Devices > IP Phone Configuration > Signaling & Payload encryption > HFA Setting > HFA Transport Protocol**

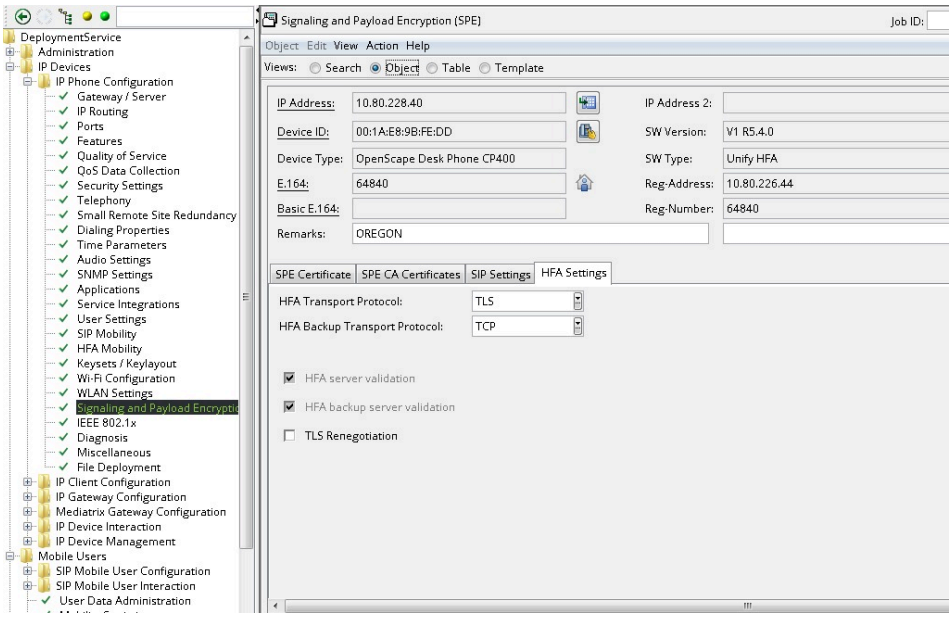


Figure 409: DLS Phone Protocol Setting

For SPE choose from **HFA Transport Protocol** and **HFA Backup Transport Protocol** select box with item **TLS** protocol.

In order to validate GW certificate on the phone side fill **HFA server validation** and **HFA backup server validation** check boxes.

18.8.4.2 Certificate Upload

Certificate for the phone verification on the GW side is possible to upload to the phone via DLS server only.

This option is located in menu: **Deployment service > IP Devices > IP Phone Configuration > Signaling & Payload encryption > SPE Certificate**

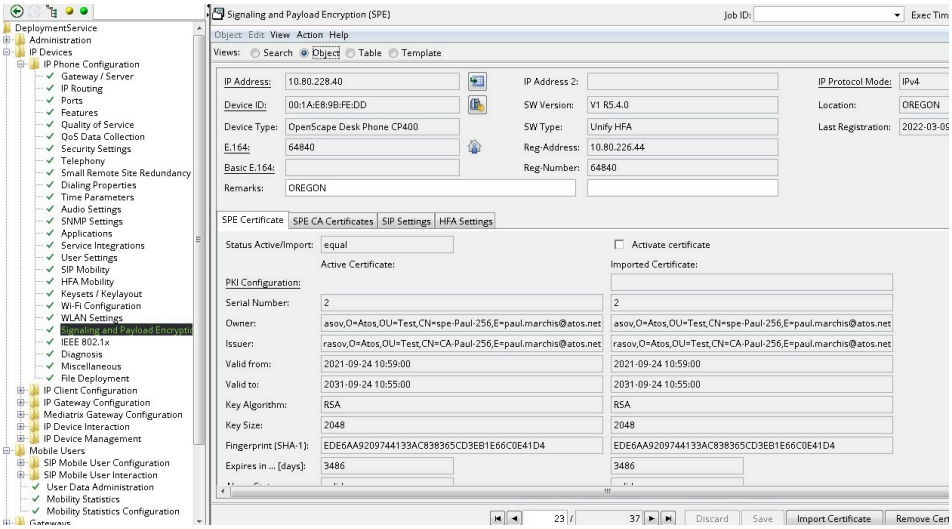


Figure 410: DLS Phone Certificate Setting

For new certificate import or currently used certificate rewriting use **Import Certificate** button. On following screen press **Browse** button and select appropriate certificate file to import. Insert the private key password, fill **Import certificate to DLS and activate on device** check box and press **OK**.

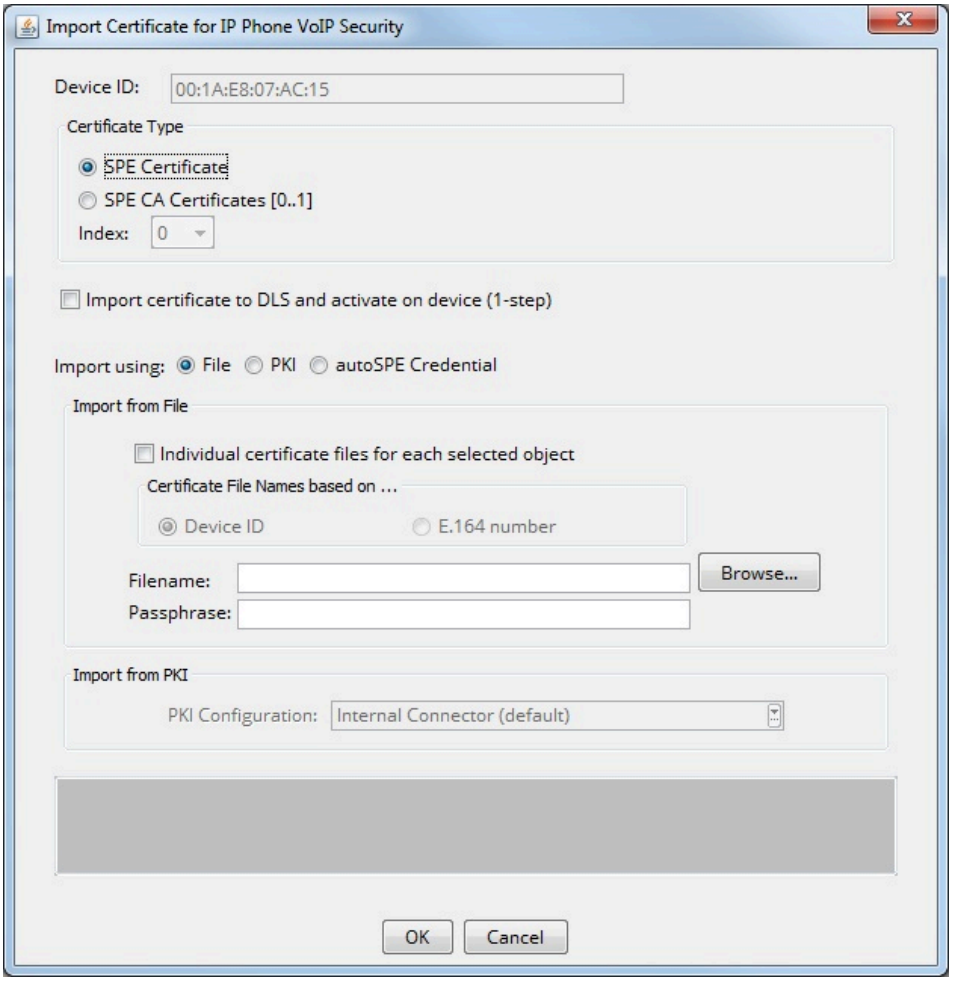


Figure 411: DLS Phone Import Certificate Dialog

18.8.4.3 CA Certificate Upload

CA Certificate for the GW certificate verification is possible to upload to the phone via DLS server only.

This option is located in menu: **Deployment service > IP Devices > IP Phone Configuration > Signaling & Payload encryption > SPE CA Certificate**

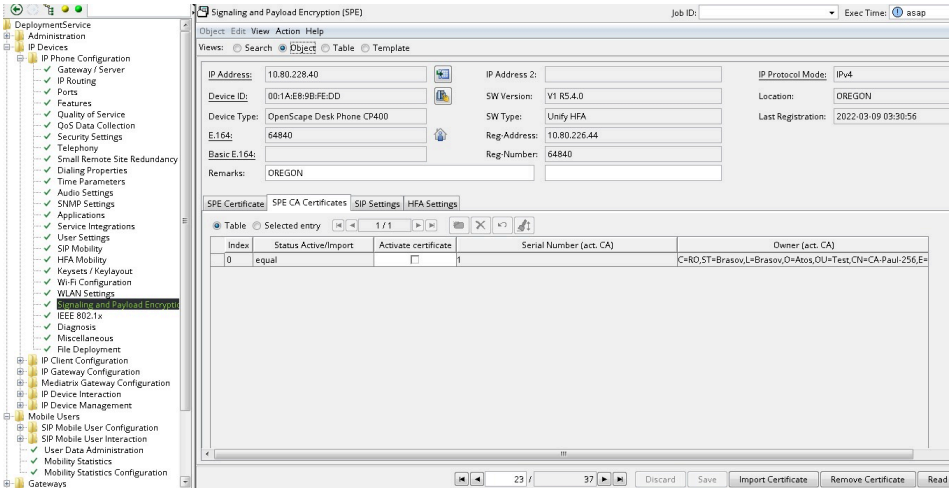


Figure 412: DLS Phone CA Certificate Setting

For new CA certificate import or currently used CA certificate rewriting use **Import Certificate** button. On following screen press **Browse** button and select appropriate CA certificate file to import. Check **Import certificate to DLS and activate on device** check box and press **OK**.

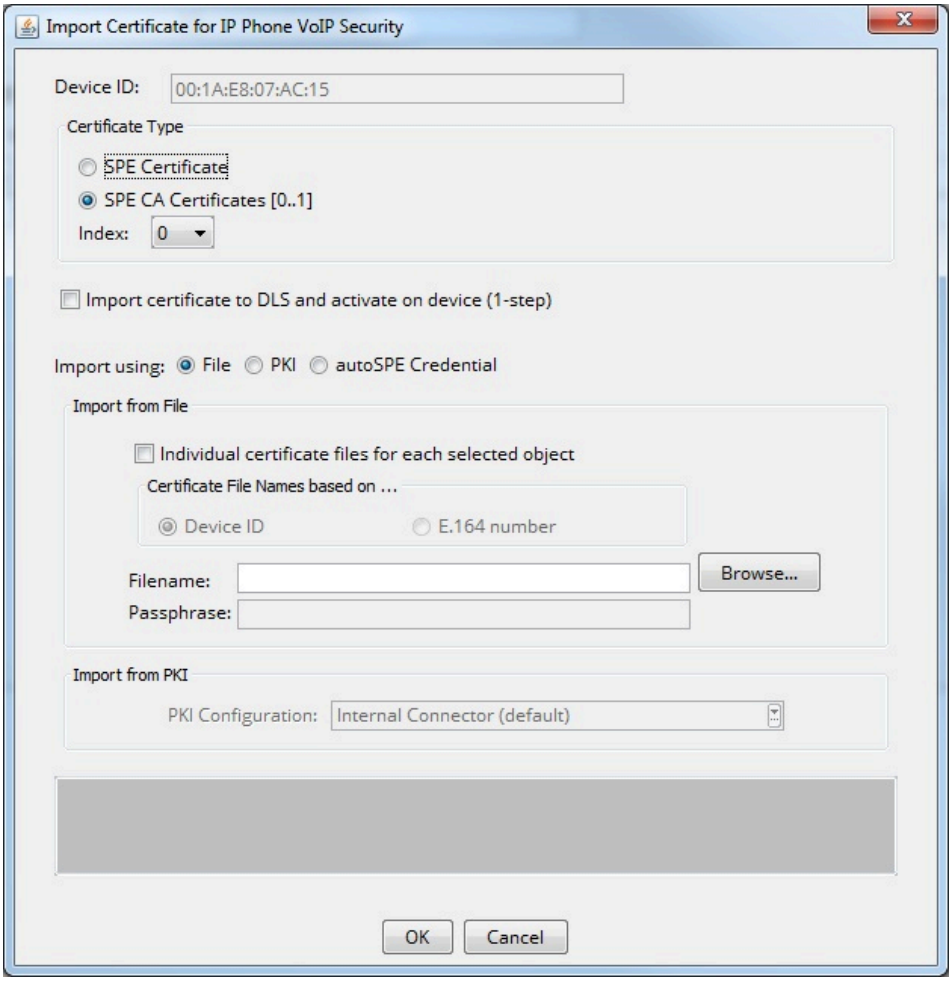


Figure 413: DLS Phone Import CA Certificate Dialog

18.8.5 HFA Implementation

18.8.5.1 CGW

18.8.5.1.1 Configuration

MTLS for HFA is indirectly enabled or disabled via option **Certificate Verification Level** in HG3500 WBM. This option is located in menu:

Configuration > Security > Signaling and Payload Encryption (SPE) > SPE Security Setup > HFA/H.323 TLS Parameters.

In order to adjust settings single click on **SPE Security Setup**.

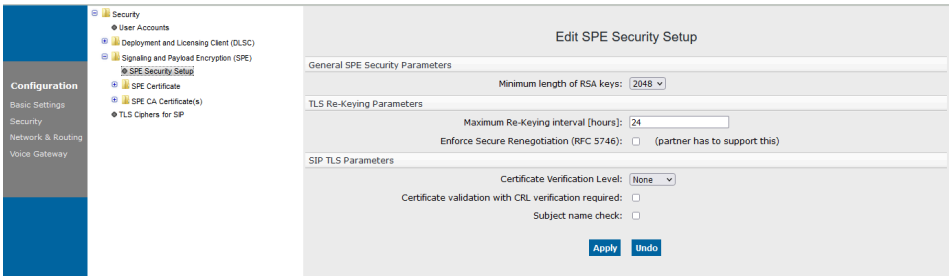


Figure 414: HFA SPE Configuration

When verification level is set to **Trusted** or **Full**, client certificate is requested and verified during SSL/TLS handshake. Client certificate must be signed by some trusted CA, whose public key certificate must be present on CGW (more CA certificates can be present).

18.8.5.1.2 CA Certificate Management

CA certificate is imported in PEM or DER format via HG3500 WBM:

Configuration > Security > Signaling and Payload Encryption (SPE) > click on **SPE CA Certificate(s) > Import trusted CA certificate (PEM or binary)**

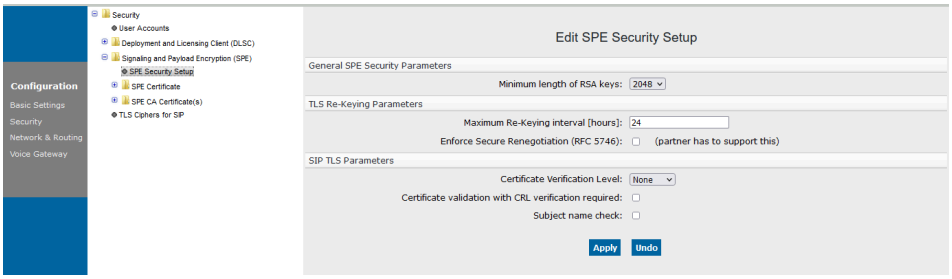


Figure 415: HFA SPE CA Certificate Import

On following screen press button “**Browse..**” and select appropriate CA certificate file to import. If CRL distribution point for imported CA is available, select CRL distribution method (currently only HTTP is supported) and fill CDP address in text field CDP.

IMPORTANT: Before CA certificate is imported in CGW, its fingerprint must be verified because from now on will be this certificate treated as trusted.

List of currently available trusted certificates present on CGW can be found in:

Configuration > Security > Signaling and Payload Encryption (SPE) > single-click **SPE CA Certificate(s).**

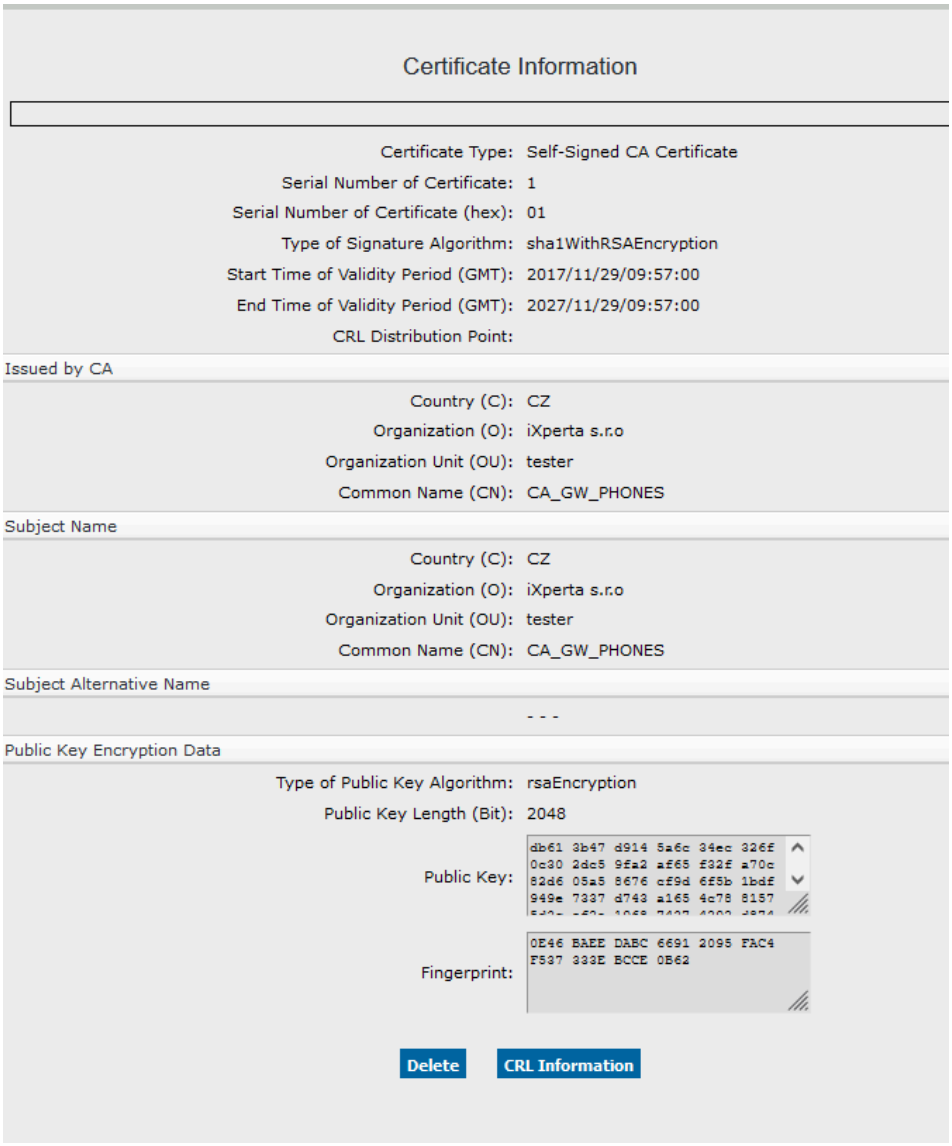


Figure 416: HFA SPE CA Certificate

To view CA certificate details, click on appropriate entry in list. To view CDP address and list of currently revoked client certificates click *CRL Information*. Certificate can be removed from trusted certificate list with a single click on certificate in list and select **“Delete.”**

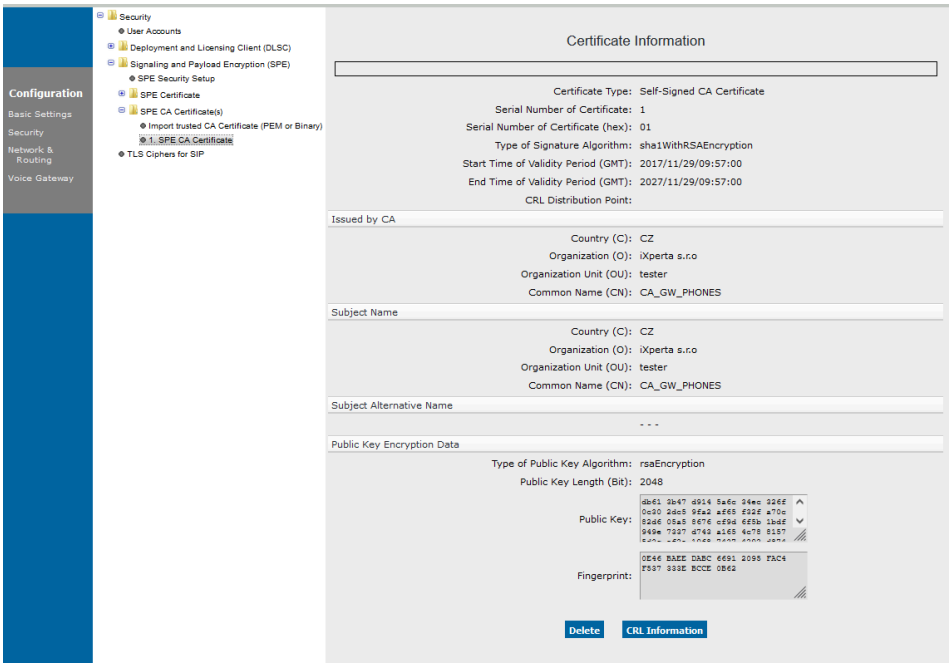


Figure 417: HFA SPE CA Certificate CRL

CRL check is enabled by option:

Configuration > Security > Signaling and Payload Encryption (SPE) > SPE Security Setup > HFA/H.323 TLS Parameters > Certificate validation with CRL verification required.

When enabled, CRL is immediately downloaded from CDP. CRLs updates are downloaded automatically on regular basis when CRL check is on. Note that currently only binary form of CRL is accepted by CGW.

18.8.5.1.3 TLSv1.2

Currently are supported only protocols TLSv1.0 and higher, SSLv2 and SSLv3 are not permitted due to security issues. The default minimum RSA key length is 2048.

TLS version is configured in WBM menu:

Configuration > Security > Signaling and Payload Encryption (SPE) > click on **TLS Ciphers for HFA > Edit TLS Cipher Configuration.**

On following screen can be configured deployed TLS version, key agreement method, encryption algorithm and used mode of operation (see https://www.ietf.org/rfc/rfc5246.txt for more information about TLSv1.2).

IMPORTANT: After changing and saving TLS HFA settings, CGW must be rebooted for the changes to take effect.

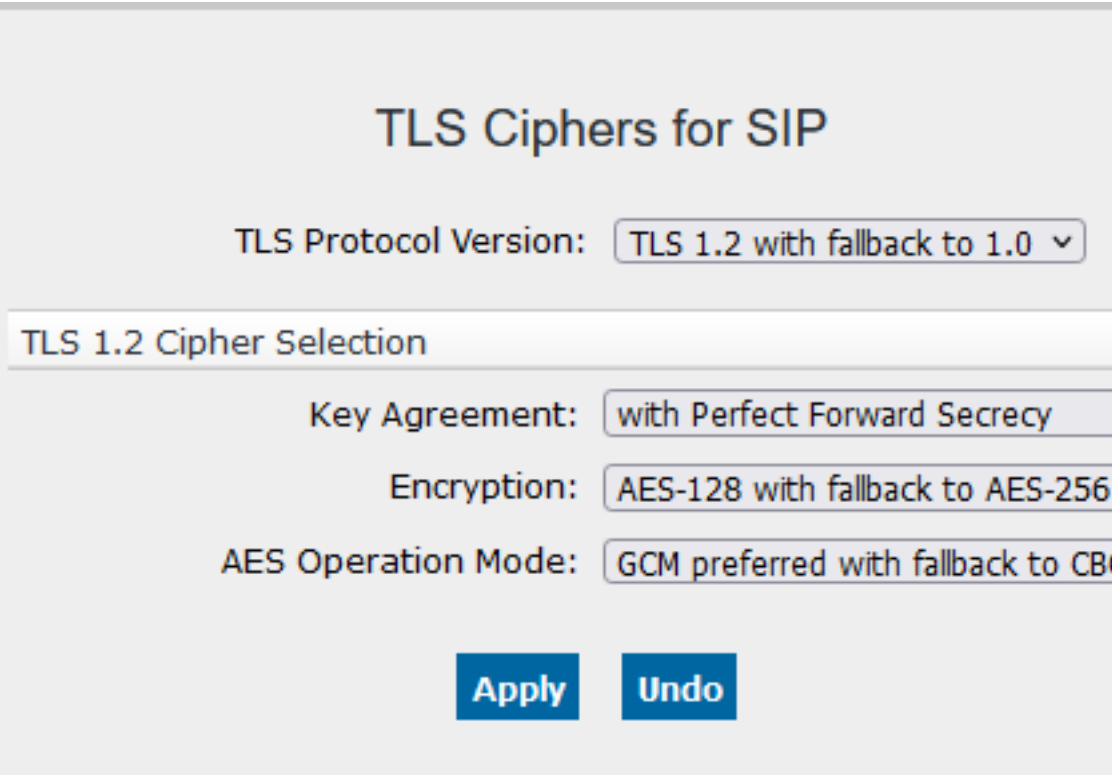


Figure 418: HFA SPE Configuration TLS

18.8.5.1.4 Trusted Level Features

When MTLS is enabled on level **Trusted**, client certificate is requested and verified in every SSL/TLS handshake (in initial handshake and also in every succeeding renegotiation).

Last certificate in certificate chain supplied by the client must be signed by one of trusted CA. None of the certificates in the chain may be expired, otherwise handshake fails immediately and connection is terminated.

When CRL revocation check is active, all unexpired CRLs are examined in order to determine revocation status for every certificate in client certificate chain.

On level **Trusted** are ignored all X509v3 extensions (even unknown and critical).

18.8.5.1.5 Full Level Features

When MTLS is enabled on level **Full**, basic client certificate verification scenario is the same as on level **Trusted**. Additionally, X509v3 extensions of client certificate are examined during SSL/TLS handshake. Certificate verification procedure fails, if any unknown critical extension occurs, or if usage of known extensions (basicConstraints, keyUsage, extendedKeyUsage and nsCertType) violates current standard.

Full client verification level also enables one to perform Subject identity check of client based on SubjectAlternativeName or CommonName present in certificate. Note, that identity check is enabled by default. This behavior can be changed by checkbox:

Configuration > Security > Signaling and Payload Encryption (SPE) > SPE Security Setup > HFA/H.323 TLS Parameters > Subject name check.

Identity check attempts to lookup SubjectAlternativeName or CommonName (respectively) via DNS and obtains IP address associated with this name. If any address is found and the address matches real IP address of connected client then identity check succeeds, handshake fails immediately otherwise.

18.8.5.1.6 Dynamic Behavior

Dynamic features:

1) Change of HFA TLS Parameters

- CA/private certificate addition/removal
- Expiration of CA/private certificate (affects rekeying)
- CRL download

Static features:

- TLS version configuration
- TLS encryption configuration
- TLS key agreement configuration
- TLS AES operation mode configuration

Static features require CGW reboot for the changes to take effect, which is also indicated by icon in WBM. All dynamic features can be adjusted during CGW runtime. Such event triggers new SSL/TLS handshake and client certificate chain verification with all consequences for all active connections. All established calls should survive if handshake succeeds.

18.8.5.1.7 Restrictions

Subject name check: Identity check resolves hostname from phone IP address and compares it with SubjectAlternativeName/CommonName in certificate. However, this behavior might change in future with new Unify recommendations.

Revocation: Only binary form of CRL in DER format is accepted by CGW (not PEM). Conversion can be done e.g. with OpenSSL CRL tool.

18.8.5.2 SoftGate

18.8.5.2.1 Configuration

MTLS for HFA is indirectly enabled or disabled via **“Certificate Verification Level”** select box in vHFA WBM. This option is located in menu:

Configuration > SPE > SPE Security Setup > TLS Parameters.

In order to adjust settings click on **Certificate Verification Level** select box and confirm by **Apply** button.

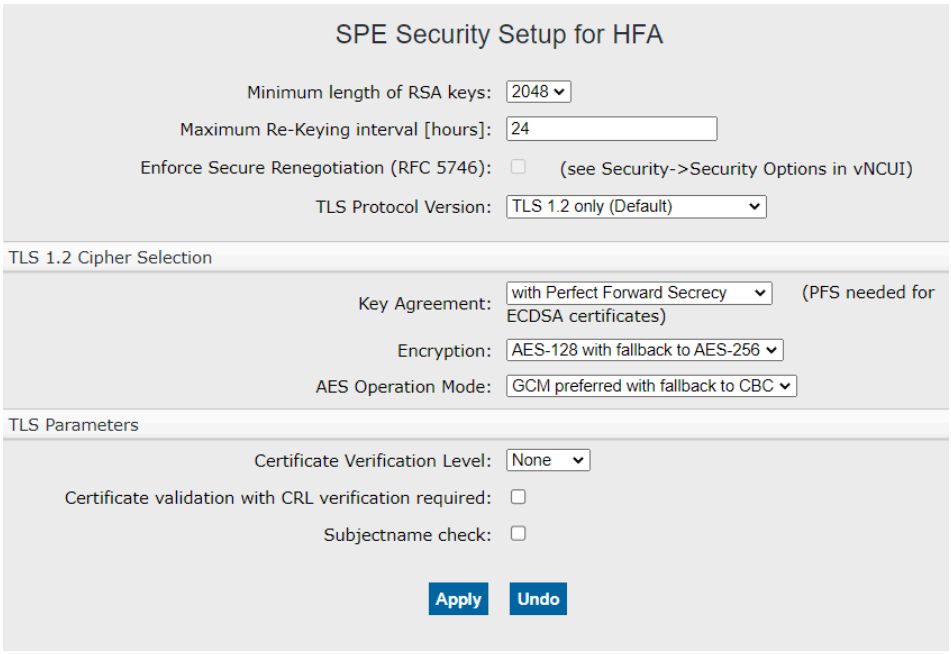


Figure 419: SPE Security Setup Key Certificate

If verification level is set to **None**, no authentication of the remote entity performed. When verification level is set to **Trusted** or **Full**, client certificate is requested and verified during SSL/TLS handshake. Client certificate must be signed by some trusted CA, whose public key certificate must be present on SG (more CA certificates can be present).

18.8.5.2.2 CA Certificate Management

CA certificate is imported in PEM or DER format via vHFA WBM:

Configuration > SPE > SPE CA Certs > click on **Import**

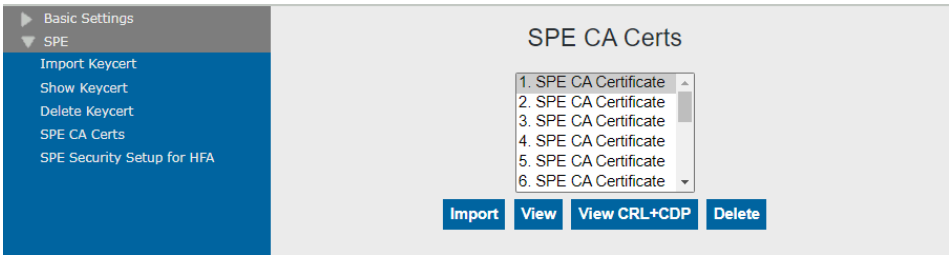


Figure 420: SPE CA Certs Import

On following screen press **Browse** button and select appropriate CA certificate file to import. If CRL distribution point for imported CA is available, select CRL distribution method (currently only HTTP is supported) and fill CDP address in text field CDP. Before CA certificate is imported in CGW, its fingerprint must be verified by click on **View Fingerprint of Certificate** because from now on will be this certificate treated as trusted!

List of currently available trusted certificates present on SG can be found in:

Configuration > SPE > SPE CA Certs

To view CA certificate details, click on appropriate entry in select box. To view CDP address and list of currently revoked client certificates click on entry in available **SPE CA Certificate** select box and click on **View CRL + CDP.**

Certificate can be removed from trusted certificate list click on certificate in select box and **Delete** button.

18.8.5.2.3 TLS

Currently are supported only protocols TLSv1.0 and higher, SSLv2 and SSLv3 are not permitted due to security issues. TLS version is configured in WBM menu:

Configuration > SPE > SPE Security Setup

On following screen, the deployed TLS version, key agreement method, encryption algorithm and operation mode can be configured (see https://www.ietf.org/rfc/rfc5246.txt and https://www.ietf.org/rfc/rfc8446.txt for more information about TLSv1.2 and TLSv1.3).

IMPORTANT: After changing and saving TLS HFA settings, **CGW must be rebooted** for the changes to take effect.

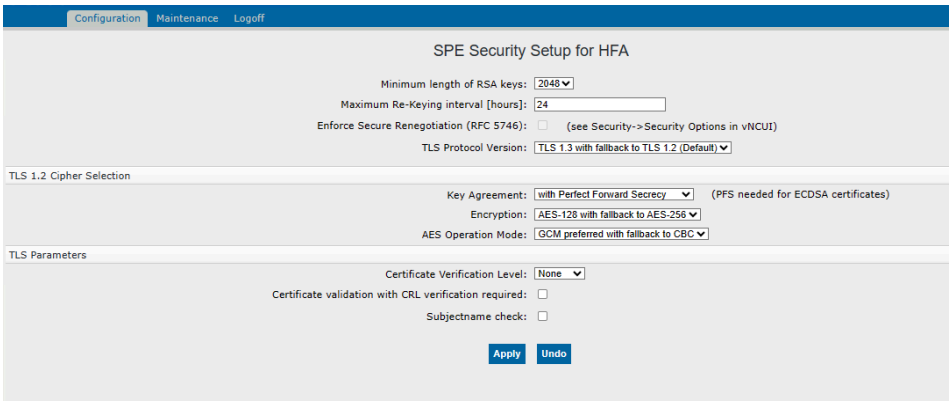


Figure 421: SPE Security Setup TLS

18.8.5.2.4 Trusted Level Features

When MTLS is enabled on level **Trusted**, client certificate is requested and verified in every SSL/TLS handshake (in initial handshake and also in every succeeding renegotiation).

Last certificate in certificate chain supplied by the client must be signed by one of trusted CA. None of the certificates in the chain may be expired, otherwise handshake fails immediately and connection is terminated.

When CRL revocation check is active, all unexpired CRLs are examined in order to determine revocation status for every certificate in client certificate chain.

On level **Trusted** are ignored all X509v3 extensions (even unknown and critical).

18.8.5.2.5 Full Level Features

When MTLS is enabled on level **Full**, basic client certificate verification scenario is the same as on level **Trusted**. Additionally, X509v3 extensions of client certificate are examined during SSL/TLS handshake. Certificate verification procedure fails, if any unknown critical extension occurs.

Full client verification level also enables one to perform identity check of client based on SubjectAlternativeName or CommonName present in certificate.

Note, that identity check is enabled by default. This behavior can be changed by checkbox:

Configuration > SPE > SPE Security Setup > Subject name check.

Identity check attempts to lookup SubjectAlternativeName or CommonName (respectively) via DNS and obtains IP address associated with this name. If any address is found and the address matches real IP address of connected client then identity check succeeds, handshake fails immediately otherwise.

18.8.5.2.6 Dynamic Behavior

Dynamic features:

1) Change of HFA TLS Parameters

- CA/private certificate addition/removal
- Expiration of CA/private certificate (affects rekeying)
- CRL download

Static features:

- TLS version configuration
- TLS encryption configuration
- TLS key agreement configuration
- TLS AES operation mode configuration

Static features require SG reboot for the changes to take effect, which is also indicated by icon in WBM. All dynamic features can be adjusted during SG runtime. Such event triggers new SSL/TLS handshake and client certificate chain verification with all consequences for all active connections. All established calls should survive if handshake succeeds.

18.8.5.2.7 Restrictions

Subject name check: this feature is currently not available for vHFA.

18.8.6 UFA IP Implementation

18.8.6.1 CGW and Softgate

18.8.6.1.1 Configuration

MTLS for HFA is indirectly enabled or disabled via option Certificate Verification Level in HG3500 WBM. This option is located in menu:

Configuration > Security > Signaling and Payload Encryption (SPE) > SPE Security Setup

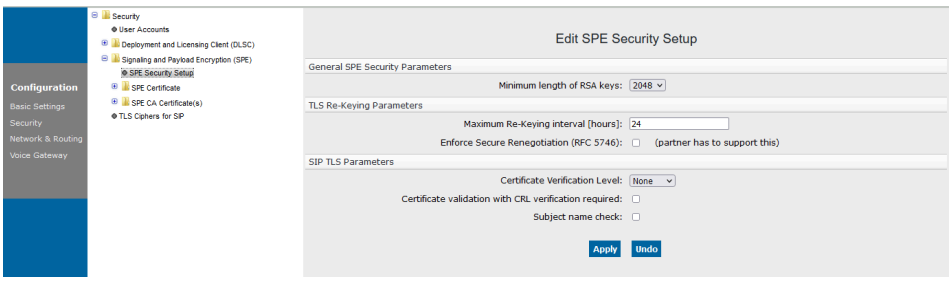


Figure 422: Edit SPE Security Setup

When verification level is set to Trusted or Full, client certificate is requested and verified during SSL/TLS handshake. Client certificate must be signed by some trusted CA, whose public key certificate must be present on GW (more CA certificates can be present).

18.8.6.1.2 CA Certificate Management

CA certificate is imported in PEM or DER format via HG3500 WBM:

Configuration > Security > Signaling and Payload Encryption (SPE) > SPE CA Certificate(s) > Import trusted CA certificate (PEM or binary)

On following screen press button “Browse..” and select appropriate CA certificate file to import. CRL check is NOT supported in current version (will be supported in V7R3).

IMPORTANT: Before CA certificate is imported in CGW, its fingerprint must be verified because from now on will be this certificate treated as trusted!

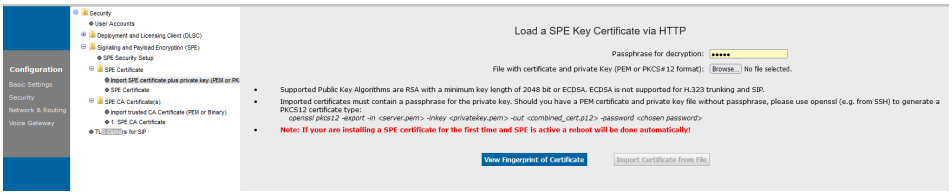


Figure 423: Import trusted CA certificate (PEM or binary)

List of currently available trusted certificates present on GW can be found in:

Configuration > Security > Signaling and Payload Encryption (SPE) > click on SPE CA Certificate(s) > Load a SPE CA Certificate via HTTP

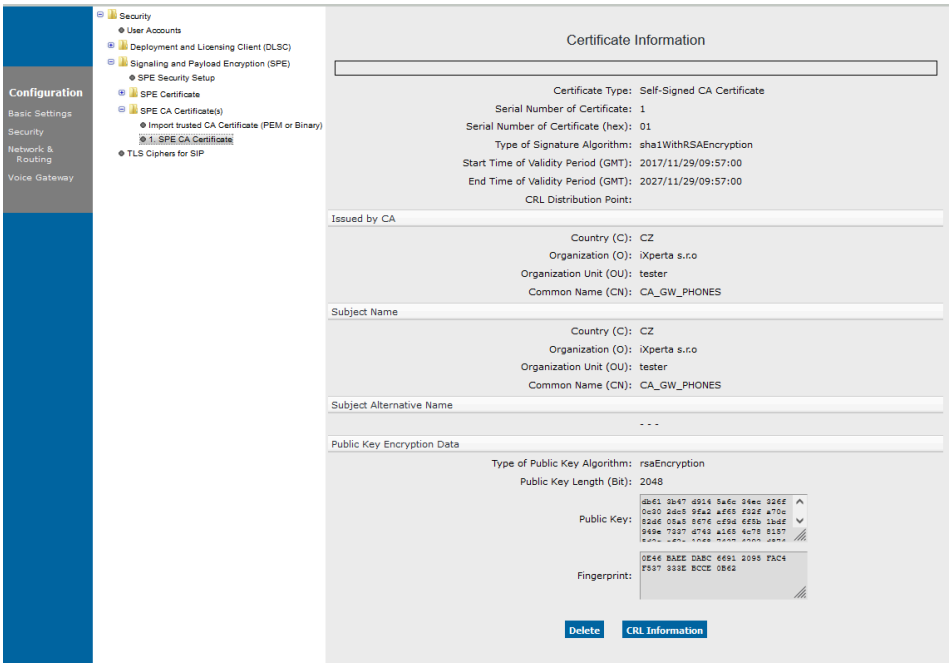


Figure 424: Certificate Information

To view CA certificate details, click on appropriate entry in list. Certificate can be removed from trusted certificate list, click the certificate in the list and select “Delete” button.

18.8.6.1.3 TLS

Currently are supported only protocols TLSv1.0 and higher, SSLv2 and SSLv3 are not permitted due to security issues. The default minimum RSA key length is 2048.

TLS version is configured in WBM menu:

Configuration > Security > Signaling and Payload Encryption (SPE) > right click on TLS Ciphers for SIP > Edit TLS Cipher Configuration.

On following screen, the deployed TLS version, key agreement method, encryption algorithm and operation mode can be configured (see https://www.ietf.org/rfc/rfc5246.txt and https://www.ietf.org/rfc/rfc8446.txt for more information about TLSv1.2 and TLSv1.3).

IMPORTANT: After changing and saving the TLS SIP settings, GW must be rebooted for the changes to take effect!

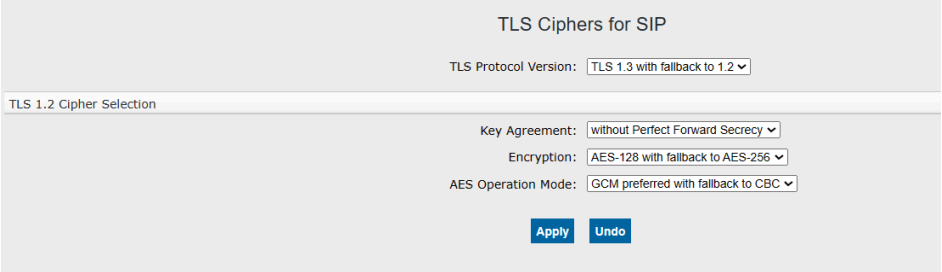


Figure 425: TLS Ciphers for SIP

Starting with V11R0, TLS version 1.3 is supported on the VoIP Interfaces (HFA and SIP).

NOTICE: TLS1.3 ciphers cannot be configured (fix settings).

18.8.6.1.4 Trusted Level Features

When MTLS is enabled on level Trusted, client certificate is requested and verified in every SSL/TLS handshake (in initial handshake and also in every succeeding renegotiation).

Last certificate in certificate chain supplied by the client must be signed by one of trusted CA and must not be expired, otherwise handshake fails immediately and connection is terminated.

Incorrect X509v3 extensions and unknown critical X509v3 extensions are not ignored on level Trusted due to underlying framework (even though they should be).

18.8.6.1.5 Full Level Features

When MTLS is enabled on level Full, basic client certificate verification scenario is the same as on level Trusted. Additionally, X509v3 extensions of client certificate are examined during SSL/TLS handshake. Certificate verification procedure fails, if any unknown critical extension occurs, or if usage of known

extensions (basicConstraints, keyUsage, extendedKeyUsage and nsCertType) violates current standard.

Full client verification level also enables one to perform identity check of client based on SubjectAlternativeName or CommonName present in certificate. Note, that identity check is enabled by default. This behavior can be changed by checkbox:

Configuration > Security > Signaling and Payload Encryption (SPE) > SPE Security Setup > SIP TLS Parameters > Subject name check.

Identity check attempts to lookup SubjectAlternativeName or CommonName (respectively) via DNS and obtains IP address associated with this name. If any address is found and the address matches real IP address of connected client then identity check succeeds, handshake fails immediately otherwise.

18.8.6.1.6 Features

1) CA/private certificate addition/ removal

- Change of SIP TLS Parameters
- Expiration of CA/private certificate (affects rekeying)
- TLS version configuration
- TLS encryption configuration
- TLS key agreement configuration
- TLS AES operation mode configuration

Features require GW reboot for the changes to take effect, which is also indicated by icon in WBM. All dynamic features can be adjusted during GW runtime. Such event triggers new SSL/TLS handshake and client certificate chain verification with all consequences for all active connections. All established calls should survive if handshake succeeds.

18.8.6.1.7 Restrictions

Revocation: Certificate revocation check is NOT supported in current version, it will be available in V7R3.

19 Payload Switching DMC

19.1 Feature Description

To support the Payload Switching feature, the Direct Media Connection DMC feature is used for Voice over IP (VoIP) connections in OpenScape 4000.

Direct Media Connections DMC can be described and defined in the following way:

1) The payload (voice channel) of an OpenScape 4000 internal or networkwide voice connection will be exchanged within a LAN in which a direct IP connection is possible without conversion into a TDM data stream.

By the use of the feature "DMC Any-to-any" payload data is transported within a HiPath 4000/OpenScape 4000 network directly between the IP endpoints without several IP-TDM conversions of the payload. This direct payload connection is called Direct Media Connection (DMC).

DMC has two purposes:

- Avoid degradation of speech quality by minimizing the number of IP/TDM hops/conversions.
- Optimize the bandwidth: for those cases activation of VAD is very important.

19.2 Direct Media Connect (DMC) in Connection with HFA Subscriber

19.2.1 Feature Description

19.2.1.1 Motivation

If two HFA IP phones are connected in a two-party call without the Direct Media Connection DMC feature, a double IP/TDM conversion of the payload would be performed. This causes a loss of quality of the voice transmission which results from the multiple conversion of the payload between IP and TDM and vice versa. To avoid this loss of quality the IP payload is exchanged directly between the two subscribers if both are in a two party connection.

IP Endpoints can be:

- HFA IP phones
- IP Trunking Gateways (z.B.: HG 3500)
- IPDA boards (z.B.: HG 3500)

The IP endpoints can be the real endpoints of the connection (i.e. there is a Master Connection between two IP phones) or the IP endpoints are only endpoints of a section within the Master Connection. E.g. an anate or digite may also profit from a DMC if it is connected to its partner via IPDA Access Point or IP Trunking Gateway.

The setup of a call is done within several steps.

Steps 1 and 2 are the normal call setup procedures as known in HiPath 4000 V1.0. The result is called Master Connection. The normal call setup procedure is extended by steps 3 and 4 to build the optional Direct Media connection.

1) In a first step, a signaling connection between the users is established.

2) Parallel to that signaling connection a so called Master Connection (MC) for the payload is established. The payload path of the Master Connection may be segmented into TDM and IP paths:

- within a TDM network this is a specific B channel
- within an IP network, this is a RTP connection.

The RTP payload connection is established and controlled by H.323 procedures (in particular by the use of the fast connect procedure).

3) After the Master Connection between the users is established and connected, i.e. both users are in the talk state, a DMC connection between the IP endpoints of the Master Connection can be established. The called IP endpoint initiates the setup of the DMC connection.

4) When the DMC connection is established, the payload is transported using this H.323 connection. However, the Master Connection exists in parallel, but without conveying payload as long as the DMC connection exists (the Master Connection is on a "stand-by" mode).

5) If the talk-state is released (e.g. for the setup of a consultation call) the IP endpoint switches back immediately to the Master Connection and releases the DMC connection.

19.2.1.2 Notes concerning Direct Media Connections DMC

- The Direct Media Connection will be switched in the two-party call state, that means in the basic call and the simple consultation call. A DMC will also be switched if the call is set up via a feature like call forwarding or picking up a group call or if a secondary line answers a keyset call. A DMC is also switched for **conference calls**.
- If the involved parties aren‘t in a two party connection the IP/TDM conversion and the switching via the TDM switching network (MTS) is executed.
- If a Direct Media Connection is established the connection path via the MTS switching network for multiple IP/TDM conversion (Master Connection) has to stay switched in parallel to the direct IP connection so that immediately after termination of the two party call state the MTS with its capabilities for tones and conferencing is available for any feature control by call processing.
- DMCs are established also for Fax/Modem connections.

19.2.1.3 Bandwidth Considerations

19.2.1.3.1 General Notes

While a DMC is active only SID (Silence Insertion Descriptor)/CN (Comfort Noise) frames are sent on the master connection if involved components are configured with VAD (see Section 2.3.3, “Voice Activity Detection (VAD)”). Therefore this master connection needs only a reduced bandwidth.

You can find the tables for bandwidth in the document “Gateways HG 3500 and HG 3575”, Section 2.5.4, “Required Bandwidth per Connection”

For additional information about bandwidth administration please refer to the Resource Manager and AMO GKTOP.

By inserting SID/CN, analog background noise is simulated digitally during silence to assure the listener that the link is active and operational. The background noise RTP packets with CN flag are sent on the master or slave connection once per second.

19.2.1.3.2 Gateways

Only DMC endpoints are aware of the DMC and able to reduce bandwidth on the Master connection accordingly.

If the gateway is not a DMC endpoint e.g. in multihop scenarios, then the gateway is **NOT** aware of the DMC. In order to reduce bandwidth usage the gateways should be configured with a codec supporting VAD and additionally VAD must be activated (VAD will then lead to the gateway generating CN packets).

IMPORTANT: HG 3530 is never a DMC endpoint.

These are recommended ASC settings in AMO CGWB:

Table 88: Recommended ASC settings in AMO CGWB

PRIO1:	CODEC = G711A	VAD = YES	RTP-SIZE = 30
PRIO2:	CODEC = G729AB	VAD = YES	RTP-SIZE = 20
PRIO3:	CODEC = G723	VAD = YES	RTP-SIZE = 30
PRIO4:	CODEC = NONE	VAD = NO	RTP-SIZE = 20
PRIO5:	CODEC = NONE	VAD = NO	RTP-SIZE = 20
PRIO6:	CODEC = NONE	VAD = NO	RTP-SIZE = 20
PRIO7:	CODEC = G729A	VAD = NO	RTP-SIZE = 20**

** This setting should be removed if bandwidth reduction is always wanted. However in this case silent suppression (VAD) **must** be activated in the phone as described under Section 2.3.3, “Voice Activity Detection (VAD)”, because there’s need of:

- G729AB: **VAD=YES** in AMO CGWB if we check silent suppression checkbox in phones

or

- G729A: **VAD=NO** in AMO CGWB if we don’t check silent suppression checkbox in phones

NOTICE: If set only G729AB **VAD=YES** in AMO CGWB and silent suppression checkbox in phones is **not checked**, then every call attempt fails and HY2 code (no Bearer Capabilities) will be displayed.

19.2.1.3.3 HFA

optiPoint phones generate CN frames on the master connection once DMC is established.

OpenStage phones **do not** generate CN on master connection once DMC is established.

VAD setting in AMO SDAT controls the sending CN for normal connections and DMC slave connections.

The phone's DSP (Digital Signal Processor) will accept VAD for G711, G729 or G723 regardless of the phone VAD SDAT setting. VAD is not defined for G722.

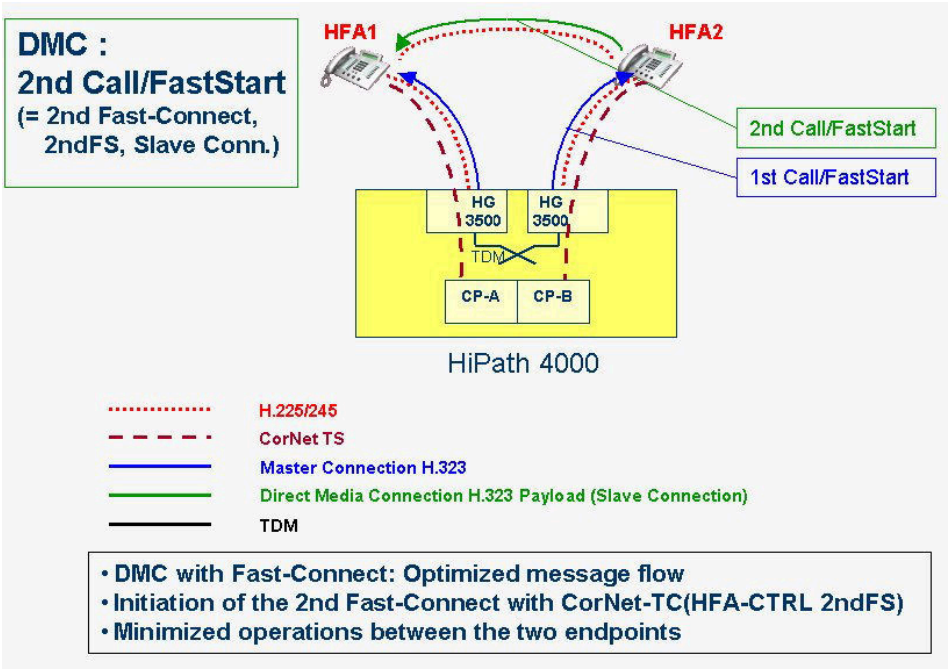
Codecs and silent suppression

- G711 - High quality codec, capable of Voice Activity Detection (VAD) and Comfort Noise Generation (CN);
- G723.1 - Audio codec for voice that compresses voice audio in 30 ms frames; Capable of silent suppression (VAD) and comfort noise (CN); Not reliable for transporting music or tones such as DTMF or fax.
- G729 - Voice compression codec; Not capable of silent suppression (VAD) - implicitly silence suppression is off
- G729A - Voice compression codec; Not capable of silent suppression (VAD) - implicitly silence suppression is off
- G729B - Voice compression codec; Capable of silent suppression (VAD); not compatible with G729 or G729A
- G729AB - Voice compression codec; Capable of silent suppression (VAD); only compatible with G729B

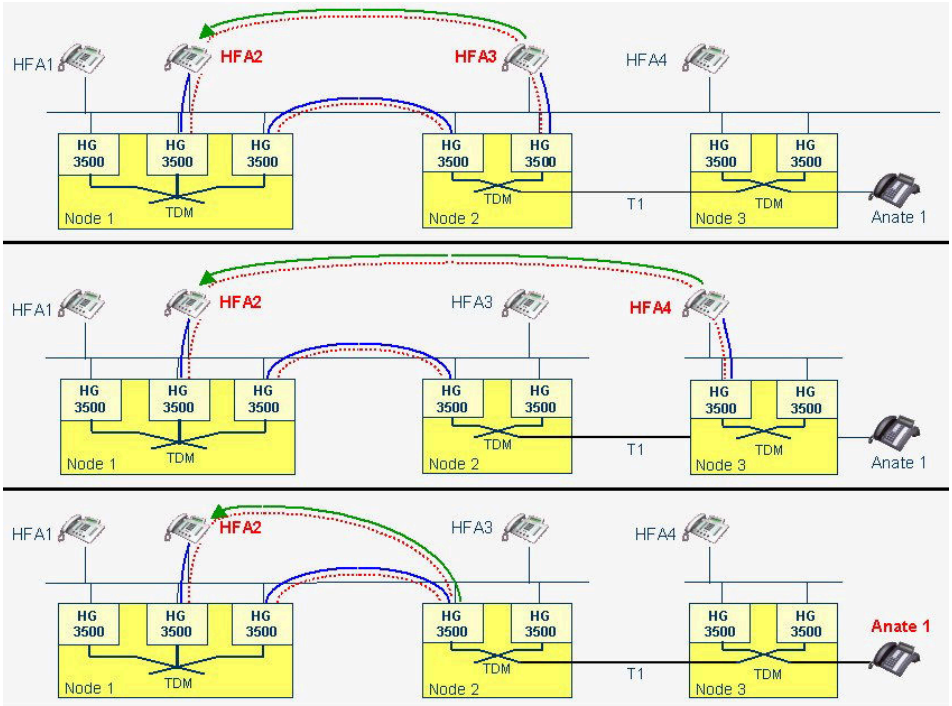
19.2.1.4 Scenarios

The following scenarios are being considered:

Scenario A: Direct Media Connection DMC within a single OpenScape 4000 node.



Scenario B: Direct Media Connection DMC between HFA IP phones within a HiPath 4000/OpenScape 4000 network.



This scenario B is supported in OpenScape 4000 in conjunction with the IP Gateway HG 3500 V4.

Scenario C: Direct Media Connections DMC between HFA IP phone and IPDA shelf within a single OpenScape 4000 node.

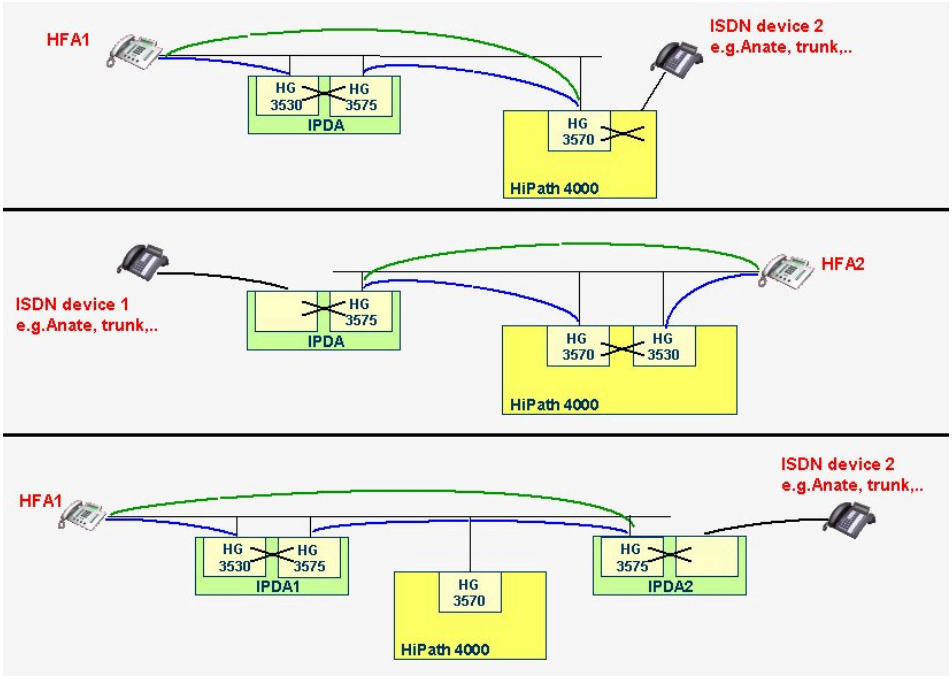
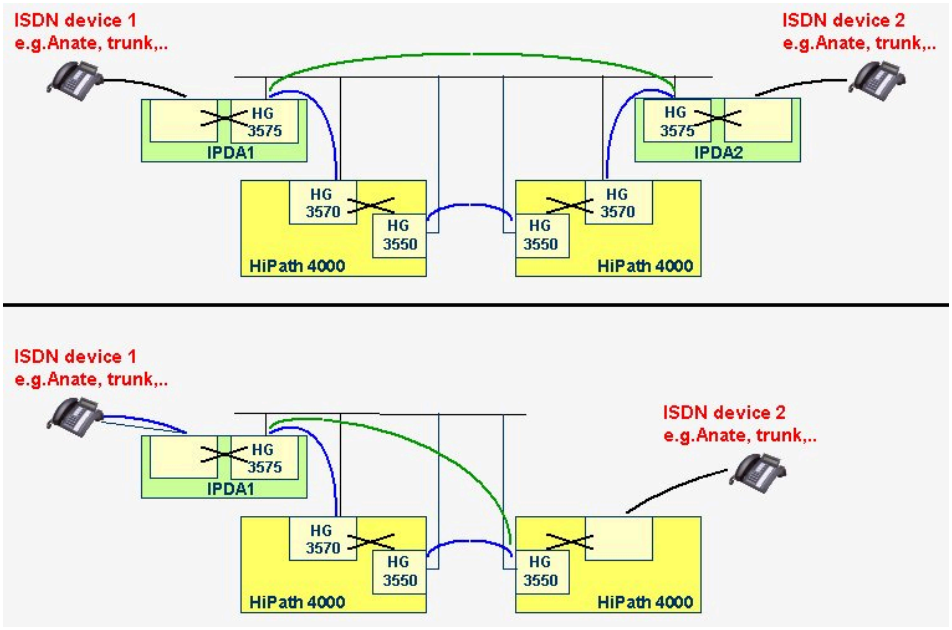
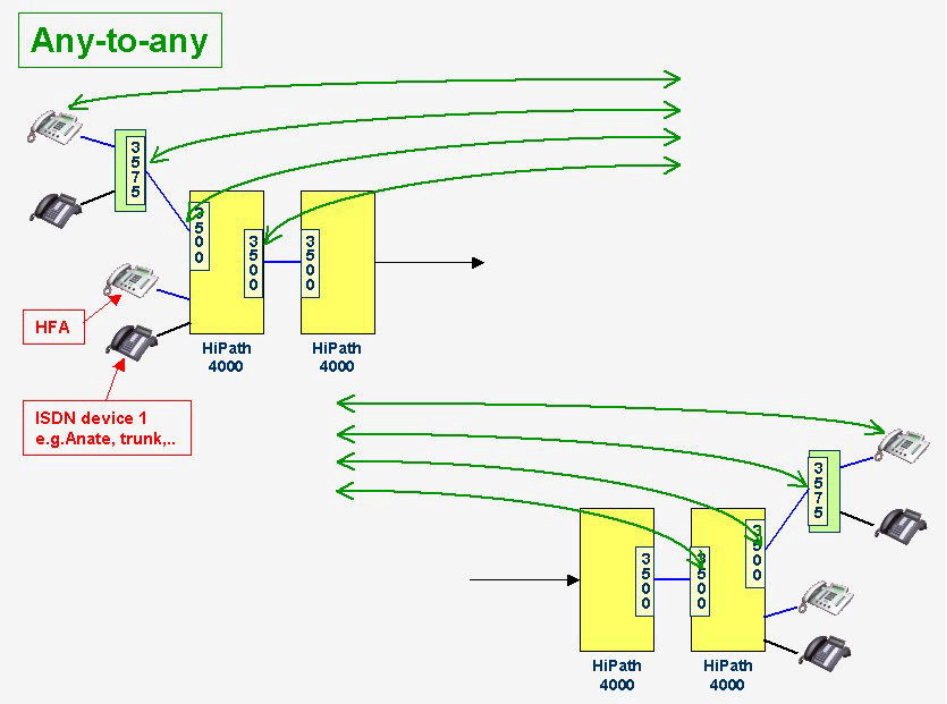


Figure 426: Scenario D: Direct Media Connections DMC between netwide IPDA-shelves.



DMC in mixed scenarios

In mixed scenarios the DMC is executed in the 2 party call state between the first possible IP address at the A-side (IP phone or HG 3575 or HG 3500 (FUNCTION=HG3570) or HG 3500 (FUNCTION=HG3550)) and the last possible IP address at the B-side (i.e. again HG 3500 (FUNCTION=HG3550) or HG 3500 (FUNCTION=HG3570) or HG 3575 or IP phone).

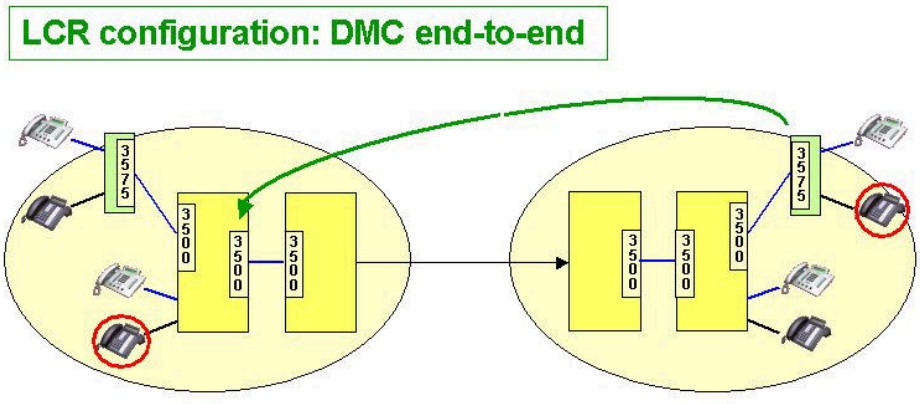


19.2.1.5 Domain concept

In very large enterprise networks it may be necessary to subdivide the network into several so called domains. Depending on the configuration DMC connections may be allowed only within these domains or end-to-end over several domains.

Example 1: DMC possible from domain A until domain B:

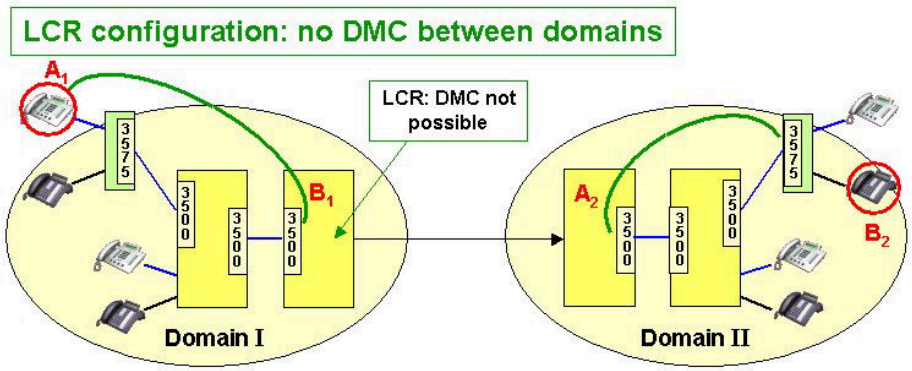
Note: for this scenario no special configuration is needed (default)



Example 2: DMC not possible from domain A to domain B, DMC only possible within domains A and B:

In this case both ends of the link between the domains have to be marked as domain end.

This is done with an attribute within LCR (see chapter Generation). This attribute has to be set in domain I for the LCR route leading to domain II, and in domain II for the LCR route leading to domain I.



19.2.1.6 DMC Interworking to HiPath 3000

Supported scenarios:

Scenario 1: HG 3500 terminates the HiPath 3000 payload switching

This scenario applies to two cases:

1) the endpoint in the HiPath 4000/OpenScape 4000 network is a TDM device or

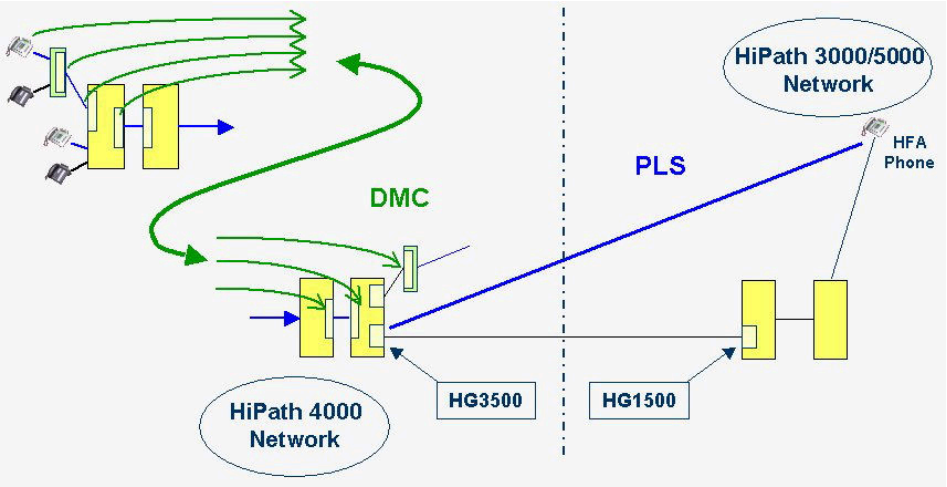
- DMC interworking between OpenScape 4000 and HiPath 3000 is not allowed (this scenario can be achieved by setting the LCR domain end attribute in the OpenScape 4000 for the route leading to the HiPath 3000 network).

In the first case the end-to-end connection consists of a TDM connection on the OpenScape 4000 side and an IP connection between the HG 3500 and the IP endpoint on the HiPath 3000 side.

In the second case the connection between the endpoint in the HiPath 4000/ OpenScape 4000 network and the endpoint in the HiPath 3000 network consists of

- a DMC part in the HiPath 4000/OpenScape 4000 network and
- Payload Switching (PLS) in the HiPath 3000 network, i.e. the PLS is terminated by the HG 3500 on the OpenScape 4000 side.

This second case is shown in the following picture:

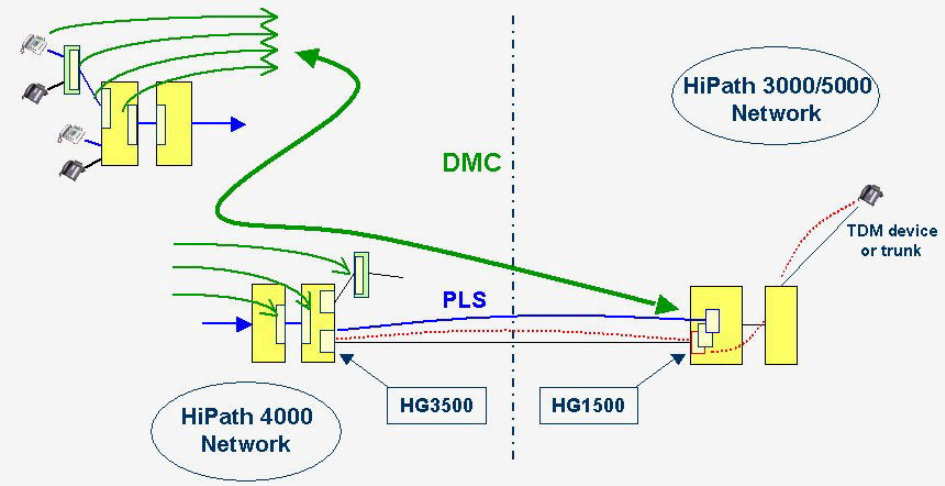


- DMC within HiPath 4000/OpenScape 4000 network: From the 1st possible A-side IP address to 1st possible B-side IP address. Signaling of A- and B-IP address takes place via CorNet-NQ (SETUP/CONNECT-messages)
- PLS (Payload Switching) within HiPath 3000 network: The IP-Gateway HG 3500 serves as Payload Switching HFA Proxy of HiPath 3000.

Scenario 2: HG 1500 terminates OpenScape 4000 Direct-Media-Connection

DMC to HG1500 in HiPath 3000

When interworking between OpenScape 4000 and HiPath 3000 is allowed and the endpoint in the HiPath 3000 network is a TDM device the HG1500 terminates the DMC.



RTP stream between the HiPath 3000 HG1500 and the OpenScape 4000 HG 3500 belongs to the master-connection.

Scenario 3: Direct-Media-Connection between HFA IP phones end-to-end

DMC to HFA Phone in HiPath 3000

When interworking between OpenScape 4000 and HiPath 3000 is allowed and the endpoint in the HiPath 3000 network is a HFA phone a DMC can be established end-to-end.

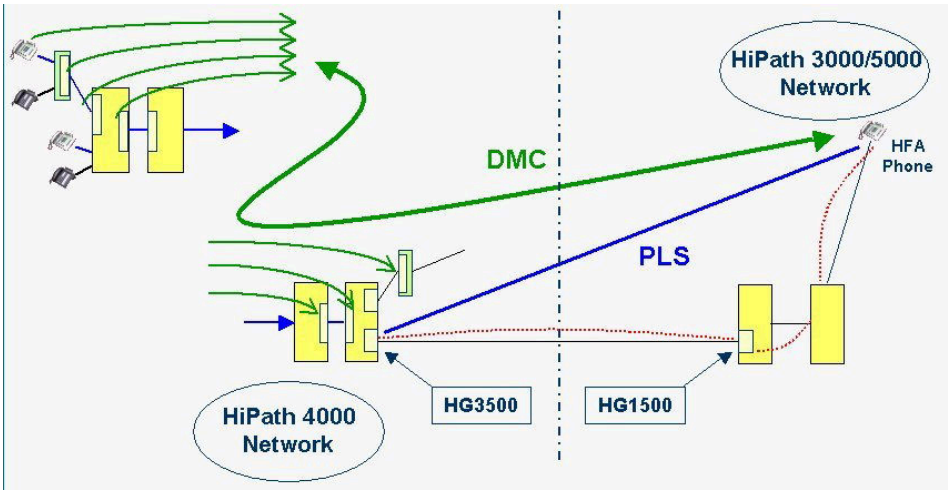
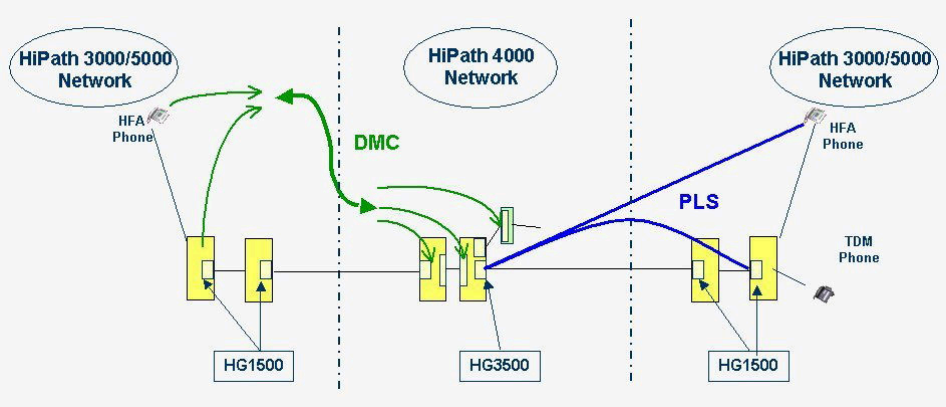


Figure 427: RTP stream between the HiPath 3000 HFA phone and HG 3500 belongs to the master-connection.

Scenario 4: OpenScape 4000 as transit node between two HiPath 3000 nodes



In this case, no end-to-end DMC connection can be set up between the HiPath 3000 IP devices (IP phones or HG1500). On the A side, a DMC is established to the most distant OpenScape 4000 DMC endpoint (HG 3500 (FUNCTION=HG3550 or HG3570) or HG3575). This DMC overlies a HiPath 3000 PLS connection (not depicted in the figure) and the IP parts of the HiPath 4000/OpenScape 4000 network.

If the HiPath 4000/OpenScape 4000 network has no IP parts, the DMC connection is omitted and the payload is transmitted on the PLS connection. This applies if, instead of a HiPath 4000/OpenScape 4000 network or an IPDA configuration, an individual OpenScape 4000 connected on both sides with HiPath 3000 systems or networks is involved. So a DMC connection on the A side only exists if an optimization is necessary.

On the B side, a payload switching connection is established.

So it always involves a connection with 2 IP hops.

19.2.2 Service Information

19.2.2.1 Features with DMC

The following list shows for which features a DMC is established:

- Basic call
- Basic call with reroute internal
- Basic call with rerouting (NW)
- Consultation call (including toggle, end of consultation (back to held party))
- Transfer talking with or without Path Replacement
- Transfer ringing with or without Path Replacement
- Immediate recall
- Centralized attendant transfer
- CFU, CFNR with forward switching or with rerouting or mixed (rerouting in transit switch)
- Call back (message waiting, busy, no reply)
- Pickup of a call in a pickup group
- Directed call pickup
- Call to Hunt group

- Application establishes call (ACL make call)
- ACD call
- Reduction of conference to 2-party call
- Call to Keyset (secondary line answers the call)
- executive/secretary (CHESE) (secretary answers the call)

19.2.2.2 Feature activation while DMC is active

When a DMC is active for a two party call and a feature is being activated the DMC is released and the call is switched back to the master connection.

This applies for features that are activated by one of the involved parties and also for features activated by a third party (e.g. campon, override).

When the feature is finished and the call returns to the normal two party talk state the DMC is not reactivated except for the features that are listed in the chapter above.

Feature response in exception situations:

- DTMF Handling
- A DMC is released if the endpoint requests the sending of DTMF via SIU (signaling unit). E.g. a HFA phone requests the sending of DTMF via access code.
- DTMF transmission over DMC
- DTMF tones are recognized in DMCs and transmitted, e.g. if the tone is received by the OpenScape 4000 system at a CO interface or a DTMF enabled anate sends DTMF by itself.

19.2.3 Generation

19.2.3.1 DMC Authorization

Possible IP endpoints have to be allowed to switch a DMC.This is done with the following AMO commands:

- IP phones:

CHANGE-SDAT:STNO=<extension number>,TYPE=ATTRIBUT,AATTR=DMCALLWD;

- NCUI:

CHANGE-STMIB:MTYPE=NCUI2,LTU=xx,TYPE=DMCDATA,DMCALLWD=YES;

- STMI pool for IPDA:

CHANGE-SIPCO:TYPE=DMCDATA,DMCALLWD=YES;

- IP trunking:

CHANGE-TDCSU:PEN=<ltg-ltu-slot-cct),DEV=HG3550IP,DMCALLWD=Y;

19.2.3.2 Maximum number of DMC connections on IP boards

Please refer to „Gateways HG 35000 and HG 3575“, Section 2.6, “B Channels”.

AMO commands:

- NCUI:

```
CHANGE-STMIB:MTYPE=NCUI2,LTU=xx,TYPE=DMCDATA,DMCCONN=<number of allowed DMC
 connections>;
```

- STMI - IP trunking:

```
CHANGE-CGWB:MTYPE=CGW,LTU=xx,TYPE=DMCDATA,DMCCONN=<number of allowed DMC
 connections>;
```

19.2.3.3 Voice Activity Detection (VAD)

In order to save bandwidth Voice Activity Detection (VAD) has to be activated for IP connections. When a DMC is established and VAD is set only idle frames are sent on the master connection.

VAD is activated with the following AMO commands:

- Station:

```
CHANGE-SDAT:STNO=<ext. number>,TYPE=DATA1,CLASSMRK=VAD&EC&G711&G729OPT;
```

- Digital trunks:

```
CHANGE-TDCSU:PEN=<ltg-ltu-slot-cct),CLASSMRK=VAD&EC&G711&G729OPT;
```

- Analog trunks:

```
CHANGE-TACSU:PEN=<ltg-ltu-slot-cct),CLASSMRK=VAD&EC&G711&G729OPT;
```

- IP trunking:
- Modifying of codecs and VAD is no longer possible via WBM and any change has to be done via AMO CGWB. However, it is still possible to display the current settings via WBM under **Configuration > Voice Gateway > Codec Parameters**

  (The same applies for HG 3575 IPDA - AMO STMIB)
- HFA: VAD must be activated at both ends of the HFA master connection.
- For IP phones: the silence suppression needs to be checked in WBM of the phone under **Administrator > Speech/Cloud > Codec Preferences**.

  For HG 3500:

  ```
  CHANGE-CGWB:MTYPE=CGW,LTU=x,SLOT=xx,TYPE=ASC,VAD=YES;
  ```

19.2.3.4 Domains

It may be necessary to subdivide a very large enterprise network into several areas (domains) where DMC is only possible within a domain and not between domains.

In order to achieve this an LCR mark has to be set at each domain end. When this mark is set DMCs are not established beyond this point.

AMO command:

```
CHANGE-LDAT:LROUTE=<route number>,LATTR=<existing attributes>&DMCEND;
```

19.2.3.5 H.323 stack on IPDA boards

The H.323 stack on IPDA boards has to be configured using the following AMO commands:

- NCUI:

```
CHANGE-STMIB:MTYPE=NCUI2,TYPE=H323,GWNAME=<string>;
```

- STMI:
- These settings are not possible via AMO. Please use WBM of the board.

  For the correct numerical values please refer to the configuration manual for IPDA boards.

  In addition, the codecs used for the DMC must be configured (Master Connection codecs see AMO SDAT / AMO TACSU / AMO TDCSU).
- NCUI:

```
CHANGE-STMIB:MTYPE=NCUI2,LTU=xx,TYPE=ASC,PRIO=PRIO1,CODEC=G729;
CHANGE-STMIB:MTYPE=NCUI2,LTU=xx,TYPE=ASC,PRIO=PRIO2,CODEC=G711;
```

- STMI:

```
CHANGE-CGWB:MTYPE=CGW,LTU=xx,SLOT=xx,TYPE=ASC,PRIO=PRIO1,CODEC=G729;
CHANGE-CGWB:MTYPE=CGW,LTU=xx,SLOT=xx,TYPE=ASC,PRIO=PRIO2,CODEC=G711;
```

1) **WBM > Configuration > Voice Gateway > Codec Parameters**

19.2.3.6 Troubleshooting Hints

If you encounter problems with DMC please check first the activation switches in Section 2.3.1, “DMC Authorization”.

Another switch to be checked is the diagnosis switch 08 in CP2 branch of `AMO DIAGS`.

```
DISPLAY-DIAGS:COMP=CP2;
```

Please remember that switch **S08=ON** means DMC is deactivated in the whole system, so the switch should be usually set to OFF in order to have DMC enabled.

Then please assure that DMC configured resources for the involved boards are not equal 0 or too few (see Section 2.3.2, “Maximum number of DMC connections on IP boards”). Check also if resource manager is configured/involved.

Further you can check if the components are not part of different domains and inter-domains DMC is allowed or not.

Supported features table should also be checked (see Section 2.2, “Service Information”).

The DMC connections can be checked by activating DIAGS switch 09 in CP2. DMC connection related information would be visible then in HISTA under:

```
F4066 M8 N4058 NO ACT BPA CP ADVISORY ALARM CLASS:CENTRAL:023 FORMAT:49 DMC
```

The flow which grants a successful DMC is:

At B party:	STATE_NEW	=	init;	event = ACT_PROXY_DMC_START
At A party:	STATE_NEW	=	active;	event = UP DMC_IND OK
At B party:	STATE_NEW	=	active;	event = UP DMC_CONF

WBM of IPDA/gateway boards could also be checked under Explorers' Statistics, for some DMC related calls.

Useful may be display of AMO ZAUSL.The result shows counters of DMC connections:

```
|N0059: NUM. OF ALL SUCCESS. DMC ATTEMPTS (ACT. OR PAS)..
 0|
|N0060: NUM. OF ALL UNSUCCES. DMC ATTEMPTS(ACT. OR PAS).
 0|
|N0061: NUM. OF SUCCESSFUL DMC ATTEMPTS, BOTH PROX. INTR.
 0|
|N0062: NUM. OF UNSUCCESSFUL DMC, BOTH PROXIES INTERNAL..
 0|
|N0063: NUM. OF ALL UNSUCCES. DMC ATTEMPTS(INSTANT DMC).
 0|
```

With G711, the CN RTP packages are displayed in wireshark as Payload Type :Comfort Noise

With G729 they appears as: Payload Type :ITU-T G729 (no difference to the normal RTP) but the length of payload is usually only 2 bytes long and total package length is 60 bytes.

With G723.1 the CN is recognized in the field: frame size and codec type:SID frame.

19.2.4 Relevant AMOs

AMO	Parameter	Sprache/ Language	Beschreibung/ Description
CGWB	MTYP=CGW	d	Konfiguration von HG 3500
	MTYPE=CGW	e	Configuration of HG 3500
	TYP=DMCDATA	d	DMC-spezifische Daten konfigurieren
	TYPE=DMCDATA	e	Configure DMC specific data
	DMCCONN	d	Anzahl der DMC-Verbindungen
	DMCCONN	e	Number of DMC connections
	TYP=ASC,VAD=J/N	d	VAD in Senderichtung erlaubt / nicht erlaubt,Wert=JA / NEIN
	TYPE=ASC,VAD=Y/N	e	VAD enabled / not enabled in send direction, value = YES / NO

AMO	Parameter	Sprache/ Language	Beschreibung/ Description
LDAT	LATTR	d	LCR Attribut, neuer Wert: DMCENDE = Ende der DMC Domaine
	LATTR	e	LCR attribute, new value: DMCEND = end of DMC domain
SDAT	EMERK & AMERK	d	Teilnehmermerkmal, Wert: DMCERL = DMC erlaubt
	AATTR & DATTR	e	subscriber attribute, value: DMCALLWD = DMC allowed
	CLASSMRK	d	Classmark, Wert VAD = Voice Activity Detection
	CLASSMRK	e	Classmark, value VAD = Voice Activity Detection
SIPCO	TYP	d	Datentyp (Verzweigungsparameter), Wert: DMCDATA
	TYPE	e	type of data (branching parameter), value: DMCDATA
	DMCERL	d	DMC erlaubt, Wert = JA/NEIN
	DMCALLWD	e	DMC allowed, value = YES/NO
STMIB	MTYP=NCUI2	d	Konfiguration der HG 3575
	MTYPE=NCUI2	e	Configuration of HG 3575
	TYP=DMCDATA	d	DMC-spezifische Daten konfigurieren
	TYPE=DMCDATA	e	Configure DMC specific data
	DMCERL	d	DMC erlaubt, Wert = JA/NEIN
	DMCALLWD	e	DMC allowed, value = YES/NO
	DMCCONN	d	Anzahl der DMC-Verbindungen
	DMCCONN	e	Number of DMC connections
TDCSU	GER=HG3550IP	d	Integriertes IP-Gateway HG 3500
	DEV=HG3550IP	e	Integrated IP Gateway HG 3500
	DMCERL	d	DMC erlaubt, Wert = JA/NEIN
	DMCALLWD	e	DMC allowed, value = YES/NO

AMO	Parameter	Sprache/ Language	Beschreibung/ Description
	CLASSMRK	d	Classmarks für IP Verbindungen, Wert VAD = Voice Activity Detection
	CLASSMRK	e	classmarks for IP connections, value VAD = Voice Activity Detection
TACSU	CLASSMRK	d	Classmarks für IP Verbindungen, Wert VAD = Voice Activity Detection
	CLASSMRK	e	classmarks for IP connections, value VAD = Voice Activity Detection

19.3 Direct Media Connect (DMC) in Connection with SIP Subscriber

19.3.1 Feature Description

One major function on the LAN side is “direct payload” (DMC -> Direct Media Connect) between the call parties. This function can be activated/deactivated for all SIP endpoints.

Given the fact that direct payload transmission between SIP subscribers and other IP devices and gateways is desirable (due to better voice quality), despite the fact that SIP subscribers do not support the H.323-based DMC procedure, HG 3500 includes a “DMC proxy”. This feature is also included in the common gateway board. In other words, as far as DMC signaling is concerned, the gateway functions on behalf of the SIP subscriber and converts the DMC signaling into SIP signaling.

For HFA subscribers the DMC connection is shown in the following diagram.

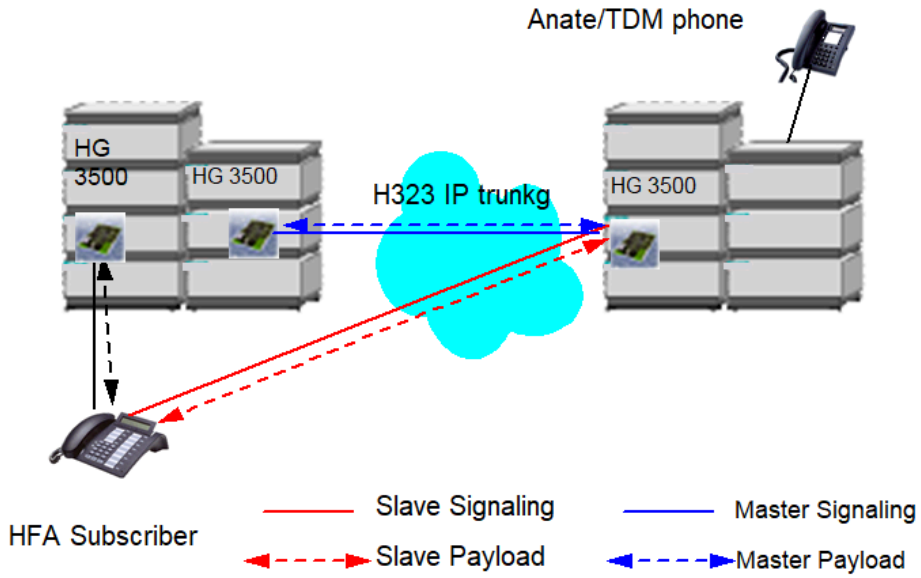


Figure 428: DMC in connection with HFA subscriber

This figure shows the situation for an HFA subscriber calling a TDM subscriber in another node via an H323 IP trunk. The master connection for both signaling and payload is maintained via the HG 3500 (in this case configured as a HFA gateway) and both HG 3500 (IP trunking) gateways. The Slave connections are the DMC connections and these are between IP endpoints, on the one side the HFA subscriber and on the other side the HG 3500 IP trunking board.

The transport addresses (IP addresses/ports) for payload transmission are transmitted as part of the DMC signaling. The DMC proxy does not transmit the actual transport address in this case, but instead transmits the address of the addressed SIP subscriber in order to facilitate a direct RTP stream for the SIP subscriber.

Given the fact that H.323 and SIP both use RTP for voice transmission, connection between

- H323,
- SIP and HFA subscribers,
- IPDA: OpenScape 4000 host system and IPDA Access Points,
- Common Gateways (IP /SIP trunking) and HG 1500 gateways

is possible.

To set up a standards-compliant payload channel for the SIP subscriber, the SIP re-invite and, preferably (provided the subscribers support it), the SIP update procedures are used (the latter also requires SIP-PRACK support). These procedures make it possible to switch a payload connection over to another destination. Unlike previous DMC endpoints, the “master” payload connection to OpenScape 4000 is not maintained in this case - i.e. the DMC payload connection replaces the master connection. However, the “master” signaling for the OpenScape 4000 remains established.

This is illustrated in the figure below:

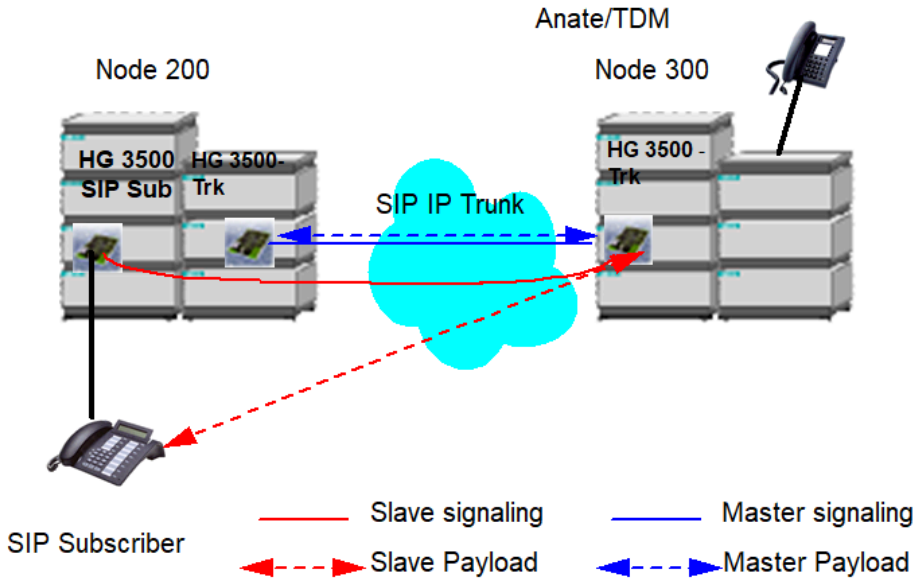


Figure 429: HG 3500 subscriber which functions as a DMC proxy

Explanation:

Figure 1 DMC in connection with HFA subscriber: DMC signaling and payload between an HFA telephone and an HG 3500 trunking gateway (see also Chapter 2, “Direct Media Connect (DMC) in Connection with HFA Subscriber”).

Figure 2 HG 3500 subscriber which functions as a DMC proxy: DMC payload is sent between the SIP phone in node 200 and an HG 3500-Trunking in Node 300. DMC signaling is between the DMC proxy in HG 3500 board and the HG 3500-SIP-Trunking board.

A distinction is made between the DMC proxy and the DMC endpoint. The latter is the endpoint for DMC signaling and the DMC payload channel (RTP). Both gateways (HG 3500, HG 3575) and subscribers function as DMC endpoints. HG 3500-Trk in node 300 and the SIP phone in node 200 are therefore DMC endpoints in the diagram.

Note that the HG 3500 in this example is not part of a payload connection. However, a DSP is reserved for the connection in case activation of a feature terminates the DMC and causes a fallback to the master connection. When the DMC is terminated, a master payload connection must be renegotiated by SIP re-invite, as the connection does not exist for the SIP subscriber.

Given the fact that the SIP subscribers are themselves not DMC-capable, we no longer talk about DMC connections as of HiPath 4000 V3.0, but instead more generally about an end-to-end payload connection, or e2epc for short.

Setup of the master connection, which leads to a master payload connection between the calling SIP endpoint and HG 3500 (requested in order to transmit announcements and tones from the OpenScape 4000 to the SIP endpoint) is not displayed. DMC is initiated with the Connect of the called side.

The procedure described above is even used for a call between two SIP subscribers, i.e. an H.323-based DMC is set up from HG 3500 to HG 3500 (or internally if both subscribers are registered on the same gateway). A direct connection between OpenScape 4000 SIP subscribers without DMC is not possible at present.

19.3.2 Restriction

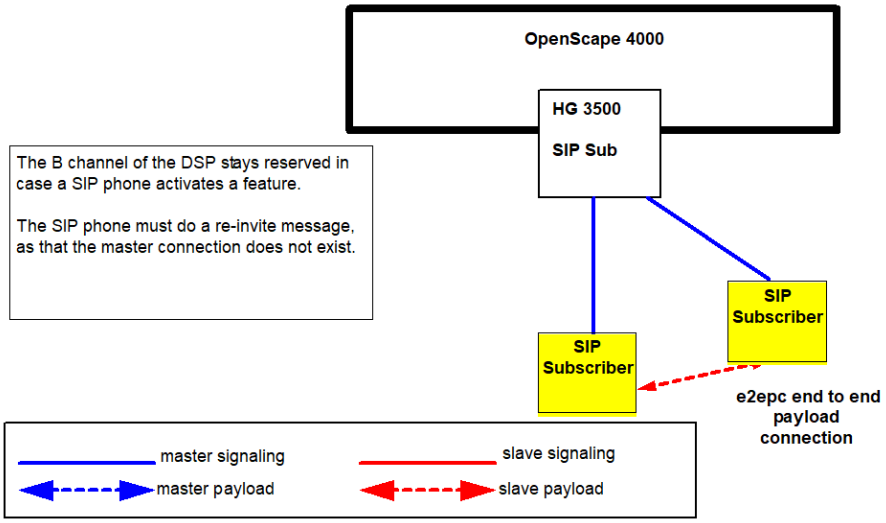
IMPORTANT: When connecting a fax adapter to a HG 3500 (SIP subscriber), DMC must be deactivated for this device (only then is T.38 transmission possible). If you want nonetheless to connect DMC for this device, the codec must be set to G.711 (fax transmission with G.711, not T.38).

19.3.3 Scenarios

The diagrams in the following sections illustrate the possible scenarios in which a SIP subscriber is involved in an e2epc, for example DMCs to HFA and SIP stations in the same (or in a different) node, and DMCs to IPDA and IP trunking boards - the latter functioning as DMC endpoints.

19.3.3.1 SIP Subscriber at same OpenScape 4000

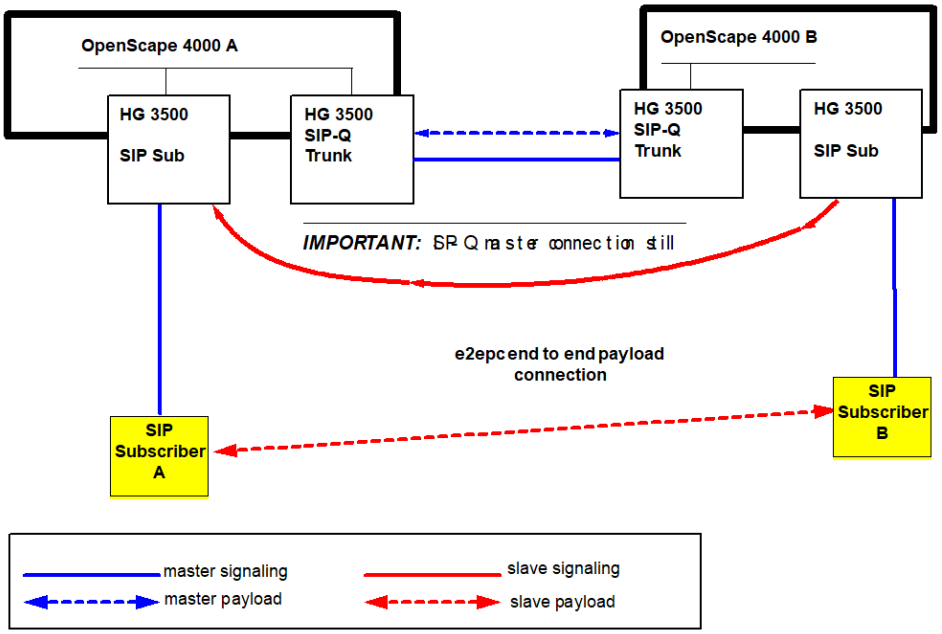
DMC signaling between the HG 3500s (or internally, if both are on the same gateway), e2epc between the stations, which replaces the master payload connection to the gateway.



19.3.3.2 SIP Subscriber at another OpenScape 4000

Slave signaling to HG 3500 SIP subscriber board, slave payload to the SIP subscriber.

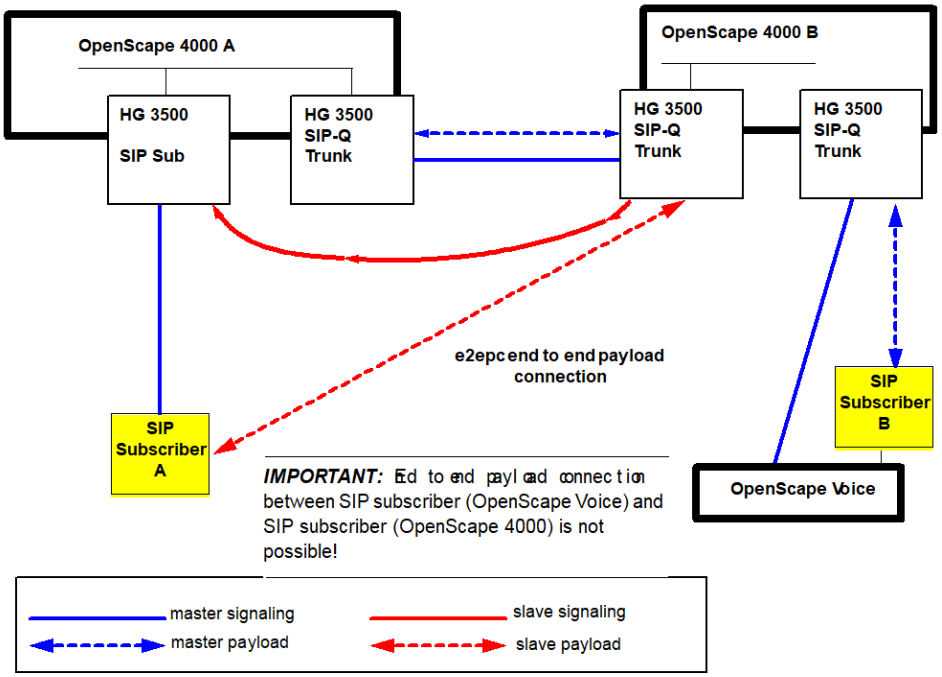
SIP subscriber A sets up a call to OpenScape 4000 A. OpenScape 4000 A routes the call via a trunking connection to OpenScape 4000 B. OpenScape 4000 B then sets up a connection to SIP subscriber B. OpenScape 4000 B initiates a DMC between SIP subscriber B and SIP subscriber A, resulting in an end-to-end payload connection.



19.3.3.3 SIP Subscriber at OpenScpae Voice

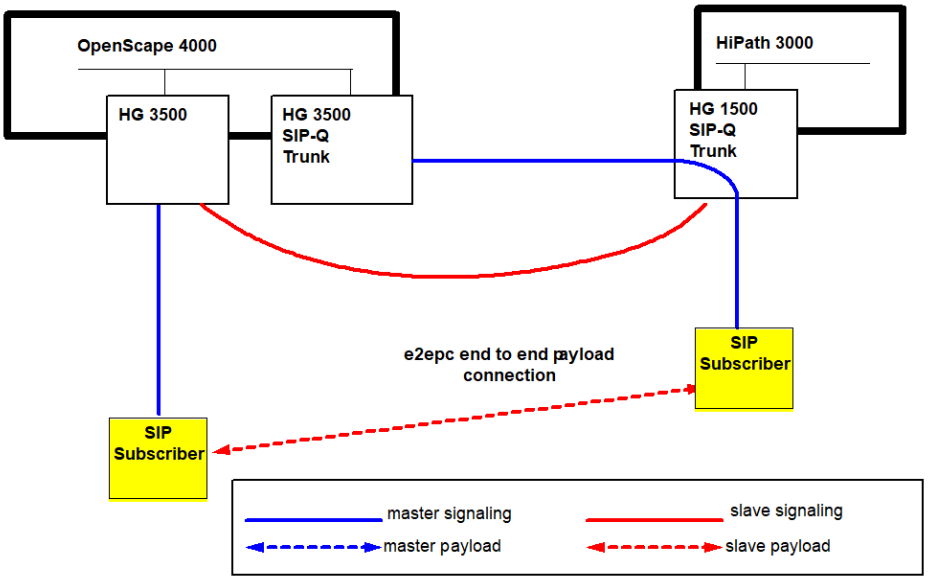
Slave signaling to HG 3500 SIP subscriber board, slave payload to the SIP subscriber.

SIP subscriber A sets up a call to OpenScape 4000 A. OpenScape 4000 A routes the call via a trunking connection to OpenScape 4000 B. OpenScape 4000 B routes the call via another trunking connection to OpenScape Voice. OpenScape Voice then sets up a connection to SIP subscriber B. OpenScape 4000 B initiates a DMC between SIP trunking gateway B and SIP subscriber A, resulting in an end-to-end payload connection.



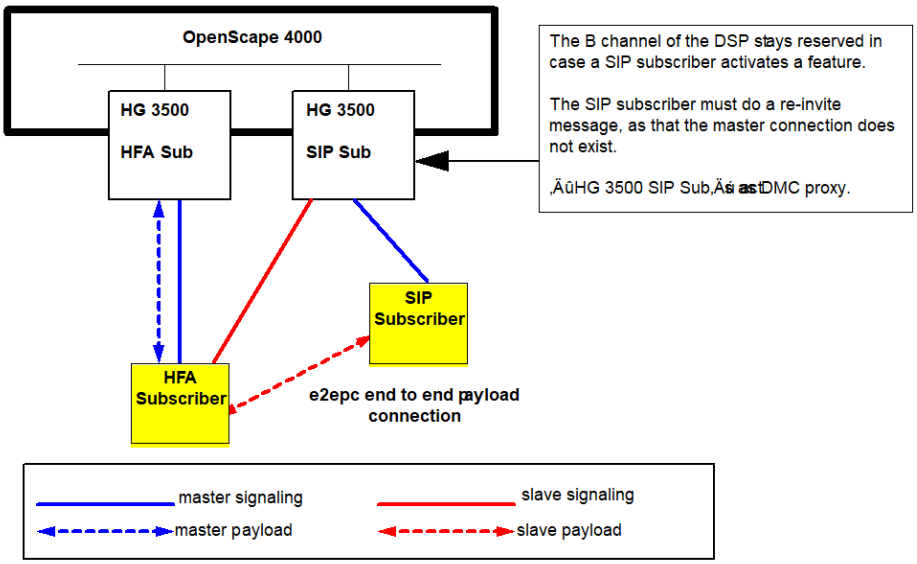
19.3.3.4 SIP Subscriber at HiPath 3000

DMC signaling between HG 3500 and HG 1500 (initiated by OpenScape 4000), e2epc between SIP subscribers.



19.3.3.5 HFA Subscriber at same OpenScape 4000

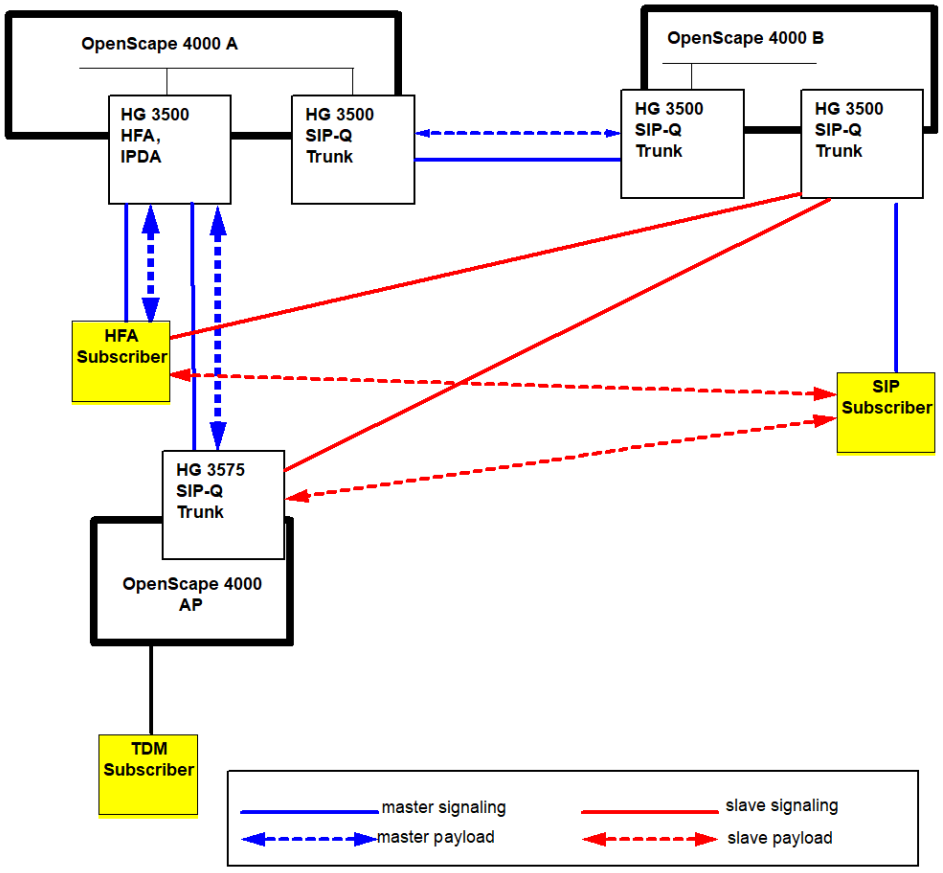
DMC signaling between HG 3500 and HFA subscriber, e2epc between the stations. A master payload connection to the HG 3500 (HFA subscriber) is retained.



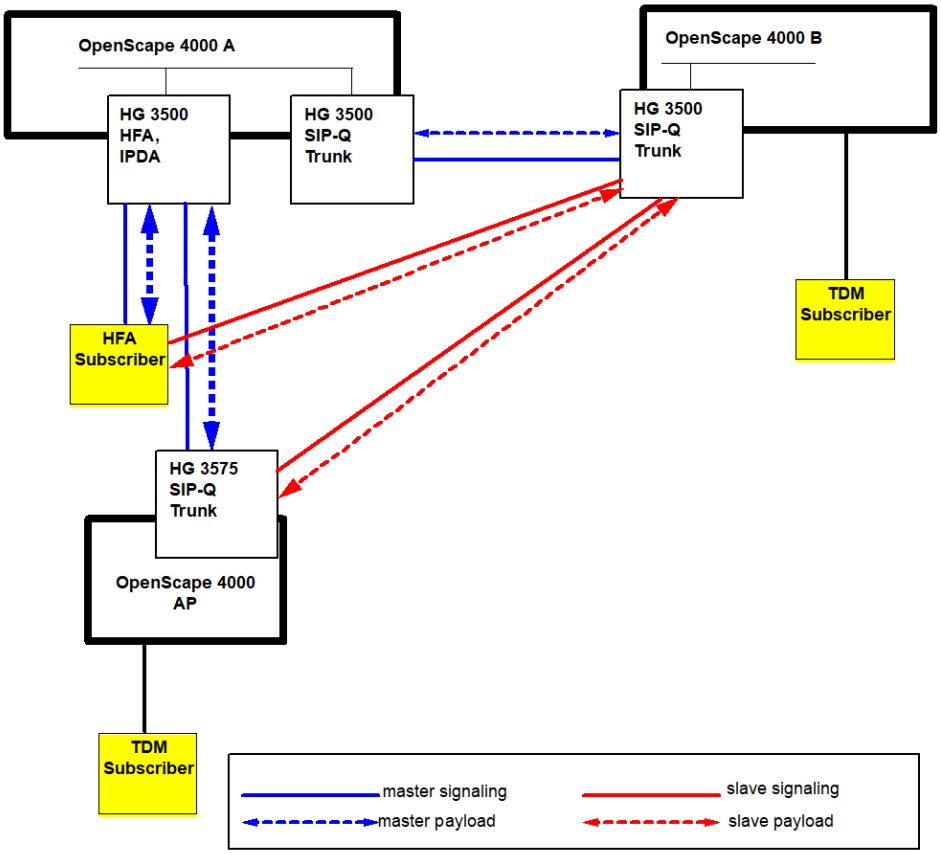
19.3.3.6 HFA Subscriber at another OpenScape 4000

Example 1: End-to-end payload between HFA and SIP subscriber (also HG 3575 and SIP subscriber)

No specific action is necessary with the HG 3500 trunking boards. OpenScape 4000 B initiates a DMC between the SIP subscriber and HFA subscriber, resulting in an end-to-end payload connection.

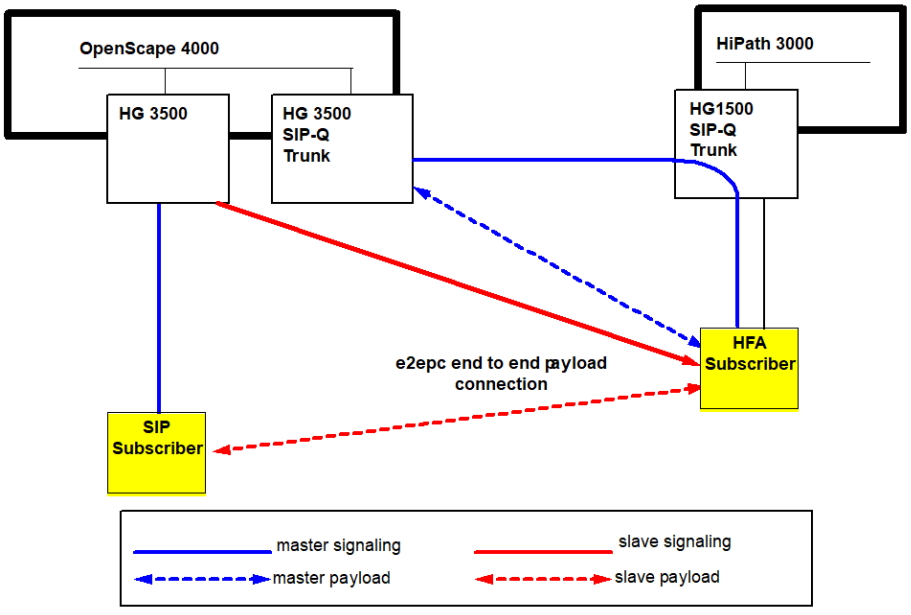


Example 2: End-to-end payload between HFA and SIP trunk (also HG 3575 and SIP trunk)



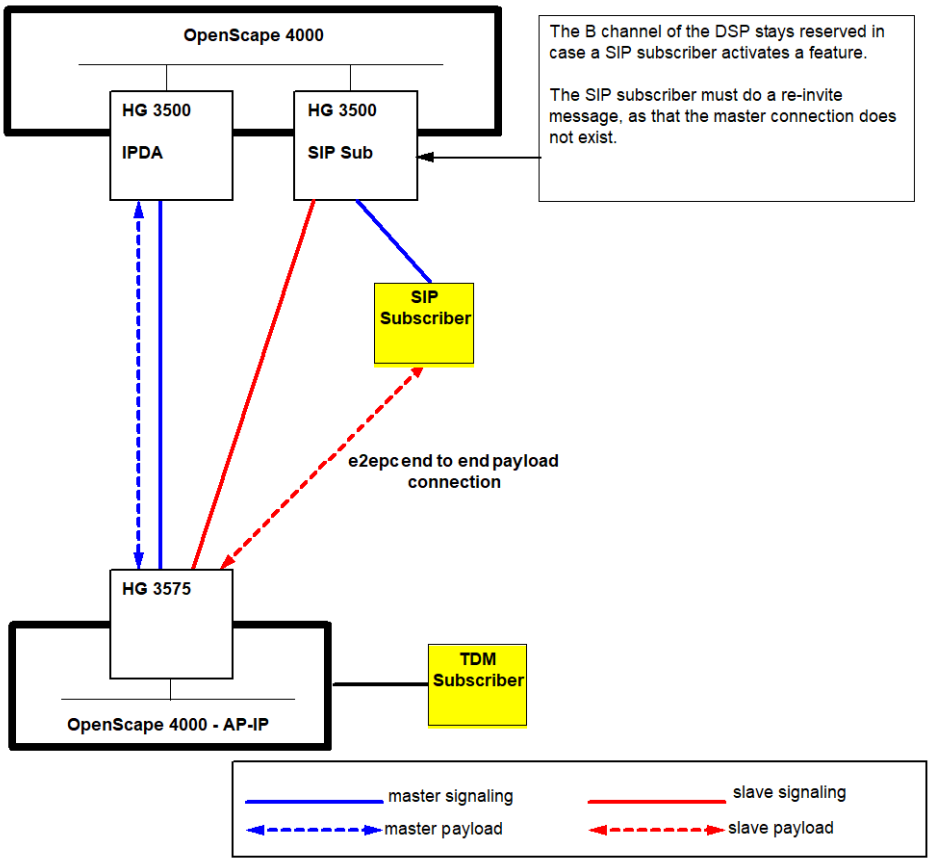
19.3.3.7 HFA Subscriber at HiPath 3000

Master signaling via HG 1500, master payload between HFA subscriber and neighboring HG 3500, slave signaling between HFA subscriber and initiating HG 3500 and slave payload between SIP and HFA subscriber.



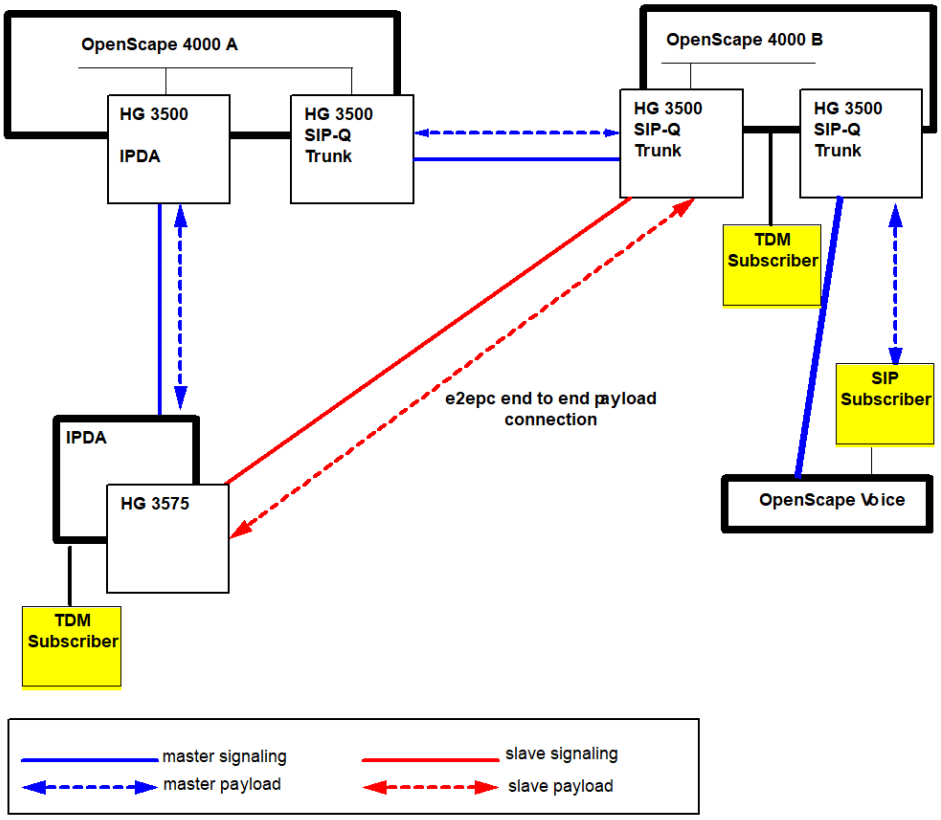
19.3.3.8 TDM Subscriber/Network behind a Remote Shelf of a OpenScape 4000

DMC signaling between HG 3500 and HG 3575, e2epc between SIP subscriber and HG 3575.



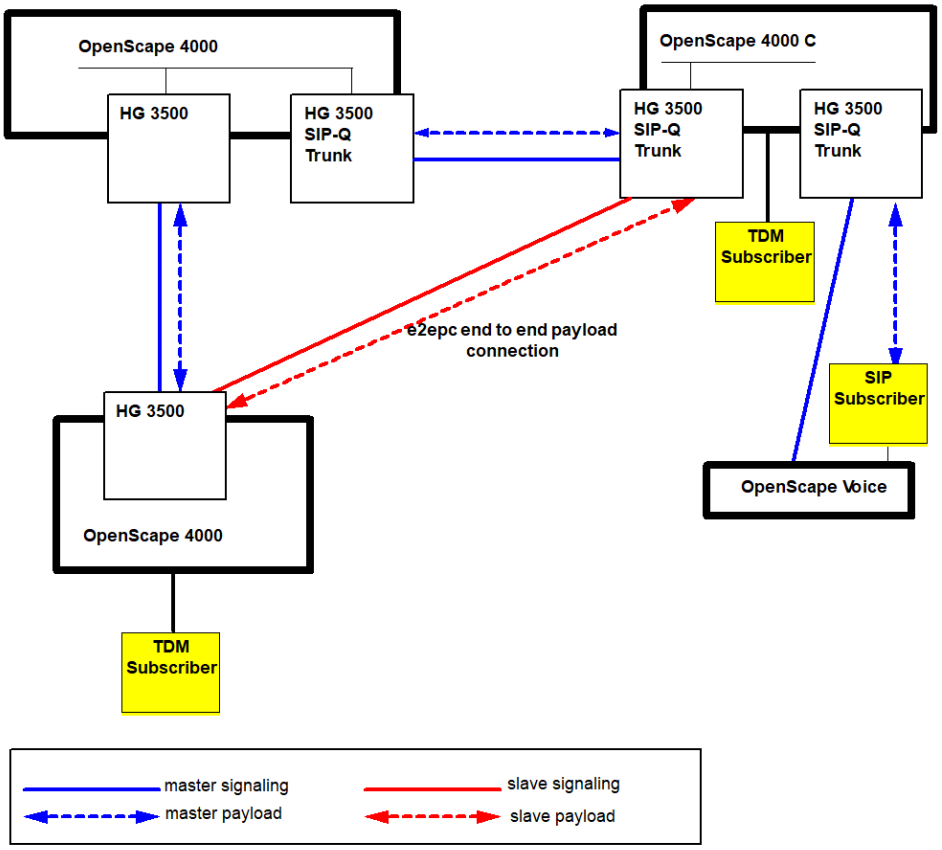
19.3.3.9 TDM Subscriber/Network at another OpenScape 4000 behind a Remote Shelf

Slave signaling and payload to HG 3575.



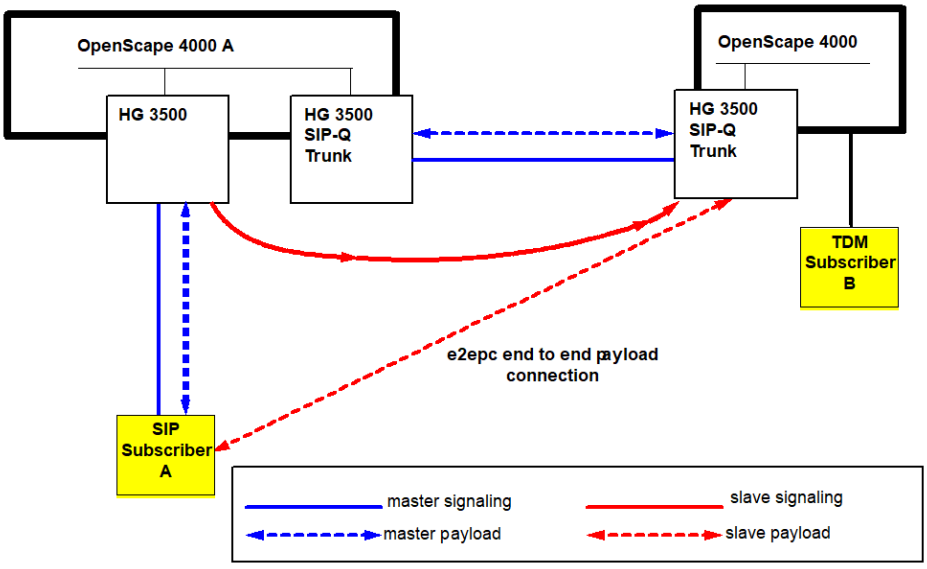
19.3.3.10 TDM Subscriber/Network at another OpenScape 4000

Example 1: Slave signaling and payload to HG 3500.



Example 2: DMC signaling between HG 3500 (SIP subscriber) and HG 3500 (Trunk), e2epc between SIP subscriber and HG 3500.

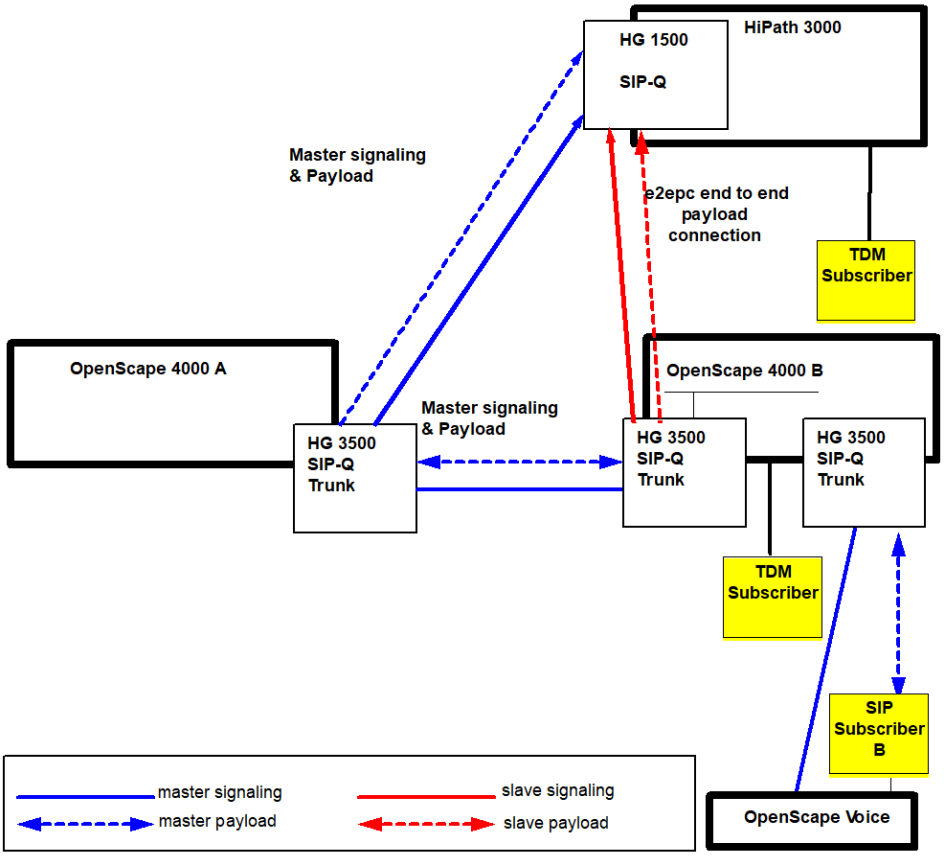
SIP subscriber A sets up a call to OpenScape 4000 A. OpenScape 4000 A routes the call via a trunking connection to OpenScape 4000 B. OpenScape 4000 B then sets up a connection to TDM subscriber B. OpenScape 4000 B initiates a DMC between HG 3500 in OpenScape 4000 B and the HG 3500 in OpenScape 4000 A. OpenScape 4000 A ensures that an end-to-end payload connection (e2epc) is established between SIP subscriber A and the HG 3500 in OpenScape 4000 B.



19.3.3.11 TDM Subscriber at HiPath 3000

Master signaling and payload between HG 1500 and neighboring HG 3500, slave signaling and payload between HG 1500 and initiating HG 3500.

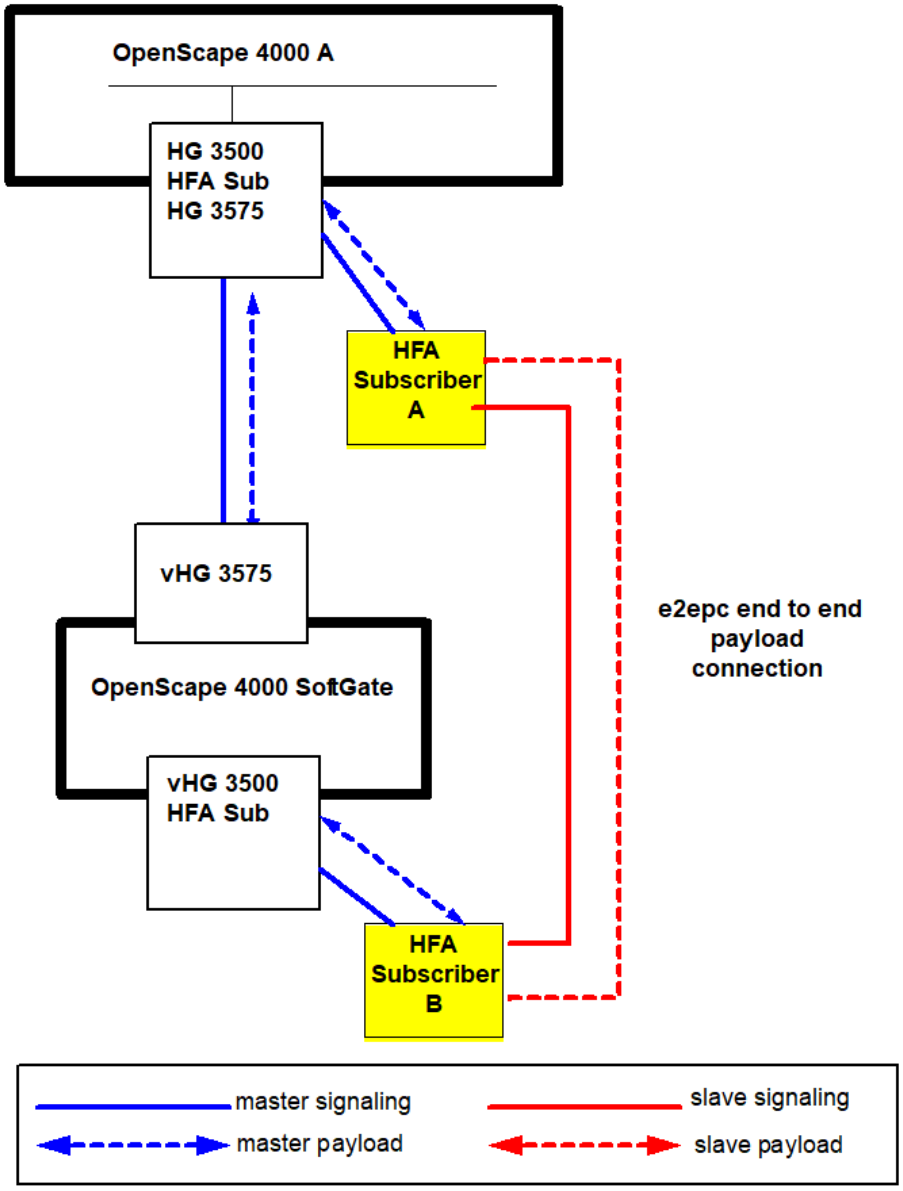
TDM subscriber at HiPath 3000 sets up a connection to OpenScape 4000 A. OpenScape 4000 A routs the call via a trunking connection to OpenScape 4000 B. OpenScape 4000 B routes the call via another trunking connection to OpenScape Voice. OpenScape Voice then sets up a connection to SIP subscriber B. OpenScape 4000 B sets up a DMC between HG 3500 in OpenScape 4000 B and HG 1500 in HiPath 3000.



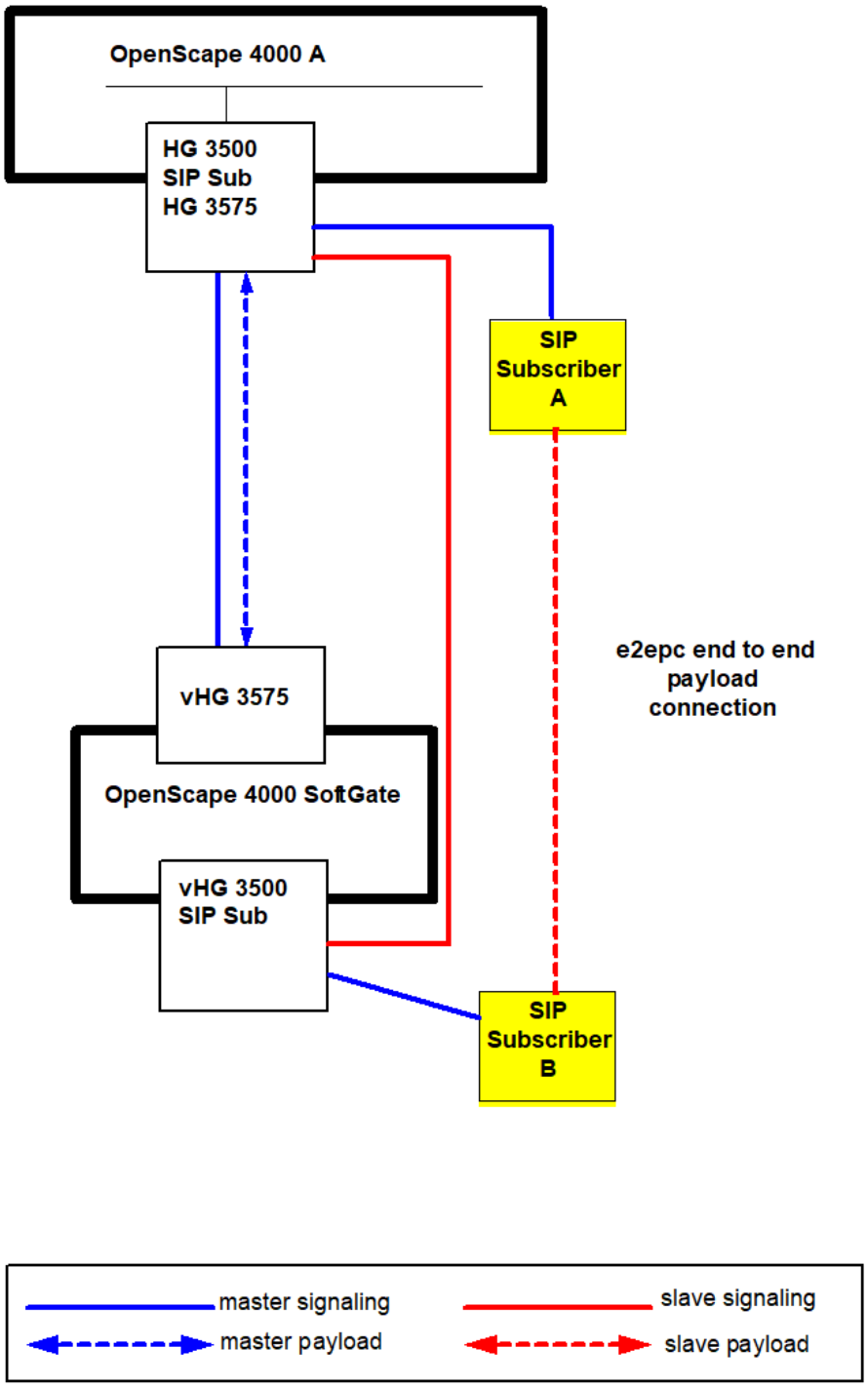
19.4 Direct Media Connect (DMC) in Connection with OpenScape 4000 SoftGate

IMPORTANT: For SIP subscriber: If DMC is not active, the payload is exchanged between the SIP subscriber and its HG 3500 (or vHG 3500). If DMC is active, the payload is exchanged **exclusively** via the end-to-end payload path.

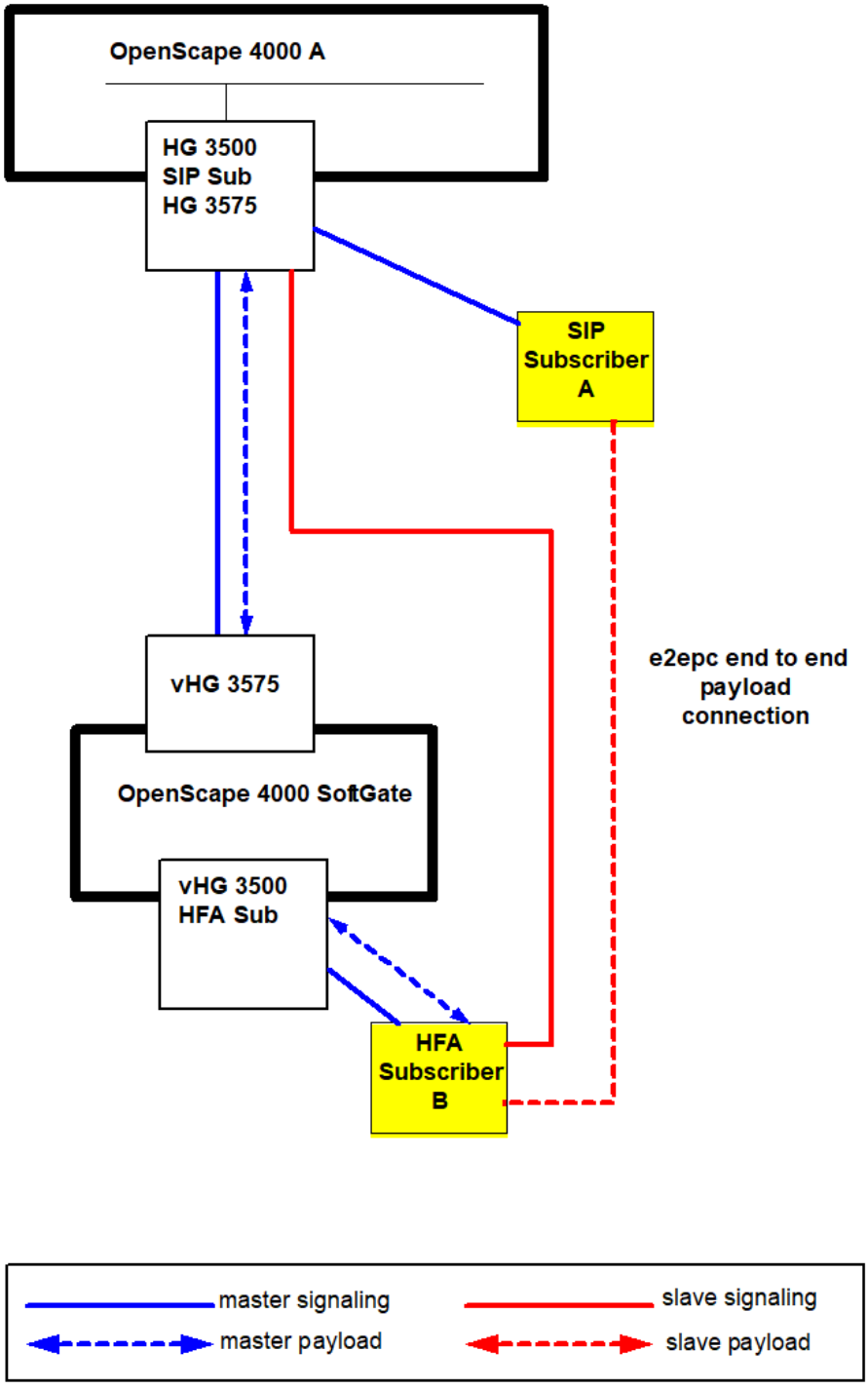
Example 1: HFA Subscriber A at OpenScape 4000 A calls HFA Subscriber B at OpenScape 4000 SoftGate



Example 2: SIP Subscriber A in OpenScape 4000 A calls SIP Subscriber B at OpenScape 4000 SoftGate

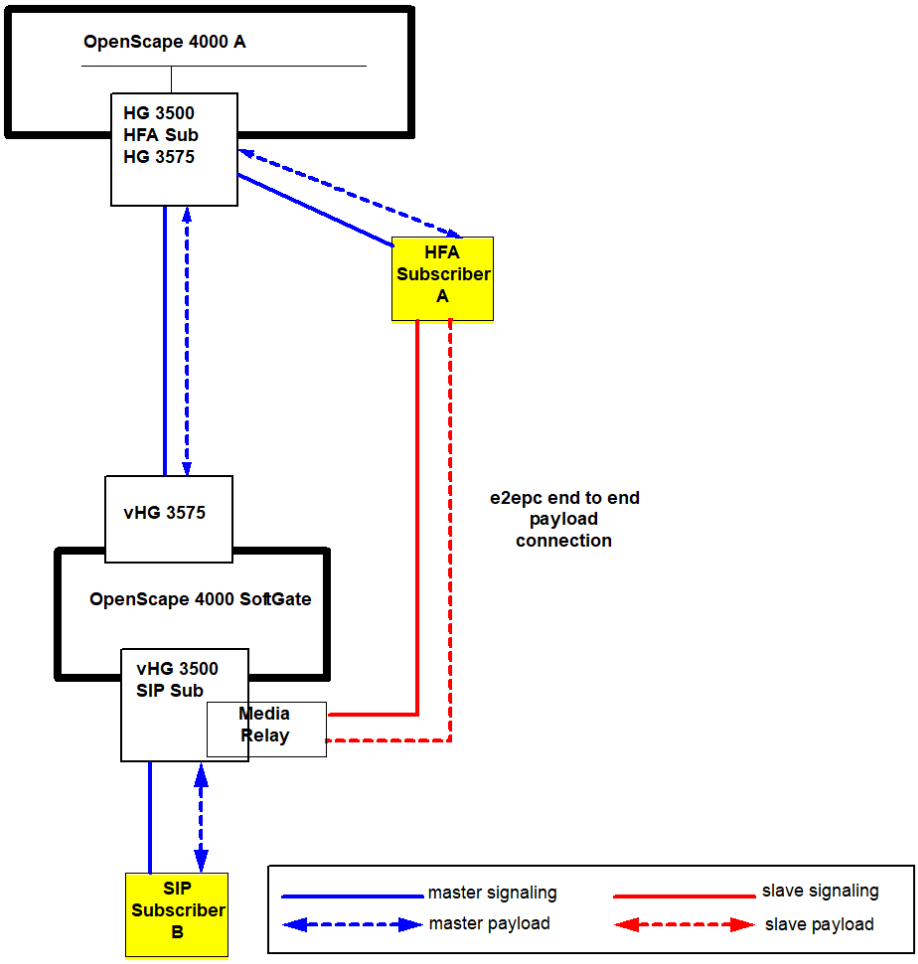


Example 3: SIP Subscriber A at OpenScape 4000 A calls HFA Subscriber B at OpenScape 4000 SoftGate

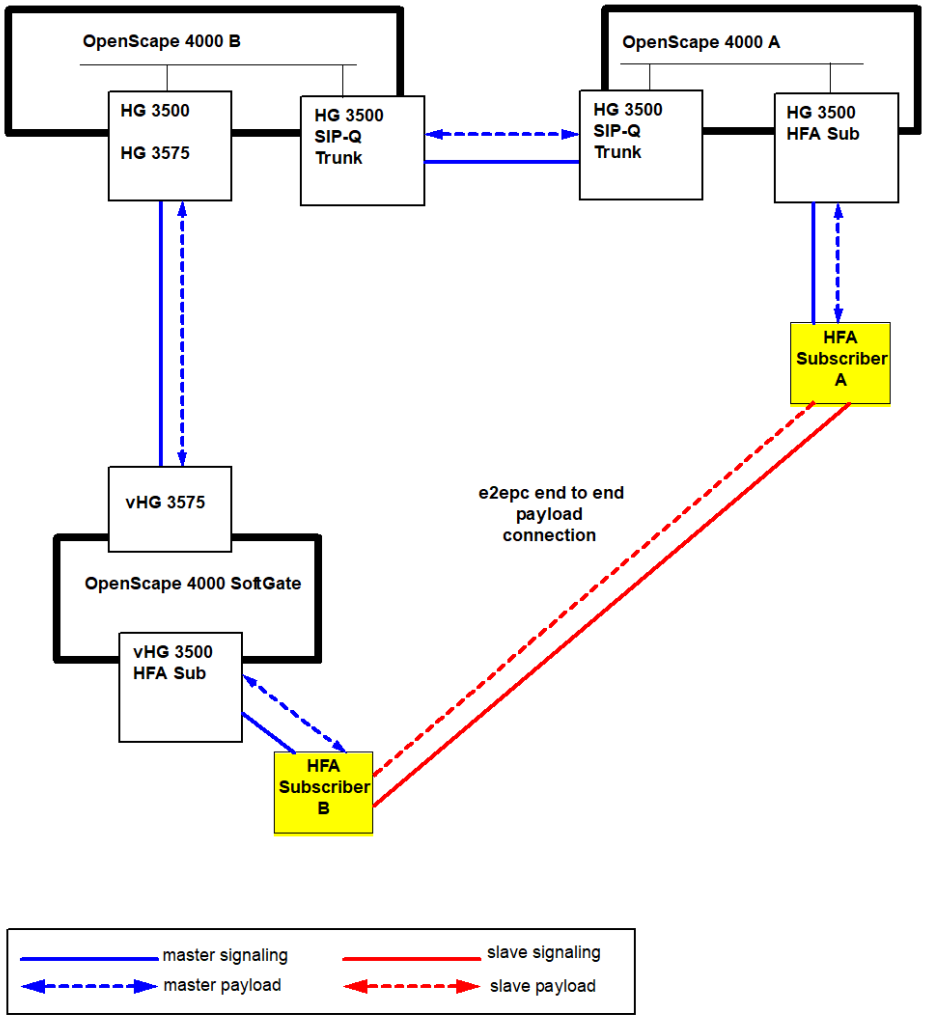


Example 4: HFA Subscriber A at OpenScape 4000 A calls SIP Subscriber B at OpenScape 4000 SoftGate

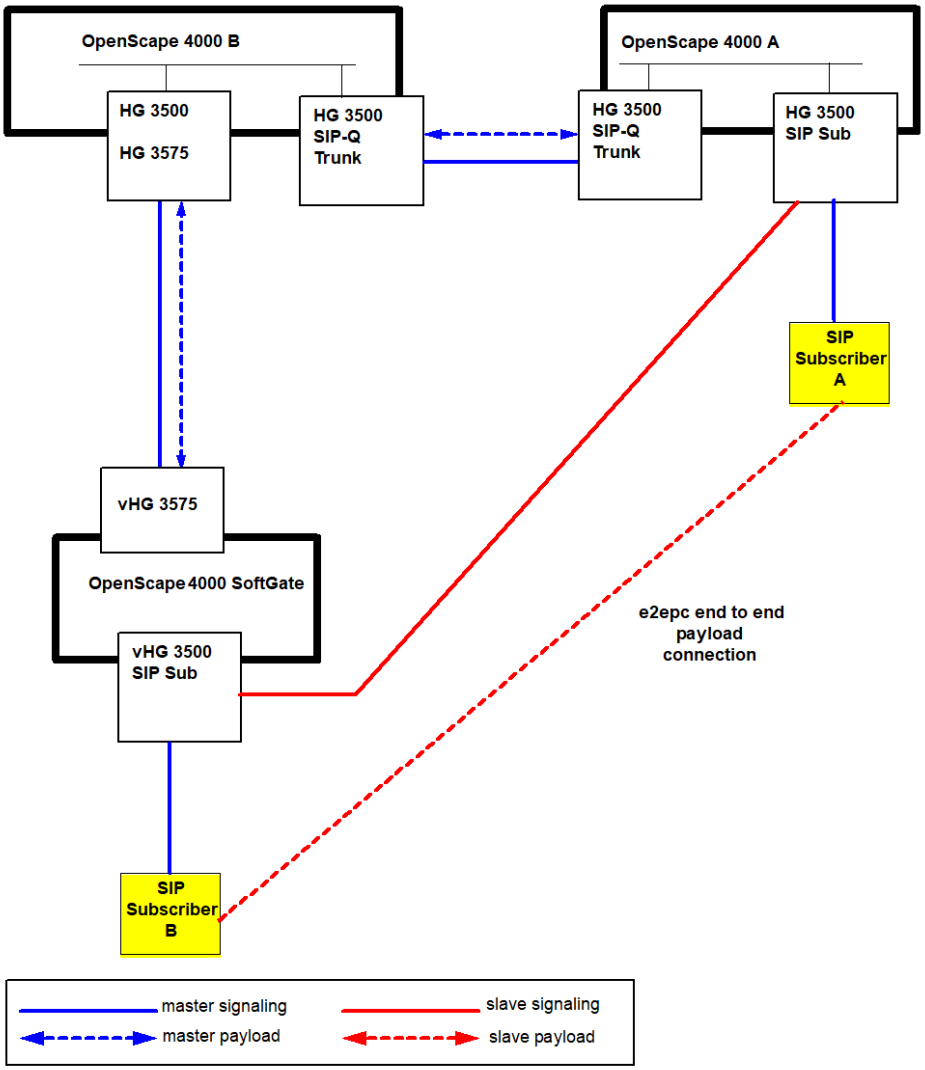
If a SIP device or SIP native trunk on OpenScape 4000 SoftGate communicates with a DMC endpoint (not DMC proxy!), a media relay on the OpenScape 4000 SoftGate is always switched between them. This corresponds to an RTP proxy which always routes the media stream (RTP) via the OpenScape 4000 SoftGate.



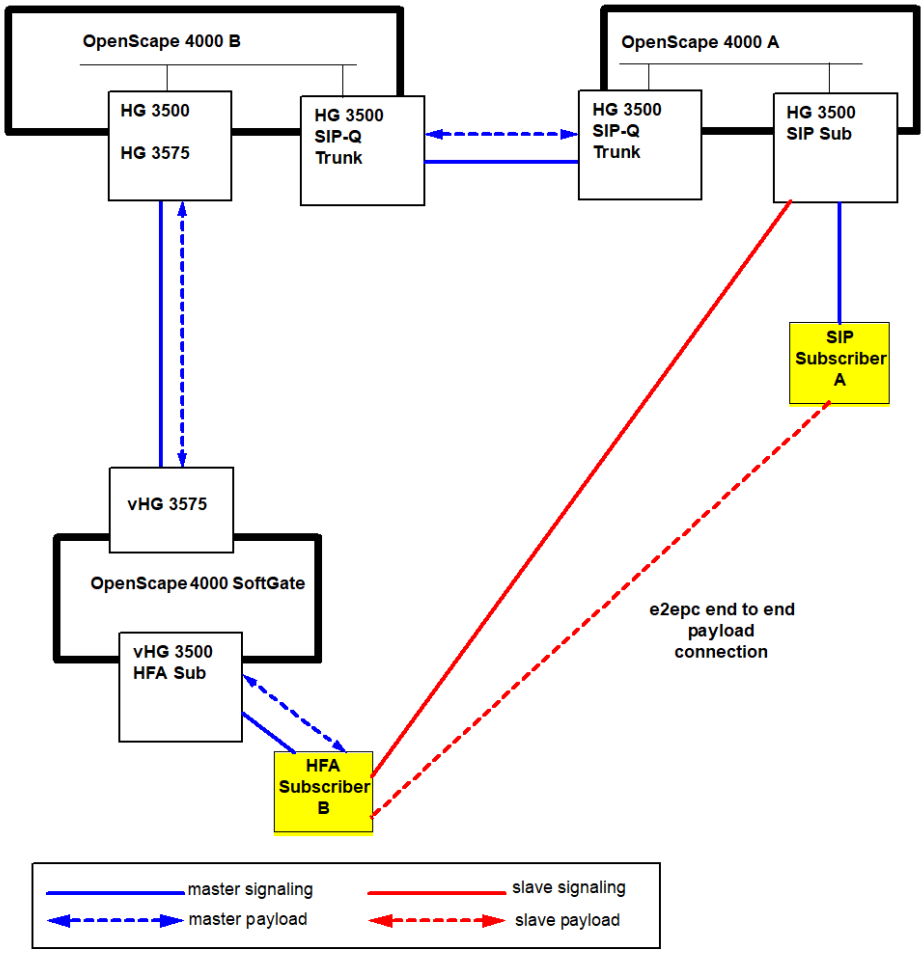
Example 5: HFA Subscriber A at OpenScape 4000 A calls HFA Subscriber at OpenScape 4000 SoftGate



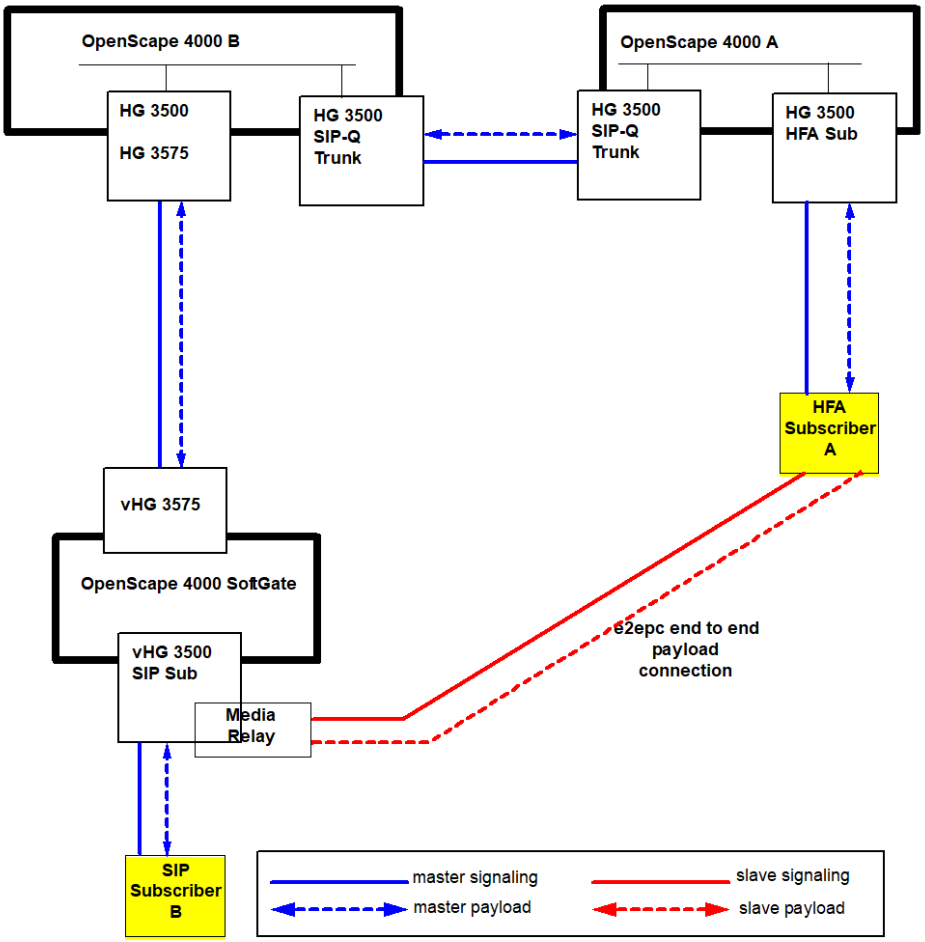
Example 6: SIP Subscriber A at OpenScape 4000 A calls SIP Subscriber at OpenScape 4000 SoftGate



Example 7: SIP Subscriber A at OpenScape 4000 A calls HFA Subscriber B at OpenScape 4000 SoftGate



Example 8: HFA Subscriber A at OpenScape 4000 A calls SIP Subscriber B at OpenScape 4000 SoftGate


OpenScape 4000 B
HG 3500
HG 3575
HG 3500
SIP-Q
Trunk
OpenScape 4000 A
HG 3500
SIP-Q
Trunk
HG 3500
HFA Sub
HFA
Subscriber
A
vHG 3575
OpenScape 4000 SoftGate
vHG 3500
SIP Sub
Media
Relay
s2epc end to end
payload
connection
SIP
Subscriber
B
master signaling
slave signaling
master payload
slave payload

20 T.38 Fax

20.1 Definition

The T.38 fax standard is a protocol which allows for fax transmission over IP networks in real time.

20.2 Feature Description

T.38 fax is supported in scenarios with common gateway, OpenScape 4000 SoftGate, IPDA NCUI, and IPDA STMI.

20.2.1 Important Notes

IMPORTANT: When connecting a SIP subscriber fax adapter on STMI2 or STMI4 boards, DMC must be deactivated for the device or T.38 transmission is not possible (the reason is classic STMIs have no internal media relay function and cannot negotiate T.38 on two separate streams). If DMC is important for the customer on those devices, the codec must be set to G.711 and T.38 switched off.

IMPORTANT: T.38 fax streams are not supported for SPE.

IMPORTANT: T.38 configuration/usage requires end-to-end DMC between OpenScape 4000 gateways (minimized IP hops) because of timing requirements according to T.38 standard. In case of multiple IP hops the fax transmission could fail with some fax machines - see Section 2.2.1, “Delay problems in scenario with 2 and more IP-hops and certain fax machines”.

IMPORTANT: T.38 can be used right from the beginning of a transmission, that is, with initial SIP invite.

20.2.2 Restrictions

20.2.2.1 Delay problems in scenario with 2 and more IP-hops and certain fax machines

If the fax transmission takes place over two or more IP-hops for some (mainly older) fax machines the roundtrip delay is too high if T.38 is used. There are two categories of errors. In the first case the negotiation fails and the fax transmission doesn’t start at all. In the second case the first page is

transmitted and received correctly but it is not acknowledged in time. This causes the fax machine to display a communication error and a second page is not transmitted. T.38 can also be used directly from the beginning of a SIP connection (meaning from the initial SIP invite).

There will be no solution with the original fax machines.

- T.38 configuration/usage requires end-to-end DMC between HP4K gateways (minimized IP hops) because of timing requirements according to T.38 standard. In case of multiple IP hops the fax transmission could fail with some fax machines, e.g. Canon FAX-L100 Canon FAX-L120 Panasonic Fax UF-595 Panasonic Fax UF-495

Resolution for affected fax machines: replacement of old fax machines or usage of G711 transparent mode instead of T.38

- If T.38 is supposed to be used with AP1120, G.711 must be configured as voice codec only, i.e. always in case a modem or fax is connected to an AP1120 the only allowed codec in the AP1120 has to set to G.711 (no option for compression).

20.2.2.2 DMC problem with AP1120

If G.729 is set as prio1 codec and the sending fax machine is connected to the AP1120 it can happen, that the master call between GW and AP1120 is switched to G.711 before the DMC is established. The AP1120 detects the CNG and switches to data mode. When the receiving fax machine goes off-hook, the DMC is established with G.729. (The GW sends G.729 and the AP1120 continues with G.711 as the master connection was already switched to data mode). After detecting the CED tone on the receive side an OLC with G.711 is sent to the AP1120. The AP1120 does not response correctly to this OLC as a switch to G.711 already took place (on the master channel).The GW itself can not switch to G.711 as the acknowledgement from AP1120 is missing. Therefore the GW continues sending G.729 packets.

NOTICE: Always if a modem or fax is connected to an AP1120 the only allowed codec in the AP1120 has to be set to G.711.

20.2.2.3 DMC not established with MTX41xx

If the sending fax is connected to an MTX41xx adapter in a DMC scenario and T.38 is enabled the DMC is often rejected.

The MTX41xx switches in the default configuration to T.38 after detecting a CNG tone. If the sending fax machine is connected to the MTX41xx adapter the possibility is very high, that the first CNG tone is detected before the receiving fax machines goes off-hook and the DMC is established. This means in this case the master channel between MTX41xx and SoftGate is reconfigured to T.38 before the DMC request is received and therefore the DMC is rejected.

Workaround In the MTX41xx there is the parameter defaultMachineDetectionCngToneDetection. If this parameter is set to disable, then the MTX41xx switches to T.38 only after detecting V.21 flags.

Remarks

1) If the CNG tone detection is disabled the switch to T.38 takes place later. On the other hand the Mediatrix adapter detects the V.21 flags only on the SCN side. This means the adapter on the sending side is detecting the fax very late (Commerzbank problem) and it is important that the fax is detected on the receive side.

This problem can only occur if the MTX41xx is connected to the SoftGate.

1) The parameter “USE Previous Media Negotiation” exists only in the DGWv2.0 load ware from Mediatrix. Therefore an upgrade from the SIPv5.0 to the DGWv2.0 load ware has to be performed on the MTX41xx devices. The tests are made with the DGWv2.0 load ware at the moment.

20.2.2.4 Parameter “USE Previous Media Negotiation” has to be set

If an interworking between MTX4104 connected to SoftGate and MTX4104 connected to CGW takes place the parameter “USE Previous Media Negotiation” has to be enabled in the MTX.

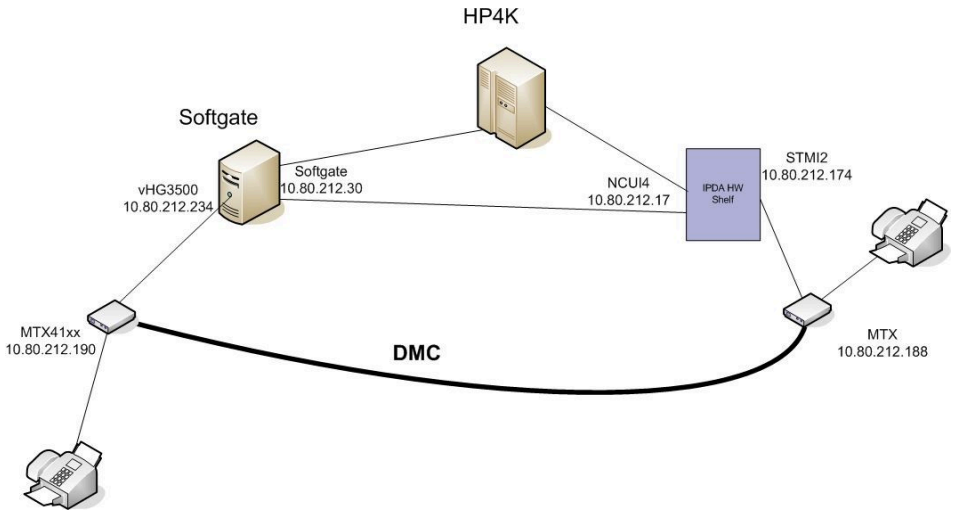


Figure 430: Scenario with T.38 disabled in the MTX 10.80.212.188

In the Scenario above T.38 is disabled in the MTX 10.80.212.188. Therefore DMC is allowed. In all other components T.38 is enabled.

Assumed the parameter “USE Previous Media Negotiation” is not set: First a DMC is established between the both MTX41xx adapters. After recognizing that a fax is connected the MTX 10.80.212.190 sends a T.38 re-invite, which will be rejected with “488 Not Acceptable” here by the vHG3500 10.80.212.234. The reason is that it is not possible to make a renegotiation of features in a DMC interworking scenario on the CGW. After the reject of T.38 a G.711 re-invite is sent by Mediatrix. Also this re-invite is rejected due to the reason mentioned above. After the second reject the MTX41xx drops the call.

If the parameter “USE Previous Media Negotiation” is set, the MTX41xx continues with G.711 after receiving the “488 Not Acceptable” for T.38 re-invite and the fax transmission works.

20.2.3 Common Gateway

T.38 is possible for

- IP trunking connections (H323 and H323A)
- SIP trunking connections (SIP-Q and native SIP)
- DMC connections from/to IPDA-STMI/HG 3570

20.2.4 OpenScape 4000 SoftGate/STMIX/STMIY

The following scenarios are supported with OpenScape 4000 SoftGate:

- Analog fax devices at Mediatrix 41xx connected to a virtual HG 3500 (SIP subscriber interface).
- Fax from central office at Mediatrix 44xx connected to a virtual HG 3500 (SIP trunk interface).
- Fax from SIP provider / OpenScape Xpression connected to a virtual HG 3500 (SIP trunk interface).
- Fax from another OpenScape 4000/HiPath 4000 system connected to a virtual HG 3500 (SIP/SIP-Q trunk interface).
- Fax from another OpenScape 4000 SoftGate, IPDA NCUI or IPDA STMI.

Each interface supports the switchover to T.38 based on tone evaluation.

NOTICE: The maximal number of parallel T.38 fax channels on STMI board is 60. The limit of 60 is independent of STMI type (i.e. whether STMI2/STMI4) or 60/120 channels, the limit of 120 applies for SoftGate and STMIX/STMIY. Further fax calls will then be processed with G711 clear channel.

NOTICE: When using STMI4/NCUI4 boards a Fax/Modem tone detection with G729 codec is possible and the gateway will automatically switch to G711 mode. STMI2/NCUI2 boards do not have enough performance capabilities to make this change.

NOTICE: If T.38 is supposed to be used with AP 1120, G.711 must be configured as voice codec only, i.e. always in case a modem or fax is connected to an AP 1120 the only allowed codec in the AP 1120 has to set to G.711 (no option for compression).

20.2.5 IPDA

The following scenarios are supported with IPDA:

- Analog fax devices connected to SLMA in the host or access point shelf.
- Analog fax devices at Mediatrix 41xx connected to HG 3500 (SIP subscriber interface).
- Fax from central office connected to TDM trunk board.
- Fax from SIP provider connected to HG 3500 (SIP trunk interface).

- Fax from another OpenScape 4000/HiPath 4000 system connected to HG 3500 (SIP trunk interface).
- Fax from another OpenScape 4000 SoftGate, IPDA NCUI, or IPDA STMI.

NCUI and IPDA STMI support the switchover to T.38 based on tone evaluation on the master call and DMC slave call.

20.3 Scenarios

OpenScape 4000 allows using T.38, also on the master channel. The following figures show some supported scenarios:

Scenario 1: OpenScape 4000 SoftGate - OpenScape 4000 host system

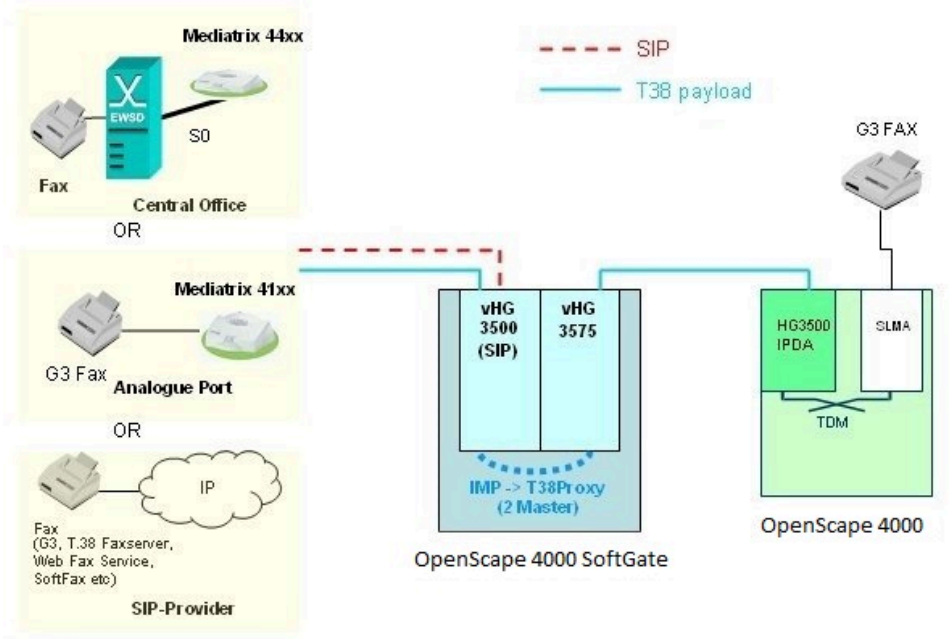


Figure 431: OpenScape 4000 SoftGate - OpenScape 4000 host system

This scenario shows a typical fax call from a small site with OpenScape 4000 SoftGate at the main site. Usually the connection will be established as a voice call. After tone detection, a switchover to T.38 will be initiated.

Scenario 2: Fax between SMP enabled endpoints

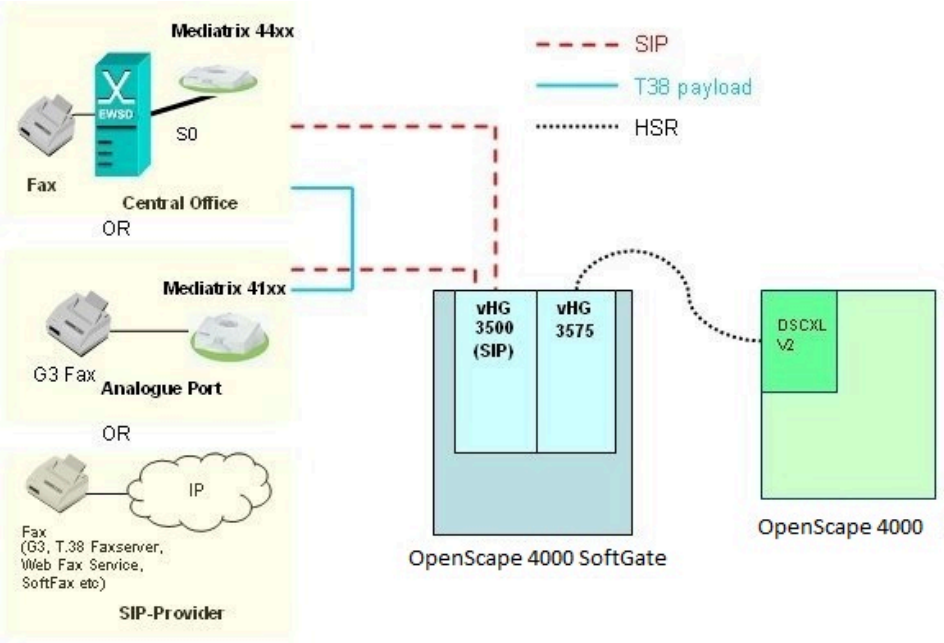


Figure 432: Fax between SMP enabled endpoints

This scenario shows a fax call between SMP (SIP Message Proxy) enabled endpoints. The media negotiation is performed end to end, i.e. the OpenScape 4000 SoftGate is not involved in media handling.

Scenario 3: Media routing in IPv6 scenario

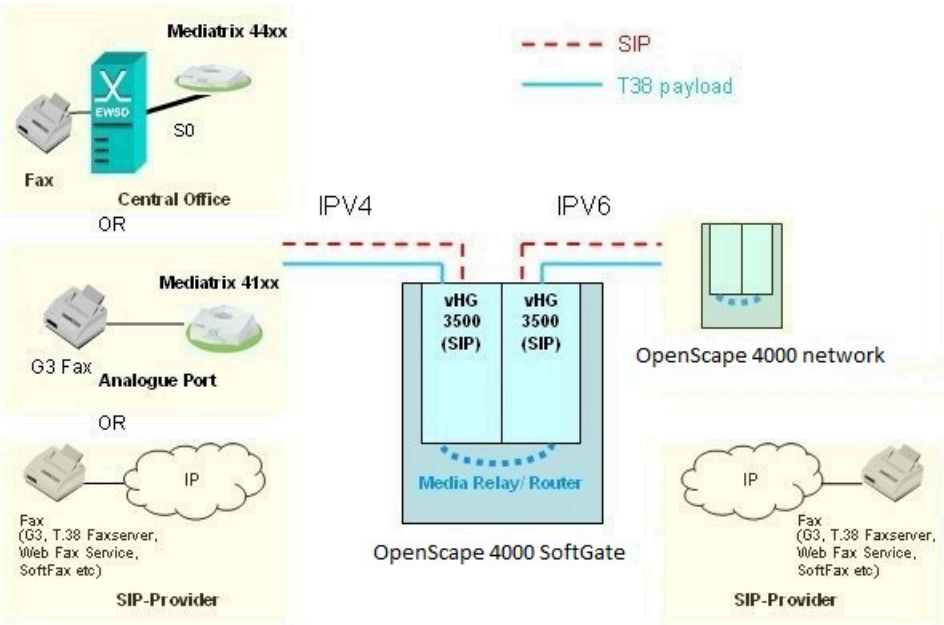


Figure 433: Media routing in IPV6 scenarios

This scenario shows a fax call between IPV4 and IPV6. The conversion between IPV4 and IPV6 is performed by the OpenScape 4000 SoftGate, which functions as media relay.

Scenario 4: Media relay scenario with DMC (Direct Media Connection)

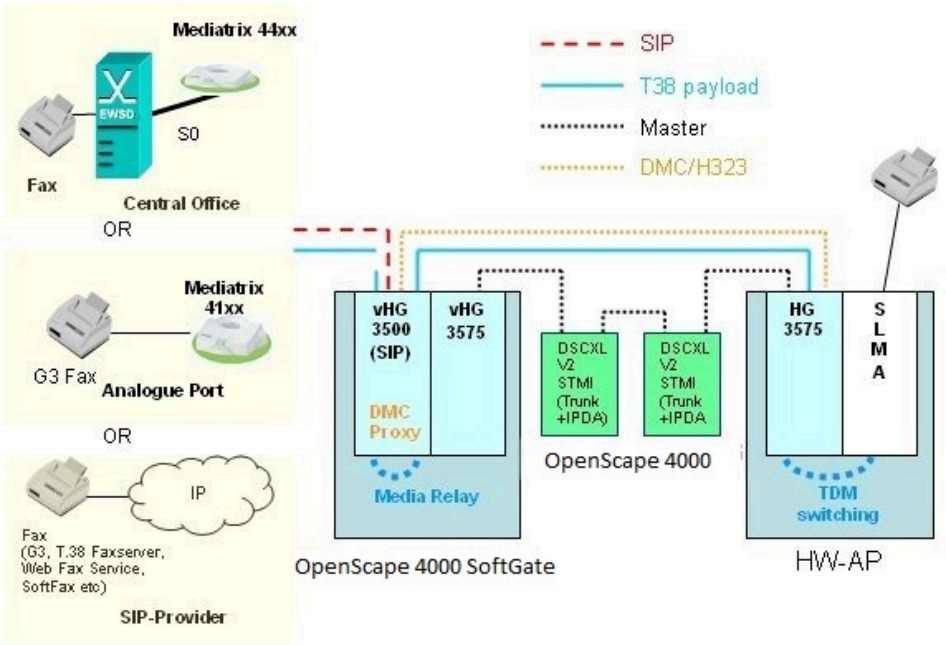


Figure 434: Media Relay scenario with DMC

This scenario shows a fax call from an OpenScape 4000 SoftGate through an OpenScape 4000 network (either SIP-Q or TDM) to a hardware access point.

A DMC is initiated. In case the fax tones are detected before the DMC has been established, the DMC is canceled, and the master channel is used instead. The OpenScape 4000 SoftGate will install a media relay between SIP and H323.

20.4 Service Information

The following T.38-related features are provided with OpenScape 4000 SoftGate:

- Codec switching on the fly
- The Mediatrix AP 41xx, as well as SIP providers, switch from G.729 to G.711 codec without signaling. Therefore, payload-based switching on the fly on the receiving side is supported.
- Jitter buffer improvements
- With HiPath 4000 V6 a greater buffer is provided for T.38 transmissions. The buffer size will be switched during a pause (idle) in the media stream.
- Usage of RFC2833 for fax
- Albeit discouraged, RFC2833 for fax tones is still supported. However, it is disabled by default. After a software update, the previously configured value will be preserved.

IMPORTANT: With some scenarios, the use of RFC2833 for fax tones may cause problems, so it must be disabled. This is the case with the following configurations: - A Mediatrix 41xx adapter is connected to a hardware gateway, and a AP1120 Cornet IP Adapter is used in the same system. If a DMC shall be established between both adapters, RFC2833

for fax must be disabled. - A SIP service provider which does not support RFC2833 for fax is connected to a hardware gateway.

20.4.1 OpenScape 4000 SoftGate/STMIX/STMIY

- SIP
- With OpenScape 4000 SoftGate, T.38 can be used right from the beginning of a transmission, that is, with initial SIP invite.
- H323/DMC
- DMC uses the existing mechanism to support a switchover to T.38 (actively and passively).

20.4.2 IPDA (NCUI/STMI)

In IPDA, two main fax connections can be distinguished:

- DMC (NCUI/STMI as endpoint) and
- master calls.

Master / Slave Connection

The master connection is controlled by the host system, whereas the slave connection (DMC) is controlled by the board itself.

Since IPDA master connections are not controlled by H323, IPDA endpoints detect T.38 with tone evaluation. Each IPDA endpoint sends a message to the DNIL in the SWU stating that T.38 is possible. If this is the case, DMC is rejected. When the DNIL has received the messages, a T.38 path switch message is sent to the endpoints.

Restrictions

- If no T.38 resources are available, G.711 is used as an alternative. The resource limitation is signaled to the DNIL. This restriction applies to all hardware gateways.
- QoS Monitoring
- QoS monitoring on the T.38 (former voice) channel is adapted to T.38 to that effect that T.38 is always regarded as "good quality". Hence, no BAD_QUALITY messages are generated.
- Bandwidth Management
- The consumed bandwidth depends on the selected redundancy factor and the fax transmission speed. There is no specific bandwidth management for T.38; it will be counted like G.711, with 30ms packet size.

  This restriction also applies to connections other than IPDA.

20.5 Generation (Example)

The following parameter settings are taken from a working configuration; it applies to all scenarios described in this chapter (see Chapter 3, “Scenarios”).

TOSPL = 184 (184) TOSSIGNL = 104 (104)

UDPPRTLO = 29100 (29100) UDPPRTHI = 30999 (30999)

T38FAX = YES (YES) REDRFCTN = YES (YES)

RFCFMOIP = NO(NO) RFCDTMF = YES (YES)

PRIO1 : CODEC = G711A VAD = NO RTP-SIZE = 30

PRIO2 : CODEC = G729A VAD = NO RTP-SIZE = 20

PRIO3 : CODEC = G723 VAD = NO RTP-SIZE = 30

PRIO4 : CODEC = NONE VAD = NO RTP-SIZE = 20

PRIO5 : CODEC = NONE VAD = NO RTP-SIZE = 20

PRIO6 : CODEC = NONE VAD = NO RTP-SIZE = 20

PRIO7 : CODEC = G729AB VAD = YES RTP-SIZE = 20

20.6 Relevant AMOs

AMO	Parameter	Sprache/ Language	Beschreibung/ Description
CGWB	T38FAX	d	Schaltet T.38 generell ein oder aus. Weitere Parameter, zur Konfiguration der T.38-Funktionalität befinden sich im WBM.
	T38FAX	e	Switches T.38 on or off generally. Further parameters for configuring the T.38 functionality are to be found in the WBM.
	RFCFMOIP	d	Schaltet RFC 2833 für Fax/Modem-Töne ein oder aus. Steht der Parameter auf JA, so werden die Fax/ Modem-Töne als RFC 2833-Events übertragen. Der Parameter hat nur Einfluss auf die Tonübertragung, also auf den Sprachkanal. Somit ist er nur in der Phase vor dem Start des T.38-Stacks relevant. Der Parameter muss im gesamten System auf den gleichen Wert gesetzt wird.
	RFCFMOIP	e	Switches RFC 2833 for fax/modem tones on or off. If the parameter is set to YES, the fax/modem tones are transmitted as RFC 2833 events. The parameter influences only the tone transmission, that is, the speech channel. Thus, it is only relevant within the phase before the T.38 stack is started. The parameter must be set to the same value in the entire system.

AMO	Parameter	Sprache/ Language	Beschreibung/ Description
	REDRFCTN	d	Schaltet RFC 2198 ein oder aus. Steht der Parameter auf JA, so werden die RFC 2833-Events redundant übertragen. Der Parameter hat nur Auswirkungen, wenn RFC 2833 eingeschaltet ist (RFCFMOIP=JA). Der Parameter muss im gesamten System auf den gleichen Wert gesetzt wird.
	REDRFCTN	e	Switches RFC 2198 on or off. If the parameter is set to YES, the RFC 2833 events are transmitted in redundant fashion. The parameter is only effective when RFC 2833 is switched on (RFCFMOIP=YES). The parameter must be set to the same value in the entire system.

21 IP Terminals

21.1 Supported IP Terminals

The following IP terminals (HFA) are supported:

- OpenStage HFA
- OpenScape Desk Phone IP 35G HFA
- OpenScape Desk Phone IP 55G HFA
- optiPoint 410/420 CorNet IP
- AP 1120 CorNet-IP (only HG 3500)
- AC-Win IP
- OpenScape Personal Edition HFA
- OpenScape UC Web Embedded Client
- OpenScape Desk Phone CP100/110/200/210/400/410/600/700/710 HFA

IMPORTANT: For the released SIP terminals please refer to section „SIP Connectivity“ > Chapter 2, “SIP Subscriber”.

21.2 Boards

IP terminals can be configured on the following boards with an Ethernet interface:

- STMI2 (Q2316-X)
- STMI2 (Q2316-X10)
- STMI4 (Q2324-X500)
- STMI4 (Q2324-X510)
- STMIX (Q2343-X)
- STMIY (Q2361-X)
- vHG 3500 with OpenScape 4000 SoftGate

IMPORTANT: Starting with V10R0 the support for STMI2 will not be offered anymore. The replacement for STMI2 is STMIX/ STMIY.

IMPORTANT: To simplify matters, the following document only refers to the STMI board. This term will be used generically for all suitable boards. The term “HFA port“ is used in the following to describe an IP port to which all IP system telephones can be connected.

21.3 optiPoint IP Terminals

21.3.1 General Information

You can connect additional terminals to an optiPoint IP telephone using the appropriate adapters that must be attached to or are already integrated in the telephone:

- The USB adapter (OPTIUSB) is already integrated as a hardware module in most optiPoint 410 telephones.
- Every optiPoint 410 is assigned “control adapter“ functionality during configuration so that a PC can be connected as a simple dialer using the USB adapter.

You can connect up to two key modules to an optiPoint 410 IP telephone. These must be specified with the **REP** parameter. You can configure other key modules but they won’t work.

IMPORTANT: Analog terminals require the optiPoint to be fed locally via a plug-in power supply. Country- and transmission-specific settings are made centrally using the `AMO ZAND:TYPE=OPTISET,TAABCTID=<string>`.

21.3.2 optiPoint 410/420

21.3.2.1 Terminal Types

There are a number of different optiPoint 410 telephone types that only differ on the basis of their functional scope and expansion capabilities. The following table provides an overview:

optiPoint telephone types	No. of function keys	Display *) lit	No. of adapter slots	Poss. no. of key modules	USB 1.1 *) master	Headset port
optiPoint 410 entry	8	No	0	0	No	No
optiPoint 410 economy	12	Yes	0	0	No	No
optiPoint 410 standard	12	Yes *)	2	2	Yes	Yes
optiPoint 410 advance	19	Yes *) 4 lines	1	2	Yes *)	Yes
optiPoint 420 advance (up to 12 characters per label)	18	Yes *) 4 lines	1	2	Yes *)	Yes

All optiPoint 410 models support Power over LAN feeding (Cisco or IEEE 802.3af). A plug-in power supply unit can be used at the same time as Power over LAN.

21.3.2.2 Adapters and key modules

The following optiPoint adapters and add-on devices can be operated at the optiPoint 410 system telephone:

Device type	Function	AMO parameter
optiPoint USB adapter (already integrated in the telephone)	For connecting standard S0 data terminals	OPTIUSB
optiPoint key module	Key module with 15 programmable function keys and 1 SHIFT key	REP
optiPoint 420 key module	Key module with 13 keys with electronic key labeling, 12 of which are programmable (up to 12 characters per label) and 1 SHIFT key	REP
optiPoint signature module	Key module with smart card reader	IDCR
OpenStage Busy Lamp Field	Busy lamp filed with 90 illuminated, programmable keys	OPTIBLF
optiPoint display module	For providing the LDAP/WAP and ENB function, as well as JAVA VM	---
optiPoint recorder adapter	For connecting a second headset or an external recorder	---
optiPoint acoustic adapter	For connecting accessories (such as loudspeakers, microphones, headsets, etc.)	---

If not already available, an OPTIUSB (optiPoint USB adapter) is automatically configured when you set up a functional terminal.

A physical adapter is not necessary because the function, depending on the terminal, is already implemented.

IMPORTANT: The command DISPLAY-SBCSU:STNO=number; displays all configured adapters, that is, both the ones that were explicitly configured and those that were automatically configured.

21.3.2.3 Modules for optiPoint Telephones

- Only one optiPoint signature module is permitted per optiPoint telephone.
- An optiPoint 420 key module must be de-energized before it is connected to an optiPoint 410.
- No specific configuration is necessary in the system for the optiPoint display module.

IMPORTANT: A suitable plug-in power supply must be connected for configuration with the optiPoint acoustic adapter when using the contact.

- You can only connect one optiPoint display module to the optiPoint 410.
- An optiPoint display module should always be directly connected to the optiPoint 410 as the first key module.

21.3.2.4 Key Layout on optiPoint Telephones

The optiPoint 410 advance and the optiPoint 420 advance use different key layouts.

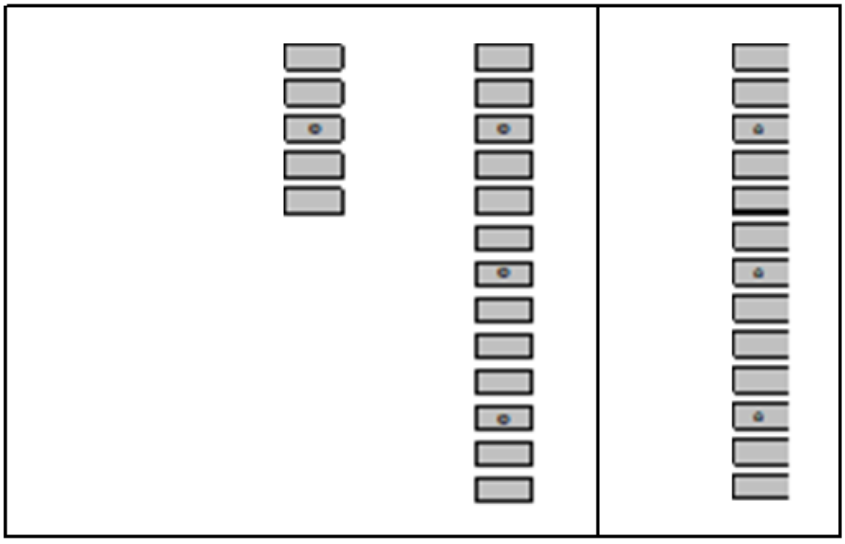


Figure 435: Key layout: optiPoint 420 advance and optiPoint 420 key module

21.3.3 OpenStage WL3/WL4

The OpenStage WL3/WL4 telephone is the enhanced telephone for mobile workplaces that use WLAN technology for transmission. It is interpreted by OpenScape 4000 as SIP phone.

More information on the OpenStage WL3/WL4 may be found on the intranet on E-Doku: http://apps.g-dms.com:8081/techdoc > Product: OpenStage WL3/WL4.

For OpenScape 4000 configuration see Section 8.4, “OpenStage WL3/ WL4 Configuration”.

21.3.4 More Adapters and Ports

21.3.4.1 OpenStage Busy Lamp Field

IMPORTANT: The OpenStage busy lamp field is also supported for optiPoint 410/420 IP.

The **DIGTYP** value **OPTIBLF** has been introduced for the busy lamp field in AMO TAPRO. A layout with this type has to be used for the key layout configuration of an optiPoint device with BLF.

The key configuration is similar as for an OpenStage device with busy lamp field. Not 90 keys are configured on one add-on device but 5 add-on devices each with 18 keys. So each column with 18 keys on the busy lamp field can be thought as one add-on device.

Configuration

A number for the key layout (**SNU=127**) for the **DIGTYP=OPTIBLF** must be configured.

Example:

```
CHANGE-TAPRO:STD=127,DIGTYP=OPTBLF,KY01=CH;
REGEN-TAPRO:TYPE=STD,STD=127;
CHANGE-TAPRO:,127,OPTIBLF ,CH ,FREE ,FREE ,FREE ,FREE ,
FREE ,FREE ,FREE ,FREE ,FREE ,
FREE ,FREE ,FREE ,FREE ,
FREE ,FREE ,FREE ,FREE ,FREE ,
" ";
CHANGE-TAPRO:,127,OPTIB1 ,FREE ,FREE ,FREE ,FREE ,FREE ,
FREE ,FREE ,FREE ,FREE ,FREE ,
FREE ,FREE ,FREE ,FREE ,FREE ,
FREE ,FREE ,FREE ;
CHANGE-TAPRO:,127,OPTIB2 ,FREE ,FREE ,FREE ,FREE ,FREE ,
FREE ,FREE ,FREE ,FREE ,FREE ,
FREE ,FREE ,FREE ,FREE ,FREE ,
FREE ,FREE ,FREE ,FREE ,FREE ,
FREE ,FREE ,FREE ;
CHANGE-TAPRO:,127,OPTIB3 ,FREE ,FREE ,FREE ,FREE ,FREE ,
FREE ,FREE ,FREE ,FREE ,FREE ,
FREE ,FREE ,FREE ,FREE ,FREE ,
FREE ,FREE ,FREE ;
CHANGE-TAPRO:,127,OPTIB4 ,FREE ,FREE ,FREE ,FREE ,FREE ,
FREE ,FREE ,FREE ,FREE ,FREE ,
FREE ,FREE ,FREE ,FREE ,FREE ,
FREE ,FREE ,FREE ;
CHANGE-TAPRO:,127,OPTIB5 ,FREE ,FREE ,FREE ,FREE ,FREE ,
FREE ,FREE ,FREE ,FREE ,FREE ,
```

```
FREE ,FREE ,FREE ,FREE ,FREE ,
FREE ,FREE ,FREE ;
AMO-TAPRO-111 PROGRAMMABLE KEY DEFINITION FOR DIGITAL TERMINALS
REGENERATE COMPLETED;
```

Additionally the parameters **REP=0** and **BLF=YES** must be set in AMO SBCSU for the subscriber.

21.3.4.2 optiPoint Recorder Adapter

The recorder adapter lets you connect an analog recording device or a second headset to an existing optiPoint 410 device.

IMPORTANT: This adapter is not configured in the PBX and consequently does not feature a parameter value in the AMO SBCSU display mask.

21.3.4.2.1 Port for Recording Device (Data cannot be modified)

During a call, the RX and TX handset signals are both routed to the jack.

1) Impedance: 6 kOhm

- Frequency range: 300 to 3000 Hz (+/- 3 dB)
- Level: 1.77 Vrms at 600 Ohm

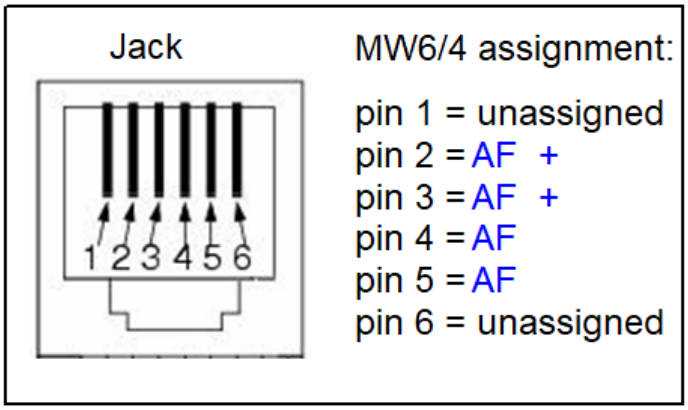


Figure 436: Recorder interface assignment

21.3.4.2.2 Second Headset Port

A second headset can be used as soon as it is connected and uses the same volume setting as the telephone to which the adapter is connected.

The volume cannot be separately set for this port.

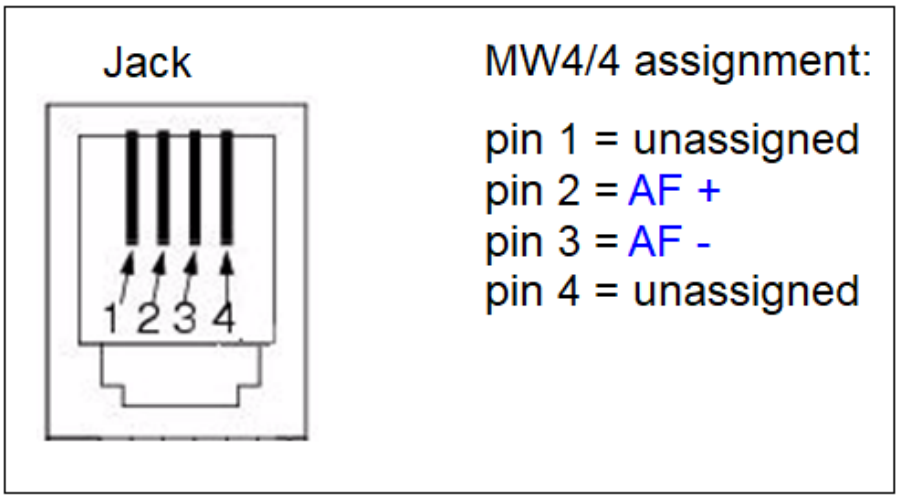


Figure 437: Second headset port assignment

21.3.4.3 optiPoint Acoustic Adapter Data

The acoustic adapter lets you connect an external microphone and speaker as well as a headset (cordless or corded) to an existing optiPoint 410 device. The adapter also features two floating contacts.

IMPORTANT: This adapter is not configured in the PBX and consequently does not feature a parameter value in the AMO SBCSU display mask.

21.3.4.4 Microphone and Loudspeaker Port

You can operate an add-on microphone and an external speaker at this port by using a cable-sharing adapter.

IMPORTANT: Any external devices connected cancel out the corresponding internal devices. No configuration changes are necessary at the PBX.

---

1) The volume can be modified in the same way as for the telephone.

- The external loudspeaker must have a separate amplifier and power supply.

.

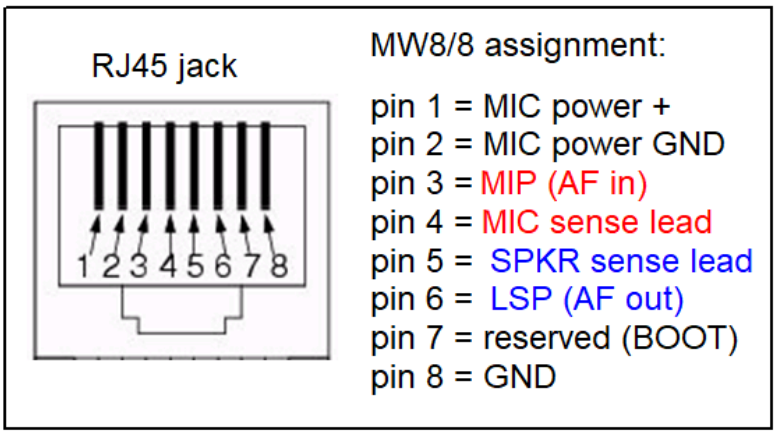


Figure 438: Microphone/loudspeaker port assignment

21.3.4.5 Headset Port

Headsets with and without key as well as wireless or wired units can be operated at this port.

IMPORTANT: If you are using a headset without hardware detection (that is, connection/disconnection is not recognized by the hardware), you must confirm its presence by pressing the HS key (HandSet, assigned with the AMO TAPRO). The parameter HEADSET must be set to NOIND in the AMO SBCSU and HSKEY must be set to correspond to the function.

A headset with a MW4/4 port needs an adapter.

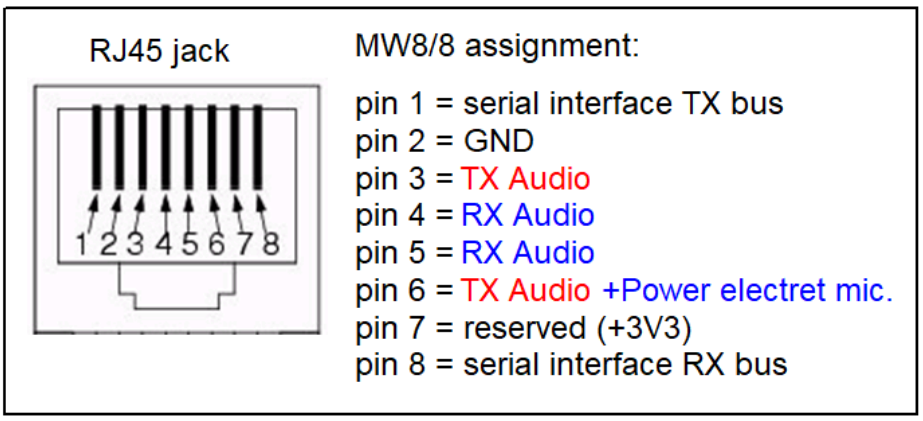


Figure 439: Headset port assignment

21.3.4.6 Contact Port

The “bell“ contact is activated when an alert message is received for the terminal.

The second contact “activity“ can be activated by pressing the keys configured with the AMO TAPRO (BUSYLAMP or DOOROPEN). The contact is closed the first time you press the “BUSYLAMP“ button and re-opened when you press it a second time. (The LED for the associated key is set and then re-set at the same time.)

IMPORTANT: This adapter is not configured in the PBX but must be present so that the door opener and busy lamp field function can be key-operated.

1) The contacts are galvanically isolated from the telephone.

- Load capacity for the AC contacts: 24 V/5 W
- Load capacity for the DC contacts: 60 V/5 W

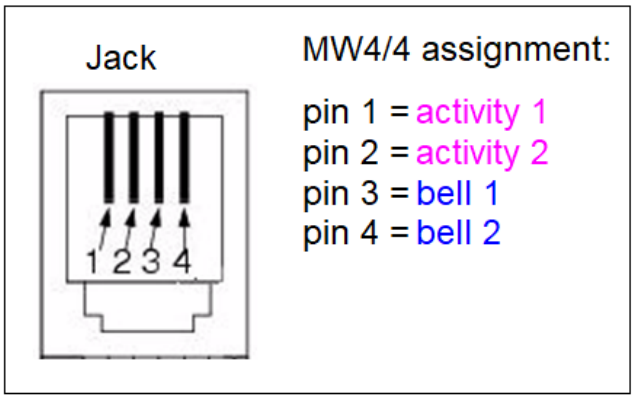


Figure 440: Contact port assignment

IMPORTANT: An external power supply must be available for the bell contact function. (Not necessary if only using a headset or microphone/loudspeaker.)

21.4 OpenStage IP Terminals

The OpenStage family is released for the use at OpenScape 4000. Please refer to the corresponding release notes regarding the released terminal types.

21.4.1 Hardware and General Features

Please refer to the data sheet of the OpenStage terminals (http://apps.g-dms.com:8081/techdoc/en/P31002S2000D101017629/index.htm)

IMPORTANT: There are no adapters for OpenStage telephones.

IMPORTANT: Both key modules, the application modules, the display modules, the busy lamp field and the adapters in the optiPoint series of telephones cannot be deployed or operated together with OpenStage. The only exception is the external power supply (L30250-F600-A190-A191-A192) for the telephones.

21.4.2 Key Assignment

OpenStage telephones have fixed keys. For this reason, the correct standard key layouts must be assigned. The keys 1-8 must correspond to the examples illustrated in Section 8.4, “OpenStage WL3/WL4 Configuration”. The variable keys start from key 9 onwards.

A SHIFT key can also be programmed for the telephone itself.

21.4.3 Key Modules

OpenStage telephones may have up to two key modules. The SHIFT key can be used to switch between two levels.

Device type	Function	AMO parameter
OpenStage key module	Key module with 15 programmable function keys (and 1 SHIFT key)	REP

SHIFT key

When the SHIFT key is pressed on an optiPoint key module, the same action is performed on all other key modules. In other words, the SHIFT level is also activated on the second and fourth key modules.

This is not the case on OpenStage telephones and key modules. In this case, the SHIFT level is only activated on the telephone/key module on which the SHIFT key was pressed.

21.4.4 OpenStage Terminal in Connection with optiClient

The following administration instructions and restrictions are temporarily for the first roll-out of the release 2. An improved handling will be enabled as soon as possible.

- The openStage of type "nn" has to be configured with the fitting standard key layout "openStage nn".
- It is not allowed to change the key assignment for a phone (AMO TAPRO) while the optiClient is active.

- The individual change of key settings by the subscriber must **not** be enabled for the combination optiClient/openStage.
- When the user previously owned the combination optiClient/optiPoint then he/she is to be informed about the new key layout which can be seen in the optiClient application. Reason for this are the fixed key functions at openStage phones.

In case of disregarding the mentioned restrictions the proper key assignment cannot assured when changing from openStage to optiClient and vice versa. This can be repaired only with deleting and configuring the complete connection again.

Configuration of a new optiClient/openStage connection:

New configuration of the openStage phone with the proper standard key layout together with the configuration of the optiClient (OPTIIP&API).

The device "optipoint 420 advance" is to be chosen in the optiClient application.

Replacement of an existing optiClient/optiPoint configuration with optiClient/openStage:

1) Regeneration of the user data
2) Delete the connection completely
3) Note: the deletion is necessary because it is currently the exclusive way to delete the so-called shadow table for key assignments. If it is not cleared correctly, the proper key assignment is not assured neither at the optiClient nor at the openStage. It depends on what had happened at the connection previously (i.e. different phone types were connected etc) if the shadow table has to be cleared.
4) The phone can be exchanged now
5) New configuration of the openStage phone as described above
6) Or the phone can be exchanged now

21.4.5 Busy Lamp Field

Feature Description

The OpenStage Busy lamp field is a key module attached to the side of the phone, that provides 90 illuminated, programmable keys.

Like keys on the phone, these keys can be programmed and used according to your needs.

Service Information

- You can attach one OpenStage Busy lamp field to your OpenStage.
- Only internal destinations can be programmed.

Configuration (Example)

Configuration of the busy lamp field:
`CHANGE-TAPRO:STD=61,DIGTYP=OST30BLF;`

Relevant AMOs

AMO	Parameter	Sprache/ Language	Beschreibung/ Discription
TAPRO	DIGTYP	d	OST30BLF - OpenStage 30 BLF OST40BLF - OpenStage 40 BLF OST60BLF - OpenStage 60 BLF (entkoppelte Freigabe)
	DIGTYP	e	OST30BLF - OpenStage 30 BLF OST40BLF - OpenStage 40 BLF OST60BLF - OpenStage 60 BLF (decoupled release)

21.5 OpenScape Desk Phone IP 35G/55G HFA

The OpenScape Desk Phone IP 35 G HFA and the OpenScape Desk Phone IP 55 G HFA are released for the use at OpenScape 4000 (as of OpenScape 4000 V7 R1).

21.5.1 Hardware and General Features

Please refer to the data sheet of the OpenScape Desk Phone IP 35 G/55G HFA terminals.

21.5.2 Key Assignment

OpenScape Desk Phone IP terminals have fixed keys. For this reason, the correct standard key layouts must be assigned (see Section 8.6, “OpenScape Desk Phone IP Configuration”). The variable keys start from key 9 onwards.

21.5.3 Key Modules

It is **not** possible to connect a key module to the OpenScape Desk Phone IP 35G HFA.

Up to two key modules with electronic labels can be connected to the OpenScape Desk Phone IP 55 G HFA.

Table 89: OpenScape key module 55

Device Type	Function	AMO Parameter
OpenScape Key Module 55	Key module with 12 free programmable function keys (on 2 levels max.)	BEIGER

21.6 OpenScape Desk Phone CP HFA

The OpenScape Desk Phones CP100, OpenScape Desk Phones CP200/205 HFA and the OpenScape Desk Phones CP400/600 HFA are released for the use at OpenScape 4000 (as of OpenScape 4000 V8 R1) and OpenScape Desk Phones CP700/700X as of OpenScape 4000 V10R0.

The OpenScape Desk Phones CP110, OpenScape Desk Phones CP210 HFA and the OpenScape Desk Phones CP410 HFA are released for the use at OpenScape 4000 (as of OpenScape 4000 V8 R2) and OpenScape Desk Phones CP710 as of OpenScape 4000 V10R1.

21.6.1 Hardware and General Features

Please refer to the data sheet of the OpenScape Desk Phone CP100/110/200/210/400/410/600/700/710 HFA terminals.

21.6.2 Key Assignment

OpenScape Desk Phone CP terminals have fixed keys. For this reason, the correct standard key layouts must be assigned (see Section 8.7, “Desk Phones CP Configuration”).

21.6.3 Key Modules

It is **not** possible to connect a key module to the OpenScape Desk Phone CP100/110/200/205/210 HFA.

Up to two key modules with paper labels can be connected to the OpenScape Desk Phone CP 400 HFA.

Up to four key modules with electronic labels can be connected to the OpenScape Desk Phone CP 600 HFA.

Up to two key modules (KM600) with electronic labels can be connected to the OpenScape Desk Phone CP700 HFA.

Up to four key modules (KM600) with electronic labels can be connected to the OpenScape Desk Phone CP700X HFA.

Up to four key modules (KM410) with paper labels can be connected to the OpenScape Desk Phone CP410/CP710 HFA.

Up to four key modules (KM710) with electronic labels can be connected to the OpenScape Desk Phone CP410/CP710 HFA.

Table 90: OpenScape key modules

Device Type	Function	AMO Parameter
OpenScape Key Module KM400	Key module with 16 free programmable function keys (on 2 levels max.)	REP

Device Type	Function	AMO Parameter
OpenScape Key Module KM600	Key module with 12 free programmable function keys (on 2 levels max.)	REP
OpenScape Key Module KM410	Key module with 16 free programmable function keys(on 2 levels max.)	REP
OpenScape Key Module KM710	Key module with 12 free programmable function keys(on 2 levels max.)	REP

21.7 Service Information

- IP terminals must be configured not only in the system but also at the terminal itself.n external
- If SPE is activated at the IP endpoints an external NTP server must be used for time synchronization. For that OpenScape 4000 Assistant **should not be** used. The performance of the hardware/software of the OpenScape 4000 Assistant is not sufficient for this use case.
- A SoftClient is configured like an optiPoint telephone (you can therefore replace an optiPoint IP telephone with a SoftClient).
- LAN port settings should always be made on the telephone to avoid duplex mismatch.
- There is no adapter for OpenStage telephones.
- A host/client configuration is only possible with OpenStage telephones.

21.8 IP Terminal Generation

For detailed information on HiPath Feature Access (HFA), refer to "HiPath Feature Access (HFA)".

Please note that all types of generation require settings to be made at the terminal itself.

The necessary settings to be made include the following network-specific data (this data can also be automatically programmed via DHCP if the telephone is appropriately configured (default factory setting)):

- **Terminal IP Address (STN IP)**
- **Terminal Mask (netmask)**
- **Default Gateway**
- (VLAN ID)

The mandatory system parameters for HFA operation are:

- **PBX Address**
- **Subscriber Number**

21.8.1 HFA (IP) Terminal at STMI

IMPORTANT: For OpenStage 60/80, OpenScape Desk Phone CP600 and OpenScape Desk Phone IP 55. Settings, like volume

or ring type, are not controlled by the system, so values set via AMO ACTDA/AMO KCSU for such devices are not used.

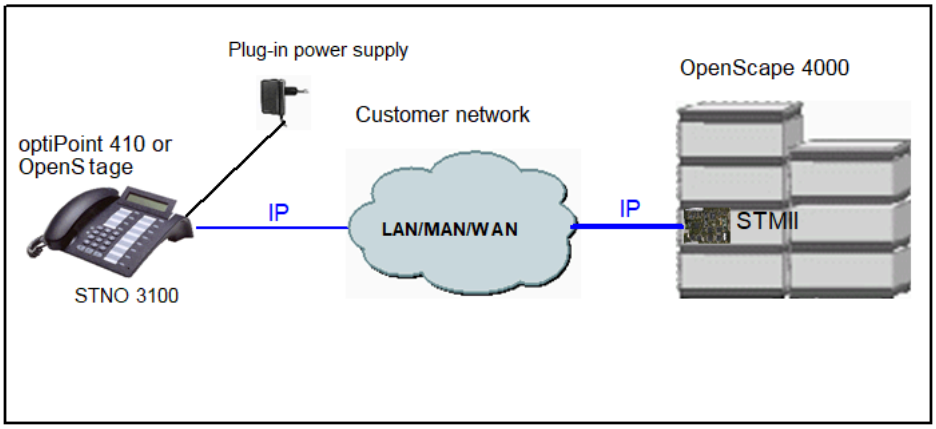


Figure 441: HFA (IP) terminal with plug-in power supply

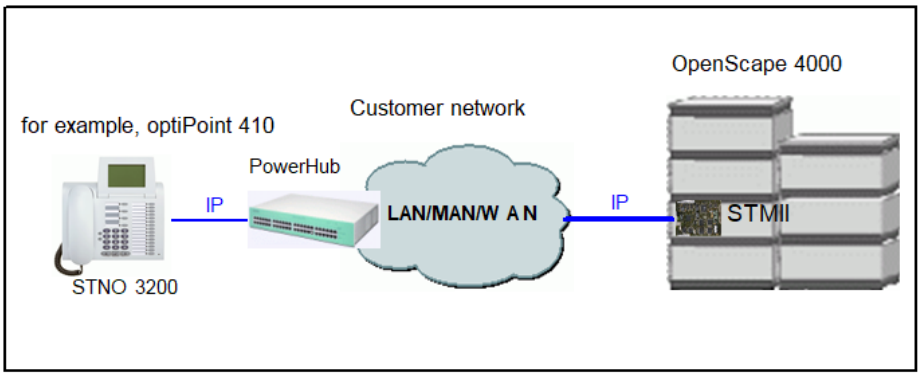


Figure 442: HFA (IP) terminal with PowerHub power supply

To configure a HFA (IP) terminal at the STMI, enter:

ADD-SBCSU:STNO=<number>,**TYPE=OPTI**,**CONN=IP2**,PEN=<ltg-ltu-slot-cct>,
DVCFIG=OPTIIP,COS1=<number>,COS2=<number>,LCOSV1=<number>,
LCOSV2=<number>,LCOSD1=<number>,LCOSD2=<number>,ITR=<number>,
DPLN=0,STD=<number>,**[IPPASSW=<Password>]**,**HEADSET=WITHIND**;

IMPORTANT: For OpenStage and Desk Phone IP: HEADSET=WITHIND must be configured to get the correct display message in case the headset key is pressed and no headset is connected.

21.8.2 PC after HFA (IP) Terminal

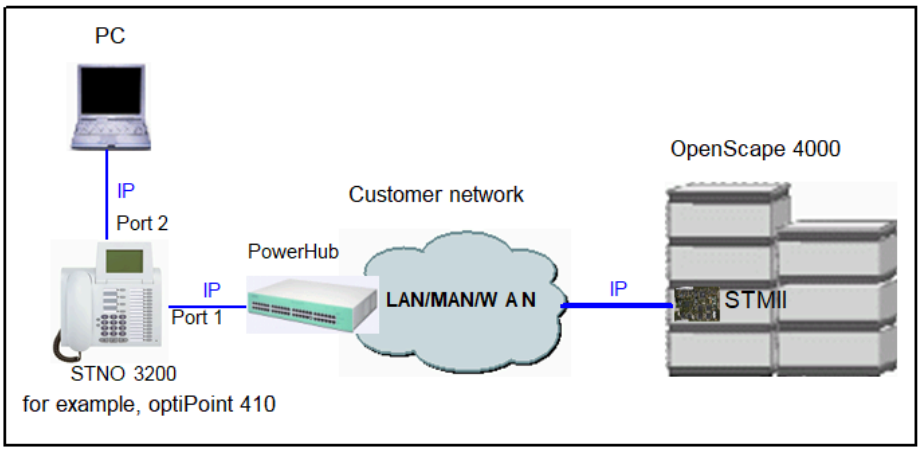


Figure 443: PC and HFA terminal with “single wire to the desk“

To configure an IP telephone at the STMI, enter:

ADD-SBCSU:STNO=<number>,**TYPE=OPTI**,**CONN=IP2**,PEN=<ltg-ltu-slot-cct>,
DVCFIG=OPTIIP,COS1=<number>,COS2=<number>,LCOSV1=<number>,
LCOSV2=<number>,LCOSD1=<number>,LCOSD2=<number>,ITR=<number>,
DPLN=0,STD=<number>,**[IPPASSW=<Password>]**;

IMPORTANT: For OpenStage and Desk Phone IP: HEADSET=WITHIND must be configured to get the correct display message in case the headset key is pressed and no headset is connected.

No special OpenScape 4000 configuration is necessary for the PC. You only have to coordinate the port settings on the telephone with those on the PC network card.

IMPORTANT: You cannot connect a PC without 802.1p/q to an optiPoint 410 where 802.1p/q is active. The 802.1p/q settings should be activated at the telephone and in the AMO, as well as in the LAN components.

21.8.3 HFA (IP) Terminal and USB for Simple Dialer

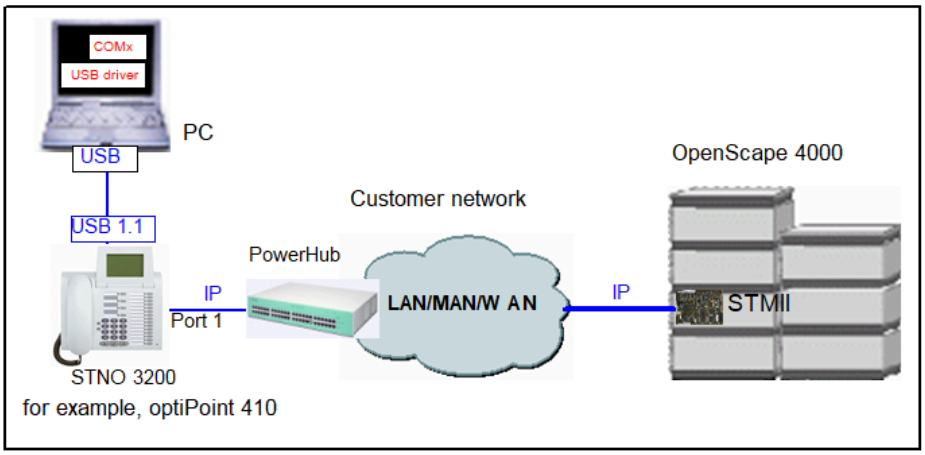


Figure 444: HFA terminal and USB for Simple Dialer

To configure a HFA (IP) terminal at the STMI, enter:

```
ADD-SBCSU:STNO=<number>,TYPE=OPTI,CONN=IP2,PEN=<ltg-ltu-slot-cct>,
DVCFIG=OPTIIP,COS1=<number>,COS2=<number>,LCOSV1=<number>,
LCOSV2=<number>,LCOSD1=<number>,LCOSD2=<number>,ITR=<number>,
 DPLN=0,STD=<number>,[IPPASSW=<Password>];
```

IMPORTANT: For OpenStage and Desk Phone IP: HEADSET=WITHIND must be configured to get the correct display message in case the headset key is pressed and no headset is connected.

No other configuration steps are necessary.

21.8.4 OpenStage WL3/WL4 Configuration

Device configuration

OpenStage WL3/WL4 must be configured as UFIP SIP devices:

```
ADD-SBCSU:STNO=44511,OPT=OPTI,CONN=IP2,PEN=1-99-5-6,DVCFIG=UFIP,
TSI=1,COS1=310,COS2=310,LCOSV1=1,LCOSV2=1,LCOSD1=1,LCOSD2=1,DPLN=0,ITR=0,
SSTNO=N,COSX=0,SPDI=0,IDCR=N,STD=0,INS=Y,ALARMNO=0,RCBKB=N,RCBKNA=N,
CBKBMAX=5,HEADSET=N,HSKEY=NORMAL,CBKNAMB=Y,TEXTSEL=ENGLISH,HMUSIC=0,COMGRP=0;
```

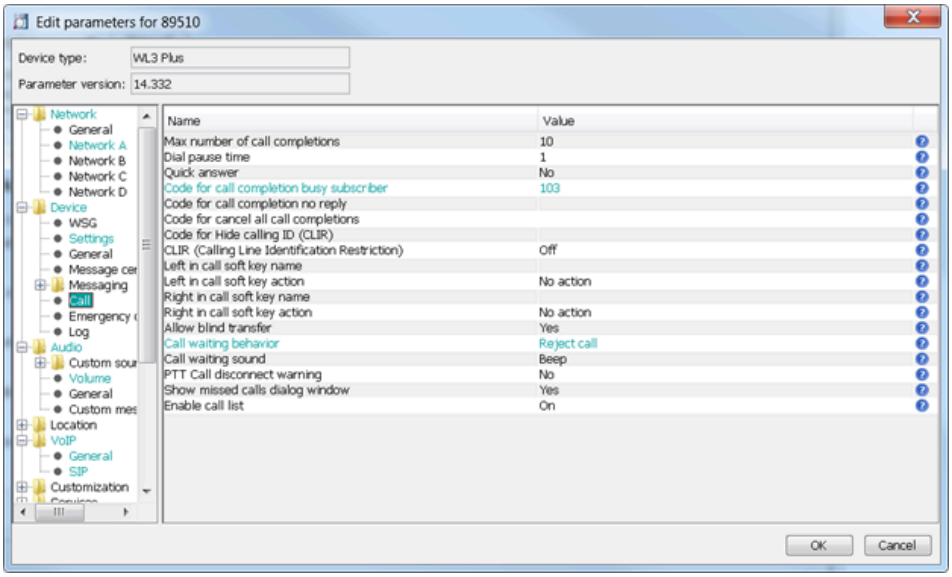
CHANGE-SDAT:STNO=44510,TYPE=ATTRIBUT,AATTR=MBCHL;

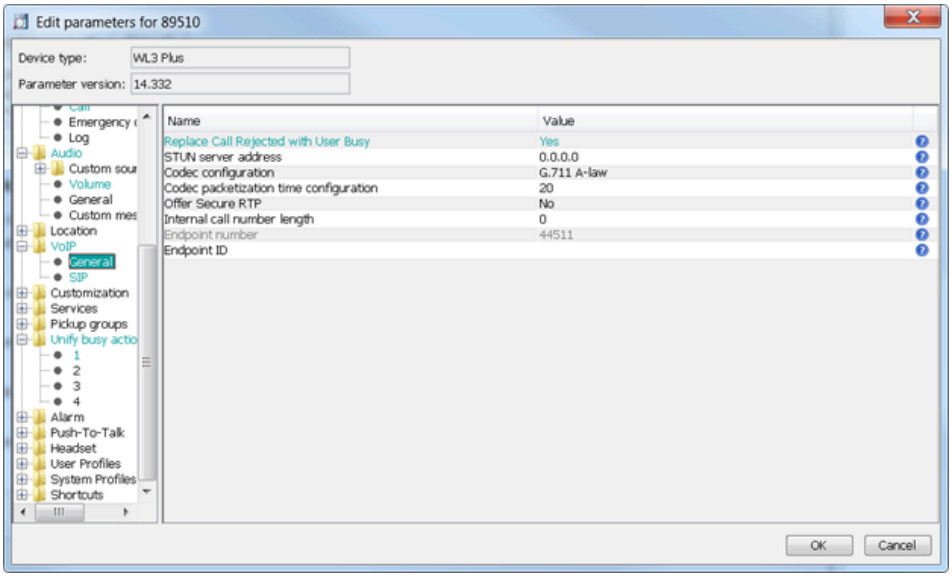
NOTICE: WL3/WL4 Central Speed Dialing for OpenScape4000 is supported.

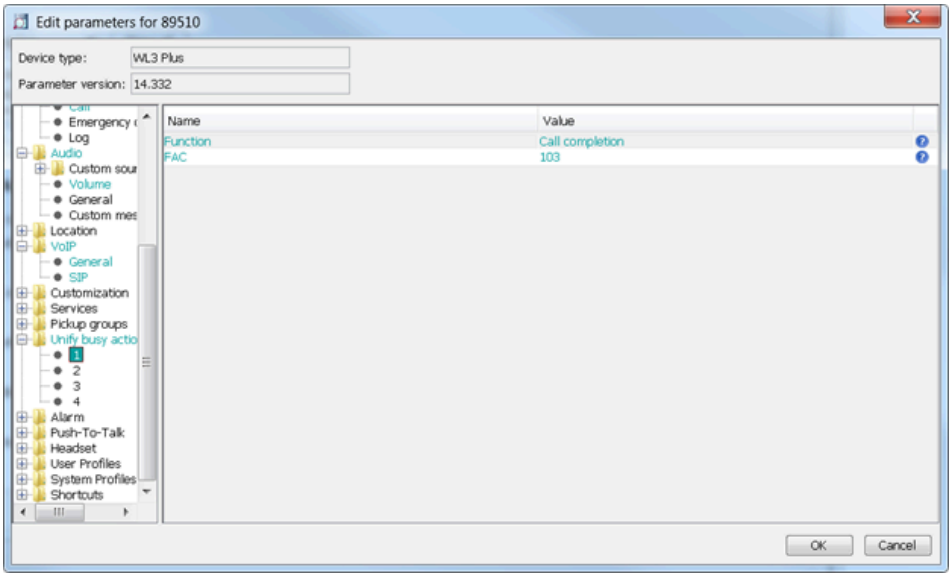
To be able to use the Callback on Busy feature with WL3/WL4 please check if WABE has an existing CBKKY DAR configured. If not you can add it with:

```
ADD-WABE:CD=103,DAR=CBKKY,CHECK=N;
```

This WABE feature access code must be configured for WL3/WL4 stations via known methods (see WL3/WL4 documentation). Find below WL3 screenshots as example:







21.8.5 OpenStage Configuration

An OpenStage HFA terminal will be configured as described in Section 8.1, “HFA (IP) Terminal at STMI”.

Key assignment

A standard key layout is predefined in AMO TAPRO in each case for OS15/ OS20/ OS40/ OS60/ OS80 HFA.

Table 91: Standard key layout for OS15/ OS20/ OS40/ OS60/ OS80 HFA

OpenStage	Key layout (STD in AMO TAPRO)
OpenStage 15	60
OpenStage 20	55
OpenStage 40	56
OpenStage 60	57
OpenStage 80	58

Sample standard key layouts for the various OpenStage variants:

```
DIS-TAPRO:TYPE=STD,STD=55&56&57&58&60;
H500:  AMO TAPRO STARTED
+-----+---------+-------------------------------------------------------------+
| STD | DIGTYP  | "SERVICE INFORMATION"           KEY LAYOUT                  |
+-----+---------+-------------------------------------------------------------+
|  55 | OPENST20| "OPENSTAGE - OS20                                    "      |
|     |         |  1 SPKR-FIX  2 FIX       3 MUTE-FIX   4 SNR-FIX   5 FWD-FIX  |
|     |         |  6 RLS-FIX   7 CH-FIX    8 MB-FIX                           |
|     + - - - - + - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -+
|     | OPTIA1  |  1 VACANT    2 VACANT    3 VACANT     4 VACANT    5 VACANT   |
|     |         |  6 VACANT    7 VACANT    8 VACANT     9 VACANT   10 VACANT   |
|     |         | 11 VACANT   12 VACANT                                        |
```

```
|     + - - - - + - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -+
|     | OPTIA2  |  1 VACANT    2 VACANT    3 VACANT     4 VACANT    5 VACANT   |
|     |         |  6 VACANT    7 VACANT    8 VACANT     9 VACANT   10 VACANT   |
|     |         | 11 VACANT   12 VACANT                                         |
|     + - - - - + - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -+
|     | OPTIA3  |  1 VACANT    2 VACANT    3 VACANT     4 VACANT    5 VACANT   |
|     |         |  6 VACANT    7 VACANT    8 VACANT     9 VACANT   10 VACANT   |
|     |         | 11 VACANT   12 VACANT                                         |
|     + - - - - + - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -+
|     | OPTIA4  |  1 VACANT    2 VACANT    3 VACANT     4 VACANT    5 VACANT   |
|     |         |  6 VACANT    7 VACANT    8 VACANT     9 VACANT   10 VACANT   |
|     |         | 11 VACANT   12 VACANT                                         |
+-----+---------+---------------------------------------------------------------+
|  56 | OPENST40| "OPENSTAGE - OS40                                          "  |
|     |         |  1 SPKR-FIX  2 HS-FIX    3 MUTE-FIX   4 SNR-FIX    5 FWD-FIX |
|     |         |  6 RLS-FIX   7 CH-FIX    8 MB-FIX     9 VACANT    10 VACANT  |
|     |         | 11 VACANT   12 VACANT   13 VACANT    14 VACANT               |
|     + - - - - + - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -+
|     | OPTIA1  |  1 VACANT    2 VACANT    3 VACANT     4 VACANT     5 VACANT  |
|     |         |  6 VACANT    7 VACANT    8 VACANT     9 VACANT    10 VACANT  |
|     |         | 11 VACANT   12 VACANT   13 VACANT    14 VACANT    15 VACANT  |
|     |         | 16 VACANT   17 VACANT   18 VACANT                             |
|     + - - - - + - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -+
|     | OPTIA2  |  1 VACANT    2 VACANT    3 VACANT     4 VACANT     5 VACANT  |
|     |         |  6 VACANT    7 VACANT    8 VACANT     9 VACANT    10 VACANT  |
|     |         | 11 VACANT   12 VACANT                                         |
|     + - - - - + - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -+
|     | OPTIA3  |  1 VACANT    2 VACANT    3 VACANT     4 VACANT     5 VACANT  |
|     |         |  6 VACANT    7 VACANT    8 VACANT     9 VACANT    10 VACANT  |
|     |         | 11 VACANT   12 VACANT                                         |
|     + - - - - + - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -+
|     | OPTIA4  |  1 VACANT    2 VACANT    3 VACANT     4 VACANT     5 VACANT  |
|     |         |  6 VACANT    7 VACANT    8 VACANT     9 VACANT    10 VACANT  |
|     |         | 11 VACANT   12 VACANT                                         |
+-----+---------+---------------------------------------------------------------+
|  57 | OPENST60| "OPENSTAGE - OS60                                          "  |
|     |         |  1 SPKR-FIX  2 HS-FIX    3 MUTE-FIX   4 FIX        5 FWD-FIX |
|     |         |  6 RLS-FIX   7 CH-FIX    8 MB-FIX     9 VACANT    10 VACANT  |
|     |         | 11 VACANT   12 VACANT   13 VACANT    14 VACANT    15 VACANT  |
|     |         | 16 VACANT                                                     |
|     + - - - - + - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -+
|     | OPTIA1  |  1 VACANT    2 VACANT    3 VACANT     4 VACANT     5 VACANT  |
|     |         |  6 VACANT    7 VACANT    8 VACANT     9 VACANT    10 VACANT  |
|     |         | 11 VACANT   12 VACANT                                         |
|     + - - - - + - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -+
|     | OPTIA2  |  1 VACANT    2 VACANT    3 VACANT     4 VACANT     5 VACANT  |
|     |         |  6 VACANT    7 VACANT    8 VACANT     9 VACANT    10 VACANT  |
|     |         | 11 VACANT   12 VACANT                                         |
|     + - - - - + - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -+
|     | OPTIA3  |  1 VACANT    2 VACANT    3 VACANT     4 VACANT     5 VACANT  |
|     |         |  6 VACANT    7 VACANT    8 VACANT     9 VACANT    10 VACANT  |
|     |         | 11 VACANT   12 VACANT                                         |
|     + - - - - + - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -+
|     | OPTIA4  |  1 VACANT    2 VACANT    3 VACANT     4 VACANT     5 VACANT  |
|     |         |  6 VACANT    7 VACANT    8 VACANT     9 VACANT    10 VACANT  |
|     |         | 11 VACANT   12 VACANT                                         |
```

```
+-----+---------+-------------------------------------------------------------+
|  58 | OPENST80| "OPENSTAGE - OS80                                    "      |
|     |         |  1 SPKR-FIX  2 HS-FIX    3 MUTE-FIX   4 FIX        5 FWD-FIX |
|     |         |  6 RLS-FIX   7 CH-FIX    8 MB-FIX     9 VACANT    10 VACANT  |
|     |         | 11 VACANT   12 VACANT   13 VACANT    14 VACANT    15 VACANT  |
|     |         | 16 VACANT   17 VACANT                                        |
|     + - - - - + - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -+
|     | OPTIA1  |  1 VACANT    2 VACANT    3 VACANT     4 VACANT     5 VACANT  |
|     |         |  6 VACANT    7 VACANT    8 VACANT     9 VACANT    10 VACANT  |
|     |         | 11 VACANT   12 VACANT                                        |
|     + - - - - + - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -+
|     | OPTIA2  |  1 VACANT    2 VACANT    3 VACANT     4 VACANT     5 VACANT  |
|     |         |  6 VACANT    7 VACANT    8 VACANT     9 VACANT    10 VACANT  |
|     |         | 11 VACANT   12 VACANT                                        |
|     + - - - - + - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -+
|     | OPTIA3  |  1 VACANT    2 VACANT    3 VACANT     4 VACANT     5 VACANT  |
|     |         |  6 VACANT    7 VACANT    8 VACANT     9 VACANT    10 VACANT  |
|     |         | 11 VACANT   12 VACANT                                        |
|     + - - - - + - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -+
|     | OPTIA4  |  1 VACANT    2 VACANT    3 VACANT     4 VACANT     5 VACANT  |
|     |         |  6 VACANT    7 VACANT    8 VACANT     9 VACANT    10 VACANT  |
|     |         | 11 VACANT   12 VACANT                                        |
+-----+---------+-------------------------------------------------------------+
|  60 | OPENST15| "OPENSTAGE 15                                        "      |
|     |         |  1 SPKR-FIX   2 FIX       3 FIX        4 FIX        5 FIX    |
|     |         |  6 FIX        7 CH-FIX    8 MB-FIX     9 NAME      10 NAME   |
|     |         | 11 NAME      12 VACANT   13 VACANT    14 VACANT    15 VACANT |
|     |         | 16 VACANT                                                    |
|     + - - - - + - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -+
|     | OPTIA1  |  1 LINE       2 LINE      3 LINE       4 LINE       5 LINE   |
|     |         |  6 LINE       7 LINE      8 LINE       9 LINE      10 LINE   |
|     |         | 11 LINE      12 LINE     13 LINE      14 LINE      15 LINE   |
|     |         | 16 LINE      17 LINE     18 LINE                             |
|     + - - - - + - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -+
|     | OPTIA2  |  1 VACANT     2 VACANT    3 VACANT     4 VACANT     5 VACANT |
|     |         |  6 VACANT     7 VACANT    8 VACANT     9 VACANT    10 VACANT |
|     |         | 11 VACANT    12 VACANT                                       |
|     + - - - - + - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -+
|     | OPTIA3  |  1 VACANT     2 VACANT    3 VACANT     4 VACANT     5 VACANT |
|     |         |  6 VACANT     7 VACANT    8 VACANT     9 VACANT    10 VACANT |
|     |         | 11 VACANT    12 VACANT                                       |
|     + - - - - + - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -+
|     | OPTIA4  |  1 VACANT     2 VACANT    3 VACANT     4 VACANT     5 VACANT |
|     |         |  6 VACANT     7 VACANT    8 VACANT     9 VACANT    10 VACANT |
|     |         | 11 VACANT    12 VACANT                                       |
+-----+---------+-------------------------------------------------------------+
```

SHIFT key

A SHIFT key can also be configured on OpenStage terminals (previously this was only possible on key modules). This is achieved with the AMO TAPRO or via the Service menu on the terminal.

CHANGE-TAPRO:STNO=<station number>,KYxx=SHIFT;

IMPORTANT: xx must be greater than 08 since the first 8 keys are fixed. Only key 9 and onwards can be freely assigned.

21.8.6 OpenScape Desk Phone IP Configuration

An OpenScape Desk Phone IP terminal will be configured as described in Section 8.1, “HFA (IP) Terminal at STMI”.

Key Assignment

A standard key layout is predefined in AMO TAPRO in each case for OpenScape Desk Phone IP 35 G/55G HFA.

Table 92: Key layout for OpenScape Desk Phone IP 35 G/55G HFA

Desk Phone	Key layout (STD in AMO TAPRO)
OpenScape Desk Phone IP 35 G HFA	62
OpenScape Desk Phone IP 55 G HFA	63

The values **DPIP35** and **DPIP55** also apply in AMO TAPRO for the DIGTYP parameter.

- OpenScape Desk Phone IP 35 G HFA
- The OpenScape Desk Phone IP 35 G HFA has three freely programmable keys (9,10,11), which are preassigned by default in the standard key layout with the functions **Release**, **Redial** and **Call List**.
- OpenScape Desk Phone IP 55 G HFA
- The OpenScape Desk Phone IP 55 G HFA has eight freely programmable keys (9 - 16) with electronic key labeling. In addition, the terminal has four keys below the display, the so-called softkeys, which can be used to select the respective menu options in the bottom row of the display.

IMPORTANT: The key functions of the softkeys as well as the Phone, Call Log and Directory keys are only assigned in the (local) terminal and therefore cannot be either administered or queried via AMO.

21.8.7 Desk Phones CP Configuration

A CP100/ CP110/ CP200/ CP210/ CP400/ CP410/ CP600/ CP700/ CP700X/ CP710 HFA terminal will be configured as described in Chapter 8, “HFA (IP) Terminal at STMI”.

Key assignment

A standard key layout is predefined in AMO TAPRO in each case for CP100/ CP110/ CP200/ CP210/ CP400/ CP410/ CP600/ CP700/CP710 HFA.

CP410 standard key layout should be used for OpenScape Desk Phone CP410 or CP710 with KM410 (Key module with 16 free programmable function keys) connected.

CP700 standard key layout should be used for OpenScape Desk Phone CP410 or CP710 with KM710 (Key module with 12 free programmable function keys) connected.

Desk Phone CP	Key layout (STD in AMO TAPRO)
OpenScape Desk Phone CP100	112
OpenScape Desk Phone CP200	109
OpenScape Desk Phone CP400	110
OpenScape Desk Phone CP600	111
OpenScape Desk Phone CP700/ CP710/CP410 (with KM710)	113
OpenScape Desk Phone CP110	114
OpenScape Desk Phone CP410/ CP710 (with KM410)	115

Sample standard key layouts for CP100 variant:

```
<DISPLAY-TAPRO:TYPE=STD,STD=112;
DISPLAY-TAPRO:TYPE=STD,STD=112;
H500:  AMO TAPRO STARTED
+-----+---------+-------------------------------------------------------------+
| STD | DIGTYP  | "SERVICE INFORMATION"          KEY LAYOUT                   |
+-----+---------+-------------------------------------------------------------+
| 112 | CP100   |  "DESKPHONE CP100                                      "    |
|     |         |   1 SPKR-FIX  2 FIX       3 MUTE-FIX  4 FIX       5 FIX     |
|     |         |   6 FIX       7 CH-FIX    8 MB-FIX    9 VACANT   10 VACANT  |
|     |         |  11 VACANT                                                  |
|     + - - - - + - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -+
|     | OPTIA1  |   1 VACANT    2 VACANT    3 VACANT    4 VACANT    5 VACANT  |
|     |         |   6 VACANT    7 VACANT    8 VACANT    9 VACANT   10 VACANT  |
|     |         |  11 VACANT   12 VACANT                                      |
|     + - - - - + - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -+
|     | OPTIA2  |   1 VACANT    2 VACANT    3 VACANT    4 VACANT    5 VACANT  |
|     |         |   6 VACANT    7 VACANT    8 VACANT    9 VACANT   10 VACANT  |
|     |         |  11 VACANT   12 VACANT                                      |
|     + - - - - + - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -+
|     | OPTIA3  |   1 VACANT    2 VACANT    3 VACANT    4 VACANT    5 VACANT  |
|     |         |   6 VACANT    7 VACANT    8 VACANT    9 VACANT   10 VACANT  |
|     |         |  11 VACANT   12 VACANT                                      |
|     + - - - - + - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -+
|     | OPTIA4  |   1 VACANT    2 VACANT    3 VACANT    4 VACANT    5 VACANT  |
|     |         |   6 VACANT    7 VACANT    8 VACANT    9 VACANT   10 VACANT  |
|     |         |  11 VACANT   12 VACANT                                      |
+-----+---------+-------------------------------------------------------------+
AMO-TAPRO-111       PROGRAMMABLE KEY DEFINITION FOR DIGITAL TERMINALS
DISPLAY COMPLETED;
```

Sample standard key layouts for CP200 variant:

```
 <DIS-TAPRO:STD,109;
DIS-TAPRO:STD,109;
H500:  AMO TAPRO STARTED
+-----+---------+-----------------------------------------------------------+
| STD | DIGTYP  | "SERVICE INFORMATION"          KEY LAYOUT                 |
+-----+---------+-----------------------------------------------------------+
| 109 | CP200   |  "DESKPHONE CP200                                    "    |
|     |         |   1 SPKR-FIX  2 HS-FIX    3 MUTE-FIX  4 TRNS-FIX  5 HOLD-FIX |
|     |         |   6 CONF-FIX  7 CH-FIX    8 MB-FIX    9 CALLOG   10 VACANT   |
|     |         |  11 FWD      12 LNR                                       |
|     + - - - - + - - - - - - - - - - - - - - - - - - - - - - - - - - - - -+
|     | OPTIA1  |   1 VACANT    2 VACANT    3 VACANT    4 VACANT    5 VACANT   |
|     |         |   6 VACANT    7 VACANT    8 VACANT    9 VACANT   10 VACANT   |
|     |         |  11 VACANT   12 VACANT                                     |
|     + - - - - + - - - - - - - - - - - - - - - - - - - - - - - - - - - - -+
|     | OPTIA2  |   1 VACANT    2 VACANT    3 VACANT    4 VACANT    5 VACANT   |
|     |         |   6 VACANT    7 VACANT    8 VACANT    9 VACANT   10 VACANT   |
|     |         |  11 VACANT   12 VACANT                                     |
|     + - - - - + - - - - - - - - - - - - - - - - - - - - - - - - - - - - -+
|     | OPTIA3  |   1 VACANT    2 VACANT    3 VACANT    4 VACANT    5 VACANT   |
|     |         |   6 VACANT    7 VACANT    8 VACANT    9 VACANT   10 VACANT   |
|     |         |  11 VACANT   12 VACANT                                     |
|     + - - - - + - - - - - - - - - - - - - - - - - - - - - - - - - - - - -+
|     | OPTIA4  |   1 VACANT    2 VACANT    3 VACANT    4 VACANT    5 VACANT   |
|     |         |   6 VACANT    7 VACANT    8 VACANT    9 VACANT   10 VACANT   |
|     |         |  11 VACANT   12 VACANT                                     |
+-----+---------+-----------------------------------------------------------+
AMO-TAPRO-111       PROGRAMMABLE KEY DEFINITION FOR DIGITAL TERMINALS
DISPLAY COMPLETED;
```

Sample standard key layouts for CP400/ CP600 variants:

```
 <DIS-TAPRO:TYPE=STD,STD=110&&111;
DIS-TAPRO:TYPE=STD,STD=110&&111;
H500:  AMO TAPRO STARTED
+-----+---------+-----------------------------------------------------------+
| STD | DIGTYP  | "SERVICE INFORMATION"          KEY LAYOUT                 |
+-----+---------+-----------------------------------------------------------+
| 110 | CP400   |  "                                                   "    |
|     |         |   1 SPKR-FIX  2 HS-FIX    3 MUTE-FIX  4 FIX       5 FIX      |
|     |         |   6 FIX       7 CH-FIX    8 FIX       9 VACANT   10 VACANT   |
|     |         |  11 VACANT   12 VACANT   13 VACANT   14 VACANT   15 VACANT   |
|     |         |  16 VACANT   17 FIX      18 FIX      19 FWD-FIX  20 FIX      |
|     |         |  21 FIX      22 FIX      23 FIX      24 FIX      25 VACANT   |
|     |         |  26 VACANT   27 VACANT   28 VACANT   29 VACANT   30 VACANT   |
|     |         |  31 VACANT   32 VACANT                                     |
|     + - - - - + - - - - - - - - - - - - - - - - - - - - - - - - - - - - -+
|     | OPTIA1  |   1 VACANT    2 VACANT    3 VACANT    4 VACANT    5 VACANT   |
|     |         |   6 VACANT    7 VACANT    8 VACANT    9 VACANT   10 VACANT   |
|     |         |  11 VACANT   12 VACANT   13 VACANT   14 VACANT   15 VACANT   |
|     |         |  16 VACANT                                                 |
|     + - - - - + - - - - - - - - - - - - - - - - - - - - - - - - - - - - -+
|     | OPTIA2  |   1 VACANT    2 VACANT    3 VACANT    4 VACANT    5 VACANT   |
|     |         |   6 VACANT    7 VACANT    8 VACANT    9 VACANT   10 VACANT   |
|     |         |  11 VACANT   12 VACANT   13 VACANT   14 VACANT   15 VACANT   |
|     |         |  16 VACANT                                                 |
```

```
|     + - - - - + - - - -
```

```
|     |         |   6 VACANT    7 VACANT    8 VACANT    9 VACANT   10 VACANT    |
|     |         |  11 VACANT   12 VACANT                                         |
|     + - - - - + - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -+
|     | OPTIA2  |   1 VACANT    2 VACANT    3 VACANT    4 VACANT    5 VACANT    |
|     |         |   6 VACANT    7 VACANT    8 VACANT    9 VACANT   10 VACANT    |
|     |         |  11 VACANT   12 VACANT                                         |
|     + - - - - + - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -+
|     | OPTIA3  |   1 VACANT    2 VACANT    3 VACANT    4 VACANT    5 VACANT    |
|     |         |   6 VACANT    7 VACANT    8 VACANT    9 VACANT   10 VACANT    |
|     |         |  11 VACANT   12 VACANT                                         |
|     + - - - - + - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -+
|     | OPTIA4  |   1 VACANT    2 VACANT    3 VACANT    4 VACANT    5 VACANT    |
|     |         |   6 VACANT    7 VACANT    8 VACANT    9 VACANT   10 VACANT    |
|     |         |  11 VACANT   12 VACANT                                         |
+-----+---------+----------------------------------------------------------------+
AMO-TAPRO-111       PROGRAMMABLE KEY DEFINITION FOR DIGITAL TERMINALS
DISPLAY COMPLETED;
```

Sample standard key layouts for CP110 variant:

```
DISP-TAPRO:STD,114;
H500:  AMO TAPRO STARTED
+-----+---------+----------------------------------------------------------------+
| STD | DIGTYP  | "SERVICE INFORMATION"          KEY LAYOUT                      |
+-----+---------+----------------------------------------------------------------+
| 114 | CP110   |  "DESKPHONE CP110                                          "   |
|     |         |   1 SPKR-FIX  2 HS-FIX    3 MUTE-FIX  4 FIX       5 FIX      |
|     |         |   6 FIX       7 CH-FIX    8 MB-FIX    9 VACANT   10 VACANT   |
|     |         |  11 VACANT                                                     |
|     + - - - - + - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -+
|     | OPTIA1  |   1 VACANT    2 VACANT    3 VACANT    4 VACANT    5 VACANT   |
|     |         |   6 VACANT    7 VACANT    8 VACANT    9 VACANT   10 VACANT   |
|     |         |  11 VACANT   12 VACANT                                         |
|     + - - - - + - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -+
|     | OPTIA2  |   1 VACANT    2 VACANT    3 VACANT    4 VACANT    5 VACANT   |
|     |         |   6 VACANT    7 VACANT    8 VACANT    9 VACANT   10 VACANT   |
|     |         |  11 VACANT   12 VACANT                                         |
|     + - - - - + - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -+
|     | OPTIA3  |   1 VACANT    2 VACANT    3 VACANT    4 VACANT    5 VACANT   |
|     |         |   6 VACANT    7 VACANT    8 VACANT    9 VACANT   10 VACANT   |
|     |         |  11 VACANT   12 VACANT                                         |
|     + - - - - + - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -+
|     | OPTIA4  |   1 VACANT    2 VACANT    3 VACANT    4 VACANT    5 VACANT   |
|     |         |   6 VACANT    7 VACANT    8 VACANT    9 VACANT   10 VACANT   |
|     |         |  11 VACANT   12 VACANT                                         |
+-----+---------+----------------------------------------------------------------+

AMO-TAPRO-111       PROGRAMMABLE KEY DEFINITION FOR DIGITAL TERMINALS
DISPLAY COMPLETED;
```

Sample standard key layouts for CP410 variant:

```
DISP-TAPRO:STD,115;
H500:  AMO TAPRO STARTED
+-----+---------+----------------------------------------------------------------+
| STD | DIGTYP  | "SERVICE INFORMATION"          KEY LAYOUT                      |
+-----+---------+----------------------------------------------------------------+
| 115 | CP410   |  "DESKPHONE CP410                                          "   |
|     |         |   1 SPKR-FIX  2 HS-FIX    3 MUTE-FIX  4 TRNS-FIX  5 HOLD-FIX |
```

```
|     |         |   6 CONF-FIX  7 CH-FIX    8 MB-FIX    9 VACANT   10 VACANT   |
|     |         |  11 VACANT   12 VACANT   13 VACANT   14 VACANT   15 VACANT   |
|     |         |  16 VACANT   17 FIX      18 FIX      19 FWD-FIX  20 FIX      |
|     |         |  21 FIX      22 FIX      23 FIX      24 FIX      25 VACANT   |
|     |         |  26 VACANT   27 VACANT   28 VACANT   29 VACANT   30 VACANT   |
|     |         |  31 VACANT   32 VACANT                                       |
|     + - - - - + - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -+
|     | OPTIA1  |   1 VACANT    2 VACANT    3 VACANT    4 VACANT    5 VACANT   |
|     |         |   6 VACANT    7 VACANT    8 VACANT    9 VACANT   10 VACANT   |
|     |         |  11 VACANT   12 VACANT   13 VACANT   14 VACANT   15 VACANT   |
|     |         |  16 VACANT                                                   |
|     + - - - - + - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -+
|     | OPTIA2  |   1 VACANT    2 VACANT    3 VACANT    4 VACANT    5 VACANT   |
|     |         |   6 VACANT    7 VACANT    8 VACANT    9 VACANT   10 VACANT   |
|     |         |  11 VACANT   12 VACANT   13 VACANT   14 VACANT   15 VACANT   |
|     |         |  16 VACANT                                                   |
|     + - - - - + - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -+
|     | OPTIA3  |   1 VACANT    2 VACANT    3 VACANT    4 VACANT    5 VACANT   |
|     |         |   6 VACANT    7 VACANT    8 VACANT    9 VACANT   10 VACANT   |
|     |         |  11 VACANT   12 VACANT   13 VACANT   14 VACANT   15 VACANT   |
|     |         |  16 VACANT                                                   |
|     + - - - - + - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -+
|     | OPTIA4  |   1 VACANT    2 VACANT    3 VACANT    4 VACANT    5 VACANT   |
|     |         |   6 VACANT    7 VACANT    8 VACANT    9 VACANT   10 VACANT   |
|     |         |  11 VACANT   12 VACANT   13 VACANT   14 VACANT   15 VACANT   |
|     |         |  16 VACANT                                                   |
+-----+---------+--------------------------------------------------------------+

AMO-TAPRO-111       PROGRAMMABLE KEY DEFINITION FOR DIGITAL TERMINALS
DISPLAY COMPLETED;
```

The values CP100, CP110, CP200, CP400, CP410, CP600, and CP700 also apply in AMO TAPRO for the DIGTYP parameter.

- OpenScape Desk Phone CP100/CP110 HFA

  The OpenScape Desk Phone CP100, CP110 have three programmable function keys (9,10,11) which can be re-programed with different functions or phone numbers at any time.
- OpenScape Desk Phone CP200/ CP210 HFA

  The OpenScape Desk Phone CP200, CP210 HFA has four freely programmable keys (9,10,11,12), which are preassigned by default in the standard key layout with the functions **Call log**, **Not assigned**, **Forwarding key** and **Last number redial**.
- OpenScape Desk Phone CP400

  The OpenScape Desk Phone C400 HFA has sixteen freely programmable keys (9 - 16 and 25 - 32). In addition, the terminal has four keys on the right side of the display, called softkeys, which can be used to select the respective menu options in the bottom row of the display.
- OpenScape Desk Phone CP600/ CP410

  The OpenScape Desk Phone C600, CP410 HFA has sixteen freely programmable keys (9 - 16 and 25 - 32) with electronic key labeling. In addition, the terminal has five keys on the right side of the display, called softkeys, which can be used to select the respective menu options in the bottom row of the display.

- OpenScape Desk Phone CP700/ CP710

  The OpenScape Desk Phone C700, CP710 HFA has sixteen freely programmable keys (9 - 16 and 25 - 32) with electronic key labeling.

  In addition, the terminal has 12 free programmable keys with LED called softkeys. The first 6 programmable keys are permanently displayed on the left panel. The last 6 programmable keys are available in Favorites.

  IMPORTANT: The key functions of the softkeys are only assigned in the (local) terminal and therefore cannot be either administered or queried via AMO.

  NOTICE: The OpenScape Desk Phone CP700/CP700X includes the REDIAL KEY, which can be configured through WBM.

Key values

The logical key values for Keymodules are the following.

	MAIN DEVICE	DSS1	DSS2	DSS3	DSS4
Layer 1	1 - 32	33-48	49-64	65-80	81-96
Layer 2	180-211	97-112	113-128	129-144	145-160

NOTICE: Even if the AMO is prepared for 4 additional keymodules, only CP600 phone supports 4 add-ons. CP400 phone supports 2 add-ons.

CP410 and CP710 phones support 4 key modules (KM410 or KM710).

21.9 Deletion at the IP Port

21.9.1 Deleting All Devices Assigned a Station Number at the IP Port

To delete all devices that are assigned a station number, enter (the optional OFFTYPE parameter with its default setting DC=“deactivate with camp-on“ takes over the mandatory task of disabling the terminals prior to deletion; this would otherwise be performed with the AMO DSSU):
`DEL-SBCSU:STNO=number,SVC=ALL[,OFFTYPE=DI];`

IMPORTANT: You can only delete the device with the main station number if there are no other devices configured under a secondary station number.

21.9.2 Deleting Non-Voice Services at the IP Port

To delete individual NV services at the IP port, enter (the optional OFFTYPE parameter with its settings DC="deactivate with camp-on" and DI="deactivate immediately" takes over the mandatory task of disabling all terminals prior to deletion and enabling the remaining terminals again afterwards; this would otherwise be performed with the AMO DSSU):

```
DEL-SBCSU:STNO=number,SVC=param [,OFFTYPE=DI];
```

IMPORTANT: If you used OFFTYPE=NL (no lock) to delete an NV service, then you must use DSSU to put the remaining terminals back into operation (in particular the voice terminal as this was not deleted).

21.9.3 Deleting the IP Telephone's Key Module

To delete all key modules assigned to a telephone, proceed as follows:

```
CHANGE-SBCSU:STNO=number,OPT=OPTI,REP=0;
```

21.9.4 Deleting the IP Telephone's Buy Lamp Field

```
CHANGE-SBCSU:STNO=number,OPT=OPTI,BLF=NO;
```

21.9.5 Deleting IP Telephone Adapters

IMPORTANT: This section only applies to optiPoint and optiClient terminals.

- You cannot delete the optiPoint USB adapter with an AMO command; it is automatically deleted at the same time as the last (functional) S0 device at the IP port.

Glossary

A

attended call transfer

A is the initiator of the call transfer. A is in a call with B and puts B on hold. Then A sets up a consultation call to C and initiates the transfer. After the transfer, B and C are connected.

B

blind call transfer

A is the initiator of the call transfer. A is in a call with B. A puts B on hold. Then A sets up a consultation call to C and transfers the call before the consultation call is connected. After the transfer, B and C are connected.

C

CLIP

CLIP - Calling Line Identification Presentation - The number of the calling party is displayed at the called party.

CLIR

CLIR - Calling Line Identification Restriction - The number of the calling party is suppressed at the called party.

CNIP

CNIP - Calling Name Identification Presentation - The name of the calling party is displayed at the called party.

CNIR

CNIR - Calling Name Identification Restriction - The name of the calling party is suppressed at the called party.

CNOP

CNOP - Connected Name Identification Presentation - The name of the connected party is displayed at the called party.

CNOR

CNOR - Connected Name Identification Restriction - The name of the connected party is suppressed at the called party.

COLP

COLP - Connected Line Identification Presentation - The number of the called party is displayed at the calling party.

COLR

COLR - Connected Line Identification Restriction - The number of the called party is suppressed at the calling party.

CSTA/ACL monitoring

CSTA/ACL monitoring provides the device status of SIP subscribers for BLF WIN applications (Busy Lamp Field) or other presence-based applications.

D

DMZ

The name is derived from the term "demilitarized zone", an area between nation states in which military action is not permitted.

In computer security, a DMZ (sometimes referred to as a perimeter networking) is a physical or logical subnetwork that contains and exposes an organization's external services to a larger untrusted network, usually the Internet. The purpose of a DMZ is to add an additional layer of security to an organization's local area network (LAN). An external attacker only has access to equipment in the DMZ, rather than any other part of the network.

I

Inbound proxy

Server name / IP address of the trunking partner from which the data is sent to the OpenScape 4000.

IP Hop

An IP Hop means Encoding and Decoding one time.

M

MediaRelay

MediaRelay is a Media proxy of the Media server in the OpenScape 4000 SoftGate that is controlled via the signaling software of the HG 3500.

O

Outbound proxy

Server name/IP address to which all outgoing messages/data are sent as first node/hop (e.g. session boarder controller).

P

Proxy

Server name / IP address of the server of the partner to which calls are routed.

T

T.38

T.38 is an ITU standard for sending fax messages accross IP networks in a real-time mode.

Abbreviations

ACC	Access Point Connection Control
AP	Access Point
APE	Access Point Emergency
BRI	Basic Rate Interface (ISDN S0)
CGW	Common Gateway, e.g. HG 3500
CLA	Customer License Agent
CLM	Customer License Manager
CO	Central Office (Deutsche Telekom)
DLS	Deployment and License Server
DMC	Direct Media Connection (VoIP)
E2E	End-to-End
ERH	Endpoint Registration Handler
HFA	HiPath Feature Access
HSR	HiPath Signaling Router
HW	Hardware
ICMP	Internet Control Message Protocol
IMP	IPDA Media Proxy
IPDA	IP Distributed Architecture
ISDN	Integrated Services Digital Network
JRE	Java Runtime Environment
LS	Local Survivability
LW	Loadware
MEK	Master Encryption Key
MXGW	Mediatrix Gateway
MTU	Maximum Transmission Unit
NAT	Network Address Translation
PBX	Private Branch Exchange
PEP	Proprietary Encryption Protocol (for IPDA signaling)
PSTN	Public Switching TDM Network

PXE	Preboot eXecution Environment
QDC	Quality of Service Data Collection
QoS	Quality of Service
SBC	Session Border Controller
SIP	Session Initiation Protocol
SPE	Signaling and Payload Encryption
SRSR	Small Remote Side Redundancy
SRTP	Secure Real Time Protocol
SSA	Session Initiation Protocol
TLS	Transport Layer Security
VoIP	Voice over IP
WBM	Web-Based Management

Index

A

Access point 524, 535, 545, 545, 548, 551, 663
Access Point Emergency 694
Access point parameters
  changing 545
Activating the SPE feature 1101
announcements per access point 635
AP Emergency 694
  Acceptance of AP Emergency configuration 727
  Administration switchover of access points 722
  Administration switchover of OpenScape 4000 SoftGates 722
  Allocating access points to a survivability unit 698
  Application support in emergency mode 703
  Configuration 703
  Configuration data 700
  configure access point 712
  configure Backup & Restore on CC-AP 734
  configure Backup & Restore on Survivable OpenScape 4000 SoftGate 734
  configure CC-AP 704
  configure emergency group 707
  configure OpenScape 4000 SoftGate 712
  configure Survivable OpenScape 4000 SoftGate 704
  Connection between subsystems (islands) 701
  Connection data 720
  delete CC-AP 706
  delete emergency group 711
  delete entire AP Emergency configuration 717
  Display on terminal 717
  FAQs - Frequently Asked Questions 753
  Feature description 694
  Information for network administrators 739
  Licensing 702
  modify CC-AP 704
  modify emergency group 707
  modify Survivable OpenScape 4000 SoftGate 704
  Normal operation 700
  OpenScape 4000 Backup & Restore 727
  OpenScape 4000 in customer LAN 703
  Quick guide 741
  removing access points 716
  Scenarios 694
  Software update 701, 701, 701
  Spreadsheets-configuration 737
  Startup
    CC-AP 726
    Survivable OpenScape 4000 SoftGate 727
  Survivability Unit in AP 3700 IP 698
  Survivability Unit on OpenScape 4000 SoftGate 698
  Switchover delay 718
  Switchover in emergency mode 699
  Switchover to normal operation 700
  Time synchronization 491, 702
  Time synchronization between host system and CC-AP 726
  Time synchronization between host system and Survivable OpenScape 4000 SoftGate 726
  verify AP Emergency configuration 727
APE 694
Architecture 38
Average data delay (ms) (parameter) 36
Average voice delay (ms) (parameter) 36

B

Bandwidth Requirements 45

C

Call scenarios 492
Changing the login and password for WBM/CLI 178
Circuit switching 491
CLI HG 3500 172
CLI HG3500
  access control 173
  DLS 176
  gateway setup 174
  general operations 173
  handling images/file 174
  maintenance 174
  SSL 176
CMI 626
Codec standards 26
Command Line Interface CLI in HG 3500 172
Configuring an access point 524

D

Data connections (Mediatrix 44xx) 279
Default security level 1087
Delay and Echo 37
Deleting All Devices Assigned a Station Number at the IP Port 1238
Deleting an access point 545
Deleting IP Telephone Adapters 1239
Deleting NV Services at the IP Port 1239
Deleting the IP Telephone's Key Module 1239
Deletion 1238
Different announcements per access point 501
Different MFV dial tone receiver per access point 501
Different Time Zones 756
Different Time Zones (DTZ) 500, 756
Different tones per access point 501
Direct link access point 535
Distributing certificates with DLS 1118

DMC 48
HFA phone at another OpenScape 4000 1186
HFA phone at HiPath 3000 1188
HFA station on OpenScape 4000 1186
SIP phone at another OpenScape 4000 1184, 1185
SIP phone at HiPath 3000 1186
SIP station on OpenScape 4000 1184
TDM phone at another OpenScape 4000 connected via H323 trunking 1190
TDM phone at another OpenScape 4000 (remote shelf) 1189
TDM phone at HiPath 3000 1192
DTMF dial tone receivers per access point 635
DTMF Outband Signaling 1054

E

Encoding 45
Example
Two HFA subscriber at different systems 479
Two HFA subscribers in the same Host 478
External Music on Hold 622

F

F8290 - Start of net weakness (statistical data concerning message runtime (round trip delay)) 590
F8290 - Start of net weakness (statistical data concerning message throughput 591
FAQs - Frequently Asked Questions 686
Fax transmission and detection 25
Fax/Modem over IP 25
Feature description 489
Feature Description 1067
Feature description Mobility session 469
FMoIP 25

G

Gatekeeper Function 413
Gatekeeper Restrictions 414
Gateways HG 3500 and HG 3575 23
General Information 413
Generation Mobility session 478
Goal of this document 22
Guidelines for Installing an IP Feature 414

H

H323 / H323 Annex connectivity 1054
H323 connectivity
Overview 1054
HG 3500 23
HG 3500 V4
DLS client bootstrapping 92
HG 3575 23, 551, 554
HG3500 65
HiPath Feature Access
Standby Board HG 3500 76
HiPath Feature Access (HFA) 447

I

Information for Network Administrators 678
Information on exchanging 3575 HG boards 554
Information on the 19“ AP 3500 IP Access Point 555
Information on the 19“ AP 3700 IP Access Point 556
IP address changes 626
IP Distributed Architecture (IPDA) 489
IP Overhead 46
IP ports 242
IP Terminal Generation 1224
IP Terminals 1211
IP trunk configuration for SPE 1090
IPDA 489, 1103
IPDA configuration 502
IPDA-Different Time Zones
Assigning the Time Classes to an AP Shelf 760
Assigning the Time Classes to an HFA Station 761
Changing the System Date/Time with AMO DATE 763
Configuring the Time Classes 759
Deleting a Time Class 761
Deleting the Daylight Savings Time Changeover 762
Feature Description 756
Generation Example 757
Relevant AMOs 763
Service Information 757
ISDN S0 data (Mediatrix 44xx) 279

J

Jitter buffer type (parameter) 36

K

Key Layout on optiPoint Telephones 1214
Key words 23

L

Large Enterprise Gatekeeper (LEGK) 413
LEGK 413
Link status display 898, 1062
Load Balancing 355
Load calculation 645
load concept 65
Loading new loadware on a HG 3575 551
Local Access Point Administration at CLI via Terminal 663
Local Configuration of an access point 548

M

Master Encryption Key 1104
Maximum data delay (ms) (parameter) 36

Maximum voice delay (ms) (parameter) 36, 36
Mediatrix 1204 gateway 303
Mediatrix 41xx gateway 296
Mediatrix 44xx gateway
scenario 264, 270, 280
Mediatrix 44xx gateway (data) 279
Mediatrix 44xx gateway voice 264, 270
Mediatrix gateways - configuration notes 263
MEK 1104
Mobile HFA Logon 469
Mobility session 469
Modem transmission and detection 25
Modules for optiPoint Telephones 1214
MOH 318
Multisite emergency calls 888
Music on hold 622
Music on Hold 318

N

Native SIP
codecs 833
Relevant AMOs 898, 1062
Network administrators 678
Network data 39
Network Requirements 38
Networked access point 525

O

OpenScape 4000 Assistant
delete IPGW 903, 1065
modify board data of IPGW 903, 1065
OpenScape 4000 SoftGate 253
OpenStage IP Terminals 1219
optiPoint Acoustic Adapter Data 1217
optiPoint IP Terminals 1211
optiPoint Recorder Adapter Data 1216
Overview 253, 413, 447

P

Packet loss/delay preference (parameter) 36
Payload - DMC authorization 1176
Payload - Domains 1177
Payload - Feature activation while DMC is active 1176
Payload - Feature Description 1166, 1166
Payload - Features with DMC 1175
Payload - Generation 1176
Payload - H.323 stack on IPDA boards 1178
Payload - Maximum number of DMC connections on IP boards 1177
Payload - Relevant AMOs 1179
Payload - Service Information 1175
Payload - Voice Activity Detection (VAD) 1177
Payload Survivability
Display problems on VNR systems 609
Power Requirements 38
Prerequisites 38
Protocol 242

R

Reference clock in access point 551
Requirements 1087
Resource Management 64
Runtime and noticeable effects 37

S

Sampling Time 45
Security 63
Service Information 1224
Service information Mobility session 475
Services 242
Shared Desk Area 471
Signaling and payload encryption (SPE) 1067
Signaling and payload encryption (SPE) configuration 1086
Signaling and Payload Separation 497
Signaling and Payload Separation (SPS) 609
Signaling survivability 581, 766
SIP Carrier 847
SIP connectivity
Boards used 803
Overview 798
SIP subscriber communication matrix 798
SIP trunking communication matrix 798
SIP Service Provider 847
SIP Subscriber
change 813
display 818
Enabling/Disabling DMC 813
Registered SIP subscriber 818
Relevant AMOs 821
remove 813
unregistered SIP subscribers 818
SIP-Q
trunking between OpenScape 4000 and OpenScape Voice with SIP-Q V2 904
SoftGate upgrade 259
Source-dependent routing 591
SPE configuration at the IP terminal 1099
SPE:external gateway configuration 1091
Special routes 569
Spreadsheets - IPDA configuration 669
Subscriber gateway (Mediatrix 44xx) 283
System capacity 491
System Requirements 38

T

Terms 23
tones per access point 635
Traffic Considerations 53

Trunking gateway (Mediatrix 44xx) 280

U

User interface Mobility session 473

V

VAD 48, 61
Voice Activity Detection (VAD) 48
Voice Quality 27

© 2025 Mitel Networks Corporation. All Rights Reserved. Mitel and the Mitel logo are trademark(s) of Mitel Networks Corporation. Unify and associated marks are trademarks of Unify Software and Solutions GmbH & Co. KG. All other trademarks herein are the property of their respective owners.