Separating Telephony and Administration Flows

09/2019

AMT/PTD/PBX/0101/4/0/EN

OPERATING MANUAL

Notice

CONTENTS

1 FOREWARD

1.1 TERMINOLOGY

1.1.1 TERMS AND EXPRESSIONS

Mitel 5000 Gateways	This term refers to all XS, XL and XD PBXs
MiVoice 5000 or MiVoice 5000 Server	Telephone switching system hosted on a PC running with Linux Redhat
XS, XL, XD	MiVoice 5000 series physical gateways
XS	This term includes XS, XS12 and XS6 systems
Mitel 500	This term includes Mitel 500, A500x and A50x systems
Mitel MiVoice 5000 Manager or M7450	Systems management centre

1.1.2 ABBREVIATIONS AND TERMINOLOGY

Web Admin	Mitel 5000 Contact Center
DHCP	Dynamic Host Configuration Protocol.
FTP	File Transfer Protocol
GSI	Gateway SIP
https	Hypertext Transfer Protocol Secure
LDAP	Light Directory Access Protocol
EAI	External Application Interface
IP	Internet Protocol
MOVACS	Multiswitch Original Virtual Addressing Communication System
PBX	Private Branch eXchange
PPP	Point-to-Point Protocol.
RTP	Real Time Protocol
SBC	Session Border Controller
SIP	Session Initiation Protocol
SNMP	Simple Network Management Protocol
TAPI	Telephony Application Programming Interface
TCP	Transport Control Protocol
TLS	Transport Layer Security, previously SSL (secure socket layer)
TMA	Terminal Management Application
TWP	Telephony Web Portal
UCP	Unified Communication Platform
VLAN	Virtual Local Area Network
VTI	Virtual Terminal Interface
XML	eXtended Markup Language

1.2 REFERENCE DOCUMENTS

The information in this manual refers to the following documents:

TITLE	REFERENCE
MITEL 5000 - Installation and Maintenance Manual	**AMT/PTD/PBX/0058/EN**
MiVoice 5000 Web Admin XD – XL – XS – XS12 – XS6– MiVoice 5000 Server – Operating Manual	**AMT/PTD/PBX/0080/EN**
MiVoice 5000 – Multi-site management - Operating manual	**AMT/PTD/PBX/0081/EN**

2 INTRODUCTION

2.1 PRINCIPLE

The purpose of separating telephony flows from administration flows is to enhance security by assigning a dedicated and distinct IP network to each of these flows.

This solution consists in defining two separate IP networks:

- The telephony network to which all the user terminals are connected via the corresponding devices. More generally, this network may be a corporate network.

- The administration network on which the management systems are deployed.

These two networks must be distinct and may consist of several IP subnets.

The architecture is based on the following principles:

- A data flow is identified through the IP addresses of the devices and the protocol used. This protocol is identified through the UDP or TCP ports (see the appendix of this document).

- Each device is connected to one of these networks, except the (Mitel 5000 Gateways or MiVoice 5000 Server) iPBXs which are connected to both networks.

- Other applications such as Mitel OMM, CC, TWP and UCP are only connected to the telephony network since the risk of loss of management data is less than with an iPBX.

- Each network is dedicated to the protocols in question.

- Communication between both networks is via an external firewall which filters data flows.

- The iPBXs can be reached via two IP addresses depending on the protocol used. A firewall integrated into the iPBXs checks the consistency of accesses and protocols.

- Remote accesses via PPP are not concerned by this environment.

The separating flows mode is available from the R5.3 SP2 release. Refer to the document AMT/PTD/PBX/0083/EN.

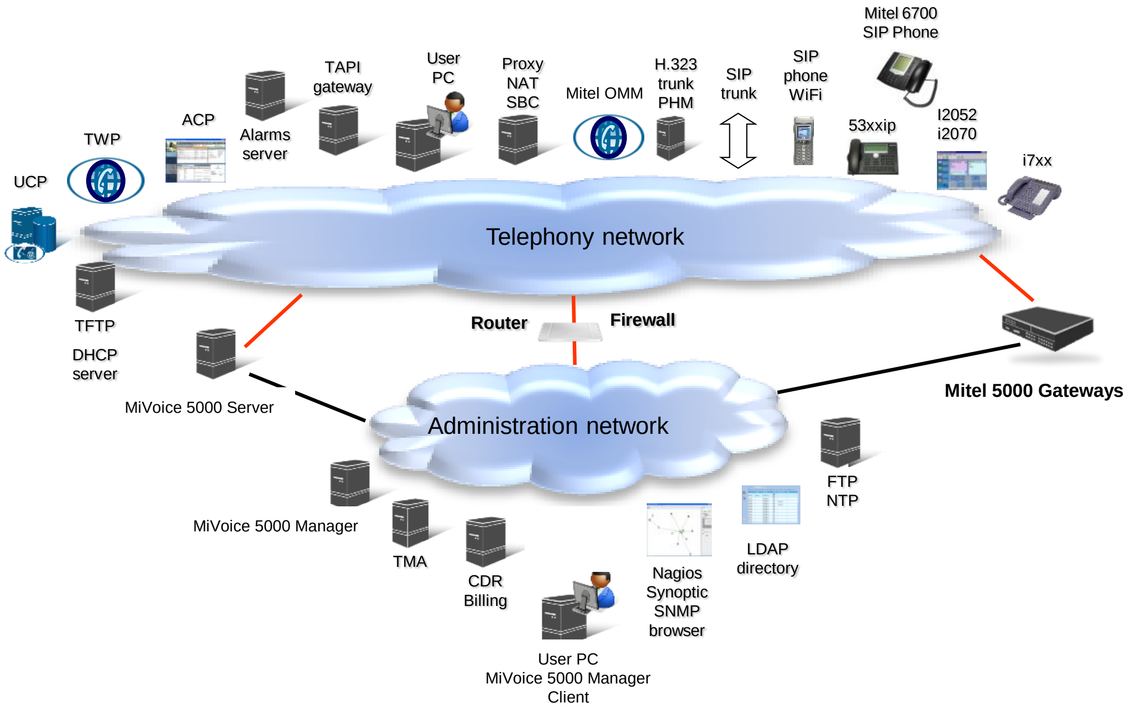
2.2 RULES AND RESTRICTIONS

Regarding the architecture, all iPBXs have to set in separating flows mode.

An external download server must be used in the current environment proposed. This server must be declared for terminal management (TMA).

Therefore, the integrated download server for Mitel 5000 Gateways cannot be used in this environment.

2.3 OVERVIEW OF THE ARCHITECTURE



3 CASE OF A NEW INSTALLATION

3.1 PREREQUISITES

Two distinct networks are working and communicating through a set of router/firewall.

⚠ **WARNING : The integrated download server cannot be used in this environment. An external download server must be declared for terminal management (TMA). Refer to the terminal installation manual - AMT/PTD/TR/0014.**

3.2 MAIN FLOW SEPARATION IMPLEMENTATION PHASES

Connect the different devices to and configure them on their respective networks.

On MiVoice 5000 Manager

Since MiVoice 5000 Manager is connected to the administration network, no particular configuration is required for the flow separation environment.

On Mitel 5000 Gateways or Mitel 500

The different network parameters must be defined using Ctrl + i.

The firewall integrated into Mitel 5000 Gateways is automatically configured at the end of this phase.

On MiVoice 5000 Server

The two network cards work with both networks.

The administration network IP address must be declared from Web Admin.

For information on how to configure the internal firewall, refer to theAppendix.

Note : Concerning AX, Mitel 500 series and MiVoice 5000 server, if the administration network comprises several subnets, define the corresponding paths (see Section 5 - Configuring the IP paths of the admin).

On the router/interconnection firewall

Configure filtering in such a way that the flows underlined in the table in Section 6.

If the administration network comprises several subnets, define the corresponding paths (see **Section 5 - Configuring the IP paths of the admin**).

3.3 CONFIGURING THE IP PARAMETERS OF TELEPHONY AND ADMINISTRATION NETWORKS FOR A FIRST INSTALLATION OF MITEL 5000 GATEWAYS

For a first installation, the flow separation must be configured using Ctrl +i.

Access is provided locally on the COM port of the CPU card, using a NULL MODEM cable (ref.:BHG0024A) connected between the COM port of the CPU card and the COM port of the administration PC.

Procedure

On the PC connected to the COM port

- Open a Hyperterminal window and configure the connection as follows:
- Bits per second: 115200 bits/s
- Data bits: 8
- Parity: none
- Stop bits: 1
- Flow control: none
- Power on the cabinet and follow the start-up progress on the PC.
- Upon display of "Identification starting"
- Press **Ctrl + I**.

The screen then displays the different configuration modes:

```
Configuration mode (F/T/S/P/E)

- F: Factory mode

- T: Total mode

- S: Standard mode

- P: Password reset

- U : USB provisioning mode

- E: for Exit
```

Select "**S**" mode (standard mode) then press "**Return**" to enter the network pre-configuration menu.

The screen then displays the system's default network pre-configuration.

It is from this screen, during a first installation, that the address defined gives access to the iPBX management via Web Admin; access is gained physically via the **LAN** port on the front panel of the CPU card.

If the administration and telephony flows are separated, the address indicated on this screen will be dedicated to the telephony network in association with the one defined for the administration network in the following menu: **ADMINISTRATION NETWORK.**

Concerning the physical accesses, in this case, on the front panel of the CPU card:

- The **LAN** port is dedicated to the telephony network.
- The **ETH2** port is dedicated to the administration network.

```
MITEL 5000 CONFIGURATION / NETWORK

*------------------------------------------------------*



| ENTER IP ADDRESS: 192.168.65.1

| ENTER NETWORK MASK: 255.255.255.0

| ENTER GATEWAY: 192.168.65.254

*--------------------------------------------------*

DO YOU WANT TO CHANGE CONFIGURATION Y(ES)/N(O)? Y
```

Answer "**y**" and validate with the "**Return**" key to access the different fields.

- Enter the network parameters successively, using the **Return** key to change line.

```
MITEL 5000 CONFIGURATION / NETWORK

*------------------------------------------------*

| ENTER IP ADDRESS: 10.100.40.150 |

| ENTER NETWORK MASK: 255.255.255.192 |

| ENTER GATEWAY: 10.100.40.129 |

*------------------------------------------------*
```

After the last line is validated, a summary of the network parameters is displayed for confirmation.

```
MITEL 5000 CONFIGURATION / NETWORK

*------------------------------------------------*

| RESUME |

*------------------------------------------------*

*------------------------------------------------*

| IPADR = 10.100.40.150 |

| NETWORKMASK = 255.255.255.192 |

| GATEWAY = 10.100.40.129 |

| NETWORKADR = 10.100.40.128 |

| BROADCAST = 10.100.40.191 |

*------------------------------------------------*

DO YOU CONFIRM (Y/N)? Y
```

If the summary is not correct:

- Press "**n**" to restart network preconfiguration.

If the summary is correct:

- Press "**y**" then "**Return**", to confirm.

The screen below is used to configure an additional and separate network for administration flows.

```
DO YOU WANT TO CONFIGURE MANAGEMENT IP NETWORK? Y/[N]
```

Note : However, network separation can be configured later from the Web Admin menu SYSTEM>Configuration>Cards>IP card parameters. See Section 4.3

In case of flow separation, press "**y** " then "**Return**", to confirm.

The screen displays the flow separation configuration for the administration network access via the ETH2 connector on the front panel of the CPU card:

```
MITEL 5000 CONFIGURATION / ADMINISTRATION NETWORK

| ENTER ADMIN IP ADDRESS:

| ENTER ADMIN NETWORK MASK: |

| ENTER ADMIN GATEWAY: |

| ENTER ADMIN STATE (0/1):

*-------------------------------------------------*
```

Enter successively the parameters of the administration network, using the Return key to change line.

Concerning the line ENTER ADMIN STATE:

- The option (1) allows flow separation to be activated immediately.
- The option (0) deletes the configuration entered previously.

After the last line is validated, a summary of the network parameters is displayed for confirmation.

```
MITEL 5000 CONFIGURATION / ADMINISTRATION NETWORK

| ADMIN IPADR = 20.100.42.121 |

| ADMIN NETWORKMASK = 255.255.255.192 |

| ADMIN GATEWAY = 20.100.42.65 |

| ADMIN NETWORKADR = 20.100.42.64 |

| ADMIN BRODCAST = 20.100.42.127

DO YOU CONFIRM (Y/N)? Y
```

If the summary is not correct:

- Press "**n**" to restart network preconfiguration.

If the summary is correct:

- Press "**y**" then "**Return**", to confirm.

The following phases are used to complete the installation and do not concern flow separation (See Installation manual AMT/PTD/PBX/0058).

At the end of the configuration process using Ctrl + i, the system restarts.

- Connect the **LAN** port to the telephony network.

- Connect the **ETH2** port to the administration network.

Therefore, Web Admin will be accessible from the URL (https://) defined for administration. The LAN port access no longer allows administration, which is now performed on ETH2.

⚠ **WARNING : If the administration network connection switch does not manage cross-over (negotiation of transmission/reception), a twisted cable must be used between the Mitel 5000 Gateways ou Mitel 500 system and this switch.**

Concerning the firewall integrated into the Mitel 5000 Gateways sytstem

After this configuration using Ctrl + i, the firewall will be automatically configured for the Mitel 5000 Gateways system.

3.4 CONFIGURING THE IP PARAMETERS OF TELEPHONY AND ADMINISTRATION NETWORKS FOR A FIRST INSTALLATION OF MIVOICE 5000 SERVER

3.4.1 PREREQUISITES

The PC hosting the MiVoice 5000 server must have two network accesses (one for the administration network, one for the telephony network).

MiVoice 5000 is installed and accessible via Web Admin.

3.4.2 DEFINING THE IP PARAMETERS OF TELEPHONY AND ADMINISTRATION NETWORKS

From Web Admin, select Menu **SYSTEM>Configuration>Cards>IP board parameters**.

The list of declared IP cards appears (for MiVoice 5000 Server, there is only one line).

- Select line **0-00**.

- On the next screen, tick **Use of an admin network**.

- Then enter the IP address of the telephony network in the **IP address** field on top (options).

- On the line **Use of an admin network**, enter the Admin network IP address (**– IP address**) field.

- Click **Confirmation**.

Note : The configuration of other fields is not specific to flow separation; see Web Admin operating manual (AMT/PTD/PBX/0080).

3.4.3 CONFIGURING THE FIREWALL (IN REDHAT)

A firewall is integrated into Redhat operating system in MiVoice 5000 Server in order to distribute data flows.

This firewall cannot be configured from Web Admin.

The administrator is responsible for configuring the firewall.

Configure the ban on all the accesses using the following command lines:

- **# /sbin/iptables -P INPUT DROP**
- **# /sbin/iptables -P OUTPUT DROP**
- **# /sbin/iptables -P FORWARD DROP**

The authorise, in input, all the source addresses by referring to Section 6.2.

The command line is as follows, based on the example of port 80:

- **# /sbin/iptables -A INPUT -p tcp -i $ETH -s 0/0 --dport 80 -j ACCEPT**

4 FOR AN EXISTING INSTALLATION

4.1 PREREQUISITES

Two distinct networks are working and communicating through a set of router/firewall.

If an internal download server is currently being used, it should no longer be used. It must be replaced by an external download server for managing terminals (TMA). See Terminal installation manual - AMT/PTD/TR/0014.

4.2 MAIN FLOW SEPARATION IMPLEMENTATION PHASES

In this first phase, leave the interconnection firewall transparent.

Move the devices dedicated to the administration of the current telephony network to the administration network.

The addresses must equally be re-assigned (MiVoice 5000 Manager, DHCP, FTP, LDAP directory, etc.).

In this phase, the administration and management of these terminals are unavailable.

On the Mitel 5000 Gateways or Mitel 500 system

Configure flow separation from Web Admin (see Section 4.3-).

On MiVoice 5000 Server

Two network accesses must be operational for both networks.

The administration network IP address must be declared from Web Admin.

For information on how to configure the internal firewall, refer to the appendix.

Note : Concerning Mitel 5000 Gateways, Mitel 500 and MiVoice 5000 server, if the administration network comprises several subnets, define the corresponding paths (see Section 5 - Configuring the IP paths of the admin).

On MiVoice 5000 Manager

Reconfigure the site addresses. See the document AMT/PTD/NMA/0040.

On the router/interconnection firewall

Configure filtering in such a way that the flows underlined in table 5.3 can pass.

If the administration network comprises several subnets, define the corresponding paths (see Section 5).

4.3 CONFIGURING THE IP PARAMETERS OF TELEPHONY AND ADMINISTRATION NETWORKS ON AN EXISTING MITEL 5000 GATEWAYS AND MITEL 500 SYSTEMS

From Web Admin, select Menu **SYSTEM>Configuration>Cards>IP board parameters**.

The list of declared IP cards appears (for MiVoice 5000 Server, there is only one line).

- Select line 0-04.
- On the next screen, tick **Use of an admin network**.
- Then enter the IP address of the telephony network in the **IP address** field on top.
- On the line **Use of an admin network**, enter the Admin network IP address (**– IP address/Mask/router** fields).
- Click **Confirmation**.

Note : The configuration of other fields is not specific to flow separation; see Web Admin operating manual (AMT/PTD/PBX/0080).

Further configuration from Web Admin

- Connect the telephony network to the **LAN** port on the CPU front panel.
- Connect the Admin network to the **ETH2**port on the CPU front panel. This link will give access to Web Admin.

4.4 CONFIGURING THE FIREWALL (IN REDHAT)

A firewall is integrated into Redhat operating system in MiVoice 5000 Server in order to distribute data flows.

This firewall cannot be configured from Web Admin.

The Linux server administrator is responsible for configuring the firewall.

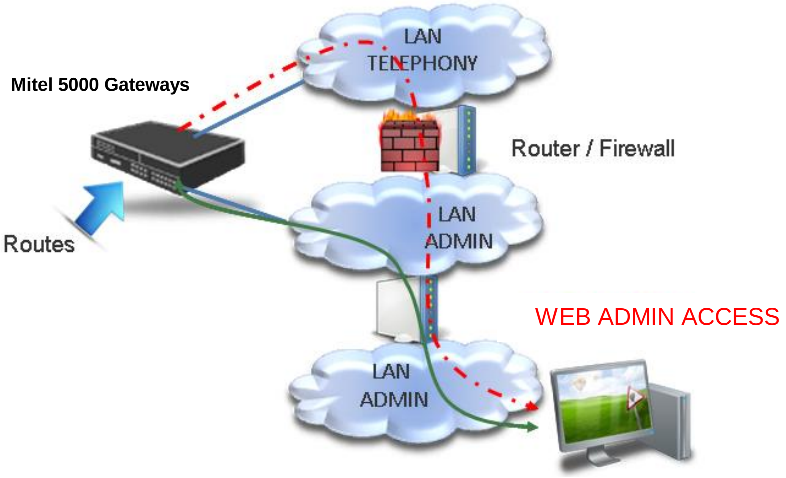
Check that all the necessary ports are open, by referring to Section 6.2.

5 CONFIGURING THE IP PATHS OF THE ADMINISTRATION NETWORK

When the administration network contains several subnets, a client terminal may reach the Mitel 5000 Gateways device on the administration network through different paths (to access Web Admin, for instance).

Therefore, it is necessary to define a path used to reach this client, or else the Mitel 5000 Gateways device may set up a path via the telephony network because it does not know that this subnet address (and default gateway) used is the default gateway of the telephony network.

Note : So, the administration network gateway will always be used during route creation. If the Web Admin, SNMP, EXT DIRECTORY, SYSLOG, DATE&TIME are not located in the same local network, it is necessary to define the paths to reach thes servers.



- The mixed red line corresponds to the default path.
- The green straight line corresponds to the path once configured.

5.1 CONFIGURING PATHS ON AX SERIES SYSTEMS

Menu **SYSTEM>Configuration>Cards>Admin network IP paths**

- This command is not available for MiVoice 5000MiVoice 5000 Server.

PATH X: IP ADDRESS

X: 1 to 120.

This line is used to enter the IP address of the subnet to be reached with this path.

The system checks the syntax and displays the error diagnosis "SYNTAX ERROR" if the value entered is not in the w.x.y.z form, or if 0.0.0.0 or 255.255.255.255 is entered.

The first time an IP address is entered, the associated mask is forced to 255.255.255.0.

When an IP address is deleted, the associated mask is deleted as well.

MASK

This line is only displayed if an IP address has been entered for this path.

This line is used to enter the mask which defines the area to be reached with this path.

The system checks the syntax and displays the error diagnosis "SYNTAX ERROR" if the value entered is not in the w.x.y.z format, or if 0.0.0.0 is entered. Moreover, the MMC checks that the value entered is a subnet mask, that is that the significant bits are contiguous and the important bit is on 1. If this is not the case, or if the mask is deleted, the error report "INCORRECT VALUE" is displayed.

Note : In this menu, the system does not check whether several paths access the same area (case of network inclusion). On the other hand, the system will delete double entries so only the required routes are configured.

Up to 120 routes can be created (IP address and mask).

The changes are saved when the menu is closed.

5.2 CONFIGURING PATHS ON MIVOICE 5000 SERVER

You must be the Linux server administrator.

Administration network routing must be programmed using the following command:

```
# route add -net xxx.xxx.xxx.xxx mask mmm.mmm.mmm gw ggg.gggg.ggg.ggg
```

6 APPENDICES

6.1 DATA FLOW FOR THE MIVOICE 5000 SOLUTION

6.1.1 DATA FLOWS FOR DEVICES CONNECTED TO THE TELEPHONY NETWORK

This table gives a list of data flows in the MiVoice 5000 R5.2 solution and for requests made by some equipment connected to the telephony network.

EQUIPMENT	DEPARTMENT	REMOTE EQUIPMENT	PROTOCOL	NETWORK
i7xx	signalling	PBX/MiVoice 5000 Server (SERVIP)	I over IP (port 3199)	Tel
	configuration	DHCP server	DHCP	Tel
	software download	Download tool	TFTP	Tel
	voice flow	End points	RTP	Tel
Download tool	software download	i7xx	Proprietary (port 9410)	Tel
i2052 or i2070	Signaling i2052	PBX/MiVoice 5000 Server	VTI/XML (port 3199)	Tel
	Signalling i2070	PBX/MiVoice 5000 Server (SERV-POWIN)	Gateway TCP/X.25	Tel
	configuration	PBX/MiVoice 5000 Server (EAI)	Gateway TCP/X.25	Admin
	directory	LDAP directory	LDAP read only	Admin
	date & time	PBX/MiVoice 5000 Server (NTP server)	NTP	Tel
	voice flow (i2052 only)	End points	RTP	Tel
MiVoice 5300 IP Phone	signalling	PBX/MiVoice 5000 Server(GSI or proxy)	extended SIP (18060)	Tel
	software download	FTP server	FTP	Admin
	configuration	DHCP server	DHCP	Tel
	voice flow	End points	RTP	Tel
Mitel 6700 SIP Phone	signalling	PBX/MiVoice 5000 Server(GSI or proxy)	SIP (5060)	Tel
	software download	FTP - TFTP server	FTP – TFTP	Admin and Tel
	configuration	DHCP server	DHCP	Tel
	telephony services	PBX/MiVoice 5000 Server (XML proxy)	Proprietary http / https	Tel
	date & time	PBX/MiVoice 5000 Server (NTP server)	NTP	Tel
	voice flow	End points	RTP	Tel
SIP phone & WiFi	signalling	PBX/MiVoice 5000 Server (GSI)	SIP (5060)	Tel
	voice flow	End points	RTP	Tel

EQUIPMENT	DEPARTMENT	REMOTE EQUIPMENT	PROTOCOL	NETWORK
SIP Trunk	signalling	PBX/MiVoice 5000 Server (GSI)	SIP (5060)	Tel
	voice flow	End points	RTP	Tel
H.323 Trunk	signalling	PHM	H.323 (H.225/H.245)	Tel
	voice flow	End points	RTP	Tel
PHM	PHM - signalling	PBX/MiVoice 5000 Server	TCP/X.25 (port 3208)	Tel
DECT-IP application	Mitel OMM – signalling	PBX/MiVoice 5000 Server (GSI)	Extended SIP	Tel
	Mitel OMM – resiliency	Mitel OMM	proprietary	Tel
	Mitel OMM – directory	LDAP directory	LDAP read only	Admin
	Mitel OMM – terminal list	PBX/MiVoice 5000 Server (Web Admin)	https	Admin
	Mitel RFP – configuration	DHCP server	DHCP	Tel
	Mitel RFP – voice flow	End points	RTP	Tel
NAT SBC PROXY	signalling	PBX/MiVoice 5000 Server (GSI)	Extended SIP (5060& 5064)	Tel
	Mitel RFP – voice flow relay	End points	RTP	Tel
PBX/MiVoice 5000 Server	Multisite signalling	PBX/MiVoice 5000 Server (SERGIC)	Movacs (tunnel 1998)	Tel
	Multisite signalling	PBX/MiVoice 5000 Server (SERGIC)	TLS	Tel
	MiVoice 5000 Server redundancy	MiVoice 5000 Server	Heartbeat	Tel
	PBX redundancy	PBX XD	DRBD	internal
	Test	PBX/MiVoice 5000 Server (AFISER)	TCP/X.25 (port 3302)	Tel
	VOIP voice flow	End points	RTP	Tel
	E-voicemail	Mail server	SMTP/POP3/IMAP4	Tel
	TMA set configuration	Mitel 6700 SIP Phone & MiVoice 5300 IP Phone web page	HTTP	Tel
User PC	White pages	PBX/MiVoice 5000 Server	HTTP	Tel
	Self admin	MiVoice 5000 Manager	https	Admin
	Mail application	Mail server	SMTP/POP3/IMAP4	Tel
	Mitel OMM - configuration	Mitel OMM application	Telnet, HTTP, TFTP	Tel
TAPI application	signalling	TAPI gateway	Proprietary (port 5001)	Tel
TAPI gateway	TAPI gateway	PBX/MiVoice 5000 Server	Gateway TCP/X.25	Tel

EQUIPMENT	DEPARTMENT	REMOTE EQUIPMENT	PROTOCOL	NETWORK
	signalling	(TAPI)		
Alarm station	signalling	M7900 alarm server	Port com emulation	Tel
M7900 alarm server	signalling	PBX/MiVoice 5000 Server	VTI/XML (port 3199)	Tel
CC	signalling	PBX/MiVoice 5000 Server	VTI/XML (port 3199)	Tel
	CTI	PBX/MiVoice 5000 Server (CSTA)	Gateway TCP/X.25	Tel
	voice flow	End points	RTP	Tel
	Directory	LDAP directory	LDAP read only	Admin
	Miscellaneous Client Server relations		HTTP, DCOM, file sharing	Tel
TWP	signalling	PBX/MiVoice 5000 Server	VTI/XML (port 3199)	Tel
	CTI	PBX/MiVoice 5000 Server (CSTA)	Gateway TCP/X.25	Tel
	media flow (voice, visio)	End points	RTP	Tel
	Directory	LDAP directory	LDAP read only	Admin
	CTI	User station	https	Tel
UCP	signalling	PBX/MiVoice 5000 Server	VTI/XML (port 3199)	Tel
	CTI	PBX/MiVoice 5000 Server (CSTA)	Gateway TCP/X.25	Tel
	voice flow	End points	RTP	Tel
	Directory	LDAP enterprise database	LDAP read only	Admin
	Fax downloading		FTP	Tel
	Miscellaneous		VPIM/SMTP/POP3 IMAP/RPC/HTTP/https	Tel
Remote user via ISDN/PPP	all	all	all	PPP
Most of the equipment	Log information	Support team equipment	Syslog (514)	Admin

6.1.2 DATA FLOWS FOR DEVICES CONNECTED TO THE ADMINISTRATION NETWORK

This table gives a list of data flows in the MiVoice 5000 R5.2 solution and for requests made by some equipment connected to the administration network.

EQUIPMENT	DEPARTMENT	REMOTE EQUIPMENT	PROTOCOL	NETWORK
MiVoice 5000 Manager	Directory synchro.	Active directory	LDAP	Admin
	Directory replication	MiVoice 5000 Server	LDAP	Admin
	Supervision	SNMP manager	SNMP (trap)	Administration

EQUIPMENT	DEPARTMENT	REMOTE EQUIPMENT	PROTOCOL	NETWORK
	Polling	PBX/MiVoice 5000 Server (agent SNMP)	SNMP (get)	Administration
	File transfer (CDR/billing)	PBX/MiVoice 5000 Server (Web Admin)	https	Admin
	PBX/MiVoice 5000 Server configuration	PBX/MiVoice 5000 Server (Web Admin)	https (XML)	Admin
		MiVoice 5000 Manager clients	Proprietary (44555)	Admin
	MiVoice 5000 Manager clients	PBX/MiVoice 5000 Server – VT100	Proprietary (8201)	Admin
	Date & time	NTP server	NTP	Administration
	Alarm	SMTP server	SMTP	Administration
	UCP configuration	UCP	Proprietary (13888)	Admin
MiVoice 5000 Manager client	Management	MiVoice 5000 Manager	https (apache server)	Admin
	PBX/MiVoice 5000 Server VT100&MMI	Via MiVoice 5000 Manager	proprietary(8201/8220)	Admin
	PBX/MiVoice 5000 Server configuration	Via AM7430	vnc client (5800/5809)	Admin
	Synoptic Nagios	PBX/MiVoice 5000 Server	https	Admin
	Synoptic Nagios	AM7430	HTTP	Admin
PBX/MiVoice 5000 Server	SNMP agent	MiVoice 5000 Manager & other managers	SNMP	Admin
	Maintenance	SNMP managers	PPP (via ISDN)	PPP
	MiVoice 5000 Server redundancy	MiVoice 5000 Server	Heartbeat	Admin
	MiVoice 5000 Server redundancy	MiVoice 5000 Server	DRBD	Admin
	Directory	LDAP directory	LDAP	Admin
	White pages	LDAP directory	LDAP	Admin
	Date & time	NTP server	NTP	Admin
User PC	GDB application	PBX/MiVoice 5000 Server (debug)	Proprietary (port 1005)	Admin
	Operator	PBX/MiVoice 5000 Server (Web Admin)	https	Admin
	Operator	PBX/MiVoice 5000 Server (Linux)	SSH	Admin
	White pages	PBX/MiVoice 5000 Server	HTTP	Tel
	Self admin	MiVoice 5000 Manager	https	Admin
	Mail application	Mail server	SMTP/POP3/IMAP4	Tel
	Mitel OMM - configuration	Mitel OMM application	Telnet, HTTP, TFTP	Tel
CDR/Billing	Data transfer	PBX/MiVoice 5000 Server (MUFACT or KITAXE)	Gateway TCP/X.25	Admin
	File transfer	MiVoice 5000 Manager	https	Admin

EQUIPMENT	DEPARTMENT	REMOTE EQUIPMENT	PROTOCOL	NETWORK
	directory	LDAP directory	LDAP read only	Admin
	configuration	PBX/MiVoice 5000 Server (EAI)	Gateway TCP/X.25	Admin
TMA	Terminal management	FTP server	FTP	Admin
	PBX/MiVoice 5000 Server configuration	PBX/MiVoice 5000 Server (Web Admin)	https (XML)	Admin
AM7430	PBX configuration	PBX/MiVoice 5000 Server in R4.2 or previous	Proprietary (TCP/X.25)	Tel

6.2 SUPPORTED PROTOCOLS

6.2.1 INPUT PROTOCOLS SUPPORTED BY THE TELEPHONY NETWORK

DESTINATION PORTS	PROTOCOLS	APPLI PROTOCOLS	SERVICES
13	TCP	DAYTIME	IPS time setting
68	UDP	DHCP	Terminal configuration
69	UDP	TFTP	File transfer
80	TCP	HTTP	White pages
123	UDP	NTP	Date and time
694	UDP	NTP	Heartbeat
1998	TCP	SERGIC tunnel	MOVACS multi-site signalling
2000 to 3196			Not assigned
3197	TCP	HTTP	XML proxy
3198	TCP	CRI	
3199	TCP	CRI / VTI-XML (proprietary)	Terminal signalling
3207	TCP		Reserved
3208	TCP	TPKT	H.323 server (for H.323/MOVACS gateway)
3209	TCP	TPKT	Gateway server for attendant console and software phone on PC (TD/PC)
3210	TCP		Reserved
3211	TCP	CSTA	CSTA Server
3212 to 3216	TCP	CSTA	Reserved
3220 to 3283	TCP	TPKT	Internal server called by TAPI Gateway
3284 to 3287	TCP		Reserved
3292 to 3299	TCP		Reserved if more ports are required for a server (providing several CCUs)
3300	TCP		Reserved
3301	TCP	TPKT	CSTA Server (the same as 3211 but TPKT mode)
3302	TCP	TPKT	AFISER Server (echo service)
3303	TCP	No D	AFISER Server (echo service)
3305 to 3399	TCP	CSTA	Reserved
3600 to 7999	TCP	CSTA	Not assigned
3998	TCP	MOVACS over TLS	MOVACS Multisite signalling
4443	TCP	HTTPS	Proxy XML for Mitel 6700 SIP Phone
5060	UDP	SIP	SIP signalling
5061	TCP	SIP	SIP signalling
5062	TCP	SIP	SIP signalling
5063	UDP	SIP	SIP signalling
5160	UDP	SIP	SIP signalling
5161	UDP	SIP	SIP signalling
5162	UDP	SIP	SIP signalling

DESTINATION PORTS	PROTOCOLS	APPLI PROTOCOLS	SERVICES
5163	UDP	SIP	SIP signalling
8001 to 65534	TCP		Not assigned

6.2.2 INPUT PROTOCOLS SUPPORTED BY THE ADMINISTRATION NETWORK

DESTINATION PORTS	PROTOCOLS	APPLI PROTOCOLS	SERVICES
20	TCP	FTP	
21	TCP	FTP	File transfer
22	TCP	SSH	Remote access
80	TCP	HTTP	White pages and XML Proxy
161	UDP	SNMP	Supervision and map
162	UDP	SNMP	Supervision and map
389	TCP	LDAP	Directory
636	TCP	LDAPS	Directory secured access
443	TCP	HTTPS	File transfer and configuration
514	UDP	SYSLOG	Log information
694	UDP		Heartbeat
1005	TCP	GDB	GDB application (Debugger)
2222	TCP	SSH	VT100 MMC
3200 to 3204	TCP	proprietary	KITAXE
3206, 3218 and 3219	TCP	proprietary	EAI
3217, 3288, 3291, 3304	TCP	proprietary	MUFACT
3302 to 3303	TCP	proprietary	AFISER
3400 to 3599	TCP	proprietary	Reserved ranges
7788	TCP	DRBD	Redundancy

6.2.3 PROTOCOLS AUTHORISED FROM THE COMPANY NETWORK TO THE ADMIN NETWORK

The external firewall must allow the following protocols to pass from the company network to the admin network:

This firewall must be set to inspection mode (STATEFULL).

DESTINATION PORTS	PROTOCOLS	AUTHORISED SOURCE ADDRESS	APPLI PROTOCOLS	SERVICES
20	TCP	All	FTP	
21	TCP	All	FTP	File transfer
389	TCP	All	LDAP	Directory
636	TCP	LDAPS		Directory secured access
443	TCP	Client PC address	HTTPS	Mitel OMM
443	TCP	Client PC address	HTTPS	Self admin (Mitel Phone suite)
514	UDP		SYSLOG	Log information