A MITEL
PRODUCT
GUIDE

MiVoice Connect

Planning and Installation Guide

Release 19.3 SP3
Document Version 2.0

22 June 2023

Mitel
Powering connections

Notices

The information contained in this document is believed to be accurate in all respects but is not warranted by **Mitel Networks™ Corporation (MITEL®).**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") or others. Use of the Trademarks is prohibited without the express consent from Mitel. Please contact our legal department at legal@mitel.com for additional information. For a list of the worldwide Mitel Networks Corporation registered trademarks, please refer to the website:http://www.mitel.com/trademarks.

Contents

What's New in this Document 1

This section describes changes in this document due to new and changed functionality in MiVoice Connect Release 19.3 SP3. The changes are summarized in the following table.

Table 1: Document Version 2.0

Feature/Enhancement	Update	Location	Publish Date
Added a note on Zerto	Added a note about the third-party application Zerto and and provided a link to the Mitel Solutions Alliance page.	Failover	June 2023

Table 2: Document Version 1.0

Feature/Enhancement	Update	Location	Publish Date
New variant of the 6920, 6930, and 6940 IP Phones.	A new variant of the 6920, 6930, and 6940 IP Phones are available called the 6920w, 6930w, and 6940w IP Phone respectively. The 69xxw IP Phone is physically identical to the 69xx IP Phone. The new features supported by the 69xxw IP Phone relative to the 69xx IP Phone are embedded Wi-Fi, Bluetooth 5.0, IEEE 802.3az standard (Energy Efficient Ethernet) capability.	Updates are made across the document.	May 2023

Preface 2

This chapter contains the following sections:

ShoreTel is now part of Mitel. Together we look forward to helping you power connections that are brilliantly simple.

This preface provides information about the objectives, organization, and conventions of the *MiVoice Connect Planning and Installation Guide*.

2.1 Audience

This guide is written for the person who plans, installs, administers, and maintains the MiVoice Connect system. This individual should be knowledgeable about data networking and telephony to use this guide effectively.

2.2 Organization

This document is generally organized into major tasks, presented in the order in which they should be completed.

2.3 Documentation Overview

The MiVoice Connect system is documented as described in the following sections.

2.3.1 System Documentation

The *MiVoice Connect Planning and Installation Guide* provides information on how to plan the implementation of the MiVoice Connect system, as well as how to install the necessary hardware, data communications, and telecommunications elements.

2.3.2 Software Documentation

The *MiVoice Connect System Administration Guide* provides detailed reference information about how to configure and administer the MiVoice Connect system using Connect Director.

If you are installing one or more service appliances, refer to the *Conferencing and Instant Messaging Planning and Installation Guide* for complete installation and configuration information.

2.3.3 Hardware Documentation

The following hardware installation documents are packaged with their associated voice switch, Service Appliance 100/400, or IP phone:

- *ShoreGear Voice Switch Quick Install Guide*
- *Safe Installation Guide*

For hardware regulatory information, see http://www.mitel.com/.

2.3.4 Release Notes

The release notes provide information about new releases and new features as well as installation and upgrade information.

2.3.5 Online Knowledge Base

To access additional information about the current release or to resolve issues with the MiVoice Connect system, you can use the online knowledge base. You can access this website at https://www.mitel.com/support.

You must download Mitel's Windows PowerShell script utility, "TacTools", to help verify server prerequisites, validate certificates, check system load balancing, and other useful functions for migration preparation and system administration. TacTools is available as a free download from the partner knowledgebase at the following location:

- For Partners: https://mitelcommunity.force.com/partner/s/article/TAC-Tools-Powershell-Scripts
- For Customers: https://mitelcommunity.force.com/customer/s/article/TAC-Tools-Powershell-Scripts

Disclaimer:

The TacTools script was written and provided by TAC. It is provided on a "best effort" basis and is not guaranteed to function properly in your environment. TAC will not troubleshoot the script in a customer's environment. Many modules are written to be "read only" to minimize any potential impact on the customer's server. Running any modules that will make any changes to your server will prompt you for confirmation. It is recommended that if you run a module that can make changes to your server, then you must run the script as part of a maintenance window, and must accept any potential service impact caused by the changes made to your server.

2.3.6 Document Conventions

Conventions used in this guide include the following:

- Data-entry field names, hypertext links, control buttons, keywords, and other items within the system management interface are in **boldface** text.
- Information that you enter in data-entry fields is in a *data_entry* font.

Getting Started 3

This chapter contains the following sections:

This chapter describes how to plan and install a MiVoice Connect system.

3.1 Overview

This document describes how to plan and install a MiVoice Connect system. Each chapter in this document begins with recommendations that help with the transition to a MiVoice Connect system.

For an installation outside the U.S., see Software and Feature Support on page 325.

3.2 Assembling the Team

To deploy a MiVoice Connect system, the members of the team might include some or all of the types of support sources:

- **System_Designer:** The System_Designer determines the number of telephones, number and type of trunks, and the call flow that the customer needs in the network.
- **Project Manager:** The project manager oversees the entire project and communicates important decisions to the entire team. The project manager usually is an IT manager.
- **IT Manager:** The IT department needs to give its full support and cooperation.
- **Electrician:** An electrician might be necessary for installing new power outlets and cooling and ventilation systems. The building that has the MiVoice Connect system must be able to provide enough power to the system.
- **Service Providers:** An effective relationship with a telephone service provider for local and long-distance telephone service is necessary. The phone company or Internet service provider and the customer must have a clear understanding of the technical requirements and characteristics that exist on both sides of the network boundary.
- **Partner:** A certified partner might be necessary for the implementation. This possibility likely depends on the complexity of the network and support package that the customer purchased.

3.2.1 Phase 1: Voice Communication System Analysis and Ordering

Table 3: Voice Communications System Analysis and Ordering

Task	Date Completed
Complete Call Flow Analysis	

Task	Date Completed
Inventory and determine trunk requirements	
Order new trunk lines	
Trunk installation date	
Inventory your existing telephone equipment	
Order new phones and/or headsets	
Review your need for a Service Appliance	
Order a Service Appliance	
Review the need for a MiVoice Connect Contact Center Solution	
Order a MiVoice Connect Contact Center Solution	
Order voice switches	
Shipping date	

3.2.2 Phase 2: Environmental and Infrastructure Analysis and Upgrade

Table 4: Environmental and Infrastructure Analysis and Upgrade

Task	Date Completed
Participate in the Phase 2 conference call	
Read about the power requirements	
Order power upgrades (as necessary)	
Scheduled power upgrade completion date	
Read about the voice switch racking requirements	
Racking installation date (if racking is ordered)	
Read about the voice switch ventilation requirements	
Ventilation system upgrade completion date (if ordered)	
Read the recommendations for uninterruptable power source (UPS)	
UPS installation date (if ordered)	
Read about the cabling requirements	
Cabling installation date (if ordered)	
Determine the overhead paging needs	
Source your Music on Hold needs	
Read about the LAN requirements	
Attach LAN topology map	
LAN installation date (if ordered)	
Read about the WAN requirements	
Attach WAN topology map	

Task	Date Completed
WAN upgrade installation date (if ordered)	
Read about the server requirements	
Order your server for the MiVoice Connect system	
Server installation date	
Read Mitel Connect client's requirements	
Schedule the Mitel Connect client's software upgrade installation date (if required or ordered)	
Scheduled installation date	

3.2.3 Phase 3: Resource Scheduling and Tracking

Table 5: Resource Scheduling and Tracking 22

Task	Date Completed
Participate in the Phase 3 conference call	
Verify Telco order is on schedule	
Verify phone order is on schedule	
Verify power order is on schedule	
Verify racking order is on schedule	
Verify ventilation order is on schedule	
Verify uninterruptable power source (UPS) order is on schedule	
Verify cabling order is on schedule	
Verify LAN upgrade order is on schedule	
Verify WAN upgrade order is on schedule	
Verify desktop upgrade order is on schedule	
Verify the order is on schedule	
Read descriptions of the different Mitel Connect client applications	
Schedule your System Administration training	
Order new business cards and business stationary if your phone n umbers are changing	
Verify that you have obtained all licenses and license keys for your planned installation.	

3.2.4 Phase 4: System Load and Configuration

Table 6: System Load and Configuration

Task	Date Completed
Participate in the Phase 4 conference call	

Task	Date Completed
Verify receipt of equipment	
Reserve IP addresses for your network	
Configure server with the appropriate server operating system	
Load the software	
Enter the database configuration	
Confirm your MiVoice Connect system installation and cut-over dates	
Confirm installation and cut-over coverage	
Verify racking is complete	
Verify power is in compliance	
Verify UPS is installed	
Verify cabling is complete	
Verify ventilation upgrade is complete	
Verify new phones and headsets have been delivered	
Verify that your System Administrators have been trained	
Schedule training for your Operators and Workgroup(s)	

3.2.5 Phase 5: Installation Readiness Review

Table 7: Installation Readiness Review

Task	Date Completed
Participate in the Phase 5 conference call	
Upgrade desktops, if necessary, and ensure readiness for Mitel Connect client software installation	
Notify users of the MiVoice Connect system implementation	
Verify telephone trunk lines are installed and tested	
Verify server appliance is installed	
Configure on-hour and off-hour schedules for Auto-Attendant menus an d Workgroups	
Configure your Workgroups	
Configure your Auto-Attendant menus	
Script and record all Auto-Attendant and department voice mail greet ings	

3.2.6 Phase 6: Cut-Over

Table 8: Cut-Over

Task	Date Completed
Participate in the Phase 6 conference call	
Complete your Cut-Over Review Checklist	
Send web-based training modules to end users	
Send phone user guides to end users	
Verify that operators are trained	
Verify that workgroups are trained	
Verify that all phones have been placed and extensions tested	
Verify that existing trunk lines have been swapped and tested	
Verify that end users have been sent the Mitel Connect client notification	
Cut-over to the MiVoice Connect system	
Complete your Post Cut-Over Survey	
Review the Mitel website to understand the available support resources	

Planning and System Design 4

This chapter contains the following sections:

This chapter describes the initial design of the MiVoice Connect system.

4.1 Overview

This chapter describes the initial design of the MiVoice Connect system.

4.2 Recommendations

The following recommendations will assist you in designing your new voice communications system.

- Ensure you understand all the unique routing and hunting requirements of your current system.
- Ensure to account for all devices, including conference rooms, lobby phones, fax machines, and modems.
- Ensure that you consider the changes to the call flow and overall System_Design that may drive the need for additional trunks.

Note:

Mitel does not support MiVoice Connect implementations in cloud environments controlled by a third party (such as Amazon Web Services) because Mitel partners and customers cannot fully control the underlying infrastructure in these environments.

4.3 Network Assessment

As you plan your phone system, Mitel recommends that you have a network assessment performed. A network assessment does the following:

- Ensure necessary protocols and standards are supported.
- Confirm that the infrastructure is optimally configured for IP telephony traffic.
- Verify that the installed WAN technologies are compatible with IP telephony.
- Measure delay, packet loss and jitter to ensure that they need acceptable thresholds for toll-quality voice calls.

To complete your System_Design, the final step is to identify your network connectivity. You should identify the following for the network connections to each site:

- Bandwidth
- Latency
- Jitter
- Packet Loss

4.4 Determine System Topology

The MiVoice Connect system has a unique distributed call control software architecture that enables you to deploy voice switches and IP phones anywhere across your IP network. Even though multiple sites are supported, the MiVoice Connect system is a single system with an extensive set of integrated applications and a single management image. The MiVoice Connect system offers unmatched simplicity through this single image system, and delivers high availability, with no single point of failure, through its distributed architecture.

The first step in planning a voice network is to determine the overall network topology. Topology information includes the following:

- Sites and Users. Number of sites and number of users at each site.
- Headquarters and Distributed Voice Servers. Number of servers required, plus the name or IP address of all servers (main and distributed).
- Teleworker Sites. Number of teleworker installations and the type of telephones supported.
- Telephone Requirements. Number of telephones at each site (by type).
- Trunk Requirements. Number of trunks required for optimal performance.
- Voice Switches. What models are needed and how many of each model.
- WAN Connections. The number of WAN connections (per site) and complete service-level information.

For detailed information about planning your network for the MiVoice Connect system, see Overview on page 30.

4.4.1 Sites and Users

Your network topology diagram should provide an accurate inventory of the different physical sites and the number of users at each site.

4.4.2 Headquarters and Distributed Voice Servers

The MiVoice Connect Headquarters server hosts the voice applications platform and the management web site, as well as the integrated voice applications. Typically, the Headquarters server is located at the largest location, containing the majority of users. Make special note of the main MiVoice Connect server on your topology diagram.

On your topology diagram, provide the following information about the servers:

- Total number of servers (that is, the sum of servers at all sites).
- Number of servers at each site.
- The name and IP address of every server.

The MiVoice Connect system also supports Distributed Voice Servers (DVS) to allow distributing voicemail and other applications. Distributed servers help accomplish the following:

- Reduce bandwidth, because local users' calls to voice mail are answered by the local voice mail application and do not go across the WAN.
- Increase system scale by extending the unified messaging and desktop call control services to additional users of the applications.
- Increase reliability by providing local support for some services and applications if a site loses connectivity with the Headquarters server.

Even though there are multiple servers, the MiVoice Connect system provides a single image system across your entire network. The system is currently certified to support up to 21 servers, one at the headquarters site and up to 20 distributed servers. You should add a server at any site that exceeds 100 users. You must deploy a server for every 1,000 users.

The distributed voice applications platform can also provide an open applications platform for extending telephone services through TAPI-compliant third-party applications. A dedicated distributed server is required to host the third-party applications. This server is deployed like other distributed servers, except that it must not have voice mail users assigned to it.

The distributed voice application servers' Remote TAPI Service Provider relies on the call control information from the main server.

4.4.3 Windows Terminal Server

Windows Terminal Server (WTS) technologies enable processing for multiple users to be aggregated on a single Windows computer. The single Windows computer is a process- and disk-sharing server for multiple users who have lightweight or thin graphics stations on their desktop. Windows Terminal Server communicates between the server and clients using the RDP protocol.

4.4.4 Teleworker Sites

IP Phones can operate away from the site. For example, employees (telecommuters) can have an IP phone at their home so that they can work from home. The topology diagram must include the number and location of off-site IP phones.

For information on configuring IP phones for teleworkers, see Overview on page 261.

4.4.5 Telephone Requirements

This section describes how to determine the telephone requirements, as follows:

1. Count the telephone users in the current environment. Include conference room telephones, lobby telephones, and telephones that multiple users share.
2. Count the number of BB24 or BB424 button boxes that operators and receptionists need. Up to four button boxes can be connected to a phone.
3. Count the number of ports that fax machines and modems will use.
4. If you are deploying IP phones, determine the number of telephones that will be IP phones and the number that will be analog phones.
5. Some users might need specialized features. For example, an operator needs a phone with programmable buttons. Therefore, consider the type of functions that each user needs to select the appropriate phone for each user.
6. Consider the needs for additional telephone ports for third-party systems, including server appliances and overhead paging systems.

> **Note**:
> For more information about selecting telephones, see Considerations for Selecting Phones on page 146.

7. Determine the number of user licenses you need.

   Each user on the system requires a user access license. The types of user licenses are listed below:

   - Extension and mailbox: Purchase of this license entitles the user to be assigned to both a physical extension and a voice mailbox.
   - Extension-only: This license lets the user have a physical extension through an explicit assignment or through the Extension Assignment feature.

Note:

An Extension-only license is a requirement for each conference room telephone, lobby telephone, fax machine, and modem. A user access license is not necessary for trunks and anonymous telephones.

- Mailbox-only: This license lets the user have only a voice mailbox.
- Audio conference: Purchase this license for each audio port that you want to use in conferences managed by a Service Appliance. A license allows one audio endpoint to participate in a conference.

4.4.6 Trunk Requirements

Trunks provide connectivity between users on the MiVoice Connect system and the public switched telephone network (PSTN). In this next task in the System_Design process, you determine the number of trunks required.

The number of trunks required on your system varies, depending on the number of users and your specific application needs. It is important to size your trunking correctly because not having enough trunks can lead to blocked calls when all trunks are busy, and too many trunks can lead to wasted money on monthly access charges.

See Planning Considerations for IP Phones on page 153 for more information about trunk features, ordering, and installation. You have several options for determining the number of trunks your site requires:

- Review the number of trunks on your current system. In general, this is one of the best methods to gauge the number of trunks you need.
- You can also request a traffic analysis from your service provider, interconnect, or telecom manager to understand your current trunk utilization. This method will help you understand your current usage and allow you to maintain the current service level.
- Visit a web site, such as www.erlang.com, to use a traffic calculator for determining your trunk requirements.
- Consider the following:
  - Larger locations can typically use lower-density trunking (15%).
  - Smaller locations need higher-density trunking (50%).
  - Some applications, such as call centers, can demand higher-density trunking (50%).

Table 9: Trunk Density

Trunk Density	Trunk Users%
Low	15%
Average	30%
High	50%

When planning trunks, consider the call volume for your workgroups or ACD groups. Since there is generally a queuing solution in place for ACD calls, the number of trunks required should be based on the

full utilization of the expected number of agents and sufficient trunks for the expected number of waiting callers.

4.5 Determine Number of Voice Switches

The MiVoice Connect telephony solution is a mixture of hardware and software components that you install across your enterprise to create a single telephone system. A critical component to the solution is the voice switch. Voice switches are the interface that connect the telephones to the MiVoice Connect system. These switches, which can be physical or virtual, provide signaling and call-setup functions for the phones and trunking to interface with service providers and other telephony networks. The voice-switch portfolio offers a broad range of telephony switches to meet the needs of our different customers.

For more information about voice switches, see Appendix C - Voice Switches on page 333. For details about virtual switches and service appliances, see Virtual Switches and Service Appliances on page 254.

For information about the features that MiVoice Connect supports outside the U.S., see Appendix A - International Planning and Installation on page 325.

4.6 WAN Connections

To complete your System_Design, the final step is to identify your network connectivity. You should identify the following for the network connections to each site:

- Bandwidth
- Latency
- Jitter
- Packet Loss

4.7 Failover

To provide high availability, MiVoice Connect supports failover at two very important points in the system: for the headquarters (HQ) server and for voice switches. For the HQ server, MiVoice Connect has been tested with the Zerto IT resilience solution through the Mitel Solutions Alliance (MSA) program. For more information about the MSA program, see https://www.mitel.com/developer/mitelsolutions-alliance. This solution supports a back-up server that monitors and can duplicate the primary server. If the primary server fails, the back-up server immediately starts operating as the HQ server with minimal interruption. After the primary server returns to operation, the system administration must perform a manual fail-back to restore the servers to their previous operation.

Note:
Zerto is a third-party application that Mitel does not support directly.

For voice switch backup, MiVoice Connect supports two approaches. The system administrator can configure extra port capacity or install a dedicated spare voice switch. A spare voice switch can be on a network that is remote to the failed voice switch.

4.8 System Capacity

The MiVoice Connect system can scale incrementally up to 2,500 endpoints and a maximum of 500 voice switches over the entire system. The system is completely nonblocking and can support 1,500 simultaneous calls at a rate of 25,000 calls per hour depending upon server configurations.

The System Capacities table provides a summary of the system capacity for various features in the MiVoice Connect system.

Note:

Refer to Real Time Capacity on page 19for information about considerations for calculating capacities for your system.

4.8.1 Servers

Server requirements are specified in three tiers:

- Servers for small systems that support up to 100 endpoints.
- Servers for medium sized systems that support up to 500 endpoints.
- Servers for large systems that support up to 2, 500 endpoints.

While the maximum capacity for a single-image system is 2,500 endpoints, larger deployment sizes are possible with prior approval from Mitel. Larger System_Designs must be reviewed by Sales Engineering and approved by Product Management and TAC. Consult with your Mitel sales representative to initiate this process if required.

To select a server for your new system deployment, first consult the sizing table and determine the tier of the server needed using the system and per server specifications. Then match that size (small, medium, or large) to the server requirements. Complete details about server capacity and hardware requirements are provided in General Recommendations on page 161.

The capacity limits for each of the server tiers depend on the following concepts:

- BHCC (Busy Hour Call Completion) per system is the total number of calls in the system during the busy hour including internal and external calls and calls terminated to desk phones, softphones, trunks, or server applications such as voicemail. This includes all traffic that can occur in the server: regular voice calls, workgroup calls, voicemail, and so on.
- BHCC per server is based on the number of calls actually handled by the server during the business hour including workgroup calls in menus and queues, auto-attendant calls, and calls to the voicemail service.

- The report generation tools that run on the server are configured by default to run at a lower priority than other, more critical services. A light demand of report generation should have little or no effect on a server with adequate minimum performance specifications. If you are a heavy report user or experience any degradation of voicemail or other server prompts on an underpowered server, you must move up to the next tier of servers.

Note:
Use the hardware specifications to size servers running Headquarters server software and Distributed Voice Services software. For example, consider a two-location system with 2,000 endpoints and 10,000 BHCC. A Headquarters server is located at the main site, and a Distributed Voice Services server is located at the remote site. Each of the servers handle 2,000 BHCC. In this case, both servers should be provisioned with hardware that meets the large tier of hardware requirements because the system capacity and both server capacities fall within this tier.

4.8.2 Virtual Phone and Virtual Trunk Switches

The MiVoice Connect system supports virtual phone switches and virtual trunk switches.

The virtual phone switch supports the following features:

- All non-TDM features (no physical trunks or analog phones)
- Up to 1,000 IP phones per switch
- Requires the Virtual Switch Phone License

Note:

The virtual phone switch does not support the Nightbell or Overhead Paging feature.

The virtual trunk switch supports up to 1,000 SIP trunks and requires the Virtual Switch SIP Trunk License.

For virtual switch capacities and requirements, see Virtual Switches and Service Appliances on page 254.

4.8.3 BHCA Call Volume

Busy Hour Call Attempts (BHCA) is the number of calls attempted at the busiest hour of the day (peak hour). The higher the BHCA, the higher the stress on the network processors. If a bottleneck in the network exists with a capacity lower than the estimated BHCA, then congestion will occur resulting in many failed calls and customer dissatisfaction.

MiVoice Connect systems support 5,000 BHCA.

4.8.4 Call Load Capacity for Switches

A MiVoice Connect system supports a maximum of 500 Voicemail Model Switches. There are no restrictions concerning the allocation of switches among the sites defined by the system.

Voicemail Model Switches support the following call load capacities:

- 5400 BHCC when supporting 90 MGCP IP Phones or 90 SIP Trunks.
- 3600 BHCC when supporting 90 SIP IP Phones or 90 SIP Trunks.

4.8.5 Extension Monitoring Limitations

There is a limit to the number of extensions that can be monitored, whether from an IP Phone BB24 or BB424 device or from an IP Phone multi-line phone. This limitation is dependent on two factors:

- Update rate (every call causes one or more monitoring phones to be updated).
- Whether the monitoring phones are spread across one or more switches.

Voice Switches support an update rate of 1 per second. This limit is independent of whether the monitored extensions are on the same switch or a different switch. If the monitored extensions are on a different switch, then IPDS is involved.

4.8.6 Voice Switch Feature Capacity

Voice switches are designed to handle the maximum load for the services it provides. Some features place a higher real-time load on the voice switch processor than others, and the use of these features must be carefully planned to take into account the impact on the processing power of a switch to handle call control signaling messages.

Feature Capacities for ST and SG Voice Switches offers some general guidelines for the number of extensions and group members for several commonly used features. Keep in mind that in addition to observing these limitations, you must stay below the real-time requirements of the switch itself.

In Feature Capacities for ST and SG Voice Switches, SG denotes ShoreGear generation switches and ST denotes ST-generation switches. Refer to the following lists for information about which devices are part of each generation:

Table 10: ShoreGear and ST Switches

ShoreGear Switches	ST Switches
• SG90 • SG90BRI • SG50 • SG30 • SG220E1 • SG220T1 • SG220T1A	• ST1D* • ST2D* • ST50A • ST100A • ST200 • ST500 • ST100DA

ShoreGear Switches	ST Switches
• SGT1k	• ST24A • ST48A

Note:
*Hunt groups and Bridged Call Appearance are not applicable to these devices.

4.8.6.1 Feature Capacity Considerations

All three points of consideration: number of groups, stack depth, and number of members — must be considered in relation to all features enabled on a physical switch. For example, while it may be possible to have a total of 24 hunt groups with a call stack of 24 and a maximum number of 16 members per group on an ST-generation switch, those numbers are achievable only if no other features are in use on the switch. Refer to the formulas in the Real Time Capacity on page 19 section and carefully consider the overall impact on the switch when planning for features that consume large amounts of resources.

4.8.6.2 IP Phones

Ringing a single user's IP phone generates only one set of call control messages. However, as the call rate increases, the load on the processor also increases. Note that the call rate is the driving factor of load and not the length of a call. For instance, sixty calls placed over one hour, with each call lasting one minute, is a much higher load on the processor than a single call lasting one hour.

4.8.6.3 Hunt Groups

Hunt groups place a significantly heavier burden on the voice switch. For example, if you have a hunt group with 16 members, a single call into the hunt group will generate 16 simultaneous calls (assuming the feature is configured to simultaneously ring each hunt group member).

To extend this example, assume that the call stack size for this hunt group is set to 16, and 16 calls arrived at the same time, this would be equivalent to 256 calls (16 x 16) simultaneous calls. The number of hunt group members (as well as the call stack depth) is a multiplying factor for the signaling load that would be generated. Therefore, you should closely engineer hunt groups to ensure that the voice switch is not overburdened in order to ensure optimal performance.

4.8.6.4 Bridged Call Appearances

With Bridged Call Appearances (BCA), additional processor load is related to the call control signaling transmission to the buttons that have been programmed on the IP phones. If a single BCA with a call stack of one is configured on a phone, this represents one load. However, if that same BCA were to appear on 24 different phones, that would represent 24 times more call signaling load than if the BCA were to appear on one phone.

4.8.6.5 Pickup Groups

Pickup Groups place an additional load on the processor related to tracking the extensions in the group (although the actual real-time load is rather light and is not factored into the real time equation).

The switch is capable of supporting 16 pickup groups with a maximum of 24 members in the group. The total number of members in all groups on the switch must not exceed 80.

4.8.7 Real Time Capacity

In addition to the overall feature capacity limit, you should calculate the real-time load on the switch(es) using the formula(s) given in the following figure:

Note:

- The real-time capacity limit for SG switches is 80.
- The real-time capacity limit for ST switches is 120.

4.8.7.1 SG-Generation Switches

Figure 1: RTC Score Calculation

$$\left(\sum_{n-1}^{\text{No. HG}} \text{HG\_Stacksize(n)*HG\_Members(n)}\right)+(0.5*\text{No\_BCA\_MonitoringLines}<=\text{RTC\_Score})$$

4.8.7.2 ST-Generation Switches

For example, consider the following configurations:

An ST-generation switch with:

- A hunt group with 10 members and a call stack of 4.
- A second hunt group with 14 members and a call stack of 3.
- Two BCA numbers, configured as follows:
  - The first BCA has a call stack size of 4 with:

    2 phones monitoring all 4 call stack positions.

    2 phones monitoring only 2 of the call stack positions
  - The second BCA has a call stack size of 4, with all positions monitored by 6 phones.

Using the formula above, the capacity would be as follows:

```
HG 1 + HG 2 + BCAs = RTC_Score
```

```
(10 x 4) + (14 x 3) + 0.5 x [ (2 x 4) + (2 x 2) + (4 x 6) ] = RTC_Score
```

```
40 + 42 + [0.5 x (8 + 4 + 24)] = RTC_Score
```

```
40 + 42 + 18 = 100
```

Because 100 < 120, this configuration fits comfortably within the real-time capacity for an ST-generation voice switch.

This configuration would not be within the limits of an SG-generation switch because SG-generation switch has a maximum RTC of 80.

4.9 Security Guidelines

This section details the security guidelines that must be followed while deploying MiVoice Connect.

MiVoice Connect (DMZ) deployment mode

MiVoice Connect servers/devices do not interact with devices or entities in the public networks except for the Edge Gateway and the Service Appliance. MiVoice Connect should be deployed behind a DMZ as a best practice to reduce attack vectors that target MiVoice Connect servers.The Edge Gateway and Service Appliances that interact with public network elements can be part of the DMZ. For more information about MiVoice Connect DMZ deployment, see Chapter 3 of the Edge Gateway guide.

Limiting Data Base access by using allowed lists

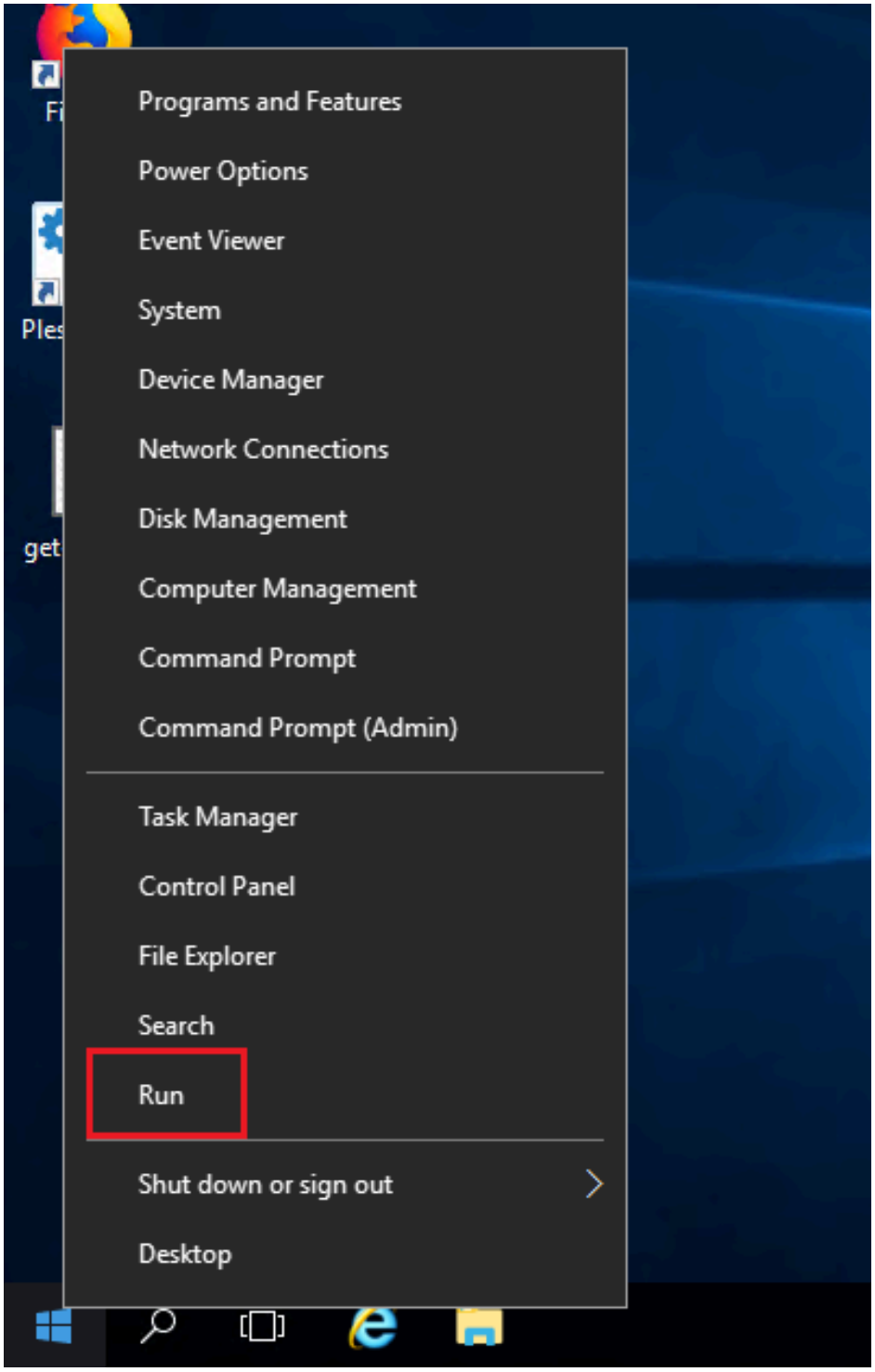
MiVoice Connect has different databases for different functionalities of the MiVoice Connect platform. Each server will run multiple databases, and each database is attached to the network interface. Access to the MiVoice Connect databases is required only by approved applications and servers. Because the databases contain critical information, it is imperative that proper security practices are followed. To reduce/avoid an attack, it is strongly advised to defend using allowed lists on the servers, that is by listing servers and applications that are allowed to access the MiVoice Connect databases.

MiVoice Connect databases are bound to ports 4308, 4309, and 4310. If allowed lists are used, MiVoice Connect administrators can control access to known MiVoice Connect servers or applications. For example, if someone tries to access the database at port 4308 without using an approved device or application, then the firewall rule causes the request to be dropped. This will safeguard the MiVoice Connect platform.

Procedure to add MiVoice Connect servers the allowed list

Following is the procedure to be followed on Windows devices (WDVS) by adding IP addresses to an allowed list:

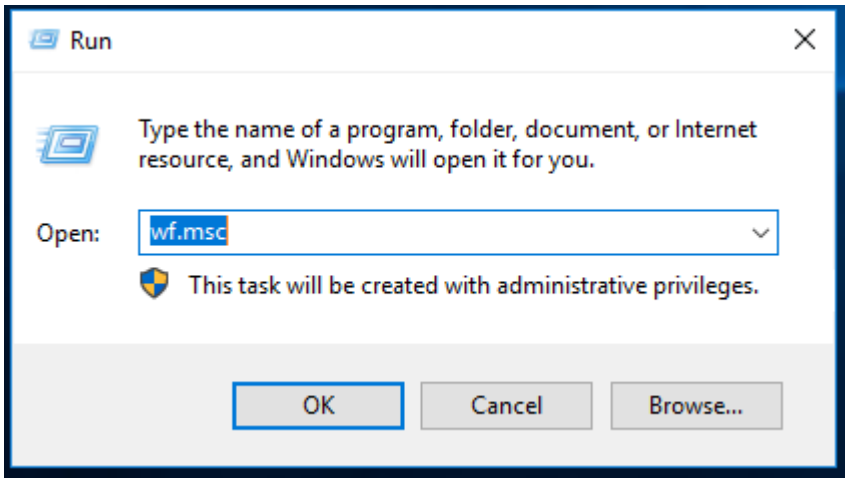
1. Log in to your windows server using RDP.
2. Right-click the start icon and click **Run**.



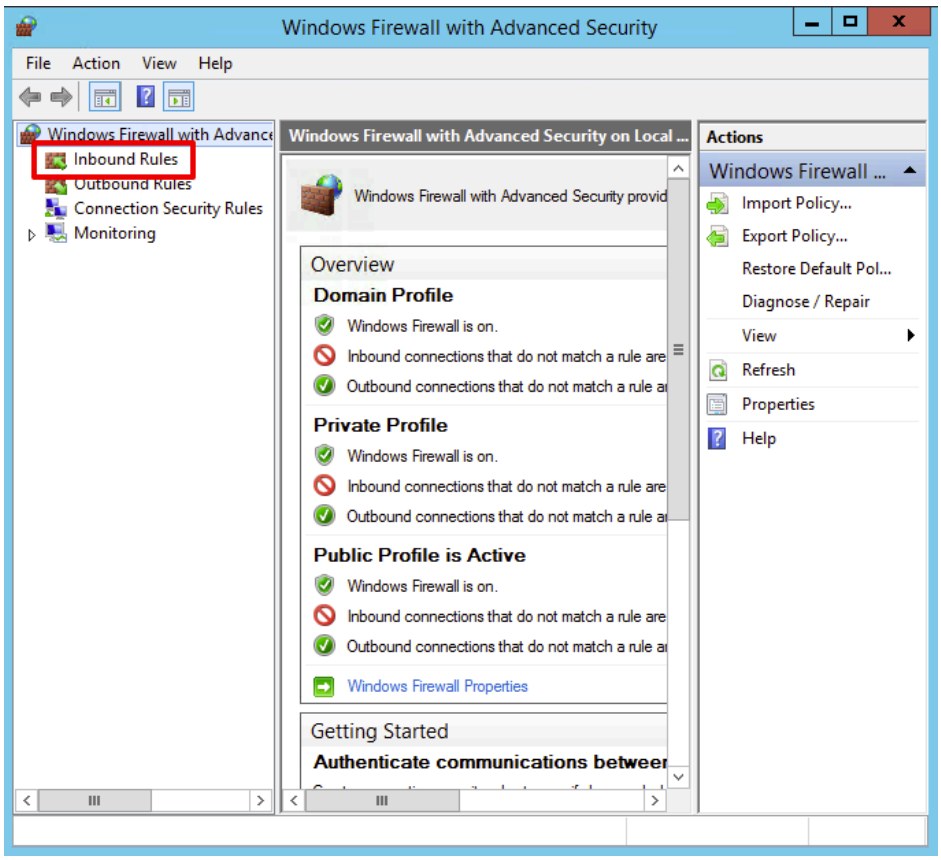
3. In the input box, type - wf.msc and click **OK**.

```
wf.msc
```

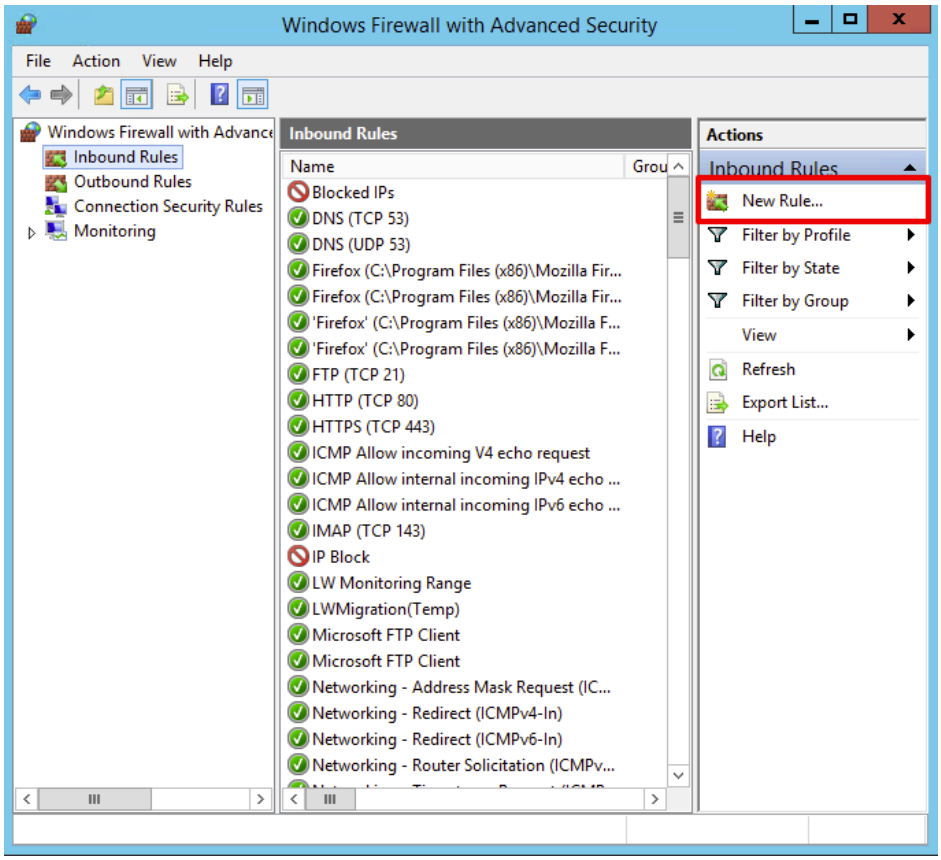
The **Windows Firewall with Advanced Security** opens.



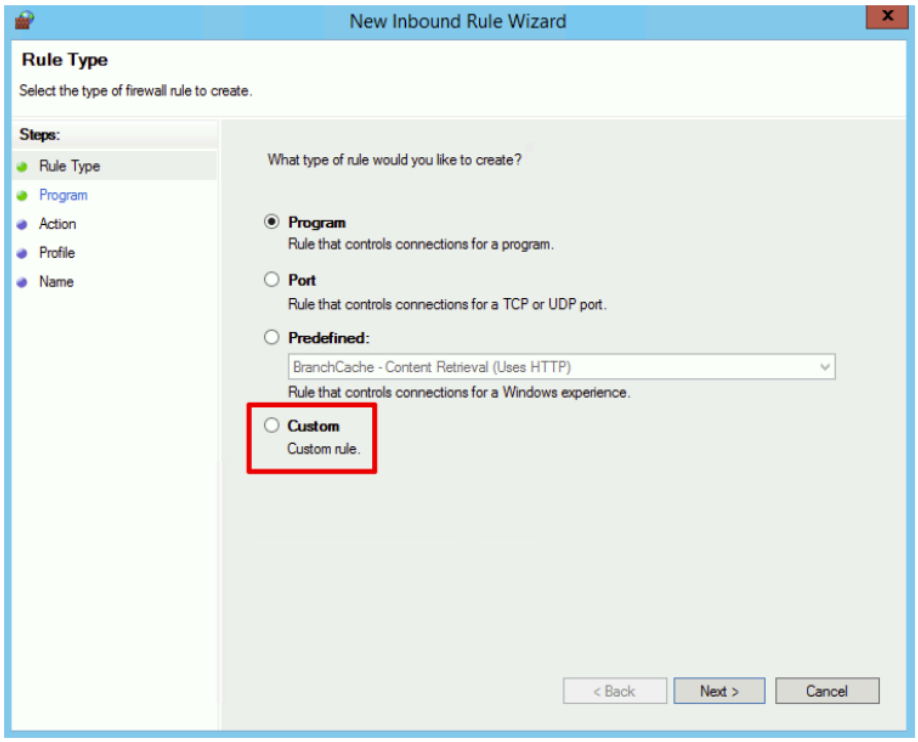
4. Click **Inbound Rules**.



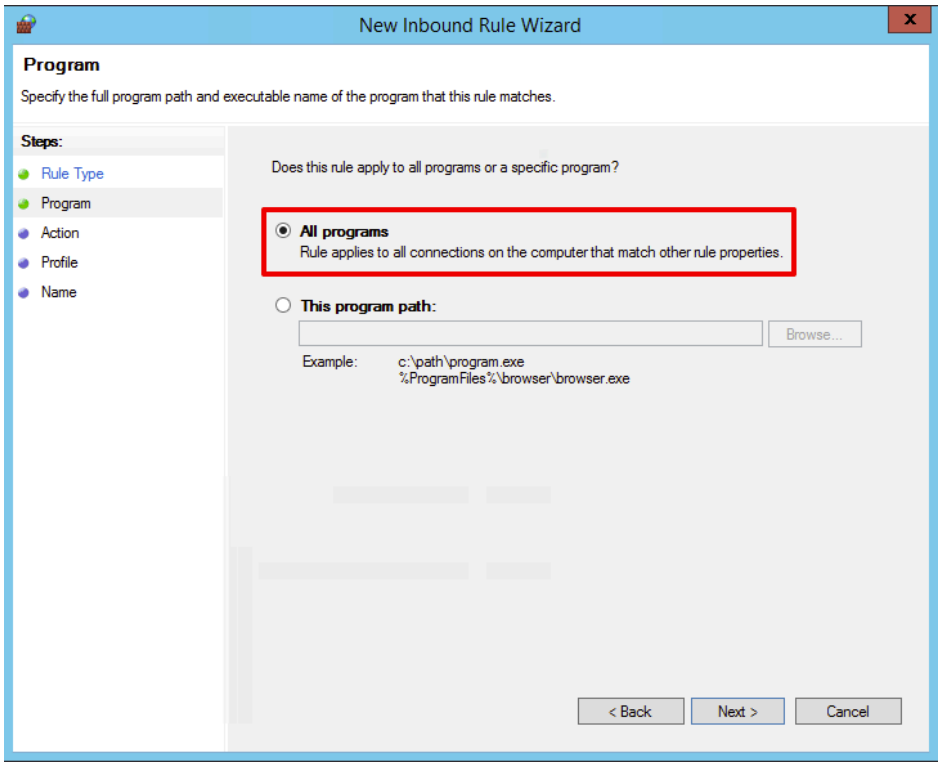
5. Click **New Rule**. This opens the New Inbound Rule wizard, which will guide you through adding your new firewall rule.



6. To begin creating an IP block rule, select the radio button next to **Custom**. Then press **Next >**.

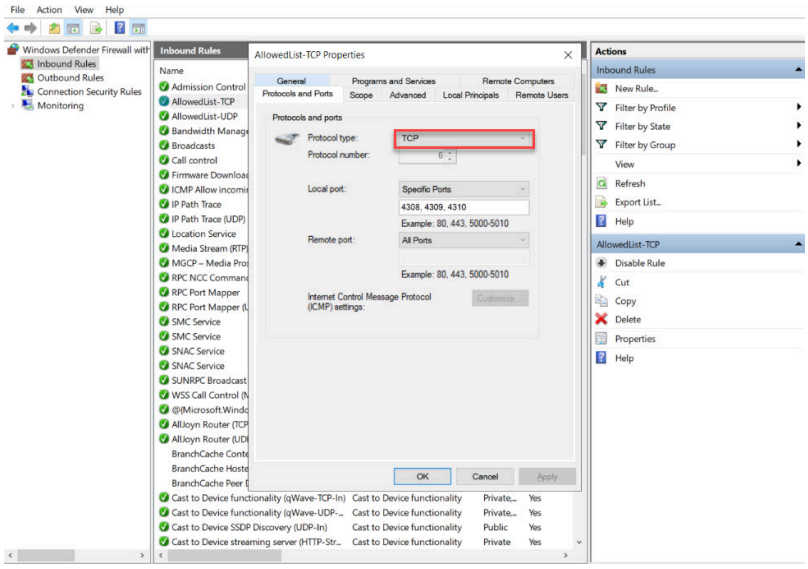


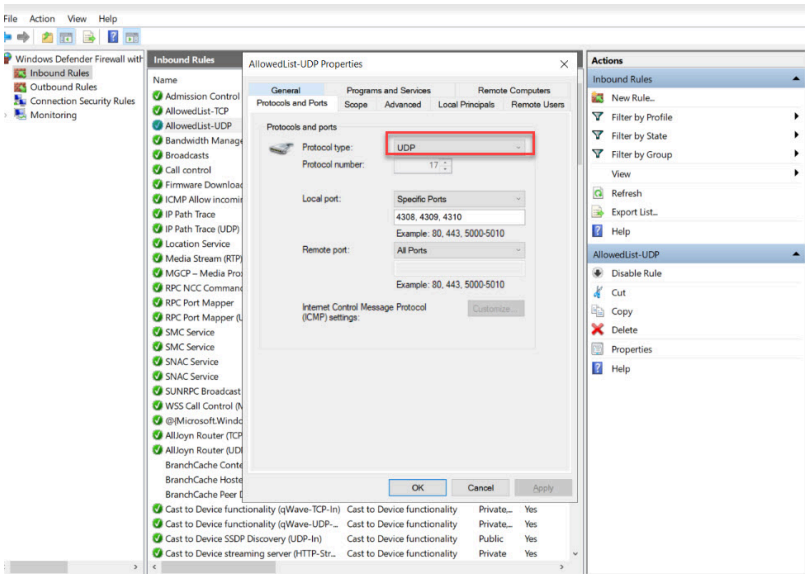
7. Ensure that the radio button **All programs** is selected and click **Next >**.



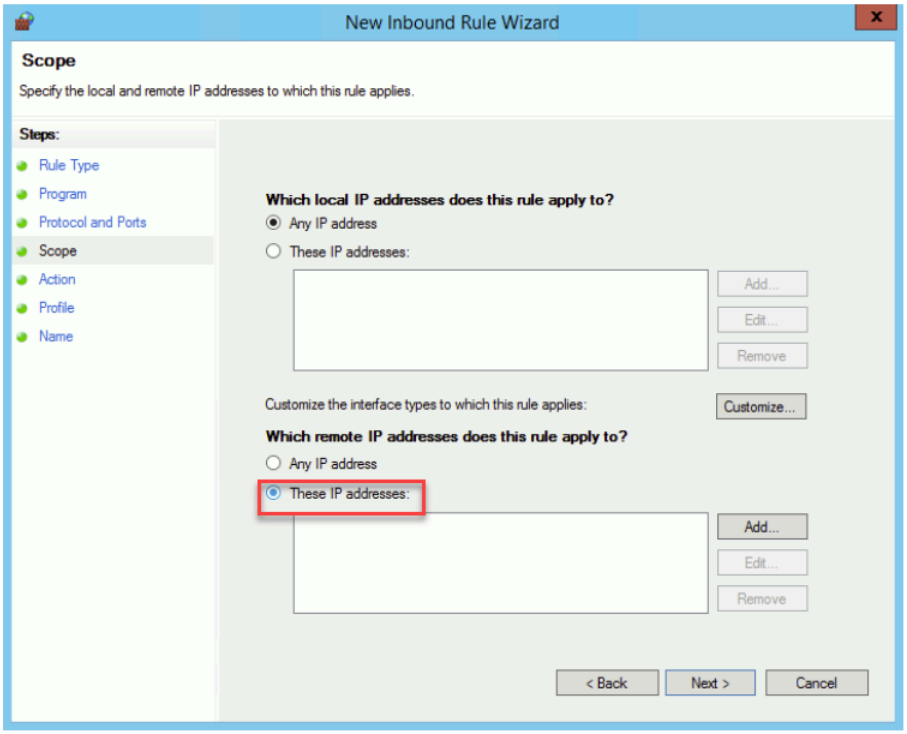
8. In the **New Inbound Rule Wizard**, enter the ports and protocols for which your rule will apply. Generally, with an IP block, you can leave the screen as it is, with the **Protocol type** set to **TCP**. Click **Next >**.

> **Note**:
> Ensure that the same procedure is followed for both the protocols (TCP and UDP).

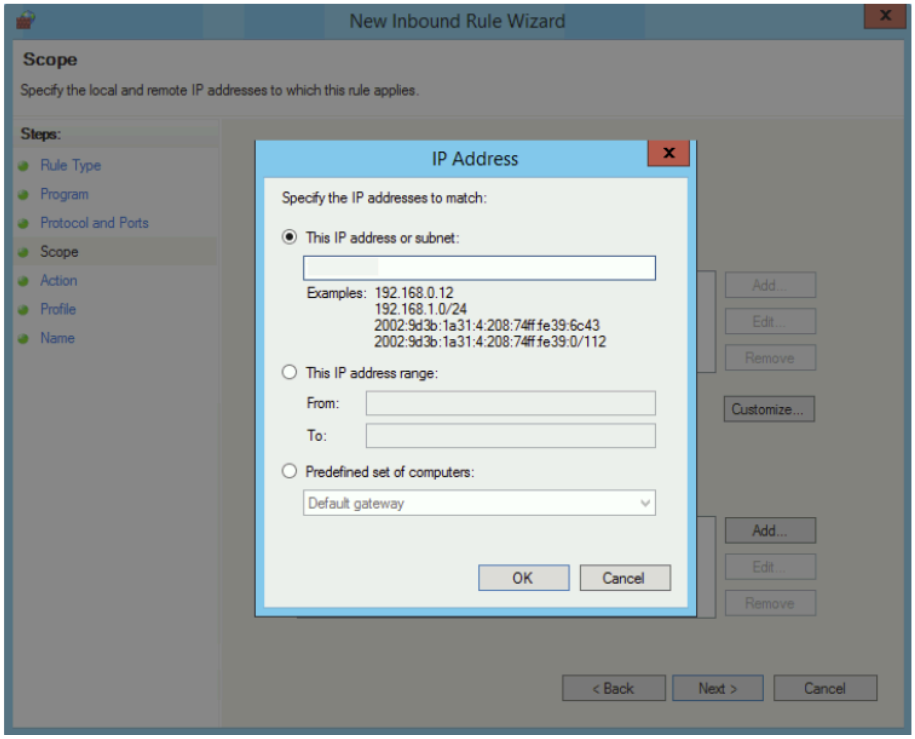




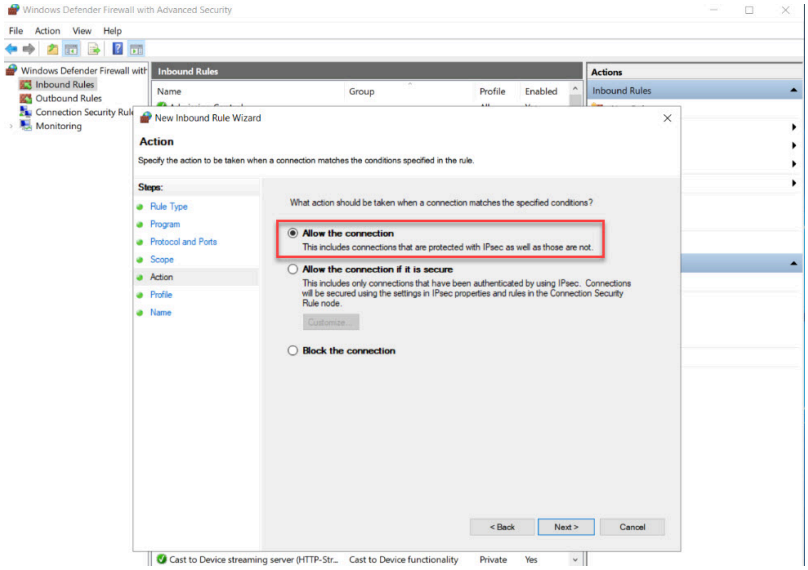
9. To allow tIP addresses, select the radio button next to **These IP addresses** in the **Which remote IP addresses does this rule apply to?** and click **Add**



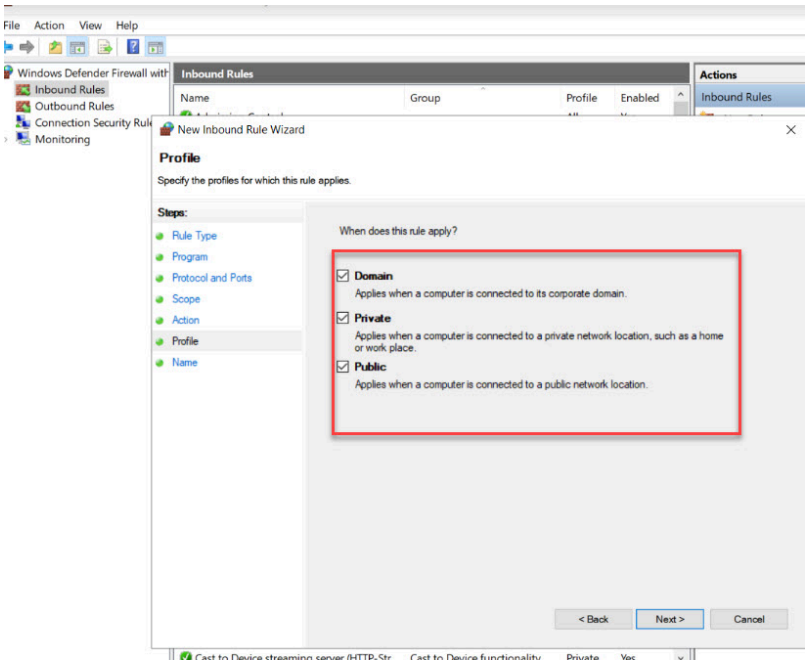
10. Select the This IP address or subnet button and in the text box below it, enter all the IP addresses from which the MiVoice Connect data can be accessed. Click **OK**.



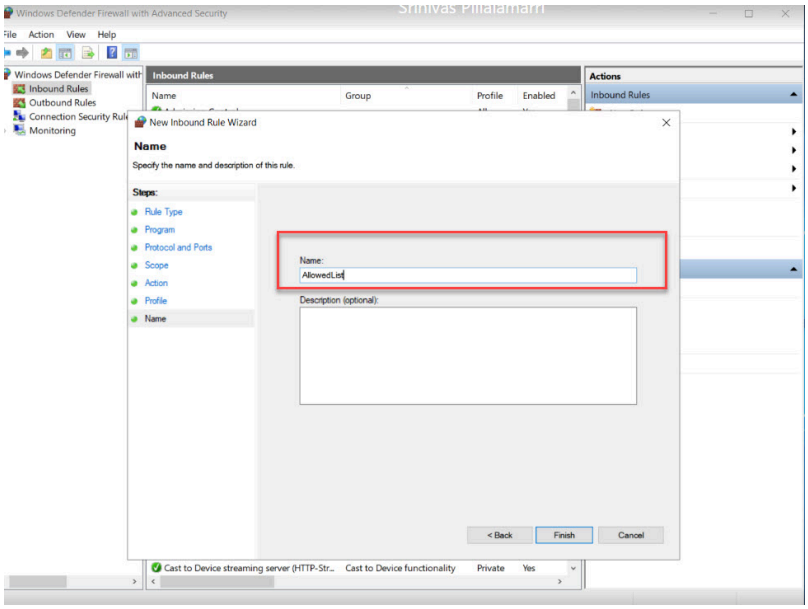
11. Select the radio button **Allow the connection** and click **Next >**.



12. Ensure that **Domain**, **Private**, and **Public** are selected and click **Next >**.



13. Provide a **Name** for the new rule created. You can keep adding IP addresses to this rule. Click **Finish** to complete the procedure.



Note:
This procedure must be repeated for all the three ports - 4308, 4309, and 4310.

Note:
This procedure is applicable for Windows devices (WDVS and HQ servers). If DDB is enabled and the WDVS is running a DDB service, then the rules set by this procedure in WDVS apply only for port 4308.

Procedure to be followed to white-list the LDVS

Following is the procedure to be followed on Linux devices (LDVS) to add firewall rules to block traffic from unknown sources by adding IP addresses to an allowed list.

Note:
Follow the procedure for LDVS only if DDB is enabled and the LDVS is a running DDB service.

1. Create an appropriate zone name to allow access to the MySQL database server.
2. Reload the **firewalld** settings to apply the change.

Note:
If you skip this step, you may get an error when you try to use the new zone name. The new zone should appear in the list of zones.

3. Enter the source IP address and the port number to open on the local server.
4. Reload the **firewalld** settings to get the new changes. Alternatively, you can allow traffic from the entire network to access a service or a port.

For more information, seehere.

Network Requirements and Preparation

5

This chapter contains the following sections:

This chapter describes the network requirements and preparation needed to use the MiVoice Connect system.

5.1 Overview

The MiVoice Connect system is an IP-based voice solution deployed across your IP network. This allows the components of the system to be located anywhere on your IP network, resulting in a single system for all your voice applications at all locations. This single system approach significantly reduces the complexity associated with legacy systems that consist of multiple PBXs, multiple voice mail systems, multiple auto-attendants, and multiple automatic call distribution systems, each with their unique management interfaces.

Because the MiVoice Connect system becomes another application on your IP network, it is important to understand how the system integrates with your data network. As you migrate your network to include voice as another application across your wide area network, it becomes necessary for your IP LAN and WAN to provide a network that meets the requirements for toll-quality voice. The ability of your network to deliver this performance will vary based on the number of simultaneous calls between locations, the voice quality required, and the other application traffic on the network. Some of the key considerations are:

- Bandwidth
- Latency
- Jitter
- Quality of service

5.2 Understanding Network Requirements for Toll-Quality Voice

The MiVoice Connect system is designed to deliver the highest possible voice quality. To ensure high quality voice transmissions, you must be sure that the entire network on which you deploy the MiVoice Connect telephony system is able to provide toll-quality voice communications throughout. Both LAN and WAN links must be adequately constructed to ensure the fluid transmission of time- and order-sensitive voice packets.

This section provides you with the background to understand the factors involved in engineering an IP network that is ready for voice communications.

5.2.1 General Network Requirements

When your voice traffic travels across your IP network, you must ensure that your network does all of the following:

- Delivers enough bandwidth
- Meets the following data network design universal quality standards to support VoIP:
  - **Latency**. No part of the VoIP data network infrastructure should have more than 150 ms, one-way (or 300 ms round-trip) propagation delay between any two VoIP end-points, servers, or switches.
  - **Jitter**. No more than 50 ms of spacing between VoIP media packets
  - **Loss**. No more than 1% of packet loss for VoIP RTP media stream packets. (No standard has been set to measure signaling loss, but while RTP is primarily time-sensitive, signaling is primarily drop-sensitive.)

You also must prioritize your voice traffic over your data traffic and configure the MiVoice Connect system's Admission Control feature.

In general, to ensure voice quality on the LAN, the MiVoice Connect system must be used in a switched Ethernet network. To ensure voice quality on the WAN, the MiVoice Connect system requires that you do the following:

- Get a service-level agreement (SLA) from your WAN service provider that guarantees prioritization of voice traffic: A WAN circuit that can prioritize traffic using QoS like MPLS is highly preferred. At least three queues for the provider to prioritize traffic are recommended:
  - a priority queue for RTP traffic
  - a medium priority queue for call-control traffic
  - a default-low priority queue for all other traffic
- Prioritize your voice traffic ahead of your data traffic on network routers
- Set the admission control feature to ensure that the voice traffic does not flood the WAN links.

Other general network requirements are as follows:

- Create separate VLANs for VOICE and DATA as well as any other types of traffic that may need to be segregated similarly to enhance data network performance on a LAN.

- Trunk all voice and data VLANs on layer-2 switches across LAN uplinks to the site's layer-3 core switch or router.
- In most cases, avoid trunking any LAN VLANs, particularly for voice, across WAN links to/from other sites.
- Each site will have its own set of voice and data VLANs with separate IP addressing per VLAN at each site.
- When using a single LAN switch for a site, ensure the switch supports both layer-2 and layer-3 routing functionality enabled to route IP traffic between local VLANs.
- When using multiple LAN switches for a site, ensure at least one “core” data switch has layer-3 IP routing functionality enabled to route IP traffic between local VLANs on all local layer-2 switches.
- Use a “hub and spoke” LAN topology where all layer-2 access level switches are the spokes connected through uplinks to the common “core” layer-3 switch.
- Use a WAN topology where all remote sites' layer-3 switch or router uses a WAN point-to-point uplink to the hub or point-to-multi-point uplink to all sites.
- Connect all ShoreGear switches and servers at a given site directly to the layer-3 data switch and only assign the local Voice VLAN as an untagged VLAN port for each.
- Use a separate /30 point-to-point VLAN to address each uplink/downlink to a remote site or to a firewall from the hub site's layer-3 switch.

With these items taken into consideration, you can simply and easily achieve toll-quality voice using the MiVoice Connect system.

The MiVoice Connect system is designed to work in multi-vendor network environments and, therefore, leverages Quality of Services (QoS) standards, including the following, to ensure voice prioritization:

- Layer 2 IP Precedence (802.1p and 802.1q) (CoS applies within a VLAN and DSCP applies between VLANs in both LAN and WAN environments.)
- Layer 3 Differentiated Services Code Point (DiffServ/ToS)

The benefits of placing data and voice traffic in separate VLANs and QoS strategies include:

- The number of Ethernet switches required in the network is reduced.
- Broadcast packets from the data network are not sent to the MiVoice Connect network.
- Large data traffic flows do not interfere with more time-sensitive voice traffic.
- Congestion, packet loss, and viruses on the data network will not affect the voice network.

5.2.1.1 Quality of Service Traffic Marking Standard

Mitel recommends the following values for QoS traffic marking:

- RTP Traffic – Expedited Forwarding or PHB-EF, that is, DSCP 46 or 184 (ToS (dec) value2q set on the Call Control Options page in Connect Director)
- Signaling Traffic – Class Selector 3 or PHB-CS3, that is, DSCP 24 or 96 (ToS (dec) value set on the Call Control Options page in Connect Director)

This QoS traffic marking standard is being updated to change the default signaling traffic DSCP value from AF31 to CS3 to better comply with industry standards. However, AF31 will still be supported during the transition period. RTP traffic will continue to be marked with DSCP value EF. Mitel devices mark traffic at layer 3 using the appropriate DSCP value. Switches automatically map the layer 3 DSCP marking down to layer 2 for QoS at layer-2.

In Connect Director, navigate to the Call Control Options page (**Administration** > **Features**> **Call Control** > **Options**) and verify the values for DiffServ /ToS Byte in the Voice Encoding and Quality of Service, Call Control Quality of Service, and Video Quality of Service sections. This value is set automatically for a new installation of MiVoice Connect, but any upgraded system will not be changed and will need to be changed manually when configuring QoS for your data networking environment to comply with the new recommendation.

Note:
The MiVoice Connect equipment marks traffic only at layer 3 (L3) with DSCP, not layer 2 (L2) with COS. The data networking equipment handles mapping the markings from L3 to L2 when needed. RTP traffic should be marked as DSCP 46 (EF), prioritized call control traffic as DSCP 24 (CS3) and all other traffic as DSCP 0. Also, as of Windows Server 2012 R2, DSCP marking calls to Windows are ignored. Therefore, a QoS Policy must be put into place on the server as a local group policy or domain-wide group policy if no other group policies are inherited by the servers.

5.2.1.2 Quality of Service Design Principles

The following QoS design principles are especially important for MiVoice Connect systems:

- Critical applications such as VoIP require service guarantees regardless of network conditions. The only way to provide service guarantees is to enable QoS queuing at any node that has the potential for congestion, regardless of how rarely this might occur.
- If you assign too much traffic for strict priority queuing (that is, EF), beyond voice RTP traffic, then the overall effect is a dampening of QoS functionality.
- Voice media is time-sensitive, and voice signaling is drop-sensitive. Due to different sensitivities, map EF voice media to the strict priority queue, exclusively, and AF31/CS3 signaling to a medium-priority queue. Never map VoIP media and VoIP signaling together in the same queue.
- Allow VoIP endpoints to self-mark QoS values for VoIP traffic and trust throughout the network. Only remark if VoIP traffic is from an untrusted source.
- RTP traffic should always be marked as EF, designated signaling traffic should be marked as CS3, and all other traffic (also called default traffic) should not be marked, while each is mapped to separate queues at each interface through QoS.
- With QoS disabled, all traffic goes through one queue to egress an interface, so prioritization cannot occur. With QoS enabled, multiple queues with separate, reserved packet buffer memory are activated for prioritized classes of traffic to pass through the interface before non-prioritized traffic.
- If VoIP traffic passes any single interface without QoS configured, the effects of quality issues are felt on a call as if no QoS is configured anywhere along the path.
- Congested packet buffer memory, rather than a congested link, is most often the QoS bottleneck.

Consult the manufacturer of your network equipment or an experienced network administrator for detailed instructions on configuring Quality of Service in your specific environment.

5.2.1.3 Impact of Long Network Outages

The MiVoice Connect system is a completely distributed system in which each voice switch provides all call control functionality for inbound and outbound calls, as well as features such as transfer, conference, pickup, and trunk selection. When there is a long network outage, the switches detect the problem and

run isolated from the switches that can no longer be reached. In the MiVoice Connect system, switches communicate every 30 seconds and disconnect when there is no response after 60 seconds.

5.2.1.4 TCP and UDP Port Usage in the MiVoice Connect System

It is imperative that all TCP and UDP ports self-marked with a DSCP (EF for RTP and CS3 for signaling) is reflected accurately. Not all ports are self marked by Mitel.

For information about the ports MiVoice Connect devices and applications use to communicate with other Mitel devices and applications, see the Port Usage appendix in the *MiVoice Connect Maintenance Guide*.

5.2.2 Bandwidth Requirements

The amount of bandwidth required for voice calls depends on these details:

- Number of simultaneous calls
- Voice encoding scheme in use
- Amount of signaling overhead

Within a site, G.722 wideband encoding is recommended because bandwidth in the LAN is inexpensive and readily available. Between sites, G.729a is recommended because it uses the least amount of bandwidth. Linear codecs provide slightly higher voice quality than G.711, but they should not be used if there are any bandwidth concerns.

If you select linear broadband or linear encoding, end points that do not support either codec negotiate for the highest quality codec for both end points, and G.711 is the only high-quality codec shared by all end points. Table: Supported Codecs in the Hardware and Network Requirements on page 432 section provides bandwidth information for different codecs.

5.2.3 Latency

Latency is the amount of time it takes for one person’s voice to be sampled, digitized (or encoded), packetized, sent over the IP network, de-packetized, and replayed to another person. The ITU G.114 Recommendation recommends not more than 150 ms one-way delay, from “mouth-to-ear.” If the latency is too high, it interferes with the natural flow of the conversation, causing the two parties to confuse the latency for pauses in speech. The resulting conversation is reminiscent of international calls over satellite facilities. The maximum latency for phones on an ideal intranet is 130 ms. Networks can inject additional latency if not properly designed. Potential trouble spots to be aware of are routers and wide-area-network interfaces. Care should be taken to ensure that all network congestion points are designed to provide sufficient capacity to ensure low latency throughput.

5.2.4 Jitter for Voice Switches

Jitter is the variation of latency across the network and the variation in packet processing inside the switches. To compensate for jitter, the voice switches and 400-Series and 6900-Series IP (6910, 6920, 6930, 6940, 6920w, 6930w, and 6940w) phones continuously measure the jitter in the system and dynamically change the size of the receive jitter buffers to optimize voice quality.

If the jitter buffer is too small, there can be packet loss from buffer underflows. This occurs when the jitter buffer runs out of valid voice samples. If the jitter buffer is too large, there will be unnecessary latency. Both conditions have a negative impact on voice quality.

The jitter buffer starts at the minimum size of 0 ms as packets from the network are placed into the switchboard queue for immediate processing. When jitter is detected on the network, the jitter buffer dynamically increases in increments of 5 ms to compensate for increased jitter and decreases in reaction to less jitter.

To set the maximum value of jitter buffer:

1. Launch Connect Director.
2. In the navigation pane, click **Administration** > **Features** > **Call Control** > **Options**.
3. In the **Voice encoding and quality of service** section, enter the **maximum inter-site jitter buffer** value.

   The jitter value can range from 20-400 milliseconds. The default value is 300 milliseconds.
4. Click **Save**.

The entered jitter buffer value is saved in the system.

As the jitter increases on the network and the jitter buffer needs to be increased to guarantee timely audio play, the latency of the audio also increases. The system attempts both to maintain a minimum jitter buffer size that provides good-quality voice without dropping packets and to provide minimum latency.

For third-party IP phones that are configured in the MiVoice Connect system, the jitter buffer is not configurable. The minimum jitter buffer is 10 ms, and the maximum is 80 ms.

Maximum jitter buffer values greater than 100 ms should rarely be necessary. If needed, this could indicate a problem in your network that should be addressed in another way. As the jitter buffer depth increases, the latency experienced by the user increases. For this reason, network jitter should be kept to a minimum.

5.2.5 Packet Loss

Lost packets can occur on the IP network for any number of reasons. Packet loss above 1% begins to adversely affect voice quality. To help reduce this problem, voice switches and 400-Series and 6900-Series (6910, 6920, 6930, 6940, 6920w, 6930w, and 6940w) phones have a feature called lost packet concealment. When a packet is lost on the network, the last sample received is replayed to the receiving party at a reduced level. This is repeated until a nominal level is reached, effectively reducing the clicking and popping associated with low levels of packet loss.

Fax and modem calls demand essentially zero packet loss to avoid missing lines on fax calls and to avoid dropped modem calls. In addition, fax and modem calls, when detected, may change to a higher-rate codec.

5.2.6 Bandwidth Management

In addition to the network requirements discussed above, bandwidth management techniques need to be deployed to ensure that real-time voice traffic is not affected by bursts or high amounts of data traffic.

5.2.6.1 Local Area Network (LAN)

To manage bandwidth in the local area network (intrasite) and meet the requirements for toll-quality voice, use Ethernet switching. Ethernet switching is cost effective and simple to provision. Your LAN configuration requirements will vary depending on your infrastructure and whether your network includes IP phones.

IP phones sample the user's voice and convert the voice signal to IP packets using the Real Time Protocol (RTP). These packets must be tagged for higher prioritization in the network. IP phones have embedded Ethernet switches and automatically prioritize voice traffic ahead of any data traffic coming from piggy-backed personal computers (for example, large file transfers and e-mail).

On the local area network, methods to prioritize voice packets include the following:

- IP Precedence – 5 (configurable, recommendation is 5)
- DiffServ/ToS – EF (configurable, recommendation is EF)

The Ethernet switch configuration should prioritize traffic using one of these methods. This allows the voice traffic arriving at the switch to travel ahead of the data traffic.

Customers typically prioritize voice traffic by setting the Differentiated Service (DiffServ) field because this configuration is easy to set up on smart Ethernet switches.

To configure the Differentiated Service (DiffServ) field for Call control quality of service:

1. Launch Connect Director.
2. In the navigation pane, click **Administration** > **Features** > **Call Control** > **Options**.
3. In the **Call control quality of service** section, in the **DiffServ/ToS byte** field enter a value of **96**.
4. Click **Save**.

The differentiated service field value is configured for calls.

Note:

Mitel only self-marks DSCP for certain ports. Mitel does not mark CoS, and the data networking equipment will automatically map the DSCP marking to CoS when needed.

When IP phones are used, the desktop connection to the user's computer and phone must also be part of the switched Ethernet network. The user's phone network port is connected to their home office router (that is, DSL or cable modem router's LAN switch ports) and their PC or laptop is connected to their phone's PC access port on the back of the IP phone, just like in the office. The phone uses its built-in VPN client to automatically connect securely to a VPN Concentrator located in the customer's corporate network to be able to register their IP phone as if it were in the office. The PC or laptop does not have access to the Voice VLAN that the VPN IP phone uses with its VPN client. The phone-connected PC or laptop has access only to the local data network for normal Internet access so voice and data are still on separate virtual networks. While piggy-backed to the phone, the PC or laptop can start its own VPN client to connect separately to the corporate data network without any conflict or issue with the phone.

If an IP phone loses power, a PC connected through the IP phone loses its connection to the network.

Voice quality can be guaranteed by putting each of the voice switches and the server on its own Ethernet switch port. A network with this topology meets the bandwidth, jitter, and latency requirements for toll-quality voice without the additional need for special prioritization of voice packets.

In summary, Mitel leverages the use of VLANs to integrate into the network topology that you, the network administrator, have decided is most appropriate for your LAN topology. Mitel neither requires nor dictates that you use a specific vendor's equipment for your LAN edge, core, WAN, switches, routers, operating systems, and so on, as long as your data hardware supports the minimum recommended requirements.

5.2.7 Virtual LANs

Virtual LANs (that is, VLANs) are a data networking design construct by which more than one logical layer-2 (that is, L2) network subnet can exist on a single physical network segment/switch while also separating layer-2 broadcast domains. In a converged data network containing both voice and data traffic, it is imperative that the voice and data packets are separated into at least two distinct VLANs (that is, a data VLAN and a voice VLAN). Failure to do so will likely result in poor voice quality, packet loss, client-to-server communication interruptions or disconnects, and lost call control/setup traffic during higher network traffic conditions.

Ethernet uses Carrier Sense Multiple Access with Collision Detection protocol (CSMA/CD) to determine when a single Ethernet device on a layer-2 subnet/VLAN can access the media similar to how a polite conversation works where one speaks and everyone else listening does not speak. In a non-switched network, when multiple devices on the subnet need to “speak”, they have to wait their turn until the one speaking or transmitting packets on the subnet is finished. In a switched network, this is less of a problem except for broadcast traffic. Transmitting voice traffic is time sensitive and the media access delay could become too great or too random at times, causing issues with voice. Smaller VLANs also control the quantity of MAC addresses that ARP tables have to store to communicate which is a more limited resource for IP phones. For example at a given site, create a data VLAN for PCs, a voice VLAN for all VoIP devices which should include ShoreGear switches, Mitel servers and all IP phones, create a Wi-Fi VLAN for wireless devices, a Printer VLAN for printers, a Server VLAN for all other servers, and so on.

Segmenting similar layer-2 traffic into separate subnets/VLANs help mitigate propagating unnecessary traffic across too many data switch interfaces resulting in a more congested data network. IP phones and voice switches can be configured on a specific VLAN. Set the voice VLAN for higher prioritization in the network. The Ethernet switch infrastructure needs to be configured to prioritize the voice VLAN. This allows the voice traffic arriving at the switch to travel ahead of the data traffic.

The benefits of placing data and voice traffic in separate VLANs and QoS strategies include:

- Reduction in the number of Ethernet switches required in the network.
- Broadcast packets from the data network are not sent to the voice network.
- Large data traffic flows do not interfere with more time sensitive voice traffic.
- Congestion, packet loss, and viruses on the data network will not affect the voice network.

5.2.8 Wide Area Network

To manage bandwidth in the wide area network, prioritize your voice traffic ahead of your data traffic. You can prioritize based on the voice switch IP address, the MAC address, or the physical port on the Ethernet switch.

You can enable default QoS on all data networking equipment which generally takes care of Layer 2. Layer 3 will need to be manually created and/or applied if generated automatically to any VLANs or interfaces where VoIP traffic will cross and switch or router. Layer 4 ports are added to the layer 3 policy if DSCP markings are not trusted and need to be remarked. See the *MiVoice Connect Maintenance Guide* appendix about ports for TCP and UDP ports that are self-marked by Director.

5.2.9 Client Bandwidth

The Mitel Connect client communicates with the MiVoice Connect server for call information and control, configuration changes, and advanced services such as extension monitoring. Typical Bandwidth Use for Mitel Connect Client provides an estimate of the client bandwidth used for each of the Mitel Connect client applications.

Table 11: Typical Bandwidth Use for Mitel Connect Client

Mitel Connect Client	Bandwidth Use
Phone Only	.2 Kbps
Connect Client	.2 Kbps
Operator Extension Monitor	.2 Kbps + 1.5 Kbps 1.5 Kbps per monitored extension
Workgroup Agent Queue Monitor	.25 Kbps 6.5 Kbps per queued call
Workgroup Supervisor Queue Monitor Agent Monitor	.25 Kbps 6.5 Kbps per queued call 1.5 Kbps per agent

5.2.10 Admission Control in the Wide Area Network

To ensure that voice traffic does not overwhelm your wide area network and degrade voice quality, the MiVoice Connect system has an Admission Control feature. From Connect Director, you can limit the amount of WAN bandwidth used for telephone calls on a per-site basis. For a telephone call to be established between sites, admission control must be met at both sites. If the admission control limit is reached at a site, additional calls cannot be placed to or from the site, thus ensuring the voice quality of calls already in progress. If the user is making an outbound call, the call is automatically routed out of a trunk at the site. When making an extension-to-extension call, the user is informed that there is insufficient network bandwidth to complete the call. The user can try again later or dial the external number of the other user.

If PSTN failover is enabled for a user extension, the user's extension-to-extension calls are automatically routed to the public switched telephone network (PSTN) when there is insufficient bandwidth for an IP phone connection.

5.2.11 Spanning Tree Protocol

Spanning Tree Protocol (STP) is used by Ethernet switches and routers to determine if there are multiple paths on the network between any two endpoints. You must disable STP on any network port that has a voice switch or server connected.

IP phones have different Spanning-Tree command requirements than voice switches or servers. IP phones should have a "port fast" command or mode configured on each data switch port to ensure faster boot times and minimize network issues when powering up IP phones.

To allow faster boot times and fewer network issues when connecting to phones, voice switches, or servers, do the following:

- For Cisco switches, set Spanning Tree to either “portfast” or “rapid spanning tree” mode
- For Juniper switches, set Spanning Tree to “edge” mode
- For HP Procurve switches, set Spanning Tree to “admin-edge-port” mode.

5.2.12 Traffic Shaping to Reduce Bottlenecks

With many applications requiring WAN bandwidth, the need to optimize is increasingly important. This is particularly true for enterprises that want to deploy voice over virtual networks where quality of service and traffic shaping are required. With traffic shaping, it is possible to set policies that determine who or what gets top priority. For example, by prioritizing the various flows of traffic, an administrator can make sure that UDP (voice) traffic gets a higher priority than FTP (file download) traffic.

5.2.13 Echo Cancellation

Echo is a consideration for networks and IP phones.

5.2.13.1 Networks

Echo in a voice communication system is caused by signal reflections generated by the electrical circuits (called hybrids) that convert between two-wire (shared transmit and receive pair) and four-wire circuits (separate transmit and receive pairs). These reflections cause the speaker's voice to be heard in the speaker's ear as delayed by many milliseconds. Echo is present even in the traditional circuit-switched telephone network, but because the delay in a local circuit-switched call is so low, the echo is not perceivable. On a packet-based voice network, there is more delay, and the speaker may perceive the echo if it is not properly canceled.

The DSP software on voice switches provides dynamic echo cancellation. When a user places an extension-to-trunk call using an analog trunk on a voice switch, the user's voice bounces off the initial four-wire to two-wire conversion in the analog trunk circuit, then off the two-wire to four-wire in the central office, and finally off the called party's telephone. This echo returns from the central office and is canceled by the echo canceler on the trunk port of the voice switch. The echo from the called party's phone, however, is usually canceled or suppressed by the central office. If this echo is not canceled, users might hear themselves talking.

In the opposite direction, the external person's voice bounces off the user's telephone. This echo returns from the telephone and is canceled by the echo canceler on the telephone port of the voice switch. If this echo is not canceled, the external party hears himself or herself talking. This same process of echo cancellation applies to extension-to-extension as well as trunk-to-trunk calls.

Voice switches can cancel echo received up to 16 ms after being sent.

5.2.13.2 IP Phones

Most IP phones supported in MiVoice Connect have hands-free, full-duplex speakerphones with built-in echo cancellation. The IP420/IP420g, however, has a half-duplex speakerphone, and for this reason it is not appropriate for use as a speakerphone in a conference room.

5.3 WAN Technology Choices

Minimum Bandwidth Requirements

The minimum WAN bandwidth required to deploy a voice switch at a site depends on the number of calls expected. With ADPCM, a single call consumes 52 Kbps, and if this call becomes a conference call, another 52 Kbps is needed, yielding a total of 104 Kbps. From a broadband perspective, the first available technology is 128 Kbps (ISDN), which leaves only 24 Kbps for other IP traffic. For teleworking applications, where only a single call is needed, 128 Kbps can be used. For other sites on the voice network, the minimum bandwidth recommended is 384 Kbps.

Various technologies, as shown in IP Connectivity Chart, are available from different service providers to provide IP connectivity between locations.

Table 12: IP Connectivity Chart

Technology	Upstream Bandwidth Kbps	Downstream Bandwidth Kbps	Calls with ADPCM
SGT1	1544	1544	26
MPLS	3000	1024	Varies
SDSL	1544	1544	26
SDSL	1024	1024	17
SDSL	768	768	13
SDSL	512	512	8

Technology	Upstream Bandwidth Kbps	Downstream Bandwidth Kbps	Calls with ADPCM
SDSL	384	384	6
IDSL	144	144	1 call only
ADSL	128	1,000 (varies)	1 call only
Cable	128 (varies)	1,000 (varies)	1 call only
ISDN BRI	128	128	Not supported

Note:

Your bandwidth will vary, based on the WAN overhead for your particular system.

5.3.1 Leased SGT1

Leased SGT1 facilities are the most robust WAN technology available. Leased SGT1s are point-to-point links that inherently meet the network requirements for toll-quality voice because no ISP is involved. Dedicated SGT1s are priced on a per-unit distance basis, making this a very cost-effective option over short distances.

5.3.2 MPLS

MPLS protects against last mile failures. If you require more simultaneous calls between your premise network and the Mitel Sky network, as well as better QoS guarantees, a tail on the MPLS network (layer 3) may be dropped into your site and a router will be installed on your network. QOS settings for the MPLS tail into your network is set to provide priority to MiVoice Connect voice traffic.

5.3.3 SDSL

SDSL is considered “business-to-business” DSL in which you can negotiate a service-level agreement with the service provider. SDSL is priced on a flat bandwidth basis, making the price “distance insensitive” and cost-effective over long distances.

Although this is an excellent option, especially moving forward, the use of SDSL is challenging, since the service providers often commit to a Service-Level Agreement (SLA) they cannot fulfill. Many service providers have grown very fast, and the IP network is a patchwork of devices. These service providers are usually geared toward providing bandwidth for typical data applications, and a voice application highlights weaknesses in their network. Only with joint troubleshooting of the service provider's network, using tools such as ping plotters, have we been able to achieve the SLA the service provider promised.

5.3.4 IDSL

IDSL modems, which have an uplink and downlink speed of 144 Kbps, can be considered for teleworking applications. Actual performance varies based on your service provider and your applications.

5.3.5 ADSL

ADSL modems, which have an uplink speed of 128 Kbps, can be considered for teleworking applications. Actual performance varies based on your service provider and your applications.

5.3.6 Cable Modems

Cable modems, which can have an uplink speed of 128 Kbps, can be considered for teleworking applications. Actual performance varies based on your service provider and your applications.

5.3.7 ISDN BRI

ISDN BRI modems, which have an uplink speed of 128 Kbps, can be considered for teleworking applications. Actual performance varies based on your service provider and your applications.

5.3.8 Dial-Up Modems

Because of their inherent latency and low bandwidth, dial-up modems are not supported.

5.4 IP Address Assignment

Each voice switch must have an IP address, and each server must have a static IP address. Use one of the following ways to assign an IP address to a voice switch:

- DHCP on a network server. IP phones and PCs get their assigned IP address and other networking configuration information dynamically from a network DHCP server. This saves administrators a considerable amount of work from having to manually configure every IP phone or PC on their data network individually, especially when network parameters change across the entire network environment. DHCP is not supported on the MiVoice Connect servers.
- The maintenance port on the front of the voice switch. For information about the location of the maintenance port on the switch, see Overview on page 333 for all switch models or refer to the quick install guide for a specific voice switch model.

If a voice switch has been configured to request a dynamic IP address, it puts a DHCP request on the network when powered on. If the voice switch receives a response, it uses the new IP address. If no

response is received, it reverts to the previous IP address. If there is no previous IP address, the voice switch continues trying to get an IP address.

If the network has a DHCP server, it is recommended that you reserve IP addresses so that the IP addresses of the voice switches do not dynamically change.

The maintenance port is for configuring the networking parameters.

The following recommendations can assist with the assignment of IP addresses:

- Ensure that only one DHCP server is on the network. Multiple DHCP servers can unexpectedly change IP addresses and disrupt operation of voice switches.
- The MiVoice Connect system must be on a private network in some situations and on a public network in other situations. For example:
  - If the enterprise is using a firewall with Network Address Translation (NAT), all remote facilities must establish VPN connections to headquarters and be on the same private network.
  - If the enterprise is using firewalls but not NAT, all remote locations must use public IP addresses.
- Each IP phone must have a unique IP address. You can configure the IP phone through DHCP or manually on the phone.
- Phones at different sites must be configured on different subnets or assigned from different address ranges so that the MiVoice Connect system can properly assign the voice switch for the IP telephone site.
- To ensure proper operation of VPN phones, remote or home networks must be configured with an IP address range that is different from the IP address range of the MiVoice Connect system's subnet in the corporate network. Ensuring that subnets do not overlap prevents issues with provisioning VPN phones or assigning users' extensions to VPN phones. For this reason, Mitel recommends that when configuring the MiVoice Connect system's subnet you select an IP address range that is not commonly used. Similarly, the IP address of the domain name server (DNS) provided to VPN phones should not overlap with common IP address ranges for remote or home networks' subnets.

5.5 Configuring DHCP for IP Phones

The MiVoice Connect server provides the latest application software and configuration information to the system's IP phones. To receive this information, the IP phone must have the server's IP address. The configuration task in this section is for specifying the IP address and other necessary information.

Note:
For information about DHCP settings for the 400-Series and 6900-Series (6910, 6920, 6930, 6940, 6920w, 6930w, and 6940w) phones, see the *MiVoice Connect Maintenance Guide*.

The phone receives the necessary information through a vendor-specific DHCP option. IP phones have a built-in configuration to seek the MiVoice Connect server's address as Vendor Specific DHCP option 156. If these options are not available, the IP phones use option 66. IP phones that support DHCP option 156 are models IP110, IP115, IP212k, IP230, IP230g, IP265, IP420, IP420g, IP480, IP480g, IP485g, IP560, IP560g, and IP655.

Note:

The IP Phone 8000 does not support option 156 for this application.

The configuration task in this section involves a number for the country of the network or subnet where the phones reside. If necessary, find the number for a country in Country Numbers for DHCP Option 156.

If your network has separate subnets, be sure to select the correct subnet. For example, if a multi-national organization needs the DHCP server to deliver Spanish tones and cadences to the IP phones in an office in Spain, specify the subnet for that office. Without this specification, all phones that boot from this DHCP server receive Spanish tones and cadences.

Another value for the configuration task is a number that points to a language by its country. Although this number refers to a language, it is bound to a country, not a language. For this reason, some countries with different languages have the same language number in the configuration of DHCP option 156. The Language Numbers by Country for DHCP Option 156 lists the language numbers. (As the Language Numbers by Country for DHCP Option 156 shows, language number 4 is a good example.) Selecting the correct language code ensures that the phone shows text in the desired language. Examples of this text are abbreviations for days and months and messages indicating that a requested service is unavailable.

Note:

400-Series and 6900-Series (6910, 6920, 6930, 6940, 6920w, 6930w, and 6940w) phones do not use the language or country parameters in DHCP Option 156. Instead, these phones obtain country and language settings from Connect Director as follows:

- The country is determined by the Country parameter on the Sites page.
- For an Available phone, the language is determined by the Language parameter on the Sites page. For an assigned phone, the language is determined by the Language parameter on the Users page.

To configure DHCP Option 156 on a Microsoft DHCP Server for IP110, IP115, IP212k, IP230, IP230g, IP265, IP560, IP560g, and IP655 phone models:

1. Open DHCP Manager on the Microsoft DHCP server.
2. Right-click the DHCP server, and then select **Set pre-defined** options.
3. Click **Add**.
4. Set **Name** to **IP Phone Boot Server**.
5. Set **Data Type** to **String**.
6. Set **Code**to **156** and add a description, if desired.
7. Navigate to the **scope** options and add option **156**.

8. Type the values for option **156** with the following syntax:

```
ftpservers=ip_address, country=n, language=n, layer2tagging=n, vlanid=n
```

Where

- *ip_address* is the IP address of the MiVoice Connect Headquarters server.
- *n* in *country=n* corresponds to the country number in Country Numbers for DHCP Option 156.
- *n* in *language=n* corresponds to the language number in Language Numbers by Country for DHCP Option 156.

For example, the following syntax specifies Germany as the country and German as the language:

```
FtpServers=192.168.0.13, country=5, language=3 layer2tagging=1, vlanid=10
```

Note:

It is possible to configure two FTP servers for option 156. Each parameter is enclosed in quotes, and separated by commas. For example, you can configure two FTP servers as follows:

```
“ftpservers = “192.168.0.13, 192.168.0.23”
```

Table 13: Country Numbers for DHCP Option 156

Number	Country
1	United States of America
2	Canada
3	France
4	Italy
5	Germany
6	Spain

Number	Country
7	United Kingdom
8	Australia
9	Hong Kong
10	Malaysia
11	Singapore
12	Brazil
13	Netherlands
14	New Zealand
15	Portugal
16	Ireland
17	Belgium
18	Mexico
19	Denmark
20	Sweden
21	Switzerland
22	Austria
23	India

Number	Country
24	China
25	Norway
26	United Arab Emirates
28	Japan
29	Taiwan
30	South Korea
31	Luxembourg
32	Finland
33	Philippines
34	Thailand
35	Poland
36	Czech Republic
37	South Africa
38	Costa Rica
39	Greece
41	Monaco (France)
42	Israel

Number	Country
44	Indonesia
46	Hungary
48	Fiji
49	Mongolia

Table 14: Language Numbers by Country for DHCP Option 156

Number	Country
1	U.S., Canada, Mongolia, Philippines, Thailand
2	Spain (CALA)
3	Germany, Austria
4	English (UK), Czech Republic, Ireland, Malaysia, Greece, Hong Kong, New Zealand, Poland, India, Romania, Singapore, South Africa, United Arab Emirates, Indonesia, Finland
5	France (Parisian), Belgium, Luxembourg, Switzerland, Monaco (France)
6	Netherlands
7	Mexico, Cost Rica, Chile
8	Denmark
9	Italy
10	Sweden

Number	Country
11	China
12	Norway, Finland
13	Brazil (Portuguese)
14	Japan
15	South Korea
17	Taiwan (Mandarin)
18	Portugal
22	Bulgaria
23	Australia, Fiji

5.6 Configuring Automatic VLAN Assignment Using DHCP

You can configure an IP phone to automatically determine its VLAN ID through DHCP. When the phone boots for the first time, it acquires an IP address via DHCP similar to any other network device. However, the DHCP response also specifies (using a proprietary DHCP option) the VLAN ID for the phone to use. The phone then releases the IP address originally assigned to it and reboots. After the phone reboots, all packets are tagged with the VLAN ID specified in the original DHCP response.

The Automatic VLAN Assignment feature is configured on the DHCP server rather than through Connect Director.

5.6.1 Configuring Automatic VLAN Assignment on a DHCP Server

1. Open DHCP Manager on your Microsoft DHCP server.
2. Right-click the **DHCP server** and select **Set pre-defined** options.
3. Click **Add**.
4. Set **Name** to **IP Phone Boot Server**.

5. Set **Data Type** to **String**.
6. Set **Code** to **156** and add a description, if desired.
7. Navigate to the scope options and add option **156**.
8. Set the value of option 156 as follows:

```
tpservers=ip_address, layer2tagging=n, vlanid=x
```

f

Where

- *ip_address* is the IP address of the MiVoice Connect Headquarters server.
- *n* in *layer2tagging=n* is *0* (to disable 802.1Q) or 1 (to enable 802.1Q). The default is 0.
- *x* in *vlanid=x* corresponds to a VLAN ID number between 0 and 4094 when 802.1Q is enabled. The default is 0.

For example, the following would enable VLAN tagging using a VLAN ID of 10:

```
FtpServers=192.168.0.13, Layer2Tagging=1, vlanid=10
```

5.6.2 Configuring Automatic VLAN - IP Phone Standard Boot Process

The configuration of Automatic VLAN Assignment using DHCP during IP phone standard boot Process is done as follows:

1. As the IP Phone powers up, a DHCP request is sent to the data network on the default, untagged VLAN.
2. The DHCP Server is on the same VLAN as the phone and replies back with the Option 156 information configured on the untagged Data VLAN DHCP Scope redirecting to the Voice VLAN ID 20.
3. Upon receipt of this information, the IP phone immediately resets and releases its Data VLAN IP address. The IP phone display briefly shows “Redirecting Network”.
4. The IP Phone sends a second DHCP request but this time to the Voice VLAN 20 DHCP Scope.
5. The L3 data switch receives this request on the Voice VLAN and forwards it, through the “IP helper address” 10.10.10.10 to the DHCP server and the Data VLAN.
6. The DHCP server replies to the IP phone with a new IP address from the Voice VLAN DHCP Scope Address Pool as well as its Option 156 network settings and other scope options.
7. The DHCP server replies to the IP phone with a new IP address from the Voice VLAN DHCP Scope Address Pool as well as its Option 156 network settings and other scope options.
8. The Phone registers successfully and is ready for service.

5.7 Configuring Automatic VLAN Assignment Using LLDP

LLDP (IEEE 802.1AB) is a vendor agnostic Layer 2 protocol designed to be used by network devices for advertising their identity, capabilities, and neighbors on a IEEE 802 Ethernet LAN. LLDP performs similar functions as several proprietary protocols such as the Cisco Discovery Protocol (CDP), Extreme Discovery Protocol, Nortel Discovery Protocol and Microsoft's Link Layer Topology Discovery. An enhancement to LLDP is LLDP-MED, Link Layer Discovery Protocol-Media Endpoint Discovery. LLDP eliminates the phone from using the untagged Data VLAN and allows only one DHCP request directly on the Voice VLAN.

5.7.1 Configuring VLAN Assignment Using LLDP-MED - IP Phone Boot

The configuration of Automatic VLAN Assignment Using LLDP-MED during the IP phone standard boot process is done as follows:

1. As the phone powers up, the Ethernet switch sends LLDP Data Units defined as LLDP_Multicast packets to the Phone.
2. The Phone responds in kind adding TIA Organizationally Specific LLDP-MED TLV's such as "TIA - Network Policy" with "VLAN Id: 0" among many other TLV extensions. "VLAN Id: 0" is the request the phone asking the Ethernet switch for the Voice VLAN ID as well as L2 Priority, DSCP value, and so on.
3. The Ethernet switch in turn responds to the phone with the same TIA LLDP-MED TLV extensions and in the "TIA - Network Policy" TLV, the designated VLAN Id of the Voice VLAN is offered to the phone (for example, VLAN Id: 50).
4. The Phone performs a typical DHCP sequence of Discover, Offer, Request, Ack to get an IP address plus available DHCP Options from the Voice VLAN.
5. The Phone downloads its configuration file through FTP or HTTPS , upgrades the Boot Image and other required files as needed, and finally reboots.
6. The Phone registers successfully and is ready for service.

5.8 Time Services

For IP phones, time services must be available to provide the telephone's date and time display. This requires a server that supports Simple Network Time Protocol (SNTP).

If an organization does not have an NTP server, it can use a publicly accessible time server. For information about publicly accessible time servers, see http://support.ntp.org/bin/view/Servers/WebHome.

The DHCP server sends SNTP server information to 100-, 200-, 500-, and 600-Series IP phones.

The 400-Series and 6900-Series (6910, 6920, 6930, 6940, 6920w, 6930w, and 6940w) phones depend on a Network Time Protocol (NTP) server to authenticate a secure connection and to provide the date and time to be displayed on for the phone's screen. The time displayed on the phone is the GMT value provided by the NTP server plus the offset from the time zone setting of the phone. On the IP480, IP480g, and IP485g phone models, users can change the time zone from the default value through the **Options** menu on the phone.

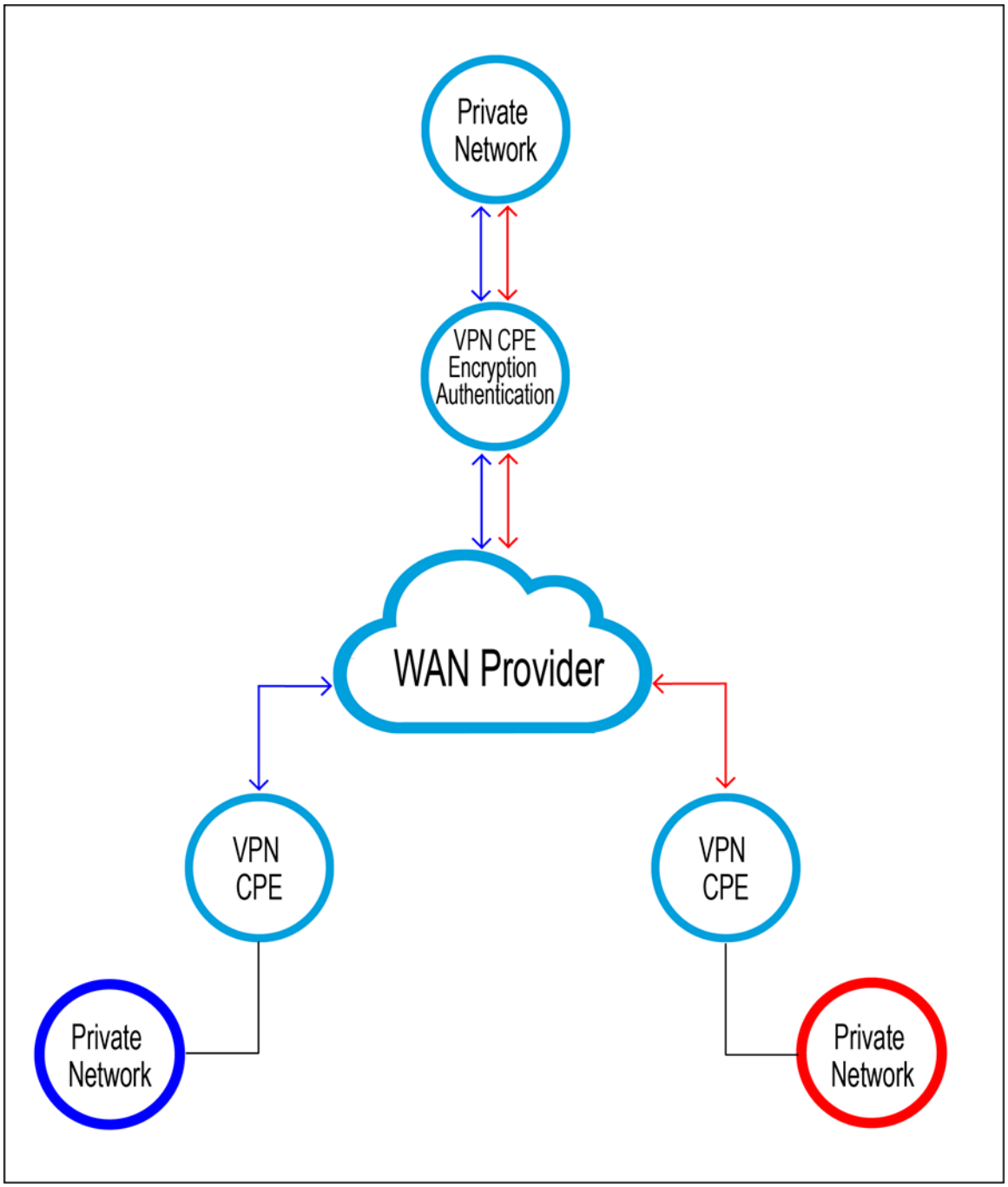
Note:
For 6900-Series (6910, 6920, 6930, 6940, 6920w, 6930w, and 6940w) phones, NTP server settings must be specified in Option 42 in the DHCP client for successful phone registration.

5.9 Virtual Private Network (VPN)

Internet Protocol Virtual Private Networks (IP VPNs) are often the secure access of choice. IP VPNs establish secure communications between employees, branches, or partners by using strong IP-based encryption and authentication techniques for transport security over the public Internet.

IP VPNs are typically viewed as falling into three major categories: remote access VPNs, intranets (company site-to-site), and extranets (business-to-business). These services are used by companies of all sizes because of the powerful combination of high-speed access links and public networks. An example is the use of high-speed, low-cost broadband DSL connectivity to enable teleworkers or branch offices to link securely with the company network via the Internet, as if they were accessing the LAN, including all network applications, at the office. A sample VPN configuration is shown in the figure below.

Figure 2: VPN Topology



IP VPNs can be provided through hardware or software solutions located at the remote facility (branch office or teleworker's home) and the customer premises. These devices or solutions use technologies such as tunneling, encryption, and authentication to guarantee secure communications across a public infrastructure.

All the components of your MiVoice Connect system must exist in the same enterprise private network. VPNs can be used to bridge your private networks across the Internet so that the networks for two buildings are both part of the same private network. For multiple locations that share a private network, bandwidth calculations should include the effective bandwidth inside the private network, rather than the raw bandwidth.

5.9.1 Tunneling

Tunneling encapsulates one type of data packet into the packet of another protocol. Multiple tunneling protocols are used today on the market:

- **Point-to-Point Tunneling Protocol (PPTP):** PPTP includes compression and encryption techniques. This protocol was introduced by Microsoft to support secure dial-up access for its desktop, which corresponds to a large share of the desktop market.
- **Layer 2 Forwarding (L2F):** Introduced by Cisco Systems, L2F was primarily used to tunnel traffic between two Cisco routers. It also allows IPX traffic to tunnel over an IP WAN.
- **Layer 2 Tunneling Protocol (L2TP):** L2TP is an extension the PPP (Point-to-Point Protocol) that merges the best features of L2F and PPTP. L2TP is an emerging IETF (Internet Engineering Task Force) standard.
- **IPSEC:** This is a collection of security protocols from the Security Working Group of the IETF. It provides ESP (Encapsulating Security Payload), AH (Authentication Header), and IKE (Key Exchange Protocol) support. This protocol, mature but still technically in a draft format, is currently considered the standard for encryption and tunneling support in VPNs.

For PPTP, IP VPN tunneling adds another dimension to the tunneling. Before encapsulation takes place, the packets are encrypted so that the data is unreadable to outsiders. Once the encapsulated packets reach their destination, the encapsulation headers are separated, and packets are decrypted and returned to their original format.

The L2TP tunneling protocol does not encrypt before encapsulation. It requires the IPSEC protocol to take the encapsulated packet and encrypt it before sending it over the Internet.

5.9.2 Performance

In the context of an IP VPN's performance, encryption can be a CPU-intensive operation. Therefore, an enterprise must answer two questions about encryption when it evaluates VPN products:

- With encryption, does the maximum throughput substantially decrease?
- With encryption, can the network have a consistent level of throughput?

Typically, a business considers the tradeoffs between performance, price, and the characteristics of software-based and hardware-based encryption.

Note:

Although a VPN is useful for data, for VoIP a VPN might not offer enough protection against latency and packet loss.

5.9.3 Integrated Security Appliances

A number of major vendors provide integrated broadband security appliances to eliminate security concerns. These devices use custom ASICs to deliver wire-speed firewall, IPSec VPN, and traffic shaping in an easy-to-deploy, cost-effective solution. Installing a security appliance, such as a NetScreen-5, eliminates the need to deal with complex PC software installations and allows IT to centrally manage the security policies of these remote offices and teleworkers. The firewall protection secures sensitive data at the remote site and can prevent both U-turn attacks and the launching of denial-of-service attacks from these computers. By combining broadband access technologies with an integrated security appliance, enterprises and service providers can safely and securely capitalize on all of the benefits of the broadband Internet.

5.10 Firewalls

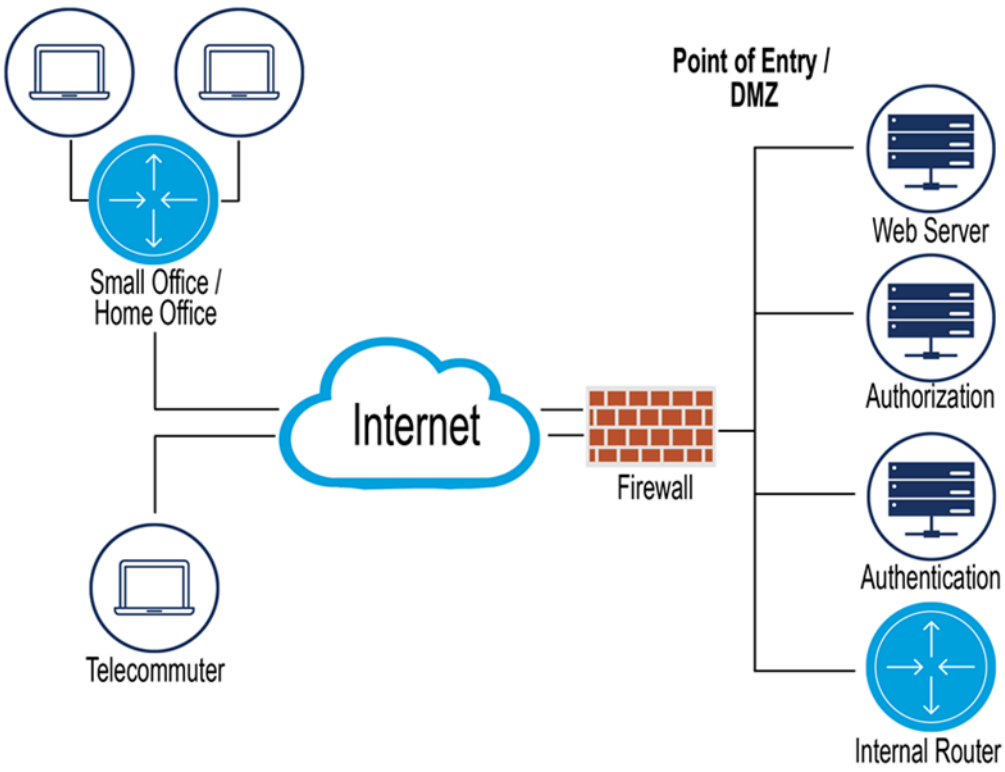
A firewall is the foundation of network security (see the Firewalls figure). It prevents unauthorized access to the network or web site by examining both incoming and outgoing traffic. Based on the predefined security policies, each individual packet is inspected and processed. Any type of traffic deemed “illegal” (based on rules that specify protocol type, source or destination IP address, and so on) is not allowed through the firewall. Using this tool, administrators can achieve tight control over the activities they allow into and out of their corporate network or e-business site. In a corporate network, a firewall prevents intruders from accessing corporate resources while allowing Internet access for employees. In an e-business site, it allows outside access to the web server while preventing unauthorized access or attacks.

Often, a typical network access point, called a DMZ (demilitarized zone), is implemented to offer an “outside” presence for e-commerce clients, e-business partners, and web surfers. The DMZ acts as the gateway through which all Internet communications with the company or site transpire. It allows for controlled access to front-end web servers while protecting mission-critical resources (databases, routers, servers, and so on). Thus, the DMZ needs to be flexible, reliable, and available.

The firewall is often the first line of defense in this environment. Always vigilant, this device must look into all traffic for the site. As part of its duty, the firewall recognizes and deals with denial-of-service attacks, such as TCP SYN flood and Ping of Death. In each of these attacks, the hackers are simply attempting to overwhelm the devices that provide an Internet presence for the company.

With a TCP SYN flood, a stream of TCP SYN packets is sent to the receiving device (often the firewall). The finite memory and size of the TCP entry tables can be overrun by spurious SYN packets, preventing any real users from making a TCP connection required for HTTP communications.

Figure 3: Firewalls



An ICMP flood attack also floods a device, by streaming ICMP echo packets at a recipient destination. This flood of packets requires the device to process and respond to these pings, burning precious resources and preventing other traffic from being serviced. By examining the site's traffic patterns, advanced firewalls can apply logical rules that prevent the device from trying to keep up with the denial-of-service attack traffic. They also prevent this traffic from reaching the valuable web, application, and database servers that create your Internet presence and service your customers.

By using firewalls in conjunction with the DMZ design technique, many businesses and service providers are striving to present as much information without permitting unwanted access to the corporate resources.

One way to keep your mission-critical resources as private as possible, while still allowing for a strong Internet presence, is to use Network Address Translation (NAT). NAT offers the outside world one, or a few, IP addresses. This allows a manager to set up whatever internal IP addressing scheme may be required by corporate policies and business needs. An internal resource's IP address (source IP) is changed as it passes through the NAT function to one of the "outside" IP addresses. Thus, the external world does not know any of the enterprise's internal IP addresses. Only the NAT device presents an IP address that is known, and used by external devices. The NAT device keeps track of these conversations and performs the IP address translation as needed.

Extending the private network of the corporate LAN to remote sites via VPN is a proven method of deploying a MiVoice Connect system across multiple sites. All IP telephony endpoints (such as servers, Voice Switches, and IP telephones) should participate in the same private network, with firewalls between the telephony system equipment and the public Internet. If needed, you can elect to open access to the server to access Connect Director through HTTP using the same precautions you would when exposing any critical web services server to the public network.

Configuring firewalls to function correctly with VoIP traffic is very difficult. Mitel does not recommend deploying MiVoice Connect equipment across firewalls.

5.11 Media Encryption

In addition to using a VPN or a firewall, another method of enhancing the security on your network is to enable media encryption through Connect Director. Media encryption, as the name suggests, encrypts calls between users on a MiVoice Connect system. The encryption scrambles communications between callers so an intruder on the network cannot eavesdrop on the conversation.

For details about media encryption, see the *MiVoice Connect System Administration Guide*.

5.12 Security for 400-Series and 6900-Series IP Phones

400-Series and 6900-Series (6910, 6920, 6930, 6940, 6920w, 6930w, and 6940w) phones use a combination of methods to provide secure communications.

The Headquarters server functions as an X.509 Certificate Authority for the system's public-key infrastructure (PKI). An X.509 certificate is a public key with identifying information, which has been digitally signed through either the associated private key (a self-signed certificate) or a Certificate Authority (CA). The X.509 certificate also includes an expiration date. In addition to the X.509 certificate, the MiVoice Connect system uses Secure Session Initiation Protocol (SIPS), which is SIP plus Transport Layer Security (TLS). This is a standard protocol that uses PKI to establish a secure connection between two entities on an IP network.

The Headquarters server software installation process generates its own self-signed CA certificate when it first boots up. This root certificate uses a 2048-bit RSA key-pair and is valid for 30 years.

IP phones download the Headquarters Certificate Authority X.509 certificate when provisioning into the system. Using that certificate, the phone is able to connect to the voice switches through SIPS, and to the server using HTTPS. The phones also have a pre-installed, unique certificate, signed by Mitel, that allows the voice switches and servers to authenticate the phone.

Note:

The root private keys, which are the basis for securing all connections, are stored in the Headquarters server in `<drive>:/Shoreline Data/keystore`. Because exposure of these private keys could invalidate the security of the system, access to this data must be physically restricted.

The following architecture also ensures system security:

- Access to 400-Series and 6900-Series (6910, 6920, 6930, 6940, 6920w, 6930w, and 6940w) phones is restricted to the Headquarters server and related equipment. The only open in-bound ports are SIP Secure and secure-shell (ssh) ports.

- Call signaling between 400-Series and 6900-Series (6910, 6920, 6930, 6940, 6920w, 6930w, and 6940w) phones and voice switches is encrypted, and participants are authenticated using standards-based security.
- If enabled in Connect Director, voice encryption uses standard SRTP AES-128 encryption. In this case, voice media is encrypted on all calls, with the following exceptions:
  - Media in calls between 400-Series and 6900-Series (6910, 6920, 6930, 6940, 6920w, 6930w, and 6940w) phones and earlier IP phone models is not encrypted.
  - Media in calls that include non-Mitel equipment is not encrypted.
  - Media in calls to softphone and to Windows-based voicemail, auto attendant, workgroups, and account codes is not encrypted.
- For 400-Series and 6900-Series (6910, 6920, 6930, 6940, 6920w, 6930w, and 6940w) phones, Directory, History, visual voicemail, extension assignment, and user preference settings are communicated between the Headquarters server and the phones through Hypertext Transfer Protocol Secure (HTTPS).
- Low-level maintenance access to the 400-Series and 6900-Series (6910, 6920, 6930, 6940, 6920w, 6930w, and 6940w) phone is limited to secure-shell (ssh) access from the Headquarters server (or any server that has a copy of the Headquarters server's private ssh key). Password-based login is not permitted. Logging in to the phone is permitted from some models of the controlling voice switch.

5.13 Session Initiation Protocol (SIP)

Deploying SIP does not involve special network requirements. The general system requirements should be adequate for SIP support. Note the following considerations:

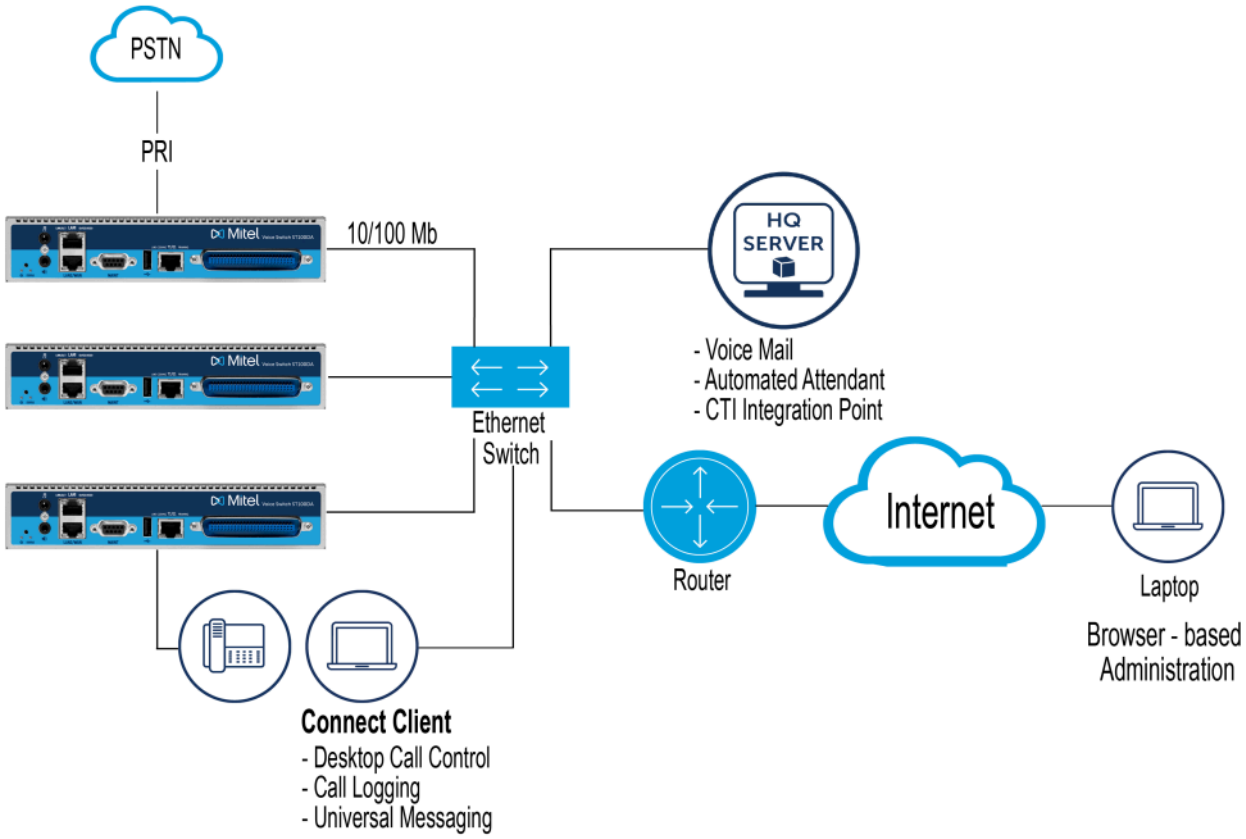
- If third-party SIP devices (SIP phones) have a static configuration, they are supported behind Network Address Translation (NAT).
- To communicate with a SIP device or service provider providing IP trunks over the Internet, the network must be able to pass SIP traffic through a firewall. This requires a SIP application layer gateway, which is a feature provided by some firewall vendors.
- SIP signaling uses TCP and UDP port 5060.
- When using SIP, the RTP port for the voice media stream is dynamic and the SIP endpoints may not always use the same ports to exchange information.

5.14 Example Network Topologies

Single-Site Implementation

The following figure shows an example of a simple, single-site implementation.

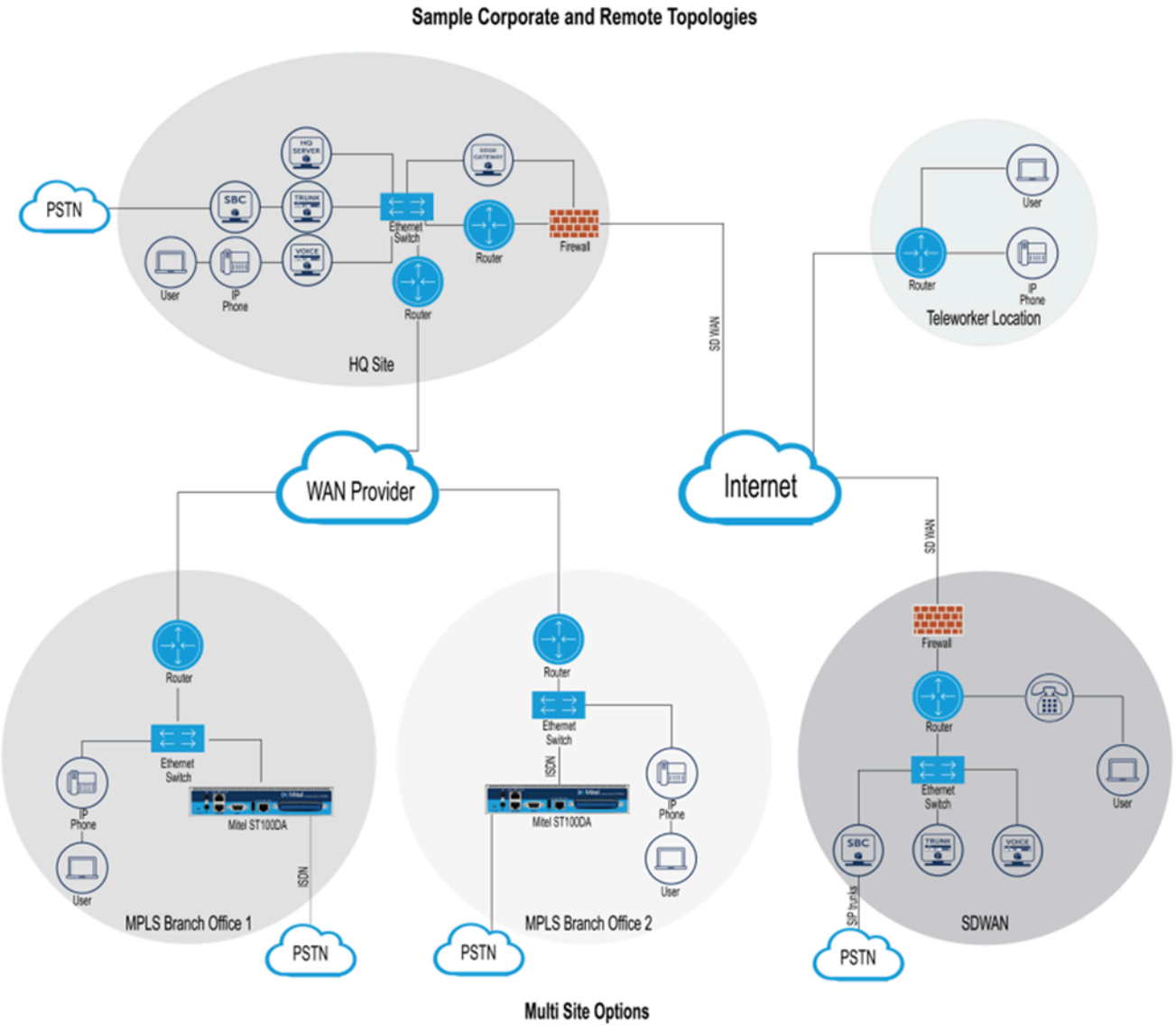
Figure 4: Single-Site



5.14.1 Multi-Site Implementation

The following figure shows an example of a multi-site implementation with various WAN technology choices.

Figure 5: Multi-Site Options



5.15 Computing Admission Control Bandwidth

This section discusses how to compute the admission control bandwidth for the site you are configuring on the Sites page. That is, the appropriate value for the Admission Control Bandwidth parameter. If you want to determine the admission control bandwidth for your site and the information is not available in this section, use one of the following formulas:

- To determine the admission control bandwidth:

  Bandwidth – (# of calls) x (bandwidth/call)

- To determine the number of calls supported with a specific admission control bandwidth value:

  # of calls – (admission control bandwidth) / (bandwidth/call)

MiVoice Connect automatically negotiates the proper voice encoder at call setup. For calls between sites, the call control software requests the voice encoder based on what is selected for intersite voice encoding as defined on the Call Control Options page. The call control software will then make sure both endpoints on the call can support the requested voice encoder.

For instance, for G.729a voice encoding to be used between two sites, the intersite voice encoding must be set to G.729a and the voice switches at each end of the call must be G.729a-capable.

5.15.1 WAN Bandwidth per Call (Full Duplex) without cRTP

Bandwidth Without cRTP lists the bandwidth, including IP overhead, that is used for each voice call between sites when RTP Header Compression (cRTP) is not used. The bandwidth depends on the voice encoding used. For example:

- If you want to support 10 calls between this site and all other sites, and G.729a voice encoding is used, set the **admission control bandwidth** to **260 Kbps**. Before you enter this value, ensure the bandwidth is available at this site.
- If you set the **admission control bandwidth** to **768 Kbps** and G.729a voice encoding is used, you can support up to 29 calls between this site and all other sites.

Mitel recommends that you configure the admission control bandwidth to be less than the bandwidth of the actual WAN link. This provides sufficient bandwidth for call control signaling and other data traffic.

Table 15: Bandwidth Without cRTP

Bandwidth in Kbps per Number of Calls	Linear	G.711	ADPCM	G.729a
1	146	82	52	26
2	292	170	104	52
3	438	255	156	78
4	584	340	208	104
5	730	425	260	130
6	876	510	312	156
7	1022	595	364	182
8	1168	680	416	208

Bandwidth in Kbps per Number of Calls	Linear	G.711	ADPCM	G.729a
9	1314	765	468	234
10	1460	850	520	260
11	1606	935	572	286
12	1752	1020	624	312
13	1898	1105	676	338
14	2044	1190	728	364
15	2190	1275	780	390
16	2336	1360	832	416
17	2482	1445	884	442
18	2628	1530	936	468
19	2774	1615	988	494
20	2920	1700	1040	520
21	3066	1785	1092	546
22	3212	1870	1144	572
23	3358	1955	1196	598
24	3504	2040	1248	624

Bandwidth in Kbps per Number of Calls	Linear	G.711	ADPCM	G.729a
25	3650	2125	1300	650
26	3796	2210	1352	676
27	3942	2295	1404	702
28	4088	2380	1456	728
29	4234	2465	1508	754
30	4380	2550	1560	780

5.15.2 WAN Bandwidth per Call (Full Duplex) with cRTP

Some routers support a feature called RTP Header Compression (cRTP) that significantly reduces the amount of IP overhead associated with voice over IP. Bandwidth With cRTP lists the bandwidth used between sites when cRTP is used. For example:

- If you want to support 10 calls between this site and all other sites, and G.729a voice encoding is used, set the **admission control bandwidth** to **120 Kbps**. Before you enter this value, ensure the bandwidth is available at this site.
- If you set the **admission control bandwidth** to **256 Kbps** and G.729a voice encoding is used, you can support up to 21 calls between this site and all other sites.

Mitel recommends that you configure the admission control bandwidth to be less than the bandwidth of the actual WAN link. This provides sufficient bandwidth for call control signaling and other data traffic.

Table 16: Bandwidth With cRTP

Bandwidth in Kbps per Number of Calls	Linear	G.711	ADPCM	G.729a
1	132	68	38	12
2	264	136	76	24
3	396	204	114	36

Bandwidth in Kbps per Number of Calls	Linear	G.711	ADPCM	G.729a
4	528	272	152	48
5	660	340	190	60
6	792	408	228	72
7	924	476	266	84
8	1056	544	304	96
9	1188	612	342	108
10	1320	680	380	120
11	1452	748	418	132
12	1584	816	456	144
13	1716	884	494	156
14	1848	952	532	168
15	1980	1020	570	180
16	2112	1088	608	192
17	2244	1156	646	204
18	2376	1224	684	216
19	2508	1292	722	228
20	2640	1360	760	240

Bandwidth in Kbps per Number of Calls	Linear	G.711	ADPCM	G.729a
21	2772	1428	798	252
22	2904	1496	836	264
23	3036	1564	874	276
24	3168	1632	912	288
25	3300	1700	950	300
26	3432	1768	988	312
27	3564	1836	1026	324
28	3696	1904	1064	336
29	3828	1972	1102	348
30	3960	2040	1140	360

To set admission control, determine the expected number of simultaneous intrasite calls for a site and multiply this number by the bandwidth required for each call for your selected intersite encoding.

When admission control is set this way, calls routing between sites will be blocked if placing the call would exceed the number of calls supported by the configured bandwidth.

For information about the Admission Control feature, see Admission Control in the Wide Area Network on page 38.

5.15.3 Setting Admission Control

The Admission Control Bandwidth parameters are set on the Sites page of Connect Director. For information on setting these parameters, see the chapter on configuring sites in the *MiVoice Connect System Administration Guide*.

Routing Calls 6

This chapter contains the following sections:

This chapter contains information about identifying the appropriate routing for inbound and outbound calls.

6.1 Overview

The purpose of this chapter is to help with identifying the appropriate routing for inbound and outbound calls. This information is important for determining the requirements for configuration and trunking.

Before installing a voice communications system, one of the most important decisions to make is how to route incoming calls. The voice communications includes the inbound calls to the customer, its individual employees, or a group of employees. The consideration is important for routing calls to their intended destination and also routing calls when they cannot reach their destination. Calls that fail to reach the intended person or group can then go to an auto attendant, operator, off-site number, pager, cell phone, or voice mail.

Another consideration is the outbound call routing. Every site has trunks that support outbound and inbound calls, and the outbound calling behavior also needs planning. At least one trunk at a site must also be able to support emergency calls.

For information about other aspects of designing a voice communications network, see Overview on page 9.

Call routing for MiVoice Connect Contact Center is a separate task. This document does not describe Enterprise Contact Center. For more information about the MiVoice Connect Contact Center, refer to the *MiVoice Connect Contact Center Administration Guide*.

6.2 Recommendations

Consider the following recommendations when designing your call flow plan:

- Determine how calls should reach employees and workgroups. You must identify the desired call routing for inbound calls at each site.
- Identify contingencies, such as alternate plans in the event that the receptionist has an unplanned absence, or the physical phone fails. For example, creating hunt groups can ensure an operator is available if the receptionist or workgroup is unavailable.
- Consider the inter-site call flow, such as your operator's or receptionist's role in handling inbound calls, and the role of others who are not physically present at the main site.

- Identify call flow early. Do not wait until the last minute, or try to identify the call flow the day of cut-over.
- Interview the key members of your organization, such as workgroups, operators, assistants, and executives, to determine their individual preferences and needs, and make sure they agree with any decisions that affect their respective areas.
- Create an off-hours call routing plan.

6.3 Hunt Groups

Hunt groups allow you to route calls to a list of extensions. Hunt groups can be accessed through an extension, DID, and/or DNIS. Hunt groups are supported by Voice Switches and remain available even when connectivity to the Headquarters server is lost. A single switch can host up to 8 hunt groups and a maximum of 16 hunt group extensions per switch. A hunt group can be used as the backup destination for an operator or workgroup, so that basic hunting occurs even when the operator or workgroup is not reachable. To maximize reliability, assign hunt groups to a switch close to the majority of the members and/or trunks associated with the hunt group.

Hunt groups can be used for:

- Backup Routing for a workgroup

  Hunt groups can be used when the workgroup server is not reachable because of a network outage or admission control. When the hunt group is set to offer each member a single call at a time, then call offering is similar to a workgroup.

- Hunt Group as a Call Forward Destination

  In a small office where individuals generally receive calls directly, users may want someone in the office to answer calls when they are unable to answer. Hunt groups can provide alternate destinations in this case.

- Distribution of Calls to Backup Operators

  A hunt group can provide backup operators for the primary operator who handles calls to a main company number.

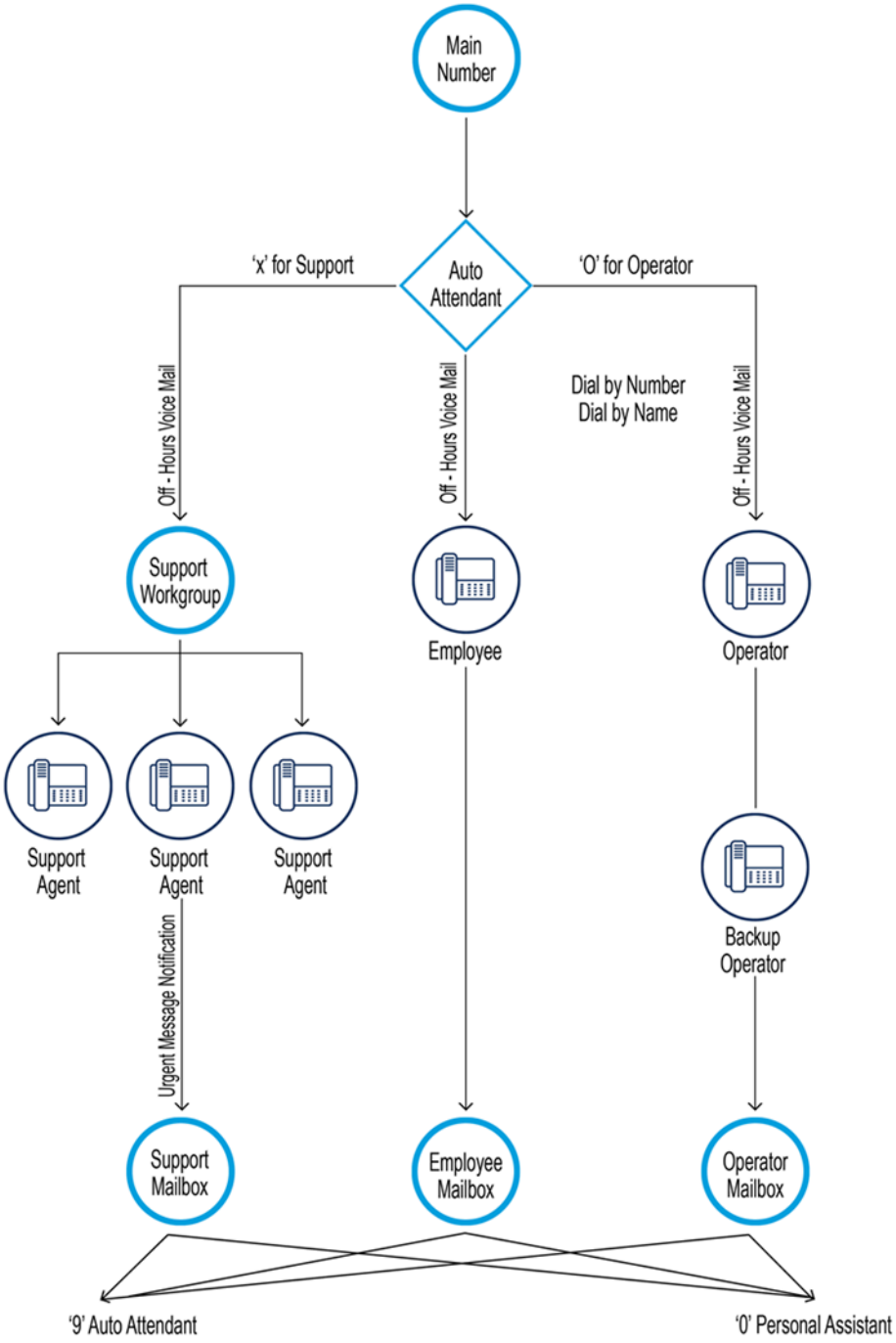
- Common Line Monitoring

  A hunt group can enable users to monitor a phone line. For example, multiple operators can monitor a line and answer calls at the same time.

6.3.1 Direct All Calls to an Auto Attendant

You can direct all inbound calls to the auto attendant, and prompt the calling party to route the call, based on menu options. Auto attendant answering is typically used by smaller companies and smaller locations that do not choose to use direct inward dial (DID) numbers. See Auto Attendant Call Routing for an illustration of auto attendant call flow.

Figure 6: Auto Attendant Call Routing



Organize the auto attendant with options for various departments. In addition, include an out for callers if they must speak to a live attendant or have a rotary telephone. This destination must be one that will always be answered. In many cases, it is a receptionist's extension that is staffed at all times, or a night bell that can be answered by any employee. If you route calls to a receptionist's position that is not always staffed or the receptionist needs to be mobile, consider installing a cordless telephone for the receptionist to wear while roaming around the office. If this is not an option, make sure the receptionist's availability states are set up appropriately.

6.3.1.1 Trunk Considerations

An auto attendant menu can be reached through analog loop-start, digital loop-start, and SGT1/SGE1 PRI trunks by pointing the trunk group at the desired menu. You can also reach a specific menu using DID or DNIS entries received over analog wink-start, digital wink-start, or SGT1/SGE1 PRI trunks.

The MiVoice Connect system supports International Caller ID, Caller ID Name, Caller ID Number, ANI, and DNIS. The Caller ID and trunk group or DNIS information is provided to the user to assist in answering the call.

6.3.1.1.1 Call Routing and Collecting Caller ID Information

The switch delays each inbound loop-start call by 1.5 rings to collect caller ID information before ringing the user's telephone. This allows caller ID information to reach the user's client at the time the call rings the extension, rather than after it rings the extension.

Features available on trunks vary by trunk type. See Understanding Trunk Features on page 86 for more information.

6.3.2 After-Hours Call Routing

For after hours, weekends, and holidays, consider how your call flow will change. Typically, a different prompt is played, since callers are routed directly to voice mail rather than to workgroups or the operator.

6.3.2.1 Example

In the call flow example shown in the figure Direct All Calls to an Auto Attendant on page 67, all calls are received by the auto attendant. The calling party can choose to be directed to one of the following:

- The support workgroup by dialing a digit

  Calls are presented to the support workgroup with a mailbox that provides coverage. The calling party can dial **0** in the mailbox to reach the workgroup assistant, or **9** to return to the auto attendant.

- An employee using Dial by Number or Dial by Name

  Calls are presented to the employee with a mailbox that provides coverage. The calling party can dial **0** in the mailbox to reach the employee's personal assistant, or **9** to return to the auto attendant.

- The operator by dialing the digit 0

  Calls are presented to the operator. If the operator does not answer, a backup operator provides coverage using the operator's availability state. If the backup operator does not answer, a mailbox provides coverage, and the calling party can dial **0** in the mailbox to reach the operator's personal assistant, or **9** to return to the auto attendant.

In this example, the workgroup, users, and operator route calls directly to voice mail after hours.

6.3.3 Direct All Calls to a Live Operator

Some companies choose to answer all inbound calls during business hours with a live operator to give callers a more personal experience. If you use a live operator, the most important thing to remember is that the operator's telephone must always be staffed. Mitel recommends the following:

- Use the Operator Access License, because the standard telephone without this access manages only a single call at a time. When a second call arrives, using the Flash button invokes call waiting, generating a swap hold situation in which calls cannot be transferred. This problem is eliminated when you use the Operator Access License.
- If the organization is a large one, consider using a button box (the BB24 or BB424). A button box provides additional shortcut functions for IP phones with multiple lines. The button box behaves like an additional set of 24 custom buttons that can be used by the operator to quickly and easily route calls to executives and other employees who receive a high volume of phone calls. Phones that support button boxes can be associated with up to four button boxes.
- If the operator does not receive a lot of telephone calls and is required to roam around the office to deliver mail, pick up faxes, make copies, and so on, a two-line cordless telephone can be used. The first line is reserved for incoming calls, while the second line is the operator's personal extension.
- Create hunt groups to ensure someone is always available to take an incoming call.
- You can choose to have calls initially routed to the operator and then forwarded to the auto attendant after a fixed number of rings.

  Operators work in one of two modes:

  - Answer all calls and transfer them to the appropriate destination.
  - Answer all calls and hold them until the parties are found.

If your operator works in the second mode, you should consider installing an overhead paging system or should consider using the Paging Groups feature. Refer to the *MiVoice Connect System Administration Guide* for details about Paging Groups.

The MiVoice Connect system supports single-zone overhead paging on a per-site basis, using the audio output jack on the switches supplied with the jack. When you need multiple-zone paging, please use the online knowledge base at https://www.mitel.com/support to access the application note on paging.

6.3.3.1 Trunk Considerations

The operator can be reached through analog loop-start, digital loop-start, and SGT1/SGE1 PRI trunks by pointing the trunk group directly at the operator. You can also reach the operator using DID or DNIS entries received over analog wink-start, digital wink-start, or SGT1/SGE1 PRI trunks.

The MiVoice Connect system supports International Caller ID, Caller ID Name, Caller ID Number, ANI, and DNIS. The Caller ID and trunk group or DNIS information is provided to the user to assist in answering the call.

Features available on trunks vary by trunk type. See Understanding Trunk Features on page 86 for more information.

6.3.3.2 After-Hours Call Routing

If you route all calls to the operator's extension, auto-attendant scheduling does not apply; only those calls routed to the auto attendant use the schedule. Therefore, if you want to use the off-hours, holiday, and custom schedules, set the operator's availability state to forward all calls to the auto attendant when the operator is unavailable.

6.3.3.2.1 Example

To route calls to a prioritized list of backup operators, create hunt groups with users who can serve as backup operators. In this scenario, a primary operator who handles calls to a main company number requires one or more secondary operators to receive the calls when the primary operator becomes too busy.

Complete the following steps to create a hunt group to back up the primary operator:

1. Create a hunt group with backup operators.
2. Enter the main operator and all the backups as members of the hunt group in the order in which they are to serve as backups.
3. Set the hunt group for multiple calls to be hunted to a given member.
4. Set the call stack size for each of the users to control the number of calls he or she can receive.

When there are incoming calls to the hunt group, the primary operator is offered the calls first. The operator may be offered multiple calls concurrently up to the limit of his or her call stack. If a member's call stack is full, the member is skipped and that particular call is not offered again unless the hunt group is set to hunt forever and no member picks up the call before the member is reached again in the hunt list.

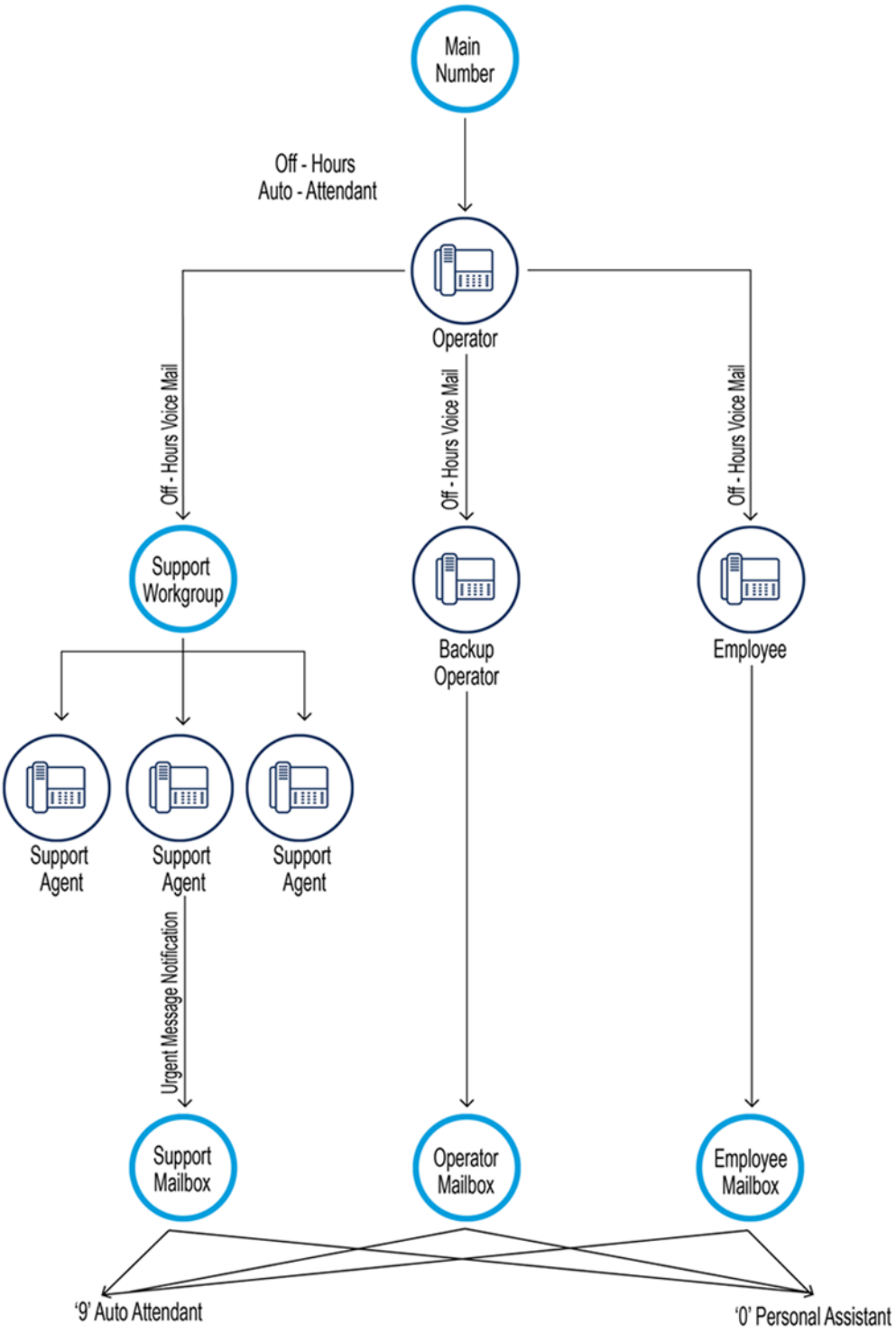
If a member of the operator group does not answer the hunt call, the call is offered to the next member after the number of configured rings. Thus, even if the primary operator has room on his or her call stack, the call is offered to the next member in the list when the operator does not answer the call in time.

For more information on Hunt Groups, refer to Hunt Groups on page 67.

6.3.3.2.2 Example of Operator Call Routing

In the example call flow shown in Operator Call Routing, all calls are received by the operator, who then transfers the calls to the appropriate destination.

Figure 7: Operator Call Routing



- Calls are transferred to the support workgroup with a mailbox that provides coverage.

  The calling party can dial **0** in the mailbox to reach the workgroup assistant, or **9** to return to the auto attendant.

- Calls are transferred to the employees with a mailbox that provides coverage.

  The calling party can dial **0** in the mailbox to reach his or her personal assistant, or **9** to return to the auto attendant.

- If the operator does not answer, a backup operator provides coverage, using the operator's availability state.

  If the backup operator does not answer, a mailbox provides coverage and the calling party can dial **0** in the mailbox to reach the operator's personal assistant, or **9** to return to the auto attendant.

In this example, after-hours call routing is handled by an auto attendant in a very similar fashion to the previous example, which is shown in Auto Attendant Call Routing. To start after-hours call handling, the operator changes his or her availability state. This can be done automatically using Microsoft Outlook Calendar in conjunction with Automated Call Handling, although it does require the operator's personal computer to remain connected with Microsoft Outlook running on it.

6.3.4 Direct All Calls to Extensions

Mitel recommends using Direct Inward Dial (DID) trunks so that callers can dial extensions directly without having to go through the operator. This provides the most efficient, professional call handling experience to your customers.

In the event that an individual is not available, preconfigured availability states route callers. This routing might include a cellular telephone, a pager, an alternate extension, or a personal assistant. Additionally, consider using the voice mail notification capabilities of the MiVoice Connect system when employees are not able to answer the telephone but need to stay in touch.

Even if you choose to direct all calls to extensions, you should still configure the auto attendant for Dial by Number, Dial by Name, and zero out to an operator.

6.3.4.1 Trunk Considerations

When using Direct Inward Dial, you must use analog wink-start, digital wink-start, SIP or SGT1/SGE1 PRI trunks. The MiVoice Connect system can receive Automatic Number Identification (ANI) over analog and digital wink-start trunks as well as Caller ID Number over SGT1/SGE1 PRI.

Features available on trunks vary by trunk type. See Understanding Trunk Features on page 86 for more information.

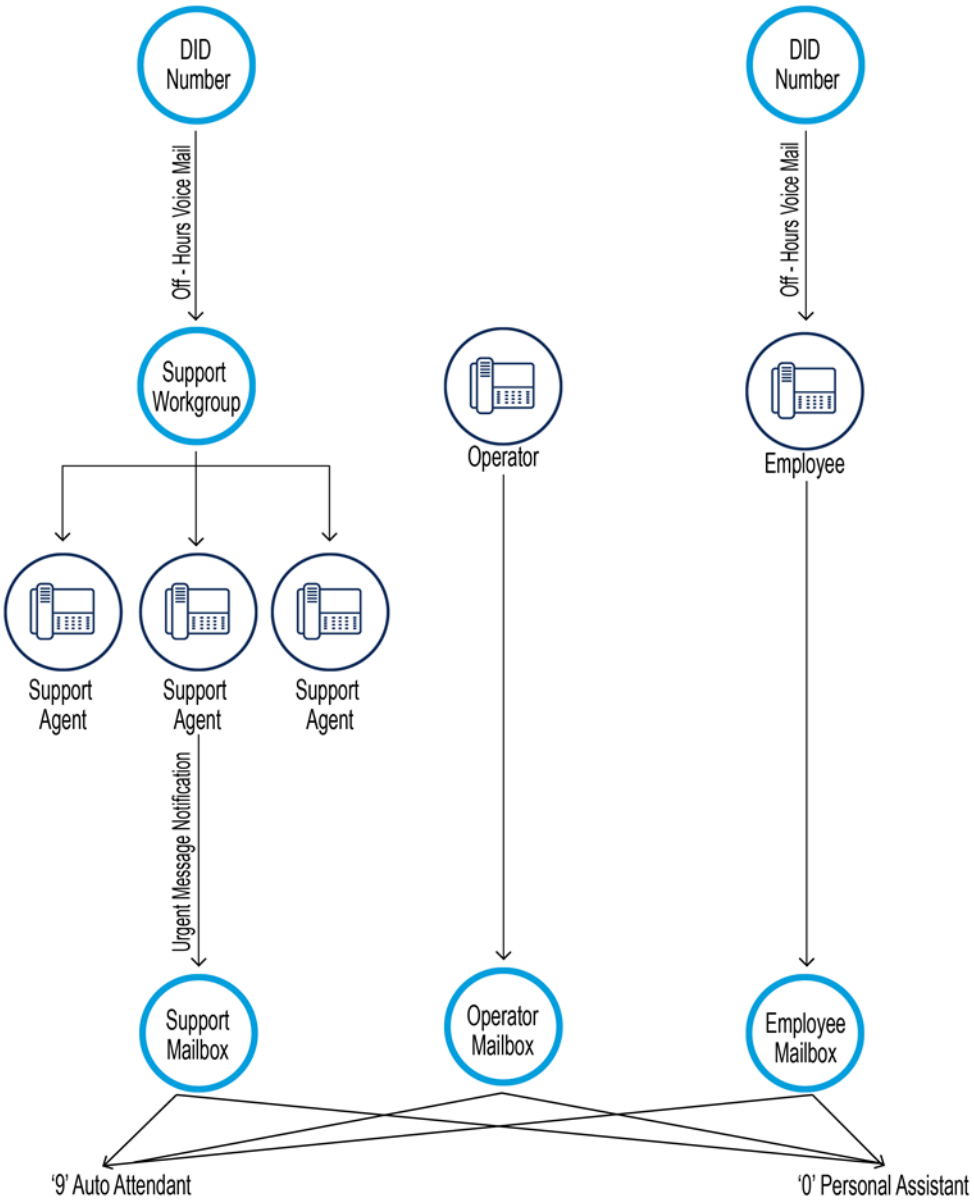
6.3.4.2 After-Hours Call Routing

By routing all calls to the individual extensions, each individual user and workgroup defines its after-hours call handling.

6.3.4.2.1 Example of Direct Inward Dial Call Routing

In the illustration shown in Direct Inward Dial Call Routing, all calls are received by workgroups or by individuals.

Figure 8: Direct Inward Dial Call Routing



- Calls are routed directly to the support workgroup with a mailbox that provides coverage.

  The calling party can dial **0** in the mailbox to reach the workgroup assistant or **9** to return to the auto attendant.

- Calls are routed directly to the employees with a mailbox that provides coverage.

  The calling party can dial **0** in the mailbox to reach his or her personal assistant, or **9** to return to the auto attendant.

- An operator provides limited call handling functions from individual mailboxes or the auto attendant.

In this example, after-hours call routing is received by the workgroups and individual employees.

6.4 Blended Call Routing

Communication systems typically use a mix of automated, live, and DID call routing to maximize user satisfaction as well as efficiency and flexibility. This usually includes taking a published main telephone number and routing it to the auto attendant, as well as installing DID lines that route calls directly to different workgroups and individual employees.

6.4.1 Trunk Considerations

An auto attendant menu can be reached through analog loop-start, digital loop-start, SIP, and SGT1/SGE1 PRI trunks by pointing the trunk group at the desired menu. You can also reach a specific menu using DID or DNIS entries received over analog wink-start, digital wink-start, or SGT1/SGE1 PRI trunks.

The operator can be reached through analog loop-start, digital loop-start, and SGT1/SGE1 PRI trunks by pointing the trunk group directly at the operator. You can also reach the operator using DID or DNIS entries received over analog wink-start, digital wink-start, or SGT1/SGE1 PRI trunks.

The MiVoice Connect system supports International Caller ID, Caller ID Name, Caller ID Number, ANI, and DNIS. The Caller ID and trunk group or DNIS information will be provided to the user to assist in answering the call.

When using Direct Inward Dial, you must use analog wink-start, digital-wink start, or SGT1/SGE1 PRI trunks. The MiVoice Connect system can receive Automatic Number Identification (ANI) over analog and digital wink-start trunks as well as Caller ID Number over SGT1/SGE1 PRI.

Features available on trunks vary by trunk type. See Understanding Trunk Features on page 86 for more information.

6.4.1.1 After-Hours Call Routing

For after hours, weekends, and holidays, you should consider how your call flow will change. Typically, a different prompt should be played, since callers are routed directly to voice mail rather than to workgroups or the operator.

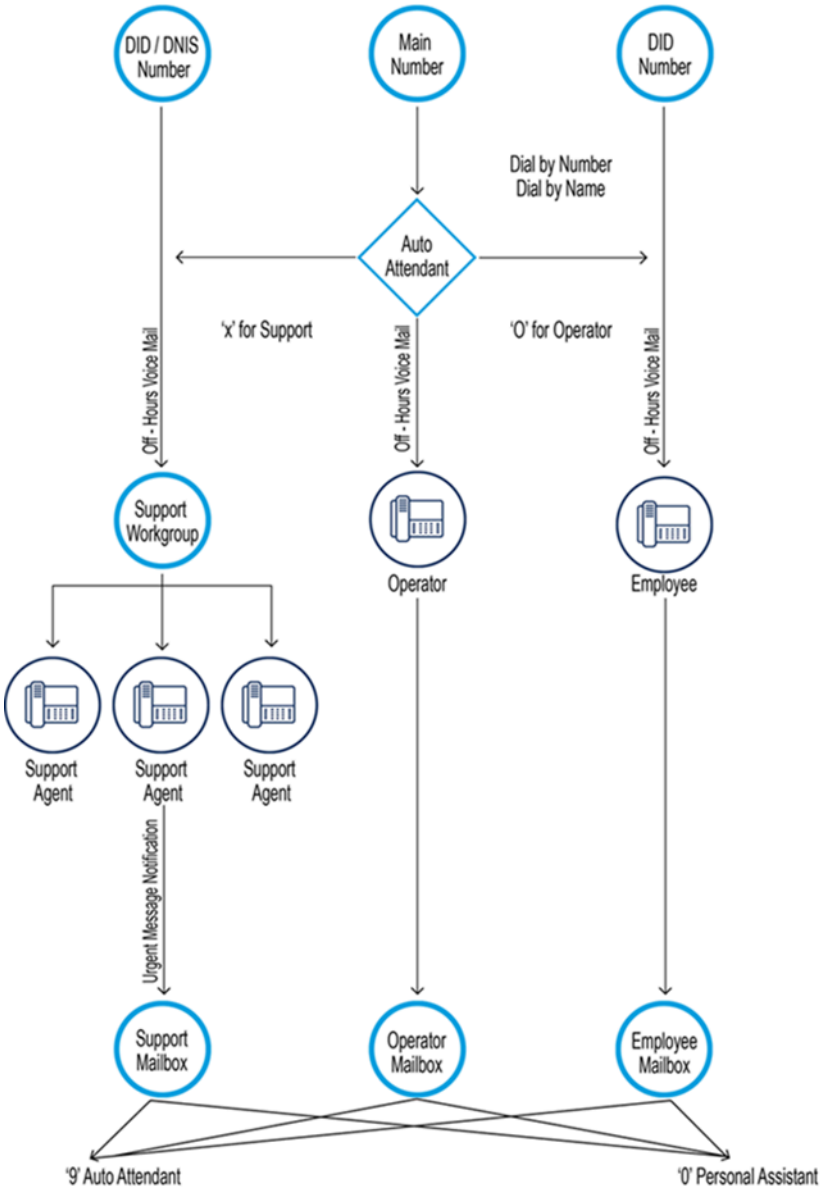
If you route all calls to the operator’s extension, auto attendant scheduling does not apply; only those calls routed to the auto attendant use the schedule. Therefore, when you want to use the off-hours, holiday, and custom schedules, set the operator’s availability state to forward all calls to the auto attendant when unavailable.

By routing all calls to the individual extensions, each individual user and workgroup defines its after-hours call handling.

6.4.1.1.1 Example of Blended Call Routing

In the example shown in Blended Call Routing, a mix of inbound call routing is used.

Figure 9: Blended Call Routing



- Calls are routed directly to the support workgroup using DID and DNIS entries and routed through the auto attendant with a mailbox that provides coverage.

  The calling party can dial **0** in the mailbox to reach the workgroup assistant, or **9** to return to the auto attendant.

- Calls are routed directly to the employees using DID and routed through the auto attendant using Dial by Number and Dial by Name with a mailbox that provides coverage.

  The calling party can dial **0** in the mailbox to reach his or her personal assistant, or **9** to return to the auto attendant.

- An operator provides limited call handling functions from individual mailboxes or the auto attendant.

In this example, after-hours call routing changes at the auto attendant and for each of the workgroups, employees, and the operator, because each workgroup defines its own after-hours call routing.

6.4.2 Analyze Outbound Call Routing

In general, you should have trunks at every site that support both outbound and inbound calling. The following are general facts about outbound trunking:

- ISDN PRI provides the most feature-rich inbound and outbound calling experience.

  This includes the support for Caller ID, DID, and DNIS. Caller ID Number is supported for both inbound and outbound calls. Caller ID Name is supported only on inbound NI-2 trunks with the exception of outbound calls to off-system extensions.

- SIP trunks can be used to place outbound calls.
- Analog wink-start trunks do not support outbound calls.
- You might want to purchase some analog loop-start trunks for emergency dial tone in case of total power failure. For more information, see Analog Loop-Start Trunks (North America) on page 81.
- Calls can be automatically routed across your wide area network (WAN) using the Network Call Routing feature. This allows users to access local and nearby area codes at one site from another site.
- You must plan for emergency calls, such as 911 in the United States, on your voice system.

The MiVoice Connect system supports all the necessary signaling for emergency calls, but note that in the case of a power failure you would need an analog loop-start trunk to have the dial tone needed to make an emergency call. Refer to the appendix on emergency 911 operations in the *MiVoice Connect System Administration Guide* for information on how to configure your system for emergency calls.

If your system uses three-digit extensions, Mitel recommends that you do not assign x11 extensions to users.

For more information, see Reviewing and Selecting Trunk Types on page 78 and Overview on page 98.

Trunk Planning and Ordering 7

This chapter contains the following sections:

This chapter provides information about trunk planning and ordering.

7.1 Recommendations

The following recommendations assist you in determining your trunk requirements and ordering your trunks from your service provider:

- Ensure you order telephone service early. SGT1 and PRI service can take up to one or two months to install.
- If you are reusing Centrex lines, ensure to change your old service and remove call waiting, call forwarding, and voice mail.
- When provisioning PRI service, ensure to confirm the protocol being used. The protocol may be NI-2, 4ESS, 5ESS, or DMS-100.

7.2 Reviewing and Selecting Trunk Types

Trunks provide a connection from the MiVoice Connect system to a service provider for the purpose of making and taking calls to and from external parties.

Supported Trunk Types - Part 1 and Supported Trunk Types - Part 2 shows which trunk types are supported on individual Voice Switches. The next section provides more detailed information about the various trunk features.

Table 17: Supported Trunk Types - Part 1

Voice Switch	Analog Loop-Start (North.Amer.)	Analog Loop-Start EMEA	Digital Loop-Start	Analog Wink-Start	Digital Wink-Start
ST1D	No	No	Yes	No	Yes
ST2D[a]	No	No	Yes	No	Yes

Voice Switch	Analog Loop-Start (North.Amer.)	Analog Loop-Start EMEA	Digital Loop-Start	Analog Wink-Start	Digital Wink-Start
ST50A	Yes	Yes	No	Yes	No
ST100A	Yes	Yes	No	Yes	No
ST200	No	No	No	No	No
ST500	No	No	No	No	No
ST100DA	Yes	Yes	Yes	Yes	Yes
ST24A	No	No	No	Yes	No
ST48A	No	No	No	Yes	No
SG90	Yes	Yes	No	Yes	No
SG90BRI	No	No	No	No	No
SG50	Yes	Yes	No	Yes	No
SG30	Yes	Yes	No	Yes	No
SG220E1	No	No	No	No	No
SG220T1	No	No	Yes	No	Yes
SG220T1A	Yes	No	Yes	No	Yes
SGT1k	No	No	Yes	No	Yes

Table 18: Supported Trunk Types - Part 2

Voice Switch	SGT1 PRI	SGE1 PRI	SIP	BR
ST1D	Yes	Yes	Yes	No
ST2D[a]	Yes	Yes	Yes	No
ST50A	No	No	Yes	No
ST100A	No	No	Yes	No
ST200	No	No	Yes	No
ST500	No	No	Yes	No
ST100DA	Yes	Yes	Yes	No
ST24A	No	No	Yes	No
ST48A	No	No	Yes	No
SG90	No	No	Yes	No
SG90BRI	No	No	Yes	Yes
SG50	No	No	Yes	No
SG30	No	No	Yes	No
SG220E1	No	Yes	Yes	No
SG220T1	Yes	No	Yes	No
SG220T1A	Yes	No	Yes	No

Voice Switch	SGT1 PRI	SGE1 PRI	SIP	BR
SGT1k	Yes	No	Yes	No

Note:

[a] On ST2D voice switches, dual SGT1 and SGE1 spans can be used as follows:

- One span can be used for SGE1/SGT1 trunking, and one span can be used for SIP trunking.
- Both spans can be used for SGE1/SGT1 trunking using the same signaling modes: both have to work in PRI signaling mode, or both have to operate in CAS mode.

7.2.1 Analog Loop-Start Trunks (North America)

Analog loop-start trunks are typically used for inbound calls to a main telephone number that are directed to an auto attendant menu, company operator, or workgroup. A caller can route a call from the auto-attendant to a user extension by entering the extension number or by spelling the user's name from the telephone keypad. Analog loop-start trunks are also used to make outbound calls.

Analog loop-start trunks support the following:

- Inbound calls
- Outbound calls
- Caller ID number
- Caller ID name
- Caller ID blocking

Analog provisioning is provided by the loop-start protocol and Dual-Tone Multi-Frequency (DTMF) signaling.

Analog loop-start trunks are used to provide power-fail transfer to selected telephones — for instance, to the operator, security station, executives, and so on. When there is a complete power failure, including loss of UPS power backup, power-fail transfer connects a specified trunk port to a specified extension port. This power-fail transfer ability provides a dial tone for making and taking critical calls in the event of power failure. Refer to the MiVoice Connect System Administration Guide for more information about the power-fail transfer port on each Voice Switch that supports this feature.

Centrex lines are analog lines that can be used as analog loop-start trunks. Your organization may already have these installed, and want to use them instead of ordering new loop-start trunks. If you have Centrex lines and do not want to change your primary company telephone number, you can keep Centrex lines. Centrex lines support Caller ID. Be sure to remove the Centrex features, including call waiting, call forward, and voice mail.

EMEA analog loop start trunk support, based on the TBR 21 standard, is supported on all 1U Half Width voice switches. BT type 1, or on hook, caller ID support is based on SIN 227 and SIN 242 standards in the UK.

7.2.2 Analog Loop-Start Trunks (EMEA)

Analog Loop-Start trunks are supported in Europe, the Middle East, and Africa. These trunks use the TBR 21 standard.

Analog loop-start Trunks (EMEA) are typically used for inbound calls to a main telephone number that are directed to an auto-attendant menu, company operator, or workgroup. A caller can route a call from the auto-attendant to a user extension by entering the extension number or by spelling the user's name from the telephone keypad. Analog loop-start trunks are also used to make outbound calls.

Analog loop-start trunks (EMEA) support:

- Inbound calls
- Outbound calls

Analog provisioning is provided by the loop-start protocol and Dual-Tone Multi-Frequency (DTMF) signaling.

Analog loop-start trunks are used to provide power-fail transfer to selected telephones — for instance, to the operator, security station, executives, and so on. When there is a complete power failure, including loss of UPS power backup, the Voice Switches provides power-fail transfer. Refer to the MiVoice Connect System Administration Guide for the power-fail transfer port on each Voice Switch that supports this feature. This power-fail transfer ability provides a dial tone for making and taking critical calls in the event of power failure.

Centrex lines are analog lines that can be used as analog loop-start trunks on the Voice Switches. Your organization may already have these installed, and want to use them instead of ordering new loop-start trunks. If you have Centrex lines and do not want to change your primary company telephone number, you can keep Centrex lines. Centrex lines support Caller ID. Be sure to remove the Centrex features, including call waiting, call forward, and voice mail.

7.2.3 Digital Loop-Start Trunks

Digital loop-start trunks are typically used for inbound calls to the main telephone number that are directed to an auto-attendant menu, company operator, or workgroup. A caller can route a call from the auto-attendant to a user extension by entering the extension number or by spelling the user's name from the telephone keypad. Digital loop-start trunks are also used to make outbound calls.

Digital loop-start trunks support the following:

- Inbound calls
- Outbound calls
- Caller ID number
- Caller ID name
- Caller ID blocking

Digital provisioning is provided by the loop-start protocol and Dual-Tone Multi-Frequency (DTMF) signaling. Voice Switches support the following:

- ESF or D4 framing formats

- B8ZS or AMI line coding

7.2.4 Analog Wink-Start Trunks (Analog DID)

Analog wink-start trunks allow external callers to dial a user's phone number directly, without having to use an auto-attendant or operator. Analog wink-start trunks support only inbound calls; they are not capable of handling outbound calls.

Analog wink-start trunks support the following:

- Inbound calls (outbound calls are not supported)
- ANI
- DID
- DNIS

Analog provisioning is provided by the wink-start protocol and Dual-Tone Multi-Frequency (DTMF) signaling.

If ANI is being used, the star (*) key must be used to delimit the ANI digits from the DID/DNIS digits, that is:

- <DID>
- <DNIS>
- *<ANI>*<DID/DNIS>*

7.2.5 Digital Wink-Start Trunks

Digital wink-start trunks allow external callers to dial a user's phone number directly, without having to use an auto attendant or operator. Digital wink-start trunks support both inbound and outbound calls.

Digital wink-start trunks support the following:

- Inbound calls
- Outbound calls
- ANI
- DID
- DNIS

Digital provisioning is provided by the wink-start protocol, which is often called E&M wink-start, and Dual-Tone Multi-Frequency (DTMF) signaling.

Voice Switches support the following:

- ESF or D4 framing formats
- B8ZS or AMI line coding

If ANI is being used, the star (*) key must be used to delimit the ANI digits from the DID/DNIS digits, that is:

- <DID>

- <DNIS>
- *<ANI>*<DID/DNIS>*

7.2.6 BRI Trunks

BRI Trunks

BRI trunks are flexible trunks that support both inbound and outbound calls.

PRI trunks support the following:

- Inbound calls
- Outbound calls
- DID
- DNIS
- Caller ID number
- Caller ID name is supported for NI-2 configured trunks
- QSIG – Calling name is supported if the standard is similar to NI2
- Inbound calling name is fully supported, but outbound calling name is only supported for Off-System Extension calls

Digital provisioning is provided by the PRI protocol and D-channel signaling. Voice Switches support:

- DMS-100, 4ESS, 5ESS, and NI-2 signaling types
- ESF or D4 framing formats
- B8ZS or AMI line coding

The NFAS and Call-by-Call features are not supported.

7.2.7 SGT1 PRI Trunks

SGT1 PRI trunks are flexible trunks that support both inbound and outbound calls.

PRI trunks support the following:

- Inbound calls
- Outbound calls
- DID
- DNIS
- Caller ID number
- Caller ID name is supported for NI-2 configured trunks
- QSIG – Calling name is supported if the standard is similar to NI2
- Inbound calling name is fully supported, but outbound calling name is only supported for Off-System Extension calls

Digital provisioning is provided by the PRI protocol and D-channel signaling. Voice Switch supports the following:

- DMS-100, 4ESS, 5ESS, and NI-2 signaling types
- ESF or D4 framing formats
- B8ZS or AMI line coding

The NFAS and Call-by-Call features are not supported.

7.2.8 SGE1 PRI Trunks

SGE1 PRI trunks are flexible trunks that support both inbound and outbound calls for international locations.

SGE1 PRI trunks support the following:

- Inbound calls
- Outbound calls
- DID
- DNIS
- Caller ID number
- Caller ID name is supported for NI-2 configured trunks
- QSIG – Calling name is supported if the standard is similar to NI2
- Inbound calling name is fully supported, but outbound calling name is only supported for Off-System Extension calls

The Voice Switches support PRI signaling using Euro-ISDN as well as other international protocols. See Trunk Access Codes on page 326.

7.2.9 SIP Trunks

SIP trunks are flexible trunks that support both inbound and outbound calls. SIP trunks are logical trunk end points that only handle SIP call control. Media flows directly between the call initiator and the call terminator.

SIP trunks support the following:

- Inbound calls
- Outbound calls
- Extension, Tandem, and default destinations for inbound calls
- Caller ID name
- Caller ID number
- DID
- DNIS

By default, the **Enable SIP Info for G711 DTMF signaling** check box is not selected. This check box must be enabled for Mitel-to-Mitel SIP tie trunks or for SIP devices that do not support RFC 2833 for G711.

7.3 Understanding Trunk Features

The MiVoice Connect system supports several different trunk types and trunk features. It is very important to understand the features available on these trunks, since some services are mutually exclusive. The Trunk Features table shows each trunk type and the associated features.

Table 19: Trunk Features

Feature	Analog Loop-Start N. Am.	Analog Loop-Start EMEA	Digital Loop-Start	Analog Wink-Start	Digital Wink-Start	SGT 1 PRI	SGE 1 PRI	SIP	BRI
Inbound									
Caller ID Number	Yes	No	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Caller ID Name	Yes	No	Yes	No	No	Yes	Yes	Yes	Yes
Direct Inward Dial (DID)	No	No	No	Yes	Yes	Yes	Yes	Yes	Yes
Dialed Number Identification Service (DNIS)	No	No	No	Yes	Yes	Yes	Yes	Yes	Yes
Outbound									
Caller ID Blocked	Yes (CO)	Yes (CO)	Yes (CO)	N/A	Yes (CO)	Yes	Yes	Yes	Yes
Caller ID Unblocked	Yes (CO)	Yes (CO)	Yes (CO)	N/A	Yes (CO)	Yes	Yes	Yes	Yes
Caller ID Blocking	Yes	No	Yes	N/A	No	Yes	No	Yes	No

Feature	Analog Loop-Start N. Am.	Analog Loop-Start EMEA	Digital Loop-Start	Analog Wink-Start	Digital Wink-Start	SGT 1 PRI	SGE 1 PRI	SIP	BRI
Override (*67, *82)									

Note:

- Via Automatic Number Identification (ANI).
- Caller ID Name is supported for NI-2 configured trunks.
- *67 and *82 codes do not work if the CO requires a pause between the code and the dialed number.

7.3.1 Legend to Trunk Features Table

Legend to Trunk Features is as follows:

- Yes — Feature is supported.
- No — Feature is not supported
- Yes (CO) — Feature is provided by the central office (CO) or legacy PBX.
- N/A — Outbound calls are not supported on analog wink-start trunks.

7.3.2 Caller ID Number

Caller ID Number delivers to the MiVoice Connect system the number of the calling party, which is displayed in the Mitel Connect client as well as on Caller ID – compatible telephones. The delivery of the caller ID number can be blocked by the calling party. The caller ID number is delivered unless the calling party has blocked the call, in which case the call is marked as Blocked, or the service provider does not have the information, in which case the call is marked as Unavailable.

Caller ID Number has the following limitations:

- The calling party may block his or her caller ID number.
- The calling party may be calling from a business and the calling number may be incorrect.
- The calling party may be calling from someone else’s number.

Caller ID Number is available on analog loop-start, digital loop-start, SIP, SGT1 PRI, and SGE1 PRI trunks.

Two different Caller ID Number formats are used to deliver caller information via loop-start trunks: Single Data Message Format (SDMF) and Multiple Data Message Format (MDMF). SDMF provides the calling

number, while MDMF provides any combination of calling name and number. The voice switches support both SMDF and MDMF dynamically, without the need for configuration. When PRI is used, the caller ID number is delivered as a D-Channel message.

Mitel supports International Caller ID, ensuring that when a switch is configured for a certain site (for example, Spain), the International ID information is automatically filled in as appropriate for that country. The feature is transparent from the user's standpoint, and no configuration is necessary.

7.3.3 Caller ID Name

Caller ID Name delivers the name of the calling party to the MiVoice Connect system. The name is displayed in the Mitel Connect client as well as on any telephones that support caller ID Name.

By default, the caller ID name is delivered unless the calling party has blocked the transfer of this information, in which case the call is marked as **Blocked**. If the service provider does not have the information, the call is marked as **Unavailable**.

Caller ID Name is available on analog loop-start and digital loop-start trunks, as well as SIP, SGT1 PRI, and SGE1 PRI trunks and is only supported on IP phone and analog phones in North America. This feature is not supported on analog phones in other countries.

When using NI-2 signaling on PRI trunks, for example in a tie-trunk scenario, Caller-ID Name is now also captured when available on all inbound calls. For outbound calls, Caller-ID Name is delivered for calls that are made to off-system extensions, but not for outbound calls.

7.3.4 Automatic Number Identification (ANI)

Automatic Number Identification (ANI) delivers the number of the calling party to the MiVoice Connect system. Although similar to Caller ID Number, ANI is tariffed differently and is not subject to the same blocking restrictions as Caller ID Number. For example, when you purchase ANI services from your service provider, you are always delivered the calling number for 800-number calls. Business practices can vary from region to region.

ANI is available on analog wink-start and digital wink-start trunks.

When ANI is being used, the star key (*) must be used to delimit the ANI digits from the DID/DNIS digits — that is, *<ANI>*<DID/DNIS>*.

7.3.5 Direct Inward Dial (DID)

Direct Inward Dial (DID) allows extensions on the system, such as users, menus, workgroups, route points, and so on, to be accessed directly, without the need of an auto-attendant or operator. This is particularly useful when users on the system want their own telephone number.

DID is available on analog wink-start, digital wink-start, PRI and SIP trunks.

DID numbers are ordered in blocks of 20 or more 10-digit telephone numbers. These numbers are assigned to a customer and are routed to a wink-start, PRI or SIP trunk connected to a voice switch. When a call is made, the service provider sends a predefined set of digits, from 3 to 10 digits, via the wink-start, PRI, or SIP trunk. The voice switches capture the digits and route the calling party to the called party.

If ANI is not being used on wink-start trunks, only the DNIS digits need to be delivered. If ANI is being used, the star (*) key must be used to delimit the ANI digits from the DID/DNIS digits as follows:

- <DID>
- <DNIS>
- *<ANI>*<DID/DNIS>*

7.3.6 Dialed Number Identification Service (DNIS)

Dialed Number Identification Service (DNIS) allows extensions on the system, such as users, menus, workgroups, route points, and so on, to be accessed directly without the need for an auto attendant or operator. This is particularly useful for workgroup and other call center applications. The DNIS information is delivered to the Mitel Connect client - Personal Access and stored in the call detail record.

DNIS is available on analog wink-start, digital wink-start, PRI, and SIP trunks.

DNIS numbers are ordered individually and map to a dialed number. When a calling party dials a specific telephone number, the service provider routes the call to a wink-start or PRI trunk connected to a voice switch. The service provider sends a predefined set of digits, from 3 to 10 digits — the DNIS digits — using DTMF signaling or a D-Channel message or SIP message. The voice switches capture the digits and route the calling party to the called party.

If ANI is not being used on wink-start trunks, only the DNIS digits need to be delivered. If ANI is being used, the star (*) key must be used to delimit the ANI digits from the DID/DNIS digits as follows:

- <DID>
- <DNIS>
- *<ANI>*<DID/DNIS>*

7.3.7 Outbound Caller ID

The user’s DID number is sent as the caller ID number for outbound calls over PRI or SIP trunks. If the DID number is unavailable, the site Caller Emergency Service ID (CESID) is used. If that number is unavailable, no caller ID is sent.

Additionally, the outbound caller ID can be configured on a per-user basis such that the configured value can take precedence over the user's DID number or the site CESID. Note that this feature is only available on outbound calls using a SGT1 PRI trunk.

- To send a single main number rather than individual user DID numbers, assign DNIS entries instead of DID numbers to each user. The Site Contact Number will be sent on outbound calls.
- To block all outbound caller ID numbers from being sent, you can configure the PRI trunk group to always block the caller ID number.
- On wink-start and loop-start trunks, the outbound caller ID is defined by the service provider.
- On SGT1 PRI and loop-start trunks, users can override the Caller ID Blocking configuration on a call-by-call basis by using commands at the telephone, such as *67, *82. Users cannot override the Caller ID Blocking configuration of wink-start and SGE1 PRI trunks.

For more information on configuring outbound caller ID, please refer to the *MiVoice Connect System Administration Guide*.

7.3.8 Tandem Trunking

Tandem trunking allows legacy voice systems to utilize a MiVoice Connect system for outbound dialing. The MiVoice Connect system supports both user-side and network-side PRI, allowing MiVoice Connect systems to flexibly support digital tie trunks to other systems.

You can enable tandem trunking support for any PRI trunk group with a check box in Connect Director. Tandem calls are associated with a user group for outbound trunk selection. Inbound calls recognized as tandem calls are redirected to an outbound trunk based on user group call permissions and trunk group access. When needed, a “dial-in prefix” can be specified that is prepended to digits collected on tandem calls. The concatenated set of digits is then used in outbound trunk selection for the tandem call.

7.3.9 Tie Trunks

The addition of network-side PRI support makes PRI tie trunks easier and more compelling to deploy. Voice Switches that support SGT1 PRI can act as either the user-side or network-side of a PRI tie trunk. The tie trunk may be used to tie a MiVoice Connect system to a legacy voice system, or potentially to another independent MiVoice Connect system.

7.4 Performing Traffic Calculations

The number of trunks required on your system will vary depending on the number of users and your specific application needs. It is important to order your trunking correctly; too few can lead to blocked calls when all trunks are busy, and too many trunks can lead to wasted money on monthly access charges.

For information about calculating the trunk requirements, refer to System Capacity on page 15.

7.5 Ordering Telephone Service

Once you have determined the types of trunks you need, you will have to either place a new order or make a change order. You can use the associated Telephone Service Order Forms that are available on the USB flash drive or on the support web site. Three order forms are provided for your use:

- Analog Service
- SGT1 Service
- SGT1 PRI Service

Mitel does not provide an SGE1 PRI form because this service varies by country. Instead, we provide a table of the SGE1 PRI parameters that must be set. See Dialing Plan Considerations on page 326 for more information.

When the form is completed, arrange a meeting with your telephone company service representative to order the new telephone services. The forms contain specific information that the service representative must have before services can be ordered.

Before ordering your telephone service, pay special attention to the installation date and time, as follows:

- If you are ordering new service, it should be installed one week before the planned cut-over date. This allows the services to be terminated on the MiVoice Connect system and tested before cut-over.
- If you are changing existing service, any changes before the cut-over date might render your existing service unusable. You must schedule these changes outside normal business hours and work closely with your service provider for a seamless transition.

When ordering DID service, the last digits of the DID numbers should match your extension numbers for ease of use. You must make sure your extension numbers do not begin with a trunk access code, zero, or any emergency numbers such as 911 in North America.

See the appendix on emergency 911 operations in the *MiVoice Connect System Administration Guide* for information on how to configure your system for emergency calls.

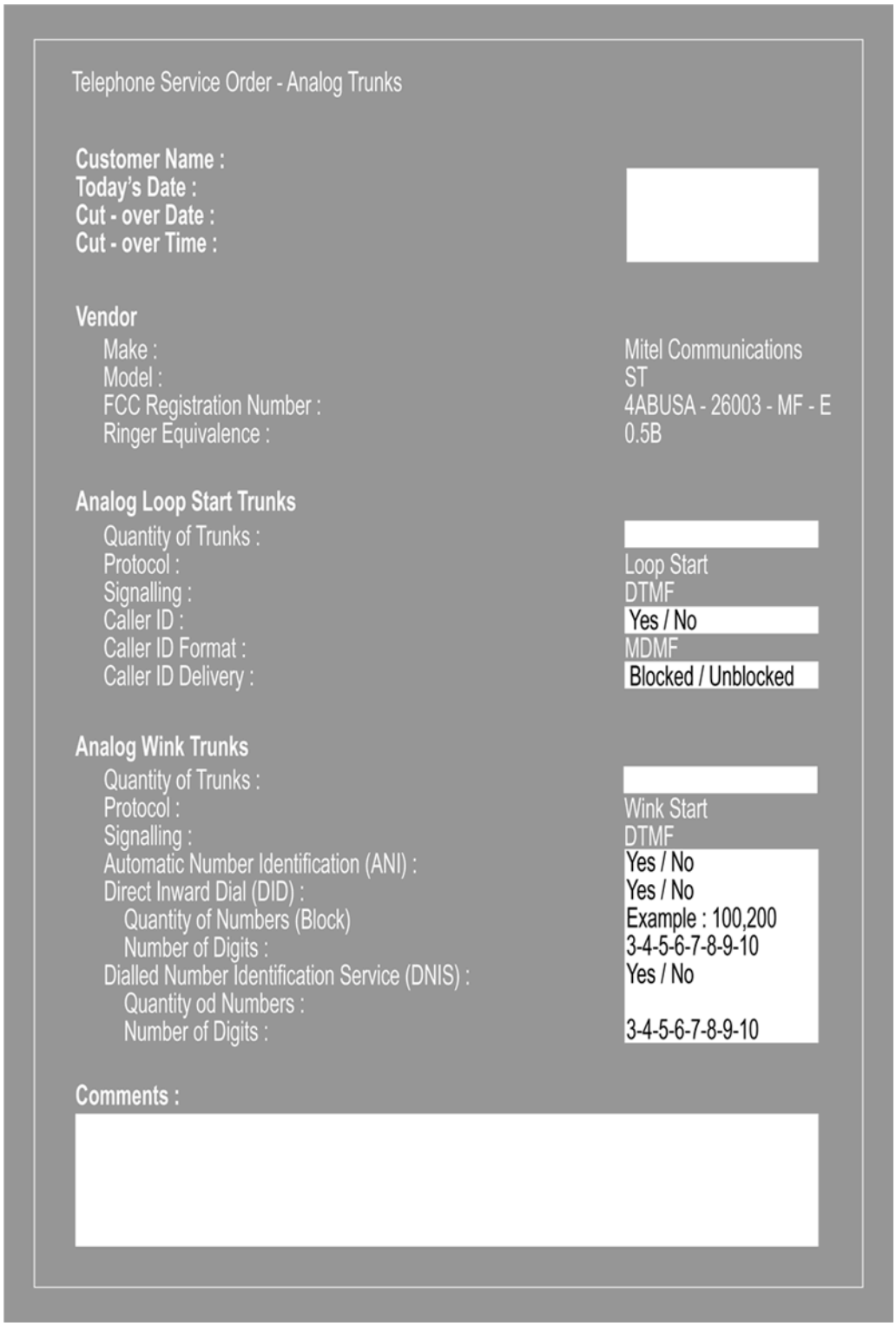
7.5.1 Analog Service

Note:

The following before requesting analog service from a telephone service provider:

- Caller ID Name and Number are supported on loop-start trunks
- ANI is supported on wink-start trunks
- ANI on wink-start trunks must be delivered as *<ANI>*<DNIS>*
- ANI on wink-start trunks must be delivered as *<ANI>*<DNIS>*

Figure 10: Telephone Service Order Form—Analog Trunks



Telephone Service Order - Analog Trunks

Customer Name :
Today's Date :
Cut - over Date :
Cut - over Time :

Vendor

Make :	Mitel Communications
Model :	ST
FCC Registration Number :	4ABUSA - 26003 - MF - E
Ringer Equivalence :	0.5B

Analog Loop Start Trunks

Quantity of Trunks :	
Protocol :	Loop Start
Signalling :	DTMF
Caller ID :	Yes / No
Caller ID Format :	MDMF
Caller ID Delivery :	Blocked / Unblocked

Analog Wink Trunks

Quantity of Trunks :	
Protocol :	Wink Start
Signalling :	DTMF
Automatic Number Identification (ANI) :	Yes / No
Direct Inward Dial (DID) :	Yes / No
Quantity of Numbers (Block)	Example : 100,200
Number of Digits :	3-4-5-6-7-8-9-10
Dialled Number Identification Service (DNIS) :	Yes / No
Quantity od Numbers :	
Number of Digits :	3-4-5-6-7-8-9-10

Comments :

7.5.2 SGT1 Service

Use the SGT1 Telephone Service Order form, shown in Telephone Service Order Form—SGT1 Trunks, to order SGT1 trunks. Note the following about SGT1 service:

- Caller ID Name and Number are supported on loop-start trunks

- ANI is supported on wink-start trunks
- ANI on wink-start trunks must be delivered as *<ANI>*<DNIS>*A channel service unit (CSU) is built into the voice switch

Figure 11: Telephone Service Order Form—SGT1 Trunks

Telephone Service Order - TITrunks

Customer Name :
Today's Date :
Cut - over Date :
Cut - over Time :

Vendor

Make :	Mitel Communications
Model :	ST
FCC Registration Number :	4ABUSA - 26003 - MF - E
Ringer Equivalence :	0.5B

Digital Loop Start Trunks

Quantity of Trunks :	
Protocol :	Loop Start
Signalling :	DTMF
Framing Format :	ESF / D4
Line Code :	B8ZS / AMI
Caller ID :	Yes / No
Caller ID Format :	MDMF
Caller ID Delivery :	Blocked / Unblocked

Digital Wink Trunks

Quantity of Trunks :	
Protocol :	Wink Start
Signalling :	DTMF
Framing Format :	ESF / D4
Line Code :	B8ZS / AMI
Automatic Number Identification (ANI) :	Yes / No
Direct Inward Dial (DID) :	Yes / No
Quantity of Numbers (Block)	Example : 100, 200
Number of Digits :	3-4-5-6-7-8-9-10
Dialled Number Identification Service (DNIS) :	Yes / No
Quantity od Numbers :	
Number of Digits :	3-4-5-6-7-8-9-10

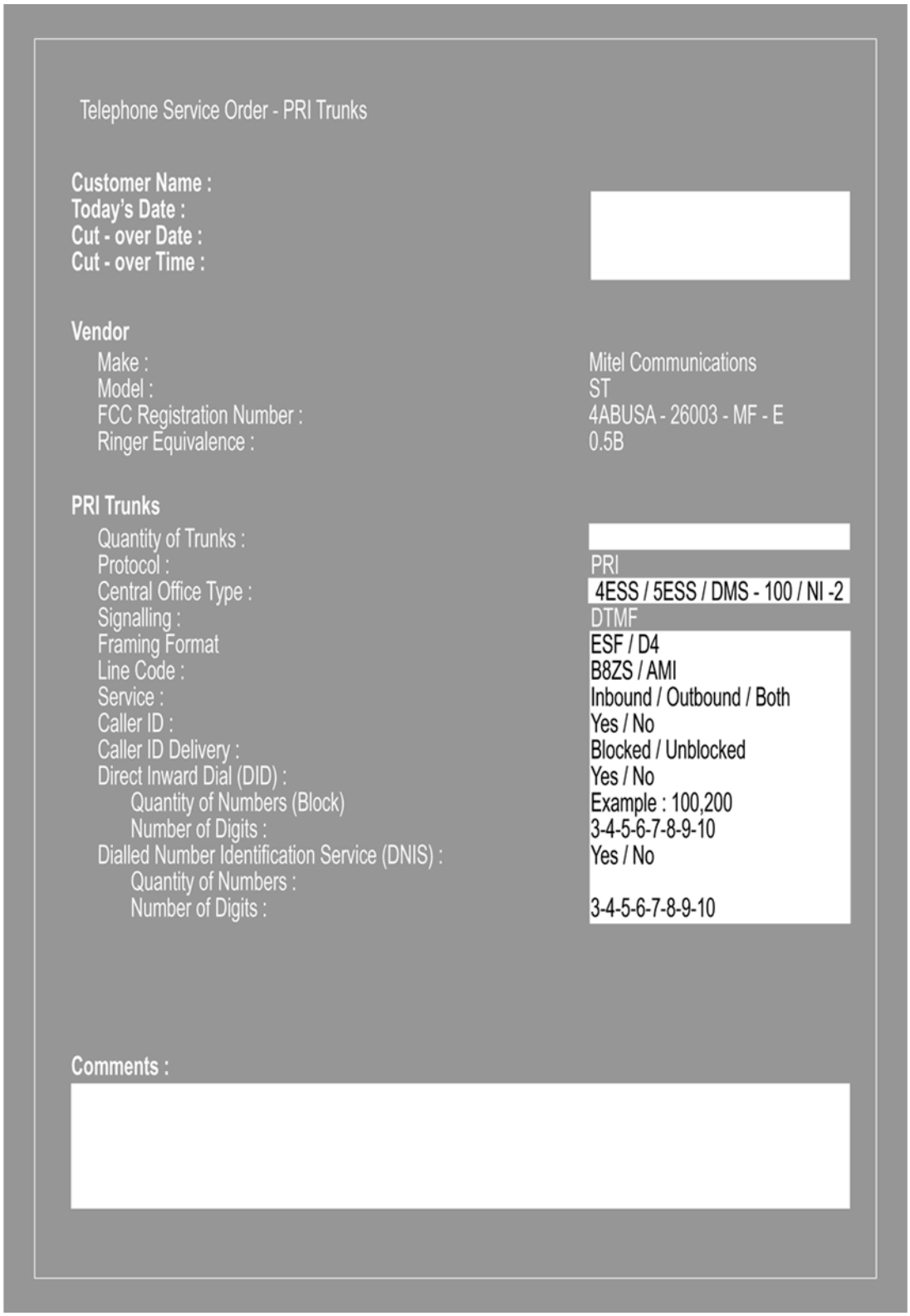
Comments :

7.5.3 SGT1 PRI Service

Use the SGT1 PRI Telephone Service Order form, shown in Telephone Server Order Form—PRI Trunks, to order SGT1 PRI trunks. Note the following about SGT1 PRI service:

- Caller ID Number is supported on SGT1 PRI trunks. Caller ID Name is supported in NI-2 configured trunks.
- A channel service unit (CSU) is built into the voice switch.

Figure 12: Telephone Server Order Form—PRI Trunks



Telephone Service Order - PRI Trunks

Customer Name :
Today's Date :
Cut - over Date :
Cut - over Time :

Vendor

Make :	Mitel Communications
Model :	ST
FCC Registration Number :	4ABUSA - 26003 - MF - E
Ringer Equivalence :	0.5B

PRI Trunks

Quantity of Trunks :	
Protocol :	PRI
Central Office Type :	4ESS / 5ESS / DMS - 100 / NI -2
Signalling :	DTMF
Framing Format	ESF / D4
Line Code :	B8ZS / AMI
Service :	Inbound / Outbound / Both
Caller ID :	Yes / No
Caller ID Delivery :	Blocked / Unblocked
Direct Inward Dial (DID) :	Yes / No
Quantity of Numbers (Block)	Example : 100,200
Number of Digits :	3-4-5-6-7-8-9-10
Dialled Number Identification Service (DNIS) :	Yes / No
Quantity of Numbers :	
Number of Digits :	3-4-5-6-7-8-9-10

Comments :

7.5.4 Ordering Service

When you order service, be sure to do the following:

- State that a new MiVoice Connect system is being installed.
- State the date and time the new telephone service must be cut over.
- Review all the items on the telephone service order form with the service representative.
- Review any existing and new telephone numbers and have the telephone company representative confirm the order.

7.5.5 SGE1 PRI Service

See Dialing Plan Considerations on page 326 for more information about ordering SGE1 PRI service.

Dialing Plan 8

This chapter contains the following sections:

This chapter provides an overview of the dialing, call routing, and digit-manipulation capabilities of the MiVoice Connect system.

8.1 Overview

This chapter provides an overview of the dialing, call routing, and digit-manipulation capabilities of the MiVoice Connect system. The information in this chapter is useful for administrators of larger, multisite installations.

Note:

- Mitel strongly recommends that administrators configure dial plans using Connect Director. Because dial plan entries can consume a large amount of switch resources, Mitel also recommends that administrators closely monitor switch CPU and memory usage. Monitoring the switch usage helps administrators determine when it is necessary to reduce the number of stored entries after adding a large number of DNIS or Prefix entries.
- Manipulation of Connect databases can cause undesired results. In the event that manual or third-party database changes cause undesired results, Mitel Support might require that those database changes be reversed to resolve the issue.
- The default and custom plan combined length for Site Dialing Rules and Trunk Dialing Rules should not exceed 2000 characters.

8.2 Dialing

When a phone number is dialed in a MiVoice Connect system, the system performs two distinct operations on a telephone number:

- Digit collection — Voice switches collect the digits in a telephone number.
- Digit manipulation — The switches manipulate the dialed numbers before outpulsing them to the service provider.

8.2.1 Define Digit Collection

When someone picks up a telephone in a MiVoice Connect system and begins dialing a telephone number, the voice switch software (or, on 400-Series IP phones, the phone software) examines each digit in the number and determines whether digit collection should continue or be terminated.

8.2.2 Configuring Internal Numbers

In a MiVoice Connect system where users dial internal numbers without an access code, the rules for digit collection are relatively straightforward.

Digit collection rules are configured through Connect Director.

8.2.2.1 Planning Your Dialing Configuration

When setting up a dialing plan for internal numbers, consider the following:

- Select an extension length. MiVoice Connect supports 3-, 4-, and 5-digit dialing for internal numbers. For most enterprises, 4-digit dialing works. Use an extension number scheme that conforms to your company's size and the convenience of your users.
- Map extension ranges. After choosing the extension length, you can allocate blocks of numbers for use by extension, starting with the first number.

For example, if you want to reserve the range of numbers 3000-3999 for extension assignment, you allocate the "3" number block for extensions.

For maximum usability, map extension numbers to the final digits of your DID (if DID is used).

Note:

Extensions cannot begin with the following combinations that include 911: 911, 911x, or 911xx.

8.2.2.2 Digit Collection Rules

When routing calls, the MiVoice Connect system follows the digit collection rules specified on the Dial Plan page in Connect Director.

For the first digit collected, the rules outlined in the Digit Collection Rules table are in effect.

Table 20: Digit Collection Rules

Digit	Rule
0	By default, 0 is configured in the dialing plan as the Operator digit. However, 0 can be configured as a trunk access code, and some other digit can be configured as Operator. Digit collection is stopped and the call is routed to the site operator or to provide trunk access.
#	Digit collection is stopped and the call is routed to voice mail login.
Any other digit	Digit collection continues until a complete extension number is dialed. If the number is valid, the call is routed to the extension. For valid off-system extensions, the call is routed to a trunk. For invalid extensions, the call is routed to the Backup Automated Attendant. This rule does not apply to trunk access codes.

8.2.2.3 Exception for 911 Emergency Calls

Emergency calls do not require an access code. The following rules apply only to emergency 911 calls:

- If **911** is dialed, the switch routes the call to a 911-capable trunk group associated with the caller's User Group.
- Before switching the emergency call, the switch invokes a brief timeout for insurance against accidental 911 calls. If any digit is entered during the timeout, the switch routes the call to the Backup Automated Attendant.

Although this section focuses on emergency calls made within the United States, the same rules apply in other countries. Refer to the appendix on emergency 911 operations in the *MiVoice Connect System Administration Guide* for information on how to configure your system for emergency calls.

8.2.2.4 Changing Extension Length

Note:

Once you increase an extension length, you cannot decrease an extension length. For example, once it is increased to 4, the minimum is 4.

The MiVoice Connect system supports 3-, 4-, and 5-digit extensions. If your system uses 3-digit extensions, Mitel recommends that you do not assign x11 extensions to users.

8.2.3 Configuring External Numbers

The MiVoice Connect system supports 1-, 2-, and 3-digit trunk access codes. When an access code is dialed, the system looks for a valid digit in the parameters.

If an invalid number is dialed, the system plays a recording to the calling party.

There are several types of valid telephone numbers, which are described in the following sections.

The MiVoice Connect system allows the system administrator to provide users at each site with a unique dialing plan to match the dialing plan of the site's geographic region. The MiVoice Connect system supports 7-digit local dialing, 10-digit local dialing, and mixed local dialing.

Note:

- For US, MiVoice Connect does not support 7-digit local dialing. This is because MiVoice Connect has enabled support for 988 calls for the Suicide Prevention Lifeline. Therefore, the users must use a 10-digit dialing for trunk calls.
- When user dial a number by using 7-digit dialing and there is no 7 digit extension configured, they will hear the recorded message **"Your call cannot be completed as dialed. You must hang up and dial again using the area code and the seven-digit number. Thank you."**. This recording is played twice, after which the call is be disconnected.

External numbers are converted into a standard "canonical format" by call control software to provide a globally consistent way of handling phone numbers. The canonical format starts with a **+** representing the international prefix, followed by the country code, area code, and subscriber number.

- External numbers that can be converted into canonical format are considered "routable" and will leverage the network call routing feature of the call control software.
- External numbers that are unique to the country (n11, 112, 911, and so on) are considered "unroutable" and will not leverage the network call routing software. These calls will be placed from the local site or the associated proxy site.

8.2.3.1 Configuring 7-Digit Local Dialing

The Local Area Code on the Sites page defines 7-digit dialing for all users at the site. When a user dials an access code followed by 7 digits, the switching software assumes the site local area has been dialed. The switching software then converts the 7-digit number into canonical format before checking call permissions and doing network call routing.

The Local Area Code and Additional Local Area Codes set on the Sites page have nothing to do with the Local Area Code, Additional Local Area Codes, and Nearby Area Codes on the Trunk Groups page. The distinctions are as follows:

- Area codes on the Sites page relate only to digit collection.
- Area codes on the Trunk Groups page relate only to Network Call Routing and Digit Manipulation.

To define 7-digit dialing, enter the 3-digit area code in the Local Area Code parameter on the **Sites** page (**General** tab) in Connect Director.

Note:
In the US, MIVoice Connect doesn't support 7 digit local number dialing using any MiVoice Connect configuration.

8.2.3.2 Configuring 10-Digit Local Dialing

If the site is in a location with overlay area codes, it can be configured to support 10-digit dialing for all the local area codes. The Additional local area codes parameter on the **Sites** page (**General** tab) in Connect Director defines the area codes for 10-digit dialing. When a user dials an access code followed by a local area code, the system collects 7 additional digits, which comes to 10 digits total, before stopping digit collection. The switching software then converts the 10-digit number into canonical format before checking call permissions and doing network call routing.

8.2.3.3 Configuring Mixed Dialing in the Same Area

In locations where users are forced to dial 7 digits for some prefixes and 1+10 digits for other prefixes in the same area, the MiVoice Connect system supports permissive dialing. That is, you can dial these numbers either as 7 digits or as 1+10 digits. It also supports permissive dialing in locations with mixed 10-digit and 1+10 digit dialing in the same area.

From a digit-manipulation, or outpulsing, point of view, the trunk group must be configured properly because some service providers do not support permissive dialing. For more information, see Define Digit Manipulation on page 103.

8.2.3.4 1+10 Digit Long-Distance Dialing

The MiVoice Connect system supports long-distance dialing. When a user dials an access code followed by **1** the software collects 10 additional digits before stopping digit collection.

8.2.3.5 International Dialing

The MiVoice Connect system supports international dialing. If the user dials a trunk access code followed by an international access code, digit collection is terminated after a timeout. The timeout can be bypassed by dialing pound (**#**).

8.2.3.6 n11 Dialing

The MiVoice Connect system supports “n11” dialing, including 411 for information and 611 for support. If the user dials an access code followed by “n11” digit collection is terminated after a brief timeout and the call is routed to a trunk.

If your system uses three-digit extensions, Mitel recommends that you do not assign x11 extensions to users.

8.2.3.7 911 Dialing

The MiVoice Connect system supports 911 dialing to emergency services. If the user dials an access code followed by **911**, digit collection is terminated immediately and the call is routed to a trunk.

911 calls are routed out of the local site’s associated trunks. If there are no 911 trunks available at the local site, the call is routed through the designated proxy site.

8.2.3.8 Explicit Carrier Selection (101xxxx) Dialing

The MiVoice Connect system supports explicit carrier selection. If the user dials an access code followed by “101”, the next four digits collected are for explicit carrier selection (101xxxx). The carrier information is retained and passed to the trunk.The digits collected are treated as unroutable calls; the digits are routed “as-is” out either local site or proxy site trunks only.

8.2.3.9 Operator-Assisted (0, 00) Dialing

The MiVoice Connect system supports operator-assisted dialing. If the user dials an access code followed by “0x”, digit collection is terminated after a brief timeout and the call is routed to a trunk.

8.2.3.10 Vertical Service Code (*67, *82) Dialing

The MiVoice Connect system supports some vertical service codes for feature activation. If the user dials an access code and then the star (*) button, the system collects the subsequent digits and then terminates after a brief timeout. The digits collected are treated as unroutable calls. They are routed “as-is” out either local site or proxy site trunks only. If the trunk is a PRI or SIP trunk, the trunk strips and interprets *67 to block outbound Caller ID, and *82 to unblock outbound Caller ID.

8.2.3.11 End Digit Collection (#)

In some cases, digit collection ends after a timeout period. To bypass the timeout and immediately send the call, the caller presses the (**#**) button.

8.2.4 Define Digit Manipulation

Once the route decision has been made, the call is passed to the trunk. The dialed number, which is normally passed within the system in canonical format, is examined and manipulated based on the trunk group configuration. This ensures that the number can be properly received by the service provider.

First, the trunk access code dialed by the user is removed. If the number is in canonical format, which is local, long distance, ERC, or international, digit manipulation can occur. If the number is unroutable, which is n11, ECS, operator, and vertical service code numbers, digit manipulation, other than the dial-out prefix, is not applied.

You specify the trunk digit manipulation parameters on the Trunk Groups page (Outbound tab) in Connect Director. See the Digital Manipulation Options table for details. For more general information about configuring trunks, see the *Configuring Trunks* chapter of the *MiVoice Connect System Administration Guide*.

Table 21: Digital Manipulation Options

Option	Description	Example
Remove leading 1 from 1+10D	This option is required by some long-distance service providers that only accept numbers dialed as 10 digits.	AT&T typically only supports 10-digit dialing.
Remove leading 1 for Local Area Codes	This option is required by some local service providers that have mixed 10-digit and 1+10 digit dialing in the same area code. Local Area Codes include both the Local Area Code and Additional Local Area Codes configured against the trunk group.	Atlanta has three local area codes that must be dialed as 10 digits. This could also be called **Dial 10 digits for Local Area Codes**.
Dial 7 digits for Local Area Code	This option is required by some local service providers that have mixed 10-digit and 1+10 digit dialing in the same area code.	Massachusetts and Maine
Prepend this Dial Out Prefix	The Dial Out Prefix is prepended to the number. This feature is typically used when connecting the MiVoice Connect system to a legacy PBX system using a voice switch. The Dial Out Prefix enables the MiVoice Connect system to seize a trunk on the legacy PBX. The Dial Out Prefix is not applied to Off-System Extensions.	Not applicable.
Vertical Service Codes	If a Vertical Service Code was dialed, digit manipulation rules do not apply. Vertical Service Codes work with ISDN PRI and SIP trunks and some loop-start trunks. With PRI and SIP trunks, Vertical Service Codes for Caller ID Blocking control will be converted to D-Channel messages.	Not applicable.

Option	Description	Example
	With loop-start trunks, the service provider must be able to accept the outpulsed digits with only 50 msecs of pause between each digit, including the service codes. Vertical Service Codes are typically not supported by service providers on wink-start trunks. If you have outbound access on wink-start trunks and you dial a vertical service code, you will likely get an error message from the service provider.	
Off System Extensions	Off System Extensions define ranges of extensions that when dialed will be routed out of this trunk group. This is typically used to interface to a legacy PBX system using a SGT1 or SGE1 circuit provided by a voice switch. Off-system extensions digits can be manipulated using a translation table. Digit manipulation, including the Dial Out Prefix, will not be applied to these calls.	Not applicable.

8.2.5 On-Net Dialing

MiVoice Connect supports On-Net Dialing (OND), an enhancement that allows users to create more flexible dialing plans than before. The On-Net Dialing feature allows users to divide phone numbers into two separately-managed parts:

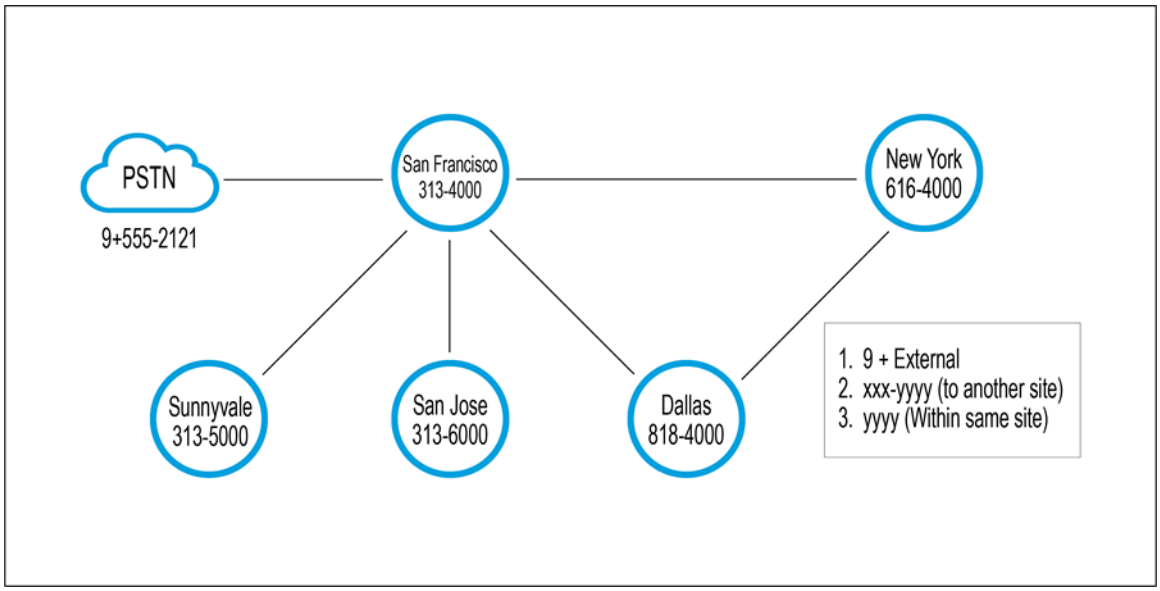
- The extension prefix is typically 3 digits in length; it is similar in concept to a site code.
- The user extension is typically 4 digits in length; it acts as the number you would dial to reach other users in your organization.

By dividing phone numbers into two parts, the OND feature provides customers with a more seamless method of migrating from their legacy phone systems to the newer MiVoice Connect system. OND allows customers to preserve their existing dialing plans when integrating Mitel equipment with their legacy equipment. While previous releases allowed customers to integrate Mitel equipment with their legacy PBX, the configurations needed to maintain the customer's existing dialing plan were complex and the complexity increased with the number of people and extensions involved.

For example, if one company acquired another company and the two companies wanted to merge their phone systems, then no two users could have the same user extension, even if they were at different sites with different prefixes.

With OND, users can call other users within a site by dialing only the user extension. For inter-site calls, the users press the numbers of the prefix and the user number. Legacy PBX systems still use off-system extensions (OSEs) to route inbound calls.

Figure 13: Abbreviated Four-digit Dialing with Extension Prefix



As the Abbreviated Four-digit Dialing with Extension Prefix figure above shows, On-Net Dialing assigns extension prefixes to each site or to a group of sites. All calls are placed on the network if they are within the same prefix, and the user need only dial the user extension. Calls preceded with the trunk access code, which is usually 9, are sent to the PSTN.

8.2.5.1 Benefits of On-Net Dialing

- Scalability — For larger organizations, On-Net Dialing enables the creation of a common and consistent dialing plan that can be replicated throughout an organization that has many offices. For example, a department store might have a phone in each of its different departments with one for clothing, furniture, kitchenware, etc. With On-Net Dialing, a user can assign the extensions of 4000, 5000, 6000, and 7000 to each of these departments. By modifying the 3-digit site code/extension prefix at each location, this approach of assigning 4-digit extensions to departments can be replicated across an entire department store, nationwide, so that a user who knows the extension for the automotive department in one city could travel to another city and would know how to reach the automotive department if he knew the site code.
- Preserve existing legacy dialing plans — To preserve the existing dialing plans when adding Mitel equipment to a deployment with legacy equipment, assign a new prefix to each new site or to users on the new MiVoice Connect system.
- Legacy integration via OSEs (Off-System Extensions) — Ability to call multiple legacy PBXs from the MiVoice Connect system.
- Multi-tenant — On-Net Dialing allows a landlord to maintain one phone system at a building that houses two or more businesses or organizations in such a way that neither organization is aware that the infrastructure or trunk lines are being shared. Despite the fact that both organizations are in the same building, you can assign different prefixes to each company and could then hide one organization's phone numbers from the other group so that neither group would see the other.

8.2.5.2 Configuration

The process of configuring On-Net Dialing consists of the following tasks:

- Planning and configuring the dialing plan
- Adding sites

- Associating an extension prefix with a site
- Assigning user extensions

The following sections include details for each of these tasks.

Note:

Small Business Edition does not support On-Net Dialing.

Enabling On-Net Dialing is an irreversible process. It permanently changes the database. Therefore, plan carefully before proceeding with the configuration

8.2.5.3 Planning and Configuring the Dialing Plan

Assigning extension prefixes to a specific digit must be done all at once. Once the dialing plan has been configured and saved, there is no way to make changes to the extension prefix assignments without erasing the database and starting all over. Therefore, we recommend carefully planning and reviewing your dialing plans before configuring the dialing plan window.

System extensions are not associated with a hard port in the system. They are always global and have a user number and a null extension prefix. Therefore, these system extensions are not affected by changes made to the extension prefix on the Dial Plan page in Connect Director. Only dialed numbers, such as user extensions, menus, workgroups, and distribution lists, are affected by changes to the extension prefix.

For details about configuring the dialing plan, see the *MiVoice Connect System Administration Guide*.

8.2.5.4 Adding Sites

You can add the sites via Connect Director before configuring your dialing plan, or you can configure your dialing plan and then add sites at a later time. For information about how to add sites, see the *MiVoice Connect Sites* chapter of the *MiVoice Connect System Administration Guide*.

Once you have created the dialing plan and saved your dialing plan configurations, you can return to the Sites page in Connect Director to verify that the changes have been propagated throughout the system.

8.2.5.5 Adding Users to the System

When the On-Net Dialing feature has been enabled and the extension prefix for a site has been updated, the first new user added to the system may not receive the site's new prefix. This issue is caused by cookies in the system populating the new user's extension with outdated information. However, after this first user has been added, subsequent users will have their extensions automatically populated with the correct site prefix.

Note:

User numbers can vary in length from 3 to 5 digits. All user numbers in the system must be the same length.

8.3 Quick Reference of Star Codes

Certain features and functions can be performed via the telephone interface through the use of star codes. By pressing the star key, or asterisk, on your phone's keypad, followed by a combination of numbers, you can perform many tasks that would otherwise require the use of a soft key, option button, or programmable button.

8.3.1 Common Star Codes

Table 22: Common Star Codes

Function	Star Code
Park a call	*11 + ext.
Unpark a call	*12 + ext.
Picking Up a Remote Extension	*13 + ext.
Picking Up the Night Bell	*14
Using the Intercom	*15 + ext.
Barge In	*16 + ext.
Silent Monitor	*17 + ext.
Toggling the Hunt Group Status	*18 + Hunt Group ext.
Whisper Page	*19 + ext.

Function	Star Code
Silent Coach	*22 + ext.
Move a call	*23 + ext.
Changing Availability State and Forwarding	VoiceMail + password +# + 72
Changing Extension Assignment	VoiceMail + password + # + 731
Unassign Extension Assignment	VoiceMail + password + # + 732
Assign Extension to External Number	VoiceMail + password + # + 733

8.3.2 Extension Assignment Star Codes

Table 23: Extension Assignment Star Codes

Function	Star Code
Transfer a call	** + destination + # #
Conference a call	** + destination + **
Hold a call	**
Hang up	# #
Access other “common” star codes	** + *star code (between 11 and 19) + ext.

8.3.3 Trunk Star Codes

Table 24: Trunk Star Codes

Function	Star Code
Blocking and Caller ID	*67 + ext. When a user places an external call, they can block their Caller ID using the “*67” command. The

Function	Star Code
	user dials *67, followed by the trunk access code, followed by the external number. When dialing in this manner, the call will be considered “non-routable” and will only access trunks at the local site. The number is dialed “as is” (as if a user dialed it). No digit manipulation will be performed.
Unblocking Caller ID	*82 + ext. When a user places an external call, they can unblock their Caller ID using the “*82” command. The user dials *82, followed by the trunk access code, followed by the external number. When dialing in this manner, the call will be considered “non-routable” and will only access trunks at the local site. The number is dialed “as is” (as if a user dialed it). No digit manipulation will be performed.

Network Call Routing 9

This chapter contains the following sections:

This chapter provides an overview of call routing and digit-manipulation capabilities of the MiVoice Connect system. The information in this chapter is particularly useful for administrators of larger, multi-site installations.

9.1 Overview

When a phone number is dialed in a MiVoice Connect system, the system performs three distinct operations on the telephone number:

- Digit collection — Voice switches collect the digits in a telephone number.
- Network call routing — After collecting the digits, the switch checks the number against a user's call permissions, adds trunks to the route list, and makes a final route decision for the call.
- Digit manipulation — The switches manipulate the dialed numbers before outpulsing them to the service provider.

This chapter describes how to plan your network call routing.

9.2 Define Network Call Routing

Once an external telephone number has been collected, the switching software checks the number against the user's call permissions, finds the list of available trunks, and then makes a routing decision based on several criteria.

9.2.1 Call Permissions

Each dialed number is compared against the user's call permissions. If the call is denied, the calling party will be routed to a fast busy intercept tone. If the call is allowed, the routing continues.

Complete the following steps to define call permissions:

1. Launch Connect Director.
2. In the navigation pane, click **Administration** > **Users** > **Class of Service** > **Call Permissions**. The **Call Permissions** page is displayed.
3. Click the name of the call permissions you want to edit.

   The **General** tab in the details pane displays parameters for the selected call permissions.
4. Under **Scope**, select the scope for the call permission.

5. In the **Restrictions and Permissions** fields, enter the desired restriction and permission rules, which are applied in addition to the scope setting.

> **Note**:
>
> Refer to the *MiVoice Connect System Administration Guide* for guidelines about entering restrictions and permissions.

9.2.2 Account Codes

If Account Code Collection Service is enabled, when a user dials a number that is outside the scope of his or her call permissions, the call is automatically routed to the Account Code Collection Service extension on the Headquarters (HQ) server or Distributed Voice Server (DVS). The Account Code Collection Service captures call details that can be reviewed in the call detail reports. For more information on these reports, refer to the MiVoice Connect System Administration Guide.

The collection of account codes is enabled on a per-user group basis and can be set to be one of three states: disabled, optional, or required.

The Account Code Collection Service is associated with a configurable extension and has a dedicated user group that defines ultimate call permissions and trunk group access.

When account code collection is enabled or required for a member of the user group, calls placed via the telephone or the Mitel Connect client are first filtered by call permissions. Calls restricted by call permissions are automatically routed to the extension associated with the Account Code Collection Service. Upon receiving the call, the Account Code Collection Service prompts the user to enter an account code and press the pound (**#**) key.

If the user enters an account code that does not match the digits in a stored account code, the system plays a message explaining the problem and prompts the user to re-enter the account code. When the user enters an account code that matches one of the stored codes, the code is collected, and the call is completed.

Call Permissions specifies the dialed numbers that are directed to the Account Code Collection Service for any user groups configured for account codes.

Calls redirected to the account codes extension are completed using the trunk access and call permissions associated with the Account Code Collection Service.

The Account Code Collection Service examines outbound calls against two sets of permissions:

- The call permissions for the caller’s user group are checked to determine if an account code must be collected.
- If user group permissions specify the collection of an account code, a check is performed on the call permissions for the Account Code Collection Service to determine whether the call will be permitted or rejected.

If the call is rejected, the intercept tone is played.

The Account Code Collection Service is associated with a system extension hosted on a SoftSwitch that runs on the HQ server or user's managing DVS.

If the SoftSwitch is unavailable to the Voice Switch from which a call originates, the call is handled according to the permissions set for the caller's user group. Calls placed by users who are configured for optional account code collection are placed. Calls placed by users who are configured for required account code collection are rejected.

Wildcard characters, which are represented with a question mark, can be used in place of DTMF digits in the account code. When wildcards are used, a length check is performed instead of a more thorough validation of the code. Although this reduces the stringency of the validation process, it allows the system to support a large number of account codes.

For more information about account codes and account code wildcards, refer to the *Setting Call Control Options* chapter in the *MiVoice Connect System Administration Guide*.

9.2.3 Trunk Availability

For a trunk to be included in the list of possible trunks that can be hunted, the following conditions must apply:

- The trunk must have an access code that matches the access code dialed.
- The trunk must be assigned to the user. Trunk groups are assigned to user groups.
- The trunk must be capable of the requested service — Local, Long Distance, International, n11, 911, Easily Recognizable Codes, Explicit Carrier Selection, and Operator Assisted. These services are defined on the Trunk Groups page.
- The trunk must be in service.
- The trunk must not already be in use.
- The trunk must be on a switch that the user's switch can reach, meaning the network is up and running.
- For multi-site calls, the admission control must be met at both sites. Admission control is defined on the Sites page.
- If the call is long distance from the trunk, it was not local to the caller. For example, network call routing will not send a local call through a trunk in another state.

9.2.3.1 Defining Trunk Services

1. Launch Connect Director.
2. In the navigation pane, click **Administration** > **Trunks** > **Trunk Groups**. The **Trunk Groups** page is displayed.
3. In the list pane, click the name of the trunk group you want to edit.

   The **General** tab in the details pane displays parameters for the selected trunk group.
4. Select the **Outbound** tab.
5. Under **Trunk services**, select the check box next to each service to enable for the selected trunk.

Refer to the *MiVoice Connect System Administration Guide* for more information about configuring trunk groups.

9.2.3.2 Defining Admission Control

1. Launch Connect Director.
2. In the navigation pane, click **Administration** > **System** > **Sites**. The **Sites** page is displayed.
3. In the **list pane**, click the name of the site you want to edit.
4. In the **Admission control bandwidth** field, enter the desired value.

Refer to the *MiVoice Connect System Administration Guide* for more information about configuring sites and for instructions about computing admission control bandwidth.

9.2.4 Specifying Parameters for the Routing Decision

After the available set of trunks is established, the switching software makes a routing decision, with the goal of minimizing toll charges and WAN bandwidth. The Network Call Routing algorithm bases the routing decision on the Local Area Code, Additional Local Area Codes, and Nearby Area Codes defined on the Trunk Groups page.

9.2.4.1 Network Call Routing Algorithm

When multiple trunks meet the same criteria, a trunk is seized randomly. In general, trunks that are configured last are hunted first. Over time, however, as trunks are deleted and added, hunting becomes increasingly random.

SIP trunks are given precedence over digital trunks, which are given precedence over analog trunks in all routing decisions. When determining the routing decision, the algorithm poses the following questions:

1. Is there a trunk at the originating site for which the call is local?
2. Is there a trunk at the proxy site for which the call is local?
3. Is there a trunk at any other site for which the call is local?
4. Is there a trunk at the originating site for which the call is considered nearby?
5. Is there a trunk at the proxy site for which the call is considered nearby?
6. Is there a trunk at any other site for which the call is considered nearby?
7. Is there a trunk at the originating site designated for long distance?
8. Is there a trunk at any proxy site designated for long distance?
9. Is there a trunk at any other site designated for long distance?
10. Are there any remaining trunks available at originating site?
11. Are there any remaining trunks available at the proxy site?

9.2.4.2 Specifying Parameters for the Routing Decision

1. Launch Connect Director.
2. In the navigation pane, click **Administration** > **Trunks** > **Trunk Groups** > **Trunk Groups**. The **Trunk Groups** page is displayed.
3. In the **list pane**, click the name of the trunk group you want to edit.

   The **General** tab in the details pane displays parameters for the selected trunk group.
4. Select the **Outbound** tab.
5. Select the **Outgoing** check box.
6. Enter values in the **Local Area Code**, **Additional Local Area Codes**, and **Nearby Area Codes** fields.
7. In the **Local prefixes** list, select the local prefix exceptions list to use for the selected trunk group.

You can create and edit local prefix lists on the **Local Prefixes** page (**Administration** > **System** > **Local Prefixes**). The Network Call Routing algorithm handles prefix exceptions for the local area code as long distance, which minimizes toll charges.

Refer to the *MiVoice Connect System Administration* Guide for more information about the Trunk Groups page and the Local Prefixes page.

The area codes on the Sites page have no impact on call routing decisions.

Planning Applications and Services 10

This chapter contains the following sections:

This chapter reviews the key MiVoice Connect applications and services to use to plan your system configuration and determine the equipment you need for completing deployment.

10.1 Account Code Collection Service

MiVoice Connect supports account codes for external calls when you enable the Account Code Collection Service. When a user dials a number that is not included in the scope of his or her call permissions, the call is routed to the Account Code Collection Service extension, where the user is prompted to enter a valid account code. Account code collection is enabled on a per-user-group basis and can be set to be one of three states: disabled, optional, or forced. The Account Code Collection Service is associated with a configurable extension and has a dedicated user group that defines ultimate call permissions and trunk group access.

A new user group is created during installation for use by the Account Code Collection Service. This user group is named Account Codes Service. Since it is only intended for use by the Account Code Collection Service, this group does not appear in drop-down lists for the assignment of User Groups to users and other objects such as workgroups. You can, however, change all attributes of the Account Codes Service User Group except the fields indicating whether Account Codes are disabled, optional, or required.

The Account Code Collection Service is distributed across all HQ and DVS servers and is associated with a system extension that is hosted on the SoftSwitches running on each HQ and DVS server. If the SoftSwitch is not reachable by the originating Voice Switch, the call is handled according to the setting on the caller's user group. Specifically, during such a connectivity outage, calls placed by users who have optional account code collection are automatically placed, and calls placed by users who have forced account code collection are automatically rejected.

10.1.1 Account Codes

Account Code Collection Service supports up to 50,000 account codes with a maximum of 20 characters. You can include non-numeric characters, such as hyphens and slashes, in the account codes; however, non-numeric characters are not used in account code collection or in the account code reports. An account code can be the same as a prefix for another account code. For example, the account codes 1234 and 12345 can coexist.

Account Code Interpretation Example gives example account codes and how the Account Code Collection Service interprets the code.

Table 25: Account Code Interpretation Example

Sample Account Code	Recorded Code
Sales 200	200
1001-3	10013
1.234A	1234
3000 Exec 2	30002

Account codes can also have user-friendly names of up to 50 characters.

10.1.2 Call Permissions

The call permissions define what dialed numbers are directed to the Account Codes Service for user groups configured with account codes. For calls that are redirected to the account codes extension, the call is completed with the trunk access and call permissions of the Account Codes Service.

This structure imposes two sets of permissions on outbound calls:

- The call permissions for the user group of the user who places the call are used to determine if an account code must be collected or not.
- The call permissions for the Account Codes Service determine whether calls are finally placed, or if the intercept tone is to be played.

10.1.3 Distributed Voice Mail

Distributed Voice Mail provides greater availability. Each Distributed Voice Server (DVS) has an instance of the telephony platform, allowing full functionality of voice mail and auto attendant services at that location during WAN outages. The Distributed Voice Mail feature allows users with mailboxes on that server to receive and pick up voice mail messages without having to depend on a WAN connection to the headquarters server that hosts the configuration database. The message waiting indicator (MWI) lights correctly update local users about voice mail with or without WAN connectivity.

Additionally, incoming calls reach the auto attendant, access the dial-by-name directory, and reach their intended local party during a WAN outage. If a party cannot be reached directly and his call handling setting would send unanswered calls to voice mail, the call is handled by the local voice mail server. If the user's voice mailbox resides on a different voice mail server, the local server will accept, store, and forward the message when connectivity to the proper voice mail server is restarted. The caller hears a generic greeting, including the intended party's recorded name, and the caller has the option to leave a message. This message will be forwarded at a later time to the home voice mail server for the addressee through SMTP.

Although each voice mail server is autonomous in delivering voice services, it must have connectivity to the headquarters server in order to carry out configuration changes. Specifically, users on an isolated remote server are not able to change availability state or make other changes that require modification to the configuration database on the headquarters server.

The Mitel Connect client applications may provide limited call control access and might not display some contents on IP phones at a remote site during WAN outages. These both require connectivity to the headquarters server for full service. For users who have their Mitel Connect client application running at the time of a WAN outage, graphical access to their voice mail box is provided, including the ability to compose and playback messages, but Mitel Connect client may not display the corresponding call activity associated with any actions.

You should provision a DVS at any site with more than 100 users to effectively manage your WAN bandwidth between that site and the headquarters or main site. In addition, you must add a distributed server with the voice mail application at any site where the required number of mailboxes exceeds 1,000.

Users should be configured for the server that is located at their home or most frequent site. If that site does not have a server, the nearest server or headquarters server should be used.

When there are multiple voice mail servers, the system-wide voice mail extension automatically maps to the extension of the local server. Voice mail media streams are therefore recorded in the CDR reports by the voice mail extension that actually handles the call.

The MiVoice Connect system provides each user with six availability states, and workgroups with four routing modes, allowing employees and workgroups to customize how calls are routed. Employees typically use the Available state to route calls to voice mail after three or four rings, and use the Out of the Office state to route calls directly to voice mail.

Users should consider the following:

- Forwarding calls to a cell phone
- Forwarding calls to an external answering service for critical users or workgroups

You must enable external call handling as part of the class of service for users who want to use these options.

To enable external call handling for a class of service:

1. Launch Connect Director.
2. Click **Administration** > **Users** > **Class of Service** > **Telephony Features Permissions**.

3. Select one of the following classes of service for which you want to enable external call handling:
   - Fully Featured
   - Minimally Featured
   - Partially Featured
4. Scroll down to the **Silent monitor/Silent coach other's calls** section.
5. Select the **Allow external call forwarding and find me destinations** option.
6. Click **Save**.

You have successfully enabled external call handling for the selected class of service.

The Message Notification feature delivers a notice to users that a message has arrived for them. Notifications can be sent upon receipt of all messages, or only upon receipt of urgent messages. The system can deliver a notification to the following destinations:

- An E-mail address, which can also include a voice mail attachment in WAV format
- A pager model that allows message notification.
- An extension that allows message playback.
- An external number, such as a cell phone if it allows message playback.
- Users who address and compose voice mail through the Telephone User Interface (TUI), the Visual Voicemail application, or the Outlook Voicemail form can mark their messages with a request for a return receipt.

10.1.4 Escalation Notifications

Similarly, the MiVoice Connect system can send any of these notifications types to specific members of an escalation profile, in support of an Escalation Notification feature.

The Escalation Notifications feature is a traditional voice mail feature that allows support groups to offer round-the-clock service to their customers. For example, if a customer calls into the MiVoice Connect system and leaves a message, the voice mail system sends out a page, phone call, or email to a designated employee in the support department. If this first employee ignores his beeping pager, the next designated employee within the escalation profile list is contacted, and so on.

Employees in the escalation profile will continue to be contacted sequentially until someone listens to the voice mail. Refer to the *Configuring Users* chapter in the *MiVoice Connect System Administration Guide* for more information.

10.1.5 Auto-Deletion of Voice Mail Messages

The MiVoice Connect system also supports the ability to automatically delete user voicemail messages that are older than a specified time limit. The system administrator can set a maximum time limit for the storage of voice mail messages, and if this time limit is exceeded, messages are automatically deleted. The tool can be used to encourage users to better manage their voice mailboxes.

10.1.6 Mailbox Full Notifications

The MiVoice Connect system can be configured to notify users when their voice mailboxes are almost full. This features warns users of the impending lack of storage space to give them ample time to delete

messages, as opposed to logging into their voice mailbox only to discover that the mailbox is full. Once a user's mailbox has passed a threshold, the system sends a notice informing them that their mailbox is almost full and that there is only enough room for 10 additional messages. This prevents users from being caught off-guard by an unexpected notification that their mailbox is full.

Refer to the *Configuring Users* chapter in the *MiVoice Connect System Administration Guide*.

10.1.7 AMIS Protocol Support

The MiVoice Connect system can send and receive voice mail messages to and from legacy voice mail systems that use the AMIS protocol Version 1 - Specification; February 1992. To send voice mail messages to remote AMIS sites, the MiVoice Connect system dials the access phone number for the remote system. Likewise, to receive voice messages from a remote system, the remote system must know the number to dial into the MiVoice Connect system. To reach the MiVoice Connect system, the remote system must be configured to dial any number that reaches an auto-attendant menu.

Note:

The Small Business Edition system does not support AMIS.

MiVoice Connect enables AMIS call support by default. Incoming AMIS voice mail is delivered in the same manner as other voice mail; however, replies cannot be sent. To send outbound AMIS voice mail, you must create AMIS systems in Connect Director.

MiVoice Connect negotiates the setup, handshaking, and teardown of AMIS system calls. Each voice mail requires a call over the AMIS delivery and call-back numbers.

10.1.7.1 Simplifying AMIS Systems, and Increasing Usability

To simplify AMIS systems and improve usability, adhere to the following guidelines:

- Use the same extension length across your enterprise.
- Use off-system extensions to match remote users' mail boxes with their extension numbers.
- To identify the remote site location, assign each system a System ID.

For more information on AMIS systems, refer to the *MiVoice Connect System Administration Guide*.

10.1.8 SMDI Protocol Support

The MiVoice Connect system supports the SMDI protocol. Two modes of operation are supported:

- In the first mode of operation, the MiVoice Connect system acts as a PBX for a legacy voice mail system. The MiVoice Connect system provides call information for forwarded or direct calls to the

legacy voice mail system, and receives incoming message waiting indication from the legacy voice mail system.

- In the second mode of operation, the MiVoice Connect system acts as the voice mail system for a number of users on a legacy PBX.

Both configurations require a serial link between a MiVoice Connect server and the legacy voice mail system, as this is the medium required by the SMDI protocol.

If using the first mode mentioned above, a group of analog trunks must be used to connect the MiVoice Connect system to the legacy voice mail system where the MiVoice Connect system is on the extension side of the trunks. The MiVoice Connect voice mail application manages the group of outgoing extensions. The MiVoice Connect server can provide digit translation if the legacy voice mail and MiVoice Connect system have different extension lengths.

It is possible to have some MiVoice Connect users on the MiVoice Connect voice mail and some on the legacy voice mail. However, these users will not be able to send messages to each other unless AMIS is implemented between the two systems. Voice mailboxes for workgroups and agents must be on the MiVoice Connect voice mail system.

Mitel Connect client operates the same way it does when a user has no mailbox:

- Voice mail viewer is not available
- Windows Control Panel does not contain Voice Mail tab
- Find Me and Notification features are not available
- Dial Mailbox and Transfer to Mailbox are not available for this user from other user's clients
- To Voice Mail button on Mitel Connect client transfers the call to the system voice mail extension

For more information about using a serial link and SMDI protocol to integrate the MiVoice Connect system with a legacy voice mail system, refer to SMDI Protocol Support on page 302.

10.1.9 Find Me Call Handling

Find Me and Auto Find Me call handling allow callers to find users at other locations when they reach the user's voice mail. When Find Me is enabled for the current availability state, inbound callers that reach a MiVoice Connect user's voice mail box can activate Find Me call handling by pressing **1**. If the caller activates Find Me call handling, the system plays a prompt indicating that it is now finding the called party: "Please hold while I try to find your party."

MiVoice Connect users can specify two Find Me destinations, which can be internal or external numbers. These numbers can be enabled or disabled for each availability state. If a call is forwarded to the first number and is not answered within a configurable number of rings, the call can either be forwarded to a second Find Me destination or can be returned to voice mail.

The Caller ID that appears on Find Me calls is the voice mail Caller ID and not the ID of the original caller. However, if the source of the original call is external to the system, then the Caller ID will be displayed. Personal Assistant (pressing "0") also works when Find Me forwarding is enabled. The voice mail system dials the configured Find Me numbers in sequence. When a Find Me call is answered, voice mail announces the call through a sequence of prompts.

The party that answers a Find Me call hears prompts similar to the following:

- “I have a call for Sam Smith from 4085551212”.
- “To accept this call, press one.”
- “To send this call to voice mail, press two.”
- “To repeat the caller ID, press three.”

The party at the Find Me number has three options for directing the call:

- Pressing **1** connects the original caller with the intended party at the Find Me destination.
- Pressing **2** directs the voice mail system to immediately start taking a message for the intended party from the original caller.
- Pressing **3** repeats the Caller ID information available on the call, if any. This also extends the timeout by 1 ring, or 6 seconds.

The voice mail system does not automatically notify callers of the Find Me call handling option. MiVoice Connect users can elect to tell callers of the Find Me option in their recorded greeting. For example, they can tell callers to “press 1 to Find Me.” If the user does not tell callers about the Find Me option in their greeting, the Find Me option can remain a hidden capability available only to selected callers. Conversely, users can automate the Find Me behavior so that when a call enters voice mail and Auto Find Me is enabled, the call is immediately sent to the Find Me destination numbers without requiring any action on the part of the caller.

10.1.10 Call Sender

Users can place a return call to the originator of a voice mail by pressing **5** from the phone during message playback. Users can also call back the voice mail sender from Mitel Connect client, Agent Monitor, or Microsoft Outlook, if the user is so provisioned. To use this feature, the user must belong to a user group with trunk-to-trunk transfer Class of Service enabled. For more information, see the *MiVoice Connect System Administration Guide*.

The user has the option of replying with either a voice message or a phone call if Caller ID information is available on the call. If no Caller ID information is available for the call, such as on calls from an outside caller, the **reply with a call** option is not available for that message.

When the user chooses to reply with a phone call, the call is transferred to the number of the originating party. When the originating party is an external caller, the message recipient must have the dialing permission to dial the Caller ID number. Once the message recipient is transferred to the number of the message originator, there is no option to return to the mailbox.

10.1.11 Time Stamps

The time stamp of the message is relative to the time on the server where the message is taken, as shown in the following examples:

- When the user views messages in the Voice Mail Viewer or Outlook Form, the user interface will adjust the time stamp based upon the time of the user’s computer.
- When the user dials into voice mail to retrieve their messages, the time stamp will be based on the time of the server.

10.2 Planning Fax Handling

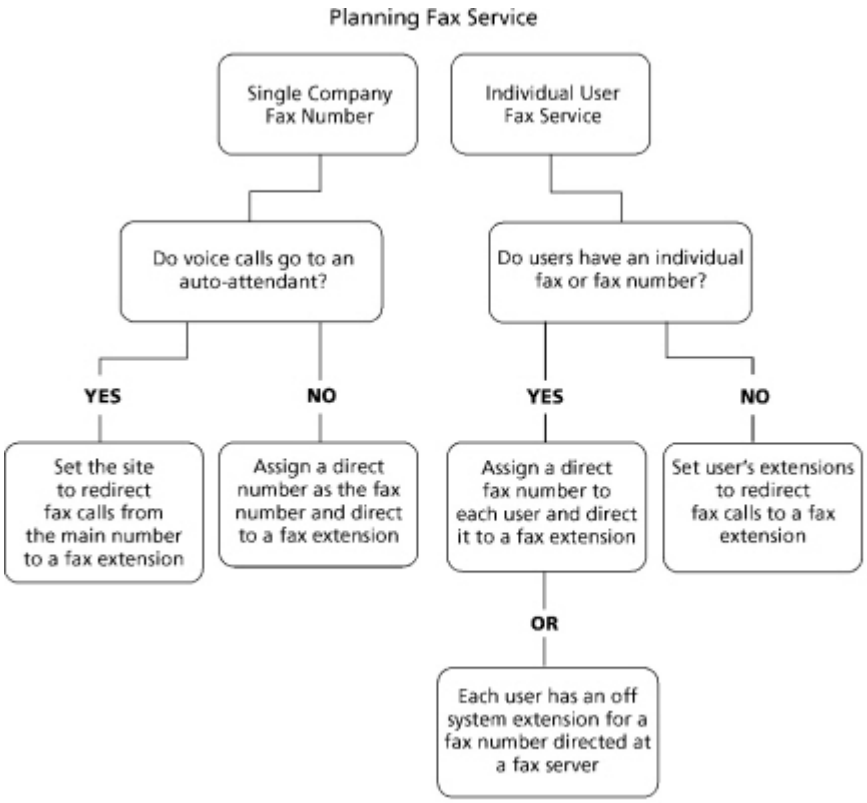
The MiVoice Connect system supports fax calls. There are several ways to configure your fax service:

- A direct fax number for each site
- Direct fax numbers for each user using either individual fax machines or a fax server
- Redirect faxes that are sent to the site's main number to a fax machine extension at the site
- Redirect faxes that are sent to a user's extension to user's local fax extension

10.2.1 Fax Options

Planning Fax Service shows how to plan your fax options.

Figure 14: Planning Fax Service



Determining how you configure your fax service with Connect Director depends on which method of fax call handling you have chosen. Refer to the steps in the following sections for information about using each method.

10.2.1.1 Using Main Number for Voice and Fax calls, and it Goes to Auto-Attendant

Using the Main Number for Voice and Fax calls, and the Main Number Goes to an Auto-Attendant

1. Configure the fax extension through the Users page in Connect Director.

> **Note**:
>
> Ensure that fax redirection is disabled for fax extension users.

2. On the **Sites** page (**General** tab), enter the fax extension you created in the **Fax redirect extension** field.

10.2.1.2 Using Main Number for Voice and Fax Calls, and it Goes to an Operator

Using the Main Number for Voice and Fax Calls, and the Main Number Goes to an Operator

1. Configure the fax extension through the Users page in Connect Director.
2. Assign a direct number as the fax number.
3. On the **DNIS** page for appropriate the trunk group, set the destination to the fax extension.

10.2.1.3 If Users Have Their own Faxes or Fax Service

If Users Have Their own Faxes or Fax Service

1. Configure the fax extensions through the Users page in Connect Director.
2. Assign a range of direct fax numbers.
3. On the DNIS page for appropriate the trunk group, set the destination for each fax number to the appropriate fax extension.

10.2.1.4 If You Plan Each User to Have a Single Number for Both Voice and Fax

If you plan for each user to have a single number for both voice and fax, follow these steps:

1. Configure the fax extensions through the Users page in Connect Director.

2. On the **Telephony** tab of the **Users** page, enable fax redirection and then enable fax redirect for the site by entering a fax extension in the **Fax redirect extension** field on the Sites page.

For more information on these settings, refer to the *MiVoice Connect System Administration Guide*.

10.2.2 Using a Fax Server

A fax server improves services available to your users, helping them be more productive. With a fax server, users can perform the following functions:

- Send faxes directly from the desktop eliminating the need to print faxes to send.
- Receive faxes directly on the desktop.
- Integrate fax communications with e-mail and voice mail applications.
- Have individual fax numbers.
- Maintain soft copies of all faxes for easy printing and document management.

Using a fax server with the MiVoice Connect system provides the following benefits:

- Share inbound and outbound trunks for fax services.
- Reduce toll charges by leveraging your VoIP network for outbound faxes.

For inbound fax support, users can be assigned a personal fax number from the DID range of one of the trunk groups and this DID number can be the same as the user's regular telephone extension. When a call is received, if the fax redirect feature is enabled, the system can differentiate between voice calls and fax calls and react appropriately.

Outbound faxes are queued by the server and then sent across the IP network to the best available trunk.

10.2.2.1 Fax Server Requirements

- Sufficient ports on MiVoice Connect voice switches
- Sufficient MiVoice Connect User Licenses
- Sufficient DID trunks to support both fax and voice DID for all users

10.2.2.2 Network Requirements

The network requirements for faxing over IP are more stringent than for voice over IP. For voice communications, a 1% packet loss has negligible impact on voice quality. However, a 1% packet loss for fax communications means a loss of approximately 3 lines per fax page. Mitel recommends that packet loss not exceed 0.1% across the LAN and WAN when using fax servers with the MiVoice Connect system.

Fax communications are also impacted by voice compression. Since fax machines typically require 19.2 Kbps, Mitel recommends that you use G.711 voice encoding for fax calls. For more information on fax requirements, refer to IP Phones on page 148.

Note:

The fax redirect feature will not work with calls that come in on SIP trunks.

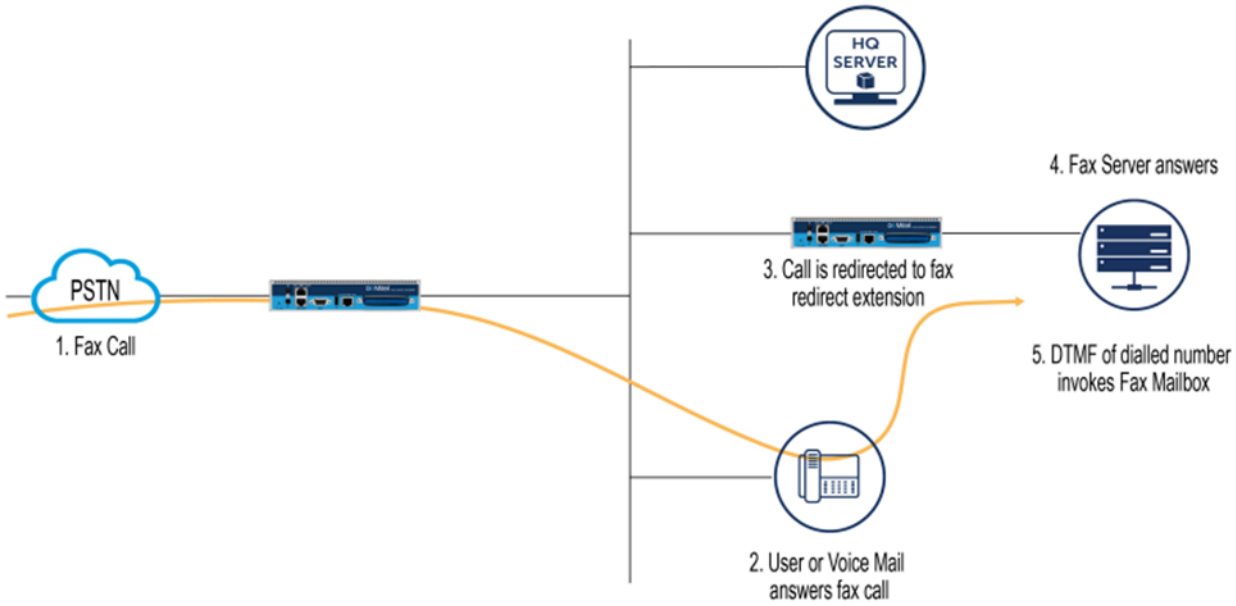
10.2.2.3 Fax Server Integration Details

Instead of requiring users to have two separate DID numbers — one for voice and one for fax — a single DID line can handle voice calls and inbound/outbound faxing.

A user's extension, which can be 3, 4, or 5 digits, is sent to a fax server via in-band Dual Tone Multi Frequency (DTMF) digits. The fax server uses this information to create a mapping between the user's extension and e-mail address.

Once configured, incoming fax calls are received at the user's phone extension. The fax server listens for the fax tone, and takes over the call when the fax redirect radio button has been selected in Director. When the fax transmission is complete, the loop current is automatically turned off to terminate the fax call, and the and fax is forwarded to the associated e-mail address.; Fax Server Integration Call Flow shows the flow for a fax call.

Figure 15: Fax Server Integration Call Flow



10.2.2.4 Enhanced FAX Server Integration

The MiVoice Connect system delivers digits to a Fax Server for DID calls routed directly to a FAX server, thus allowing the call to go directly to the fax extension and provide DID/DNIS digits, instead of to an extension number and then to the fax server.

10.2.2.5 Configuring Fax Server Integration

At a high level, the process of setting up the Fax Server Integration feature involves three tasks:

- Connecting the hardware (i.e., connecting the fax server ports to the analog ports on the switch)
- Creating a user account to represent each analog port
- Enabling the Fax Server Integration feature for each user account

10.2.2.6 Configuring the Fax Server Integration Feature

1. Configure a fax server per the manufacturer's instructions.
2. Connect the fax server to one of the analog ports on a Voice Switch that supports analog.
3. Create user accounts to represent each analog switch port that connects to the fax server.
4. Launch Connect Director.
5. In the navigation pane, click **Administration** > **Users** > **Users**. The **Users** page is displayed.
6. Click **New**. The **General** tab is displayed with blank parameters.
7. On the **General** tab, enter information for the following fields:
   - License Type — Extension-Only
   - User Group — Select the user group that you have already appropriately configured for a fax server. The User Group should have the Class of Service for Call Permissions set to No Restrictions to transfer inbound and outbound faxes
   - Primary Phone Port — Select the Port radio button and then use the drop-down menu to select the switch where the fax server will be connected.
   - Include in System Dial By Name Directory — Enable this option if you want callers to be able to locate the fax number using the Dial by Name feature.
8. Click the **Telephony** tab, and do the following:
   - In the Call stack depth field, enter **1**.
   - In the **Fax support** field, select **Fax Server** from the drop-down list
9. Click the **Voice Mail** tab, and enable the **Accept broadcast messages** option.
10. Click **Save**.
11. Configure the availability state for each of the user accounts associated with a port connected to the fax server.
12. On the **Users** page, select the user account representing the fax server connection.
13. Click the **Routing** tab and the **Availability States** subtab.
14. On the **Available** subtab, in the **Call forward condition** field, select the **No Answer/Busy** option.
15. In the **Busy destination** and **No answer destination** fields, specify the analog port where incoming fax calls will be directed if the first fax port is busy

    For example, if you have set up three ports to receive fax calls, you might configure the first port in this series to redirect to the second port, and the second port would specify the third as a failover.
16. Click **Save**.

This configuration assumes multiple analog ports will be used to connect the switch to the fax server. If only one fax server port will be used to connect to the fax server, then set the Call forward condition field

to Never. Similarly, if this port is the last one in a chain of ports dedicated to the fax server, then the Call forward condition field must be set to Never.

If you are using multiple analog switch ports to connect to the fax server you must specify the first redirect extension in that chain. This is the site's fax redirect extension.

1. Launch Connect Director.
2. In the navigation pane, click **Administration** > **System** > **Sites**. The **Sites** page is displayed.
3. Click the site where the switch and fax server are located.
4. On the **General** tab, in the **FAX redirect extension** field, enter the extension associated with the first port in the chain of fax server ports.

> **Note**:
>
> This is the first place incoming faxes will be sent.

5. Click **Save**.
6. Configure settings for each user that will be using the Fax Server Integration feature.
7. In the navigation pane, click **Administration** > **Users** > **Users**. The **Users** page is displayed.
8. Click the name of a user who will be using the Fax Server Integration feature.
9. Click the **Telephony** tab, and in the **Fax support** field, select **User-Redirect** from the drop-down list.
10. Click **Save**.

10.3 Private Numbers

Users can have private numbers that are not listed in the System Directory or in Mitel Connect client Quick Dialer and for which Caller ID information suppressed. Private Numbers are enabled through a check box on the User edit page in Connect Director. When checked, the user's extension becomes a Private Number.

10.3.1 Conditions for Private Numbers

- Private Numbers do not appear in the QuickDialer for dial-by-name operations or in the Connect Directory Viewer.
- Calls placed from a Private Number to an internal party show the caller's name but not his or her number to the dialed party.
- Calls placed from a Private Number to an external party do not deliver a Direct-Inward-Dial (DID) number as Caller ID when PRI trunks are used for the outbound call. The site CESID number is used for the outbound Caller ID.
- Calls from a Private Number to an off-system extension on PRI trunks with NI2 signaling deliver calling name information but not calling number information.
- Routing slips and the Mitel Connect client History viewer show the Private Number user's name but not his or her extension number.

- The Private Number users are listed with name and number in the **Extension Monitor extension selection** dialog box.
- The Private Number user can be dialed directly via the telephone or the Mitel Connect client if his or her extension is known.
- Contacts imported from Outlook or Exchange are never private and are fully visible in the Mitel Connect client Quick Dialer.
- CDR database records show both number and name for Private Number users. However, the Caller-ID Flags field indicates that only the name is valid.
- CDR legacy log files show the number of Private Number user calls that are inbound or outbound calls.
- Connect Director shows number information for Private Number users as with other users, for example on the User list page.

10.4 Auto Attendant

The MiVoice Connect system comes bundled with an automated attendant feature that runs on the HQ servers and DVSs. The system supports up to 1000 menus, with every server having all menus and with four scheduled modes, providing a simple, flexible solution.

10.4.1 Applications for the Auto-Attendant Menus

You can set up auto-attendant menus for the following:

- Answering the main number
- Routing calls to workgroups, such as sales, support, and so on
- Providing automated directions
- Providing a way for users to log in to voice mail. Mitel recommends using the “#” button.

Although the automated attendant is a useful tool, you should take care to design a menu structure that does not frustrate your callers. Here are some helpful hints to keep in mind:

- Create no more than two or three levels of menus.
- Provide a **zero-out** option on every menu, so the call can go to a live person. Mitel recommends using the **0** key for this option.
- Provide an option to return to the previous menu. Mitel recommends using the * key for this option.
- Keep prompts short, quick, and efficient.

Users can record auto attendant menu prompts from their own telephone instead of having to go through Director. This ability frees the system administrator from having to be involved with the task of recording attendant menu menus, allowing him or her to delegate the task to more appropriate team members. For details on enabling this feature, refer to the *MiVoice Connect System Administration Guide*.

10.5 Call Handling Delegation

Some users of the MiVoice Connect system, particularly senior management, often have an administrative assistant who helps them manage items such as their e-mail, calendar, and voice communication. The MiVoice Connect system administrator can grant permission from Connect Director to individual users to

change another's current availability state settings. Users with the proper access license who have been delegated to change availability state settings can make changes to the current availability state settings for other users using the Mitel Connect client. For more information on configuring call-handling delegation, refer to the *MiVoice Connect System Administration Guide*.

10.6 Mitel Connect Client for Desktops

Mitel Connect client for Windows is the Windows-based client application that runs on the user's computer. Mitel Connect client for Windows offers the following features:

- **Search Bar:** Find a contact instantly by entering their name or number in the search bar.
- **Contact Card:** Look up information about a contact instantly, including all your interactions with the contact (also known as conversation history).
- **Contact Groups:** Create and organize your contacts into favorites and custom groups. On creating groups you can send a group message or voicemail.
- **Availability State:** Find out if your contacts are available to talk or chat by checking their availability state. Your availability state reflects your Microsoft Office Outlook schedule, whether you are in a meeting, out of office, or simply do not want to be disturbed.
- **Calling:** Call your contacts instantly through your desk phone.
- **Instant Messaging (IM):** Chat instantly with one or more contacts.
- **Call Transfer:** Transfer an incoming call to a selected contact.
- **Call Routing:** Automatically route calls to external or other numbers based on your availability state.
- **Voicemail:** Leave a voicemail message for a contact who is unavailable to talk, or record a voicemail greeting message for contacts leaving a message in your voicemail inbox.
- **Conferencing and Collaboration:** Create a conference to communicate and collaborate with a wide variety of contacts.
- **Conversation History:** Instantly check all call, voicemail, and IM history with a contact.
- **Sharing Screens:** Choose to share your screen with a contact any time on or off a call.

For a list of all the capabilities and other details about Mitel Connect client, see the *Mitel Connect Client User Guide*.

10.7 Bridged Call Appearances

The Bridged Call Appearances (BCA) feature provides "bridged" information between many separate IP phones, offering the benefit of faster call handling between users. The feature is intended for key system environments, such as a small office with a moderate number of trunks, IP Phones, and users.

Custom buttons are configured on each IP phone so that information about incoming calls to a BCA extension is shared among the phones via blinking colored LEDs. Similarly, IP phones can share information about outbound calls placed from a BCA extension by blinking green or red on each phone. Refer to the *MiVoice Connect System Administration Guide* for details.

Custom buttons can be programmed on an IP phone such that each button represents a position in the call stack.

Pressing the top-most BCA custom button for outbound calls does not necessarily access trunk 1. There is no one-to-one correlation between the custom buttons programmed for BCA extensions and a particular trunk. Trunks can be associated with BCA extensions in any manner specified by the system administrator.

10.7.1 Switch Support for Bridged Call Appearances

The voice switches support BCA functionality with the following caveats:

- Up to 24 BCA extensions can be configured per switch.
- The sum of all the trunks that are assigned to a BCA, plus the call stack size of all BCAs used for extension appearances on a switch cannot exceed 24. For example, you can configure 8 BCAs, each targeted with 3 trunks on the same switch.
- A maximum of 32 phones can be configured to point to the same BCA extension. This means that there is a single programmable button monitoring a single call stack position of the BCA extension for 32 phones. If a single phone has n programmable buttons for a single BCA for n different call stack positions, then it is considered as n phones. For example, if a single phone has 4 programmable buttons for a single BCA for 4 different call stack positions, then it is considered as 4 phones.
- Up to 128 BCA extensions on other switches can be monitored.

For details on configuring the BCA feature, see the *MiVoice Connect System Administration Guide*.

10.8 Hunt Groups

Hunt groups allow you to route calls to a list of extensions. Hunt groups can be accessed through an extension, DID, and/or DNIS. Hunt groups are supported by Voice Switches and remain available when connectivity to the servers is lost. The hunt group can be used as the backup destination for a workgroup, which allows basic hunting even when the workgroup server is not reachable. To maximize reliability, assign hunt groups to a switch close to the majority of the members and/or trunks associated with the hunt group.

Each hunt group is composed of an ordered list of users as follows:

- SG-generation switches — A maximum of 8 hunt groups and a maximum of 16 hunt group extensions per group can be assigned to a single switch.

  You can have up to 8 hunt groups on a switch. Each individual hunt group can have up to 16 members, and each hunt group can have a call stack of 16. The maximum number of members across all groups on the switch is 16.

- ST-generation switches — A maximum of 24 hunt groups with a maximum of 16 members each can be assigned to a single switch. Each hunt group can have a call stack of 24.
- Virtual switches — A maximum of 24 hunt groups with a maximum of 16 members each can be assigned to a single virtual switch. Each hunt group can have a call stack of 16.

Note:

Consider that the maximum group and member values listed here are subject to the overall capacity of the switch and must take into consideration all other features that use switch resources. Refer to the formulas in the Real Time Capacity on page 19 section.

Hunt groups have scheduled call handling modes similar to route points. For more information about route points, refer to the “Setting Call Control Options” chapter in the MiVoice Connect System Administration Guide. There are call handling modes for on-hours and off-hours/holiday (combined). For on-hours, destinations can be set for Always, Busy, and No Answer. For the other call handling modes, only a Call Forward Always destination is provided. When the hunt group is in a call handling mode other than on-hours, the hunt group forwards calls to the Call Forward Always destination.

A hunt group can be a destination anywhere in the system where a workgroup is allowed as a destination. This includes call forward destinations from users, workgroups, route points, personal assistants, site operators, site fax redirect extensions, and Find Me destinations.

10.8.1 Hunt Group Busy State

The hunt group can be set as busy from both the switch maintenance page in Director and with a star code from the Telephone User Interface. This feature allows hunt group members to disable hunt group routing when they are temporarily unavailable or leave work early. The busy state of the hunt group is maintained by the hunt group’s switch and is not saved in the configuration database or to flash memory. When a switch boots or reboots, the hunt group is in the available state.

Use the star code ***18** followed by the hunt group extension to toggle the busy state of the hunt group from a telephone. A class of service setting controls whether a user can change the hunt group busy state.

When the hunt group is in the busy state during on-hours, calls are forwarded to the busy destination.

10.8.2 Configurable Hunting

There are two types of hunting available with hunt groups: top down or simultaneous ring. All hunt group members are hunted for each call received. For example, in top-down hunting, if the switch is hunting members for an initial call when a second call is received, the second call hunts through all the members again. In other words, each call is hunted independently and in the case of top down, hunting starts at the top.

You can also configure the following:

- The number of rings per member. The same number of rings are used for each member to whom the call is offered.
- Whether calls should go to a no answer destination after all members have been hunted once or whether members are hunted again.
- Whether multiple calls are offered to a member simultaneously when the hunt group receives multiple calls. Calls are not offered to members with full call stacks.

- Whether members should be hunted when the member's call handling is set to Call Forward Always (DND).

10.8.3 Hunt Group Applications

Hunt groups provide solutions to a several call routing scenarios.

10.8.3.1 Backup Routing for Workgroup

To use a hunt group as a backup when the workgroup server cannot be reached, create a hunt group with workgroup members who will serve as backup members. To use the hunt group when the workgroup server is not reachable because of a network outage, admission control, or a server outage, set the workgroup's backup number to the hunt group. When the hunt group is set to offer each member a single call at a time, then call offering is similar to a workgroup. Hunt group members are hunted even though they are logged out or in wrap-up with respect to the workgroup.

10.8.3.2 Hunt Group as a Call Forward Destination

In a small office where individuals generally receive calls directly, users may want someone in the office to answer calls when they are unable to answer. To handle this situation, create a hunt group with everyone in the small office as a member. Individual users can set their call forward destinations to this hunt group. The hunt group can be configured with simultaneous ring, which rings to hunt members only once, and to go to voice mail with Call Forward Busy and Call Forward No Answer conditions.

When configured as described above, if a user's call was forwarded to the hunt group after it wasn't answered, the hunt switch hunts everyone in the office. If the call was not answered after the maximum number of rings, the call is forwarded to voice mail where the caller can leave a message in the original target's mailbox.

10.8.3.3 Distribution of Calls to Backup Operators

In this scenario, a primary operator who handles calls to a main company number requires one or more secondary operators to receive the calls when the primary operator becomes too busy.

To create a hunt group to back up the primary operator, create a hunt group with backup operators. Enter the main operator and all the backups as members of the hunt group in the order in which they are to serve as backups. Set the hunt group for multiple calls to be hunted to a given member, and set the call stack size for each of the users to control the number of calls he or she can receive.

When there are incoming calls to the hunt group, the primary operator is offered the calls first. The operator may be offered multiple calls concurrently up to the limit of his or her call stack. If a member's call stack is full, the member is skipped and that particular call is not be offered again unless the hunt group is set to hunt forever and no member picks up the call before the member is reached again in the hunt list.

If a member of the operator group does not answer the hunt call, the call is offered to the next member after the number of rings configured for call forwarding. Thus, even if the primary operator has room on his or her call stack, the call is offered to the next member in the list when the operator does not answer the call in time.

If you want calls to go directly to a backup when the primary operator is not available, then set the hunt group not to hunt the members when their current availability state is configured to Call Forward Always (DND). Operators can use this configuration to pass calls to other hunt group members by changing their availability state to a state that has Call Forward Always configured.

You might wish to have a hunt group that goes immediately to voice mail or another number during non-working hours. The hunt group can be configured with an off-hours schedule. Setup a schedule for on-hours during which the call handling mode for the hunt group is configured to forward calls to another number only if the hunt group is busy or no one answers. For off-hours, set the hunt group to call forward always to voice mail or another number. The auto-attendant automatically changes the hunt group's current call handling mode based upon the configured schedule.

10.8.3.4 Common Line Monitoring

A hunt group can be used for line monitoring. For example, several operators may wish to monitor the same line and all have an opportunity to answer calls at the same time. For this case, set up a hunt group with simultaneous ring. When a call is received, the hunt switch rings all operators in the hunt group whose call stack is not full to the number of rings configured. If the hunt group is set to hunt forever, when the number of rings is reached the hunt switch hunts the same users again. However, the members who have room on their call stack for additional calls may have changed, so each additional hunt may result in different phones ringing.

10.9 Pickup Groups

Group Pickup is a traditional PBX and key system feature used in group environments. The feature allows users in a pickup group to answer any ringing phone in that group, and the feature works best in places where several people work together on a daily basis, such as design firms. If a group member is away from her desk and across the room while her phone rings, she can quickly answer the call from another person's IP phone by pressing the relevant soft key or programmable button, or by using a simple star command from an analog phone.

The following example may help illustrate how this feature is used.

Assume three users — Mike, Joe, and Sarah — work together and have jobs that require extensive collaboration. They also sit near one another. Their extensions — x1001, x1002, x1003, respectively — would be added to an extension list, and then this list would be associated with a pickup group.

The pickup group would have its own extension, for example x3755.

Note:

This extension is invalid and cannot be dialed, and thus acts more like a code than an extension. This non-dialable extension could be programmed into a Mitel Connect client toolbar button or an IP phone programmable button on Mike's, Joe's, and Sarah's phones.

So, assume Joe's phone, x1002, rings while he is having a conversation with Sarah at her desk. He would hear his phone ringing at his desk, yet he could press the pre-programmed button on Sarah's IP phone to answer his own call.

Alternatively, if Sarah had an analog phone, Joe could press ***13 + 3755** to answer the call.

10.9.1 Types of Extensions for Pickup Groups

Types of Extensions for Pickup Groups

- User extensions
- Workgroup extensions
- Bridged Call Appearance (BCA) extensions

Note:

Be aware that because workgroup extensions are on a separate server, using call pickup to pick up a workgroup call may have unexpected results if the workgroup server transfers the call at the same time that someone from outside the workgroup attempts to pick it up.

10.9.1.1 Details

- Pickup groups can be associated with a programmable toolbar button, or with a programmable button on an IP phone, and can work with Extension Assignment.
- The user whose phone will be picked up must have class of service “Call Pickup Allowed” to use this feature. However, other users need not be members of the pickup group to pickup a call.
- The call pickup feature will support:
  - 24 members per group
  - 16 groups per switch
  - The sum of all members assigned to all Pickup Groups on a switch cannot exceed 80.
  - A single user can be a member of up to 5 Pickup Groups.
- A single switch can host a combined total of up to 24 Hunt Groups, Bridged Call Appearances, and Pickup Groups.
- Users can use this feature in several different ways:
  - IP Phone — If a programmable button has been configured for Pickup Groups, the user can press the button, or key, and enter the extension for the Pickup Group to answer the call.
  - IP Phone — If a soft key has been programmed, the user can press the “pickup” soft key and enter the extension to answer the call.
  - Mitel Connect client — If one of the pre-programmed buttons in Mitel Connect client has been set up for Pickup Groups, a user can enter the extension of the Pickup Group to answer the call. If the key

has already been programmed with the extension of the Pickup Group, then it is not necessary to enter the extension.

- Mitel Connect client — Alternatively, the user can access the “pickup” command from the Call Menu, followed by the extension.
- Analog Phone — The user can enter the *13 command, followed by the Pickup Group extension to answer calls from an analog phone.

10.10 Workgroups

The MiVoice Connect system supports up to 256 workgroups, with up to 300 members per workgroup, with a maximum of 300 agents total in the MiVoice Connect system. A workgroup enables a group of users to appear as a single unit to calling parties. Calls can be routed in top-down, longest-idle, round-robin, and simultaneous-ring fashion. The Simultaneous Ring feature is limited to workgroups that contain a maximum of 16 members. Workgroups are typically used by support and sales groups to help automate call handling.

The Workgroup Agent Access and Workgroup Supervisor Access software licenses are required to use workgroup functionality in the MiVoice Connect system. In addition, you can run workgroup reports on the server to help you understand and assess workgroup activity and performance.

Analog phones do not display Caller ID for calls forwarded from a workgroup.

10.10.1 Agent Multiplicity

Users can be members of multiple workgroups. The workgroups can be configured for any hunt pattern and can have queuing enabled.

A single agent status is applied to all workgroups of which the user is a member. With one status, an agent is either logged-in, logged-out, or in wrap-up for all workgroups of which he or she is a member. In order to manage their own logged in status, users must be provisioned as a Workgroup Agent. Agents can manage their logged-in state via Mitel Connect client, or through the TUI menu in their voice mailbox or via their IP phone programmable button.

When an agent is a member of more than one workgroup, that agent can receive calls from any of the workgroups. When an agent is available to take calls from more than one workgroup, and the workgroup would select that agent based on the current hunt pattern for a call, the oldest call is offered to the agent.

Queue Monitor shows calls from all the queues of which the user is a member. If the user is a member of only one queue, there is no change to the interface. However, if the user is a member of multiple workgroups, the Queue Monitor shows statistics for each workgroup, and for all workgroups. The user can specify a filter to show only a subset of the queues. The filter only changes the information displayed and does not alter the hunting behavior; the user will still be offered calls from all workgroups of which the user is a member.

For workgroup supervisors the Agent Monitor shows all agents from the workgroups of which the supervisor is a member. The Agent Monitor also allows supervisors to filter agents being monitored by selecting individual workgroups.

10.10.2 Call Monitor and Barge In

Call Monitor creates a limited conference call where the monitoring party hears the other parties, but the monitored parties do not hear the monitoring party. When a call is being monitored, a warning tone may be played to the participants of the call. The warning tone can be disabled using an option for an Auto-Attendant Menu. Call center administrators typically disable the warning tone to silently evaluate agent performance. When the warning tone is disabled, the menu prompt typically informs the caller that their conversation may be monitored or recorded.

Barge In allows one party to join an existing call as a fully conferenced participant. When Barge In is initiated, a brief intrusion tone is played to the other participants.

A recording warning tone may be played to the customer during silent monitor. The warning tone is enabled from Connect Director. No tone is played during a Barge In call.

Note:

Mitel does not warrant or represent that your use of silent monitoring or barge in features of the Software will be in compliance with local, state, federal, or international laws that you may be subject to. Mitel is not responsible for ensuring your compliance with all applicable laws. Before configuring the call monitoring features, you may wish to consult with legal counsel regarding your intended use.

To simplify discussion of this feature, we will refer to three parties: the supervisor, the agent, and the customer. The supervisor initiates the silent monitor by selecting an agent. The agent is on a call with the customer. The customer may be an internal or external caller, but supervisors and agents must be on extensions.

In Silent Monitor, a supervisor hook flash is ignored. However, a hook flash by the other parties works the same as in a two-party call. In particular, an agent flash puts the call on hold and allows a consultative transfer or conference.

Because there is a limit of three parties in a conference call, if the agent or customer makes a consultative transfer or conference, the supervisor is automatically dropped. Similarly, if another party barges in a monitored extension, then the silent monitor is dropped.

If a conference call is already in progress, it cannot be monitored. If a silent monitor is already in progress, no one else can monitor the call.

The supervisor can barge in on a call he or she is silent monitoring. It is not possible to revert a barge in call to a monitored call. If desired, the supervisor can hang up and restart monitoring.

After a barge in, the agent remains the controlling party of the call. A subsequent agent hook flash disconnects the supervisor, who is the last party added.

10.10.2.1 Barge In and Silent Monitor Telephony COS Configuration

Each telephony class-of-service (COS) permission has several additional check boxes and radio buttons in Connect Director to configure Intercom/Paging, Barge In, Call Recording, and Silent Monitor.

Table 26: Barge In and Silent Monitor Telephony COS Configuration Parameters

Parameter	Definition
Allow initiation for Intercom/Paging	If this check box is selected, users within this COS may place an intercom call or page to other system users. If cleared, then no intercom/paging can be initiated.
Accept Intercom/Paging	Accept None — If selected, users within this COS may not receive intercom calls or pages. Accept All — If selected, users within this COS may receive intercom calls or pages from anyone in the COS. Accept Only From — If selected, users within this COS may only receive intercom calls or pages from the person specified in the associated field.
Allow initiation for barge in	If this check box is selected, users within this COS may barge in on the calls of other system users. If cleared, then no barge in can be initiated.
Accept barge in	Accept None — If selected, users within this COS may not receive barge-in's from anyone. Accept Al — If selected, users within this COS may receive barge-in's from anyone else with this COS permission. Accept Only From — If selected, users within this COS may only receive barge-in's from the person specified in the field accosted with this radio button.
Allow initiation for record others calls	If this check box is selected, users within this COS may record the calls of other system users. If cleared, then no call recording of others can be initiated.

Parameter	Definition
Accept record others calls	Accept None — If selected, users within this COS may not have their calls recorded from anyone. Accept All — If selected, users within this COS may have their calls recorded from anyone else with this COS permission. Accept Only From — If selected, users within this COS may only have their calls recorded by the person specified in the field associated with this radio button.
Allow initiation for silent monitor	If this check box is selected, users within this COS may monitor other system users. If cleared, then no monitoring of others can be initiated.
Accept silent monitor	Accept None — If selected, users within this COS cannot be monitored by anyone. Accept All — If selected, users within this COS can be monitored by anyone else with this COS permission. Accept Only From — If selected, users within this COS can only be monitored by the person specified in the field associated with this radio button.

There are no special permissions for Enterprise Contact Center agents or supervisors. They must have these same COS permissions with appropriate settings to enable contact center silent monitoring and barge in.

10.11 Enterprise Telephony Features

10.11.1 Music On Hold

MiVoice Connect provides two options for implementing music on hold (MOH).

- Jack-Based Music on Hold: Audio is provided through the audio input port on the Voice Switches that support MOH. A site needs only one MOH source. Overview on page 333 describes the switches that support MOH.
- File-Based Music on Hold: Audio is provided through a digital file.

10.11.1.1 Jack-Based Music on Hold

Connecting the desired music source to the selected Voice Switch provides MOH. The source can be recorded music or custom music, with prerecorded announcements or other information for callers.

Each site with music on hold must have its own music source. To conserve bandwidth, music is not sent across the WAN between sites, and MOH is selected by the Voice Switch where the CO trunks are configured (that is, the holding party). IP phone users do not receive MOH when they are on an internal call. See the *MiVoice Connect System Administration Guide* for additional information.

Before installing the system, confirm that you have music sources for each site, including the music and the required equipment for playback.

10.11.1.1.1 Details related to MOH over SIP Trunks

- Music On Hold for SIP trunks is offered for environments where external users reach the MiVoice Connect system through SIP trunks (such as BRI via a SIP gateway).
- If there is a MOH source at the same site as a SIP trunk, these trunks are connected to that source when placed on hold, and the device at the other end of the trunk connects directly to the MOH switch.
- The existing rules for MOH also apply to MOH for SIP Trunks:
  - MOH is not sent across sites.
  - The MOH source must be at the same site as the SIP trunk that utilizes it.
- If one of the parties in a conversation places the other party on hold, only the person who was placed on hold hears MOH.
- MOH is supported on a SIP tie trunk to IP Phones in the following scenarios:
  - From an IP phone to another IP phone.
  - From an analog phone to an IP phone (that is, putting the call on hold from an analog phone).
  - From any trunk (PRI/analog) while placing an IP phone caller on hold.
  - From any phone type to a SIP trunk device such as a Hitachi phone over the SIP tie trunk and onto the SIP trunk device.

10.11.1.2 File-Based Music on Hold

Music on hold audio files can be added to the system using Connect Director. The file can be recorded music or custom music, with prerecorded announcements or other information for callers. When file-based MOH is enabled, files can be played to all endpoints, except SIP-tie trunks.

To enable file-based MOH, MOH source(s) must be configured to play the uploaded music files. Any combination of Headquarters Server, DVS Server(s), or V-Switch(es) can be configured as MOH sources.

When an MOH file is added to the system, the file is stored on the Headquarters server, and is then automatically distributed to each server in the system that has file-based MOH enabled.

An MOH music file can be assigned to a specific user or group of users via Director. See the *MiVoice Connect System Administration Guide* for additional information.

When a call is put on hold with file-based MOH enabled, the streaming source is selected from the configured sources for the site. Sources with a higher maximum concurrent call limit are selected more frequently.

After a source reaches the maximum call limit, the source is no longer available for additional MOH calls. In this case, another configured MOH source for the site is tried. If all the sources at a site are unavailable or unreachable, MOH falls back to the parent sites and repeats the process. If all file-based MOH sources for the site and all its parents are exhausted, the call attempts to fall back to jack-based MOH using the rules described in Jack-Based Music on Hold.

The resources used to generate MOH are shared with other voicemail services on these sources. When planning, it is important to consider if a source will be able to handle concurrent usage of MOH calls, VM, and AA activity. If more resources are required, an additional source dedicated to MOH can be added to the MiVoice Connect system. For example, a DVS can be added with file-based MOH enabled and no voice mailboxes or other server features configured. For more information, see General Feature Limitations on page 331.

10.11.1.3 Which File Is Played When a Call Is Put On Hold?

The file played when a call is put on hold is selected using the following rules:

1. If the call is incoming through DNIS and an MOH file is configured for that DNIS number, the MOH file is played for the duration of the call, even after a transfer.
2. If the first rule does not apply and an MOH file is configured for the User Group of the user holding the call, that User Group's MOH file is played.
3. If neither of the rules above applies and an MOH file is configured for the default system MOH file, the system MOH file is played.
4. If none of the rules above applies, MOH uses the Jack-based MOH according to the rules described in Jack-Based Music on Hold.

10.11.1.4 Jack-Based MOH versus File-Based MOH

Jack-Based MOH vs. File-Based MOH compares jack-based MOH and file-based MOH.

Table 27: Jack-Based MOH vs. File-Based MOH

MOH Feature	Jack-Based MOH	File-Based MOH
Can control music to be played?	Yes, per site.	Yes, by DNIS, User Group or System Default.
Can stream music crosssite?	No.	Yes.
Can stream music to internal phones?	No, external only.	Yes.

MOH Feature	Jack-Based MOH	File-Based MOH
Can stream music to SIP extensions?	No, external only.	Yes.
Music streaming source?	MOH Jack on switches.	File saved on server or voicemail model switches.
When call is first held, does music start from the beginning?	No.	Yes.
If call is held a second time, does the music resume from where it last ended?	No.	Yes.
Does each stream use its own bandwidth?	No, bandwidth is used only once per switch, except for SIP trunks.	Yes.

10.11.2 Overhead Paging

The MiVoice Connect system can provide single-zone overhead paging for each site by using the audio output port on those voice switches that provide an audio output port.

For sites that require overhead paging, you must designate one of the voice switches to provide paging. In addition, you must provision your selected paging equipment for connection to the MiVoice Connect system.

For more information about the Paging Adapter, see Paging Adapter and System Contact Closure Support on page 248.

10.11.3 Multi-site Paging Groups

As an alternative to a paging system, you can designate groups of system extensions that can be paged by dialing a single system extension. In this way, audio is routed to a group of phones and played on the phone speaker as opposed to playing the audio announcement on an overhead paging system.

Note:

Paging groups are not supported on voicemail model switches.

You can also add a paging extension, which is associated with a site's overhead paging system, to a paging group in order to simultaneously play audio on a group of phones and also an overhead paging system. Refer to the *MiVoice Connect System Administration Guide* for details.

Additionally, if more than one server is installed in the MiVoice Connect system, an administrator can choose to record and deliver the group page to another site using that site's DVS. This will decrease WAN bandwidth consumption if there is a need to deliver a page to users at a remote site.

Pages to on-hook IP phones will automatically be announced on the IP phone speaker. Pages to IP phones or analog phones that are already on a call are treated as a normal call. Availability states and their associated call handling do not apply to page calls.

A maximum of 100 extensions can be paged at one time. Group paging is not available to external callers.

Refer to the *MiVoice Connect System Administration Guide* for more information about establishing and managing paging groups.

10.11.4 Night Bell

The MiVoice Connect system can provide an overhead night bell on a per site basis using the audio output port associated with Voice Switches that provide an audio output port.

10.11.5 Intercom

A user can initiate an intercom call through a programmable button on an IP phone that has been programmed with the Intercom feature, via the Mitel Connect client, or through the phone by entering ***15** + extension number. Users must be configured to use the intercom feature through Connect Director.

All intercom calls defeat the user's availability state settings, and cannot be forwarded.

An intercom call to an idle IP phone is auto-answered and connected through the called party's speakerphone. Immediately after the call is auto-answered, the called party hears an announcement tone and the calling party hears a beep tone. If the called phone was taken off-hook automatically, the switch puts the phone back on-hook when the intercom call terminates.

An intercom call to an analog phone or SoftPhone that is off-hook with no active call, such as in hands-free mode, is auto-answered through the audio device that is currently active. If the called party is on-hook or is on an active call, the call is offered as an ordinary call, except that call coverage is still defeated.

An intercept tone (fast-busy) is played if the calling user does not have the appropriate permissions. If the called party does not accept intercom calls due to CoS permissions, the call is offered as an ordinary call.

10.11.5.1 Intercom Telephony COS Configuration

Each telephony class-of-service permission has two additional check box settings in Connect Director to configure intercom permissions:

- Allow initiation for Directed Intercom/Paging — If enabled, users with this COS may make intercom calls to other users of the system. If disabled, then intercom calls cannot be made.

- Accept Directed Intercom/Paging — If enabled, users with this COS may accept intercom calls. If disabled, then intercom calls are received as normal calls.

10.11.6 Call Recording

The MiVoice Connect system provides the capability for users to record calls. To be available, call recording must be configured in Connect Director by a system administrator. Refer to the MiVoice Connect System Administration Guide for details on configuring this feature.

Users can use the Personal Access license to request that a call be recorded to voice mail. Supervisors may use Agent Monitor to record an agent's call. Ordinarily, both Mitel Connect client and Agent Monitor will indicate when a call is being recorded, but this behavior can be overridden with the Silent Recording feature to prevent agents from knowing that their calls are being recorded.

With Silent Recording, if the call is recorded by the workgroup supervisor, the indicator does not appear in Agent Monitor. The person invoking the recording sees the indicator — other parties do not. In this way, calls can be silently recorded to allow operators and supervisors to hide the fact that they are recording agents' calls. This hidden behavior may be desirable when a supervisor is monitoring the telephone manners of a new employee. When the recording is silent or hidden, Mitel Connect client offers no visual or audible indication that the call is being recorded, and the periodic beeping sound, which is used to notify call participants that their calls are being recorded, is suppressed.

The maximum number of simultaneous recordings equals the number of trunk ports.

The following limitations apply to call recording:

- Call recording is only available via the Personal Access license or a programmable button on IP phones.
- Only calls on trunks (not extensions-to-extensions) can be recorded.
- 2-way and 3-way calls can be recorded if one of the legs of the call is a trunk.
- Calls to a legacy Conference Bridge cannot be recorded.
- Recording stops when the call is parked, unparked, or transferred.

Mitel does not warrant or represent that your use of call monitoring or recording features of the software will be in compliance with local, state, federal or international laws that you may be subject to. Mitel is not responsible for ensuring your compliance with all applicable laws. Before configuring the call recording feature, you may wish to consult with legal counsel regarding your intended use.

Note:

- Call recording on MiContact Center Business (MiCCB) using MiVoice Call Recording (formerly known as the Oaisys Call Recorder) requires that you enter **Hairpin = 1** in the Tie Trunk SIP profile to record MiCCB calls. This configuration is provided in the Default ITSP option.
- Call recording on MiVoice Connect using MiVoice Call Recording requires that you enter **Hairpin = 1** in the trunk group's SIP profile for recording calls successfully.

10.12 Make Me Conferencing

The MiVoice Connect system allows up to eight callers to participate in a conference call without the use of a Conferencing Service or Converged Conferencing Solution. To use the Make Me conference feature you need an IP Phone and, for calls greater than three parties, the proper Class of Service must be configured in Connect Director. If you do not have an IP phone, the feature can also be used from the soft button “join” on an analog phone, in conjunction with the Mitel Connect client. The conference ports must also be reserved on the Voice Switch, and the maximum number of callers allowed in a Make Me conference depends on the voice switch type. The Make Me conference feature does not require Conferencing Services or a service appliance.

10.13 MiVoice Connect Contact Center

If you purchased MiVoice Connect Contact Center, you must configure an appropriate number of route points with adequate call stacks.

For information on route points, see the *MiVoice Connect System Administration Guide*. For information on MiVoice Connect Contact Center, see the *MiVoice Connect Contact Center Installation Guide* and the *MiVoice Connect Contact Center Administration Guide*.

10.14 MiVoice Connect with MiContact Center Business

If you purchased MiVoice Contact Center Business, you must configure the appropriate servers and deploy the appropriate OVAs. For more information about installing and configuring MiVoice Connect with MiContact Center Business, see the *MiVoice Connect - Installing and Configuring MiVoice Connect with MiContact Center Business Guide* located at https://www.mitel.com/document-center/business-phone-systems/mivoice-connect/mivoice-connect-platform.

Telephone Planning and Ordering 11

This chapter contains the following sections:

This chapter provides information about the types of telephones supported by the MiVoice Connect system and what to consider when planning phones for your system.

11.1 Recommendations

The following recommendations can assist you with planning, ordering, and installing your telephones:

- Select your telephones based on user requirements, your wiring infrastructure, and system objectives.
- Order your telephones early. If you need a large quantity of telephones, you should order them several weeks in advance.
- Have your cabling contractor place and test all your telephones. Have the contractor unpack, assemble, place, and test every telephone so that you can avoid this simple but time-consuming task.
- If the telephone you choose requires local power, make sure an outlet is available at each location.

11.2 Considerations for Selecting Phones

Before ordering telephones, you should consider how the phone will be used by various types of users or in certain locations (such as in a conference room or lobby). This section describes the phone features and functionality that different types of users or locations typically require.

11.2.1 Operators and Call Center Agents

Operators and other employees who answer and transfer large numbers of calls could benefit from phones that support the following features:

- The programmable buttons feature, which is available on multi-line IP phones and on the BB24 and BB424 button box devices, allows users or administrators to assign functions to custom keys. For example, an operator could assign speed dial numbers to programmable buttons.
- The Automatic Off-Hook Preference feature, which is available on multi-line IP phones, allows users to select which audio path (speakerphone or headset) is automatically activated when a call is placed or received. In addition, the HandsFree Mode feature suppresses the dial tone, which is a preference that people who use headsets often prefer. With these supports, employees can use the Mitel Connect client

to answer and transfer calls rapidly. Many employees in this type of job role stop using their telephone, opting instead to use the Mitel Connect client and their headset.

11.2.2 Administrative Assistants and Receptionists

Phone users in these roles are typically satisfied with a standard desk telephone that has speakerphone and mute buttons and supports Caller ID and Message Waiting. In addition, administrative assistants or receptionists could benefit from multi-line phones that offer programmable buttons that support extension monitoring. With this feature, users can monitor multiple system extensions.

11.2.3 Executives and Professionals

Most executives and professionals need advanced phones with full feature sets to handle multiple calls themselves or enable assistants to monitor their extension. For this reason, people in this role generally need multi-line phones with several programmable buttons to support features such as shared call appearance and speed dial.

11.2.4 Roaming Workers

Employees whose jobs involve walking around rather than sitting at a desk need a cordless telephone that they can carry with them so that they can receive calls wherever they roam at the work site. The following DECT cordless phones meet these needs:

- IP8430M (multi-cell)
- IP8630M (multi-cell)
- IP8830M
- IP93OD

Workers who need the flexibility to work inside or outside the office can use the Connect for Mobile applications integrated with a smartphone.

11.2.5 General Users

Typically, most general users are satisfied with a standard desk telephone that has speakerphone and mute buttons and supports Caller ID and Message Waiting. IP phones are fully featured and appropriate for most users. IP phones come with features such as Directory and Conference available on preprogrammed buttons.

11.2.6 Conference Rooms

Most conference rooms need a speakerphone that supports discussions including multiple people. In addition, a phone in a conference room should offer single-button access to features such as transferring and conferencing calls.

11.2.7 Lobby Phones

A cost-effective wall-mount, slim-line, or desk telephone is adequate for most lobby phones, hall phones, and the like.

11.2.8 Teleworkers

Both analog and IP phones can be included in a MiVoice Connect system as remote phones. Analog phones require use of the Extension Assignment, while IP phones are supported by setting an IP address range through Connect Director.

11.3 IP Phones

IP Phone Models provides information about IP phones supported in MiVoice Connect. For complete details about each model, see https://www.mitel.com/products/devices-accessories/ip-phones and https://www.mitel.com/document-center/devices-and-accessories/ip-phones.

The IP Phone BB24 and BB424, and M695 Programmable Key Module (PKM) are devices that provide multiple additional programmable buttons for a phone.

Table 28: IP Phone Models

Phone Model	User or Purpose	Feature
IP 930D Handset, Base, and Repeater	Roaming employees such as floor managers, filing clerks, and security guards	Cordless (DECT technology), 3 lines
IP 8830M Handset	Roaming employees such as floor managers, filing clerks, and security guards	Ruggedized cordless (multi-cell DECT) handset for tough duty applications, such as factories and hospitals
IP 8660M Base	Roaming employees such as floor managers, filing clerks, and security guards	Base unit for all multi-cell DECT handsets
IP 8630M Handset	Roaming employees such as floor managers, filing clerks, and security guards	Mid-range, mainstream cordless (multi-cell DECT) handset for offices
IP 8430M Handset Roaming employees such as floor managers, filing clerks, and security guards		

Phone Model	User or Purpose	Feature
Entry-level cordless (multi-cell DECT) handset		
IP 655	Executives, advanced professionals, remote workers, conference rooms	12 lines, large color touch screen, integrated VPN client, Gigabit Ethernet Enhanced directory and call history applications, with real-time telephony presence information and visual voicemail
IP 565g	Executives, advanced professionals, remote workers	6 lines, integrated VPN client, Gigabit Ethernet, Bluetooth
IP 560g	Operators, contact center agents, assistants, receptionists, advanced professionals, remote workers	6 lines, integrated VPN client, Gigabit Ethernet
IP 530	Professionals	3 lines, InstaDial™ functionality
IP 485g	Executives, advanced professionals	8 lines, large color screen, SIP, Gigabit Ethernet, USB port, visual voicemail, enhanced directory and call history applications, real-time telephony presence information
IP 480g	Operators, contact center agents, assistants, receptionists, advanced professionals	8 lines, large black-and-white screen, SIP, Gigabit Ethernet, visual voicemail, enhanced directory and call history applications, real-time telephony presence information
IP 480	Professionals, contact center agents	8 lines, large black-and-white screen, SIP, visual voicemail, enhanced directory and call history applications, real-time telephony presence information
IP 420g	Contact center agents, classrooms	2 lines, SIP, Gigabit Ethernet

Phone Model	User or Purpose	Feature
IP 420	Contact center agents, lobbies, break rooms, classrooms	2 lines, SIP
IP 265	Operators, contact center agents, assistants, receptionists, advanced professionals	6 lines, color screen
IP 230g	Professionals, advanced professionals, contact center agents, remote workers	3 lines, integrated VPN client, Gigabit Ethernet
IP 230	Professionals	3 lines
IP 212k	Small business	12 lines
IP 115	Contact center agents, lobbies, break rooms, classrooms	Single-line, speakerphone
IP 110	Contact center agents, lobbies, break rooms, classrooms	Single-line
BB24	Operators, assistants, receptionists	24 lines, feature keys, Ethernet switch port allows connection of a PC or an additional BB24 or IP phone Supported by the 100-, 200-, and 500-Series IP Phones
BB424	Operators, assistants, receptionists	Supports 96 programmable buttons by either connecting up to four BB424 devices (with 24 physical buttons on each) or through virtual pages when fewer devices are used Supported by IP485g phones through the USB port

Phone Model	User or Purpose	Feature
M695 Programmable Key Module	Operators, assistants, receptionists	• Supported on the Mitel MiVoice 6920, 6930, and 6940 IP phones • 4.3" 480x272 pixel color backlit LCD display • 3 x 28 programmable softkeys with LEDs • Can be daisy-chained up to a total of three M695 PKMs
6910 IP	Professionals	• LCD screen with backlight • Built-in two-port, 10/100/1000 Gigabit Ethernet switch, which enables you to share a connection with your computer • 8 programmable top keys • Support for up to 8 call lines with LEDs • Wideband handset • Wideband, full-duplex speakerphone for handsfree calls • Headset mode support • AC power adapter (sold separately) • Set paging
6920 IP	Professionals	• 3.5” QVGA (320x240) color TFT LCD display with brightness controls • Built-in-two-port, 10/100/1000 Gigabit Ethernet switch - lets you share a connection with your computer • USB 2.0 port (100mA maximum) • 6 top softkeys and 4 context-sensitive bottom softkeys • Wideband handset • Enhanced wideband, full-duplex speakerphone for handsfree calls • Extensive support for peripherals and modules: USB, S720 Bluetooth Speaker, DHSG/ EHSHandset, and wired analog headset, Mitel M695 Programmable Key (PKM) Module (button box),and Mitel Wireless LAN Adapter • AC power adapter (sold separately)
6930 IP	Professionals	• 4.3 inches WQVGA (480x272) color TFT LCD display with brightness controls • Built-in-two-port, 10/100/1000 Gigabyte Ethernet switch - lets you share a connection with your computer • Embedded Bluetooth 4.0 • USB 2.0 port (500mA maximum)

Phone Model	User or Purpose	Feature
		• 12 top softkeys and 5 context-sensitive bottom softkeys • Supports up to 24 call lines with LEDs • Mobile integration using Bluetooth wireless technology • Wideband handset • Enhanced wideband, full-duplex speakerphone for handsfree calls • Extensive support for peripherals and modules: Mitel cordless Bluetooth handset, Bluetooth, USB, S720 Bluetooth Speaker, integrated DECT Headset, DHSG/EHS, and wired analog headset, M695 Color Programmable Key (PKM) module (button box), and Mitel Wireless LAN Adapter • AC power adapter (sold separately)
6940 IP	Professionals	• 7 inches WVGA (800x480) color TFT capacitive touch-screen LCD display with brightness controls • Built-in-two-port, 10/100/1000 Gigabit Ethernet switch • Embedded Bluetooth 4.0 • USB 2.0 port (500mA maximum) • Cordless Bluetooth handset • Enhanced wideband, full-duplex speakerphone for handsfree calls • Extensive support for peripherals and modules: Mitel Cordless Bluetooth handset, Mitel Integrated DECT Headset, S720 Bluetooth Speaker, Bluetooth headset, M695 Color Programmable Key (PKM) modules (button box), and Mitel Wireless LAN Adapter • AC power adapter (sold separately) • 12 touchscreen top softkeys supporting up to 48 functions and six state-based touchscreen bottom softkeys supporting up to 30 functions
6920w IP	Professionals	• 3.5" QVGA (320x240 pixel) color display • Wi-Fi – dual band 802.11 a/b/g/n • Bluetooth 5.2 • Mitel PCLink • MobileLink mobile device integration • Mobile phone charging point • High quality full-duplex speakerphone • Native EHS/DHSG analog headset support

Phone Model	User or Purpose	Feature
		• USB port for headsets and accessories
6930w IP	Professionals	• 4.3" (480x272 pixel) color display • Wi-Fi – dual band 802.11 a/b/g/n • Bluetooth 5.2 • Mitel PCLink • MobileLink mobile device integration • Mobile phone charging point • Support for optional Cordless handset • Enhanced full-duplex speakerphone • Highly customizable via broad array of optional add-on accessories
6940w IP	Professional	• 7" (800x480 pixel) color LCD Touch Display • Wi-Fi – dual band 802.11 a/b/g/n • Bluetooth 5.2 • Mitel PCLink • MobileLink mobile device integration • Mobile phone charging point • Cordless handset • Enhanced full-duplex speakerphone • Highly customizable via broad array of optional add-on accessories

11.4 Planning Considerations for IP Phones

You must be aware of the following important installation planning considerations for IP phones and button boxes:

Note:

For information about the important installation planning considerations for 6900-Series IP phones, see the *Mitel IP Sets - Engineering Guidelines* Guide.

- The IP230, IP230g, IP420, IP420g, IP480, IP480g, IP485g, IP560g, IP565g, and IP655 models require a power-over-Ethernet (POE) power supply that complies with IEEE802.3af. For Gigabit Ethernet service, the POE switch must provide Gigabit Ethernet support.

  For capacity planning, use the following details:

  - The IP230 is a Class 2 device with a maximum consumption of 4.4 watts. Use 4.4 watts for capacity planning with POE switches on multiple deployments.
  - The IP230g is a Class 2 device with a maximum consumption of 5.9 watts. Use 5.9 watts for capacity planning with Gigabit Ethernet POE switches on multiple deployments.
  - The IP420 phone is a Class 1 device with a maximum consumption of 3.84 watts. Use 3.84 watts for capacity planning with POE switches on multiple deployments.
  - The IP420g phone is a Class 2 device with a maximum consumption of 6.49 watts. Use 6.49 watts for capacity planning with POE switches on multiple deployments.
  - The IP480 phone is a Class 2 device with a maximum consumption of 6.49 watts. Use 6.49 watts for capacity planning with POE switches on multiple deployments.
  - The IP480g phone is a Class 2 device with a maximum consumption of 6.49 watts. Use 6.49 watts for capacity planning with Gigabit Ethernet POE switches on multiple deployments.
  - The IP485g phone is a Class 0 device with a maximum consumption of 12.95 watts. Use 12.95 watts for capacity planning with Gigabit Ethernet POE switches on multiple deployments. These capacity planning numbers also allow for operation of BB424 button boxes.
  - The IP560g phone is a Class 3 device with a maximum consumption of 8.2 watts. Use 8.2 watts for capacity planning with Gigabit Ethernet POE switches on multiple deployments.
  - The IP565g phone is a Class 3 device with a maximum consumption of 8.2 watts. Use 8.2 watts for capacity planning with Gigabit Ethernet POE switches on multiple deployments.
  - The IP655 phone is a Class 3 device with a maximum consumption of 9.1 watts. Use 9.1 watts for capacity planning with Gigabit Ethernet POE switches on multiple deployments.
- The IP420g, IP480g, IP485g, IP560g, IP565g, and IP655 phone models require Category 5e or Category 6 Ethernet cables when deployed in Gigabit Ethernet configurations. We do not certify the use of Category 5 Ethernet cables because they can lead to lower connection speed or performance issues during high-rate data transfers.
- Two or more BB424 button boxes attached to an IP485g phone require an additional power adapter.
- The IP560g and IP565g models cannot be daisy-chained from the BB24 button box. The BB24 pass-through power is limited to Class 2 devices, and these phones are Class 3 devices. This means the BB24 cannot forward adequate power to these phones.
- The IP420, IP420g, IP480, IP480g, IP485g, and IP655 phone models cannot be deployed with a BB24 button box.

11.5 Analog Phone Requirements

The MiVoice Connect system supports standard analog 2500-type telephones, including the CLASS (Custom Local Area Signaling Services) features of Caller ID Name, Caller ID Number, and Message Waiting in the United States and Canada.

Outside the United States and Canada, the MiVoice Connect system supports the local standard analog telephones that support DTMF signaling. Analog Caller ID Number and Message Waiting are supported in the following countries:

- France

- Germany
- Italy
- Spain
- United Kingdom

Outside of the United States, Canada, and the countries mentioned in the bulleted list above, the features of Caller ID Name, Caller ID Number, and Message Waiting are not supported. See Dialing Plan Considerations on page 326 for more information.

The following list summarizes key requirements for analog phones:

- **2500-type telephones:** The MiVoice Connect system supports standard 2500-type telephones. (It does not support 500-type rotary telephones.)
- **DTMF signaling, even during power failure:** The MiVoice Connect system uses DTMF tones for signaling with telephones and trunks. It is mandatory that the telephone support DTMF signaling even when power is interrupted, to allow users to make calls in emergency situations.
- **Flash button:** A Flash button is required on analog phone sets to activate call control features from the telephone, including transfer, conference, pickup, and park. Mitel does not recommend using the hook switch to simulate the Flash button, since this can lead to accidental hang-ups.

If a speakerphone is required:

- **Mute button:** Users in the enterprise typically demand that their speakerphone have a mute button. Since telephones are often designed with the residential market in mind, some speakerphones do not have a mute button, which may lead to end-user complaints.

If message waiting is required (United States and Canada only):

- **CLASS (FSK) message waiting indicator:** CLASS message waiting–compatible telephones provide a highly reliable method for turning message waiting lights on and off.

Telephones that rely on a stutter dial tone to control the message waiting light are unreliable and should be avoided.

ST24A/ST48A Voice Switches support telephones that use voltage-driven message-waiting lights.

Select telephones from a reputable manufacturer. Although most phones on the market have good quality, we recommend that customers avoid “clone” or “low-end” phones.

Here are some additional considerations:

- **Not too many buttons:** Some telephones come with lots of complicated buttons and options that drive up the price of the device. The MiVoice Connect system delivers advanced features through desktop applications that are integrated with your enterprise tools. Telephones with lots of features and buttons are not necessary.
- **No answering machine:** The MiVoice Connect system includes an integrated voice mail system for all users at all sites. Telephones with integrated answering machines are not necessary.
- **No hold button:** Telephones with a hold button do not actually put the caller on system hold, so the caller will not hear music on hold or have the correct call control status details.

11.5.1 Caller ID Standard Support for Analog Phones

Caller ID Standard Support for Analog Phones by Country lists the caller ID standards the MiVoice Connect system supports for analog telephones by country.

Table 29: Caller ID Standard Support for Analog Phones by Country

Caller ID Standard	Country
BELLCORE	United States
BELLCORE	Canada
BELLCORE	Hong Kong
BELLCORE	Singapore
BELLCORE	Mexico
BELLCORE	China
BELLCORE	United Arab Emirates
BELLCORE	South Korea
BELLCORE	Philippines
BELLCORE	South Africa
BELLCORE	Costa Rica
BELLCORE	Israel
BELLCORE	Indonesia
BELLCORE	Fiji

Caller ID Standard	Country
BELLCORE	Mongolia
ETSI	France
ETSI	**Luxembourg
ETSI	Monaco
ETSI	**Saudi Arabia
ETSI	Romania
ETSI	Chile
ETSI	Hungary
ETSI	Germany
ETSI	Switzerland
ETSI	Austria
ETSI	Norway
ETSI	**Taiwan
ETSI	**Thailand
ETSI	Poland
ETSI	**Czech Republic
ETSI	Italy

Caller ID Standard	Country
ETSI	Spain
ETSI	*Argentina
BT	United Kingdom
BT	Ireland
None	Australia
None	Malaysia
None	Brazil
None	Netherlands
None	New Zealand
None	Portugal
None	Belgium
None	Denmark
None	Sweden
None	India
None	Japan
None	Finland (unsupported DTMF variation)
None	Greece

Caller ID Standard	Country
None	Bulgaria

Note:

**Indicates uncertainty as to whether country supports configured standard.

11.6 Fax Machines and Modems

Fax and modem calls are more sensitive to network problems than voice conversations. The human ear does not notice a lost packet during a voice conversation, but when a packet is lost during a fax transmission the line may be dropped. During a modem call, a lost packet can cause a retransmission. In the worst case, fax machines and modems will not establish a connection or may drop the call altogether. In general, fax and modem calls work across a local area network, but work on wide area networks only when there is virtually no packet loss and little jitter.

The MiVoice Connect system automatically detects both fax and modem tones, and boosts the voice encoding to a higher value to increase throughput. (G.711 at 64 Kbps is recommended.) It also stops the nonlinear processing of the echo canceler and fixes the size of the jitter buffer to a preset level. In addition, for modems, the echo canceler is frozen or stopped, since the modems use their own network echo cancelers.

11.6.1 Fax Machines

Fax machines require a high-quality IP network for proper operation.

The MiVoice Connect system supports distinctive ringing for inbound calls: calls from external parties have the classic single ring, whereas calls from internal parties have a distinctive double ring. Some fax machines detect the ringing pattern before answering and might not answer internal calls because of the distinctive ring pattern. In particular, you must turn off the **Intelligent Ring Mode** on some Hewlett-Packard fax machines to receive calls from internal parties.

11.6.2 Modems

The MiVoice Connect system supports “moderate-use” modem applications on the system. This is generally considered to be modem calls up to 28.8 Kbps that do not last longer than 15 minutes. If your application demands greater performance, you should bypass the MiVoice Connect system or move your modem application to a pure IP-based solution.

The expected modem performance in different configurations is as follows:

- Analog connection speeds will not exceed 33.6 Kbps and could be lower. External factors, including poor-quality trunk lines, ISP limitations, and multiple analog-to-digital conversions in the network, can have a significant impact on connection speeds.
- Modem calls demand a high-quality network with virtually no packet loss. Packet loss should not exceed 0.1%, which can be achieved on a local area network or in a wide area network using leased SGT1 facilities.
- Analog trunk ports should not be used if a digital trunk (SGT1) is available, since performance will be limited to 28.8 Kbps maximum. Digital trunks should be used instead.
- Connection speeds are significantly affected by multiple packet-to-circuit conversions (including modem calls from one MiVoice Connect system to another). If a SGT1 line is used, modems should be able to connect at K56Flex/V.90 or approximately 48 Kbps.

Server Requirements 12

This chapter contains the following sections:

This chapter provides specific hardware and software requirements for Headquarters servers and Distributed Voice Servers.

12.1 General Recommendations

The following recommendations can help you select the servers to buy:

You must download Mitel's Windows PowerShell script utility, "TacTools", to help verify server prerequisites, validate certificates, check system load balancing, and other useful functions for migration preparation and system administration. TacTools is available as a free download from the partner knowledgebase from the following location:

- For Partners: https://mitelcommunity.force.com/partner/s/article/TAC-Tools-Powershell-Scripts
- For Customers: https://mitelcommunity.force.com/customer/s/article/TAC-Tools-Powershell-Scripts

Disclaimer:

The TacTools script was written and provided by TAC. It is provided on a "best effort" basis and is not guaranteed to function properly in your environment. TAC will not troubleshoot the script in a customer's environment. Many modules are written to be "read only" to minimize any potential impact on the customer's server. Running any modules that will make any changes to your server will prompt you for confirmation. It is recommended that if you run a module that can make changes to your server, then you must run the script as part of a maintenance window, and must accept any potential service impact caused by the changes made to your server.

- Buy a server that is intended to function as a server and to host the MiVoice Connect software. The MiVoice Connect Headquarters server must be a dedicated server with no other applications installed. This means you should not use this server for any of the following:
  - Windows Domain controller
  - Terminal Server
  - Database Server (with MySQL)
  - Web server
  - Exchange server
- Ensure that each server that runs MiVoice Connect server software has enough processing capacity to support the planned telephony workload. The Softswitch on MiVoice Connect servers perform call control for calls that traverse the Softswitch. The server also provides services for voicemail, automated attendant, workgroup management, configuration databases, and more. The Headquarters server also hosts the system configuration tool, hosts Web pages for the user-interface and conferencing, and maintains call records and the history database.

You must download Mitel's Windows PowerShell script utility, "TacTools", to help verify server prerequisites, validate certificates, check system load balancing, and other useful functions for migration preparation and system administration. TacTools is available as a free download from the partner knowledgebase at the following location:

- For Partners: https://mitelcommunity.force.com/partner/s/article/TAC-Tools-Powershell-Scripts
- For Customers: https://mitelcommunity.force.com/customer/s/article/TAC-Tools-Powershell-Scripts

Disclaimer:

The TacTools script was written and provided by TAC. It is provided on a "best effort" basis and is not guaranteed to function properly in your environment. TAC will not troubleshoot the script in a customer's environment. Many modules are written to be "read only" to minimize any potential impact. Any modules that will make any changes to the server will prompt for confirmation. It is recommended that if you are running a module that can make changes to your server, then you must run the script as part of a maintenance window, and you must accept any potential service impact as a result of making changes to your server.

12.2 System Licenses

MiVoice Connect ships with four types of system licenses:

- Enterprise Edition (EE)—Fully featured MiVoice Connect system with no restrictions imposed by the system license.
- Small Business Edition 100 (SBE 100)—A solution for small businesses under 100 users is provided as a turn-key bundle. By installing an SBE 100 system license, the system is restricted to 100 users, 120 mailboxes, 5 sites, and 7 switches. Other restrictions also apply. Customers can upgrade from Small Business Edition 100 to Enterprise Edition by applying a new system license (a license to upgrade from SBE 100 to EE).
- Small Business Edition (SBE)—A solution for small businesses under 50 users. Small Business Edition is supported, but it is no longer available for sale.
- Demo Kit—Special version of the MiVoice Connect system used for demo purposes as a sales tool.

12.3 Requirements for Enterprise Systems

This section provides information necessary to provision servers on which to install MiVoice Connect Enterprise software.

The Enterprise Edition system is scalable. In the spirit of economy and efficiency, Enterprise customers provide their own server hardware, allowing them to build the optimum phone system for their environment. To assist in creating the optimum system, Mitel has defined a tier system based on the number of users the system is to support and sets minimum server requirements for each tier.

The tiers are as follows:

- Small Business Edition
- Small servers that support up to 100 endpoints
- Medium servers that support up to 500 endpoints
- Large servers that support up to 2,500 users

Note:

- If a planned upgrade to the current release means that the current server cannot adequately support the new release of MiVoice Connect software, upgrade the server to a model with greater capacity before doing the server software upgrade.
- SBE 100 systems upgraded to Enterprise Edition support the same capacities as the Enterprise system. However, appropriate hardware needs to be provided to support the required capacities.

12.3.1 Capacity and Hardware Requirements for HQ Servers

Headquarters Server Capacity and Hardware Requirements (New Server/Existing Server) - Part 1 and Headquarters Server Capacity and Hardware Requirements (New Server/Existing Server) - Part 2 shows information about system capacity and hardware requirements for each tier of Headquarters servers for customers who have new or existing physical servers. The table shows the number of users, calls, and reports that the server can support for each tier. Use this table to determine the specifications for your Headquarters server. You can mix servers of different capacities, but choose the right servers for your telephony environment.

Note:

- MiVoice Connect is compatible with MySQL 5.7.40 Community Edition and earlier versions. Therefore, MiVoice Connect installation is supported only on hard drives with 512 bytes physical sector size.
- Before you upgrade your system from 19.1 or earlier versions to 19.2, it is mandatory that you disable the Distributed Database feature. After the upgrade process is complete, if required, you can manually re-enable the Distributed Database feature.

12.3.2 Capacity and Hardware Requirements for DVS

Headquarters Server Capacity and Hardware Requirements (New Server/Existing Server) - Part 1 and Headquarters Server Capacity and Hardware Requirements (New Server/Existing Server) - Part 2 provides information about system capacity and hardware requirements for each tier of distributed voice servers (DVSs) for customers who have new or existing physical servers. The table provides information about the number of users and calls that a DVS in each tier can support. Use this table to calculate the requirements for the DVSs in your MiVoice Connect deployment. You can mix servers of different capacities. Choose the right servers for the entire telephony environment.

Note:

- A MiVoice Connect system supports a maximum of 20 distributed voice servers
- All other servers should be benchmarked against the information provided in this table to ensure equivalent or better performance. CPU benchmarking is available at: https://www.cpubenchmark.net/

12.3.3 Operating System Requirements for All Servers

For the latest information about supported operating systems for MiVoice Connect Headquarters and distributed voice servers, refer to the MiVoice Connect Build Notes. If you are upgrading a system, review the Build Notes for special instructions that might apply.

For information on additional supported operating systems for SBE 100, see SBE 100 Operating System Requirements on page 167.

Note:

Servers (Headquarters and DVS) on the same network can have different operating systems.

12.4 Capacities of the SBE 100 Systems

The section describes the capacities of the SBE 100 systems. It begins with a summary of the major differences between the features supported on the SBE 100 and the Enterprise Edition (EE).

Major Differences in Features Supported on SBE 100 and EE lists the major differences between the features supported on the SBE 100 and the EE systems.

12.4.1 SBE 100 Requirements

SBE 100 can be shipped with or without a server. If the SBE 100 is shipped with a UC Server 30, the server has the embedded Microsoft Windows Server OS for Telecommunications Systems. The server is configured, tested, and prepared for the installation of Mitel Connect Director software.

12.4.1.1 SBE 100 Option with a Provided Server

Hardware-based bundles include UC Server 30 or UC Server 75, depending on the customer needs.

12.4.1.1.1 UC Server 30

UC Server 30 can run a single application (for example, the HQ server or DVS). It is usually positioned for the customers who only need core telephony or UC applications.

The server shipped with SBE 100 (UC Server 30) meets or exceeds the following specifications:

- Processor: Intel Xeon E3-1225v5 8 M Cache, 3.3 GHz
- Memory: 8 GB (2 x 4 GB), DDR4; 64 GB Max
- Hard drive: Seagate EC3.5v5 1 TB SATA
- Operating system: Microsoft Windows 2016 Embedded OS (pre-installed)
- Power consumption: Idle: 34 Watt, Load: 67 Watt
- Form factor: Rack-mountable 1U
- Dimensions (WxHxD): 16.8 x 1.7 x 14 inches (42.6 x 4.3 x 35.6 cm)

12.4.1.1.2 UC Server 75, UC Server 25, and UC Server 20 (Legacy Servers)

UC Server 75, while still supported by MiVoice Connect, reached End of Sale effective 15 May, 2020.

UC Server 20 is an outdated server and is not supported by MiVoice Connect. However, UC Server 25 is supported by MiVoice Connect and its earlier versions such as ST14.2.

Note:
Unlike the UC Server 20, the UC Server 25 can be used as an HQ server for small business environments (50 or fewer users). It can also be used as a Distributed Voice Server (DVS) on MiVoice Connect.

Customers using either of these servers are advised to migrate to UC Server 30 or to virtualize their SBE deployment instead.

12.4.1.2 SBE 100 Option without a Provided Server

For the customers who buy their own server, the server must meet or exceed the specifications of the server shipped with the solution as specified in UC Server 30 on page 165.

SBE 100 can also run on a virtual server. The detailed server requirements for such deployments are specified in Capacity and Server Requirements in VMware Environments on page 167.

Note:
The SBE 100 system scales up to 100 users. Customers who grow beyond 100 users can purchase an upgrade from SBE 100 to Enterprise Edition. Such an upgrade will provide the customers with an Enterprise system license. Also, some customers might need to use more server resources than required for 25 simultaneous calls for features such as paging to multiple phones, by using more than 25 workgroups simultaneously, or running Web Reports. These customers should consider buying their own server that has, at a minimum, the hardware parameters of the Small Enterprise Server specified in Headquarters Server Capacity and Hardware Requirements (New Server/Existing Server) - Part 1 and Headquarters Server Capacity and Hardware Requirements (New Server/Existing Server) - Part 2 in the Server Requirements on page 441 section.

12.4.1.3 Using Mitel UC Server 30 in Enterprise Setup

If a customer grows beyond 100 users, an upgrade from a Mitel Connect Small Business Edition 100 to the Enterprise Edition is required. Mitel UC Server 30 can be reused in the Enterprise system with the following restrictions:

- System capacity shall not exceed 500 users.
- Server capacity shall not exceed 500 users (phones and switches managed by server).
- Simultaneous media paths (for example, voicemail calls to the server) are limited to 50.
- Busy hour completion: 2500
- Web reports during business hours are not recommended.

12.4.1.4 Microsoft Server OS Software Compatibility

Mitel UC Server 30 is shipped with the following Windows Server OS:

- Windows Server 2016 Embedded Telecom Edition

Servers provided by customers must run one of the following operating systems:

- Windows Server 2012 R2 (Standard, Datacenter)
- Windows Server 2016 (Standard, Datacenter)

12.4.2 SBE 100 Operating System Requirements

For SBE 100, the operating systems listed in this section are supported.

12.4.2.1 Supported Operating Systems for Servers Shipped to Customers

- Windows Server 2012 R2, 64-bit, Embedded Telecom Edition
- Windows Server 2016, Embedded (currently shipping)

12.4.2.2 OS Requirements for Servers Provided by Customers

The Operating System Requirements for Servers Provided by Customers are as follows:

- Windows Server 2012 R2, 64-bit (Standard, Datacenter)
- Windows Server 2016 (Standard, Datacenter)
- Windows Server 2019 (Standard, Datacenter)

12.5 Requirements for VMware Environments

This section provides information necessary to install the MiVoice Connect system software on servers running VMware.

12.5.1 Capacity and Server Requirements in VMware Environments

For details about the capacity and server requirements for the following virtual servers and appliances in VMWare environments, see the following referenced tables:

- Headquarters server information is provided in VMware or Hyper-V Capacity and Server Requirements for Headquarters Server.
- Windows distributed voice server information is provided in VMware or Hyper-V Capacity and Server Requirements for a Windows DVS.
- Linux distributed voice server information is provided in VMware or Hyper-V Capacity and Server Requirements for a Linux DVS.
- Virtual SIP Trunk Switch information for G.711 signaling is provided in VMware or Hyper-V Virtual SIP Trunk Switch (G.711 Signaling).

- Virtual SIP Trunk Switch information for G.729 signaling is provided in VMware or Hyper-V Virtual SIP Trunk Switch (G.729 Signaling).
- Virtual IP Phone Switch information is provided in VMware or Hyper-V Virtual IP Phone Switch.
- Virtual Edge Gateway Appliance information is provided in Table 102: VMware or Hyper-V Edge Gateway - Part 1 on page 454, Table 103: VMware or Hyper-V Edge Gateway - Part 2 on page 455, and Table 104: VMware or Hyper-V Edge Gateway - Part 3 on page 455.
- Virtual Service Appliance information is provided in VMware or Hyper-V Capacity and Server Requirements for Virtual Service Appliance.

These tables provide information for specific server types. All other servers should be benchmarked against the information provided to ensure equivalent or better performance. CPU benchmarking is available at https://www.cpubenchmark.net/.

12.5.2 Supported Components under VMware

VMware supports the following components on Windows Server 2012 R2, Windows Server 2016, and Windows Server 2019:

- Headquarters Server
- Distributed Voice Server (Windows)

12.5.3 Capacities in VMware Environments

When you create a Virtual Machine (VM), you must specify various properties related to size, such as the number of CPUs, the amount of memory, and the size of the disk.

VMware or Hyper-V Capacity and Server Requirements for Headquarters Server in the Virtual Server / Appliance Requirements on page 444 section provides the recommended configuration values for small, medium, and large deployments. The values listed are typical, but they might not be appropriate for all deployments.

12.5.4 Supported Guest Operating Systems for VMware

MiVoice Connect supports VMware with the following guest operating systems:

- For VMware vSphere (ESX/ESXi) 6.0:
  - Windows Server 2012 R2
  - Windows Server 2016
- For VMware vSphere (ESX/ESXi) 6.5 and 6.7:
  - Windows Server 2012 R2
  - Windows Server 2016
  - Windows Server 2019
- For VMware vSphere (ESX/ESXi) 7.0:
  - Windows Server 2012 R2
  - Windows Server 2016
  - Windows Server 2019

12.5.5 VMware Software Requirements

Refer to the Release Notes for supported versions of VMware ESXi.

12.6 Requirements for Microsoft Hyper-V Environments

Microsoft Hyper-V is the Microsoft virtual computing infrastructure, consisting of Microsoft Hyper-V servers, Hyper-V Manager, and related components.

For details about the capacity and server requirements for the following virtual servers and appliances in Microsoft Hyper-V environments, see the following referenced tables:

- Headquarters server information is provided in VMware or Hyper-V Capacity and Server Requirements for Headquarters Server.
- Windows distributed voice server information is provided in VMware or Hyper-V Capacity and Server Requirements for a Windows DVS.
- Linux distributed voice server information is provided in VMware or Hyper-V Capacity and Server Requirements for a Linux DVS.
- Virtual SIP Trunk Switch information for G.711 signaling is provided in VMware or Hyper-V Virtual SIP Trunk Switch (G.711 Signaling).
- Virtual SIP Trunk Switch information for G.729 signaling is provided in VMware or Hyper-V Virtual SIP Trunk Switch (G.729 Signaling).
- Virtual IP Phone Switch information is provided in VMware or Hyper-V Virtual IP Phone Switch.
- Virtual Edge Gateway Appliance information is provided in Table 102: VMware or Hyper-V Edge Gateway - Part 1 on page 454, Table 103: VMware or Hyper-V Edge Gateway - Part 2 on page 455, and Table 104: VMware or Hyper-V Edge Gateway - Part 3 on page 455
- Virtual Service Appliance information is provided in VMware or Hyper-V Capacity and Server Requirements for Virtual Service Appliance.

These tables provide information for specific server types. All other servers should be benchmarked against the information provided to ensure equivalent or better performance. CPU benchmarking is available at https://www.cpubenchmark.net/.

12.6.1 Supported Components under Microsoft Hyper-V

The following table shows the support for MiVoice Connect components under Microsoft Hyper-V.

Table 30: Supported Components under Microsoft Hyper-V - Part 1

Components	Windows Server 2012 R2 Generation 1	Windows Server 2012 R2 Generation 2	Windows Server 2016 Generation 1
Headquarters Server	Yes	Yes	Yes
Distributed Voice Server (Windows)	Yes	Yes	Yes

Components	Windows Server 2012 R2 Generation 1	Windows Server 2012 R2 Generation 2	Windows Server 2016 Generation 1
Distributed Voice Server (Linux)	Yes	Yes	Yes
Switches (IP Phone and Trunk)	Yes	Yes	Yes
Virtual Service Appliance (Collaborations)	Yes	Yes	Yes
Edge Gateway	No	Yes	Yes

Table 31: Supported Components under Microsoft Hyper-V - Part 2

Components	Windows Server 2016 Generation 2	Windows Server 2019 Generation 1	Windows Server 2019 Generation 2
Headquarters Server	Yes	Yes	Yes
Distributed Voice Server (Windows)	Yes	Yes	Yes
Distributed Voice Server (Linux)	Yes	Yes	Yes
Switches (IP Phone and Trunk)	Yes	Yes	Yes
Virtual Service Appliance (Collaborations)	Yes	Yes	Yes
Edge Gateway	Yes	Yes	Yes

Note:

- Microsoft Hyper-V Windows 2016 Generation 2 is not supported. Sites that have Microsoft Hyper-V Windows 2012 Generation 2 will need to change to Generation 1 before upgrading to Microsoft Hyper-V Windows 2016.
- This Generation 1 only limitation will be removed when Mitel releases a MiVoice Connect version that includes support for the Secure Boot feature in Windows Server 2016.

12.6.2 Capacities in Microsoft Hyper-V Environments

When you create a Virtual Machine (VM), you must specify various properties related to size, such as the number of CPUs, the amount of memory, and the size of the disk.

VMware or Hyper-V Capacity and Server Requirements for Headquarters Server in the Virtual Server / Appliance Requirements on page 444 section provides the recommended configuration values for small, medium, and large deployments. The values listed are typical, but they might not be appropriate for all deployments.

12.6.3 Supported Guest Operating Systems for Microsoft Hyper-V

MiVoice Connect supports Microsoft Hyper-V with the following guest operating systems:

- Microsoft Hyper-V 2016:
  - Windows Server 2016 Generation 1 for all supported components
- Microsoft Hyper-V 2012 R2:
  - Windows Server 2012 R2 Generation 1 and Generation 2 for all supported components
  - Windows Server 2012 R2 for Connect Contact Center

12.6.4 Microsoft Hyper-V Software Requirements

Refer to the Release Notes for supported Microsoft Hyper-V versions.

12.7 Hard Disk Requirements

This section provides information about the general hard disk requirements for MiVoice Connect servers and clients and information about the hard disk utilization of critical functions. Consider the utilization of these resources before selecting a hard drive for the server. Hard Disk Space Minimum Requirements for Applications in the Hardware and Network Requirements on page 432 section shows the minimum amount of hard disk required for the applications. In addition, hard disk space is needed for the dynamic files for voice mail, the call detail records on the Headquarters server only, and the log files.

12.7.1 Voicemail Utilization

The space used for user voicemail messages on the server hard drive depends on the number of users, the number of messages per user, and the duration of each message. You need approximately 30 MB of hard disk space per hour of recorded messages for voice mail storage.

Note:

When callers try to leave voicemail messages or users attempt to call an auto attendant, a recording plays stating that there is no space available and a message cannot be left. In the voicemail log for calls, a message indicates the current percentage of disk space used.

Example:

```
09:12:20.017 ( 4600: 5096) [MS] VMSystem::getAvailableMessageStores ,
maxMessageStores = 1

09:12:20.017 ( 4600: 5096) [MS] Calling GetDiskFreeSpaceEx, Path= C:
\Shoreline Data\Vms\Message

09:12:20.017 ( 4600: 5096) [MS] GetDiskFreeSpaceEx method returned,
FreeSpace=2526 MB

09:12:20.017 ( 4600: 5096) [MS]
VMSystem::getAvailableMessageStores ,FreeSpace.QuadPart <
MIN_DISKSTORAGE_FOR_RECORD returning -1, FreeSpace =2526 MB,
currPercentUsed=96

09:12:20.017 ( 4796: 4992) [PM] VoiceApp::recordMessage, messageStoreIndex
= -1

09:12:20.017 ( 4796: 4992) [PM] PM: Play phrase 80 lang 1
```

Recordings are no longer created if 95% or more of disk space has been used.

Clearing space on the drive will correct this issue.

Voice Mail Hard Disk Space provides some conservative guidelines to estimate the amount of hard disk space used for voice mail, assuming each user has 15 one-minute voice messages.

12.7.2 Call Detail Records

For each call on the system, call detail records are generated on the Headquarters server. The hard disk space used on the server for call detail records varies depending on the call load on the system. The amount of hard disk space for a typical system is shown in Call Detail Records.

12.7.3 Log Files

Log files are generated on the system for technical support. The hard disk space used on the server for log files varies, depending on the overall system activity.

The size of the log files on the server is determined by parameters set in Connect Director. Log files can remain 1–30 days (the default is 7 days), with a size in the range 0.5–5.0 GB (the default is 4 GB). Log File Hard Disk Space in the Hardware and Network Requirements on page 432 section shows the hard disk space that log files need.

12.7.4 Log Files for Emergency Location Change Update

Location change information is logged if related flags are enabled for teleworker endpoints. This information is saved in log files named `EmergencyLocationUpdateInfo`. The files are located in the standard log folder `<drive>:\Shoreline Data\Logs`.

Because the teleworker endpoint location updates and user acknowledgment information contained in these files might be required to audit RAY BAUM compliance issues, these files are not automatically deleted by the system. System administrators are allowed to delete them manually after they are sure they have been backed up.

12.8 Preparing the Server for Operation

This section describes how to prepare the server for operation in the MiVoice Connect telephony network.

12.8.1 Server IP Address

The MiVoice Connect server should have a static IP address. If the server suddenly gets a new IP address, system operation can be unpredictable.

Note:

You should always configure the server to be part of a domain and make sure that it remains in the domain.

12.8.2 DHCP on the Server

Mitel recommends that the server not be used as a Dynamic Host Configuration Protocol (DHCP) server.

12.8.3 Microsoft Windows Server 2012 R2 Configuration

Before you install the MiVoice Connect server software, you must prepare Microsoft Windows Server 2012 R2 64-bit to run MiVoice Connect services by enabling IIS, COM+, SMTP, and FTP, as well as changing the SMTP and FTP startup type to automatic. This section describes how to prepare a Microsoft Windows Server 2012 R2 server to use MiVoice Connect software.

Note:

- User Account Control must be disabled on the server.
- Windows Server 2012 R2 64-bit must be activated through Microsoft before installing the MiVoice Connect server software.
- During installing the server operating system, select the Server with a **GUI** option, instead of **Server Core Installation** option.
- Disable the Windows Base Filtering Engine and the Windows Firewall services.
- Mitel recommends that the customer disable the Windows Firewall and Base Filtering Engine on the HQ Server and all Windows DVS. If the customer's IT security policy or other business needs require Windows Firewall and Base Filtering Engine services to be enabled, it is the customer's responsibility to configure the system to permit all traffic destined for the port numbers and ranges used by HQ Server and Windows DVS. See the table in the *Port Usage* section of the *MiVoice Connect Maintenance Guide* for a complete list of the port numbers and ranges that must be permitted. During troubleshooting, Mitel TAC technicians might require you to disable the Windows Firewall and Base Filtering Engine.

12.8.3.1 Server Roles and Features

This section describes how to configure the server roles in Microsoft Windows Server 2012 R2 that are required to run the MiVoice Connect server. In this procedure, you add application server and web server roles, and then you add services for each role.

Note:

Run the Windows updates and all the related patches before adding the Roles and Features.

1. On the Windows desktop, click **Start** > **Programs** > **Administrative Tools** > **Server Manager** to launch the Server Manager Dashboard.
2. In the Server Manager Dashboard, under **Configure this local server**, click **Add roles and features**. The **Add Roles and Features Wizard** appears, and displays the **Before you begin** page.
3. After reading the Before you begin page, click **Next**. The **Select installation type** page appears.
4. In the middle pane, select **Role-based or feature-based installation**, and then click **Next**. The **Select destination server** page appears.

5. Check **Select a server from the server pool**, and then highlight a server in the pool and click **Next**. The **Select server roles** page appears.
6. Check the **Application Server** and **Web Server (IIS)** check boxes, and expand these selections to see the sub-roles for each selection.
7. Select all of the following roles and sub-roles:

- Application Server
  - .NET Framework 4.5
  - COM+ Network Access
  - Distributed Transactions
  - WS-Atomic Transactions
  - Incoming Network Transactions
  - Outgoing Network Transactions
  - TCP Port Sharing
- Web Server (IIS) Support
  - Windows Process Activation Service Support
  - HTTP Activation
  - Message Queuing Activation
  - Named Pipes Activation
  - Web Server
  - Common HTTP Features (select all options)
  - FTP Server (select all options)
  - Health and Diagnostics
  - HTTP Logging
  - Logging Tools
  - Request Monitor
  - Tracing
  - IIS Hostable Web Core (select all options)
  - Management Tools (select all options)
  - Performance (select all options)
  - Security (select all options)
  - Application Development
  - .NET Extensibility 3.5
  - .NET Extensibility 4.5
  - ASP
  - ASP.NET 3.5
  - ASP.NET 4.5
  - CGI
  - ISAPI Extensions
  - ISAPI Filters
  - Server Side Includes

8. Click **Next**. The **Select features** page appears, and displays the **Application Server Features** menu.

9. Select all the following features:
   - .NET Framework 3.5 Features (select all options)
   - .NET Framework 4.5 Features (select all options)
   - Quality Windows Audio Video Experience
   - SMTP Server
10. Click **Next**. The **Confirm installation selections** page appears.
11. Click **Install.**
12. After installation, follow the instructions in Setting SMTP, FTP, and Quality Windows Properties on page 179.

12.8.4 Microsoft Windows Server 2016 Configuration

Before you install MiVoice Connect server software, you must prepare Microsoft Windows Server 2016 to run MiVoice Connect services by installing the proper server roles and features. This section describes how to prepare a Microsoft Windows Server 2016 server to use MiVoice Connect software.

Note:

- Windows Server 2016 must be activated through Microsoft before installing the MiVoice Connect server software.
- During installing the server operating system, select the Server with a GUI option, instead of Server Core Installation option.
- Disable the Windows Base Filtering Engine and the Windows Firewall services.
- Mitel recommends that the customer disable the Windows Firewall and Base Filtering Engine on the HQ Server and all Windows DVS. If the customer's IT security policy or other business needs require Windows Firewall and Base Filtering Engine services to be enabled, it is the customer's responsibility to configure the system to permit all traffic destined for the port numbers and ranges used by HQ Server and Windows DVS. See the table in the *Port Usage* section of the *MiVoice Connect Maintenance Guide* for a complete list of the port numbers and ranges that must be permitted. During troubleshooting, Mitel TAC technicians might require you to disable the Windows Firewall and Base Filtering Engine.

When installing MiVoice Connect Server in Windows Server 2016, the installer fails to recognize the current IIS version as valid IIS version. To resolve this, do the following on the MiVoice Connect Server:

1. Run `SetIIS_version.vbs` to update the registry.
2. Start the MiVoice Connect server installation on Windows Server 2016.
3. After the installation is complete, run `ResetIIS_version.vbs`

Note:

- `SetIIS_version.vbs` and `ResetIIS_version.vbs` are located in the `2016 Scripts` folder in the `MiVoice Connect Installation Media`.
- You must perform these steps only once on Windows Server 2016 because the subsequent upgrade will already have the prerequisites.
- This applies only to the HQ server installation.

12.8.4.1 Server Roles and Features

This section describes how to configure the server roles and features required to run the MiVoice Connect server.

Note:

Run the Windows updates and all the related patches before adding the server roles and features

1. On the Windows desktop, click **Server Manager** to launch the Server Manager Dashboard.
2. In the Server Manager Dashboard, under **Configure this local server**, click **Add roles and features**. The **Add Roles and Features Wizard** appears, and displays the **Before you begin** page.
3. After reading the Before you begin page, click **Next**. The **Select installation type** page appears.
4. In the middle pane, select **Role-based or feature-based installation**, and then click **Next**. The **Select destination server** page appears.
5. Check **Select a server from the server pool**, and then highlight a server in the pool and click **Next**. The **Select server roles** page appears.
6. Select the following roles and sub-roles:
   - File and Storage Services
     - File and iSCSI Services: File Server and File Server Resource Manager
     - Storage Services
   - Web Server (IIS) (Installed):
     - Web Server (Select all options)
     - FTP Server (Select all options)
     - Management Tools (Select all options)
7. Click **Next**. The **Select features** page appears, and displays the **Application Server Features** menu.

8. Select the following features:
    - .NET Framework 3.5 Features
        - .NET Framework 3.5
        - HTTP Activation
        - Non-HTTP Activation
    - .NET Framework 4.6 Features
        - .NET Framework 4.6
        - ASP.NET 4.6
        - WCF Services
    - IIS Hostable Web Core
    - Internet Printing Client
    - LPR Port Monitor
    - Media Foundation
    - Message Queuing
        - Message Queuing Services
        - Message Queuing Server
        - Directory Service Integration
        - HTTP Support
        - Message Queuing Triggers
        - Multicasting Support
        - Routing Service
        - Message Queuing DCOM Proxy
    - Quality Windows Audio Video Experience
    - Remote Assistance
    - Remote Server Administration Tools
        - Feature Administration Tools
        - SMTP Server Tools
        - Role Administration Tools
        - File Services Tools
        - File Server Resource Manager Tools
    - SMTP Server
    - Windows Defender Features
    - Windows PowerShell
        - Windows PowerShell 5.1
        - Windows PowerShell 2.0 Engine
        - Windows PowerShell ISE
    - Windows Process Activation Service
    - WoW64 Support
9. Click **Next**. The **Confirm installation selections** page appears.
10. Click **Install.**
11. After installation, follow the instructions in Setting SMTP, FTP, and Quality Windows Properties on page 179.

12.8.4.2 Setting SMTP, FTP, and Quality Windows Properties

Along with MiVoice Connect server software, SMTP, FTP, and Quality Windows Audio Video Experience services are also installed. By default, the startup type for SMTP and Quality Windows Audio Video Experience is Manual, and for FTP it is Automatic.

Note:

- If the startup type is Manual, click the **Start** button to start the service.
- Administrators must manually start the Quality Windows Audio Video Experience service. If this service is not manually started, the Compatibility Checker will determine that the service is not installed or running, and this will cause the installation to fail.

The following procedure changes the startup type for SMTP. Repeat these steps for the Quality Windows Audio Video Experience service.

Note:

Check and verify that you have at least read access to the FTP root folder in the `Inetpubs directory`.

1. Access the **Services** page by selecting **Start** > **Administrative Tools** > **Services**.
2. Right-click **Simple Mail Transfer Protocol** and select **Properties** from the menu. The **Simple Mail Transfer Protocol (SMTP) Properties** page appears.
3. Select From the **Startup Type** drop-down menu, select **Automatic** and then click **OK**.
4. Click **OK** to return to the **Services** page.
5. Right-click **Microsoft FTP Service** and select **Properties** from the menu. The **Microsoft FTP Service properties** page appears.
6. In the **Startup type** field, confirm that the **Automatic** option is selected.
7. Click **OK**.

12.8.5 Microsoft Windows Server 2019 Configuration

Before you install MiVoice Connect server software, you must prepare Microsoft Windows Server 2019 to run MiVoice Connect services by installing the proper server roles and features. This section describes how to prepare a Microsoft Windows Server 2019 server to use MiVoice Connect software.

Note:

- Windows Server 2019 must be activated through Microsoft before installing the MiVoice Connect server software.
- During installing the server operating system, select the Server with a GUI option, instead of Server Core Installation option.
- Disable the Windows Base Filtering Engine and the Windows Firewall services.
- Mitel recommends that the customer disable the Windows Firewall services and Base Filtering Engine on the HQ Server and all Windows DVS. If the customer's IT security policy or other business needs require Base Filtering Engine and Windows Firewall services to be enabled, it is the customer's responsibility to configure the system to permit all traffic destined for the port numbers and ranges used by HQ Server and Windows DVS. See the table in the *Port Usage* section of the *MiVoice Connect Maintenance Guide* for a complete list of the port numbers and ranges that must be permitted. During troubleshooting, Mitel TAC technicians might require you to disable the Base Filtering Engine and Windows Firewall services.

12.8.5.1 Configuring Server Roles and Features and Completing the Installation

This section describes how to configure the server roles and features required to run the MiVoice Connect server and complete the installation.

Note:

Run Windows updates and all related patches before adding the server roles and features.

1. On the Windows desktop, click **Server Manager** to launch the Server Manager Dashboard.
2. In the Server Manager Dashboard, under **Configure this local server**, click **Add roles and features**. The **Add Roles and Features Wizard** appears, displaying the **Before you begin** page.
3. After reading the **Before you begin** page, click **Next**. The **Select installation type** page appears.
4. In the middle pane of the **Select installation type** page, select **Role-based or feature-based installation**, and then click **Next**. The **Select destination server** page appears.
5. Select **Select a server from the server pool**, highlight a server in the pool, and click **Next**. The **Select server roles** page appears.
6. Select the following roles and sub-roles:
   - File and Storage Services
     - File and iSCSI Services: File Server and File Server Resource Manager
     - Storage Services
   - Web Server (IIS) (Installed):
     - Web Server (select all options)
     - FTP Server (select all options)
     - Management Tools (select all options)

7. Click **Next**. The **Select features** page appears, displaying the **Application Server Features** menu.
8. Select the following features:
   - .NET Framework 3.5 Features
     - .NET Framework 3.5
     - HTTP Activation
     - Non-HTTP Activation
   - .NET Framework 4.6 Features
     - .NET Framework 4.6
     - ASP.NET 4.6
     - WCF Services
   - IIS Hostable Web Core
   - Internet Printing Client
   - LPR Port Monitor
   - Media Foundation
   - Message Queuing
     - Message Queuing Services
     - Message Queuing Server
     - Directory Service Integration
     - HTTP Support
     - Message Queuing Triggers
     - Multicasting Support
     - Routing Service
     - Message Queuing DCOM Proxy
   - Quality Windows Audio Video Experience
   - Remote Assistance
   - Remote Server Administration Tools
     - Feature Administration Tools — SMTP Server Tools
     - Role Administration Tools — File Services Tools and File Server Resource Manager Tools
   - SMTP Server
   - Windows Defender Features
   - Windows PowerShell
     - Windows PowerShell 5.1
     - Windows PowerShell 2.0 Engine
     - Windows PowerShell ISE
   - Windows Process Activation Service
   - WoW64 Support
9. Click **Next**. The **Confirm installation selections** page appears.
10. Click **Install**. A status bar indicates the progress of the installation.
11. After the installation is complete, follow the instructions in Setting SMTP, FTP, and Quality Windows Properties on page 179.

Note:
For MiVoice Connect installation in Windows Server 2019, after you configure the server roles and features, verify that the `inetpub` and the `wwwroot` folders are created.

12.8.5.2 Setting SMTP, FTP, and Quality Windows Properties

Along with MiVoice Connect server software, SMTP, FTP, and Quality Windows Audio Video Experience services are also installed. By default, the startup type for SMTP and Quality Windows Audio Video Experience is Manual, and for FTP it is Automatic.

Note:

- If the startup type is Manual, click the **Start** button to start the service.
- Administrators must manually start the Quality Windows Audio Video Experience service. If this service is not manually started, the Compatibility Checker will determine that the service is not installed or running, and this will cause the installation to fail.

The following procedure changes the startup type for SMTP. Repeat these steps for the Quality Windows Audio Video Experience service.

Note:

Check and verify that you have at least read access to the FTP root folder in the `Inetpubs directory`.

1. Access the **Services** page by selecting **Start** > **Administrative Tools** > **Services**.
2. Right-click **Simple Mail Transfer Protocol** and select **Properties** from the menu. The **Simple Mail Transfer Protocol (SMTP) Properties** page appears.
3. Select From the **Startup Type** drop-down menu, select **Automatic** and then click **OK**.
4. Click **OK** to return to the **Services** page.
5. Right-click **Microsoft FTP Service** and select **Properties** from the menu. The **Microsoft FTP Service properties** page appears.
6. In the **Startup type** field, confirm that the **Automatic** option is selected.
7. Click **OK**.

12.8.6 Additional Considerations

This section discusses additional recommendations and requirements for installing the MiVoice Connect server.

12.8.6.1 Maximum Transmission Unit (MTU) Size for Connections

The default Maximum Transmission Unit (MTU) setting for PPP (Point-to-Point Protocol) clients, VPN (Virtual Private Network) clients, PPP servers, or VPN servers running Routing and Remote Access on MiVoice Connect systems is 1400. To change the MTU value, you must edit the registry. For further information, contact Mitel Support.

Note:
Change MTU size to 1500 when registry settings are not propagated to LDVS servers.

12.8.6.2 Windows Firewall Settings

The basic Windows firewall must be disabled for the Headquarters server and any Windows Distributed Voice Servers before installation.

Note:

Mitel recommends that the customer disable the Windows Firewall and Base Filtering Engine on the HQ Server and all Windows DVS. If the customer's IT security policy or other business needs require Windows Firewall and Base Filtering Engine services to be enabled, it is the customer's responsibility to configure the system to permit all traffic destined for the port numbers and ranges used by HQ Server and Windows DVS. See the table in the *Port Usage* section of the *MiVoice Connect Maintenance Guide* for a complete list of the port numbers and ranges that must be permitted. During troubleshooting, Mitel TAC technicians might require you to disable the Windows Firewall and Base Filtering Engine.

12.8.6.3 IE Enhanced Security Configuration

The IE Enhanced Security Configuration parameter must be disabled for Administrators.

12.8.6.4 IPv6

IPv6 parameter must be disabled for the primary NIC.

12.8.6.5 Data Execution Prevention (DEP)

Data Execution Prevention is recommended for essential Windows Programs and Services only. The default is for all programs and services.

12.8.6.6 Adobe Acrobat Reader

Install Adobe Acrobat Reader on the server if you do not already have it, so that you can access the online documentation. You can install Adobe Acrobat Reader from the MiVoice Connect USB flash drive or download it from the Adobe web site.

12.8.6.7 Internet Information Server (IIS) Default Web Site

The web site for Connect Director is `http://<server_name>/shorewaredirector`. You should not change the default IIS web site of the server to redirect to Connect Director, since this will cause navigation problems within Connect Director.

12.8.6.8 Access to the Distributed Server Maintenance Page

If you are using Microsoft Internet Explorer and the distributed server is configured with an IP address rather than a server name, you must enable session cookies on your client computer to access the Distributed Server Maintenance Page. To enable session cookies:

1. Launch Internet Explorer.
2. Click **Tools** > **Internet Options**. The **Internet Options** dialog box appears.
3. Click the **Privacy** tab and then the **Advanced** button. The **Advanced Privacy Settings** dialog box appears.
4. Select the **Override automatic cookies** check box.
5. Select **Always allow session cookies**.
6. Click **OK** to save the changes.

12.8.6.9 Microsoft Updates on the Server

For each new release, the MiVoice Connect Release Notes document is updated with the Microsoft patches that have been certified against the build. Any Mitel software changes required by the Microsoft patches are highlighted. Mitel recommends that customers continue to install Microsoft updates delivered after the date of the release notes. However, it is possible that a future update might not be compatible with Mitel software. If you do install an update and encounter issues, TAC might recommend you roll back the update and repair or reinstall the Mitel software.

To reduce potential impact, it is advisable that you apply only critical and high-importance updates. Mitel recommends that customers back up their MiVoice Connect system before installing any Microsoft updates. See the *System Backup and Restore* section in the *MiVoice Connect System Administration Guide* for instructions on backing up the system.

12.8.6.10 Virus Protection on the Main and Distributed Servers

The use of industry-standard virus protection software on the main and distributed servers is supported.

12.8.6.10.1 Anti-Virus Folder Exclusions

The following is a list of folders and sub-folders that must be excluded from Virus checker software or from disk backup or restore software:

Note:

These folders and sub-folders can be excluded from Virus checker software or restore software only after the software is installed.

- Mitel Connect client:
  - `<Drive>:\Users\%User%\AppData\Local\Mitel`
  - `<Drive>:\Program Files (x86)\Mitel`
  - `<Drive>:\Program Files (x86)\Mitel Presenter`
- MiVoice Connect Contact Center
  - `<Drive>:\Users\%User%\AppData\Roaming\ShoreTel Contact Center`
  - `<Drive>:\Users\%User%\AppData\Local\ShoreTel Contact Center`
- HQ/ DVS Server:
  - `<Drive>:\Program Files (x86)\Shoreline Communications`
  - `<Drive>:\Shoreline Data\`
- Mac client:
  - `<Drive>:/Applications/Mitel\ Connect.app`
  - `<Drive>:/Users/%username%/Library/Application\ Support/Mitel` (Replace `%username%` with the user name of the user logged in to the Mac client. The folder might be in the same path but with ShoreTel instead of Mitel.

Note:

If the folders listed above are not excluded before installation, your installation of the current version of MiVoice Connect will fail and your system will roll back to the previous version. This will also result in a corrupted database if you perform nightly backups.

12.9 Requirements for MiVoice Connect Mobility Router

MiVoice Connect supports the following versions of the Mobility Router Appliance:

- Mobility Router 2000
- Mobility Router 4000
- Mobility Router 6000
- Virtual Mobility Router

MiVoice Connect Server Installation 13

This chapter contains the following sections:

This chapter describes installation procedures for main and distributed MiVoice Connect headquarters servers and distributed servers.

13.1 Checking Server Compatibility

A compatibility checker is available for identifying potential issues prior to installing or upgrading the MiVoice Connect Server software. You can run the compatibility checker as a separate utility before the installation process or through the installation wizard as part of the installation process.

The compatibility checker requires that Microsoft Visual C++ Redistributable 2015 be installed. Microsoft Visual C++ is installed automatically as part of the MiVoice Connect installation process, but if you run the standalone compatibility checker before installing MiVoice Connect, you need to ensure that the latest Microsoft updates and Microsoft Visual C++ Redistributable 2015 are installed before running the utility.

When running the compatibility checker on a system that does not currently have the MiVoice Connect Server software installed, the utility checks for the following:

- Roles and features needed for HQ and DVS
- Supported OS and service packs
- VBScript issues that may occur during installation
- Amount of space needed for the installation

When running the compatibility checker prior to upgrading the MiVoice Connect Server software, the utility checks for the following:

- Roles and features needed for HQ and DVS
- Supported OS and service packs
- Supported upgrade paths

- Amount of space needed for the installation
- State of MySQL services and MiVoice Connect services

13.1.1 Running the Compatibility Checker

Run the compatibility checker from the Universal Serial Bus (USB) flash drive before running the installer.

1. Install the latest Microsoft operating system updates, as described in the MiVoice Connect Release Notes.
2. Install the Microsoft Visual C++ Redistributable.
3. Insert the MiVoice Connect USB flash drive into the USB port.
4. Navigate to the USB flash drive on your computer, open the **Tools** folder.
5. Double-click **CompatibilityChecker.exe**.
6. Select **Run**.
7. Click **Compatibility Checker**. All components and any compatibility issues are listed.

Note:

- You must address all compatibility issues before beginning the software installation.
- The compatibility checker is also available as part of the installer and can be run from the installation wizard

13.2 Prerequisites and Validation Steps For Upgrading the MiVC Server

Prerequisities

The following are the tasks you must perform before you proceed to upgrade the MiVoice Connect Server software:

- Enable the primary network interface card (NIC) for the server and ensure that it is on top of the NIC BindingList. This maintains the priority of the adapter so that the TAPI provider IDs do not change.
- Ensure that IPV6 for the primary NIC is disabled on the headquarters (HQ) and Windows Distributed Voice Servers (DVS) servers.
- (For US customers) Before you upgrade MiVoice Connect to 19.2 SP2 version, you must ensure that the prerequisities for enabling RAY BAUM in your MiVoice Connect system are met. For information about the prerequisities, see the *Prerequisities for Enabling RAY BAUM* section in the *MiVoice Connect System Administration Guide*.
- When you run the MiVoice Connect installer file in your system, MiVoice Connect will install the Microsoft redistributable 2013 update to the target system if this update is not already on the system. After these dependencies are installed, the MiVoice Connect installer might prompt the user to restart

the system now or later. You must select the **Restart now** option, after which the MiVoice Connect installer will continue automatically.

- There is a version change in the CDR database. You must take a backup of the CDR database. While taking a backup of the CDR database, you will be prompted to press **OK** to continue and **Cancel** to abort the operation.

Validation Steps for Windows Server

Perform the following validation steps on Microsoft Windows Server 2012:

1. On the HQ and Windows DVS servers, go to **Network and Adapter settings** > **Change adapter settings** and click **Advanced Menu**.
2. In the window that opens, click **Advanced settings**.
3. In the window that opens, under **Connections**, adjust the binding order for the NICs to ensure that the primary NIC for the Voice network is at the top of the NIC BindingList.
4. For the selected primary NIC, under **Bindings for Network Connect Adapter**, clear the **Internet Protocol Version 6 (TCP/IPv6)** option.

Perform the following validation steps on Microsoft Windows Server 2016/Microsoft Windows Server 2019:

Note:
Microsoft Windows Server 2016 uses the Interface Metric property of a network adapter to determine which route has the highest priority. The lower the Interface Metric property value, the higher the priority accorded to a route.

1. On the HQ and Windows DVS servers, go to **Network and Adapter settings** > **Change adapter settings**.
2. Select the primary network adapter, right-click it, and select **Properties**.
3. In the window that opens, clear the **Internet Protocol Version 6 (TCP/IPv6)** option.
4. Select the **Internet Protocol Version 4 (TCP/IPv4)** option and click **Properties**.
5. In the window that opens, click **Advanced**, clear the **Automatic metric** option, and enter a low value in the **Interface metric** field.

Note:
The lower the Interface metric property value, the higher the priority accorded to a route.

While you are preparing HQ Windows Server 2016/Windows Server 2019 to run the MiVoice Connect services, the server might fail to recognize the valid IIS version (currently, IIS 10). To resolve this, run the

.vbs utilities (`SetIIS_version.vbs`and `ResetIIS_version.vbs`) included with the Installation Media under the 2016 Scripts folder.

1. Run `SetIIS_version.vbs` to update the registry.
2. Start the MiVoice Connect server installation on Windows Server (Windows Server 2016/Windows Server 2019).
3. After the installation is complete, run `ResetIIS_version.vbs`

Validation Steps for Linux Server

Prior to upgrade, execute permission of /cf/ftproot folder must be enabled so that phones/ switches can download configuration post upgrade.

To enable the execute permission, do the following:

1. Connect to LDVS through putty.
2. Login as super user.
3. Run the following command: `chmod 755 -R /cf/ftproot`

After successful upgrade or fresh install, when all the phones and switches are up and running fine, administrator needs to disable the execute permission of */cf/ftproot* folder in LDVS.

To disable the execute permission, do the following:

1. Connect to **LDVS** through putty.
2. Login as **super user**.
3. Run the following command:

```
chmod 744 -R /cf/ftproot
```

13.3 Headquarters Server Software Installation

This section describes how to install, verify, and register the MiVoice Connect headquarters server software. Use the procedures for upgrades or new installations.

- Installing the Headquarters Server Software Using the USB on page 192
- Installing the HQ Server Software using the Shortpath Name on page 193
- Verifying the Headquarters Installation on page 194
- Registering the Headquarters Server Software on page 194

Note:

It is recommended to install the HQ server software using the USB.

13.3.1 Before you Begin

Before beginning software installation or upgrade, do the following:

- Ensure that the server meets the physical requirements for the implementation. For more information, see General Recommendations on page 161.
- Ensure that all recommended Microsoft software updates, as described in the MiVoice Connect Release Notes, are installed before beginning the installation process.

Note:

- Mitel recommends that customers continue to install Microsoft updates delivered after the date of the release notes. However, it is possible that a future update might not be compatible with Mitel software. If you do install an update and encounter issues, TAC might recommend you roll back the update and repair or reinstall the Mitel software.
- To reduce potential impact, it is advisable that you apply only critical and high-importance updates. Mitel recommends that customers back up their MiVoice Connect system before installing any Microsoft updates. See the *System Backup and Restore* section in the *MiVoice Connect System Administration Guide* for instructions on backing up the system.

- Close all programs on the server.
- Verify that no anti-virus software or endpoint software is running during installation
- Verify that Microsoft Visual C ++ Redistributable 2015 is installed.
- Connect the server to the Ethernet network. The server must be connected to the network with the correct IP address before installing the software.
- Install MiVoice Connect server software on an NTFS partition.
- Optional, but strongly recommended: Run the compatibility checker. You can run the compatibility checker from the installation wizard. For more information, see Checking Server Compatibility.
- Your server must be equipped with at least 2 GB of RAM. If it has less than 2 GB of RAM, the installer displays a warning message before it starts the installation or upgrade.
- Install the OS, IIS, and all other pertinent software.
- Back up the registry on the server.

13.3.2 Installing the Headquarters Server Software Using the USB

The default parameters presented by the MiVoice Connect installer are recommended. However, if MiVoice Connect software is to be located in a different location, select the correct installation path during the install process.

Note:

The data files are unique to your system and include your system configuration, voice messages, and automated attendant prompts. These files will be stored in a Shoreline data folder and should be included as part of your back-up plan for the server.

1. Insert the USB flash drive. The installer launches automatically.

Note:

If the installer does not launch automatically, navigate to the USB flash drive on your computer, open the Server and Setup folders, and then double-click **setup.exe**

2. Click **Install MiVoice Connect HQ Server**. The **MiVoice Connect HQ serverInstall Wizard** appears.

   The MiVoice Connect installation software performs an initial check of your system. You are prompted to install any required software that is not already installed. You must install the required software before continuing.
3. Click **Compatibility Checker** to check for any compatibility issues.

Note:

You must address all compatibility issues before continuing with the installation.

4. Follow the instructions in the wizard to install the server software.
5. When the installation completes, you are prompted to restart your server. Click **Finish** to restart.

Note:

The current software release does not support port 5004. If you are upgrading from an older release with port 5004 enabled, the installer displays the warning message.

6. If upgrading, restart the Voice Switches to finish the upgrade.

   This process upgrades the firmware on the switches but also affects all calls in progress.

Note:

You must be aware that selecting the check box to apply an upgrade to all appliances in the **Maintenance** > **Status** > **Appliances** page selects only the appliances on that page. If you want to upgrade more appliances than those shown on a page, you must manually select additional appliances on subsequent pages.

7. Mandatory: Register the software. For more information, see Registering the Headquarters Server Software on page 194.
8. Install your license keys. For more information, see Installing License Keys on page 198.

13.3.3 Installing the HQ Server Software using the Shortpath Name

The default parameters presented by the MiVoice Connect installer are recommended. However, if MiVoice Connect software is to be located in a different location, select the installation path during the install process.

1. Set the **8dot3name**.
2. Enter: `Fsutil set 8dot3name <install drive location>: 0`
3. Navigate to the Registry Editor. In the command prompt, enter **Regedit:**
4. Expand **HKEY_LOCAL_MACHINE** > **SYSTEM** > **CurrentControlSet** > **Control** > **FileSystem**. In the right window, select **NtfsDisable8dot3NameCreation**. Set the value to **0**.
5. Stop all the MiVoice Connect related services.
6. In the command prompt, go to `C:\program files (x86)\shoreline communications \shoreware server\quickinstall.exe -man`
7. Reboot the server.
8. To identify which folder does not have shortpath, run the `dir /X` command at the root of the folders. This displays all the folders which have shortpaths.
9. If there are no shortpaths, use the following procedure to create one. Enter the following: `C:\>fsutil file setshortname "C:\Program Files (x86)" PROGRA~2`

13.3.4 Verifying the Headquarters Installation

It typically takes about 30 to 60 seconds after the operating system is up and running for the Microsoft Internet Information Services (IIS) and voice services to be running. You can do the following to verify that these applications are running.

1. Click the **Connect Director** desktop icon to launch Connect Director.

   If IIS is not running, an error message appears. If IIS is running, the Connect Director log in page appears.
2. Log in to Connect Director.

   a. In the **User ID** field, enter the user name that you want to use.

      The default user ID is **admin**.
   b. In the **Password** field, enter the password for the user.

      The default password is **changeme**.
   c. Click **Login**.
3. To verify that Connect Director has been successfully installed on your system, do the following:

   a. In the navigation menu, click **Maintenance** > **Status** > **Servers**. The **Servers** page is displayed.
   b. In the **Servers** list pane, verify that the Headquarters server has a green circle in the first column and that the value in the **Status** column is **In Service**.

13.3.5 Registering the Headquarters Server Software

After upgrading or installing the headquarters server software, you must register the software with Mitel. Registration is mandatory.

Mitel encourages you to register the software promptly so that we have the most up-to-date information concerning your products and installation. If registration is not received by Mitel within 45 days of installation, access to Connect Director is limited. You can only see the registration form. All other portions of the Connect Director is not displayed.

The software can be registered automatically, over the Internet, or through email.

When registering automatically or over the Internet, registration data is transmitted to Mitel over a secure connection to ensure integrity and privacy. The software is registered automatically for upgrades that meet the following prerequisites:

- Contact Information is saved in Connect Director before starting the upgrade process.
- A valid MiVoice Connect system license key is installed before starting the upgrade process.
- Your system can connect through the Internet to the Support web site located at https://MiAccess.mitel.com.

For new installations or upgrades that do not meet these prerequisites, you are prompted to register the software the first time you launch Connect Director after installing or upgrading.

You can also choose to register the software over the Internet or through email. Registration over the Internet is quicker than registration through email.

If an installation does not have adequate or current licenses, Connect Director opens at the License Preview page when you have completed or skipped registration. If registration is not received by Mitel within 45 days of installation, access to Connect Director is limited. You can only see the registration form. All other portions of Connect Director are not displayed.

13.3.5.1 Information Collected through Product Registration

When a customer performs an upgrade or performs a fresh install and requests license keys, the following information is collected through product registration:

- Contact information
- License key list: features activated; features available for activation for each licensed feature
- Server MAC address
- Sales Order Number (for initial installations only)
- Switch inventory: switch types; MAC addresses; serial numbers
- Installed software version information: product name; build number; install timestamp

All this information is included in the End User License Agreement (EULA) provided for an upgrade or installation.

13.3.5.2 Automatic Registration

1. Upgrade MiVoice Connect software.
2. Reboot Headquarters Services.

   Registration information is sent over the Internet to Mitel. Upon receipt, a response is sent. When the response is received, a Compliance Token is created on the Headquarters server, and Connect Director is unlocked. Until registration is completed, a Reminder Notification message (**out-of-date**) is posted in red letters on the Contact Information page.
3. Confirm registration:

   a. Click **Administration** > **System Parameters** > **Contact Information** to navigate to the Contact Information page.
   b. Click **Refresh this page**. The Reminder Notification message is no longer posted.
4. Install your license keys, if necessary. See Installing License Keys on page 198.

If registration information is not received by Mitel (for any reason), Connect Director submits the information every hour for seven days after upgrading. If the process is unsuccessful, you must submit the Contact Information again (over the internet or through email) as often as necessary until registration is completed. If registration is not received by Mitel within 45 days of installation, access to Connect Director is limited, and you can see only the registration form. All other portions of Connect Director are not displayed.

13.3.5.3 Internet Registration

1. Upgrade or install Mitel software, and launch Connect Director.
2. Do one of the following to display the **Contact Information** page:
   - When prompted to register, click **Now**.
   - Click **Administration** > **System Parameters** > **Contact Information**.
3. Enter the requested information in the applicable fields.

> **Note**:
> The **Server MAC Address** field is automatically populated with information from the MiVoice Connect Server. You should change this information only if you want a license for a server other than the one to which you are currently connected. If you have changed this information but instead want the defaults, click Refresh this page. The Sales Order Number is on the packing slip. (Supplying this information is optional for system upgrades.)

4. Click **Now to Register and request product verification**. The **License Preview** page appears.
5. Request a license key, if you do not have one:
   a. Review the information in the **License Preview** page.
   b. Do one of the following:
      - Click **Print** at the top of the page to print the information.
      - Click **Submit** to send the request immediately to Mitel. After verifying the information, Mitel emails the license key within three business days. Until the license key arrives, you can click on **Later** in the **Connect Director Welcome** screen to enter Connect Director. You have up to 45 days to install the license key.
      - Click **Save to File** to save the request for later submission.
6. Click **Submit**.

   Registration information is sent over the Internet to Mitel. Upon receipt, a response is sent. When the response is received, a Compliance Token is created on the Headquarters server, and Connect Director is unlocked. Until registration is completed, a Reminder Notification message (“out-of date”) is posted in red letters on the Contact Information page.
7. Confirm registration:
   a. Exit and then relaunch Connect Director.
   b. Navigate to the **Contact Information** page.
   c. Click **Refresh this page**. The Reminder Notification message is no longer posted.
8. Install your license keys, if necessary. See Installing License Keys on page 198.

If registration information is not received by Mitel (for any reason), Connect Director submits the information every hour for seven days after upgrading. If the process is unsuccessful, you must submit the Contact Information again (over the Internet or through email) as often as necessary until registration is completed. If registration is not received by Mitel within 45 days of installation, access to Connect Director is limited. You can only see the registration form. All other portions of the Connect Director is not displayed.

13.3.5.4 Email Registration

1. Upgrade or install the MiVoice Connect software, and launch Connect Director.
2. Display the Contact Information page by doing one of the following:
   - When prompted to register, click **Now**.
   - Click **Administration** > **System Parameters** > **Contact Information**.
3. Enter the requested information in the applicable fields.

> **Note**:
>
> The **Server MAC Address** field is automatically populated with information from the MiVoice Connect Server. You should change this information only if you want a license for a server other than the one to which you are currently connected. If you have changed this information but instead want the defaults, click Refresh this page. The Sales Order Number is on the packing slip. (Supplying this information is optional for system upgrades.)

4. Click **Now to Register and request product verification**. The **License Preview** page appears.
5. Request a license key, if you do not have one:
   a. Review the information in the **License Preview** page.
   b. Do one of the following:
      - Click **Print** at the top of the page to print the information.
      - Click **Submit** to send the request immediately to Mitel. After verifying the information, Mitel emails the license key within three business days. Until the license key arrives, you can click on **Later** in the **Connect Director Welcome** screen to enter Connect Director. You have up to 45 days to install the license key.
      - Click **Save to File** to save the request for later submission.
6. Click **Save to File**. Follow the steps required to save the (SLR) file on your desktop.
7. Email the SLR file to Mitel at: **license.support@mitel.com**.

   Upon receipt, a response is sent containing a compliance token granting access to Connect Director. This token (or, license key) is associated with the Server MAC address and a System Build Number.
8. Verify the compliance token.
   a. Click **Administration** > **System Parameters** > **Product Verification**. The **Product Verification** page appears.
   b. Enter the Compliance Token and click **Verify**. If the token is valid, a confirmation message is displayed.
9. Confirm registration:
   a. Exit and then relaunch Connect Director.
   b. Navigate to the **Contact Information** page.
   c. Click **Refresh this page**. The Reminder Notification message is no longer posted.

10. Install your license keys, if necessary. see Installing License Keys on page 198.

If registration information is not received by Mitel (for any reason), Connect Director submits the information every hour for seven days after upgrading. If the process is unsuccessful, you must submit the Contact Information again (over the internet or through email) as often as necessary until registration is completed. If registration is not received by Mitel within 45 days of installation, access to Connect Director is limited, and you can see only the registration form. All other portions of Connect Director are not displayed.

13.3.5.5 Installing License Keys

1. View the license packet that you received from Mitel.
2. Launch Connect Director.
3. In the navigation pane, click **Administration** > **System Parameters** > **Licenses** > **Keys**. The **License Key Info** dialog box appears.
4. Click the **New** button at the top of the page.
5. In the **Key** field, enter the license key that you received from Mitel.
6. In the **Comment** field, enter a description of the license.
7. Click **Save**.

The license activates and the information is posted in the License Key page.

If you have not already obtained your license keys, see Obtaining Licenses on page 198.

13.3.5.6 Obtaining Licenses

1. Contact your Mitel partner or reseller and purchase the number and type of needed licenses. The partner or reseller will give you a purchase order number.
2. Launch Connect Director and then log in.
3. Click **Administration** > **System Parameters** > **Licenses** > **Keys**. The **License Key Info** dialog box appears.
4. Click the **Register and Request System Key** button at the top of the page. The **Contact Information** page appears.
5. Enter the information requested in the Register and request system key section. Ensure to include the Sales order number from the purchase order and the customer's primary contact information.
6. Click the **Now** button above the information fields.

The system sends the request to Mitel for processing. After processing the request, Mitel sends the licenses in an email.

13.4 Distributed Voice Server Software Installation

The Distributed Voice Server (DVS) must be a dedicated server with no other applications installed. This means you should not use this server for any of the following: Windows Domain controller, Terminal Server,

Database Server (with MySQL), Web server, nor exchange server. This DVS server must be exclusively dedicated to supporting MiVoice Connect.

A DVS has the same software prerequisites as the Headquarters server.

Before beginning software installation, do the following:

- Ensure that the server meets the requirements for either a Windows DVS or Linux DVS implementation. For more information, see General Recommendations on page 161.
- Windows DVS: Ensure that all recommended Microsoft software updates, as described in the MiVoice Connect Release Notes, are installed before beginning the installation process.
- Connect the server to the Ethernet network. The server must be connected to the network with the correct IP address before installing the software.
- If you are running anti-virus software, ensure that you disable it.

Note:

Installing the anti-virus software is not mandatory on the MiVoice Connect system.

- Verify that Microsoft Visual C ++ Redistributable 2015 is installed.
- Linux DVS: Verify access to a vSphere Client and connection to an EXSi server.
- Install the remote server software on an NTFS partition.
- Optional: Run the compatibility checker to check for any compatibility issues. The compatibility checker is available as part of the server installation and as a standalone utility. For information about using the compatibility checker, see Checking Server Compatibility on page 187.

13.4.1 Installing the DVS Software: Windows

- Installing DVS Software Using USB Flash Drive on page 199
- Installing the DVS Software Using the shortpath Name on page 201

Note:

Mitel recommends that you install the DVS software from the USB flash drive.

13.4.1.1 Installing DVS Software Using USB Flash Drive

1. Insert the MiVoice Connect USB flash drive.
2. Copy all the contents from the USB flash drive to a local folder.

3. Click **Install MiVoice Connect Remote Server**. The **MiVoice Connect Server InstallShield Wizard** appears.

Note:

- The MiVoice Connect installation software performs an initial check of your system. You are prompted to install any required software that is not already installed. You must install the required software before continuing.
- The installer launches automatically and the splash screen appears.
- If the installer does not launch automatically, go to the folder and right-click and run as Administrator on `setup.exe`.

4. Select the Compatibility Checker as described in Running the Compatibility Checker

Note:

You must address all compatibility issues before continuing with the installation.

5. Follow the instructions in the wizard to install the server software.

Note:

- The wizard prompts you to enter the IP address of the Headquarters server. Ensure that the IP address of the remote server does not conflict with the IP address of the Headquarters server.
- During installation, the installer pauses and prompts you to install the appropriate version of Microsoft .NET Framework, which is required for the current software release. The installer downloads .NET Framework from the Microsoft site, so you will need an Internet connection to complete the installation.

6. When the installation completes, click **Finish**. A dialog box appears, prompting you to restart the server.
7. Click **Yes**.

Note:

- After the server restarts, all the necessary software restarts automatically. It typically takes about 30 to 60 seconds after the operating system is up and running for the Microsoft Internet Information Services (IIS) and MiVoice Connect voice services to be running
- Mitel supports the use of a remote desktop to install the remote server software.

13.4.1.2 Installing the DVS Software Using the shortpath Name

1. Set the **8dot3name**.
2. Enter: `Fsutil set 8dot3name <install drive location>: 0`
3. Navigate to the Registry Editor. In the command prompt, enter **Regedit:**
4. Expand **HKEY_LOCAL_MACHINE** > **SYSTEM** > **CurrentControlSet** > **Control** > **FileSystem**. In the right window, select **NtfsDisable8dot3NameCreation**. Set the value to **0**.
5. Stop all the MiVoice Connect related services.
6. In the command prompt, go to `C:\program files (x86)\shoreline communications \shoreware server\quickinstall.exe -man`
7. Reboot the server.
8. To identify which folder does not have shortpath, run the `dir /X` command at the root of the folders. This displays all the folders which have shortpaths.
9. If there are no shortpaths, use the following procedure to create one. Enter the following: `C:\>fsutil file setshortname "C:\Program Files (x86)" PROGRA~2`

13.4.2 Installing the DVS Software: Linux

Follow the steps to create a new virtual machine for LinuxDVS, Virtual Service Appliance (Collaboration), and Virtual Phone/Trunk Switch:

- Downloading Virtual Appliances Software on page 201
- Creating New Virtual Machines in VMware or Hyper-V on page 202
- Configuring and Installing the Software on page 204

13.4.2.1 Downloading Virtual Appliances Software

You can obtain the virtual appliances installation software from the Headquarters server or through Connect Director.

The .iso installer is available from the following location on the Headquarters server:

`C:\inetpub\ftproot\centos\ConnectApplianceInstall.iso`

To download the ConnectApplianceInstall.iso installer from Connect Director:

1. Log in to Connect Director.
2. On the navigation pane, click **System** > **Downloads**. The **Downloads** page appears.
3. Click **VIRTUAL APPLIANCE INSTALL**. A download pop-up window is displayed to let you save the file.
4. Click **Save**.

13.4.2.2 Creating New Virtual Machines in VMware or Hyper-V

VMware

Before creating a new virtual machine in VMware, it is recommended to upload the ISO installer to the VMware datastore. The ISO installer is uploaded only once for a given build, and it can be reused for creating multiple new virtual machines.

To upload ISO Installer file to the vSphere Web Client ESXi 6.0 , 6.5, or 6.7 do the following:

1. Open the vSphere Desktop Client and log in to VMware ESXi server with valid credentials.
2. Navigate to Home, and click **Inventory**.
3. Click **Datastores and Datastore Clusters**.
4. On the **Datastores and Datastore Clusters** tab, select the datastore to which you want to upload the ISO installer file.
5. Right-click the datastore and select **Browse Datastore**. The **Datastore Browser** window appears.
6. Optional: Select the root folder and click **Create a new folder** icon from the menu bar, type the required name, and click **OK**.
7. Select the folder that you created or select an existing folder, and click **Upload a File** icon from the menu bar, and select **Upload File**.
8. Select the appropriate ISO Installer location and click **Open**.
9. For HQ/WinDVS, the ISO Installer file is located at:

   `C:\inetpub\ftproot\centos\ConnectApplianceInstall.iso`.

> **Note**:
>
> Time required to upload the ISO installer file varies, depending on the file size and the network upload speed.

10. In the confirmation dialog box, click **Yes**.
11. Refresh the datastore file browser to verify the uploaded ISO installer file is in the list.

To create a new virtual machine in VMware:

1. On the vSphere Web Client, click **Create/Register VM**. The new **Virtual Machine wizard** appears.
2. On the **Select creating type** tab, select **Create a new virtual machine** and click **Next**.
3. On the **Select a name and guest OS** tab, type the name of a new virtual machine in the **Name** field. The virtual machine name must be unique within each ESXi instance and can contain up to 80 characters.

4. Select Virtual Machine Compatibility and Guest operating system version:
   - For vSphere 6.0:
     - From the **Compatibility** drop-down menu, select **ESXi 6.0 virtual machine**.
     - From the **Guest OS version** drop-down menu, select **CentOS 4/5 or later (64-bit)**.
   - For vSphere 6.5 or 6.7:
     - From the **Compatibility** drop-down menu, select **ESXi 6.5 virtual machine**.
     - From the **Guest OS version** drop-down menu, select **CentOS 4/5/6/7 (64-bit)**.
5. Select **Linux** from the **Guest OS family** drop-down menu.
6. Click **Next**.
7. In the **Select storage** tab, select the datastore location and click **Next**.
8. On the **Customize settings** tab, click the **Virtual Hardware** tab, enter values for CPU, Memory size and Hard disk size based on the appliance type:
   - For Linux DVS and Virtual Service Appliance (Collaboration), the minimum configurations should be:
     - CPU: 4
     - Memory: 8352 MB
     - Hard disk 1: 100 GB
   - For Phone or Trunk switch, minimum configurations should be:
     - CPU: 1
     - Memory: 2304 MB
     - Hard disk 1: 20 GB

     Note:

     These configurations can be higher in the production based on the requirement.

   - By default, SCSI Controller 0 and SATA Controller 0 are added to virtual machine based on the guest operating system that you have selected. To change the values, do the following:
     - SCSI Controller 0: VMware Paravirtual
     - SATA Controller 0:
   - USB controller 1: USB 2.0
   - Network Adapter 1: VM Network and enable Connect.
     - To add a new Network Adapter, click **Add network adapter**.
   - From the **CD/DVD drive 1** drop-down menu, select **Data store ISO**.
   - In the Datastore browser, select **ConnectApplianceInstall.iso**.
   - To add a new CD/DVD drive to a virtual machine, click **Add other device** and **CD/DVD drive**.
   - Video Card: Specify custom settings.
9. Click **Next**.

10. On the **Ready to complete** tab, review the virtual machine settings and click **Finish**.

    The virtual machine appears on the **vSphere Web Client** window.
11. Right-click the virtual machine and select **Power On**.

13.4.2.2.1 Hyper-V

To create a new virtual machine in Hyper-V:

1. On the Hyper-V Manager, right-click **HYP-V** and click **New**.
2. In the pop-up menu, select **Virtual Machine**. The new virtual machine creation wizard appears.
3. On the **Specify Name and Location** tab, type the required virtual machine name, and click **Next**.
4. On the **Specify Generation** tab, select **Generation 1**, and click **Next**.
5. On the **Assign Memory** tab, type the memory size to allocate to the virtual machine:
   - For LinuxDVS and Virtual Service Appliance (Collaboration), the minimum configurations should be:
     - Startup memory: 4096 MB (4GB).
   - For Phone or Trunk switch, minimum configurations should be:
     - Startup memory: 2048 MB (2GB).
6. Click **Next**.
7. On the **Configure Networking** tab, select **Broadcom NetXtreme Gigabit Ethernet #3 - virtual Switch** from the **Connection** drop-down menu, and click **Next**.
8. On the **Connect Virtual Hard Disk** tab, type the virtual hard disk size:
   - For Linux DVS and Virtual Service Appliance (Collaboration), the minimum configurations should be:
     - Size: 100 GB
   - For Phone or Trunk switch, minimum configurations should be:
     - Size: 20 GB
9. Click **Next**.
10. On the **Installation Options** tab, select **Install an operating system from a bootable CD/DVD-ROM**. Select **Image file (.iso)**. Click **Browse**, select **ConnectApplianceInstall.iso** from the file location, and click **Next**.
11. In the **Completing the New Virtual Machine Wizard**, verify the details you have entered and click **Finish**. From the virtual machines list, right-click the newly created virtual machine and do the following:
    - Click **Start** to start the virtual machine.
    - Click **Connect** to connect to the console

13.4.2.3 Configuring and Installing the Software

1. Start the virtual machine to view the boot menu.
2. Type **Enter** to start the installer.

3. To configure the installer type, press tab and do one of the following:
   - For **LinuxDVS**, type **1**.
   - For **Virtual Service Appliance (Collaboration)**, type **2**.
   - For **Virtual IP Phone or SIP Trunk Switch**, type **3**.
4. Press **Enter**.
5. To configure the network settings, for **Do you use DHCP or static IP addressing (dhcp/static)?, type dhcp or static**. Press **Enter**.

   If you select dhcp:

   a. For Enter Server IP address, type the IP address of the managing server.
   b. For Enter Image server IP address, type the IP address of HQ.
   c. For Enter Image version, type the build version to be installed.
   d. Press **Enter**.
   e. Verify the details you have entered, type **yes** to confirm, and press **Enter**.

   If you select static:

   a. For Enter IP address, Enter **netmask**, and Enter **gateway**, type the IP addresses of the appliance respectively.
   b. **Enter the Management Service IP address** and **Enter the Management Service netmask** are optional. The values have to be entered only if you use a second NIC for management.
   c. Enter the **Primary DNS IP address** and entering the **Secondary DNS IP address** is optional.
   d. For **Enter Domain name**, type the domain name for the appliance.
   e. For **Enter Server IP address**, type the IP address of the managing server.
   f. For **Enter Image server IP address**, type the IP address of the HQ.
   g. For **Enter Image version**, type the build version to be installed.
   h. Press **Enter**.
   i. Verify the details you have entered, type **yes** to confirm, and press **Enter**.
6. For **Enter CentOS version (eg. 7)**, enter the CentOS version, which is the latest operating system version on the Mitel-maintained Connect Managing Sever. Currently, the latest version number is 7. Hence, type **7**, and press **Enter**.
7. For **Choose software download from location**, type the Mitel-maintained Connect Managing server location, type **2** and press **Enter**.
8. Installer will install the OS and the Mitel software

> **Note**:
>
> Based on the network speed, the installation approximately takes 10 to 15 minutes.

9. After the installation is complete, the CentOS login screen is displayed.
10. For localhost login, enter the root/Mitel or admin/Mitel login credentials, and press **Enter**.
11. Add the appliance in the HQ. The status indicator for the appliance must turn green.

Note:

For Linux DVS, you must reboot the appliance.

13.4.3 Installing the Software from the Web

Note:
Mitel supports the use of a remote desktop to install the remote server software. The following instructions for installing the remote server software from the Web do not apply for a first time installation for Linux DVS.

1. In a Web browser, log in to **Mitel Software Download Center** (SWDC) either through the partner or through the customer portal at https://MiAccess.mitel.com, or directly at https://swdlgw.mitel.com.

   Note:
   In the MiAccess Partner Portal, the **Mitel Software Download Center** is available under the **Applications** tab.

2. In the **Mitel Software Download Center**, browse to the current version of the remote server software under **MiVoice Connect** > **MiVoice Connect PBX** and download the zip file to a temporary folder on your computer.
3. Unzip the file in the temp folder. To launch the installer as Administrator, right-click **Setup.exe** and select **Run as Administrator**.

   Note:
   The installation wizard checks for any compatibility issues, which must be addressed before continuing with the installation.

4. Follow the instructions in the wizard to install the server software.
5. The wizard prompts you to enter the IP address for the Headquarters server. Ensure that the IP address for the remote server does not conflict with the IP address for the Headquarters server.
6. When the installation is complete, click **Finish**. A dialog box appears, prompting you to restart the server.
7. Click **Yes**.

Note:
After the server restarts, all the necessary software restarts automatically. It typically takes about 30 to 60 seconds after the operating system is up and running for the Microsoft Internet Information Services (IIS) and MiVoice Connect voice services to resume.

13.5 Backing up the Headquarters Server

This section describes how to back up the server operating system.

You have multiple options for backing up a MiVoice Connect server. Both options take the system down during the backup. Either option to create a backup interrupts the normal system operations. Therefore, it should be performed when service impact can be minimized or during the scheduled maintenance period, off-hours.

13.5.1 Option 1. Run the Stop All Script and Copy the Shoreline Data Folder

1. Stop and disable all MiVoice Connect services, then reboot after confirming services are stopped:

   For 64-bit systems: `<drive>:\Program Files (x86)\Shoreline Communications \ShoreWare Server\Scripts\hq_shoretel-stop-svcs.bat`
2. Copy the Shoreline Data folder to a safe location, and label the version and build in the folder in which it is located.
3. Run the start services script to get the phone system services running:

   For 64-bit systems: `<drive>:\Program Files (x86)\Shoreline Communications \ShoreWare Server\Scripts\hq_shoretel-start-svcs.bat`

13.5.2 Option 2. Automating the Scheduled Back-up Tasks for the Server

Use the Windows Task Scheduler to automate a scheduled backup for the MiVoice Connect server.

1. Navigate to the following directory:

   For 64-bit systems: `<drive>:\Program Files (x86)\Shoreline Communications \ShoreWareServer\Scripts\Sample_Backup_Restore`

2. Edit the file `sw_backup_restore.ini`:

```
[Shoreware File Locations]
```

```
ShoreWare.Drive = C:
```

```
ShoreWare.Scripts.Root.Directory = C:\Program Files (x86)\Shoreline
 Communications\ShoreWare Server\Scripts\
```

```
ShoreWare.Scripts.DVM.Root.Directory = C:\Program Files (x86)\Shoreline
 Communications\ShoreWare Server\Scripts\
```

```
ShoreWare.SVCCLI.CMD = /shoretel/bin/svccli
```

```
ShoreWare.Root.Directory = \Program Files (x86)\Shoreline Communications
\ShoreWare Server
```

```
ShoreWare.DVM.Root.Directory = \Program Files (x86)\Shoreline
 Communications\ShoreWare Remote Server
```

- Ensure the Shoreware.Drive parameter value in the [Shoreware File Locations] section, specifies the location where the Shoreline Communications is located.
- If your system includes any V-switch models, make sure the VMB.ip.list parameter under the [VMB] section specifies all of their assigned IP addresses in a comma separated list.
- If your system includes conference bridges, make sure the UCB.ip.list parameter under the [UCB] section specifies all of their assigned IP addresses in a comma separated list.
- Ensure the backup is labeled correctly, and that it is on the correct drive and folder location.

> **Note**:
>
> If you chose a network drive for your backup, be sure the user profile that runs the task has permissions to write to that drive and directory.

3. Open the Task Scheduler by clicking **Start** > **Programs** > **Accessories** > **System Tools** > **Task Scheduler**.
4. Right-click and select **Create new Task**. The **Create Task** screen appears.
5. Enter a name for the task.

6. Select the following Security options:
   - **Run whether user is logged on or not**
   - **Run with highest privileges**
   - **Configure for: Windows Server 2012 R2, Windows Server 2016, or Windows Server 2019**
   - Configure **Change User or Group** to be a user you created to be the back-up user, or the server administrator. You must enter your password for this user.
7. Click the **Triggers** tab.
8. Click **New** to create a new trigger, or click **Edit** to change an existing trigger. The **Edit Trigger** screen appears.
9. Fill out the schedule for when you want the process to run.
10. Click the **Actions** tab and then click **New**. The **New Action** screen appears.
11. Click **Browse** to locate the script: `shoreware_backup.bat`.
12. Enter the path to the script in the **Start in (optional)** field and ensure the script name is shown in the **Program/script** field.
13. Click **OK**.
14. Click the **Conditions** tab and fill in the form according to your business requirements.
15. Click the **Settings** tab and fill in the form according to your business requirements.
16. Click **OK** to save the task.

Note:

During non-business hours, be sure to right-click the script task and run it to ensure that it works

13.6 Upgrading the Server System

This section describes how to migrate an ST14.x system to MiVoice Connect. It also provides information on how to upgrade a system with new hardware:

- Upgrading from 64-bit Windows Server to 64-bit Windows Server on page 210
- Upgrading the System to New Hardware (Same OS) on page 215

Supported components for Next Gen Intel chipset server

Following are the components support Next Gen Intel chipset:

- **Windows**: HQ and WinDVS.
- **CentOS**: Virtual appliances (vPhone Switch, vTrunk Switch, LinuxDVS) and UCB (SA100, SA400 and vUCB).

Note:
Next Gen Intel chipset server - servers using Latest Intel Xeon family chipset which require OpenSSL Version to be >= 1.1.1.

13.6.1 Migrating from a 32-bit to 64-bit Windows Server

The following procedure is required to migrate the server operating system, from any 32-bit Windows Server to a 64-bit Windows Server.

Note:

Disable a user's Active Directory settings before proceeding with the upgrade process. If a user's Active Directory setting is not disabled, you will not be able to log into Connect Director after upgrading.

1. Complete the instructions for backing up your server in Backing up the Headquarters Server before proceeding.
2. Ensure that Windows 2012 R2 64-bit Server, Windows Server 2016, or Windows Server 2019 is installed. MiVoice Connect is supported only on these Windows Servers. Refer to the MiVoice Connect Release for details in addition to the instructions below.

13.6.2 Upgrading from 64-bit Windows Server to 64-bit Windows Server

The following procedure is required to upgrade the operating system from any Windows Server 64-bit to a higher version of 64-bit Windows Server on a server.

Note:
Disable a user's Active Directory settings before proceeding with the upgrade process. If a user's Active Directory setting is not disabled, you will not be able to log into Connect Director after upgrading.

1. Ensure that the server meets the hardware requirements as set forth in the Build Notes
2. Disable a user's Active Directory setting (if enabled). This is an administrator's account into Connect Director.

3. Perform the upgrade during a time window that allows you between 3-8 hours. Systems with only 1-5 switches usually take anywhere between 1-3 hours. The time frame depends on the size of your MiVoice Connect system.

> **Note**:
>
> You will be taking services down to perform this backup and upgrade. Be sure to perform this procedure during a maintenance window.

4. Back up the following databases with the commands listed:

> **Note**:
>
> The default location for the database dumps is C:\.

- CDR database

```
C:\Program Files (x86)\Shoreline Communications\ShoreWare Server\MySQL
\MySQL Server\Examples\backupCDR.bat
```

> **Note**:
>
> Before you back up the CDR database, stop archiving on the Headquarters server.

- Configuration database

```
C:\Program Files (x86)\Shoreline Communications\ShoreWare Server\MySQL
\MySQL Server\Examples\backupConfig.bat
```

- WebBridge database

```
C:\Program Files (x86)\Shoreline Communications\ShoreWare Server\MySQL
\MySQL Server\Examples\backupWebBridge.bat
```

- Monitoring database

```
C:\Program Files (x86)\Shoreline Communications\ShoreWare Server\MySQL
\MySQL Server\Examples\RestoreMonitoring.bat
```

- Archive database on ST12.3 and before: (If your system has an archived database, run the following command.)

```
C:\Program Files (x86)Shoreline Communications\ShoreWare Server\MySQL
\MySQL Server 5.0\bin\mysql.exe --user=root --password=shorewaredba
```

```
--port=4309 --database databasename >"c:\ArchiveCDRdump.sql" 2>>C:\
\RestoreArchiveCDR.log
```

- Archive database on ST13 and above: (If your system has an archived database, run the following command.)

```
C:\Program Files (x86)\Shoreline Communications\ShoreWare
Server\MySQLConfig\MySQL Server\bin\mysql.exe --user=root --
password=shorewaredba --port=4309 --database databasename >"c:
\ArchiveCDRdump.sql" 2>>C:\\RestoreArchiveCDR.log
```

Note:

The \Database folder is excluded from the backup because, in a few rare cases, Windows Server is unable to read database files after they are moved from Windows 2003. To avoid this scenario, Mitel recommends that you back up and restore the databases.

5. For all the backups, ensure the file size is greater than 0 KB.
6. Stop and disable all MiVoice Connect services by running the following batch file:

```
C:\Program Files\Shoreline Communications\ShoreWare Server\Scripts
\hq_shoretel-stop-svcs.bat
```

7. Confirm that all MiVoice Connect services have stopped.
8. Reboot.
9. Copy the Shoreline Data folder (excluding the \Database folder) to a safe location and label the version and build in the folder in which it is located. It is recommended that you copy off the server to a safe location.
10. Restart the MiVoice Connect services by running the following command:

```
C:\Program Files\Shoreline Communications\ShoreWare Server\Scripts\
hq_shoretel-start-svcs.bat
```

11. Ensure that everything is up and running properly.
12. Reboot.
13. Pull off to a safe location the Connect Director Installation files and any other files that you may want to keep.
14. After everything is off the server, reboot and boot from the Windows 64-bit CD-ROM.
15. Format the hard drive and install the Windows 64-bit server.
16. Log in through the local Admin Account.
17. Adjust the NIC so that it has the same static IP and name that it did before.
18. Add the server to the domain. (Be sure that it is placed in an empty Organizational Unit (OU) with Block Inheritance.) No Group Policies should be applied. If Group Policies do need to be applied, be sure that they have already been tested against MiVoice Connect.

Note:

Do not install any Anti-Virus software or Network security software. The MiVoice Connect server is a Telephony Appliance. If you absolutely need Anti-Virus software or Network security software due to security regulations, use KB16704 to configure this properly.

19. Ensure that all of the Application Server Roles and Web Server Roles are installed.
20. Install the SMTP Role under Features.
21. Set DEP to Windows Programs and Services.
22. Install all of the Windows updates approved to the date specified in the Build Notes for the build on your system.
23. Disable Windows updates.
24. Disable Internet Explorer Enhanced Security.
25. Disable the pop-up blocker.
26. Copy your old Shoreline Data folder back to the drive where you want to install the software.
27. Install overtop the old Shoreline Data folder the exact same version of the MiVoice Connect server software that was installed before.

Note:
When installing the MiVoice Connect server on Windows Server 2012 R2 64-bit, Windows Server 2016. or Windows Server 2019, you must launch Setup.exe using the **Run as Administrator** option.

28. Copy the following database dumps to the C:\ directory:

    - Config
    - CDR
    - WebBridge
    - Monitoring
    - Archive SQL (if your system has an archived database)

29. Import the SQL database dumps by running the following commands:

    - To import the CDR database dump:

      ```
      C:\Program Files (x86)\Shoreline Communications\ShoreWare Server\MySQL
      \MySQL Server\Examples\RestoreCDR.bat
      ```

    - To import the Config database dump:

      ```
      C:\Program Files (x86)\Shoreline Communications\ShoreWare Server\MySQL
      \MySQL Server\Examples\RestoreConfig.bat
      ```

    - To import the WebBridge database dump:

      ```
      C:\Program Files (x86)\Shoreline Communications\ShoreWare Server\MySQL
      \MySQL Server\Examples\RestoreWebBridge.bat
      ```

    - To import the Monitoring database dump:

      ```
      C:\Program Files (x86)\Shoreline Communications\ShoreWare Server\MySQL
      \MySQL Server\Examples\RestoreMonitoring.bat
      ```

    - To import the Archive database dump on ST12.3 and before (if your system has an archived database):

      ```
      C:\Program Files (x86)\Shoreline Communications\ShoreWare Server\MySQL
      \MySQL Server 5.0\bin\mysql.exe --user=root --password=shorewaredba
      --port=4309 --database databasename > "c:\ArchiveCDRdump.sql" 2>>C:\
      \RestoreArchiveCDR.log
      ```

    - To import the Archive database dump (if your system has an archived database):

      ```
      C:\Program Files (x86)\Shoreline Communications\ShoreWare
      Server\MySQLConfig\MySQL Server\bin\mysql.exe --user=root --
      password=shorewaredba --port=4309 --database databasename > "c:
      \ArchiveCDRdump.sql" 2>>C:\\RestoreArchiveCDR.log
      ```

13.6.2.1 Perform the following steps on the new server

1. Change the IP of the new server to the IP of the original server.
2. Change the Name of the new server to the Name of the original server.
3. Reboot.
4. Copy the Shoreline data folder that you copied from Step 5 to the new server.
5. Install overtop the old Shoreline Data folder the exact same version of the MiVoice Connect server software that was installed before.

> **Note**:
>
> When installing the MiVoice Connect server on Windows Server, you must launch Setup.exe using “Run as Administrator”.

6. Log in to Connect Director.

13.6.3 Upgrading the System to New Hardware (Same OS)

Note:

This procedure will take down all services performed by the server. Mitel recommends that you perform this procedure during non-business hours.

You must be aware that after the MiVoice Connect software is installed on the server, the server is considered a Telephony Appliance. As a Telephony Appliance, it does not adhere to the same policies, procedures, or security as a data server.

13.6.3.1 Perform the Following Steps on the New Server

1. Ensure that the new server meets the hardware requirements in the Build Notes.
2. Format the hard drive and install the supported Windows Server software.
3. Log in through the local Admin Account.
4. Add the server to the domain.

Note:

- Ensure that the server is placed in an empty Organizational Unit (OU) with Block Inheritance
- No Group Policies should be applied.
- If Group Policies need to be applied, ensure that they have already been tested against MiVoice Connect.
- Do not install any Anti-Virus software or Network security software. The MiVoice Connect server is a Telephony Appliance. If you absolutely need Anti-Virus software or Network security software due to security regulations, use KB16704 to configure this properly.

5. Ensure that all of the Application Server Roles and Web Server Roles are installed.
6. Install the SMTP Role under Features.
7. Set DEP to Windows Programs and Services.
8. Install all of the Windows updates approved to the date specified in the Build Notes for the build on your system.
9. Disable Windows updates.
10. Disable Internet Explorer Enhanced Security.
11. Disable the pop-up blocker.

13.6.3.2 Perform the Following Steps on the Old Server

1. Disable a user's Active Directory setting (if enabled). This is an administrator's account into Connect Director.
2. Stop and disable all MiVoice Connect services by running the following batch file:

   ```
   C:\Program Files (x86)\Shoreline Communications\ShoreWare Server\Scripts\
   hq_shoretel-stop-svcs.bat
   ```
3. Confirm that all MiVoice Connect services have stopped:

   a. Go to the Run menu (WIN + R).
   b. Type **services.msc**.
   c. Review all of the MiVoice Connect services to ensure that they show **Manual** and that the services are stopped.
4. Reboot.
5. Copy the Shoreline Data folder (excluding the \Database folder) to a safe location and label the version and build in the folder in which it is located. It is highly recommended that you copy off the server to a safe location.

> **Note**:
>
> Mitel recommends that you back up these files to a storage device separate from the server that you intend to upgrade.

6. Restart the MiVoice Connect services by running the following batch file:

   ```
   C:\Program Files\Shoreline Communications\ShoreWare Server\Scripts\
   hq_shoretel-start-svcs.bat
   ```
7. Confirm that all MiVoice Connect services are up and running:

   a. Go to the Run menu (WIN + R).
   b. Type **services.msc**.
   c. Review all of the MiVoice Connect services to ensure that they show **Automatic** and that the services are started.
8. Change the name of the server.
9. Change the IP of the server to something different.
10. Reboot.

13.6.3.3 Perform the Following Steps on the New Server

1. Change the IP of the new server to the IP of the original server.
2. Change the Name of the new server to the Name of the original server.
3. Reboot.
4. Copy the Shoreline data folder that you copied from Step 5 to the new server.
5. Install overtop the old Shoreline Data folder the exact same version of the MiVoice Connect server software that was installed before.

> **Note**:
>
> When installing the MiVoice Connect server on Windows Server, you must launch Setup.exe using “Run as Administrator”.

6. Log into Connect Director.

13.7 Upgrading MiVoice Connect Server

Follow these steps to upgrade MiVoice Connect server:

1. Run the Compatibility Checker. See Running the Compatibility Checker on page 188 for instructions on running the Compatibility Checker.

> **Note**:
>
> - The Compatibility Checker verifies the following:
>   - Support for the operating system
>   - The upgrade path
>   - Disk space
>   - State of MySQL service
>   - Database log
> - The minimum disk space is 30.19 GB.

2. Address all the issues reported by Compatibility Checker.
3. Perform a backup of the Headquarters server. See Backing up the Headquarters Server on page 207 for instructions on backing up of the Headquarters server.
4. Perform a backup of the SQL database.

5. For a Hyper-V or VMware environment, take a snapshot of all virtual switches and servers of MiVoice Connect. This will ensure that in case the upgrade fails or needs to be rolled back, reverting to the snapshot will have the system back in working state.

13.8 Upgrading Appliances from MiVC Wind River Linux to CentOS

Note:
Sites with Virtual Appliances utilizing VMware: Sites upgrading from builds older than 21.86.1827.0 that have Virtual Phone Switches, Virtual Trunk Switches, or Connect Linux DVS must have the administrative access to the vSphere console to change the SCSI Controller type or else the upgrade will fail for those virtual components.

This section describes how to upgrade the existing virtual appliances (vPhone Switch, vTrunk Switch, vCollab, and LinuxDVS), and physical appliances (SA100 and SA400) from MiVoice Connect Wind River Linux to CentOS. In addition to supporting VMware, CentOS provides the capability to support Microsoft Hyper-V.

Note:

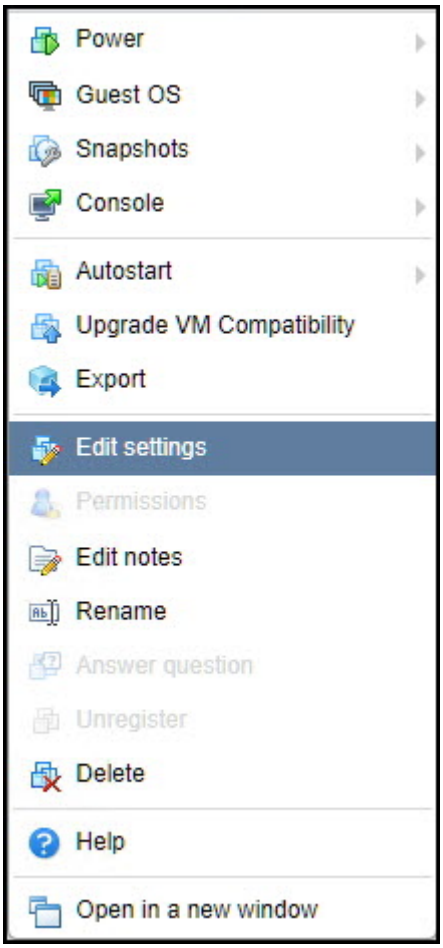
Before upgrading the virtual appliance to CentOS in VMware, the SCSI controller type must be changed to VMware Paravirtual if it is BusLogic Parallel.

1. Log in to the **vSphere** console with the administrative access.

2. Use the following procedure to change the SCSI controller type to VMware Paravirtual if it is BusLogic Parallel:

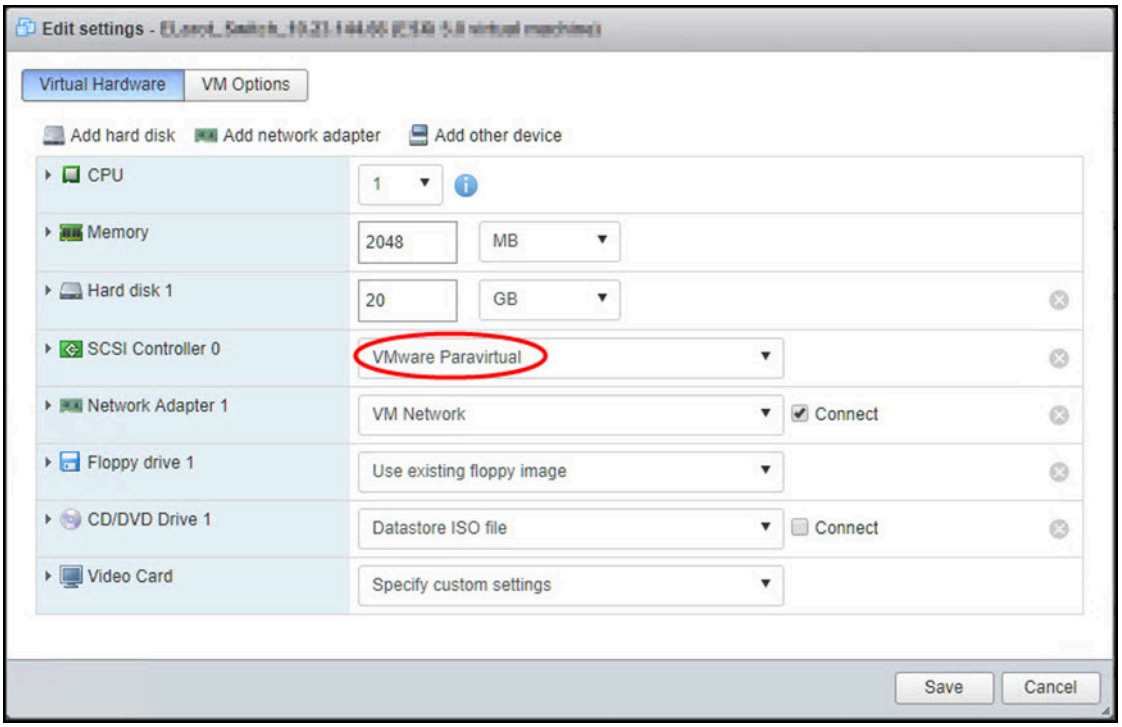
   a. Shut down the Virtual Machine, and click Edit settings.

Figure 16: vSphere



   b. On the **Virtual Hardware** tab of the **Edit Settings** window, change the **SCSI Controller 0 type** field to **VMware Paravirtual**, and click **Save**.

Figure 17: Virtual Hardware Tab



c. Turn on the virtual machine.

3. Set the Image Server for Appliance managed by Linux DVS. To upgrade the appliances from MiVoice Connect to CentOS, the Image Server has to be set as the Headquarters server for the appliances managed by Linux DVS:

   a. Connect to the switch by using Secure Shell (SSH).
   b. Type **stcli**.
   c. Type **3** to select **Change system configuration**.
   d. Type **f** or **F** to change the **Image server IP address** and press **Enter**.
   e. Type the new Image Server IP address to set the **Image Server IP address** to the **Headquarters IP address**.
   f. Press **Enter**.
   g. Press **0**.
   h. For **Do you want to save the changes?**, type **y** to save the changes.

4. Upgrade the virtual appliance by using Connect Director or Command Line Interface (CLI) for the appliances managed by the Linux DVS or the Headquarters server.

Refer to the *Voice Switches* chapter in the *MiVoice Connect Maintenance Guide* for information about the upgrade procedure.

13.8.1 Rollback the Appliance

You can rollback the virtual appliances (vPhone, vTrunk, vCollab, and Linux DVS) and physical appliances (SA100 and SA400) if the upgrade from MiVoice Connect Wind River Linux to CentOS fails. The following are the three types of rollback procedures:

Note:

- For the Headquarters, Windows DVS, Image Server, and other Virtual Machines, use the existing rollback procedure.
- For Rollback SA100 and SA400 Appliance for ST14.2 on page 222, you must rename the MD array before initiating the rollback.

13.8.1.1 Force Upgrade

Use this procedure if you want to roll back the appliances in bulk. Although the appliances are upgraded from MiVoice Connect Wind River Linux to CentOS successfully, if you still want to roll back, do the following:

1. Log in to Connect Director.
2. Navigate to **Maintenance** > **Status and Maintenance** > **Appliances**. The **Appliance** page appears.
3. Select the appropriate appliance(s).
4. Select **Update Software** in the Command, and then select **Force Appliance(s) update** in the command sub list.
5. Click **Apply**.

Alternatively, you can rollback the appliance individually by using `upgrade -v 3` in the Command Line Interface.

13.8.1.2 Changing the Boot Menu

Use this procedure if you want to roll back the appliances individually. This involves the manual update of the appliance and is recommended for a small number of appliances to rollback. Although the appliances are upgraded from MiVoice Connect Wind River Linux to CentOS successfully, if you still want to rollback, do the following:

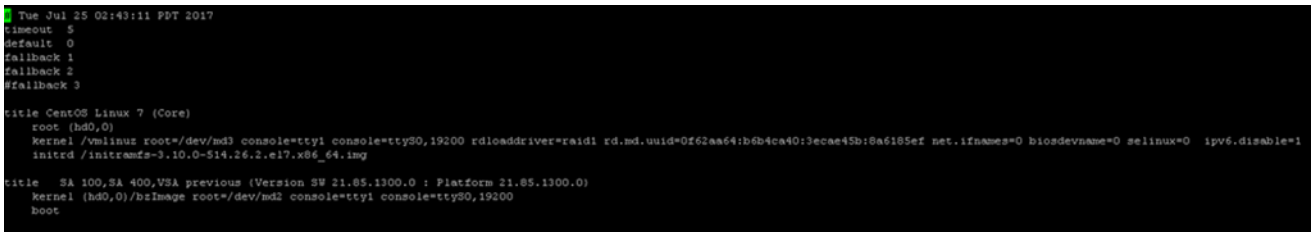
Note:

You must have the administrative access to use the vSphere client.

1. Log in to the appliance host by using either through SSH or vSphere client and switch to root account.
2. Open the **/boot/grub/menu.lst** file by using **vi editor**. The below screen appears as shown in the figure below.

3. On the **Virtual Hardware** tab of the **Edit Settings** window, change the **SCSI Controller 0 type** field to **VMware Paravirtual**, and click **Save**.

Figure 18: Edit Grub Menu



4. Change **default 0** to **default 1**.
5. Save the changes and restart the appliance by running reboot command on the console or resetting the Virtual Machine host by using vSphere client. The appliance will restart in Wind River Linux.

13.8.1.3 Rollback SA100 and SA400 Appliance for ST14.2

Note:

You must rename the MD array before initiating the “SA100 and SA400 Appliance for ST14.2” rollback.

To rollback the SA100 and SA400 appliance, which are upgraded from ST14.2 Wind River Linux to CentOS, do the following:

1. Check any three digit MD array in **/dev/md*** by using the following command:

```
[root@SA400 admin]# ls /dev/md

md0 md1 md126 md2 md5
```

2. Stop the three digit MD array by using the following command:

```
mdadm -stop /dev/md126
```

3. If /dev/md2 is present, rename the three digit MD array to `/dev/md3`.

   If /dev/md3 is present, rename it to /dev/md2.

   For example, **1bmd2** is present, rename **md126** to **md3**.

   You can find the UUID of **md126** by using `mdadm -Es command`.

   ```
   [root@SA400 admin]# mdadm -Es

   ARRAY /dev/md1 level=raid1 num-devices=2
   UUID=0c050efb:04eeb0a2:5eaff68d:a5d1d50c

   ARRAY /dev/md2 level=raid1 num-devices=2
   UUID=b642bbd4:cf8f7dbc:5eaff68d:a5d1d50c

   ARRAY /dev/md126 level=raid1 num-devices=2
   UUID=89b7a3cd:9c5db658:5eaff68d:a5d1d50c

   ARRAY /dev/md5 level=raid1 num-devices=2
   UUID=e7edb04c:5902067a:5eaff68d:a5d1d50c
   ```

4. Rename the UUID by using the following command:

   ```
   mdadm -assemble -uuid=<UUID> --update=super-minor /dev/md3
   ```

5. Start the rollback by using upgrade -v 3 command or use the Force Upgrade procedure by using Connect Director.

13.9 Migrating Connect PBX from VMware to Microsoft Hyper-V

This section describes how to migrate your existing Connect PBX from VMware infrastructure to Microsoft Hyper-V environment. Refer to the following sections for prerequisites and restrictions before proceeding with the migration.

13.9.1 Prerequisites

Before migrating Connect PBX from VMware to Microsoft Hyper-V, you must upgrade the existing Connect PBX on the VMware system to 21.87.3629.0 build.

13.9.2 Restrictions

The following restrictions apply to migrating Connect PBX from VMware to Microsoft Hyper-V:

- For the Headquarters Server, Generation 1 hardware type is supported on Hyper-V with the Windows Server 2016 as the guest operating system. Generation 2 hardware type is not supported on Hyper-V with Windows Server 2016 as the guest operating system.

- Standalone Microsoft Hyper-V Server 2016 is supported. Hyper-V role on Windows Server 2016 is not supported.
- System administrations must retain the same networking parameters such as IP address, subnet mask, default routes, and so on, while bringing up the new PBX system on Hyper-V infrastructure.
- After migrating PBX to the new virtual machine, you must manually change the MAC address of the appliances from Connect Director. You must request for a new license key within 45 days of migration to Hyper-V.
- This procedure is applicable only to migration of VMware infrastructure to Hyper-V infrastructure. For more information about updating Hyper-V 2012 to Hyper-V 2016, refer to the Microsoft standard upgrade procedure.

13.9.3 Upgrading PBX on VMware to 21.87.3629.0 Build

Following are the currently supported upgrades:

- Upgrade ST14.2 to 21.87.3629.0 build

Note:

Refer to the *Migrating the PBX* chapter in the ST14.2 to *MiVoice Connect Migration Guide* for information about the upgrade procedure.

- Upgrade MiVoice Connect to 21.87.3629.0 build

Note:

Refer to Upgrading Appliances from MiVoice Connect Wind River Linux to CentOS for information about the upgrade procedure.

13.9.4 Backing Up PBX on VMware

After upgrading the PBX on VMware to the 21.87.3629.0 build, follow the steps to back up all the files of the Headquarters server, Windows DVS, Linux DVS, and Virtual Service Appliance (Collaboration) as appropriate.

13.9.4.1 Backing Up Linux DVS and VSA (Collaboration)

Note:

This procedure is applicable only if you have deployed a Linux DVS or Virtual Service Appliance (Collaboration) on your system.

1. Log in to the Headquarters server with valid credentials.
2. Open Connect Director.
3. Navigate to **Administration** > **Appliances/Servers** > **Platform Equipment**. The **Platform Equipment** page appears.
4. Click the appliance name to configure in the List pane. The **General** tab in the details pane displays parameters for the selected appliance.
5. In the **General** tab, do either of the following:

   - Follow these steps to enable backup using FTP:

     a. Select the **Enable Daily Backup** check box.
     b. In the **IP Address** field, enter the IP address of the FTP server that you want the device to use for backup.
     c. In the **FTP Port** field, enter the port number that you want the Service Appliance to use to connect to the FTP server. The default value is **21**.

     Note:

     The FTP port must be set to 21. The Service Appliance can perform backup and restore only against FTP server running on port 21.

     d. In the **Directory** field, enter the name of the directory to which you want the Service Appliance to back up files on the FTP server. This file will be create the first time a backup is run.
     e. In the **User ID** field, enter the user name that you want the Service Appliance to use to login to the FTP server account to back up files.
     f. In the **Password** fields, enter the password the Service Appliance needs to use to log in to the FTP server.
   - Follow these steps to enable backup using HTTPS:

     a. Select the **Enable Daily Backup** check box.
     b. In the **IP Address** field, enter the IP address of the HQ server that you want the unit to use for backup.
     c. In the **Directory** field, enter the name of the directory to which you want the Voicemail Model Switches or Service Appliance to back up files on the HQ server. This file will be create the first time a backup is run.
     d. Select the **Enable HTTPS** check box.

Note:

You must provide the Headquarters server (HQ) IP address in the **IP Address** field so that HQ server acts as an FTP or HTTPS server to save the backup files.

6. Click **Save**.
7. Open a command prompt on the Headquarters server and run the following command:

   - For Linux DVS:

     ```
     svccli <LinuxDVS IP address>

     backupvm
     ```

     Note:

     The status of the backup is displayed on the command line. For the successful completion of the backup procedure, ensure that the backup files are created in the location specified in the .ini file.

   - For Virtual Service Appliance (Collaboration):

     ```
     svccli <Virtual Service Appliance (Collaboration) IP address>

     backupweb
     ```

     Note:

     The status of the backup is displayed on the command line. For the successful completion of the backup procedure, ensure that the backup files are created in the location specified in the .ini file.

13.9.4.2 Backing Up the Headquarters Server

1. Log in to the Headquarters server with valid credentials.
2. Open a command prompt and run the following command:

```
C:\Program Files (x86)\Shoreline Communications\ShoreWare Server\Scripts
\Sample_Backup_Restore>shoreware_backup.wsf hq all
```

Note:

A notification appears when the backup is complete.

3. For the successful completion of the backup procedure, ensure that the backup files are created in the location specified in the .ini file.

13.9.4.3 Backing Up the Windows Distributed Voice Servers

1. Log in to the Windows DVS with valid credentials.
2. Open a command prompt on the Windows DVS and run the following command:

```
C:\Program Files (x86)\Shoreline Communications\ShoreWare Remote Server
\Scripts\Sample_Backup_Restore>shoreware_backup.wsf dvm all
```

Note:

A notification appears when the backup is complete.

3. For the successful completion of the backup procedure, ensure that the backup files are created in the location specified .ini file.

Note:

If you have installed more than one Windows DVS, then repeat the steps for all the instances.

Refer to the *System Backup and Restore* chapter of the *MiVoice Connect System Administration Guide* for more information about the backup procedure.

4. After the backup of the Headquarters server and the Windows DVS is completed, do the following:

   a. Store the files that are backed up on a temporary storage device such as shared drive, PC, USB storage, and so on.

Note:

The Headquarters server backup is taken after backing up the Linux DVS and the Virtual Service Appliance (Collaboration). The backup files that are created for Linux DVS and Virtual Service Appliance (Collaboration) under `C:\intepub\ftproot\` are automatically stored in the `Shoreware backup` folder during the Headquarters server backup process.

b. Turn off all the virtual machines on VMware infrastructure to ensure that the IP address does not conflict with VMware after turning on the appliances on Hyper-V infrastructure.

13.9.5 Creating New Virtual Machines for PBX on Microsoft Hyper-V

1. Create a new virtual machine on the Microsoft Hyper-V infrastructure for PBX components similar to that of VMware infrastructure.

   For information about the capacities and the specifications of disk space, RAM, processor, and so on, see Hardware and Network Requirements on page 432.

   We assume that the reader is proficient at managing a Hyper-V infrastructure. In this section, we do not provide steps for creating a new virtual machine on Hyper-V infrastructure.

   Refer to Installing the DVS Software: Linux for information about creating a new virtual machine on Hyper-V infrastructure.
2. Install the Headquarters server and the Windows DVS with 21.87.3629.0 software on the newly created virtual machines on Hyper-V.

13.9.6 Restoring the MiVoice Connect PBX on Hyper-V

After creating new virtual machines for the MiVoice Connect PBX on Hyper-V, follow these steps to restore the PBX backup taken in Backing Up PBX on VMware into the newly installed Headquarters server and the Windows DVS on the Hyper-V infrastructure:

13.9.6.1 Restoring the Headquarters Server

1. Log in to the Headquarters server with valid credentials.

   Place the file that is backed up in the C drive of the Headquarters server.
2. Open a command prompt on the Headquarters server and run the following command:

   ```
   C: \Program Files (x86)\Shoreline Communications\ShoreWare Server\Scripts
   \Sample_Backup_Restore>shoreware_restore.wsf hq all
   ```
3. In the confirmation dialog box, click **OK**.

Note:

A notification appears when the restore is complete.

4. For the successful completion of the backup procedure, ensure that the backup files are created in the location specified .ini file.

Note:

PBX system license and token (license key) are associated with the Headquarters server MAC address. After the migration process, the Headquarters server MAC address gets changed; therefore, you must delete the existing license key, and then request for a new license key with a new Headquarters server MAC address. You have to resubmit the token (license key) to receive a new product verification token. There are up to 45 days to install the license key.

13.9.6.2 Restoring the Distributed Voice Servers

1. Log in to the Distributed Voice Servers with valid credentials.

   Place the file that is backed up in the C drive of the Distributed Voice Servers.
2. Open a command prompt on the Distributed Voice Servers and run the following command:

   ```
   C:\Program Files (x86)\Shoreline Communications\ShoreWare Server\Scripts
   \Sample_Backup_Restore>shoreware_restore.wsf dvm all
   ```
3. In the **confirmation** dialog box, click **OK**.

   A notification appears when the restore is complete.
4. For the successful completion of the backup procedure, ensure that the backup files are created in the location specified .ini file.

13.9.7 Creating New VMs for other Virtual Appliances on Microsoft Hyper-V

1. Create new virtual machines for other virtual appliances such as Linux DVS, Switches and Virtual Service Appliance (Collaboration) on the Microsoft Hyper-V infrastructure similar to that of VMware infrastructure. You must note the values for IP address and MAC address by typing ifconfig -a in the command prompt.

Note:

You must retain the same networking parameters for Linux DVS, Switches, and Virtual Service Appliance (Collaboration) as that of the VMware server.

2. Change the MAC address for Linux DVS, Switches, and Virtual Service Appliance (Collaboration):

   a. Open Connect Director
   b. Navigate to **Administration** > **Appliances/Servers** > **Platform Equipment**. The Platform Equipment page appears.
   c. In the **Name** column, select the required appliance to change the MAC address

      The **General** tab in the details pane displays parameters for the selected appliance.
   d. Change the required MAC address for the appliance.

Refer to Installing the DVS Software: Linux for information about creating a new virtual machine on Hyper-V infrastructure.

13.9.8 Restoring Linux DVS and Virtual Service Appliance (Collaboration)

This procedure restores the configuration and the data that is backed up from Linux DVS and Virtual Service Appliance (Collaboration).

Note:

This procedure is applicable only if you have deployed a Linux DVS or Virtual Service Appliance (Collaboration) on your system.

1. Log in to the Headquarters server with valid credentials.

2. Open a command prompt on the Headquarters Server and run the following command:
   - For Linux DVS:

     ```
     svccli <LinuxDVS IP address>

     restorevm
     ```

     The status of the backup is displayed on the command line.
   - For Virtual Service Appliance (Collaboration):

     ```
     svccli <Virtual Service Appliance (Collaboration) IP address>

     restoreweb
     ```

     The status of the backup is displayed on the command line.
3. After the restore is completed, restart the Linux DVS and the Virtual Service Appliance (Collaboration).

13.9.9 Regenerating HQ Self-signed Certificate

After the restore for Linux DVS and Virtual Service Appliance (Collaboration) is completed, regenerate the Headquarters self-signed certificate.

To regenerate the Headquarters self-signed certificate, do the following:

1. Log in to the Headquarters server with valid credentials.
2. Open Connect Director.
3. Navigate to **Administration** > **Appliances/Servers** > **Platform Equipment**. The Platform Equipment page appears.
4. In the List pane, click the name of the Headquarters server.

   The details for the Headquarters server are displayed in the details pane.
5. Click the **Certificate** tab on the details pane.

   It shows the details for the newly installed Mitel self-signed certificate or any previously imported certificate.
6. Click **Delete Current Certificate**.
7. In the confirmation dialog box, click **OK**, and **Save**.
8. Restart the Headquarters server.

Ensure that the Headquarters server has restored the old certificate.

After regenerating the Headquarters self-signed certificates, make sure the status indicator for all the appliances turns green and is in service in Connect Director. Also, ensure that the basic calls, conferences, Voicemails and call recordings, and the MAC address are matching in Connect Director against the Ethernet interfaces by using the stcli menu in Command prompt.

13.9.10 Rolling Back from Microsoft Hyper-V to VMware

To roll back from Microsoft Hyper-V to VMware, do the following:

1. Turn off all the appliances on the Hyper-V infrastructure.
2. Delete all the virtual machines of the appliances from the Hyper-V server.
3. Turn on the VMware infrastructure, and all the appliances.

13.10 Upgrading the DVS Software

If you are upgrading the Windows DVS server software, follow the instructions in the Installing the DVS Software: Windows. Setup will automatically determine that an upgrade is in process, and you will be presented with a subset of the installation wizard screens. (There is no need to change the destination folders of the MiVoice Connect files.

Note:

- If upgrading and moving users to a LinuxDVS, complete the instructions in the “Move Users from a Windows DVS to a Linux DVS” section of the “Configuring Application Servers” chapter of the MiVoice Connect System Administration Guide. Perform this procedure after adding a Linux DVS to the system. If moving users to a new site, see General Recommendations on page 161 for planning information before completing the task of moving users from Windows DVS to Linux DVS.
- If the Windows DVS server that you are upgrading is on the same server where the BluStar server is installed, you will get the **The installation of Microsoft Visual C++ 2015 Update 3 Redistributable Package (x86) appears to have failed. Do you want to continue the installation?** message. Select **Yes** to proceed with the installation.

If you are upgrading the server software to Windows 2012 R2 64-bit or Windows 2016 from Windows 2008 R2 32-bit/64-bit, perform the following steps:

1. Stop all MiVoice Connect services, and then copy the Shoreline Data folder to a safe location on a different storage device. (If any MiVoice Connect processes are running that prevent you from copying the Shoreline Data folder, use Task Manager to stop the processes.)
2. Back up the registry keys to the same backup location as the Shoreline Data folder. (For a server running a 64-bit operating system, you can open the Registry Editor, right-click the **HKEY_LOCAL_MACHINE\SOFTWARE\ShorelineTeleworks** folder, and select **Export**.)
3. Uninstall the MiVoice Connect system software.
4. Upgrade the operating system to Windows Server 2012 R2 64-bit, Standard or Data Center Edition, or Windows Server 2016, Standard or Data Center Edition.
5. Install the same version of the MiVoice Connect system software that you uninstalled in Step 3.
6. Copy the Shoreline Data folder back to the original location.

7. Restore the registry keys as follows:

   - For a 64-bit operating system, restore the registry by opening the Registry Editor, right-clicking the **HKEY_LOCAL_MACHINE\SOFTWARE\ShorelineTeleworks** folder, selecting **Import**, and specifying the location where you backed up the registry keys folder.
   - For a 32-bit operating system, manually copy the registry entries modified specifically for your system.

13.11 Migrating the Headquarters Server

Sometimes it is necessary to replace an existing Headquarters server. This might be the case when a hardware failure has occurred, the server is being migrated onto a VMware server, or you want to upgrade the operating system.

When you migrate a Headquarters server, you must take care to properly migrate the data and certificates, as described in this section.

The following instructions describe how to replace Server A with Server B on Windows Server 2012.

1. Install MiVoice Connect on Server B by following the instructions in this chapter. Install the same MiVoice Connect version that is running on Server A.
2. On Server A, make a complete backup copy of the Headquarters server files, as described in the *Backing Up the Headquarters Server* section in the *System Backup and Restore* chapter of the *MiVoice Connect System Administration Guide*.
3. Copy the entire backup directory (typically `<drive>:\Shoreware Backup`) from Server A to Server B.
4. Shut down Server A.
5. Reconfigure Server B to have Server A's old IP address, as follows:

   a. In Windows Explorer, right-click **Network and select Properties**.
   b. In the left pane, click **Change adapter settings**.
   c. Right-click **primary interface** and select **Properties**.
   d. Select the **Internet Protocol Version 4 (TCP/IPv4)** check box and then click the **Properties** button.
   e. Enter the old IP address of Server A, and click **OK**.
6. Edit the registry to replace Server B's old IP address with the IP address of Server A, as follows:

   a. Run regedit to open the Registry Editor.
   b. Select the following path:

      `Computer\HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Shoreline Teleworks`
   c. Change the IP addresses for the following registry values:

      - HQServerAddress
      - LocalDBServerAddress
      - ServiceIPAddress

7. On Server B, remove the IIS binding for port 443, as follows:

   a. Run IIS Manager.
   b. Click the computer's local connection.
   c. Under Sites, select **Default Web Site**.
   d. In the **Actions panel** on the right, under **Edit Site** select **Bindings**.
   e. In the Site Bindings dialog, select the line for port 443 and click **Remove**.
8. On Server B, restore the Headquarters server as described in the *Restoring the Headquarters Server* section in the *System Backup and Restore* chapter of the *MiVoice Connect System Administration Guide*.

13.12 Ensuring Proper Server Performance

This section contains guidelines for ensuring the best performance from your MiVoice Connect server. This list is not exhaustive.

Note:
For more server maintenance information, refer to the Microsoft system recommendations at https://www.microsoft.com/en-in/.

- Verify the server meets the hardware requirements, especially memory.
- Regularly defragment your hard drive and perform disk checks at least every other month.
- Optimize server performance for background services rather than for applications.

The voice services running on the server are real-time services that could be negatively affected by having an application running in the foreground. Perform the following steps to optimize server performance:

1. On the MiVoice Connect server desktop click **Start** > **Control Panel** > **System**.
2. Select the **Advanced** tab or click **Advanced system settings**.
3. Depending on your system, do one of the following:
   - Click **Performance Options**. The **Performance Options** dialog box appears.
   - Under **Performance**, click **Settings**, and then select the **Advanced** tab.
4. Select the **Background services** radio button.
5. Ensure the paging file size (virtual memory) on the server is large enough.

Note:

The paging file size should be 1 to 3 times larger than the physical memory on the server. If you have 512 MB of memory, the paging file size should be between 512 MB and 1536 MB. To increase the paging file size, click **Change**.

13.12.1 Setting Server to Maximize Network Performance

1. On the MiVoice Connect server desktop click **Start** > **Control Panel** > **Network and Internet Connections** > **Network Connections**.
2. Depending on your system, do one of the following:
   - Right-click the **Local Area Connection** icon, and then select **Properties**.
   - Click **Local Area Connection**, and then click **Properties**.

   The **Local Area Connection Properties** dialog box appears.
3. Select the **File and Printer Sharing for Microsoft Networks** check box.
4. Deselect the **Internet Protocol Version 6 (TCP/IPV6)** check box.

Note:

The current release of MiVoice Connect software does not support IPv6. For all MiVoice Connect applications to run properly, you must disable IPv6 on all servers.

5. Click **OK**.

Site Requirements and Preparation 14

This chapter contains the following sections:

This chapter provides information about preparing a site for the MiVoice Connect system.

14.1 Recommendations

The following recommendations can assist in the planning and preparation of a site for a MiVoice Connect system.

- Hire a cabling contractor to install the equipment racks, patch panels, and cabling.
- Have RJ-48C cables available for each Voice Switch.

14.1.1 Switch Models

You can locate the model number of your switches on the front or rear panel, as shown in the figure below. This document distinguishes between switches based on the model number and the number of RUs the switch occupies.

Figure 19: ST200 Model Number Label

See Appendix C - Voice Switches on page 333 for information about all Voice Switches. The information describes phone capabilities, connectors, and LED behavior.

14.2 Voice Switch Requirements

This section includes physical requirements for mounting voice switches, along with other switch-related power and heat dissipation requirements and specifications.

14.2.1 Physical Requirements

The voice switches are designed to be mounted in a standard 19-inch rack. The older voice switches and analog port switches are “full width” switches. Each occupies a full rack mount position. The newer voice switches are “half width” switches. Two of these switches can be mounted side by side in a single rack position. Voice Switch Physical Specifications shows the specifications for each voice switch. For more information, see the *Quick Install Guide* included with each voice switch.

Table 32: Voice Switch Physical Specifications

Model	Form Factor	Dimensions (H x W x D)	Weight	Switches per Rack Mount Unit	Max Stacked per Shelf
SG24A	Full Width	1.72 x 17.16 x 14.28 inches 44 x 436 x 363 mm	9 lbs4.08 kg	1	3
SG30	Half Width	1.69 x 8.39 x 14.88 inches 43 x 213 x 378 mm	5.3 lbs2.4 kg	2	3 pairs
SG50	Half Width	1.69 x 8.39 x 14.88 inches 43 x 213 x 378 mm	5.3 lbs2.4 kg	2	3 pairs
SG50V	Half Width	1.69 x 8.39 x 14.88 inches 43 x 213 x 378 mm	5.3 lbs2.4 kg	2	3 pairs
SG90	Half Width	1.69 x 8.39 x 14.88 inches 43 x 213 x 378 mm	5.3 lbs2.4 kg	2	3 pairs
SG90V	Half Width	1.69 x 8.39 x 14.88 inches 43 x 213 x 378 mm	5.3 lbs2.4 kg	2	3 pairs

Model	Form Factor	Dimensions (H x W x D)	Weight	Switches per Rack Mount Unit	Max Stacked per Shelf
SGT1k	Half Width	1.69 x 8.39 x 14.88 inches 43 x 213 x 378 mm	5.3 lbs2.4 kg	2	3 pairs
SGE1k	Half Width	1.69 x 8.39 x 14.88 inches 43 x 213 x 378 mm	5.3 lbs2.4 kg	2	3 pairs
SG220T1	Half Width	1.69 x 8.39 x 14.88 inches 43 x 213 x 378 mm	5.3 lbs2.4 kg	2	3 pairs
SG220E1	Half Width	1.69 x 8.39 x 14.88 inches 43 x 213 x 378 mm	5.3 lbs2.4 kg	2	3 pairs
SG220T1A	Half Width	1.69 x 8.39 x 14.88 inches 43 x 213 x 378 mm	5.3 lbs2.4 kg	2	3 pairs
SG30BRI	Half Width	1.69 x 8.39 x 14.88 inches 43 x 213 x 378 mm	5.3 lbs2.4 kg	2	3 pairs
SG90BRI	Half Width	1.69 x 8.39 x 14.88 inches 43 x 213 x 378 mm	5.3 lbs2.4 kg	2	3 pairs
SG90BRIV	Half Width	1.69 x 8.39 x 14.88 inches 43 x 213 x 378 mm	5.3 lbs2.4 kg	2	3 pairs
ST50A	Half Width	1.65 x 8.35 x 14.65 inches 42 x 212 x 372 mm	5.3 lbs2.4 kg	2	3 pairs
ST100A	Half Width	1.65 x 8.35 x 14.65 inches 42 x 212 x 372 mm	5.3 lbs2.4 kg	2	3 pairs

Model	Form Factor	Dimensions (H x W x D)	Weight	Switches per Rack Mount Unit	Max Stacked per Shelf
ST100DA	Half Width	1.65 x 8.35 x 14.65 inches 42 x 212 x 372 mm	5.3 lbs2.4 kg	2	3 pairs
ST1D	Half Width	1.65 x 8.35 x 14.65 inches 42 x 212 x 372 mm	5.3 lbs2.4 kg	2	3 pairs
ST2D	Half Width	1.65 x 8.35 x 14.65 inches 42 x 212 x 372 mm	5.3 lbs2.4kg	2	3 pairs
ST200	Half Width	1.65 x 8.35 x 14.65 inches 42 x 212 x 372 mm	5.3 lbs2.4 kg	2	3 pairs
ST500	Half Width	1.65 x 8.35 x 14.65 inches 42 x 212 x 372 mm	5.3 lbs2.4 kg	2	3 pairs
ST24A	Full Width	1.73 x 17.36 x 14.80 inches 44 x 441 x 376 mm	12 lbs5.4 kg	1	3
ST48A	Full Width	1.73 x 17.36 x 14.80 inches 44 x 441 x 376 mm	12 lbs5.4 kg	1	3

To mount one or two half width voice switches, the rack must be equipped with a Rack Mount Dual Switch Tray. The Dual Switch Tray is equipped with two pairs of “ears” to enable attachment of the switch to the tray. A pair of mounting ears is also supplied with each half width voice switch.

14.2.2 Input Power and Heat Dissipation Requirements

For backup purposes, Mitel recommends that all voice switches and the server be connected to an uninterruptable power supply (UPS). This ensures that telephone service will continue in the event of a utilities power interruption.

The voice switches dissipate power and heat. Voice Switch Power and Heat Dissipation Specifications shows the power and heat-dissipation requirements for voice switches. Mitel recommends that you use this information to help calculate the ventilation requirements of the room that contains the switches.

Table 33: Voice Switch Power and Heat Dissipation Specifications

Model	Input Voltage	Current Consumption @100 VAC (Maximum)	Power Consumption (Maximum)	Heat Dissipation
SG24A	110 - 240 VAC 50 - 60 Hz	2 A	63 W	
SG30	110 - 240 VAC 50 - 60 Hz	1 A	23 W	137 BTU/hr
SG50	110 - 240 VAC 50 - 60 Hz	1 A	23 W	137 BTU/hr
SG50V	110 - 240 VAC 50 - 60 Hz	1 A	25 W	137 BTU/hr
SG90	110 - 240 VAC 50 - 60 Hz	1 A	31 W	137 BTU/hr
SG90V	110 - 240 VAC 50 - 60 Hz	1 A	33 W	137 BTU/hr
SGT1k	110 - 240 VAC 50 - 60 Hz	1 A	18 W	137 BTU/hr
SGE1k	110 - 240 VAC 50 - 60 Hz	1 A	18 W	137 BTU/hr
SG220T1	110 - 240 VAC 50 - 60 Hz	1 A	18 W	137 BTU/hr
SG220E1	110 - 240 VAC 50 - 60 Hz	1 A	18 W	137 BTU/hr
SG220T1A	110 - 240 VAC 50 - 60 Hz	1 A	29 W	137 BTU/hr
SG30BRI	110 - 240 VAC 50 - 60 Hz	1 A	22 W	137 BTU/hr

Model	Input Voltage	Current Consumption @100 VAC (Maximum)	Power Consumption (Maximum)	Heat Dissipation
SG90BRI	110 - 240 VAC 50 - 60 Hz	1 A	23 W	137 BTU/hr
SG90BRIV	110 - 240 VAC 50 - 60 Hz	1 A	25 W	137 BTU/hr
ST50A	110 - 240 VAC 50 - 60 Hz	1 A	60 W	170 BTU/hr
ST100A	110 - 240 VAC 50 - 60 Hz	1 A	65 W	170 BTU/hr
ST100DA	110 - 240 VAC 50 - 60 Hz	1 A	65 W	170 BTU/hr
ST1D	110 - 240 VAC 50 - 60 Hz	1 A	50 W	170 BTU/hr
ST2D	110 - 240 VAC 50 - 60 Hz	1 A	50 W	170 BTU/hr
ST200	110 - 240 VAC 50 - 60 Hz	1 A	50 W	170 BTU/hr
ST500	110 - 240 VAC 50 - 60 Hz	1 A	50 W	170 BTU/hr
ST24A	110 - 240 VAC 50 - 60 Hz	3 A	125 W	215 BTU/hr
ST48A	110 - 240 VAC 50 - 60 Hz	3 A	200 W	290 BTU/hr

14.2.3 Environmental Requirements

The voice switches require that the environmental specifications provided in Environmental Specifications be met.

Table 34: Environmental Specifications

Parameter	Specification
Operating temperature	0° to 50° C (32° to 122° F)
Operating humidity (non-condensing)	5% to 90%
Storage temperature	-30° to 70° C (-34.4° to 158° F)

14.2.4 Reliability and Availability

The MiVoice Connect system is designed for high reliability. Distributed call control software ensures that there is no system-wide single point of failure. If a single voice switch fails, all other voice switches continue to operate. In addition, Mitel recommends deployments with backup capacity so that other deployed hardware can automatically take over the load from a failed switch with minimal impact to users. Individual system elements, such as voice switches, can be replaced easily, and operation can be restored within minutes.

The following sections provide details about reliability for voice switches and IP phones.

14.2.4.1 Voice Switches

Voice switches are embedded system appliances that are designed to be extremely reliable over a long service lifetime. Hardware components—especially potentially vulnerable parts, such as fans and power supplies—are designed and selected for years of reliable, trouble-free operation. Each power supply has a very high individual Mean Time Between Failures (MTBF).

ST and SG Voice Switches—Currently Available shows both Predicted (calculated based on reliability attributes of hardware components) and Demonstrated (derived from actual performance of the products in customer installations) MTBF values.

These tables also show the expected availability of the voice switches. The Availability calculation is:

Availability = MTBF/(MTTR + MTBF)

The Availability calculation uses the Demonstrated MTBF value, if available, or the Predicted MTBF value, if not. Mean Time to Repair (MTTR) for the calculation is assumed to be one hour.

Table 35: ST and SG Voice Switches—Currently Available

Voice Switch Model	Predicted MTBF Hours	Demonstrated MTBF Hours	Availability (1-Hour MTTR)
ST50A	238008	4,977,870	100.0000%

Voice Switch Model	Predicted MTBF Hours	Demonstrated MTBF Hours	Availability (1-Hour MTTR)
ST100A	225,961	3,501,810	100.0000%
ST100DA	231933	3,102,865	100.0000%
ST1D	253,709	2,636,760	100.0000%
ST2D	238,985	TBD	99.9996%
ST200	261,436	TBD	99.9996%
ST500	261,436	TBD	99.9996%
ST24A	203,508	1,346,850	99.9999%
ST48A	154,657	TBD	99.9994%
SG30	190,606	N/A	99.9995%
SG50	190,606	N/A	99.9995%
SG90	171,493	1,347,789	99.9999%
SG50V	175,803	N/A	99.9994%
SG90V	159,416	N/A	99.9994%
SGT1K	189,373	4,282,180	100.0000%
SGE1K	154,229	312,709	99.9997%
SG220T1	189,373	1,585,560	99.9999%
SG220E1	189,373	N/A	99.9995%

Voice Switch Model	Predicted MTBF Hours	Demonstrated MTBF Hours	Availability (1-Hour MTTR)
SG220T1A	163,516	3,878,490	100.0000%
SG24A	93,733	4,150,050	100.0000%
SG30BRI	172,659	N/A	99.9994%
SG90BRI	172,659	N/A	99.9994%
SG90BRIV	162,931	N/A	99.9994%

14.2.5 Memory and Processing

Memory and processor specifications for voice switches are shown in the following table.

Table 36: Voice Switch Memory and Processor Specifications

Type	ShoreGear Full Width Voice Switches	ShoreGear Half Width Voice Switches	ST Voice Switches
Flash Memory	16 MB	128 MB	4 GB
Random Access Memory	128 MB	128 MB (non V switches)512 MB (V switches)	1 GB
Main Processor	PowerPC 8245	AMCC 440EP	MIPS 6K, multi-core
Digital Signal Processor	Texas Instruments 5409A	Texas Instruments 5502	Texas Instruments 665x, multi-core

14.2.6 Connectors

ShoreGear Voice Switch Connectors summarize all of the connectors on the voice switches. Diagrams showing where these connectors are located are provided later in this chapter.

Table 37: ShoreGear Voice Switch Connectors

Port/Connector	SG220T1 SG220E1	SG220T1A
Power	110 VAC	110 VAC
Ethernet	2 RJ-45	2 RJ-45
Analog telephone/trunk		RJ-21X plug 0–2,000 feet
Digital trunk	RJ-48C	RJ-48C
SGT1 trunk monitor	N/A	N/A
Audio input (Music on Hold)	3.5 mini-mono	3.5 mini-mono
Audio output (Paging, Night Bell)	3.5 mini-mono	3.5 mini-mono
Maintenance	DB-9 socket	DB-9 socket

Table 38: Voice Switch Connectors

Port/Connector	ST200/ST500	ST50A/ST 100A	ST100DA	ST1D/ST2D	ST24A/ST48A
Power	100 - 240 VAC +/-10%	100 - 240 VAC +/-10%	100 - 240 VAC +/-10%	100 - 240 VAC +/-10%	100 - 240 VAC +/-10%
Ethernet	2 RJ-45	2 RJ-45	2 RJ-45	2 RJ-45	2 RJ-45
Analog telephone/ trunk	—	RJ-21X plugFXS: 0–3000ftDID/CO Trunk: 15000 ft	RJ-21X plugFXS: 0–3000ftDID/ CO Trunk: 15000 ft.	—	RJ-21X plugFXS: 0–11,000 feet

Port/Connector	ST200/ST500	ST50A/ST 100A	ST100DA	ST1D/ST2D	ST24A/ST48A
Digital trunk	—	—	RJ-48C	RJ-48C	—
USB 2.0	A-type, 5W	A-type, 5W	A-type, 5W	A-type, 5W	A-type, 5W
Audio input (Music on Hold)	3.5 mini-stereo	3.5 mini-stereo	3.5 mini-stereo	3.5 mini-stereo	3.5 mini-stereo
Audio output (Paging, Night Bell)	3.5 mini-stereo*	3.5 mini-stereo*	3.5 mini-stereo*	3.5 mini-stereo*	3.5 mini-stereo*
Maintenance	DB-9 socket	DB-9 socket	DB-9 socket	DB-9 socket	DB-9 socket
*Supports contact closure with Paging Adapter					

Note:

The cabling referenced in the Analog/telephone trunk row is 26 AWG twisted pair cabling.

14.2.6.1 Power Cabling

Each voice switch comes equipped with a standard 110 VAC modular power cord. A localized modular power cord can be ordered. Mitel recommends that every voice switch, as well as the server, be connected to an uninterruptable power supply (UPS).

14.2.6.2 Ethernet Cabling

Each voice switch has two RJ-45 connectors that provide auto-sensing Ethernet interfaces. ST voice switches support triple 10/100/1000Mbps speeds, and ShoreGear switches support dual 10/100Mbps speeds. These are connected to the local area network using standard Category 5 cabling.

The voice switches come with two network interfaces, LAN1 and LAN2, allowing for a network fault tolerant deployment. You can connect to either or both connectors; there is no primary/secondary relationship. When both are connected, only one will be active at any time. If the currently active interface loses the link, the alternate interface becomes active. Both interfaces will use the same MAC Ethernet address, and IP address.

There are two levels of fault tolerance. To protect against Ethernet switch failure, connect LAN1 and LAN 2 to separate Ethernet switches. To protect against port or cable failure, connect LAN1 and LAN2 to separate ports on the same Ethernet switch.

10/100 Base-T and 10/100/1000 Base-T can typically support up to 100 meters.

14.2.6.3 IP Phone Cabling

Each IP phone has an RJ-45 connector that provides an auto-sensing 10/100M or 10/100/1000M Ethernet interface. This is connected to the local area network using standard Category 5 cabling.

14.2.6.4 Analog Telephone and Trunk Cabling

Voice switches that support analog protocols provide an RJ-21X plug connector for mass termination of the telephones and trunks. This should be connected using a standard 25-pair cable. Mitel recommends using the RJ-21X and connecting to a patch panel to provide simple moves, adds, and changes.

Telephones can be supported from 0 to 11,000 feet from the voice switch over standard cabling, depending on the switch. Use larger gauge wires for longer distances. See the ShoreGear Voice Switch Connectors table for cabling information specific to switches.

It is recommended that an analog telephone be provisioned in the equipment room for troubleshooting purposes.

Pinout information for the voice switches is provided in the quick install guide for each voice switch.

14.2.6.5 Digital Trunk and Trunk Monitor Cabling

Voice switches that support digital trunks have an RJ-48C connector as the telco interface to the SGT1/SGE1 trunk from the telephone service provider.

These voice switches provide an internal Channel Service Unit (CSU).

SG voice switches that support SGT1 and SGE1 trunks have an additional RJ-48C connector that is wired to the telco interface for the purpose of troubleshooting the SGT1 or SGE1 interface with specialized test equipment. This connector is normally not used.

ST voice switches with SGT1/SGE1 interfaces do not include the additional RJ-48C monitor connector.

14.2.6.6 Audio Input (Music on Hold) Cabling

Various voice switches have a 3.5 mm mini-stereo input connector that provide music or some other recording to callers when they are on hold. The input port supports low-level line audio from a preamplifier or mini-CD player, at 47 kW nominal impedance. The audio input cable can be up to 10 feet long. Refer to the quick install guide for your voice switch to determine whether your switch provides the 3.5 mm mini-stereo input connector.

The audio input port on the voice switches is a mono connection. If you connect a stereo input, the stereo signal is converted to a mono signal.

To minimize bandwidth, music on hold is not streamed across the wide area network, so you will need one music source per site.

The music and music source are not included with the MiVoice Connect system.

Note:

In accordance with United States copyright laws, a license may be required from the American Society of Composers, Authors, and Publishers, or a similar organization, if radio or TV broadcasts are played for music on hold. As an alternative, an ASCAP-approved CD or tape can be used. Mitel disclaims any liability out of failure to obtain such a license.

14.2.6.7 Audio Output (Paging and Night Bell) Cabling

Various voice switches have a 3.5 mm mini-stereo audio output connector for overhead paging and night bell on a per site basis. The audio output port provides low-level line audio with a sufficient input level for a typical amplifier. The paging port output is about one volt peak to peak, similar to the line output of a CD player, and can drive inputs that are 600 ohms or higher. Refer to the quick install guide for your voice switch to determine whether your switch provides the 3.5 mm mini-stereo input connector.

The audio output is a mono signal. If you use a stereo jack, the signal is available on one channel, but the other channel will be silent.

This is a single-zone paging system. If more zones are required, see the relevant Application Note in the online knowledge base.

14.2.6.7.1 Paging Adapter and System Contact Closure Support

The Paging Adapter is an accessory that provides transformer-coupled line level audio between a voice switch and a paging system. This accessory is useful for mitigating 60Hz and ground noise found in some paging installations, and it supports contact closure when used with ST voice switch paging ports. Refer to the *Paging Adapter Quick Install Guide* for more information.

14.2.6.8 Maintenance Cabling

The voice switches support a maintenance port for a connection terminal using a standard, straight-through DB-9 socket connector. This maintenance port is typically used only when assigning networking parameters if DHCP is not used.

14.2.6.8.1 USB 2.0 Port

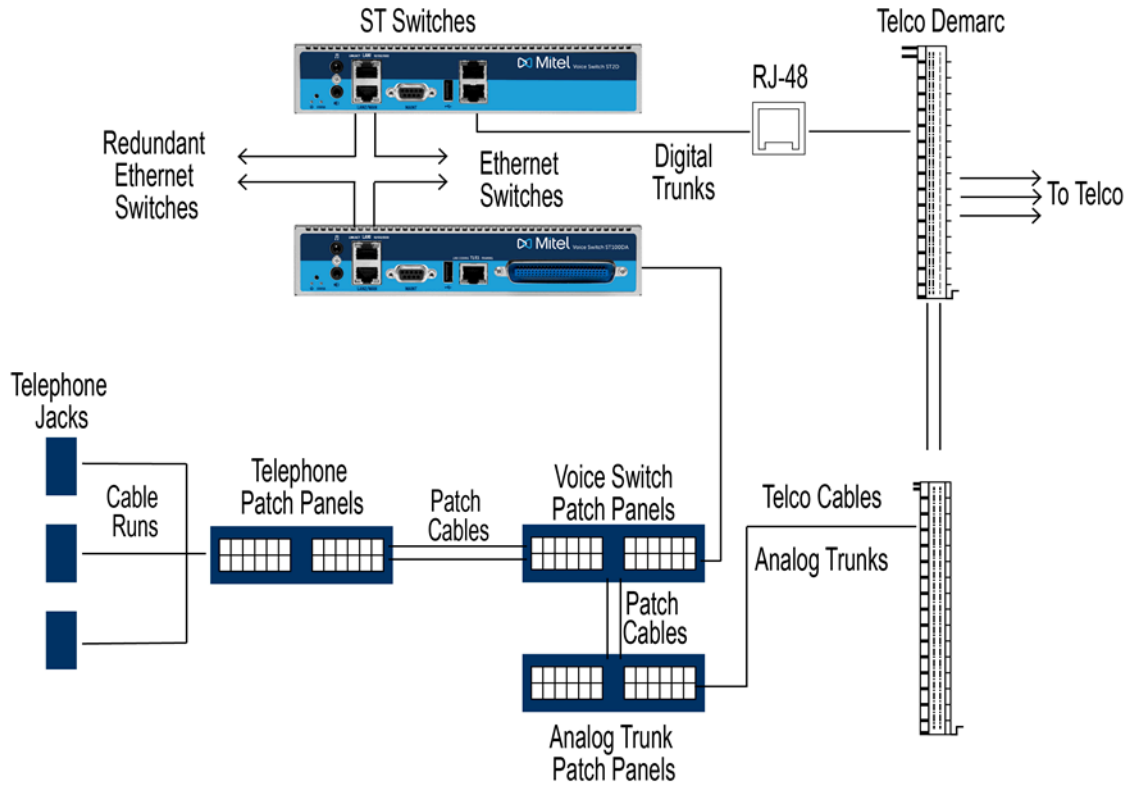
ST voice switches provide a USB 2.0 A-type port to support logging and troubleshooting.

14.3 Racks and Cabling

General Cabling Overview

Cabling Overview highlights the key components with respect to cabling for your voice network.

Figure 20: Cabling Overview



Starting from the lower left in the figure above, the telephone cabling is organized as follows:

- A telephone jack (RJ-11) is provided for each telephone.
- Telephone cabling (Category 3 or better) is terminated on the telephone jack and runs back to the equipment room to a modular connector (RJ-21X) on a telephone patch panel.
- The telephone patch panel provides a flexible cable management solution for the telephone cabling. The patch panel has RJ-21X connections for the telephone cabling and RJ-11 connections on the front.
- Patch cords are connected from the telephone patch panel (RJ-11) to the voice switch patch panel (RJ-11).
- The voice switch patch panel provides a flexible cable management solution for the voice switches. The patch panel has RJ-21X connections running to the voice switches and RJ-11 connections on the front.

Starting from the right in Cabling Overview, the trunk cabling is organized as follows:

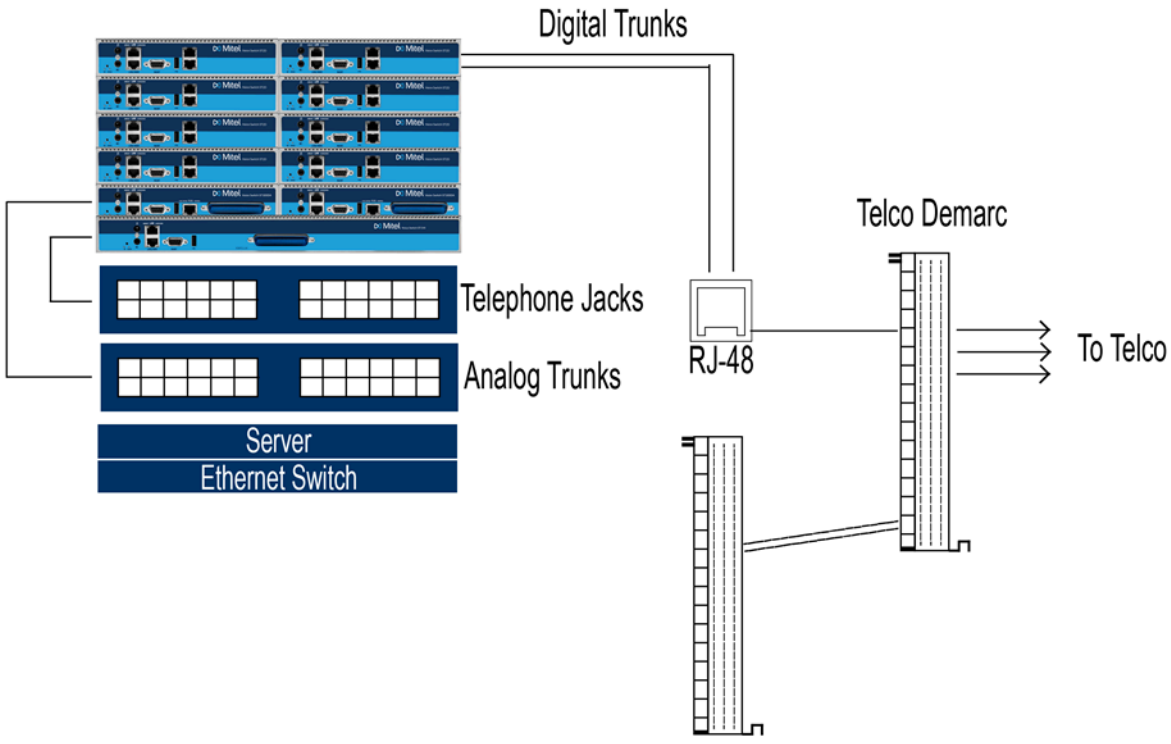
- The digital (SGT1/SGE1) and analog trunks are terminated on a punch-down block.
- The digital service is further terminated at a service provider demark with an RJ-48 connector.
- An RJ-48 cable from the SGT1/SGE1 demark connects to the SGT1 or SGE1.
- The analog service is cross-connected to a modular (RJ-21X) punch-down block.
- A telco cable is connected to the modular (RJ-21X) punch-down jack and runs to a modular connector (RJ-21X) on an analog trunk patch panel.
- Like the telephone cabling, patch cords are connected from the analog trunk patch panel (RJ-11) to the voice switch patch panel (RJ-11).

As an alternative, patch panels can be replaced with punch-down blocks. This may be more cost-effective but is less flexible.

14.3.1 Rack Overview

Rack Installation shows a typical rack installation

Figure 21: Rack Installation



A 19-inch data rack, shelf, and modular patch panels can be purchased from most major electrical suppliers.

Installing Voice Switches 15

This chapter contains the following sections:

This chapter provides planning and installation information for the voice switches, virtual switches, and virtual Service Appliances. Information on switch connectors and LEDs can be found in General Recommendations on page 161. The topics discussed include the following:

15.1 Planning

Note:

Throughout this document, references to switches encompass the ST and SG generations of switches.

In the MiVoice Connect system, switches perform vital roles in connecting endpoints in a call whether the endpoints are located on the network, another private network, or the PSTN. Every IP phone on the network must register with a switch. The switch provides dial and ring tone to the phone when required, performs call setup and teardown task, sets up call legs, communicates with other switches and devices. The switches also provide the physical and logical interface that allows the system to connect with external service providers and other phone networks. When you plan for switches, consider the following:

- The number of IP phones that will connect to the switch
- The type of interface you provision from the external service provider
- Failover

15.2 Mounting the Voice Switches

Stacking the Voice Switch in a Rack

1. Remove the voice switch from its shipping container.
2. Place the switch on a flat platform, such as a shelf.

3. Stack up to three switches on top of each other.

15.2.1 Mounting a Full-width Voice Switch in a Rack with Brackets

1. Remove the voice switch from its shipping container.
2. Attach the two included mounting brackets by using the screws provided.
3. Use standard screws to mount the switch in the rack.

15.2.2 Mounting a Half-width Voice Switch in a Rack with Brackets

Note:

- To prevent overheating and fire hazard, do not use the Rack Mount Dual Switch Tray to wall mount the following devices: ST1D/ST2D, ST50A/ST100A, ST200/ST500, or ST100DA. Use the ST Voice Switch Wall Mount Bracket to wall mount these devices. Refer to the *ST Voice Switch Wall Mount Bracket Kit Quick Install Guide* for information about this kit.
- Refer to the *Quick Install Guide* for the Dual Tray, which is included with half-width switches, for information about the kit.

1. Remove the voice switch from its shipping container.
2. Mount a Dual Tray into the rack with the screws provided.
3. Install the half-width switch into the tray on either the left or right side of the tray. Two half-width switches can be placed in the same tray.
4. Use standard screws to mount the switch in the tray.

15.3 Installing Voice Switches

Note:

Before applying power to a new voice switch, configure the DHCP server.

15.3.1 Installing a Voice Switch

1. Connect the switch to the appropriate LAN segment, such as a LAN switch, with the Category 5 RJ-45 interface cable. For guaranteed voice quality, all voice switches can be connected to an isolated LAN segment.
2. Plug an AC surge protector into a grounded AC power source (not provided). Electrical surges, typically lightning transients, are very destructive to equipment connected to AC power sources.
3. Plug the power cord into the power receptacle on the switch's back panel and then into an available socket on the AC surge protector. Most voice switch models do not have a power switch. They turn on when you connect the switch to a power source.

   The power LED flashes momentarily, and remains lit. If the LED is not lit, ensure that the power cord is plugged into the switch and the power source. If the LED continues flashing, there is an internal error. Unplug the switch to power it off, then power it back on. Refer to the *MiVoice Connect System Administration Guide* for a description of the flash patterns and their meaning.

   Once network communications are established, the network LEDs will indicate that the switch is connected to a 10 Mbps or 100 Mbps Ethernet environment, and that the switch is receiving and transmitting data.
4. If applicable, connect the music-on-hold source to the audio input port.
5. If applicable, connect your site's paging system to the audio output port.

Note:

A Paging Adapter is available to facilitate paging connections. See the *Paging Adapter Quick Install Guide* for more information.

6. Configure the switch network parameters:

   a. Use a straight-through serial cable, DB9 plug to DB9 socket, or suitable USB-to-RS-232 serial adapter to connect the switch maintenance port to a console PC.
   b. On the PC or laptop, start a terminal emulation program and connect to the voice switch using the following serial communication settings:

      - 8 data bits
      - 115,200 bps for ST voice switches or 19,200 bps for SG voice switches
      - no parity
      - one stop bit
      - no handshake

   c. At the login prompt, enter:

      - Login: root
      - Password: ShoreTel

   d. Type `stcli` to bring up the configuration tool to set network parameters and view current status. The default switch configuration is to use DHCP for network parameters and automatic detection of speed, duplex, and flow control settings.
   e. Select **Menu Options** and follow the onscreen instructions for setting network parameters, including IP address, subnet mask, and gateway.
7. Use Connect Director to configure the voice switch according to your site's requirements. Refer to the *Configuring Voice Switches* chapter of the *MiVoice Connect System Administration Guide* for information about this procedure.
8. Connect your trunk and telephone lines using the appropriate connector for your switch. Refer to the quick install guide for your voice switch for connector pinout information.

15.3.2 RJ-21X Cable Retainer Installation

A cable retainer for the RJ-21X port is included with some voice switches. The retainer consists of a metal bracket with a velcro strap.

15.3.3 Installing the Retainer

1. Using a number 1 Phillips screwdriver, remove the two black Phillips head screws on either side of the RJ-21X port.
2. Place the retainer in the recessed area around the RJ-21X port.
3. Reinstall the two screws.
4. Plug in the RJ-21X cable.
5. Pull the velcro strap tightly around the connector on the RJ-21X cable, and fasten it.

15.4 Virtual Switches and Service Appliances

This section describes the following virtual devices:

- Virtual Phone Switch (vPhone Switch)
- Virtual Trunk Switch (vTrunk Switch)
- Virtual Service Appliance (SA-vCollab)

These virtual devices get delivered as separate ISO files and are part of the system installation on the Headquarters Server and the DVS.

You can deploy a virtual device by using a VMware vSphere client on a vSphere ESXi server.

15.4.1 Default Configurations

The installation process creates default configurations for virtual switches and service appliances.

- Memory: 2 GB
- CPU/Cores: 4
- Hard disk: 40 GB
- Video card: Specify custom settings
- SCSI controller: VMware Paravirtual
- Network adapter: VM Network and enable Connect.

Note:

For recommended virtual service appliance capacities, see *Chapter 4, Site Requirements and Preparation*, in the *MiVoice Connect Conferencing and Instant Messaging Planning and Installation Guide*.

15.4.1.1 Virtual Phone Switch Capacity Requirements

Virtual phone switch capacity requirements are provided in Requirements for VMware Environments on page 167.

15.4.1.2 Virtual Phone Switch Feature Capacities

Virtual Phone Switch Feature Capacities table in the Real Time Capacities on page 460section provides the feature capacities for the following virtual switch capacities:

- Up to 1000 phones

15.4.1.3 Virtual Trunk Switch Features and Capacity

Virtual trunk switch capacity requirements are provided in Requirements for VMware Environments on page 167. Virtual trunk switches support up to 1,000 SIP trunks.

15.4.1.4 Virtual Service Appliance Features and Capacity

Virtual and Physical Service Appliance Features and Capacity Requirements table in the Virtual Server / Appliance Requirements on page 444 section provides the virtual service appliance feature capacities.

15.4.2 Downloading and Installing a Virtual Device

For information about the downloading and installing a virtual device, refer to Installing the DVS Software: Linux on page 201.

1. Complete the installation by following the on-screen instructions.

   The installation process creates a virtual machine with the default hardware configuration. For more information about default virtual device configurations, see Default Configurations.

> **Note**:
> You can only increase the disk size before you turn on the virtual machine. If you need to have more disk space for conference recording, you must change it before you turn on the virtual machine.

2. Turn on the virtual machine and allocate the required resources, depending on the capacity of the virtual phone or the virtual trunk switch you want to create:

   - 1000 IP phones
   - 1000 SIP trunks

> **Note**:
>
> The MiVoice Connect system analyzes the allocated resources and determines the capacity of the switch. To change the capacity of the switch, you must change the allocated VM resource

3. Open the console on the virtual switch you want to configure and log in with the following credentials:

   - User ID: admin
   - Password: ShoreTel

4. Enter the DHCP and server IP information that the server will use to download firmware updates. After you enter this information, the switch will begin downloading and installing, and after the installation is complete, restart the switch.
5. When the virtual switch comes back online, open its console and log back in using root/ShoreTel.
6. To open the parameters screen, enter `stcli`.
7. On the parameters screen, note the values for IP address and MAC address. Save these values for configuring the virtual switches in the next step.

8. Configure the virtual device:

   - To configure virtual switches, see *Chapter 5, Configuring Voice Switches*, in the *MiVoice Connect System Administration Guide*.
   - To configure virtual Service Appliances, see *Chapter 6, Configuring the Service Appliance*, in the *MiVoice Connect Conferencing and Instant Messaging Planning and Installation Guide*.

15.5 Connect Director Switch Configuration

To complete the installation, configure the voice switches with Connect Director. For more information, refer to *Chapter 5, Configuring Voice Switches*, in the *MiVoice Connect System Administration Guide*.

15.6 Reference

Environmental Requirements

The voice switches require that the environmental specifications provided in Voice Switch Environmental Specifications be met.

Table 39: Voice Switch Environmental Specifications

Parameter	Specification
Operating temperature	0° C to 50° C
Operating humidity (non-condensing)	5% to 90%
Storage temperature	–30° C to 70° C
Storage humidity (non-condensing)	20% to 90%

15.6.1 Packaging Requirements

Voice Switch Packaging Specifications lists the packaging requirements for the following voice switches:

- Full-width switches – (ST24A/ST48A)
- Half-width switches – (ST1D/ST2D, ST50A/ST100A, ST100DA, ST200/ST500, SG90, SG50, SG220T1/SGE1/T1A)

Table 40: Voice Switch Packaging Specifications

Parameter	Specification
Vibration	Devices can withstand the following: • 3 to 5 Hz sinusoidal vibrations (variable) that are 0.5 inch in amplitude (1-inch peak-to-peak). • Vibration in the vertical direction that lasts for 45 minutes.
Power:	0.4 Grms, 1h per axis
Spectral Density:	5-500Hz @ 0.000323303 g2/Hz
Operation	
Power:	1.5G RMS
Spectral Density:	5-500Hz @ 0.00454645 g2/Hz
Packaged Transportation	
Material:	275 C Brown
Dimensions (full-width switches):	21.5 x 19.5 x 6.5
Dimensions (half-width switches):	18.0 x 12.75 x 6.0
Weight (full-width switches):	13.0 lb (5.9 kg)
Weight (half-width switches):	8.0 lb (3.6 kg)
Mechanical Shock:	80 Gs non-operating
Packaged Bounce	Face: 76cm drop on each Corner: 76cm drop on each

15.6.2 Regulatory Compliance

Table 41: SG90, SG50, SG30 Voice Switch Physical Specifications

Parameter	Physical Specifications
Safety	UL 60950, Third Edition, CAN/CSA 22.2 No. 60950, EN60950 (2000)
Telephony Registration	FCC Part 68, Canada CS-03
EMI	FCC Part 15, ICES-003, EN 55022, Class A
	Radio and Telecommunications Terminating Device Directive (R&TTE) 99/5/EC
	Low Voltage Directive 73 / 23 / EEC
	EMC Directive 89 / 336 / EEC With Amendment 93 / 68 / EEC
	GS Mark from TUV Rheinland (Notified Body)
	EN 55024: 1998 +A1:2001 +A2:2003

15.6.3 Compliance Specifications

Table 42: SG220T1, SG220T1A, SGT1k Voice Switch Compliance Specifications

Parameter	Compliance Specification
Safety	UL 60950, Third Edition, CAN/CSA 22.2 No. 60950, EN60950 (2000)
Telephony Registration	FCC Part 68, Canada CS-03
EMI	FCC Part 15, ICES-003, EN 55022, Class A
	Radio and Telecommunications Terminating Device Directive (R&TTE) 99/5/EC

Parameter	Compliance Specification
	Low Voltage Directive 73 / 23 / EEC
	EMC Directive 89 / 336 / EEC With Amendment 93 / 68 / EEC

15.6.4 General Specifications

The specifications in Voice Switch Specifications apply to the following devices:

- SG90
- SG50
- SG220T1/E1/T1A
- ST50A
- ST100A
- ST100DA
- ST1D
- ST2D
- ST200
- ST500
- ST24A
- ST48A

Table 43: Voice Switch Specifications

Parameter	Specifications
Power Supply	100-240 VAC 50-60 Hz 2A max (SG full-width switches) 3A max (ST full-width switches) 1A max (all half-width switches)
Mounting Options	19 inch rack mount
Integrated OA&M	

IP Phone Installation 16

This chapter contains the following sections:

This chapter describes the steps required to install IP phones.

16.1 Overview

The supported IP phones are pre-configured to work with a MiVoice Connect system and the network's Dynamic Host Configuration Protocol (DHCP) server. After you configure the servers and voice switches and plug the phones into the network, the MiVoice Connect system automatically adds the phones to the network.

This chapter describes prerequisites, network considerations, and procedures for installing IP phones in your system.

16.2 Preparing Your MiVoice Connect System for IP Phones

Preparing your system for IP phones involves the following steps:

- Configure voice switches to support IP phones.
- Assign configuration switches to phones.
- Set IP address ranges for each site if your system includes more than one site.

16.2.1 Configuring Voice Switches for IP Phone Support

To provide PSTN local dialing for IP phone users, every site where IP phones are in use must have a voice switch configured to support the number of IP phones at the site, plus local analog or SGT1 trunks.

Configuring IP phone support on a voice switch involves reserving ports for IP phones. You do this through the Platform Equipment page in Connect Director. For additional information, see the chapter on configuring switches in the *MiVoice Connect System Administration Guide*.

Voice switches send a heartbeat to the IP phones every 60 seconds. If the heartbeat is not acknowledged within approximately 4 seconds, the switch considers the IP phone to be offline or unavailable. The voice switches continue to broadcast the heartbeat every 60 seconds. If an IP phone that was previously offline recovers and returns an acknowledgment, it is then considered online and available.

16.2.2 Assigning the Configuration Switches

You need to designate a voice switch to handle configuration, including initial service requests, for IP phones installed on your MiVoice Connect system. Every IP phone installation must have at least one configuration switch. In addition, to provide a backup in case of network problems, you have the option of assigning two switches for the IP phone configuration function. If you do not assign a switch for configuration, the MiVoice Connect system automatically assigns the first two voice switches added to the system that are managed by the Headquarters server.

To be added to the system, IP phones must be able to contact at least one voice switch, as follows:

- 400-Series and 6900-Series (6910, 6920, 6930, 6940, 6920w, 6930w, and 6940w) IP phones must be able to contact any voice switch at the Headquarters or at the site to which their IP address is mapped.
- The 100-, 200-, 500-, and 600-Series phones must be able to contact at least one of the assigned configuration switches when first connected to the network.

1. Launch Connect Director.
2. Click **Administration** > **Telephones** > **Options**. The **Telephone Options** page is displayed.
3. In the **IP phone configuration switch 1** drop-down list, select a switch to serve as the first configuration switch.
4. In the **IP phone configuration switch 2** drop-down list, select a switch to serve as the second configuration switch.
5. Click **Save**.

16.2.3 Setting IP Address Ranges

If your MiVoice Connect system consists of more than one site, you must define an IP address range for IP phones at each site. Setting IP address ranges for each site ensures that new phones added to the system are associated with the correct voice switch at the designated site.

If a phone with an IP address that is not within a specified range for any site is added or there are no IP address ranges defined for any site, the phone is automatically assigned to the Headquarters site. As a result:

- Any seven-digit numbers dialed from the IP phone are dialed as numbers within the area code of the Headquarters site.
- All calls to users who are not at the Headquarters site use the configured intersite voice encoding for that system.

To set the IP address range for phones at each site:

1. Launch Connect Director.
2. Click **Administration** > **Telephones** > **IP Phone Address Map**. The **IP Phone Address Map** page is displayed.
3. Click **New**. The **General** tab is displayed.
4. In the **Site** drop-down list, select the site for which you want to configure an IP address range.
5. In the **Low IP address** field, enter the lowest IP address to use for the site. The IP address must be valid for the network in which the site is located.
6. In the **High IP address** field, enter the highest IP address to use for the site. The IP address must be valid for the network in which the site is located.
7. In the **Caller's emergency service identification (CESID)** field, type the caller ID number that the system passes to emergency responders when an emergency call originates on an IP phone at the site.

Note:

For information about configuring a system for emergency calls, see the *MiVoice Connect System Administration Guide*.

8. If teleworkers might use the site, select the **Use remote IP phone codec list** check box.
9. Click **Save**.

   The information you configured for the site is listed on the **IP Phone Address Map** page list pane.
10. Repeat steps 3 - 9 to set IP address ranges for other sites in the system.

16.3 Implementing LLDP-MED

Link Layer Discovery Protocol-Media Endpoint Discovery (LLDP-MED) is an enhancement to the Link Layer Discovery Protocol (LLDP) that addresses the following aspects:

- Device location discovery to support location databases and VoIP E911 services
- Auto-discovery of LAN policies to support "plug and play" networking
- Extended and automated power management of PoE endpoints
- Inventory management

Implementing LLDP-MED requires network switches that support the protocol.

MiVoice Connect implements LLDP-MED through the following methods:

- By setting a parameter on the IP phones:
  - On 100-, 200-, 500-, and 600-Series IP phones, you can enable or disable LLDP-MED through the **LLDP Enable** option, which you can access through **MUTE 73887# (SETUP#)**. The default is **On** (enabled).
  - On 400-Series IP phones, you can enable or disable LLDP-MED through the **Use LLDP-MED** option available in the **Admin options** > **Network policy** menu, which you can access through **MUTE 73887# (SETUP#)**. The default is **On** (enabled).

- By modifying configuration settings. When setting up IP phones, parameter settings are obtained from the following sources, listed in order of highest to lowest precedence:
  - Configuration files
  - DHCP (if active)
  - LLDP (if active)
  - Setup command
  - Default values

The IP Phone models IP110 and IP115 do not support LLDP-MED.

Implementing LLDP for 6900-Series IP Phones

To implement LLDP on 6900-Series (6910, 6920, 6930, 6940, 6920w, 6930w, and 6940w) phones, follow these steps:

1. Go to **Settings**.
2. Select **Advanced**.
3. Enter the password in the **Enter Administrator Password** field.

> **Note**:
>
> If the phone is in factory-default settings, enter **22222** as the password. If the phone is registered with the MiVC system, use the default password **1234** or the password set by the administrator.

4. Select **Enter**.
5. Select **Network**.
6. Select **LLDP**.

> **Note**:
>
> The **Enabled** option is selected by default.

16.4 Implementing IEEE 802.1x

Most IP phones in the MiVoice Connect system support 802.1x network authentication. The IP phones support the following aspects of 802.1x authentication:

- MD-5 challenge method only. However, the MD-5 challenge method is not supported in Windows Server 2008 R2 and later. Using 802.1x with the MD-5 challenge method requires a separate authentication server.
- Multicast and unicast frames
- Devices attached to the second Ethernet port (PC port) using 802.1x PAE multicast frames
- EAPOL frames can be prioritized. EAPOL VLAN tags are not supported.
- Mandatory TIA-1057 LLDP-MED functionality for Class III communication device endpoints

IP phones that support 802.1x authentication are shipped with the feature enabled by default. The first time the phone connects to a network that has 802.1x enabled, the phone must present an ID and password for the user. The default secure user ID is the last six characters of the phone's MAC address; the password must be manually entered when the phone boots for the first time. The password is cached if authentication succeeds. If the authentication fails, the phone does not boot.

The 802.1x Protocol on the IP phone facilitates media-level access control, and offers the capability to permit or deny network connectivity, control LAN access, and apply traffic policy, based on user or endpoint identity. This feature supports both the EAP-MD5 and EAP-TLS Protocols.

On networks where 802.1x authentication is not enabled, IP phones boot normally when they connect to the Ethernet switch.

If upgrading from a firmware version that supports 802.1x (3.3.x or 3.4.x), the previous settings (802.1x on/off, SID, password) are preserved. If upgrading from a firmware version that does not support 802.1x (2.2, 2.3, 3.1, 3.2), Logical Link Discovery Protocol (LLDP) is turned on by default, and a default SID of the last six characters of the MAC address is applied.

While 802.1x is enabled by default in ST11 and higher, 802.1x might have been explicitly enabled in earlier releases through the IP phone parameter 802.1xEnable (a 1-character ASCII parameter). If 802.1x is enabled on the IP phone and disabled on the network switch, the IP phone never comes up.

You can modify the 802.1x setting through a parameter on IP phones:

- On 100-, 200-, 500-, and 600-Series IP phones, you can enable or disable 802.1x through the **802.1x Enable** option, which you can access through **MUTE 73887#** (SETUP#). Valid settings are as follows:
- 8021xEnable – 1 (802.1 authentication is enabled.)
- 8021xEnable – 0 (802.1 authentication is disabled. This is the default.)
- On 400-Series IP phones, you can enable or disable 802.1x through the **Use 802.1X** option available in the **Admin options** > **Ethernet menu**, which you can access through **MUTE 73887#** (SETUP#). The default is "On" (enabled).
- On 6900-Series (6910, 6920, 6930, 6940, 6920w, 6930w, and 6940w) phones, you can enable or disable 802.1x through the **802.1x** option available in **Settings** > **Advanced** > **Network** > **802.1x**.

The IP Phone models IP110 and IP115 do not support 802.1x.

16.5 DHCP Settings

IP phones are pre-configured to use the network's DHCP server for addressing. In addition to its address and standard network addresses, the DHCP server's response also provides the following addresses for phone configuration:

- MiVoice Connect server address

  The MiVoice Connect server provides the IP phones with the latest application software and the configuration information that enables IP phones to be automatically added to the MiVoice Connect system. The MiVoice Connect server's address must be provided to the phone as a vendor-specific option. IP phones are pre-configured to look for the MiVoice Connect server's address to be specified as Vendor Specific DHCP Option 156. If this option is not available, the IP phones use Option 66. For information about configuring these DHCP options, see Configuring DHCP for IP Phones on page 43.

- SNTP server address

The DHCP server should be configured to provide the address of your network's SNTP server to provide date and time information to the IP phones.

Note:

If you previously used phones in an environment where automatic provisioning through DHCP was not used or the phones are from a vendor other than Mitel, the phones might not boot properly because incorrect configuration information is present in the phone. For information about clearing a phone's configuration, see Clearing a Phone's Configuration Settings on page 277.

16.6 Installing IP Phones

Installing IP phones involves plugging the phones into the network. The MiVoice Connect system automatically adds the phones to the network. For instructions on manually configuring phones, see Manually Configuring IP Phones on page 267.

16.7 Updating Firmware for IP Phones

After you install new IP phones, you should update the phone firmware.

16.7.1 400-Series and 6900-Series IP Phones

After 400-Series and 6900-Series (6910, 6920, 6930, 6940, 6920w, 6930w, and 6940w) phones are added to the MiVoice Connect system, rebooting the phones updates configuration information and can update the phone firmware to the recommended firmware, depending on settings in the Diagnostics &

Monitoring system (Maintenance menu) available through Connect Director. To update phone firmware or specify automatic upgrades to the recommended firmware level, use the Diagnostics & Monitoring system (Maintenance page) in Connect Director. For details about upgrading phone firmware, see the *MiVoice Connect Maintenance Guide*.

Note:

The firmware version for 400-Series IP phones is different from that for 6900-Series (6910, 6920, 6930, 6940, 6920w, 6930w, and 6940w) phones.

16.7.2 100-, 200-, 500-, 600-, and 900-Series IP Phones

When these phones are initially connected to the network, they reboot and their firmware is updated automatically. You can initiate subsequent firmware updates by triggering a reboot through the Diagnostics and Monitoring system, which is available through Connect Director. For details on upgrading phone firmware, see the *MiVoice Connect Maintenance Guide*.

The boot sequence for these phones is as follows:

1. DHCP on default VLAN. Reboot.
2. DHCP on voice VLAN. Reboot.
3. Connect to the Headquarters server for firmware code. Reboot.

Note:

The Headquarters server uploads the latest phone firmware code to the phone. When the firmware code on the phone is an old version, the server uploads each successive firmware update until the firmware code on the phone is the current version. The phone reboots after each update. The update can take several minutes if the system makes many updates.

4. Connect to Media Gateway Control Protocol (MGCP).

16.8 Manually Configuring IP Phones

If you are not using a DHCP server to provide the IP address and configuration parameters to the phone, you need to manually set configuration parameters on the phone. You can enter the phone configuration menu at bootup or by entering a key sequence from the phone's keypad.

16.8.1 Manual Configuration at Bootup

Use the following procedures to enter the configuration menu while the phone is booting up.

16.8.1.1 On 100-, 200-, 500-, and 600-Series IP Phones

1. Connect the Ethernet cable to the data jack on the back of the IP phone or BB24.

> **Note**:
> To access the BB24 setup screen, press the upper left and lower right buttons.

2. At the **Password=?** prompt, enter the default password **1234**, or the password provided by your system administrator, followed by **#**.

> **Note**:
>
> - You have four seconds to enter the password, after which the phone enters normal operation with its current settings.
> - The default password is set in Connect Director. For more information, see the *MiVoice Connect System Administration Guide*.

3. At the **Clear All Values** prompt, press **#** (No).
4. At each prompt, enter the appropriate value listed in Configuration Values for 100-, 200-, 500-, and 600-Series IP Phones.
5. Press **#** to advance to the next setting or * to exit.
6. To accept changes, press **#**.

The boot process begins after you finish entering new values or accepting existing values. The phone downloads the latest firmware from the MiVoice Connect server and, in the process, reboots several times. When the phone displays the date and time, the boot and upgrade process is complete. See the *MiVoice Connect Maintenance Guide* for details about upgrading the phone's firmware.

Table 44: Configuration Values for 100-, 200-, 500-, and 600-Series IP Phones

Field	Description
DHCP –	Press * to toggle to the Off position, and then press #.
FTP –	Enter the IP address of your MiVoice Connect server, and then press #.

Field	Description
MGC –	Press **#**. The phone obtains the address from configuration files on the MiVoice Connect server.
SNTP –	Enter the IP address of your time server, and then press #.
802.1Q Tagging – Off	Press **#**. **Note**: Consult your network administrator before changing this value.
VLAN ID –	Press #.
Country –	Enter the country code (see Table 10 on page 52)
Language –	Enter the language code (see Table 11 on page 53).
Save all Changes	Press #. (Yes)

16.8.1.2 On 400-Series and 6900-Series IP Phones

To enter the configuration menu while the phone is booting up, follow these steps for 400-Series IP phones:

Note:

For 6900-Series phones, if the phone is in factory-default settings, enter **22222** as the password. If the phone is registered with the MiVC system, use the default password **1234** or the password set by the administrator.

1. Connect the Ethernet cable to the data jack on the back of the IP phone.
2. As the phone boots, press any key when prompted, to enter setup.
3. At the **Admin Password** prompt, enter the default password **1234** or the password provided by your system administrator.

Note:

This password is configured through Connect Director in the **Administration** > **Telephones** > **Options** page. The parameter name is IP phone password. If the phone uses factory defaults, and the phone has never been connected to a server, and you have not modified the IP phone password value, use the default password, **1234**.

4. Do one of the following:
   - On the IP420 and IP420g, press **#**.
   - On the IP480, IP480g, and IP485g, press the **OK** soft key. The **Admin options** menu opens.
5. Use the navigation key pad and the selector button to open the submenus necessary to configure parameters as follows:
   - If you are not using a DHCP server to provide an IP address, enter the following information:
     - Internet protocol > Use DHCP (Toggle to Off.)
     - Internet protocol > IPv4 address
     - Internet protocol > Subnet mask
     - Internet protocol > Gateway
     - Internet protocol > SNTP server (Enter the IP address of the time server.)
   - If you are not using DHCP to provide configuration parameters, enter the following information:
     - **Services** > **Config server** (Enter the IP address of the MiVoice Connect configuration server.)

     For descriptions of these parameters, see Configuration Values for 400-Series IP Phones.
6. With the appropriate submenu highlighted, do one of the following:
   - On the IP420 and IP420g, press the selector button on the navigation key pad.
   - On the IP480, IP480g, and IP485g, press the **Edit** soft key.
7. To return to the previous menu, do one of the following:
   - On the IP420 and IP420g, scroll down to the **Back** option and press the selector button on the navigation key pad until you return to the top-level menu.
   - On the IP480, IP480g, and IP485g, press the **Back** soft key until you return to the top-level menu.
8. To apply the changes, do one of the following:
   - On the IP420 and IP420g, with **Exit** selected, press the selector button on the navigation key pad.
   - On the IP480, IP480g, and IP485g, press the **Apply** soft key. The phone reboots and applies settings.

Note:

On IP480, IP480g, and IP485g phones, to apply the changes and exit the menu, press and hold the **Back** soft key for 2 seconds.

Table 45: Configuration Values for 400-Series IP Phones

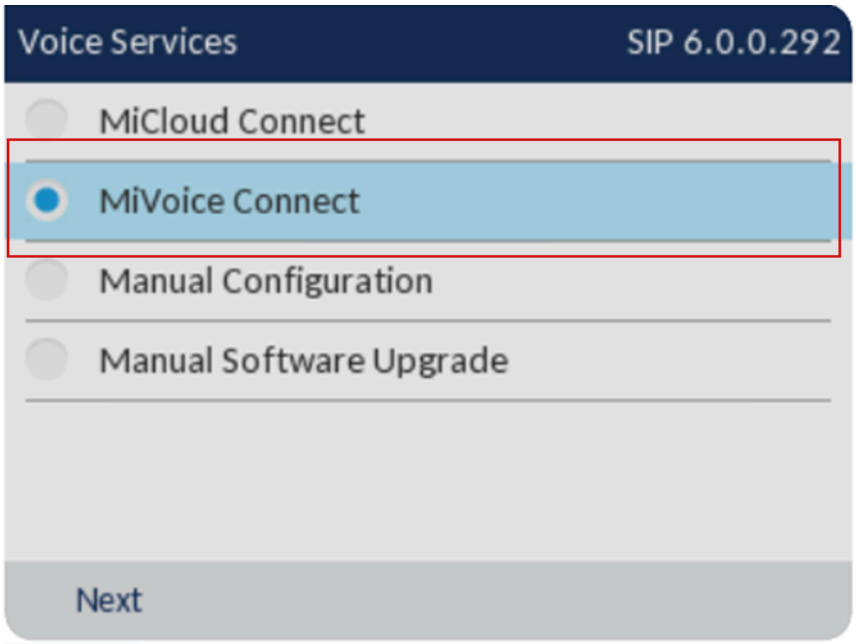
Admin Options Menu Submenu	Option Name	Value to Enter
Internet Protocol	Use DHCP	Toggle to Off.
	IPv4 address	Enter the static IP address of the phone.
	Subnet mask	Enter the static IP subnet mask of the phone.
	Gateway	Enter the static IP gateway.
	SNTP server	Enter the IP address of the time server.
Services	Config server	Enter the IP address of the MiVoice Connect configuration server.

Configuring 6900 IP Phones

To enter the configuration menu while the phone is booting up using DHCP, follow these steps for 6900-Series (6910, 6920, 6930, 6940, 6920w, 6930w, and 6940w) phones:

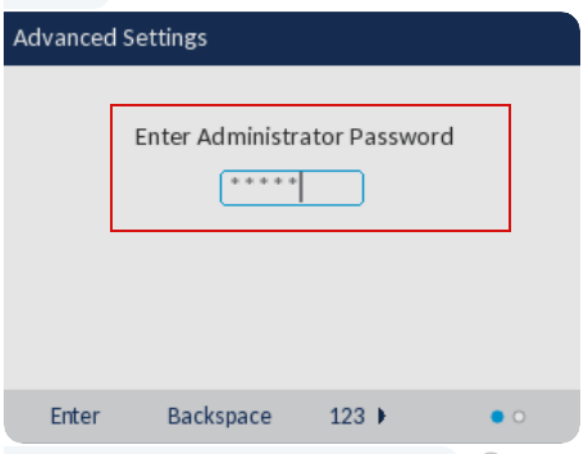
1. Under **Voice Services**, select **MiVoice Connect** from the list of options, and select **Next**.

Figure 22: Voice Services page



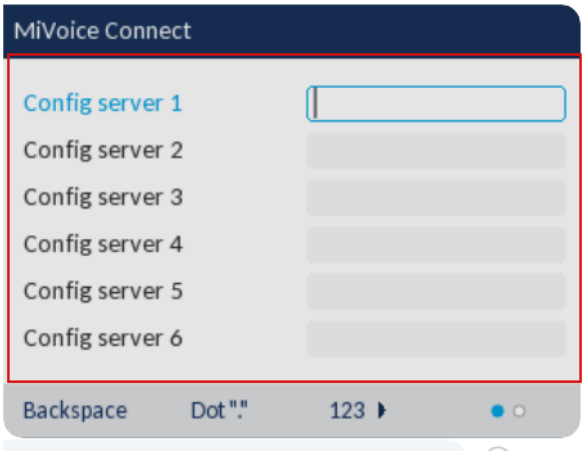
2. Enter the password in the **Enter Administrator Password** field and select **Enter**.

Figure 23: Enter Administration Password Field



3. Enter the **Configuration Server**.

Figure 24: Configuration Server Field



4. Select **Save**. The phone reboots
5. After the phone is back Online in **Available** state, you must assign an extension and password.

Note:
You can register a 6900-Series phone with out-of-the box MiNet firmware only with a MiVoice Connect system that uses a certificate signed by a well-known Certificate Authority (for example, VeriSign, GoDaddy, and GeoTrust) or a UC certificate Authority (ShoreTel UC CA). This is because 6900-Series phones cannot authenticate a certificate signed by a third-party Certificate Authority as the root certificate of third-party CA is not available in the trusted store on 6900-Series phones. If the root certificate of third-party CA were available in the trusted store on 6900 series phones, the phones would have authenticated the certificates as expected. This feature will be supported in a future release.

To enter the configuration menu while the phone is booting up using Static IP, follow these steps for 6900-Series (6910, 6920, 6930, 6940, 6920w, 6930w, and 6940w) phones:

1. Go to **Settings**.
2. Select **Advanced**.
3. Enter the password in the **Enter Administrator Password** field.
4. Go to **Network** > **Settings**.
5. Disable **Use DHCP** option.
6. Enter the IP address in the field.
7. Provide the relevant details in the following fields:
   - **IP Address**
   - **Subnet Mask**
   - **Gateway**
   - **Primary DNS**
   - **Secondary DNS**
8. Select **Save**. The phone reboots.
9. Follow the steps 1 - 7 provided to enter the configuration menu while the phone is booting up using DHCP.

16.8.2 Manual Configuration from the Key Pad

Use the following procedures to enter the configuration menu after the phone has booted.

16.8.2.1 On 100-, 200-, 500-, and 600-Series IP Phones

1. With the phone on hook, press the **MUTE** key followed by **73887#** (SETUP#).
2. At the **Password** prompt, enter **1234**, or the password provided by your system administrator, followed by the **#** key.
3. Enter the values listed in Configuration Values for 100-, 200-, 500-, and 600-Series IP Phones when prompted. Press **#** to advance to the next setting or * to exit.

The phone downloads the latest firmware from the MiVoice Connect server and, in the process, it reboots several times. When the phone displays the date and time, the boot and upgrade process is complete.

16.8.2.2 On 400-Series IP Phones

1. With the phone on hook, press the **MUTE** key followed by **73887#** (SETUP#).
2. At the **Admin Password** prompt, enter the default password **1234** or the password provided by your system administrator.

Note:

This password is configured through Connect Director in the **Administration** > **Telephones** > **Options** page. The parameter name is **IP phone password**. If the phone uses factory defaults, the phone has never been connected to a server, and you have not modified the **IP phone password** value, use the default password, **1234**.

3. Do one of the following:
   - On the IP420 and IP420g, press **#**.
   - On the IP480, IP480g, and IP485g, press the **OK** soft key. The **Admin options** menu opens.
4. Use the navigation key pad and the selector button to open the submenus necessary to configure parameters as follows:
   - If you are not using a DHCP server to provide an IP address, enter the following information:
     - Internet protocol > Use DHCP (Toggle to Off.)
     - Internet protocol > IPv4 address (Enter the static IP address of the phone.)
     - Internet protocol > Subnet mask (Enter the static IP subnet mask of the phone.)
     - Internet protocol > Gateway (Enter the static IP gateway.)
     - Internet protocol > SNTP server (Enter the IP address of the time server.)
   - If you are not using DHCP to provide configuration parameters, enter the following information:
     - Services> Config server (Enter the IP address of the MiVoice Connect configuration server.)

     For descriptions of these parameters, see Configuration Values for 400-Series IP Phones.
5. With the appropriate submenu highlighted, do one of the following:
   - On the IP420 and IP420g, press the selector button on the navigation key pad.
   - On the IP480, IP480g, and IP485g, press the **Edit** soft key.
6. To return to the previous menu, do one of the following:
   - On the IP420 and IP420g, scroll down to the **Back** option and press the selector button on the navigation key pad until you return to the top-level menu.
   - On the IP480, IP480g, and IP485g, press the **Back** soft key until you return to the top-level menu.
7. To apply the changes, do one of the following:
   - On the IP420 and IP420g, with Exit highlighted press the selector button on the navigation key pad.
   - On the IP480, IP480g, and IP485g, press the **Apply** soft key. The phone reboots and applies settings.

Note:

On IP480, IP480g, and IP485g phones, to exit the menu and apply changes, press and hold the **Back** soft key for 2 seconds.

16.9 Displaying Settings for an IP Phone

You can display information about an IP phone by entering a key sequence on the phone's key pad.

16.9.1 On 100-, 200-, 500-, and 600-Series IP Phones

1. With the phone on hook, press the MUTE key followed by **4636# (INFO#)**.

   The phone displays the first one or two parameters, depending on the phone model.
2. Press **#** to advance the display or ***** to exit.

   The phone resumes normal operation after the last parameter has been displayed.

16.9.2 On 400-Series and 6900-Series IP Phones

Note:

For 6900-Series (6910, 6920, 6930, 6940, 6920w, 6930w, and 6940w) phones, if the phone is in factory-default settings, enter **22222** as the password. If the phone is registered with the MiVC system, use the default password **1234** or the password set by the administrator.

Follow these steps to display the settings for 400-Series IP phones:

1. With the phone on hook, press the **MUTE** key followed by **4636# (INFO#)**. The **Admin Options** menu opens.
2. Use the navigation key pad and the selector button to scroll through and open the submenus as necessary to see the phone's settings.

Note:

For descriptions of the parameters, see the *MiVoice Connect Maintenance Guide*.

3. To close the **Admin Options** menu, do one of the following:

   - On IP420 and IP420g phones, with **Exit** selected, press the selector button on the navigation key pad.
   - On IP480, IP480g , and IP485g phones, press the **Exit** soft key.

Follow these steps to display the settings for 6900-Series (6910, 6920, 6930, 6940, 6920w, 6930w, and 6940w) phones:

1. Go to **Settings** ⚙.
2. Select **Advanced**.
3. Enter the password in the **Enter Administrator Password** field.
4. Select **Enter**. The settings for the phone are displayed

16.10 Resetting an IP Phone

You can reset a phone by entering a key sequence on the phone's key pad.

16.10.1 On 100-, 200-, 500-, and 600-Series IP Phones

1. With the phone on hook, press the **MUTE** key followed by **73738# (RESET#)**. The phone reboots.
2. At the **Reset Phone?** prompt, press **#**. The phone reboots.

> **Note**:
>
> The reboot process is complete when the phone displays the date and time.

16.10.2 On 400-Series and 6900-Series IP Phones

> **Note**:
>
> For 6900-Series (6910, 6920, 6930, 6940, 6920w, 6930w, and 6940w) phones, if the phone is in factory-default settings, enter **22222** as the password. If the phone is registered with the MiVC system, use the default password **1234** or the password set by the administrator.

Follow these steps to reset the configuration 400-Series IP phones:

1. With the phone on hook, press the **MUTE** key followed by **73738# (RESET#)**. The phone displays the **Reset phone** screen.
2. Do one of the following:

   - On IP420 and IP420g phones, with **Reset** selected, press the **selector** button on the navigation key pad.
   - On IP480, IP480g, and IP485g phones, press the **Reset** soft key.

   The phone reboots.

Follow these steps to reset the configuration of 6900-Series (6910, 6920, 6930, 6940, 6920w, 6930w, and 6940w) phones:

1. Go to **Settings** ⚙.
2. Select **Advanced**.
3. Enter the password in the **Enter Administrator Password** field.
4. Select **Enter**.
5. Select **Restart** to reset the phone.

16.11 Clearing a Phone's Configuration Settings

You can clear a phone's configuration settings and return it to factory settings by entering a key sequence on the phone's key pad.

If a phone displays "No Service" after it boots, you can use this procedure to clear the settings.

Note:

If you move 400-Series IP phones from one MiVoice Connect system to another, you must clear each phone's configuration settings.

16.11.1 On 100-, 200-, 500-, and 600-Series IP Phones

1. With the phone on hook, press the **MUTE** key followed by **25327# (CLEAR#)**.
2. Press ***** to clear all values. The phone reboots.

Note:

The reboot process is complete when the phone displays the date and time.

16.11.2 On 400-Series and 6900-Series IP Phones

Note:

For 6900-Series (6910, 6920, 6930, 6940, 6920w, 6930w, and 6940w) phones, if the phone is in factory-default settings, enter **22222** as the password. If the phone is registered with the MiVC system, use the default password **1234** or the password set by the administrator.

Follow these steps to clear the configuration of the 400-Series IP phone:

1. With the phone on hook, press the **MUTE** key followed by **25327# (CLEAR#)**. The phone displays the **Clear Configuration** screen.
2. Do one of the following:
   - On the IP420 and IP420g, with **Clear & reboot** highlighted, press the selector button on the navigation key pad.
   - On the IP480, IP480g, and IP485g, press the **Clear** soft key.

   The phone reboots and applies the factory-default settings.

Follow these steps to clear the configuration of the 6900-Series (6910, 6920, 6930, 6940, 6920w, 6930w, and 6940w) phones:

1. Go to **Settings** .
2. Select **Advanced**.
3. Enter the password in the **Enter Administrator Password** field.
4. Select **Enter**.
5. Select **Reset** > **Factory Default** > **Select** to clear the phone's configuration.

Desktop Installation 17

This chapter contains the following sections:

This chapter describes the procedures for installing the Mitel Connect client software on desktop computers.

17.1 Overview

This chapter describes the hardware and software requirements and the subsequent procedures for installing the Mitel Connect client software, and the Mitel Connect client for Windows and Mac computers.

There are two methods of installing Mitel Connect client software:

- Silent Client Install
- Standard Integrated Software Distribution

Note:

The procedures for installing the Mitel Connect client are covered in this chapter. The procedures for installing other Mitel Connect client software are in described in General Recommendations on page 161.

17.2 Prerequisites

The following section describes the requirements and recommendations to be fulfilled prior to installing the Mitel Connect client application on a Windows or Mac computer.

- Verify that each computer meets the minimum requirements as outlined in the *Mitel Connect Client User Guide*.
- Install the Client for the Microsoft Networking component.
- Close all applications before starting the MiVoice Connect software installation.
- Users must have local administrative privileges to install the MiVoice Connect software.

- During a fresh install or upgrade to the Mitel Connect client, Visual Studio Tools for Office (VSTO) pre-requisites need to be installed first. The VSTO prerequisites will be installed automatically during the Mitel Connect client installation.
- Learn the following information: the server name, user name, password, and extension number. This information must be available before the first-time use of the Mitel Connect client application.
- Microsoft Outlook must be configured in Corporate or Workgroup mode for Microsoft Outlook Integration to function properly. Internet Only mode is not supported.
- Users should be informed of which Mitel Connect client application they will be using.
- Close all applications before starting the software installation.
- With the Silent Client Install feature, the client software upgrade process on remote machines do not require administrative rights by the person installing or upgrading software on client machines. Administrators can upgrade the software on all client machines using Active Directory Group Policies regardless of the permissions associated with those machines or the users who log into those machines.
- Many of the changes are reliant on Microsoft Active Directory. Microsoft Outlook must be configured in **Corporate or Workgroup** mode for Outlook integration to function properly. **Internet Only** mode is not supported.

17.2.1 .NET Installation

On Windows-based computers, Mitel Connect client requires the installation of .NET Framework version 4.6 or higher. The Mitel Connect client installer automatically downloads the correct .NET Framework version if it is not present during the upgrade or install. Users are then prompted to accept the End User License Agreement from Microsoft to proceed with the .NET installation. Internet connectivity is required during the installation process.

Installing Mitel Connect client for Windows on a 64-bit platform places files in the default location: `C:\Program Files(x86)`. The default location for 32-bit client dll files is `C:\Windows\SysWow64`.

17.3 Methods of Installation

This section describes the two ways in which the software can be installed on your computer.

- Silent Client Install
- Standard Integrated Software Distribution

17.3.1 Silent Client Install

The Silent Client install allows the Mitel Connect client software to be installed or upgraded on a client machine from a remote machines without the need for administrative rights. An administrator can easily upgrade the software on all client machines regardless of the permissions associated with those machines or the users who log into those machines.

Many of the changes are reliant on Microsoft Active Directory. The Microsoft Active Directory software handles the following tasks:

- Creating a Group Policy Object to use to distribute the software package
- Assigning a package to a group of computers running Windows 7, Windows 8.1, or Windows 10

- Publishing a package
- Removing a package

You must have the following files from the Client USB flash drive accessible with file permissions set to Share and File level Access by group <everyone>:

- `Data1.cab`
- `Setup.exe`
- `Mitel Connect.msi`

Before installing the client, ensure that Microsoft Visual C++ Redistributable 2015 is installed.

Enabling the new Remote Client Upgrade functionality requires performing a number of tasks using Microsoft Active Directory. For information on performing those tasks, refer to the following Microsoft Reference article:

- How To Use Group Policy to Remotely Install Software in Windows Server 2008 and Windows Server 2003, Microsoft Article ID 816102

Mitel recommends selecting the **Prevent users from initiating client upgrades** check box on the Other System Parameters page in Connect Director. For details about other parameters, refer to the *MiVoice Connect System Administration Guide*.

17.3.1.1 Installation in Large Deployment that Uses AD

Some unique requirements exist for the installation of Mitel Connect client in a large deployment that uses Active Directory. This section outlines both the manual and the automated installation of Mitel Connect client in a large site with Active Directory. The decision for how to proceed depends on the following key factors:

- Whether manual (local) or remote installation is used
- Presence on the server of .NET Framework version 4.6 or higher
- Access to the World Wide Web (if .NET Framework is not on the server)

The version of .NET Framework that is used should be the 64-bit version for a 64-bit server.

17.3.1.1.1 Manual Installation

The ability to install the software manually depends on the availability of .Net Framework 4.6 or higher. If the `Prerequisites` folder contains .Net Framework 4.6 or higher and other correct files, the system administrator can run `setup.exe` while the system is disconnected from the Internet. If the `Prerequisites` folder does not contain .Net Framework 4.6 or higher, the system must have Internet connectivity because, when the system administrator runs `setup.exe`, the system automatically downloads .Net Framework 4.6 or higher.

17.3.1.1.2 Automated Installation

To use the Mitel Connect client in a large-scale deployment that includes Active Directory, the remedy is for system administrators to install individual items in the order listed below. The administrator must push the following packages in the order shown through GPO or any other deployment tool:

1. Microsoft .Net Framework 4.6 or higher (not located in the `Prerequisites` folder). Either .Net Framework exists on the system or the system must be connected to the Web (so that initiation of `setup.exe` causes a download of .Net Framework).
2. Interop Assemblies (in the Prerequisites folder) should contain Primary Interop Assemblies for 2007 and Visual Studio Tools for Office (VSTO). This resides in the `Prerequisites` folder.
3. Mitel Connect client located in the Setup folder.

17.3.2 Standard Integrated Software Distribution

To simplify installation, the MiVoice Connect system provides an integrated software distribution feature. Using Connect Director, the system administrator can send an e-mail message to each user configured with an e-mail address.

You can send all users, some users, or just one user an e-mail message using the following procedure:

1. Launch Connect Director.
2. Click **Administration** > **Features** > **Client** > **Notify Users**. The **Notify Users** page is displayed.

MiVoice Connect's integrated software distribution feature simplifies installation. Although the process presents a number of screens, there is a default installation that requires no input; you click through the screens until the installation completes.

Users receive an e-mail message from the MiVoice Connect system containing the information they need to install the Mitel Connect client application. The installation program is accessed using the URL listed in the e-mail notification. Notice that the e-mail notification includes the server name and the user name: Users will need this information when they start the Mitel Connect client application for the first time. The software can also be installed from the Mitel Connect client CD.

For the procedures and related requirements on installing the Mitel Connect client, see the *Mitel Connect Client User Guide*.

17.4 Configuring Instant Messaging

To configure the instant messaging feature for users of Mitel Connect client, use the following procedures:

- Enabling Instant Messaging for the Mitel Connect client
- Enabling Class of Service for Instant Messaging
- Enabling Instant Messaging for a User

17.4.1 Enabling Instant Messaging for Mitel Connect Client

1. Launch Connect Director.
2. Click **Administration** > **System** > **Other System Parameters**. The **Other System Parameters** page is displayed.
3. Enter the following information in the Instant Messaging section:

   a. In the **Domain Name** field, enter the domain name used for your organization.
   b. In the **Sessions Timeout** field, enter the duration, in minutes, that you want the system to keep an IM session open without an exchange before timing out. You can enter a range between 10 and 600 minutes.
   c. Select the **Enable Offline Messaging** option if you want to allow users to leave off line messages for their contacts.
   d. If you are using an SSL certificate, select the **Enable TLS** option to allow users to encrypt IM messages using Transport Layer Security (TLS) protocol.
   e. Enter the number of days you want the Mitel Connect client to retain the history in the **Client History Retention Period** field. You can select a range between 0 and 549 days. If you want the retention period to not have a limit, select the **Unlimited** box.
4. Click **Save** at the bottom right corner of the page.

Instant messaging has been successfully enabled on the Mitel Connect client.

17.4.2 Enabling Instant Messaging for a Class of Service

1. Launch Connect Director.
2. Click **Administration** > **Users** > **Class of Service** > **Telephony Features Permissions**.

   The following different classes of service are displayed for telephony:

   - Fully Featured
   - Minimally Featured
   - Partially Featured
3. Select the feature class on the list pane for which you want to enable instant messaging services.

   The details pane displays more information about the selected class.
4. On the **IM Presence Invitation Handling** drop-down list, select one of the following options:

   - **User defined:** Allows the user to choose the method of handling IM invitations.
   - **Auto accept invitation:** Forces IM invitations to be accepted automatically. The invitee must still invite the inviter.
   - **Prompt to accept invitation:** User is prompted when a new invitation is issued.
5. Click **Save**.

Instant messaging has been successfully enabled for the selected class of service.

17.4.3 Migrating Instant Messaging Users to a Service Appliance

1. Launch Connect Director.
2. Click **Administration** > **Users** > **Users**. The **Users** page is displayed.
3. Select the user on the list pane for whom you want to enable the service.

   The user details are displayed on the details pane.
4. Click the **Applications** tab.
5. In the **Instant Messaging Server / Appliance** section, select the service appliance you want to be associated with the user for instant messaging.
6. Click **Save**.

The selected service appliance replaces the MiVoice Connect server that is used for handling instant messages sent and received by the user.

You should notify the user to uninstall and reinstall Outlook calendar integration in Mitel Connect client for Windows if they are using Outlook calendar integration. See the *Mitel Connect Client User Guide* for instructions about how to configure Outlook calendar integration.

17.5 Upgrading MiVoice Connect Software

When the MiVoice Connect system is upgraded, users running older versions of Mitel Connect client may be informed that they must upgrade. Upgrades of the system might not require client upgrades. Refer to the Support web site (https://www.mitel.com/support) to determine if a system upgrade requires client modifications.

17.6 User Licensing

Mitel offers three user license types:

- Extension and mailbox
- Extension-only
- Mailbox-only

These new choices allow users to request a phone extension license without having to purchase a mailbox at the same time. This additional flexibility may be helpful in situations where a fax machine, a modem, or a lobby phone is desired and a mailbox for voice mail was not needed. Similarly, users can purchase a mailbox without having to purchase a phone extension.

Earlier releases of the MiVoice Connect product offered Single Site and Multi-Site Enterprise license keys. In this release, the Single Site key is no longer available. For existing users, the Single Site key can still be used and will be renamed as a **Single Site Extension and Mailbox** license. Previous Multi-Site Enterprise keys become **Extension and Mailbox** licenses.

17.6.1 Purchasing User Licenses

Each user must be configured with one of those three license types. A license must be purchased for each user, based upon the needs of that user. To see if an installation is in compliance with the number of licenses purchased, all Extension-Only, Mailbox-Only, and Mailbox-and-Extension users are counted and compared against the sum of the licenses purchased.

- Extension and mailbox: Purchase of this license entitles the user to be assigned to both a physical extension and a mailbox.
- Extension-only: Purchase of this license entitles the user to be assigned to a physical extension, either via explicit assignment or via Extension Assignment.
- Mailbox-only: Purchase of this license allows the user to be assigned to a voice mail-box.

17.6.2 Language Licenses

MiVoice Connect supports multiple languages in addition to US English (which will remain the default language for new installations). One or more languages can be running at a site by purchasing a language license.

If only one language is needed at a single site, there is no need to purchase a language license.

For instructions on configuring the User Licenses or Language Licenses through Connect Director, see the *MiVoice Connect System Administration Guide*.

17.6.3 License Control

License Control adds enforcement and branding to the MiVoice Connect product and provides tighter enforcement (via MAC address-based node locking) on existing licensing. When an existing MiVoice Connect system is upgraded to the current software release, an enforcement scheme requires entry of a system key.

When launching Connect Director, you are asked to enter either a Small Business Edition (SBE) or Enterprise Edition (EE) key (see below for details on the differences between these two). You can request a key online via Director. If an invalid key is entered or if the field is left empty, you will be allowed to log into the system for 45 days.

If no action is taken within the 45-day grace period, Connect Director will be locked and you will be unable to make any configuration changes to the system (although the phones will continue to work).

This 45-day period allows for unplanned, ad hoc changes that may cause you to exceed license limits while providing time to comply with the license requirements by either removing unneeded configurations or by ordering additional licenses.

You will be forced to purchase one of two keys available:

- SBE 100 key – required for Small Business Edition 100
    - This key is for smaller systems under 100 users and 5 sites.
    - Use of this key results in the display of SBE 100 branding (on the initial login page above the navigation pane).
    - The SBE 100 license allows a maximum of 100 users with an extension and mailbox, and the customer can add up to 20 users who have only a mailbox.

      For an SBE system, the following features are not available:

        - AMIS
        - SMDI
        - On-net Dialing
        - Distributed Database, workgroups, account codes
        - SBE does not support integration with another MiVoice Connect system or any third-party PBX.
        - TSP
- EE key – required for Enterprise Edition
    - This is for larger businesses with more than three sites.
    - The existing branding appears.
    - System behaves as it does today, except that number of sites is enforced via nagging.
    - Block adding an additional SBE or EE key

For instructions on configuring licenses in Connect Director or for information about Keyed and Self-Audited licenses, see the *MiVoice Connect System Administration Guide*.

Integration with External Applications 18

This chapter contains the following sections:

To work with some external applications, the MiVoice Connect system may require additional set-up after system installation. This chapter identifies and describes how to set up the system to integrate with external applications.

18.1 Overview

Using the ImportContacts.bat utility, you can import public contacts from the Public Folder on a Microsoft Exchange Server and upload them into the System Directory in Connect Director for use by MiVoice Connect system users. Before running the utility, you must configure the settings for the batch file in a configuration file (`ImportContactsconfig`). When run, the batch utility performs the following procedures:

- Connects to your Microsoft Exchange Server (2013) through the Exchange Web Services.
- Reads the contacts in the Exchange Public Folder.
- Copies the contacts into a comma-separated value (CSV) file. Be aware that the batch utility provides an option to ignore fields during CSV-file generation.
- Invokes the DBImport tool (dbimport.exe), which uses the contents of the CSV file to update the MySQL user database. The tool adds, deletes, and modifies user account records based on the contents of the CSV file.

The imported and uploaded contacts are displayed in endpoints that can access the MiVoice Connect System Directory, such as Outlook, telephones, and Mitel Connect client. MiVoice Connect system users can dial the numbers of the imported and uploaded contacts, create buddies, and so on.

18.1.1 Important Considerations

When you upload public contacts from a Microsoft Exchange Server, be aware of the following considerations:

- Client hardware memory requirements can change if public contacts are imported and uploaded: Memory requirements can increase in relation to the number of contacts imported and uploaded.
- Contacts imported from a Microsoft Exchange Server and uploaded to the MiVoice Connect System Directory are never private and are fully visible in the Mitel Connect client.

18.2 Uploading Public Contacts

Running the ImportContacts.bat utility updates the MiVoice Connect System Directory as follows:

- Contacts added to the Public Folder on a Microsoft Exchange Server are added to the MiVoice Connect System Directory.
- Contacts modified in the Public Folder on a Microsoft Exchange Server are modified in the MiVoice Connect System Directory.
- Contacts deleted from the Public Folder on a Microsoft Exchange Server are deleted from the MiVoice Connect System Directory.

To limit exposure, contacts imported from the Public Folder on a Microsoft Exchange Server and uploaded into the MiVoice Connect System Directory can be deleted from the System Directory using Connect Director. See the MiVoice Connect System Administration Guide for information on using Connect Director to manage the System Directory, including adding and deleting records.

Note: Contacts that you delete from the System Directory by using Connect Director are deleted only from the System Directory; they are not deleted from the Public Folder on a Microsoft Exchange Server

Contacts in the Public Folder can be imported and uploaded at any time, but it is usually best to run the batch utility during off-peak system hours.

You can also import and upload contacts by using the Windows Task Scheduler. For more information, see Using the Windows Task Scheduler to Upload Public Contacts on page 292.

18.2.1 Prerequisites

To upload public contacts, you system must comply with the following prerequisites:

- Your system must be running Microsoft Exchange Server 2013.
- Your Microsoft Exchange Server must contain Public Folders.
- You must be familiar with Exchange server concepts and terminology and be proficient at managing an Exchange server. This document is not a tutorial on Exchange servers. For complete information on installing, configuring, and managing Exchange servers, see the Microsoft web site (http://www.microsoft.com/exchange).
- You must have System Administrator permissions to perform the following tasks:
  - Read Public Contacts from a Microsoft Exchange Server.
  - Edit the Import Contacts Configuration file.
  - Run the Public Contacts Windows Batch file.

18.2.2 Editing the Import Contacts Configuration File

Note:

To perform this procedure, you must have system administrator permissions.

To edit the import contacts configuration file on the Headquarters server, follow this procedure:

1. Open a Command Prompt window (on your Headquarters server).
2. CD to the location of the Import Contacts Configuration file as follows:

```
C:\Program Files (x86)\Shoreline Communications\Shoreware Server
\ImportContacts\ImportContactsconfig
```

3. Open the Import Contacts Configuration file.
4. Modify the parameters. (The parameters are listed and described in the table below)
5. Save and close the Import Contacts Configuration file.

Table 46: Import Contacts Configuration File Parameters

Parameter	Definition
Version	Exchange server version (0 or 1). • 0 = Exchange server 2010. • 1 = Exchange server 2013.
UserName	Your Exchange user name. Required only if you are not using Network Credentials.
Password	Your Exchange password. Required only if you are not using Network Credentials.
Domain	Name of your Exchange domain. Required only if you are not using Network Credentials.
EWSUrl	Exchange Web Service location. For example, https://10.XX.XXX.XX/EWS/exchange.asmx.
PF	Path to your company's Public Folder.

Parameter	Definition
	Location where your company's public contacts are stored. ("Testfolder"" and "Testcontact" are placeholders in the example.)
OptionalColumns	Specifies information that is not imported and uploaded. For example, the home address or height of a contact.
LogFile	Specifies the log file name. The default location is `C:\Program Files (x86)\Shoreline Communications\ShoreWare Server\ImportContacts`.
CSVFile	Specifies the CSV file name that is generated. The default location is `C:\Program Files (x86)\Shoreline Communications\ShoreWare Server\ImportContacts`.

18.2.3 Running the Import Public Contacts Windows Batch File

Note:

To perform this procedure, you must have system administrator permissions.

To run the Import Public Contacts Windows batch file, follow these steps:

1. Open a Command Prompt window (on your Headquarters server).
2. CD to the location of the Import Public Contacts Windows Batch File:

   ```
   C:\Program Files (x86)\Shoreline Communications\Shoreware Server
   \ImportContacts\
   ```

   The location of the file is shown in Import Public Contacts Windows Batch File Location.
3. Run the Import Public Contacts Windows Batch File. The status of the procedure is shown in the example in Example Import Public Contacts Windows Batch File Status. The contacts are imported from

the Public Folder on your Microsoft Exchange Server and uploaded to the MiVoice Connect System Directory for use by MiVoice Connect system users.

Figure 25: Import Public Contacts Windows Batch File Location

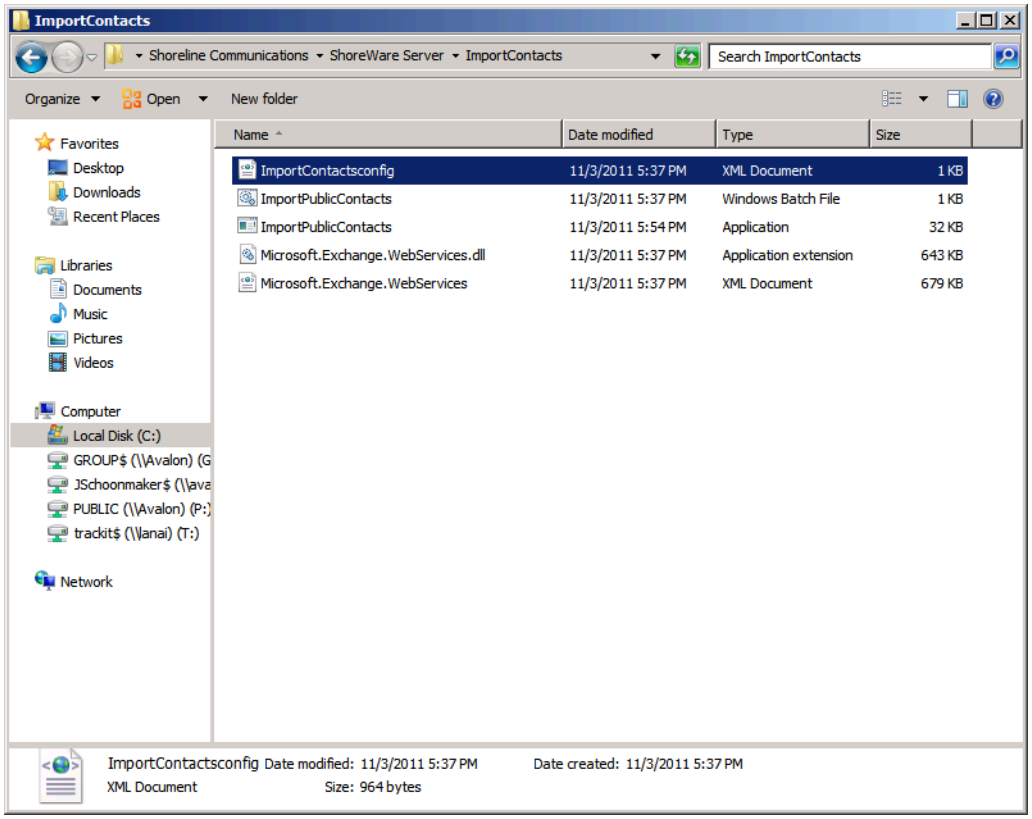
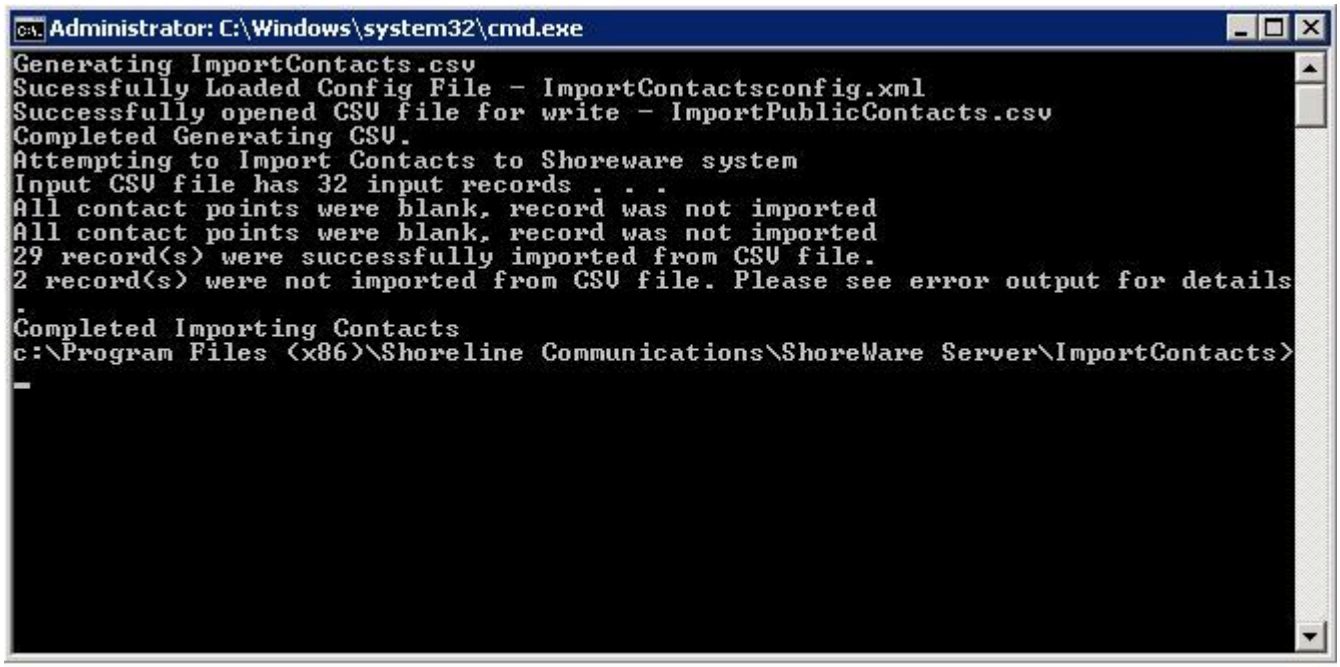


Figure 26: Example Import Public Contacts Windows Batch File Status



18.2.4 Verifying that Public Contacts Are Uploaded

Note:

To perform this procedure, you must have system administrator permissions

To run the Import Public Contacts Windows batch file, follow these steps:

1. Open Connect Director.
2. Under **Administration**, click **System Directory**.

   The **System Directory** window appears, which displays the imported and uploaded contacts. If the Public Contacts are not displayed in the System Directory, they were not imported and uploaded.
3. To check for errors in the import and upload process, open and view a Log File (DBImport.err) on your Headquarters server.

   ```
   C:\Program Files (x86)\Shoreline Communications\Shoreware Server
   \ImportContacts\DBImport.err
   ```

18.2.5 Using the Windows Task Scheduler to Upload Public Contacts

Note:
To perform this procedure, you must have system administrator permissions.

Using the Windows Task Scheduler, you can also import public contacts from the Public Folder on a Microsoft Exchange Server and upload them into the System Directory in Connect Director.

The Task Scheduler enables you to automatically run the Import Public Contacts Batch File on your Headquarters Server.

The Task Scheduler wizard opens the Import Public Contacts Batch File according to the schedule you choose. The tasks can be scheduled to execute at a specific time on a daily, weekly, or monthly schedule.

For more information on how to use the Task Scheduler on your Windows Server, see the Microsoft Corporation website.

18.3 Installing the Telephony Interface

The system installation wizard does not automatically install the ST Telephony Interface (STI) during installation.

If you are using third-party or supplementary applications that interact with the MiVoice Connect system, you may need to manually install the STI.

This section describes how to install the STI on Windows clients with third-party applications that integrate with Mitel Connect client for Windows.

18.3.1 Prerequisites

Before you install the STI, perform the following prerequisite steps:

- Close all open programs, because a reboot will be required during the installation process.
- Ensure that the Mitel Connect client for Windows is installed, and log into the client to enable the required configuration settings.
- Ensure you know the location of MiVoice Connect system software on your system.

18.3.2 Installing the STI

1. If it is not already installed, install (or upgrade) Mitel Connect client for Windows.
2. Launch Windows Explorer.
3. Enter the following URL:

   http://serverIP/shorewareresources/shoreteltelephonyinterface

   The ST Telephony Interface Install site appears.
4. Click the link to install the ST Telephony Interface, and then download and install the interface on the client computer.

> **Note**:
>
> If you are running Windows 7 64 bit with UAC turned on, ensure to download the installer, right click and select **Run as Administrator** to properly install the TAPI provider

5. Reboot the client computer.

18.3.3 Verifying that the Interface Is Installed

1. Open Control Panel.

2. Click **Phone and Modem** Options.
3. Click **Advanced**.
4. Verify that Remote TAPI Service Provider is installed.
5. Select **Remote TAPI Service Provider**.
6. Click **Configure**. The **Remote TSP** dialog appears.
7. In **Provider Usage**, verify that the provider is enabled.
8. Launch Mitel Connect client for Windows.

The TAPI service registers the ID, password, and address of the user for transactions with the third-party application.

18.4 Installing the TSP Package

You must install the Telephony Service Provider (TSP) package on clients that require TAPI for third-party applications (for example, Professional Service applications).

There are three ways to install the third-party TSP package on client operating systems for third-party applications:

- Running setup
- Using the Microsoft GPO Deployment tool
- Using the Professional Services application

The installation procedure for each method is described in the following sections.

18.4.1 Running Setup

1. Navigate to `http(s)://<server name>/ShorewareResources/ShoretelTelephonyInterface` where <server name> is the FQDN or IP address of your headquarters server.
2. Download and install the third-party TSP package.
3. Follow the default settings and finish the installation.
4. Reboot the client machine.

This user can now run third-party applications that use TAPI.

18.4.2 Using the Microsoft GPO Deployment Tool

Using GPO, install (push) the TSP package to larger sites. GPO is Microsoft Corporation's Group Policy Object (GPO) deployment tool. For more information about GPO, see the Microsoft support website, http://support.microsoft.com, and search for GPO.

18.4.3 Using Advanced Applications

When a user runs an advanced application that needs the TSP, the user will be prompted to download and install the TSP.

18.4.4 Installing Third-Party TSP Package in Terminal Licensing Server

To Install third-party TSP Package in a Terminal Licensing Server Environment (Windows):

1. Navigate to `http(s)://<server name>/ShorewareResources/ShoretelTelephonyInterface` where <server name> is the FQDN or IP address of your headquarters server.
2. Download and install the third-party TSP package.
3. On the Windows desktop, open the Control Panel.
4. Click **Phone and Modem**.
5. Click **My Location**.
6. Click **Advanced**.
7. Select **Remote TAPI Service Provider**.
8. Click **Remove**.
9. Click **OK**.
10. On the Windows desktop, open a command prompt window.
11. Navigate to the following location:

    ```
    \Program Files\ShoreTel\ShoreTel 3rd Party
    ```

12. Run the following command:

    ```
    TSPinstall -i StServer HQ servername (IP address)
    ```

13. On the Windows desktop, open the Control Panel.
14. Click Phone and **Modem** > **My Location** > **Advanced**.

Verify that the Remote TAPI Service Provider is listed.

Mitel Connect client can now use third-party applications.

18.4.4.1 Configure the TSP Credentials

The TSP installer launches a credentials configuration utility to gather the appropriate user credentials, and then to populate system registry values with the information gathered.

1. In the TSP configuration utility, verify or change the following information:

   - **Username**
   - **Password**
   - **Server name**

   The TSP configuration utility launches with the Username and Server name set to current registry values.

   For local users, the credentials entered are the client username and password. For active directory users, the credentials entered can be the domain username, client email, or client username along with the password. This client information is defined for the user in the Connect Director **Administration** > **Users** > **Users page**.
2. Click **Save** to authenticate the user, update the registry keys, and restart the system.

If the authentication fails, the TSP configuration utility will display error messages to describe the point of failure.

Legacy Integration 19

This chapter contains the following sections:

Mitel provides a way to convert a TDM-based voice network into the MiVoice Connect system. Integrating the MiVoice Connect system with an old PBX allows a customer with different systems to support phone and voice mail communication between systems. This chapter describes how to migrate your legacy system to the MiVoice Connect system.

19.1 Overview

An integrated voice network can provide the following streamlining for your system:

- Simplify communications for your users with an enterprise-wide coordinated dialing plan using extension dialing.
- Exchange voice mail messages between users on different sites using different voice mail systems. Standard commands such as compose, forward, and replay, extend the value of your different voice mail systems.
- Consolidate trunks with different traffic types.
- Reduce service costs by redirecting inter-site calls across your IP network.

19.2 Legacy PBX

A digital trunk tie line integrates the MiVoice Connect system with a legacy PBX. The connection is between the legacy system's PRI interface and the PRI interface of a voice switch located anywhere in your IP network.

There are four different types of activities that occur on the interface:

- Calls from MiVoice Connect users or applications to an extension located on the other system are routed across the tie trunk. When a call is placed, the trunk is accessed and the MiVoice Connect system sends the configured number of digits to the PBX identifying the called extension.
- Calls from users on the legacy system or from trunks, or other applications on the legacy PBX, are routed across this interface. When the legacy user places their call, the legacy system accesses the trunk and then sends the digits as DNIS.
- Outbound calls from users or applications on the MiVoice Connect system can be routed across the trunk to the legacy PBX. When a call is placed, the trunk access code or trunk configuration of the connection to the legacy PBX indicates the outbound call is to be placed to the PBX.
- Calls between the MiVoice Connect and legacy system's voice mail applications are carried across the trunk connecting the two systems. The voice mail systems make calls to configured destinations on the other system to send voice mail messages to users on the other system.

A tie trunk is not required to enable voice mail or AMIS integration. The two voice mail systems can communicate by dialing each other via the PSTN. In general, when a tie trunk is in place, AMIS calls should be routed via the trunk to reduce PSTN costs.

The connection between the two systems can be provided by either SGT1 trunks, PRI, or SIP interface. Mitel recommends that you use PRI or SIP to enable calling number information exchanges between the two systems.

19.3 Coordinated Dialing

Coordinated dialing allows users to dial between the systems using extension-to-extension dialing as well as enabling consolidation of inbound and outbound services. To effectively plan the integration, consider the following items:

- Expected call traffic between the two systems to provide sufficient trunking
- Current numbers of extensions and extension lengths at both systems
- Service plans to determine which PSTN services are provided at each voice system
- What type of legacy PBX equipment is integrated with the MiVoice Connect system

19.4 Trunk Requirements

The number of digital trunks required between the MiVoice Connect system and the legacy PBX depends on the expected traffic between the two systems. To determine the number of trunks, you need to estimate the number of calls per hour that are placed between the two systems. When estimating the call volume between the two systems, consider the following:

- The volume of direct calls between users on the two systems
- Traffic related to Automated Call Distributor (ADC) calls
- Outbound call volume (when outbound trunking to the PSTN is provided by one of the systems for all users, such as a PSTN trunk connected to the legacy PBX that provides long distance services for users on both the legacy and MiVoice Connect system)
- Inbound call volume (when inbound services are provided by one system to all users)

Additionally, you can rely on the estimated calls-per-hour number to determine the number of trunks to configure between the two systems.

For more information on trunk requirements, see Reviewing and Selecting Trunk Types on page 78.

19.5 Coordinated Dialing Plan

With legacy integration, users on both systems can dial one another using abbreviated or extension dialing. This includes dialing from applications on the systems, such as the MiVoice Connect voice mail application, and would also include forwarding a call to an assistant at an extension on the legacy PBX. To determine the coordinated dialing plan configuration, you must identify the current numbering of users on both systems:

- When the systems are located together, extensions can normally be assigned from a single numbering plan, or from a single DID number range provided by the local carrier. In this case, the extensions on the two systems are assigned such that there is no overlap using the desired extension length.
- When systems are at different locations, each system's numbering plan is often based on the DID range supplied by the local telephone company. In this case, overlap of the extension ranges can occur at the currently used extension length.

For example, consider the following situation:

- One location is assigned DID range 408-555-2000 through 2999
- The second location is assigned range 650-333-2500 through 2799
- The systems currently use four-digit dialing matching the trailing 4 digits of the DID numbers.

In this case, there are users on both systems currently assigned extension 2500. To provide a coordinated dialing plan across the systems, the extensions must be adjusted to make them unique system-wide. In the integration, four-digit extensions that overlap are made unique by increasing the extension length across the system. When the extension length is increased, the first digit becomes the "system" number and the remaining digits are the "extension." In the above example, the extension length would be increased to five-digit dialing, and at the first location would be extensions 52000 through 52999, while users at the second location would be assigned extensions 32500 through 32799.

The extensions on all systems that are integrated together should be configured to be the same length.

Ensure to document the planned integrated dialing plan prior to configuring the systems to streamline the configuration process. Information to take note of is provided in Dial Plan Template.

Table 47: Dial Plan Template

	System One	System Two
Location		
DID Range		

	System One	System Two
Local Extensions(Prefix + Number)		
Remote Extensions(Prefix + Number)		

19.6 PSTN Services

The number of trunks, your integration plan, and the overall System_Design includes the provisioning of services across the network. PSTN services can be provided at both systems in the integration or consolidated together on one system.

19.7 Multi-Site Integration

When the systems are located at different sites, both systems should have local trunking for both inbound and outbound calls. Local inbound numbers make it easy for nearby customers to reach you, while local outbound trunks allow you to save on telephone charges by using local services at the site.

In this configuration, the trunk lines connecting the systems are used for the inter-site calling between extensions or applications on the two systems. The interfaces on the two systems are configured to dial out to the remote or off-system extensions, and to accept incoming calls using DNIS.

The voice switch that connects to the legacy PBX should be located at the site with the legacy PBX. This leverages the IP network to extend the calls to the other sites with the MiVoice Connect system.

19.8 Single Site Integration

When the systems are located at the same site, it is not required that both systems be connected to the PSTN. The systems can be configured to best match your requirements.

In a single site configuration, the PSTN connections for inbound calls can be connected to each system. In this environment, the trunks connecting the two systems are configured to dial out the remote or off-system extensions and to accept incoming calls using DNIS.

Alternatively, inbound services can be consolidated on either the MiVoice Connect system or the legacy PBX. In this environment, calls to users on the other systems are forwarded to the remote or off-system extensions through the trunk lines connecting the systems.

When all inbound trunks are consolidated on the MiVoice Connect system, the trunks are configured to support off-system extensions within the range of extensions on the other PBX.

When all inbound trunks are configured on the legacy PBX, the trunks on the MiVoice Connect system are configured to support inbound services with call routing to the extensions on the MiVoice Connect system.

When DID numbers are already in place on one of the PBX's which will be connected, Mitel recommends that the inbound DID service not be moved or split between the systems but configured to remain on the system where they are currently configured and have calls to users on the other system forward across the connecting trunks.

In the single site configuration, Mitel recommends that services for outbound calls be connected to the legacy PBX. In this configuration the trunk interfaces on the system are configured to support outbound local and long distance dialing while the interface on the PBX is configured to route the received outbound calls.

19.9 Consolidated Long Distance

Long distance calls can be consolidated into a single PSTN interface across both the MiVoice Connect system and the integrated legacy PBX. In this configuration, you gain the benefits of reduced long distance rates by consolidating all your enterprise's long distance calls into a single carrier. When it is required, the outbound long distance trunks are connected to the legacy PBX and the MiVoice Connect system is configured to route long distance calls outbound across the digital trunk connecting the systems.

19.10 Voice Mail Integration

The primary issue with voice mail integration is they are often proprietary and the interfaces defined to connect the same and disparate systems are very old, complex and difficult to implement. In fact, many voice systems from the same vendor are not connected. The interface with which most customers are familiar is AMIS. This is an analog interface that has been around for a long time, but is a real challenge to implement and can be very expensive from legacy voice mail providers. It is not uncommon to pay $10,000 per site for this capability. Another widely-used interface, Simplified Message Desk Interface (SMDI), was developed in the days when the PBX and voice mail systems were separate systems. It operates on a serial link between a PBX and voice mail system and allows them to work together. Mitel supports both AMIS and SMDI protocols for voice mail integration.

19.10.1 AMIS Protocol Support

The MiVoice Connect system sends and receives voice mail messages to and from legacy voice mail systems using AMIS protocol Version 1 - Specification February 1992. To send voice mail messages to remote AMIS sites, MiVoice Connect dials the access phone number for the remote system. Likewise, to receive voice messages from a remote system, the remote system must know the number to dial into the MiVoice Connect system. To reach the MiVoice Connect system, the remote system must be configured to dial any number that reaches an auto-attendant menu.

AMIS call support is enabled by default. Incoming AMIS voice mail is delivered in the same manner as other voice mail; however, users cannot send replies. To send outbound AMIS voice mail, you must define AMIS System profiles in Connect Director.

MiVoice Connect negotiates the setup, handshaking, and teardown of AMIS system calls. Each voice mail requires a call over the trunk group defined for the AMIS delivery and call-back numbers.

19.10.1.1 Simplifying AMIS Systems and Increasing Usability

- Use the same extension length across your enterprise.
- Use off-system extensions to match remote users' mail boxes with their extension numbers.
- Assign each system a System ID to identify the remote site location

For more information on AMIS systems, see the *MiVoice Connect System Administration Guide*.

19.10.2 SMDI Protocol Support

MiVoice Connect supports the SMDI protocol, enabling seamless integration of MiVoice Connect equipment with legacy phone systems and enabling a smooth migration toward an all-IP telephony solution.

The SMDI protocol evolved at a time when voice mail services and PBX services were provided by separate physical devices. Over the years, manufacturers have managed to offer both PBX and voice mail services within a single device, and the need for SMDI has diminished. However, the protocol can still be useful in situations where newer equipment will be integrated into a network of older devices.

19.10.2.1 How It Works

SMDI enables the separate devices that provide PBX and voice mail services to share information over an out-of-band serial cable connection. The PBX shares information with the voice mail system about incoming calls. The following information is passed to the voice mail system:

- Who the call is from
- Where the call is going (that is, user extension)
- The reason the call is going to voice mail instead of being answered

In response, the voice mail system returns a notification to the PBX that a message was left on the voice mail server. The PBX system then uses this information to alert the user by turning on the message waiting light on his or her phone.

19.10.2.2 Configurations of Integrated Equipment

With SMDI support, there are essentially two possible ways the MiVoice Connect and legacy equipment can be configured:

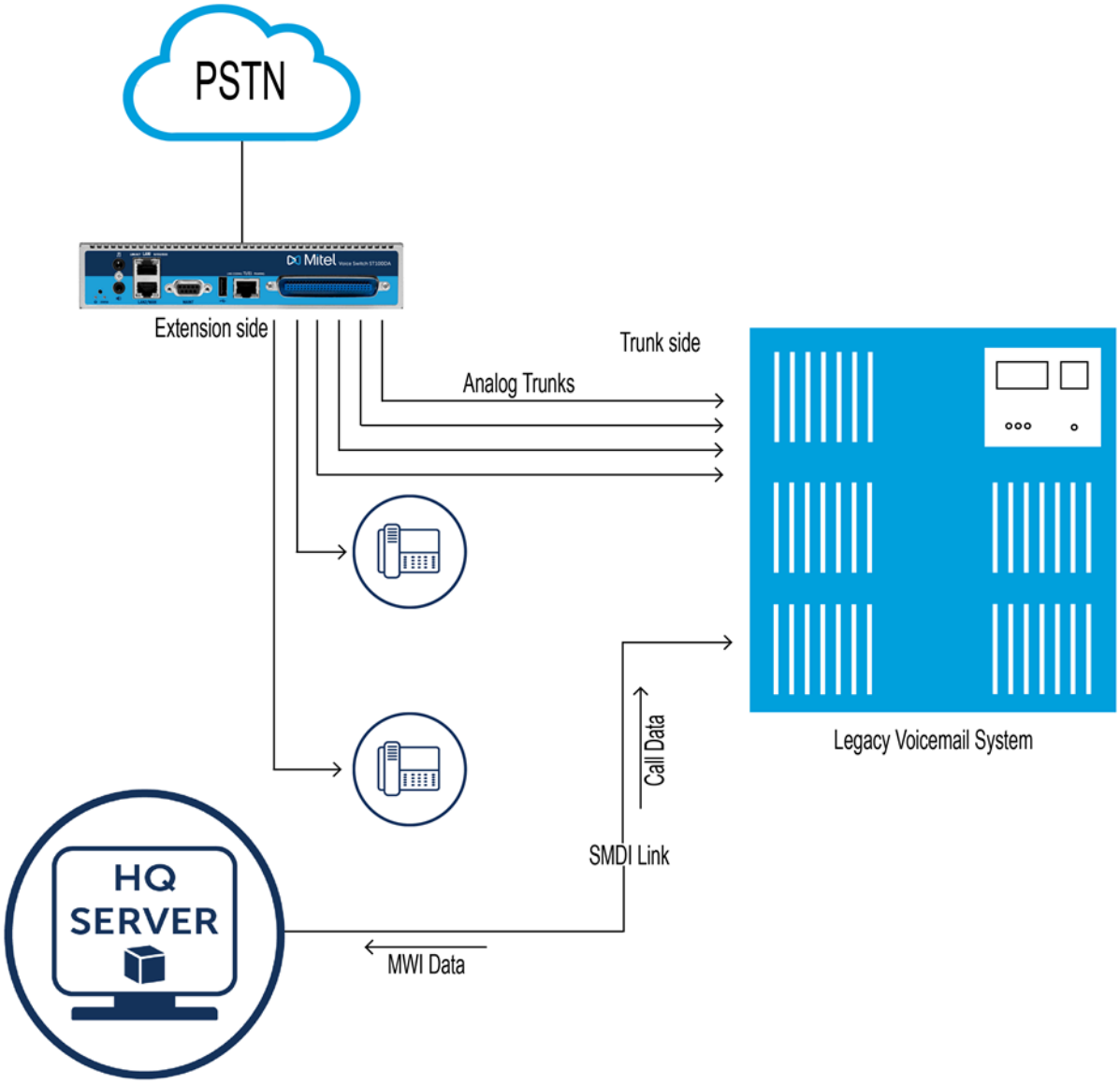
- External Voice Mail Configuration — The legacy system provides voice mail services while the MiVoice Connect system acts as the PBX.
- MiVoice Connect Voice Mail Configuration — The MiVoice Connect system provides voice mail services while the legacy system acts as the PBX.

19.10.2.3 Additional Details

A group of analog trunks from the MiVoice Connect system is used to access the legacy voice mail system. The MiVoice Connect system is on the extension side of the trunks. The MiVoice Connect voice mail application manages the group of outgoing extensions. The MiVoice Connect server can provide digit translations if the legacy voice mail and MiVoice Connect system have different extension lengths.

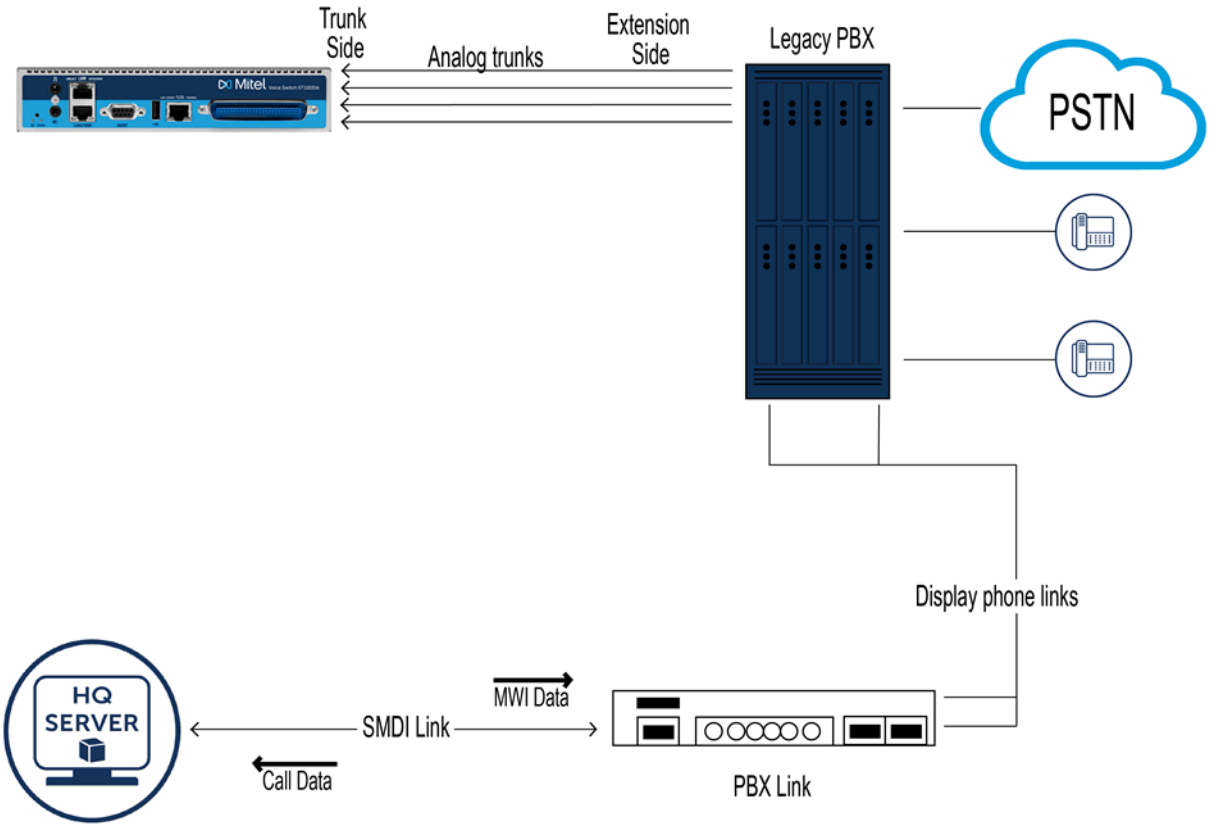
External Voice Mail with MiVoice Connect as PBX shows the MiVoice Connect system providing PBX services and the legacy equipment providing voice mail services.

Figure 27: External Voice Mail with MiVoice Connect as PBX



MiVoice Connect Voice Mail with Legacy PBX shows the legacy system providing PBX services and the MiVoice Connect equipment providing voice mail services.

Figure 28: MiVoice Connect Voice Mail with Legacy PBX



19.10.2.4 Details

- The Figure 28: MiVoice Connect Voice Mail with Legacy PBX on page 304 figure in the Additional Details on page 303 section shows a voice switch connected to a legacy PBX through several analog trunks. These phone lines carry voice information from the PBX to the voice mail server. Signaling information is carried out-of-band on the separate serial line, which is shown near the bottom of the illustration.
- A voice mail server is connected through a serial cable to a PBX link device. The PBX link device provides the basic SMDI services that were not included in some of the older legacy PBX devices. This device must be purchased separately and configured per the manufacturer's instructions.
- The MiVoice Connect server and PBX link exchange information. The PBX link sends call data to the MiVoice Connect voice mail server, and the call data contains information related to the source and destination of the phone call, and provides information about why the call is going to voice mail — user did not answer, line was busy, and so on.
- The MiVoice Connect server, in return, sends MWI (Message Waiting Indicator) information that is used by the legacy PBX to turn on the message-waiting mechanism on a user's phone to let her know she has received a message.

19.10.2.5 Information Transferred through SMDI

The COM port is used to send call information between the MiVoice Connect system and the legacy voice mail system. The SMDI protocol transmits the following call information from the MiVoice Connect system to the legacy system:

- Message desk number: 1-999
- Logical Terminal number (terminal identifier): 1-9999
- Call type (All, Busy, Direct, No Answer, Unknown)
- Called party
- Calling party

The SMDI MWI protocol transmits the following information from the legacy voice mail system to the MiVoice Connect system:

- Message waiting indication control
- Extension
- On/Off indication

19.10.3 Configuring Legacy Voice Mail Integration Using SMDI

As mentioned before, there are two modes of operation with respect to integrating a MiVoice Connect system and a legacy system:

- External Voice Mail Configuration — In this configuration, the legacy system provides voice mail services while the MiVoice Connect system acts as PBX for users.
- MiVoice Connect Voice Mail Configuration — In this configuration, the MiVoice Connect system provides voice mail services while the legacy system acts as a PBX for users.

19.10.3.1 Integrating a Legacy Voice Mail System with MiVoice Connect

To integrate a Legacy Voice Mail System with MiVoice Connect, do the following:

- Configure the server's COM port for SMDI connections to the legacy system.
- Configure interface options from Connect Director.
- Create a user group for users with access to the integration extensions.

19.10.3.2 COM Port Setup

To establish the SMDI link between the MiVoice Connect server and the legacy voice mail system, connect one end of a DB-9 serial cable to the COM port on the MiVoice Connect server and the other end of the cable to a COM port on the legacy voice mail server.

The COM port settings on the MiVoice Connect server must match the settings of the COM port on the legacy voice mail server. Obtain the legacy voice mail COM port settings from the legacy voice mail server's administration guide or from your system integration manager. You need the following information:

- Baud rate
- Data bits
- Parity

- Stop bits
- Flow control

19.10.3.3 Configuring COM Port Communication

1. From the Start menu on the Windows server connected to the legacy voice mail server, select Settings, and then Control Panel.
2. In the Control Panel, open the Computer Management folder.
3. Open the Device Manager.
4. From the right pane in the window, expand the item Ports (COM & LTP).
5. Right-click the COM port used to connect the MiVoice Connect server and legacy voice mail system, and select **Properties** from the menu.

> **Note**:
>
> Contact your server administrator if you need help in determining the correct COM port.

6. In the **Properties** window, enter the settings for the legacy voice mail server COM port.
7. Click **OK** to save the settings.
8. Follow the instructions for configuring the server as described in Configuring MiVC Server for Communication with Legacy Server on page 306.

19.10.3.4 Analog Trunk Port Setup

The MiVoice Connect system sends calls to the legacy voice mail server over analog trunks connecting the two systems. The extensions are on the MiVoice Connect side, and the legacy voice mail system is on the trunk side. The MiVoice Connect system sends calls made to these extensions to the legacy voice mail system when voice mail is needed. Before the call is sent, the SMDI protocol sends information about the call to the legacy voice mail system through the SMDI serial link. This allows the legacy voice mail system to handle the call correctly.

19.10.3.4.1 Configuring the Extensions

- Create a list of the extensions and include the Logical Terminal Number for each extension.
- Configure the extensions with a new dial number (DN) type and marked as private users with no mail box.
- Assign a physical port to each extension in Director. Configure the extensions to forward to the Backup Auto Attendant on no answer or busy.

19.10.3.5 Configuring MiVC Server for Communication with Legacy Server

Follow these steps to set up communication between MiVoice Connect and the legacy voice mail server.

1. Launch Connect Director.
2. Navigate to **Administration** > **Appliances/Servers** > **Platform Equipment**. The **Platform Equipment** page opens.
3. Click the name of the server connected to the legacy voice mail system.

   Details for the server are displayed in the details pane.
4. Select the **Voice Application** tab.
5. In the **Voice mail interface mode** field, from the drop-down list select **External Voice Mail, SMDI**.
6. In the **COM port** field, enter the COM port the server will use for SMDI communications.
7. In the **Message desk number** field, enter the Message Desk number.

> **Note**:
>
> This number identifies a specific voice mail system and must be set to the value the voice mail system expects. In configurations where a number of SMDI links are daisy chained together, this value is used to allow each system to know what data belongs to it. Because most systems use only one SMDI link, this parameter is normally set to **1**.

8. In the **Number of digits** field, enter the extension length. The range is 2-32 digits.

> **Note**:
>
> This value is used to determine how many digits the MiVoice Connect system sends in **SMDI extension** fields. This value needs to be set to the value the voice mail system expects. The most common values are either **7** or **10.** If the system extension length is less than the number of SMDI digits, then the extension number will be padded. For example, if the MiVoice Connect system needs to send extension 456 and the number of SMDI digits is set to **7**, extension 0000456 is sent. If no padding is desired, the number of digits should be set to **2**. In the above example with the number of SMDI digits set to 2 only 456 will be sent.

9. In the **Translation table** field, select a translation table.

> **Note**:
>
> Translation tables are created in Connect Director. If you are using a translation table, ensure the **Use for Call data** and **Use for MWI data** check boxes are selected. For more information on building translation tables, refer to the *MiVoice Connect System Administration Guide*.

10. Click **Save**.

19.10.3.6 Digit Translation

If MiVoice Connect system extensions and legacy voice mail system extensions differ in length, you need to create digit translation tables that map the MiVoice Connect extensions to legacy system extensions. The digit translation tables must be added as a group of named tables from the Voice Mail section of Connect Director. For more information, refer to the *MiVoice Connect System Administration Guide*.

Digit Translation Mapping - 1 shows a digit translation table mapping shorter MiVoice Connect extensions to longer legacy system extensions. For example, MiVoice Connect extensions in the range of 5xx will be in the 65xx range on the PBX, and the original digit, 5, will be replaced by 65.

Table 48: Digit Translation Mapping - 1

Extension Mapping		Digit Translation Table	
MiVoice Connect	Legacy	Original Digits	Replacement Digits
5xx	65xx	5	65
3xx	73xx	3	73
2xx	83xx	2	83

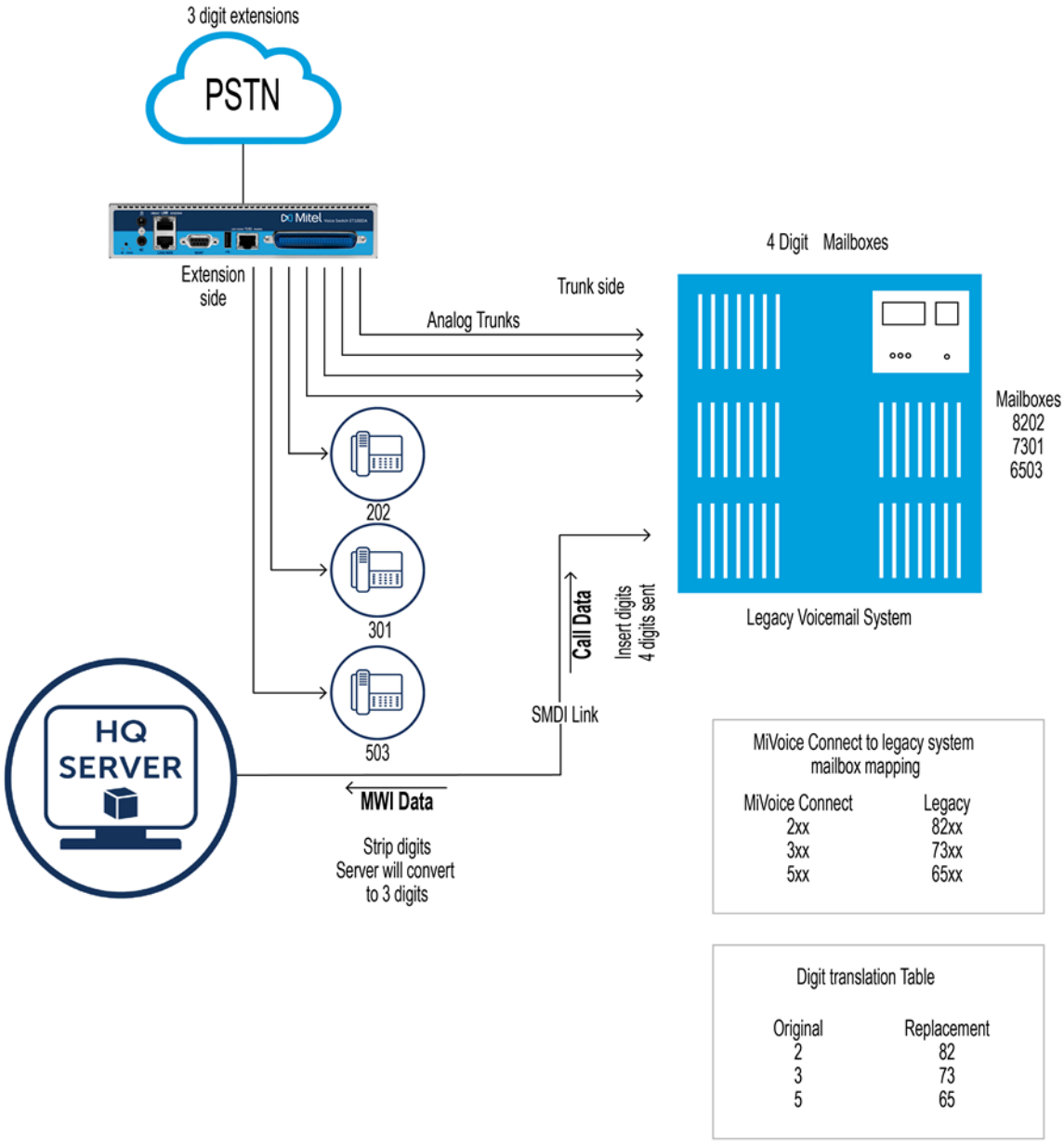
Digit Translation Mapping - 2 shows a digit translation table mapping longer MiVoice Connect extensions to shorter legacy system extensions. For example, MiVoice Connect extensions in the range of 75xx will be in sent to extensions in the 3xx range on the legacy voice mail system, and the original digits, 75, will be replaced by 3.

Table 49: Digit Translation Mapping - 2

Extension Mapping		Digit Translation Table	
MiVoice Connect	Legacy	Original Digits	Replacement Digits
65	5xx	65	5
66xx	6xx	66	6
75xx	3xx	75	3

Mixed Extension Length SMDI Integration illustrates how digit translation functions between the MiVoice Connect server and legacy voice system.

Figure 29: Mixed Extension Length SMDI Integration



19.10.3.6.1 Creating a Digit Translation Table

1. Launch Connect Director.
2. In the navigation pane, click **Administration** > **System** > **Digit Translation Tables**. The **Digit Translation Tables** page is displayed.
3. Click **New**.
4. Enter a name in the **Name** field and click **Add** for each row that you want to add to the digit translation table.

5. In each row, enter a value for the original digit in the **Original** field and a value for the replacement digit in the **Replacement** field.
6. Click **Save**.
7. In the navigation pane, click **Appliances/Servers** > **Platform Equipment**.
8. Click the name of the MiVoice Connect server that will handle the digit translation.
9. Click the **Voice Application** tab.
10. In the **Voice mail interface mode** field, from the drop-down list select **Mitel Voice Mail, SMDI**. Additional fields are displayed on the **Voice Application** tab.
11. In the **Translation table** field, from the drop-down list select the appropriate digit translation table.
12. Enable the **Use for Call data** and **Use for MWI data** options. This allows for the digit translation to occur under the following circumstances:

    - Data about a call is transferred between the legacy and MiVoice Connect systems.
    - Message Waiting Indicator information is transferred between the two systems to notify the legacy PBX that a message was left on the MiVoice Connect voice mail.
13. By default, the Use flash to route calls check box is enabled. Leave this as is. If enabled, calls sent to the MiVoice Connect Auto Attendant from the SMDI trunk group are automatically transferred to the dialed extension using flash. If not selected, calls are routed using other lines.

    The extension length must be the same on each of the systems for the Use flash to route calls feature to work because no translation is applied.
14. Click **Save**.

19.10.3.7 Setting up the User Group in Connect Director

Follow these steps to set up a user group for those users who will have their voice mail redirected to the legacy voice mail system:

1. Launch Connect Director.
2. In the navigation pane, click **Administration** > **Users** > **User Groups**. The **User Groups** page is displayed.
3. Click the name of an existing user group or click **New** to create a new user group. The **General** tab for the selected or new user group is displayed.
4. In the **Voice mail interface mode** field, from the drop-down list select **Mitel Voice Mail, SMDI**.
5. Click **Save**.

19.10.4 Configuring Voice Mail Integration Using SMDI

As mentioned before, there are two modes of operation with respect to integrating a MiVoice Connect system and a legacy system:

- External Voice Mail Configuration — In this configuration, the legacy system provides voice mail services while the MiVoice Connect system acts as PBX for users.
- MiVoice Connect Voice Mail Configuration — In this configuration, the MiVoice Connect system provides voice mail services while the legacy system acts as a PBX for users.

External voice mail configuration is discussed in Configuring Legacy Voice Mail Integration Using SMDI on page 305. The procedure for MiVoice Connect voice mail configuration follows.

MiVoice Connect voice mail configuration consists of the following major tasks:

- Creating a Trunk Group
- Creating Trunks
- Configuring the MiVoice Connect Server for SMDI
- Creating a User Group
- Adding an Individual User
- Configuring the Serial Connection
- Configuring Digit Translation Tables
- PBX link

19.10.4.1 Creating a Trunk Group

One of the first tasks involved in configuring SMDI is to create a trunk group. The trunk group is used to manage the individual trunk lines between the voice switch and the legacy PBX. Instructions for creating the trunk group are provided below. For additional details on setting up trunk groups, see the *MiVoice Connect System Administration Guide*.

Complete the following steps to create a trunk group for SMDI trunks:

1. Launch Connect Director.
2. In the navigation pane, click **Administration** > **Trunks** > **Trunk Groups** > **Trunk Groups**. The **Trunk Groups** page is displayed.
3. Click **New**.
4. Enter the trunk group's name and site in the appropriate fields.
5. In the **Trunk type** field, from the drop-down list select **Analog Loop Start**.
6. Click the **Inbound** tab, and enter a voice mail extension in the **Destination** field to direct inbound calls to the MiVoice Connect Auto Attendant system.
7. Click **Save**.

19.10.4.2 Creating Trunks

After creating the trunk group, the next step is to create one or more trunk lines representing each data connection between the MiVoice Connect voice mail system and the legacy PBX. The lines between the PBX and MiVoice Connect voice mail must be trunk lines, with MiVoice Connect as the trunk side and the legacy PBX as the extension side. For example, calls leaving the PBX for the voice mail system will leave on extensions. The PBX-to-voice mail connection might also be a SGT1 trunk that uses a channel bank to provide extensions to the legacy PBX.

1. Launch Connect Director.
2. In the navigation pane, click **Administration** > **Trunks** > **Trunks**. The **Trunks** page is displayed.
3. Click **New**. The **General** tab is displayed in the details pane.
4. In the **Site** field, select the site name from the drop-down list.
5. In the **Trunk group** field, select the trunk group name from the drop-down list.

6. In the **Number** field, enter the **Logical Terminal Number (LTN)**. This value can range from 1 to 9999. For many systems the extension number of the port is used.

> **Note**:
>
> The LTN identifies the port the PBX will use to send the call to the MiVoice Connect voice mail system. It is very important that the LTN match what the PBX will send. You must check with your PBX vendor to determine what will be sent.

7. Click **Save**.

19.10.4.3 Configuring the MiVoice Connect Server for SMDI

After creating the trunk lines, you will configure the MiVoice Connect voice mail server. Configuration involves setting up the various SMDI parameters:

1. Launch Connect Director.
2. Navigate to **Administration** > **Appliances/Servers** > **Platform Equipment**. The **Platform Equipment** page opens.
3. Click the name of the MiVoice Connect server that will act as the voice mail server for the legacy PBX.

   Details for the server are displayed in the details pane.
4. Select the **Voice Application** tab.
5. In the **Voice mail interface mode** field, from the drop-down list select **Mitel Voice Mail, SMDI**.

   Additional fields are displayed on the Voice Application tab.
6. From the **Trunk group** drop-down list, select the name of the SMDI trunk group that you created earlier.

> **Note**:
>
> This will make the server aware of the name of the trunk group from which it should expect to receive voice mail calls.

7. In the **COM port** field, enter the numerical value, which is between 1 and 10, that corresponds to the serial port of the MiVoice Connect server where you will be connecting the serial port. This serial port will be used to route out-of-band SMDI signaling information between the PBX link device and the MiVoice Connect server.
8. The Message desk number, which has a range of 1-999, is optional and can be set to the default value of **1**. Check with the vendor for this value.

Note:

The Message desk number is used to indicate a specific system in situations where a number of SMDI links have been daisy-chained together. This value allows each system to known which data belongs to it. In most cases this parameter is set to **1**, because only one system will be using the SMDI link.

9. The **Number of Digits** field, which has a range of 2-32, is optional.

Note:

This value determines how many digits the MiVoice Connect system sends in SMDI extension fields. This value needs to be set to the value the voice mail system expects. The most common values are either 7 or 10. If the system extension length is less than the number of SMDI digits, then the extension number will be padded. For example, if the MiVoice Connect system needs to send extension 456 and the number of SMDI digits is set to 7, extension 0000456 will be sent. If no padding is desired the number of digits should be set to 2. In the above example with the number of SMDI digits set to 2 only 456 will be sent.

10. The translation table is optional and can be left as is for now.
11. Click **Save**.

19.10.4.4 Creating a User Group

After setting up the MiVoice Connect voice mail server for SMDI, the next step is to add users to the system. To do this, you first create a user group that specifies that all members will use MiVoice Connect voice mail. After this step is complete, you modify individual users' profiles.

Complete the following steps to create a user group for users on the legacy PBX system:

1. Launch Connect Director.
2. In the navigation pane, click **Administration** > **Users** > **User Groups**. The **User Groups** page is displayed.
3. Click **New**. The **General** tab for the new user group is displayed.
4. In the **Name** field, enter the name of the user group.
5. In the **Voice mail interface mode** field, from the drop-down list select **Mitel Voice Mail, SMDI**.
6. Click **Save**.

19.10.4.5 Adding an Individual User

After creating the user group, you can create user profiles for the legacy PBX users.

1. Launch Connect Director.
2. In the navigation pane, click **Administration** > **Users** > **Users**. The **Users** page is displayed.
3. Click **New**. The **General** tab for the new user is displayed.
4. On the **General** tab, enter a name for the user in the **First name** and **Last name** fields.
5. In the **License type** drop-down list, select **Mailbox-Only**.

> **Note**:
>
> Because the new user is located on the legacy system, the user does not require a MiVoice Connect extension.

6. In the **User Group** drop-down list, select the name of the user group you just created.
7. Click **Save**.

19.10.4.6 Configuring the Serial Connection

The MiVoice Connect voice mail system supports only one serial link per application server. To support another legacy PBX, you will need another Mitel distributed application server. A serial cable, such as a null modem, should be used to connect the legacy PBX to one of the COM ports of the MiVoice Connect server. Note that the MiVoice Connect system will extract the serial port settings, such as baud rate and parity bit values, from the Windows COM port settings. These settings can be verified by following the procedure below:

1. Right-click **My Computer**.
2. Select **Manage**.
3. Select **Device Manager**.
4. Left-click on **Ports (COM & LPT)**.
5. Right-click **Communications Port (COM1)** and select **Properties**.
6. Left-click on the **Port Settings** tab.
7. Verify that the settings match those suggested by the documentation that came with your legacy PBX device.

19.10.4.7 PBX

Table 50: Supported PBXs

Manufacturer	Model
Nortel	Meridian 1 Nortel Norstar

Manufacturer	Model
Avaya	System 75/85 Definity
Mitel	SX50 SX200 SX2000
Siemens	300S
NEC	NEAX

19.10.4.8 PBXLink

A PBXLink device may be needed to provide SMDI services for a legacy PBX that does not offer support for SMDI. The PBXLink devices, manufactured by CTL, provide integration services to allow certain digital PBXs to interface seamlessly with a Voice Messaging System. The PBXLink connects to the PBX using a digital telephone line and to the Voice Messaging System using an RS-232 link. The PBXLink uses information appearing on the emulated digital set to determine the original source and destination of the calls being forwarded to the voice mail system. This information is then communicated to the voice mail system on an RS-232 serial link using the industry standard Centrex SMDI protocol. The PBXLink is compatible with SMDI-compatible voice mail systems.

When using SMDI and MiVoice Connect voice mail configuration, the following features are not supported:

- Extension Assignment
- Setting availability state
- Setting agent state

The following features are supported:

- Recording greeting and name
- Setting TUI password
- Enable/disable envelope information
- Email voice message options
- Find Me
- Message functions including call back
- Message sending functions
- Workgroup
- MiVoice Connect voice mail
- Agents cannot be extensions in the legacy PBX

- System configuration
- Configuration parameters

19.11 System Requirements

The following are required on the MiVoice Connect system, or on the legacy PBX to enable the integration of the two systems:

- MiVoice Connect system
  - Voice switch that supports a SGT1 circuit
- Legacy PBX
  - SGT1 or PRI card for the PBX
  - Available card slot and capacity for the added trunks
  - Required software or licenses to support the desired trunk interface

If PRI is used in the integration interface, the legacy PBX must emulate the CO or support Network Side PRI.

19.12 Connection Cable

Special Considerations - Nortel PBX

When integrating with a Nortel Meridian PBX, a SGT1 connection must be used since the legacy system does not support Network Side PRI.

19.12.1 Special Considerations — Avaya/Lucent PBX

Universal Dial Plan (UDP) Must be Active — This capability enables transparent dialing between the Avaya/Lucent PBX and the MiVoice Connect system. If this is not active, users on the PBX will either have to dial a trunk access code to reach the users on the MiVoice Connect system, or configure forwarding from an extension in the legacy system to the MiVoice Connect extension using the trunk access code and the extension.

In some cases, this feature must be purchased separately from Avaya/Lucent.

19.13 Administration and Configuration

Tie Trunk Configuration

The following summary describes the administration and configuration of the digital trunk for connecting the MiVoice Connect system to the legacy system.

19.13.1 Services Summary

Before starting, a summary of the required configuration should be made based on the required services in the interface.

Table 51: Service Configuration Requirements

Desired Service	Required Configuration
Extension-to-Extension Calling	Enable inbound services on the trunk.
	Direct inbound calls using extension routing to the MiVoice Connect extensions.
	Enable off-system extensions.
	Define off-system extension range to match extensions on the remote PBX.
Inbound Trunks on Remote PBX	Enable inbound services on the trunk.
	Direct inbound calls using extension routing to the MiVoice Connect extensions.
	Outbound trunks on the remote PBX enable outbound services on the trunk.
	Configure any required access code for the trunk and the local area code for the trunks connected to the remote PBX.
	Configure the desired trunk services such as local, long distance, and so on.
	Configure the dialing format and any required digit sequences that are to be pre-pended to the dialed numbers.
	Users require trunk group access rights to use the trunk for outbound calls.
Consolidated Long Distance	Enable outbound services on the trunk.

Desired Service	Required Configuration
	Configure any required access code for the trunk and the local area code for the trunks connected to the remote PBX.
	Configure trunk services, such as long distance and international.
	Configure the dialing format and any required digit sequences that are to be pre-pended to the dialed numbers. Users require trunk group access rights to use the trunk for outbound calls.

19.14 Trunk Configuration for Legacy PBX Integration

The following steps describe how to configure the trunk for integrating the legacy PBX and the MiVoice Connect system. Some steps are optional depending on the types of services desired as summarized above.

19.14.1 Creating a New Trunk Group

1. Launch Connect Director.
2. In the navigation pane, click **Administration** > **Trunks** > **Trunk Groups**. The **Trunk Groups** page is displayed.
3. Click **New**.
4. On the **General** tab, do the following:
   - In the **Name** field, specify a name for the trunk group.
   - In the **Site** field, select the site from the drop-down list.
   - In the **Trunk Type** field, select the type of trunk to configure — **Digital Wink Start** for SGT1 or **PRI** for PRI.
5. Click **Save**.

19.14.2 Configuring Inbound Services with Extension Routing

1. Launch Connect Director.
2. In the navigation pane, click **Administration** > **Trunks** > **Trunk Groups** > **Trunk Groups**. The **Trunk Groups** page is displayed.

3. Click the name of the trunk group for which you want to configure inbound services.

   Details for the selected trunk group are displayed on the General tab.
4. Click the **Inbound** tab.
5. In the **Number of digits from CO** field, enter the number of digits received to match the number of digits sent by the remote PBX. This must match the extension length
6. Enable the **Extension** option.

> **Note**:
>
> This directs all the received calls to the configured MiVoice Connect extension that matches the received DNIS digits

7. In the **Destination** field, provide a back-up extension to use when the received digits do not match an extension in the MiVoice Connect system.
8. Click **Save**.

19.14.3 Configuring Off-System Extensions

1. Launch Connect Director.
2. In the navigation pane, click **Administration** > **Trunks** > **Trunk Groups** > **Off-System Extensions**. The **Off-System Extensions** page is displayed.
3. Click **New**.
4. On the **General** tab, in the **Trunk group** field select the trunk group for which you want to configure off-system extensions.
5. In the **From** and **To** fields, define the extension ranges for the extensions off the remote PBX.
6. Click **Save**.

19.14.4 Configuring Outbound Call Routing through Remote PBX

1. Launch Connect Director.
2. In the navigation pane, click **Administration** > **Trunks** > **Trunk Groups** > **Trunk Groups**. The **Trunk Groups** page is displayed.
3. Click the name of the trunk group for the tie trunk.

   Details for the selected trunk group are displayed on the General tab.
4. Click the **Outbound** tab, and enable the Outgoing option.
5. Configure the access code and area codes for the trunk to match the PSTN connection of the remote PBX.
6. Select the desired trunk services to match the services provided via the remote PBX.
7. Select the desired Trunk Digit Manipulations to match the tie trunk and the required dialing for the PSTN connection to your legacy PBX.

8. As needed, configure the local prefixes and pre-pend digits to match the tie trunk and the required dialing for the PSTN connection to your legacy PBX.

For additional information on trunk configuration and options, see the *MiVoice Connect System Administration Guide*.

Cut-Over 20

This chapter contains the following sections:

This chapter provides the requirements and other information for implementing the cut-over from your existing telephone system to the MiVoice Connect system.

20.1 Cut-Over Requirements

As cut-over approaches, you should review and confirm your plan, assemble the cut-over tools, and line up resources to support the cut-over.

20.1.1 Cut-Over Worksheet

The cut-over worksheet is used by the installer during the cut-over to move all end-users from the old system to the new. It is extremely important that the cut-over worksheet be prepared before the cut-over begins. You can use the cut-over worksheet at the end of this chapter to document all new and existing connections. A soft copy of this form is available in a planning and installation workbook from Mitel. Make copies as necessary.

20.1.2 New Trunks

New trunks should be installed before cut-over. This allows time for them to be terminated, configured, and tested with the MiVoice Connect system.

20.1.3 Cut-Over Coverage

There are two aspects to cut-over coverage:

- The team involved with planning the MiVoice Connect system must be on site before, during, and after cut-over.
- Appropriate coverage must be scheduled to monitor the newly installed MiVoice Connect system for errors and last-minute configuration changes, and to help end-users with any questions they might have. Mitel recommends that you have support personnel on site before the first users arrive, to ensure that the system is functional and that telephone calls are processed properly.

20.2 Cut-Over Implementation

Once planning is completed, it is time to bring the MiVoice Connect system into service. Use the checklists in this section to implement the cut-over, starting with the top-level checklist below.

Table 52: Cutover Implementation Checklist

Description	Completed
Complete the tasks listed on the basic cut-over checklist.	
Cut-over and test all trunks.	
Cut-over and test the remaining devices (telephone, fax machines, modems, and so on).	
Confirm the cut-over coverage.	

20.2.1 Basic Cut-Over Checklist

Table 53: Basic Cut-Over Checklist

Description	Completed
Secure the telephone company's contact names, telephone numbers, and pager numbers for testing.	
Set up a command center to support cut-over activities.	
Ensure that copies of the floor plans and cut-over worksheets are available.	
Secure access to building and office areas that require voice switches and telephones.	
Ensure that a telephone is installed next to the voice switch for testing.	
Ensure that music-on-hold is installed and tested.	
Record and test the auto-attendant greeting for on-hours and off-hours.	
Test all telephones.	
Test paging and night bell features, if applicable.	

20.2.2 Trunking Cut-Over

For existing trunking, use the cut-over worksheets to identify the trunks that are used from the old system (if applicable), and terminate them on the voice switches. Use a test telephone to dial in and out of each trunk, verify that it routes to the correct location, and listen closely to the voice quality.

When preparing new trunks for installation, use the following checklist.

Table 54: Trunking Cutover Checklist

Description	Completed
Identify the new trunks.	
Terminate the new trunks on the voice switches.	
Contact the telephone company's tester, and test each trunk (one at a time).	
Agree on the specific trunk that is being tested.	
Have the tester dial in on the new trunk.	
Answer the incoming call on a test telephone.	
Observe overall voice quality.	
Go through this checklist until all trunks are tested.	

When all of the trunks have been tested, have the telephone company's tester open the trunk group, and allow the callers to use the new trunks.

20.2.3 Cut-Over of Remaining Devices

Use the following checklist to test each new end-user device that is being installed.

Table 55: Remaining Devices Cutover List

Description	Completed
Place an internal call from the new device.	

Description	Completed
Place an external call from the new device.	
If applicable, place a DID call.	
If the device is for a user with voice mail, leave a welcome message.	
Leave user guides or quick reference cards for the phone and the client on the user's desk. These guides provide information about MiVoice Connect's commonly used features as well as general system information.	

20.2.4 Cut-Over Coverage

After the cut-over is implemented, it is recommended that the Cut-Over team arrives at the site before the beginning of the next business day to answer the questions from the end-users because they begin to use the MiVoice Connect system.

20.3 Cut-Over Worksheet

Table 56: Cutover Worksheet

Name	Extension	Port #	Patch Panel #	IDF	Station Cable

Appendix A - International Planning and Installation

This chapter contains the following sections:

This chapter provides information about voice switches, operating systems, and features that are supported when the MiVoice Connect system operates outside the United States of America.

21.1 Software and Feature Support

For information about our worldwide support for software and features, contact a Sales Partner or refer to the Country Availability Web page at:

https://www.mitel.com/

21.2 Language Packs

Language packs determine the language in the following parts of the system:

- Voice prompts (Voice mail, Auto Attendant, system announcements)
- Telephone User Interface (telephone display and Mitel Connect client interface)
- Online help for Mitel Connect client

Language pack availability affects the behavior of the system in the following areas:

- Site
- Trunk
- Workgroup
- Auto Attendant
- Voice Mail
- User
- Mitel Connect client

21.2.1 Language Options

The following pages in Connect Director allow you to program language options. In language priority, a workgroup language overrides the language associated with a trunk, which in turn overrides the language associated with an individual user.

- The Sites page specifies the language pack used by the Backup Auto-Attendant (BAA) or by any 400-Series and 6900-Series (6910, 6920, 6930, 6940, 6920w, 6930w, and 6940w) phones that do not have a user assigned. To access the Sites page, in the navigation pane select **Administration** > **System** > **Sites**. Click the name of the desired site, and then locate the **Language** field on the **General** tab.
- The Workgroups page specifies the language the system uses for playing prompts to inbound callers. To access the Workgroups page, in the navigation pane select **Administration** > **Features** > **Workgroups**. Click the name of the desired workgroup, and then locate the **Language** field on the **General** tab.
- The Trunk Groups page specifies the language for prompts that are played to incoming callers. To access the Trunk Groups page, in the navigation pane select **Administration** > **Trunks** > **Trunk Groups**. Click the name of the desired trunk group, and then locate the **Language** field on the **General** tab.
- The Users page specifies the language prompts used for the user's telephone interface and voicemail prompts. To access the Users page, in the navigation pane select **Administration** > **Users** > **Users**. Click the name of the desired user, and then locate the **Language** field on the **General** tab.

21.3 Analog Telephones, Tones, Cadences, and Impedances

For all supported countries, standard analog telephones are available on a per-country basis. The main difference between telephones in different countries is the line impedance. The MiVoice Connect Distributed Call Control software will provide the appropriate impedance required for each supported country. Tones, cadences, and impedance requirements are matched on a per-country basis.

21.4 Dialing Plan Considerations

When planning a global voice network, remember that the MiVoice Connect system is a single image system and that you must consider all countries and locations when designing the international dialing plan. The MiVoice Connect system can match the dialing plan requirements of the local service provider for the supported countries.

21.4.1 Single-Extension Plan

Across the global voice network, all extensions must be unique and cannot overlap.

21.4.2 Trunk Access Codes

Across the global voice network, when you configure trunk access codes, that portion of the dialing plan will be reserved so you will be sacrificing one digit. Typically in the US, customers use 9 as a trunk access code. Internationally, those in the EMEA, for instance, often use 0 as a trunk access code. The following are some things to consider when you create a trunk access code:

- Using two different trunk access codes will limit users to only being able to access certain trunk groups.
- If you use a single trunk access code, some users will need to be retrained.
- Alternatively, 8 could be defined for the trunk access code globally.

Mitel recommends proper identification from the beginning. The trunk access code should not be changed later.

21.4.3 Operator Digit

The leading digit of 0 is typically reserved for dialing the operator in the US. The operator digit is configurable. Similarly, EMEA customers are accustomed to dialing 9 to reach the operator.

Mitel recommends choosing a single digit for the trunk access code and selecting a different single digit for the operator.

21.4.4 Emergency Numbers

The MiVoice Connect system allows dialing of emergency numbers with and without trunk access codes. For this reason, you should architect the dialing plan for this feature.

- 911 is used in the US.
- 112 is used in Europe and other countries.
- Check for other countries and regions for local requirements.

Thus, extensions should not begin with 0, 1, or 9 to make use of this feature.

Each site can have a maximum of ten emergency numbers to accommodate locations where multiple emergency service numbers are required.

For more information about emergency numbers, see the appendix in the *MiVoice Connect System Administration Guide* about emergency 911 operations.

21.4.5 National Suicide and Crisis Lifeline Number

988 is the National Suicide and Crisis Lifeline number for North America.

To configure 988 as the Suicide and Crisis Lifeline number, you must add it as an emergency number under US MiVoice Connect site. When the user dials 988, the call is not treated as an emergency number but as a normal trunk call that is routed through normal trunks.

Note:
When 988 call is made a new event with event-id 1370 will be generated.

As part of the 988 implementation federal government has updated and mandated the dialing rules for local numbers, users must always dial 10 digit local numbers rather than 7-digit numbers which wont have area

code prefixed. The main reason being newly incorporated 988 service number which also happens to be prefix of 7 digit local numbers, thus creating dialing rule clash for service providers. (988xxxx identifies active local number in existing US network).

21.4.6 DID Numbers

DID numbers are related to the trunk group in which they are associated. You should strive to match the last digits of the DID number to the user's extension number.

21.5 Carrier Codes

Certain countries provide an option for requiring one or two numbers that the MiVoice Connect user must press after the trunk access code (usually a 9 or an 8) and before an area code or another nation's country code. The purpose of this option is to get the lowest-cost route for long-distance or international calls. When the user presses this code, the call goes out a trunk to a carrier that the system administrator has specified. If the user makes a long-distance or international call without this code, the MiVoice Connect system selects the trunk.

This section defines the carrier codes that certain countries use and lists the numbers that the user presses to utilize the associated trunks. The two definitions that readers need for this description are as follows:

- **Carrier code:** This number specifies a carrier. The system administrator assigns this code to a trunk group so that calls go to that carrier when the user prepends the country code to a phone number. System administrators in applicable countries must know the code for the carriers they want to give preferential business. The user does not see this carrier code.
- **Country code:** This country code is a nation-wide number that a user presses to direct long-distance or international calls to the carrier that the carrier code specifies. This country code is not the number that callers from outside a country use to reach the country. For example, the country code that callers outside of Singapore use to reach that country is 65, but from inside Singapore, the country code that a caller presses to direct an international call to a specific carrier is 01.

Using the Singapore example: if a trunk access code is 9 and the MiVoice Connect user with international calling permission initiates a call to India, the number sequence is as follows:

9 01 91 <telephone number>

As of the current release, six countries use this code function. Carrier Code by Country lists the carrier code and application for the countries that use them.

Table 57: Carrier Code by Country

Code	Country and Application
55	Brazil, all calls
1	Hong Kong, international calls

Code	Country and Application
2	South Korea, international calls
01	Singapore, international calls
2	Taiwan, international calls
1	Thailand, international calls

Appendix B - Session Initiation Protocol

This chapter contains the following sections:

This chapter provides information about the Session Initiation Protocol (SIP). You should refer to this chapter for help in planning a SIP deployment on your MiVoice Connect system.

Note:

For SIP configuration steps and other SIP details, see the Session Initiation Protocol (SIP) chapter in the *MiVoice Connect System Administration Guide*.

22.1 Overview

The protocol, which works at the application layer, allows users to initiate interactive sessions between any network devices that support the protocol. SIP is capable of initiating or terminating Internet telephony calls and other multimedia applications such as video or gaming.

The protocol is based on a client-server model. With support for redirection services, networked users can initiate a call or receive a call, regardless of their physical location.

In its networking negotiations SIP takes into account the following pieces of information:

- The address of the end system
- The physical media
- The call recipient's acceptance to the invitation

The protocol then configures the parameters for the session and handles the call setup and tear-down.

SIP allows two discrete MiVoice Connect systems to be integrated with any IP connection, without the need for physical tie trunking. (Note that care should be taken to make sure that the extension numbering plans in the two systems do not overlap, and that if they do overlap, translation tables need to be used to resolve conflicts.)

In the current release of the MiVoice Connect system, the SIP trunks and SIP tie-trunks support the SIP capabilities. Like other trunk, the SIP trunk assignments are switches, so that SIP calls into and out of the MiVoice Connect system traverse these SIP trunks. However, up to five SIP trunks can be associated with one analog switch port, meaning that there will be no physical channel/port associated with each SIP trunk. The SIP trunk is a logical trunk end point which only handles call control responsibilities. The media flows

directly between the end-point SIP devices (that is, call initiator and the call terminator), freeing the switch from the burden of controlling media flow.

22.2 General SIP Comments

Conferencing

- Ports for Make Me conferences must be available on the initiating side of a 3-way conference call involving a SIP end-point.
- On third-party SIP phones, Make Me conference ports are needed even for 3-way conferences. Note that configuration of any Make Me conferencing support in Connect Director requires at least 4 available conference ports.
- MiVoice Connect SIP trunks support from 4-way up to a maximum of 8-way conferences. This conferencing relies on MiVoice Connect's Make Me capability. End-users can set up Make Me conference calls by using their Mitel Connect client. Like extensions with support of Media Gateway Control Protocol (MGCP), SIP extensions require permissions and a minimum of 4 Make Me ports to set up Make Me conference call.
- An individual SIP trunk must be provisioned for each call to the SIP device (including conference-in or transferred calls). Thus, static SIP trunks must be provisioned with additional trunks in line with the highest anticipated number of such calls.

22.2.1 DTMF

MiVoice Connect supports RFC2833 (DTMF) for users calling over SIP trunks regardless of the negotiated voice codec.

MiVoice Connect can be configured to use SIP INFO for DTMF signaling in environments where out-of-band DTMF is needed but RFC 2833 is not applicable. SIP INFO for DTMF signaling is available on only SIP trunks.

22.2.2 Foreign Language Support

In addition to English, MiVoice Connect supports other languages (for Caller Name, Called Name, User Name, and so on) over SIP tie trunks and service provider trunks. Some third-party devices might not be able to display all of a languages' characters.

22.2.3 General Feature Limitations

- A music on hold (MOH) switch supports 15 streams of MOH, but some of these can be used to fan out MOH to other trunk switches. If some MOH streams go to other switches, the actual number of MOH streams on SIP trunks is less than 15.
- Three-way conference on a SIP trunk call uses Make Me conference ports. A minimum of 3 Make Me ports must be configured to support 3-way conferencing.
- A SIP trunk can be a member of a 3-party conference but cannot initiate a 3-way conference (unless the SIP device merges the media streams itself).
- MiVoice Connect SIP supports basic transfers (blind transfers) and attended transfers (consultative transfers).

- In the current release, the following features are supported by SIP only if the trunk has a SIP trunk profile with hairpinning and the trunk is on a half-width switch:
  - Silent Coach
  - Silent Monitor
  - Barge-In
  - Call recording
- Silence detection on trunk-to-trunk transfers is not supported because it requires a physical trunk.
- Extension Assignment is limited using SIP trunks. Either DTMF over INFO must be used, or in—the absence of such support—the features that use DTMF are not supported (including **Accept call by pressing 1**.)
- Fax (and modem) redirection on SIP trunks is supported if T.38 is used.

22.2.4 Additional Configuration Considerations

- Overlapping number plans are not allowed between two systems tied with SIP trunks unless digit translation is used.
- When translating digits between two MiVoice Connect systems tied with SIP trunks, even system extensions like VM, AA should be properly translated.
- Multiple trunks (SIP and non-SIP trunks) can be created or deleted at one time.

Appendix C - Voice Switches

This chapter contains the following sections:

This appendix describes the voice switches supported in MiVoice Connect.

23.1 Overview

Switch model numbers are located on the rear panel, as shown in the following figure.

Figure 30: Switch Model Number Label

All voice switches include a Default Switch, which is a recessed button available on the front panel. This switch can be used to reset the following static configurations to factory default:

- Static IP address
- Server address
- Phone extension assignments
- Ethernet negotiation settings

Press and hold the default switch for more than five seconds to reset the listed configurations to factory defaults. Refer to the front panel images in the following sections for the location of the Default Switch.

23.2 Switch Models

The classification of voice switch models is in three switch families that depend on the chassis type of the switch:

- 1-U Half Width Switches
- 1-U Full Width Switches

The following is a brief description of each switch family.

23.3 1-U Half Width Voice Switches

The 1-U Half Width Switch family is the most recent switch design. 1-U Half Width have a smaller footprint, use less power, and have lower heat dissipation requirements than earlier switches. These switches offer higher granularity in the number of IP users supported, allowing customers to precisely program the switch to satisfy their requirements.

The switches can be stacked or mounted in a standard 19-inch rack. Rack mounting 1-U Half Width Switches requires the Dual Tray. One or two switches are inserted into the Dual Tray, which is then mounted into the 19-inch rack. Two switches are mounted side by side Rack mounting the switches require the Dual Tray.

1-U Half Width Voice Switch models include:

- Voice Switch ST1D/ST2D
- Voice Switch ST50A/ST100A
- Voice Switch ST200/ST500
- Voice Switch ST100DA
- Voice Switch SG30
- Voice Switch SG30BRI
- Voice Switch SG50
- Voice Switch SG90
- Voice Switch SG90BRI
- Voice Switch SG220T1
- Voice Switch SG220T1A
- Voice Switch SGT1k
- Voice Switch SG220E1
- Voice Switch SGE1k

23.3.1 Voicemail Model Voice Switches

Voicemail Model Switches are switches that provide voicemail services and access to auto attendant menus for extensions hosted by the switch. Voicemail Model (V Model) switches provide local access to voicemail while being controlled by a Distributed server at a different location.

The switches can be stacked or mounted in a standard 19-inch rack. Rack mounting 1-U Half Width Switches requires the Dual Tray. One or two switches are inserted into the Dual Tray, which is then mounted into the 19-inch rack. Two switches are mounted side by side Rack mounting the switches require the Dual Tray.

V Model Switch models include:

- Voice Switch SG90V
- Voice Switch SG50V
- Voice Switch SG90BRIV

Note:
Voicemail switches such as SG90V and SG50V do not support survivable voicemail and auto-attendant features at a remote (non-headquarters) site.

23.3.1.1 Capacity

Number of V Model switches allowed per system

A MiVoice Connect system supports a maximum of 500 V Model Switches. There are no restrictions concerning the allocation of switches among the sites defined by the system.

23.3.1.1.1 Simultaneous Voicemail Calls per V Model switches

Voicemail Model Switches support the following number of simultaneous voicemail calls.

- SG50V – Maximum of 5 Voicemail calls per switch
  - G711 calls: 5
  - G729 calls: 2
- SG90V – Maximum of 9 Voicemail calls per switch
  - G711 calls: 9
  - G729 calls: 4
- SG90BRIV – Maximum of 9 Voicemail calls per switch
  - G711 calls: 9
  - G729 calls: 4

23.3.1.1.2 Call Load

Voicemail Model Switches call load capacity is as follows:

- 5400 BHCC when supporting 90 MGCP IP Phones or 90 SIP Trunks
- 3600 BHCC when supporting 90 SIP IP Phones or 90 SIP Trunks

23.3.1.1.3 Compact Flash Memory

Voicemail Model switches store voicemail and Auto Attendant files on compact flash. Flash card capacity for V Model Switches is:

- SG50V: 1 Gb
- SG90V: 2 Gb
- SG90BRIV: 2 Gb

23.3.1.1.4 Media Support

Voicemail Model Switches support the following media streams:

- G711
  - Music on Hold (MOH): 15 calls
  - Backup Auto Attendant (BAA): 50 calls
- G729
  - Music on Hold (MOH): none
  - Backup Auto Attendant (BAA): none

23.3.1.1.5 SIP support

Voicemail Model Switches support the following SIP media streams:

- G711 Ringback tone (Hunt Groups and Work Group calls): 50 media streams
- G729 Ringback tone (Hunt Groups and Work Group calls): no support

23.3.2 1-U Full Width Voice Switches

Full width switch models can be stacked or mounted directly into a standard 19-inch equipment rack. These switches are 1 RU and have an RJ21X connector for connection to analog phones and trunks. They also feature redundant Ethernet LAN connections for greater availability and reliability.

1-U Full Width Voice Switch models include:

- Voice Switch ST24A/ST48A
- Voice Switch SG24A

23.4 Specifications - ST 1-U Half-Width Switches

23.4.1 Voice Switch ST1D/ST2D

The following sections describe Voice Switch ST1D/ST2D resource capacity, LED behavior, and connectors. Voice Switch ST1D Front Plate and Voice Switch ST2D Front Plate display the ST1D/ST2D front plate.

Figure 31: Voice Switch ST1D Front Plate

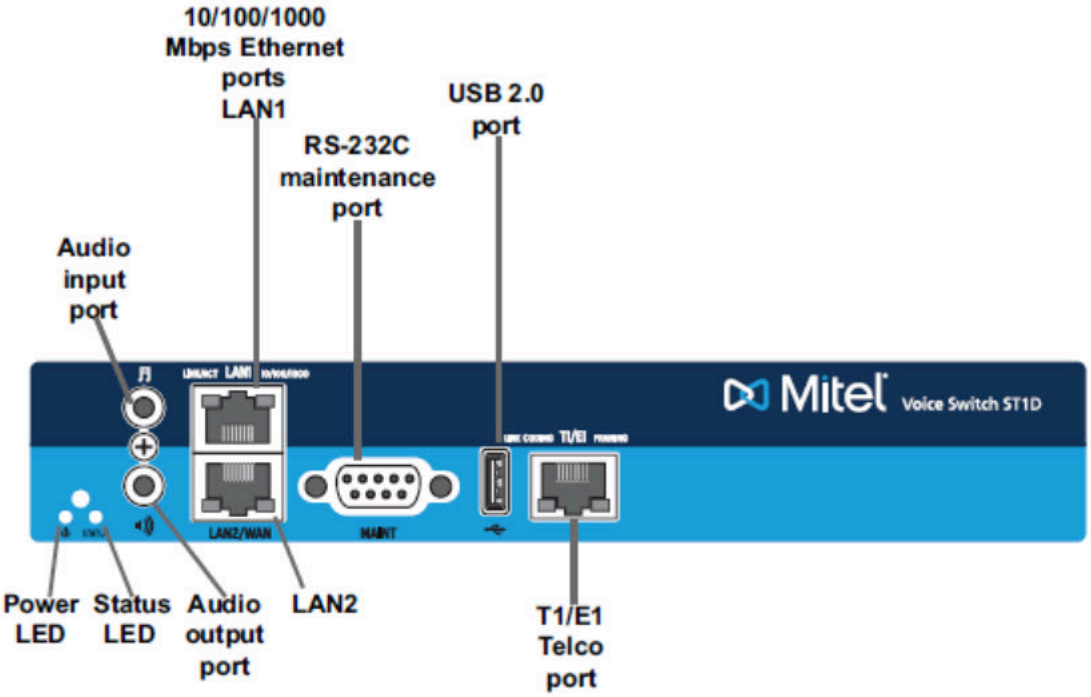
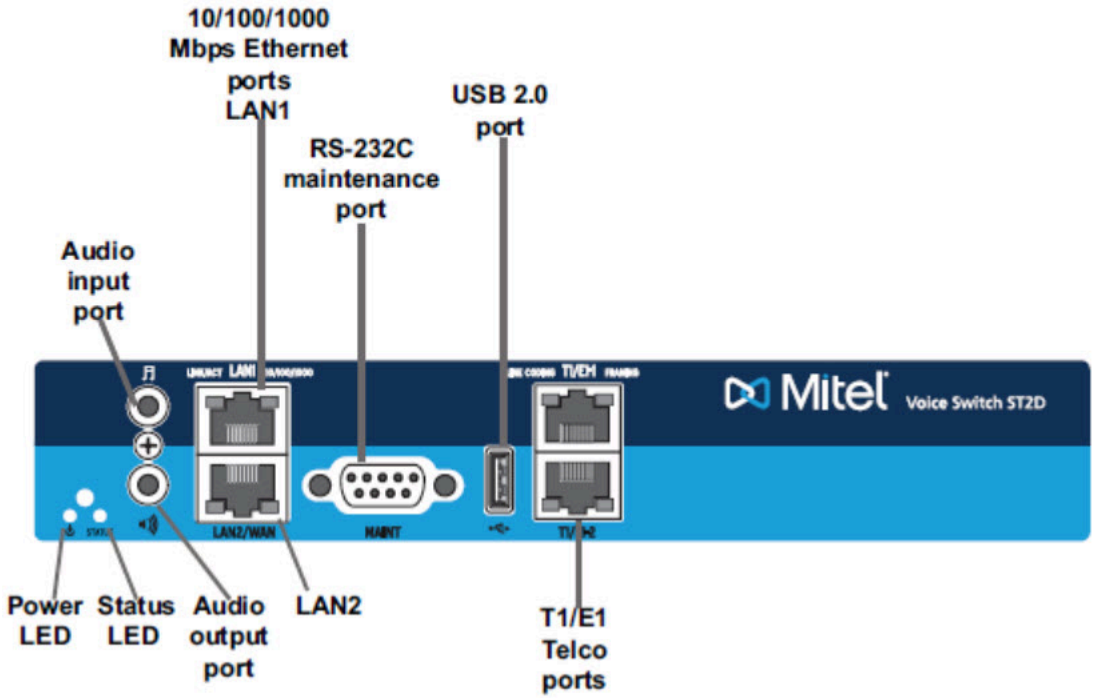


Figure 32: Voice Switch ST2D Front Plate



23.4.1.1 Switch Capacity

- Digital Circuit Resources
  - ST1D Voice Switch — One SGT1/SGE1 circuit, 24 channels per circuit: 24 channels maximum
  - ST2D Voice Switch — Two SGT1/SGE1 circuits, 24 channels per circuit: 48 channels maximum
- Make Me Conference Resource: None for both devices
- Maximum IP Phone Resources
  - ST1D SIP Media Proxies: 30
  - ST2D SIP Media Proxies: 60

23.4.1.2 LED Descriptions

Power LED

The Voice Switch ST1D/ST2D has one power LED, which indicates the following:

- On: The switch is operating normally.
- Off: The switch has no power.
- Flashing: Continuous flashing or a two-flash pattern indicates a failed internal self-test (that is, hardware failure).

23.4.1.2.1 Network LEDs

The Voice Switch ST1D/ST2D network LEDs (LAN1 and LAN2) indicate the speed at which the switch is communicating with the network and whether there is network activity.

The network LED descriptions are as follows:

- Link/Activity: When lit, this LED indicates that the switch is connected to an Ethernet network. This LED indicates network activity, as follows:
  - When flashing, network activity is detected.
  - When on (not flashing), the switch is connected to an Ethernet network.
  - When off, the switch cannot detect an Ethernet network.

  This LED is not directly related to any switch's individual network activity. For example, if three switches are connected to the same hub and one switch's Traffic LED shows activity, the other switches will indicate the same activity.
- 10/100/1000 Mbps
  - When off, the switch is connected to a 10BaseT network.
  - When green, the switch is connected to a 100BaseT network.
  - When yellow, the switch is connected to a 1000BaseT network.

23.4.1.2.2 Status LED

The Voice Switch ST1D/ST2D has one status LED to provide general information about the ports. The color and blink pattern of the LED indicate the port function:

- Off — No ports are assigned
- Green Steady— No ports are handling active calls
- Green Flashing Fast — At least one port is handling an active call.
- Yellow Steady — No ports are handling active calls and at least one port is out of service.
- Yellow Flashing Slow — The switch is not connected (or has lost connection) to a server.
- Yellow Flashing Fast — At least one port is handling an active call and at least one port is out of service.

23.4.1.2.3 SGT1/SGE1 LEDs

The Voice Switch ST1D/ST2D has one status LED to provide general information about the ports. The color and blink pattern of the LED indicate the port function:

Line coding

- Green — For the SGT1 connection, this indicates the AMI or B8ZS line coding signal is good. For the SGE1 connection, this indicates the HDB3 line coding signal is good.
- Yellow — This switch is receiving bipolar violations (BPV) at one-second intervals.
- Solid Red — The trunk is configured for SIP Media Proxy.
- Flashing Red* — A loss of signal (LOS) has occurred.

- Off — The switch has no power.

Framing

- Green — The SGT1 or SGE1 signal is in frame (synchronized)
- Yellow — The CO has sent a yellow alarm.
- Yellow Flashing — The frame-bit error rate has exceeded its limits.
- Solid Red — The trunk is configured for SIP Media Proxy.
- Flashing Red* — SGT1 signal is out-of-frame (OOF) and cannot be framed to the Extended Superframe (ESF) or D4 format. SGE1 signal is out-of-frame (OOF).
- Off — The switch has no power.

*If both the line coding and framing LEDs are simultaneously flashing red, loopback is enabled.

23.4.1.3 Voice Switch ST1D/ST2D Connectors

The Voice Switch ST1D voice switch contains the following components:

- One audio input port (3.5 mm stereo) for connecting to a music-on-hold source
- One audio output port (3.5 mm stereo) for connecting to a corporate paging system or night bell.
- Two RJ-45 10/100/1000 Mbps LAN connectors
- One DB-9 (socket), RS-232C maintenance port (default 115,200 bps, 8 bits, no parity, 1 stop bit, no handshake) for serial communications
- USB port for logging/troubleshooting

> **Note**:
>
> Only vFAT/FAT32 storage is supported for USB logging.

- RJ-48C Telco port(s) for connecting the switch to a telephone company line(s). This is the SGT1/SGE1 configurable connection.

23.4.2 Voice Switch ST50A/ST100A

The following sections describe Voice Switch ST50A/ST100A resource capacity, LED behavior, and connectors. Voice Switch ST50A Front Plate and Voice Switch ST100A Front Plate display the ST50A/ST100A front plate.

Figure 33: Voice Switch ST50A Front Plate

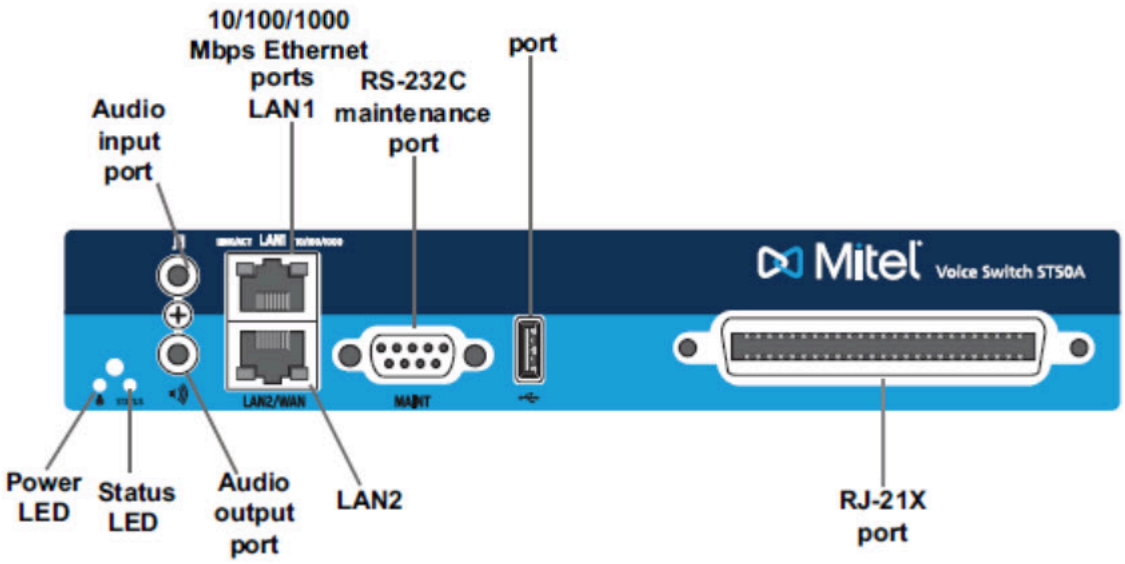
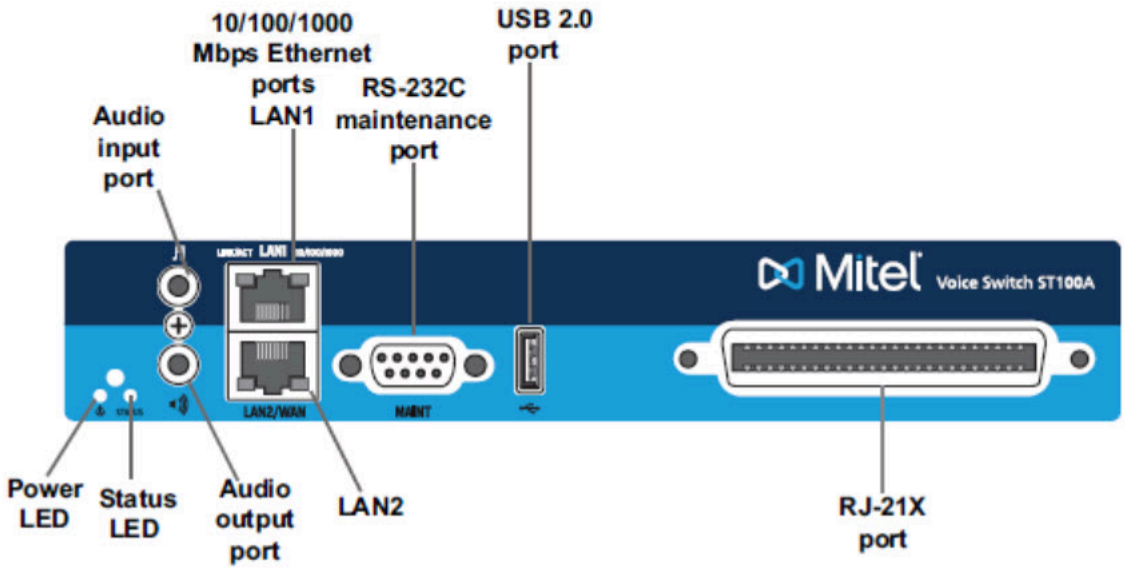


Figure 34: Voice Switch ST100A Front Plate



23.4.2.1 Switch Capacity

ST50A Analog Circuit Resources

- Ports 1-4: Four Loop Start Trunks
- Ports 9-12: Four Extensions or DID Trunks. A single command configures all ports as either Extensions or DID trunks.
- Power Failure Transfer Unit: Trunk Port 1 to Extension Port 12

23.4.2.1.1 ST100A Analog Circuit Resources

- Ports 1-8: Eight Loop Start Trunks
- Ports 9-14: Six Extensions or DID Trunks. A single command configures all ports as either Extensions or DID trunks.
- Power Failure Transfer Unit: Trunk Port 1 to Extension Port 12

23.4.2.1.2 Make Me Conference Resources

- ST50A: 6 ports
- ST100A: 12 ports

23.4.2.1.3 Maximum IP Phone Resources

- ST50A
  - Built-in IP Phone ports: 50
  - Built-in SIP Proxy ports: 500
  - SIP Media Proxies: 8
- ST100A
  - Built-in IP Phone ports: 100
  - Built-in SIP Proxy ports: 500
  - SIP Media Proxies: 14

23.4.2.2 LED Descriptions

Power LED

The Voice Switch ST50A/ST100A has one power LED, which indicates the following:

- On: The switch is operating normally.
- Off: The switch has no power.
- Flashing: Continuous flashing or a two-flash pattern indicates a failed internal self-test (that is, hardware failure).

23.4.2.2.1 Network LEDs

The Voice Switch ST50A/ST100A network LEDs (LAN1 and LAN2) indicate the speed at which the switch is communicating with the network and whether there is network activity.

The network LED descriptions are as follows:

- Link/Activity: When lit, this LED indicates that the switch is connected to an Ethernet network. This LED indicates network activity, as follows:
  - When flashing, network activity is detected.
  - When on (not flashing), the switch is connected to an Ethernet network.
  - When off, the switch cannot detect an Ethernet network.

  This LED is not directly related to any switch's individual network activity. For example, if three switches are connected to the same hub and one switch's Traffic LED shows activity, the other switches will indicate the same activity.
- 10/100/1000 Mbps
  - When off, the switch is connected to a 10BaseT network.
  - When green, the switch is connected to a 100BaseT network.
  - When yellow, the switch is connected to a 1000BaseT network.

23.4.2.2.2 Status LED

The Voice Switch ST50A/ST100A has one status LED to provide general information about the ports. The color and blink pattern of the LED indicate the port function:

- Off — No ports are assigned.
- Green Steady— No ports are handling active calls.
- Green Flashing Fast — At least one port is handling an active call.
- Yellow Steady — No ports are handling active calls and at least one port is out of service.
- Yellow Flashing Slow — The switch is not connected (or has lost connection) to a server.
- Yellow Flashing Fast — At least one port is handling an active call and at least one port is out of service.

23.4.2.3 Voice Switch ST50A/ST100A Connectors

The Voice Switch ST50A/ST100A voice switch contains the following components:

- One audio input port (3.5 mm stereo) for connecting to a music-on-hold source
- One audio output port (3.5 mm stereo) for connecting to a corporate paging system or night bell.
- Two RJ-45 10/100/1000 Mbps LAN connectors
- One DB-9 (socket), RS-232C maintenance port (default 115,200 bps, 8 bits, no parity, 1 stop bit, no handshake) for serial communications
- USB port for logging/troubleshooting

> **Note**:
>
> Only vFAT/FAT32 storage is supported for USB logging.

- One RJ-21X port (plug) for connecting the switch to analog lines and trunks

23.4.2.3.1 Voice Switch ST50A RJ-21X Telephone and Trunk Connector

ST50A RJ-21X Telephone and Trunk Connector lists the RJ-21X Ring and Tip pin numbers for the ST50A.

Table 58: ST50A RJ-21X Telephone and Trunk Connector

Port	Type	Ring		Tip	
		Pin #	Cable Color	Pin #	Cable Color
1	Trunk	1	Blue/White	26	White/Blue
–		2	Orange/White	27	White/Orange
2	Trunk	3	Green/White	28	White/Green
–		4	Brown/White	29	White/Brown
3	Trunk	5	Slate/White	30	White/Slate
–		6	Blue/Red	31	Red/Blue
4	Trunk	7	Orange/Red	32	Red/Orange
–		8	Green/Red	33	Red/Green
5		9	Brown/Red	34	Red/Brown
–		10	Slate/Red	35	Red/Slate
6		11	Blue/Black	36	Black/Blue
–		12	Orange/Black	37	Black/Orange
7		13	Green/Black	38	Black/Green
–		14	Brown/Black	39	Black/Brown

Port	Type	Ring		Tip	
		Pin #	Cable Color	Pin #	Cable Color
8		15	Slate/Black	40	Black/Slate
–		16	Blue/Yellow	41	Yellow/Blue
9	Extension - DID	17	Orange/Yellow	42	Yellow/Orange
–		18	Green/Yellow	43	Yellow/Green
10	Extension - DID	19	Brown/Yellow	44	Yellow/Brown
–		20	Slate/Yellow	45	Yellow/Slate
11	Extension - DID	21	Blue/Violet	46	Violet/Blue
–		22	Orange/Violet	47	Violet/Orange
12	Extension - DID	23	Green/Violet	48	Violet/Green
–		24	Brown/Violet	49	Violet/Brown
–		25	Slate/Violet	50	Violet/Slate

23.4.2.3.2 Voice Switch ST100A RJ-21X Telephone and Trunk Connector

ST100A RJ-21X Telephone and Trunk Connector lists the RJ-21X Ring and Tip pin numbers for the ST100A.

Table 59: ST100A RJ-21X Telephone and Trunk Connector

Port	Type	Ring		Tip	
		Pin #	Cable Color	Pin #	Cable Color
1	Trunk	1	Blue/White	26	White/Blue
–		2	Orange/White	27	White/Orange
2	Trunk	3	Green/White	28	White/Green
–		4	Brown/White	29	White/Brown
3	Trunk	5	Slate/White	30	White/Slate
–		6	Blue/Red	31	Red/Blue
4	Trunk	7	Orange/Red	32	Red/Orange
–		8	Green/Red	33	Red/Green
5		9	Brown/Red	34	Red/Brown
–		10	Slate/Red	35	Red/Slate
6	Trunk	11	Blue/Black	36	Black/Blue
–		12	Orange/Black	37	Black/Orange
7	Trunk	13	Green/Black	38	Black/Green
–		14	Brown/Black	39	Black/Brown
8	Trunk	15	Slate/Black	40	Black/Slate
–		16	Blue/Yellow	41	Yellow/Blue

Port	Type	Ring		Tip	
		Pin #	Cable Color	Pin #	Cable Color
9	Extension - DID	17	Orange/Yellow	42	Yellow/Orange
–		18	Green/Yellow	43	Yellow/Green
10	Extension - DID	19	Brown/Yellow	44	Yellow/Brown
13	Extension - DID	20	Slate/Yellow	45	Yellow/Slate
11	Extension - DID	21	Blue/Violet	46	Violet/Blue
14	Extension - DID	22	Orange/Violet	47	Violet/Orange
12	Extension - DID	23	Green/Violet	48	Violet/Green
–		24	Brown/Violet	49	Violet/Brown
–		25	Slate/Violet	50	Violet/Slate

23.4.3 Voice Switch ST200/ST500

The following sections describe Voice Switch ST200/ST500 resource capacity, LED behavior, and connectors. Voice Switch ST200 Front Plate and Voice Switch ST500 Front Plate display the ST200 and ST500 front plates.

Figure 35: Voice Switch ST200 Front Plate

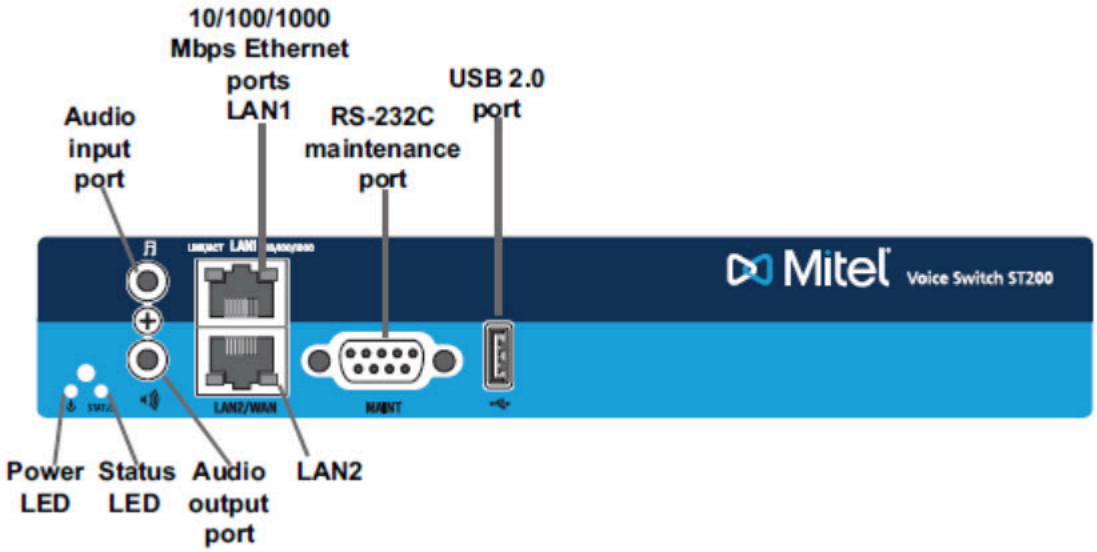
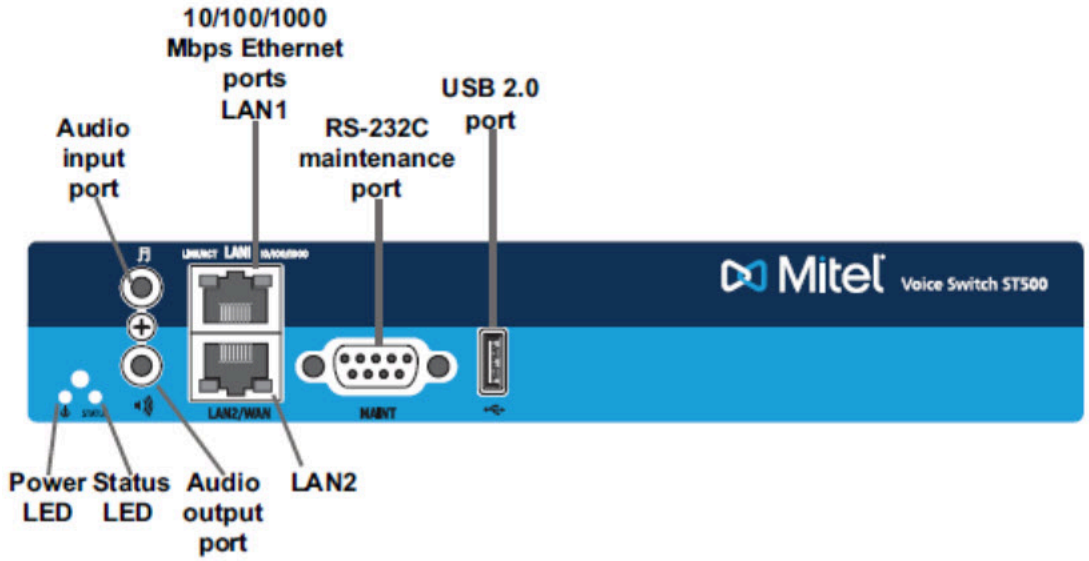


Figure 36: Voice Switch ST500 Front Plate



23.4.3.1 Switch Capacity

Make Me Conference Resources

- ST200: 12 ports
- ST500: 24 ports

23.4.3.1.1 Maximum IP Phone Resources

- ST200
  - Built-in IP Phone ports: 200
  - Built-in SIP Proxy ports: 500
- ST500
  - Built-in IP Phone ports: 500
  - Built-in SIP Proxy ports: 1000

23.4.3.2 LED Descriptions

Power LED

The Voice Switch ST200/ST500 has one power LED, which indicates the following:

- On: The switch is operating normally.
- Off: The switch has no power.
- Flashing: Continuous flashing or a two-flash pattern indicates a failed internal self-test (that is, hardware failure).

23.4.3.2.1 Network LEDs

The Voice Switch ST200/ST500 network LEDs (LAN1 and LAN2) indicate the speed at which the switch is communicating with the network and whether there is network activity.

The network LED descriptions are as follows:

- Link/Activity: When lit, this LED indicates that the switch is connected to an Ethernet network. This LED indicates network activity, as follows:
  - When flashing, network activity is detected.
  - When on (not flashing), the switch is connected to an Ethernet network.
  - When off, the switch cannot detect an Ethernet network.

  This LED is not directly related to any switch's individual network activity. For example, if three switches are connected to the same hub and one switch's Traffic LED shows activity, the other switches will indicate the same activity.
- 10/100/1000 Mbps
  - When off, the switch is connected to a 10BaseT network.
  - When green, the switch is connected to a 100BaseT network.
  - When yellow, the switch is connected to a 1000BaseT network.

23.4.3.2.2 Status LED

The Voice Switch ST200/ST500 has one status LED to provide general information about the ports. The color and blink pattern of the LED indicate the port function:

- Off — No ports are assigned.
- Green Steady— No ports are handling active calls.
- Green Flashing Fast — At least one port is handling an active call.
- Yellow Steady — No ports are handling active calls and at least one port is out of service.
- Yellow Flashing Slow — The switch is not connected (or has lost connection) to a server.
- Yellow Flashing Fast — At least one port is handling an active call and at least one port is out of service.

23.4.3.3 Voice Switch ST200/ST500 Connectors

The Voice Switch ST200/ST500 voice switch contains the following components:

- One audio input port (3.5 mm stereo) for connecting to a music-on-hold source
- One audio output port (3.5 mm stereo) for connecting to a corporate paging system or night bell
- Two RJ-45 10/100/1000 Mbps LAN connectors
- One DB-9 (socket), RS-232C maintenance port (default 115,200 bps, 8 bits, no parity, 1 stop bit, no handshake) for serial communications
- USB port for logging/troubleshooting

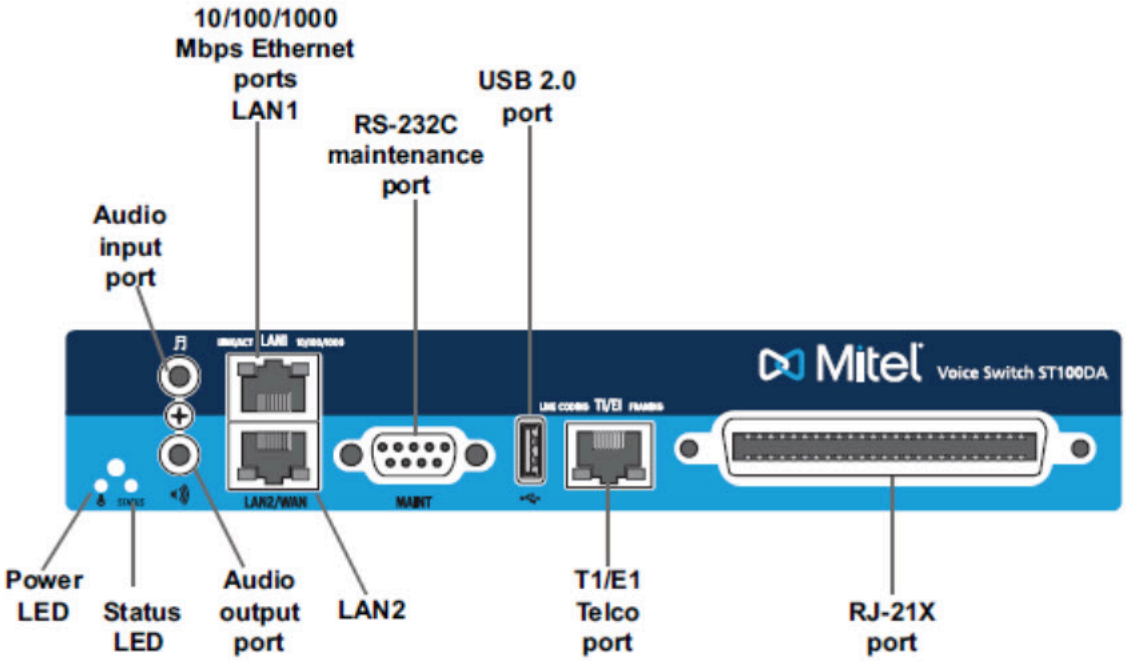
Note:

Only vFAT/FAT32 storage is supported for USB logging.

23.4.4 Voice Switch ST100DA

The following sections describe Voice Switch ST100DA resource capacity, LED behavior, and connectors. Voice Switch ST100DA Front Plate displays the ST100DA front plate.

Figure 37: Voice Switch ST100DA Front Plate



23.4.4.1 Switch Capacity

Digital Circuit Resources

- One SGT1/SGE1 circuit, 24 channels per circuit: 24 channels maximum

23.4.4.1.1 Analog Circuit Resources

- Ports 1 and 2: Two Loop Start Trunks
- Ports 9-14: Six Extensions or DID Trunks. A single command configures all ports as either Extensions or DID trunks.
- Power Failure Transfer Unit: Trunk Port 1 to Extension Port 12

23.4.4.1.2 Make Me Conference Resources: 12 ports

Maximum IP Phone Resources

- Built-in IP Phone ports: 100
- Built-in SIP Proxy ports: 500
- SIP Media Proxies: 38

23.4.4.2 LED Descriptions

Power LED

The Voice Switch ST100DA has one power LED, which indicates the following:

- On: The switch is operating normally.
- Off: The switch has no power.
- Flashing: Continuous flashing or a two-flash pattern indicates a failed internal self-test (that is, hardware failure).

23.4.4.2.1 Network LEDs

The Voice Switch ST100DA network LEDs (LAN1 and LAN2) indicate the speed at which the switch is communicating with the network and whether there is network activity.

The network LED descriptions are as follows:

- Link/Activity: When lit, this LED indicates that the switch is connected to an Ethernet network. This LED indicates network activity, as follows:
  - When flashing, network activity is detected.
  - When on (not flashing), the switch is connected to an Ethernet network.
  - When off, the switch cannot detect an Ethernet network.

  This LED is not directly related to any switch's individual network activity. For example, if three switches are connected to the same hub and one switch's Traffic LED shows activity, the other switches will indicate the same activity.
- 10/100/1000 Mbps
  - When off, the switch is connected to a 10BaseT network.
  - When green, the switch is connected to a 100BaseT network.
  - When yellow, the switch is connected to a 1000BaseT network.

23.4.4.2.2 Status LED

The Voice Switch ST100DA has one status LED to provide general information about the ports. The color and blink pattern of the LED indicate the port function:

- Off — No ports are assigned.
- Green Steady— No ports are handling active calls.
- Green Flashing Fast — At least one port is handling an active call.
- Yellow Steady — No ports are handling active calls and at least one port is out of service.
- Yellow Flashing Slow — The switch is not connected (or has lost connection) to a server.
- Yellow Flashing Fast — At least one port is handling an active call and at least one port is out of service.

23.4.4.2.3 SGT1/SGE1 LEDs

The Voice Switch ST100DA has one status LED to provide general information about the ports. The color and blink pattern of the LED indicate the port function:

Line Coding

- Green — For the SGT1 connection, this indicates the AMI or B8ZS line coding signal is good. For the SGE1 connection, this indicates the HDB3 line coding signal is good.
- Yellow — This switch is receiving bipolar violations (BPV) at one-second intervals.
- Solid Red — The trunk is configured for SIP Media Proxy.
- Flashing Red* — A loss of signal (LOS) has occurred.
- Off — The switch has no power.

Framing

- Green — The SGT1 or SGE1 signal is in frame (synchronized).
- Yellow — The CO has sent a yellow alarm.
- Yellow Flashing — The frame-bit error rate has exceeded its limits.
- Solid Red — The trunk is configured for SIP Media Proxy.
- Flashing Red* — SGT1 signal is out-of-frame (OOF) and cannot be framed to the Extended Superframe (ESF) or D4 format. SGE1 signal is out-of-frame (OOF).
- Off — The switch has no power.

*If both the line coding and framing LEDs are simultaneously flashing red, loopback is enabled.

23.4.4.3 Voice Switch ST100DA Connectors

The Voice Switch ST100DA voice switch contains the following components:

- One audio input port (3.5 mm stereo) for connecting to a music-on-hold source
- One audio output port (3.5 mm stereo) for connecting to a corporate paging system or night bell
- Two RJ-45 10/100/1000 Mbps LAN connectors
- One DB-9 (socket), RS-232C maintenance port (default 115,200 bps, 8 bits, no parity, 1 stop bit, no handshake) for serial communications
- USB port for logging/troubleshooting

> **Note**:
> Only vFAT/FAT32 storage is supported for USB logging.

- RJ-48C Telco port(s) for connecting the switch to a telephone company line(s). This is the SGT1/SGE1 configurable connection.
- RJ-21X port for connections to analog lines and trunks

23.4.4.3.1 Voice Switch ST100DA RJ-21X Telephone and Trunk Connector

ST100DA RJ-21X Telephone and Trunk Connector lists the RJ-21X Ring and Tip pin numbers for the ST100DA.

Table 60: ST100DA RJ-21X Telephone and Trunk Connector

Port	Type	Ring		Tip	
		Pin #	Cable Color	Pin #	Cable Color
1	Trunk	1	Blue/White	26	White/Blue
–		2	Orange/White	27	White/Orange
2	Trunk	3	Green/White	28	White/Green
–		4	Brown/White	29	White/Brown
3	Trunk	5	Slate/White	30	White/Slate
–		6	Blue/Red	31	Red/Blue
4	Trunk	7	Orange/Red	32	Red/Orange
–		8	Green/Red	33	Red/Green
5		9	Brown/Red	34	Red/Brown
–		10	Slate/Red	35	Red/Slate
6	Trunk	11	Blue/Black	36	Black/Blue
–		12	Orange/Black	37	Black/Orange
7	Trunk	13	Green/Black	38	Black/Green

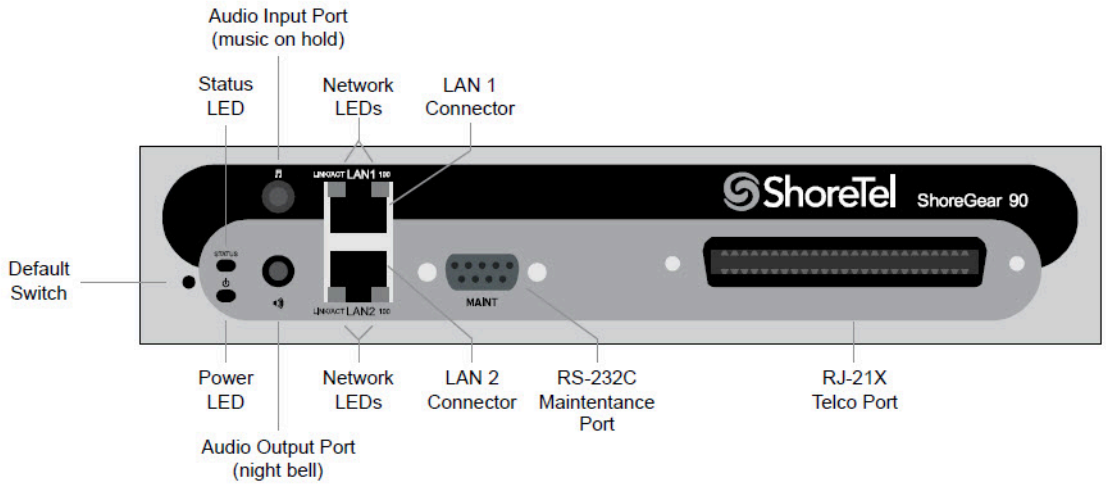
Port	Type	Ring		Tip	
		Pin #	Cable Color	Pin #	Cable Color
–		14	Brown/Black	39	Black/Brown
8	Trunk	15	Slate/Black	40	Black/Slate
–		16	Blue/Yellow	41	Yellow/Blue
9	Extension - DID	17	Orange/Yellow	42	Yellow/Orange
–		18	Green/Yellow	43	Yellow/Green
10	Extension - DID	19	Brown/Yellow	44	Yellow/Brown
13	Extension - DID	20	Slate/Yellow	45	Yellow/Slate
11	Extension - DID	21	Blue/Violet	46	Violet/Blue
14	Extension - DID	22	Orange/Violet	47	Violet/Orange
12	Extension - DID	23	Green/Violet	48	Violet/Green
–		24	Brown/Violet	49	Violet/Brown
–		25	Slate/Violet	50	Violet/Slate

23.5 Specifications – SG 1-U Half-Width Switches

23.5.1 SG90 Voice Switch

The following sections describe SG90 resource capacity, LED behavior, and connectors. The SG90 is not supported in installations outside the U.S. and Canada. SG90 Front Plate figure displays the SG90 front plate.

Figure 38: SG90 Front Plate



23.5.1.1 Switch Capacity

- Analog Circuit Resources
  - Ports 1-8: Eight Loop Start Trunks
  - Ports 9-12: Four Extensions or DID Trunks. A single command configures all ports as either Extensions or DID trunks.
  - Power Failure Transfer Unit: Trunk Port 1 to Extension Port 12
- Make Me Conference Resources: 12 ports
  - Ports 1-12
- Maximum IP Phone Resources: 90 devices
  - Analog Port Reallocation: 60
  - Built-in Resources: 30

23.5.1.2 LED Descriptions

Power LED

The SG90 has one power LED, which indicates the following:

- On: The switch is operating normally.

- Off: The switch has no power.
- Flashing:
  - 2 flashes — The switch failed its internal self-test. This indicates a hardware failure. Replace the unit and submit a Return Material Authorization (RMA) to Mitel.
  - 3 flashes — Booting through FTP. Flash memory might be corrupted. Use the pages available through the Maintenance menu in Connect Director to check and ensure that the system is running properly.
  - 4 flashes — The IP address is unavailable. DHCP did not respond to the IP address request, and the IP address is not available in nonvolatile memory to continue boot process. The switch will automatically reboot in five seconds and try again. Check the DHCP server and the network configuration to ensure that the voice switch is receiving a valid IP address.
  - 5 flashes — The operating system is not available. The switch is booting from FTP, but cannot find the boot files. The switch automatically reboots in 5 seconds. You can use DHCP to tell the switch where the files are. If you are using a DHCP server that supports options 66 and 67, set option 66 to the MiVoice Connect server's IP address, and set option 67 to /tsk/vxworks.
  - 6 flashes — Using a previously stored IP address. A DHCP transaction was attempted, but the DHCP server did not respond. The switch continues to use the IP address stored in nonvolatile memory until it receives a valid response. If the switch receives a response that provides a different IP address, it reboots using the new IP address. If the switch receives a response that matches the IP address stored in nonvolatile memory, it continues operation, and the power LED stops flashing. If the problem persists, check the DHCP server and network configuration.

23.5.1.2.1 Network LEDs

The SG90 network LEDs (LAN1 and LAN2) indicate the speed at which the switch is communicating with the network and whether there is network activity.

The network LED descriptions are as follows:

- Link/Activity: When lit, this LED indicates that the switch is connected to an Ethernet network. This LED indicates network activity, as follows:
  - When flashing, network activity is detected.
  - When on (not flashing), the switch is connected to an Ethernet network.
  - When off, the switch cannot detect an Ethernet network.

  This LED is not directly related to any switch's individual network activity. For example, if three switches are connected to the same hub and one switch's Traffic LED shows activity, the other switches will indicate the same activity.
- 100M
  - When green, the switch is connected to a 100BaseT network.
  - When off, the switch is connected to a 10BaseT network.

23.5.1.2.2 Status LED

The SG90 has one status LED to provide general information about the ports. The color and blink pattern of the LED indicate the port function:

- Status LED (Green)
  - When on steady, no ports are handling active calls.
  - When flashing fast, at least one port is handling an active call.
- Status LED (Yellow)
  - When on steady, no ports are handling active calls and at least one port is out of service.
  - When flashing slow, the switch is not connected (or has lost connection) to a MiVoice Connect server.
  - When flashing fast, at least one port is handling an active call and at least one port is out of service.
- Off: No ports are assigned.

23.5.1.3 SG90 Connectors

The SG90 voice switch contains the following components:

- 1 3.5 mm mono connector for audio input (music on hold)
- 1 3.5 mm mono connector for audio output (overhead paging and night bell)
- 1 DB-9 socket connector for maintenance
- 2 RJ-45 connectors for the LAN interface
- 1 RJ-21X plug connector for mass termination of the telephone/trunk ports
  - Power Failure Transfer Unit: Trunk Port 1 to Extension Port 12
  - Backup Operator: Extension Port 12

23.5.1.3.1 SG90 RJ-21X Telephone and Trunk Connector

SG90 RJ-21X Telephone and Trunk Connector lists the RJ-21X Ring and Tip pin numbers for the SG90.

Table 61: SG90 RJ-21X Telephone and Trunk Connector

Port	Type	Ring		Tip	
		Pin #	Cable Color	Pin #	Cable Color
1	Trunk	1	Blue/White	26	White/Blue
–		2	Orange/White	27	White/Orange
2	Trunk	3	Green/White	28	White/Green
–		4	Brown/White	29	White/Brown

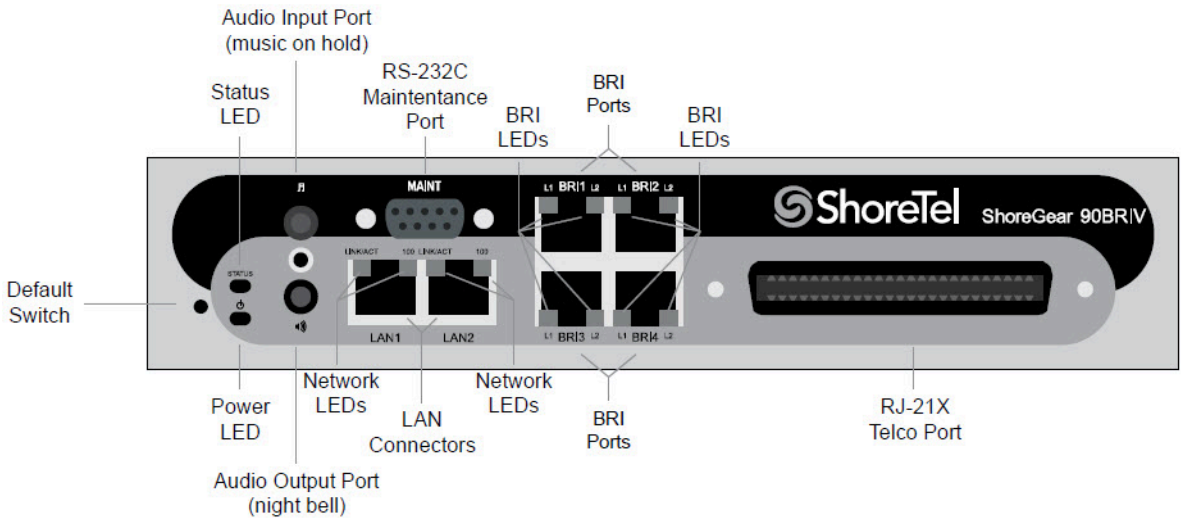
Port	Type	Ring		Tip	
		Pin #	Cable Color	Pin #	Cable Color
3	Trunk	5	Slate/White	30	White/Slate
–		6	Blue/Red	31	Red/Blue
4	Trunk	7	Orange/Red	32	Red/Orange
–		8	Green/Red	33	Red/Green
5		9	Brown/Red	34	Red/Brown
–		10	Slate/Red	35	Red/Slate
6		11	Blue/Black	36	Black/Blue
–		12	Orange/Black	37	Black/Orange
7		13	Green/Black	38	Black/Green
–		14	Brown/Black	39	Black/Brown
8		15	Slate/Black	40	Black/Slate
–		16	Blue/Yellow	41	Yellow/Blue
9	Extension - DID	17	Orange/Yellow	42	Yellow/Orange
–		18	Green/Yellow	43	Yellow/Green
10	Extension - DID	19	Brown/Yellow	44	Yellow/Brown
–		20	Slate/Yellow	45	Yellow/Slate

Port	Type	Ring		Tip	
		Pin #	Cable Color	Pin #	Cable Color
11	Extension - DID	21	Blue/Violet	46	Violet/Blue
–		22	Orange/Violet	47	Violet/Orange
12	Extension - DID	23	Green/Violet	48	Violet/Green
–		24	Brown/Violet	49	Violet/Brown
–		25	Slate/Violet	50	Violet/Slate

23.5.2 SG90BRI Voice Switch

The following sections describe SG90BRI resource capacity, LED behavior, and connectors. SG90BRI Front Plate displays the SG90BRI front plate.

Figure 39: SG90BRI Front Plate



23.5.2.1 Switch Capacity

Switch Capacity

- Analog Circuit Resources
  - Ports 9-12: Extensions
- Digital Circuit Resources
  - Four BRI Spans, each comprising two channels: Eight channels maximum
- Make Me Conference Resource: None
- Maximum IP Phone Resources: 90 devices
  - Analog Port Reallocation: 20
  - Digital Channel Reallocation: 40
  - Built-in Resources: 30

23.5.2.2 LED Descriptions

Power LED

The SG90BRI has one power LED, which indicates the following:

- On: The switch is operating normally.
- Off: The switch has no power.
- Flashing:
  - 2 flashes — The switch failed its internal self-test. This indicates a hardware failure; replace the unit and submit a Return Material Authorization (RMA) to Mitel.
  - 3 flashes — Booting through FTP. Flash memory might be corrupted. Use the pages available through the Maintenance menu in Connect Director to check and ensure that the system is running properly.
  - 4 flashes — The IP address is unavailable. DHCP did not respond to the IP address request, and the IP address is not available in nonvolatile memory to continue boot process. The switch will automatically reboot in five seconds and try again. Check the DHCP server and the network configuration to ensure that the voice switch is receiving a valid IP address.
  - 5 flashes — The operating system is not available. The switch is booting from FTP, but cannot find the boot files. The switch automatically reboots in 5 seconds. You can use DHCP to tell the switch where the files are. If you are using a DHCP server that supports options 66 and 67, set option 66 to the MiVoice Connect server's IP address, and set option 67 to /tsk/vxworks.
  - 6 flashes — Using a previously stored IP address. A DHCP transaction was attempted, but the DHCP server did not respond. The switch continues to use the IP address stored in nonvolatile memory until it receives a valid response. If the switch receives a response that provides a different IP address, it reboots using the new IP address. If the switch receives a response that matches the IP address stored in nonvolatile memory, it continues operation, and the power LED stops flashing. If the problem persists, check the DHCP server and network configuration.

23.5.2.2.1 Network LEDs

The SG90BRI network LEDs (LAN1 and LAN2) indicate the speed at which the switch is communicating with the network and whether there is network activity.

The network LED descriptions are as follows:

- Link/Activity: When lit, this LED indicates that the switch is connected to an Ethernet network. This LED indicates network activity, as follows:
  - When flashing, network activity is detected.
  - When on (not flashing), the switch is connected to an Ethernet network.
  - When off, the switch cannot detect an Ethernet network.

  This LED is not directly related to any switch's individual network activity. For example, if three switches are connected to the same hub and one switch's Traffic LED shows activity, the other switches will indicate the same activity.
- 100M
  - When green, the switch is connected to a 100BaseT network.
  - When off, the switch is connected to a 10BaseT network.

23.5.2.2.2 Status LED

The SG90BRI has one status LED to provide general information about the ports. The color and blink pattern of the LED indicate the port function:

- Status LED (Green)
  - When on steady, no ports are handling active calls.
  - When flashing fast (100 msec on/off), at least one port is handling an active call.
- Status LED (Yellow)
  - When on steady, no ports are handling active calls and at least one port is out of service.
  - When flashing slow (1 sec. on/off), the switch is not connected (or has lost connection) to a MiVoice Connect server.
  - When flashing fast (100 msec on/off), at least one port is handling an active call and at least one port is out of service.
- Off: No ports are assigned.

23.5.2.2.3 BRI LED

Each BRI connector has two LEDs to indicate port activity. The color and blink pattern of the LED indicate the port function:

- LED 1: Off, LED 2 Off – Port not configured in Director
- LED 1: Yellow, LED 2 Off – Port inactive or not connected
- LED 1: Off, LED 2 Off – Layer 1 active. Layer 2 not established
- LED 1: Off, LED 2 Green – Layer 1 active. Layer 2 active.
- LED 1: Off, LED 2 Green flashing – Call in progress (Layer 1, Layer 2, and Layer 3 active).

23.5.2.3 SG90BRI Connectors

The SG90BRI voice switch contains the following components:

- 1 3.5 mm mono connector for audio input (music on hold)

- 1 3.5 mm mono connector for audio output (overhead paging and night bell)
- 1 DB-9 socket connector for maintenance
- 2 RJ-45 connectors for the LAN interface
- 1 RJ-21X plug connector for mass termination of the telephone/trunk ports
- 4 RJ-45 SGT1 telco port

23.5.2.4 SG90BRI RJ-21X Telephone and Trunk Connector

SG90BRI RJ-21X Telephone and Trunk Connector Pins lists the RJ-21X Ring and Tip pin numbers for the SG90BRI.

Table 62: SG90BRI RJ-21X Telephone and Trunk Connector Pins

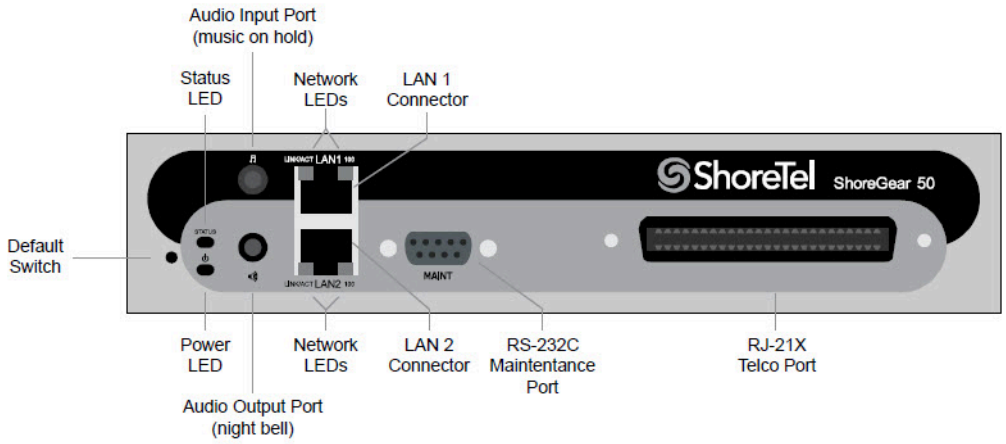
Port	Type	Ring		Tip	
		Pin #	Cable Color	Pin #	Cable Color
–	Trunk	1	Blue/White	26	White/Blue
–		2	Orange/White	27	White/Orange
–	Trunk	3	Green/White	28	White/Green
–		4	Brown/White	29	White/Brown
–	Trunk	5	Slate/White	30	White/Slate
–		6	Blue/Red	31	Red/Blue
–	Trunk	7	Orange/Red	32	Red/Orange
–		8	Green/Red	33	Red/Green
–		9	Brown/Red	34	Red/Brown
–		10	Slate/Red	35	Red/Slate
–		11	Blue/Black	36	Black/Blue

Port	Type	Ring		Tip	
		Pin #	Cable Color	Pin #	Cable Color
–		12	Orange/Black	37	Black/Orange
–		13	Green/Black	38	Black/Green
–		14	Brown/Black	39	Black/Brown
–		15	Slate/Black	40	Black/Slate
–		16	Blue/Yellow	41	Yellow/Blue
9	Extension - DID	17	Orange/Yellow	42	Yellow/Orange
–		18	Green/Yellow	43	Yellow/Green
10	Extension - DID	19	Brown/Yellow	44	Yellow/Brown
–		20	Slate/Yellow	45	Yellow/Slate
11	Extension - DID	21	Blue/Violet	46	Violet/Blue
–		22	Orange/Violet	47	Violet/Orange
12	Extension - DID	23	Green/Violet	48	Violet/Green
–		24	Brown/Violet	49	Violet/Brown
–		25	Slate/Violet	50	Violet/Slate

23.5.3 SG50 Voice Switch

The following sections describe SG50 resource capacity, LED behavior, and connectors. The SG50 is not supported in installations outside the U.S. and Canada. SG50 Front Plate displays the SG50 front plate.

Figure 40: SG50 Front Plate



23.5.3.1 Switch Capacity

- Analog Circuit Resources
  - Ports 1-4: Four Loop Start Trunks
  - Ports 11-12: Two Extensions or DID Trunks. A single command configures all ports as either Extensions or DID trunks.
  - Power Failure Transfer Unit: Trunk Port 1 to Extension Port 12
- Make Me Conference Resources: six ports
  - Ports 1-4, 11-12
- Maximum IP Phone Resources: 50 devices
  - Analog Port Reallocation: 30
  - Built-in Resources: 20

23.5.3.2 LED Descriptions

Power LED

The SG50 has one power LED, which indicates the following:

- On: The switch is operating normally.
- Off: The switch has no power.

- Flashing:
  - 2 flashes — The switch failed its internal self-test. This indicates a hardware failure; replace the unit and submit a Return Material Authorization (RMA) to Mitel.
  - 3 flashes — Booting through FTP. Flash memory might be corrupted. Use the pages available through the Maintenance menu in Connect Director to check and ensure that the system is running properly.
  - 4 flashes — The IP address is unavailable. DHCP did not respond to the IP address request, and the IP address is not available in nonvolatile memory to continue boot process. The switch will automatically reboot in five seconds and try again. Check the DHCP server and the network configuration to ensure that the voice switch is receiving a valid IP address.
  - 5 flashes — The operating system is not available. The switch is booting from FTP, but cannot find the boot files. The switch automatically reboots in 5 seconds. You can use DHCP to tell the switch where the files are. If you are using a DHCP server that supports options 66 and 67, set option 66 to the MiVoice Connect server's IP address, and set option 67 to /tsk/vxworks.
  - 6 flashes — Using a previously stored IP address. A DHCP transaction was attempted, but the DHCP server did not respond. The switch continues to use the IP address stored in nonvolatile memory until it receives a valid response. If the switch receives a response that provides a different IP address, it reboots using the new IP address. If the switch receives a response that matches the IP address stored in nonvolatile memory, it continues operation, and the power LED stops flashing. If the problem persists, check the DHCP server and network configuration.

23.5.3.2.1 Network LEDs

The SG50 network LEDs (LAN1 and LAN2) indicate the speed at which the switch is communicating with the network and whether there is network activity.

The network LED descriptions are as follows:

- Link/Activity: When lit, this LED indicates that the switch is connected to an Ethernet network. This LED indicates network activity, as follows:
  - When flashing, network activity is detected.
  - When on (not flashing), the switch is connected to an Ethernet network.
  - When off, the switch cannot detect an Ethernet network.

  This LED is not directly related to any switch's individual network activity. For example, if three switches are connected to the same hub and one switch's Traffic LED shows activity, the other switches will indicate the same activity.
- 100M
  - When green, the switch is connected to a 100BaseT network.
  - When off, the switch is connected to a 10BaseT network.

23.5.3.2.2 Status LED

The SG50 has one status LED to provide general information about the ports. The color and blink pattern of the LED indicate the port function:

- Status LED (Green)
  - When on steady, no ports are handling active calls.
  - When flashing fast, at least one port is handling an active call.
- Status LED (Yellow)
  - When on steady, no ports are handling active calls and at least one port is out of service.
  - When flashing slow, the switch is not connected (or has lost connection) to a MiVoice Connect server.
  - When flashing fast, at least one port is handling an active call and at least one port is out of service.
- Off: No ports are assigned.

23.5.3.3 SG50 Connectors

The SG50 voice switch contains the following components:

- 1 3.5 mm mono connector for audio input (music on hold)
- 1 3.5 mm mono connector for audio output (overhead paging and night bell)
- 1 DB-9 socket connector for maintenance
- 2 RJ-45 connectors for the LAN interface
- 1 RJ-21X plug connector for mass termination of the telephone/trunk ports
  - Power Failure Transfer Unit: Trunk Port 1 to Extension Port 12
  - Backup Operator: Extension Port 12

23.5.3.4 SG50 RJ-21X Telephone and Trunk Connector

SG50 RJ-21X Telephone and Trunk Connector Pins lists the RJ-21X Ring and Tip pin numbers for the SG50.

Table 63: SG50 RJ-21X Telephone and Trunk Connector Pins

Port	Type	Ring		Tip	
		Pin #	Cable Color	Pin #	Cable Color
1	Trunk	1	Blue/White	26	White/Blue
–		2	Orange/White	27	White/Orange
2	Trunk	3	Green/White	28	White/Green
–		4	Brown/White	29	White/Brown

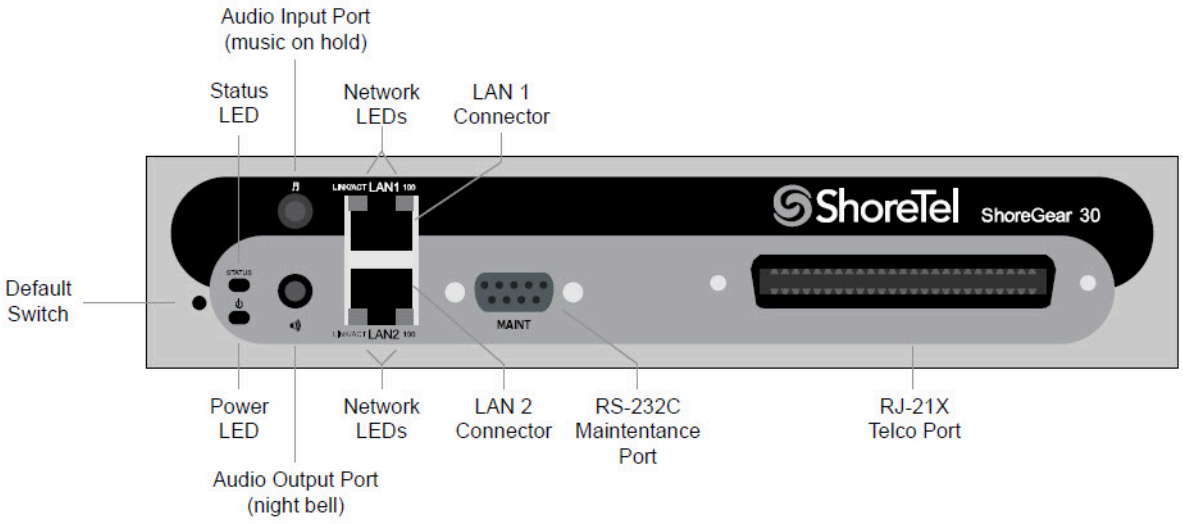
Port	Type	Ring		Tip	
		Pin #	Cable Color	Pin #	Cable Color
3	Trunk	5	Slate/White	30	White/Slate
–		6	Blue/Red	31	Red/Blue
4	Trunk	7	Orange/Red	32	Red/Orange
–		8	Green/Red	33	Red/Green
5		9	Brown/Red	34	Red/Brown
–		10	Slate/Red	35	Red/Slate
6		11	Blue/Black	36	Black/Blue
–		12	Orange/Black	37	Black/Orange
7		13	Green/Black	38	Black/Green
–		14	Brown/Black	39	Black/Brown
8		15	Slate/Black	40	Black/Slate
–		16	Blue/Yellow	41	Yellow/Blue
9	Extension - DID	17	Orange/Yellow	42	Yellow/Orange
–		18	Green/Yellow	43	Yellow/Green
10	Extension - DID	19	Brown/Yellow	44	Yellow/Brown
–		20	Slate/Yellow	45	Yellow/Slate

Port	Type	Ring		Tip	
		Pin #	Cable Color	Pin #	Cable Color
11	Extension - DID	21	Blue/Violet	46	Violet/Blue
–		22	Orange/Violet	47	Violet/Orange
12	Extension - DID	23	Green/Violet	48	Violet/Green
–		24	Brown/Violet	49	Violet/Brown
–		25	Slate/Violet	50	Violet/Slate

23.5.4 SG30 Voice Switch

The following sections describe SG30 resource capacity, LED behavior, and connectors. The SG30 is not supported in installations outside the U.S. and Canada. SG30 Front Plate displays the SG30 front plate.

Figure 41: SG30 Front Plate



23.5.4.1 Switch Capacity

- Analog Circuit Resources
  - Ports 1-2: Two Loop Start Trunks
  - Ports 11-12: Two Extensions or DID Trunks. A single command configures all ports as either Extensions or DID trunks
  - Power Failure Transfer Unit: Trunk Port 1 to Extension Port 12
- Make Me Conference Resources: none
- Maximum IP Phone Resources: none
  - Analog Port Reallocation: 20
  - Built-in Resources: 10

23.5.4.2 LED Descriptions

Power LED

The SG30 has one power LED, which indicates the following:

- On: The switch is operating normally.
- Off: The switch has no power.
- Flashing:
  - 2 flashes — The switch failed its internal self-test. This indicates a hardware failure. Replace the unit and submit a Return Material Authorization (RMA) to Mitel.
  - 3 flashes — Booting through FTP. Flash memory might be corrupted. Use the pages available through the Maintenance menu in Connect Director to check and ensure that the system is running properly.
  - 4 flashes — The IP address is unavailable. DHCP did not respond to the IP address request, and the IP address is not available in nonvolatile memory to continue boot process. The switch will automatically reboot in five seconds and try again. Check the DHCP server and the network configuration to ensure that the voice switch is receiving a valid IP address.
  - 5 flashes — The operating system is not available. The switch is booting from FTP, but cannot find the boot files. The switch automatically reboots in 5 seconds. You can use DHCP to tell the switch where the files are. If you are using a DHCP server that supports options 66 and 67, set option 66 to the MiVoice Connect server's IP address, and set option 67 to /tsk/vxworks.
  - 6 flashes — Using a previously stored IP address. A DHCP transaction was attempted, but the DHCP server did not respond. The switch continues to use the IP address stored in nonvolatile memory until it receives a valid response. If the switch receives a response that provides a different IP address, it reboots using the new IP address. If the switch receives a response that matches the IP address stored in nonvolatile memory, it continues operation, and the power LED stops flashing. If the problem persists, check the DHCP server and network configuration.

23.5.4.2.1 Network LEDs

The SG30 network LEDs (LAN1 and LAN2) indicate the speed at which the switch is communicating with the network and whether there is network activity.

The network LED descriptions are as follows:

- Link/Activity: When lit, this LED indicates that the switch is connected to an Ethernet network. This LED indicates network activity, as follows:
  - When flashing, network activity is detected.
  - When on (not flashing), the switch is connected to an Ethernet network.
  - When off, the switch cannot detect an Ethernet network.

  This LED is not directly related to any switch's individual network activity. For example, if three switches are connected to the same hub and one switch's Traffic LED shows activity, the other switches will indicate the same activity.
- 100M
  - When green, the switch is connected to a 100BaseT network.
  - When off, the switch is connected to a 10BaseT network.

23.5.4.2.2 Status LED

The SG30 has one status LED to provide general information about the ports. The color and blink pattern of the LED indicate the port function:

- Status LED (Green)
  - When on steady, no ports are handling active calls.
  - When flashing fast, at least one port is handling an active call.
- Status LED (Yellow)
  - When on steady, no ports are handling active calls and at least one port is out of service.
  - When flashing slow, the switch is not connected (or has lost connection) to a MiVoice Connect server.
  - When flashing fast, at least one port is handling an active call and at least one port is out of service.
- Off: No ports are assigned.

23.5.4.3 SG30 Connectors

The SG30 voice switch contains the following components:

- 1 3.5 mm mono connector for audio input (music on hold)
- 1 3.5 mm mono connector for audio output (overhead paging and night bell)
- 1 DB-9 socket connector for maintenance
- 2 RJ-45 connectors for the LAN interface
- 1 RJ-21X plug connector for mass termination of the telephone/trunk ports
- Power Failure Transfer Unit: Trunk Port 1 to Extension Port 12
- Backup Operator: Extension Port 12

23.5.4.4 SG30 RJ-21X Telephone and Trunk Connector

SG30 RJ-21X Telephone and Trunk Connector Pins lists the RJ-21X Ring and Tip pin numbers for the SG30.

Table 64: SG30 RJ-21X Telephone and Trunk Connector Pins

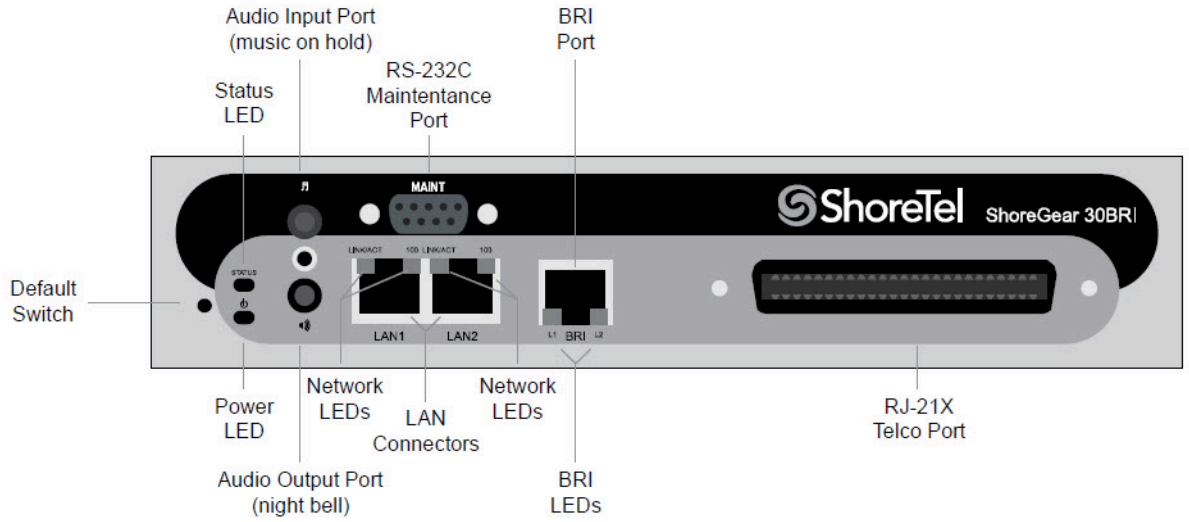
Port	Type	Ring		Tip	
		Pin #	Cable Color	Pin #	Cable Color
1	Trunk	1	Blue/White	26	White/Blue
–		2	Orange/White	27	White/Orange
2	Trunk	3	Green/White	28	White/Green
–		4	Brown/White	29	White/Brown
–	Trunk	5	Slate/White	30	White/Slate
–		6	Blue/Red	31	Red/Blue
–	Trunk	7	Orange/Red	32	Red/Orange
–		8	Green/Red	33	Red/Green
–		9	Brown/Red	34	Red/Brown
–		10	Slate/Red	35	Red/Slate
–		11	Blue/Black	36	Black/Blue
–		12	Orange/Black	37	Black/Orange
–		13	Green/Black	38	Black/Green

Port	Type	Ring		Tip	
		Pin #	Cable Color	Pin #	Cable Color
–		14	Brown/Black	39	Black/Brown
–		15	Slate/Black	40	Black/Slate
–		16	Blue/Yellow	41	Yellow/Blue
–		17	Orange/Yellow	42	Yellow/Orange
–		18	Green/Yellow	43	Yellow/Green
–		19	Brown/Yellow	44	Yellow/Brown
–		20	Slate/Yellow	45	Yellow/Slate
11	Extension - DID	21	Blue/Violet	46	Violet/Blue
–		22	Orange/Violet	47	Violet/Orange
12	Extension - DID	23	Green/Violet	48	Violet/Green
–		24	Brown/Violet	49	Violet/Brown
–		25	Slate/Violet	50	Violet/Slate

23.5.5 SG30BRI Voice Switch

The following sections describe SG30BRI resource capacity, LED behavior, and connectors. SG30BRI Front Plate displays the SG30BRI front plate.

Figure 42: SG30BRI Front Plate



23.5.5.1 Switch Capacity

- Analog Circuit Resources
  - Ports 11-12: Extensions
- Digital Circuit Resources
  - One BRI Span comprising two channels: two channels maximum
- Make Me Conference Resource: None
- Maximum IP Phone Resources: 30 devices
  - Analog Port Reallocation: 10
  - Digital Channel Reallocation: 10
  - Built-in Resources: 10

23.5.5.2 LED Descriptions

Power LED

The SG30BRI has one power LED, which indicates the following:

- On: The switch is operating normally.
- Off: The switch has no power.
- Flashing:
  - 2 flashes — The switch failed its internal self-test. This indicates a hardware failure. Replace the unit and submit a Return Material Authorization (RMA) to Mitel.
  - 3 flashes — Booting through FTP. Flash memory might be corrupted. Use the pages available through the Maintenance menu in Connect Director to check and ensure that the system is running properly.
  - 4 flashes — The IP address is unavailable. DHCP did not respond to the IP address request, and the IP address is not available in nonvolatile memory to continue boot process. The switch

will automatically reboot in five seconds and try again. Check the DHCP server and the network configuration to ensure that the voice switch is receiving a valid IP address.

- 5 flashes — The operating system is not available. The switch is booting from FTP, but cannot find the boot files. The switch automatically reboots in 5 seconds. You can use DHCP to tell the switch where the files are. If you are using a DHCP server that supports options 66 and 67, set option 66 to the MiVoice Connect server's IP address, and set option 67 to /tsk/vxworks.
- 6 flashes — Using a previously stored IP address. A DHCP transaction was attempted, but the DHCP server did not respond. The switch continues to use the IP address stored in nonvolatile memory until it receives a valid response. If the switch receives a response that provides a different IP address, it reboots using the new IP address. If the switch receives a response that matches the IP address stored in nonvolatile memory, it continues operation, and the power LED stops flashing. If the problem persists, check the DHCP server and network configuration.

23.5.5.2.1 Network LEDs

The SG30BRI network LEDs (LAN1 and LAN2) indicate the speed at which the switch is communicating with the network and whether there is network activity.

The network LED descriptions are as follows:

- Link/Activity: When lit, this LED indicates that the switch is connected to an Ethernet network. This LED indicates network activity, as follows:
  - When flashing, network activity is detected.
  - When on (not flashing), the switch is connected to an Ethernet network.
  - When off, the switch cannot detect an Ethernet network.

  This LED is not directly related to any switch's individual network activity. For example, if three switches are connected to the same hub and one switch's Traffic LED shows activity, the other switches will indicate the same activity.
- 100M
  - When green, the switch is connected to a 100BaseT network.
  - When off, the switch is connected to a 10BaseT network.

23.5.5.2.2 Status LED

The SG30BRI has one status LED to provide general information about the ports. The color and blink pattern of the LED indicate the port function:

- Status LED (Green)
  - When on steady, no ports are handling active calls.
  - When flashing fast (100 msec on/off), at least one port is handling an active call.
- Status LED (Yellow)
  - When on steady, no ports are handling active calls and at least one port is out of service.
  - When flashing slow (1 sec. on/off), the switch is not connected (or has lost connection) to a MiVoice Connect server.
  - When flashing fast (100 msec on/off), at least one port is handling an active call and at least one port is out of service.

- Off: No ports are assigned.

23.5.5.2.3 BRI LED

Each BRI connector has two LEDs to indicate port activity. The color and blink pattern of the LED indicate the port function:

- LED 1: Off, LED 2 Off – Port not configured in Director
- LED 1: Yellow, LED 2 Off – Port inactive or not connected
- LED 1: Off, LED 2 Off – Layer 1 active. Layer 2 not established
- LED 1: Off, LED 2 Green – Layer 1 active. Layer 2 active.
- LED 1: Off, LED 2 Green flashing – Call in progress (Layer 1, Layer 2, and Layer 3 active).

23.5.5.3 SG30BRI Connectors

The SG30BRI voice switch contains the following components:

- 1 3.5 mm mono connector for audio input (music on hold)
- 1 3.5 mm mono connector for audio output (overhead paging and night bell)
- 1 DB-9 socket connector for maintenance
- 2 RJ-45 connectors for the LAN interface
- 1 RJ-21X plug connector for mass termination of the telephone/trunk ports
- 4 RJ-45 SGT1 telco port

23.5.5.4 SG30BRI RJ-21X Telephone and Trunk Connector

SG30BRI RJ-21X Telephone and Trunk Connector Pins lists the RJ-21X Ring and Tip pin numbers for the SG30BRI.

Table 65: SG30BRI RJ-21X Telephone and Trunk Connector Pins

Port	Type	Ring		Tip	
		Pin #	Cable Color	Pin #	Cable Color
–		1	Blue/White	26	White/Blue
–		2	Orange/White	27	White/Orange
–		3	Green/White	28	White/Green
–		4	Brown/White	29	White/Brown

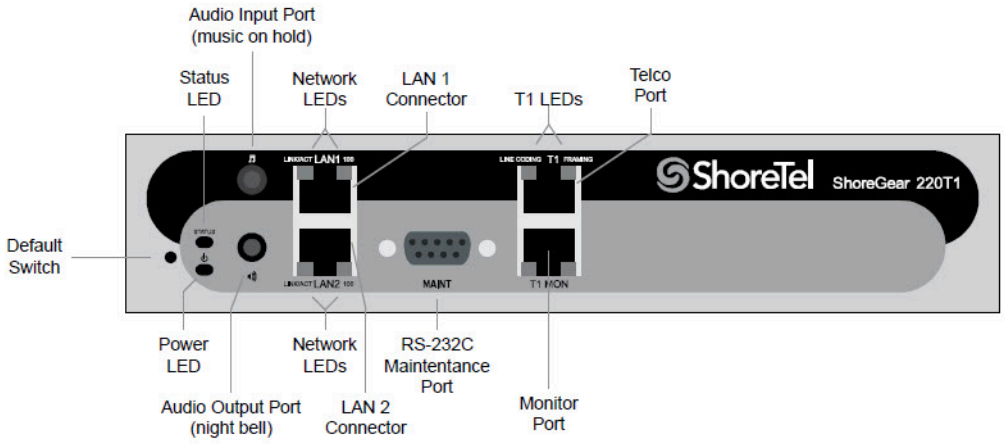
Port	Type	Ring		Tip	
		Pin #	Cable Color	Pin #	Cable Color
–		5	Slate/White	30	White/Slate
–		6	Blue/Red	31	Red/Blue
–		7	Orange/Red	32	Red/Orange
–		8	Green/Red	33	Red/Green
–		9	Brown/Red	34	Red/Brown
–		10	Slate/Red	35	Red/Slate
–		11	Blue/Black	36	Black/Blue
–		12	Orange/Black	37	Black/Orange
–		13	Green/Black	38	Black/Green
–		14	Brown/Black	39	Black/Brown
–		15	Slate/Black	40	Black/Slate
–		16	Blue/Yellow	41	Yellow/Blue
–		17	Orange/Yellow	42	Yellow/Orange
–		18	Green/Yellow	43	Yellow/Green
–		19	Brown/Yellow	44	Yellow/Brown
–		20	Slate/Yellow	45	Yellow/Slate

Port	Type	Ring		Tip	
		Pin #	Cable Color	Pin #	Cable Color
11	Extension	21	Blue/Violet	46	Violet/Blue
–		22	Orange/Violet	47	Violet/Orange
12	Extension	23	Green/Violet	48	Violet/Green
–		24	Brown/Violet	49	Violet/Brown
–		25	Slate/Violet	50	Violet/Slate

23.5.6 SG220T1 Voice Switch

The following sections describe SG220T1 resource capacity, LED behavior, and connectors. The SG220T1 is not supported in installations outside the U.S. and Canada. SG220T1 Front Plate displays the SG220T1 front plate

Figure 43: SG220T1 Front Plate



23.5.6.1 Switch Capacity

- Digital Circuit Resources: 24 channels maximum
  - One SGT1 circuit, 24 channels per circuit: 24 channels maximum
- Make Me Conference Resource: None

- Maximum IP Phone Resources: 220
  - Digital Channel Reallocation: 120
  - Built-in Resources: 100
  - SIP Media Proxies: 20

23.5.6.2 LED Descriptions

Power LED

The SG220T1 has one power LED, which indicates the following:

- On: The switch is operating normally.
- Off: The switch has no power.
- Flashing:
  - 2 flashes — The switch failed its internal self-test. This indicates a hardware failure. Replace the unit and submit a Return Material Authorization (RMA) to Mitel.
  - 3 flashes — Booting through FTP. Flash memory might be corrupted. Use the pages available through the Maintenance menu in Connect Director to check and ensure that the system is running properly.
  - 4 flashes — The IP address is unavailable. DHCP did not respond to the IP address request, and the IP address is not available in nonvolatile memory to continue boot process. The switch will automatically reboot in five seconds and try again. Check the DHCP server and the network configuration to ensure that the voice switch is receiving a valid IP address.
  - 5 flashes — The operating system is not available. The switch is booting from FTP, but cannot find the boot files. The switch automatically reboots in 5 seconds. You can use DHCP to tell the switch where the files are. If you are using a DHCP server that supports options 66 and 67, set option 66 to the MiVoice Connect server's IP address, and set option 67 to /tsk/vxworks.
  - 6 flashes — Using a previously stored IP address. A DHCP transaction was attempted, but the DHCP server did not respond. The switch continues to use the IP address stored in nonvolatile memory until it receives a valid response. If the switch receives a response that provides a different IP address, it reboots using the new IP address. If the switch receives a response that matches the IP address stored in nonvolatile memory, it continues operation, and the power LED stops flashing. If the problem persists, check the DHCP server and network configuration.

23.5.6.2.1 Network LEDs

The SG220T1 network LEDs (LAN1 and LAN2) indicate the speed at which the switch is communicating with the network and whether there is network activity.

The network LED descriptions are as follows:

- Link/Activity: When lit, this LED indicates that the switch is connected to an Ethernet network. This LED indicates network activity, as follows:
  - When flashing, network activity is detected.
  - When on (not flashing), the switch is connected to an Ethernet network.
  - When off, the switch cannot detect an Ethernet network.

  This LED is not directly related to any switch's individual network activity. For example, if three switches are connected to the same hub and one switch's Traffic LED shows activity, the other switches will indicate the same activity.
- 100M
  - When green, the switch is connected to a 100BaseT network.
  - When off, the switch is connected to a 10BaseT network.

23.5.6.2.2 Status LED

The SG220T1 has one status LED to provide general information about the ports. The color and blink pattern of the LED indicate the port function:

- Status LED (Green)
  - When on steady, no ports are handling active calls.
  - When flashing fast, at least one port is handling an active call.
- Status LED (Yellow)
  - When on steady, no ports are handling active calls and at least one port is out of service.
  - When flashing slow, the switch is not connected (or has lost connection) to a MiVoice Connect server.
  - When flashing fast, at least one port is handling an active call and at least one port is out of service.
- Off: No ports are assigned.

23.5.6.2.3 Monitor and Telco LEDs

The Monitor and Telco LEDs indicate line coding, network framing, and loopback status. These LEDs are color coded—green, yellow, and red. The Monitor and Telco LED descriptions follow.

Telco and Monitor LED alarms and errors are logged as switch events in Connect Director's event log.

- Line Coding: This LED indicates line coding status, as follows:
  - When green, the line coding signal is good.
  - When yellow, bipolar violations (BPV) are being received at one second intervals.
  - When red, a loss of signal (LOS) has occurred.
  - When flashing red, loopback is active (local or CO).
  - When off, the switch has no power.

- Framing: This LED indicates network framing status, as follows:
  - When green, the SGT1/SGE1 signal is in frame; the signal is synchronized.
  - When yellow, a yellow alarm has been received from the Central Office.
  - When flashing yellow, the frame-bit error rate has exceeded its limits. A small number of frame-bit errors (>1 per million) have occurred; this state will take up to 10 minutes to clear.
  - When flashing fast yellow, a series of frame-bit errors (>1 per 1000) have occurred.
  - When red, the SGT1/SGE1 signal is out-of-frame (OOF). The received signal cannot be framed to the Extended Superframe (ESF) or D4 format.
  - When flashing red, loopback is active (local or CO).
  - When off, the switch has no power.

23.5.6.3 SG220T1 Connectors

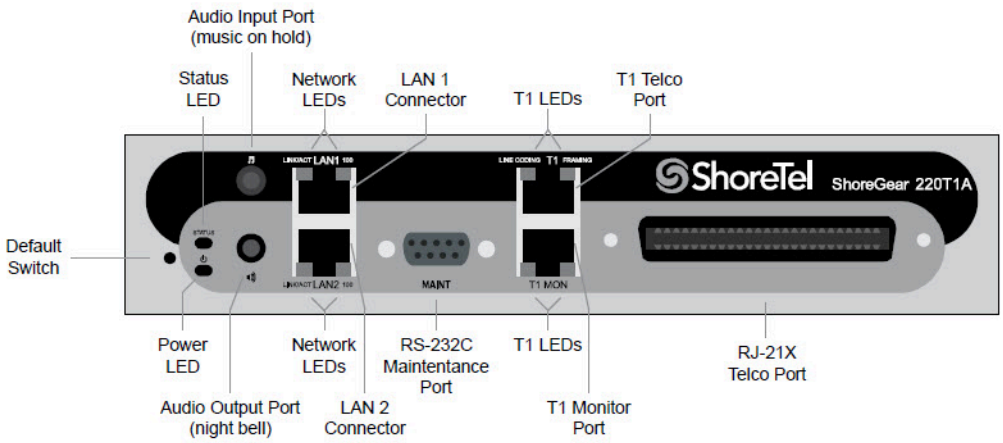
The SG220T1 voice switch contains the following components:

- 1 3.5 mm mono connector for audio input (music on hold)
- 1 3.5 mm mono connector for audio output (overhead paging and night bell)
- 1 DB-9 socket connector for maintenance
- 2 RJ-45 connectors for the LAN interface
- 1 RJ-45 SGT1 telco port
- 1 RJ-45 SGT1 monitor port for connecting test equipment

23.5.7 SG220T1A Voice Switch

The following sections describe SG220T1A resource capacity, LED behavior, and connectors. The SG220T1A is not supported in installations outside the U.S. and Canada. SG220T1A Front Plate displays the SG220T1A front plate.

Figure 44: SG220T1A Front Plate



23.5.7.1 Switch Capacity

- Analog Circuit Resources
  - Ports 1-2: Two Loop Start Trunks
  - Ports 9-12: Four Extensions or DID Trunks. A single command configures all ports as either Extensions or DID trunks.
  - Power Failure Transfer Unit: Trunk Port 1 to Extension Port 12
- Digital Circuit Resources: 24 channels maximum
  - One SGT1 circuit, 24 channels per circuit
- Make Me Conference Resource: Six ports
  - Ports 1-2, 9-12
- Maximum IP Phone Resources: 220 devices
  - Analog Channel Reallocation: 30
  - Digital Channel Reallocation: 120
  - Built-in Resources: 70
  - SIP Media Proxies: 20

23.5.7.2 LED Descriptions

Power LED

The SG220T1A has one power LED, which indicates the following:

- On: The switch is operating normally.
- Off: The switch has no power.
- Flashing:
  - 2 flashes — The switch failed its internal self-test. This indicates a hardware failure. Replace the unit and submit a Return Material Authorization (RMA) to Mitel.
  - 3 flashes — Booting through FTP. Flash memory might be corrupted. Use the pages available through the Maintenance menu in Connect Director to check and ensure that the system is running properly.
  - 4 flashes — The IP address is unavailable. DHCP did not respond to the IP address request, and the IP address is not available in nonvolatile memory to continue boot process. The switch will automatically reboot in five seconds and try again. Check the DHCP server and the network configuration to ensure that the voice switch is receiving a valid IP address.
  - 5 flashes — The operating system is not available. The switch is booting from FTP, but cannot find the boot files. The switch automatically reboots in 5 seconds. You can use DHCP to tell the switch where the files are. If you are using a DHCP server that supports options 66 and 67, set option 66 to the MiVoice Connect server's IP address, and set option 67 to /tsk/vxworks.
  - 6 flashes — Using a previously stored IP address. A DHCP transaction was attempted, but the DHCP server did not respond. The switch continues to use the IP address stored in nonvolatile memory until it receives a valid response. If the switch receives a response that provides a different IP address, it reboots using the new IP address. If the switch receives a response that matches the IP address stored in nonvolatile memory, it continues operation, and the power LED stops flashing. If the problem persists, check the DHCP server and network configuration.

23.5.7.2.1 Network LEDs

The SG220T1A network LEDs (LAN1 and LAN2) indicate the speed at which the switch is communicating with the network and whether there is network activity.

The network LED descriptions are as follows:

- Link/Activity: When lit, this LED indicates that the switch is connected to an Ethernet network. This LED indicates network activity, as follows:
  - When flashing, network activity is detected.
  - When on (not flashing), the switch is connected to an Ethernet network.
  - When off, the switch cannot detect an Ethernet network.

  This LED is not directly related to any switch's individual network activity. For example, if three switches are connected to the same hub and one switch's Traffic LED shows activity, the other switches will indicate the same activity.
- 100M
  - When green, the switch is connected to a 100BaseT network.
  - When off, the switch is connected to a 10BaseT network.

23.5.7.2.2 Status LED

The SG220T1A has one status LED to provide general information about the ports. The color and blink pattern of the LED indicate the port function:

- Status LED (Green)
  - When on steady, no ports are handling active calls.
  - When flashing fast (100 msec on/off), at least one port is handling an active call.
- Status LED (Yellow)
  - When on steady, no ports are handling active calls and at least one port is out of service.
  - When flashing slow (1 sec. on/off), the switch is not connected (or has lost connection) to a MiVoice Connect server.
  - When flashing fast (100 msec on/off), at least one port is handling an active call and at least one port is out of service.
- Off: No ports are assigned.

23.5.7.2.3 Monitor and Telco LEDs

The Monitor and Telco LEDs indicate line coding, network framing, and loopback status. These LEDs are color coded—green, yellow, and red. The Monitor and Telco LED descriptions follow.

Telco and Monitor LED alarms and errors are logged as switch events in Connect Director's event log.

- Line Coding: This LED indicates line coding status, as follows:
  - When green, the line coding signal is good.
  - When yellow, bipolar violations (BPV) are being received at one second intervals.
  - When red, a loss of signal (LOS) has occurred.
  - When flashing red, loopback is active (local or CO).
  - When off, the switch has no power.
- Framing: This LED indicates network framing status, as follows:
  - When green, the SGT1/SGE1 signal is in frame; the signal is synchronized.
  - When yellow, a yellow alarm has been received from the Central Office.
  - When flashing yellow, the frame-bit error rate has exceeded its limits. A small number of frame-bit errors (>1 per million) have occurred; this state will take up to 10 minutes to clear.
  - When flashing fast yellow, a series of frame-bit errors (>1 per 1000) have occurred.
  - When red, the SGT1/SGE1 signal is out-of-frame (OOF). The received signal cannot be framed to the Extended Superframe (ESF) or D4 format.
  - When flashing red, loopback is active (local or CO).
  - When off, the switch has no power.

23.5.7.3 SG220T1A Connectors

The SG220T1A voice switch contains the following components:

- 1 3.5 mm mono connector for audio input (music on hold)
- 1 3.5 mm mono connector for audio output (overhead paging and night bell)
- 1 DB-9 socket connector for maintenance
- 1 RJ-21X plug connector for mass termination of the telephone/trunk ports
- 2 RJ-45 connectors for the LAN interface
- 1 RJ-45 SGT1 telco port
- 1 RJ-45 SGT1 monitor port for connecting test equipment

23.5.7.4 SG220T1A RJ-21X Telephone and Trunk Connector

SG220T1A RJ-21X Telephone and Trunk Connector Pins lists the RJ-21X Ring and Tip pin numbers for the SG220T1AI.

Table 66: SG220T1A RJ-21X Telephone and Trunk Connector Pins

Port	Type	Ring		Tip	
		Pin #	Cable Color	Pin #	Cable Color
1	Trunk	1	Blue/White	26	White/Blue
–		2	Orange/White	27	White/Orange

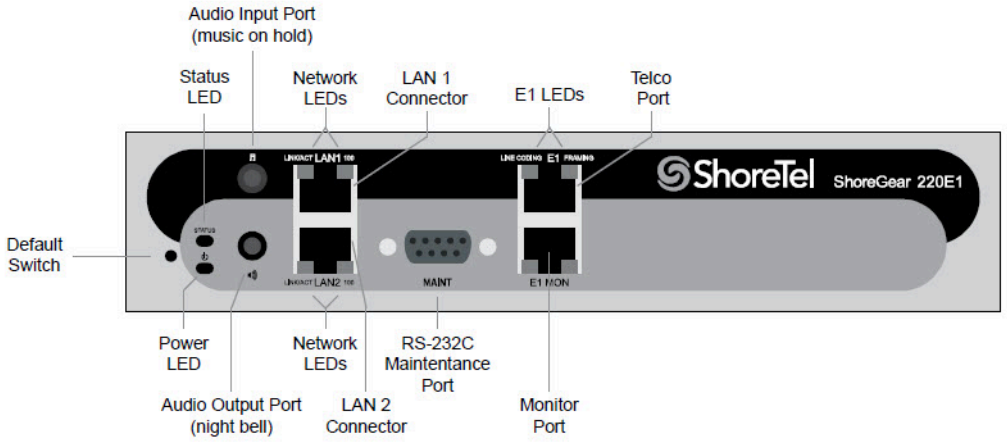
Port	Type	Ring		Tip	
		Pin #	Cable Color	Pin #	Cable Color
2	Trunk	3	Green/White	28	White/Green
–		4	Brown/White	29	White/Brown
–		5	Slate/White	30	White/Slate
–		6	Blue/Red	31	Red/Blue
–		7	Orange/Red	32	Red/Orange
–		8	Green/Red	33	Red/Green
–		9	Brown/Red	34	Red/Brown
–		10	Slate/Red	35	Red/Slate
–		11	Blue/Black	36	Black/Blue
–		12	Orange/Black	37	Black/Orange
–		13	Green/Black	38	Black/Green
–		14	Brown/Black	39	Black/Brown
–		15	Slate/Black	40	Black/Slate
–		16	Blue/Yellow	41	Yellow/Blue
9	Extension	17	Orange/Yellow	42	Yellow/Orange
–		18	Green/Yellow	43	Yellow/Green

Port	Type	Ring		Tip	
		Pin #	Cable Color	Pin #	Cable Color
10	Extension	19	Brown/Yellow	44	Yellow/Brown
–		20	Slate/Yellow	45	Yellow/Slate
11	Extension	21	Blue/Violet	46	Violet/Blue
–		22	Orange/Violet	47	Violet/Orange
12	Extension	23	Green/Violet	48	Violet/Green
–		24	Brown/Violet	49	Violet/Brown
–		25	Slate/Violet	50	Violet/Slate

23.5.8 SG220E1 Voice Switch

The following sections describe SG220E1 resource capacity, LED behavior, and connectors. SG220E1 Front Plate displays the SG220E1 front plate.

Figure 45: SG220E1 Front Plate



23.5.8.1 Switch Capacity

- Digital Circuit Resources: 30 channels maximum
  - One SGE1 circuit, 30 channels per circuit
- Make Me Conference Resource: none
- Maximum IP Phone Resources: 220
  - Digital Channel Reallocation: 150
  - Built-in Resources: 70
  - SIP Media Proxies: 20

23.5.8.2 LED Descriptions

Power LED

The SG220E1 has one power LED, which indicates the following:

- On: The switch is operating normally.
- Off: The switch has no power.
- Flashing:
  - 2 flashes — The switch failed its internal self-test. This indicates a hardware failure. Replace the unit and submit a Return Material Authorization (RMA) to Mitel.
  - 3 flashes — Booting through FTP. Flash memory might be corrupted. Use the pages available through the Maintenance menu in Connect Director to check and ensure that the system is running properly.
  - 4 flashes — The IP address is unavailable. DHCP did not respond to the IP address request, and the IP address is not available in nonvolatile memory to continue boot process. The switch will automatically reboot in five seconds and try again. Check the DHCP server and the network configuration to ensure that the voice switch is receiving a valid IP address.
  - 5 flashes — The operating system is not available. The switch is booting from FTP; but cannot find the boot files. The switch automatically reboots in 5 seconds. You can use DHCP to tell the switch where the files are. If you are using a DHCP server that supports options 66 and 67, set option 66 to the MiVoice Connect server's IP address, and set option 67 to /tsk/vxworks.
  - 6 flashes — Using a previously stored IP address. A DHCP transaction was attempted, but the DHCP server did not respond. The switch continues to use the IP address stored in nonvolatile memory until it receives a valid response. If the switch receives a response that provides a different IP address, it reboots using the new IP address. If the switch receives a response that matches the IP address stored in nonvolatile memory, it continues operation, and the power LED stops flashing. If the problem persists, check the DHCP server and network configuration.

23.5.8.2.1 Network LEDs

The SG220E1 network LEDs (LAN1 and LAN2) indicate the speed at which the switch is communicating with the network and whether there is network activity.

The network LED descriptions are as follows:

- Link/Activity: When lit, this LED indicates that the switch is connected to an Ethernet network. This LED indicates network activity, as follows:
  - When flashing, network activity is detected.
  - When on (not flashing), the switch is connected to an Ethernet network.
  - When off, the switch cannot detect an Ethernet network.

  This LED is not directly related to any switch's individual network activity. For example, if three switches are connected to the same hub and one switch's Traffic LED shows activity, the other switches will indicate the same activity.
- 100M
  - When green, the switch is connected to a 100BaseT network.
  - When off, the switch is connected to a 10BaseT network.

23.5.8.2.2 Status LED

The SG220E1 has one status LED to provide general information about the ports. The color and blink pattern of the LED indicate the port function:

- Status LED (Green)
  - When on steady, no ports are handling active calls.
  - When flashing fast, at least one port is handling an active call.
- Status LED (Yellow)
  - When on steady, no ports are handling active calls and at least one port is out of service.
  - When flashing slow, the switch is not connected (or has lost connection) to a MiVoice Connect server.
  - When flashing fast, at least one port is handling an active call and at least one port is out of service.
- Off: No ports are assigned.

23.5.8.2.3 Monitor and Telco LEDs

The Monitor and Telco LEDs indicate line coding, network framing, and loopback status. These LEDs are color coded—green, yellow, and red. The Monitor and Telco LED descriptions follow.

Telco and Monitor LED alarms and errors are logged as switch events in Connect Director's event log.

- Line Coding: This LED indicates line coding status, as follows:
  - When green, the line coding signal is good.
  - When yellow, bipolar violations (BPV) are being received at one second intervals.
  - When red, a loss of signal (LOS) has occurred.
  - When flashing red, loopback is active (local or CO).
  - When off, the switch has no power.

- Framing: This LED indicates network framing status, as follows:
  - When green, the SGT1/SGE1 signal is in frame; the signal is synchronized.
  - When yellow, a yellow alarm has been received from the Central Office.
  - When flashing yellow, the frame-bit error rate has exceeded its limits. A small number of frame-bit errors (>1 per million) have occurred; this state will take up to 10 minutes to clear.
  - When flashing fast yellow, a series of frame-bit errors (>1 per 1000) have occurred.
  - When red, the SGT1/SGE1 signal is out-of-frame (OOF). The received signal cannot be framed to the Extended Superframe (ESF) or D4 format.
  - When flashing red, loopback is active (local or CO).
  - When off, the switch has no power.

23.5.8.3 SG220E1 Connectors

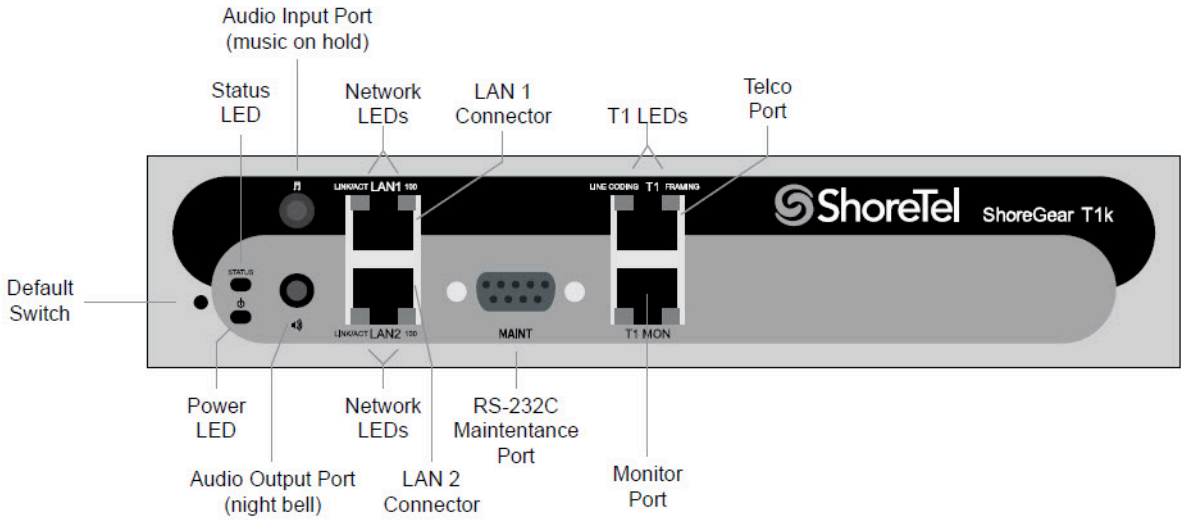
The SG220E1 voice switch contains the following components:

- 1 3.5 mm mono connector for audio input (music on hold)
- 1 3.5 mm mono connector for audio output (overhead paging and night bell)
- 1 DB-9 socket connector for maintenance
- 2 RJ-45 connectors for the LAN interface
- 1 RJ-45 SGT1 telco port
- 1 RJ-45 SGT1 monitor port for connecting test equipment

23.5.9 SGT1k Voice Switch

The following sections describe SGT1k resource capacity, LED behavior, and connectors. The SGT1k is not supported in installations outside the U.S. and Canada. SGT1k Front Plate displays the SGT1k front plate.

Figure 46: SGT1k Front Plate



23.5.9.1 Switch Capacity

- Digital Circuit Resources: 24 channels maximum
  - One SGT1 circuit, 24 channels per circuit
- Make Me Conference Resource: None
- Maximum IP Phone Resources
  - SIP Media Proxies: 20

23.5.9.2 LED Descriptions

Power LED

The SGT1k has one power LED, which indicates the following:

- On: The switch is operating normally.
- Off: The switch has no power.
- Flashing:
  - 2 flashes — The switch failed its internal self-test. This indicates a hardware failure. Replace the unit and submit a Return Material Authorization (RMA) to Mitel.
  - 3 flashes — Booting through FTP. Flash memory might be corrupted. Use the pages available through the Maintenance menu in Connect Director to check and ensure that the system is running properly.
  - 4 flashes — The IP address is unavailable. DHCP did not respond to the IP address request, and the IP address is not available in nonvolatile memory to continue boot process. The switch will automatically reboot in five seconds and try again. Check the DHCP server and the network configuration to ensure that the voice switch is receiving a valid IP address.
  - 5 flashes — The operating system is not available. The switch is booting from FTP; but cannot find the boot files. The switch automatically reboots in 5 seconds. You can use DHCP to tell the switch where the files are. If you are using a DHCP server that supports options 66 and 67, set option 66 to the MiVoice Connect server's IP address, and set option 67 to /tsk/vxworks.
  - 6 flashes — Using a previously stored IP address. A DHCP transaction was attempted, but the DHCP server did not respond. The switch continues to use the IP address stored in nonvolatile memory until it receives a valid response. If the switch receives a response that provides a different IP address, it reboots using the new IP address. If the switch receives a response that matches the IP address stored in nonvolatile memory, it continues operation, and the power LED stops flashing. If the problem persists, check the DHCP server and network configuration.

23.5.9.2.1 Network LEDs

The SGT1k network LEDs (LAN1 and LAN2) indicate the speed at which the switch is communicating with the network and whether there is network activity.

The network LED descriptions are as follows:

- Link/Activity: When lit, this LED indicates that the switch is connected to an Ethernet network. This LED indicates network activity, as follows:
  - When flashing, network activity is detected.
  - When on (not flashing), the switch is connected to an Ethernet network.
  - When off, the switch cannot detect an Ethernet network.

  This LED is not directly related to any switch's individual network activity. For example, if three switches are connected to the same hub and one switch's Traffic LED shows activity, the other switches will indicate the same activity.
- 100M
  - When green, the switch is connected to a 100BaseT network.
  - When off, the switch is connected to a 10BaseT network.

23.5.9.2.2 Status LED

The SGT1k has one status LED to provide general information about the ports. The color and blink pattern of the LED indicate the port function:

- Status LED (Green)
  - When on steady, no ports are handling active calls.
  - When flashing fast, at least one port is handling an active call.
- Status LED (Yellow)
  - When on steady, no ports are handling active calls and at least one port is out of service.
  - When flashing slow, the switch is not connected (or has lost connection) to a MiVoice Connect server.
  - When flashing fast, at least one port is handling an active call and at least one port is out of service.
- Off: No ports are assigned.

23.5.9.2.3 Monitor and Telco LEDs

The Monitor and Telco LEDs indicate line coding, network framing, and loopback status. These LEDs are color coded—green, yellow, and red. The Monitor and Telco LED descriptions follow.

Telco and Monitor LED alarms and errors are logged as switch events in Connect Director's event log.

- Line Coding: This LED indicates line coding status, as follows:
  - When green, the line coding signal is good.
  - When yellow, bipolar violations (BPV) are being received at one second intervals.
  - When red, a loss of signal (LOS) has occurred.
  - When flashing red, loopback is active (local or CO).
  - When off, the switch has no power.

- Framing: This LED indicates network framing status, as follows:
  - When green, the SGT1/SGE1 signal is in frame; the signal is synchronized.
  - When yellow, a yellow alarm has been received from the Central Office.
  - When flashing yellow, the frame-bit error rate has exceeded its limits. A small number of frame-bit errors (>1 per million) have occurred; this state will take up to 10 minutes to clear.
  - When flashing fast yellow, a series of frame-bit errors (>1 per 1000) have occurred.
  - When red, the SGT1/SGE1 signal is out-of-frame (OOF). The received signal cannot be framed to the Extended Superframe (ESF) or D4 format.
  - When flashing red, loopback is active (local or CO).
  - When off, the switch has no power.

23.5.9.3 SGT1k Connectors

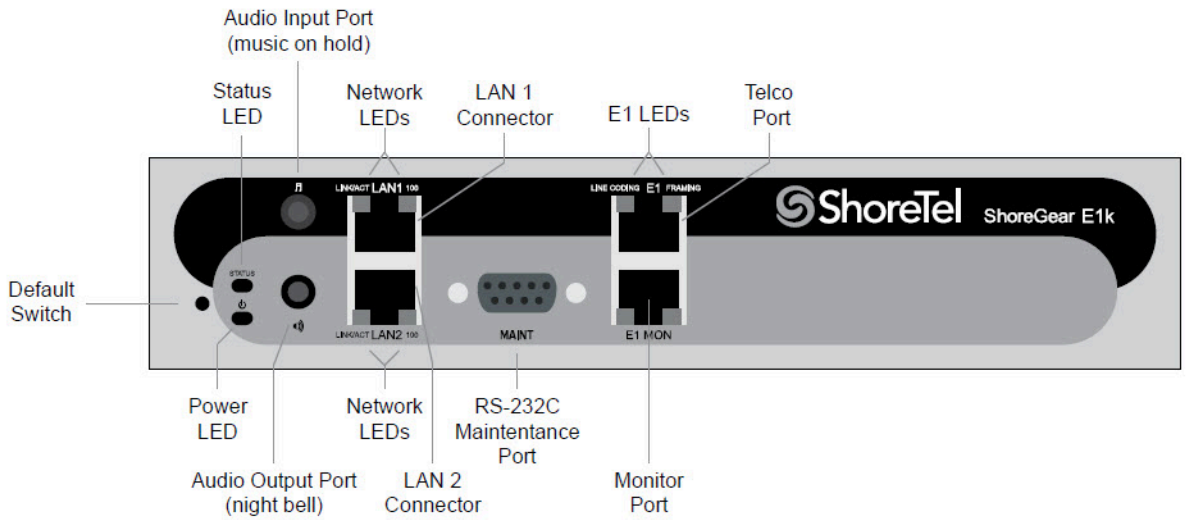
The SGT1k voice switch contains the following components:

- 1 3.5 mm mono connector for audio input (music on hold)
- 1 3.5 mm mono connector for audio output (overhead paging and night bell)
- 1 DB-9 socket connector for maintenance
- 2 RJ-45 connectors for the LAN interface
- 1 RJ-45 SGT1 telco port
- 1 RJ-45 SGT1 monitor port for connecting test equipment

23.5.10 SGE1k Voice Switch

The following sections describe SGE1k resource capacity, LED behavior, and connectors. SGE1k Front Plate displays the SGE1k front plate.

Figure 47: SGE1k Front Plate



23.5.10.1 Switch Capacity

- Digital Circuit Resources: 30 channels maximum
  - One SGE1 circuit, 30 channels per circuit
- Make Me Conference Resource: None
- Maximum IP Phone Resources
  - SIP Media Proxies: 20

23.5.10.2 LED Descriptions

Power LED

The SGE1k has one power LED, which indicates the following:

- On: The switch is operating normally.
- Off: The switch has no power.
- Flashing:
  - 2 flashes — The switch failed its internal self-test. This indicates a hardware failure. Replace the unit and submit a Return Material Authorization (RMA) to Mitel.
  - 3 flashes — Booting through FTP. Flash memory might be corrupted. Use the pages available through the Maintenance menu in Connect Director to check and ensure that the system is running properly.
  - 4 flashes — The IP address is unavailable. DHCP did not respond to the IP address request, and the IP address is not available in nonvolatile memory to continue boot process. The switch will automatically reboot in five seconds and try again. Check the DHCP server and the network configuration to ensure that the voice switch is receiving a valid IP address.
  - 5 flashes — The operating system is not available. The switch is booting from FTP; but cannot find the boot files. The switch automatically reboots in 5 seconds. You can use DHCP to tell the switch where the files are. If you are using a DHCP server that supports options 66 and 67, set option 66 to the MiVoice Connect server's IP address, and set option 67 to /tsk/vxworks.
  - 6 flashes — Using a previously stored IP address. A DHCP transaction was attempted, but the DHCP server did not respond. The switch continues to use the IP address stored in nonvolatile memory until it receives a valid response. If the switch receives a response that provides a different IP address, it reboots using the new IP address. If the switch receives a response that matches the IP address stored in nonvolatile memory, it continues operation, and the power LED stops flashing. If the problem persists, check the DHCP server and network configuration.

23.5.10.2.1 Network LEDs

The SGE1k network LEDs (LAN1 and LAN2) indicate the speed at which the switch is communicating with the network and whether there is network activity.

The network LED descriptions are as follows:

- Link/Activity: When lit, this LED indicates that the switch is connected to an Ethernet network. This LED indicates network activity, as follows:
  - When flashing, network activity is detected.
  - When on (not flashing), the switch is connected to an Ethernet network.
  - When off, the switch cannot detect an Ethernet network.

  This LED is not directly related to any switch's individual network activity. For example, if three switches are connected to the same hub and one switch's Traffic LED shows activity, the other switches will indicate the same activity.
- 100M
  - When green, the switch is connected to a 100BaseT network.
  - When off, the switch is connected to a 10BaseT network.

23.5.10.2.2 Status LED

The SGE1k has one status LED to provide general information about the ports. The color and blink pattern of the LED indicate the port function:

- Status LED (Green)
  - When on steady, no ports are handling active calls.
  - When flashing fast, at least one port is handling an active call.
- Status LED (Yellow)
  - When on steady, no ports are handling active calls and at least one port is out of service.
  - When flashing slow, the switch is not connected (or has lost connection) to a MiVoice Connect server.
  - When flashing fast, at least one port is handling an active call and at least one port is out of service.
- Off: No ports are assigned.

23.5.10.2.3 Monitor and Telco LEDs

The Monitor and Telco LEDs indicate line coding, network framing, and loopback status. These LEDs are color coded—green, yellow, and red. The Monitor and Telco LED descriptions follow.

Telco and Monitor LED alarms and errors are logged as switch events in Connect Director's event log.

- Line Coding: This LED indicates line coding status, as follows:
  - When green, the line coding signal is good.
  - When yellow, bipolar violations (BPV) are being received at one second intervals.
  - When red, a loss of signal (LOS) has occurred.
  - When flashing red, loopback is active (local or CO).
  - When off, the switch has no power.

- Framing: This LED indicates network framing status, as follows:
  - When green, the SGT1/SGE1 signal is in frame; the signal is synchronized.
  - When yellow, a yellow alarm has been received from the Central Office.
  - When flashing yellow, the frame-bit error rate has exceeded its limits. A small number of frame-bit errors (>1 per million) have occurred; this state will take up to 10 minutes to clear.
  - When flashing fast yellow, a series of frame-bit errors (>1 per 1000) have occurred.
  - When red, the SGT1/SGE1 signal is out-of-frame (OOF). The received signal cannot be framed to the Extended Superframe (ESF) or D4 format.
  - When flashing red, loopback is active (local or CO).
  - When off, the switch has no power.

23.5.10.3 SGE1k Connectors

The SGE1k voice switch contains the following components:

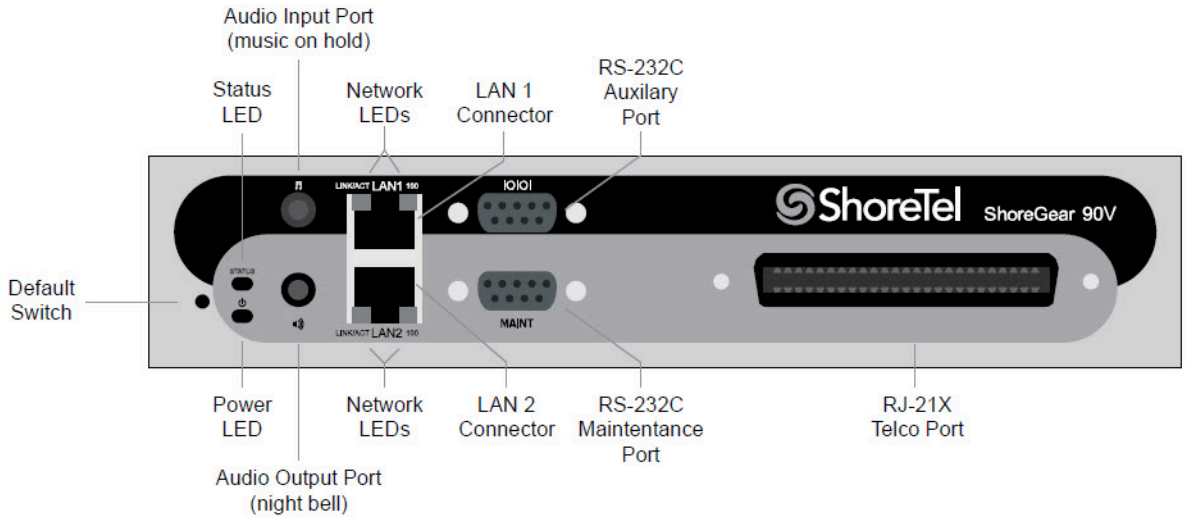
- 1 3.5 mm mono connector for audio input (music on hold)
- 1 3.5 mm mono connector for audio output (overhead paging and night bell)
- 1 DB-9 socket connector for maintenance
- 2 RJ-45 connectors for the LAN interface
- 1 RJ-45 SGT1 telco port
- 1 RJ-45 SGT1 monitor port for connecting test equipment

23.6 Specifications – SG Voice Model Switches

23.6.1 SG90V Voice Switch

The following sections describe SG90V resource capacity, LED behavior, and connectors. The SG90V is not supported in installations outside the U.S. and Canada. SG90V Front Plate displays the SG90V front plate.

Figure 48: SG90V Front Plate



23.6.1.1 Switch Capacity

- Analog Circuit Resources
  - Ports 1-8: Eight Loop Start Trunks
  - Ports 9-12: Four Extensions or DID Trunks. A single command configures all ports as either Extensions or DID trunks
  - Power Failure Transfer Unit: Trunk Port 1 to Extension Port 12
- Make Me Conference Resources: 12 ports
  - Ports 1-12
- Maximum IP Phone Resources: 90 devices
  - Analog Port Reallocation: 60
  - Built-in Resources: 30

23.6.1.2 LED Descriptions

Power LED

The SG90V has one power LED, which indicates the following:

- On: The switch is operating normally.
- Off: The switch has no power.

- Flashing:
  - 2 flashes — The switch failed its internal self-test. This indicates a hardware failure. Replace the unit and submit a Return Material Authorization (RMA) to Mitel.
  - 3 flashes — Booting through FTP. Flash memory might be corrupted. Use the pages available through the Maintenance menu in Connect Director to check and ensure that the system is running properly.
  - 4 flashes — The IP address is unavailable. DHCP did not respond to the IP address request, and the IP address is not available in nonvolatile memory to continue boot process. The switch will automatically reboot in five seconds and try again. Check the DHCP server and the network configuration to ensure that the voice switch is receiving a valid IP address.
  - 5 flashes — The operating system is not available. The switch is booting from FTP; but cannot find the boot files. The switch automatically reboots in 5 seconds. You can use DHCP to tell the switch where the files are. If you are using a DHCP server that supports options 66 and 67, set option 66 to the MiVoice Connect server's IP address, and set option 67 to /tsk/vxworks.
  - 6 flashes — Using a previously stored IP address. A DHCP transaction was attempted, but the DHCP server did not respond. The switch continues to use the IP address stored in nonvolatile memory until it receives a valid response. If the switch receives a response that provides a different IP address, it reboots using the new IP address. If the switch receives a response that matches the IP address stored in nonvolatile memory, it continues operation, and the power LED stops flashing. If the problem persists, check the DHCP server and network configuration.

23.6.1.2.1 Network LEDs

The SG90V network LEDs (LAN1 and LAN2) indicate the speed at which the switch is communicating with the network and whether there is network activity.

The network LED descriptions are as follows:

- Link/Activity: When lit, this LED indicates that the switch is connected to an Ethernet network. This LED indicates network activity, as follows:
  - When flashing, network activity is detected.
  - When on (not flashing), the switch is connected to an Ethernet network.
  - When off, the switch cannot detect an Ethernet network.

  This LED is not directly related to any switch's individual network activity. For example, if three switches are connected to the same hub and one switch's Traffic LED shows activity, the other switches will indicate the same activity.
- 100M
  - When green, the switch is connected to a 100BaseT network.
  - When off, the switch is connected to a 10BaseT network.

23.6.1.2.2 Status LED

The SG90V has one status LED to provide general information about the ports. The color and blink pattern of the LED indicate the port function:

- Status LED (Green)
  - When on steady, no ports are handling active calls.
  - When flashing fast, at least one port is handling an active call.
- Status LED (Yellow)
  - When on steady, no ports are handling active calls and at least one port is out of service.
  - When flashing slow, the switch is not connected (or has lost connection) to a MiVoice Connect server.
  - When flashing fast, at least one port is handling an active call and at least one port is out of service.
- Off: No ports are assigned.

23.6.1.3 SG90V Connectors

The SG90V voice switch contains the following components:

- 1 3.5 mm mono connector for audio input (music on hold)
- 1 3.5 mm mono connector for audio output (overhead paging and night bell)
- 1 DB-9 socket connector for maintenance
- 2 RJ-45 connectors for the LAN interface
- 1 RJ-21X plug connector for mass termination of the telephone/trunk ports
- Power Failure Transfer Unit: Trunk Port 1 to Extension Port 12
- Backup Operator: Extension Port 12

23.6.1.4 SG90V RJ-21X Telephone and Trunk Connector

SG90V RJ-21X Telephone and Trunk Connector Pins lists the RJ-21X Ring and Tip pin numbers for the SG90V.

Table 67: SG90V RJ-21X Telephone and Trunk Connector Pins

Port	Type	Ring		Tip	
		Pin #	Cable Color	Pin #	Cable Color
1	Trunk	1	Blue/White	26	White/Blue
–		2	Orange/White	27	White/Orange
2	Trunk	3	Green/White	28	White/Green
–		4	Brown/White	29	White/Brown

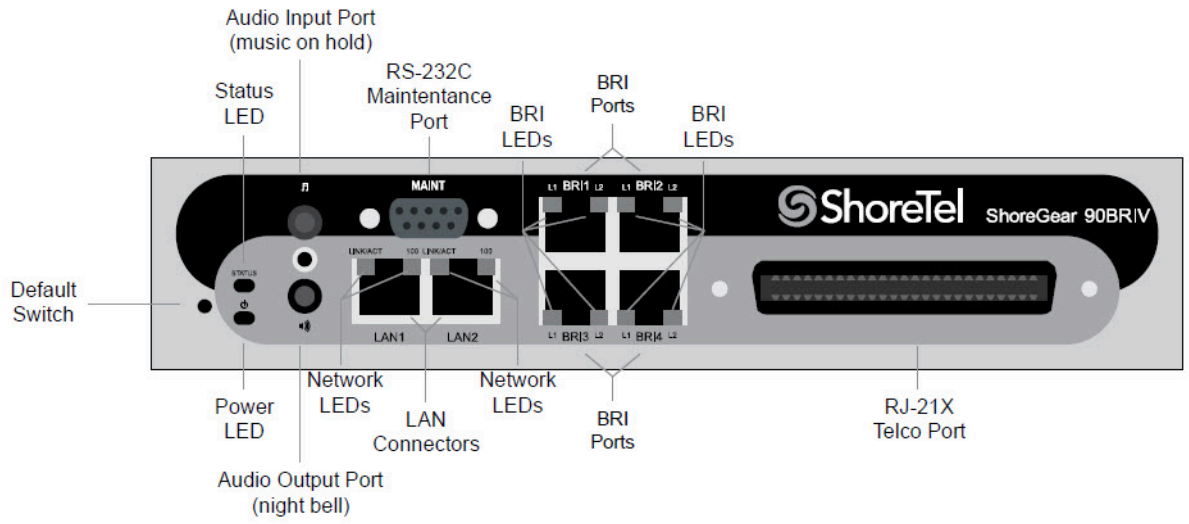
Port	Type	Ring		Tip	
		Pin #	Cable Color	Pin #	Cable Color
3	Trunk	5	Slate/White	30	White/Slate
–		6	Blue/Red	31	Red/Blue
4	Trunk	7	Orange/Red	32	Red/Orange
–		8	Green/Red	33	Red/Green
5		9	Brown/Red	34	Red/Brown
–		10	Slate/Red	35	Red/Slate
6		11	Blue/Black	36	Black/Blue
–		12	Orange/Black	37	Black/Orange
7		13	Green/Black	38	Black/Green
–		14	Brown/Black	39	Black/Brown
8		15	Slate/Black	40	Black/Slate
–		16	Blue/Yellow	41	Yellow/Blue
9	Extension - DID	17	Orange/Yellow	42	Yellow/Orange
–		18	Green/Yellow	43	Yellow/Green
10	Extension - DID	19	Brown/Yellow	44	Yellow/Brown
–		20	Slate/Yellow	45	Yellow/Slate

Port	Type	Ring		Tip	
		Pin #	Cable Color	Pin #	Cable Color
11	Extension - DID	21	Blue/Violet	46	Violet/Blue
–		22	Orange/Violet	47	Violet/Orange
12	Extension - DID	23	Green/Violet	48	Violet/Green
–		24	Brown/Violet	49	Violet/Brown
–		25	Slate/Violet	50	Violet/Slate

23.6.2 SG90BRIV Voice Switch

The following sections describe SG90BRIV resource capacity, LED behavior, and connectors. SG90BRIV Front Plate displays the SG90BRIV front plate.

Figure 49: SG90BRIV Front Plate



23.6.2.1 Switch Capacity

- Analog Circuit Resources
  - Ports 9-12: Extensions

- Digital Circuit Resources
  - Four BRI Spans, each comprising two channels: Eight channels maximum
- Make Me Conference Resource: None
- Maximum IP Phone Resources: 90 devices
  - Analog Port Reallocation: 20
  - Digital Channel Reallocation: 40
  - Built-in Resources: 30

23.6.2.2 LED Descriptions

Power LED

The SG90BRIV has one power LED, which indicates the following:

- On: The switch is operating normally.
- Off: The switch has no power.
- Flashing:
  - 2 flashes — The switch failed its internal self-test. This indicates a hardware failure. Replace the unit and submit a Return Material Authorization (RMA) to Mitel.
  - 3 flashes — Booting through FTP. Flash memory might be corrupted. Use the pages available through the Maintenance menu in Connect Director to check and ensure that the system is running properly.
  - 4 flashes — The IP address is unavailable. DHCP did not respond to the IP address request, and the IP address is not available in nonvolatile memory to continue boot process. The switch will automatically reboot in five seconds and try again. Check the DHCP server and the network configuration to ensure that the voice switch is receiving a valid IP address.
  - 5 flashes — The operating system is not available. The switch is booting from FTP; but cannot find the boot files. The switch automatically reboots in 5 seconds. You can use DHCP to tell the switch where the files are. If you are using a DHCP server that supports options 66 and 67, set option 66 to the MiVoice Connect server's IP address, and set option 67 to /tsk/vxworks.
  - 6 flashes — Using a previously stored IP address. A DHCP transaction was attempted, but the DHCP server did not respond. The switch continues to use the IP address stored in nonvolatile memory until it receives a valid response. If the switch receives a response that provides a different IP address, it reboots using the new IP address. If the switch receives a response that matches the IP address stored in nonvolatile memory, it continues operation, and the power LED stops flashing. If the problem persists, check the DHCP server and network configuration.

23.6.2.2.1 Network LEDs

The SG90BRIV network LEDs (LAN1 and LAN2) indicate the speed at which the switch is communicating with the network and whether there is network activity.

The network LED descriptions are as follows:

- Link/Activity: When lit, this LED indicates that the switch is connected to an Ethernet network. This LED indicates network activity, as follows:
  - When flashing, network activity is detected.
  - When on (not flashing), the switch is connected to an Ethernet network.
  - When off, the switch cannot detect an Ethernet network.

  This LED is not directly related to any switch's individual network activity. For example, if three switches are connected to the same hub and one switch's Traffic LED shows activity, the other switches will indicate the same activity.
- 100M
  - When green, the switch is connected to a 100BaseT network.
  - When off, the switch is connected to a 10BaseT network.

23.6.2.2.2 Status LED

The SG90BRIV has one status LED to provide general information about the ports. The color and blink pattern of the LED indicate the port function:

- Status LED (Green)
  - When on steady, no ports are handling active calls.
  - When flashing fast, at least one port is handling an active call.
- Status LED (Yellow)
  - When on steady, no ports are handling active calls and at least one port is out of service.
  - When flashing slow, the switch is not connected (or has lost connection) to a MiVoice Connect server.
  - When flashing fast, at least one port is handling an active call and at least one port is out of service.
- Off: No ports are assigned.

23.6.2.2.3 BRI LED

Each BRI connector has two LEDs to indicate port activity. The color and blink pattern of the LED indicate the port function:

- LED 1: Off, LED 2 Off – Port not configured in Director
- LED 1: Yellow, LED 2 Off – Port inactive or not connected
- LED 1: Off, LED 2 Off – Layer 1 active. Layer 2 not established
- LED 1: Off, LED 2 Green – Layer 1 active. Layer 2 active.
- LED 1: Off, LED 2 Green flashing – Call in progress (Layer 1, Layer 2, and Layer 3 active).

23.6.2.3 SG90BRIV Connectors

The SG90BRIV voice switch contains the following components:

- 1 3.5 mm mono connector for audio input (music on hold)
- 1 3.5 mm mono connector for audio output (overhead paging and night bell)

- 1 DB-9 socket connector for maintenance
- 2 RJ-45 connectors for the LAN interface
- 1 RJ-21X plug connector for mass termination of the telephone/trunk ports
- 4 RJ-45 SGT1 telco port

23.6.2.4 SG90BRIV RJ-21X Telephone and Trunk Connector

SG90BRIV RJ-21X Telephone and Trunk Connector Pins lists the RJ-21X Ring and Tip pin numbers for the SG90BRIV.

Table 68: SG90BRIV RJ-21X Telephone and Trunk Connector Pins

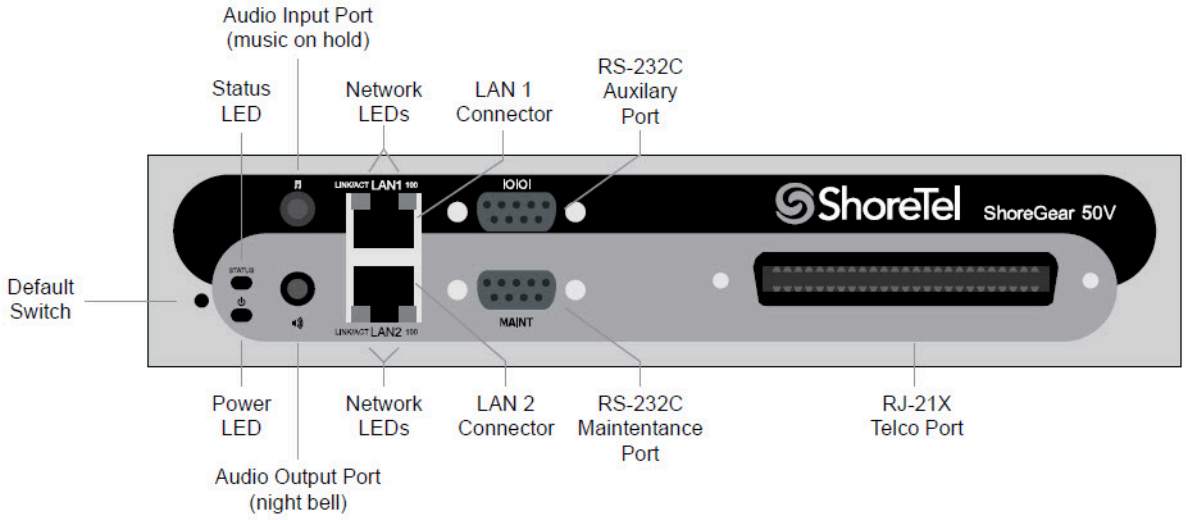
Port	Type	Ring		Tip	
		Pin #	Cable Color	Pin #	Cable Color
–		1	Blue/White	26	White/Blue
–		2	Orange/White	27	White/Orange
–		3	Green/White	28	White/Green
–		4	Brown/White	29	White/Brown
–		5	Slate/White	30	White/Slate
–		6	Blue/Red	31	Red/Blue
–		7	Orange/Red	32	Red/Orange
–		8	Green/Red	33	Red/Green
–		9	Brown/Red	34	Red/Brown
–		10	Slate/Red	35	Red/Slate
–		11	Blue/Black	36	Black/Blue

Port	Type	Ring		Tip	
		Pin #	Cable Color	Pin #	Cable Color
–		12	Orange/Black	37	Black/Orange
–		13	Green/Black	38	Black/Green
–		14	Brown/Black	39	Black/Brown
–		15	Slate/Black	40	Black/Slate
–		16	Blue/Yellow	41	Yellow/Blue
9	Extension	17	Orange/Yellow	42	Yellow/Orange
–		18	Green/Yellow	43	Yellow/Green
10	Extension	19	Brown/Yellow	44	Yellow/Brown
–		20	Slate/Yellow	45	Yellow/Slate
11	Extension	21	Blue/Violet	46	Violet/Blue
–		22	Orange/Violet	47	Violet/Orange
12	Extension - DID	23	Green/Violet	48	Violet/Green
–		24	Brown/Violet	49	Violet/Brown
–		25	Slate/Violet	50	Violet/Slate

23.6.3 SG50V Voice Switch

The following sections describe SG50V resource capacity, LED behavior, and connectors. The SG50V is not supported in installations outside the U.S. and Canada. SG50V Front Plate displays the SG50V front plate.

Figure 50: SG50V Front Plate



23.6.3.1 Switch Capacity

- Analog Circuit Resources
  - Ports 1-4: Four Loop Start Trunks
  - Ports 11-12: Two Extensions or DID Trunks. A single command configures all ports as either Extensions or DID trunks
  - Power Failure Transfer Unit: Trunk Port 1 to Extension Port 12
- Make Me Conference Resources: six ports
  - Ports 1-4, 11-12
- Maximum IP Phone Resources: 50 devices
  - Analog Port Reallocation: 30
  - Built-in Resources: 20

23.6.3.2 LED Descriptions

Power LED

The SG50V has one power LED, which indicates the following:

- On: The switch is operating normally.
- Off: The switch has no power.

- Flashing:
  - 2 flashes — The switch failed its internal self-test. This indicates a hardware failure. Replace the unit and submit a Return Material Authorization (RMA) to Mitel.
  - 3 flashes — Booting through FTP. Flash memory might be corrupted. Use the pages available through the Maintenance menu in Connect Director to check and ensure that the system is running properly.
  - 4 flashes — The IP address is unavailable. DHCP did not respond to the IP address request, and the IP address is not available in nonvolatile memory to continue boot process. The switch will automatically reboot in five seconds and try again. Check the DHCP server and the network configuration to ensure that the voice switch is receiving a valid IP address.
  - 5 flashes — The operating system is not available. The switch is booting from FTP; but cannot find the boot files. The switch automatically reboots in 5 seconds. You can use DHCP to tell the switch where the files are. If you are using a DHCP server that supports options 66 and 67, set option 66 to the MiVoice Connect server's IP address, and set option 67 to /tsk/vxworks.
  - 6 flashes — Using a previously stored IP address. A DHCP transaction was attempted, but the DHCP server did not respond. The switch continues to use the IP address stored in nonvolatile memory until it receives a valid response. If the switch receives a response that provides a different IP address, it reboots using the new IP address. If the switch receives a response that matches the IP address stored in nonvolatile memory, it continues operation, and the power LED stops flashing. If the problem persists, check the DHCP server and network configuration.

23.6.3.2.1 Network LEDs

The SG50V network LEDs (LAN1 and LAN2) indicate the speed at which the switch is communicating with the network and whether there is network activity.

The network LED descriptions are as follows:

- Link/Activity: When lit, this LED indicates that the switch is connected to an Ethernet network. This LED indicates network activity, as follows:
  - When flashing, network activity is detected.
  - When on (not flashing), the switch is connected to an Ethernet network.
  - When off, the switch cannot detect an Ethernet network.

  This LED is not directly related to any switch's individual network activity. For example, if three switches are connected to the same hub and one switch's Traffic LED shows activity, the other switches will indicate the same activity.
- 100M
  - When green, the switch is connected to a 100BaseT network.
  - When off, the switch is connected to a 10BaseT network.

23.6.3.2.2 Status LED

The SG50V has one status LED to provide general information about the ports. The color and blink pattern of the LED indicate the port function:

- Status LED (Green)
  - When on steady, no ports are handling active calls.
  - When flashing fast, at least one port is handling an active call.
- Status LED (Yellow)
  - When on steady, no ports are handling active calls and at least one port is out of service.
  - When flashing slow, the switch is not connected (or has lost connection) to a MiVoice Connect server.
  - When flashing fast, at least one port is handling an active call and at least one port is out of service.
- Off: No ports are assigned.

23.6.3.3 SG50V Connectors

The SG50V voice switch contains the following components:

- 1 3.5 mm mono connector for audio input (music on hold)
- 1 3.5 mm mono connector for audio output (overhead paging and night bell)
- 1 DB-9 socket connector for maintenance
- 2 RJ-45 connectors for the LAN interface
- 1 RJ-21X plug connector for mass termination of the telephone/trunk ports
- Power Failure Transfer Unit: Trunk Port 1 to Extension Port 12
- Backup Operator: Extension Port 12

23.6.3.4 SG50V RJ-21X Telephone and Trunk Connector

SG50V RJ-21X Telephone and Trunk Connector Pins lists the RJ-21X Ring and Tip pin numbers for the SG50V.

Table 69: SG50V RJ-21X Telephone and Trunk Connector Pins

Port	Type	Ring		Tip	
		Pin #	Cable Color	Pin #	Cable Color
1	Trunk	1	Blue/White	26	White/Blue
–		2	Orange/White	27	White/Orange
2	Trunk	3	Green/White	28	White/Green
–		4	Brown/White	29	White/Brown

Port	Type	Ring		Tip	
		Pin #	Cable Color	Pin #	Cable Color
3	Trunk	5	Slate/White	30	White/Slate
–		6	Blue/Red	31	Red/Blue
4	Trunk	7	Orange/Red	32	Red/Orange
–		8	Green/Red	33	Red/Green
–		9	Brown/Red	34	Red/Brown
–		10	Slate/Red	35	Red/Slate
–		11	Blue/Black	36	Black/Blue
–		12	Orange/Black	37	Black/Orange
–		13	Green/Black	38	Black/Green
–		14	Brown/Black	39	Black/Brown
–		15	Slate/Black	40	Black/Slate
–		16	Blue/Yellow	41	Yellow/Blue
–		17	Orange/Yellow	42	Yellow/Orange
–		18	Green/Yellow	43	Yellow/Green
–		19	Brown/Yellow	44	Yellow/Brown
–		20	Slate/Yellow	45	Yellow/Slate

Port	Type	Ring		Tip	
		Pin #	Cable Color	Pin #	Cable Color
11	Extension - DID	21	Blue/Violet	46	Violet/Blue
–		22	Orange/Violet	47	Violet/Orange
12	Extension - DID	23	Green/Violet	48	Violet/Green
–		24	Brown/Violet	49	Violet/Brown
–		25	Slate/Violet	50	Violet/Slate

23.7 Specification – ST 1U Full Width Switches

23.7.1 Voice Switch ST24A/ST48A

The following sections describe ST24A/ST48A resource capacity, LED behavior, and connectors. The ST24A/ST48A is not supported in installations outside the U.S. and Canada. Voice Switch ST24A Front Plate and Voice Switch ST48A Front Plate display the ST24A/ST48A front plates.

Figure 51: Voice Switch ST24A Front Plate

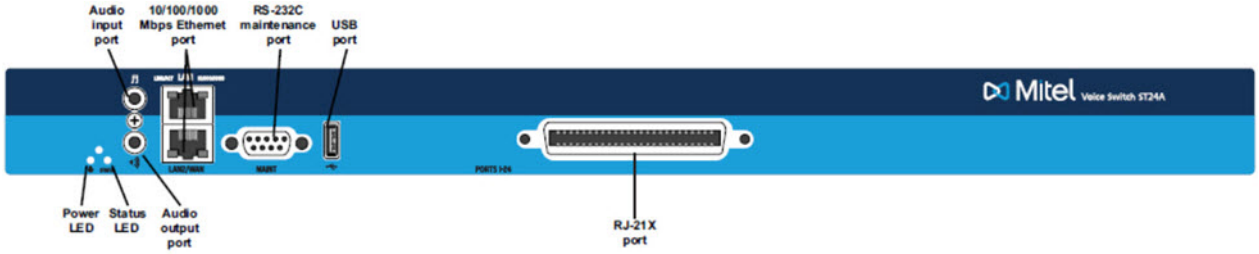
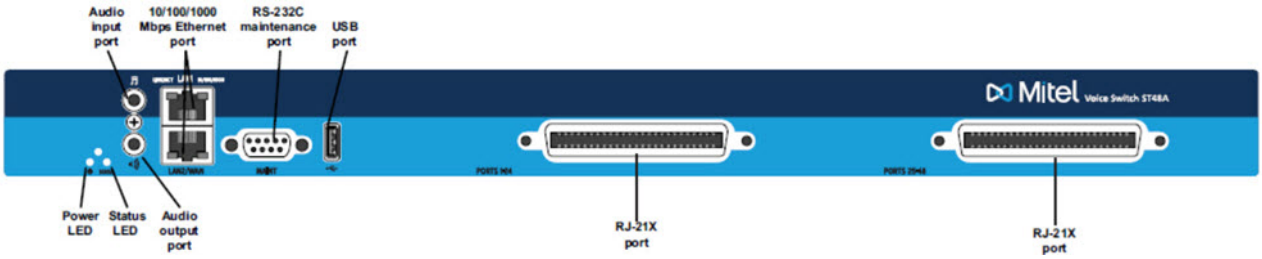


Figure 52: Voice Switch ST48A Front Plate



23.7.1.1 Switch Capacity

Analog Circuit Resources

- ST24A: Ports 1-24 (twenty four extensions)
- ST48A: Ports 1-24 (forty eight extensions)

23.7.1.1.1 Make Me Conference Resource

- ST24A: Ports 1-24
- ST48A: Ports 1-48

23.7.1.1.2 Maximum IP Phone Resources

None

23.7.1.2 LED Descriptions

Power LED

The Voice Switch ST24A/ST48A has one power LED, which indicates the following:

- On: The switch is operating normally.
- Off: The switch has no power.
- Flashing: Continuous flashing or a two-flash pattern indicates a failed internal self-test (that is, hardware failure).

23.7.1.2.1 Network LEDs

The Voice Switch ST24A/ST48A network LEDs (LAN1 and LAN2) indicate the speed at which the switch is communicating with the network and whether there is network activity.

The network LED descriptions are as follows:

- Link/Activity: When lit, this LED indicates that the switch is connected to an Ethernet network. This LED indicates network activity, as follows:
  - When flashing, network activity is detected.
  - When on (not flashing), the switch is connected to an Ethernet network.
  - When off, the switch cannot detect an Ethernet network.

  This LED is not directly related to any switch's individual network activity. For example, if three switches are connected to the same hub and one switch's Traffic LED shows activity, the other switches will indicate the same activity.
- 100M
  - When green, the switch is connected to a 100BaseT network.
  - When off, the switch is connected to a 10BaseT network.

23.7.1.2.2 Status LED

The Voice Switch ST24A/ST48A has one status LED to provide general information about the ports. The color and blink pattern of the LED indicate the port function:

- Off — No ports are assigned
- Green Steady— No ports are handling active calls.
- Green Flashing Fast — At least one port is handling an active call.
- Yellow Steady — No ports are handling active calls and at least one port is out of service.
- Yellow Flashing Slow — The switch is not connected (or has lost connection) to a MiVoice Connect server.
- Yellow Flashing Fast — At least one port is handling an active call and at least one port is out of service.

23.7.1.3 Voice Switch ST24A/ST48A Connectors

The Voice Switch ST24A/ST48A voice switch contains the following components:

- One audio input port (3.5 mm stereo) for connecting to a music-on-hold source
- One audio output port (3.5 mm stereo) for connecting to a corporate paging system or night bell
- Two RJ-45 10/100/1000 Mbps LAN connectors
- One DB-9 (socket), RS-232C maintenance port (default 115,200 bps, 8 bits, no parity, 1 stop bit, no handshake) for serial communications
- USB port for logging/troubleshooting

> **Note**:
>
> Only vFAT/FAT32 storage is supported for USB logging.

- One or two RJ-21X ports (plug) for connecting the switch to analog lines and trunks

23.7.1.4 Voice Switch ST24A/ST48A RJ-21X Telephone and Trunk Connector

ST24A/ST48A RJ-21X Telephone and Trunk Connector lists the RJ-21X Ring and Tip pin numbers for the ST24A/ST48A.

Note:

When the ST48A is connected directly to a 24-port patch panel, the voice switch's lower 24 analog channels, 1 through 24, map to ports 1 through 24 on the patch panel connected to the left RJ-21X connector. The voice switch's upper 24 analog channels, 25 through 48, map to ports 1 through 24 on the right RJ-21X connector.

Table 70: ST24A/ST48A RJ-21X Telephone and Trunk Connector

Port	Type	Ring		Tip	
		Pin #	Cable Color	Pin #	Cable Color
1	Extension - FXS	1	Blue/White	26	White/Blue
2	Extension - FXS	2	Orange/White	27	White/Orange
3	Extension - FXS	3	Green/White	28	White/Green
4	Extension - FXS	4	Brown/White	29	White/Brown
5	Extension - FXS	5	Slate/White	30	White/Slate
6	Extension - FXS	6	Blue/Red	31	Red/Blue
7	Extension - FXS	7	Orange/Red	32	Red/Orange
8	Extension - FXS	8	Green/Red	33	Red/Green
9	Extension - FXS	9	Brown/Red	34	Red/Brown

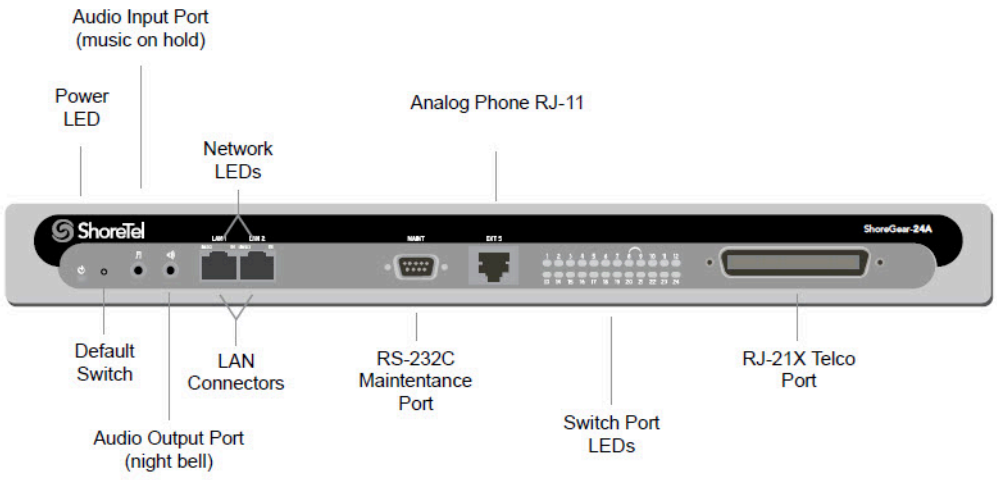
Port	Type	Ring		Tip	
		Pin #	Cable Color	Pin #	Cable Color
10	Extension - FXS	10	Slate/Red	35	Red/Slate
11	Extension - FXS	11	Blue/Black	36	Black/Blue
12	Extension - FXS	12	Orange/Black	37	Black/Orange
13	Extension - FXS	13	Green/Black	38	Black/Green
14	Extension - FXS	14	Brown/Black	Black/Brown	39
15	Extension - FXS	15	Slate/Black	40	Black/Slate
16	Extension - FXS	16	Blue/Yellow	41	Yellow/Blue
17	Extension - FXS	17	Orange/Yellow	42	Yellow/Orange
18	Extension - FXS	18	Green/Yellow	43	Yellow/Green
19	Extension - FXS	19	Brown/Yellow	44	Yellow/Brown
20	Extension - FXS	20	Slate/Yellow	45	Yellow/Slate
21	Extension - FXS	21	Blue/Violet	46	Violet/Blue
22	Extension - FXS	22	Orange/Violet	47	Violet/Orange
23	Extension - FXS	23	Green/Violet	48	Violet/Green
24	Extension - FXS	24	Brown/Violet	49	Violet/Brown
–		25	Slate/Violet	50	Violet/Slate

23.8 Specification – SG 1U Full Width Switches

23.8.1 SG24A Voice Switch

The following sections describe SG24A resource capacity, LED behavior, and connectors. The SG24A is not supported in installations outside the U.S. and Canada. SG24A Front Plate displays the SG24A front plate.

Figure 53: SG24A Front Plate



23.8.1.1 Switch Capacity

- Analog Circuit Resources
  - Ports 1-24: Twenty four extensions
- Make Me Conference Resource: 24 Ports
  - Ports 1-24
- Maximum IP Phone Resources: None

23.8.1.2 LED Descriptions

Power LED

The SG24A has one power LED, which indicates the following:

- On: The switch is operating normally.
- Off: The switch has no power.

- Flashing:
  - 2 flashes — The switch failed its internal self-test. This indicates a hardware failure. Replace the unit and submit a Return Material Authorization (RMA) to Mitel.
  - 3 flashes — Booting through FTP. Flash memory might be corrupted. Use the pages available through the Maintenance menu in Connect Director to check and ensure that the system is running properly.
  - 4 flashes — The IP address is unavailable. DHCP did not respond to the IP address request, and the IP address is not available in nonvolatile memory to continue boot process. The switch will automatically reboot in five seconds and try again. Check the DHCP server and the network configuration to ensure that the voice switch is receiving a valid IP address.
  - 5 flashes — The operating system is not available. The switch is booting from FTP; but cannot find the boot files. The switch automatically reboots in 5 seconds. You can use DHCP to tell the switch where the files are. If you are using a DHCP server that supports options 66 and 67, set option 66 to the MiVoice Connect server's IP address, and set option 67 to /tsk/vxworks.
  - 6 flashes — Using a previously stored IP address. A DHCP transaction was attempted, but the DHCP server did not respond. The switch continues to use the IP address stored in nonvolatile memory until it receives a valid response. If the switch receives a response that provides a different IP address, it reboots using the new IP address. If the switch receives a response that matches the IP address stored in nonvolatile memory, it continues operation, and the power LED stops flashing. If the problem persists, check the DHCP server and network configuration.

23.8.1.2.1 Switch Port LEDs

The SG24A has 24 telephone/trunk port LEDs. The color of the LED indicates the port function:

- Green when the port is a telephone port.
- Yellow when the port is a trunk port.
- Off indicates the port is reserved for IP phones, for conferencing, or is not configured.

The following describes the switch port LED behavior and meaning:

- Telephone Port LEDs (Green)
  - When on steady, the port is configured as a telephone port and the telephone is idle.
  - When flashing with ring cadence, the telephone is ringing
  - When flashing slowly, the telephone is off hook.
  - When flashing fast, the port is in use (call in progress)
- Trunk Port LED (Yellow):
  - When on steady, the port is configured as a trunk port and the trunk is idle
  - When flashing slowly, the trunk is off hook.
  - When flashing fast, the trunk is in use (call in progress).
- Port LED Alternating Green/Yellow: The port is out of service. The LED periodically alternates green/yellow or yellow/green. The color of the LED between alternating colors indicates the port type: green for phone and yellow for trunk.
- Off (IP phone): When the LED is off, the port is reserved for IP phones, for conferencing, or is not configured.

23.8.1.2.2 Network LEDs

The network LEDs (LAN1 and LAN2) indicate the speed at which the switch is communicating with the network and whether there is network activity.

The network LED descriptions are as follows:

- Link/Activity: When lit, this LED indicates that the switch is connected to an Ethernet network. This LED indicates network activity, as follows:
  - When flashing, network activity is detected.
  - When on (not flashing), the switch is connected to an Ethernet network.
  - When off, the switch cannot detect an Ethernet network.

  This LED is not directly related to any switch's individual network activity. For example, if three switches are connected to the same hub and one switch's Traffic LED shows activity, the other switches will indicate the same activity.
- 100M
  - When green, the switch is connected to a 100BaseT network.
  - When off, the switch is connected to a 10BaseT network.

23.8.1.3 SG24A Connectors

The SG24A voice switch contains the following components:

- 1 3.5 mm mono connector for audio input (music on hold)
- 1 3.5 mm mono connector for audio output (overhead paging and night bell)
- 1 DB-9 socket connector for maintenance
- 2 RJ-45 connectors for the LAN interface
- 1 RJ-11 connector for connecting an analog phone (extension 9)
- 1 RJ-21X plug connector for mass termination of the telephone/trunk ports

23.8.1.4 SG24A RJ-21X Telephone and Trunk Connector

SG24A RJ-21X Telephone and Trunk Connector Pins lists the RJ-21X Ring and Tip pin numbers for the SG24AI.

Table 71: SG24A RJ-21X Telephone and Trunk Connector Pins

Port	Type	Ring		Tip	
		Pin #	Cable Color	Pin #	Cable Color
1	Extension	1	Blue/White	26	White/Blue

Port	Type	Ring		Tip	
		Pin #	Cable Color	Pin #	Cable Color
2	Extension	2	Orange/White	27	White/Orange
3	Extension	3	Green/White	28	White/Green
4	Extension	4	Brown/White	29	White/Brown
5	Extension	5	Slate/White	30	White/Slate
6	Extension	6	Blue/Red	31	Red/Blue
7	Extension	7	Orange/Red	32	Red/Orange
8	Extension	8	Green/Red	33	Red/Green
9	Extension	9	Brown/Red	34	Red/Brown
10	Extension	10	Slate/Red	35	Red/Slate
11	Extension	11	Blue/Black	36	Black/Blue
12	Extension	12	Orange/Black	37	Black/Orange
13	Extension	13	Green/Black	38	Black/Green
14	Extension	14	Brown/Black	Black/ Brown	39
15	Extension	15	Slate/Black	40	Black/Slate
16	Extension	16	Blue/Yellow	41	Yellow/Blue
17	Extension	17	Orange/Yellow	42	Yellow/Orange

Port	Type	Ring		Tip	
		Pin #	Cable Color	Pin #	Cable Color
18	Extension	18	Green/Yellow	43	Yellow/Green
19	Extension	19	Brown/Yellow	44	Yellow/Brown
20	Extension	20	Slate/Yellow	45	Yellow/Slate
21	Extension	21	Blue/Violet	46	Violet/Blue
22	Extension	22	Orange/Violet	47	Violet/Orange
23	Extension	23	Green/Violet	48	Violet/Green
24	Extension	24	Brown/Violet	49	Violet/Brown
–		25	Slate/Violet	50	Violet/Slate

Appendix D - Installing Mitel Connect Client on Citrix and WTS

This chapter contains the following sections:

This appendix describes how to install the Mitel Connect client for WTS or Citrix on Windows servers.

24.1 Overview

You can install the Mitel Connect client for Windows servers that are using Citrix XenApp, Citrix XenDesktop, or Windows Terminal Services (WTS) to provide MiVoice Connect functionality to terminal services clients.

Citrix XenApp hosts published applications that can be accessed from remote Windows clients. Citrix XenDesktop maps remote Windows clients to their dedicated desktops, and their desktops host applications such as Mitel Connect client. This mapping is a one-to-one mapping. WTS, also known as Remote Desktop Services, hosts published applications that can be accessed from remote Windows clients.

For detailed information on Citrix XenApp, Citrix XenDesktop, and Windows Terminal Services, refer to the documentation from the manufacturer.

For simplicity, the remainder of this appendix refers to the XenApp and XenDesktop products as Citrix.

24.2 Citrix Support Considerations

This section provides information about best practices and restrictions when installing the Mitel Connect client for Windows in a Citrix environment.

24.2.1 Citrix Environment Best Practices

Mitel recommends the following best practices for computers running the Mitel Connect client on Citrix servers/systems:

- Use only Citrix-ready anti-virus software on XenApp/XenDesktop servers.
- Run XenApp/XenDesktop and MiVoice Connect servers on a Citrix-qualified server platform.
- Perform frequent defragmentation of the Citrix server disk.
- Co-locate the Citrix/WTS server with the Headquarters server.

Note:

To prevent the user from receiving a warning message about enhanced security, Mitel recommends that you disable Enhanced Security on the Microsoft server running Citrix or Windows Terminal Services

24.2.2 Citrix Restrictions

Mitel Connect client for Windows does not support the following Citrix operations:

- Streaming mode
- Application Isolation Environment (AIE)

The following Mitel Connect client for Windows features are not supported in the Citrix XenApp environment:

- SoftPhone
- 1:1 Video

24.3 Windows Terminal Server Support Considerations

This section provides information about restrictions when installing the Mitel Connect client for Windows Terminal Server (WTS) in a Windows Server environment.

Note:
The number of clients supported for WTS is 30 per server.

24.3.1 Windows Terminal Server Restrictions

The following Mitel Connect client for WTS features are not supported in the Windows Server environment:

- SoftPhone
- 1-1 Video
- Recording or playing voicemail and greetings through speakers

24.4 Installing Citrix for MiVoice Connect

Install and configure the necessary components for your implementation of Citrix. See https://www.citrix.com/ for information, instructions, and downloads.

If you are using XenApp, you must add the Mitel Connect client after you finish installing and configuring Citrix. See the Citrix documentation for information about how to add applications using the Citrix Delivery Groups functionality.

24.4.1 Installation Considerations

Citrix includes the following core components. See the Citrix documentation for more information.

- Delivery Controller
- Studio
- Director
- License Server
- StoreFront
- Virtual Delivery Agent (VDA)

When installing Citrix using the manufacturer instructions, consider the following:

- Citrix — Install the Delivery Controller on the primary server, and then install all components except the VDA and Director components on a separate server using the same installer.
- XenDesktop — All desktops must be running Windows Server or Windows workstation versions as required by XenDesktop.
- XenApp — Needs only one Windows Server where the Mitel Connect client is installed for the VDA component.
- Citrix — Install the VDA component on each of the XenDesktop systems and only on the primary server for a XenApp configuration.
- XenApp — Install the Mitel Connect client on the server where VDA is installed in previous step for XenApp. See Installing MiVoice Connect on WTS or Citrix on page 421 for more information about this installation procedure.
- XenDesktop — Install the Mitel Connect client on all the Windows systems where VDA is installed. See Installing MiVoice Connect on WTS or Citrix on page 421 for more information about this installation procedure.

24.5 Installing MiVoice Connect on WTS or Citrix

MiVoice Connect is supported on the following platforms:

- Windows Server 2012 R2 (Standard and Data Center)
- Windows Server 2016
- Windows Server 2019
- Citrix 7.15 LSTR

24.5.1 Preliminary Steps for Upgrading MiVoice Connect on 64-bit Platforms

The Mitel Connect client for Windows requires .NET Framework version 4.6 or higher on 64-bit Windows Terminal Services platforms.

Mitel does not ship the .NET Framework as part of the software package, but if it is not installed already, it is downloaded and installed as part of the Mitel Connect client installation process.

Note:

If the .NET Framework is not installed on the target terminal server and the .NET Framework file in the Mitel folder is empty, the target terminal server must be able to access the Internet so that the .NET Framework can be downloaded during the Mitel Connect client installation process.

24.5.2 Installing the Mitel Connect Client on a Terminal Server

Note:

Administrative rights on the terminal server are required in order to install the Mitel Connect client for Windows.

1. Open a browser on the terminal server.
2. Enter the following URL: **http://<Connect_server_name>/ShoreWareresources/clientinstall**

Note:

Connect_server_name is the name or IP address of the Headquarters server that manages the client software for the MiVoice Connect server

The MiVoice Connect Install page for Windows is displayed.

3. Review the information on this page, then click **Click Here to Install MiVoice Connect**.

Note:

The download process starts, and the InstallShield Wizard is launched.

4. Follow the prompts to install the Mitel Connect client.

Note:

On 64-bit systems, the installation process places files in this folder by default:

- `C:\Program Files (x86)\Shoreline Communications\ShoreWare Server \ShoreWare Resources\ClientInstall`

5. Using Remote Desktop Client on the Windows client system, connect to the server where the Mitel Connect client is installed.
6. Launch the Mitel Connect client and enter login credentials and server information.

24.6 Installing the Microsoft Office Outlook Add-in

WTS and Citrix 7.15 LTSR support the Microsoft Office Outlook add-in for Mitel Connect Client.

This add-on feature enables support for contact import, conference scheduling, availability state, and Outlook presence.

Note:

You must install Microsoft Outlook before installing Mitel Connect Client.

To install Microsoft Office Outlook add-in, do the following:

1. Log on to the Citrix server for the desired individual user.
2. Start the Mitel Connect client, which installs the Outlook add-in automatically.

24.7 Adding Mitel Connect Client Application in Citrix XenApp

You can add the MiVoice Connect application in Citrix XenApp by using the Delivery Groups functionality in Citrix Studio. A Delivery group is a collection of machines selected from one or more machine catalogs. The Delivery group specifies which users can use those machines, and the applications available to those users.

Note:

In XenDesktop, the Mitel Connect client must be installed on each of the desktops created when you installed and configured Citrix. Also, for XenDesktop, the Mitel Connect client is not part of the delivery groups in Citrix studio; it is part of the whole desktop.

To add the MiVoice Connect application in a delivery group:

1. Launch the Citrix Studio.
2. Click **Delivery Groups** in the **Studio** navigation pane.
3. Click **Applications** tab and then select **Create Applications** in the **Actions** pane.

   A list displays the applications that were discovered on the App-V management server (Reviewer, see earlier comment in the Installing Citrix for MiVoice Connect section).
4. Choose an application to add to the delivery group.
5. Select or add StoreFront URLs that will be used by the Citrix Receiver that is installed on each machine in the Delivery group.

You have successfully added the Mitel Connect client in Citrix Studio.

24.7.1 Launching MiVoice Connect Application on Citrix XenApp

To add MiVoice Connect application on the user's desktop when the user is using Citrix XenApp:

1. Launch a browser, and then enter the URL created in Citrix studio for the site.

   For example, the URL may be similar to http://<FQDN>/Citrix/XenApp.
2. Install the Citrix Receiver.
3. Log in to the Citrix server from the Citrix Receiver, and then launch the Mitel Connect client.
4. Enter your Mitel Connect client login credentials and server information.

You have successfully launched the Mitel Connect client on the user’s desktop.

24.8 Supported Limits

The following limits apply for the Mitel Connect client on Citrix and WTS servers.

24.8.1 XenApp System Configuration

- MiVoice Connect

  Refer to the build notice for specific software build versions.
- XenApp 7.15 LTSR
- Complete the following steps on the Citrix VDA server:

  1. Enable the Remote Desktop Session Host Windows Installer using gpedit.
  2. Browse to Computer Configuration\Administrative Templates\Windows Components\Remote Desktop Services\Remote Desktop Session Host\Application Compatibility.
  3. Set Turn off Windows Installer RDS Compatibility to Enabled. Run the installer again.

- System configurations:
  - (Main) Citrix Server:
    - Windows Server 2012 R2 64-bit
    - RAM — 16 GB
    - CPU — 8 cores at2.70 GHz
  - (Main) Citrix Server:
    - Windows Server 2016
    - RAM — 16 GB
    - CPU — 8 cores at 2.70 GHz
  - (Main) Citrix Server:
    - Windows Server 2019
    - RAM — 16 GB
    - CPU — 8 cores at 2.70 GHz
  - (Dir) Citrix Server:
    - Windows Server 2012 R2 64-bit
    - RAM — 16 GB
    - CPU — 8 cores at 2.70GHz
  - (Dir) Citrix Server:
    - Windows Server 2016
    - RAM — 16 GB
    - CPU — 8 cores at 2.70 GHz
  - (Dir) Citrix Server:
    - Windows Server 2019
    - RAM — 16 GB
    - CPU — 8 cores at 2.70 GHz
  - (VDA) Citrix Server:
    - Windows Server 2012 R2 64-bit
    - RAM — 16 GB
    - CPU — 16 cores at 2.70 GHz
  - (VDA) Citrix Server:
    - Windows Server 2016
    - RAM — 16 GB
    - CPU — 16 cores at 2.70 GHz
  - (VDA) Citrix Server:
    - Windows Server 2019
    - RAM — 16 GB
    - CPU — 16 cores at 2.70 GHz
  - Client:
    - Windows 10
    - RAM — 4 GB

    - CPU — 2 cores at 2.11 GHz
  - Client:
    - Windows 11
    - RAM — 4 GB
    - CPU — 2 cores at 2.11GHz

Limitations:

- Desk phones only
- No softphone support
- No 1:1 video support
- 30 Citrix clients per server, 20 calls per hour per XenApp client. If you need more than 30 clients, add a Citrix server to accommodate the additional clients.

> **Note**:
>
> The user may experience slow performance for the XenApp client with performance becoming slower and slower until the XenApp client appears to be non-responsive. Viewing server performance may reveal a lack of memory. For optimal performance, Mitel recommends that users restart the Mitel Connect client every 2-3 days.

- Disable system notifications for incoming calls — In the Mitel Connect client, navigate to **Settings** > **Notifications** > **Popup** and ensure **Show a system notification for an incoming Call** is not selected.

24.8.2 XenDesktop System Configuration

- MiVoice Connect
  - XenDesktop 7.15 LTSR
  - 10 XenDesktop servers
  - Citrix Main server and Citrix Dir server are each running on a separate Windows Server 2012 R2 (Standard or Datacenter Editions only) (64-bit version). Each server has 16 GB RAM and a CPU of 8 cores at 2.7GHz
- (Main) Citrix Server:
  - Windows Server 2012 R2 64-bit
  - RAM — 16 GB
  - CPU — 8 cores at 2.70 GHz
- (Main) Citrix Server:
  - Windows Server 2016
  - RAM — 16 GB
  - CPU — 8 cores at 2.70 GHz

- (Main) Citrix Server:
  - Windows Server 2019
  - RAM — 16 GB
  - CPU — 8 cores at 2.70 GHz
- (Dir) Citrix Server:
  - Windows Server 2012 R2 64-bit
  - RAM — 16 GB
  - CPU — 8 cores at 2.70 GHz
- (Dir) Citrix Server:
  - Windows Server 2016
  - RAM — 16 GB
  - CPU — 8 cores at 2.70 GHz
- (Dir) Citrix Server:
  - Windows Server 2019
  - RAM — 16 GB
  - CPU — 8 cores at 2.70 GHz
- Client:
  - Windows 10
  - RAM — 2GB
  - CPU — 2 cores at 2.11 GHz
- Client:
  - Windows 11
  - RAM — 2 GB
  - CPU — 2 cores at 2.11 GHz
- There are no other applications running on the client except for a few browser sessions.

The results of this testing show that the amount of the RAM on the server determines the number of Connect clients supported. Ten Connect clients were tested against a server with 16 GB RAM. Mitel surmises that 128 GB of RAM supports no more than 50 clients. In most cases, this estimate allows for adequate spare memory to support other non-client activities.

The following table is designed to provide memory size estimates for clients running in a Citrix XenDesktop environment.

Table 72: XenDesktop System Configuration for Client

Number of Clients	Recommended Server Quantity and RAM Size
50	One server with at least 128 GB
50 to 100	One server with 256 GB

Number of Clients	Recommended Server Quantity and RAM Size
101 to 150	One server with 256 GB supporting 100 clients. Additional server with at least 128 GB supporting remaining clients
151 to 200	Two servers with 256 GB per server. One server supports 100 clients, and the second server supports the remaining clients.
201 to 250	Two servers with 256 GB per server. Each server supports 100 clients. One server with at least 128 GB supporting remaining clients
251 to 300	Three servers with 256 GB per server. Two servers support 100 clients each, and the third server supports the remaining clients.
301 to 350	Three servers with 256 GB per server. Each server supports 100 clients. One server with at least 128 GB supporting the remaining clients.
351 to 400	Four servers with 256 GB per server. Three servers support 100 clients per server, and the fourth server supports the remaining clients.

24.8.3 WTS System Configuration

- Hardware configurations:
  - WTS Server:
    - Windows Server 2012 R2 64-bit
    - RAM — 16 GB
    - CPU — 16 cores at 2.70 GHz
  - WTS Server:
    - Windows Server 2016
    - RAM — 16 GB
    - CPU — 16 cores at 2.70 GHz
  - WTS Server:
    - Windows Server 2019
    - RAM — 16 GB
    - CPU — 16 cores at 2.70 GHz
  - Client:
    - Windows 10
    - RAM — 4 GB
    - CPU — 2 cores at 2.11GHz
  - Client:
    - Windows 11
    - RAM — 4 GB
    - CPU — 2 cores at 2.11 GHz
- Complete the following steps on the WTS:

  1. Enable the Remote Desktop Session Host Windows Installer using gpedit.
  2. Browse to Computer Configuration\Administrative Templates\Windows Components\Remote Desktop Services\Remote Desktop Session Host\Application Compatibility.
  3. Set Turn off Windows Installer RDS Compatibility to Enabled. Run the installer again.

- Limitations:
  - Desk phones only.
  - No softphone support
  - No 1:1 video support
  - Users cannot play voicemail using PC/laptop speakers
  - 30 Citrix clients per server, 20 calls per hour per WTS client. If you need more than 30 clients, add a Citrix server to accommodate the additional clients.

Note:

The user may experience slow performance for the WTS client with performance becoming slower and slower until the WTS client appears to be non-responsive. Viewing server performance may reveal a lack of memory. For optimal performance, Mitel recommends that users restart the Mitel Connect client every 2-3 days.

- Disable system notifications for incoming calls — In the Mitel Connect client, navigate to **Settings** > **Notifications** > **Popup** and ensure **Show a system notification for an incoming Call** is not selected.

Appendix E - Capacities and Specifications

This chapter contains the following sections:

This appendix describes the details about capacities and specifications for MiVoice Connect.

25.1 Hardware and Network Requirements

Table 73: New Switch Hardware / Network Requirements

Switch	IP	SGT1 / SGE1	SIP Max*	FXO	FXS	Conf Inc	Conf Max*	Hg PG	BCA	PFT	BHCC	Long Loop
ST50A	50		8	4	4	6	14	24	36	yes	450	
ST100A	100		14	8	6	12	26	24	36	yes	1800	
ST100DA	100	1	38	2	6	12	50	24	36	yes	1800	
ST1D		1	30								7200	
ST2D		2	60								14400	
ST200	200					12	12	24	36		3600	
ST500	500					24	24	24	36		7200	

Switch	IP	SGT1 / SGE1	SIP Max*	FXO	FXS	Conf Inc	Conf Max*	Hg PG	BCA	PFT	BHCC	Long Loop
ST24A					24		48	24	36		3600	yes
ST48A					48		48	24	36		7200	yes
Virtual SW			1000			60*		40*	120		25000	
Virtual TR			1000									

Note:

* These are the maximum parameters depending on VMware specifications.

Table 74: Legacy Switch Hardware / Network Requirements

Switch	IP	Built-In	PRI	MP*	SIP BRI	FXO	FXS	MB	MB
SG30	30	10				2	2		
SG30BRI	30	10			1		2		
SG50	50	20				4	2		
SG50V	50	20				4	2	50	5
SG90	90	30				8	4		
SG90V	90	30				8	4	90	9
SG90BRI	90	30			4		4		

Switch	IP	Built-In	PRI	MP*	SIP BRI	FXO	FXS	MB	MB
SG90BRIV	90	30			4		4	90	9
SG220T1	220	70	SGT1	20					
SG220T1A	220	70	SGT1	20		2	4		
SG220E1	220	70	SGE1	20					
SGT1K	0	0	SGT1	20					
SG24A	0	0					24		

Note:

* These are the maximum parameters depending on VMware Specifications

Table 75: Hardware / Network Requirements for Service Appliance

Service Appliance	Capacity	Max Size of Conference
SA100	Codec: G711/G729 50 Audio Codec: G722 15 Audio 50 Web, 500 IM	Max 16 Conferences, upto 400 Hours of conference data, max 5 units per system image.
Small VSA	Codec: G711/G729 50 Audio Codec: G722 15 Audio	Max 25 Conferences

Service Appliance	Capacity	Max Size of Conference
	50 Web, 500 IM	
SA400	Codec: G711/G729 200 Audio Codec: G722 60 Audio 200 Web, 2000 IM	200 Audio, 200 Web, Max 64 Conferences, up to 1000 hours of conference data, max 5 units per system image.
Large VSA	Codec: G711/G729 200 Audio Codec: G722 60 Audio	200 Web, 2000 IM Max 100 Conferences

Table 76: Hardware / Network Requirements for Mobility Router

Mobility Router	Capacity	Additional Notes
2000 Series	10-100 Endpoints	PB and UC Integration, Security Integration, App Layer Security, Policy Management, Reporting and trending.
4000 Series	10-1000 Endpoints	All of the above and plus High Availability

Table 77: Supported Codecs

Codec	Sample Rate	Data Rate
L16/1600 (Linear Broadband)	16 KHz	256 Kbps
L16/8000 (Linear)	8 KHz	128 Kbps
G.711 μ-law (PCMU)	8 KHz	64 Kbps
G.711 A-law (PCMA)	8 KHz	64 Kbps

Codec	Sample Rate	Data Rate
G.722	16 KHz*	32 Kbps
G.729a	8 KHz	8 Kbps
iLBC	8 KHz	13.33 Kbps
AAC_LC	32 KHz	
BV-32	16 KHz	32 Kbps
BV-16	8 KHz	16 Kbps
DV-14	8 KHz	
T.38		

Note:

* In network traces, G.722 often appears as “G722/8000” even though it should be “G722/16000”. This is due to an historical error in notation. Mitel follows the Internet Engineering Task Force recommendation of maintaining the G722/8000 notation.

Table 78: Typical Bandwidth Use for Connect Client

Connect Client	Bandwidth Use
Phone Only	.2 Kbps
Connect Client	.2 Kbps
Operator Extension Monitor	.2 Kbps + 1.5 Kbps 1.5 Kbps per monitored extension
Workgroup Agent	.25 Kbps

Connect Client	Bandwidth Use
Queue Monitor	6.5 Kbps per queued call
Workgroup Supervisor Queue Monitor Agent Monitor	.25 Kbps 6.5 Kbps per queued call 1.5 Kbps per agent

Table 79: Hardware Requirements

Ingate Feature /Model No.	SIParator 21	SIParator 52	SIParator 22	SIParator 42	Software SIParator
Interfaces (10/100/1000 Mbit/s)	4	6	4	6, 2 Gbps opt	HW dependent
Power consumption (typical)	25 W	100 W	10 W	20 W	HW dependent
Max numbers of VLANs (802.1q)	32	128	32	128	HW dependent
SIP Connection set up, max calls/s	40	60	40	60	100
RTP data delay (10 Mbps/100 Mbps) network	0.19/ 0.08 ms	0.19/ 0.08 ms	0.02/0.07 ms	0.02/0.07 ms	0.02/0.05 ms
Max number of concurrent calls (20 ms G.711 voice packets)	400	2,000	800	2,000	20,000
Secure VoIP sessions (TLS+SRTP)	300	1,500	550	1,100	8,000

Table 80: Voice Mail Hard Disk Space

# Endpoints	# Messages	Length (minutes)	Storage (hours	Storage (GB)
100	15	1	25	0.8 GB
500	15	1	125	3.8 GB
2,500	15	1	625	18.8 GB

Table 81: Call Detail Records

# Calls/Day	# Calls/Month (20 da ys)	Storage/Month	Storage/ 3 Months
100	2,000	3 MB	9 MB
1,000	20,000	30 MB	90 MB
10,000	200,000	300 MB	900 MB
50,000	100,0000	1,500 MB	4,500 MB

Note:

20 working days per month (4 weeks/month X 5 days/week = 20)

Table 82: Voice Mail Options

Voicemail Options	Application Server	Distributed Applicat ion Server	V Voice Appliances
100	2,000	3 MB	9 MB
1,000	20,000	30 MB	90 MB
10,000	200,000	300 MB	900 MB

Voicemail Options	Application Server	Distributed Application Server	V Voice Appliances
50,000	100,0000	1,500 MB	4,500 MB

Table 83: Hard Disk Space Minimum Requirements for Applications

Type	Space Required
Connect Headquarters Server	1600 MB
DVS Server	800 MB
Connect client	600 MB

Note:

Additional space to install the client might be necessary if you are installing from off the network. In this situation, the process creates a copy of the installer.

Table 84: Log File Hard Disk Space

File Size	Storage
Minimum	0.5 GB
Default	4.0 GB
Maximum	30.0 GB

25.2 License and Phone Requirements

Table 85: License and Descriptions

License	Description
Virtual Switch Licenses	

License	Description
Virtual Phone	One license required for call controlled device, which includes Anon ymous, VPN, Mobility, Softphones. Bundles Available.
Virtual SIP Trunk	One license required for SIP Trunk, which includes SIP Media Pro xy. SIP Trunk Software License not required with Virtual switch.
Virtual SA	Free with Audio and Web License.
Edge Gateway	Free with Standard and Advanced, used for Secure connection to r emote clients and phones.
Ingate SIParator Traversal License	One license required for SIP trunk connected to Ingate SIParator appliances and Software SIParator.
Applications Server	
Add Language License	One license required for each additional language per system ima ge.
SIP Trunk Software License	One license required for SIP trunk connected to Voice appliances.
SIP Device License	One license required for third-party SIP device (Not required for 400 and 6900 series).
SIP Based Third-Party messaging integrat ion License	Used to connect to Third-Party Party Voice mail system via SIP, for example Microsoft Exchange.
Distributed Voice Services License	Used to allow large network design, voice mail optimization, work gr oup or database resiliency. (refer to system capacity) or to integrate with Third-Party Applications.
Additional Site License	One license required for all remote sites from HQ. Design recomm endation is to have one for every site to allow HQ Server portability.
Unified Communications	
Audio Conferencing	One license required for concurrent audio conference port Works with SA100,SA400 and Virtual SA.
Web Conferencing	One license required for concurrent desktop sharing session. This works with SA100, SA400 and Virtual SA.
License, Remote Phone for Edge Gateway	Used to enable Internet audio connectivity for users on a conference without a Connect Client.
Connect Profiles	
Courtesy	Ext only, No VM, No client, No add-ons.
Telephony	Ext + Mbx, Ad hoc Third-Party audio-conferencing, Not for client, No add-ons.
Essentials	Ext + Mbx, Connect client including softphone and video, Ad hoc 8-party audio conferencing, IM and Collaboration (Service Appliance required), Web and App Dialer, Connect for Mobile (Mobility Router required), Connect for Chrome (Edge Gateway required) and Con nect Telephony for Microsoft.
Standard	Essentials + Remote Phone (Edge Gateway) and SFDC/other CRM.
Advanced	Standard + Workgroup Agent, Workgroup, Supervisor, or Operator. Purchase entitles user to one of the included licenses.

25.3 Server Requirements

Server types in this section are provided for reference only. All other customer-provided servers should be benchmarked against the information provided in this table to ensure equivalent or better performance. CPU benchmarking is available at: www.cpubenchmark.net/.

Note:
The requirements for a server that processes real-time audio and video data are different from those for a traditional file or database server, especially regarding network configuration. A one-second delay in packet forwarding might be negligible during a file transfer, but it could cause substantial disruption to an audio call. This requirement has strong implications especially for virtual servers, where call operations can be negatively impacted when there is insufficient network availability due to shared resources.

Table 86: Headquarters Server Capacity and Hardware Requirements (New Server/Existing Server) - Part 1

Server Size	Max Endpoints per System	Max Endpoints per Server (Phones Managed by Switches Managed by Server)	Max System BHCC	BHCC per Server (Reports run outside of business hours)	Maximum BHCC per Server (Reports run during business hours)
Small Business Edition Class					
UC 25 (Small Business Edition 100)	100	100	1,000	1,000	Not recommended
UC 30 (Small Business Edition 100)	100	100	5,000	2,500	Not recommended
Small	100	100	5,000	2,500	Not recommended
Medium	500	500	5,000	2,500	Not recommended
Large	2,500	1,000	25,000	5,000	1,000
Diagnostics and Monitoring Standalone Server					
Standalone D&M Server	2,500	Not Applicable	50,000	Not Applicable	Not Applicable

Table 87: Headquarters Server Capacity and Hardware Requirements (New Server/Existing Server) - Part 2

Server Size	Processor	RAM	Disk Space	Network
Small Business Edition Class				

Server Size	Processor	RAM	Disk Space	Network
UC 25 (Small Bus iness Edition 100)	Celeron J1900 /2.0 GHz	4 GB	500 GB	100 Base-T or Gi gabit Ethernet
UC 30 (Small Bus iness Edition 100)	Intel Xeon E3-1225 v5 3.3 GHz	8 GB	1 TB - Default drive (minimum requir ement: 500 GB)	100 Base-T or Gi gabit Ethernet
Small	Intel Xeon E3-1225 v5 3.3 GHz	8 GB	500 GB	100 Base-T or Gi gabit Ethernet
Medium	Intel Xeon E5-2620 v3 2.4 GHz	8 GB	500 GB	100 Base-T or Gi gabit Ethernet
Large	Intel Xeon E5-2640 v3 2.6 GHz	12 GB	500 GB	Gigabit Ethernet
Diagnostics and Monitoring Standalone Server				
Standalone D&M S erver	Intel Xeon CPU E 5-2640 v3 @2.6 G Hz – 2 processors	4 GB		Gigabit Ethernet

Note:

- All other servers should be benchmarked against the information provided in this table to ensure equivalent or better performance. CPU benchmarking is available at: www.cpubenchmark.net/.
- BHCC (Busy Hour Call Completion) per system is the total number of system calls during the busy hour including internal and external calls, calls terminated to desk phones, softphones, trunks or server applications such as voicemail.
- BHCC per server is based on the number of calls actually handled by the server during the busy hour including workgroup calls in menus and queues, auto-attendant calls, and calls to the voicemail service.
- By default, the report generation tools that run on the server have a lower priority than other more critical services. Low-demand report generation should have little or no effect on a server with adequate performance specifications. If you are a heavy report user or experience any degradation of voicemail or other server prompts on an underpowered server, you must move up to the next tier level of servers.
- Report generation has an impact on system performance. Mitel recommends that customers run reports outside of business hours. If you need to run reports during business hours, the supported calls per server for the medium and large server tiers is reduced as noted in the table.

Table 88: Distributed Voice Server Capacity Requirements (New Server/Existing Server) - Part 1**

Server Size	Max Endpoints per System	Max Endpoints per Server (Phones Managed by Switches Managed by Server)	Max System BHCC	BHCC per Server (Reports run outside of business hours)	Maximum BHCC per Server (Reports run during business hours)	Processor
UC 25 with SBE 100 license	100	100	1,000	1,000	Not recommended	Celeron J1900, 2-2.4 GHz
UC 30	500	500	5,000	2,500	Run on HQ	Intel Xeon E3-1225 v5 3.3 GHz
Small	100	100	5,000	2,500	Run on HQ	Intel Xeon E3-1225 v5 3.3 GHz
Medium	500	500	25,000	5,000	Run on HQ	Intel Xeon E3-1275 v5 3.6 GHz
Large	2,500	2,500	50,000	10,000	Run on HQ	Intel Xeon E3-1275 v5 3.6 GHz

Table 89: Distributed Voice Server Capacity Requirements (New Server/Existing Server) - Part 2**

Server Size	RAM	Disk Space	Virtual Cores Max	Network
UC 25 with SBE 100 license	4 GB	500 GB	NA	100 Base-T or Gigabit Ethernet
UC 30	8 GB	1 TB - Default drive (minimum requirement: 500 GB)	NA	100 Base-T or Gigabit Ethernet

Server Size	RAM	Disk Space	Virtual Cores Max	Network
Small	8 GB	500 GB	NA	100 Base-T or Gigabit Ethernet
Medium	8 GB	500 GB	NA	100 Base-T or Gigabit Ethernet
Large	8 GB	500 GB	NA	Gigabit Ethernet

25.4 Virtual Server / Appliance Requirements

To ensure adequate real-time system performance, follow these criteria for virtual servers:

- If the physical host's network interface card (NIC) for MiVoice Connect HQ NIC is 1Gigabit card, use a dedicated NIC. If the NIC is a 10-Gigabit or 40-Gigabit card, then the network traffic can be shared with other virtual servers.
- The virtual machine CPU and memory must be reserved or dedicated to the guest computer so that real-time communications are not delayed while being allocated to the host resources.
- A dedicated NIC can be shared with all MiVoice Connect virtual appliances. Total bandwidth use must be considered. If the real-time audio is impacted, then the appliances using real-time audio (for example, LDVS, UCB, and so on.) must be moved to their own dedicated NICs.
- Never use a 100-Mbit Ethernet for any MiVoice Connect virtual server.

Table 90: VMware or Hyper-V Capacity and Server Requirements for Headquarters Server

Server Size	Max Endpoints per System	Max Endpoints per Server (Phones Managed by Switches Managed by Server)	Max System BHCC	Max BHCC per Server (Reports run outside of business hours)	Max BHCC per Server (Reports run during business hours)	Processor	Virtual Cores	RAM per VM	Disk Space	Network
Small	100	100	5,000	1,000	Not recommended	Intel Xeon E3-1275 v5 3.60 GHz	4	4 GB	200 GB	Gigabit Ethernet (dedicated) or 10GB shared
Medium	500	500	5,000	2,500	1,000	Intel Xeon CPU E5-2630 v4 2.2 GHz	4	4 GB	200 GB	Gigabit Ethernet (dedicated) or 10GB shared
Large	2,500	1,000	25,000	5,000	1,000	Intel Xeon CPU E5-2630 v4 2.2 GHz	4	8 GB	200 GB	Gigabit Ethernet (dedicated) or 10GB shared

Table 91: VMware or Hyper-V Capacity and Server Requirements for a Windows DVS

Server Size	Max Endpoints per System	Max Endpoints per Server (Phones Managed by Switches Managed by Server)	Max System BHCC	BHCC per Server (Reports run outside of business hours)	Max BHCC per Server (Reports run during business hours)	Processor	Virtual Cores	RAM per VM	Disk Space	Network
Small	100	100	5,000	1,000	Run on HQ	Intel Xeon E3-1275 v5 3.60 GHz	2	4 GB	200 GB	100 Base-T or Gigabit Ethernet
Medium	500	500	5,000	2,500	Run on HQ	Intel Xeon CPU E5-2630 v4 2.2 GHz	2	4 GB	200 GB	100 Base-T or Gigabit Ethernet
Large	2,500	1,000	25,000	5,000	Run on HQ	Intel Xeon CPU E5-2630 v4 2.2 GHz	4	8 GB	200 GB	Gigabit Ethernet

Table 92: VMware or Hyper-V Capacity and Server Requirements for a Linux DVS

Server Size	Max Endpoints per System	Max Endpoints per Server (Phones Managed by Switches Managed by Server)	Max System BHCC	BHCC per Server (Reports run outside of business hours	Max BHCC per Server (Reports run during business hours)	Processor	Virtual Cores	RAM per VM	Disk Space	Network
Small	100	100	5,000	1,000	Run on HQ	Intel Xeon E3-1275 v5 3.60 GHz	2	4 GB	200 GB	100 Base-T or Gigabit Ethernet
Medium	500	500	5,000	2,500	Run on HQ	Intel Xeon CPU E5-2630 v4 2.2 GHz	2	4 GB	200 GB	100 Base-T or Gigabit Ethernet
Large	2,500	1,000	25,000	5,000	Run on HQ	Intel Xeon CPU E5-2630 v4 2.2 GHz	4	8 GB	200 GB	Gigabit Ethernet

Table 93: UC75 Server Capabilities for Deploying Several Applications (using VMware or Hyper-V)

Server Size	Max Endpoints per System	Max Endpoints per Server (Phones Managed by Switches Managed by Server)	Max System BHCC	BHCC per Server (Reports run outside of business hours)	Max BHCC per Server (Reports run during business hours)	Processor	Virtual Cores Max	RAM	Disk Space	Network
With SBE 100 license	100	100	5,000	2,500	Not recommended	Intel Xeon E3-1275 v6 3.8 GHz	12	16 GB	2 drives 1 TB RAID1 array	100 Base-T or Gigabit Ethernet
With Enterprise License	500	500	5,000	2,500	Not recommended	Intel Xeon E3-1275 v6 3.8 GHz	12	16 GB	2 drives 1 TB RAID1 array	100 Base-T or Gigabit Ethernet

Table 94: VMware or Hyper-V Capacity and Server Requirements for Virtual Service Appliance

Server Size	G711	G722	G729	Secure Web Sessions	IM	Processor	Virtual Cores	RAM per VM	Disk Space	Network
Small	50	15	50	50	500	Intel Xeon E3-1275 v5 3.60 GHz	4	2 GB	100 GB	100 Base-T or Gigabit Ethernet
Large	200	60	200	200	2,000	Intel Xeon CPU E5-2630	8	6 GB	100 GB	Gigabit Ethernet

Server Size	G711	G722	G729	Secure Web Sessions	IM	Processor	Virtual Cores	RAM per VM	Disk Space	Network
						v4 2.2 GHz				
IM-only	0	0	0	0	2,000	Intel Xeon E3-1275 v5 3.60 GHz	2	2 GB	20 GB	Gigabit Ethernet

Note:

The above numbers are recommendations. You can allocate fewer virtual processor cores, but monitor the performance load to ensure that CPU utilization is less than 75 percent.

Table 95: Virtual and Physical Service Appliance Features and Capacity Requirements

Feature	SA100	Small VSA	SA400	Large VSA
Audio with SRTP				
Max G711 Audio Ports	50	50	200	200
Max G.729 Audio Ports	50	50	200	200
Max G.722 Audio Ports	15	15	60	60
Max audio conferences	16	25	64	100
Web with HTTPS				
Max number of web (HTTPS) endpoints	50	50	200	200
Max attendees per conference	50	50	200	200
IM with TLS				
Max number of IM endpoints	500	500	2000	2000
Capacity Requirements				
CPU Cores/Speed	4/2.9 GHz	4/2.9 GHz	24/2.9 GHz	8/2.9 GHz

Feature	SA100	Small VSA	SA400	Large VSA
Memory	2 GB	2 GB	6 GB	6 GB
Hard Disk	250 GB/500 GB	100 GB (thin)	500 GB	500 GB (thin)
Data Storage*	210 GB/460 GB	60 GB	460 GB	460 GB
Web ports	50	50	200	200
IM ports	500	500	2000	2000
Recording Hours Max	1044/2089	280	2089	2089
Recording Hours/ Web User	20/41	5.5	10	10

Note:

*Excluding hard disk spaces for the operating system, root file system, and applications.

Table 96: VMware or Hyper-V Virtual Server Requirements for Ingate SIParator

Number of Trunks	Up to 100	Up to 200	Up to 1,000
Memory	500 MB	1 GB	2 GB
Cores	1	2	4
Disk	20 GB	20 GB	20 GB
Processor	Intel Xeon CPU E5-2630v4 at 2.2 GHz*		

Table 97: VMware or Hyper-V Mobility Router

Max Number of Endpoints	Max Number of local Wi-Fi clients	Max Num of local Wi-Fi calls (not bridged through SMR)	Max Num of Remote Tunnels	Max Num of Secure Remote Voice Calls using Default Encryption	Max Num of Remote calls that require transcoding	Virtual Cores	RAM per VM	Disk Space	Network	Network Interfaces
100	100	100	100	100	50	2	2 GB	100 GB	100 Base-T or Gigabit Ethernet	2
1,000	1,000	1,000	1,000	300	150	4	4 GB	100 GB	100 Base-T or Gigabit Ethernet	2
Processor	Intel Xeon E3-1275 v5 3.60 GHz									

Table 98: Mobility Router Appliance Capacity

Mobility Router	Max Endpoints	Max Calls	Max Calls with Transcoding	Max SRV Endpoints	Max SRV Calls
2000	100	100	50	100	20
4000	1000	500	300	500	200
6000	5000	2000	1250	2500	1000
Virtual	1000	500	300	500	200

Table 99: VMware or Hyper-V Virtual SIP Trunk Switch (G.711 Signaling)

Max SIP Trunks managed by Switch without Advanced Feature	Total Number of Streams	Virtual Cores	Processor	RAM per VM	Disk Space	Network
50	100	1	Intel Xeon E3-1275 v5 3.60 GHz	2 GB	20 GB	100 Base-T or Gigabit Ethernet
100	200	2	Intel Xeon E3-1275 v5 3.60 GHz	2 GB	20 GB	100 Base-T or Gigabit Ethernet
200	400	4	Intel Xeon CPU E5-2630 v4 2.2 GHz	2 GB	20 GB	Gigabit Ethernet
400	800	7	Intel Xeon CPU E5-2630 v4 2.2 GHz	2 GB	20 GB	Gigabit Ethernet
600	1,200	10	Intel Xeon CPU E5-2630 v4 2.2 GHz	2 GB	20 GB	Gigabit Ethernet
1,000	2,000	16	Intel Xeon CPU E5-2630 v4 2.2 GHz	2 GB	20 GB	Gigabit Ethernet

Note:

- Every core can handle up to 125 streams in G.711 signaling.
- Basic calls utilize two streams. Advanced features (Call Recording and Three-Party Conferencing) require one additional stream. Carefully consider how you will use advanced features when planning for capacity and hardware requirements.
- The numbers in this table are recommended guidelines, but you can choose to provision above these numbers. However, you must monitor the performance of your virtual machines and ensure that CPU utilization does not exceed 75 percent.

Table 100: VMware or Hyper-V Virtual SIP Trunk Switch (G.729 Signaling)

Max SIP Trunks managed by Switch without Advanced Feature	Total Number of Streams	Virtual Cores	Processor	RAM per VM	Disk Space	Network
25	50	1	Intel Xeon E3-1275 v5 3.60 GHz	2 GB	20 GB	100 Base-T or Gigabit Ethernet
50	100	2	Intel Xeon E3-1275 v5 3.60 GHz	2 GB	20 GB	100 Base-T or Gigabit Ethernet
100	200	4	Intel Xeon CPU E5-2630 v4 2.2 GHz	2 GB	20 GB	100 Base-T or Gigabit Ethernet
200	400	7	Intel Xeon CPU E5-2630 v4 2.2 GHz	2 GB	20 GB	Gigabit Ethernet
300	600	10	Intel Xeon CPU E5-2630 v4 2.2 GHz	2 GB	20 GB	Gigabit Ethernet

Max SIP Trunks managed by Switch without Advanced Feature	Total Number of Streams	Virtual Cores	Processor	RAM per VM	Disk Space	Network
500	1,000	16	Intel Xeon CPU E5-2630 v4 2.2 GHz	2 GB	20 GB	Gigabit Ethernet

Note:

- Every core can handle up to 50 streams in G.729 signaling.
- Basic calls utilize two streams. Advanced features (Call Recording and Three-Party Conferencing) require one additional stream. Carefully consider how you will use advanced features when planning for capacity and hardware requirements.
- The numbers in this table are recommended guidelines, but you can choose to provision above these numbers. However, you must monitor the performance of your virtual machines and ensure that CPU utilization does not exceed 75 percent.

Table 101: VMware or Hyper-V Virtual IP Phone Switch

Max phones managed by switch	Virtual Cores	RAM per VM	Disk space	Network
1,000	1	2 GB	20 GB	100 Base-T or Gigabit Ethernet
Processor		Intel Xeon E3-1275 v5 3.60 GHz		

Table 102: VMware or Hyper-V Edge Gateway - Part 1

Size	Virtual Cores	RAM per VM	Disk Space	Networks	Processor
Small	2	2 GB	100 GB	100 Base-T or Gigabit Ethernet	Intel Xeon E3-1275 v5 3.60 GHz

Size	Virtual Cores	RAM per VM	Disk Space	Networks	Processor
Medium	4	4 GB	100 GB	Gigabit Ethernet	Intel Xeon CPU E5-2630 v4 2.2 GHz
Large	8	8 GB	100 GB	Gigabit Ethernet	Intel Xeon CPU E5-2630 v4 2.2 GHz

Table 103: VMware or Hyper-V Edge Gateway - Part 2

Size	400-Series IP Phones Using RAST: Registered	400-Series IP Phones Using RAST: Active Calls	Clients: Registered	Clients: Concurrent Voice Calls
Small	100	50	50	50
Medium	500	100	400	100
Large	2,000	200	2,000*	200

Table 104: VMware or Hyper-V Edge Gateway - Part 3

Size	AIC Registered with KPI Dashboard**	AIC Registered with KPI Dashboard + Client Registered	Contact Center: Concurrent Voice Calls
Small	200	50	50
Medium	200	200	100
Large	200	200	100

Note:
Combinations of RAST connections and Client connections are limited to a maximum of 2,000. Similarly, the 200 maximum Calls value applies to combinations of RAST and Softphone calls.

Note:
The Clients Registered can either be Connect Client or Chrome Plugin or a combination of both Connect Client and Chrome Plugin.

Note:
* A maximum of 2000 connections is applicable for existing softphone user registrations and 500 concurrent connections for first-time softphone user logins. Only the first-time user request goes to the HQ server. After the login is successful, a corresponding server will be assigned and later all the subsequent login requests goes to the assigned server.

Note:
**AIC refers to the Agent Interaction Center web page. See the *Reverse Proxy > Client Endpoint* section in the MiVoice Connect Administration Guide for Edge Gateway for more information. The KPI Boards feature allows you to configure the Interaction Center to include key performance information (KPI) about specific interactions. For more information, see the *Using KPI Boards* section in the MiVoice Connect Contact Center Administration Guide.

25.5 System Capacities

Table 105: System Capacities

Component	Capacity	Notes
System		
Sites	500	Exact number varies by configuration.
Switches	100/site 100/system 100/server	Exact number varies by configuration.
Route Points	254/server	This is per server
Analogue Ports	2,500	Exact number varies by configuration.
IP Phones	2,500 (max)	Exact number varies by configuration. See Headquarters Server Capacity and Hardware Requirements (New Server/Existing Server) - Part 1 and Headquarters Server Capacity and Hardware Requirements (New Server/Existing Server) - Part 2 for size and traffic considerations.
Simultaneous Calls	1,500	1,500 calling 1,500
Busy Hour Call Completion	25,000	Depending upon server configurations.
Endpoints		

Component	Capacity	Notes
Endpoints	2,500	While the maximum capacity for a single-image system is 2,500 endpoints, larger deployment sizes are possible with prior approval from Mitel. Larger System_Designs must be reviewed by Sales Engineering and approved by Product Management and TAC. Consult with your Mitel sales repr esentative to initiate this process if required.
– Port Based Endpoin ts	500	
– IP Phone Endpoints	2,000	
– Virtual Endpoints	1,000 per server	
Endpoint Groups	250	
Telephony Permissions	100	
Call Permissions	100	
Voice Mail Permissions	100	
Trunks		
Trunks	1,500	
Trunk Groups	1,500	
Number of Trunks/TG	500	
Servers		
Number of servers	21	1 main, 20 distributed (for voice mail, autoattendant, m essaging, directory, configuration services, and desktop cal l control). Each server is certified to support up to 1,000 endpoints.
Number of Voice-mail Box Switches (VMBs)	500/system 100/server	20
Number of Third-Party SIP Servers	20	
Media streams (G.711 per server)	254	
Media streams (G.729 per server)		
Media streams (total)	9,384	
Voice Mail		
Mailboxes (total)	2,500	These can be distributed across servers.
Mailboxes (per server)	1,000	
Storage	Unlimited	
Auto-Attendant		
Menus (total)	1,000	
Hunt Groups		

Component	Capacity	Notes
Hunt groups per SG s witch	8	
Total hunt group mem bers per hunt group (SG switches)	16	
Hunt groups per ST s witch	24	
Total hunt group mem bers per hunt group (ST switches)	24	
Total hunt group mem bers per hunt group on virtual switches	16	
Workgroups		
Workgroups per s ystem	256	
Members per work group	300	
Workgroup Agents per system	300	
Workgroup Agents	16	Simultaneous ring
Calls in Queue per Q ueue	254/server	Overflow is directed to the workgroup backup extension.
BHCC/system without reports during busin ess hours	Large HW = 10,000 Med HW = 5,000 Small HW = 2,500	See Headquarters Server Capacity and Hardware Requirements (New Server/Existing Server) - Part 1 and Headquarters Server Capacity and Hardware Requirements (New Server/Existing Server) - Part 2 for size and traffic considerations.
BHCC/system with rep orts during business hours	Large HW = 5,000 Med HW = 1,000 Small HW = not recommended	See Headquarters Server Capacity and Hardware Requirements (New Server/Existing Server) - Part 1 and Headquarters Server Capacity and Hardware Requirements (New Server/Existing Server) - Part 2 for size and traffic considerations.
Paging Groups		
Paging Groups (total)	300/system	
Paging Group Mem bers	300/system	
Max # of simultaneous pages	100/server	
Account Codes		

Component	Capacity	Notes
Account Codes (per system)	100,000/system	
Call Detail Record		
Storage	1.5 GB (MySQL has a capacity of 64 TB)	500,000 Workgroup calls, or 1.5 million extension-to-extension calls, or1.0 million combined call records implementing a database of this size typically requires 4.0 GB of disk space, including disk space for the main database (1.5 GB), the archive database (1.5 GB), and temporary space required to generate reports (1.0 GB).
Connect Client		
Connect Client	2,000/system 1,000/server	
Softphone endpoints	2,000/system 250 on Headquarters server 400/Linux DVS 250/Windows DVS	If softphones are used with resource intensive features (such as workgroups, hunt groups, route points, simultaneous ring, and BCA/SCAs), the maximum number of supported softphone endpoints per Headquarters server, Linux DVS, and Windows DVS would be 30 percent lower.
Phone Only	2,000	Number of phones that can be managed using the Connect Client
Workgroup Agent	300/server 300/system	
Workgroup Supervisor	128/server 128/system	
Operator	200	Up to 500 monitored extensions per operator, depending on the value of the Max buddies per user field on the Telephony Features Permission page in Connect Director.
Music on Hold (MOH)		
File-based music on hold	255 calls/server	
Jack-based Music on Hold	36 calls	One switch can provide up to 36 MOH streams.
Programmable Buttons		

Component	Capacity	Notes
IP phone buttons con figured for extension monitoring (per switch)	1024	
Phones that can moni tor an extension	32	
Voice Switch Capacity		
Media streams/switch (No encryption)	60	
Media streams/switch (encryption)	60	
Media streams/switch (SRTP)	40	
Media streams/switch (SRTP + authenticat ion)	30	
G.711 Limits for VMB	9	
G.729 Limits for VMB	5	
BAA Simultaneous # of calls - Voice Switch	60	
Simultaneous # of ca lls SIP Ringing - Voice Switches -G.711	60	
Simultaneous # of ca lls SIP Ringing - Voice Switches -G.729	0	

25.6 Real Time Capacities

Table 106: Major Differences in Features Supported on SBE 100 and EE

Feature	SBE 100	Enterprise Edition
Sites	5	500
Switches	7	500
Endpoints (with extensions)	100 (Small Business Edition system key) 200 (Enterprise Edition system key)	2,500

Feature	SBE 100	Enterprise Edition
Telephones	100	2,500
Trunks	100	1,500
Simultaneous calls, extension-to-extension	50	1,500
Busy Hour Call Completion	1,000	25,000
Distributed Voice Server	4	20
Integration with MiVoice Connect system or third-party PBX (for example, through tie trunks)	No	Yes
On-net dialing	No	Yes
Voice mailboxes	120	500/system 100/server
Simultaneous calls per server	25	254
AMIS	No	Yes
SMDI - External voicemail	No	Yes
SMDI - MiVoice Connect voicemail	No	Yes
Service Appliance 100 (SA100)	2	5
SA100 audio/web/IM ports	100/50/100	256/300/128
Service Appliance 400 (SA400)	No	Yes
Virtual Service Appliance	1	5

Feature	SBE 100	Enterprise Edition
Workgroups (groups, agents, supervisors)	100/100/100	256/300/128
Mobility clients	100	5,000
Distributed features: Workgroups, database, paging, account codes	No	Yes

Note:

- The SBE 100 was previously available with a Mitel-provided server, and now must be deployed with a customer-provided server. The server supplied by the customer must meet the minimum server requirements as indicated below.
- The SBE 100 can be upgraded to the Enterprise Edition (EE).
- The Headquarters server must be at least dual-core and have 4GB of RAM.

Table 107: Feature Capacities for ST and SG Voice Switches

	Hunt Group	Bridged Call Appearance	Pickup Group	IP Phones
Extension/Group	SG: Up to 8 groups ST: Up to 24 groups	SG: 24 ST: 36	SG:16 ST:24	SG: 120
Members/ extensions	Refer to Total members on all extensions below	SG: 32 ST: 44 Phones monitoring for same extension	SG:24 ST:24	N/A
Stack size/ extensions	SG: 16 ST: 24	SG: 24 ST: 36	N/A	SG: 24

	Hunt Group	Bridged Call Appearance	Pickup Group	IP Phones
Total members on all extensions	SG: 16 ST: 16	N/A	SG:80 ST:80	N/A

Table 108: Virtual Phone Switch Feature Capacities

Feature	Up to 1000 Phones
Backup Auto-attendant Streams	50
Make Me Conferences	60
Extension monitor buttons	5,000
BHCC	25,000
Hunt Groups*	
Total hunt groups	24
Total hunt-group endpoints	160
Endpoint per hunt group	16
Pick-up Groups*	
Total pick-up groups	80
Total pick-up group endpoints	400
Users per pick-up group	24
Bridged Call Appearances (BCA)	
Total BCA	120
BCA call stack	24
BCA extensions	32

Real Time Capacity features in a virtual phone switch, which can be run in parallel, provided you keep within the above parameters.

*The maximum number of endpoints per feature group on a virtual switch is variable depending on the size and configuration of the virtual system. Watch the Diagnostics and Monitoring system (Maintenance menu) in Connect Director to ensure that the virtual system is not overloaded.

25.7 Contact Center Capacities and Requirements

Table 109: Contact Center Element Capacities

Contact Center	Max Value
Max Configured Agents	2000

Contact Center	Max Value
Max Simultaneous Agents	1000
Max DNIS Routes	1500
Number of Agent Groups	256
Number of Agent Queues	1000
Max number of groups to which an agent can belong	64
Max Skills	512
Max Wrap Up/ Release Codes	512
Max Secondary Announcements	20
Max IVR Ports per server	254
Max Calls in Queue per server	254
Max Agent Boards	256
Max Active Supervisors	100
Max Wallboards/Agent-boards	256
Database Backup Periodicity	1 a day
Maximum interactions	15,000 calls (voice, email, and chat) per hour with up to 600 agents, 10,000 calls (voice, email, and chat) per hour with 601 to 1000 agents.
Max IRN	1500

Contact Center	Max Value
Max Active Supervisors tested in performance	15
Maximum number of scheduled reports in an hour	10
Wallboard API Feed Active?	Yes
Agent Board API Feed Active?	Yes
CCIR Enabled?	Yes

Table 110: Contact Center Hardware Capacities

PC Requirements	Supervisor PC running CC only	Supervisor PC with CC and Client	Agent PC running CC only	Agent PC with CC and client
CPU	Pentium IV 2.0 GHz	Dual Core 1.6 GHz	Pentium III 800 MHz	Pentium IV 2.0 GHz
Available Memory	1 GB	1 GB	512 MB	1 GB
Hard Disk Space	2 GB	2 GB	1 GB	1 GB
CD	Optional			
First Network Adapter	10/100 MB			
External Modem	Optional			
Windows 7/ Windows 8 Operating System				

Table 111: Contact Center License Requirements

License	Description
System	The node-locked system license key is required for all systems.
Voice	The maximum number of agents, who log into a group require a license to handle incoming and outbound voice calls, which can be logged into the system concurrently.

License	Description
Email	The maximum number of agents, who log into a group require a license to handle incoming email contacts, that can be logged on the system concurrently.
Chat	The maximum number of agents, who log into a group that require a license to handle incoming chat contacts, which can be logged into the system concurrently.
Dial Lists	The maximum number of agents, who log into a group that require a license to handle outbound dial lists calls, which can be logged into the system concurrently.
IVR Ports	The maximum number of IVR ports the system will use. Note that you have to additional IVR ports than the number for which you have license. This allows you to use IVR stations to create redundant IVR stations.
Supervisor	The maximum number of supervisors that can be logged into the system concurrently. Contact Center currently supports up to 100 concurrent supervisors.
Redundancy	Enables running the Contact Center system in a redundant configuration.
Agent Activity API	The number of external applications able to connect and receive agent data.
Group Activity API	The number of external applications able to connect and receive group data.

Table 112: Contact System Server Requirements

Size	ACD Agents per System	Max ACD BHCA	Processor/Server	Min RAM	Networks	Free Disk Space
Small	<300	7500	Intel Core 2 Duo E8400, Single DualCore 3.00 Ghz Intel Core i3-540 Processor	4 GB	100 Base-T or Gigabit Ethernet	200 GB

Size	ACD Agents per System	Max ACD BHCA	Processor/Server	Min RAM	Networks	Free Disk Space
			(4M Cache 3.06 GHz) Intel Xeon 3430 Single QuadCore 2.4 Ghz			
Medium	300-600	15000	Intel Xeon 5520 Single QuadCore 2.27 GHz	8 GB	100 Base-T or Gigabit Ethernet	200 GB
Large	600-1000	10000	Intel Xeon 5520 Dual QuadCore 2.27 GHz	8 GB	100 Base-T or Gigabit Ethernet	200 GB
IVR Server	250 ports per server		Intel Core 2 Duo E8400, Single DualCore 3.00 Ghz Intel Core i3-540 Processor (4M Cache 3.06 GHz) Intel Xeon 3430 Single QuadCore 2.4 GHz	4 GB	100 Base-T or Gigabit Ethernet	500 GB

Table 113: Virtual CC System Requirements

System Size	Num of Agents	Call Load per System	Cores per VM RAM per VM	Disk size for CC System	Server
Small	< 100	7,500	2	4 GB	200 GB
Medium	100-599	15,000	4	8 GB	500 GB
Large	600-1,000	10,000	4	8 GB	750 GB

25.8 Call Data Record Database Size Recommendations for MiVoice Connect

MiVoice Connect logs every call in the Call Data Record (CDR) database, which is stored on the HQ server. If that database grows too large, it can affect server performance, which in some cases can interfere with normal phone system functions. This section provides recommendations for the maximum CDR size based on testing by the Mitel QA Lab.

The size of the CDR database (DB) must not exceed 1.5 million records, which is about 4 GB of disk space as seen in the `C:\Shoreline Data\Database\ShoreTelCDR\Data` folder.

For systems in which the CDR DB has grown beyond 1.5 million records, it is strongly recommended that the System Administrator reduce the DB size on the HQ by using one of these methods:

- Lower the retention period for CDR data under the **Report Options** screen of Connect Director to retain fewer days' data in the CDR DB.
- Set up a CDR archive database to offload Call Data Records to a separate database or external server (reports can still be run from this database).

With 1.5 million CDR records, the following were observed:

- The CDR database size is 4 GB.
- Trunk Activity Detail Reports (25% of the total number of CDR records contained trunk activity) ran in 3 minutes 30 seconds.
- Workgroup Agent Detail Reports (5% of the total number of CDR records involved workgroup activity) ran in 5 minutes.
- While the reports were running, the system worked normally, and the CPU, memory, and disk performance were within normal limits.

Note:
The numbers given here were measured on a system configuration with normal phone activity occurring. Given the number of variables involved, the numbers given here might not be representative for every system.

25.9 Ingate Benchmarking

The MiVoice Connect system can scale incrementally up to 2,500 Teleworker endpoints (IP phones). Endpoints must be distributed among all the DVS servers over the entire system.

25.10 Ingate Concurrent Calls

A MiVoice Connect system supports a maximum of 800 concurrent teleworker calls in large system configurations.

Following is the required system configuration and Ingate software SIPrator configuration for a MiVoice Connect sysetm:

Table 114: System configuration and Ingate software SIPrator configuration

Servers/Ingate	CPU	RAM	Disk Space
HQ server	4 cores	8 GB	300 GB
DVS servers	4 cores	8 GB	300 GB
Software SIPrator	12 cores	16 GB	100 GB

Note:
To support a higher number of concurrent calls (more than 300 concurrent calls), you must change the media port allocations from standard to **40000 - 60999** and modify the **Port Allocation Ranges** accordingly by going to **Basic Configuration** > **Advanced Settings** in Ingate. Following is the configuration:

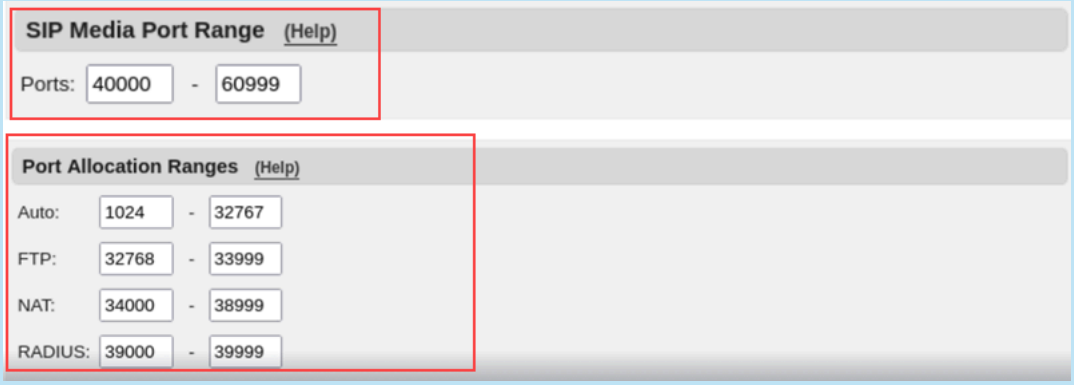


Figure 54: Port allocation ranges