A MITEL
PRODUCT
GUIDE

MiVoice Business

Engineering Guidelines

Release 9.4

Document Version 1.0

September 2022

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

About this Document 1

This chapter contains the following sections:

1.1 Overview

Note:
The Release Number mentioned in the Front Page of the published document indicates that the document is updated for that release. However, all the documents posted in a release are applicable to the current product release.

These guidelines will assist you in planning an installation of a MiVoice Business Communications Platform. The guidelines describe specific areas of the product that need to be considered before installation. Also, field experience highlights specific areas that might not have previously been covered. These guidelines should not be considered as a comprehensive list, but as useful reminders or pointers that should be considered before installation.

The contents of this document gather general platform guidelines together. Where there are guidelines that are specific to a feature or a particular use of a product, then this document may contain references to those specific documents. Typical examples of this include references to "Resiliency" or use of IP networking and Clustering configurations where specific documents can provide more extensive detail.

In planning an installation other documents should also be referenced in addition to these Engineering Guidelines; most of these documents can be found on the Mitel Document Center web site.

1.2 About Mitel MiVoice Business

Mitel® MiVoice Business is the brand name of the call-processing software that runs on several hardware platforms including industry standard servers, virtual machines, and the Mitel 3300 ICP.

Note:
As of MiVoice Business Release 9.2, port 3999 (unsecure) is no longer accessible and port 3998 (secure) will be exclusively used for communication between MiVoice Business and the supported MiNET sets. Firewall configuration changes must be made to ensure continued operation of connected sets.

1.3 What's new in this Document

This section describes changes in this document due to new and changed functionality in the MiVoice Business Release 9.4. The changes are summarized in the following table.

Table 1: Document Version 1.0

Feature/Enhancement	Document Updates	Location	Publish Date
Port diagrams	Modified the port diagrams.	MiVoice Business and 3300 IP Ports on page 166	May 2022
IP Trunk backward Compatibility	Updated the compatibility restrictions for IP Trunks and for SDS.	Networking and Product Release Compatibility on page 101	March 2022
Added support for new 69xx device types.	Updated the MiVoice IP Phones section for 69xx sets.	MiVoice IP Phones on page 66	March 2022

1.4 About the MiVoice Business Documentation Set

Mitel Product Documentation

Documents for MiVoice Business and other Mitel® products are available in the Mitel Document Center.

The following guides provide complete information about the MiVoice Business:

- *Technician's Handbook:* installation, upgrade, maintenance, troubleshooting instructions.

- *Hardware Technical Reference Manual:* hardware specifications.
- *System Administration Tool Help for MiVoice Business:* programming, maintenance, and troubleshooting.
- *Resiliency Guidelines:* overview of the Mitel Resiliency solution and the tools to understand, plan, and implement a resilient network.
- *Migration Guidelines:* guidelines for migrating pre-9.0 systems to 9.0.
- *EX Controller Deployment Guide:* installation, upgrade, maintenance, and troubleshooting instructions.
- *Security Guidelines:* secure deployment and operation of the MiVoice Business system.
- *General Information Guide:* General product overview including deployments, architecture, products and features.
- *Safety Instructions:* to be read BEFORE installation.
- *Clustering Design and Implementation* (Download document and associated .xls files): Cluster planning and installation guide for migrating to and using SDS sharing, Multi-Node Management.
- *Site Planning Guide:* Product installation checklist.

To access the product documentation follow the steps below:

1. Go to https://www.mitel.com/
2. Click **SUPPORT**.
3. On the left panel under **Customer Support**, click **Technical Documentation**.
4. Click **BUSINESS PHONE SYSTEMS > MIVOICE BUSINESS**.

Product Bulletins

To access Mitel Product Bulletins follow the steps:

1. Log on to MiACCESS Portal.
2. In the left pane, click **InfoChannel**.
3. In the select **InfoChannel** list, select **Mitel-Worldwide**.
4. In the left pane, click **Product Bulletins & Announcements**.

Mitel Knowledge Base Articles

To access Mitel Knowledge Base Article follow the steps:

1. Log on to MiACCESS Portal.
2. In the left pane, click **Knowledge Management System**.

Additional Documentation

The following documentation is related to deploying IP phones and can be found on other Mitel websites:

- Mitel IP Sets Engineering Guidelines
- Network Engineering for IP Telephony
- Wireless Telephony, Planning and Troubleshooting
- Ethernet Twisted Pair Cabling Plant, Power and Grounding Guidelines

Related Tools

The following tools related to configuring MiVoice Business systems for specific customer traffic and user requirements are available on InfoChannel Worldwide under the Technical Training menu, look for Technician's Toolbox:

- MiVoice Business System Engineering Tool
- Mitel Streamline Power Calculator

1.5 System Management Tools

The System Administration Tool, the Group Administration Tool and the Desktop Tool are GUI based tools for configuring and administering MiVoice Businessand MiVoice IP Phones. The System Management Tools are accessed via an internet browser.

For MiVoice Business Release 8.0, IE 11 or later with the latest service pack and Mozilla Firefox 36.0.4 or later.

For MiVoice Business Release 9.0, IE 11 or later with the latest service pack, Mozilla Firefox 36.0.4 or later, Google Chrome 59 or later and Microsoft Edge 38 or later.

For MiVoice Business Release 9.1, Mozilla Firefox 36.0.4 or later, Google Chrome 59 or later and Microsoft Edge 38 or later

1.6 About the MiVoice Business System Engineering Tool

Most systems can be engineered, in terms of their hardware components, from the fairly simple rules presented in these guidelines. The Mitel sales quotation tool (CPQ) builds in most of these rules. When an installation requires a system that is complex or close to some operating limits, contact Mitel's Customer Engineering Service. The customer service engineers have access to the System Engineering Tool (SET), which can analyze a system and determine in much greater detail the overall hardware requirements and expected performance. This tool will identify the modules required, traffic limits, and the processor Performance Index (PI).

The SET is developed using Microsoft Excel 2013, and tested in versions from 2007 to 2016. It is no longer supported in Excel versions older than 2007. The SET does not work in Excel Online and Open Office, which do not support macros.

System Overview 2

This chapter contains the following sections:

2.1 System Architecture

The MiVoice Business is built upon Mitel's legacy proprietary architecture delivering sophisticated call management, applications and desktop solutions to businesses. Mitel delivers a highly scalable, resilient, and robust call control that fully utilizes the power of IP while fully supporting the traditional TDM-based telephony for legacy devices and PSTN connectivity.

All MiVoice Business platforms use the IP network to connect both internal and external IP telephony devices, while the 3300 and EX appliances provide a supplementary TDM (time division multiplexing) subsystem to switch calls between traditional telephone devices.

The following figure shows how the MiVoice Business 3300 has the advantage of being able to optimally switch both types of traffic, IP or TDM. The PSTN can also be accessed using SIP trunks by any of the MiVoice Business variants.

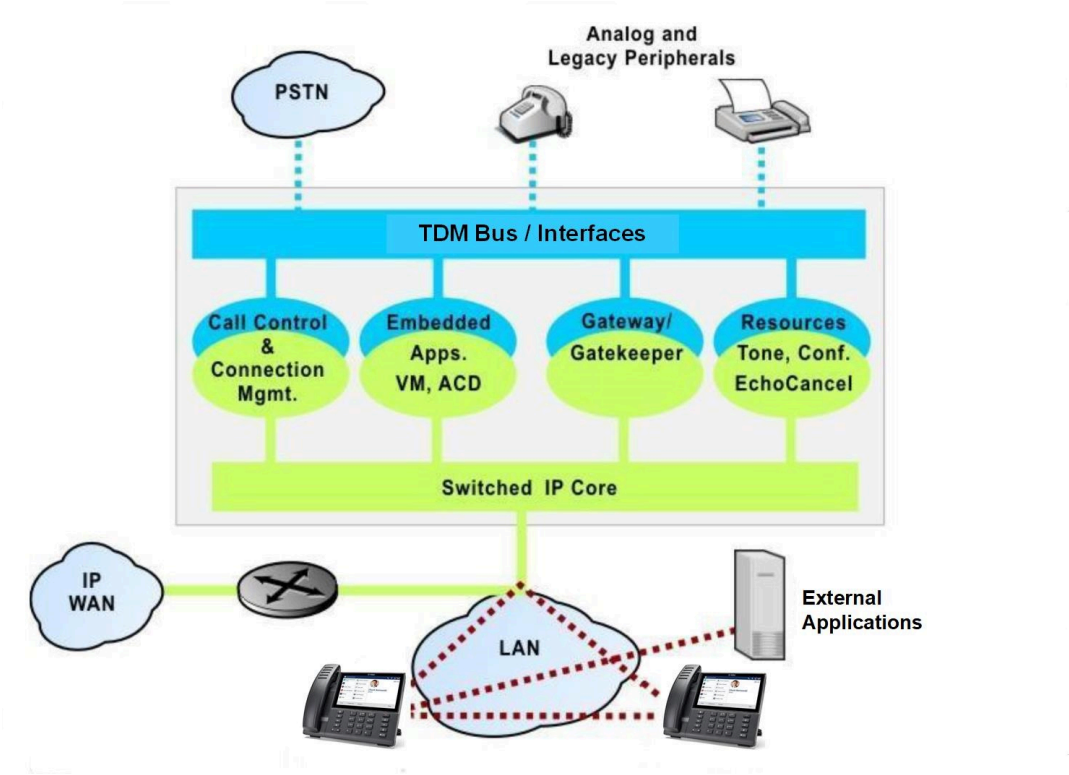


Figure 1: 3300 ICP System Architecture

This ability to use two different switching techniques simultaneously means that

- All traffic is switched with minimum conversion between packet and traditional telephony to provide optimum voice quality in all call scenarios.
- Embedded gateway functionality is required only between the IP and non-IP networks optimizing the use of system resources.
- Migration from traditional PBX to IP telephony is seamless and efficient.

2.2 MiVoice Business Controller

The MiVoice Business controller provides the voice, signaling, central processing, and communications resources for the system. There are several controller configurations supported for release MiVoice Business 9.1 including 3300 ICP Controllers and industry standard servers:

- AX controller with 512MB memory and 16 GB flash card
- CX-II / CXi-II controller with 1024 MB memory
- MXe III Base or Expanded controller with 1024MB memory
- MiVoice Business for Industry Standard Servers (MiVB ISS)
- MiVoice Business Virtual (vMiVB)

- MiVoice Business EX

Note:
All older variants of the 3300 ICP appliances cannot be upgraded to MiVoice Business 9.0 or newer because of their limited memory capacity (fixed at 512 MB).

The functionality of the 3300 controllers can be expanded by installing optional modules such as: Digital Signal Processors (DSP), Dual T1/E1 Framers, Quad BRI Framers, and T1/E1 Combo Modules.

The EX controller can be expanded with a DSP module, PRI Modules, FXS and FXO Modules. The EX DSP and PRI modules are not the same as the CX and MXe modules.

2.3 Supported Countries

During the installation process the MiVoice Business system can be configured for operation in a particular country or region. The Embedded System Management interface (ESM) allows the installer to choose the most appropriate country or region from a list of supported countries and regions. Country/region support includes

- language support for set display prompts
- loss level plans and tone plans that have been specifically designed for the selected country
- analog station and trunk port parameters that have been specifically designed for the selected country.

Currently supported countries and regions include

- Australia
- Brazil
- China
- France
- Germany
- Italy
- Latin America (Argentina, Chile, Mexico)
- Netherlands
- New Zealand
- North America (Canada, USA)
- Portugal
- Spain

- UK.

In some cases MiVoice Business can be deployed in countries that are not included in the above list. In these cases, regional office personnel will be able to suggest the country selection that will provide the best transmission performance.

Note:

Refer to the *Hardware Technical Reference Manual*, available on the Mitel Document Center website, for complete tone plans and loss tables for each of these countries.

Typical Configurations 3

This chapter contains the following sections:

3.1 System Configurations

The MiVoice Business product line includes a number of platforms, IP phones, and applications. Each platform is designed for a different business segment and size, but each contains a number of common components. The main difference between the units is the quantity of components contained in each.

The units are flexible and can be used in a number of different configurations, for example:

- IP-PBX with phones, Voice Mail, and PSTN gateway
- Standalone controller, in conjunction with other units
- Standalone PSTN gateway
- Standalone Voice Mail
- Standalone wireless gateway
- Standalone IP network gateway
- Standalone Teleworker gateway
- Resilient backup controller

The use of the LAN infrastructure and IP networking allows the units to be installed and used in a number of different configurations. It also allows for a more distributed architecture and dispersal of equipment compared to a more traditional central TDM PBX system. MiVoice Businesshas a reliable, mature call control with a large feature set enabling multiple integration possibilities with an existing installation.

The remainder of this chapter describes typical configurations, and provides some sample configurations.Configuration Tablesshow the maximum capacity for each feature or resource for each type of controller.

For more information on the following topics that may affect the system configuration, see:

- *MiVoice Business Technician's Handbook*for Slot Number convention
- *MiVoice Business Hardware Technical Reference Manual*for external interfaces and external TDM interfaces.

3.2 Typical Installation Configurations

The MiVoice Businessplatform can be designed into different network configurations to suit the organization of the enterprise. See the following examples for an illustration of how the organization of the enterprise affects the overall network and unit configurations:

- Multiple Units System

- Distributed System
- Hybrid System

In the descriptions and drawings below, a unit is considered to be a 3300 ICP with a particular configuration and is part of the overall telephony system. With no TDM interfaces this could be any other MiVoice Business variant. A controller may be a standalone system, or one with only users and no PSTN access. In all cases, PSTN access can be either TDM or SIP trunks.

3.2.1 Multiple Units System

In a multiple unit configuration, a number of units are clustered together, but each unit functions independently. The units connect to each other through the network, using IP trunks or TDM trunks. In the event of a unit failure, some of the overall system will fail. In the event of a network failure, the units still maintain PSTN access. In a small- or medium-sized office, a number of units could be installed together to make a larger system. Another scenario could be a small- or medium-sized business with a number of branch offices (for example, an automobile dealership), where local access is needed, but intershop traffic is also a requirement.

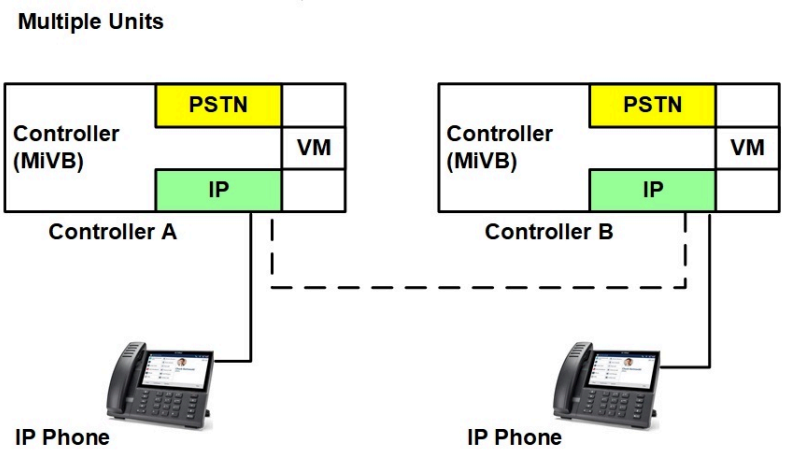


Figure 2: Examples of a Multiple Units Configuration

3.2.2 Distributed System

In a distributed system, different telephony system functions are dedicated to individual units. These are then distributed to different parts of the network, or business as required. This may be a large and geographically dispersed enterprise. For example, a number of units could act purely as TDM gateways providing central access, with other units acting as central voice mail and others acting as the user controllers. An example is a university campus where each building possesses the group controller and local phones, but the PSTN access is in a separate secure building. A different scenario

is a large enterprise with corporate headquarters in different cities. Each would have distributed trunk units and could be considered multiple copies of the campus scenario.

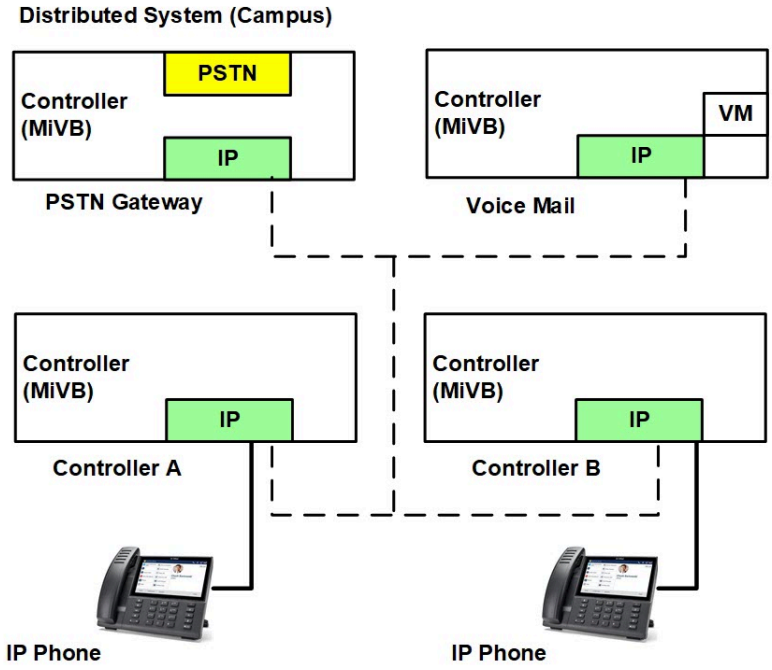


Figure 3: Example of a Campus Environment Configuration

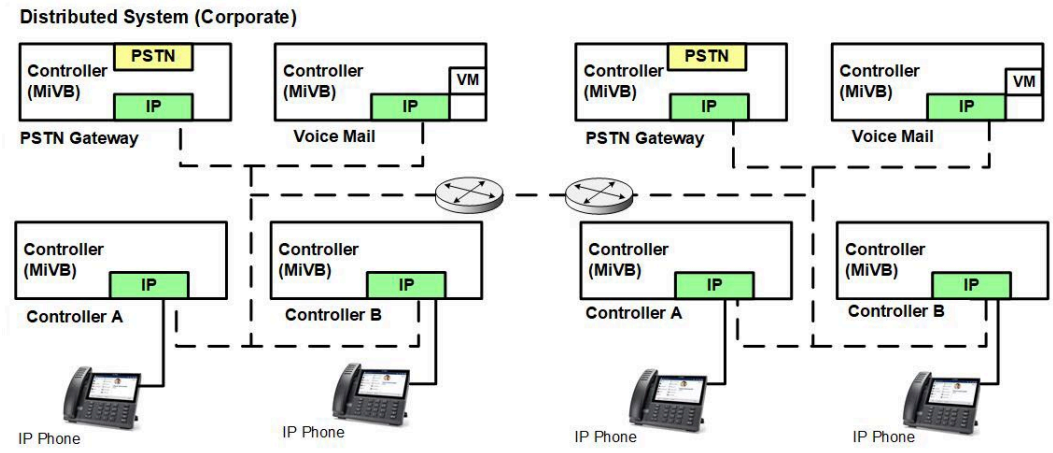


Figure 4: Example of a Corporate Configuration with Multiple HQs

3.2.3 Hybrid System

A Hybrid system combines both of the previous scenarios and involves a distributed system for a headquarters and combined units for remote branch offices. The branch office has access to corporate PSTN access as well as local access through the local

group controller. In the event the WAN link is lost, the separate sites can still operate as independent units.

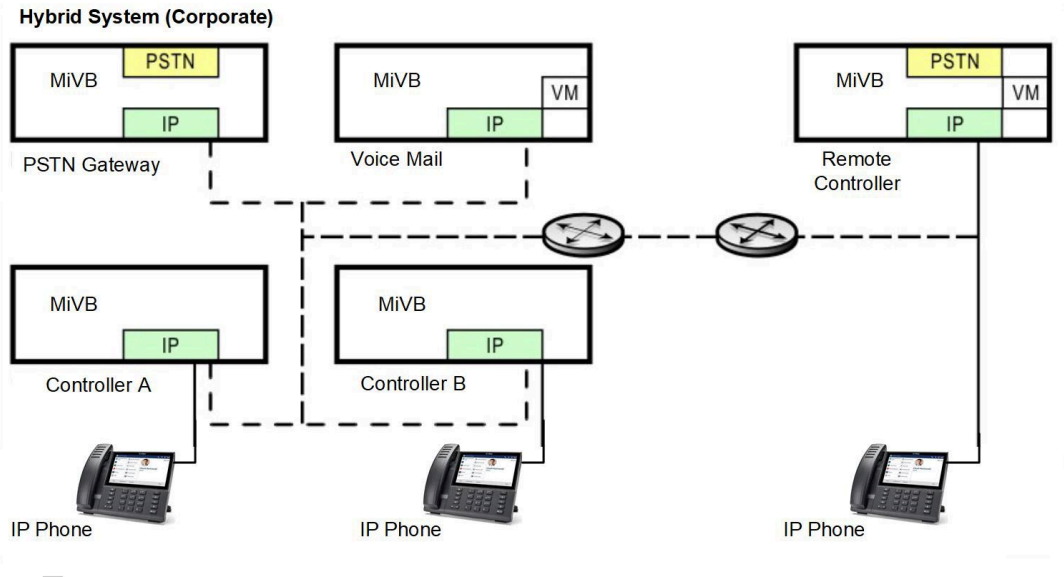


Figure 5: Example of a Hybrid Configuration

3.3 Sample MiVoice Business Configurations

The sections below describe sample configurations:

- MiVoice Business as a Trunk Gateway
- MiVoice Business as a Trunk Tandem
- MiVoice Business and Contact Centers

3.3.1 MiVoice Business as a Trunk Gateway

If a CX II, MXe III or EX is used as a trunk gateway, the unit may act purely as a TDM-to-IP gateway, or it may be a SIP-to-IP Trunk gateway. In either case it will probably not have IP phones registered. If phones are registered, then the number of trunks that can be handled will be reduced. Other controllers will have large numbers of phones connected to them but no PSTN trunks (group controller or user gateway).

The limiting factor on a TDM trunk gateway will usually be the number of E2T (Ethernet to TDM) channels available on it. If a controller that is used as a trunk gateway also acts as a resilient backup for all or some of the IP phones on a group controller, the trunk capacity will not necessarily be affected. The assumption is that when the phones fail over to this controller there will be much less IP trunk traffic to the other controllers in the network.

The trunks are expected to be in use 75% to 100% during busy hour, to be cost effective. Therefore on a TDM gateway the number of trunks and the number of E2T channels are directly linked.

- On the MXe III expanded controller, the maximum number of trunk channels is about 120 channels, or 4 E1 / 5 T1 links (to match the 128 E2T channels) when using 53xx Minet phones and Mitel proprietary voice encryption.
- With SRTP enabled (the only encryption option when connecting to SIP or 69xx series phones) the maximum channel capacity is reduced to 123 channels when all the concurrent calls are SRTP, G711. Existing systems upgrading to Release 9.0 or beyond must consider these limits, and if insufficient be replaced with the EX as a TDM trunk gateway.
- In the MXe III Controller 192 Gateway, the maximum number of trunks would be 180 E1 trunks (6 links) or 192 T1 trunks (8 links) in older releases. The maximum capacity of the E2T card is reduced to 123 (4 E1 links or 5 T1 links) channels when all the concurrent calls are G711, SRTP and to 185 channels when all the concurrent calls are G.729, SRTP. With the E2T limits further reduced below 128 channels with SRTP enabled in 9.0 and 9.1, the 192 Gateway configuration is no longer practical. Available options are to use 53xx series phones with Mitel encryption (default), remove the requirement for encryption entirely, or replace the existing gateway with the EX as a high capacity TDM gateway.
- The CX II system has a typical limit of 60 PRI channels (64 E2T channels) when using 53xx phones and Mitel proprietary encryption. This capacity is retained in release 9.0.
- In the CX II with SRTP enabled for SIP or 69xx phones, the E2T capacity is reduced to 40 channels, and the same options are available to change the encryption or replace the system with the EX.
- In the MiVoice Business EX controller, the maximum number of PRI trunks that can be supported is 240. Since each trunk card has its own DSP and E2T resources, all 240 channels can be used at the same time, on all phone types, with or without SRTP enabled.

When the MiVoice Business is used as a trunk gateway to the PSTN with SIP trunks, the capacity is limited only by the maximum traffic of the controller (voice streams do not go through the box) so that any of the controller variants (appliance, virtual, or ISS, depending on traffic type and volume) may be used for this function.

3.3.2 MiVoice Business as a Trunk Tandem

When the MiVoice Business acts as a Trunk Tandem, it functions similar to that described for the gateway unit using SIP trunks. Typically, this configuration is applied where there is already an established network where the multiple controllers are being used for toll bypass, or as alternative routes to the PSTN.

As with the trunk gateway, the tandem controller does not have end users directly connected. The heavy performance load and/or the limited number of E2T channels in an MXe III or CX II will restrict the capacity of this configuration. The connections for a

tandem configuration may be TDM trunk to TDM trunk, IP trunk to TDM trunk, SIP trunk to TDM trunk, or IP trunk to SIP trunk. The first three require a TDM to IP conversion, and are limited by the number of channels available (same as the TDM gateway), with the best option usually the EX. The last configuration requires no TDM and can be any of the appliances or server variants, depending only on capacity requirements.

3.3.3 MiVoice Business and Contact Centers

A typical call center (ACD) installation consists of several separate components which integrate to make up the complete system. The MiVoice Business components are discussed here, but for more detail on the MiContact Center Business components refer to the MiContact Center Business and MiVoice Analytics

- ACD controller may be either MiVoice Business on a server platform (MiVoice Business for ISS, MiVoice Business Multi-instance, and MiVoice Business Virtual) or either the MXe-III or EX platforms. This can either be all functions in one standalone controller, or a network of trunk gateways and agent controllers.
- MiContact Center Business, for reporting and some interactive functions.
    - Interactive Voice Response (IVR), the auto-attendant function, which may also act as a source for recorded announcements (RADs).

Note:

Adding contact center agents to a normal business system will reduce the capacity to handle office traffic. The System Engineering Tool will allow modeling of both types on traffic, and show how much each type of use must be reduced from the maximum values shown in this document.

When MiVoice Business controllers are used for ACD applications, there are several factors that must be considered in determining the capacity limitations. The performance of the controller will be limited because of the high number of calls made in comparison to a system with normal office traffic. In addition, the performance cost of each call will be much higher, to account for IVR interaction in the call (including RAD playback) and for agent skills groups and multiple path queues. When agents are connected to TDM trunks, the number of E2T channels will be critical to the number of agents and/or trunks that can be supported.

SIP trunks provide an alternative means of connecting to the PSTN. These will be used most often with MiVoice Business servers as controllers, although it is also possible to use them with any of the appliance controllers if system size and other connectivity requirements would suggest that.

RAD sources may be embedded (using the voice mail ports) or off-board (for example, Mitel Contact Center IVR). In the networked configurations, the RAD playback and distribution should be located on the MiVoice Business where the ACD paths are programmed.

- Embedded RAD in 3300 ICP (TDM source)
  - RAD plays directly into the TDM switch fabric (no E2T channels used).
  - RAD stream is connected directly to **n** output channels for TDM trunks (no E2T).
  - RAD stream uses n E2T channels to connect to SIP trunks (total = n E2T channels). Therefore, using a 3300 is not recommended if using SIP trunks; instead, use an ISS or VMware.
- External IP RAD in 3300 ICP
  - RAD plays through one E2T channel to **n** output channels for TDM trunks (only 1 E2T channel used).
  - RAD stream uses n E2T channels to connect to SIP trunks (total = n+1 channels).
- Embedded RAD in MiVoice Business for ISS and Virtual System
  - RAD plays within Media Server portion of the controller (1 channel used)
  - RAD stream is played to n channels to connect to SIP trunks (total = n+1 channels).
- External IP RAD in MiVoice Business for ISS and Virtual System
  - RAD plays into Media Server portion of the controller (1 channel used).
  - RAD stream is played to n channels to connect to SIP trunks (total = n+1 channels).

Conference resources are needed in the ACD environment for Silent Monitor/Whisper Coach and consultation calls by the agents. In the network installations these resources are provided on the agent controller(s).

MiCollab SIP Softphones may be used for ACD agents under various conditions. The following is a summary of how ACD agents may be connected to MiVoice Business systems.

Hot Desk ACD agents are supported on:

- MiVoice IP Phones directly connected to the system, or via a MiVoice Border Gateway

External Hot Desking Agents are supported on:

- Mobile phones that connect as EHDA to the system via BRI or PRI TDM trunks
- Analogue phones that connect as EHDA to the system via BRI, PRI TDM, or IP Trunks*
- SIP phones that connect as EHDA to the system via SIP or IP Trunks*
- Third Party PBX phones that connect as EHDA to the system via PRI, SIP, QSIG Trunks*

* Refer to MiContact Center Business Deployment Guide for further detailed restrictions.

3.4 Standalone ACD Controller

Smaller ACD installations will use a single controller with all trunks, agents, groups and paths on it. The IVR and Call Centre Manager are both connected to this controller (through the local network), as are the agents. The calls will come into the call center from the PSTN through either TDM or SIP trunks, will be routed through the IVR system and queued to a path. RADs may be played either from the embedded resources on the controller, or from the IVR system. This configuration is shown in the following figure.

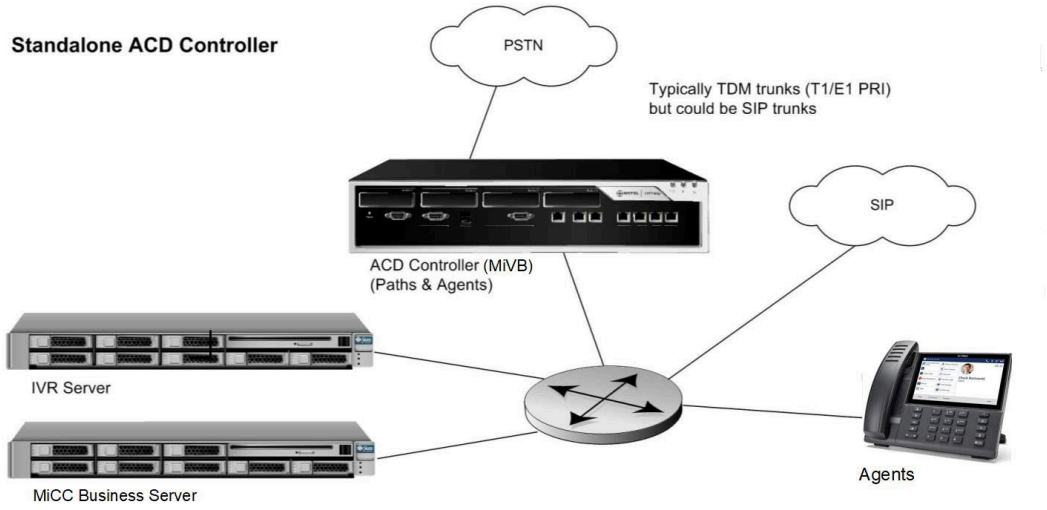


Figure 6: Example of a Standalone ACD Installation

3.5 Network ACD Controllers

For large installations, splitting the system into multiple nodes allows a higher capacity in terms of both agents and trunks. This also allows for resiliency between two (or more) agent controllers. This configuration is shown in the following figure. Here the calls enter from the PSTN on the trunk gateway(s), are routed to the IVR system, and are queued to paths on those gateways which in turn queue to groups on the agent controllers. When callers are on hold, RADs are played to them using the distribution resources in the trunking gateways. The agent gateways control the routing of calls to the agents, but there is no streaming through them since the IP streams go directly to the IP phones, except when the agents are using TDM phones (as EHD agents), or when conference resources are used.

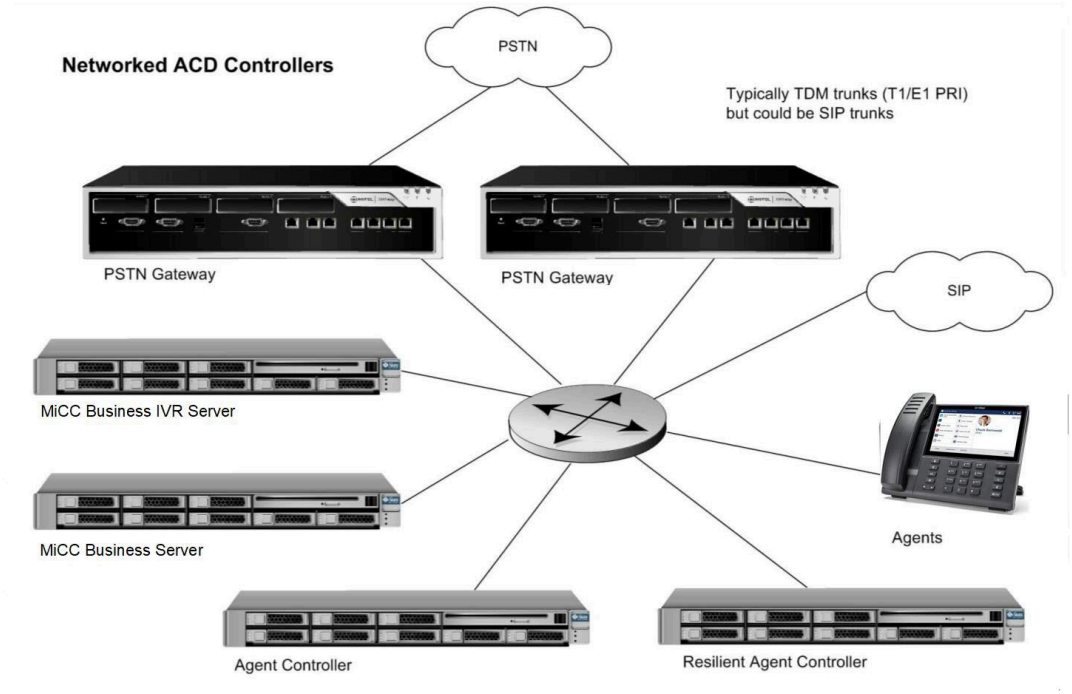


Figure 7: Example of a Networked ACD Installation

3.6 ACD limits

The following tables show the maximum number of IP agents and TDM or SIP trunks that can be installed on the various controllers when used in either standalone or networked configurations. The figures shown are a theoretical maximum based on the conditions shown. A specific installation may be able to support more or less agents and traffic depending on whether conditions are more or less stressful than these assumptions.

Typical Call Center

- Trunk to agent ratio is 1.5 (lower trunk ratios will allow increased system capacity, at the expense of more rejected (busy tone) calls).
- Traffic per agent is at 27 CCS and 120 sec call handling time, that is, 30 CPH per agent.
- Mitel Contact Center Business is used to provide call handling and reporting.
- There is an IVR system handling incoming calls. With no IVR, calls will ring directly to the path(s) with less overhead, but there is less functionality in terms of call handling. The IVR must be on the path controller (trunk gateway) for networked ACD.
- RADs are played to callers waiting in queue(s), either from internal resources or from an external system.
- Active agents are in an average of five groups or less.
- There is one overflow or interflow on the paths.

- All agents are local to their controller except in the rows for EHD agents. If used, EHDA will affect the number of agents and amount of traffic that can be supported on a controller. When the maximum EHDA are connected, the total local agents must be reduced to zero (see chart of Local vs. EHD Agents).

  Maximum Number of ACD Agents and Trunks in a Call Center

ACD Agent and Trunk Configuration		MiVB for ISS	MiVB Virtua (250)	MiVB Virtua (1500)	MiVB Virtua (2500	CX-II / CXi-II	Mxe-III (base	EX
Standalone	Total Agents	350	30	100	175	40	50	100
	EHD Agents	100	10	50	100	10	10	50
	TDM Trunks	0	0	0	0	60	75	150
	SIP Trunks	525	45	150	250	75	90	150
User Gateway (Agent Controller)	Total Agents	1200	40	200	1200	50	80	150
	EHD Agents	200	10	100	200	10	10	50
	Total Trunks	0	0	0	0	0	0	0
Trunk Gateway (Path Controller)	Total Agents	0	0	0	0	0	0	0
	TDM Trunks	0	0	0	0	60	60	240
	SIP Trunks	525	60	250	350	75	90	300

Note:

- **SRTP Restrictions:** The CX II, and MXe III base are limited by E2T and other DSP resources. Mitel proprietary voice encryption is supported in ACD deployments. However, due to the increased load SRTP places on the solution SRTP voice encryption is not supported in all single processor 3300 ICP deployments (CX II, and MXe III Base) and must be disabled via ESM. However, it is supported in the MXe III Expanded, EX, ISS, and Virtual variants.
- **Larger Systems:** MiVoice Business Virtual can be used in the 5000-user configuration for a larger agent controller. Both MiVoice Business for ISS and Virtual (5000) can be used for up to 1200 agents in total. However, there can still be limitations in the number of media channels available for Whisper Coach and other supervisory activities. Use the System Engineering Tool to evaluate such large configurations.
- When multiple trunking gateways are used in a networked configuration the maximum number of trunks on each gateway is as shown in the table.

In the standalone configuration, adding more groups for the agents or allowing overflow on the paths will add a processing load for each call, and will therefore reduce the capacity of the system. In the networked configuration, the agent controller has been relieved of the processing load for the IVR, so the nominal call capacity increases significantly from that of a standalone system. Multiple agent groups and path overflows still affect this node and reduce its capacity. The path controller (Trunk gateway) is still carrying the IVR load, but it is not dealing with the agent groups.

Contact Mitel for assistance for any configuration with:

- more agents and/or trunks
- different traffic pattern
- more agent groups
- greater path overflow and interflow
- additional or alternate applications attached.

3.7 Active agents vs. traffic

The maximum number of agents shown in the above tables is based on each agent handling an average of 30 CPH, corresponding to an average total call handling time (CHT) of 120 seconds, including work timer. If the call traffic is a different rate, the number of active agents that can be supported on a controller will change. The following tables show typical numbers for several representative configurations. In each case we are still assuming agents in an average of 5 groups, and one overflow per path

Table 2: Active Agents on ISS Standalone Controller

Agents	CHT (SEC)	CPH	CPH/Agent
100	34	10500	105
350	120	10500	40
700	240	10500	15
1050	360	10500	10

Table 3: Active Agents on ISS Agent Controller

Agents	CHT (SEC)	CPH	CPH/Agent
100	30	21000	210
350	90	21000	60
700	120	21000	30
1050	180	21000	20
1400	240	21000	15

Table 4: Active Agents on MXe-III Standalone Controller (with PRI)

Agents	CHT (SEC)	CPH	CPH/Agent
10	30	1200	120
20	60	1200	60

Agents	CHT (SEC)	CPH	CPH/Agent
30	120	1200	30
40	180	1200	20
60	240	1200	15
80	300	1200	12
100	360	1200	10

Table 5: Active Agents on MXe-III Agent Controller

Agents	CHT (SEC)	CPH	CPH/Agent
25	30	3000	120
50	60	3000	60
75	90	3000	40
100	120	3000	30
150	180	3000	20
200	240	3000	15
250	300	3000	12
300	360	3000	10

3.8 Local Agents vs. EHD Agents

As stated previously, when EHDA is used for some or all of the agents, the total number of agents that can be supported on a controller is reduced. The above table is a summary of the maximum number of agents and EHD agents on the various platforms for an agent controller in an advanced call center configuration.

Table 6: Active Agents on Agent Controller in Advanced Call Center

Platform	Maximum Agents	Maximum EHD Agents
MiVoice Business for ISS	1200	200
MiVoice Business Virtual (150)	30	10
MiVoice Business Virtual (2500)	1200	200
CX II/CXi II	50	10
MXe III (base)	80	10
MXe III (expanded)	150	40

The following figure shows how the number of local and external hot desk agents must be balanced on an agent controller (example shown is for MiVoice Business for ISS (with 700 agents). The same principle must be used for any other controller configuration.

Figure 8: Example of Local vs. EHD Agents on ISS Agent Controller

3.9 Configuration Tables

The following tables show the maximum capacity for each feature or resource in each type of controller. You cannot configure a system to support all maximum values at the same time.

- IP devices includes all telephones and all applications which emulate telephones, including SIP phones.
- IP devices includes all telephones, including SIP phones, and all applications that emulate IP phones.
- Compression channels include only those channels that may be necessary to connect IP trunks and IP sets to TDM trunks or sets (on 3300 appliances), or IP trunks and sets to internal resources (on all variants). IP sets can stream compressed or uncompressed audio to another IP port without using any internal resources on the controller.
- Digital links refers to embedded BRI (4 links, 8 lines or trunks per module), or embedded T1/E1 (1 link, 23/24/30 trunks, or 2 links, 46/48/60 trunks per module).

For a list of the factory default provisions of the MiVoice Business appliances, see table Table 18: Device and User Limits on page 60.

3.10 AX Controller

Table 7: Maximum AX Configuration

Features/ Resource	Value/Quantity	Notes
RTC processor	450 MHz	-
E2T processor	N/A	The AX uses a single processor for both RTC and E2T functions.
Memory (RAM)	512 MB	AX controller is not supported in Release 9.0 because of the limited memory, but it is supported in MiVoice Business Release 9.1.
IP Users and Devices (including SIP users)	100/300	Maximum IP devices or users. The lower number of devices/users can be supported on any system at normal office traffic. The large number can be supported only at reduced traffic (2-3 CCS) in hospitality applications.
TDM Devices	288	ONS devices only.
Total Devices	300/575	Maximum total devices, IP and TDM combined. The lower number of devices can be supported on any system at normal office traffic. The larger number can be supported only at reduced traffic (2-3 CCS) in hospitality applications.
ACD users (active agents)	50	IP devices only

Features/ Resource	Value/Quantity	Notes
Echo canceler channels/IP gateway (E2T)	40/128	The default channels provided by the on-board DSPs are increased with an EC module installed.
Conference channels	64	The maximum number of conference sessions is 21 and the maximum number of conferees per session is 8. The combination cannot exceed 64.
Voice Mail	20	Voice mail is limited to 20 ports on the AX.
Compression channels	64	Requires installation of DSP II module.
T.38	16	DSP-II is required for T.38 functionality.
Record-a-call	8	Every Record-a-Call session uses a conference resource and a voice mail session from the available pool. The maximum number of simultaneous sessions supported is 8, but may be limited to less than this by the available resources.
CIM ports	0	The quad CIM is not supported on the AX.
ASUs supported	0	ASUs are not supported on the AX.
LS trunks	48	-

Features/ Resource	Value/Quantity	Notes
IP networking	Yes	The system can support a maximum of 2000 programmed IP trunks, but the number which can be used at any one time will be limited by other resources.
MMC modules (installed slots)	Quad DSP (int, ext) Echo Canceler (int, ext) Dual T1/E1 (ext) T1/E1 Combo (ext) Quad BRI (ext) DSP II (int, ext)	Modules may be installed in the internal or external locations as shown.
Digital links	2	-

3.10.1 AX Controller ONS Port Limitation

You can install up to twelve 24 Port ONS cards in the AX Controller to provide up to 288 ONS ports. However no more than 150 of the ports can be in an active call state at any given time, and this limit may be dynamically reduced further if some of the users are on long loops (anything greater than 1.1 mile or 1.7 km on 24 AWG cable). Any users beyond the allowed maximum who attempt to originate a call receive silence (that is, no dial tone). Users attempting to place a call beyond the allowed maximum to a circuit on the AX controller receive error tone and the call is not completed. In addition to the off-hook limitation, there are limits to the number of lines that may be ringing at any given time, both on each individual line card (3 maximum on 4 brush cycles = 12 total) and on the overall system (24 maximum on 4 brush cycles = 96 total). This ringing limitation also applies when the 24 Port ONSP card is used in the ASU II, but the port usage limitation above does not. The maximum number of ONS MWI lamps which can be activated on an AX is 288 (i.e. all of the lines), but this will be reduced in practiceby a software algorithm that relates the total number of ONS sets in Off-hook, ringing, or message waiting state. Refer to the System Engineering Tool (the Physical sheet) to determine these limits for a specific configuration.

3.11 CX II/CXi II Controller

Table 8: Maximum CX II/CXi II configuration

Feature/ Resource	Value/Quantity	Notes
RTC processor	400 MHz	This processor is listed as 450 MHz in the Engineering Tool.
E2T processor	N/A	The CX II uses a single processor for both RTC and E2T functions.
Memory (RAM)	1024 MB	Existing 512 MB must be expanded to 1024 MB in release MiVB 9.0
IP Users and Devices (Including SIP Users)	150	Up to 16 IP devices may be connected directly to the powered Ethernet ports on the front of the CXi cabinet.
TDM Devices	150	ONS devices only.
Total Devices	150	-
ACD users (active agents)	50 (Maximum) 38 (SRTP)	To install the maximum number of ACD users will require the maximum number of digital trunks and DSP resources.When SRTP is enabled along with ACD functionality the E2T capacity is reduced to 38 channels, limiting the number of active ACD agents.
IP gateway (E2T)	32 (default) 64 (max) 48 (with SRTP)	Echo cancellation is done in one DSP for the basic system. Each T1/E1 combo module provides 32 channels of hardware echo cancellation.

Feature/ Resource	Value/Quantity	Notes
Conference channels	30	Each conference may have from three to eight members, but the total cannot exceed the allowed maximum.
Voice Mail	16	The maximum allowed number of voice mail ports is fixed at 16 in this controller.
Compression channels	64	G.729a compression is not a standard offering on base systems. Additional DSP resources are needed to achieve the values shown. Compression is added in blocks of 8 bi-directional channels on DSP II modules only.
T.38	16	DSP-II is required for T.38 functionality.
Record-a-Call	8	Every Record-a-Call session uses a conference resource and a voice mail session from the available pool. The maximum number of simultaneous sessions supported is 8, but may be limited to less than this by the available resources.
CIM ports	3	One Quad CIM card can be installed, but only the first 3 ports will be functional.
ASUs supported	3	Up to 3 external ASU and ASU II cabinets can be installed.
LS trunks (in ASU)	36	Up to 12 on internal AMB/AOB, and 24 in external ASU.

Feature/ Resource	Value/Quantity	Notes
IP networking	yes	The system can support a maximum of 2000 programmed IP trunks, but the number which can be used at any one time will be limited by other resources.
MMC modules (installed slots)	DSP II (2,3) T1/E1 Combo (1,2) Quad BRI (1,2) Quad CIM (1,2)	The Dual DSP, Quad DSP, Dual FIM, and the Dual T1/E1 modules are NOT supported on the CX II.
Digital links	2 T1/E1/PRI, 8 BRI	Digital trunks may be either on Quad BRI (8) or T1/E1 Combo modules (2). Dual T1/E1 module does not have the added DSP and echo cancellation resources needed for this system.

3.12 MXe III Controller

Table 9: Maximum MXe III configuration

Feature/ Resource	Value/Quantity		Notes
	Base MXe	Expanded	
RTC processor	533 MHz	533 MHz	The base MXe uses a single processor for both RTC and E2T functions.
E2T processor		533 MHz	Optional, to increase capacity. The two processors operate independently, one as RTC and the second as E2T.

Feature/ Resource	Value/Quantity		Notes
	Base MXe	Expanded	
Memory (RAM)	1024 MB		Existing 512 MB memory must be expanded to 1024 MB in MiVoice Business 9.0.
IP Users and Devices (Including SIP Users)	300	1400	Maximum 300/1400 IP users or devices. A separate TFTP server is required for more than 200 69xx phone sets.
TDM Devices	196	576	ONS devices only.
Total devices	350	1500	The total number of IP plus TDM devices should not exceed the value shown with maximum IP devices installed, or 1.5 times the IP limit with fewer IP devices, under typical office traffic conditions.
ACD users (active agents)	80	150	To install the maximum number of ACD users will require the maximum number of digital trunks and DSP resources. The number of IP ACD agents can be increased to 150 by off loading all of the TDM functions to dedicated gateways (Net ACD). The total number of active ACD agents might have to be reduced on an installation because of performance limitations, based on high traffic or other installed applications. Use of SRTP does not reduce agent capacity.

Feature/ Resource	Value/Quantity		Notes
	Base MXe	Expanded	
Echo canceler channels/ IP gateway (E2T)	64	128/192 128/182 (with Mitel SRTP) 123/123 (with SRTP)	The second number is available in the 192-channel gateway configuration, when the extra EC module is installed. This capacity is reduced when SRTP encryption is enabled.
Conference channels	64		Conference channels in the MXe are a fixed allocation. Each conference may have from three to eight members but the total number of conferees cannot exceed the allowed maximum.
Voice Mail	30		The default system configuration is 20VM session. Units can expand to 30VM sessions without adding DSP resources.
Compression channels	64	192	G.729a compression is not a standard offering on base systems. Additional DSP resources are needed to achieve the values shown. Compression is added in block of 8 bi-directional channels on DSP II modules only.
T. 38	16	48	DSP-II is required for T.38 functionality.
Record-a-Call	12		The maximum number of simultaneous sessions supported is 12, but may be limited to less than this by the available resources.

Feature/ Resource	Value/Quantity		Notes
	Base MXe	Expanded	
CIM ports	4	12	These ports may be used to connect ASU cabinets only. Up to 2 Quad CIM cards can be installed to increase the number of CIM ports.
Analog trunks	36	96	-
ASUs supported	4	12	Additional ASU cabinets may be connected to the Quad CIM cards.
LS trunks (in ASU)	22 (38)		The internal ASU (AMB) has 6 LS trunks and up to four Universal ASU cabinets may be added with 4 LS trunks each (or four ASU II cabinets with 8 LS trunks each).
IP networking	yes		The system can support a maximum of 2000 programmed IP trunks, but the number which can be used at any one time will be limited by other resources.
MMC modules (installed slots)	Echo Canceler (3,4,5,6) Quad DSP (3,4,5,6) DSP II (4,5,6) T1/E1 (1,2,3,4) Quad BRI (1,2,3,4) Quad CIM (1,2,3,4)		The maximum number of usable framer modules may be limited by the E2T capacity of the system, especially in the base configuration (single processor).

Feature/ Resource	Value/Quantity		Notes
	Base MXe	Expanded	
Digital links	8		Digital trunks may be on embedded Quad BRI modules (12), Dual T1/E1 modules (8), or T1/E1 combo modules (4).

3.13 MXe Controller 192 Gateway limitations

The MXe III Controller can be configured as a 192 channel TDM gateway, as shown in the table called "MXe III, and 192 Channel PSTN Gateway DSP Resources" in the Technician's Handbook. In Release 9.0 this configuration is only practical when used with 53xx phones using Mitel proprietary encryption, or with 53xx, 69xx and SIP phones using no encryption. The maximum capacity of the E2T card is reduced to 123 channels when all the concurrent calls are G711 with SRTP, and to 185 channels when all the concurrent calls are G.729 with SRTP. Therefore, the 192 channel gateway is not viable with SRTP enabled. Refer to the System Engineering Tool for an analysis of the required and available channels. Any upgrade of the 192-channel gateway must consider this, and replace the unit, if necessary.

3.14 EX Controller

The EX controller is a fully configured system, similar to the CX II and MXe III systems, but running on an X86 processor like the larger server variants (but much smaller CPU than the server variants). The MiVoice Business software is deployed in a virtual environment and consists of the following components:

- Mitel MiVoice Business Release 9.4 software
- Mitel Media Server
- Mitel Standard Linux Operating System (MSL 11)

In all tables throughout these Guidelines, if not explicitly stated the EX Controller shall be assumed to have the same limits as the MXe III Controller.

The EX is available in three variants with combinations of Processor, RAM, SSD and Power Supply:

1. 4GB RAM, 60GB SSD, 1 PSU
2. 8GB RAM, 120GB SSD, 2 PSU
3. 16GB RAM, 120GB SSD, 2 PSU

Table 10: Maximum EX Controller configuration

Feature/Resource	Value/Quantity	Notes
Processor	1, 2 Intel Celeron @ 1.8 GHz 3 AMD Ryzen @ 2.0 GHz	-
Memory and Storage	4/8/16 GB RAM 60/120 GB SSD	3GB RAM are available to MiVoice Business partition. Other applications (for example, MPA blade, MBG) may be added in 16GB systems.
IP Users and Devices (Including SIP Users)	1400	-

Feature/Resource	Value/Quantity	Notes
TDM Devices	28	ONS (FXS) and FXS LP devices only. May require the addition of a DSP module. Up to 7 quad modules may be installed, in slots shared with LS (FXO) and PRI trunks. For Australian Installations: The FXS interface must be installed on-premise only. The wiring cannot be bundled with any network cabling and the FXS port wiring must be routed in separate cables away from any network cables. The FXS LP interface must be installed in the same manner as the FXO trunk interface for off premises applications.
ACD users(active agents)	100	Use of SRTP does not reduce agent capacity.
IP gateway (E2T)	240 (to interface cards) 64 (to media server)	Echo cancellation and E2T functionality is done on the DSP and PRI modules for this platform, except when the call is using media server features (conference, paging, voice mail).

Feature/Resource	Value/Quantity	Notes
Conference channels	24	Conferencing is done in the Media Server. Each conference may have from three to eight members, but the total cannot exceed the allowed maximum.
Voice Mail	30 ports total	Voice Mail ports are shared with RADs and Record-a-Call.
Media Channels	64 G.729 on Media Server 64 G.711 on Media Server 240 G.711 or G.729 on DSP and PRI modules	Compression on the Media Server is licensed in blocks of 8 channels. The DSP and PRI modules provide it as no license required for FXS, FXO, and PRI, but Media Server resources are used if necessary for conference and other internal features.
T.38	All TDM channels	T.38 is on by default for all TDM trunks and endpoints. If the other end does not support T.38, it will revert to G.711 pass-through.
Record-a-Call	8	Every Record-a-Call session uses a conference resource and a voice mail session from the available pool.
CIM ports	0	not supported on this platform

Feature/Resource	Value/Quantity	Notes
ASUs supported	0	not supported on this platform
LS (FXO) trunks	28	Up to 7 quad modules may be installed, in slots shared with FXS and PRI. For Australian Installations: The FXO interface is voice only, and does not support FAX or modem.
IP networking	yes	The system can support a maximum of 2000 programmed IP trunks.
Modules(installed slots)	DSP (1,2) T1/E1 PRI (1-8) Quad FXS (2-8) Quad FXS LP (2.8) Quad FXO (2-8)	These modules are NOT the same as the MMC modules used on the CX-II and MXe-III. The DSP module and the PRI module have all of the resources necessary for compression and echo cancellation on the digital and analogue links.
Digital links	8 T1/E1 (PRI)	Digital trunks may be either T1 or E1.

3.15 MiVoice Business for ISS

MiVoice Business is a software solution that provides hardware independent call control functions. MiVoice Business for ISS (Industry Standard Services) provides the platform interface (controller) and associated media server to allow the MiVoice Business call-control to run on Industry Standard Server platforms. Three main components are included with the MiVoice Business for ISS Release:

- Mitel MiVoice Business Release 9.1 software
- Mitel Media Server (included with MiVoice Business for ISS software package)
- Mitel Standard Linux Operating System 11

3.16 Hardware Requirements

Intel-Based Servers

The minimum Intel based server hardware required to support the MiVoice Business for ISS must comply with:

- Xeon E3v3 or Xeon E5v2 (or newer)
- 4 cores with hyperthreading enabled, 8 cores without hyperthreading 2.0GHz minimum

AMD-Based Servers

The system may also be installed onAMD based servers, and has been shown to operate with the following minimum hardware requirements:

- Opteron 2400 series processor including Rapid Virtualization Indexing technology8 cores
- 2.0GHz minimum

Note:

1. Although a Dual CPU server is recommended for best performance it is possible to deploy with only a single CPU (with minimum 8 cores - physical or hyperthreaded). This impacts the number of media channels that can be handled and as a consequence reduces the number of users in a typical office configuration. It is recommended to use the System Engineering Tool to verify suitability for small servers or large installations.
2. RAID 1 requires that both hard disk drives are identical. One disk is used to copy information, so although two disks are fitted, the usable space is equal to only one disk. Other hardware RAID configurations may be used if more disks are fitted. RAID 0 is not recommended.
3. Use of multiple memory lanes may require specific provisioning of memory to the CPU cores, i.e. distributed. This may require more RAM be fitted than specified for the minimum. Refer to the Server vendor documentation to determine optimum memory installation configuration.
4. Applications that require local serial ports (such as SMDR) are not directly supported off the server hardware and will require additional IP/Serial units for connectivity.

3.17 System Capacities

Table 11: Maximum Capacities for MiVoice Business for ISS

Function	Quantity	Notes
IP Users and Devices	5000 active users 5600 programmed users and devices.	Exact quantity will be defined by usage, type of sets and attached applications.
Media Channels	1000 channels (total, all features) 1000 channels G.711 256 channels G.729	Up to 1000 channels or user maximum setting. Use of G.729 compression reduces available G.711 channels.

Function	Quantity	Notes
Conference	600 channels	Each conferee uses one media channel.
Music-on-Hold	1000 channels 65 sources	Internal Music-on-Hold sources do not count as channels, so the full number of media channels is available for output.
Paging	1000 channels 32 sources	64 channels per page group
External Recorded Announcement Devices (RAD)	1000 channels	-
Embedded Voice Mail (Embedded Mitel Express Manager (EMEM))	120 channels	Each active embedded mail port uses one channel.

The number of users is based on nominal office traffic of 6CPH per phone. The main restriction is the number of available media channels, which in turn is controlled by the number and speed of CPU cores. If the traffic rate is reduced, for example with hospitality, then it will be possible to register up to the standard MiVoice Business limits (up to 5000 registered users and devices) in a smaller server, depended on the configuration, types of phones and applications.

The total number of media channels is dependent on the number of CPU cores and the core speed, with an absolute maximum of 1000 channels. The total number of channels may be distributed among the various features, but the total available will remain fixed. A tool is available at installation time to calculate, view, and modify the total number of channels available. Refer to Adjusting media server capacity on ISS and virtual systems on page 182 for additional information. Caution must be used when increasing the limit above the calculated value, as the additional CPU load may cause issues with Voice Quality or call processing.

For Paging, each source input consumes a channel. The recommended IP Paging group size of 64 is based on expected media server traffic and shared channel usage in an

office environment with office levels of traffic. With lower traffic and demands for media channels it may be possible to exceed the recommended value of 64 up to 200.

An external Recorded Announcement Device (RAD) will consume a single channel per source. A single RAD source may be distributed to many external end devices or trunks, so it could be possible to consume all media channels with few RAD sources. For large number of RAD ports to a single RAD source, use of phased timers may be required.

With all functions active, it may be possible to exceed the available maximum Media Server channels. In this situation blocking will occur and connections may not be made. Under normal office traffic conditions it is not expected that this situation will occur. Such a condition may occur when there are multiple large paging groups being activated at the same time, or the server doesn't have sufficient capacity for the traffic.

Table 12: Media Server Compression Resources

Compression Function	Quantity	Notes
Conference	Up to 256	One Compression per channel
Music-on-Hold	Up to 65	One compression per concurrent source
Paging	Up to 32	One compression per concurrent source
External Recorded Announcement Devices (RAD)	Up to 256	One compression per concurrent source
Embedded Mitel Express Manager (EMEM)	Up to 120	One compression per channel
TOTAL Compression Channels	Up to 256	Some resources have multiple channels, but only require one compression channel per source, e.g. MOH.

Compression Resources can go up to 256 channels but may be limited to a lower number in a server with a smaller number of cores. However, where there is a common concurrent source, such as Music-on-Hold or Paging, only one compression resource is needed per source. Multiple External RADs or paging sources require one compression per concurrent source, i.e. if three paging groups are concurrently active, three compression resources are needed independent of the number of end devices.

Compression licenses may be shared between the functions on the same media server. Traffic levels and functional usage should be considered when determining the number of required licenses.

The maximum number of channels is up to the selected value based on server capacity with 20ms frame rate. For a frame rate of 10ms, the maximum number of media channels should be adjusted accordingly, e.g. at 10ms the limit will be 1000 x 10ms/20ms = 500, i.e. the realizable channel number may be less than the selected limit due to the increase in packets to be handled.

3.18 MiVoice Business Virtual

MiVoice Business Virtual is a virtualized voice communication software application that is hosted by the VMware ESX and ESXi hypervisor. This is the same MiVoice Business software solution that was deployed on industry standard servers (MiVoice Business-ISS). The MiVoice Business software is packaged in Open Virtualization Archive format (OVA) for deployment into a VMware environment. MiVoice Business Virtual is comprised of the following software components:

- MiVoice Business for ISS.
- Mitel Standard Linux Operating System 11
- VMware tools used to manage MiVoice Business Virtual

3.19 Hardware Requirements

Intel-Based Servers

The minimum Intel based server hardware required to support the MiVoice Business Virtual must comply with:

- Xeon E3v3 or Xeon E5v2 (or newer)
- 4 cores with hyperthreading enabled, 8 cores without hyperthreading 2.0GHz minimum

AMD-Based Servers

The system is not formally tested with AMD based servers, but has been shown to operate with the following minimum hardware requirements:

- Opteron 2400 series processor including Rapid Virtualization Indexing technology8 cores
- 2.0GHz minimum

Note:

1. Although a Dual CPU server is recommended for best performance it is possible to deploy with only a single CPU (with minimum 8 cores - physical or hyper-threaded). This impacts the number of media channels that can be handled and as a consequence reduces the number of users in a typical office configuration. It is recommended to use the System Engineering Tool to verify suitability for small servers or large installations.
2. Applications that require local serial ports (such as SMDR) are not directly supported off the server hardware and will require additional IP/Serial units for connectivity.

3.20 MiVoice Business Virtual Machine Resource Requirements

The table below defines the MiVoice Business Virtual Machine resource requirements. The MiVoice Business Virtual entries exclude the additional server requirements for the VMware hypervisor and Embedded Voice Mail per MiVoice Business Virtual, which are shown as separate entries. The hypervisor requirements need to be added on a per server basis. The Voice Mail requirements have to be added for each MiVoice Business Virtual that has Voice Mail enabled. The default values, below, are based on a typical office environment running at 6CPH (Calls Per Hour). If the deployed environment has increased traffic rates, these values may need to be increased, specifically the Network IO, Disk IO and vCPU GHz. See MiVoice Business Virtual Server Capacity for additional information.

The above paragraph refers to systems using the VMware hypervisor. When using the Microsoft Hyper-V as the hypervisor, additional resources must be applied in order to maintain the same capacity as shown in the following table. For more details on VMware and Hyper-V requirements, refer to the *Mitel Virtual Deployment Solutions Guide*.

Table 13: MiVoice Business Virtual Machine Resource Requirements

Nominal size (Users)	vCPU	RAM	HDD(Disk)	Network I/O	Disk I/O	CPU Ghz
250	2 vCPU	1.5 GBytes	20 GBytes	Expected usage up to 25 Mbits/s	Expected Usage up to 28 I/O per second	1GHz
1500	3 vCPU	2.0 GBytes	20 GBytes	Expected usage up to 25 Mbits/s	Expected usage up to 28 I/O per second	3GHz
2500	4 vCPU	2.0 GBytes	20 GBytes	Expected usage up to 50 Mbits/s	Expected usage up to 28 I/O per second	5GHz
5000	6 vCPU	2.0 GBytes	20 GBytes	Expected usage up to 100 Mbits/s	Expected usage up to 56 I/O per second	8 GHz
Embedded Voice Mail 120 channels	N/A	N/A	Included	Expected usage up to 3 Mbits/s	Expected usage up to 36 I/O per second N/A	N/A
Hypervisor	1 vCPU	2.0 GBytes	N/A	N/A	N/A	2GHz

Note:

1. The CPU, Memory, Disk Space and CPU/memory reservation is defaulted at installation time. The network and disk I/O are estimates of what is required to achieve the best Voice quality. Changing the MiVoice Business Virtual Machine settings from vSphere may result in performance degradation or Voice quality issues.
2. The CPU reservation can be altered to support different system configurations. Use of the System Engineering Tool is recommended, varying the allocated virtual CPUs and the GHz reservation to determine what is required for a specific number of users and the traffic pattern, including phone set types and applications.
3. Voice Mail usage is based on 12 active channels. Scale the figures as required based on the number of assigned ports.Resource usage is additional to the MiVoice Business Virtual.
4. Local or networked storage (SAN) can be used to store the MiVoice Business Virtual local disk. Please refer to the relevant version of the vSphere/ESXi documentation at https://docs.vmware.com for setting up the required storage solution.
5. The vCPU reservation required to support these system capacities must be doubled when using the Microsoft Hyper-V hypervisor.

The MiVoice Business Virtual is managed from a vSphere Client connected directly to the physical server (host system), or through vCenter. The MiVoice Business Virtual can be installed, monitored, and powered up/down. It can also be migrated from one host (server) to another host in support of server maintenance or workload balancing. This can be accomplished using the "Migrate…" facility from vCenter, with the Virtual Machine containing MiVoice Business Virtual first powered off.

For more information on VMware vSphere, VMware vCenter, and other VMware virtual infrastructure management functions, please refer to the appropriate VMware solution or product documentation.

For minimum and recommended versions of VMWare and Hyper-V software refer to the Mitel Virtual Deployment Solutions Guide.

3.21 System Capacities

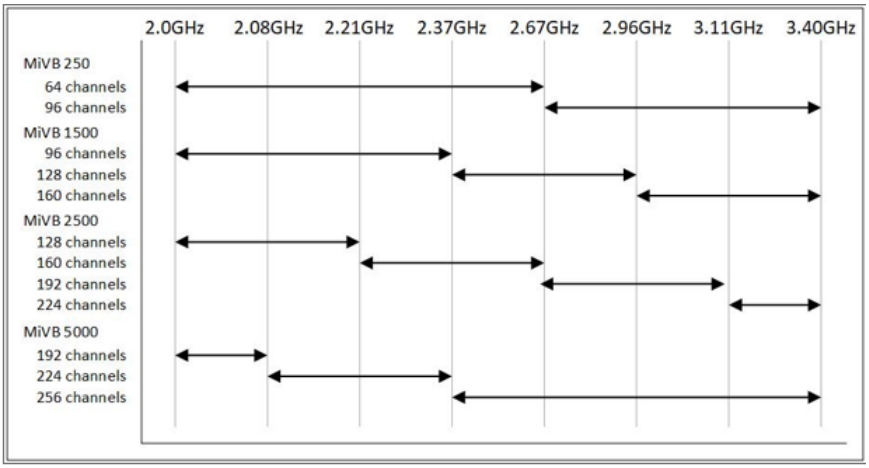
Table 14: Maximum Capacities for MiVoice Business Virtual

Nominal System Size	Function	Maximum Quantity	Notes
250 users	IP Users and Devices	250 active devices 5600 IP User profiles	Exact quantity will be defined by usage, type of sets and attached applications.
	Media Channels	64 to 96 in total (Note 1)	Depends on CPU speed
	Conference	Up to 96 channels (conferees)	Maximum of 8 parties per conference
	Music-on-Hold	Up to 96 channels, 65 sources	-
	Paging	Up to 96 channels, 32 sources	-
	Embedded Voice Mail	30 channels (ports), 250 mailboxes	Ports are shared with RADs.
1500 Users	IP Users and Devices	1500 active devices 600 IP User profiles	Exact quantity will be defined by usage, type of sets and attached applications.
	Media Channels	96 to 160 total (Note 1)	Depends on CPU speed

Nominal System Size	Function	Maximum Quantity	Notes
	Conference	Up to 160 channels (conferees)	Maximum of 8 parties per conference
	Music-on-Hold	Up to 160 channels, 65 sources	-
	Paging	Up to 160 channels, 32 sources	-
	Embedded Voice Mail	48 channels (ports), 1500 mailboxes	Ports are shared with RADs.
2500 Users	IP Users and Devices	2500 active devices 5600 IP User profiles	Exact quantity will be defined by usage, type of sets and attached applications.
	Media Channels	128 to 224 total (Note 1)	Depends on CPU speed
	Conference	Up to 224 channels (conferees)	Maximum of 8 parties per conference
	Music-on-Hold	Up to 224 channels, 65 sources	-
	Paging	Up to 224 channels, 32 sources	-
	Embedded Voice Mail	60 channels (ports), 2500 mailboxes	Ports are shared with RADs.

Nominal System Size	Function	Maximum Quantity	Notes
5000 Users	IP Users and Devices	5000 active devices 5600 IP User profiles	Exact quantity will be defined by usage, type of sets and attached applications.
	Media Channels	224 to 256 in total (Note 1)	Depends on CPU speed
	Conference	Up to 256 channels (conferees)	Maximum of 8 parties per conference
	Music-on-Hold	Up to 256 channels, 65 sources	-
	Paging	Up to 256 channels, 32 sources	-
	Embedded Voice Mail	120 channels (ports), 5000 mailboxes	Ports are shared with RADs.
	Embedded Recorded Announcement Devices (RAD)	120 channels (ports)	Ports are shared with voice mail.

Note:
The maximum values shown for Embedded Voice Mail and RADs are recommended limits for most systems. These values can be increased up the Embedded Voice Mail limit of 120 channels or to the maximum media channels, whichever is less.



The total number of channels may be distributed among the various features, but the total available will remain fixed. A tool is available at installation time to calculate, view, and modify the total number of channels available. Refer to Adjusting media server capacity on ISS and virtual systems for additional information. It is not always possible to know the core speed of the hardware used in a virtual environment, so caution must be used when increasing the limit above the calculated value, as the additional CPU load may cause issues with Voice Quality or call processing.

Note:
If the maximum media streams is adjusted from the default value calculated on installation, the firewall settings must be changed using the formula in the section Voice Gateway IP Ports.

The number of channels for a particular service, e.g. conference cannot exceed the total number of media channels. If the installation defines a lower setting for the maximum number of media channels, then this will take overriding control. The number of compression channels cannot exceed 256 channels for a MiVoice Business deployment, even if the number of media channels is statically assigned to a larger value.

Although the table above highlights the configuration limits, this also has to be tempered by the functionality applied to these devices or how they are deployed. For example some users may have a multi-device user group programmed, in which case it may not be possible to reach the maximum number of users before the device limit is reached. As another example, it may be possible to have multiple hot-desk users but only those that can sign in to active and registered devices will be able to make calls.

3.22 MiVoice Business Resiliency and VMwarevCenter High Availability

MiVoice Business Virtual offers inherent software resiliency with primary node failure detection and automated failover to a secondary node, thereby offering users with highly available phone service. Certain policies must be adhered to when using MiVoice Business Virtual resiliency. For instance, anti-affinity rules should be established to ensure that the primary MiVoice Business Virtual and secondary failover MiVoice Business Virtual are never started on the same physical host server within a VMware cluster.

The anti-affinity rule to prevent the primary and secondary MiVoice Business Virtual from being started on the same server is set in the DRS (Distributed Resource Scheduling) affinity rules. Simply create an affinity rule to **Separate Virtual Machine** and specify the primary and secondary virtual machine name.

As part of vCenter, VMware offers VMware High Availability (HA) - a service that automatically detects physical server failure or virtual machine failure, and restarts virtual machines on alternate servers when a failure is detected. In the case of MiVoice Business Virtual, VMware HA will detect a failure of the server that is hosting the MiVoice Business Virtual or the failure of the virtual machine containing MiVoice Business. Upon failure, VMware HA will restart a new instance of the MiVoice Business Virtual on an alternate server host. Standard VMware configuration rules and certain policies must be adhered to. For example, shared storage technology such as iSCSI, NFS or SAN must be available in the HA cluster.

Both MiVoice Business resiliency and VMware HA can be used at the same time. The following figure shows contrasts the various possible configurations and MiVoice Business availability levels that can be obtained.

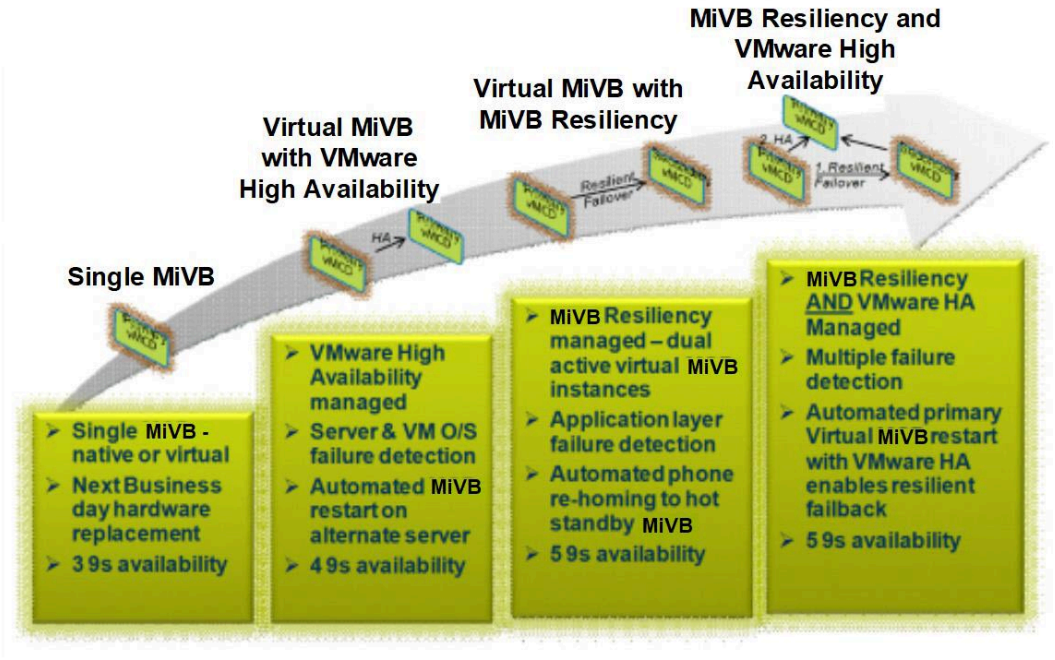


Figure 9: MiVoice Business Resiliency and VMware High Availability

3.23 Other MiVB Maximum Limits

These are additional limits that apply to MiVoice Business in all virtual, ISS and appliance configurations.

Table 15: Other Maximum Limits

Feature/ Resource	Value/Quantity	Notes
MiTAI™ Device or User monitors and Feature monitors	Based on the Maximum Configurable IP Users and Devices field in the License and Option Selection form in the System Administration Tool. See Notes.	For Maximum Configurable IP users = 700: • for an ISS, virtual and EX variants device or user is 5600. Feature is 1000. • For all 3300 appliances, device or user is 2000. Feature is 5000. For Maximum Configurable IP users = 5600: • for an x86 Processor, device or user is 17000. Feature is 30000. • For a Power PC Processor, device or user is 4000. Feature is 5000. Refer to the OIG Engineering Guidelines for more details and examples, or use the System Engineering Tool that accurately counts monitors and identifies the limits.
Wireless sets	Nominal system line size.	The maximum number of wireless devices supported is the IP system line size (150, 300, 1400 etc.) or the number of IP device licenses, whichever is lower.

Feature/ Resource	Value/Quantity	Notes
IP Consoles	24 (default) 48 (maximum)	Under the System Administration Tool, the Dimension Selection form allows this maximum to be raised if internal resources are available.
Compression zones	999	Increased at MCD 6.0
SIP trunks	2000	Limit is set in ESM as “Maximum Simultaneous Calls” and will usually be limited by other resources.
DTMF Receivers	128	-
Call processes	1280 (3300 ICP) 4000 (all x86 variants)	A call process is equivalent to one party in a call. A normal call will use two call processes, a 3-party conference call will use 3 call processes.
Simultaneous two-party connections	640 (3300 ICP) 2000 (all x86 variants)	-
Device Campons per system	172 (3300 ICP) 480 (all x86 variants)	-
Group Campons per system	84 (3300 ICP) 240 (all x86 variants)	-

Feature/ Resource	Value/Quantity	Notes
Hard Holds per system	312 (3300 ICP) 870 (all x86 variants)	-
Wake-up Calls in 1 minute	100 (3300 ICP) 213 (all x86 variants)	-
Wake-up Calls in 5 minutes	400 (3300 ICP) 852 (all x86 variants)	-

3.24 Use of SRTP

The Secure Real-Time Protocol employs a highly secure form of data encryption to the voice packets. This requires some compute resources to complete for both encryption of outgoing data and decryption and authentication of incoming data.

As a result of having SRTP enabled, additional processing is needed. For the 3300 ICP systems this results in a de-rating of the user rating in order to stay within the E2T capacity. The MXe III Expanded is only affected when used in the 192 port gateway mode, in which case the E2T capacity is reduced to 160 channels. The virtual systems also suffer a de-rating of system sizes in order to maintain the same OVA performance profile, and the same number of instances per server type. The ISS is not usually affected by the addition of the SRTP load since it tends to have more cores than the virtual machines. The following table indicates the de-rating levels for different system types when SRTP is enabled:

Table 16: De-rating of User Levels when SRTP is Enabled

System Type	Traffic: 2ccs	traffic: 6ccs	Traffic: 12ccs
MiVoice Business AX	288 users	200 users	100 users
MiVoice Business CX/CXi II	150 users	150 users	100 users

System Type	Traffic: 2ccs	traffic: 6ccs	Traffic: 12ccs
MiVoice Business MXe III base	300 users	300 users	150 users
MiVoice Business MXe III Expanded	1400 users	600 users	300 users
MiVoice Business EX	1400 users	1000 users	500 users
MiVoice Business Virtual 250	250 users	250 users	100 users
MiVoice Business Virtual 1500	1500 users	1200 users	550 users
MiVoice Business Virtual 2500	2500 users (See note)	2100 users (See note)	1000 users
MiVoice Business Virtual 5000	5000 users (See note)	3500 users (See note)	1500 users

Note:

These upper values may also have limits on the number of TLS enabled devices, i.e. the TLS limit may apply before this SRTP limit.

The higher traffic rate (12CCS) either requires more media channels than can be provided, or requires a processing level of SRTP that is outside the standard OVA settings.

SRTP allows encryption for third party devices as well as Mitel proprietary devices. SRTP is enabled by default for new installations of MiVoice Business since release 8.0. If the user does not require SRTP for third party devices, this can be disabled to improve available performance. For new installations, SRTP will be enabled by default. For upgrades, the database migration will have SRTP disabled

Mitel SRTP voice encryption is supported in ACD deployments. However, due to the increased load standard SRTP places on the solution, standard SRTP is not recommended in single processor ACD controllers (AX, CX, and MXe III Base) and should be disabled via ESM, or restricted to a very small number of agents.Standard SRTP is supported in the MXe III Expanded and on all server variants.

3.25 Upgrade Rules for 3300 ICP Appliances

- The line size of any controller can be increased up to the defined maximum by the addition of expansion modules (DSP, Echo Cancelers). In most cases it cannot be increased into the next size range except by total replacement of the controller. The exception is upgrading the MXe III from the base 300 users to 1400 users.
- If additional DSP resources are required for compression, install the DSP-II card. Existing DSP modules used for telecom functions do not need to be replaced.
- The basic MXe III can be upgraded with a second processor (E2T) to increase capacity. The addition of a second power supply and a second hard drive with RAID (redundant array of independent disks) controller to mirror data on both hard drives, will provide redundancy. SeeController Power Input on page 73for information about the use of a UPS to ensure data integrity.
- The performance of a system can only be improved by increasing the speed of the processor and, in all cases, this means replacing the controller.
- To upgrade an installation beyond the capacity of a single MiVoice Business, either get a second applicance and cluster the pair with trunk sharing, or move the users to one of the server variants and repurpose the appliance as a TDM trunking gateway.

3.26 Paging and Background Music Limitations

Using the speaker on IP phones for either group paging or playing of background music can require significant resource usage on the controller. In the 3300 ICP controllers one channel of the E2T function is used for every device either receiving a page or listening to a music source (whether that source is analogue, digital, or embedded). Although only a single echo canceler is used in either case, the heavy use of E2T channels could cause blocking on trunk calls or other features. Similar limitations exist in the media server channels with MiVoice Business on servers (MiVoice Business for ISS, MiVoice Business Multi-instance, and MiVoice Business Virtual).

The following table shows recommended and maximum values for the various platforms, although these limits can be exceeded on systems with lower than normal traffic (e.g. hospitality), up to the number of available E2T/media server channels. Be aware that paging to a large number of users takes time to set up all of the voice connections, especially under heavy system traffic, and the first words spoken may not be heard by some recipients.

Table 17: Music and Paging Limits

Controller Type	Recommended Limit	Maximum Limit
CX/CXi II	16	32
AX, EX, MXe III base	32	64
MXe III expanded	64	128
MiVoice Business for ISS, MiVoice Business Multi-instance, MiVoice Business Virtual	100	250

Note:

In the CX/CXi II and AX systems the number of available echo cancelers might be less than the numbers shown here, depending on the specific combination of modules installed. In the server variants the actual maximum will be dependent on the CPU availability and/or allocation for the Media Server.

3.27 Summary of Device and User Limits

The numbers in the following table indicate the number of IP, SIP, and analog devices that can be licensed and active on the various systems.

- The total number of active IP sets includes all device types (52xx, 53xx, 55xx, and 69xx) and all applications that use emulated IP sets as their interface to the system. For example, a 60-port external IP Voice Mail system registers with the controller as 60 basic IP sets.
- Additional IP users (Hot Desk) or SIP sets can be licensed beyond the number of active devices, but only the numbers shown in this table will be able to register with the controller and become active.

- Analog extensions in the ASU II and in the AX card slots must be licensed, and count against the limit of Total Devices. Analog extensions in the embedded analog are not part of the Total Device limits, but they still have separate limits.
- The actual limits on licensed analog extensions and analog trunks are determined by the number of cards that can be installed in ASU II cabinets connected to the controller.
- "Total Devices" refers to licensed ONS and IP devices only.
- A Hot Desk user logged in to any standard IP phone does not change the total limit of active devices, but counts as an additional device when logged into a 53xx type set.

For all of the cases shown, it may be possible to purchase licenses for more users or devices than are nominally supported on a given controller, based on an option package. The fact that the licenses have been supplied for a system does not guarantee that the system will work to full capacity with all devices and users registered (active).Mitel recommends that youcheck system performance with the System Engineering Tool before installing a system in which multiple limits are approached.

Table 18: Device and User Limits

Active Limits	SYSTEM TYPE					
	CX II/ CXi II	AX	MXe III Base	MXe III Exp	EX	All Servers
Total Devices	150	575	350	1500	1500	5000
IP Devices (Note 1)	150	300	300	1400	1400	5000
53xx/69xx Display Sets (Note 2)	150	200	300	1400	1400	5000
SIP Sets	150	300	300	1000	1400	5000
ONS (licensed)	150	288	192	576	28	0

Active Limits	SYSTEM TYPE					
	CX II/ CXi II	AX	MXe III Base	MXe III Exp	EX	All Servers
Analog Trunks	36	48	36	96	28	0
Hot Desk Users	150	100	300	1400	1400	5000
Standard Sets + Hot Desk Users	300	200	600	2800	2800	5000
53xx/69xx Sets + Hot Desk Users	300	200	600	2000	2800	5000

Note:

1. The 5304, 5312, 5324, 6905 and 6910 are considered standard sets (52xx IP devices) when used in their basic mode. When any HTML applications are enabled on these sets, they must be considered with the 53xx/69xx family of sets in terms of performance and quantity allowed on a controller.
2. The number of display sets is a subset of the total sets (IP devices) but the controller may not be able to support additional basic sets if the maximum number of display sets is installed. Refer to the System Engineering Tool to verify performance limits or other limits.

3.28 Upgrading the System

There are several reasons to upgrade a system –to ensure compliance with SWAS, to obtain the latest product features and security improvements,to increase the line size or to improve performance.

With Mitel the network is the system, so it can also be expanded (and resiliency added) by adding more controllers into a clustered "virtual system". Individual controllers can be upgraded as shown below, or new controllers can be added into a cluster to create a larger virtual system.

3.29 Provisioning System Resources

The table below shows the capacity of each MiVoice Business appliance in its factory default configuration, with no additional modules or other upgrades purchased .

Note:

1. No compression is possible in the base configurations.
2. The AX must have a 16GB flash card installed to support Release 9.1.

Table 19: Standard Configurations

Feature/ Resource	CX II	MXe III Standard	AX	EX
IP users (note 1)	150	300	100	1400
TDM users (note 2)	150	96	192	0/28
ACD users	50	0	0	0

Feature/ Resource	CX II	MXe III Standard	AX	EX
Echo canceler channels/E2T	32	64	40	32
Compression channels	0	0	0	0
Conference channels	30	64	64	24
Voice Mail ports	16	30	0	30
CIM ports	0	4	0	0
ASU supported	0	4	0	0
LS trunks	6	6	48	0/28
IP networking (note 3)	yes	yes	yes	yes
Echo slot number	0	5	0	N/A
Quad DSP slot number	0	0	0	N/A

Note:

1. This is the maximum number of IP users that can be installed without additional DSP resources.
2. The first value is the maximum number of ONS users or LS trunks that can be installed on the default ports, and the second is the maximum that can be installed with additional ports and DSP resources.
3. The base system can support IP networking and compression between IP sets, but not compression for calls that use the E2T function.
4. It is assumed that digital (or analog LS) trunks will be installed in or connected to the controller to access the PSTN. BRI links should be considered a subset of T1/E1, with 8 voice channels per card (4 BRI links), instead of 48 T1 or 60 E1 (2 T1/E1 links).

3.29.1 Provisioning for Traffic

All 3300 ICP controllers contain an internal TDM switching fabric. Calls between TDM sets, or from TDM sets to trunks, will stay within this TDM switch. Calls between IP phones stream their voice packets directly over the data network without going into the TDM domain in the 3300 ICP controller, but calls between IP sets and TDM devices (including both lines and trunks) must go from the IP domain to the TDM switch fabric through the TDM gateway (E2T processor). All of these calls require bandwidth or channels within the various domains and may require specific resources (DSP tone generators and detectors, echo cancellation, etc.) within the controller. The provisioning of these resources is done using the standard type of traffic analysis.

The TDM only switching fabric in all of the 3300 ICP controllers is non-blocking, but the limitations in the number of channels available in the TDM gateway, and other resources mean that the system itself is not.

Under most ordinary conditions, the “rules of thumb” provisioning suggested in previous sections gives a good estimate of the resources required for the number of lines (users) and trunks in a system. For systems that are approaching the limits of the system, more detailed calculations may be required through Customer Engineering Services.

Traffic analysis considerations:

- 36 CCS = 1 erlang (1 e) = 3600 call seconds during the busy hour.
- Call rates (CPH) and duration may vary from business to business. It may be necessary to monitor a business to get more accurate values.
- Typical phone calls are 100 seconds in duration.

- Typically, a normal office phone is busy 16% of the time, or 0.16 e, or 6 CCS (this is 6 CPH @ 100 seconds, i.e. 600 call seconds or 6 centum call seconds or 10 minutes).
- Typically, a hotel phone is busy 6% of the time, or 0.06 e, or 2 CCS.
- Typically, a busy office phone, such as one handling dispatch orders, can be busy 33% of the time, or 0.33 e, or 12 CCS.
- Call volume is typically split in thirds, with 33% incoming from trunks, 33% outgoing to trunks, and 33% handling internal calls (50% is making calls and 50% receiving calls).
- For normal users, typically one voice mail session is needed for 20 users. Modify this number accordingly if you expect heavier or lighter voice mail traffic per user, or significant auto-attendant usage.
- Typically, ACD workers are busy 75% to 100% of the time. One ACD agent normally requires one resource, such as one 1 E2T channel, one echo channel, one DSP channel (compression), and one trunk. ACD traffic ranges from 27 to 36 CCS (27 to 36 calls per hour).
- Typically, in a given ACD group, all calls are either incoming or outgoing trunks, rarely mixed.
- Traffic blocking is calculated using the ErlangB formula. Erlang adds a statistical blocking factor and is always higher than the straight calculation. Add a further 10% to 20% to PI estimates as a rough estimate, and round up.
- Operators or attendants can typically handle up to 100 calls per hour (as long as transfer is handled quickly and number lookup is sufficiently quick). Most incoming trunk calls arrive at the operator station.
- Traffic blocking probability for internal/intercom traffic is P.001 (1 in 1000 calls blocked).
- Traffic blocking probability for trunk traffic is P.01 (1 in 100 calls blocked).

3.29.2 CX/CXi II Hardware Configurations

The CX-II and CXi-II have enough DSP resources on board for all normal telephony requirements up to their rated line size, and there are 32 echo cancelers available in the base configuration. To get additional echo cancelers the T1/E1 Combo Module must be installed; 32 channels are added with the first module, to the maximum available of 64. A second module does not increase the EC channels.

Compression channels can be added using the DSP devices on the T1/E1 Combo modules (if compression is licensed), but these only can provide up to a maximum of 16 channels. The DSP-II module must be added to get more than 16 compression channels, to a maximum of 64. This module is also required for T.38 FAX. The DSP-II module DOES NOT PROVIDE additional telephony resources (tone detectors and receivers, voice mail, or conference). When a DSP-II module is added, the DSP devices on the T1/E1 Combo Module will not be used for compression, but will provide additional telephony resources if they are needed.

Phones and Voice Applications 4

This chapter contains the following sections:

4.1 MiVoice IP Phones

The MiVoice Business supports the following MiVoice IP Phones:

- the 5212, 5215 DM, 5220 DM, 5224 DM, and the 53xx range of IP phones
- the 5505 SIP and the 5540 IP console
- the 5560 IPT (only supported on the MXe III ICP, the CX/CXi II ICP, and all server variants)
- the 6905, 6910, 6920/6920w, 6930/6930L/6930w, 6940/6940w, and 6970 display phones

All other phone types are no longer supported in MiVoice Business 9.0 as the software loads are not available for download from the system. The only exceptions to this are the 5020 and 5240 IP phones, which are supported only as emulated devices in external applications(the application supplies the set software). Additionally, the 3300 ICP supports the use of the Gigabit Ethernet phone stand and the Wireless LAN with the 5200/5300 series of supported IP phones.

The number of sets that can be connected to a system is determined by the nominal size of the system (analog and digital sets) and by the number of IP user licenses.

- The number of IP user and IP device licenses determines the absolute maximum number of IP sets that can be installed.
- The system size (150, 250, 700, 1400 etc.) is an indicator of the approximate number of sets that could be supported with no other applications installed.

The number of IP consoles (5540 and MiVoice Business Console) that can be connected to a system is determined by the absolute maximum number of IP consoles that can be configured on the system and number of IP User licenses. The number of MiVoice Business Consoles that can be active (operator present) on a system at any given time is determined the number of MiVoice Business Active Operator Licenses.

The voice or telephony applications generally add to the number of “sets” on the system because they emulate IP sets. Each pseudo IP set counts the same as a real set for purposes of system limits, so it is possible to reach the system limit without having that number of real sets installed if there are a large number of applications. The quantity of real + emulated sets can never exceed the number of IP device licenses on the system. Applications also use other internal resources, such as DSP and E2T functions.

All IP sets and applications use up a combination of IP sockets for MiNET, MiTAI and voice sockets, which have a finite limit. For more information, seeIP Sockets and Monitors. A detailed analysis of the socket usage on a system is included in the calculations done as part of the System Engineering Tool.

4.2 5560 IPT Limits

The 5560 IPT is supported on three platform types, the CX/CXi II, the MXe (MXe II and MXe III expanded versions only) and the MiVoice Business for ISS and MiVoice Business Virtual server. Because of the typical use of this device, in an extremely high traffic environment, there are restrictions on the number of these appliances which can be deployed on the various systems. The servers can support a maximum of 125 devices, the MXe 32, and the CX/CXi-II only eight.

The default number of programmable keys on the 5560IPT is 96 keys. This can be increased to 192 keys with a license selection. This can only be applied to a system that is configured with the 700 users option.

The 5560 IPT is normally used in key-system mode, and the number of devices supported will be reduced by shared line or trunk appearances on the keys. Similarly a high traffic rate (short call hold time) will reduce the number of devices that can be supported. The following table shows examples of the interaction of these factors for each of the system types. The highlighted rows indicate typical traffic of 120 calls per hour per user, or 30 second hold time per call.

Table 20: Impact of Shared Line Appearances and Traffic Rates on Number of 5560 IPT Supported

Controller Type	Number of sets (users)	Shared Line Appearances	CPH per user	Equivalent Call hold time (sec)
All server variants	125	12	60	60
	100	16	60	60

Controller Type	Number of sets (users)	Shared Line Appearances	CPH per user	Equivalent Call hold time (sec)
	50	44	60	60
	125	2	120	30
	100	6	120	30
	50	16	120	30
	125	1	150	24
	100	3	150	24
	50	12	24	50
	100	1	15	100
	50	8	15	50
MXe III	32	1	60	60
	16	10	60	60
	16	1	120	30
	16	0	140	25
	8	4	180	20
	8	1	240	15

Controller Type	Number of sets (users)	Shared Line Appearances	CPH per user	Equivalent Call hold time (sec)
CX II	8	16	50	72
	8	4	100	36
	8	0	150	24

4.3 NuPoint Unified Messaging

The 3300 ICP is able to provide Automatic Gain Control (AGC) on calls destined for NuPoint that originated on 3300 ICP LS trunks. Use of AGC can alleviate problem calls where the audio is too low.

The AGC capability resides in the 3300 ICP, however it is a selected via an option on NuPoint Messenger. The default setting is AGC off. The AGC capability is only switched on when the Administrator enables it on NuPoint, once AGC is enabled on NuPoint then NuPoint will send a request to the 3300 ICP to have AGC turned on.

4.4 MiCollab Client and MiCollab Client Softphone

Access Connections

MiCollab Client (desktop and mobile) andMiCollab Client Softphone use a number of access connections to both theMiVoice Business controller and toMiCollab Client Service (the function installed on a server).MiCollab Client,MiCollab Client Service, andMiCollab Client Softphones use the following resources to connect to the ICP:

- MiCollab Client service uses a single MiTAI socket per MiVB controller, and requests a monitor for every phone (IP, SIP, or ONS) or trunk that is required to have call state monitored A monitor is needed to allowMiCollab Client to display a BLF for any telephone on the system.
- TheMiCollab Client (desktop or mobile) does not need a monitor or a MiTAI socket to communicate with the ICP, since all communication is via theMiCollab Client Service (see outputclass="fm:Table with Number (i.e. Table 1)" IP_Sockets_and_Monitors
- TheMiCollab Client Softphone uses SIP to communicate withMiVoice Business via one IP socket. TheMiCollab Client Service will place a monitor on this set, the same

as with any other user device. A Micollab desktop client will normally be associated with theMiCollab Client Softphone. There is no direct communication between the softphone and the desktop client.

For more information on MiTAI limits, refer to the Mitel OIG 4.0 Engineering GuidelinesFor example, a system with 200MiCollab Clients with desk phones, with 100 of these also havingMiCollab Client Softphones, and aMiCollab Client server, will use:

- 1 MiTAI socket (MiCollab Client server only)
- 300 monitors (1 for each client's device).

If theMiCollab Client installation is set up to monitor every port (line or trunk) in the enterprise, it may use more monitors than there areMiCollab Clients on the system. In this case it may not be possible to reach the maximum number of users and trunks on the system before running out of monitors

Networking Considerations for MiCollab Client

TheMiCollab Client Softphone is an application that runs on the PC on which it is installed. This means that the Mitel only DHCP options (e.g. VLAN, DSCP) are not available to the application.

MiCollab Client incorporates a MiAudio softphone. For details regarding MiAudio refer to the document called "Mitel Universal SDK, Installation and Maintenance Guide". As of MiVB 9.4 MiAudio (Xfsdk) supports OpenSSL 1.1.1.

MiCollab Client is able to use two different QoS settings. The selection of which QoS setting is used is made in the IP Phone Emulation Settings Window.

In the IP Phone Emulation Settings Window, above the Start/Stop Phone Emulation Service button, there is a check box called “*Use the internal QoS settings, with a fixed DSCP of 0xa0*”.If this setting is checked,MiCollab Client will use the Microsoft setting which is a DSCP value of 40, the equivalent of a precedence of 5 for legacy TOS based routers.

If the setting is unchecked (the default setting),MiCollab Client will use the Mitel setting which is a DSCP value of 46, and provides marking into the Expedited Forwarding queue for DSCP based routers.

A TOS based router will work correctly with a DSCP value of 40. However, a DSCP value of 40 could give unpredictable results if used in a network that employs DSCP based routing schemes.

DSCP to 802.1p mapping in the Ethernet switch should be used when VLANs are applied at the network switch to prioritize the voice traffic at the Ethernet Layer. A DSCP value of 46 should be used so that, in networks that employ DSCP based routing, voice priority will be maintained.

4.5 MiVoice Business Console

Access Connections

The MiVoice Business Console uses a number of access connections to the MiVoice Business (or ICP) controller.

- The MiVoice Business Console uses MiNet to communicate with the MiVoice Business for call processing via a single IP socket. It also uses the same IP socket to obtain directory information for incoming call display, phonebook and busy lamp display.

Networking Considerations for MiVoiceBusinessConsole

TheMiVoiceBusiness Console is an application that runs on the PC on which it is installed. This means that the Mitel-only DHCP options (e.g. VLAN, DSCP) are not available to the application

Console incorporates a MiAudio softphone. For details regarding MiAudio refer to the document called Mitel Universal SDK, Installation and Maintenance Guide Release 1.2. As of SDK Version 1.2, MiAudio supports QoS settings for voice packets.

The selection of QoS settings is made using theMiVoiceBusiness Console Configuration Wizard Quality of Service settings window. By default, theMiVoiceBusiness Console will use the Mitel setting for voice media which is a DSCP value of 46 and TOS value of 5. TheMiVoiceBusiness Console must be run as administrator for non-default QoS settings to take effect.

DSCP to 802.1p mapping in the Ethernet switch should be used when VLANs are applied at the network switch to prioritize the voice traffic at the Ethernet Layer. A DSCP value of 46 should be used so that, in networks that employ DSCP based routing, voice priority will be maintained.

Power 5

This chapter contains the following sections:

Note:

Power information for IP sets and how to plan a PoE installation are found in the IP Sets Engineering Guidelines.

5.1 Installation Practices

Data signals on an Ethernet or similar connection are low power and are susceptible to electromagnetic interference. It is important to correctly install the data equipment and interconnections in a controlled manner to minimize electromagnetic interference onto the cables and equipment and to minimize signal loss.

Mitel strongly recommends using Uninterruptible Power Supply (UPS) units or similar power backup systems to protect the 3300 controllers against AC power outages. For more information on this subject, see Uninterruptible Power Supply (UPS).

Follow the relevant safety and building installation codes for the location.

For more information on acceptable wiring practices, equipment installation, and equipment grounding, see *MiVoice Business Ethernet Twisted Pair Cabling Plant, Power and Grounding Guidelines* or Appendix B of the *MiVoice Business Hardware Technical Reference Manual*.

5.1.1 Using UPS to Power the System

Consider the entire voice path from one device to another when distributing power. Consider especially which devices need to maintain power during a general power outage. Although the end devices such as phones will continue to need power, so will the underlying network infrastructure, if phone service is to be maintained.

The use of local UPS supplies as well as larger central power backup schemes, local generators, for example, may need to be considered.

An example of how to calculate UPS power is given in Uninterruptible Power Supply (UPS).

5.2 Controller Power Input

The controllers have flexible power input operating over a wide range to allow global connectivity. The units operate with standard supplies of 60/50 Hz and 110/230 VAC input, and are auto-sensing.

During a local power failure, data that is being written to a disk or FLASH module may not be completely stored and it can become corrupted. Use of RAID can improve the integrity and data validation, but cannot guarantee data that was not completely transferred due to loss of power. Systems most affected will be those undergoing updates or those that store voice mail. We strongly recommend that these systems, be powered through UPS units or similar power backup systems.

More details on platform power consumption and settings can be found in the*3300 ICP Hardware Technical Reference Manual*.

5.3 3300 CXi II ICP 802.3af Power over Ethernet capabilities

The CXi II includes a 16-port managed Layer 2 Ethernet switch. The 16 Ethernet ports comply with the 802.3af Power over Ethernet (PoE) specification, which enables them to deliver power to IP phones and other Ethernet devices over Category 3, 5 or 6 cabling.

The CXi II controller’s Layer 2 switch can provide 100 Watts of power to 802.3af-compatible devices according to the following general rules:

- Depending on the phone and option power requirements, up to 16 IP Phones could be supported.
- Any 53xx set with more than one PKM and any 6900 set with a PKM requires an AC adapter.
- UC360 conference units require an AC adapter, the 6970 conference phone does not..
- Class 1, 2, and 3 devices receive 4, 7, and 13 Watts, respectively. Unclassified (Class 0) devices are budgeted 7.5 Watts by the PoE subsystem, but can receive up to 13 Watts.
- Port 1 has the highest priority, port 16 the lowest.

The CXi II PoE sub-section measures the actual current that the phones are drawing. A maximum of 100 Watts of PoE power is enforced.

If the maximum system power budget of 100 watts is exceeded, power will be turned off to the ports, starting with port 16 and ending with port 1, until less than 100 Watts is being consumed.

The System Administration Tool provides a maintenance command (L2 PoEStatus) that can be used to determine what power advertisements the CXi has received from the various phones.

If you are using a CXi II, this maintenance command will provide the actual power being consumed, based on measurements by the phones that have been installed.

5.4 Uninterruptible Power Supply (UPS)

Use uninterruptible power supplies when phones, the associated controllers, PC-based consoles, and the LAN infrastructure need to continue to operate during a power failure. UPSs can range from simple local battery units to larger central installations that include backup generators. Consider the following factors to determine the type of unit to use:

- The power to be drawn by attached units
- The power output of the UPS, and its efficiency with battery capability
- The time the UPS must supply power
- The size of the unit.

Note:

1. If VoIP service must be operational during a power failure, each of the network components must also be on the UPS.
2. The System Engineering Tool will estimate the amount of power used by each of the cabinets in the system configuration when running the existing traffic. The estimate does not include the power for other network equipment (L2 switches, and so forth).

5.4.1 Worked Example

Consider a small installation with a LAN switch and some powered phones. The LAN switch draws 100 W and 16 attached phones draw 8 W each. The UPS has a 12 V battery of 55 AH and runs at 70% efficiency. How long can this combination be powered?

- The output power available is 462 VAH (volt-amperes hour) (55 x 12 x 70%).
- The consumption is 228 VA (100 W + 16 x 8 W).

- The time available is 2 hours or 462 VAH / 228 VA.

Note:

Volt-Amperes (VA) is equivalent to Watts (W) if the Power Factor Correction (PFC) of the power supply in question has a PFC value of close to 1. Most data switches on the market today will have a PFC value close to 1.

Performance 6

This chapter contains the following sections:

6.1 System Performance

In order to calculate the performance limits of a system, different weighting values are assigned to various types of calls, streaming with various codecs, and feature interactions. Based on the expected calls per hour (CPH) of all of the user ports on the system and the associated traffic patterns and feature usage, the system performance (processor loading) can be calculated.

In addition to traffic, many other factors affect system performance. For example, a large number of voice mail ports can significantly increase the CPU load because streaming data to the hard disk is a CPU-intensive operation. Similarly, call monitors applied by features such as ACD, Hot Desk, and several external applications, along with SMDR logging, can add processor load. These are all taken into account automatically in the System Engineering Tool.

Table 21: Factors affecting Performance Index (PI)

System Feature	PI Impact
SMDR reporting	10%
MiTAI monitoring	10%
MiTAI call control (MiCollab Client and applications)	40%
Embedded Voice Mail	up to 80%
Voice Compression (G.279)	up to 50%

6.1.1 Performance Limitations

The following figure of *Performance Limitations for MXe III Expanded* shows the performance limitations for a 1400 user MXe III controller; and the figure *Performance Limitations for MiVoice Business Servers*shows the performance limitations for a typical MiVoice Business for ISS.These charts show typical behavior with unencrypted calls. Use of SRTP may reduce the call capacity, especially on the MiVoice Business appliance systems.The maximum calls per hour are fordistributed traffic measured at peak hour. The number of registered sets is the number that is actually connected to the controller, including those that might be connected because of failover in a resilient configuration. The limits shown in these figures are determined by performance only; there may be

other limits (for example, licenses) which restrict operation to lower traffic or numbers. Use these graphs in conjunction with the System Engineering Tool to determine the appropriate configuration. Note that for larger systems, typically with more than 500 users attached, the maximum performance may only be obtained by using the MiVB as a group controller in conjunction with other units providing functions such as TDM gateways and voice mail services.

Normal operation is within the P.99 region(probability that 99% of calls will succeed). The system may be pushed into the P.95 region, for short duration, for example during a resilient failover condition. However, certain call parameters, such as delay to dial tone, may be extended beyond the normal expected timings. Operation beyond P.95 is not recommended.

For accurate predictions of behavior for any system, Mitel recommends using the System Engineering Tool (SET).

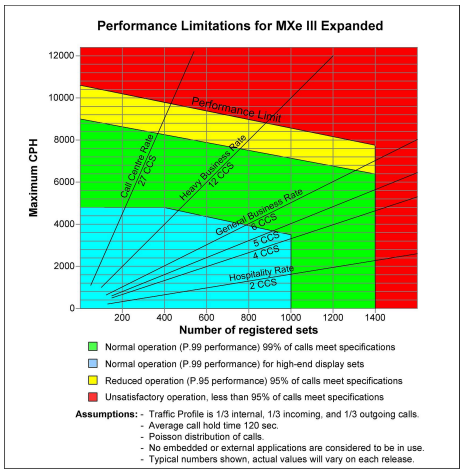


Figure 10: Performance Limitations for MXe III

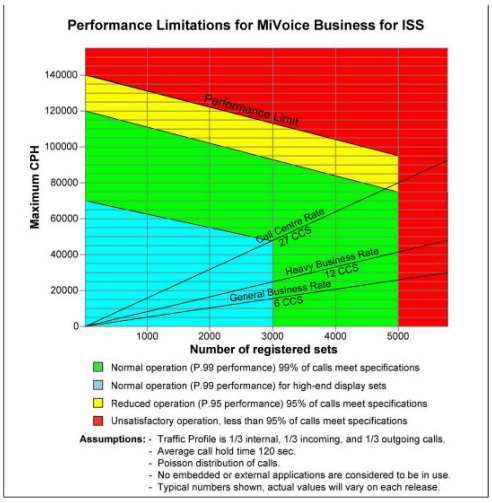


Figure 11: Performance Limitations for MiVoice Business Servers

6.1.2 Performance in an ACD Environment

There are many features of an office telephone system which are always present and which individually use a large amount of CPU performance, but since they are rarely used in an office or hospitality environment, they are insignificant to the overall performance numbers of the system. These same features, when used in the high traffic ACD (contact center) environment, can rapidly drive the system to (or beyond) its maximum CPU capacity.

When a call comes into the contact center on a trunk, it will often be queued to be answered by the IVR system. This system will then transfer the call to a path (another queue), where it waits, listening to MOH or a message until an agent is available. The call might go back to a the IVR for an update message (i.e. “All of our agents are still busy… your call is important to us … please stay on the line …”), be transferred back into the agent queue, and then finally be transferred to a free agent. This means that each call into the system is a minimum of two internal calls (the IVR and the agent) and could easily be more than five calls, depending on how busy the call center is and how many callers are waiting in queues.

When a system is sized such that the number of trunks is less than 1.5 times the number of agents, the overall call rate will typically be less than 2.5 times the incoming (trunk) call rate. When the number of trunks into the system is more than 1.5 times the number of active agents, then the overall call rate rapidly climbs due to the multiple handling of the calls into and out of the various queues. When an agent appears in several groups, as soon as he answers a call in one group the agent must be made unavailable in all of the other groups. Similarly, when he becomes free this must be applied to all of the groups to which he belongs. This adds significantly to the processor load, and reduces the capacity of the system. When calls overflow on a path to additional groups, a similar increase in processing occurs because calls have to ring in multiple locations and then be removed when answered.

6.1.3 Performance with Ring Groups

The method of searching ring groups can have a significant effect on the overall performance of a system.

Terminal ring groups are good for a small number of members, but can be extremely slow and CPU-intensive with a larger number. Large ring groups should be configured for Circular hunting for optimum performance.

Ring All ring groups can also have a large impact on performance. As every member of a ring group requires a call setup in order to ring, and even though only one may be answered, each of the call setups still has to be torn down, so the number of apparent calls in the system is multiplied by the number of members in the ring group. Large ring groups should be configured for Cascade hunting for optimum performance.

Clustered ring groups can also help to improve the performance of Ring All ring groups as processing is distributed across multiple controllers.

Clustered ring groups can also have impact on resources. When members are not local to the ring group, the additional call setup is now an internal trunking call rather than a local call and therefore consumes internal trunking resources. Ring groups should be configured in such a way that the majority of members are co-located with the ring group to optimize performance and resources.

For further information on ring group configuration to optimize performance and resources, see the System Engineering Tool and the *System Administration Tool Help for MiVoice Business*.

6.1.4 Performance with Hunt Groups

The method of searching hunt groups can have a significant effect on the overall performance of a system. Terminal hunt groups are good for a small number of ports (e.g. RADs) but can be extremely slow and CPU intensive with a large number of members. Large hunt groups should be configured for circular hunting for optimum performance. Selection of hunt group (VoiceMail, RAD, Voice, etc.) can have a serious performance impact, especially on auto-attendant and IVR operation. Hunt groups containing auto attendant or IVR ports should be configured as VoiceMail type groups to take advantage of automatic camp-on; otherwise, in a high traffic site, the system may experience slowdowns if calls are rejected by call control due to excessive processing.

6.1.5 Performance with SDS Distribution

When an Import is performed with a CSV file containing User and Services Configuration records, an excessive number of SDS Distributions build up, potentially causing the Import to fail.

The following are the factors to be considered:

1. The size of the network.
2. The relative speed of the SDS master versus the SDS slave controllers.
3. The number of records to be imported.
4. Other network traffic that competes with the SDS process, e.g. call processing.

Calculate the number of SDS Distributions to be generated.

For an import of one record (for a resilient device) the following SDS Distributions will be generated:

- Nine distributions to the resilient secondary network elements.

- Five distributions to the all other network elements. elements)

> **Note**:
> This is approximate; some of these go to cluster members, others to network elements.

If N = the number of network elements, and R = the number of records to import, the total SDS distributions becomes:

(9 x R) + (5 x R x N)

For example, an import of 100 USC records for a network of 30 controllers produces:

(9 x 100) + (5 x 100 x 30) = 15,900 distributions.

Ensure that the Import is not overflowing the SDS distribution buffer:

- In software releases less than 9.1 SP1, the SDS buffer for distributions is 60,000.
- In software releases 9.1 SP1 and up, the SDS buffer for distributions is 200,000.

If the buffer is overflowed, you will see an error such as:

- Unable to perform the record update as the maximum number of SDS Shared Data Updates has been reached.
- The SDS distribution update store is full.

Applications 7

This chapter contains the following sections:

The MiVoice Business supports a number of applications. This includes applications that are embedded in the product, such as voice mail, through to providing DSP resource to allow connections to external devices, for example a remote central voice mail in another unit. Other interfaces include MiTAI forMiCollab Client Softphone operation.

Refer to the application's documentation for setup information

7.1 External Hot Desk Users, Personal Ring Groups, and Multi Device User Groups

The concept of external hot desk users (EHDU), Personal Ring Groups (PRG), and Multi-Device User Groups (MDUG) must be carefully considered when determining the total call traffic in a system and the number of trunks required.

- A call between an EHDU and an internal DN uses a trunk. A call between an EHDU and an external DN (i.e. a public number) uses two trunks.

- Each call to a DN in a personal ring group counts as a call in the total system traffic. If a call comes in from an external trunk to a PRG with three members, then that call becomes three calls for purposes of calculating traffic performance (cph).
- Only the one call that is answered counts as a completed call for purposes of traffic intensity (CCS or Erlangs), although all of the attempted calls do use a channel for a few seconds while in the ringing state.
- The voice channels used during ringing state are important when counting the number of trunks that might be necessary to support this type of call traffic. Each external device that is called as part of a PRG requires one B-channel on a digital trunk while it is ringing, but when one line is answered all of the other voice channels are dropped. If a user has a desk phone and two external numbers in his PRG, then a call to him from the PSTN will use three B-channels while ringing (one incoming and two outgoing) and two if answered on one of the external phones (one incoming and one outgoing). A call from an internal user to that same person will use only two trunks while ringing, one if answered on one of the outside lines, and none if answered on the internal line.

- If there is only a single EHDU associated with an internal set then the pair can use External Twinning, which operates in the same was as any other EHDU but does not required an IP license for the second (external) set.

7.2 Embedded Voice Mail

MiVoice Business includes an integrated, fully featured voice mail system. Up to 120 ports are available for voice mail calls with support for a maximum of 5000 mailboxes and up to 130 hours of storage time. The ports are shared between Voice Mail (VM) and Recorded Announcement Devices (RAD) for use with the embedded Auto Attendantand Record-a-Call (RAC) functions.

Table 22: Voice Mail Capacities

Parameter	Limits

Voice mail ports (Concurrent voice mail or auto attendant sessions)	• Servers
	  • MiVoice Business on ISS: 120VM or RAD ports.
	  • MiVoice Business Virtual:up to 120 VM and/or RAD ports.
	• Appliances
	  • AX: 20 VM or RAD ports.
	  • CX II: 16 VM or RAD ports.
	  • MXe III: 30 VM or RAD ports.
	  • EX: 30 VM or RAD ports.

Mailboxes	maximum 750 on appliances, 5000 on servers
Disk space for voice mail files	• 14 GB with hard disk drive or 64 GB(or greater)SSD • 13 GB with 32GB flash card on CXII and <64GB SSD on MXeIII or EX • 4 GB with 16GB flash card on AX

Parameter	Limits
Hours of voice storage	• 450 with 13-14GB partition (130 if backup is required) • 130 with 4GB partition (30 if backup is required
Message storage per mailbox	100 maximum messages (programmable)
Message retention	From one day to indefinitely for saved messages; indefinitely for unread messages. (Programmable on a per mailbox basis).
Prompt languages	North American English, UK English, European French, Canadian French, European Spanish, Latin American Spanish, Dutch, German, Italian, Brazilian Portuguese, European Portuguese, Chinese, Arabic, Farsi, Flemish, Turkish, Swedish, North American English Overlaid and Dutch Overlaid (one default and one alternate language are permitted simultaneously)

7.3 Embedded Music On Hold

Embedded Music On Hold is a software feature that allows digital audio files to be transferred to the controller's hard drive. These embedded files are then loaded into RAM and used as an audio source for providing music to users that are on hold.

Embedded music on hold provides the following advantages over traditional analog music on hold:

- Streamlines the changing of music sources on a system or on multiple systems.
- Provides the customer with the ability to take an audio format file and easily transfer it to the controller. This can be done using the System Administration Tool or using MiVoice Enterprise Manager's Audio File Manager.
- No external music source is required to support embedded music on hold.

An audio source can be considered to have a performance equivalent to ½ an E2T connection . Every IP endpoint connection to this source will use an E2T connection and this must be taken into account when designing a system. A TDM endpoint connection to this source will not use an E2T connection. Instead, a TDM channel will be consumed.

Table 23: Embedded Music on Hold Capabilities

Platform	Total RAM	Total Play Time	Maximum Number of Embedded MOH Sources
All server variants (including EX)	128 MB	256 minutes	64
MXe Expanded	16 MB	32 minutes	64
MXe base	16 MB	32 minutes	16
CX/CXi II	4 MB	8 minutes	5
AX	2 MB	4 minutes	2

Emergency Services 8

This chapter contains the following sections:

Emergency services such as 911 are available from most phone devices according to how the class of service and restrictions for the phone are set. The default is to enable 911 emergency service access.

For solutions in the US see the MiVoice Business Emergency Services (911) for more details on how to apply the RAY BAUM'S Act.

8.1 Location Information

MiVoice IP Phones report network connectivity information. This information can be used to provide location information to the Emergency Services database(Caller Emergency Service ID, or CESID). When an IP phone is moved to a new physical location the phone reports the new location information to the MiVoice Business and the CESID directory is automatically updated. When wireless devices and Wireless Access Points (WAPs) are used, the Base Station Service ID (BSSID) must be mapped to the correct CESID.

IP phone move detection is accomplished by analyzing data reported from the Spanning Tree Protocol/Rapid Spanning Tree Protocol, the Cisco Discovery Protocol or Link Layer Discovery Protocol / Media Endpoint Discovery.

The location for IP phones can also be determined using the IP address.

8.2 Network Configuration

Location Change Indication is provided in the IP network by identifying the L2 port MAC address to which the IP phone is connected and cross-referencing it to a physical location stored in the Emergency Responder database.

The IP phones determine the MAC addresses of the L2 ports to which they are connected by using Spanning Tree Protocol (STP)/Rapid Spanning Tree Protocol (RSTP), Cisco Discovery Protocol (CDP), or Link Layer Discovery Protocol/Media Endpoint Discovery (LLDP/LLDP-MED). The IP phones then report to the ICP, sending the MAC address of the L2 switch port to which they are connected.

Note:

The network port MAC addresses and physical locations must be known before the IP phones are deployed.

Automatic CESID updating is designed to work in a homogeneously configured network where allthe access L2 switches in a particular subnet (to which IP phones are connected) report MAC address information by the following methods:

- STP/RSTP
- CDP
- LLDP/LLDP-MED

By ensuring one or both protocols are consistently and uniformly enabled on all L2 switches within a sub-net, the network administrator can guarantee that each IP phone is able to reliably detect the L2 MAC address and the L2 Port Number of the switch to which it is connected.

The system administrator must define the preferred protocol (STP/RSTP, CDP, or LLDP/LLDP-MED) to detect when a phone has moved to a different physical location. This selection is made during system initialization using the CESID Assignment form in the System Administration Tool.

The following figure *Preferred Network Configurations for E911 Compatibility*depicts the three preferred network configurations for E911 compatibility. Note that the access L2 switches are configured uniformly in that they have STP/RSTP, CDP, or LLDP/LLDP-MED. Each phone can detect a unique L2 Port MAC Address and L2 Port Number from the L2 port to which it is connected.

For illustrative purposes the Port Address and Port Number are shown in the format of “A, 1”, where “A” represents the Port Address and “1” represents the Port Number.

The following figure *Preferred Network Configurations for E911 Compatibility* contains three panels. For the configuration in the left panel (CDP), the administrator must set the preferred protocol to CDP in the CESID Assignment form; for the configuration in the middle panel (STP), the administrator must set the preferred protocol to STP, and for the configuration in the right panel, the preferred protocol is set to LDP.

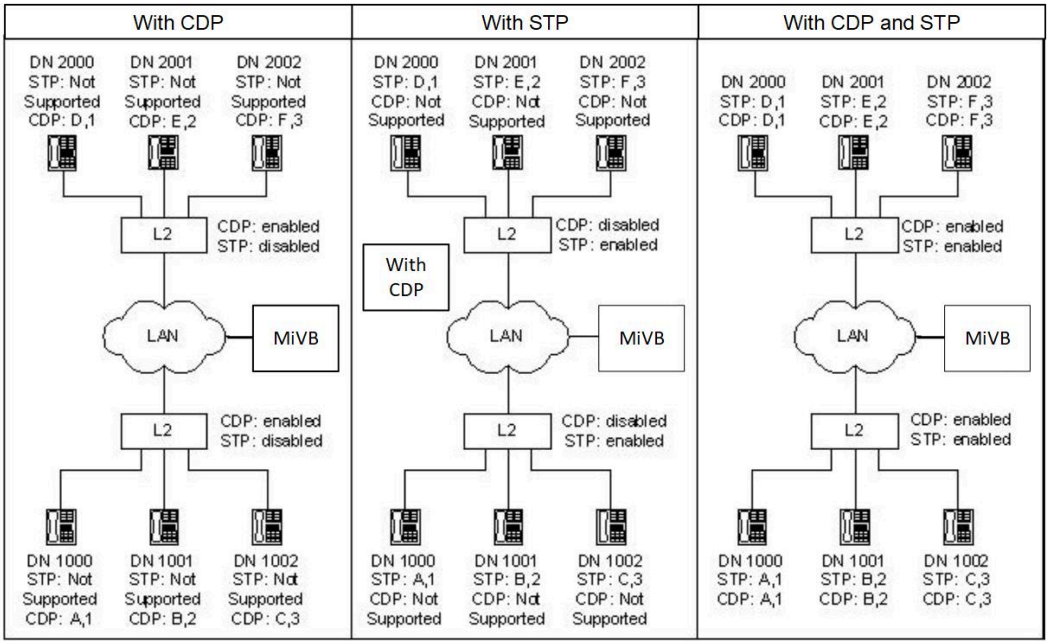


Figure 12: Preferred Network Configurations for E911 Compatibility

If a conflict is detected between the protocol data, a log is generated. Logs are recorded for all device moves and CESID-related activity and alarms are raised when the system identifies a device (DN) with a missing CESID, typically when a device moves to an unknown locationthe Ethernet switch is changed, or a new device is added into the network.

8.3 CESID auto updates, unsupported Configurations

Automatic updating of CESID via L2 when a phone moves to a new location will notwork under the following circumstances:

- If the IP phone is connected to an Ethernet hub.
- If the IP phone is connected to an L2 switch that does not have CDP, STP/RSTP or LLDP/LLDP-MED enabled.
- If multiple IP phones report connectivity to the same L2 port. The system will detect this condition upon device registration.

The following examples of network configuration should not be used in an installation that requires E911 services:

- Some L2 switches use CDP and others use STP/RSTP or LLDP/LLDP-MED (see *Non-compatible Network Configuration - L2 Switches with Mixed Protocols*). The problem with this network configuration is that the MiVoice Business could receive information from STP/RSTP that conflicts with information received from CDP. Since

the MiVB is not receiving data for all ports from both protocols, conflicts cannot be resolved.

- Some or all L2 switches have both CDP and STP/RSTP disabled (see *Non-compatible Network Configuration - L2 Switch - CDP and STP Disabled*).
- The sets are connected to an L2 switch via a hub (see *Non-compatible Network Configuration - Devices Connected via Hub*). From the perspective of the MiVB, it will appear that several devices are all plugged into the same L2 port (i.e. the port of the L2 switch that is one step higher in the network tree). For Location reporting

to function correctly, an IP phone should be associated with only one L2 port MAC address.

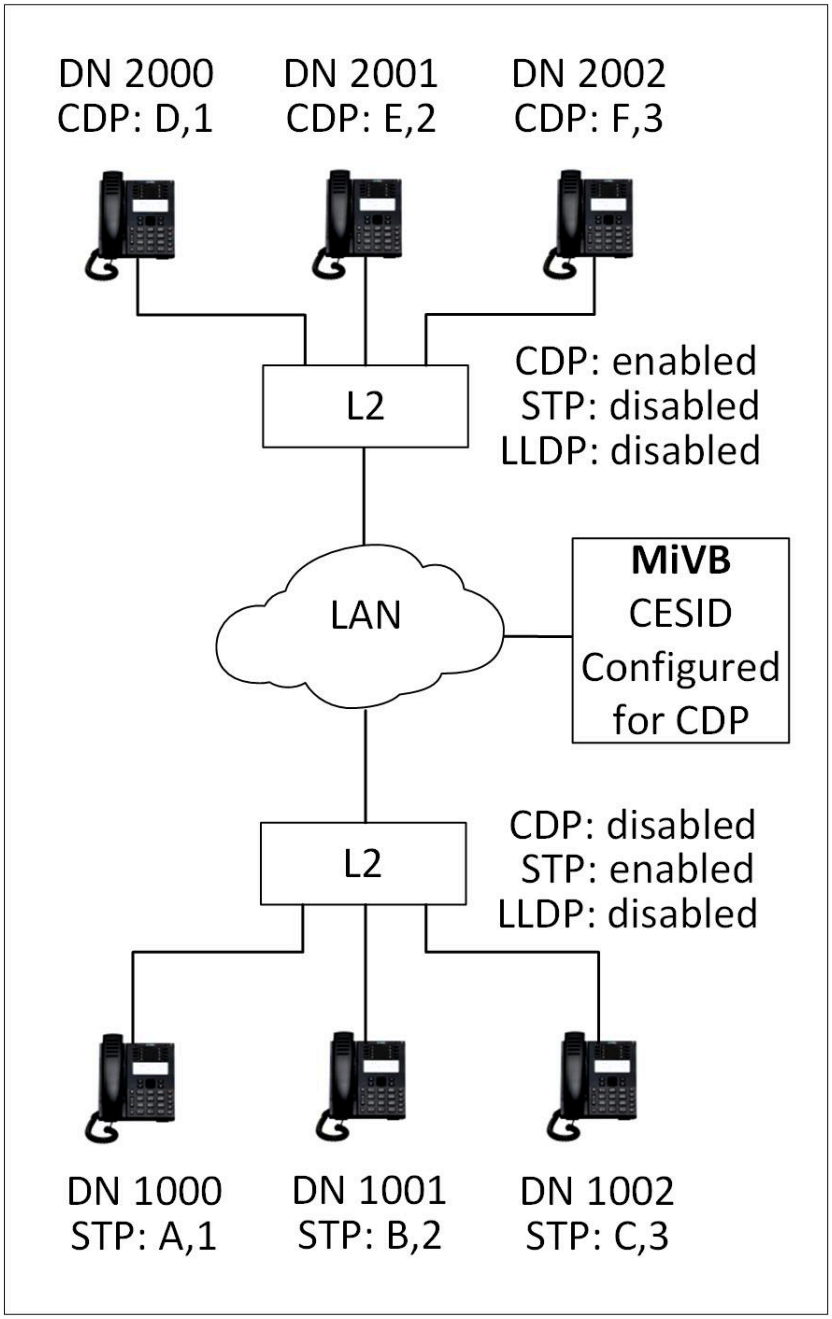


Figure 13: Non-compatible Network Configuration - L2 Switches with Mixed Protocols

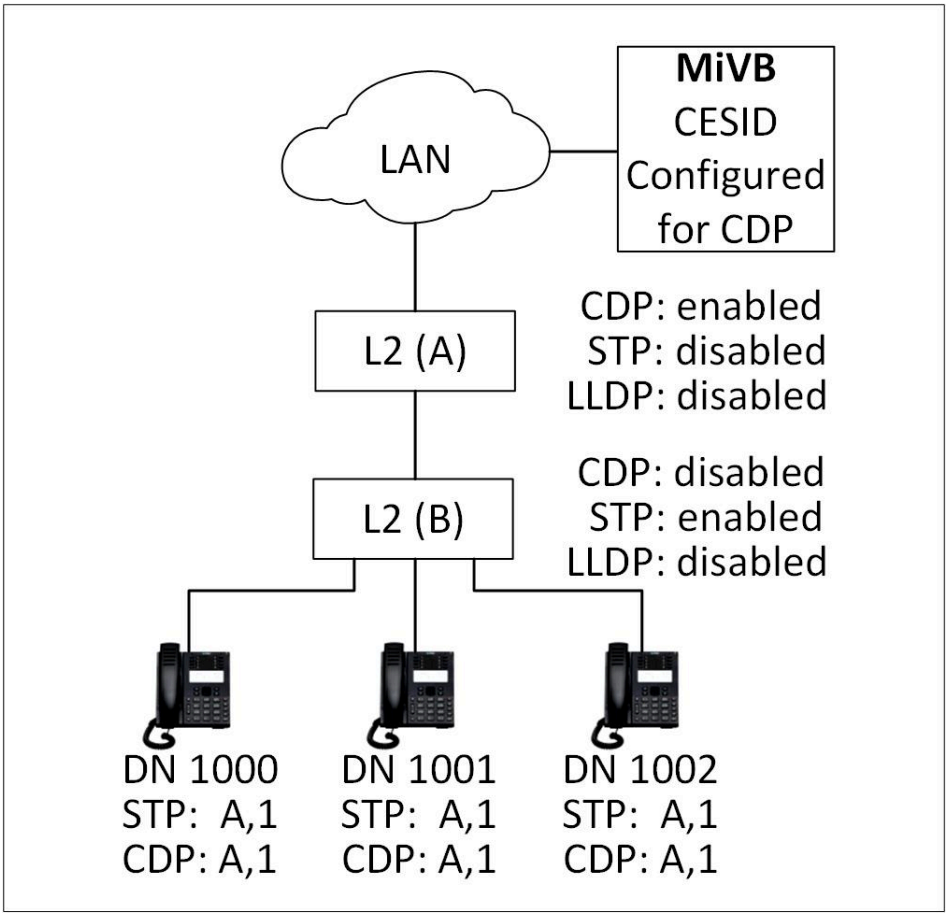


Figure 14: Non-compatible Network Configuration - L2 Switch - CDP and STP Disabled

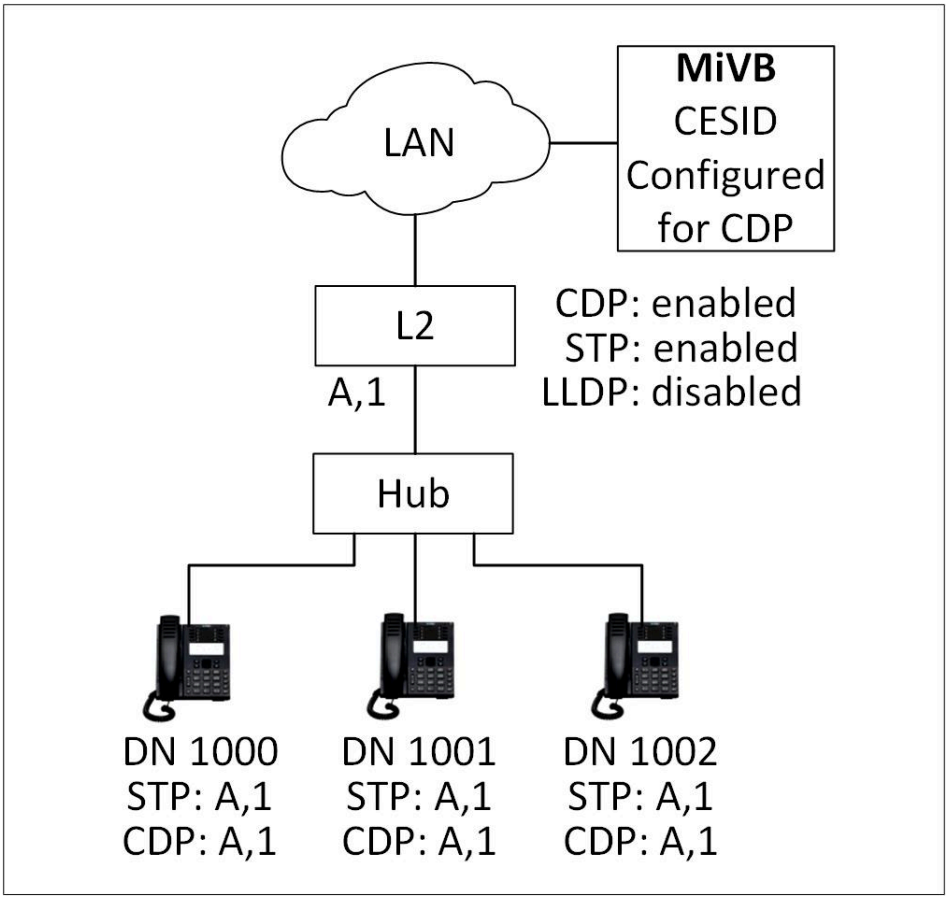


Figure 15: Non-compatible Network Configuration - Devices Connected via Hub

8.4 Other considerations

- The Spanning Tree Protocol allows multiple ethernet connections to be made between a device and the network without introducing a network loop. In the event that the active network connection fails, the Spanning Tree Protocol will enable a standby connection so that network connectivity is maintained.
- RSTP (Rapid Reconfiguration of Spanning Tree Protocol) is available on most network devices.Today, most network devices support RSTP. Very few now revert back to STPRSTP is backward-compatible with STP and is the preferred setting.
- Using RSTP reduces disconnection time to approximately 3 seconds(compared to Spanning Tree at up to 50 seconds), which has a much smaller effect on IP phone operation and is the preferred setting throughout the network.

Note:

More details on Rapid Spanning Tree configurations can be found in the MiVoice Business Resiliency Guide.

- In the event that an L2 switch vendor does not adhere to the STP/RSTP or CDP protocols correctly, there could be issues that prevent E911 from functioning as required. At the time of writing, Mitel is not aware of any specific L2 switches that fail to comply with STP/RSTP or CDP.
- When provisioning users with 911 services, the System Administrator should consider:
  - employing redundant trunks for PSTN access
  - using uninterruptible power supplies or redundant mains power for the controller and the phones
  - deploying the MiVoice Business in a resilient fashion.

IP Networking for MiVoice Business 9

This chapter contains the following sections:

These sections describes how IP networking and IP trunks affect the MiVoice Business. The terms “IP networking” and “IP trunks” have become synonymous. However, “IP networking” covers the whole picture, while “IP trunks” refers to the individual call connections.

9.1 IP Networking Node Restrictions

A MiVoice Business is considered a node for IP networking. A node is defined through the numbering plan and must be unique among networked devices. A single controller has the following limitations:

- If **no** loop-back is set up, no more than 249 nodes can be connected to a single node.
- If a loop-back **is** set up, no more than 248 nodes can be connected to a single node.
- No more than 2000 calls can be made across IP trunks between any two nodes, and no more than 2000 IP trunk calls can be made from one controller at any one time.

9.2 Multi Node Management Restrictions

Multi-Node Management provides a number of installer functions that simplify provisioning and management of a sub-group of controllers or gateways. Because of the performance impact of distributing data to a large number of nodes simultaneously, the maximum size of an Administrative Group with Multi-Node Management enabled is 20 nodes. In releases MCD 4.0 and MCD 4.1 this is recommended but not strongly

enforced. In MCD Release 4.2 if the size of the Administrative Group is larger than 20 nodes, Multi-Node Management is automatically disabled. Refer to Clustering for Multi-Node Management under Administrative Groups for more details on this limitation.

9.3 Clustering

Clustering and networking between units introduces additional performance overhead and limitations on the individual MiVoice Business systems, but allows a much greater overall system to be deployed, over potentially a large geographic area. To determine the impact of such configurations and use with users and applications, it is highly recommended to use the System Engineering Tool to gauge the headroom and overall impact of such configurations.

- **Standalone:**An individual unit that is not connected by any form of networking, for example, a small or medium-sized business.
- **Networked:**A number of locations that are interconnected, but the level of inter-office traffic is not particularly high, for example, a business with multiple corporate offices in different cities.
- **Clustered (with PSTN trunk sharing):**A number of systems that interoperate to create a bigger system; for example, a larger office where there are a number of trunk connections to the PSTN, but where the PSTN can present a call to any of the trunks. An incoming call could arrive on any system, and likewise on outgoing call could also go through any system.
- **Clustered (without PSTN trunk sharing):**A business that is connected dispersed(perhaps across a city) where each office is connected to the PSTN through local trunks, but where internal traffic can flow freely from office to office. Examples include a campus environment, a large department chain, or a government establishment.
- **User Controller:** This is a 3300ICP or MiVoice Business system that only deals with IP Phones and users. It does not have direct connectivity to TDM PSTN trunks, although it will have access to IP-Trunks to other MiVoice Business systems and 3300ICPs. A user controller connected via SIP trunks could also be modeled by a standalone configuration.
- **Trunking Gateway PSTN/TDM:** This is a 3300ICP or EX that is primarily a tandem controller that interfaces IP-Trunks to PSTN/TDM trunks, or analogue phones. Typically such a unit will not have associated IP users, but it may have associated applications for call handling or queuing, for example with call centres.
- **Trunking gateway PSTN/SIP:**This is a MiVoice Business system that is primarily a tandem controller that interfaces between internal IP-Trunks and external SIP trunks. Typically such a unit will not have associated users, but it may have associated application for call handling or queuing, for example with call centers.

9.4 IP Trunk Connection Limitations

- The number of IP-Trunk channels per connection, or route, is 2000. The number of channels in use can still be restricted in the IP/XNet trunk group configuration
- The total number of IP-Trunk channels on the node, gateway or controller is limited to 2000 active channels, i.e. it is possible to overprovision
- The number of IP/XNet trunk groups is 999.
- Provision for IP-Trunk connections, or routes, can also be made via "Direct-IP" rather than through IP/XNet Trunk Groups

The use of "Direct IP" and IP/Xnet Trunk Groups are mutually exclusive for a connection from a programming point of view, but usage of both methods can be intermixed on the same node. Use of Direct-IP removes the channel provisioning limit, or requirement, and also the need to program up an additional IP/XNet Trunk Groups form.

IP trunking models

Examples of fully-meshed and hierarchical network configuration networks are shown in the figures *Fully-Meshed Network*and *Hierarchical Network*.

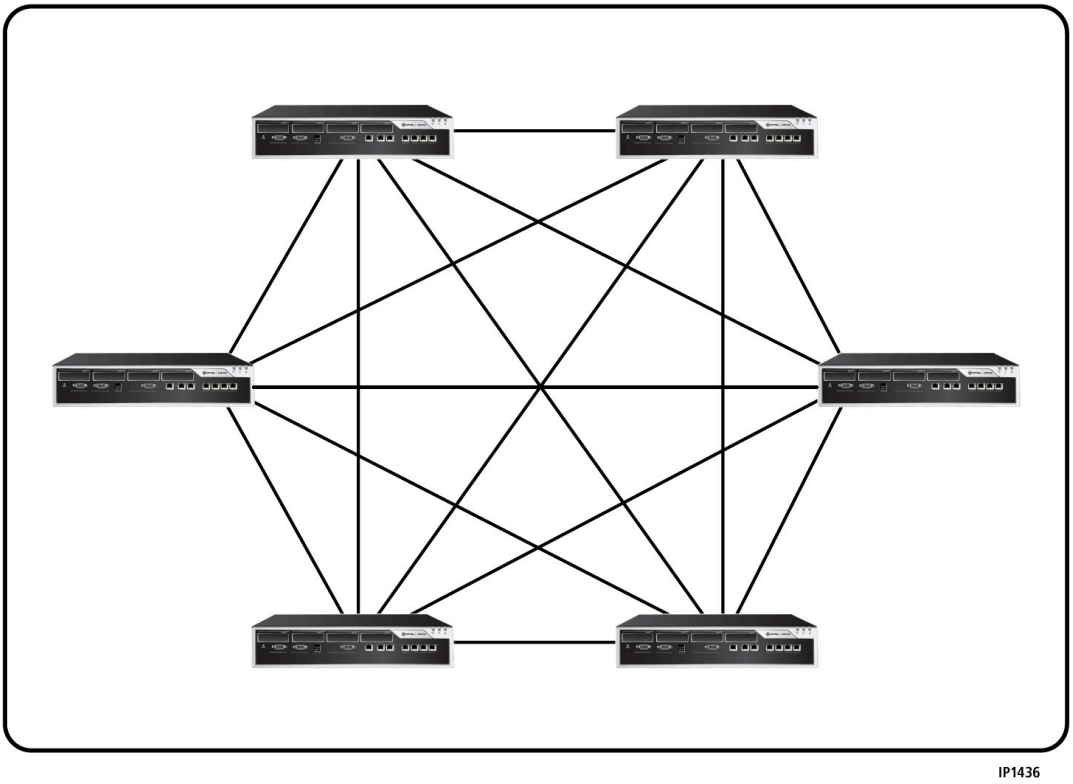


Figure 16: Fully-Meshed Network

In a fully-meshed network, every node is connected to every other node. The benefit of a fully-meshed network arrangement is that one, or even more than one, link can go down, and nodes can still reach each other—there are many alternative routes.

For deployments of 20 nodes or less, the fully meshed model is easy to deploy, but as each new node is added, there is additional management overhead on every existing unit to add the new IP trunk. Every node requires N-1 IP trunk connections, so for 20 nodes, there are 380 IP trunks (20 x (20-1))—760 end-points to be programmed.

For larger systems, especially for those with many smaller remote nodes, it may be more practical to deploy a hierarchical network.

In a hierarchical network, as shown in the figure *Hierarchical Network*, a central group of core routing controllers are fully meshed, but only one or two links are required to connect to the remote nodes, or to other applications. Adding a new node requires only an update at the central group and at the new remote site.

In the example 20-node system, you might need only 38 IP trunks, with 76 end-points to be programmed in a hierarchical system. Adding the 21st node would require programming of four additional IP trunks, compared to 40 for the meshed system.

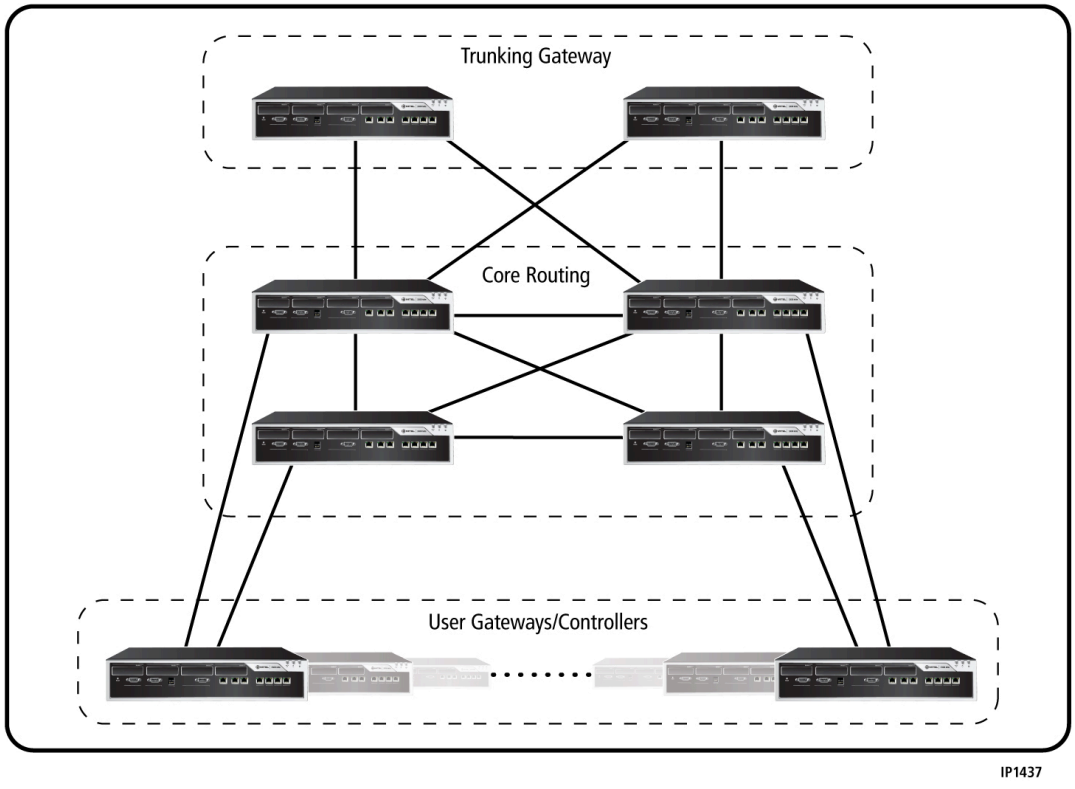


Figure 17: Hierarchical Network

9.5 Call Handling, Routing, and Bandwidth

A call consists of two parts: signaling and voice streaming.

Using TDM, typically over the PSTN, the two parts of the call follow the same path and are closely linked in their routing. In a tandem connection from site A to site C, via tandem site B, voice is handled by the TDM switch at site B. In effect, the tandem TDM switch reroutes the voice part of the call and establishes a second signaling path. It is involved in both voice and signaling connections.

Using IP, voice can stream directly between endpoints (usually), but signaling still travels via the tandem unit. Thus, in a tandem connection, voice streams directly from A to C, while signaling goes from A to B and then B to C.

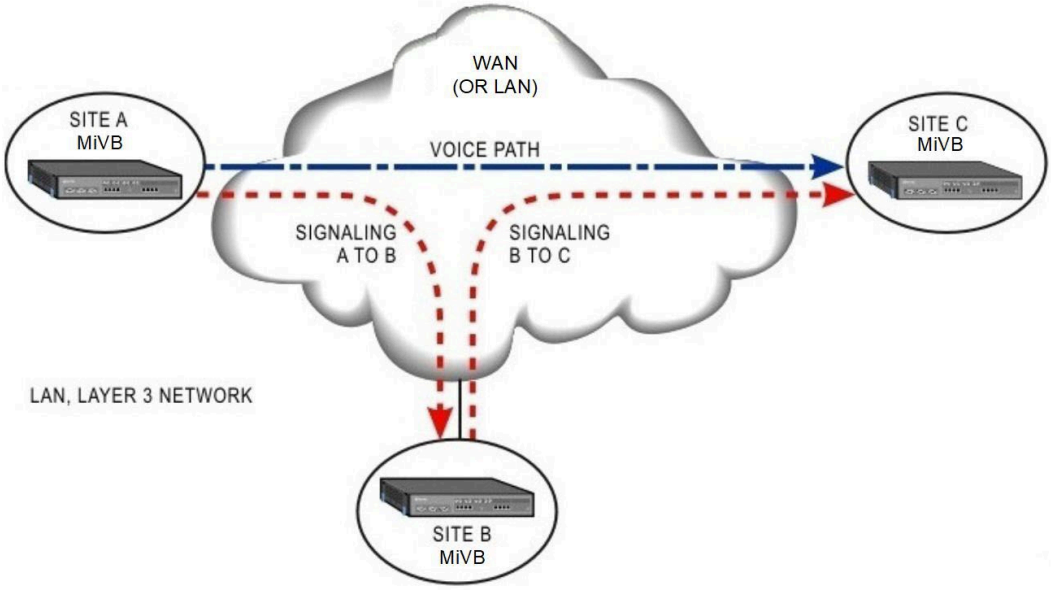


Figure 18: Signaling and Voice Path Example 1

In the tandem case, a virtual IP trunk is used from A to B and another virtual IP trunk is used from B to C. These trunks are counted against the routing limit.

In certain networks, especially external WANs that use VPNs, the most direct path from A to C may actually be through the IP router at site B. However, the 3300 ICP at this site only handles the signaling and not the voice traffic.

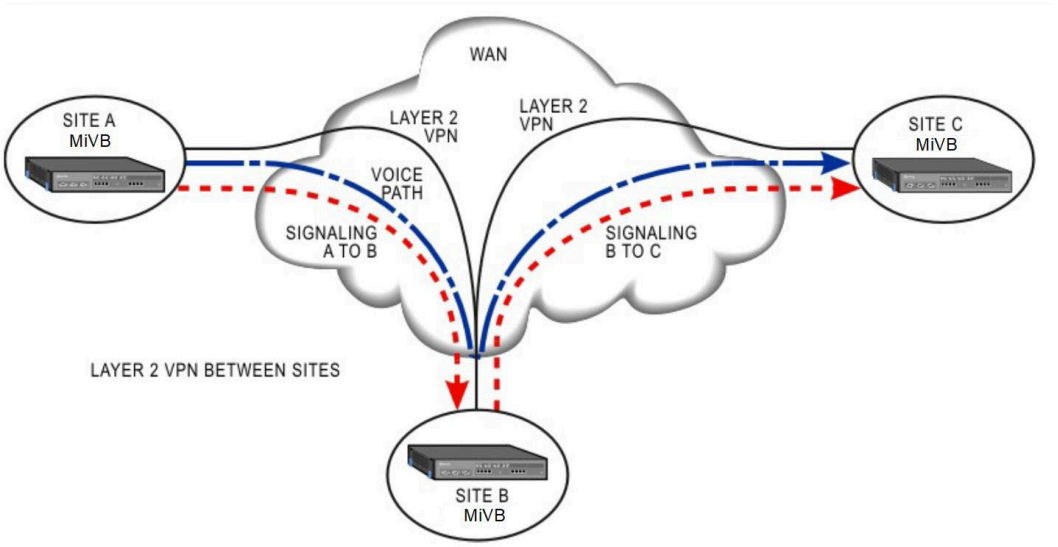


Figure 19: Signaling and Voice Path Example 2

Consider the different routing in different parts of the network when bandwidth calculations are involved. Refer to Traffic and Bandwidth Calculations for bandwidth calculations.

9.6 Variable RTP Packet Rates

Currently, the MiVoice Business has only one means of connecting to service providers via IP technology: over SIP Trunks. Some service providers of SIP trunks may require packet rates that are not 20 ms. In this case the installer can select packet rates for SIP trunks other than the default value of 20 ms. Alternatively, the installer can use an MiVoice Border Gatewayat the edge of the customer network to adapt packet rates to what the service provider requires.

The bandwidth used by the IP media streams will vary according to the packet rate value chosen. Relative to current usage, bandwidth usage will rise by 27% when using a 10 ms packet rate for G.711 and by 80% when using G.729, but will decrease if the packet size chosen is greater than 20 ms. Chapter 11,*Bandwidth, Codecs and Compression*provides specific details on bandwidth requirements to support SIP trunks with different packet rates.

The working packet rate should be a multiple of the working CODEC frame rate. Chapter 12,*Maintaining Availability of Connections*, provides specific details under the CODEC Selection heading of CODEC frame rates.

MiVoice Businesssupports packet rates from 10ms to 80ms in steps of 10ms. MiVoice Border Gatewaygoes up to 60ms (also in 10ms increments).

The following Mitel devices and applications will support variable RTP packet rates:

- E2T/Media Server
- 5304
- 5215
- 5220
- 5212/24
- 5312/24
- 5330/40/60
- 6905/10/20/30/40
- MiVoice Business Console
- 5560
- MiVoice Border Gateway(Teleworker)
- Mobile Extension

9.7 Constraints

At this time, a limited number of 3rd-party phones and applications will be compatible with a non-default (i.e. 20 ms) packet rate.

Since the 3300 ICP does not support rate adaptation between media streams using different packet rates, it will not be possible to connect a media stream between two service providers that require different packet rates through the 3300 ICP.

The MiVoice Border Gatewaycan provide packet rate adaptation between the internal and external address interfaces. This can be used to provide a different packet rate to a carrier compared to a local packet rate, thus allowing internal devices and applications to run at a common rate that may be different from the carrier.

Note:

If some applications and/or phones that do not support variable RTP packet rates are combined into a solution which requires variable RTP packet rates it will result in undefined behaviors. Specifically, the users may experience scenarios where there is no audio in one direction or both directions. These types of audio problems can be difficult to isolate and resolve. Before deploying any phones or applications that employ variable RTP packet rates, the administrator or installer should review all sets and applications that comprise a particular solution to determine if they are all compatible with variable RTP packet rates.

9.8 Service provider behavior

Some Service Providers require that a specific packet rate be used on both receive and transmit streams, in these situations the MiVoice Business will attempt to comply with the Service Provider's requirements.

In cases where the MiVoice Business cannot meet the Service Provider's requirements, some Service Providers will allow the call to proceed with unacceptable packet rates, only to block the media stream. Other Service Providers might fail the negotiation entirely, and the call will never be connected.

For correct operation it is necessary that calls to or from a Service Providers contain, in the original SDP (Session Description Protocol) negotiation, the packet rate (or "ptime" parameter) that the Service Provider is willing to accept. The 3300 ICP will communicate this requirement to the eventual endpoint.

9.9 Automatic Route Selection

When Automatic Route Selection (ARS) involves TDM connections that include switched DPNSS or X-Net, restrictions apply to the range of IP addresses used on the ICP RTC. Each ICP controller requires an IP address to uniquely identify it and each uses a fixed effective subnet mask of 255.255.255.192. IP addresses between units must be different than the effective mask. Examples are shown in the table below:

Table 24: Examples of IP Address Assignment for Use in Automatic Route Selection

ICP 1 IP address	ICP 2 IP address	Acceptable?
192.168.1.2	192.168.1.66	Yes (different subnet)
192.168.1.2	192.168.1.130	Yes (different subnet)
192.168.1.2	192.168.1.127	No (broadcast address on second subnet)
192.168.1.2	192.168.1.62	No (within same subnet mask range)

Further details on installation can be found in the *Technician's Handbook*and in the *System Administration Tool Help* for MiVoice Business.

9.10 Number Planning and Restrictions

The length of number plans for clustering and resiliency should be consistent among all units to prevent confusion in routing. Plan the location of systems and number assignments before installation.

Clustering is the recommended configuration for larger systems. Clustering is required for Resiliency and hot desking between systems.

Further details can be found in the Clustering and Resiliency documentation.

9.11 Networking and Product Release Compatibility

Product improvement is part of an important and ongoing process and it includes the need for new product releases. While every effort is made during the development process to ensure that the new release is compatible with earlier releases, there may be instances where this cannot be fully achieved. This may become apparent due to, but not limited to, differences in expected system operation and feature availability. To minimize such instances, ensure that networked units operate with the same software release numbers or at least minimal differences between release levels.

Known compatibility restrictions for IP Trunks and for SDS include:

- MiVB 6.0 and higher are compatible up to and including MiVB 9.0 SP3 .
- MiVB 7.1 and higher are compatible with MiVB 9.1 and higher.

9.12 SIP Trunking

Service providers and carriers offer their customers the option of connecting to the service provider via a SIP (Session Initiated Protocol) trunk. SIP Trunking can be a more cost effective method of obtaining PSTN connectivity.

9.12.1 SIP Trunking Basics

The MiVoice Business can use SIP trunks to connect to service providers that offer SIP gateway or trunk connectivity. The SIP trunking solution provides basic telephony functionality, billing capability, emergency services support, FAX support, and more.

The SIP trunking solution also provides T.38 Fax over IP capabilities, for additional information see Support for FAX over IP.

Licenses

You can purchase SIP trunking as an option. The MiVoice Business supports a maximum of 2000 SIP licenses. SIP licenses are obtained through the AMC server.

Networking ICPs with IP trunks

When using IP trunks to network multiple ICPs together, all ICPs in the network should be upgraded to a recent version of software if SIP is licensed. This will ensure RTP stream compatibility for DTMF digits, NAT traversal, etc

Networking ICPs with TDM trunks

Networks that connect ICPs together using TDM trunks will continue to function as they did in previous releases. SIP does not affect this behavior. In fact, the 3300 ICP can operate as a Gateway between a TDM connected PBX and a SIP Service Provider.

Applications compatibility

To ensure applications compatibility with an ICP that is using SIP trunking, the System Administrator needs to ensure that all applications that use MiAudio or emulate a MiNET phone are upgraded to versions that support RFC 4733.

RFC 4733, RTP Payload for DTMF Digits, Telephony Tones and Telephony Signals is an IETF memo that describes how to carry DTMF signaling, other tone signals, and telephony events in RTP packets.

Third-party phone compatibility

DeTeWe and SpectraLink setsand Mitel DECT base stations and sets,support RFC 4733, NAT keep-alives, and utilize a single port for transmit and receive streams. As a result, these sets are compatible with an MiVoice Business that is using SIP trunking.

Support for FAX over IP

When using SIP trunks to connect the 3300 ICP to the service provider, G.711 FAX pass through and T.38 Fax over IP are both supported.

When the ICP detects a FAX calling tone or a V.21 tone, if both the ICP and the Service Provider support T.38 capability, then the ICP will disable the echo canceler and the call will proceed as a T.38 call. However if the FAX is to be transported via G.711 pass through, then the ICP will leave the echo canceler on the line and a Jitter buffer designed for FAX pass through will be enabled.

Class of Service (COS) options

An option called ‘Fax Capable’ appears in the ‘Class of Service Options’ form. This new option is located under the ‘Fax’ heading.

For correct operation, ports that are used to connect to Fax machines must have the following COS option enabled:

- Fax Capable (Set to “Yes”)

In addition to the Fax Capable COS option, the Administrator is advised to set the following COS options as indicated. If some of these overrides are not set as indicated and a tone is generated on this port while a Fax transmission is in progress, then the Fax transmission will likely fail.

- Campon Tone Security (Set to “Yes”)
- Busy Override Security (Set to “Yes”)
- External Trunk Standard Ringback (Set to “Yes”)
- Return Disconnect Tone When Far End Party Clears (Set to “Yes”)

The Administrator should "enable" V.34 Fax Interop at V.17 speeds with SIP Gateways; the factory default for this is disabled. This setting is a global setting; the setting is applied to all ports on a system. This setting can be found under "Fax Advanced Settings"; for details see the *System Administration Tool Help* for MiVoice Business.

SIP aware firewall

The MiVoice Business supports integration with SIP Firewalls. Mitel recommends that a SIP aware Firewall be configured as the Outbound Proxy through the Network Elements form. Then the SIP Peer Profiles can reference the Outbound Proxy Server and route all signaling via the Firewall.The MiVoice Border Gateway or a commercial SIP Border Controller can be used for this purpose.

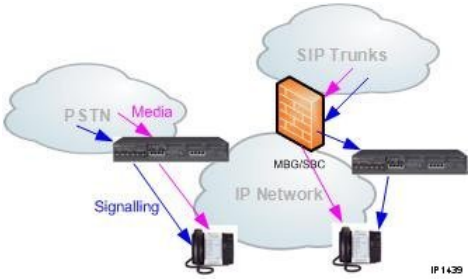


Figure 20: Enterprise Site with SIP Aware Firewall

The ingate SIP Firewall is interoperable with the 3300 ICP based SIP solution. You can obtain the Ingate product documentation at www.ingate.com. The Mitel SIP firewall product is the MiVoice Border Gateway. Information is available on Document Center

TCP IP port usage

The 3300 ICP uses the following default ports for SIP trunking:

- 5060 for TCP/UDP SIP
- 5061 for TCP SIP-TLS (Transport Layer Security)

> **Note**:
>
> When establishing firewall rules, keep in mind that TLS is, by default, over TCP.

You can modify these values using the System Administration Tool. The valid port ranges are 1 to 65535.

Resiliency

Some service providers may offer service resiliency. There are two different mechanisms for making use of service provider resiliency; IP addressing or FQDNs (Fully Qualified Domain Names). The ICP does not support service resiliency using IP addressing, but it can use FQDNs to make use of service resiliency. For details, refer to the MiVoice Business *Resiliency Guidelines* .

Mitel resilient call state and call survivability is not supported in conjunction with SIP trunking.

911 emergency services

SIP trunking supports 911 emergency services. The System Administrator can choose whether or not the SIP service provider should be the outgoing emergency route.

If the SIP service provider will provide support for 911 emergency services, the following requirements must be met:

- Ensure that the contract with the service provider covers 911 emergency service support. If the SIP service provider passes this information to the PSTN when the call leaves the SIP network then the PSAP will have the proper information for the emergency service.
- Ensure that any geographical differences between the location of the phones and the location of the service provider are addressed by the service provider.
- Ensure that the CESID information is programmed.

The System Administrator should also provision the installation with a backup connection to the local PSTN to maintain connectivity in the event the SIP trunk fails.

Licensing 10

This chapter contains the following sections:

10.1 System Licenses

There are two switch packaging options (System Types) which are defined as follows:

- Standalone
- Enterprise

In “Enterprise” systems users can be made Resilient, but in “Standalone” systems they cannot. “Enterprise” systems allow network or cluster programming, whereas “Standalone” systems do not. Licenses may also be shared among the nodes in a network of “Enterprise” systems. The requirement that a resilient device only consumes one set of licenses in an Enterprise system is maintained.

Note:

MiTAI Applications will not be able to connect if MiVoice Business is unlicensed.

MiVoice Businessrequires the following licenses to operate:

- IP Users license/Multi Device User License

An IP user license is needed for every user (including SIP) connected to the MiVoice Businesssystem as their primary controller. IP user licenses are not required on secondary (resilient) controllers or on "userless" devices that provide basic functionality (emergency/attendant calls and hot desk login).

The maximum number of active IP user licenses varies by controller type as follows (these are guidelines only – they are not software-enforced rules):

- CX/CXi II - 150

- MXe III Standard - 300
- EX and MXe III Expanded - 1400
- MiVoice Business ISS and Virtual servers - 5000
- AX Controller - 700

The concept of “Trusted Applications” removes the need for IP licenses on some applications that use emulated IP phones to connect to the MiVoice Businesssystem. Although these applications do not consume a license, the IP sets that they use to connect with the system do consume resources, and therefore still count towards the maximum number of users on a system. The following applications may be considered “Trusted” if the installed revision of the application is able to support the concept of a trusted application:

- MiCollabApplications (MiVoice Border Gateway; Unified Messaging; Audio, Web, and Video Conferencing, MiContact Center Business, etc.)
- MiCollabUnified Messaging (UM)
- MiContact Center BusinessandMiCC IVR

All other applications (including the above if they do not support the “Trusted” concept) are considered “Untrusted” and still require an IP user license for each emulated phone.

If no IP User (IPU) license is available (none is allocated or all are consumed), the system automatically consumes an available Multi-device User (MDU) license on behalf of the following IPU users: Full Service IP User, IP Console, External Twin Multi-device User Group. When an IPU license becomes available (for example, when additional IPU licenses are allocated), the MDU license returns to the pool and one of the newly allocated IPU licenses is automatically consumed.

- SIP Trunks license

A SIP license is needed for every SIP trunk connected to the MiVoice Businesssystem. This includes SIP trunks to a SIP Trunk Service Provider, as well as SIP trunks to other SIP devices, such as SIP gateways or applications, through the SIP protocol over the IP network.

- Hot Desk User and External Hot Desk User license

External Hot Desking is an extension of the system’s hot desking capabilities. The hot desk function consumes a user license in the system. This is also true when External Hot Desking is employed. An External Hot Desk User (EHDU) License is required to extend the hot desking function to an external device. This will also use an IP user license, even if there is no IP phone involved, since a device number must still be allocated. The maximum number of available “External Hot Desk User Licenses” will be equal to 100% of supported IP users if these are the users’ only sets, but if the users have both internal desk sets and EHD sets then the number of users supported will be reduced by one half.

- Multi-device Users license

It is possible to create Personal Ring Groups (PRGs) whose members are collectively licensed under a single Multi-Device License instead of being individually licensed as users.

MDU licenses are automatically consumed on behalf of the following IPU license users if no IPU license is available: Full Service IPU User, IP Console, External Twin Multi-device User Group. When an IPU license becomes available, the MDU license automatically returns to the pool.

- Multi-device Suites license

It is possible to create suites whose members are collectively licensed under a single Multi-Device License instead of being individually licensed as users.

- Single Line User License

A Single line user license is needed for each ONS port on the ASU II or AX, and for each FXS port on the EX. If you attempt to program an ONS or FXS device on an ASU II, AX or EX and you exceed the number of purchased Analog Line Licenses, the system rejects the programming change. The Single line license is also required for single line IP and SIP users. The System Capacity form in the system administration tool displays the number of Purchased Licenses and the number of Used Licenses.

- ACD Active Agent license

An ACD Agent license is needed for every active agent on the system. A business that runs shift work patterns may have more agents in the database than those currently logged in. A traditional ACD Agent can only use licensed devices. ACD Hotdesk Agents consume an ACD Agent license when they log in. All ACD Agents consume an IP user license when they log in on the primary node, but resilient agents do not consume a license on the secondary.

- Embedded Voice Mail license

A Voice Mail license is needed for every simple voice mailbox user that has been configured. Functions include Basic Voice Mail, Basic Auto-Attendant, Voice Mail Language Support, and Multi-level Auto-Attendant.

- Digital Links license

A Digital (Network) Link license is needed in order to enable a single T1/E1 link.

- Compression license

A compression license is needed for every call that passes through a MiVoice Business/3300 ICP controller that requires a compression resource.Calls that do not pass voice through the controllers (IP trunk to IP set, or IP set to IP set) do not use a compression license. Calls that typically require a MiVoice Business/3300 ICP compression resource are those that are associated with an IP trunk where the call

traverses TDM to IP, or vice versa, and where there is a remote connection with limited bandwidth. The use of compression is defined through compression zone configuration and the zone with which the phone is associated. In the systems using dedicated MiVoice Business/3300 ICP hardware, additional DSP hardware must be added in order to enable compression. For MiVoice Businessin commercial servers, compression resources are provided in software by the Media Server component (software blade). Compression licenses are available in increments of 8 sessions.

- Fax over IP (T.38)

A T.38 license is required to allow an ICP to originate or terminate Faxes over IP or SIP trunks from TDM ports. A field called ‘Fax over IP (T.38) licenses” can be found under purchasable option. The Wizard will validate that the value input is a multiple of 4. Minimum value: 0, maximum value: 64 (recommended maximum 48). Enter the number of licenses purchased. Licenses can be purchased in groups of 4 up to a maximum of 64. A reboot is required to enable new licenses. This option is only available on dedicated MiVoice Business/3300 ICP hardware which can terminate FAX calls on TDM interfaces. It is not applicable to servers which cannot connect to TDM ports.

Note:

FAX over IP support requires the DSP II cardin the CX-II and MXe-III systems. You can purchase and configure licenses on the system before you install the required DSP II cards in the system. However, an alarm will be raised after you reboot the system if required DSP II cards are not installed.In the EX Fax over IP is supported natively by the DSP resources on the PRI card with no additional licenses required.

- HTML Applications license

Each license allows you assign HTML applications to a device using the User and Device Configuration form in the System Administration Tool. Up to 5600 licenses are supported.

- X-NET Networking license

This license is enabled for “Enterprise” system, and disabled for “Standalone”.

- IP Networking license

This license is enabled by default in an “Enterprise” system, and disabled for “Standalone”.

- Voice Mail networking license

This license is enabled by default in an “Enterprise” system, and disabled for “Standalone”.

- Advanced Voice Mail license

This license is enabled by default in all systems.

- Embedded Voice Mail PMS license

An embedded voice mail PMS (Property Management System) license is needed to enable access to hospitality/PMS services.

- Tenanting license

The Tenanting package allows the MiVoice Businesssystem to be configured to look like a separate system to each participating tenant. The functionality that this option provides includes: definition of up to 64 tenant groups, multiple music sources, tenant-based restrictions and permissions, tenant-based outgoing and incoming trunk behavior (includes tenant-based route selection), and tenant- based night services.

- MiVoice BusinessIDS Connection license

An Integrated Directory Services (IDS) license is needed to add IDS forms to the MiVoice Businessinterface.

10.2 Device Licensing

The 3300 ICP requires a number of device licenses in order to operate. The following table lists these licenses.

Table 25: Devices and licenses

Device	License
IP phone[3]	IP user license
User on IP phone	IP user license
User on SIP phone	IP user license
Resilient User on SIP Phone	No user license required on resilient controller

Device	License
User on ONS Phone	Analog line license[4]
CITELink phone	IP user license
Wireless phone (SpectraLink)	IP user license
Wireless phone (IP DECT - EMEA)	IP user license
Resilient phone on secondary controller	IP device license
Hot Desk user	IP user license
External Hot Desk User	External hot Desk User License
Hot Desk phone	IP device license
Unified Communicator Mobile	One IP device license and one IP user license for each line monitor, call agent, and TUI agent used in the Unified Communicator Mobile Server
MiCollab Client	None needed
MiCollab Client Softphone	IP user and IP device licenses
ACD Agent	ACD Agent license
Voice Mailbox[2]	Voice Mailbox license (1 per user)
Basic Auto-Attendant	Voice Mailbox license

Device	License
Multi-Level Auto-Attendant	Voice Mailbox license (1 per node in the tree)
Record-a-Call	Advanced Voice Mail license (system-wide)
Auto Forward to Email	Advanced Voice Mail license
Personal Contacts	Advanced Voice Mail license
Networked Voice Mail, VPIMv2	One Voice Mail Networking license per ICP
NuPoint	One IP device license and one IP user license per port to 3300 ICP
IP Networking (IP Trunk)	One IP Networking license needed per ICP to enable IP Trunk calls
Digital trunk (PRI, etc.)	One Network Link license per digital trunk span
Fax over IP (T.38) licenses[5]	A T.38 license is required to allow T.38 transmission or reception of Fax over an IP or SIP trunk when the call path may encounter TDM interfaces—for example, T1/E1 trunks, analog loop start trunks, or ONS ports. The T.38 licenses are provisioned in multiples of 4; the minimum value is 0 and the maximum value is 64.

Device	License
Compression (TDM/IP)	A Compression license is needed for TDM to IP or IP to TDM calls that require the use of the DSP compression. One Compression license can handle up to 8 calls
Teleworker Solution (6010)	One IP user license per phone
Customer Interaction Solutions[1]	One IP user license per port to 3300 ICP
HTML Apps Infrastructure Licenses	A license is required to assign HTML applications to a device.
Speech Server[1]	One IP user license per port to 3300 ICP
Messaging Server[1]	One IP user license per port to 3300 ICP
Hospitality / PMS	Hospitality option
X-NET over TDM	One license to enable X-Net networking over TDM links
Tenanting	Tenanting license
Multi-device User Group	Multi-device user license (for Standard group) IP user or Mult-device user license (for External Twin MdUG)[5]

Note:

1. The licenses described are those applicable to the 3300 ICP. The Customer Interaction Solutions, Speech Server, and Messaging Server also require application licenses to enable their functions.
2. The number of voice mailboxes is not the same as the number of voice mail ports enabled. The number of ports required depends on the quantity and duration of calls to the mailboxes and can be adjusted up to the limit of 30 ports within ESM without changing any licensing.
3. The IP user licenses limit includes SIP and MiNET devices as well as users.
4. A Single line user license is required for ONS ports on the ASU II and the AX, and for FXS ports on the EX. ONS ports on the ASU and the AMB/AOB do not require licenses.
5. If no IP user (IPU) license is available (all are consumed or none are allocated), the system instead automatically consumes an available Multi-device user (MDU) license on behalf of the following users: Full Service IP User, IP Console, External Twin MdUG.

10.3 Licensing Limits

Available resources determine if license limits can be achieved. For example, if there is insufficient DSP for voice mail, the operational limit may be reached before the license limit. Be very careful with large numbers of licenses for voice mail and compression. Because DSP resources are allocated at initialization based on license numbers, not traffic requirements, it is possible to allocate all DSP resources and have nothing left for telecom tone receivers and generators, so calls cannot be made on the system. The table below shows limitations to the licenses.

Table 26: License limits

License type	Maximum limit
IP user license	5600
SIP trunking license	2000

License type	Maximum limit
T.38 Fax Over IP.	Maximum of 64 licenses (recommended limit 48)
Compression license	64 licenses (256 channels on 2 DSP-II modules)
Analog line license	5000
Voice mail license	750 (includes advanced VM licenses)
Mailbox license	cannot exceed the maximum number of user voice mailboxes available (up to 750)
ACD Agent license	2100 (the limit for active agents is much lower, depending on the type of controller – refer to #unique_25/unique_25_Connect_42_id203BAF001GA)
Digital Link license	8
IP networking (IP trunk) license	Y/N
Advanced Voice Mail license	Y/N
Hospitality / PMS license	Y/N
Voice Mail Networking license	Y/N
Tenanting license	Y/N

10.3.1 Licensing Example

The following example shows how to determine the number of licenses required. For more accurate traffic calculations, contact Customer Engineering Services. Please note that the numbers below are approximations.

Consider an installation with two headquarters and one remote office connected to the first headquarters. The following table shows a list of the equipment installed at each of the sites.

Table 27: License example

Headquarters 1	Remote 1 connected to HQ1	Headquarters 2
3300 ICP MXe III	No controller, linked to HQ1	3300 ICP MXe III
Resilient secondary for HQ2 (200 ph ones)	No resiliency support	Resilient secondary for HQ1 (400 ph ones at HQ only)
PSTN access via PRI, 4 links	Access via HQ1	PSTN access via HQ1 (backup on LS for 4 trunks)
IP networking to HQ2	Direct connection to HQ1	IP networking to HQ1
Compression enabled to HQ2 Comp ression disabled to remote	Compression enabled to HQ2 Comp ression disabled to HQ1	Compression enabled to HQ1 Comp ression enabled to remote
400 IP phones (mixture)	20 IP phones (5312)	200 IP phones
Includes 20 ACD and display board	No ACD	No ACD
Includes 10 MiCollab Client	No MiCollab Client	No MiCollab Client
Includes 10 MiCollab Client Softph one	No MiCollab Client Softphone	No MiCollab Client Softphone
16 ONS phones	No ONS	2 ONS phones
20 Voice Mail sessions, 420 Mailbox users	Use Voice Mail at HQ1	10 Voice Mail sessions, 200 Mailbox users
2 Auto Attendant sessions	No Auto Attendant	No Auto Attendant
1 Record-a-Call session	Record-a-Call in HQ1	No Record-a-Call
No Hot Desk operations	No Hot Desk operations	No Hot Desk operations
No TDM networking	No TDM networking	No TDM networking

Taking each of the licenses in turn, the above information results in the following calculations and resulting licenses:

- **IP user License**

IP user licenses apply to IP phones. There are 420 users on HQ1 (400 local and 20 remote) and 200 users on HQ2. Thus the site total is 620 licenses.

- **Hot Desk License**

There are no Hot Desk services, so no Hot Desk licenses are needed.

- **ACD License**

There are 20 active ACD agents on HQ1, so 20 licenses are needed.

- **Digital Link License**

Only HQ1 has digital links, and these are 4 spans, so 4 licenses are needed.

- **Compression License**

IP phones already include compression licenses, so calls between IP phones do not need additional licenses. Licenses are needed for calls through the 3300 ICP. Compression is enabled between HQ1 and HQ2. Compression is disabled between HQ1 and the remote site. So, only trunk calls via HQ1 from HQ2 are needed. There are 200 IP phones, few TDM, so with a trunk traffic rate of 4 CCS (6 CCS x 2/3) then 24 channels are needed (200 x 4 / 36 x 1.1 (+10%)). Since hardware compression comes in either 32 or 64, then 32 licenses are purchased for HQ1. This allows some degree of expansion and error margin, even though only 24 licenses are needed.

- **X-Net License**

There is no networking between units over TDM, so no X-Net licenses are required.

- **IP Trunk License**

This includes all calls between HQ1 and HQ2. One license is needed per ICP, making a total of two for the installation. For configuration of IP trunk limits on the route, both trunk and internal calls must be considered. From the compression license, 24 channels are needed for trunks. A further two channels are needed for internal calls, making a total of 26 IP trunks (200 X 2/36 X 15% (networking) X 1.1 (+ 10%)).

- **Voice Mail License**

At HQ1 there are 420 voice mailboxes. At HQ2 there are 200 voice mailboxes. For the site, a total of 620 licenses are needed.

- **Advanced Voice Mail License**

At HQ1 there are additional services: two Auto-Attendants and one Record-a-Call. Thus, a total of three licenses is needed.

- **Hospitality (PMS) License**

There is no connection to a PMS system and so no PMS licenses are needed.

Note:

The numbers and calculations are a rough estimation. More accurate results can be obtained by using the System Engineering Tool.

10.4 Application Management Center (AMC)

The online licensing process managed by the Mitel Application Management Center (AMC) allows Solution Providers who have accounts on the AMC to manage software licenses online. Each company is able to supply customers instantly if new licenses are required. Refer to “Requirements for AMC Connection” in the *MiVoice Business Technician's Handbook* for Software Installer Tool and 3300 ICP system networking requirements.

Bandwidth, Codecs and Compression 11

This chapter contains the following sections:

CODEC Introduction

The word CODEC is a concatenation of two words: Coder and Decoder. The CODEC is actually two functions, coding and decoding, for the conversion of media, in this case, voice, into some data format that can be returned at the far end into something akin to the original. For voice, this usually involves converting the analog signals into digital signals and levels and returning them back to analog.

The most popular CODEC, G.711, has become standardized across large parts of the telephony network. As such, it has become the baseline for IP devices to perform to. The G.711 CODEC comes in two varieties: A-Law and µ-Law. Typically these coding laws were kept separated by geographic boundaries, but with increasingly global IP traffic, both types are regularly encountered. Therefore a G.711 CODEC has to negotiate which coding law to use as well.

Other coding laws also exist. One that gives good voice quality and is also efficient at coding is G.729. This also comes in different formats:

- G.729 - original version—very processor intensive
- G.729a - reduced processor effort and compatible with G.729 (Supported by MiVoice Business)
- G.729b - includes voice activity detection and ability to send background information. Compatible with G.729 and G.729a (Not supported by MiVoice Business)

G.729 and G.729a are functionally equivalent, and although MiVoice Business actually uses the G.729a algorithm in the products, all references to G.729 and G.729a in this document can be treated as equivalent.

Wideband audio, up to 7kHz (50Hz to 7.0kHz) of voice bandwidth, is available with the G.722 range of codecs. Although there are a number of wideband codecs under the G.722 banner a number of these are not compatible with each other, so extra care is needed when specifying these.

The wideband codec used by Mitel is G.722.1 at 32kbits/s (which is not to be confused with the G.722 wideband codec, or the G.722.1C codec, or the G.722.1 at 24kbits/s).

Mitel currently uses the following CODECs in IP Telephony:

- G.711 (A-Law and µ-Law)
- G.729a
- G.722.1 at 32kbits/s

CODEC G.729 is generally referred to as "compression" even though this is a generic term. CODEC G.722.1 is generally referred to as "wideband" even though it also provides a bandwidth usage improvement over G.711.

Voice quality and codec selection

The voice quality of the CODECs available is usually expressed in terms of a Mean Opinion Score (MOS). The scores range in value from 1 to 5. Scores 4 and above are considered toll quality. The table below shows some typical CODEC MOS scores.

Table 28: CODEC MOS Scores

CODEC type	MOS	LAN bandwidth
G.711	4.4	~100 kbit/s
G.729a	4.0	~40 kbit/s
G.722.1	4.4	~65 kbit/s

Transcoding and compression

The terms “transcoding” and “compression” are often used interchangeably. Transcoding is the changing of voice information from one CODEC type to another. However, most CODEC devices rely on G.711 as the base entry level. Transcoding from G.729a to G.726 is likely done through G.711. Compression is simply reducing the amount of data. For voice traffic, this can be achieved by going from G.711 to G.729a, for example.

Any form of voice compression works by removing a certain amount of information deemed non-essential. This may include not sending data during silent periods, as well as sending only the main voice frequency elements rather than the full bandwidth. As a result, some information is lost. G.729 compressed voice is never as good as uncompressed voice, but the required intelligibility is maintained.

In the LAN environment where bandwidth is plentiful, there is little reason to compress voice, and so G.711, or G.722.1 between compatible devices, are normally the CODECs of choice. is normally the CODEC of choice. In a WAN environment, where access bandwidth may be limited, use of the G.729a CODEC can increase the amount of voice traffic that can be carried on a particular link. In some instances, such as connection to an external PSTN trunk, G.711 is still preferred for voice quality, but voice traffic will be limited on the link.

Wideband voice

The use of IP and the ability to use bandwidth values that are not directly linked to TDM channel limits, allows the use of new CODECs and features.

A wideband audio CODEC has been added to the system capability and is supported on media servers and some IP devices. The CODEC implemented is G.722.1 and is based on ITU-T standards. It provides voice capability with a bandwidth of 50Hz to 7kHz, compared to 300-3400Hz for a standard telephony channel.

Wideband audio is not supported over the analogue PSTN. The G.722.1 CODEC is also not easily supported over the digital PSTN (BRI, PRI) and could nominally be used only for point to point connections. For these reasons the G.722.1 CODEC is only supported on IP end devices with the CX-II, MXe-III and EX, but is supported for conferencing and other internal features on the media server in the MiVoice Business ISS and Virtual variants.

The G.722.1 wideband codec is also supported by some 3rd party SIP products, so allowing for interoperability of this feature between different vendor end devices.

Bandwidth, Bandwidth Management, Codecs and Compression

An IP packet carrying voice information has a number of additional “wrappers” (see graphic below) so that different network devices know how to route the information (IP address), how to forward information between physical devices (MAC address), and how to identify when a packet starts and finishes (Ethernet).

These additional wrappers add overhead to the overall packet. This overhead increases the bandwidth required to transport a voice packet. To understand the true bandwidth requirements, this overhead must be taken into account.

Codecs are devices or programs that encode or decode a signal into a digital format, in this case, the voice payload. Different codecs can provide different sized voice payloads given the same input information. A reduction in payload is often referred to as compression.

The following sections discuss bandwidth, codecs and compression in further detail.

11.1 Bandwidth Management

Bandwidth management and call admission control

The terms “Bandwidth Management” and “Call Admission Control” are often used interchangeably to mean the management, and potential re-routing, of calls across an IP network between end devices. In reality these are two separate concepts. Bandwidth management gathers information about the availability and use of bandwidth on particular connections and links. Call Admission Control uses this information to decide whether a call should be completed or not.

Although the IP network is often considered as a “cloud,” it is actually made up of many parts, including LANs, MANs and WANs. There are constraints on the amounts of data that can be handled at the transitions between the different networks, and often within the networks themselves.

If a link is bandwidth limited, it is desirable to be able to determine the available bandwidth across the link and manage it to ensure that it is available for voice use. Once the bandwidth is known, it is possible to determine how many virtual channels can be established and to admit, redirect or reject calls based on current available resources, that is, bandwidth. The latter is the task of Call Admission Control between end nodes.

Call admission control updates

Currently, Call Admission Control is applied to calls that must pass between different controllers and nodes, including when using IP Networking or IP Trunks. The same mechanism also applies to SIP Trunks. In most cases, this is an appropriate way to limit and re-direct calls. This mechanism is now being expanded across the entire installation through the use of common zone numbering. This will provide finer control of call admission in situations including:

- multiple nodes that use a common network connection
- remote workers who don't use IP Networking, including hot desk users
- resilient/redundant switchover to a backup controller at a remote site with limited bandwidth
- identification of bandwidth usage

Call Admission Control works by:

- knowing the network topology and identifying bottlenecks such as edge routers
- tracking bandwidth usage at the bottleneck/gateway points
- specifying voice limits for a connection, e.g. voice may only be allowed to use 50% of the link
- following the media path connection, that is, the most direct path. Signaling may involve a number of units and may follow a different path than the media does. When

traversing zones, however, the calls must go through a bandwidth controller to be counted.

The zones and network topology are defined and propagated between the controllers and the Enterprise Manager. Some additional tuning may be required locally at controllers where bandwidth is shared. You may need to specify alternative routes where multiple routes go through a common bottleneck, or where bandwidth is shared between a primary and secondary controller for resilient operation in the event of a controller failure.

Call Admission Control and re-routing applies to normal calls. Emergency calls, certain priority calls and established calls being re-routed, for example, calls on hold, do not need to negotiate access. The use of the resource will be noted and subsequent (non-emergency) calls from the same extension may be restricted.

More details on programming and defining zones are highlighted in the System Administration Tool Help for MiVoice Business. Some typical network deployments are shown below, along with how they would be realized using the tree topology information.

There are some important points to consider with the Call Admission Control in place.

- For Call Admission Control and Bandwidth Management to be effective, call setup must pass through all the bandwidth managers responsible for monitoring the bandwidth along the entire path taken by the call's audio stream.
- Available bandwidth can be allocated across multiple bandwidth managers (up to 6 with single level mapping). Bandwidth managers need routing lists to link to each other so the bandwidth can be shared dynamically.
- Mitel recommends multiple bandwidth managers and multiple zone access paths for resilient operation so that bandwidth control is maintained if a single unit fails.
- Integrate the bandwidth manager with the controller hosting the phones. This will allow you to monitor the bandwidth of remote phones hosted from a central call server.
- Bandwidth managers should be logically located with the bandwidth pipe to be monitored, either upstream, or downstream, that is, the call should monitored as it exits or enters through a router connection.

Determining the position of the root node in meshed and non-meshed WAN

When building up the connection tree, the most important point to recognize is the location of the root zone. Often this is the WAN (as shown in the Figure 1), but this may not always be the case.

Fully meshed WAN connections

In a fully meshed network where the WAN can switch data, or where VPNs exist from every access point to every access point, then the root node is the WAN. In the case with multiple nodes, this can lead to many VPN connections.

The following figure shows a deployment example of a fully meshed WAN network. In this example, a distributed sales organization is linked using an MPLS network.

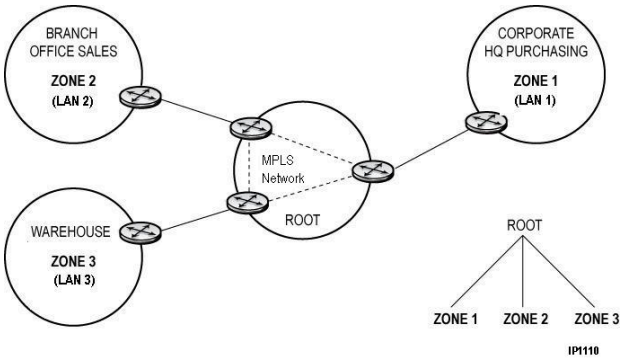


Figure 21: Fully-Meshed WAN Connections - Deployment Example

Table 29: Fully-meshed Network with WAN as the Root

Zone	Parent
1	Root (WAN)
2	Root (WAN)
3	Root (WAN)

In a multi-node installation, it is also possible to link a single VPN back to headquarters at another site using a star configuration. If the WAN network router (Service Provider Router; see the following figure *Fully-meshed WAN Connections - Star Configuration*) at the HQ site can perform routing between the different sites, this is equivalent to a fully meshed network, since the network router will re-direct the data and not use bandwidth back to the headquarter site.

This star configuration can still be described by the table *Fully-meshed Network with WAN as the Root,* and is illustrated in the following figure. The number of routes within the WAN are reduced, but from the end user view, this configuration behaves in the same manner as the fully meshed configuration. The only consideration for this star configuration is that the central router will be dealing with all internode traffic, and must have the necessary performance to handle the bandwidth and packet rate expected within the WAN connections.

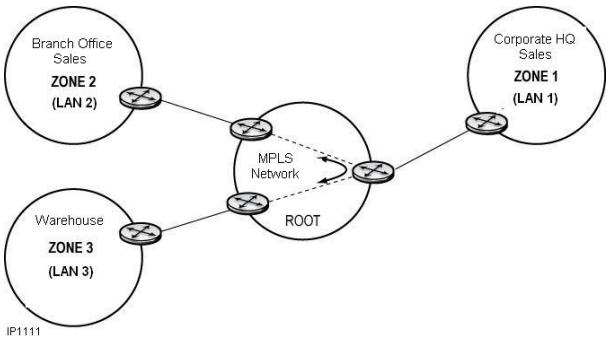


Figure 22: Fully-meshed WAN Connections - Star Configuration

Non-meshed WAN connections

If all VPNs terminate at the HQ access router in a star configuration, then connections between remote nodes will use bandwidth twice on the access link to HQ, and this needs to be counted. An example of a business configuration like this is a franchise where internode traffic is either limited in volume or regulated by call control. In this situation, the location of the root node HQ site, and the WAN in Zone 4 is simply a method to connect sites and is not be included in the configuration.

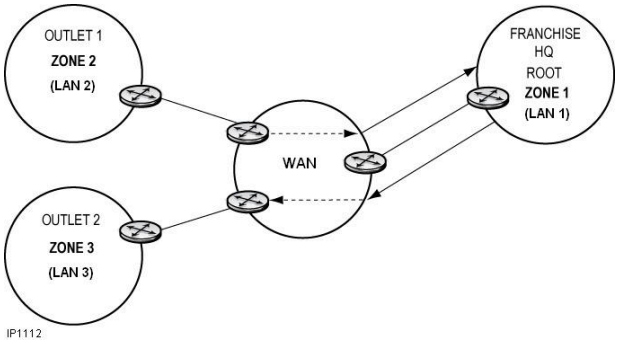


Figure 23: Non-meshed WAN

Table 30: Non-meshed WAN

Zone	Parent
1	Root (1)
2	Root (1)
3	Root (1)

This non-meshed configuration is a little different, as it requires that data be forced to travel back through the central control node. This configuration requires that the “Media Anchor” function be used, and that all outlying nodes be treated as independent units. This is similar to a large deployment, for example, a business with multiple corporate HQ in different countries.

To achieve this forced routing, the topology diagram is a little more complex and is shown below. The tree is divided into three independent trees. Dummy nodes are added as perimeter nodes and delineate the boundary of each tree with the network.

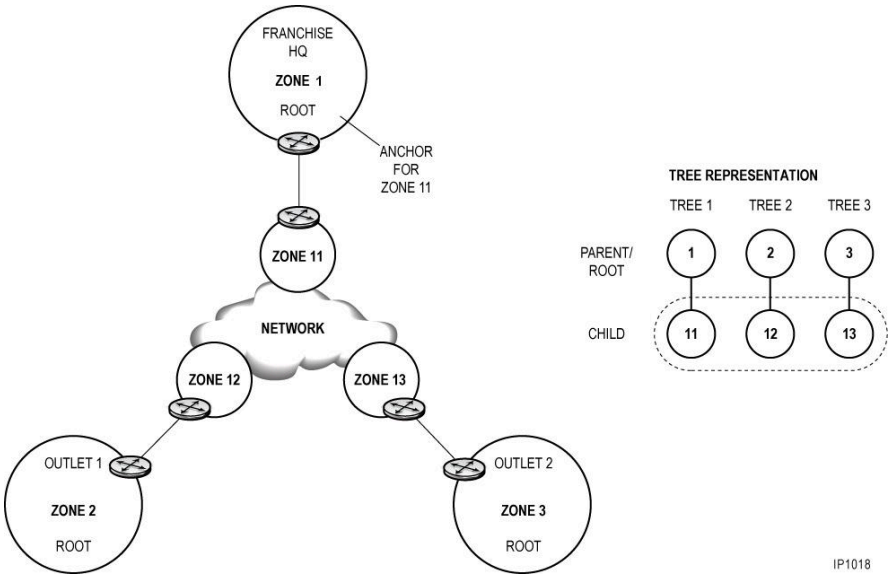


Figure 24: Topology for Non-meshed Configuration

The fundamental point with this configuration is to force all internode bandwidth monitoring back through zone 11 and then back through Zone 1. The effect of the call traffic between Zone 2 and Zone 3 going in and out of the link to Zone 1 is simulated by defining Zone 1 to be the “Media Anchor” zone for Zone 11. In this way, any traffic that flows between Zones 12 and 13 must go through Zone 11 and up and down to Zone 1. The bandwidth monitors A, B, and C will be located in Zones 1, 2, and 3 respectively. Thus the bandwidth monitor in Zone 1 will monitor both incoming and outgoing WAN traffic, as required.

The configuration table will look similar to the following table.

Table 31: Non-meshed Configuration

Zone	Parent	Perimeter	Anchor	Manager	Bandwidth
1	none	No	Yes	-	-

Zone	Parent	Perimeter	Anchor	Manager	Bandwidth
2	none	No	-	-	-
3	none	No	-	-	-
11	1	Yes	-	Unit A in Zone 1	1024 kbps
12	2	Yes	-	Unit B in Zone 2	256 kbps
13	3	Yes	-	Unit C in Zone 3	256 kbps

Deployment boundaries

There are limitations that apply to the current configuration of nodes and paths within the Call Admission Control tree. These are listed below.

- Maximum 6 paths per pipe
- Maximum 6 levels on the configuration tree. A “perimeter node” is considered an end point.
- Maximum 999 zones within a configuration tree

6 paths per pipe

A common pipe between zones can carry multiple connections. One example is IP Trunks between nodes and connections to remote terminals hosted from a remote controller. Each of these would be considered a single path, and so this example has two paths in a common pipe.

6 levels on the tree

Typically, this would allow up to 6 levels of branching from the root node, including the root node. A “perimeter node” is a termination point for the tree. This makes it possible to break a complex configuration into smaller, localized trees and connect these through the overall “perimeter nodes.”

Using the examples above

- the meshed network is a single network with 2 levels

- the non-meshed appears to have 4 levels, but is actually 3 networks, each with 2 levels connected by a common set of perimeter nodes

999 zones within a Configuration Tree

This limits the number of zones that can be configured in a single configuration tree. A perimeter node terminates the zone count. This allows configuration of more complex networks with more zones.

Redundant WAN links and load sharing

The usable bandwidth to be counted on such links (by number of calls using the link) must be considered and may be set according to business requirements. A standby link may provide the same, or reduced, bandwidth as compared to the main link that has failed. In this case, the usable bandwidth is likely to drop when the backup link is activated. Each individual business must consider if this is likely to cause problems and either set the limits to match, or accept that, under failure conditions, some call issues may occur.

A load sharing link is similar to the standby link described above, since the overall bandwidth is again likely to be reduced. Again, the business needs to determine what level of bandwidth is acceptable.

Mitel recommends that you determine the minimum available bandwidth during the failure condition, and use this as the normal limit. This will ensure that a failed WAN link has minimal impact on the voice quality.

Routers that can deal with load sharing and hot standby links include protocols such as Virtual Router Redundancy Protocol (VRRP), Global Load Balancing Protocol (GLBP)and/or Hot Standby Router Protocol (HSRP)at a default gateway level.

Additional information

For more details and for programming information refer to the Mitel System Administration Tool Help for MiVoice Business.

Inter zone bandwidth settings

As well as defining the zones and links between locations, the available bandwidth also needs to be defined. Generally the available bandwidth on these links is also determined by the WAN link protocol. This could be a dedicated link running cPPP, or may be a more general purpose connection such as MPLS, or xDSL. Although the payload (IP) is common to these WAN protocols, the bandwidth on the physical wire link may not be. The MiVoice Business system considers the throughput, or payload bandwidth, with some minor overhead and is defined in the table below.

Table 32: CODEC Throughput

CODEC type	IP Payload + %overhead
G.711	32
G.722.1 (32k)	56
G.729	88

Therefore, define the link bandwidth based on the IP throughput.An alternative method is to determine the physical wire bandwidth and define the number of voice streams, or “channels”, that are required or achievable across the link, using the physical wire bandwidth per connection. Once the number of “channels” is defined, multiply this by the numbers defined in the table above to define the Inter-zone bandwidth limit. For example, suppose a link has a physical bandwidth of 200kbits/s and running DSL. The protocol is PPPoEoATM and on such a link, a G.729 call uses ~64kbits/s. With this link it should be possible to achieve 3 voice streams, albeit with high utilization (200/(3x64)). Therefore, a bandwidth value of 96 should be defined for the link or maybe 64 in order to maintain usage below 80%. See the above table for more details of wire bandwidth, codec type, frame rate and WAN protocols.

11.2 CODEC selection

The CODEC to be used for a connection depends on a number of configurable parameters including:

- Which Zone the network elements and devices are in
- Bandwidth Management - Call Admission Control Thresholds
- Network Zones - Intra-zone compression - Yes/No
- Network Zone Topology - Bandwidth Limits
- ARS Routes - Compression On/Off/Auto. Compression 'On' may override zone settings (Auto setting is recommended)

The endpoint CODEC to use is also influenced by:

Can the end device support this CODEC? (Not all phones will support G.722.1, and some earlier phone models may not support G.729. See phone details)

- Can the CODEC frame rate fit with the packet rate specified

- The MiVoice Business/3300ICP system can negotiate different CODEC types, but can only terminate calls in G.711 or G.729, e.g. when used as a PSTN or TDM gateway. The same applies to services for conference, MOH, Paging, Voice Mail, RADs, etc. that originate or terminate on a 3300 ICP
- Is the end device SIP based, which can independently negotiate CODEC settings

Note that somethe 69XX phones support G.722.1 andSIP phones and SIP gateways may support G.722.1 (32kbits/s).

Low bit-rate CODECs send data as bursts of data, or Frames. The packet rate must be an exact multiple of the frame rate in order to achieve a connection. The G.711 CODEC does not use a Frame mechanism and is not part of this consideration.

Table 33: Codec Frame Size and Packet Rates

Codec	Frame Size	Acceptable Packet Rates
G.729	10 ms	10, 20, 30, 40, 50, 60, 70, 80, 90, 100 ms
G.722.1	20 ms	20, 40, 60, 80, 100 ms

An ability to modify the CODEC selection is also provided within the MiVoice Business node. This allows supported codec types to be added or removed from the node negotiation. For example, the Administrator may wish to remove the G.729 CODEC so that only the G.722.1 and G.711 CODECs can be negotiated. This functionality does not allow the G.711 codec to be removed as this is the base functionality required by all IP devices, including other 3rd party products including SIP gateways and SIP phones. The form called ‘Codec Settings’ allows the Administrator to specify which CODECS would be offered for negotiation by devices at each end of a call within the MiVoice Business network.

Assuming that the end devices are capable of supporting the available CODECs, then the following table will highlight the operation for calls within a common zone as well as calls between zones.

Table 34: Codec Zone Interconnects

Zone Interconnect	IntraZone Compression	InterZone Compression	Route Compression	To Zone 1	To Zone 2
Zone 1	No*	Yes** (Defined Setting)	Off	G.722.1 G.711	G.729 G.722.1 G.711
			On	G.729 G.722.1 G.711	G.729 G.722.1 G.711
			Auto*	G.722.1 G.711	G.729 G.722.1 G.711
	Yes		Off	G.729 G.722.1 G.711	G.729 G.722.1 G.711
			On	G.729 G.722.1 G.711	G.729 G.722.1 G.711
			Auto*	G.729 G.722.1 G.711	G.729 G.722.1 G.711

Zone Interconnect	IntraZone Compression	InterZone Compression	Route Compression	To Zone 1	To Zone 2
Zone 2	No*	Yes* (Defined Setting)	Off	G.729 G.722.1 G.711	G.722.1 G.711
			On	G.729 G.722.1 G.711	G.729 G.722.1 G.711
			Auto*	G.729 G.722.1 G.711	G.722.1 G.711
	Yes		Off	G.729 G.722.1 G.711	G.729 G.722.1 G.711
			On	G.729 G.722.1 G.711	G.729 G.722.1 G.711
			Auto*	G.729 G.722.1 G.711	G.729 G.722.1 G.711

* Recommended setting.

** Predefined setting and not user configurable.

The Following figure illustrates how the preceding table and rules can be applied in a typical scenario. The following assumptions are made within the following *Codec Zone Interconnect Example* figure:

- The SIP Gateway(either MiVBG or SBC)is capable of G.722.1 and G.711
- The SIP Gateway is associated with Zone1
- The MiVoice Business controllers are capable of G.711 and G.729
- The default settings for inter and intrazone codec selection are in operation

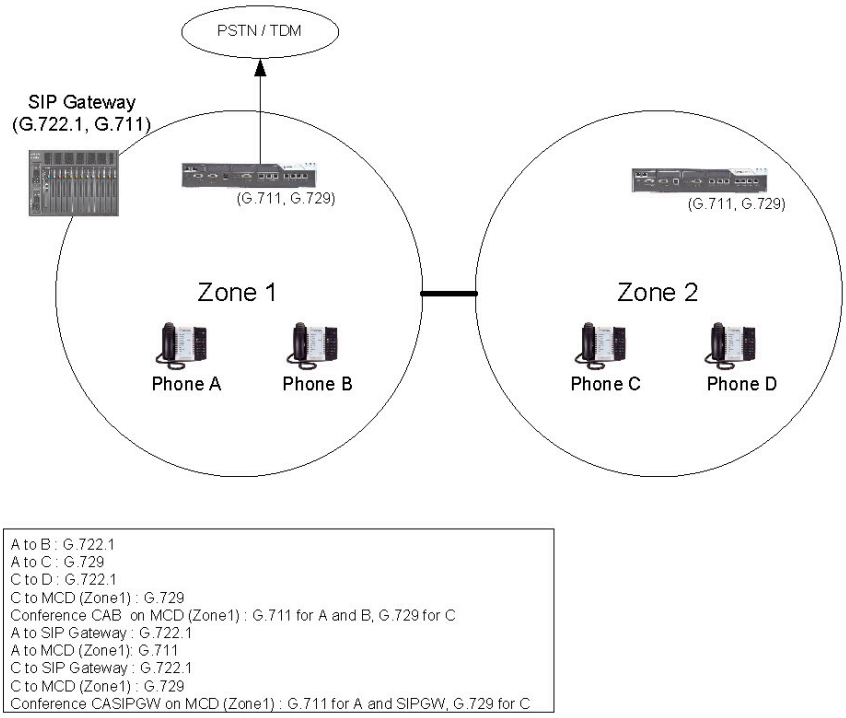


Figure 25: Codec Zone Interconnect Example

11.3 Operation through MiVoice Border Gateway and SRC

There is no transcoding support for the wideband G.722.1 CODEC via the MiVoice Border Gateway or SRC. As such, the MiVoice Border Gateway and SRC will default to only negotiate connections with G.711 and G.729 CODEC types.

The SRC will ensure that the connected phones only negotiate to G.711 or G.729 and will provide G.729 to G.711 transcoding, if needed, when compression licenses are installed. Any Call Recording Equipment (CRE) attached to the SRC will continue to be supported with G.711 and G.729 CODEC types.

The MiVoice Border Gateway will ensure that the connected phones only negotiate to G.711 or G.729 and will provide G.729 to G.711 transcoding, if needed, when compression licenses are installed.

11.4 Compression Guidelines

Generally when compression is mentioned, it is usually mentioned with a CODEC, for example, “G.729 Compression.” This just refers to the ability to reduce the amount of data that needs to be carried across the IP infrastructure.

In the case of CODEC compression, this works by reducing the amount of data that needs to be carried in the voice payload. However, the IP header information still needs to be added, so although there is a reduction in required bandwidth, the gain is not always as much as might be expected.

Other forms of data compression also exist in the network. It is possible to do a level of header compression on certain fixed links, e.g. RFC 1993. Other data compression techniques include Compressed RTP (RFC 2508 or Enhanced CRTP-RFC 3545), or they may only compress up to the IP layer. Data and header compression is typically used for lower speed links, less than 1.5 Mbps, where every last bit per second counts. Since the link is point-to-point, the header information is simply repeat information and is redundant. In this case, much of the information can be established before the data is sent, and the far end router re-applies this data before it is sent onwards. Although this can work well for data, it adds delay to the transmission as well as using valuable router resources.

11.5 3300 ICP compression guidelines

Compression affects a number of call connection types. These include:

- IP phone to IP phone
- IP phone to TDM and vice versa
- IP phone at a remote site back to TDM or IP
- IP connection across an IP trunk route

Compression affects other aspects of the 3300 ICP as well. These include IP phones,MiVB controllers,3300 ICP devices, IP applications, IP networking routes and trunk routes, and licenses.

IP Phones and compression

Some IP phones include compression capability and licenses. If required, these devices can stream directly with compressed voice withoutMiVoice Businessintervention.

Other IP phones, however, do not support compression. Calls to and from these devices are restricted to G.711 only. The following IP phone have this restriction:

- 5201, 5205, and 5207

MiVoice Businesscontrollers and compression

All MiVoice Business controllers require compression licenses if any of the internal resources are used with compression.A single controller has the following limitations:

- If the 3300 controller has one compression DSP module, the maximum number of compression sessions is 32. If the controller has two compression DSP modules, the maximum number of compression sessions is 64.
- If the 3300 controller has DSP-II fitted, this is capable of up to 64 compression sessions per module.
- The EX controller can support up to 28 compression sessions on the EX DSP module. Each EX PRI module can support compression on its digital link without an additional DSP card.
- All server variants require compression channels within the media server to support internal devices. The number of channels available is determined by the processor speed and number of cores. Refer to the Configuration Tables for limits on different platform sizes.
- No more than 999 compression zones are possible from a single MiVoice Business/ ICP system.
- E2T compression is used primarily to deal with TDM devices such as ONS phones or PSTN connections.
- The CX-II, MXe-III and EXcan only terminate calls with G.711 or with G.729 compression CODECs. Termination of G.722.1 connections is not provided, although the 3300ICP will handle through negation of the G.722.1 connection between end devices.

InternalMiVoice Business devices and compression

Conference

The conference feature is based on G.711 format, and is considered a TDM device.A compression resourceis needed in theMiVoice Businessto communicate with each IP phone that normally uses compression to a TDM device.

Voice Mail

Internal Voice Mail stores data in G.711 format, but compression can be used to and from this device. An IP phone that uses compression to a TDM device uses compressionresources and licensing on the MiVoice Businessto the voice mail.

Music On Hold

Music-on-Hold (MOH) can be sent with compression (at the expense of audio quality). Each MOH session to an IP destination uses a compressionresource andlicense.

IP applications and compression

Most Mitel IP-based applications support compression.

To get the best voice quality performance from devices such as voice auto-attendant and IP voice mail, allocate them in a common compression zone with other devices not running compression, e.g. default zone 1.

Consider the effect of allocating them to a compression zone where an application is used as a central resource over a WAN link. Bandwidth restrictions may still require compression to be enabled.

11.6 IP networking routes and compression

Compression can be enabled in IP networking routes betweenMiVoice Businessunits if the end devices are capable of this operation. For more details see Compression Zones.

Compression zones

This section briefly describes compression zones, IP trunk routes, and network issues to consider when planning the location of different devices.

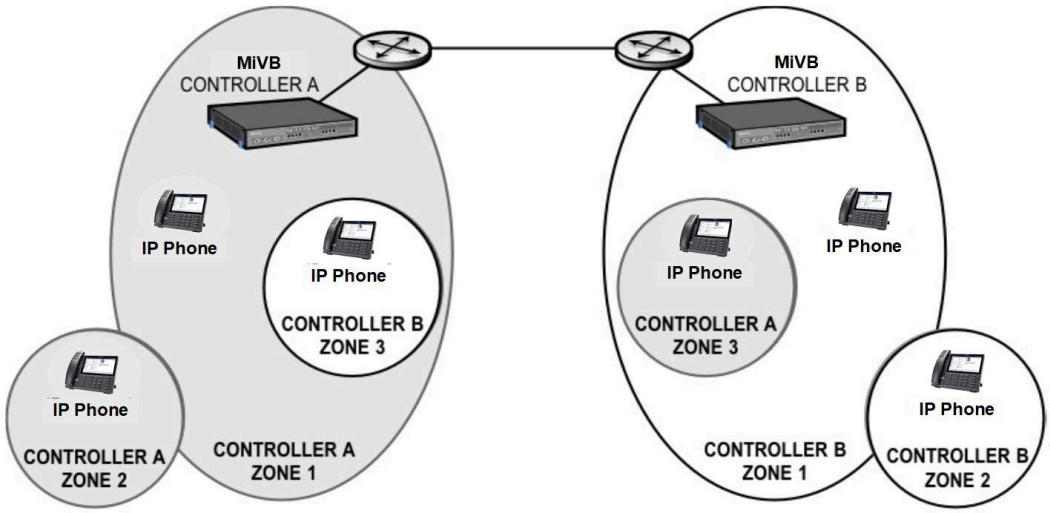


Figure 26: IP Networking Compression Zones Example

Although the network shown in the figure above is not a real network, it highlights some of the areas to consider in allocating bandwidth in different parts of the network:

- Calls within Zone 1 of both controllers are not compressed.

- Calls between controller A and controller B are sent over an IP networking route (IP trunk) and are compressed but can be set up as non-compressed.
- All IP networking connections are considered as originating from Zone 1. If the IP network connection is not compressed, but a call originates in a zone that normally uses compression and it goes back to Zone 1, the call is completed with compression.
- Although the two units are logically separated, they share a common physical infrastructure. This is similar to network VLAN operation, but can lead to some unusual operations, similar to VLAN, where local devices talk through a router. In effect, the controllers can be considered as voice routers.
- The IP phone in controller A, Zone 3 registers with controller A over the WAN link. Bandwidth used by this device to talk to other devices on controller A is not counted against the IP networking limits. Bandwidth for this remote phone should be considered in addition to the IP networking requirements, since both IP network connections and remote connections share a common infrastructure.
- If the phone in controller A, Zone 3 wants to communicate with the phone in controller B Zone 1, it consumes an IP trunk session or channel, but no actual WAN bandwidth since the two phones stream directly within the LAN. This call could also be blocked if there are insufficient IP trunk sessions or channels allocated.
- A controller can have a maximum of 999 compression zones.

More details on zones and setup can be found in the *Technician's Handbook* and the installation documentation.

11.7 IP trunk routes and compression

The IP trunk route is a virtual path from one 3300 ICP to another 3300 ICP. One of the parameters assigned to this route is compression. Assuming that the end devices are capable of compression, compression is enabled on the route, and there are sufficient available channels, or sessions, then the end devices stream using compression. Otherwise the call is blocked, rerouted, or streamed with G.711 (uncompressed).

Maintaining_Availability_of_Connections_org/ Mitel_MiVoice_Business_Engineering_Guidelines_Release_8_0_11. for more details on bandwidth requirements for different LAN and WAN links with and without compression.

11.8 IP networking and compression licenses

Compression and available bandwidth affect voice quality. Compression sessions and IP networking require licenses. Setting different compression zones and assigning different IP phones to the different zones determines when to use compression licenses. The IP networking license determines whether calls can be routed between units over its IP infrastructure, and how many of the sessions are allowed over a particular connection

between different controllers. Compression and IP networking work together, but can also be used independently.

From a voice quality view, if the number of calls requiring compression exceeds the number of licenses, a call does not fail, but it is not compressed. It will use more bandwidth than expected. If IP trunks are used, the number of concurrent sessions can also be defined; see the section IP networking limit working example.

11.9 Compression and licenses

Some guidelines for compression licenses and connections in IP:

- An IP phone-to-IP phone connection does not use a compression license in the 3300 ICP when the call is connected by an IP trunk over a WAN.
- An IP phone (node A) to TDM phone (node B) call uses a compression license on node B only when the call is connected by an IP trunk over a WAN and the call is compressed across the IP trunk.
- A TDM phone (node A) to TDM phone (node B) call uses an E2T compression license on both nodes A and B when the call is connected by an IP trunk over a WAN and the call is compressed across the IP trunk.
- Conference calls use one compression license for each IP connection in the conference that would normally require a compression license when connected to a TDM device.
- Compression can be used with calls to voice mail. Each of these calls consumes a compression license if the call would normally use compression when connected to a TDM device.
- Music-on-Hold (MOH) that is passed to a device that normally uses compression consumes a compression license. If MOH is passed to multiple devices, then multiple licenses are required, matching the number of devices.

11.10 Calculating and Measuring Bandwidth

Note:

1. To calculate and measure bandwidth, use the Mitel calculator rather than a third-party tool. The Mitel calculator uses 802.1p/Q (8100) frames, which ensure the highest degree of accuracy. Many third-party tools use standard Ethernet (0800) frames, which are less accurate and do not account for VLANs.
2. PC-based applications for monitoring IP network traffic often do not indicate the actual bandwidth being used. These applications usually do not include IP packet overhead information, and as a result using these applications to try and measure bandwidth will provide misleading results.

Bandwidth can be described in a number of ways:

- Payload bandwidth, voice: sufficient bandwidth to transfer the usable information.
- IP bandwidth: bandwidth to transfer the data between the two end devices. Note that this doesn't include the transport protocol, which may change between devices and network.
- Wire bandwidth: This includes all of the bits and timing gaps that are transmitted onto the media. This includes the payload, the IP address information and the transportation and synchronization information.

It is important to note which bandwidth is being described when comparing information. For instance, a G.711 Ethernet connection with 20 ms frames will have the following values:

- Payload bandwidth: 64 kbps
- IP bandwidth: 80 kbps
- Wire bandwidth: 96.8 kbps

Note:

Some network analyzers will not monitor the full Ethernet frame, excluding checksums and synchronization data, and therefore they give a bandwidth somewhere between wire and IP bandwidth. For the example shown, this would typically be 87.2 kbps, including VLAN. This is the standard and assuming the same sampling rates and CODEC does not vary between vendors.

What is the media bandwidth?

Depending upon how this is measured, this could be simply the payload bandwidth, which is similar to TDM, or it could be the bandwidth of the packet carried across the network. During a conversation, this bandwidth is consumed at a constant rate. It may change if the CODEC includes Voice Activity Detection (VAD) and reduce consumption of bandwidth, but it won't exceed a particular level even when network bandwidth is available. This is in contrast to general TCP data traffic, where bandwidth is consumed to the maximum current capacity of the link. Mitel doesn't support VAD or silence suppression as both affect voice quality negatively.

What is the signaling bandwidth?

The level of signaling is dependent upon call traffic. If there are no phone calls being set up, then signaling is low (less than 1% of expected media bandwidth). However, setting up a call uses bandwidth. In practice, adding 10% to the voice bandwidth for signaling has been found to be a good rule of thumb that provides sufficient margin.

The following table shows typical wire data rates for different protocols and LAN/WAN interfaces.

As the table shows, the physical wire bandwidth required by an IP phone for Ethernet is usually

- G.711 (about 100 kbps at nominal 20ms packet rate)
- G.729a (about 40 kbps at nominal 20ms packet rate)

Under most conditions the default packet rate used by the end devices is 20ms. However when connecting to other third party products packet rate values may vary from 10ms to 40ms in 10ms steps. Typical packet rates and usage include:

- 10ms (for reduced latency at PSTN gateway)
- 20ms (default IP rate, provides good delay and bandwidth usage efficiency)
- 30ms (reduced packet rate, for example wireless base stations)
- 40ms (limited bandwidth connections where reduced header size and larger packet increase efficiency)

Both LAN (Ethernet) and WAN bandwidth usage is shown in the following tables. Often the bandwidth quoted for Ethernet differs between measurement equipment and in values quoted by different vendors but if everyone is using the same CODECs and sampling rate then they should be the same. The values highlighted in the following tables include all the bits on the wire as would be seen by an oscilloscope. This includes bits used to delimit the packets and also the inter-packet gap. Although these bits and time do not carry user information, they do consume bandwidth, which is unusable by any other connected device.

Table 35: Ethernet/LAN IP and On-the-wire Bandwidth

	Codec:	G. 711 / G.722		G.729		G.722.1	
	Payload: 64 kbits/s		8 kbits/s		32 kbits/s		-
LinkTyp	Packet Rate (ms)	IP (kbits/s)	Wire (kbits/s)	IP (kbits/s)	Wire (kbits/s)	IP (kbits/s)	Wire (kbits/s)
Ethernet	10ms	96.0	129.6	40.0	73.6	64.0	97.6
	20ms	80.0	96.8	24.0	40.8	48.0	64.8
	30ms	74.7	85.9	18.7	29.9	42.7	53.9
	40ms	72.0	80.4	16.0	24.4	40.0	48.4

Table 36: Other Protocols: On-the-wire Bandwidth

Payload:	Codec:		G. 711 / G.722	G.729	G.722.1
	-	-	64kbits/	8kbit/s	32kbit/s
Link Type	Packet Rate (ms)		Wire (kbits/s)	Wire (kbits/s)	Wire (kbits/s)
PPP 20ms 30ms 40ms	10ms		104.0	48.0	72.0
	-	-	84.0	28.0	52.0
	-	-	77.3	21.3	45.3

Payload:	Codec:		G. 711 / G.722	G.729	G.722.1
	-	-	64kbits/	8kbit/s	32kbit/s
Link Type	**Packet Rate (ms)**		**Wire (kbits/s)**	**Wire (kbits/s)**	**Wire (kbits/s)**
	-	-	74.0	18.0	42.0
cPPP 20ms 30ms 40ms	10ms		72.0	48.0	40.0
	-	-	68.0	28.0	36.0
	-	-	66.7	21.3	34.7
	-	-	66.0	10.0	34.0
VoATM (AAL5, IP) 20ms 30ms 40ms	10ms		127.2	84.8	84.8
	-	-	106.0	42.4	63.6
	-	-	98.9	28.3	56.5
	-	-	84.8	21.2	53.0
PPPoEoA 20ms 30ms 40ms	10ms		169.6	84.8	127.2
	-	-	106.0	63.6	84.8
	-	-	98.9	42.4	70.7
	-	-	95.4	31.8	53.0

Before determining the bandwidth for particular links, it is important to consider the traffic flow and where devices are located relative to their controllers. The use of compression zones and IP networking also have a bearing on traffic flow in parts of the network.

See Maintaining Availability of Connections on page 145 for details on bandwidth requirements for different LAN and WAN links with and without compression.

Other users of Bandwidth

SDS is used to share system information around the network. The SDS protocol runs on TCP and the bandwidth consumed is determined dynamically by the TCP protocol.

SDS information contains many components and has both sustained and peak data transfer rates. SDS has been proven to work with link speeds as low as 100kbits/s. For minimal impact a minimum bandwidth of 300kbits/s is recommended. To handle the occasional peak burst a connection of 100Mbits/s is ideal. Where this higher bandwidth is not available, e.g. WAN link, the TCP protocol will adjust the data rate to match the available bandwidth. In this case, some data may transfer at a slower rate.

Note that SDS only shares data between systems when there are configuration changes to the system. These can occur manually, or through tool automation, but generally require some management activity to start the process. As such, the suggested bandwidths are not consumed on a continual basis, but only as needed; i.e. when SDS is activated to share information. The suggested rates are only recommended rates to maintain expected responsiveness, rather than as a value that needs to be continually reserved.

Bandwidthavailability

The advertised rate for a particular link is the speed at which the data travels; it is not necessarily the available data rate. In practice, a percentage of this bandwidth is lost due to communications between end devices because the data is asynchronous and requires certain guard bands. In a synchronous telecom link, these issues are resolved through mechanisms such as framing data into fixed timeslots. The following table contains some simple guidelines for LAN and WAN links.

Table 37: LAN and WAN Link Guidelines

Data connection type	Percentage of bandwidth available	Example
LAN – 10BaseT Full Duplex	80%	10 Mbps => 8 Mbps available

Data connection type	Percentage of bandwidth available	Example
LAN – 100BaseT Full Duplex	80%	100 Mbps => 80 Mbps available
WAN – 1.5 Mbps Frame Relay without QoS mechanism in router	40%	1.5 Mbps => 600 kbps available
WAN – 1.5 Mbps Frame Relay with QoS mechanism in Router	70%	1.5 Mbps => 1.05 Mbps available

LAN bandwidth

The following table contains some simple guidelines for LAN connections (assuming that all the available bandwidth is used for voice traffic only).

Table 38: LAN Connections Guidelines (based on a 20 ms packet rate)

Cable capacity	Bandwidth	Phone usage at G.711	Voice channels G.711	Voice channels G.729a (x 2.5)
10BaseT	80%	1%	80	200
100BaseT	80%	0.1%	800	2000

“ The LAN connections guidelines table” reflects the maximum usable bandwidth based on the physical connection. Other factors in the network must also be considered, including:

- the percentage of data traffic shared with the voice on a common connection.
- the percentage of broadcast traffic; a “flatter” LAN will result in more traffic.
- the percentage of data traffic allowed in the egress queues even under congestion.
- whether the uplink from a switch is blocking in terms of possible data input, e.g. a 1 Gbps uplink may not be enough for a 24 port switch running 100 Mbps on each input link.

- whether the switch backplane can handle the data throughput in terms of available bandwidth and packet per second rate.

The LAN connection guidelines table also shows the maximum capability of a LAN link assuming that the link is used purely for voice traffic. If the link is shared with other devices such as PCs, then some priority mechanism is required to ensure that the voice gets the available bandwidth when needed. Also, in a busy network with multiple broadcasts, the available bandwidth is reduced by this percentage. For example, in a network with 10% broadcast traffic (at 10 Mbps), the 40% available bandwidth is reduced to 30% for a half duplex link, and the number of voice channels is reduced accordingly.

Table 39: Voice Channels Supported by a 1.5 Mbps Link(based on a 20 ms packet rate)

Cable capacity	Bandwidth %	Voice channels G.711	Voice channels G.729a (x 2.5)	Voice channels G.722.1
1.5 Mbps without QoS mechanism	40%	6	15	9

Maintaining Availability of Connections 12

This chapter contains the following sections:

Introduction

The quality of service for signaling measures how long a user needs to wait before a service becomes available, or whether the user becomes blocked from using a function. For example, delays in receiving dial tone, or blocking that occurs if there are insufficient PSTN trunks degrade the quality of service.

Quality of service can be ensured by proper provisioning. The sections below provide more information on traffic guidelines and bandwidth calculations, and IP Networking and compression.

12.1 System Capabilities

As the system grows and traffic increases, it has to deal with more tasks, resulting in slower feature interaction. ICP systems are engineered to ensure that with different combinations of devices, services are still maintained within normal working parameters. The exact details are not captured here, but are specific to particular releases, since changes in software or hardware have a bearing on the results.

Use of the System Engineering Tool is recommended to ensure that the expected configuration is within the capabilities of the selected 3300ICP controller, or network of 3300ICPs.

12.2 Traffic and Bandwidth Calculations

The level of traffic that the units need to handle has the largest effect on performance and availability. A number of areas are affected by traffic:

- Trunks to PSTN
- E2T (Gateway) channels
- DSP channels
- LAN blocking between devices
- WAN blocking between endpoints.

See Provisioning for Traffic for the traffic guidelines used to calculate system performance.

You can calculate the amount of TDM traffic that needs to be presented in terms of CCS and match this to a number of trunk channels. With IP, fixed channels do not exist, so this calculation is more complicated.

To calculate the amount of traffic that can be handled over a LAN or WAN link, apply the bandwidth calculations in the previous section on Bandwidth, Codecs and Compression on page 118. Use these to work out the number of voice channels and assign a particular CCS rating.

WAN traffic working example

In this example, assume the following configuration:

- 50 IP phones at the corporate centre.
- 10 IP phones over a T1 link at a remote site.
- Trunk traffic is 65% of all traffic (approximate split 1/3 each for incoming, outgoing and intercom).
- Traffic between remotely located IP phones stays local to the remote site (it does not traverse the WAN link).

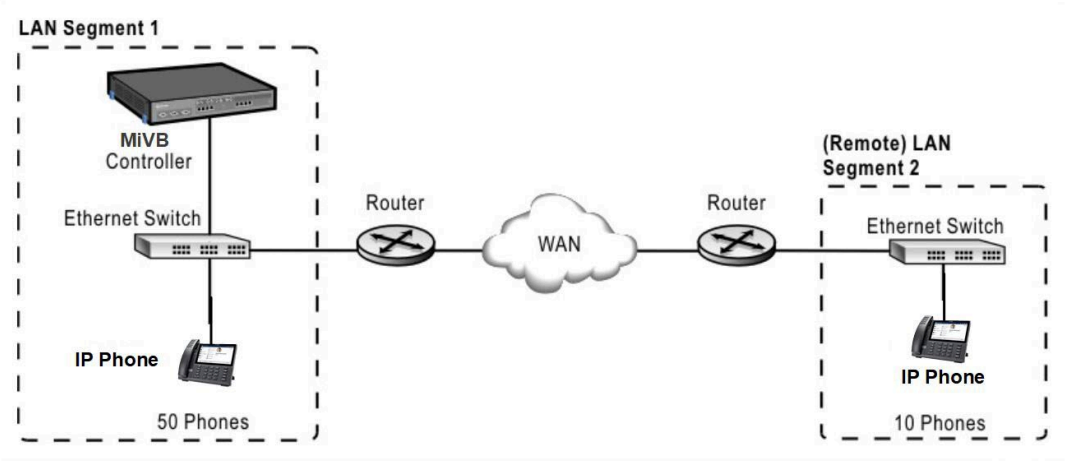


Figure 27: WAN traffic example

Table 40: CCS Calculation Example

Calculation	Formula	Result
Remote phones		10

Calculation	Formula	Result
Total CCS at the remote site	Remote phones x 6 CCS	60 CCS
Percentage of trunk traffic	Total CCS x 65%	39 CCS
Percentage of intercom traffic	Total CCS x (100 – trunk traffic)%	21 CCS
Local intercom traffic	Intercom traffic x Ratio of local phones / total phones (21x10/60)	3.5 CCS
Total traffic over the WAN	Total traffic – local traffic	56.5 CCS

Therefore

- The total traffic handled is 60 CCS.
- 3.5 CCS is local traffic.
- WAN traffic is 60 -3.5 = 56.5 CCS

WAN link could handle six G.711 voice channels. From ErlangB tables with P.001 blocking, such a link can handle 41.1 CCS. There is a mismatch between presented traffic and carrying capacity.

Solutions that come from this example can then be covered by:

- Compression (G.729a) to the remote phones can be used to increase the voice channel capability. However, it also reduces voice quality, which may not be acceptable.
- The WAN link bandwidth can be increased.
- The blocking ratio can be changed to P.01, and such a link would handle 68.8 CCS.
- The number of remote phones or the overall number of phones can be reduced.
- Ensure that QoS/Priority mechanisms are in place and active.

These are all potential solutions and each has to be investigated to understand the nature of the installation. Doing this calculation before equipment is bought and installed ensures that such issues are highlighted.

12.3 IP networking and Use of Compression

IP networking allows the construction of larger systems, and the combining of systems in different geographic locations into a single system.

If LAN/WAN connections exist between nodes, this medium can be used to pass traffic. A limit on the number of conversations for this connection is programmed at installation. If the limit is exceeded, an alternative path is tried through ARS, either through a different node connected by IP trunks, or through the PSTN TDM network.

The value of the IP trunk restriction is set for a particular connection. This setting relies very much on traffic and also the bandwidth available.

Since the bandwidth is derived from the number of conversations, it is important to understand which CODEC is used across the link (G.729a, G.711,G.722.1 or some combination).

Note:

Music On Hold and messages to and from Voice Mail can be handled with G.729a,if licensed and resourced to do so

Also, the level of networking between nodes and whether it includes PSTN trunk traffic or only internal intercom traffic needs to be understood.

As a general guideline, consider that a single node might have a high networking traffic ratio of 15%. For a particular node with a number of devices, the amount of traffic to and from this node remains constant. What differs is the level of traffic destined for another particular node. For example, 15% of traffic might be destined for the second node in a two-node system, but 7.5% is destined for each of the other two nodes in a three-node system. Obviously, in the second scenario, less bandwidth is needed to and from a particular node, but the total per node remains about the same.

A number of factors determine compression operation:

- Are there sufficient resources (i.e. are there enough DSP channels available)?
- Have sufficient compression licenses been acquired?
- Can the end device handle compression? Some older phones can handle only G.711.
- See the application information to determine whether compression is handled.
- Is compression enabled.
- Are the IP trunks (IP networking routes) configured with compression?

IP networking limit working example

Consider the following example:

- Two equal-sized systems.
- 250 IP devices/phones.
- Calls from TDM, or to TDM devices including trunks, use G.711 CODEC.
- Calls between IP devices use the G.729a CODEC.
- Traffic is typically 35% (100-65) internal, the remainder to and from PSTN trunks.
- Calls internally are typically 50% outgoing and 50% incoming.
- Traffic is rated at 6 CCS per device.
- Traffic between nodes is 15%.

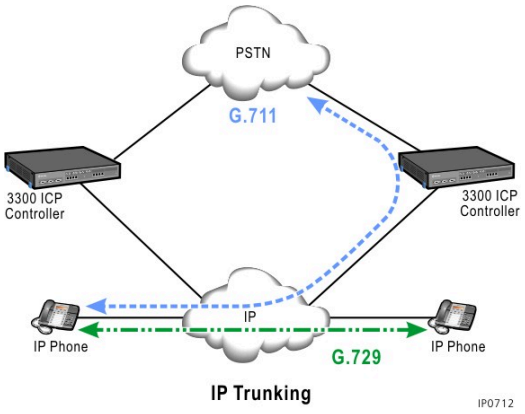


Figure 28: IP trunk limit example

Table 41: IP Networking Limit Calculations

Calculation	Formula	Result
Traffic from IP sets	Number of sets (250) x 6 CCS	1500 CCS
Percentage networked	Total traffic x 15%	225 CCS
Percentage traffic intercom	Networked traffic x 35%	79 CCS
Percentage traffic trunk to PSTN	Networked traffic – intercom traffic	146 CCS

Calculation	Formula	Result
Total Number of IP trunk channels needed	ErlangB on total IP trunk traffic (225 CCS)	13 channels (P.01)
Number of channels needed for PSTN trunks (G.711)	ErlangB on PSTN trunk traffic (146 CCS)	0 channels (see note) (P.01)
Number of channels needed for intercom/ internal traffic (G.729a)	ErlangB on Intercom traffic (79 CCS)	7 channels (see note) (P.01)
Bandwidth needed (use worst case)	Number of G.711 channels (10) x 100k + [Total number of channels (13) – PSTN trunk channels(10)] x 40k	1120 kbps
WAN bandwidth required	Assume with QoS so / 70%	1600 kbps
Number of channels (IP trunk) for IP networking	Total number of channels	13 Channels

Note:

- Seven channels are needed for internal traffic and ten are needed for external traffic, but together the total is only 13. The reason is that a number of channels have shared use: in this case, it is 4 (10+7-13). The higher G.711 rate is used to ensure adequate bandwidth at all times.
- This data rate is close to a T1 rate. Options are to increase the available link rate by upgrading to an E1 link or to multiple T1 links, or to accept a lower quantity of IP trunk calls (a slight reduction in inter-node traffic).
- The bandwidth calculations should also include signaling and link utilization factors.
- With IP networking, it is possible to restrict the number of conversations on a connection, so although calculations suggest 13 channels, the link settings could be set to only 10 channels to reduce bandwidth usage. ARS will then come into play when this number is exceeded, resulting in the call being routed elsewhere, for example TDM, if possible, or presentation of re-order/busy tone to the user.

Network Configuration Specifics 13

This chapter contains the following sections:

Introduction

The chapter covered a number of general guidelines that may be applicable depending on the network to be used. This chapter highlights a number of specific network guidelines.

13.1 Start-Up Sequence and DHCP

The previous chapter “MAINTAINING AVAILABILITY OF CONNECTIONS” deals with network conditions and call traffic. However, before any of this can occur, the system first needs to be installed and the phones need to obtain their operating software.

LAN Policy” consists of a set of three parameters that are used to control segregation and priority of voice traffic across the network. These parameters are

- VLAN ID (IEEE 802.1Q)
- Layer 2 priority (IEEE 802.1D/p)
- Diffserv Codepoint (DSCP, Layer 3 priority)

13.1.1 Startup Sequence for the Controller

The controller startup sequence involves bringing up the RTC where call control resides. This also includes the local DHCP and TFTP servers.

In order to correctly program some of the options within DHCP, such as the RTC and TFTP server, it is necessary to pre-assign an IP address to the 3300 ICP. This address is used by the IP networking handler and is entered into the database of other remote ICP units.

The DHCP server in the 3300 ICP controller should be used for local devices on the voice VLAN. This can be disabled, but then an external DHCP server is required to service devices on the voice VLAN.

Where multiple DHCP servers are used on a LAN, for example in a redundant or load balancing situation, the information in the different servers must be consistent for all the phones to start up correctly.

MiVoice Business EX, ISS, and Virtual

The MiVoice Business EX, do not support an integral DHCP server. The 3300 internal DHCP server can be used if a 3300 ICP is included in the installation. Otherwise a third party DHCP server must be provided.

13.1.2 MiVoice Business TFTP Server

The MiVoice Business internal TFTP server is used to provide the IP phones with application software. This section provides information about the interaction that takes place between the IP phones and the TFTP server.

The TFTP server in x86-based controllers (MiVoice Business for ISS) can handle 50 simultaneous sessions. The other controllers can handle 10. This value is not configurable.

The 69xx display sets have a larger software load and take longer to download. An external TFTP server must be configured for all 3300 ICP controllers with more than 200 69xx phones (including EX Controllers) to ensure all devices are in operations withing 2 hours. It is not necessary to add an external TFTP server with MiVoice Business X-86 based servers (virtual or ISS) as these cab download all sets within approximately 1 hour.

If a particular phone can’t get access to the TFTP server, it will try repeatedly for a number of seconds, after which it will re-boot and start again.

Some time-out values of interest are:

- Phones will attempt to access the TFTP server three times before rebooting. Attempts to access the TFTP server will be made at intervals of 15-30 seconds. This interval is random to even out the loading on the TFTP server, and to avoid a situation where multiple sets are attempting to access the TFTP server simultaneously.

- Inter-packet timeout can be up to four seconds. More reliable transmissions will cause the inter-packet time to lessen and the transmission of acknowledgement packets and any retries that might occur will speed up.
- Phones will attempt to complete the TFTP download in 20 minutes.

When a phone is setting up a TFTP session with the 3300 ICP's internal TFTP server or an external TFTP server there is an "auto-negotiation" process that they go through to establish the block size.

The devices will try to establish the block transfer size at 4096 bytes, then they try 2048 bytes, then they try 1024 bytes and finally they try 512 bytes.

Block size is not user configurable on either the 3300 or the phone, however TFTP block size could be user configurable on some 3rd party external TFTP servers.

In situations where phones are accessing an external TFTP server over a very slow connection reduce, if possible, the transmitted block size from 4096 to a smaller number; 512 or 1024. This will increase the number of ack/nack messages, but will ensure that the four second inter-packet timer is less likely to be exceeded, especially when multiple phones share the same restricted link.

For best performance the TFTP server should be connected to the network with a minimum bandwidth of 100Mbits/s. Lower bandwidth will reduce the throughput and result in increased delays to bring the phones into service.

For a WAN link, the minimum bandwidth to ensure timely startup with minimum retries at the phone is 15 kbits/s per phone. Higher bandwidths will result in phones returning to service quicker, and a practical value to consider might be 100kbits/s/phone. Less available bandwidth may result in phones retrying to complete the download and hence take additional time.

Depending on the total number of phones that require access to the common TFTP server and the time to have these in service the following WAN minimum bandwidths per phone are recommended:

Table 42: TFTP Server Recommended Bandwidth

Total number of phones on TFTP server	Recommended Minimum WAN bandwidth per phone
500	20kbits/s
1000	35kbits/s

Total number of phones on TFTP server	Recommended Minimum WAN bandwidth per phone
1500	50kbits/s
2000	70kbits/s
2500	85kbits/s
3000	100kbits/s
3500	120kbits/s
4000	135kbits/s
4500	150kbits/s
5000	170kbits/s

Although lower bandwidths may be used, this may result in a number of phones failing to complete the download in the expected time, resulting in subsequent retries and time to come into service.

13.2 Fax Considerations

This section describes a number of specific items to consider for the 3300 ICP network:

- Fax and modem connections over IP using G.711 Pass Through
- DTMF Signaling over IP Networks
- T.38 FoIP Guidelines
- Bandwidth Management
- T.38 Frequently Asked Questions
- MiVoice Business and 3300 IP Ports on page 147
- Voice Gateway IP Ports
- Interconnection Summary

13.2.1 Fax and modem connections over IP using G.711 Pass Through

The 3300 ICP supports the transmission of Fax over IP (FoIP) via G.711 pass through, and also Fax over IP and SIP via the ITU T.38 recommendation.

G.711 Fax pass through overview

The ICP controllers can transmit Fax information over an IP trunk from one controller to another as G.711 packets. In effect, the data modulated signals are passed as voice across the IP network. For this reason, compression cannot be used on these signals. Fax machines are sensitive to time delays and error rates. Typically, these devices are designed to run over TDM links. A lost IP packet can contain a significant quantity of data. Although the Fax application can recover from some losses, it may not be able to handle large losses such as a burst loss of IP packets.

Within the PSTN, echo cancelers will be disabled if tone detectors within the PSTN detect a FAX or MODEM calling tone (2100 Hz).

The controllers, however, do not currently support this functionality. As a result, if a FAX machine is connected directly to an ONS or LS port on the ICP so that the data can be transported to another ICP via IP trunk forwarding, the ICP will not disable the internal echo canceler. The presence of an echo canceler will impede the ability of the FAX to establish a full duplex connection, resulting in a slower half duplex connection being established.

G.711 Fax pass through performance guidelines

Due to the many variables involved in sending Fax data over G.711 pass-through on IP trunks, there is no guarantee of reliable transport. However, practical experience has shown that, with some careful network considerations, such a link can be made to work. These considerations include:

- The IP trunk link must use G.711 only.
- The rate of packet loss on the link must be less than 0.1%.
- The link delay must be below 200 ms.
- Jitter must be less than 30 ms (ideally less than 20 ms).

With these settings, G3 FAX at V.17 speeds has been found to work with good reliability as compared to standard TDM connections, however without error correction mechanisms such connections should only be considered as best effort. Use of T.38 for transporting Faxes over IP networks is strongly recommended.

T.38 – reliable Fax over IP transport

Under normal circumstances, transmitting Fax over IP should not be considered without appropriate interfaces to provide signal redundancy and error correction. The two most prominent protocols are T.37 and T.38, which allow a standard T.30 fax to be connected over an IP network, T.37 is a store and forward protocol and T.38 is a real time protocol. These are generally point-to-point connections and provide a means of toll bypass. Fax within a pure IP environment makes little financial sense, considering that e-mail is far less sensitive to timing issues, and generally uses an error-correcting IP protocol to ensure delivery.

Since G.711 Fax cut through can only be used successfully on very high quality networks it is recommended that T.38 be used to support the transmission of FoIP. If the IP network introduces too much latency, jitter or almost any packet loss Fax transmissions using G.711 pass through will be error prone.

The T.38 protocol provides mechanisms to deal with network latency, jitter and packet loss.

Information pertaining to the use of T.38 for fax transmission can be found in T.38 FoIP Guidelines .

G.711 modem pass through

Sending tones between IP end devices can be problematic as the voice stream data rates will not be synchronized. This may result in gaps in the voice channel. Normally, these gaps are infrequent and have little effect on speech. However, they do affect tones and therefore they affect DTMF and MODEM tones. DTMF and MODEM devices can handle some data loss but IP networks can introduce more than expected, resulting in poor performance of these services.

Because there is no guarantee that it will work, connecting Modems over IP trunks is not recommended, however If it is necessary to transport Modem data across an IP trunk then the following guidelines should be adhered to:

- The IP trunk link must use G.711 only.
- The rate of packet loss on the link must be less than 0.1%.
- The link delay must be below 200 ms.
- Jitter must be less than 30 ms (ideally less than 20 ms).

Do not expect MODEM speeds to exceed 22.8 kbps.

Warning:
Modem signals require a special connection setup to be sent over an IP network; as a result, it is not recommended to send modem signals over an IP network at the present time.

Warning:
Due to the unreliability of sending Modem data over an IP network, this type of connection should never be used for any kind of critical application such as alarm systems.

13.3 DTMF Signaling over IP Networks

Generally, DTMF tones are used to establish a call between two end point at the start of a call. These tones are detected by the end equipment or connected interface and information is sent via the signaling channel, or out-of-band to the voice channel, which is yet to be established. This is normal DTMF usage.

However, there are instances where DTMF signals may be sent in-band (within the voice channel) after a call has been set up. In-band DTMF signals may be impacted (lost or altered due to packet loss or jitter) when passed over an IP network. To counteract this possibility, the DTMF signals are carried through the IP network as RFC4733 DTMF.

RFC4733 is intended to work with analog devices or TDM interfaces that use telecom dialing and timings for DTMF digits. However, certain speed dialing devices—e.g. Alarm monitors and Point of Sales (POS) terminals—may send or expect to receive DTMF digits that differ from standard telecom practices. Such devices may suffer performance degradation when used over a voice over IP connection, i.e. in-band signaling.

Use of such speed dialing devices should be considered as best-effort and may work in some situations, but not others. Should these devices suffer degradation, some suggestions include changing the dialing characteristics on the end devices, or use an alternative directly IP connected device, effectively as an overlay network onto the same IP infrastructure. Connections to the PSTN should terminate on an analogue or digital TDM trunk. The same logic applies to SIP trunks as well as IP trunks.

13.4 T.38 FoIP Guidelines

T.38 is the protocol recommended by the ITU to allow for transmission of real-time Group 3 Fax transmission over IP networks.

Mitel's T.38 implementation support V.17 speeds. Fax calls that are v.34 based will be handled at V.17 speeds by the 3300 ICPs.

T.38 is not supported on any of the server platforms, since it is a conversion between TDM and IP transmission, and these platforms do not have any TDM lines or trunks. T.38 is supported on the following platforms:

- 3300 MXe III

- 3300 CX/CXi II
- 3300 AX

DSP II

The DSP II card contains eight DSP devices and is required to support T.38.

An individual DSP device on the DSP II can be loaded with eight T.38 sessions; however, licensing limits dictate how many overall T.38 sessions can be supported. Also, one DSP device needs to be loaded with Tone/V.21 detectors to support Fax machine detection.

T.38 is a licensable option. Licenses can be purchased in increments of four up to a maximum of 64. The recommended maximum number of T.38 licenses supported on various platforms are:

- 3300 CX/CXi II, AX, MXe base – 16 T.38 sessions
- 3300 MXe III expanded – 48 T.38 sessions

Signaling

- The open standard signaling protocol used for establishing T.38 calls is SIP Version 2.0, which is based on RFC-3261.
- A T.38 call from a 3300 ICP to a 3300 ICP over an IP trunk will use Mitel's proprietary IP Trunk signaling protocol.
- The T.38 engine uses UDP to transport packets. TCP/IP is not supported.
- T.38 data is not encrypted.
- NuPoint Messenger does not support T.38 Fax. T.38 operation with NuPoint will only be possible with the same workaround that NuPoint Unified Messenger uses for G.729 compression. Operation with NuPoint is achieved by placing a T1 card on the 3300 into loopback mode to terminate the T.38 call. The call is then transferred to NuPoint via G.711. For additional information, see T.38 Frequently Asked Questions.

Warning:
For details on how to use a 3300 ICP as a Fax gateway for NuPoint, please refer to theNuPoint Unified Messaging Engineering Guidelines.

Operation

- T.38 will support T.30 operating modes 2 and 4, which means the calling Fax can operate in automatic or manual mode and the called Fax operates in automatic mode.
- Placing a voice call and then switching to Fax will work as long as the Fax call is initiated within 60 seconds of the set going off-hook.
- Switching to voice after a Fax transmission has completed is not recommended.
- The T.38 solution supports V.17 Fax calls at 14,400 bps or lower.

- Mitel's T.38 solution does not support V.34 (Super G3) Fax calls, however if a V.34 capable machine is set to operate in V.17 mode then the call can be handled as a T.38 call.

Warning:
V.34 (Super G3) Fax calls are only supported over links that are TDM end to end, these calls are not supported over IP by T.38 or G.711 pass through.

Line Circuits and COS (MiVB Class of Service) Options

For software releases prior to Release MCD 5.0 SP2

For correct operation, ports that are used to connect to Fax machines should have the following COS options enabled:

- Campon Tone Security/FAX Machine (Set to “Yes”)
- Busy Override Security (Set to “Yes”)
- External Trunk Standard Ringback (Set to “Yes”)
- Return Disconnect Tone When Far End Party Clears (Set to “Yes”)

For software Release MCD 5.0 SP2 and greater

For Release MCD 5.0 SP2 a new option called ‘Fax Capable’ has been added in the ‘Class of Service Options’ form. This new option is located under the ‘Fax’ heading. Another change introduced in MCD 5.0 SP2 is the renaming of the ‘Campon Tone Security/Fax Machine’ option to ‘Campon Tone Security’.

For correct operation, ports that are used to connect to Fax machines must have the following COS option enabled:

- Fax Capable (Set to “Yes”)

In addition to the Fax Capable COS option, the Administrator is advised to set the following COS options as indicated. If some of these overrides are not set as indicated and a tone is generated on this port while a Fax transmission is in progress, then the Fax transmission will likely fail.

- Campon Tone Security (Set to “Yes”)
- Busy Override Security (Set to “Yes”)
- External Trunk Standard Ringback (Set to “Yes”)
- Return Disconnect Tone When Far End Party Clears (Set to “Yes”)

The Administrator should "enable" V.34 Fax Interop at V.17 speeds with SIP Gateways; the factory default for this is disabled. This setting is a global setting; the setting is

applied to all ports on a system. This setting can be found under "Fax Advanced Settings"; for details see theSystem Administration Tool Help for MiVoice Business.

Resources required

- T.38 is a licensable option that also requires DSP resources. Licenses can be purchased in increments of four.
- A maximum of 56 T.38 sessions are supported on a DSP II card.
- At the start of a fax call an echo canceler is used. Once the call switches to T.38 mode, the echo canceler is placed in by-pass mode but continues to be allocated for the duration of the call.
- At the start of a call a Fax Tone/V.21 detector is used to determine if the call is a fax call. After 60 seconds the detector is relinquished.

Warning:
T.38 licenses are only required to allow an ICP to originate or to terminate Faxes sent over IP or SIP trunks, T.38 licenses are not required on an intermediate or tandem ICP.

DSP provisioning

- At start up, the system provisions the DSP II card with T.38 first, and then G.729.
- More T.38 or G.729 licenses can be purchased than the system hardware configuration supports. This allows licenses to be purchased prior to the installation of the DSP II card.
- A system reboot is required for licensing changes to take effect.

Zones

- As a general rule, T.38 should be used to transport Faxes between different zones.
- Zones are used to control where compression and Bandwidth Management are used.
- Zones can also be used to control where T.38 will be used. For instance, in some cases there may not be enough T.38 resources available for all Fax calls, in these situations the Administrator may want some Fax calls to be handled as G.711 Pass Through so that other specific routes can be guaranteed the use of T.38 resources.
- Networks and endpoints that communicate with each other over a WAN should be configured in different zones to allow for the use of T.38.
- The use of compression and T.38 within a zone can be configured independent from one another.
- In ESM there is form called the "Fax Service Profiles". This form allows the administrator to define how inter-zone (between zones) and intra-zone (within a zone) faxes will be handled.
- There is a pre-programmed default profile for both inter-zone and intra-zone traffic.

- The Administrator has the ability to create custom profiles for intra-zone traffic. Custom profiles cannot be created for inter-zone traffic.
- If two 3300s/EX are located in the same zone and have different Intra-zone T.38 settings configured. The system will attempt to place the call with the T.38 profile that uses the least amount of bandwidth.
- The Fax Service Profiles form can be shared via SDS. Sharing restrictions do not apply to this form.

Inter zone default profile

- There is only one profile available for inter-zone Fax traffic.
- This profile determines how Faxes will be handled when transmitted between devices located in different zones.
- The default Fax transmission speed for Inter-zone Faxes is 7200 bps, this speed was chosen so that the bandwidth requirements will be similar to the bandwidth requirements for a G.729 voice call which would typically be used across a bandwidth constrained inter-zone link.
- All other fields can be modified except for the "Label" field.

Intra zone default profile

- This profile determines how Faxes will be handled when transmitted between devices that are located in the same zone.
- The Intra-zone Fax profile uses a default Fax profile setting of "1".
- A Fax profile setting of "1" causes Faxes to be handled as G.711 Pass Through

Other intra zone profiles

- If a Fax profile other than "1" has been selected the Fax will be transmitted via T.38.
- The Administrator can create customized Fax profiles from "2" to "63".
- Each Fax profile can have a unique configuration.

Recommended settings

- Generally, a Fax transmission speed of 14,400 bps should be selected; however, the Administrator may want to select a slower speed if there are bandwidth constraints.
- Fax transmissions are comprised of two different portions or phases, a low speed phase (300 baud) that the Fax machines use to learn about each other's capabilities, and a high speed phase (14,400 baud) that the fax machines use to transmit the actual Fax data.
- Mitel's T.38 solution uses UDP to transport ethernet packets. UDP does not have the ability to re-send packets if packets are lost, so packet redundancy is supported. This allows the Administrator to select the level of redundancy required for both the high speed and low speed portions of a fax call.

- The 3300/EX ICP uses a redundancy default value of 3 for the low speed portion of the Fax call, and 1 for the high speed portion.
- In ESM, if a redundancy level of 0 is selected, there will be no redundant packets transmitted by the 3300/EX ICP, only the original packet will be transmitted. If a redundancy level of 3 is selected, then the 3300 ICP will transmit the original packet and three redundant copies of this packet.
- For most applications, the default values of 3 for the low speed portion of the Fax call and 1 for the high speed portion should be fine.
- Error Correction Mode (ECM) should be enabled if this capability is supported and enabled on both Fax machines.
- Non Standard Facilities (NSF) capabilities. Whether or not to enable this capability requires experimentation.

What happens if there are insufficient DSP resources or T.38 licenses?

- If DSP resources are not available for a T.38 call a generic DSP resource exhaustion alarm will be raised and the call will be handled as G.711 pass through.
- If the 3300/EX has not been provisioned with enough T.38 licenses, an incoming Fax call will be handled as G.711 pass through.

Are there fax speed restrictions?

- V.17 at 14,400 bps is the fastest speed supported by the T.38 solution.
- A V.34 fax machine attempting a call should renegotiate to V.17. The call will then be processed as a T.38 call; however, the V.34 machine must transmit a 'CNG' tone so that the 3300 can switch to T.38.
- If a V.34 fax machine attempts a call and does not renegotiate to V.17, the call will be processed as a G.711 pass through, however the success of the call cannot be guaranteed.

13.4.1 Bandwidth Management

- Mitel's Bandwidth Management solution will keep track of the Bandwidth consumed by Fax calls and Call Admission Control decisions will be made according to the system's configuration.
- As a rule of thumb the System Administrator may want to limit the bandwidth used by Fax calls to the same amount of bandwidth used by voice calls. For example, if zoning rules dictate that calls between two points should use G.729a compression, which uses 8000 bps of bandwidth, then the Administrator may want to limit Fax calls between these two points to 7200 bps.
- Inter-zone Fax Profile 1 by default will set Fax bandwidth usage to 14.4 kbps.

Minimum network requirements

The following tables indicate the minimum network requirements for various T.38 Fax calls, Voice and G.711 Pass Through are provided for reference.

Voice Network Limits

PACKET LOSS	JITTER	END TO END DELAY	
< 0.5%	< 20 ms	< 50 ms	Green = Go
< 2%	< 60 ms	< 80 ms	Yellow = Caution
> 2%	> 60 ms	> 80 ms	Red = Stop

Fax Over G.711 Pass Through

PACKET LOSS	JITTER	END TO END DELAY	
< 0.1%	< 20 ms	< 300 ms	Green = Go
< 0.2%	< 40 ms	< 500 ms	Yellow = Caution
> 0.2%	> 40 ms	> 500 ms	Red = Stop

T.38 UDP, Low Speed Redundancy=0, High Speed Redundancy=0

PACKET LOSS	JITTER	END TO END DELAY	
< 0.1%	< 20 ms	< 300 ms	Green = Go
< 0.2%	< 40 ms	< 500 ms	Yellow = Caution
> 0.2%	> 40 ms	> 500 ms	Red = Stop

T.38 UDP, Low Speed Redundancy=3, High Speed Redundancy=0

PACKET LOSS	JITTER	END TO END DELAY	
< 0.1%	< 1000 ms	< 6000 ms	Green = Go
< 0.2%	< 2000 ms		Yellow = Caution
> 2%	> 2000 ms	> 6000 ms	Red = Stop

T.38 UDP, Low Speed Redundancy=3, High Speed Redundancy=1 (Default Values)

PACKET LOSS	JITTER	END TO END DELAY	
< 2%	< 1000 ms	< 6000 ms	Green = Go
< 5%	< 2000 ms		Yellow = Caution
> 5%	> 2000 ms	> 6000 ms	Red = Stop

T.38 UDP, Low Speed Redundancy=3, High Speed Redundancy=2

PACKET LOSS	JITTER	END TO END DELAY	
< 5%	< 1000 ms	< 6000 ms	Green = Go
< 7%	< 2000 ms		Yellow = Caution
> 7%	> 2000 ms	> 6000 ms	Red = Stop

T.38 UDP, Low Speed Redundancy=8, High Speed Redundancy=3

PACKET LOSS	JITTER	END TO END DELAY	
< 7%	< 1000 ms	< 6000 ms	Green = Go
< 10%	< 2000 ms		Yellow = Caution
> 10%	> 2000 ms	> 6000 ms	Red = Stop

13.5 T.38 Alarms

For Release MCD 5.0 SP2 a new alarm has been added called ‘T.38 Load Alarm’. The purpose of this alarm is to indicate if there is an issue with the T.38 software/hardware/ configuration when the system starts up. For example this alarm will be set if a DSP II card is not installed in the system or if the DSP II card is defective and the system is unable to load software onto the DSP II card.

DSP resource exhaustion alarm

If DSP resources are not available for a T.38 call a generic DSP resource exhaustion alarm will be raised and the call will be handled as G.711 pass through.

13.6 T.38 Frequently Asked Questions

The following answers to frequently asked questions are provided for persons deploying T.38 in their networks.

Q: Why is the maximum number of T.38 Fax sessions set at 64?

A: 64 is the maximum number of T.38 Fax licenses that are allowed through AMC. In practice for a single DSP II card, the maximum number of sessions is 56 since one of the DSP devices is needed for V.21 FAX Tone detection.

Q: Does this mean the 3300/EX can only support 64 T.38 Fax machines?

A: No, 64 is the maximum number of T.38 CODECs supported on the ICP. Since Fax machines are typically not busy all of the time, it is possible to support more than 64 Fax machines. This is similar to the way that subscribers and trunks are allowed to be oversubscribed based on traffic patterns.

Q: How can an installer see how many active T.38 sessions are in progress?

A: The command line entry of 'e2tShow' will cause a line to be output such as:

'T2E crypto/clear/T.38 Channels active 0/0/0(high 1/0/1)'

The first numeric field indicates the number of currently active T.38 sessions. The second numeric field, in brackets indicates the maximum number of T.38 sessions that were ever active.

Q: What QoS settings are used for T.38 packets and signaling?

A: T.38 packets are transmitted using the same QoS settings as voice. QoS for T.38 cannot be programmed independently of voice QoS settings, T.38 and E2T (Voice) traffic share the same global variable for the QoS setting.

Q: How does the 'loopback' method used to allow T.38 to interoperate with NuPoint work?

A: Because NuPoint does not support T.38 natively a 3300 ICP needs to act as a Fax gateway in front of the NuPoint server. The 3300 ICP will terminate the T.38 call and then forward the Fax call to NuPoint as a G.711 pass though call.

For the 3300 ICP to act as a Fax gateway for NuPoint it is necessary to have a dual T1/E1 card installed in the 3300 ICP. A loopback cable is then used to connect the two ports of the T1/E1 card together. Using ARS, with digit insertion and removal, the G.711 Fax pass through call is directed out one port of the T1 card, then the call is received on the other T1 port via the loopback cable. The 3300 ICP will then forward the fax call to NuPoint over an IP link as a G.711 pass through call.

For details on how to use a 3300 ICP as a Fax gateway for NuPoint, please refer to the NuPoint Unified Messaging Engineering Guidelines.

Q: How are new third party T.38 gateways added to the compatibility list?

A: Additional gateways are added to the compatibility list via testing with the SIP interoperability lab. Devices can be submitted for approval through the SIP Interoperability Lab, model and manufacturer should be stated when applying for compatibility testing.

13.7 MiVoice Business and 3300 IP Ports

The table below shows the IP port numbers used with standalone MiVoice Business and 3300 ICP systems. It is not a definitive list, but is sufficient to identify voice connectivity. New features and applications may result in changes to this list.

Additionally there may be ports in here that are specific to the 3300 ICP that may not be available on a MiVoice Business for ISS platform using x86 processors. The MiVoice Business Multi-instance Media Server port ranges will differ and are covered in the specific Engineering Guidelines for that product.

For information regarding which ports are used by applications that are external to the 3300 ICP, refer to the documentation for that particular application.

Although the list can be used to open access across a firewall, where a firewall and NAT are used (for example, at the Internet), there might be issues with simply opening up ports from a functional and security viewpoint. Columns 2 and 3 in the following table indicate which ports should typically be opened in the firewall in MiVoice Business Release 9.2/9.1/9.0 and in pre-9.0 installations. The port diagrams that follow show

the interconnection between MiVoice Business and other products and applications, including the releases in which the ports are used and should be open.

Table 43: MiVoice Business and 3300 ICP port numbers

IP port number	MiVoice Business Release 9.2	PRIOR TO MiVoice Business Release 9.0	Transport	Description
20	No	Yes	TCP	FTP (data)
21	No	Yes	TCP	FTP (control)
22	Yes	Yes	TCP	AMC License server: outgoing (destination) Secure Terminal Access (SSH): incoming
23	No	Yes	TCP	Telnet
25	Yes	Yes	TCP	Non-secure Email
53	Yes	Yes	UDP	DNS: outgoing (destination) to server
67	Yes	Yes	UDP	DHCP server: incoming
68	Yes	Yes	UDP	DHCP client: outgoing
69	No	Yes	UDP	TFTP
80	Yes	Yes	TCP	HTTP

IP port number	MiVoice Business Release 9.2	PRIOR TO MiVoice Business Release 9.0	Transport	Description
	Yes	No	TCP	HTTP: Software Download Centre (SWDLC): Outgoing (destination)
137	No	Yes	TCP	NetBIOS for ETX/APC
138	No	Yes	UDP	NetBIOS for ETX/APC
161	Yes	Yes	UDP	SNMP
162	Yes	Yes	UDP	SNMP trap: outgoing (destination) to trap server
222	No	Yes	TCP	Telnet
389	Yes	Yes	TCP	LDAP
443	Yes	Yes	TCP	HTTPS
	Yes	No	TCP	HTTPS: Software Download Centre (SWDLC): Outgoing (destination)
	Yes	No	TCP	HTTPS for MiWalkThru
465	Yes	No	TCP	SSL/TLS to Email
587	Yes	No	TCP	STARTTLS to Email

IP port number	MiVoice Business Release 9.2	PRIOR TO MiVoice Business Release 9.0	Transport	Description
636	Yes	Yes	TCP	LDAPS
1066	Yes	Yes	TCP	IP Trunks Signaling (only available in unsecured mode)
1067	Yes	Yes	TCP	IP Trunks Signaling (secured)
1750	No	Yes	TCP	Software logs printer port
1751	No	Yes	TCP	Maintenance logs printer port
1752	Yes	Yes	TCP	SMDR printer port
1753	Yes	Yes	TCP	PMS/Hotel printer port
1754	Yes	Yes	TCP	General printer port
3300	No	Yes	TCP	-
3997	No	Yes	TCP	SAC (application)
3998	Yes	Yes	TCP	SAC (application)
3999	No	Yes	TCP	SAC (application)
5009	No	Yes	TCP	Teldir for eManager

IP port number	MiVoice Business Release 9.2	PRIOR TO MiVoice Business Release 9.0	Transport	Description
5060	Yes	Yes	TCP	SIP
5061	Yes	Yes	TCP/UDP	SIP-TLS
5320	Yes	Yes	TCP	MiTAI
5432	Yes	Yes	TCP	MiVoice Business Console Call History
6543	Yes	Yes	TCP	NSU Upgrade connection
6800	Yes	Yes	TCP	MiNET (only available in unsecured mode)
6801	Yes	Yes	TCP	Secure MiNET
6802	Yes	Yes	TCP	Secure MiNET
6803	Yes	Yes	TCP	Secure MiNET
6804	Yes	Yes	TCP	Secure MiNET (trusted applications only)
6830	Yes	Yes	TCP	Third-party voice mail/ PMS
6900 to 6999	Yes	Yes	TCP	MiNET Client source ports on phones

IP port number	MiVoice Business Release 9.2	PRIOR TO MiVoice Business Release 9.0	Transport	Description
7011	Yes	Yes	TCP	Data Services access
7050	Yes	Yes	TCP	SDS
8000	No	Yes	TCP	MiTAI Client (legacy)
8001	No	Yes	TCP	MiTAI Client (legacy)
10990	Yes	Yes	TCP	Remote Management between MiVoice Business
10991	No (9.0) Yes (9.1)	No	TCP	Remote Management between MiVoice Business (secured)
15373	Yes	Yes	TCP	ACD real-time events
15374	Yes	Yes	TCP	IP PMS
20001	Yes	Yes	UDP	TFTP
49500 to 49549	Yes	Yes	TCP	Data Services ports used for legacy connections in conjunction with port 7011
50000 to 50511	Yes	Yes	UDP	Voice/Media ports
16320 to 32767	Yes	Yes	TCP/UDP	DECT voice and signaling

The MSPLogs Viewer application communicates with MiVoice Business through the Data Service port (7011). If the MiVoice Business system is behind a firewall, then port 7011 must be opened and routed to the system. Older versions of MiVoice Business (before MiVoice Business 7.0) will attempt to establish a new connection back to the MSPLogs Viewer on its configured IP:Port combination (as stated in the wire protocol at connection time) which can be modified with command line options to traverse through firewalls and NAT. By default, the LogViewer will be listening for connections on the first available port in the range from 49500 to 49549.

Although the port listing in the Table 43: MiVoice Business and 3300 ICP port numbers on page 167 table identifies the default port range of 50000 to 50511 for voice media (RTP) connections, this is the default setting. Different gateways provide different capabilities that may reduce, or extend the upper value of this range. See the section Voice gateway IP ports on page 180 for further details.

New port updates for MiVoice Business Release 9.0 are:

- The following ports are no longer accessible: 20, 21, 23, 25, 69, 137, 138, 222, 1066 (available in unsecured mode), 1606, 1750, 1751, 3300, 3997, 3998, 5009, 6800 (available in unsecured mode), 8000, 8001, 9000 and 9002.
- Port 5320: Used by MiVoice Business to communicate with Mitel Open Integration Gateway (OIG), Live Business Gateway (LBG), and MiTAI.

New port 10991 is added in MiVoice Business 9.1 for secure Remote Management (RMI).

The following diagrams highlight the connections to and from MiVoice Business based on the above port information as well as IP-Phone connections. The following key is used to identify the connections:

- Arrow direction shows initial connection direction. Arrow head points to server.
- A double ended arrow means that connection is, or may be, established in both directions; i.e. an end device might be both a client and a server.
- Description above the line is the destination (server) termination point.
- Description below the line is the source (client) origination point.
- No description on the connection implies that any acceptable port may be used, typically within the ephemeral range, which may be defined on a particular device, but typically in the range 1024 to 65535.

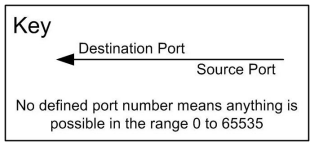


Figure 29: 3300 Port Connections - Key

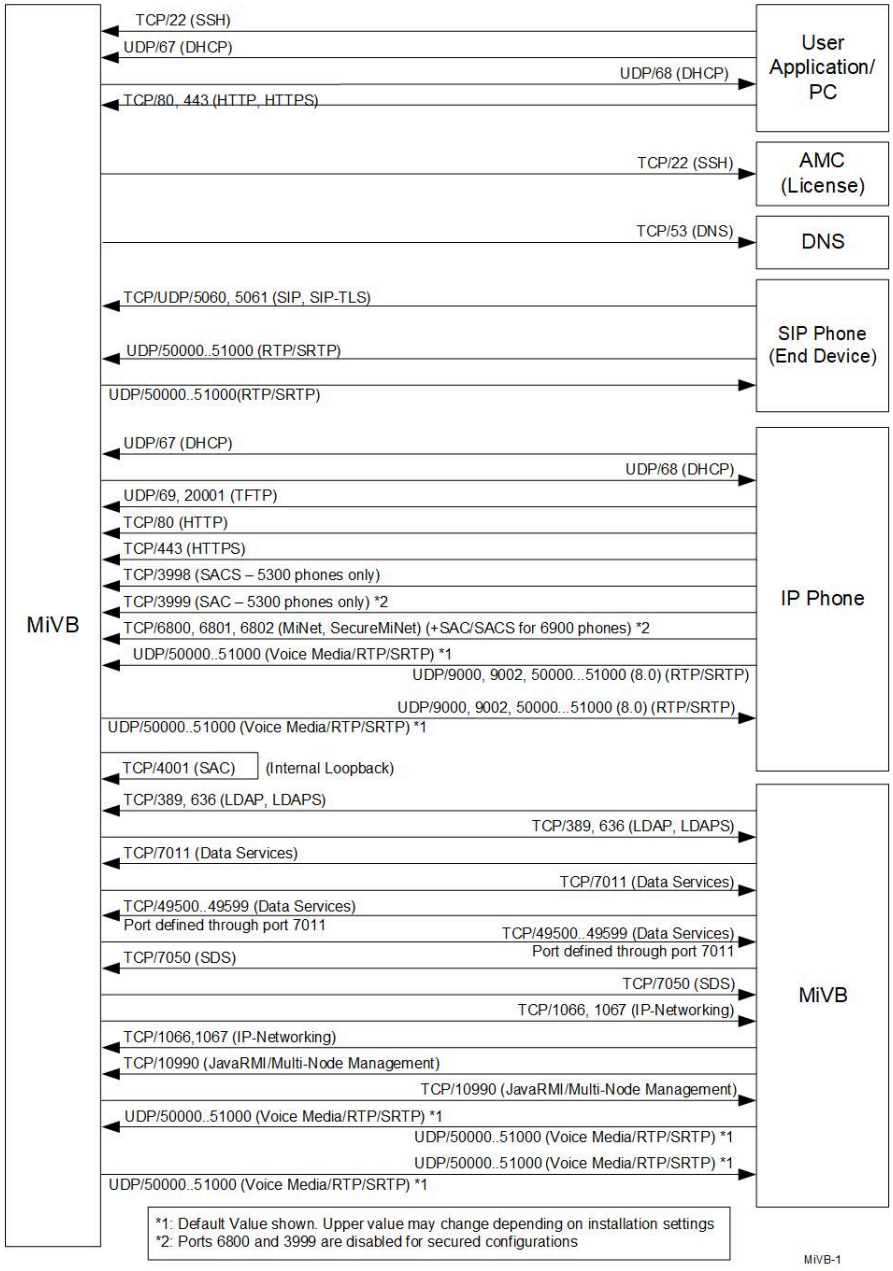


Figure 30: MiVoice Business Port Diagram 1

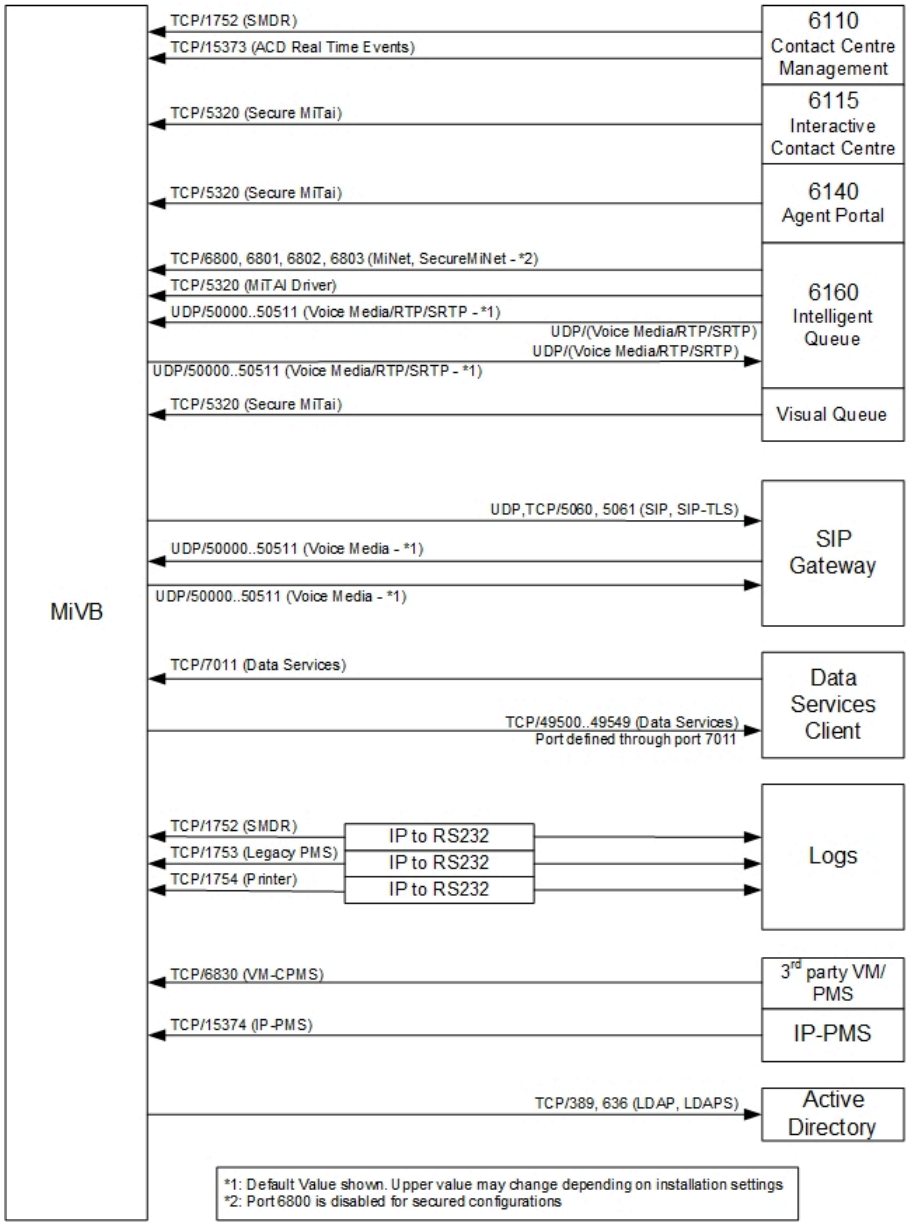


Figure 31: MiVoice Business Port Diagram 2

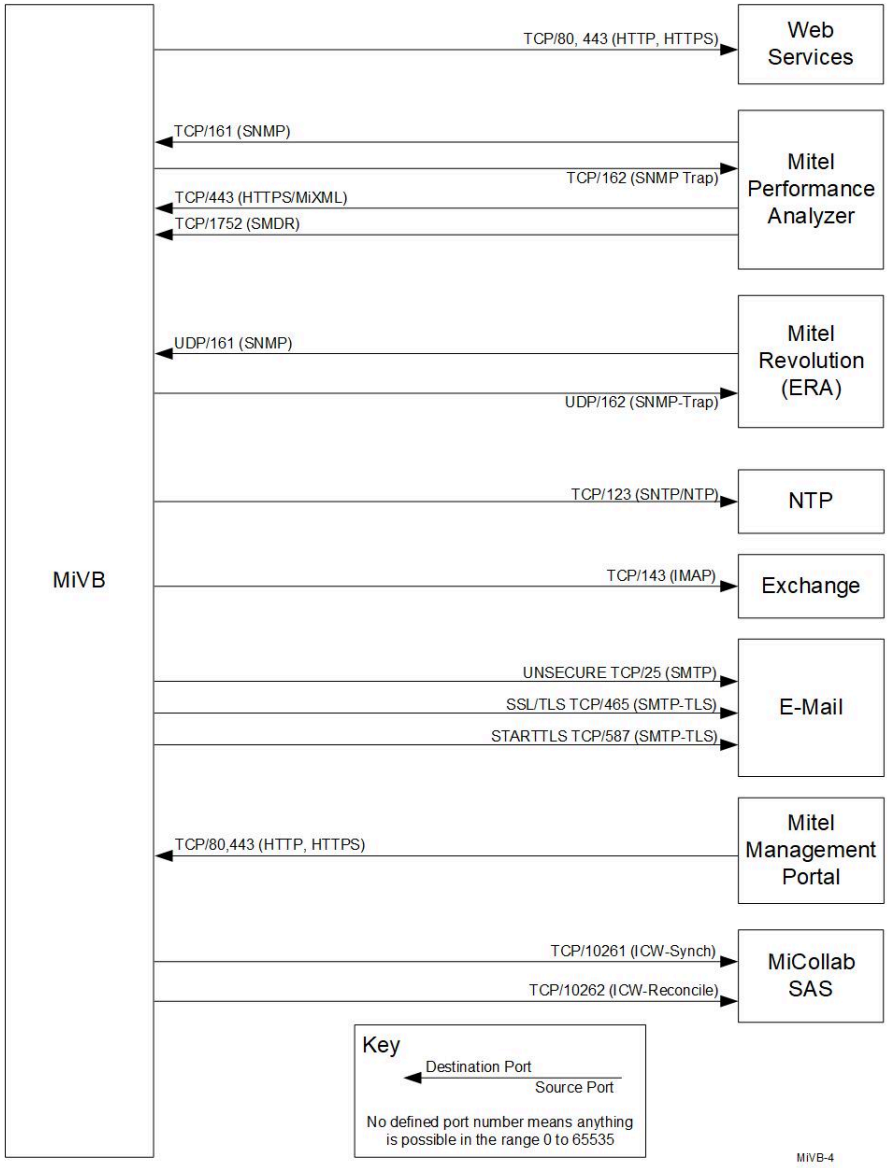


Figure 32: MiVoice Business Port Diagram 3

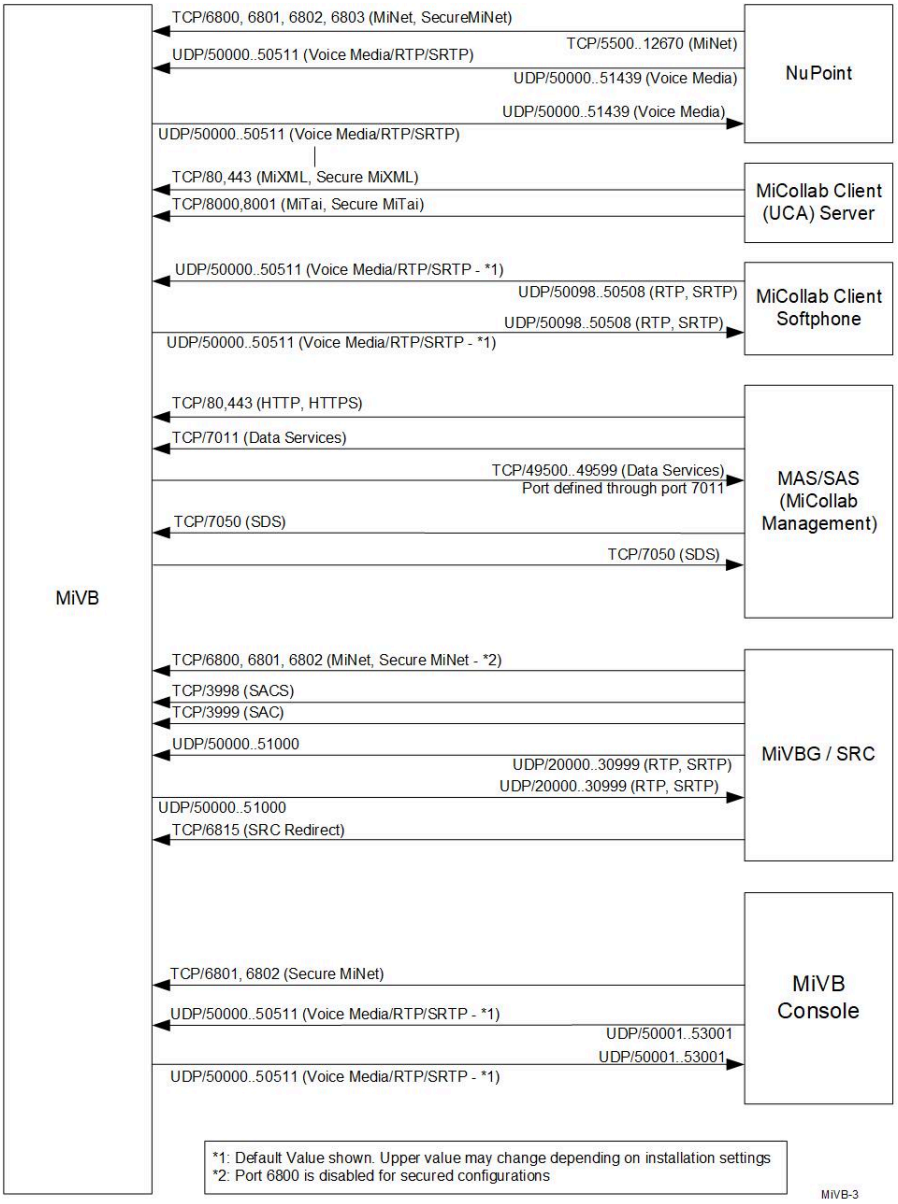


Figure 33: MiVoice Business Port Diagram 4

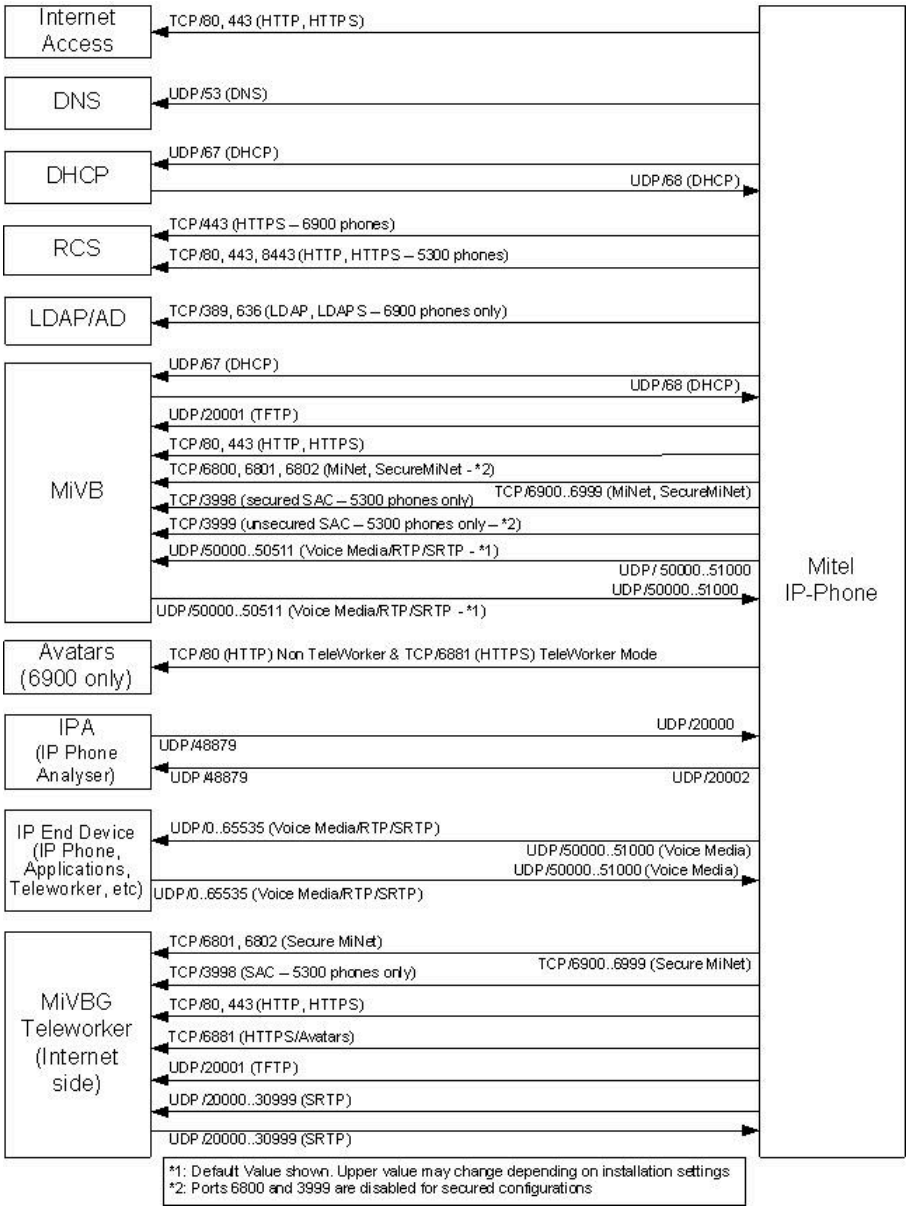


Figure 34: MiVoice Business Port Diagram 5

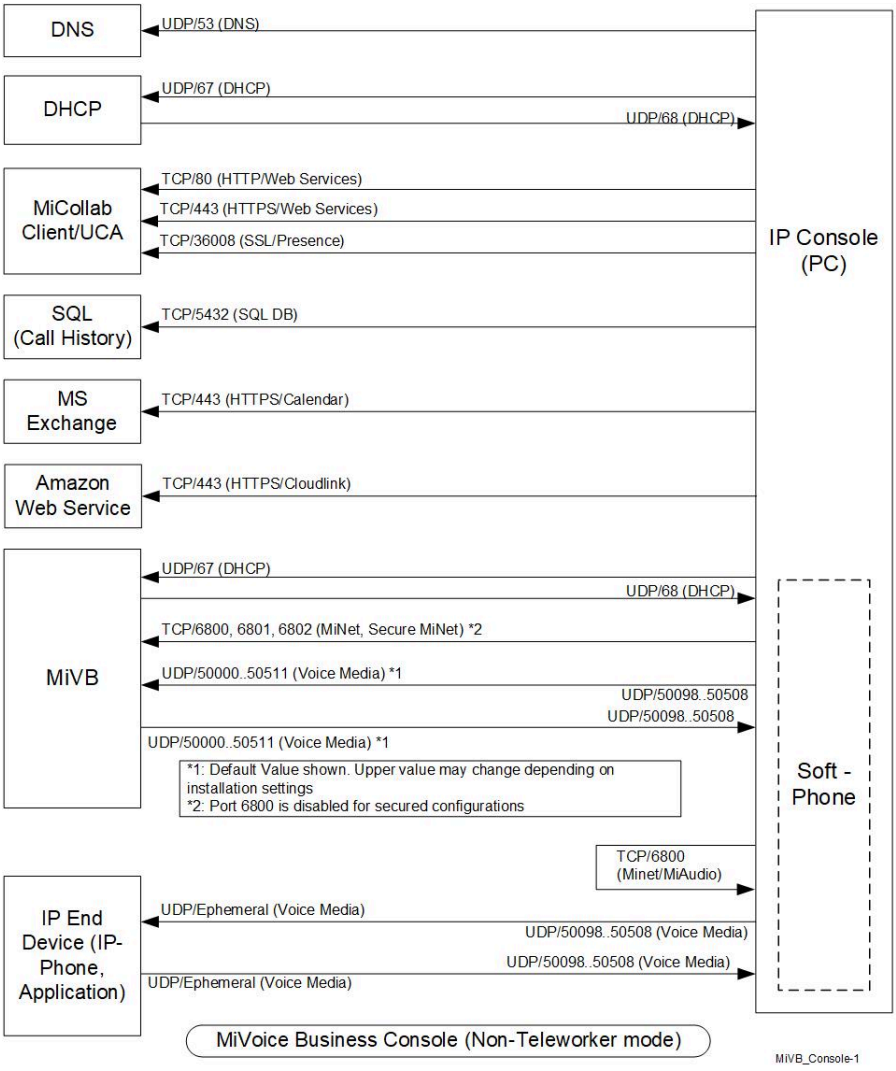


Figure 35: MiVoice Business Console in LAN mode

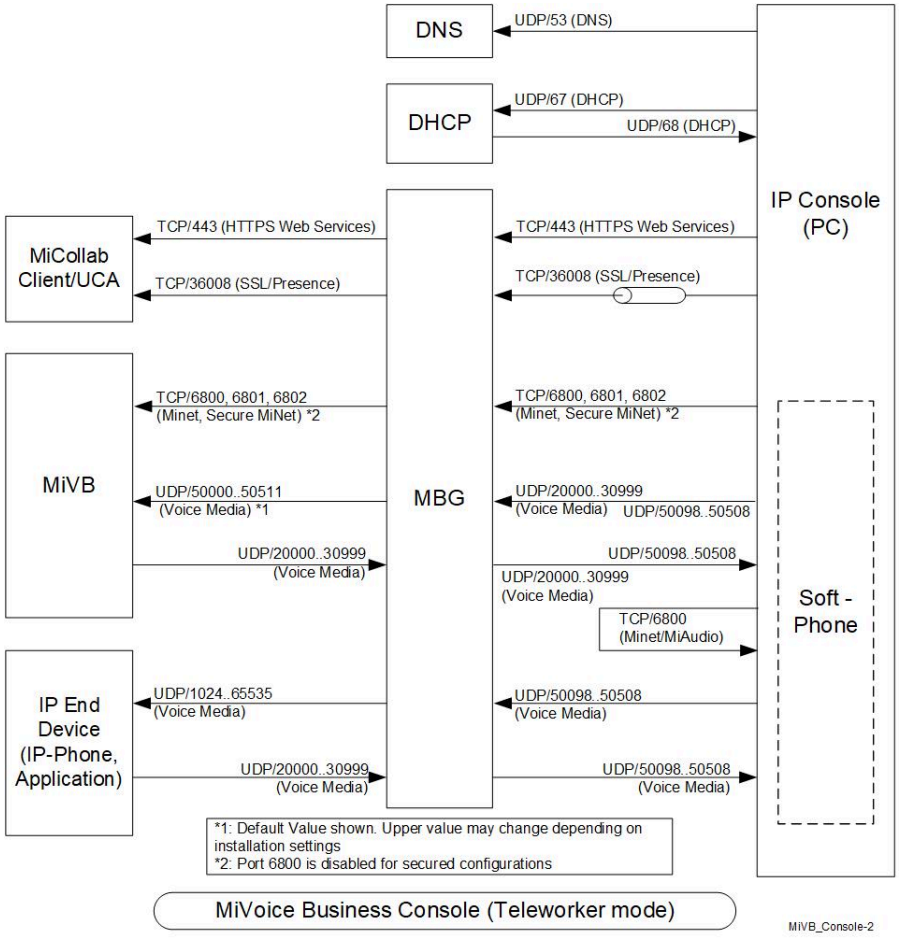


Figure 36: MiVoice Business Console in WAN mode

13.8 Embedded firewalls

The 3300ICP MiVoice Business product and phones include micro-firewalls to protect against unexpected levels of activity and will restrict traffic and responses according to some built in rules.

The 3300 MiVoice Business system will limit traffic based on current operating conditions and traffic expected to be handled. The phones use a “credit” system to limit unexpected packet rates and will discard if these limits are exceeded. This may occur during an attack, but may also occur for certain protocols where there are large subnets. Subnets greater than 1022 (/22) are not recommended, the normal being 254 (/24).

Table 44: Packet Rate Limits at Phone Firewall

Packet type	Rate (packet/second)	Burst handling (packets)
CDP, STP, LLDP	5	25
DNS	30	20
ARP, ICMP	5	50
RTP (per stream)	110	0

13.9 Voice gateway IP ports

Different configurations of MiVoice Business may have the capacity to provide more, or less channels than the default 256 audio channels. Details of the required port range is shown in the table below, Table 46: Active Media Channels on MiVoice Business Virtual on page 182.

In releases prior to MiVoice Business Release 9.0, it is possible to check and adjust the value of “Maximum Number of Audio Channels”, within the MSL management panel (check under 'MiVoice Business' for "Maximum Number of Audio Channels"). With MiVoice Business Release 9.0, the values are determined by the system resources. See the section Adjusting media server capacity on ISS and virtual systems for further details.

The maximum value of the RTP port range is calculated using the following formula: 50000 to (50000 + 2 x Maximum Number of Audio Channels - 1), e.g 96 channels results in a range of 50000-50191.

The table below shows the Voice Gateway IP port numbers.

Table 45: Voice Gateway IP Port Numbers

Platform	MEDIA Port RANGE	NOTES
CX II, CXi II	50000-50127	64 channels, RTP even ports

Platform	MEDIA Port RANGE	NOTES
MXe III (base)	50000-50127	64 channels, RTP even ports
MXe III (expanded)	50000-50255	128 channels, RTP even ports (See Note)
AX	50000-50255	128 channels, RTP even ports
EX	50000-50127	64 channels, RTP even ports
MiVB Virtual (all types)	50000-50511	256 channels, RTP even ports
MiVB ISS	50000-51999	1000 channels, RTP even ports

Note:

The ports on the MXe III expanded are associated with the E2T (voice gateway) IP address rather than the RTC IP Address. Other platforms use the common RTC/E2T IP address.

The number of active media channels on MiVoice Business Virtual is determined by the OVA settings and results in different maximum values depending upon the CPU core speed. The following table highlights the different values achievable:

Table 46: Active Media Channels on MiVoice Business Virtual

MiVB Virtua system size	vCPU	2.00 GHz	2.08 GHz	2.33 GHz	2.38 GHz	2.67 GHz	2.97 GHz	3.12 GHz	3.4 GHz
250	2	64	64	64	64	96	96	96	96
1500	3	96	96	96	128	128	160	160	160
2500	4	128	128	160	160	192	192	224	224
5000	6	192	224	224	256	256	256	256	256

For MiVoice Business Virtual deployments that result in a lower number of channels, this will also reduce the required upper port value. For example, for MiVB Virtual (250) with only 96 channels, the required port range 50000-50191.

For MiVoice Business on Industry Standard Server (ISS), the maximum number of active channels is 1000, based on a physical server with 2CPU, Quad Intel Core, hyperthreading enabled and a CPU clock speed in the range 2GHz to 3.4GHz.

13.10 Adjusting media server capacity on ISS and virtual systems

For MiVoice Business Release 9.0, it is possible to determine the capacity of the number of media channels on MiVoice Business ISS and Virtual MiVoice Business Release through use of the inbuilt resource capacity utility. If you are unfamiliar with using the utility, then contact Mitel Technical Support for further assistance.

In MiVoice Business Release 9.0, a new utility called mcd-set-media-streams.pl (a perl script) is available on x86 platforms (MiVB-ISS and MiVB-Virtual only, MiVB-EX has fixed allocations) that can be used to display and set the number of media channels. This utility is accessed from the Linux command line to determine, or modify the maximum allowed media streams after initial deployment.

There are several command line options for this utility:

- recalculate (mutually exclusive with streams option)

- streams=<number of streams> (assign fixed value, mutually exclusive with recalculate)
- firewall (limit streams to available firewall ports)
- nofirewall (default option, do not check firewall ports)
- maxfirewallport=<default 50511> (specify the firewall range 50000 to last open port)
- dryrun (calculate and display results, but to not save)
- nodryrun (default option, calculate and save to database)
- help (or -h, display full help, including examples)

The nominal default stream limit for the maximum number of channels is fixed at:

- 256 channels for the MiVoice Business Virtual deployments
- 1000 channels for the MiVoice Business-ISS deployments.

Other values can be programmed statically through the streams option.

Note:
If the maximum media streams is adjusted from the default value calculated on installation, the firewall settings must be changed using the formula in the section Voice Gateway IP Ports.

During an upgrade, the allowed media streams will be carried through from the old database, based on the assumption that if the customer was happy with the previous setting they will still be happy with it. On a new deployment, the script will be run to calculate and set up default parameters based on the underlying number or cores or vCPU, the processor speed, and the presence (or absence) of Hyperthreading. If for any reason the allowed number of streams is not satisfactory, the command allows the installer to modify the number of media streams, including an option to recalculate without changing the database to see what the default might be on new or existing hardware with a new software load (-dryrun).

The calculations for the Media Server capacity are designed to optimize the real-time processing ability of the system, balancing the requirements for responsiveness on call handling and maintenance activities with the need for good voice quality on media streams. Changes to the media server capacity are at the customer's risk. A reduction from the calculated value can allow higher call traffic, or increased system density in a virtual environment for multiple systems with limited numbers of users, if the need for media streams is known to be low. Increases above the calculated value can allow more media streams when the call traffic and feature use rate is low. It may be necessary to contact Professional Services for advice on using these options.

Command examples:

The following is an example of using the mcd-set-media-streams.pl utility to determine stream capacity:

mcd-set-media-streams.pl -recalculate

System has 4 CPU(s) with a clock rate of 2596 MHz and can support 184 streams.

Will set port_end to 50367

Conference Streams

The number of conference channels is provided up to the maximum number of media streams, or the maximum number of allowed conference streams (MiVoice Business limited to 600), whichever is lower.

For example, if the stream limit is 1000 (ISS), the number of media streams is 1000, and the conference limit is 600 (MiVoice Business), then the number of conference channels will be 600. If the stream limit is 1000, the number of media streams is 400, and the conference limit is 600, then the number of conference channels will be 400.

Compression

Compression capability is provided up to the limit of 256 channels, or the maximum number of media streams, whichever is lower.

For example, if the number of media streams is limited to 224 channels, then the number of compression channels is also 224. If the number of media channels is set to 320, then the number of compression channels is the maximum limit of 256 channels. Additional channels are provided using the G.711 CODEC.

13.11 IP Address Restrictions

- The controller reserves some IP addresses for internal use. Communication to the 3300 ICP using an IP address in these ranges will fail to get a response. See the 3300 ICP Technician's Handbook for the up-to-date list of reserved IP addresses.
- Reserved IP Addresses: 169.254.10.0/15 -> 169.254.30.0/15, inclusive

Note:
one of these reserved addresses can be used by devices that need to communicate with the 3300 ICP (e.g. MITEL Phones, E2T). These reserved IP address ranges can be used elsewhere in an IP network (i.e. network not connected to the 3300 ICP).

13.12 Interconnection Summary

The following illustrations provide a summary of the different interconnections between the ICP and associated peripheral cabinets. The analog interfaces both on the ASU and on the embedded Analog Main Board/Analog Option Board (AMB/AOB) have not been shown. These are standard telecom wiring, a nd likely use RJ-11 connections with a single pair.

Certain connections, such as those that terminate on the BRI or PRI interfaces are considered as telecom connections and rules that apply to this type of cable must be applied. Typically the connections to these interfaces are made with RJ-45 connectors and the cable pairs used are compatible with CAT 5 wiring. In a structured wiring infrastructure, it is possible to mix both data and digital telecom and use common CAT 5 cable throughout. Only at the MDF/Termination point will the cables be routed in different directions. CAT 3 cable may not provide the correct connections pairs and would require different implementations for data a telecom.

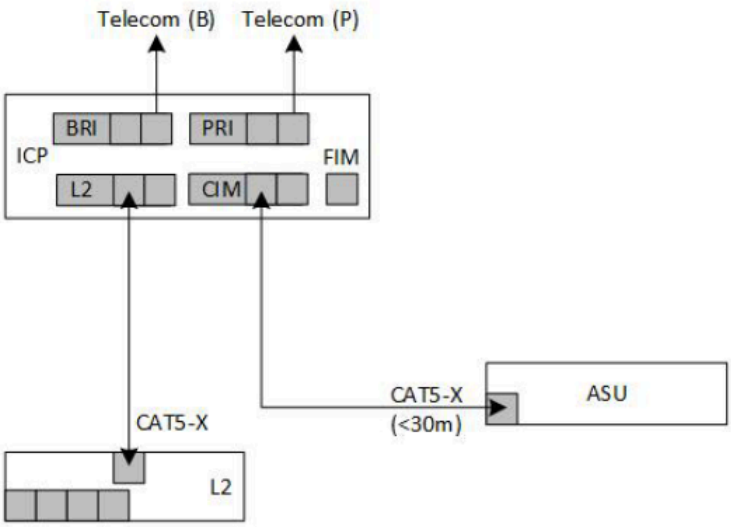


Figure 37: Interconnection Summary Diagram 1

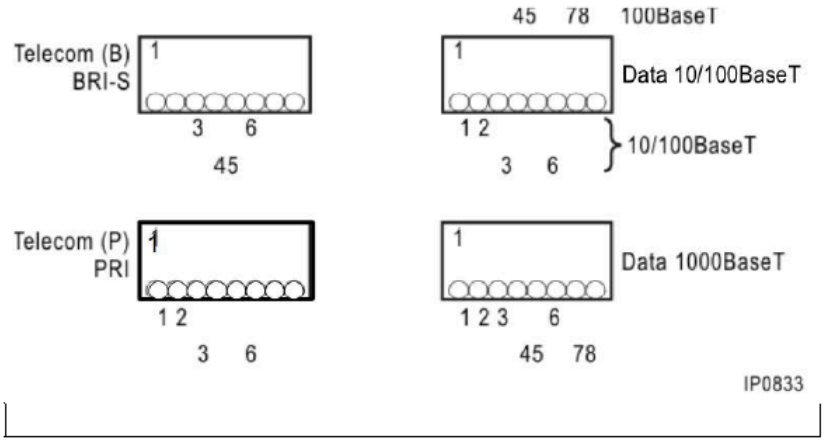


Figure 38: Interconnection Summary Diagram 2

Appendix A: Installation Examples 14

This chapter contains the following sections:

14.1 Using Cisco Routers and Catalyst Switches

The Cisco 2600 series routers tested were running Software (C2691-JS-M), Version 12.3(9) and the Catalyst C3550 Software (C3550-IfQ3L2-M), Version 12.0(20)EA1.

14.2 Basic Rules

- To segregate traffic, voice and data devices should be run on separate VLANs
- To transmit VLAN information and Ethernet priority between switches, the inter-switch connections must be defined as VLAN Trunks. We recommend IEEE 802.1Q VLAN trunks.
- Separate VLANs means that voice and data will also be running on separate IP subnets.
- To communicate between two different subnets (and between VLANs) traffic must pass through a router—same subnet communication does not and stays within its VLAN.

14.3 Basic IP Addressing Information

IP addresses can be written in several different ways; the two most common are:

- 192.168.100.1/24
- 192.168.100.1 255.255.255.0

To an end device these are the same - 255.255.255.0 is 24 binary 1s, therefore the /24. It is binary mathematics on a combination of the IP addresses and subnet mask that defines whether traffic being sent has to be directed to the router.

14.4 Basic Quality of Service (QoS)

In a VoIP network QoS exists at two layers:

1. Layer 2 – Ethernet priority information is used by switches to prioritize voice traffic over data. It is set using 3 bits within the 802.1Q VLAN header called the 802.1p bits. We recommend an 802.1p value of 6. However, an alternate value may be used provided that it is consistent throughout the network and that QoS is set appropriately.

1. If a MiVoice IP Phone learns its VLAN information via CDP and no other priority information is set (static or DHCP), then the 802.1p priority defaults to a value of 5.
2. When utilizing Cisco auto-qos, Cisco is expecting an 802.1p value of 5.
3. Layer 3 – IP priority is set using 6 bits within the IP header called Differentiated Services Code Point (DSCP). DSCP is used by routers to prioritize traffic. The Mitel default value was 44. This value is programmable to any value. Many IP networks expect a value of 46 - also called Expedited Forwarding (EF). On older ICP software loads the DSCP value may need to be changed at the first router.

- When utilizing Cisco auto-qos, Cisco is expecting a DSCP value of 46.

Note:
MiVoice IP Phones set the 802.1q bits as they are using VLAN tagged traffic. However the ICP controller does not send VLAN tagged traffic and so cannot set Ethernet priority. The switch port the controller connects to should set the Ethernet priority. This also applies to other non-VLAN aware VoIP devices, such as NuPoint Unified Messenger Rel. 8.5.

It is important that QoS be set up in the network end to end, not just in a few places. Internet VPN connections (for example, IP Sec) are not under the control of the customer so QoS is not end to end. VoIP is not controllable and quality is variable.

14.5 Define the IP Addressing

The first step in planning a VoIP network is deciding upon the VoIP addressing scheme. Usually a data network IP addressing scheme will already exist, so that will already be decided.

Choose an IP address range for the VoIP system that is not used elsewhere. Choose from one of the private address spaces (10.0.0.0/8, 172.16.0.0/12, 192.168.0.0/16), such as 192.168.100.0/24.

If possible, do not use IP addressing that conflicts with the internal IP addresses of the 3300 ICP, 192.168.10.0/28 to 192.168.13.0/28. (For Rel. 7.0 and later, 169.254.10.0/28 to 169.254.30.0/28 are reserved.)

Devices that conflict with the internal addresses will NOT be able to communicate with the ICP in any manner. Different networks must have different IP address ranges. There can't be two networks using the same IP addresses or the router can't route traffic correctly. Each interface (real or virtual) on a router is on a different network.

14.6 Define the VLAN

Most of the time, data will already exist and by default will be on VLAN 1. The next step in planning a VoIP network is deciding on the voice VLAN, VLAN 100, for example.

To create a VLAN:

Switch# configure terminalSwitch(config)# vlan 100Siwtch(config-vlan)# name VoiceVLANSwitch(config-vlan)# end

The IP address ranges that were previously selected will be used on the voice VLANs.

14.7 MiVoice IP Phone

Each MiVoice IP Phone must know (as a minimum)

- its own IP address
- its subnet mask
- its default gateway
- its VLAN (not required by a PC)
- its controller (not required by a PC)

Note:
A PC will also have other settings such as DNS and WINS that the MiVoice IP Phone does not require.

IP settings on a MiVoice IP Phone can be assigned:

- Statically or
- Dynamically using DHCP (the 3300 has an integrated DHCP server.)

VLAN settings on a MiVoice IP Phone can be:

- Assigned statically or
- Learned dynamically via CDP or
- Learned dynamically via DHCP double lookup.

QoS settings on a MiVoice IP Phone can be assigned:

- Statically or
- Dynamically using DHCP.

If a MiVoice IP Phone learns its VLAN information via CDP and no other priority information is set (static or DHCP), then the 802.1p priority defaults to a value of 5.

14.8 Example Network Topology

The following selections are used in the example, as shown in the following figure:

- Voice VLAN 100
- Voice IP addressing scheme of 192.168.100.0/24 and 192.168.200.0/24
- An existing data network of 10.0.0.0/16 running on the default VLAN is assumed.

The WAN link shown is a serial interface but could be any technology (Frame Relay, ATM, MPLS).

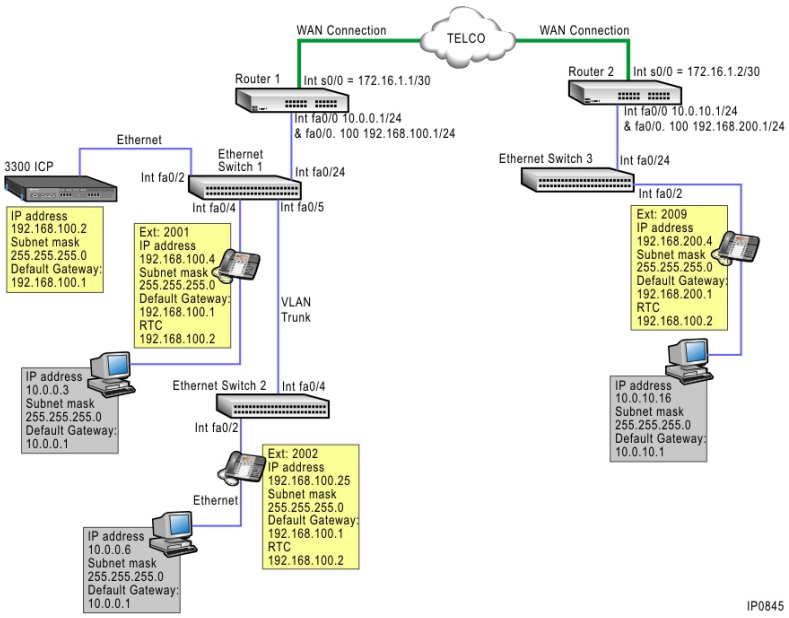


Figure 39: Example Network Topology

Ethernet Switch 1 configuration

There are four physical connections in the example topology for Ethernet Switch 1.

1. Fa0/2 to the 3300 ICP
2. Fa0/4 to IP Phone extension 2001
3. Fa0/5 to Ethernet Switch 2
4. Fa0/24 to Router 1 port Fa0/0

In this example VLANs are being assigned to the IP phones using CDP. Configurations for each switch interface follow (assumes no Cisco VLAN Trunking Protocol):

Switch# configure terminal	-
Switch1(config)# mls qos	[sets up QOS on the switch globally]
Switch1(config)# vlan 100	[create the voice VLAN]
Switch1(config-vlan)# name VoiceVLAN	[Give it a name]
Switch1(config-vlan)# exit	-

These steps are to set up QoS on the Catalyst 3550 and create the Voice VLAN.

Switch1(config)# interface fa0/2	[the connection to the 3300 controller]
Switch1 (config-if)# no cdp enable	[turn off unrequired CDP on this interface]
Switch1(config-if)# description “Connection to Mitel 3300 ICP”	-
Switch1(config-if)# switchport mode access	[port defaults to standard Ethernet frame]
Switch1(config-if)# switchport access vlan 100	[sets the VLAN]
Switch1(config-if)# mls qos cos 6	[sets the Ethernet priority (802.1p) to 6]
Switch1(config-if)# priority-queue out	[makes queue 4 a strict priority queue]
Switch1(config-if)# mls qos trust dscp pass-through cos	[required to allow DSCP & 802.1p through]
Switch1(config-if)# spanning-tree portfast	[bypasses the spanning the startup procedure]
Switch1(config-if)# exit	-

Interface fa0/2 is connected to the 3300 ICP which does not send VLAN tagged Ethernet frames. Hence the 802.1p value is set manually. The mls qos trust dscp pass-through cos interface command allows the DSCP value and 802.1p value to remain unchanged.

Switch1(config)# interface fa0/4	[the connection to the ext. 2001]
Switch1(config-if)# description "Connection to Ext.2001"	-

Switch1(config-if)# switchport mode access	[port defaults to standard Ethernet frame]
Switch1(config-if)# switchport voice vlan 100	[allows the IP set to learn the VLAN via CDP]
Switch1(config-if)# mls qos trust dscp pass-through cos	[required to allow DSCP & 802.1p through]
Switch1(config-if)# priority-queue out	[makes queue 4 a strict priority queue]
Switch1(config-if)# spanning-tree portfast	[bypasses the spanning the startup procedure]
Switch1(config-if)# spanning-tree bpdufilter enable	[stops spanning tree messages from being sent]
Switch1(config-if)# exit	-

Interface fa0/4 is connected to a MiVoice IP Phone that is capable of sending VLAN tagged Ethernet frames. When learning the voice VLAN via CDP (as configured) an 802.1p value of 5 is initially assumed. However, if the Mitel proprietary DHCP option 133 is used then this will overwrite the initial value. Mitel recommends an 802.1p value of 6 (unless using Cisco auto-qos). By default 802.1p value 6 is a member of queue number 4. This is the expedited queue created by the priority-queue out command on a Catalyst 3550. This interface configuration assumes that DHCP option 133 is set to 6. If an alternate value (e.g. 5) is used then the queue members need further defining.

Switch1(config)# interface fa0/5	[the VLAN trunk connection to Switch 2]
Switch1(config-if)# description "Connection to Switch 2"	-
Switch1(config-if)# switchport trunk encapsulation dot1q	[Forces 802.1Q frame]
Switch1(config-if)# switchport mode trunk	[sends VLAN information across the link]

Switch1(config-if)# priority-queue out	[makes queue 4 a strict priority queue]
Switch1(config-if)# exit	-

Interface fa0/5 is the VLAN trunk connection between Switch 1 and Switch 2. For Ethernet priority information to be sent between the switches the VLAN trunk must be configured.

Switch1(config)# interface fa0/24	[connection to Router 1 fa0/0]
Switch1(config-if)# description "Connection to Router 1 fa0/1 - Voice"	-
Switch1(config-if)# switchport trunk encapsulation dot1q	[Forces 802.1Q frame]
Switch1(config-if)# switchport mode trunk	[sends VLAN information across the link]
Switch1(config-if)# priority-queue out	[makes queue 4 a strict priority queue]
Switch1(config-if)# exit	-
Interface fa0/24 is connected to the router.	-

Ethernet Switch 2 configuration

There are two connections shown on the example topology for Ethernet Switch 2.

1. Fa0/2 to IP Phone extension 2002
2. Fa0/24 to Ethernet Switch 1

In this example VLANs are being assigned to the IP phones using CDP. Configurations for each port follow (assumes no VTP):

Switch2# configure terminal	-

Switch2(config)# mls qos	[sets up QOS on the switch globally]
Switch2(config)# vlan 100	[create the voice VLAN]
Switch2(config-vlan)# name VoiceVLAN	[Give it a name]
Switch2(config-vlan)# exit	-

These steps are to set up QoS on the Catalyst 3550 and create the Voice VLAN.

Switch2(config)# interface fa0/2	[the connection to the ext. 2002]
Switch2(config-if)# description "Connection to Ext.2002"	-
Switch2(config-if)# switchport mode access	[port defaults to standard Ethernet frame]
Switch2(config-if)# switchport voice vlan 100	[allows the IP set to learn the VLAN via CDP]
Switch2(config-if)# mls qos trust dscp pass-through cos	[required to allow DSCP & 802.1p through]
Switch2(config-if)# priority-queue out	-
Switch2(config-if)# spanning-tree portfast	[bypasses the spanning the startup procedure]
Switch2(config-if)# spanning-tree bpdufilter enable	[stops spanning tree messages from being sent]

Interface fa0/2 is connected to a MiVoice IP Phone that is capable of sending VLAN tagged Ethernet frames. When learning the voice VLAN via CDP (as configured), an 802.1p value of 5 is initially assumed. However, if the Mitel proprietary DHCP option 133 is used then this will overwrite the initial value. Mitel recommends an 802.1p value

of 6 (unless using Cisco auto-qos). By default 802.1p value 6 is a member of queue number 4. This is the expedited queue created by the priority-queue out command on a Catalyst 3550. This interface configuration assumes that DHCP option 133 is set to 6. If an alternate value (e.g. 5) is used then the queue members need further defining.

Switch2(config)# interface fa0/24	[the VLAN trunk connection to Switch 1]
Switch2(config-if)# description "Connection to Switch 1"	-
Switch2(config-if)# switchport trunk encapsulation dot1q	[Forces 802.1Q frame]
Switch2(config-if)# switchport mode trunk	[sends VLAN information across the link]
Switch2(config-if)# priority-queue out	[makes queue 4 a strict priority queue]

Interface fa0/24 is the VLAN trunk connection between Switch 2 and Switch 1. For Ethernet priority information to be sent between the switches the VLAN trunk must be configured.

Ethernet Switch 3 configuration

There are two connections in the example topology for Ethernet Switch 3.

1. Fa0/2 to IP Phone extension 2009
2. Fa0/24 to Router 2 port Fa0/0

In this example VLANs are being assigned to the IP phones using CDP. Configurations for each port follow (assumes no VTP):

Switch3# configure terminal	-
Switch3(config)# mls qos	[sets up QOS on the switch globally]
Switch3(config)# vlan 100	[create the voice VLAN]
Switch3(config-vlan)# name VoiceVLAN	[Give it a name]

Switch3(config-vlan)# exit	-

These steps are to set up QoS on the Catalyst 3550 and create the Voice VLAN.

Switch3(config)# interface fa0/2	[the connection to the ext. 2009]
Switch3(config-if)# description "Connection to Ext.2009"	-
Switch3(config-if)# switchport mode access	[port defaults to standard Ethernet frame]
Switch3(config-if)# switchport voice vlan 100	[allows the IP set to learn the VLAN via CDP]
Switch3(config-if)# mls qos trust dscp pass-through cos	[required to allow DSCP & 802.1p through]
Switch3(config-if)# priority-queue out	[makes queue 4 a strict priority queue]
Switch3(config-if)# spanning-tree portfast	[bypasses the spanning the startup procedure]
Switch3(config-if)# spanning-tree bpdufilter enable	[stops spanning tree messages from being sent]

Interface fa0/2 is connected to a MiVoice IP Phone that is capable of sending VLAN tagged Ethernet frames. When learning the voice VLAN via CDP (as configured) an 802.1p value of 5 is initially assumed. However, if the Mitel proprietary DHCP option 133 is used then this will overwrite the initial value. Mitel recommends an 802.1p value of 6 (unless using Cisco auto-qos). By default 802.1p value 6 is a member of queue number 4. This is the expedited queue created by the priority-queue out command on a Catalyst 3550. This interface configuration assumes that DHCP option 133 is set to 6. If an alternate value (e.g. 5) is used then the queue members need further defining. A local DHCP server or "IP helper" to a remote DHCP server is required at the site.

Switch3(config)# interface fa0/24	[connection to Router 1 fa0/0]

Switch3(config-if)# description "Connection to Router 2 fa0/1 - Voice"	-
Switch3(config-if)# switchport trunk encapsulation dot1q	[Forces 802.1Q frame]
Switch3(config-if)# switchport mode trunk	[sends VLAN information across the link]
Switch3(config-if)# priority-queue out	[makes queue 4 a strict priority queue]
Interface fa0/24 is connected to the router.	-

Router 1 configuration

There are two physical interfaces on the Router 1 and an additional virtual interface.

- S0/0 is the serial interface to the WAN. This could be an alternative technology but we show PPP in this example.
- Fa0/0 is the 10/100 physical Ethernet interface to Ethernet Switch 1 that connects to the Data VLAN (i.e. VLAN 1).
- Fa0/0.100 is the virtual interface that only "listens" to the Voice VLAN (i.e. VLAN 100).

An example configuration using static routes follows. If using dynamic routing protocols (RIPv2, OSPF etc.) the static routes are not required.

Programming the IP addresses

Router1# configure terminal	-
Router1(config)# interface s0/0	-
Router1(config-if)# description "To Telco"	-
Router1(config-if)# ip address 172.16.1.1 255.255.255.252	
Router1(config-if) encapsulation ppp	-

Router1(config-if)# no shutdown	-
Router1(config)# interface fa0/0	-
Router1(config-if)# description "Default Gateway for 10.0.0.0/24 Network"	
Router1(config-if)# ip address 10.0.0.1 255.255.255.0	-
Router1(config-if)# no shutdown	-

These previous steps are probably already in place for the data network.

Router1(config)# interface fa0/0.100	-
Router1(config-subif)# encapsulation dot1q 100	[set the interface to tag traffic with VLAN 100]
Router1(config-subif)# description "Default Gateway for 192.168.100.0/24 VoIP Network"	-
Router1(config-subif)# ip address 192.168.100.1 255.255.255.0	-

This is the step for setting the IP interface for the VoIP traffic.

Programming static routes

Router1(config)# ip route 10.0.10.0 255.255.255.0 172.16.1.2
Router1(config)# ip route 192.168.200.0 255.255.255.0 172.16.1.2

Setting up QoS for Router1 using Low Latency Queuing

Create an Extended Access Control List (ACL)

Router1(config)# ip access-list extended Mitel	[Sets up a filter that matches Mitel VoIP traffic only]
Router1(config-ext-nacl)# permit udp 192.168.100.0 0.0.0.255 192.168.200.0 0.0.0.255	

ACLs have an implicit deny at the end so no other traffic meets the criteria listed.

Create Class Maps

Router1(config)# class-map match-all MitelClassMapIn	-
Router1(config-cmap)# match access-group name Mitel	[Matches the ACL created above]
Router1(config)# class-map match-all MitelClassMapOut	-
Router1(config-cmap)# match ip dscp ef	[Matches the DSCP value of 46]

Create the Policy Maps

Router1(config)# policy-map MitelPolicyIn	[Only required if default DSCP is being changed]
Router1(config-pmap)# class MitelClassMapIn	[Matches the class map looking for Mitel traffic]
Router1(config-pmap-c)# set ip dscp ef	[Overwrite DSCP bits with a value of 46]
Router1(config)# policy-map MitelPolicyOut	-
Router1(config-pmap)# class MitelClassMapOut	[Matches the class map looking for DSCP 46]

Router1(config-pmap-c)# priority percent 30	[Mitel traffic is guaranteed 30% of the bandwidth]
Or	-
Router1(config-pmap-c)# priority "bandwidth"	[Alternatively specify actual bandwidth amount]
Router1(config-pmap-c)# exit	-
Router1(config-pmap)# class class-default	[What to do with other traffic]
Router1(config-pmap-c)# fair-queue	-

Note:
Priority is specified in either Percent or Bandwidth, NOT both.

Router1(config)# class-map match-all MitelClassMapP-Bit	-
Router1(config-cmap)# match ip dscp ef	[Matches the DSCP value of 46]
Router1(config)# policy-map MitelPolicyMapP-Bit	-
Router1(config-pmap)# class MitelClassMapP-Bit	[Matches the class map looking for DSCP 46]
Router1(config-pmap-c)# set cos 6	[set the 802.1p bit to 6 if DSCP = 46]

No "priority" statement has been set in this Policy Map. This is because the Fast Ethernet outbound queue is assumed not to be congested due to the ingress traffic coming from the serial interface being much lower than 100Mbps of the Fast Ethernet interface. If the

Fast Ethernet is congested for other traffic reasons then a "priority" statement will be required on the Fast Ethernet sub-interface Policy Map as well.

Now place the policy maps on the interfaces

Router1(config)# interface fa0/0	-
Router1(config-if)# service-policy input MitelPolicyIn	[applying the inbound policy map]
	-
Router1(config)# interface fa0/0.100	-
Router1(config-subif)# service-policy output MitelPolicyMapP-Bit	[applying the outbound policy map]
	-
Router1(config)# interface Serial0/0	-
Router1(config-if)# max-reserved-bandwidth 100	[makes the priority % command be a true %]
Router1(config-if)# service-policy output MitelPolicyOut	[applying the outbound policy map]

Router 2 configuration

There are two physical interfaces on the Router 2 and an additional virtual interface.

- S0/0 is the serial interface to the WAN. This could be an alternative technology but we show PPP in this example.
- Fa0/0 is the 10/100 physical Ethernet interface to Ethernet Switch 3 that connects to the Data VLAN (i.e. VLAN 1).
- Fa0/0.100 is the virtual interface that only "listens" to the Voice VLAN (i.e. VLAN 100).

An example configuration using static routes follows. If using dynamic routing protocols (RIPv2, OSPF etc.) the static routes are not required.

Programming the IP addresses

Router2# configure terminal	-
Router2(config)# interface s0/0	-
Router2(config-if)# description "To Telco"	-
Router2(config-if)# ip address 172.16.1.2 255.255.255.252	
Router2(config-if) encapsulation ppp	-
Router2(config-if)# no shutdown	-
	-
Router2(config)# interface fa0/0	-
Router2(config-if)# description "Default Gateway for 10.0.10.0/24 Network"	
Router2(config-if)# ip address 10.0.10.1 255.255.255.0	-
Router2(config-if)# no shutdown	-

These previous steps are probably already in place for the data network.

Router2(config)# interface fa0/0.100	-
Router2(config-if)# encapsulation dot1q 100	[set the interface to tag traffic with VLAN 100]
Router2(config-if)# description "Default Gateway for 192.168.200.0/24 VoIP Network"	

Router2(config-if)# ip address 192.168.200.1 255.255.255.0

This is the step for setting the IP interface for the VoIP traffic.

Programming static routes

Router2(config)# ip route 10.0.0.0 255.255.255.0 172.16.1.1
Router2(config)# ip route 192.168.100.0 255.255.255.0 172.16.1.1

Setting up QoS for Router2 using Low Latency Queuing

Create an Extended Access Control List (ACL)

ip access-list extended Mitel	[Sets up a filter that matches Mitel VoIP traffic only]
permit udp 192.168.200.0 0.0.0.255 192.168.100.0 0.0.0.255	

ACLs have an implicit deny at the end so no other traffic meets the criteria listed. This can be programmed with more detail if preferred by the customer, e.g. UDP port #s, etc. but is not required for this example.

Create Class Maps

Router2(config)# class-map match-all MitelClassMapIn	-
Router2(config-cmap)# match access-group name Mitel	[Matches the ACL created above]
Router2(config)# class-map match-all MitelClassMapOut	-
Router2(config-cmap)# match ip dscp ef	[Matches the DSCP value of 46]

Create the Policy Maps

Router2(config)# policy-map MitelPolicyIn	[Only required if default DSCP is being changed]
Router2(config-pmap)# class MitelClassMapIn	[Matches the class map looking for Mitel traffic]
Router2(config-pmap-c)# set ip dscp ef	[Overwrite DSCP bits with a value of 46]
	-
Router2(config)# policy-map MitelPolicyOut	-
Router2(config-pmap)# class MitelClassMapOut	[Matches the class map looking for DSCP 46]
	-
Router2(config-pmap-c)# priority percent 30	[Mitel traffic is guaranteed 30% of the bandwidth]
Or	-
Router2(config-pmap-c)# priority "bandwidth"	[Alternatively specify actual bandwidth amount]
	-
Router2(config-pmap-c)# exit	-
Router2(config-pmap)# class class-default	[What to do with other traffic]
Router2(config-pmap-c)# fair-queue	-

Note:
Priority is specified in either Percent or Bandwidth, NOT both.

Router2(config)# class-map match-all MitelClassMapP-Bit	-
Router2(config-cmap)# match ip dscp ef	[Matches the DSCP value of 46]
Router2(config)# policy-map MitelClassMapP-Bit	-
Router2(config-pmap)# class MitelClassMapP-Bit	[Matches the class map looking for DSCP 46]
Router2(config-pmap-c)# set cos 6	[set the 802.1p bit to 6 if DSCP = 46]

Note:
No "priority" statement has been set in this Policy Map. This is because the Fast Ethernet outbound queue is assumed not to be congested due to the ingress traffic coming from the serial interface being much lower than 100Mbps of the Fast Ethernet interface. If the Fast Ethernet is congested for other traffic reasons then a "priority" statement will be required on the Fast Ethernet sub-interface Policy Map as well.

Now place the policy maps on the interfaces

Router2(config)# interface fa0/0	-
Router2(config-if)# service-policy input MitelPolicyIn	[applying the inbound policy map]
-	-
Router2(config)# interface fa0/0.100	-

Router2(config-subif)# service-policy output MitelClassMapP-Bit	[applying the outbound policy map]
-	-
Router2(config)# interface Serial0/0	-
Router2(config-if)# max-reserved-bandwidth 100	[makes the priority % command be a true %]
Router2(config-if)# service-policy output MitelPolicyOut	[applying the outbound policy map]

Miscellaneous

To add an 802.1p value to the high priority queue

Switch1(config-if)# wrr-queue cos-map 4 5	-
Switch1(config-if)# wrr-queue cos-map 3 6 7	-

This example moves 802.1p value 5 to the high priority queue (queue number 4) created with the "priority-queue out" command and 802.1p values 6 and 7 to queue 3.

To use a data VLAN other than VLAN 1

In this example VLAN 10 is used as the data VLAN. It is likely that VLAN 1 will still be being used for network management.

Switch1(config)# vlan 10	[create the data VLAN]
Switch1(config-vlan)# name DataVLAN	[Give it a name]
Switch1(config-vlan)# interface fa0/5	-

Switch1(config-if)# switchport access vlan 10	[still an access port - just using VLAN 10]

Setting up Router 2 to be a local DHCP server

ip dhcp excluded-address 192.168.200.1 (the router address - add any others that can't be used)

ip dhcp pool Mitel

network 192.168.200.0 255.255.255.0	-
domain-name customername.com	-
dns-server ip addresses	-
default-router 192.168.200.1	[default gateway]
option 128 ip 192.168.100.2	[IP Phone TFTP server]
option 129 ip 192.168.100.2	[RTC IP address]
option 130 ascii "MITEL IP PHONE"	[required for the Mitel phones to accept]
option 132 hex 0000.0064	[VLAN 100 in hex]
option 133 hex 0000.0006	[802.1p priority 6]
lease 14	[lease length in days]

Remember to save your configurations!

14.9 Using the CXi II or MXe III Internet Gateway

By default, the System IP Gateway IP address is the same as the L2 Switch IP address.

The CXi II/MXe III Internet Gateway can be used to provide the following functionality:

- Forwarding of local traffic to the intranet, by virtue of network list lookups
- Forwarding of all other traffic onto the Internet.

In the figure *CXi/CXi II Internet Gateway*, a L2 expansion switch has been connected to the Gigabit Ethernet Uplink port of the CXi II. A router has been attached to the L2 expansion switch.

The CXi II System Gateway IP address needs to be changed from the default value so that it matches the router's IP address. This is necessary because the CXi II System Gateway IP address is also the Default Gateway IP address used by the CXi II internal L2 Switch's network list entry table.

The intranet may contain corporate servers and other MiVoice Business phone systems that will now be reachable via IP trunking. Call Control uses the System Gateway IP address to reach those other networks. The PCs and IP phones use DHCP Option 3 (which equals the L2 Switch IP address) to reach known intranet, and unknown internet networks.

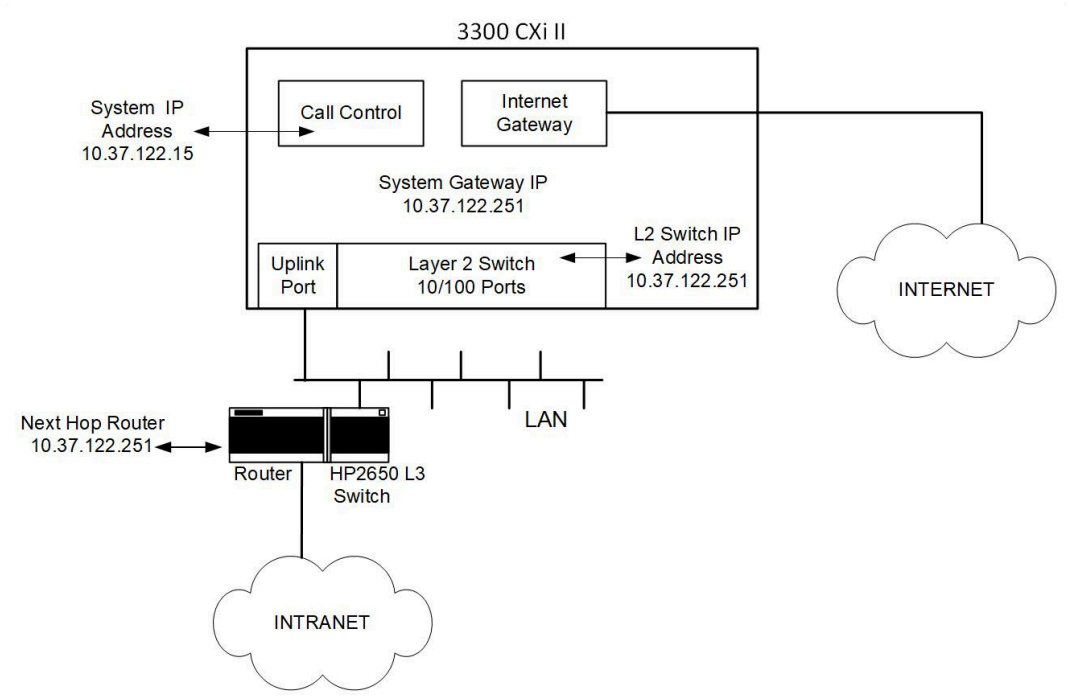


Figure 40: CXi/CXi II Internet Gateway

Appendix B: LLDP and LLDP-MED Configuration Examples

15

This chapter contains the following sections:

LLDP, LLDP MED Overview

LLDP (Link Layer Discovery Protocol – IEEE 802.1AB) provides a standards-based Layer 2 protocol for enabling network switches to advertise themselves and learn about adjacent connected LLDP devices. LLDP-MED (LLDP Media specific – ANSI/TIA-1057) is an extension to LLDP to provide auto-configuration and exchange of media related information, such as Voice VLAN and QoS, and is designed to provide enhanced VoIP deployment and management.

Typically phones will need information such as QoS settings and also location information. Since these network settings are specific to a location, or connection point, then having the IP-Phone auto discover this information from the local Ethernet switch reduces setup within other areas of the network, e.g. DHCP, and eases Moves, Adds and Changes of devices.

The following example describes how to set up LLDP/LLDP-MED for an access port on a ProCurve Networking 5300xl Ethernet switch. Commands may differ depending upon manufacturer and model. (LLDP instructions for the ProCurve 2600, 3500, 5300 and 5400 model switches are the same.) Instructions in the sections below only contain a subset of CLI commands available. Please read the device documentation to determine the correct instruction set to use.

Note:
For additional clarity, the user input is shown in **bold font** within this appendix.

15.1 Configuration Overview

A number of parameters within the Layer 2 access switch need to be configured in order to advertise the correct LLDP/LLDP-MED information to the end devices.

LLDP-MED includes information regarding the voice VLAN ID, DSCP and Priority and supports both tagged and untagged voice devices. However, since Untagged voice devices do not include the VLAN header or L2 Priority information, the Switch Access Port parameters will need to reflect this and apply policy changes at the ingress port. This is described further in Connecting non VLAN enabled voice devices to the network.

By default, LLDP and LLDP-MED are enabled, and default Priority and DSCP values are already defined for voice services. All that is required is to identify the voice VLAN with "voice" service and assign the voice VLAN to the required ports.

LLDP MED advertising information determination

LLDP-MED has the capability to provide the following information to the voice devices connected to the network switch:

- VLAN ID
- Priority
- DSCP

The information advertised by LLDP-MED is obtained from various switch settings. These settings need to be configured in order to get the correct information on the relevant port. Note that some of these commands are used for other functions, which includes the policy enforcement, some of which operate on a VLAN or switch level, not just at the port.

These areas are highlighted in the diagram below, and described in more detail in the following sections.

The shaded areas identify the end devices and areas linked with policy enforcement through the Access Layer Switch. Information from a number of areas is used to identify the service, in this case, voice, which is combined to create the LLDP/LLDP-MED advertisement.

The following figure *LLDP-MED Advertisement Information Sources* identifies that the end device will use VLAN tagging, in this case VLAN 63, will use Priority 6 and DSCP value 46 (101110), commonly referred to as Expedited Forwarding. These values are used throughout this Appendix to illustrate network switch settings and configurations.

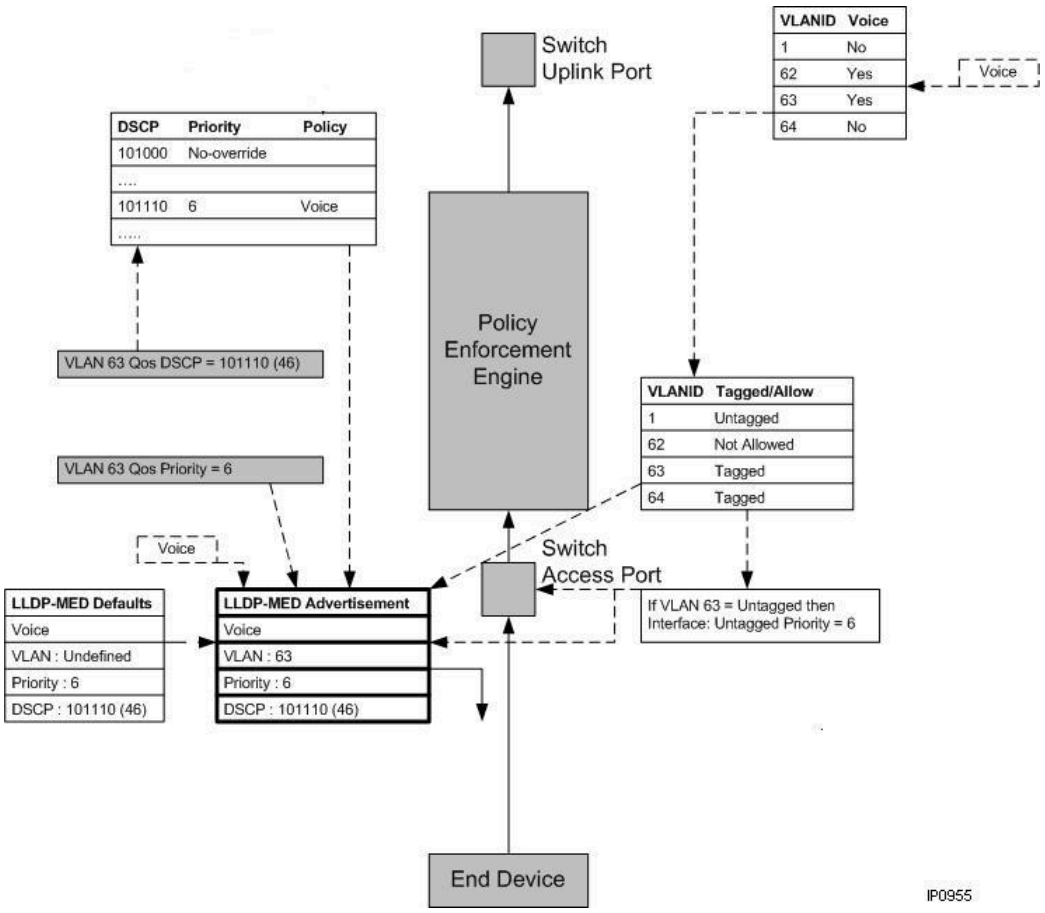


Figure 41: LLDP-MED Advertisement Information Sources

By default, LLDP and LLDP-MED are enabled across the switch. LLDP-MED requires that the voice VLAN be identified at a port before the port becomes active in advertising of VLAN, Priority and DSCP.

The information to be advertised can come from a number of sources, but follows the general flow outlined below:

- Defaults for LLDP-MED for voice at the Access Port are: Priority = 6; DSCP = 46. Defaults are overwritten with other information, if available and configured.
- The lowest value voice VLAN ID that is enabled at the port will be used. If a voice VLAN is not identified, LLDP-MED will not be advertised.
- If the voice VLAN is assigned as "untagged", then the default priority is sent over LLDP-MED. The DSCP information also uses the default value.
- If the voice VLAN is identified as "tagged" then the QoS settings can come from one of the following locations:
- · through Policy Enforcement of a VLAN QoS Priority setting that applies to the particular voice VLAN. The DSCP information will come from the default.

- · through Policy Enforcement of a VLAN QoS DSCP setting that applies to the particular voice VLAN. This also uses the DSCP Map to obtain Priority information, if available.

The information in the remaining parts of this appendix provide more details on a number of different network switch parameters that can be used to configure and adjust LLDP-MED values for more custom operation.

15.2 Quick Start Getting LLDP MED Running Quickly

To get LLDP-MED working quickly, all that is required is to identify the appropriate VLAN with the "voice" services as part of the normal switch configuration procedures. The example, below uses VLAN 63, but this can be replaced with any valid VLAN ID value.

```
HP ProCurve Switch 5304XL(config)# vlan 63 voice
```

By default, LLDP and LLDP-MED are enabled, and default Priority and DSCP values are already defined for voice services. All that is required is to identify the voice VLAN with "voice" service and enable this at the required port.

15.3 LLDP MED for Network Policy Information (VLAN and QoS)

ForMiVoice IP Phones to be fully operational for QoS, three network policy parameters need to be configured. These are:

- VLAN ID
- Layer 2 Priority (IEEE 802.1p) (CoS)
- DSCP (Diff Serv Code Point)

This information can be learned from LLDP-MED compliant network switches.

To ensure that the correct settings are applied, use the following sequence of commands:

- Define Voice VLAN and assigned ports.
- Define DSCP to Priority Mapping (optional) or voice VLAN priority settings (optional).
- Define QoS Policy Enforcement at the access port (optional).
- Ensure that LLDP is enabled.

Defining voice VLAN and ports

First, determine which VLANs are configured and which are configured for voice:

```
HP ProCurve Switch 5304XL (config)#show vlan

Status and Counters - VLAN Information

Maximum VLANs to support : 8

Primary VLAN : DEFAULT_VLAN

Management VLAN :

802.1Q VLAN ID  Name            |  Status      Voice
--------------  --------------- +  ----------  ------
1               DEFAULT_VLAN    |  Port-based  No
64              V64Net          |  Port-based  No
```

In this example, VLAN 63 will be designated for voice use, assigned a name and a particular port.

```
HP ProCurve Switch 5304XL(config)#vlan 63 tagged a1

HP ProCurve Switch 5304XL(config)#vlan 63 voice

HP ProCurve Switch 5304XL(config)#vlan 63 name V.63

HP ProCurve Switch 5304XL(config)#show vlan

Status and Counters - VLAN Information

Maximum VLANs to support : 8
```

```
Primary VLAN : DEFAULT_VLAN

Management
VLAN :

802.1Q VLAN ID  Name            |  Status      Voice
--------------  --------------- +  ----------  ------
1               DEFAULT_VLAN    |  Port-based  No
63              V.63            |  Port-based  Yes
64              V64Net          |  Port-based  No
```

Rather than immediately assigning a VLAN to a particular port, a VLAN can be created by simply defining it, and then later assigning this VLAN to the desired ports:

```
HP ProCurve Switch 5304XL(config)#vlan 63 voice

HP ProCurve Switch 5304XL(vlan-63)#
```

Assigning a port, or range, to a particular VLAN:

```
HP ProCurve Switch 5304XL(vlan-63)#vlan 63 tagged a1
HP ProCurve Switch 5304XL(vlan-63)#show vlan ports a1

Status and Counters - VLAN Information - for ports A1

802.1Q VLAN ID  Name  |  Status  Voice
```

----------	----------	+	----------	------
1	DEFAULT_VLAN	|	Port-based	No
63	VLAN63	|	Port-based	Yes

Note:

ProCurve switches will only advertise LLDP-MED for ports that are members of VLANs with the "voice" attribute, as shown above.

A range of ports would be assigned to a voice VLAN in the following manner:

```
HP ProCurve Switch 5304XL(vlan-63)#vlan 63 tagged a1,a3,b1-b16
```

In this example, ports A1, A3 and a range of B1 to B16 are assigned to the voice VLAN 63.

Note that multiple VLANs can be assigned to be voice VLANs. However, the typical operation would be to assign a single voice VLAN to a particular port. In the event that multiple voice VLANs are assigned to a port, then only the lowest value VLAN ID will be advertised by LLDP-MED.

Defining DSCP to Priority (COS) mapping (optional)

The DSCP and Layer 2 Priority values, to be advertised by LLDP-MED, may be obtained from the DSCP to Priority map list (where the default LLDP-MED settings are not to be used, then this is the recommended method, as it allows the voice QoS policy to be defined without the requirement to apply a general switch Policy Enforcement).

By default, the Procurve switches will already have a Priority value of 7 applied to the DSCP Expedited Forwarding (value of 46, or 101110). All that is required is to identify the DSCP 46 as being used for voice policy.

In most network switches a Priority value of 6 or 7 will make little difference, other than to identify the packet as high priority and higher than standard data. Some administrators prefer to reserve Priority 7 for network management only, and to use Priority 6 for voice. This example will be shown. Other values can also be configured if needed depending on installation.

It is important to complete the DSCP to Priority (CoS) mappings before assigning any Priority/QoS Enforcement policies at the individual port, or across the network switch. Failure to do this may result in mismatched information and unexpected error conditions.

First, determine the current DSCP mapping.

```
HP ProCurve Switch 5304XL(config)#show qos dscp-map

DSCP -> 802.p priority mappings

DSCP policy      802.1p tag        Policy nam

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

000000           No-override

000001           No-override

.
.

101101           No-override

101110           7

.
.

111111           No-override
```

The DSCP value of interest is 46, or 101110 in binary format. We recommend assigning a priority of 6 for this DSCP value and assigning a policy name to identify that it is for use with voice. (Note that to simplify the displayed information, the complete mapping table is not shown).

```
HP ProCurve Switch 5304XL(config)#qos dscp-map 101110 priority 6HP ProCurve
Switch 5304XL(config)#qos dscp-map 101110 name voice
```

These commands result in the following L3/L2 map settings:

```
HP ProCurve Switch 5304XL(config)#show qos dscp-map

DSCP -> 802.p priority mappings

DSCP policy      802.1p tag       Policy name
------------     ---------------  ---------------
000000           No-override
000001           No-override
.
.
101101           No-override
101110           6                voice
.
.
111111           No-override
```

Applying DSCP to Priority QoS Policy Enforcement at the Access Port (optional)

This function is not a requirement of LLDP/LLDP-MED, but may be used where the end device is not trusted or does not send frames with all the appropriate QoS information. In this case the ProCurve switch will modify the QoS contents of the outbound packet, based on the ingress port policy configuration.

An example of such a connection could be a softphone on a PC. The PC will run multiple applications, but will not be able to provide VLAN tagging or Priority information. Currently, voice applications will have a user, or predetermined DSCP value.

In the case of a Softphone being used on a PC, then DSCP information is provided by the voice application, but Priority information and VLAN assignment must be configured at the access port on the switch.

VLAN assignment for Data will be on the untagged Data VLAN. By default, this is VLAN 1. Untagged data packets will use the port priority, which defaults to 0. For voice, the

DSCP value can be used to identify a higher Priority value, as defined in the DSCP to Priority map. In this example, the voice packets should have Priority 6 assigned, which will be achieved by using the incoming DSCP information in the packet.

The DSCP to Priority map is defined in the ProCurve switch by default. The commandqos type-of-service diff-services enables the switch-wide mapping of incoming DSCP data to Priority mapping. Be aware that this affects all ports on the switch.

Applying PER VLAN Priority and DSCP QOS (optional)

A VLAN can be assigned a Priority value or a DSCP with associated Priority values, on a per VLAN basis. Note that all packets on this VLAN will have their QoS parameters adjusted as defined by the VLAN settings.

A VLAN can be assigned a per VLAN Priority value that will be applied on a VLAN basis and will force all packets on a VLAN to have a common Priority value. This may not be desirable for some applications, as some voice packets may need to have different priority levels. If this VLAN is identified as voice and is enabled at an Access Port, then LLDP-MED will advertise this Priority value rather than the default. The default DSCP value will continue to be used.

```
HP ProCurve Switch 5304XL(config)#vlan 63 qos priority 6
```

A VLAN can be assigned a per VLAN DSCP value that will be applied on a VLAN basis and will force all packets on a VLAN to common DSCP and Priority values. The priority values are based on the DSCP to Priority map settings. This may not always be desirable for some applications, as some voice packets may need to have different priority levels. If this VLAN is identified as voice and is enabled at an Access Port, the LLDP-MED will advertise the defined DSCP value with associated Priority value, rather than the default values.

```
HP ProCurve Switch 5304XL(config)#vlan 63 qos dscp 101110
```

Connecting non VLAN enabled voice devices to the network

Typically these would be voice servers, applications and gateways. These devices may not support VLAN tagging capability, but may provide DSCP, depending on the application. In this case, the VLAN would be assigned asuntagged to the Ethernet switch port and the DSCP to Priority map could be used to assign the appropriate Priority level to the incoming data.

Alternatively, the port priority can be applied on a per port basis. This would be configured through the commandinterface <port-list> qos priority <0-7>.

LLDP/LLDP-MED will advertise DSCP, VLAN and Priority from anuntagged access port, but the VLAN and Priority values are only provided for informational purposes, since the end device is sending untagged frames and as such, will only be able to make use of the DSCP information.

It is important that the static priority value configured at the interface port lines up with priority settings advertised to other voice devices that are LLDP aware in order to have a common QoS policy throughout the network.

Ensure that LLDP is enabled

By default, LLDP and LLDP-MED will be enabled when using HP Procurve switches.

There are a number of individual settings to enable or disable LLDP or LLDP-MED. More detailed instructions can be found within the ProCurve switch installation and configuration manual. For this example, the main activity is to ensure that LLDP functionality is operational.

To enable or disable LLDP across the switch use the following:

```
HP ProCurve Switch 5304XL(config)#lldp run (enable)

HP ProCurve Switch 5304XL(config)#no lldp run (disable)
```

15.4 LLDP MED for Location Information

The example in this section shows how to determine and set the individual port settings for location information. This can take different formats depending upon local administration or regulatory requirements. The example uses the civic address format rather than the coordinate or number system. The subcategories used are those highlighted in the ProCurve Networking manual.

Note:
Mitel Phones do not currently support the LLDP-MED location ID feature. Instead, Mitel Phones use a proprietary implementation to support emergency call service in conjunction with the Mitel Emergency Response Adviser.

Current information can be obtained by the following:

```
HP ProCurve Switch 5304XL(config)#show lldp config a1
```

```
LLDP Port Configuration Detail

Port : A1

AdminStatus [Tx_Rx] : Tx_Rx

NotificationEnabled [False] : False

Med Topology Trap Enabled [False] : False

Country Name                    : US

What                            : 2

Ca-Type                         : 1
```

To redefine these setting the full information must be entered:

```
HP ProCurve Switch 5304XL(config)#lldp config a1-a4 medportlocation civic-addr
CA 2 1 ON 3 Ottawa 4 Kanata 6 "Legget Drive"
```

Note:
Spaces are used to separate the different fields, and so a name with an intended space must be enclosed in “quotation marks”.

To view the location configuration:

```
HP ProCurve Switch 5304XL(config)#show lldp config a1

LLDP Port Configuration Detail

Port : A1
```

```
AdminStatus [Tx_Rx] : Tx_Rx

NotificationEnabled [False] : False

Med Topology Trap Enabled [False] : False

Country Name                    : CA

What                            : 2

Ca-Type                         : 1

Ca-Length                       : 2

Ca-Value                        : ON

Ca-Type                         : 3

Ca-Length                       : 6

Ca-Value                        : Ottawa

Ca-Type                         : 4

Ca-Length                       : 6

Ca-Value                        : Kanata

Ca-Type                         : 6

Ca-Length                       : 6

Ca-Value                        : Legget Drive
```

15.5 Additional Useful Commands

Further commands, details and settings can be found in the network switch installation and configuration documentation, as supplied by the switch vendor. The above examples simply illustrate how to start up an initial LLDP-MED configuration with ProCurve Networking switches, to ease initial installations and moves, adds and changes.

To determine how a particular VLAN may be configured for QoS Policy Enforcement, the following command can be used:

```
HP ProCurve Switch 5304XL(config)#show qos vlan

VLAN priorities

VLAN ID     Apply rule     |     DSCP      Priority
----------  -------------  +     --------  --------
1           No-override    |               No-override
63          No-override    |               No-override
64          DSCP           |     011010    4
100         DSCP           |               3
```

The remote device can also be interrogated to determine the settings it is using. This is useful as a cross check that LLDP/LLDP-MED is working, or to diagnose configuration conflicts:

```
HP ProCurve Switch 5304XL(config)#show lldp info remote-device b2

LLDP Remote Device Information Detail
```

Local Port	: B2
ChassisType	: network-address
ChassisId	: ddde
PortType	: mac-address
PortId	: 08 00 0f 12 2a 7a
SysName	: regDN 63022,MITEL 5220 DM
System Descr	: regDN 63022,MITEL 5220 DM,LIM,h/w rev 0,ASIC rev 0,f/w Bo...
PortDescr	: LAN port
System Capabilities Supported	: bridge, telephone
System Capabilities Enabled	: bridge, telephone
Remote Management Address	
Type	: ipv4

Address	: 100.100.100.101
MED Information Detail	
EndpointClass	:Class3
Media Policy Vlan id	:100
Media Policy Priority	:6
Media Policy Dscp	:46
Media Policy Tagged	:True
Poe Device Type	:PD
Power Requested	:51
Power Source	:Unknown
Power Priority	:High

To determine which LLDP-MED options are operational on a particular port, the following commands can be used:

```
HP ProCurve Switch 5304XL(config)#sh lldp config b2
```

LLDP Port Configuration Detail

Port : B2

AdminStatus [Tx_Rx] : Tx_Rx

NotificationEnabled [False] : False

Med Topology Trap Enabled [False] : False

TLVS
Advertised:

* port_descr

* system_name

* system_descr

* system_cap

* capabilities

*
network_policy

* location_id

* poe

*
macphy_config

IpAddress
Advertised:

The**capabilities** option and**network policy** are both needed for auto configuration of the end devices.

The different services can be enabled or disabled through the following commands. Use the**no** format to disable an option:

#lldp config <port-range>**medTlvEnable capabilities#**

lldp config <port-range>**medTlvEnable network_policy**

#lldp config <port-range>**medTlvEnable poe**

#lldp config <port-range>dot3TlvEnable macphy_config

Appendix C: VoIP and VLANs 16

This chapter contains the following sections:

16.1 VoIP Installation and VLAN Configurations

Although this section refers to VLAN configurations, it can also be used to consider whether or not VLANs are needed for a particular installation.

There are, currently, six configurations that have been identified. These are not expected to cover all possible configurations, there will always be exceptions, but as a guideline for the more general installations. The number of configuration variations has arisen because of the introduction of the CXi II product, which includes a VoIP capable Layer 2 switch. In effect the CXi II is now an integral part of the network, whereas the MXe III is considered more as an end point or server within the network.

The main installations that are likely to be encountered are:

- A standalone CXi II, voice-only devices, including expansion Layer 2 switch.
- Segregation of data and voice networks, with a router connecting the two. (In effect this is a physical solution, rather than the logical solution through use of VLAN.)
- Standalone CXi II unit with dedicated ports for voice and data devices, no expansion switch.
- CXi II with expansion Layer 2 switch, voice and data using dedicated ports on both CXi II and expansion switch
- Data devices using second port of voice devices, i.e. both devices share a common connection
- CXi II is more a server and connects to a larger network infrastructure. The voice and data devices are connected elsewhere within the network. (This is also the connection scenario for the MXe III.)

16.2 When to use VLANs?

VLANs are used to provide a level of logical separation between voice devices and other devices in the network. The main requirement is to ensure that there is adequate priority setting at the various network egress points, and that priority queues are enabled

at these points. Layer 2 priority setting can only be provided in conjunction with VLAN settings.

The simple question to ask is probably, “Will the voice information need to share a common connection with other data?” If it does, then priority schemes are needed at that point, which implies VLANs are needed, at that point. Larger networks will also tend to use VLANs to provide a level of isolation and security between different services. However, the main requirement with voice is to get access to the priority settings and information.

16.3 Network Configurations

The following is a brief description of the different network configurations and whether VLANs are needed.

Standalone CXi II, voice only

This is a self-contained configuration, with only the CXi II unit involved in the network. There are only voice devices connected to the CXi II.

There is only a single device at each egress point of the Layer 2 switch, and so there are no contention issues with data. There are also no data devices, so assigning priority to voice is meaningless, since all voice devices will have equal priority. The network switch internal bandwidth is in excess of the port capabilities, and much higher than the voice devices need to handle. There is unlikely to be any throughput issues.

Connection to an expansion Layer 2 switch is also not an issue. Again the connection bandwidth (Gig Ethernet) is in excess of that needed for the number of voice devices. Again VLAN and priority settings will not provide benefit on this link.

In effect, for this configuration, there is no requirement for VLAN settings.

Physical segregation of voice and data networks

One method to maintain priority between voice and data networks is to operate these as two independent networks. Although this may seem a little counter intuitive, it can be useful in providing demarcation between the different services where different personnel look after different parts of the network. The two networks are then joined at a higher level through a router. The two “networks” would still need to be considered as a single system and IP addresses assigned as appropriate.

From the voice side of the network this is very similar to the standalone case. The main difference is a single connection to a router. This should be taken from the highest hierarchical point in both voice and data networks.

Connection of the router allows various PC devices to gain access to services of the ICP controller (CXi II), if needed. For basic data operation, use of VLANs is unlikely to be needed, since the bandwidth available at the CXi II will be higher than the router connection.

The one exception to VLAN usage might be on the data side of the network where MiCollab Client Softphones are in use. These devices are PC based, but are in effect voice devices. For the MiCollab Client Softphone, it is possible to queue data within the network, based on the value of the DSCP/Type of service field. It may be necessary to implement VLAN within the data section of the network in this case. The standard PC services will then take a VLAN and low priority value. The voice applications will need to map the Type of service field to a VLAN priority, to ensure correct priority queuing. All data from the PC will be in the same VLAN, just voice will have a higher priority marking. The router will remove the VLAN information.

So, in general:

- VLAN is not needed in the voice portion of the network
- VLAN is not needed in the data portion of the network, except when MiCollab Client Softphones are in use.

Standalone CXi II without expansion switch, dedicated voice and data ports

In this configuration, the CXi II controller becomes the network, albeit limited to 16 ports. There are no egress queuing issues since each device, either voice or data, has its own dedicated port. In this situation, the internal switching bandwidth of the internal Layer 2 switch exceeds that from the external ports. There is no need for priority mechanisms, hence no requirement for VLANs.

With this reduced configuration, there is no requirement for VLAN settings.

Expanded CXi II, dedicated voice and data ports

This is similar in configuration to the standalone CXi II with dedicated voice and data ports. The biggest difference is the connection between the CXi II controller and the expansion Layer 2 switch. This link will be shared between voice and data devices. In practice, if the data requirements are low, then there should be sufficient bandwidth to run without priority queuing. However, data demands can vary, and there is a potential for congestion. In this case the voice traffic should be tagged with the higher priority.

The link between the CXi II and expansion Layer 2 switch should have VLAN enabled.

The individual end devices can have VLAN and priority assigned at the ingress point of the network switches, and may use a common VLAN (and subnet). The priority will obviously be different. However, this is a physical implementation and requires ports to be reconfigured every time a device is moved. A general setting can be applied, with the data devices going to the default VLAN and the voice devices being assigned to the voice VLAN, such as through DHCP, or manual settings.

In this case the individual access ports should have VLAN enabled.

Common network connection for both voice and data devices

Where voice and data devices share a common connection to the network, there is a mix of data possible on the connection. On ingress to the network port, the phone will prioritize data. However, on egress, at the far end connection, this will not occur. Priority marking is needed to allow the egress priority to be carried through the network.

For this configuration VLAN should be enabled at access and network device interconnections.

Connection to corporate network

In this case the end devices are likely physically connected to network devices that are remote from the controller, e.g. different floors, separate building, etc. The connections through the network will carry a wide range of information, both data and voice. The controller is likely to be connected to the network at a point normally associated with other server devices. In this case it will be a voice server, be it a group controller, a voice gateway, or combination thereof.

Connections for the end devices, such as the phones, require VLAN to be enabled, at the access points.

For the controllers, or servers, VLAN and priority is also needed. However, this can be configured in different places. The VLAN, and priority, information can be added at the network access point. In this case all information will carry the voice VLAN, but will also carry equal priority for all services. It is also possible to differentiate services and overwrite the VLAN priority by mapping the type of service (Layer 3) priority field into the VLAN priority field. This is sometimes described as ‘TOS to COS’ or ‘DSCP to COS’ conversion.

Alternatively, the VLAN can be added at the server/controller and the network access point configured to accept VLAN information.

Appendix D: VoIP Security 17

This chapter contains the following sections:

17.1 Security Support with Mitel VoIP

A number of devices in the Mitel IP product range now include additional security measures. These include:

- Encryption of voice and signaling payload data
- Network Access Authentication (802.1X)

Encryption is used to “hide” the information that is carried in the payload from unauthorized users and applications.

Network access authentication is a method to restrict connections to the network, or guide the device to particular parts of the network.

17.2 Data Encryption

Encryption hides both the signaling information and the voice streaming. The network connection, or path, remains the same whether the data in the payload is secured or not. Both secure and non-secure devices use the same network paths to establish voice connections. Although quite complex, data encryption involves two main aspects. These are:

- key exchange
- data encryption and decryption

Encryption scrambles the data using the available key information such that it cannot be easily read and decoded by a third party. Only the endpoints have the necessary key information to encode and decode the data correctly. The method used to pass this key information between endpoints is known as the key exchange.

There are a number of standard methods to encrypt data. These are very secure in their coding, and have been field tested over a number of years with critical information

such as financial and personal data. From a user view, all that is important is to know is that the data is secured. The method used to encrypt the data is negotiated by the endpoints. If one or both of the endpoints do not support encryption, the connection may still be established, but will be unsecured. That is, a voice call can still be established with equipment that doesn't support encryption methods.

Bandwidth considerations (voice and signaling encryption)

The secure connection uses data encryption to modify the contents of the payload so that someone collecting data packets will be unable to read the contents. It doesn't modify the contents of the IP header, since this is still needed to pass data over the existing Layer 3 routers and Layer 2 network switches. If the headers were also encrypted, then every router in the path would need to know how to decipher the information.

The data in the payload is intended for a particular application. It is the application that knows how to decode the information. For the Voice over IP application, this payload contains the signaling information or voice streaming.

When the data is encrypted, it is simply replaced with a scrambled version. This is a 1 for 1 transformation, so there are no additional bytes. As a result, the bandwidth is the same for encrypted or non-encrypted information. This is NOT true for Secure RTP (SRTP) which appends either 4 or 10 bytes to the voice payload depending on the cipher mode used. Voice streaming security (SRTP)

For the signaling information, there are some additional messages related to setting up the secure connections. However, these are minimal when compared to the remainder of the signaling bandwidth, which is already quite low. For voice information the bandwidth remains the same for both encrypted and unencrypted payloads.

As an analogy, the encryption can be considered as simply another voice CODEC or an additional process in the voice-streaming path. For voice streaming, G.711 and G.729 CODECs are often used. The encryption merely makes these secure, so the result is a secure-G.711 and a secure-G.729 CODEC. The bit rate remains the same, as does the network bandwidth requirements.

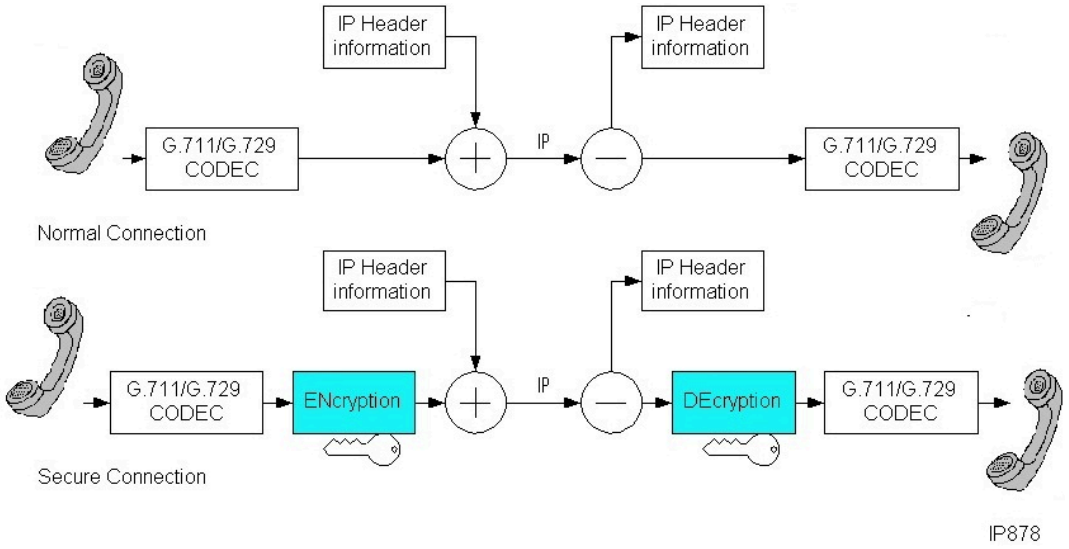


Figure 42: Unsecured vs. Secured Connection

Signaling and media paths

Media and signaling path encryption is supported for all of Mitel's IP phones on the MiVoice Business.

Media path encryption is accomplished with Secure RTP using 128-bit Advanced Encryption Standard (AES). Encryption is backwards compatible to support both currently shipping desktops and previously deployed Mitel IP desktops. Mitel provides encryption of the media path between multiple 3300 ICPs using an Secure Sockets Layer (SSL) protocol. This allows scalability of applications by configuring 3300 ICPs into clusters or deploying them as part of a centrally managed but distributed architecture.

The signaling path is generally between the controller and the IP Phone or other end-device. This path is established as a secure connection. Signaling information is interpreted within the controller. Where a message needs to be sent to another controller, such as with IP-Networking, or to another end device, an independent secure connection is used. Thus a call between two phones on two controllers will require the establishment of three secure signaling channels, that is, a secure connection at each controller and one between the controllers.

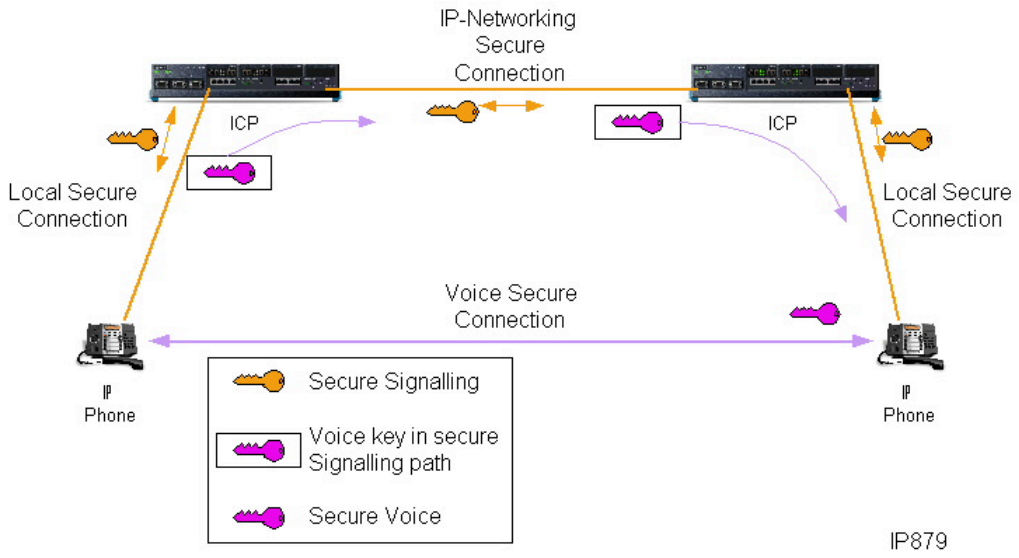


Figure 43: Media and Signalling Path Encryption

The signaling paths with security do not take different network routes compared to those without security. The only difference is that the contents of the payload are encrypted. The only additions for security are messages to establish the point-to-point secure connections and the negotiation of the secure voice connection. Thus the signaling is secured; MiNET becomes Secure-MiNET and MiTAI becomes Secure-MiTAI.

Once the signaling paths are established and a voice connection can be made, the two end devices will negotiate the keys and method of voice encryption. Once agreed, the voice now streams directly between the two devices. This is the same as the unencrypted case, only the voice data is encrypted.

Voice streaming security (SRTP)

Mitel controllers and selected IP sets and applications support RFC 3711 standard Secure RTP. This provides added confidentiality, message authentication and replay protection over the standard RTP protocol. A call will be encrypted, and will use the most secure method if both ends support encryption. Calls initiated on a controller, an IP Phone, or an end device that does not support encryption are still supported, but will not be encrypted.

SRTP will be enabled by default on all X86 systems (EX and servers) as of release MiVB 9.4.

Media (voice) streaming between Mitel sets and controllers will use a version of SRTP with a predefined algorithm (Mitel SRTP), so that negotiation of the secure connection is very quick. Mitel products connecting to third-party equipment must negotiate the key exchange for the security algorithm, and the process will be more processor intensive.

Signaling security

Two main methods are used to secure a signaling channel. These are:

- TLS (Transport Layer Security), both open standards
- Secure MiNET (a Mitel proprietary standard)

Mitel's Secure MiNET protocol uses the Advanced Encryption Standard (AES) to encrypt call control packets. Using secure MiNET ensures that call control signaling packets between the IP phones and the 3300 ICP are protected from eavesdropping. Using secure MiNET also protects the 3300 ICP from unauthorized control packets.

Secure MiNET uses a predefined algorithm to encode the signaling messages. Negotiation of the encryption method is not needed, so this provides a simpler and faster method to establish secure connections with third party applications. Some SIP phones may also use TLS, which is an updated and more open version of the SSL standard. Because the encryption algorithms for SSL and TLS are not predefined as with secure MiNET, the end points must negotiate the security at the time of each connection, and performance may be impacted somewhat. When evaluating the performance of SIP phones with the System Engineering Tool (SET), the default connection will be TLS, which should reflect the actual negotiated selection in most cases. The user of the tool may also select UDP or TCP if it is known that those will be used in the particular installation. Performance adjustments for use with SIP-TLS phones is highlighted in the earlier performance section.

In addition to Secure MiNET, a standard encryption method that uses SSL is also available on certain end devices. SSL is used to negotiate which encryption method to use at the endpoints. This standard allows interaction with third party applications.

As of release MiVB 7.1, a third option for signaling encryption is available between controllers and selected phone set types. The Protected Extensible Authentication Protocol (PEAP) is a protocol that encapsulates the Extensible Authentication Protocol (EAP) within an encrypted and authenticated TLS tunnel.

Mitel 53xx series IP phones are enhanced to support 802.1x with PEAPv0-MSCHAPv2 authentication. The existing EAP- MD5 authentication mode continues to be supported for the purpose of backward compatibility.

- Supported set types are 5360, 5340e, 5330e, 5320e, 5324, 5312, 5304, and 69xx series.
- 5340, 5330 and 5320 do not support PEAP authentication.
- Firmware required is version 6.3.0.12 (released with MiVB 7.1) or higher.
- These sets automatically trust the server certificate for TLS connection.
- The configuration of username and password on these IP sets remains unchanged.

The SSL security protocol provides data encryption, server authentication message integrity, and optional client authentication for a TCP/IP connection. SSL will prevent unauthorized access to administrative functions. SSL encrypts all traffic on the link to prevent sniffing of usernames and passwords.

The IP Phones will determine which secure method to use, first trying SSL, then secure MiNET and then, if neither of these is supported, the call will go unsecured.

The ICP uses multiple IP ports to differentiate these protocols (6800, 6801, 6802) as defined in the IP port information. If the relevant port is blocked with a firewall or a router, for instance, the negotiation may fail and a connection may not be established.

IP Networking communication between ICP controllers and gateways only use SSL or no encryption. MiNET encryption is not supported.

Voice streaming to external gateway PSTN connection

In voice streaming to an external gateway PSTN connection, the voice path is established between the IP Phone and the IP/TDM Gateway. This might be the local ICP, or another unit dedicated to this function and connected via IP Networking. There is no difference in the connection path between secure and non-secure call establishment. Connections will be established as secure where possible.

Voice streaming to TDM connections

Where an ICP has a number of TDM connected devices, calls to these devices will be via local IP/TDM gateway. Encryption applies to the packet part of the connection, and so the IP path to the gateway will be secure, where possible. The connection on the TDM side will continue, as it always has, to use a dedicated connection to the end device.

Voice streaming to internal voice mail, Record a Call and conference

Where there are internal features like voice mail, Record-a-Call or conference at the ICP, these are considered TDM devices. Encryption applies to the packet part of the connection, so the IP path to the gateway will be secure, where possible. The connection on the TDM devices will remain a dedicated connection to the requested service.

A conference call with a number of users requires multiple connections to the IP gateway. Connections between the IP end device and this gateway will be encrypted, where possible. Connections to the conference bridge are established over the internal TDM infrastructure.

PSTN connections or TDM devices connected into this bridge will not use encryption, but will maintain their normal dedicated connections.

Voice streaming to applications

A number of applications and end devices support encryption. There are some, however, that do not support encryption measures. Connections to these devices will be established without encryption. For a list of devices and applications that support encryption, refer to Table #unique_154/unique_154_Connect_42_id203AI0V01J8.

End devices that connect to the external port of theMiVoice Border Gateway (formerly Teleworker solution) are secure, but when similar end devices are used within the LAN environment, they may not be fully secured.

Further details can be found in theMiVoice Border GatewayEngineering Guidelines. TheMiVoice Border Gateway also terminates both internal and external secure connections. This allows for differences in encryption methods; external secure connection and unsecured internal connection.

MiCollab Client provides a softphone with encrypted call path and call signaling and secure instant messaging to keep IM traffic encrypted and inside the network.

The SpectraLink wireless phones and the Mitel WLAN stands may use security on the air access interface (radio link) such as WEP or WPA2. However, this only covers the wireless connection and not necessarily the remaining connection across the remaining network infrastructure.

Worm and virus protection

The 3300 ICP uses an embedded real-time operating system. This system is less susceptible to virus or worm attacks that target is not affected by the viruses and worms typically found on networks and the Internet. This also makes it difficult for an attacker to write a virus targeted at generic VxWorks implementations.

Application servers based on Windows must be properly maintained with current operating system security updates. Mitel products based on Windows include the Contact Center Solutions, Speech Server and Messaging Server systems. These key application servers must be maintained with the latest in Microsoft security updates and worm protection.

Prevention of toll abuse

Any communication system that has a combination of Direct Inward System Access (DISA) integrated auto attendant or RAD groups, and peripheral interfaced auto attendant or voice mail can be susceptible to toll abuse. Therefore it is important to assign appropriate telephone privileges and restrictions to devices. In addition, public telephones should be denied toll access unless authorized through an attendant.

The 3300 ICP system has comprehensive toll control as an integral part of the call control. It lets you restrict user access to trunk routes and/or specific external directory numbers. It also provides Class of Restriction (COR) and Class of Service (COS) features that can substantially reduce the risk of toll abuse.

As a deterrent to toll abuse by internal callers, Station Message Detail Recording (SMDR) can be used to track calls from within your company, providing detailed information such as the originating extension number, time, duration, and number dialed. SMDR record access should be restricted as with any other function.

Secure management interfaces

The 3300 ICP includes a fully integrated set of management tools designed to install, manage, and administer 3300 ICP systems. Three levels of access are provided in order to meet the needs of system technicians, group administrators, and the desktop telephony users themselves. All of these integral management tools use Secure Socket Layer (SSL) security for data encryption. User access to the management tools is controlled by a login and password. Once a user logs into the 3300 ICP, the system displays a menu of the specific tools to which they have been granted access. Mitel also offers the Management Access Point to provide secure remote administration for VPN or dial-up access.

17.3 Dual Port Phones

A number of Mitel's IP phones are dual port, meaning that there are two ethernet ports on the phone. One ethernet port is used to connect to the LAN. The other ethernet port can be used to connect a PC to the network via the phone, this capability is useful in environments where the phone and the PC need to share a single ethernet connection.

COS option is provided that can be used by the System Administrator to disable the second ethernet port on dual port phones, which in turn will bar unauthorized access at the second ethernet port. The default condition is for all second ethernet ports to be enabled; for details on how to set a COS option to disable secondary ethernet ports on IP phones, refer to theSystem Administration Tool Help for MiVoice Business.

17.4 SIP Security

Mitel has a number of phones that support the Session Initiation Protocol (SIP). SIP is a signaling protocol used for establishing and terminating IP phone calls. SIP signaling is not encrypted; however, phones using SIP are authenticated before providing access to system features.

Glossary 18

ACD – Automatic Call Distribution. A package of advanced call processing features, relating to groups of agents who handle calls and agent supervisors.

AMC – Applications Management Center. Used to activate new hardware and software licenses for Mitel products.

ARP – Address Resolution Protocol. Used to identify a MAC address against an IP address.

ARS – Automatic Route Selection. This is a method whereby call control can best determine the path from one controller to another and provide a seamless connection to the user.

ASU – Analog Services Unit. This unit provides a combination of analog ONS interfaces for phones and/or LS trunks.

BRI – Basic Rate Interface. Digital ISDN connection to PSTN or local digital phone. This is the smallest quantity of digital channels that can be delivered, and consists of 2 digital channels for voice and data. Variants include the U interface for North America and S0 in Europe.

Call Control.Software to create connections and paths between end user devices.

CAT 3 – Category 3 Cable. A type of UTP cable for use in a LAN, capable of 16 Mbps. Typically used for voice and data on 10BASE-T Ethernet.

CAT 5 – Category 5 Cable. A type of UTP cable for use in a LAN, capable of 100 Mbps.

CCS – Centum Call Second. A measure of call traffic. One call lasting 100 seconds is referred to as 1CCS.

CDP – Cisco Discovery Protocol. A Cisco proprietary protocol that allows IP devices and L2 switches to communicate with each other for configuration purposes

CEID – Cluster Element ID. A means of identifying different system units to maintain a consistent number plan.

CESID – Customer Emergency Services Identifier. A means of correlating a user and a directory number to information stored in a physical location data base.

CIM – Copper Interface Module. A TDM interface module used to connect the ICP to various peripherals via CAT 5 UTP.

CIR – Committed Information Rate. A means to identify how much information MUST be carried in a connection, e.g. CIR = 64 kbps for voice.

CODEC – COder and DECcoder. Coder and decoder commonly used as a single function. A means to convert analog speech into digital PCM and vice versa.

Controller. Control element of ICP (see also RTC).

COS – Class of Service. This refers to the priority value in the Layer 2 part of an IP packet when IEEE 802.1p is used.

CPH – Calls Per Hour. For example, 6 CPH means 6 calls per hour.

CSM – Customer Service Manager.Former name for MiContact Center Office, an entry level contact center solution hosted on MiCollab for basic contact centers or workgroups with up to 100 agents.

CSMA/CD – Carrier Sense Multiple Access Collision Detect.The mechanism used on shared Ethernet connections to ensure that devices are not sending at the same time, and if they are, to initiate a back-off and retry algorithm.

CTI – Computer Telephony Integration. Means of combining computer functions to control operation of telephony equipment.

Datagram –A logical grouping of information sent as a network layer unit over a transmission medium without prior establishment of a virtual circuit. IP datagrams are the primary information units in the Internet. The terms “frame”, “message” and “packet” are also used to describe a datagram.

DECT – Digital Enhanced Cordless Telephony. Originally this was a European standard for digital cordless phones. This is now a worldwide standard, hence, the name change to Enhanced. Standard DECT phones are not available in North America.

DHCP – Dynamic Host Configuration Protocol. A means of passing out IP addresses in a controlled manner from a central point/server.

DiffServ – Differentiated Services. DiffServ is a protocol for specifying and controlling network traffic by class so that certain types of traffic get precedence. For example, voice traffic, which requires a relatively uninterrupted flow of data, might get precedence over other kinds of traffic. Differentiated Services is the most advanced method for managing traffic in WAN connections. This uses the Type of Service field at Layer 3 in an IP packet. See also DSCP.

DN – Directory Number. A telephone or extension number.

DNS – Domain Name Server. A means of translating between typed names and actual IP addresses, e.g. microsoft.com = 207.46.134.222

DPNSS – Digital Private Network Signaling System. A British common channel signaling protocol for requesting or providing services from/to another PBX.

DSCP – Differentiated Services Code Point. This is a value that is assigned to the Type of Service byte in each outgoing packet. The value can be in the range of 0 to 63 and allows

routers at Layer 3 to direct the data to an appropriate queue. Value 46 is recommended for voice and will use the Expedited Forwarding queue or Class of Service.

DSP – Digital Signal Processor.This is a programmable device that can manipulate signals, such as audio, to generate and detect a range of signals, for example, DTMF signaling.

DSU – Digital Service Unit. A peripheral which provides digital ports for the ICP.

DTMF – Dual Tone Multi-Frequency. In-voice-band tones used by telephones to signal a particular dialed digit. Also known as touch tone.

E – Erlang. A measure of usage of a resource, e.g. 0.75e = 75%. 1 e = 36 CCS.

E1 –Primary Rate running at 2.048 Mbps providing 30 channels of voice of PCM.

E2T – Ethernet to TDM. This is the conversion of voice streaming between TDM and IP.

E911 – Enhanced 911 (Emergency Services). Also 999 (UK) and 112 (International).

eMOH – Embedded Music On Hold.

ESM – Embedded System Management. Means to program a system from the System Administration Tool, Group Administration Tool, or Desktop Tool.

FAX – Facsimile. A means of transmitting printed text or picture information with acoustic tones

FIM – Fiber Interface Module. A fibre optic TDM interface module used to connect the ICP to various peripherals.

FTP – File Transfer Protocol. An electronic method to transfer file information.

G.711 –PCM Voice Streaming. ITU standard for conversion of voice-streaming to digital PCM (64 kbps).

G.729 –Voice Streaming CODEC. Reduced bit rate from G.711 (8 kbit/s)

Gateway –A path between different media streaming technologies, in this case between TDM and IP.

Group Controller –The call control of the ICP is in control of a number of units, where the functions are more dedicated, e.g. to a separate gateway

GRP – Gateway Routing Protocol. A generic term which refers to routing protocols.

HSRP – Hot Standby Routing Protocol. A Cisco proprietary protocol used to increase availability of default gateways used by end hosts.

ICMP – Internet Control Message Protocol. Messages to help identify when devices are present and create warnings when they fail.

ICP – IP Communications Platform. Includes gateway function, call control, plus a number of other features, such as voice mail.

IP Address – Internet protocol address. A 32-bit address assigned to hosts using TCP/IP. An IP address belongs to one of five classes (A, B, C, D, or E) and is written as 4 octets separated by periods (dotted decimal format). Each address consists of a network number, an optional subnetwork number, and a host number. The network and subnetwork numbers together are used for routing, while the host number is used to address an individual host within the network or subnetwork.

IP – Internet Protocol. An encapsulation protocol that allows data to be passed from one end user to another. Typically this was over the Internet, but the same protocol is now used within businesses.

IrDA – Infrared Data Association. The IrDA is an industry-sponsored organization set up in 1993 to create international standards for the hardware and software used in infrared communication links. Infrared radiation (IR) is the same technology used to control a TV set with a remote control.

IRDP – ICMP Router Discovery Protocol. An extension to the ICMP protocol that provides a method for hosts to discover routers and a method for routers to advertise their existence to hosts.

ISDN – Integrated Services Digital Network. The digital PSTN network. Integrated because this network carries both voice and data and provides direct digital connectivity to the user via BRI or PRI connections.

ISL – Inter-Switch Link. Cisco-proprietary protocol that maintains VLAN information as traffic flows between switches and routers.

L2 – Layer 2. The second layer of encapsulation of data to be transferred. Typically with TCP/IP this includes the MAC layer.

L3 – Layer 3.The third layer of encapsulation of data to be transferred. Typically with TCP/IP this includes the IP address.

LAN – Local Area Network. This is a network within a local area, typically within a radius of 100 m. The transmission protocol is typically Ethernet II.

Leased IP –An IP address that has been assigned through DHCP and is valid only for the duration of the agreed lease time.

LLDP – Link Layer Discovery Protocol.A low level protocol used to pass information about the connection configuration between two end devices, for example VLAN. Typically this would be between an end device such as a PC or IP phone and the network access port on the Layer 2 switch.

LLDP-MED – Link Layer Discovery Protocol - Media End-point Discovery.LLDP-MED is an extension of LLDP that provides auto-configuration and exchange of media-related

information such as Voice VLAN and QoS. It is designed to provide enhanced VoIP deployment and management.

LS – Loop Start. This is a particular analog trunk protocol for signaling incoming and outgoing calls.

MAC – Media Access Controller. This is the hardware interface that data (media) travels through. Typically this will be assigned a world-wide unique address.

MAN – Metropolitan Area Network. This is a larger network that may connect a number of LANs within a business, as well as a number of businesses. Typically, this would cover a city area, and use fibre optics to get maximum bandwidth.

Mbps – MegaBits Per Second.Million bits per second is a measure of bandwidth on a telecommunications medium. May also be written as Mbits/s or Mb/s. Mbps is not to be confused with MBps (megabytes per second).

MFRD – Mitel Feature Resources Dimensions. This is a definition of the number of features that can be used on a particular unit.

MHz – Mega Hertz. Frequency measurement.

MiNet – Mitel Network Protocol. This is Mitel's proprietary stimulus-based protocol that is used to signal between phones and controllers, for example key and display information.

MiTAI – Mitel Telephony Application Interface. This Mitel implementation of TAPI is used to connect to external applications, e.g. ACD controllers.

Mitel OIG – Mitel Open Integration Gateway.

MODEM – MOdulator-DEModulator. Device that converts digital and analog signals. At the source, a modem converts digital signals to a form suitable for transmission over analog communication facilities. At the destination, the analog signals are returned to their digital form. Modems allow data to be transmitted over voice-grade telephone lines.

MOH – Music on Hold.

MSW – Mitel Sales Workbench.

MTBF – Mean Time Between Failures. The statistical time between expected component failures.

MTU – Maximum Transmission Unit. An MTU is the largest size packet or frame, specified in octets (eight-bit bytes), that can be sent in a packet- or frame-based network, such as the Internet.

MWI – Message Waiting Indicator. A visual indicator in a telephone that indicates to the user that a message is waiting.

NAT – Network Address Translation. A means of translating internal IP addresses to a defined limited range of internet IP addresses. The benefit is the ability to use a limited range of internet addresses and map these to a much larger internal range.

NIC – Network Interface Card. Physical connection to the network. In a PC, this is often a plug-in card.

NSU – Network Services Unit. This interface connects between the PSTN Primary Rate trunks and the ICP.

ONS – On-Premise Line. This is a two-wire analog telephony interface, within an office environment, and not passed outside.

OPS – Off-Premise Line. This is a two-wire analog telephony interface, typically installed external to a building, e.g. external shed or guard house.

OSPF – Open Shortest Path First. A link-state routing protocol used for routing IP traffic over the most cost-efficient route.

PC – Personal Computer.

PCM – Pulse Code Modulation. The digital representation of analog signals.

PDA – Personal Digital Assistant. A handheld personal organizer that can interface to a PC or a Mitel PDA Phone.

Permanent IP –An IP address that has been leased (from DHCP) on a permanent basis.

PI – Performance Index. A calculation of the performance limits of a system. Different weighting values are assigned to various types of calls. Based on the expected calls per hour (CPH) of all of the user ports on the system, a system performance index (PI) can be calculated. The system PI is used as an indication of how much traffic the 3300 ICP can handle at any one time.

Ping –This is a means of sending a test message and waiting for a reply to determine if a network device is reachable. On a PC, this is invoked with the command ping.

PPM – Parts Per Million. This is a measurement of accuracy, or the expected error in one million events. Therefore 1 ppm means that 999,999 to 1,000,0001 events occurred when 1,000,000 were expected. This is 0.0001% error. For example, a household clock that is 1 second accurate per day is 11.5 ppm, or would need to be 0.086 seconds incorrect per day to be 1 ppm.

PRI – Primary Rate Interface. This is a connection to the PSTN where a number of trunk channels are multiplexed onto a common connection. Both T1 and E1 variants are available.

PSTN – Public Switched Telephone Network. The telephone network that provides local and long distance connections, e.g. Bell, AT&T, BT.

PTT – Poste, Telefonie, Telegrafie. PSTN services. Often countries combine postal services and telephony under a common service provider, e.g. the government.

RAD – Recorded Announcement Device.

RAID –Redundant Array of Independent Disks. Array of hard drives on which the information is duplicated. A controller manages the disks, switching automatically from the primary to the secondary in the event of the failure of the primary hard drive.

RDN – Remote Directory Number. The Remote DN Table is used to identify alternate ICPs to check for availability of devices, and to determine if a device is located on the Primary or Secondary ICP.

RFC – Request For Comments. A document that is created, maintained and distributed by the Internet Engineering Task Force. An RFC is the vehicle that is used to discuss and evolve a networking related protocol. RFCs usually get approved and issued as standards.

RFP – Radio Fixed Parts. The Radio Fixed Parts (RFPs) connect to the 3300 ICP through the LAN. The wireless phones communicate with the RFPs using standard Digital Enhanced Cordless Telecommunications (DECT) protocol.

RGP – Router Gateway Protocol. A means whereby routers on a common subnet can communicate with and identify each other. Useful when ICMP Re-direct is needed to identify an alternative path.

RIP – Routing Information Protocol. A networking protocol that maintains a database of network hosts and routers and exchanges information about the topology of the network.

RSTP – Rapid Spanning Tree Protocol. A version of STP that will converge networks more rapidly than STP (see STP).

RTC –Real Time Complex. This is the control block within an ICP. This includes Call Control and internal controls for the unit.

RTP – Real Time Protocol. Protocol used to identify sequence of voice packets with timing information before being sent to a user via UDP.

SAC – Switch Application Communications

SET –System Engineering Tool. Used for calculating system parameters, limits and allowable additions.

SIP – Session Initiation Protocol. An IETF standard for signaling over IP.

SME – Small to Medium Enterprise. A small- to medium-sized business.

Static IP –An IP address that has been manually assigned and fixed. Typically, static addresses are exceptions within DHCP.

STP – Spanning Tree Protocol. A means whereby the network can determine multiple paths between two points and disconnect them to leave a single path, removing broadcast issues.

Subnet –A subnet (short for “subnetwork”) is an identifiably separate part of an organization's network. Typically, a subnet may represent all the machines at one geographic location, in one building, or on the same local area network (LAN).

SWB – Mitel Sales Workbench.

T.37 –Internet Protocol for FAX (Store and Forward). A means of taking a TDM FAX, converting it to data, passing it via IP and reconverting it back to TDM.

T.38 –Internet Protocol for FAX (Real Time). Similar to T.37 in function, but carried out in real time, i.e. with minimum delay.

T1 –Primary Rate. Provides 23 or 24 channels of trunks per connection.

TAPI – Telephony Applications Programming Interface. TAPI is a standard programming interface that lets you and your computer communicate over telephones or video phones to people or phone-connected resources.

TAR – Tape Archive and Retrieval. A file transfer utility.

TCP – Transmission Control Protocol. The methods of transmitting data between two end-points using IP with acknowledgement.

TDM – Time Division Multiplex. A means of combining a number of digitally encoded data or voice channels onto a common digital stream, e.g. T1.

TFTP – Trivial File Transfer Protocol. A simplified version of FTP used to transfer data with minimal overhead.

TOS – Type of Service. A field within the Layer 3 (IP) encapsulation layer to identify some properties relating to service parameters; in this case, delay and priority of handling.

UCA – Unified Communicator Advanced. Fomer name for MiCollab Client, a PC-based office management application, MiCollab Client Softphone is an enhanced version of MiCollab Client that includes a PC-based phone.

UDP – User Datagram Protocol. A layer 4 protocol with minimal handshaking and overhead. Used to stream voice. Considered connectionless.

Unicast –A process of transmitting messages from one source to one destination, as opposed to a broadcast or multicast.

UPS – Uninterruptible Power Supply. A unit capable of providing output power for a period of time when the local mains supply fails. Usually relies on storage devices such as batteries.

UTP – Unshielded Twisted Pair. Cable that reduces emissions and maintains an impedance match through the twists per metre in the cable without resorting to shielding.

VLAN – Virtual LAN. A means of providing virtual LANs on a network using common physical components. Such VLANs are logically unconnected except through some Layer 3 device.

VM – Voice Mail.

WAN – Wide Area Network. A network connection to a network that could be global, e.g. via Frame Relay.

Wi-Fi – Wi-Fi Alliance technology for Wireless LAN based on IEEE 802.11.

WLAN – Wireless LAN.

WAV – WAVe file. Wav is an audio file format, created by Microsoft, that has become a standard PC audio file format for everything from system and game sounds to CD-quality audio. A Wave file is identified by a file name extension of .wav.