MiVoice Conference and Video Phone

MARCH 2016

Release 2.1, SP5

ENGINEERING GUIDELINES

NOTICE

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.

TRADEMARKS

Mitel's Power Over Ethernet (PoE) Powered Device (PD) products are covered by one or more of the U.S. patents (and any foreign patent counterparts thereto) identified at Mitel's website: www.mitel.com/patents

For more information on the PD patents that are licensed, please refer to www.cmspatents.com

MiVoice™ Conference/Video Phone
Engineering Guidelines
Release 2.1, SP5

March 2016

List of Tables

List of Figures

About this Document

Overview

This document provides engineering guidelines for the MiVoice™ Conference Phone and MiVoice Video Phone.

These guidelines include information about IP networking requirements, WAN requirements and installation recommendations.

New in Release 2.1, SP5

- Support for the import of contacts from MiVoice Business and MiVoice Office 250 in formatted CSV files. These files can be imported from either USB flash drive or from the HTTP configuration server. See Contacts Settings.
- Support for WV-SPN311 camera. See Ethernet Camera Firmware.
- Support for OfficeWRX™ — replaced Smart Office 2.

New in Release 2.1, SP4

- Software fixes only.

New in Release 2.1, SP3

- Support for the Panasonic WV SPN310 camera
- A new option "Trust All HTTPS Servers" in **Upgrade System Software** setting. You can enter https:// in the HTTP Server Address.
- Ability to upgrade a MiVoice Conference Phone to a MiVoice Video Phone by applying a purchased license file.

- Support for a NTP configurable server.
- Swedish language support.
- Mitel Redirection and Configuration Service (RCS) for auto-configuration of the MiVoice Conference/Video phone.
- New Mitel product branding, which includes an updated Mitel logo and MiCollab icon.

For more details, refer to the *MiVoice Conference/Video Phone Administration Guide*.

New in Release 2.1, SP2

As of Release 2.1, SP2, the Mitel UC360 Collaboration Point has been rebranded and is referred to as the MiVoice Conference Phone or MiVoice Video Phone. In this document, it is referred to as the Conference/Video Phone, and shortened to phone in some cases.

Any references in early releases still retain the original name of UC360.

Conference/Video Phone Documentation

Knowing Which Document to Consult

General Audience

- MiVoice Conference Phone and MiVoice Video Phone Product Bulletins
- MiVoice Conference Phone and MiVoice Video Phone Interoperability Update Product Bulletin

Administrators and Installers

- MiVoice Conference/Video Phone Installation Guide
- Multi-Port GigE PoE Switch Installation Guide
- MiVoice Conference/Video Phone Universal Camera Mounting Bracket Installation Guide
- Revolabs Dual Channel System Microphones Installation Guide
- MiVoice Conference/Video Phone User Guide
- MiVoice Conference/Video Phone Administration Guide

End Users

- MiVoice Conference/Video Phone User Guide
- MiVoice Conference/Video Phone Quick Reference Guide

Accessing Documentation, Release Notes, Articles, and Downloads

Documents and Help Files

To access phone- and system-specific documentation:

1. Log in to Mitel Connect.
2. Click **Mitel Online**.
3. Point to **Support** and then click **Product Documentation**.
4. In the right panel, select **Product Documentation**.
5. Point to **Conferencing and Collaboration > MiVoice Conference/Video Phones.**
6. To view a document, click on the document title.

Related Documentation

- **Mitel MiVoice Business Engineering Guidelines** – this guide provides guidelines for installing the 3300 IP Communications Platform.
- **MiVoice Conference/Video Phone Installation Guide** – this guide provides instructions on how to physically connect the Conference Phone or the Video Phone.
- **MiVoice Conference/Video Phone Universal Camera Mounting Bracket Installation Guide** – this guide provides procedures on how to attach the camera to the mounting bracket and display monitor.
- **Revolabs Dual Channel System Microphones Installation Guide** – this guide provides instructions on how to install the Revolabs HD Single/Dual Channel Wireless Microphone system. It also provides guidelines on charging, placing, and using the extension microphones on the MiVoice Conference/Video Phone.
- **Multi-Port GigE PoE Switch Installation Guide –** this guide provides instructions on how to install the Multi-Port GigE Switch in a MiVoice Conference/Video Phone configuration.
- **MiVoice Conference/Video Phone Quick Reference** – this guide provides basic procedures on how to make conference calls, handle calls, and do in-room and remote presentations.
- **MiVoice Conference/Video Phone User Guide** – this guide provides a general description of the Conference/Video Phone and user procedures.
- **MiVoice Conference/Video Phone Administration Guide** – this guide provides detailed information on configuring the Conference/Video Phone. Detailed information is also included for programming the MiVoice Business and 5000 CP for the Conference/Video Phone.

Device Overview

The MiVoice Conference/Video Phone is an all-in-one multimedia collaboration appliance that provides multi-party audio and video conferencing, in-room presentation display, and remote collaboration for personal office meeting areas and conference rooms.

The Conference/Video Phone provides users with a high quality collaboration experience approaching the type of experience offered by high-end telecollaboration solutions but at a cost approaching that of an audio-only conference phone.

Note: In this document, Conference/Video Phone is shortened to phone in most cases.

Supported Countries

The phone can be configured by the installer to generate country-specific call progress tones. Tone plans for the following counties and/or regions are supported.

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

In some cases, the phone 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 most suitable tone plan.

Conference/Video Phone Features

The Conference/Video Phone is a Collaboration Hub, an all-in-one conference room and executive office solution that provides superior audio conferencing capabilities. The phone provides:

- A built in high resolution 7” color touch screen display.
- Built-in presentation display capability via an HDMI interface that supports a connection to high definition LCD display or projector.
- Superior audio conferencing capability including a beam forming microphone array of 16 microphones.
- Support for 7 kHz wideband telecom audio.
- Built-in MS Office readers and editors.
- Access to the Browser to open email through Gmail and Outlook Web Access, and display web-based content.
- Access to join.me™ to use a simple screen sharing tool to share your desktop.
- Remote desktop access (no need to bring laptop to give a presentation).
- Support for multiple file transfer methods, including USB Flash Drive, SD Card, Google® Docs.
- Audio conferences for up to four parties.
- High Definition video conferencing for up to four parties with an integrated conference bridge.
- Support for integration with Active Directory and LDAP.
- Ability to display Remote Presentations.
- Ability to launch Mitel MiCollab Conference and BluStar clients.

Product Variants

Mitel offers two products variants:

- MiVoice Conference Phone
- MiVoice Video Phone

Each variant has its own customer orderable part number. Both variants use the same hardware and software; however, product functionality for the two variants is different.

You can identify the variant by either the product part number or by looking at the main screen on the phone. You will see one of two options:

- Audio Enabled Conferencing
- Video Enabled Conferencing

These options are described below. These product names appear in the **About** information in order to differentiate the product variants.

- The MiVoice Conference Phone is an Audio Conference Bridge with In-room Collaboration, Part Number 50006580
- The MiVoice Video Phone is a Video Conference Bridge with Remote Collaboration, Part Number 50006591

For more details, refer to the *MiVoice Conference/Video Phone User Guide*.

The MiVoice Conference Phone can be upgraded to a MiVoice Video Phone by applying a purchased license file. For details on the upgrade procedure, refer to the *MiVoice Conference/Video Phone Administration Guide*.

MiVoice Conference Phone

The Conference Phone provides audio conferencing with local presentation capability.

It supports audio conferences with a maximum of four parties natively within the Conference Phone (that is, the Conference Phone plus three external participants) plus the ability to set up an additional private call with an external party.

It should be noted that one of these external participants could be a link into another conference bridge (like AWC or AMC), that allows many parties to be audio conferenced together.

MiVoice Video Phone

The Video Phone provides the same functionality as the Conference Phone while also enabling remote presentation and multi-party video conferencing functionality.

This variant supports video conferences with a maximum of four parties natively within the Video Phone (that is, the Video Phone, plus three external participants).

It should be noted that one of these external participants could be a link into another video conference bridge.

When a Video Phone is connected to another Video Phone, presentation sharing capabilities are supported even if the far end and near end Video Phones do not have network cameras.

Installation Checklist

The following installation checklists give an overview of the phone installation process. These checklists also direct you to the applicable section in this guide and/or the *MiVoice Conference/Video Phone Administration Guide* for more details.

What You Received

Unpack the phone and verify that you have received the following:

- A MiVoice Conference Phone or a MiVoice Video Phone
- Standard 7' CAT5e cable
- Security plate kit (containing two screws, mounting plate, and tie wrap)

See the *MiVoice Conference/Video Phone Installation Guide* for more details.

Preparation for Installation

- Ensure that you received the correct variant of the phone – see Product Variants
- Determine the networking bandwidth requirements for the LAN and WAN to support the video conferencing solution. Verify that the Customer and/or the IT department are aware of these requirements.

Additional Items You Need for Installation

You will need to procure the following items listed in the table below.

Item	For More Information, see …
HDMI Display	High Definition Multimedia Interface Displays
Ethernet Camera	Ethernet Cameras
Ethernet Camera Mounting Bracket	*Camera Mounting Bracket Installation Guide*
Extension Microphones	*Revolabs Dual Channel System Microphones Installation Guide*
AC Power Bar	High Definition Multimedia Interface Displays
Appropriate HDMI Cable	HDMI Interface Cable Information
Keyboard and Mouse	Keyboards and Mouse
MiVoice Conference/Video Phone License for the MiVoice Business or Third-Party License for Third-Party SIP Server	Conference/Video Phone Licensing
For power and data connectivity, you will need one of the following options:	
Mitel Multi-Port GigE PoE Ethernet Switch, Part Number 51301282	Mitel Multi-Port GigE PoE Ethernet Switch
Mitel In-Line IEEE 802.3at power adapter, Part Number 51301339	In-Line PoE Power Adapter
Customer provided connection will be suitable if an acceptable Access L2 switch is available on the LAN and there are sufficient ethernet connections available in the installation room	Consult with the customer or the customer's IT department

Initial Setup

- Verify that the room or office in which the Conference/Video Phone is to be installed meets recommendations – see Conference Room and Office Recommendations.
- Ensure that the LAN has adequate bandwidth – see Video Bandwidth Requirements.
- Ensure that the WAN has adequate bandwidth and that appropriate Service Level Agreements are in place – see Video Bandwidth Requirements and WAN Guidelines.
- Ensure that networking switches and routers will honor the Conference/Video Phone QoS settings – refer to IP Network Configuration for the and discuss these requirements with the System Administrator.
- Decide how the phone will be powered – see Phone Powering Options.
- Decide how the phone and the camera will be connected to the network – refer to LAN Connection Guidelines.

Install Hardware

Hardware	For more information, see …
Install the HDMI Display	High Definition Multimedia Interface Displays
Ensure the HDMI Display is grounded as per recommendations	High Definition Multimedia Interface Displays
Install the Ethernet Camera and Camera Mounting Bracket	Ethernet Cameras *MiVoice Conference/Video Phone Camera Mounting Bracket Installation Guide*
Connect the phone to the camera and HDMI	*MiVoice Conference/Video Phone Installation Guide*
Ensure the guidelines for routing the Ethernet and HDMI cables have been observed	HDMI Cable Routing

Preparation for Phone Configuration

- Confirm that the phone, the camera, the MiVoice Business, and if required, the MBG meet the minimum software requirements.
- If using a DHCP server, ensure that it is configured correctly.
- If not configuring statically, DHCP can be configured through the Redirection and Configuration Service (RCS). See the *MiVoice Conference/Video Phone Administration Guide* and the *Redirection and Configuration Service (RCS) User Guide* for more information.
- If using a DNS server, ensure that it is configured correctly.
- If using a third party SIP Server, ensure that the SIP server meets the minimum software requirements.
- If using a third party SIP Server, ensure that it is configured correctly.

Configure the Phone, MiVoice Business, and SIP Servers

Item	For more information, see …
Configure the phone	*MiVoice Conference/Video Phone Administration Guide – Conference/Video Phone Configuration* Network Settings Menu
Configure the Ethernet Camera's networking parameters	*MiVoice Conference/Video Phone Administration Guide – Conference/Video Phone Configuration* Camera Settings Menu
Configure the MiVoice Business	*MiVoice Conference/Video Phone Administration Guide – MiVoice Business Configuration*
Configure SIP Servers (if applicable)	Deployment with SIP Servers and End Points *SIP Reference Guide 08-5159-00014_x*
Ensure that the phone can obtain the required network policy information (VLAN and QoS policy), via DHCP or by another approved method	Conference/Video Phone Quality of Service Settings VLAN/QoS Discovery Mechanisms
Verify that the phone and the camera have obtained the required networking policy	VLAN/QoS Discovery Mechanisms

WAN Connection

If the phone is going to be used to connect to another end point via a WAN connection, ensure the following:

- That the WAN connection has adequate bandwidth.
- That the network routers on both ends of the WAN will honor the phone QoS settings.
- That the network router queues are correctly configured on both ends of the WAN.
- Ensure that an appropriate SLA is in place with the WAN network provider.
- If more than one WAN network provider is involved, ensure that all SLAs are aligned.
- Ensure that firewalls are configured so that the phone can traverse the firewall.

See IP Network Configuration for the more information.

> **Note:** If more than four phones are being deployed at the Customer site, ensure that the Customer is aware that a Calendar/Resource Booking Tool should be used to manage LAN and WAN bandwidth resources.

For more information, see Multiple Four-Party Conferences.

Teleworker Connection

If the phone is going to be deployed as a Teleworker end point, ensure that the phone and MBG are correctly configured.

For more information, see Teleworker and MiVoice Border Gateway Deployments.

Resilient Operation

If phone resilient operation is a requirement, ensure that the phone is registered with two MiVoice Business' or SIP Servers. Also, ensure that the DNS Server(s) and the DHCP Server are configured correctly.

If the phone is being deployed as a resilient end point, then correct resilient operation should be verified by either disabling the connection to the primary MiVoice Business/SIP Server or by powering down the MiVoice Business/SIP Server and observing that the behavior is as expected.

For more information, see Maintaining Availability.

Test Audio and Video Quality and Connections

Action/Test	For more information, see …
Put the phone into local preview mode and verify that the camera position, field of view, and room lighting are acceptable and make any required adjustments	*MiVoice Conference/Video Phone User Guide – Preparing for a Video Call*
Initiate a two-party video conference call and verify that both audio and video quality are acceptable to both parties	*MiVoice Conference/Video Phone User Guide – Making an Audio or Video Conference Call*
Initiate a three-party video conference call and verify that both audio and video quality are acceptable to all parties	*MiVoice Conference/Video Phone User Guide – Making an Audio or Video Conference Call*
Initiate a four-party video conference call and verify that both audio and video quality are acceptable to all parties	*MiVoice Conference/Video Phone User Guide – Making an Audio or Video Conference Call*

Emergency Calls

Ensure that recommendations regarding emergency (911/999) calls have been observed. See *MiVoice Conference/Video Phone User Guide – Emergency Calls* and Emergency Services and Contacts Settings in this guide.

Peripheral Devices

Depending on the application, the phone may be interfaced to a number of peripheral devices such as HDMI displays, HDMI projectors, video cameras, keyboards and mice. This section discusses these peripherals.

High Definition Multimedia Interface Displays

The phone has a High Definition Multimedia Display (HDMI) Type ‘A’ interface that allows the phone to be connected to HDMI flat panel display or an HDMI projector.The phone supports wide screen displays and projectors with resolutions of up to WUXGA
(1920 x1080p).

Some HDMI monitors utilize ungrounded (2-prong) AC power cords; these types of displays may have electrical noise present on their HDMI connector. When present, this electrical noise will be conducted onto the HDMI cable.

This noise can create issues with connected devices, including the phone. These issues may include erratic touch screen behavior on the phone, or in some cases, failure for the phone to power up correctly if the HDMI monitor is already powered on. For optimal performance, it is recommended to utilize HDMI monitors that employ grounded (3-prong) AC power cords.

If the above issues are encountered with a monitor that utilizes a 2-prong power cord, try grounding the monitor to resolve the issue. A simple method for grounding a monitor is to utilize a power bar with integrated surge-protection devices.

- Select a power bar from a reputable manufacturer, such as Belkin or Levition that incorporates surge-protection for coax cables.
- Connect a coax cable from the power bar’s coax cable (F) connector to the coax (F) connector located on the back of the HDMI monitor.
- Plug the power bar into a grounded AC outlet and the monitor is now grounded.

It is recommended that when selecting an HDMI display, it should be a model that allows the user to turn off or disable any 'overscan' capabilities. The option to disable 'overscan' is usually found under the 'Picture' or 'Aspect ratio' menus.

When the phone is used with an HDMI monitor that is set to 'overscan', the top, bottom and the sides of the displayed image will be cropped off.

Some manufacturers may offer an alternate way of disabling 'overscan' or they may refer to 'overscan' by a different name. Some manufacturers may refer to overscan as 'zoom'. It should also be noted that selecting an aspect ratio of 16:9 will cause the display to overscan. To disable overscan some manufacturers have you select 'screen fit, 'just scan', 'no overscan' or 'no zoom'.

> **Note:** It is recommended that the HDMI display or projector that is to be used with the phone be of a type that employs a grounded AC power cord. In North America this power cord is referred to as a ‘3-prong grounded plug’ or a NEMA 5-15-P. In regions other than North America, different designations are used to describe grounded AC power cords.
>
> If the local electrical regulations allow for the use of dedicated AC mains outlets, then it is recommended that the HDMI display or projector be powered from a dedicated AC mains outlet. For details consult a qualified electrician.

Note: It is recommended that the HDMI source be turned off before attaching the HDMI cable to the MiVoice Video phone.

Conference/Video Phone HDMI Capabilities

The phone supports the following HDMI capabilities and features:

- 1080p @60hz or
- 720p @60hz
- For best picture quality, use the 1080p setting.

HDMI Versions Supported

The phone HDMI interface is compliant with HDMI Version 1.4a.

HDMI Interface Cable Recommendations

To complete the connection to the HDMI display, the installer will need to purchase an appropriate HDMI cable.

The cable should meet the following requirements:

- The cable should be an HDMI Category 2 or High Speed cable.
- One end should be terminated with a Type ‘A’ male connector so that it can connect with the phone.
- One end should be terminated with a connector type that is compatible with the customer’s HDMI display, typically this will be a Type ‘A’ male connector.
- The overall length of cable from phone to the HDMI display should be kept as short as possible. The generally accepted industry rule is that the overall cable length should be kept as short as possible and should not exceed 15 m. Distances beyond 15 m will require an HDMI repeater.

HDMI monitors may provide an HDMI interface connector and also a combined HDMI/dvi interface connector. It is recommended that the phone only be connected to an HDMI interface connector.

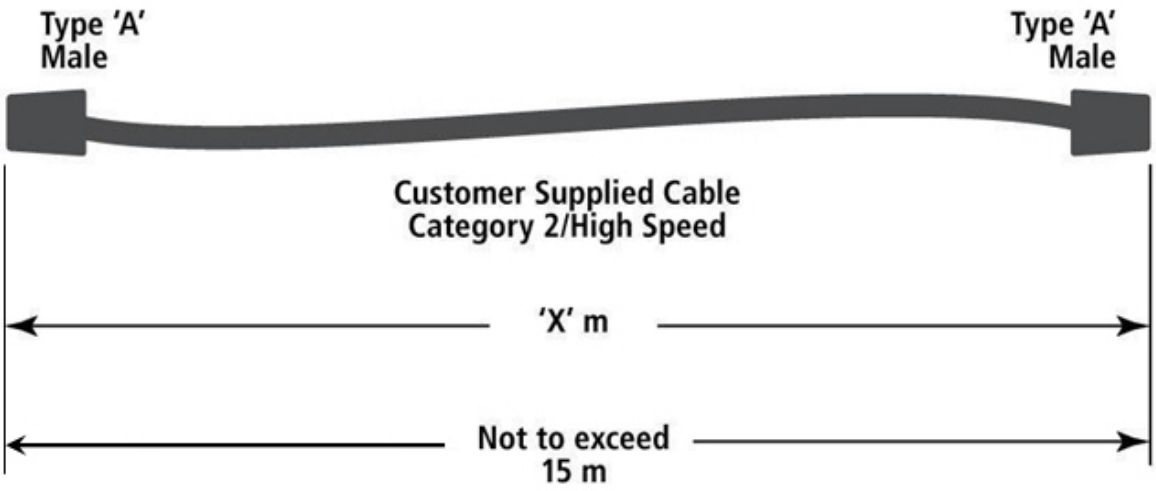

Figure 1 HDMI Cabling

HDMI Cable Routing

The signals carried by the HDMI cable are susceptible to Radio Frequency (RF) and electrical noise. As a result, care should be exercised when routing the HDMI cable between the phone and the HDMI Display or projector.

In general, the HDMI cable should not be routed in close proximity to mains power cables, fluorescent lights or Wi-Fi Access Points.

HDMI Interface Cable Information

The HDMI specifications do not specify a maximum length for HDMI cables; however, signal attenuation which is dependant on the cable construction and quality will limit the useable length of a particular cable.

The HDMI 1.4 specification specifies a number of different cable types. However, only two cable types are applicable to video conferencing applications:

- Category 1 cables

  Category 1 cables are also called Standard HDMI cables. These cables are designed to support display resolutions of up to 720p.

- Category 2 cables

  Category 2 cables are also called High Speed HDMI cables. These cables are designed to support display resolutions of 1080p.

The installer must use a high quality Category 2 cable (or High Speed HDMI cable) to connect the phone to the HDMI display.

Further information on HDMI cables can be found at:

http://www.hdmi.org/

> **Note:** The use of sub-standard HDMI cables or the use of HDMI cables that are too long may result in degraded video being displayed on the HDMI screen.

Video degradation can appear as random sparkles or snow. This is occurring because some pixels in the image are being displayed as white. Excessive video degradation over an HDMI cable can result in no image whatsoever being displayed.

For further information refer to Troubleshooting Video Quality Problems.

HDMI Interface Connector Pin Assignments

The following Table shows the pin assignments for the phone HDMI connector.

Table 1. HDMI Connector Pin Assignments

Pin #	Signal Name	Description
Pin 1	TMDS Data2+	
Pin 2	TMDS Data2 Shield	Ground
Pin 3	TMDS Data2–	
Pin 4	TMDS Data1+	
Pin 5	TMDS Data1 Shield	Ground
Pin 6	TMDS Data1–	
Pin 7	TMDS Data0+	
Pin 8	TMDS Data0 Shield	Ground
Pin 9	TMDS Data0–	
Pin 10	TMDS Clock+	
Pin 11	TMDS Clock Shield	Ground
Pin 12	TMDS Clock–	
Pin 13	CEC	
Pin 14	NC	No connect
Pin 15	SCL	I²C Serial Clock for DDC
Pin 16	SDA	I²C Serial Data Line for DDC
Pin 17	GND	Ground
Pin 18	P5V0	Power
Pin 19	HPD	Hot Plug Detect

External HDMI speakers should not be used with the phone as they can interfere with speaker phone operation, to prevent interference, mute and/or turn down the HDMI Display's speakers.

Ethernet Cameras

For the Video Phone, a local video camera must be provided. It is designed to interface to an HDTV 1 Megapixel (720p) camera via an ethernet LAN connection. This camera will capture a video image from the conference room.

Ethernet Camera Requirements

Cameras that are suitable for use with the Video Phone should meet the following requirements:

- The camera should be IEEE 802.3af PoE compliant, allowing the camera to receive its power over the LAN connection.
- The camera must be ONVIF (Open Network Video Interface Forum) compliant. ONVIF defines a protocol for the exchange of information between different video devices. ONVIF compliancy is intended to ensure interoperability between devices.
- The camera must support the H.264 video compression standard and it must also support video streaming via RTP over UDP.
- The camera should support video resolutions of up to 720p @ 30 fps (HDTV).
- The camera must provide a 10BASE-T/100BASE-TX ethernet network interface.

Recommendations for specific camera models are discussed further on in this section.

IP Networking Requirements for Ethernet Cameras

Connecting the Camera

Ethernet cameras that meet the above-stated requirements can be interfaced to the Video Phone in two different ways:

- Locally Connected - The camera can be connected to the Mitel Multi-Port PoE Ethernet Switch, which in turn is connected to the Video Phone. Camera power is provided from the Mitel Multi-Port PoE Ethernet Switch.
- LAN Connected - The camera can be connected to a remotely located PoE compliant L2 switch, which in turn provides connectivity to the Video Phone. Camera power is provided from the remote L2 switch.

  For details on these powering options, refer to the section of this document on *Power*.
- It is recommended that the camera always be installed on the same IP subnet as the Video Phone. This ensures that network latency is kept to a minimum and it also allows the Camera Discovery Protocol (which is non-routable) to function correctly.

A minimum of CAT-5 cabling should be used for making LAN connections to the camera.

> **Note:** For details on how to configure the camera and the L2 switch networking parameters, see LAN Connection Guidelines.

Ethernet Cable Routing

The signals carried by the ethernet cable are susceptible to Radio Frequency (RF) and electrical noise. As a result, care should be exercised when routing the ethernet cable between the Video Phone and the camera. In general, the ethernet cable should not be routed close to mains power cables, fluorescent lights or Wi-Fi Access Points.

IP Address

The camera will need an IP address so that it can communicate on the LAN. Depending on the camera manufacturer, the IP address may be set to a factory default value. This can be changed to the required address, either statically or via DHCP.

Other addressing fields that may need to be configured are the subnet mask and the default router IP address. Camera vendors usually provide software that allows for camera set up and configuration from a personal computer.

Camera Discovery Protocol

Under Camera Settings, there is a **Search** function.

The search function invokes the Camera Discovery Protocol which will search for any available cameras in the Video Phone's subnet. When a camera is found, its IP address and/or Host Name will be displayed on the Video Phone screen.

The Camera Discovery Protocol is a non-routable protocol; it will only work when the camera and the Video Phone are located in the same subnet.

For further details, refer to the *MiVoice Conference/Video Phone Administration Guide*.

Bandwidth Requirements

The camera’s LAN bandwidth requirements will be on average 6 Mb/s; however, traffic bursts of up to 100 Mb/s should be expected. These bandwidth requirements pertain to traffic flowing from the camera to the Video Phone. Traffic from the Video Phone to the camera is negligible

Ethernet Camera QoS Settings.

Most camera vendors provide the ability to assign Layer 3 (L3) Quality of Service (QoS) to outgoing packets. Cameras will usually allow L3 QoS to be applied independently to video packets, events/alarm packets and management packets.

If the camera is capable of supporting L3 QoS, then it is recommended that the feature be used to ensure the correct treatment of traffic on the LAN.

The following Table shows the recommended L3 QoS values. Management refers to OAM network traffic. Events/Alarms refer to signaling type traffic. For details, refer to the camera manufacturer’s literature.

Table 2. Ethernet Camera L3 QoS

Packet Type	DSCP Value
Management	16 (CS2)
Video	34 (AF41)
Events/Alarms	24 (CS3)

Camera Security

The System Administrator may want to ensure that the camera cannot be controlled by unauthorized individuals and that video streams cannot be accessed by unauthorized individuals.

To secure the camera, the System Administrator should consult the camera vendor's documentation, in particular:

- There may be the ability to set 'root' passwords in order to control access to camera configuration parameters.
- There may be the ability to set HTTP and RTSP passwords.
- The camera may support an IP address filter or an access control list; both are mechanisms that control which IP addresses are allowed to connect with the camera.
- The camera may support the IEEE 802.1x authentication protocol.
- The administrator may want to disable the camera's NAT firewall traversal abilities.
- The administrator may want to disable anonymous viewer login capabilities.

> **Note:** Depending on how the camera is connected to the LAN - locally or at the LAN access switch – it may have an impact on how 802.1x (network authentication) should be configured. For details see the section on *Security and Authentication.*

Recommended Ethernet Cameras

For optimum video quality, it is recommended that the Panasonic WV-SP105, Panasonic WV-SP305, Panasonic WV-SPN310, or Panasonic WV-SPN311 be used with the Video Phone.

Tested Ethernet Cameras

If a recommended ethernet camera cannot be obtained, then the Administrator can use one of the following cameras. These cameras have been tested with the Video Phone and found to offer satisfactory results. The Administrator should only use Recommended or Tested cameras.

- Axis Communications – Axis M1054
- Axis Communications – Axis M1104 (minimum UC360 SP1)
- Sony CH-110
- Sony CH-120

Ethernet Camera Firmware

It is important to ensure that the ethernet cameras are running the correct versions of firmware. The Axis cameras MUST run a specific version of firmware; see the Table below for the Required Firmware Revision.

The Sony cameras must run the minimum version of firmware shown in the Table below; however, the Sony cameras can be run with newer versions of firmware.

If you are using an Axis camera, depending on when you purchased the camera it may be necessary to reinstall the camera's firmware. It may require an upgrade or a downgrade to ensure that the Axis camera is running the exact revision of firmware shown. If necessary you can obtain a copy of the required firmware at Mitel On-Line.

Table 3. Ethernet Camera Required Firmware Revisions

Ethernet Camera	Firmware Revision, Release 2.1, SP5	Firmware Revision, Release 2.1, SP3	Firmware Revision, Release 2.1, SP2	Firmware Revision, Release 2.1, SP1	Firmware Revision, Release 2.1
Axis M1054	5.50.3.4	5.50.3	5.50.3	5.50.3	5.50.3
Axis M1104	5.50.3	5.50.3	5.50.3	5.50.3	5.50.3
Sony - CH-110	1.85	1.85	1.82	1.82	1.82
Sony - CH-120	1.85	1.85	1.82	1.82	1.82
Panasonic WV-SP105	2.15	2.10	2.01	2.01	1.82
Panasonic WV-SP305	2.13	2.10	2.02	2.01	1.83
Panasonic WV-SPN310	2.00	1.71	Not supported		
Panasonic WV-SPN311	2.00	Not supported			

Note: Release 2.1, SP4 has the same Firmware versions as Release 2.1, SP3.

Ethernet Camera Initialization

The Ethernet camera has a number of parameters that need to be configured so that it is ready for operation. These parameters can be grouped into two categories: Network Settings and Operational Settings.

Network Settings

The following table shows some typical ethernet camera Network Settings that may need to be configured and recommendations on how to set them.

> **Note:** For details on how to configure the camera and the L2 switch networking parameters, see LAN Connection Guidelines.

Table 4. Ethernet Camera Network Settings

Camera Network Setting	Recommended Setting
IPv4 versus IPv6 operation	The Video Phone is an IPv4 device, so the camera should be set to IPv4 operation.
DHCP enabled or not	This depends on how the Administrator would like network parameters to be discovered. For further information, see the Section on IP Network Configuration Specifics.
IP Address, Subnet mask and Default Router IP address	This depends on how the Administrator would like to provide IP addresses. For further information, see the Section on IP Network Configuration Specifics. Because of network delays incurred when traversing a router, it is recommended that the camera be in the same subnet as the Video Phone.
RTSP protocol, enable	This should be enabled.
L3 QoS (DSCP) for Management, Video and Signaling	Management = 16 (CS2) Signaling = 24 (CS3) Video = 34 (AF41)
RTP/H.264 IP address port range	50000 to 50511 is recommended
RTP/H.264 Time To Live value	Use the default setting
MTU size	Must not exceed 1280

Operational Settings

The following is a typical list of camera operational settings that the administrator may need to configure:

- Bit rate control – Constant Bit Rate or Variable Bit Rate

In general, it is recommended that the camera be set to Variable Bit Rate. While a setting of Constant Bit Rate will prevent bursts of transmitted packets, it will also have the negative effect of adding latency to the packets being transmitted by the camera. It should be noted that this parameter may be automatically configured by the Video Phone. In this case, the Video Phone configuration will overwrite the manually-configured setting.

- Color level
- Brightness
- Contrast
- White balance
- Sharpness
- Exposure settings
- Iris adjustment
- Focus adjustment

Camera vendors usually provide software that you install on a PC and use to configure the camera. Once communication between the PC and the camera is established, the installer can then view a preview screen on the PC while optical adjustments are being made to the camera.

The Video Phone also has a camera preview mode that can be used to ensure that the camera's field of view is set correctly. To activate the preview mode, press the 'Show camera' button.

The Video Phone supports the ONVIF protocol and uses this protocol to set the camera's frame rate and resolution on a call-by-call basis.

Recommendations for Operational Settings

This section provides some recommendations on how to set the various camera settings and provides some general information on video and camera terminology.

HDMI Display Settings

Before starting to set up the camera, it is recommended that you set up the HDMI display or projector that is connected to the Video Phone. You can start by selecting the predefined settings on your HDMI display. Some HDMI displays have settings called Dynamic, Standard, Vivid, Movie, and so forth. Select the setting that works best for the room in which the display is located. If you are not completely satisfied with the display presets available, you can consult the manufacturer's documentation as to how to customize the settings.

Ethernet Camera Settings

Each model of camera has a different set of configuration options along with a different set of defaults. The following Table shows a few examples of the type of settings that are available for each camera.

The Administrator should refer to the Camera Vendor's documentation for camera set up information.

It should be noted that there are no settings and configurations that will work satisfactorily in all deployments since each conference room or executive office has different characteristics (e.g., lighting in the room, lighting from windows behind the camera and lighting from window in front of the camera).

As a result, the characteristics of the room that the camera is being deployed in may require you to change the settings from the factory default settings to produce the best possible picture.

Table 5. Ethernet Camera Settings

Model	Characteristics	Available Settings
Axis 1054	84 degrees, fixed iris, fixed focus	Resolution, Color, Brightness, Sharpness, Contrast, White Balance, Exposure Settings
Sony - CH-110	80.7 degrees viewing angle	Resolution, Color, Brightness, Contrast, White Balance
Sony - CH-120	96.5 degrees to 33.9 viewing angle	Resolution, Color, Brightness, Contrast, White Balance
Panasonic WV-SP105, WV-SP305 WV-SPN310, and WV-SPN311	70.3 degrees to 55.4 degrees viewing angle	White Balance, Light Control Mode - 50Hz/60Hz, Backlight Compensation, AGC

Effects of Various Camera Settings

This section describes what effect the various camera settings will have on an image, and some setting recommendations are also included.

Color

Increasing the Color level increases the color saturation. When set to the minimum level a black and white image is produced. The maximum level setting provides maximum color saturation. Use this setting to achieve the truest colors for your conference room or executive office. An image of a person’s head is usually useful for setting the color level as the humane eye is very familiar with flesh tones.

Brightness

Increasing the brightness value produces brighter images. This setting should be increased when the room has dim lighting. This setting should be decreased when the room has bright lights or a lot of natural lighting from outside windows.

Sharpness

Increasing this value produces sharper images. A higher setting produces a sharper image but may increase the image noise in low-light deployments. A lower setting produces less image noise but the image will not appear as sharp. Image noise is random variations of brightness or color information in the image.

White Balance

White balance is used to make colors in the image appear the same regardless of the color temperature of the light source. White balance tells the camera what the color white is supposed to be, and once set the rest of the colors are displayed more accurately. Some cameras can automatically identify the light source and compensate for its color.

Contrast

Contrast changes the relative difference between dark and light. When this is set too high or too low the image will lose definition and clarity. This setting has an interactive effect with the brightness setting and vice versa.

Light Control Mode 50 Hz 60 Hz Compensation

When flicker is caused by fluorescent lighting this control will allow the camera to be automatically compensate for the flicker. Select 50 Hz or 60 Hz corresponding to the location where the camera is in use.

Keyboards and Mouse

It is recommended that a wireless PC keyboard and a wireless PC mouse be used with the phone.

It is best to connect the external keyboard while the phone is powered off. Then power on the phone. Alternatively, you can reboot the phone after the keyboard has been connected.

The phone has two Type ‘A’ USB interface receptacles. It is recommended that the USB/Wireless receiver be installed in the USB connector located on the bottom of the phone. Alternatively, a powered USB 2.0 hub could be used to connect the keyboard and mouse to the phone.

Refer to Phone USB Port Power Capabilities for additional details on the USB ports.

Conference Room and Office Recommendations

Room Dimensions

For optimum acoustical performance, the phone should be operated in a room where the room volume does not exceed 9,800 cubic feet (277 cubic meters).

For practical purposes, assuming that the room has an 8’ (2.43 m) high ceiling, then the maximum size room (if square) would be 35’ wide by 35’ long (10.68 m x 10.68 m).

To ensure that spoken voice can be accurately captured by the phone, it is recommended that the individual speaking should not be more than 12’ (3.65 m) away from the phone.

Acoustical Treatment of Room

Each conference room will have unique acoustical characteristics; the room’s acoustical characteristics can be affected by a number of different factors such as room dimensions, floor coverings, wall coverings, ceiling construction, furniture and the number of occupants.

In most cases a room’s dimensions cannot be altered. As a result, the only way to modify a room’s acoustical properties is through the use of different building or decorating materials.

In general, rooms can be grouped into three different acoustical categories: neutral, too live or too dead.

In a room that is acoustically too live, sounds will echo or reverberate. This is due to there being too many surfaces in the room that reflect sound waves. Items that will reflect sound waves are typically hard flat surfaces such as, tiled floors and hardwood floors, glass walls and windows, ceramic walls, and dry-walled ceilings.

In a room that is too acoustically dead, sounds will seem to disappear or be absorbed by the room. This is due fact that there are not enough reflective surfaces in the room. Items that will absorb sound waves are typically soft materials and irregular surfaces such as carpeted floors, curtains and draperies, venetian blinds, upholstered furniture and people.

A room that has neutral acoustical characteristics will provide the most natural sounding environment since sounds waves will not be excessively reflected or absorbed.

> **Note:** The conference phone has the ability to compensate for rooms that have less than ideal acoustical properties, but there are limits to this capability.

In situations where the room is acoustically too live for the conference phone to compensate for the people participating in a conference call, typically the participants on the far end may hear unacceptable levels of echo.

To resolve this situation, the conference room may require acoustical treatment to reduce the amount of acoustical reflection that is, in turn, causing echo.

Some easy techniques for reducing acoustical reflection in a room are the following:

- Add some artwork; a wall surface that presents varying depths reduces reflections.
- Place a fabric covered office cubicle wall against a wall; it acts as a sound absorber.
- Add draperies or tapestries to a wall; fabrics absorb audio energy.
- Add draperies or fabric blinds over windows, window glass is highly reflective; fabrics absorb audio energy.
- Bare floors are very reflective; add an area rug, the deeper the pile the better.
- If the chairs in the room have hard surfaces, consider using upholstered furniture; it is less reflective.
- If the ceiling is a hard surface such as non-stippled drywall, or even worse masonry, consider having acoustical ceiling tiles installed.

Ambient Noise

When selecting a conference room, some consideration should be given to possible sources of ambient noise that may impede the usability of the phone. Potential sources of unwanted sounds are noise coming from adjacent rooms, hallways or stairways. The installer must also consider unwanted sounds that may be produced from machinery, office equipment or fans used for building heating and air conditioning.

HDMI Display Placement

The HDMI display will typically be mounted on a wall at a height off of the floor that allows for comfortable viewing by individuals that are seated in the room. As a guideline, most desks and tables will have work surfaces that are approximately 29” (736 mm) high. The bottom of the HDMI Display should be positioned a little higher that the table top.

Whether the HDMI display is mounted on a wall or placed on a table care should be taken to ensure that the display will not be affected by vibrations. Care should also be taken to ensure that the HDMI display is not installed above a source of heat.

The installer should also refer to the section in this document on HDMI Cable Routing.

Ethernet Camera Placement

The ethernet camera will usually be mounted or placed at a height that is close to the bottom of the HDMI Display with the lens pointing towards the people viewing the HDMI Display. This allows all parties involved in a conference call have the sensation that they are looking at each other eye-to-eye.

The installer needs to be aware that the HDMI Display may produce a significant amount of heat, and the camera should not be subjected to this heat source.

Fine tuning of the camera placement can be accomplished with use of a PC running software that is provided by the camera vendor that allows the camera to be used in a preview mode or via the Video Phone camera preview mode. To activate the Video Phone camera mode, press the ‘Show Camera’ button.

Ethernet Camera Mounting

Refer to the camera vendor's documentation for details on how to mechanically attach the camera to its mounting bracket; it is imperative that you use the fasteners or screws specified by the vendor.

The camera vendor may offer several different mounting and/or housing options, when you order the camera you must select the most appropriate housing and mounting mechanism for your application, refer to the camera vendor's documentation for details.

Mitel also provides a Universal Camera Mounting Bracket that can be used to mount the camera. The Mitel part number is 50006614 Universal Camera Mounting Bracket (Video Phone). Additional information can be found in the *UC360 Camera Mounting Bracket Installation Guide*.

The installer should ensure that the camera or projector is mounted on a surface or structure that is not prone to vibrations.

The installer should also refer to the section in this document on Ethernet Cable Routing.

Ethernet Camera Lenses

When the camera is purchased, the camera usually is shipped with a standard lens; however, this lens may not be the most suitable lens for the intended application. Lenses should be selected with certain requirements in mind such as:

- Mechanical attachment method; the lens must be compatible with the chosen camera.
- Field of view or scene dimensions; you must decide how wide and how high the captured image should be.
- The distance from the camera to the subjects.

> **Note:** Other factors involved in lens selection that are not variable once a particular camera is chosen are the camera's resolution and the dimensions of the video detector integrated circuit.

Once the above requirements are defined the installer can determine the focal length of the lens to satisfy the above requirements.

Almost all camera vendors provide a Lens Calculator on their web sites. These calculators allow you to determine what the lens focal length should be based on the desired field of view and the desired distance between the camera and the subject. These calculators account for the camera resolution and the video detector dimensions once you have selected a particular camera model.

There are also generic or non-vendor based calculators available, however, usage of these calculators requires that you know the camera's resolution and the dimensions of the video detector.

Most of these calculators will also allow you to determine the field of view based on a given focal length and distance from camera to subject.

Phone Placement

To ensure optimal audio performance, the Video Phone will need to be correctly placed with respect to the HDMI display and the people in the conference room.

The HDMI display (or HDMI projector screen) and the ethernet camera will usually be located at one end of the conference room, and the people in the conference room will typically be located at the opposite end of the conference room.

Placing the Video Phone *between* the persons attending the conference and the HDMI display will ensure that all of the people in the conference room will be facing the Video Phone when they are viewing the HDMI display. As a result, all attendee's voices will be picked up clearly by the Video Phone's microphones. This placement of the Video Phone will avoid a situation where an attendee is facing away from the Video Phone when he or she is speaking.

Note that like any speakerphone, the Video Phone's speakerphone performance will be negatively affected if it placed too close to a reflective surface such as a wall, partition or window, or if the Video Phone is placed underneath a shelving unit.

Should the Video Phone's speakerphone operation be unsatisfactory due to echo or if the audio switching between the far end is unpredictable, then try relocating the phone away from any acoustically reflective surfaces.

Room Lighting

The installer should ensure that the camera will not be pointed into direct sunlight as this will overload or blind the camera.

Rooms that are decorated with minimal contrasts, e.g. neutral colors are most suitable for video conferencing.

The installer should ensure that camera is positioned so strong backlighting behind the conference attendees is eliminated. For example, having the camera pointing at attendees who are sitting in front of a window on a sunny day is not an acceptable practice.

The installer should position the camera to avoid such a situation or make use of blinds or curtains to stop sunlight entering the room. If a strong backlight cannot be avoided, then the situation might be alleviated by providing a source of front lighting to compensate for the backlighting. Another reason to avoid strong backlighting is that it may make the HDMI Display hard to see from certain points in the room.

Florescent lighting can sometimes cause cameras to flicker at the Mains frequency. To minimize this problem, avoid pointing the camera at a strong florescent light fixture. Depending on the camera vendor, there may also be settings available in the camera configuration menu to automatically eliminate 50 Hz or 60 Hz flicker problems.

External Microphones

The phone has a TRS 3.5 mm audio Line In receptacle for accepting an audio input from an external microphone amplifier. However, this capability is not supported under Release 1.0.

Table 6. Audio Line in Connector

1	GND	Ground
2	Right	MIC 1
4	Left	MIC 2

Extension microphones are supported in Release 2.1 and higher. For more information on extension microphones, see the Revolabs Dual Channel System Microphones Installation Guide.

External Speakers

External HDMI speakers **should not** be used with the phone as it may prevent the speaker phone feature from operating correctly. To prevent this from occurring, mute and/or turn down the volume on the HDMI display's speakers.

Power

Phone Power Requirements

Under normal operating conditions, the phone may consume up to 25.5 Watts of power; however, the typical power consumption will be:

- 16.2 Watts when the Ethernet port is operating at 100 Mb/s
- 20 watts when the Ethernet port is operating at 1 Gb/s

To conserve power, when the phone is not in use it enters an idle state and power consumption requirements are curtailed. The idle current requirements are:

- When connected to a 100 Mb/s LAN, idle power is 4.5 watts
- When connected to a 1 Gb/s LAN, idle power is 5.7 watts

Phone USB Port Power Capabilities

The phone has two USB 2.0 interface ports. If required, these ports can provide power to connected USB devices. Each USB port can provide 2.5 Watts of power (5V @ 500 milliamps) to a connected device.

Phone Powering Options

The phone receives its operating power via Power over Ethernet (PoE). PoE is a method of providing power to an ethernet connected device over the existing ethernet wiring that the device uses for connecting to the LAN. Ethernet cameras are also able to accept power via PoE.

The Gigabit Ethernet port on the phone is compliant with the IEEE 802.3at PoE standard.

The phone can be powered locally or remotely. The Administrator will have to decide which option is most suitable for their particular application.

> **Note:** Mitel's Power Over Ethernet (PoE) Powered Device (PD) products are covered by one or more of the U.S. patents (and any foreign patent counterparts thereto) identified at Mitel's website: www.mitel.com/patents
>
> For more information on the PD patents that are licensed, please refer to www.cmspatents.com

> **CAUTION:** The particular Conference/Video Phone powering option used will have implications on how the camera and L2 switch network parameters should be programmed.
>
> For details on how to configure the camera and the L2 switch networking parameters, refer to the section LAN Connection Guidelines.

Local Power

There are two options for providing the phone with local power, the Mitel Multi-Port GigE PoE Switch, (which is a 3 port Gigabit Ethernet switch with two PoE capable ports) or the In-Line Power over Ethernet Adapter.

Mitel Multi-Port GigE PoE Ethernet Switch

The Mitel Multi-Port GigE PoE Switch is advantageous in situations where there is only one LAN connection present in the conference room or office and the phone is being installed as a Video Conference Bridge. The Multi-Port GigE PoE Ethernet Switch obtains its power locally from the AC mains. All three ports on the Multi-Port GigE PoE Ethernet Switch support Gigabit Ethernet speeds.

The Multi-Port GigE PoE Ethernet Switch has the following three RJ-45 receptacles:

- The phone port – this port is used to power the phone and to provide connectivity to the phone. This port is IEEE 802.3at compliant and will provide up to 25.5 watts of power.
- The ACC (Accessory) port – this is used to provide connectivity and power to a conference room camera. This port is IEEE 802.3af compliant and can provide up to 15.4 watts of power.
- The LAN port – this port does not support PoE. It is used to provide connectivity to the customer's LAN.

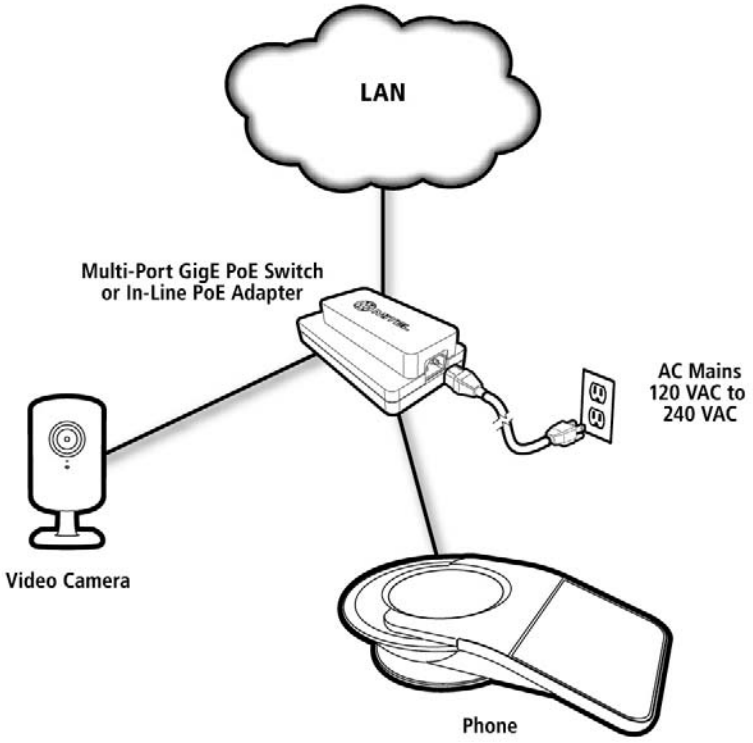

Figure 2. Connecting the Multi-Port GigE PoE Switch

If the Administrator prefers to power the conference room camera via existing LAN infrastructure, then the phone can be powered from the In-Line PoE Adapter.

When the phone is being installed, there isn't a need to power a camera, so it can be powered from the In-Line PoE Adapter.

For additional details on installation, refer to the *Multi-Port GigE PoE Switch Installation Guide.*

CAUTION: If the Multi-Port GigE PoE Switch is going to be used, refer to the section on Security for important information regarding IEEE 802.1x authentication operation.

In-Line PoE Power Adapter

Mitel offers an in-line IEEE 802.3at compliant adapter that can be used to power the phone. This adapter obtains its power locally from the AC mains; the Mitel Part Number is 51301339.

The In-Line PoE Adapter can be useful in situations where the phone is being installed without a local camera, and an IEEE 802.3at compliant L2 switch is not available.

Remote Power

In cases where a managed IEEE 802.3at compliant switch is available, the phone can be remotely powered by this switch.

Since L2 switches such as this are usually installed in a wiring closet. The ability to have the L2 switch power supported with an Uninterruptable Power Supply (UPS) is a viable option should high availability of the phone be a requirement.

A managed L2 switch also offers the administrator a higher level of manageability than either of the local powering schemes.

If phone is going to be powered with a remote L2 switch, three options can be used for powering the conference room camera.

The first option as shown below connects the conference room camera to the IEEE 802.3at compliant switch that is being used to power the phone.

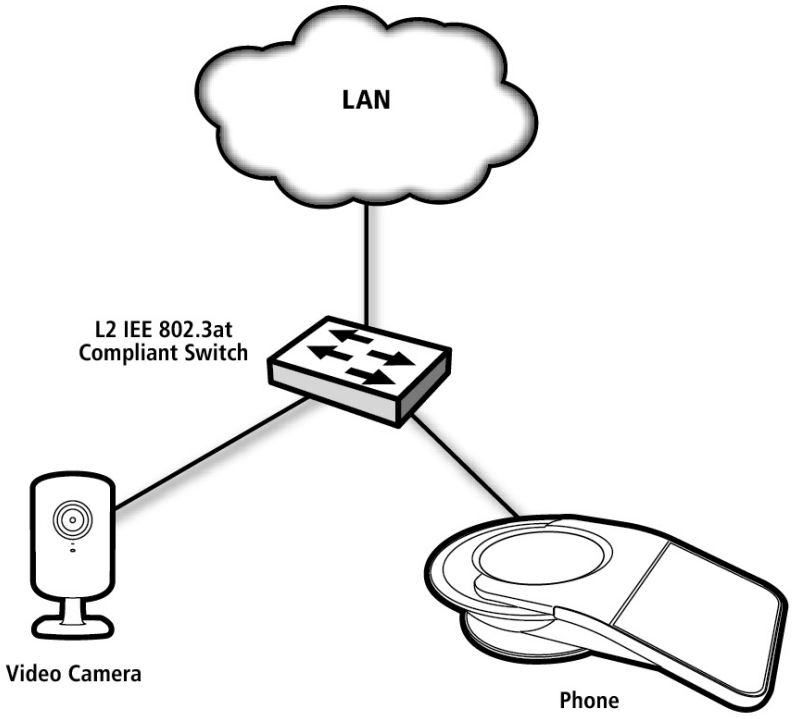

Figure 3. Connecting the Phone and Camera to a Remote L2 Switch

The second and third options connect the camera to either the Multi-Port GigE PoE Switch (or the In Line PoE Adapter), which in turn is connected to the Access L2 Switch.

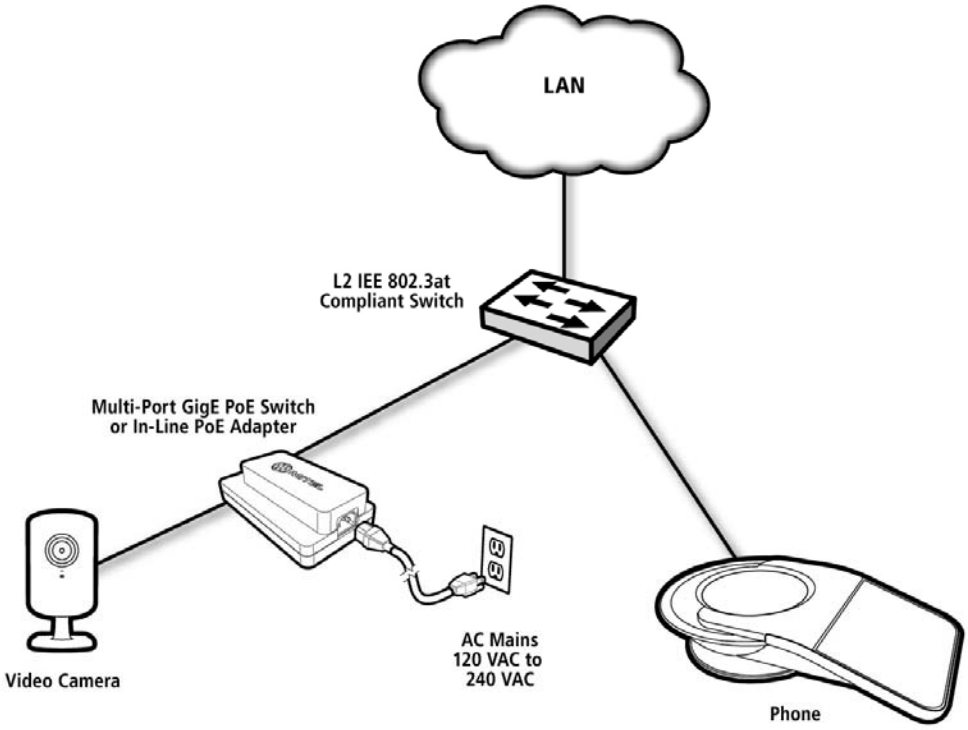

Figure 4. Connecting the Phone to a Remote L2 Switch and the Camera to a Local PoE Switch or In-Line PoE Adapter

IEEE 802.3af and 802.3at Compliant Switches

IEEE 802.3af compliant L2 switches have been available from numerous vendors for several years; as a result there should be no difficulty in procuring these switches.

IEEE 802.3af compliant L2 switches should only be used to power the ethernet camera.

To power the phone, an IEEE 802.3at compliant L2 switch is required.

While IEEE 802.3at compliant L2 switches are relatively new (2009), several vendors of enterprise class switches offer such products. These products can provide up to 25.5 watts of power over a single CAT-5 cable.

Some vendors refer to their IEEE 802.3at switches as ‘PoE+’ or ‘PoE Plus’; however, the administrator should ensure that the chosen switch is in fact IEEE 802.3at compliant.

There are also switches on the market that offer up to 51 watts of power over a single CAT-5 cable and their manufacturers claim that they are IEEE 802.3at *compatible* rather than *compliant.* These switches are not suitable.

Prior to PoE standardization, there were several proprietary PoE products brought to market and some of this equipment may still be deployed. These types of switches are not suitable for this deployment.

Spare Pair Powering or Phantom Powering

The networking industry uses two methods to deliver power over ethernet cables for 10 Mb/s and 100 Mb/s ethernet. In one mode, the power is delivered on the data pairs of the cable. This is called phantom powering. The second mode uses the unused pairs of the cable. This is called spare pair.

In the case of Gigabit ethernet (1000 Base-T), there are no spare pairs available in the cable, and power is only delivered using the phantom technique.

The phone and the Multi-Port PoE Ethernet Switch use only the phantom powering technique.

Regarding ethernet connected cameras, the administrator should consult the camera manufacturer’s literature for their powering requirements and ensure that the camera supports the phantom powering technique.

Phone Power Advertisements

The phone can use one of three different communication standards to advertise its power requirements to a powered Ethernet switch; however, the powered Ethernet switch must comply with one of these three standards:

- IEEE 802.3at Power Over Ethernet Standard (PoE)
- IEEE 802.3ab Link layer Discovery Protocol (LLDP-MED)
- Cisco Discovery Protocol (CDP)

Power advertisements for the various protocols are as follows:

IEEE 802.3at

The phone is an IEEE 802.3at (Type 2) Class 4 device. IEEE 802.3at (Type 2) Class 4 devices draw from 12.95 Watts to 25.5 Watts.

IEEE 802.3ab (LLDP-MED)

The phone advertises 20 W as a power requirement.

CDP

The phone advertises 5.0 W as a power requirement; however, this is not the actual power consumption but rather a value that allows interoperability with Cisco gear.

Planning a PoE Installation

When planning a power over Ethernet (PoE) installation, the power management features of the powered L2 switch should be taken into consideration.

Some vendors of IEEE 802.3af and IEEE 802.3at compliant switches provide power management features that can help to manage a situation where a group of PoE powered devices might require more total power than the L2 switch can provide.

Under such conditions, the power capabilities of the L2 switch could be exceeded and indeterminate device behavior may result. L2 switch vendors incorporate power management capabilities into their switches to prevent indeterminate device behavior. There are two power management schemes in use:

- Dynamic Power Distribution: If some devices do not require maximum power, the switch will re-distribute the unused power to other devices that may require more power.
- Power Prioritization per Port: This mechanism allows certain ports or ranges of ports to be deemed “critical”. Power to devices connected to critical ports will be guaranteed. Devices connected to ports that are not deemed critical may not receive power if the power capacity of the L2 switch has been exceeded.

For details on specific L2 Switch capability and how to configure port power prioritization, refer to the L2 switch vendor’s documentation.

Gigabit Ethernet Port

The Gigabit Ethernet port is IEEE 802.3at Power over Ethernet compliant and it supports the following features:

- Auto MDI/MDIX Capability (Auto Cross over)
- Auto Polarity
- Auto Negotiation

Ethernet PHY Configuration and Network Statistics

The Gigabit Ethernet port on the phone does not have configurable parameters. The port auto-negotiates with the L2 switch to which the phone is connected to determine the settings for the link speed and duplex.

The administrator can check what link speed and duplex the phone is running by looking under the Network Settings menu and then under the Hardware menu.

Connector Pin Outs

The phone Gigabit Ethernet port uses a standard RJ-45 receptacle. The following table shows the phone Gigabit Ethernet port pin assignments.

Table 7. Gigabit Ethernet Port Pin Assignments

Pin #	Description
1	Transmit/Receive Positive Channel 0
2	Transmit/Receive Negative Channel 0
3	Transmit/Receive Positive Channel 1
4	Transmit/Receive Negative Channel 1
5	Transmit/Receive Positive Channel 2
6	Transmit/Receive Negative Channel 2
7	Transmit/Receive Positive Channel 3
8	Transmit/Receive Negative Channel 3

Ethernet Cabling

The phone Gigabit Ethernet port is designed to operate with a minimum of Category 5e UTP cabling. Category 6 and Category 6a cabling plants are also acceptable.

If the Administrator would like the phone to connect to the LAN at 1 Gb/s speeds, then the Administrator should ensure that the LAN wiring plant is CAT-5e compliant (or better) from the phone ethernet connector to the Access L2 switch.

Cable plant compliance should be tested and verified by a certified communications cabling contractor. For further information, contact Mitel Professional Services.

General Information on IP Networking

This section provides general information on IP networking and is intended to provide the reader with background information.

Voice and Video over IP Networks

It is essential to assess and configure the network in order to maintain the voice quality, video quality and functionality for the user. This may require that the existing network be changed, or that equipment with certain capabilities be installed.

The main network issues affecting voice and video quality are:

- Delay
- Jitter
- Packet Loss

Care has been taken in the design of the phone to reduce any echo present through the inclusion of an echo cancellation device.

Jitter and a certain degree of packet loss are also taken care of by the phone jitter buffer. The phone uses a dynamically adjustable jitter buffer.

For more information on these possible network issues, see Issues Affecting Quality of Service.

Before designing a network to handle VoIP and video over IP, consider the following areas (these are recommendations, and there will always be exceptions):

- QoS (Quality of Service) Quality of service is that which is provided to the user, not network equipment settings. However, certain network equipment configurations can greatly assist in ensuring adequate QoS to a user. These include
  - **IEEE 802.1**p/Q: This is also known as VLAN tagging, priority, or COS (different from the PBX/telecom Class of Service). IEEE 802.1p/Q operates at Layer 2 to ensure high priority for voice and video traffic.
  - DiffServ (also known as DSCP): DSCP information is contained in a field in the IP packet header; it is used to define different service categories. DSCP operates at Layer 3 to ensure high priority for voice and video traffic.
- Switched L2 Networks: The use of L2 switched networks allows full-bandwidth to be provided to all devices on the network. Switched L2 networks are also able to support IEEE 802.1p/Q (L2 priority). The older ethernet hubs should not be used because they force network devices to share bandwidth and they do not support any priority mechanisms.
- Network topology: Networks should be designed in a hierarchical manner where bandwidth between devices is controlled and understood. Simply linking switches in a long chain will work for data, but it introduces jitter and unnecessary bandwidth bottlenecks between devices.
- Network pre-installation and post-installation analysis: The network should be investigated before installation to determine its suitability for transporting voice or video. Once an installation is completed, it should also be tested to ensure that the guideline limits have not been exceeded. For further information refer to the section of this document called IP Network Readiness Assessment.

- Network address translation (NAT) and firewall: To allow voice and video packets through a firewall, a number of ports will need to be opened on the firewall. Opening all possible ports negates the usefulness of the firewall. NAT needs to change addresses, but may have difficulty mapping a single device to multiple internet addresses, or translating IP addresses that are buried in control messages. Generally, these issues are resolved by using VPNs between sites.
- Virtual Private Network (VPN): VPNs are simply a pipe or tunnel across an ISP network, which allow a remote device to react as though it is still connected to the enterprise network. Be aware that the VPN may be across an unknown network or across the Internet. It may be necessary to get certain Service Level Agreements (SLA) to ensure timely delivery of data. Where encryption is used, additional delay may also be added to the data.

General Guidelines for Quality of Service

Two main issues that affect system installation and user perceptions:

- Quality of Service (voice and video quality during a conference call)
- Availability of the service (setting up and clearing of connections or signaling)

The sections below discuss several issues related to Quality of Service.

Issues Affecting Quality of Service

The following sections describe some areas that affect Quality of Service and briefly explain their importance.

Network Delay

As delay increases in a conversation, it becomes increasingly difficult to sustain normal two-way communication. Such a conversation rapidly changes from an interactive exchange to an “over to you” radio-style conversation. The delay is noticeable at 150 ms to 200 ms delay, and is radio-style at a 400 ms delay. These guidelines identify the delays that can be tolerated to ensure that voice and video quality are maintained.

Jitter

Jitter is the variation in delay that can occur in networks. The major source of jitter is serialization delay, which occurs when a packet cannot be sent at the ideal time because another packet is already being sent on the same connection. The result is that the packet must wait. For high-speed links, a maximum packet size of about 1500 bytes is sent in microseconds, so jitter is negligible. However, for slower WAN connections, such as a Frame Relay connection, the delay becomes significant.

Use of multiple WAN connections and load-sharing can also introduce jitter due to different path delays. Ideally, voice and video should pass down one path or another and may be configurable based on DiffServ (DSCP) values.

Packet Loss

Packet loss within the network can occur for a number of reasons; mainly congestion related to a particular connection, where the buffers can overflow and data is lost. Packets may also be discarded at routers due to congestion or at the phone if the jitter is so variable that when the packet arrives it is too late to be used for voice or video. Out-of-sequence packets can also occur over WAN connections. These are like packets with excessive jitter and can also result in packet discard. Incorrect duplex settings on LAN connections can also lead to data collisions and packet loss.

Although some packet loss can be handled on an ongoing basis, bursts of packet loss will become noticeable. A network with 0.1% packet loss spread out over time sounds much different on a VoIP call than a network with the same loss but occurring in bursts of three or more packets.

Available bandwidth

If a connection is rated at a particular bandwidth, this does not necessarily mean that all of this bandwidth is available. Connections between LAN and WAN network devices include a certain amount of overhead for inter-device traffic, including link termination devices and general broadcast traffic. In summary, the available bandwidth is always less than the connection bandwidth.

Packet priority mechanisms

In a network oriented towards data devices, absolute delay is not as important as accuracy.

For voice or video traffic, however, a certain amount of incorrect or lost information is acceptable, but information delivered in an untimely manner is not. It is important to ensure that any voice or video traffic gets “pushed” to the front of any connection queue. If PC-type data is slightly delayed, this is less important. There are two similar mechanisms at work to determine priority: 802.1p/Q at Layer 2 and Diffserv at Layer 3.

WAN connections

The best Quality of Service is obtained when the customer has control of the external WAN connections. This can be achieved by using dedicated leased lines between sites, or by ensuring a guaranteed service-level agreement (SLA) from the external network provider (ISP).

When specifying an SLA it is important that the guaranteed committed information rate (CIR) is specified and includes a guard band. Data sent in excess of the CIR is likely to be discarded during congestion periods in order to maintain guarantees on the SLA. It may also be advantageous to split voice and video traffic from normal data traffic with different SLAs.

Some carriers may also offer an SLA that honors and provides queuing for incoming (download to the customer) data as well. There may be an additional charge, but this will provide the added queuing on the far end of the often bandwidth limited connection between the customer and the carrier. With the customer providing priority queuing on the outgoing (uplink from the customer), this link will then have priority queuing at both ends of the connection, to ensure priority for voice and video traffic.

If a WAN connection provides both data and voice/video traffic on a common path, then priority schemes need to be employed. When correctly configured, the phone will use appropriate DiffServ field settings. Priority queuing should be enabled on the end routers, even if priority is not used within a separate voice/video network

For more dedicated links, some additional protocols can be used to improve bandwidth usage.

The data in an Ethernet LAN connection includes a data layer for Ethernet and a data layer for IP. In a WAN connection, the Ethernet layer may not be needed. However, other layers are needed to transport the IP layer and voice data. As a result, certain WAN protocols can use less bandwidth. These include the more dedicated links such as PPP and compressed PPP.

LAN architecture

Well-designed networks usually consist of different layers, the two main parts being the core network and the access network. Larger networks can include additional layers such as a distribution layer.

Ideally, the PBX or Soft Switch should have a connection higher up in the network, located more towards the core than at an access point. The optimum connection point is in the distribution layer. The phone should connect to the access layer.

Core network

The core network potentially carries data on dedicated links at 1 Gb/s or higher. The switches at this level probably include some Layer 2 and Layer 3 switching and unite a number of subnets, or a small number of units. These units almost certainly have UPS backup and are cross-connected in redundant configurations, so that the failure of one device is unlikely to result in total network failure.

Distribution layer

The distribution layer connects the core network and the users on the access layer. A distribution layer is used within a local area, for example, within a single building or in a campus environment.

This allows local switching to stay off the core network and provides a level of continued operation if problems occur in the core. Typically, network devices such as servers and printers are connected to the distribution layer. This is where the PBX or Soft Switch connects in such a large system. Devices in this layer usually use UPS backup.

Access layer

The access layer connects to the distribution layer by single or multiple connections. It provides the connections to the user. These can be cross-connected within geographic locations.

If a device fails here, then only the locally connected devices will fail. These units may or may not have UPS backup.

Maintaining Voice and Video Quality on IP Networks

As discussed in the previous section, the following issues affect voice and video quality of service being transported over IP connections:

- End-to-end delay
- Jitter or delay variation
- Packet loss
  - Due to link congestion resulting in discarded or out of sequence packets
  - Due to lack of or incorrectly configured QoS controls on LAN and WAN connections
  - Due to forced discard of packets caused by excessive jitter

IP Network Readiness Assessment

An assessment of the LAN should be conducted prior to installing VoIP or video over IP equipment. The assessment can provide the following information:

- Determine if an IP network is currently capable of handling voice and video traffic and at what capacity.
- Document the tested voice and video call capacity and characteristics of an IP network.

Typically, networks are designed to handle peak traffic. It is important to determine how well VoIP and video will perform on a network by measuring simulated VoIP traffic and calculating voice quality based on a Mean Opinion Score (MOS). Some networks only require minor modifications to deliver reliable, high-quality voice and video services. Others require more significant overhauls.

There are a number of products in the marketplace that can be used to perform a LAN assessment.

Sometimes a network that is already successfully providing voice and video transport services starts experiencing problems. This can be due to a change that has been made in the network infrastructure, topology or the addition of more users or new applications. In this situation. a reassessment of the network can help to determine the cause of the problem either locally or remotely.

If you are having problems locating tools for conducting an assessment, you should contact Mitel Professional Services. Alternatively Mitel Professional Services could carry out an evaluation.

To contact Mitel Professional Services, go to Mitel On-Line and select Professional Services.

A Network Planning Worksheet is provided in Appendix B. Use of this worksheet may help the Administrator identify areas of the network that need improvement.

Network Measurement Criteria

Assuming that jitter and packet loss are not an issue, the one parameter left that affects the voice and video quality is end-to-end delay. From ITU-T recommendations (and practical experience), the end-to-end delay across the network should not exceed 150 ms.

In assessing a network, consider the network limits shown in the following table.

Table 8. Network Limits

	Packet loss	Jitter	End-to-end delay	Ping delay
Go!	<0.5%	<20 ms	<50 ms	<100 ms
Caution	<2%	<60 ms	<80 ms	<160 ms
Stop!	>2%	>60 ms	>80 ms	>160 ms

“Ping” delay is the value obtained using a PC ping utility. The ping utility sends a message from one PC to a second PC. When the second PC receives the message, it sends a message back to the first PC. The first PC determines the propagation delay encountered on the network between the two PCs. Typically the send and receive paths have equal delays. Estimate jitter by using ping over a short and longer-term period. Estimate packet loss by using ping over a longer period (24 hours or more). Networks that are used for both voice and data can have variations in the amount of network delay. For instance, if computer backup utilities run on a regularly scheduled basis, network delay can increase. Perform longer-period delay measurements over a time period that represents the customer's core operational hours.

Other tools, such as network analyzers, can also be used to determine packet loss. Many analyzers look for VoIP and RTP packets, and can identify when a packet is missing as well as average jitter. Although ping can be used as a quick check or as a backup method, it is recommended that networks be fully evaluated before installation. Mitel Professional Services can perform a full VoIP network pre-installation evaluation.

> **Note:** The phone display provides a Network Health icon that indicates when there is Network Congestion causing packet loss. This Icon, when active, is reporting that there is packet loss in the receive stream. In other words, a percentage of packets being transmitted from the far end to this phone are being lost somewhere in the network. For details, refer to the *MiVoice Conference/Video Phone Administration Guide*.

Network Priority Mechanisms

Two areas where priority mechanisms operate in the network to ensure that voice traffic maintains high priority are

- Layer 2 in the LAN through use of IEEE 802.1p/Q
- Layer 3 in the WAN through use of DiffServ/TOS/Precedence

LAN L2 Priority

The priority mechanism used relies on that described in IEEE 802.1p. This is a subsection of IEEE 802.1Q also known as VLAN tagging.

IEEE 802.1p (Layer 2 priority) uses a field in the IEEE 802.1Q tag to provide eight levels of priority. IEEE 802.1Q is the open VLAN standard that extends the Ethernet header by adding an additional 4 bytes to tagged packets. Because the 802.1p priority is part of the VLAN header, ports that need to convey multiple VLANs/802.1p priorities must use tagging.

The following figure highlights an Ethernet packet format, and the location of the Layer 2 Priority and Layer 3 Priority fields. This view is of a tagged frame, since it included IEEE 802.1p/Q information. The values in the figure are based on a voice call that uses a G.729a CODEC and 20 ms Frame Rate.

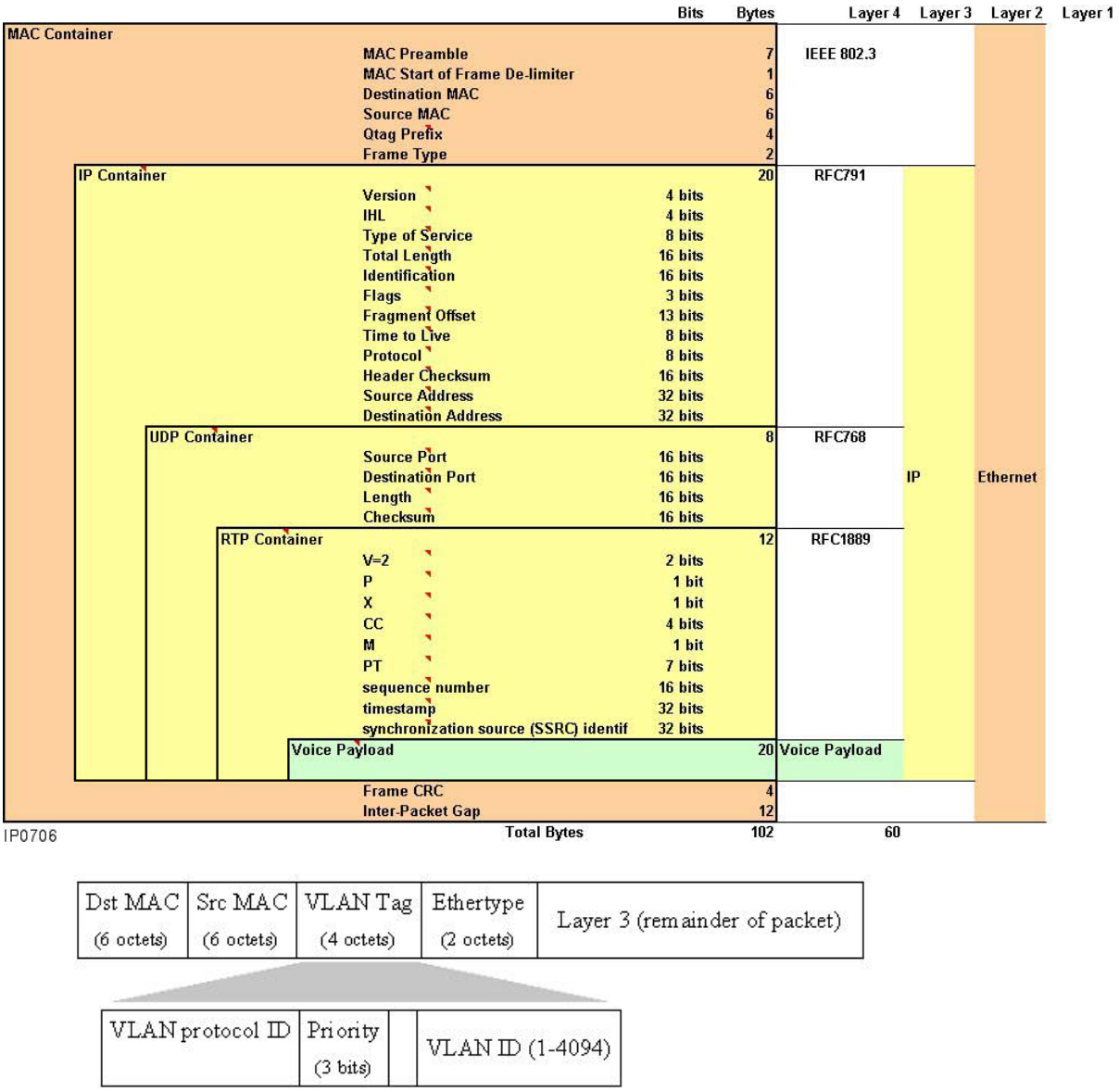

Figure 5. Ethernet Packet Format

There is potential in the VLAN specification to interpret the standard, with respect to VLAN 0, in different ways. This can lead to incompatibility between different vendor units. Do not use VLAN 0.

The main requirements are

- Ports should be configurable to provide VLAN tagging to incoming untagged information and remove this tagging when passing out of the switch. This is used by the controller and associated applications.
- Ports should be configurable to pass all active VLANs with tagging from one switch to another (there is no untagged information present in the connection). This is used between LAN switches and maintains priority information between units.

Some other VLAN guidelines for use with voice and video are the following:

- Additional bandwidth is always good.
- Use full duplex connections.
- Do not use VLAN 0.
- Set Priority to value 6 for voice. (Value of 5 used in Cisco networks)
- Set Priority to value 3 for signaling. (Value of 3 used in Cisco networks)
- Set Priority to value 4 for Multimedia. (Value of 4 used in Cisco networks)
- Set Priority to value 0 for Standard (Best Effort) (Value of 0 used in Cisco networks)
- Use VLAN 1 to 999 with Cisco products. VLANS can be extended from 1000 upwards. Care in selection should be exercised in this case as some VLANs are already reserved for other network usage.
- Set Priority for untagged VLAN/native VLAN/default_vlan to 0.
- Hubs don’t support priority queuing, so use managed Layer 2 switches with 802.1p/Q support.
- Do not use VLAN 4095 with HP products; this is reserved for inter-switch use.

WAN L3 Priority

A number of different WAN or L3 technologies allow for data routing with different priorities and Service Level Agreements (SLA). Most of these WAN technologies rely on information being presented in the Differentiated Services Code Point (DSCP) field.

Differentiated Services Code Point (DSCP) or DiffServ uses the precedence and some of the TOS bits to provide 64 different service levels.

- It is recommended that voice packets be sent in the Expedited Forwarding (EF) queue which is represented by a DSCP value of 46.
- Video or multimedia conferencing packets should be sent in the Assured Forwarding (AF) queue which is represented by a DSCP value of 34.
- Signaling packets should be sent in the Class Selector (CS) queue which is represented by a DSCP value of 24.
- Standard packets should be sent in Best Effort (BE) queue which is represented by a DSCP value of 0.

IP Network Configuration for the Phone

This section provides IP networking information that is specific to configuring the phone. It provides the information required to install the phone into an IP network.

> **Note:** There are a number of different options available for powering the phone and the ethernet camera. The particular option used will dictate the network connection topology. The Administrator will need to consider the powering option used and then configure the phone, camera and L2 switches as recommended under LAN Connection Guidelines.

The phone has a number of network parameters that need to be configured before the phone can be fully integrated into the LAN.

As explained later in the section called VLAN/QoS Discovery Mechanisms, the phone can obtain some of these parameters automatically from a number of different sources.

> **Note:** If installing the phone with a MiVoice Business, it may be easier for the installer to use 'static' VLAN and QoS values by manually entering the information into the phone Network Settings menu rather than obtaining parameters via DHCP or other methods.

However, if the installer chooses to have a DHCP server provide these values to the phone, it should be noted that the MiVoice Business/ DHCP server may not support a field for defining L2 and L3 QoS values for Multimedia Conferencing. In this case, the L2 and L3 QoS values for Multimedia Conferencing will need to be statically programmed.

The following sections describe the fields that are found under the phone Network Settings, Network Camera Settings, SIP Settings, LDAP/AD Settings, and Video Setting menus, where applicable. Default settings are also shown. Additional information can be found in the *MiVoice Conference/Video Phone Administration Guide*.

For installations where the factory default settings are not used, refer to the latter part of this section which discusses network settings in greater detail.

Network Time

By default, the phone date and time is obtained from its configured SIP server, and NTP (Network Time Protocol) is disabled. However, this will only work when the SIP server supports the optional SIP Date header in its registration 200 OK responses.

Many SIP servers support this; however, some servers may not. In that case, NTP should be enabled. NTP (Network Time Protocol) allows the phone to set its time of day clock. The phone will access the default server at the URL - *2.android.pool.ntp.org* - on the internet to obtain the current time of day. A customer can also use DHCP Option 42 for an NTP server.

If an NTP server is not programmed in **Settings**, and an NTP server is not obtained from DHCP, the default NTP server is used.

If an NTP server is programmed in Settings, it is used even if an NTP server is obtained via DHCP.

Network Settings Menu

See the *MiVoice Conference/Video Phone Administration Guide* for detailed information on configuring the Network Settings. For additional information, refer to the section on Security and Authentication.

Camera Settings Menu

See the *MiVoice Conference/Video Phone Administration Guide* for detailed information on configuring the Camera Settings.

SIP Settings Menu

See the *MiVoice Conference/Video Phone Administration Guide* for detailed information on configuring the SIP Settings.

Contacts Settings

For corporate directory access, the MiVoice Conference/Video Phone can use CSV (Command Separated Values) files or LDAP. You can configure the phone to populate the corporate contacts from CSV files or from an LDAP server. The default is LDAP.

The MiVoice Conference/Video phones supports a maximum LDAP Directory size of 20,000 entries with pictures and 40,000 entries without pictures.

For configuration details, refer to the *MiVoice Conference/Video Phone Administration Guide*.

CSV Import

The Conference/Video Phone imports contacts only from CSV files that are formatted as generated by either the MiVoice Business Telephone Directory export or from the MiVoice 250 Phone - Individual export.

LDAP Import

Active Directory (AD) is a database for a Windows domain environment. It is included as part of most Windows Server operating systems. Servers that run AD are also called domain controllers.

AD is used for network administration and security. AD authenticates and authorizes all users and computers running in the AD domain.

The Lightweight Directory Access Protocol (LDAP) is used for searching and modifying the AD database.

The Administrator may want to include an Emergency Services Profile in the Active Directory for users who need to place emergency calls.

Video Settings

Video Settings allow you to adjust video bandwidth parameters for both the uplink and downlink LAN connections. The video settings menu also allows the Administrator to enable or disable the Dynamic Bandwidth Allocation (DBA) capability introduced in Release 2.0.

DBA is an algorithm the phone uses to reduce packet loss on a congested communication link. DBA will lower the phones' transmitted bit rate according to the packet loss feedback it receives from the remote end, with the end goal being that a reduction in the transmission rate should alleviate congestion and packet loss.

DBA relies on the RTCP protocol. At the time of writing, the MBG does not support the RTCP protocol. As a result, if the phone is connected to an MBG the Administrator should disable the DBA feature on the phone.

For more information, see Dynamic Bandwidth Allocation and the *MiVoice Conference/Video Phone Administration Guide*.

Conference/Video Phone Quality of Service Settings

This section provides detailed information on Mitel's Multi-Class Quality of Service (QoS) Model, the recommended L2 and L3 QoS settings for the phone, and the various methods that the phone can utilize to obtain L2 and L3 QoS settings.

Mitel Multi-Class QoS Settings Model

The following table represents Mitel's Multi-Class QoS Model which shows Mitel's recommended L2 QoS and L3 QoS (DSCP) settings for specific Service Class levels.

Using the recommended L2 and L3 QoS values ensures that voice and video packets are treated with a higher priority by networking equipment than other types of traffic.

The rows in the table that are grey are included for completeness; these Service Class categories are not applicable to the phone.

Table 9. Mitel's Multi Class QoS Model

Service Class	L2 Values	DSCP Values
Network Control	6	48 (CS6)
Telephony (Voice)	6	46 (EF)
Signaling	3	24 (CS3)
Multimedia Conferencing	4	34 (AF41)
Real Time Interactive	4	32 (CS4)
Multimedia Streaming	4	32 (CS4)
Broadcast Video	3	24 (CS3)
Low Latency Data	2	18 (AF21)
OAM	2	16 (CS2)
High Throughput Data	1	10 (AF11)

Service Class	L2 Values	DSCP Values
Standard	0	0 (DF) (BE)
Low Priority Data	1	8 (CS1)

Mitel Application Level to DSCP Mapping

The Mitel Application Level to DSCP Mapping Table shows Mitel's recommendations for the mapping of specific applications to DSCP (L3 QoS) values.

The DSCP Default values are held by the phone in non-volatile memory. The Installer DSCP values are values that can be entered via manual programming or obtained from automatic programming mechanisms such as DHCP, LLDP-MED or CDP.

If the phone detects Cisco equipment on the network, then Cisco inferred values, which are held by the phone in non-volatile memory may also be used.

If the administrator does not manually enter values, and values are not obtained automatically, then the DSCP default values will be used.

Table 10. Mitel Application Level to DSCP Mapping

Application (Service Class)	DSCP Default Values (Non Writeable)	DSCP Installer Values (Writeable Fields)
Telephony (Voice)	46 (EF)	46 (EF)
Signaling	24 (CS3)	24 (CS3)
Multimedia Conferencing	34 (AF41)	34 (AF41)
Standard	0 (BE)	0 (BE)

Mitel Application Level to L2 QoS Mapping

The Mitel Application Level to L2 QoS Mapping Table shows Mitel's recommendations for the mapping of applications to L2 Priority values.

The L2 Priority values are held by the phone in non-volatile memory. The Installer L2 Priority values are values that can be entered via manual programming or obtained from automatic programming mechanisms such as DHCP, LLDP-MED or CDP.

If the phone detects Cisco equipment on the network, then Cisco inferred values, which are held by the phone in non-volatile memory may also be used.

If the administrator does not manually enter values, and values are not obtained automatically, then the L2 Priority default values will be used.

Table 11. Mitel Application Level to L2 QoS Mapping

Application (Service Class)	L2 Priority Default Values (Non Writeable)	L2 Priority Installer Values (Writeable Fields)
Telephony (Voice)	6	6
Signaling	3	3
Multimedia Conferencing	4	4
Standard	0	0

Cisco Inferred QoS Values

If the phone detects CDP running on the network, then values for certain parameters not provided directly by CDP can be inferred based on the fact that Cisco equipment is present in the network.

If the phone is being deployed in a Cisco Environment the Administrator should consult the section called Operating in a Cisco Environment.

The values that the phone uses for Cisco Inferred QoS values are shown in the following table.

Table 12. Cisco Inferred QoS Values

Service Class	phone Cisco Inferred Values	
Telephony (Voice)	L2 = 5	DSCP = 46
Signaling	L2 = 3	DSCP = 24
Multimedia Conferencing	L2 = 4	DSCP = 34
Standard	L2 = 0	DSCP = 0

VLAN/QoS Discovery Mechanisms

The phone can automatically discover its VLAN and QoS information in several ways. These methods are described in the following sections.

Options for Obtaining LAN Policy Setting Information

The four potential methods that the phone can use to obtain network configuration information, such as IP addresses, L2 priority settings, L3 priority settings and VLAN information are

- Static values that are held in the phone memory. (The installer can program the phone with static values).
- The Voice VLAN may be learned via LLDP-MED.
- The Voice VLAN may be learned via CDP.
- The Voice VLAN may be learned via DHCP.

> **Note:** The VLAN Enabled Check Box must be set to 'Enabled' (default value) for the phone to be able to acquire and utilize VLAN information. The VLAN Enabled Check Box can be found under the Tools and Features menu.

Sources to Obtain Network Policy Information

It is possible to program some network configuration information manually and obtain other information via LLDP-MED, DHCP or CDP and also use default values.

The phone looks for VLAN setting information and network configuration information in a specific priority order until all of the appropriate fields have been filled in. This priority order for obtaining information is described in the following sections.

> **Note:** If the phone has obtained network configuration information via manual programming, this information will be held by the phone permanently, that is, other methods cannot overwrite these values and the values will be maintained even if the phone is rebooted. This includes the following values:

- IP address for the phone
- Gateway IP address
- Subnet mask
- DNS server 1 & 2 IP addresses
- IPA Server IP address
- LAN Policy (VLAN, L2 priority, DSCP)

The following table indicates which LAN Policy parameters can be obtained from each of the different sources of information.

Table 13. Sources of Network Policy Information

Source of Information	Phone IP Address	Default Gateway IP Address	Subnet Mask	VLAN (802.1Q) Informa-tion	L2 QoS Priority (802.1d/p)	L3 QoS (DSCP)	PBX IP Address	DNS IP Address
Manual Entry	Yes	Yes	Yes	Yes	Yes (0-6)	Yes (0-63)	Yes	Yes
LLDP-MED	N/A	N/A	N/A	Yes	Yes (0-6)	Yes (0-63)	N/A	N/A
CDP	N/A	N/A	N/A	Yes	See Note	N/A	N/A	N/A
DHCP	Yes	Yes	Yes	Yes (Uses double fetches)	Yes (0-6)	Yes (0-63)	Yes	Yes
Default Values	N/A	N/A	N/A	No VLAN, untagged	6 (If VLAN via CDP then default is 5)	46 See Note	N/A	N/A

Notes:

1. A DSCP value of 46 is recommended for newer installations using DSCP-aware routers. Value 46 will place the voice into the Expedited Forwarding Queue (EF).
2. Depending on certain network conditions, the phone will use different DSCP default values. The default values under specific conditions are the following:
   - If the VLAN information was learned via CDP, signaling will use a default DSCP value of 46 and voice will use a default DSCP value of 46. These values can be changed with additional programming.
   - In situations where VLAN information cannot be learned from either CDP or DHCP, the phone will use a DSCP value of 0 for both signaling and voice.
3. N/A means Not Applicable.

VLAN Setting Information Sources and Priorities

When seeking VLAN information, the phone will start with level 5 and proceed through the list in a descending order. Information obtained via level 5 will always override information obtained by a lesser level.

A higher priority setting always takes precedence over attempted re-writes by a lower priority source.

Table 14. Priority levels for the Various Sources of VLAN Setting Information

Source of VLAN Setting Information	Priority Level	Notes
Manual Entry (Static)	5	Programmed by installer via the phone User Interface
LLDP-MED	4	Information obtained from the L2 switch
CDP	3	CDP only provides VLAN information to the phone, however if CDP is detected on the LAN the phone will use the 'Cisco Inferred Values'. Refer to Cisco Inferred QoS Values.
DHCP	2	The first time the phone receives DHCP information it must contain an IP address for the PBX. This is also true for the double DHCP fetch mechanism. If the phone fetches DHCP information a second time, this information will over write the previous values.
Default Values	1	Default Value = No VLAN, untagged

L2 and L3 QoS Setting Information Sources and Priorities

The priority levels assigned to each source used for obtaining L2 and L3 QoS settings are shown in the following table. The highest priority level is 5 and the lowest is 1, such that a higher priority setting always takes precedence over lower attempted re-writes by a lower priority source.

When seeking QoS information, the phone will collect information from all available sources and use the highest priority information available.

The section Potential Issues with Using LLDP-MED in Cisco Environments on page 58 provides an example of a situation where the initial LAN Policy values are overwritten with values obtained from a higher priority source.

Table 15. Priority levels for the Various Sources of L2/L3 QoS Settings

Source of L2 & L3 QoS Settings	Priority Level	Notes
Manual Entry (Static)	5	Programmed by installer via the phone User Interface
DHCP	4	The first time the phone receives DHCP information it must contain an IP address for the PBX. This is also true for the double DHCP fetch mechanism. If the phone fetches DHCP information a second time, this information will over write the previous values. DHCP can be used to provide separate L2 and L3 QoS values for both signaling and media. If DHCP has only been programmed with one value, the phone will use this value for both signaling and media.
LLDP-MED	3	CDP only provides VLAN information to the phone, however if CDP is detected on the LAN the phone will use the 'Cisco Inferred Values'. Refer to the section called Cisco Inferred QoS Values.
CDP	2	The first time the phone receives DHCP information it must contain an IP address for the PBX. This is also true for the double DHCP fetch mechanism. If the phone fetches DHCP information a second time, this information will over write the previous values.
Default Values	1	Default Value = No VLAN, untagged

Notes:

1. A DSCP value of 46 is recommended for newer installations using DSCP-aware routers. Value 46 will place the voice into the Expedited Forwarding Queue (EF).
2. Depending on certain network conditions, the phone will use different DSCP default values. The default values under specific conditions are:
   - If the VLAN information was learned via CDP, signaling will use a DSCP value of 46 and voice will use a DSCP value of 46.
   - In situations where VLAN information cannot be learned from either CDP or DHCP, the phone will use a DSCP value of 0 for both signaling and voice.

Potential Issues with Using LLDP-MED in Cisco Environments

Issue

Erroneous Voice QoS values have been noted when using LLDP-MED with the following Cisco IOS software releases:

- IOS 12.2(37)
- IOS 12.2(40)

Cisco switches running the above operating systems with LLDP-MED enabled will issue these LAN Policy values for voice to the phone:

- Valid VLAN ID
- L2 (802.1p) = 0 (Incorrect value)
- L3 (DSCP) = 0 (Incorrect value)

Since these Cisco switch values are non-user programmable, they cannot be changed by the system administrator.

These values do not provide the correct priority levels for voice media at either L2 or L3; therefore, the use of these values will potentially cause severe voice quality issues.

Solutions

If it is a requirement to keep LLDP-MED running on the Cisco switches:

- Leave LLDP-MED running on the Cisco switches.
- Use DHCP to provide the phone with the correct L2 and L3 priority settings.

DHCP learned values have a higher priority and will override the LLDP-MED learned values.

In situations where there is no requirement to have LLDP-MED and CDP running on the Cisco switches:

- Disable LLDP-MED on the Cisco switches.
- Disable CDP on the Cisco switches.
- Use DHCP with double fetches to provide the phone with the correct L2 and L3 priority settings

If there is no requirement to keep LLDP-MED running on the Cisco switches:

- Disable LLDP-MED on the Cisco switches.
- Enable CDP to provide the phone with VLAN information.
- When the phone detects that CDP is present on the LAN, it will use the Cisco inferred values for L2 and L3 priority.

Operating in Cisco Environment

Cisco equipment has slightly different recommendations for QoS settings than Mitel recommends. To accommodate these differences, the Administrator will need to either:

- Configure the phone to comply with the QoS settings used by the Cisco network equipment, or
- Configure the Cisco equipment remap the QoS values used by the phone into the correct queue.

The L2 (802.1p) and L3 (DSCP) priority values recommended for operating in a Cisco environment are listed in the table below.

Table 16. Cisco Recommended QoS Values

Service Class	L2 (802.1p)	L3 (DSCP)
Telephony (Voice)	5	46
Signaling	3	24
Multimedia Conferencing	4	34
Standard	0	0

Note: The inferred Cisco L2 and L3 values used by the phone could potentially be replaced with values obtained via DHCP.

CISCO AutoQoS

AutoQoS is a Cisco feature provided in Cisco's IOS and Catalyst operating systems.

Like the name suggests, AutoQoS automates the programming of QoS parameters on Cisco routers and switches based on Cisco's best practice recommendations.

In addition to L2 priority and DSCP settings AutoQoS will also configure Cisco router and switch parameters related to queuing, depth of queues and drop thresholds.

After AutoQoS has run, if it is necessary, the system administrator can modify parameters on the Cisco switches and routers that were set by AutoQoS to suit any site specific application needs.

Deploying the phone in an AutoQoS environment

AutoQoS is a Cisco proprietary protocol. As a result, the phone and other non-Cisco equipment will be unable to automatically learn what QoS settings are being used by Cisco equipment that has been configured with AutoQoS.

When deploying the phone in a network where AutoQoS has been run on Cisco routers and switches it will be necessary for the System Administrator to check and ensure that the phone and any non-Cisco equipment are configured to comply with the Cisco settings.

If the phone is being installed in an environment where AutoQoS has been run, then the administrator should perform their own check to see what the L2 and L3 QoS values have been set to and adjust the phone setting accordingly.

CODECs

The word CODEC is a concatenation of two words: Coder and Decoder. The CODEC performs two functions: coding and decoding for the conversion of media. In this case, voice or video is converted into some data format that can be returned at the far end into something akin to the original.

For voice and video, this usually involves converting the analog signals into digital signals and levels and returning them back to analog.

Telephony (Audio) CODECs

The most popular telephony CODEC, G.711, has become standardized across large parts of the telephony network. As such, it has become the baseline to which IP devices perform.

But to make it interesting, 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.

CAUTION: When modifying CODEC selections, the G.711 CODEC should not be removed.

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

- G.729 - original version—very processor intensive
- G.729a - reduced processor effort and compatible with G.729
- G.729b - includes voice activity detection and ability to send background information. Compatible with G.729 and G.729a

Wideband audio, which supports up to 7 kHz (50 Hz to 7.0 kHz) 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 Conference Phone currently supports the following CODECs:

- G.711 (A-Law and µ-Law) @ 64 kb/s Note 1
- G.729a @ 8 kb/s Note 1
- G.729b @ 8 kb/s Note 2
- G.722 @ 64 kb/s
- G.722.1 @ 32 kb/s Note 1

Notes:

1. G.729b support in the phone does not support silence suppression; however, it is compatible with G.729b endpoints that do support silence suppression.
2. 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.

Wideband audio

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

The Conference Phone supports both the G.722 CODEC and the G.722.1 CODEC; these CODECS are based on ITU-T standards.

- The G.722 CODEC is a 7 kHz audio CODEC that can operate at a bit rate of 64 kb/s.
- The G.722.1 CODEC is a 7 kHz audio CODEC that can operate at a bit rate of 32 kb/s. The G722.1 CODEC algorithm is based on Polycom's Siren 7 CODEC, however the G.722.1 implementation does not support Siren 7's bit rate of 16 kb/s.

The G.722 and G.722.1 CODECs sample audio at 16 kHz — twice the rate of traditional telephony CODECS — which provides a superior frequency response over traditional CODECS. The voice bandwidth of these CODECs is 50 Hz to 7 kHz, compared to 300-3400 Hz 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 and SIP end devices.

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 following table shows some typical CODEC MOS scores.

Table 17. CODEC MOS Scores

CODEC Type	MOS Score	LAN Bandwidth
G.711	4.4	~100 Kb/s
G.729a	4.0	~40 Kb/s
G.722.1	4.4	~65 Kb/s

MBG Transcoding Support

At this time the MBG does not provide transcoding support for SIP devices, including the phone.

However, the MBG does support pass-through mode for G.711, G.729a, G.729b and G.722.1 CODECs. That is, if one of these CODEC types is enabled on both endpoints and both of the endpoints want to use the same CODEC, then no transcoding is required and the call will be supported via the MBG pass-through mode.

Note that the MBG does not support either transcoding or pass-through mode for the G.722 CODECs.

Video CODECs

The Video Phone uses an H.264 compliant video CODEC. H.264 is an ITU video CODEC standard that offers high definition video while maintaining low network bandwidth requirements.

H.264 may also be referred to as AVC, which stands for Advanced Video Coding, MPEG-4 Part 10. AVC is an ISO/IEC standard and H.264 is an ITU standard, both standards refer to the same CODEC; the terms H.264 and AVC are interchangeable.

The H.264 standard defines a number of video coding profiles; at Release 1.0, the phone supports the H.264 Baseline profile. At Release 2.0, the phone supports both the H.264 Baseline profile and the H.264 High profile.

Notes

1. The Video Phone must be reset if the H.264 video codec is not enabled, and has been enabled for the first time.
2. When using URI dialing, only the H.264 baseline profile CODEC is supported.

Voice Bandwidth Requirements

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).

Figure 6. IP Packet Format

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 and video payload. Different CODECs can provide different sized voice payloads given the same input information. A reduction in payload is often referred to as compression.

Some routers can also provide header compression on point-to-point connections, but this can introduce added delays. Typically this provides benefits on reduced bandwidth connections that typically would not be suitable for video.

Calculating and Measuring Voice Bandwidth

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 Kb/s, including VLAN.

What is the voice 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.

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 both voice and signaling 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 Tables show typical wire data rates for different protocols and LAN/WAN interfaces.

Table 18. Ethernet/LAN IP and On-the-wire Bandwidth

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

Table 19. Typical WAN: On-the-wire Bandwidth

	Codec	G.711	G.729	G.722.1
	Payload	64kbits/	8kbit/s	32kbit/s
Link Type	Packet Rate (ms)	Wire (kbits/s)	Wire (kbits/s)	Wire (kbits/s)
Ethernet	10ms	129.6	73.6	97.6
	20ms	96.8	40.8	64.8
	30ms	85.9	29.9	53.9
	40ms	80.4	24.4	48.4
Frame Relay (Layer 2)	10ms	123.2	67.2	91.2
	20ms	93.6	37.6	61.6
	30ms	83.7	27.7	51.7
	40ms	78.8	22.8	46.8
Frame Relay (Layer 3)	10ms	102.4	46.4	70.4
	20ms	83.2	27.2	51.2
	30ms	76.8	20.8	44.8
	40ms	73.6	17.6	41.6
PPP	10ms	104.0	48.0	72.0
	20ms	84.0	28.0	52.0
	30ms	77.3	21.3	45.3
	40ms	74.0	18.0	42.0

Page 1 of 2

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

Page 2 of 2

Variable packet rates

The phone supports variable ethernet packet rates; the value used for a particular call will depend on the outcome of negotiations between the phone and the device it is attempting to connect to.

Under most conditions the default packet rate used by the phone is 20 ms. However, packet rate values may vary from 10 ms to 120 ms in 10 ms steps. Typical packet rates and usage include:

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

Larger packet intervals reduce the number of packets per second, but also introduce added delays at both transmitter and receiver and are more likely to lead to voice and conversation quality issues since a lost packet becomes more noticeable to the end user.

A packet rate of 20 ms provides a good trade off between consumed bandwidth, packet rate and voice and video quality to the end user.

Video Bandwidth Requirements

Why is Bandwidth Provisioning Necessary?

Even when L2 and L3 QoS mechanisms are employed in the network to ensure that video and voice packets are handled with the requested priority by L2 switches and routers, it does not alleviate the requirement for the Administrator to provision sufficient network bandwidth to carry the expected traffic.

QoS mechanisms are designed to try and ensure that specific classes of traffic receive consistent treatment from networking equipment, but with insufficient bandwidth, QoS cannot guarantee performance for the high priority traffic such as video, nor does QoS ensure that low priority traffic will not be completely blocked by higher priority traffic such as video.

If a network interface does not provide enough bandwidth or a network router is unable to process the volume of packets it is receiving fast enough, then the packets will be at risk of being corrupted, delayed or completely lost, regardless of the QoS setting applied to the packets.

All video streams both from the ethernet camera and to/from the Video Phone will be encoded using H.264 CODECs.

While the H.264 CODEC is able to produce high definition video at a relatively low bit rate, there is significant bandwidth overhead required to transport the video information over the network. For instance, the Video Phone encapsulates the H.264 video stream to be transmitted into RTP packets, which in turn are encapsulated in UDP, which is then encapsulated in IP, which is finally encapsulated into Ethernet frames. This means that an Ethernet frame carrying H.264 video is comprised of:

- 18 octets for Ethernet + 20 octets for IP + 8 octets for UDP + 12 octets for RTP = 58 octets + the H.264 payload.

For the reasons discussed above, the Administrator must ensure that the network has been provisioned with enough bandwidth from end-to end to support video conferencing as well as other traffic types.

How Much Video Bandwidth is Required?

When calculating the phone's bandwidth requirements, the following should be considered:

- The phone supports a maximum of 4 parties in a video conference; this is comprised of the local party and 3 remote parties.

- If the ethernet camera and the phone are located in the same subnet, then the Ethernet camera video stream will be from the camera to the local phone and this stream will not be transmitted anywhere else; it remains local. For details, see the section called LAN Connection Guidelines.

- The ethernet camera will consume an average of 5.4 Mb/s of bandwidth. However, the camera is capable of consuming up to 97 Mb/s of bandwidth in bursts on a 100 Mb/s ethernet link. This bandwidth consumption is from the camera to the phone. Bandwidth utilization from the phone to the camera is insignificant. Due to the high burst rates that can occur between the camera and the phone, specific recommendations regarding the method used to physically connect the camera and the phone to the LAN are provided in the section called LAN Connection Guidelines.
- The phone Gigabit ethernet port and all network segments should be configured for full duplex operation; half duplex operation would double the bandwidth requirements on this connection. Half duplex operation is not recommended.

Determining bandwidth usage for a two-party video conference is fairly straight forward since both parties will use equal amounts of bandwidth.

However, determining bandwidth usage for a three-party or four-party video conference is a bit more complicated because the phone that initiates the video conference will also act as the video bridge. The video bandwidth requirements to and from the phone serving as the video bridge will be higher than the video bandwidth requirements for phones that are **participants** because traffic must flow to and from each participant to the bridge.

The required amounts of bandwidth are provided in the next section.

- When transmitting H.264 video, there will be both an average rate of bandwidth consumption and occasional bursts of bandwidth consumption that will exceed the average rate. The transmission of H.264 video consists of an occasional large video frame update followed by many more minor video frame updates. This drastically reduces the amount of bandwidth that would have been required if the video were in a raw, uncompressed format.

When specifying a WAN link, it's a common practice to reserve or guarantee a certain amount of the bandwidth for an application, in this case video, but also to allow this application to peak into other allocations, if the bandwidth is available.

For example, given a 100 Mb/s link, the minimum guarantee rate might be set to support a four-party conference with an average rate of 6.3 Mb/s. But, if the other 93.7 Mb/s of bandwidth on this link is available, then the video could be allowed to use this. The ability to fully handle the burst rate means minimal contention on the link, and faster display updates.

Video Bandwidth Optimization

Release 2.0 includes the following video bandwidth utilization improvements over Release 1.0:

- The phone now supports both the High Profile and Base Line Profile versions of the H.264 video CODEC.
- While maintaining video quality, the bandwidth required to transmit a video stream has been reduced.
  - In Release 1.0 a single video stream requires 2.1 Mb/s of bandwidth.
  - In Release 2.0 a single video stream requires 1.5 Mb/s of bandwidth.
- While the reduction in bandwidth requirements for a single video stream is significant, the benefit for 3-party and 4-party video conferences is even greater.
- For installations that must use low bandwidth connections, such as Teleworker Applications, some new settings under the 'Cable/DSL' menu have been introduced that allow the user to limit the maximum amount of bandwidth required by the phone for both the uplink (transmit) and the downlink (receive) directions.
- Dynamic Bandwidth Allocation (DBA) is a new feature in Release 2.0 that allows the phone to dynamically reduce the amount of data it is transmitting when it has been determined that the connection is congested. When the congestion condition clears, the phone will return to its normal transmit speed.

Video Bandwidth Required for a Two-Party Conference

To support a two-party video conference, both phones will require identical bandwidth provisioning.

Release 1.0

Each phone will require an average bandwidth of 2.1 Mb/s with traffic bursts of up to 12 Mb/s. This means that the WAN link will need to accommodate an average traffic rate of 2.1 Mb/s in both directions and traffic bursts of up to 12 Mb/s in both directions.

If QoS settings have been set correctly, the video traffic will be directed into the WAN router's Assured Forwarding (AF) queue. A typical router configuration may have 30% of the WAN's bandwidth allocated to the AF queue.

Based on a 30% bandwidth allocation for the AF queue, a WAN link of 7 Mb/s will be required to support the average video traffic for a two-party video conference, the Administrator needs to also consider other traffic such as voice and data

The Administrator will be able to configure the routers at the edge of their own network, but the Administrator will not be able to configure the routers owned by the Service Provider. The Administrator needs to ensure that a SLA is in place with the Service Provider and that the SLA defines the QoS policy and the bandwidth requirements.

Release 2.0

Assuming that the Cable/DSL setting is disabled and that Dynamic Bandwidth Allocation is disabled in Video Settings, then each UC360 will require an average bandwidth of 1.6 Mb/s with traffic bursts of up to 12 Mb/s for both the H.264 Baseline CODEC and the H.264 High Profile CODEC.

This means that the WAN link will need to accommodate an average traffic rate of 1.6 Mb/s in both directions and traffic bursts of up to 12 Mb/s in both directions.

If QoS settings have been set correctly, the video traffic will be directed into the router's Assured Forwarding (AF) queue. A typical router configuration may have 30% of the WAN's bandwidth allocated to the AF queue.

Based on a 30% bandwidth allocation for the AF queue, a WAN link of 5.3 Mb/s will be required to support the average video traffic for a two party video conference; the Administrator needs to also consider other traffic such as voice and data

The Administrator will be able to configure the routers at the edge of their own network, but the Administrator will not be able to configure the routers owned by the Service Provider. The Administrator needs to ensure that an SLA is in place with the Service Provider and that the SLA defines the QoS policy and the bandwidth requirements.

Bandwidth Table - Two Party Conference

Figure 7 depicts a two-party video conference. Refer to the associated table to determine what the bandwidth requirements would be on each network segment for a particular UC360 software release. These figures are based on the Cable/DSL setting being disabled and Dynamic Bandwidth Allocation being disabled in Video Settings.

Note that the figures in the following table are the actual bandwidth required by the Video Phone's for video; they do not take into account the WAN router's queue allocations for other traffic such as voice or data. The Administrator must consider the router configuration, other traffic and how it affects the amount of bandwidth purchased from the Network Service Provider.

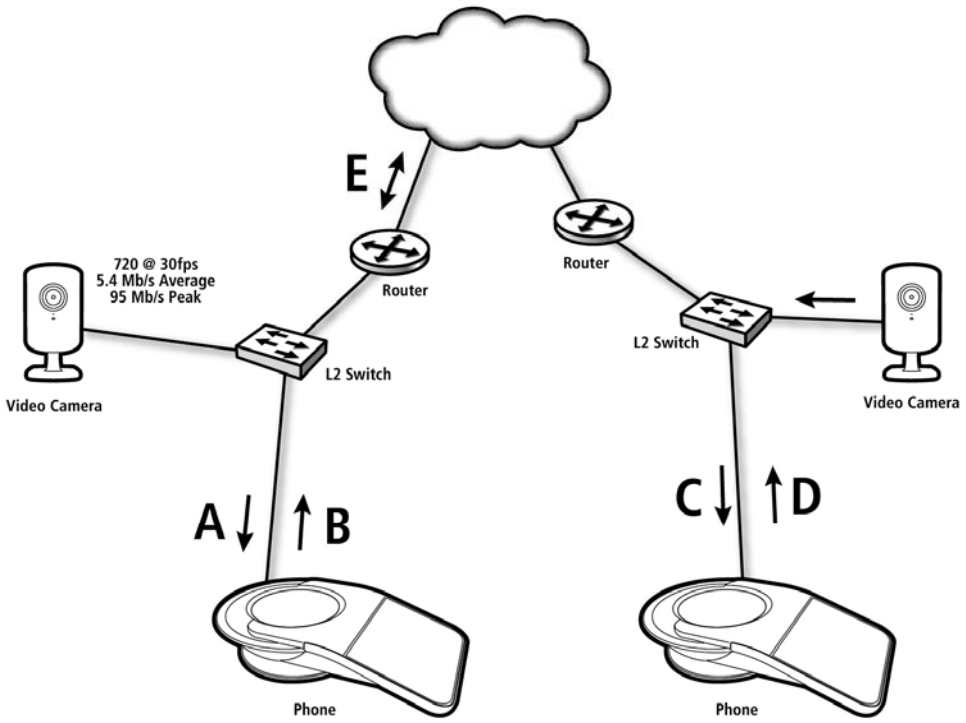

Figure 7. Bandwidth Consumed for a Two-Party Conference

Network Segment	Release 1.0	Release 2.0 Baseline Profile H.264	Release 2.0 High Profile H.264	Notes
A	7.5 Mb/s Average 107 Mb/s Peak	7 Mb/s Average 107 Mb/s Peak	7 Mb/s Average 107 Mb/s Peak	This segment includes traffic from the far end plus traffic from the local camera
B	2.1 Mb/s Average 12 Mb/s Peak	1.6 Mb/s Average 12 Mb/s Peak	1.6 Mb/s Average 12 Mb/s Peak	
C	7.5 Mb/s Average 107 Mb/s Peak	7 Mb/s Average 107 Mb/s Peak	7 Mb/s Average 107 Mb/s Peak	This segment includes traffic from the far end plus traffic from the local camera
D	2.1 Mb/s Average 12 Mb/s Peak	1.6 Mb/s Average 12 Mb/s Peak	1.6 Mb/s Average 12 Mb/s Peak	
E	2.1 Mb/s Average 12 Mb/s Peak	1.6 Mb/s Average 12 Mb/s Peak	1.6 Mb/s Average 12 Mb/s Peak	The bandwidth requirement shown is for each direction on the WAN

Video Bandwidth Required for Three-Party Conference

Determining bandwidth usage for a three-party video conference is a bit more complicated than determining bandwidth usage for a two-party conference because the phone that **initiates** the video conference will also act as the video bridge. The video bandwidth requirements to and from the phone serving as the video bridge will be higher than the video bandwidth requirements for the phone's that are only **participants** because traffic must flow to and from each participant to the bridge.

Release 1.0

In a three-party conference, the highest bandwidth requirement will be on the WAN link connected to the phone that was the **initiator** of the conference. This connection needs to carry traffic to and from both of the far-end phone **participants**.

The WAN link connecting to the conference **initiator** will see an average traffic rate of 4.2 Mb/s in both directions and could experience bursts of up to 24 Mb/s in both directions.

A phone that is strictly a **participant** will require an average bandwidth of 2.1 Mb/s in both directions with traffic bursts of up to 12 Mb/s in both directions.

If QoS settings have been set correctly, the video traffic will be directed into the WAN router's Assured Forwarding (AF) queue. A typical router configuration may have 30% of the WAN's bandwidth allocated to the AF queue.

Based on a 30% bandwidth allocation for the AF queue:

- The WAN link connecting to the phone that is the initiator will require 14 Mb/s of bandwidth (based on a 30% AF queue allocation).
- If the Administrator would like all three parties to be capable of initiating a video conference, then each party's WAN link will need to be provisioned for 14 Mb/s of bandwidth (based on a 30% AF queue allocation).
- If both party 1 and party 2 are never going to be conference initiators, then both of these party's WAN links could be provisioned with 7 Mb/s of bandwidth (based on a 30% AF queue allocation).

> **Note:** This last point must be carefully considered when deploying the phone in an office that may have a low capacity WAN link. Since the WAN link may not be capable of providing the necessary bandwidth for a phone that is originating a conference, the Administrator may need to place restrictions on this phone.

The Administrator will be able to configure the routers at the edge of their own network, but the Administrator will not be able to configure the routers owned by the Service Provider. The Administrator needs to ensure that an SLA is in place with the Service Provider and that the SLA defines the QoS policy and the bandwidth requirements.

Release 2.0

In this scenario it is assumed that for all three phone's, the Cable/DSL setting is disabled and Dynamic Bandwidth Allocation is disabled in Video Settings.

In a three-party conference, the highest bandwidth requirement will be on the WAN link connected to the phone that was the **initiator** of the conference. This connection needs to carry traffic to and from both of the far-end phone **participants**.

This means that the WAN link connecting to the conference **initiator** may need to accommodate an average traffic rate of 3 Mb/s and traffic bursts of up to either 20 Mb/s.

A phone that is strictly a **participant** may require an average bandwidth of 1.5 Mb/s with traffic bursts of up to 9.6 Mb/s.

Note that the specific bandwidth requirements are dependant on the video CODEC in use, for specific values see Figure 8. **Bandwidth Consumed for a Three-Party Conference**.

If QoS settings have been set correctly, the video traffic will be directed into the router's Assured Forwarding (AF) queue. A typical router configuration may have 30% of the WAN's bandwidth allocated to the AF queue.

Based on a 30% bandwidth allocation for the AF queue:

- The WAN link connecting to the phone that is the initiator may require up to 10 Mb/s of bandwidth (based on a 30% AF queue allocation).
- If the Administrator would like all three parties to be capable of initiating a video conference, then each party's WAN link may need to be provisioned for 10 Mb/s of bandwidth (based on a 30% AF queue allocation).
- If both party 1 and party 2 are never going to be conference initiators, then both of these party's WAN links might be provisioned with 5 Mb/s of bandwidth (based on a 30% AF queue allocation).

> **Note:** This last point must be carefully considered when deploying the phone in an office that may have a low capacity WAN link. Since the WAN link may not be capable of providing the necessary bandwidth for a phone that is originating a conference, the Administrator may need to place restrictions on this phone.

The Administrator will be able to configure the routers at the edge of their own network, but the Administrator will not be able to configure the routers owned by the Service Provider. The Administrator needs to ensure that an SLA is in place with the Service Provider and that the SLA defines the QoS policy and the bandwidth requirements.

Bandwidth Table - Three Party Conference

Figure 8 depicts a three-party video conference. Refer to the associated table to determine what the bandwidth requirements would be on each segment for a particular phone software release. These figures are based on the Cable/DSL setting being disabled and Dynamic Bandwidth Allocation being disabled.

Note that the figures in the following table are the actual bandwidth required by the phone's for video; they do not take into account the WAN router's queue allocations for other traffic such as voice or data. The Administrator must consider the router configuration, other traffic and how it affects the amount of bandwidth purchased from the Network Service Provider.

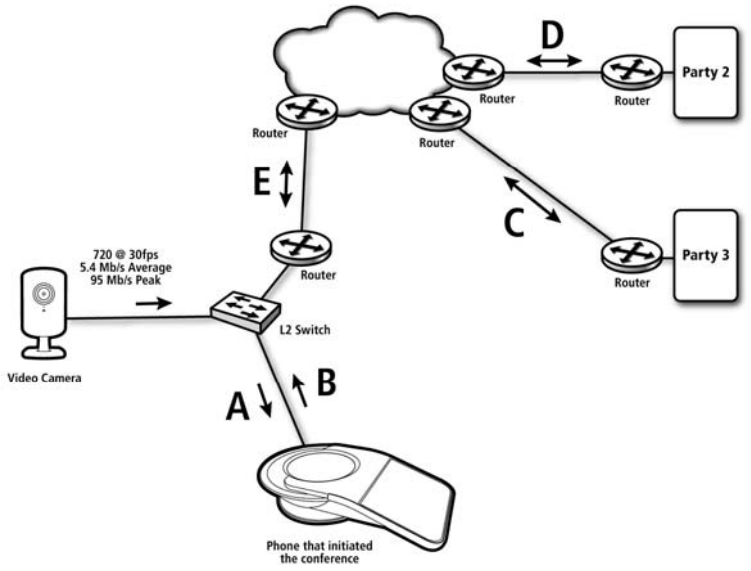

Figure 8. Bandwidth Consumed for a Three-Party Conference

Network Segment	Release 1.0	Rel 2.0 Baseline Profile H.264	Rel 2.0 High Profile H.264	Notes
A	9.6 Mb/s Average 119 Mb/s Peak	7.4 Mb/s Average 110 Mb/s Peak	6.6 Mb/s Average 106 Mb/s Peak	Segment includes traffic from the far end plus traffic from the local camera
B	4.2 Mb/s Average 24 Mb/s Peak	3.0 Mb/s Average 19.2 Mb/s Peak	3.2 Mb/s Average 19.6 Mb/s Peak	Segment includes traffic being transmitted to both far end phones from the bridge
C	2.1 Mb/s Average 12 Mb/s Peak 2.1 Mb/s Average 12 Mb/s Peak	1.0 Mb/s Average 7.6 Mb/s Peak 1.5 Mb/s Average 9.6 Mb/s Peak	0.63 Mb/s Average 5.7 Mb/s Peak 1.6 Mb/s Average 9.8 Mb/s Peak	The bandwidth requirements shown are for both directions, the first pair of numbers are to the bridge, the second pair of numbers are from the bridge. (For local camera bandwidth requirements refer to the section on Two Party Conferences)
D	2.1 Mb/s Average 12 Mb/s Peak 2.1 Mb/s Average 12 Mb/s Peak	1.0 Mb/s Average 7.6 Mb/s Peak 1.5 Mb/s Average 9.6 Mb/s Peak	0.63 Mb/s Average 5.7 Mb/s Peak 1.6 Mb/s Average 9.8 Mb/s Peak	The bandwidth requirements shown are for both directions, the first pair of numbers are to the bridge, the second pair of numbers are from the bridge. (For local camera bandwidth requirements refer to the section on Two Party Conferences)
E	4.2 Mb/s Average 24 Mb/s Peak 4.2 Mb/s Average 24 Mb/s Peak	2.0 Mb/s Average 15.2 Mb/s Peak 3.0 Mb/s Average 19.2 Mb/s Peak	1.26 Mb/s Average 11.4 Mb/s Peak 3.2 Mb/s Average 19.6 Mb/s Peak	The bandwidth requirements shown are for both directions, the first pair of numbers are to the bridge, the second pair of numbers are from the bridge.

Video Bandwidth Required for a Four-Party Conference

Determining bandwidth usage for a four-party video conference is a bit more complicated than determining bandwidth usage for a two-party conference because the Video Phone that **initiates** the video conference will also act as the video bridge. The video bandwidth requirements to and from the phone serving as the video bridge will be higher than the video bandwidth requirements for the phones that are only **participants** because traffic must flow to and from each participant to the bridge.

Release 1.0

In a four-party conference, the highest bandwidth requirement will be on the WAN link connected to the phone that was the **initiator** of the conference. This connection needs to carry traffic to and from all three of the far-end phone **participants**.

The WAN link connecting to the conference **initiator** will see an average traffic rate of 6.3 Mb/s in both directions and could experience bursts of up to 36 Mb/s in both directions.

A phone that is strictly a **participant** will require an average bandwidth of 2.1 Mb/s in both directions with traffic bursts of up to 12 Mb/s in both directions.

If QoS settings have been set correctly, the video traffic will be directed into the WAN router's Assured Forwarding (AF) queue. A typical router configuration may have 30% of the WAN's bandwidth allocated to the AF queue.

Based on a 30% bandwidth allocation for the AF queue:

- The WAN link connecting to the phone that is the initiator will require 21 Mb/s of bandwidth (based on a 30% AF queue allocation).
- If the Administrator would like all four parties to be capable of initiating a video conference, then each party's WAN link will need to be provisioned for 21 Mb/s of bandwidth (based on a 30% AF queue allocation).
- If party 1, party 2 and party 3 are never going to be conference initiators, then both of these party's WAN links could be provisioned with 7 Mb/s of bandwidth (based on a 30% AF queue allocation).

> **Note:** This last point must be carefully considered when deploying the phone in an office that may have a low capacity WAN link. Since the WAN link may not be capable of providing the necessary bandwidth for a phone that is originating a conference, the Administrator may need to place restrictions on this phone.

The Administrator will be able to configure the routers at the edge of their own network, but the Administrator will not be able to configure the routers owned by the Service Provider. The Administrator needs to ensure that a SLA is in place with the Service Provider and that the SLA defines the QoS policy and the bandwidth requirements.

Release 2.0

Assuming that for all four phones the Cable/DSL setting is disabled and that Dynamic Bandwidth Allocation is disabled, then:

In a four-party conference, the highest bandwidth requirement will be on the WAN link connected to the phone that was the **initiator** of the conference. This connection needs to carry traffic to and from all three of the far-end phone **participants**.

This means that the WAN link connecting to the conference **initiator** may need to accommodate an average traffic rate of 4.8 Mb/s and bursts of up to 29 Mb/s.

A phone that is strictly a **participant** may require an average bandwidth of 1.0 Mb/s with traffic bursts of up to 7.6 Mb/s.

Note that the specific bandwidth requirements are dependant on the video CODEC in use, for specific values see Figure 9. **Bandwidth Consumed for a Four-Party Conference**.

If QoS settings have been set correctly, the video traffic will be directed into the router's Assured Forwarding (AF) queue. A typical router configuration may have 30% of the WAN's bandwidth allocated to the AF queue.

Based on a 30% bandwidth allocation for the AF queue:

- The WAN link connecting to the phone that is the initiator may require 16 Mb/s of bandwidth (based on a 30% AF queue allocation).
- If the Administrator would like all four parties to be capable of initiating a video conference, then each party's WAN link will need to be provisioned for 16 Mb/s of bandwidth (based on a 30% AF queue allocation).
- If both party 1, party 2 and party 3 are never going to be conference initiators, then both of these party's WAN links could be provisioned with 3.3 Mb/s of bandwidth (based on a 30% AF queue allocation).

> **Note:** This last point must be carefully considered when deploying the phone in an office that may have a low capacity WAN link. Since the WAN link may not be capable of providing the necessary bandwidth for a phone that is originating a conference, the Administrator may need to place restrictions on this phone.

The Administrator will be able to configure the routers at the edge of their own network, but the Administrator will not be able to configure the routers owned by the Service Provider. The Administrator needs to ensure that a SLA is in place with the Service Provider and that the SLA defines the QoS policy and the bandwidth requirements.

Bandwidth Table – Four-Party Conference

Figure 9 depicts a four party video conference. Refer to the associated table to determine what the bandwidth requirements would be on each segment for a particular phone software release. These figures are based on the Cable/DSL setting being disabled and Dynamic Bandwidth Allocation being disabled.

Note that the figures in the following table are the actual bandwidth required by the phones for video, they do not take into account the WAN router's queue allocations for other traffic such as voice or data. The Administrator must consider the router configuration, other traffic and how it affects the amount of bandwidth purchased from the Network Service Provider.

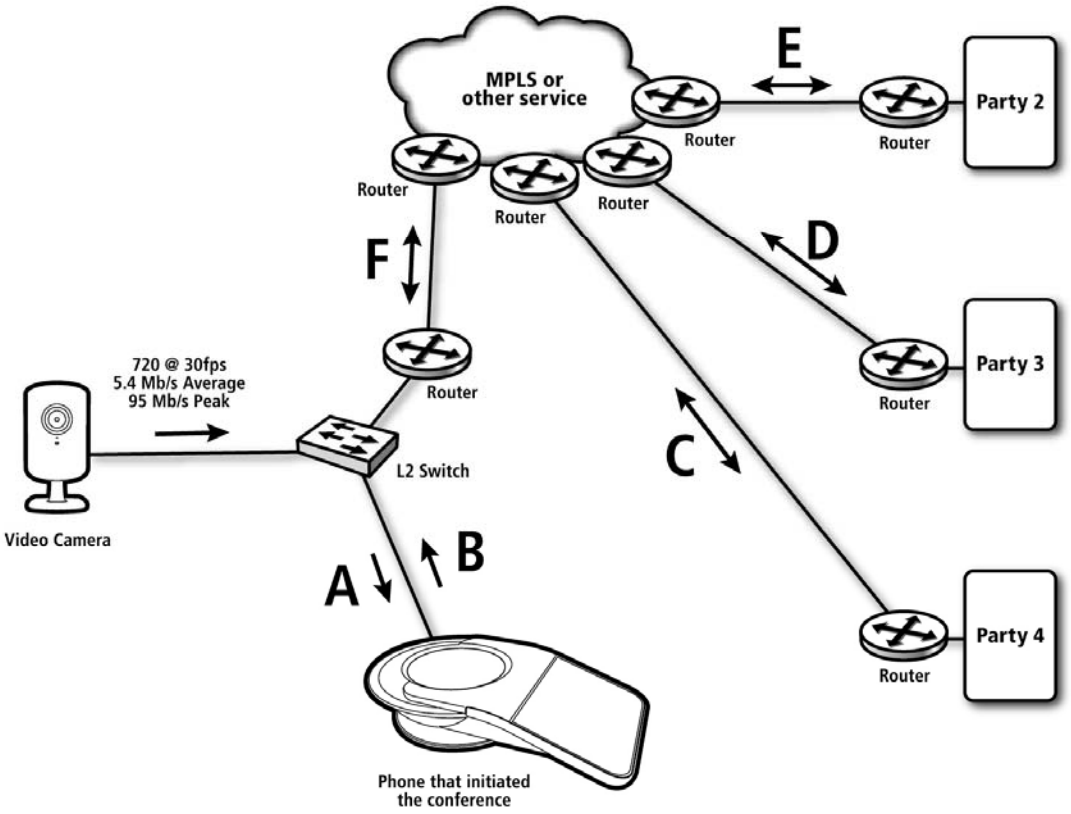

Figure 9. Bandwidth Consumed for a Four-Party Conference

Network Segment	Release 1.0	Release 2.0 Baseline Profile H.264	Release 2.0 High Profile H.264	Notes
A	11.7 Mb/s Average 131 Mb/s Peak	8.4 Mb/s Average 117.8 Mb/s Peak	7.29 Mb/s Average 112.1 Mb/s Peak	This segment includes traffic from the far end plus traffic from the local camera
B	6.3 Mb/s Average 36 Mb/s Peak	4.5 Mb/s Average 28.8 Mb/s Peak	4.8 Mb/s Average 29.4 Mb/s Peak	This segment includes traffic being transmitted to all far end phones from the bridge
C	2.1 Mb/s Average 12 Mb/s Peak	1.0 Mb/s Average 7.6 Mb/s Peak 1.5 Mb/s Average 9.6 Mb/s Peak	0.63 Mb/s Average 5.7 Mb/s Peak 1.6 Mb/s Average 9.8 Mb/s Peak	The bandwidth requirements shown are for both directions, the first pair of numbers are to the bridge, the second pair of numbers are from the bridge. (For local camera bandwidth requirements refer to the section on Two Party Conferences)
D	2.1 Mb/s Average 12 Mb/s Peak	1.0 Mb/s Average 7.6 Mb/s Peak 1.5 Mb/s Average 9.6 Mb/s Peak	0.63 Mb/s Average 5.7 Mb/s Peak 1.6 Mb/s Average 9.8 Mb/s Peak	The bandwidth requirements shown are for both directions, the first pair of numbers are to the bridge, the second pair of numbers are from the bridge. (For local camera bandwidth requirements refer to the section on Two Party Conferences)
E	2.1 Mb/s Average 12 Mb/s Peak	1.0 Mb/s Average 7.6 Mb/s Peak 1.5 Mb/s Average 9.6 Mb/s Peak	0.63 Mb/s Average 5.7 Mb/s Peak 1.6 Mb/s Average 9.8 Mb/s Peak	The bandwidth requirements shown are for both directions, the first pair of numbers are to the bridge, the second pair of numbers are from the bridge. (For local camera bandwidth requirements refer to the section on Two Party Conferences)
F	6.3 Mb/s Average 36 Mb/s Peak	3.0 Mb/s Average 22.8 Mb/s Peak 4.5 Mb/s Average 28.8 Mb/s Peak	1.89 Mb/s Average 17.1 Mb/s Peak 4.8 Mb/s Average 29.4 Mb/s Peak	The bandwidth requirements shown are for both directions, the first pair of numbers are to the bridge, the second pair of numbers are from the bridge.

Bandwidth Limiting

For installations that must use low bandwidth connections, such as Teleworker Applications, some new settings have been introduced that allow the user to limit the maximum amount of bandwidth required by the phone for both the uplink (transmit) and the downlink (receive) directions. These settings are found under the Cable/DSL menu under Settings -> Advanced -> System Settings -> Video Settings.

Three different bandwidth settings can be independently applied to the uplink and downlink connections:

- High – limits the bandwidth to 1.5 Mb/s
- Medium – limits the bandwidth to 1.0 Mb/s
- Low – limits the bandwidth to 512 kb/s

The bandwidth limiting selections available under the Cable/DSL menu result in the behavior described in the sections below.

Two-party Video Conference

- When a user sets the phone uplink speed to high, medium or low, the phone will limit its own transmit rate according to the setting.
- When the user sets the phone downlink speed to high, medium or low, the phone will advertise this setting via SIP messages to the far end conference participant, the far end conference participant will limit its transmit rate accordingly.

Three-party or Four-Party Video Conferences

The phone that initiated the conference will also be performing the video bridging function. If a participant (non-bridge) phone has requested that bandwidth being sent to it be limited, then all participants will receive the same limited bandwidth. In the case where two participant phones have requested that they receive limited bandwidth and the participant phone's have requested different limits, the lowest requested limit will be applied to transmissions to all phone participants. For example:

- The phone that is the bridge receives a request from participant 'A' to limit the bandwidth being sent to participant 'A' at 512 kb/s.
- The phone that is the bridge receives a request from participant 'B' to limit the bandwidth being sent to participant 'B' at 1.0 Mb/s.
- The phone that is the bridge receives a request from participant 'C' to limit the bandwidth being sent to participant 'A' at 1.5 Mb/s.

The end result will be that the bridge phone will limit bandwidth at 512 kb/s to all three phone participants.

> **Note:** The Administrator should be aware that limiting the bandwidth to 512 kb/s will result in a slightly degraded video quality compared to video quality that is bandwidth limited to 1.0 Mb/s or 1.5 Mb/s.

Dynamic Bandwidth Allocation

Release 2.0 includes Dynamic Bandwidth Allocation (DBA) which is a new feature that allows the phone to dynamically reduce the amount of data it is transmitting when it has determined that the connection is congested. When the congestion condition clears the phone will return to its normal transmit speed.

The phone's DBA feature uses the Real Time Control Protocol (RTCP) to collect quality of service statistics from the far-end phone.

Based on these statistics, the sending phone can determine if the far end phone is experiencing packet loss, then, if necessary the transmitting phone can take corrective action.

RTCP is a companion protocol to the Real Time Protocol (RTP), RTCP collects statistics for a specific media connection; it does not transport any media packets itself.

RTP packets are usually transmitted on an even port number, and the associated RTCP packets are usually transmitted on the next higher odd port number.

By default, DBA uses 1.5 Mb/s as the maximum transmit speed. However, if bandwidth limiting has been enabled under the 'Cable/DSL' menu, then DBA will use the maximum transmit speed selected in the 'Cable/DSL' menu as the maximum transmit speed for DBA.

If using DBA, the Administrator should ensure that RTCP pass through is enabled on the applicable network routers. For details on how to enable DBA, refer to the *MiVoice Conference/Video Administration Guide*.

> **Note:** The Administrator should be aware that MBG does not support RTCP pass through, as a result the Administrator should ensure that DBA is disabled on any phone that is connected to an MBG

Multiple Four-Party Conferences

As discussed earlier, a four-party video conference will require that the WAN be provisioned to support the expected average and burst video traffic of one four-party video conference.

If there were a requirement to support a second four-party video conference across the same WAN link, then the Administrator will need to ensure that the WAN bandwidth is scaled up to accommodate the additional bandwidth.

For example, if a four-party video conference (conference ‘A’) is underway that consumes 6.3 Mb/s of WAN bandwidth and another four party video conference (conference ‘B’, which requires 6.3 Mb/s of bandwidth) is initiated across the same WAN link, there is going to be a doubling of the WAN bandwidth requirements.

The WAN will now need to be able to support an average of 12.6 Mb/s of video traffic. If this extra bandwidth requirement is not accounted for, it is likely that both video conference ‘A’ and ‘B’ will experience severe degradation.

As an alternative to over-provisioning the network for multiple 4-party conferences, it is recommended that the System Administrator make use of a system such as Lotus Notes Calendar or Google Calendar. Calendar tools can assist users with management of phone Conferencing resources and bandwidth resources.

Remote Desktop Protocol (RDP) Bandwidth Requirements

The Remote Desktop Protocol bandwidth requirements are shown below. Typically, the RDP traffic will be confined to the LAN, since the traffic flow is between the user's remote PC and the phone.

- When there are no display updates in the RDP session, the bandwidth utilized will be less than 1 kb/s.
- During a RDP session when there is a full window update, there will be a burst of traffic about 500 ms long that will consume 1 Mb/s or less of bandwidth.
- During an RDP session when the user has edited a document such as an Excel spreadsheet, the bandwidth consumed will typically be less than 10 kb/s.

Bandwidth Availability on Various Connections

The advertised data rate for a particular link 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.

NA Carriers are making WAN connections available in multiples of T1 links, so it is possible to purchase digital trunks that have bandwidth capacities of for example 3 Mb/s, 6 Mb/s and 9 Mb/s.

The following table provides some simple guidelines for LAN and WAN links.

Table 20. Bandwidth Availability

Data Connection Type	Percentage of Bandwidth Available	Example
LAN 100 BaseT Half Duplex	40%	100 Mb/s = 40 Mb/s available
LAN 100 BaseT Full Duplex	80%	100 Mb/s = 80 Mb/s available
LAN 1000 BaseT Half Duplex	40%	1000 Mb/s = 400 Mb/s available
LAN 1000 BaseT Full Duplex	80%	1000 Mb/s = 800 Mb/s available
WAN 1.5 Mb/s without QoS mechanism in router	40%	1.5 Mb/s = 600 Kb/s available
WAN 1.5 Mb/s with QoS mechanism in router	70%	1.5 Mb/s = 1.05 Mb/s available
WAN 3.0 Mb/s without QoS mechanism in router	40%	3.0 Mb/s = 1.2 Mb/s available
WAN 3.0 Mb/s with QoS mechanism in router	70%	3.0 Mb/s = 2.1 Mb/s available
WAN 6.0 Mb/s without QoS mechanism in router	40%	6.0 Mb/s = 2.4 Mb/s available
WAN 6.0 Mb/s with QoS mechanism in router	70%	6.0 Mb/s = 4.2 Mb/s available
WAN 9.0 Mb/s without QoS mechanism in router	40%	9.0 Mb/s = 3.6 Mb/s available
WAN 9.0 Mb/s with QoS mechanism in router	70%	9.0 Mb/s = 6.3 Mb/s available

IP Ports and Firewall Configuration

An IP end point is defined by the combination of an IP address and an IP port identifier or socket. IP ports are used to establish a communication path between two end points, typically a server and a client.

The Administrator needs to be aware of the IP ports used by a particular network device so that:

- Based on specific port numbers, communication paths can be opened across firewalls.
- If Policy Based Routing is employed, the router can be properly configured based on port numbers.

IP Port Usage

The following Table lists all of the IP ports used by the phone, the protocol associated with the port number, and what the connection is used for. In the table below, *Phone* refers to the phone.

Table 21. TCP I/P Ports Used by the Conference/Video Phone

IP Port Number	Protocol	Internal or External	Usage	Notes
53	UDP	Phone to LAN	DNS	
67	UDP	Phone to LAN	DHCP to Server	
68	UDP	LAN to Phone	DHCP to Client	
80	TCP	Phone to LAN LAN to Phone	HTTP for Web Collaboration HTTP for Remote Diagnostics Web Server	
123	UDP	Phone to LAN	NTP	
389	TCP	Phone to LAN	LDAP	
443	TCP	Phone to LAN LANT to Phone	HTTPS for Web Collaboration HTTP for Remote Diagnostics Web Server	
636	TCP	Phone to LAN	LDAPS (SSL)	
3389	TCP	Phone to LAN	RDP	
5060	TCP	Phone to LAN LAN to Phone	SIP	
5061	UDP	Phone to LAN LAN to Phone	SIP-TLS	
5555	TCP	LAN to Phone	Android Debug (ADB)	
20000	UDP	LAN to Phone	RxSource to IP Phone analyzer	
20000 (Source)	UDP	Phone to LAN	TxSource to IP Phone analyzer	
48879	UDP	Phone to LAN LAN to Phone	IP Phone Analyzer	Connects to/from ports 2000 & 20002
50000 to 50511	UDP	Phone to LAN LAN to Phone	Voice & Video	Symmetrically assigned. Media: Even Number RTCP: Odd Number

Interoperating with Routers that are using Policy Based Routing

Policy Based Routing (PBR) allows the System Administrator to configure the router so that the router will route packets based on IP address, port numbers, protocol, or packet size.

PBR can also use these same parameters to re-map the packet's DSCP bits.

PBR can also be used to specify specific network paths for certain types of traffic, for example, packets that require a high level QoS such as video or voice might be routed over a traffic engineered path to ensure a high level of QoS through the network.

When PBR is to be employed, the System Administrator will need to configure PBR on the routers so that specific TCP I/P port numbers associated with the phone are mapped to an appropriate Policy Based Routing scheme and/or network connection.

The following table lists the port numbers associated with the Conference/Video, their application and what type of PBR scheme should be used.

Table 22. Conference/Video Phone Port Numbers Required for PBR

TCP I/P Port	Protocol	Application	Mitel Service Class Level
Not Applicable	ICMP	Ping	Standard
53	UDP	DNS	Standard
67	UDP	DHCP to Server	Standard
68	UDP	DHCP to Client	Standard
80	TCP	HTTP for Web Collaboration	Standard
123	UDP	NTP	Standard
389	TCP	LDAP	Standard
443	TCP	HTTPS for Web Collaboration (SSL)	Standard
636	TCP	LDAPS (SSL)	OAM (Operation, Administration & Maintenance)
3389	TCP	RDP	Standard
5060	TCP/UDP	SIP	Signaling
5061	TCP	SIP-TLS	Signaling
5555	TCP	Android Debug (ADB)	Standard
20000	UDP	RxSource to IP Phone analyzer	OAM
20000	UDP	TxSource to IP Phone analyzer	OAM
48879	UDP	IP Phone Analyzer	OAM
50000 to 50511	UDP	Voice & Video	Telephony & Multimedia Conferencing

The following diagram shows all of the IP ports that the Conference/Video Phone uses for communicating with other devices, applications and data bases. In the diagram, the arrows indicate the direction of data transmission and the port numbers used.

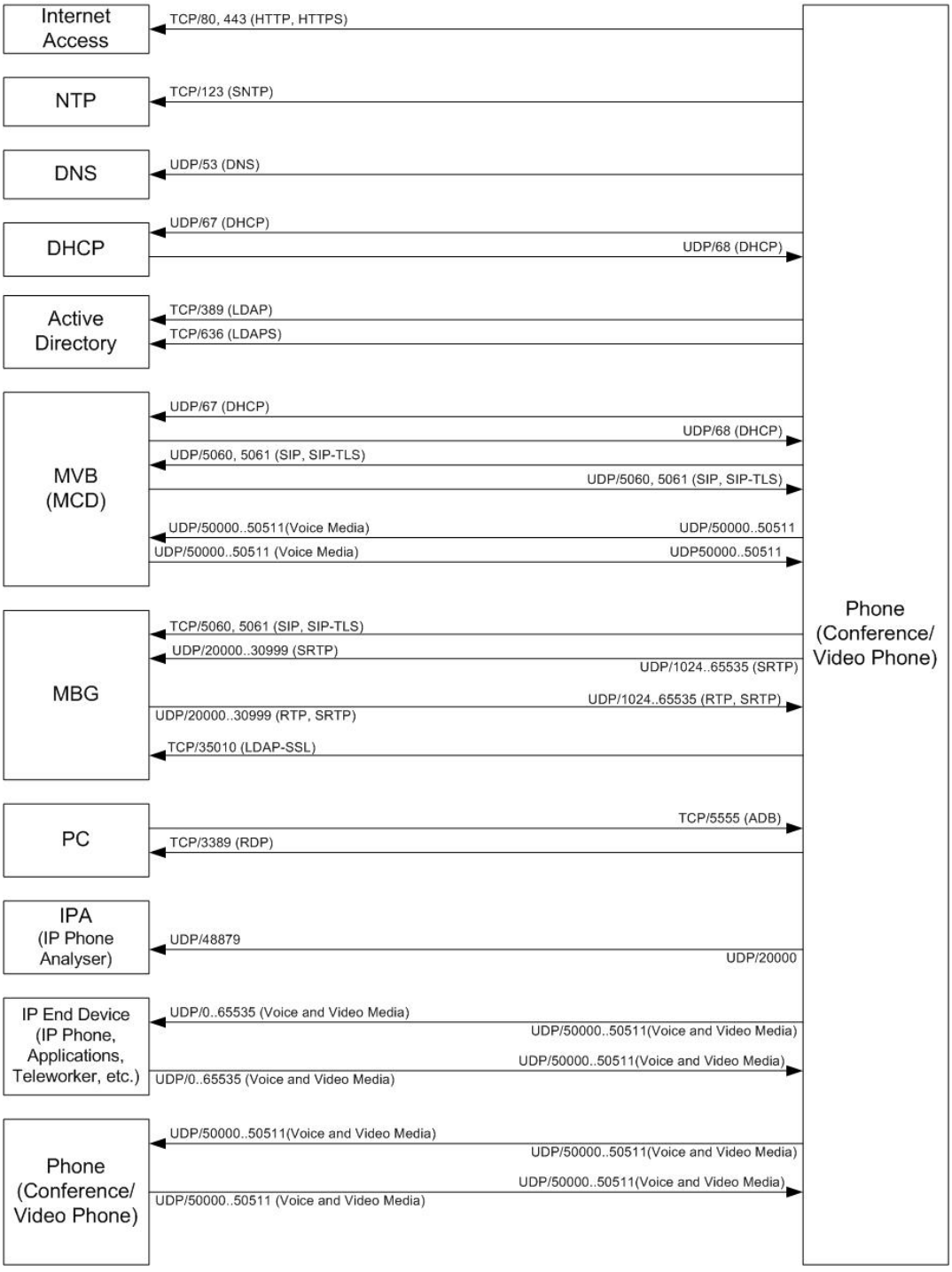

Figure 10. Conference/Video Phone IP Ports

Requirements for Firewall Traversal

For communication paths to be established ‘across’ a firewall or router it is necessary for the system administrator to program the firewall so that specific IP ports are not blocked so that communication paths can be established between the IP end points.

The following table indicates which ports are required for the phone to communicate with other end points. In the table below, phone refers to the phone.

Table 23. Ports Required for Firewall Traversal

IP Port Number	From/To	Purpose
80	Phone to LAN/WAN	HTTP for Web Collaboration
123	Phone to LAN/WAN LAN/WAN to Phone	NTP - Used to access a time server, for setting the Phone time of day clock
443	Phone to LAN/WAN	HTTPS for Web Collaboration
5060	Phone to LAN LAN to Phone	SIP
5061	Phone to LAN LAN to Phone	SIP-TLS
50000 to 50511	Phone to LAN LAN to Phone	Voice and Video

Conference/Video Phone Micro-Firewall

The phone contains a micro-firewall or packet filter. This firewall can be enabled or disabled via the Tools and Features menu. The firewall filtering parameters themselves are non-configurable.

When the firewall is enabled, it will discard packets that are not relevant to the phone. The firewall also acts as a packet limiter which means that if there is a burst of multiple packets of the same type some of the packets may be discarded based maximum allowable packet rate.

It is recommended that the micro-firewall be enabled as it limits the phone’s susceptibility to network problems and denial of service attacks.

LAN Connection Guidelines

The following sections discuss how to connect the phone and the ethernet camera into the Customer's local area network. Connection and configuration requirements may be different depending on the version of phone software; these differences are discussed for various software loads available.

Recommendations are provided for configurations that use the Mitel Multi Port GigE PoE Switch and also for configurations that do not use the Mitel Multi Port GigE PoE Switch, but instead connect directly to the Customer's LAN.

> **Note:** There are a number of different options available for powering the phone and the ethernet camera.

The particular powering option that the Administrator chooses to use will dictate which one of the network connection topology described in the following sections should be used. For details on powering options see the section called Power.

The Administrator will need to decide on a particular powering option and then connect and configure the phone, camera and L2 switches as recommended in the following sections.

> **CAUTION:** The Administrator should be aware that in general ethernet cameras do not perform IEEE 802.1p/Q tagging. As a result, these cameras will not place the camera's traffic on a specific VLAN and they will not place L2 tags on outgoing packets. Without the correct network design, this untagged traffic from the camera may cause network problems on the customer's LAN.

> **Note:** Release 2.0 introduces a new menu item in the Camera Settings called Search. The Search function invokes the Camera Discovery Protocol which will search for any available camera in the phone's subnet. When a camera is found, its IP address and/or host name is displayed on the phone LCD screen. The Camera Discovery Protocol is a non-routable protocol and will only work when the camera and the phone are located in the same subnet.

Using the Mitel Multi-Port GigE PoE Switch

The Mitel Multi Port GigE Switch is most useful in the following situations:

- Where there is only one ethernet connection available in the room in which the phone is being installed, the Mitel Multi-Port GigE Switch can be used to combine the connection from the phone and the ethernet camera onto the single ethernet connection to the customer's LAN.
- If the room that the phone is being installed in does not have a network connection available that supports IEEE 802.3at PoE (which is required by the phone), then the Mitel Multi-Port GigE Switch can be used to provide connectivity and power to the phone.

Mitel Multi Port GigE Switch - Acceptable Configuration

This section describes how the phone and the camera should be connected and configured for the correct operation. The requirements vary for different versions of the phone software.

Figure 11. Multi-Port GigE PoE Switch – Acceptable Configuration shows how the phone and the ethernet camera **should be** connected to the Mitel Multi-Port GigE PoE Switch.

> **Note:** DSCP values must be correctly set on the phone. For details, see phone Quality of Service Settings. For details, see Conference/Video Phone Quality of Service Settings and Ethernet Camera QoS Settings.

For Release 1 and Release 1 SP1

The phone should have the following parameters manually programmed.

- IP address of the phone
- Subnet Mask
- Default Gateway IP address

Ensure that the DSCP values are correctly set on both the camera and the phone.

Programming these parameters manually (statically) will ensure that the phone will ignore any values obtained via DHCP, LLDP-MED or CDP, as a result the phone will transmit packets without L2 tagging, which is the desired mode of operation for this configuration.

Release 1 SP2

The phone should be configured as follows.

The phone should have VLAN tagging disabled. This setting is found under the Tools and Features menu. When VLAN tagging is disabled, the phone will ignore all VLAN information that might be provided by DHCP, LLDP-MED and CDP. As a result, the phone will transmit packets without L2 tagging, which is the desired mode of operation for this configuration.

Ensure that DSCP values are correctly set on both the Camera and the phone.

As illustrated in Figure 11. Multi-Port GigE PoE Switch – Acceptable Configuration:

- The phone and the ethernet camera will both transmit packets without L2 tagging.
- The camera traffic will be locally switched by the Mitel Multi Port GigE PoE Switch and sent only to the phone, this traffic will not be sent to the Customer’s router.
- Traffic from the phone will be sent to the Mitel Multi Port GigE PoE Switch, which in turn will send the traffic to the Customer’s Network L2 Switch.
- The Customer’s Network L2 Switch must be programmed to tag packets arriving from the Mitel Multi Port GigE PoE Switch to the correct IEEE 802.1 p/Q values based on the packet’s DSCP value.
- The Customer’s Network L2 Switch should also be programmed to strip L2 tagging from packets that are being sent to the Mitel Multi Port GigE PoE Switch.
- It is recommended that the connection between the Mitel Multi-Port GigE PoE Switch and the Customer's Access L2 switch be running at 1 Gb/s, however if 1 Gb/s is not supported a 100 Mb/s connection should provide satisfactory performance.

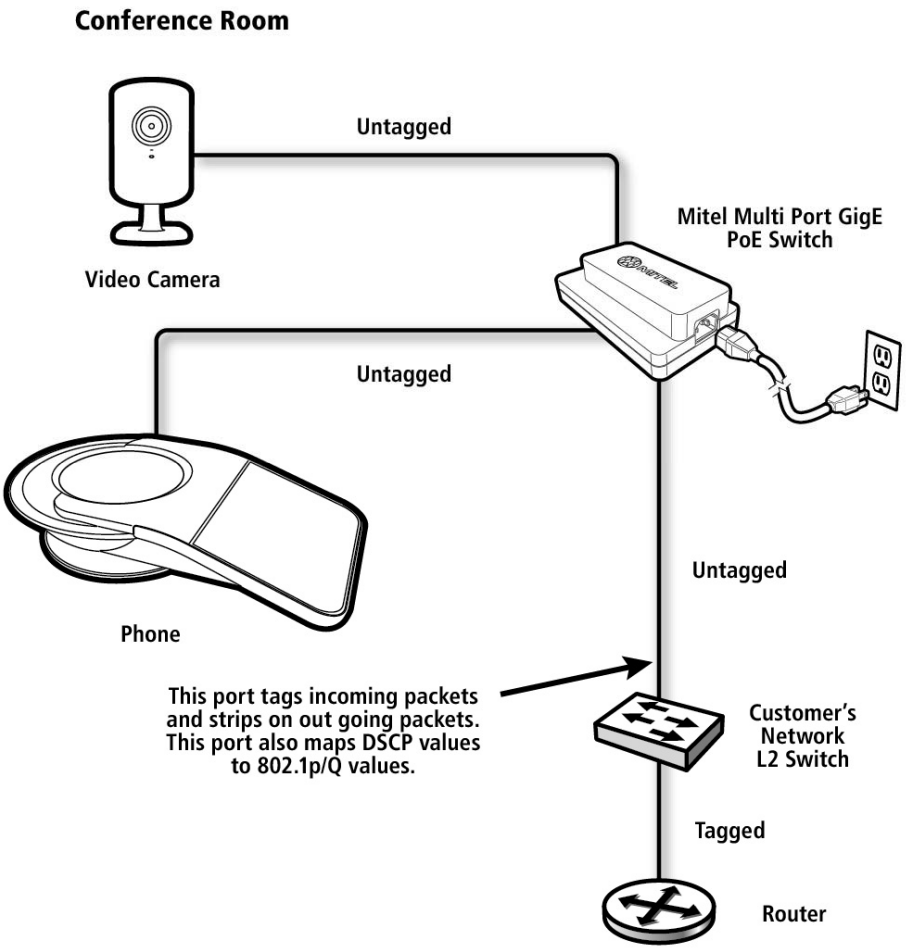

Figure 11. Multi-Port GigE PoE Switch – Acceptable Configuration

Mitel Multi Port GigE Switch - Unacceptable Configuration

The following diagram shows a configuration scenario that **should not be used** to connect the phone and the ethernet camera to the Mitel Multi-Port GigE PoE Switch.

This configuration **is not acceptable** because the traffic from the camera, which has no L2 tagging gets put onto the data VLAN by the Mitel Multi-Port GigE PoE Switch. The traffic is then forced to go to the Customer's network router before it can be redirected back to the phone.

Ethernet cameras can consume significant amounts of LAN bandwidth, and if this traffic is allowed onto the data VLAN there will likely be congestion and packet loss.

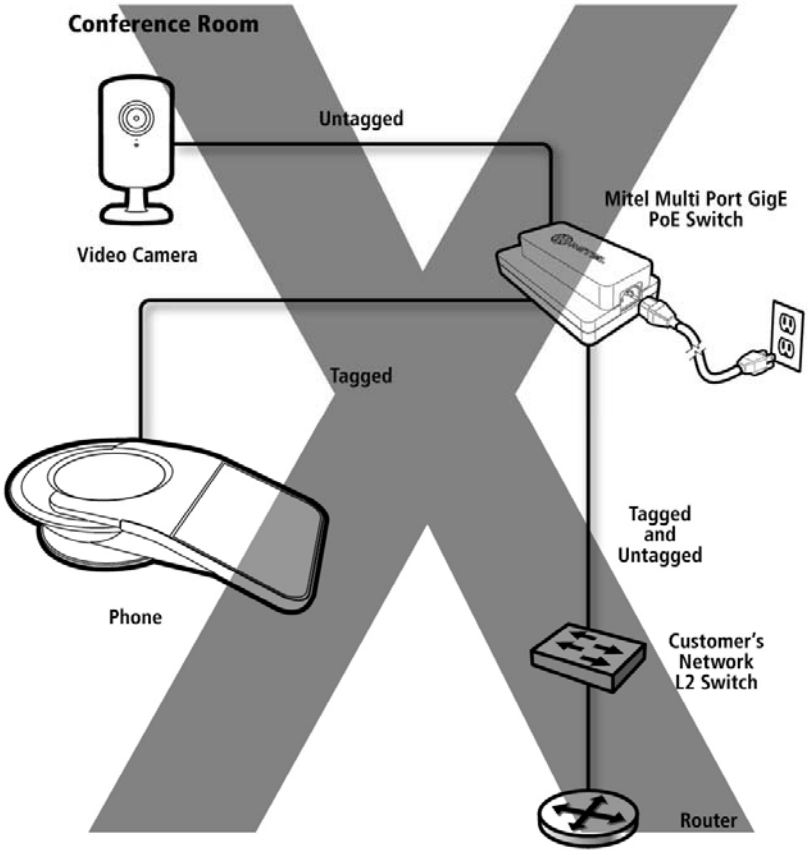

Figure 12. Multi-Port GigE PoE Switch – Unacceptable Configuration

Using the Customer's Network L2 Switch

In some situations, the Mitel Multi-Port GigE PoE Switch may not be required to provide LAN connectivity to the phone and the ethernet camera. In these situations, the phone and the ethernet camera may be connected directly to the Customer's Network L2 Switch if the guidelines below are followed:

- There are two ethernet connections to the Customer's LAN available in the room where the phone is being installed.
- The ethernet camera will typically require a 100 Mb/s connection into the LAN.
- It is recommended that a 1 Gb/s connection be used to connect the phone into the LAN. If a 1 Gb/s connection is not supported, the use of a 100 Mb/s connection may work satisfactorily. However, use of a 100Mb/s connection may cause intermittent packet loss which will degrade the video quality.
- The Customer's Network L2 Switch is IEEE 802.3at PoE compliant.
- The Customer's Network L2 Switch can be programmed to put IEEE 802.1p/Q tags on incoming packets based on the packet's DSCP value.

The following sections provide configuration guidelines for Release 1.0, Release 1.0, SP1 and SP2, and Release 2.0

Configuration for Using the Customer's L2 Switch (Release 1.0, SP1 and SP2)

Figure 13. Configuration for Using Customer's L2 Switch, Release 1.0, SP1 and SP2 below shows the preferred configuration to use if the Administrator wishes to connect the phone and the Ethernet camera directly to Customer's LAN.

> **Note:** DSCP values must be correctly set on the phone, for details see phone Quality of Service Settings**.** For details see Conference/Video Phone Quality of Service Settings and Ethernet Camera QoS Settings.

For Release 1.0 and Release 1.0, SP1

The phone should have the following parameters manually programmed.

- IP address of the phone
- Subnet Mask
- Default Gateway IP address

Ensure that DSCP values are correctly set on both the camera and the phone.

Programming these parameters manually (statically) will ensure that the phone will ignore any values obtained via DHCP, LLDP-MED or CDP. As a result, the phone will transmit packets without L2 tagging, which is the desired mode of operation for this configuration.

For Release 1.0, SP2

The phone should have VLAN tagging disabled. This setting is found under the **Tools and Features** menu. When VLAN tagging is disabled, the phone will ignore all VLAN information that might be provided by DHCP, LLDP-MED and CDP. As a result, the phone will transmit packets without L2 tagging, which is the desired mode of operation for this configuration

Operational Description

As the following diagram illustrates

- The phone and the ethernet camera will both transmit packets without L2 tagging.
- The camera traffic will be locally switched by the Customer's Network L2 Switch and sent only to the phone. This traffic will not be sent to the Customer's router.
- Traffic from the phone will sent to the Customer's Network L2 Switch, which in turn will send the traffic to the Customer's router.
- The Customer's Network L2 Switch must be programmed to tag packets arriving from the phone and the ethernet camera to the correct IEEE 802.1 p/Q values based on the packet's DSCP value.
- The ethernet camera will typically require a 100 Mb/s connection into the LAN.
- It is recommended that a 1 Gb/s connection be used to connect the phone into the LAN. If a 1 Gb/s connection is not supported, the use of a 100 Mb/s connection may work satisfactorily. However, use of a 100Mb/s connection may cause intermittent packet loss which will degrade the video quality.

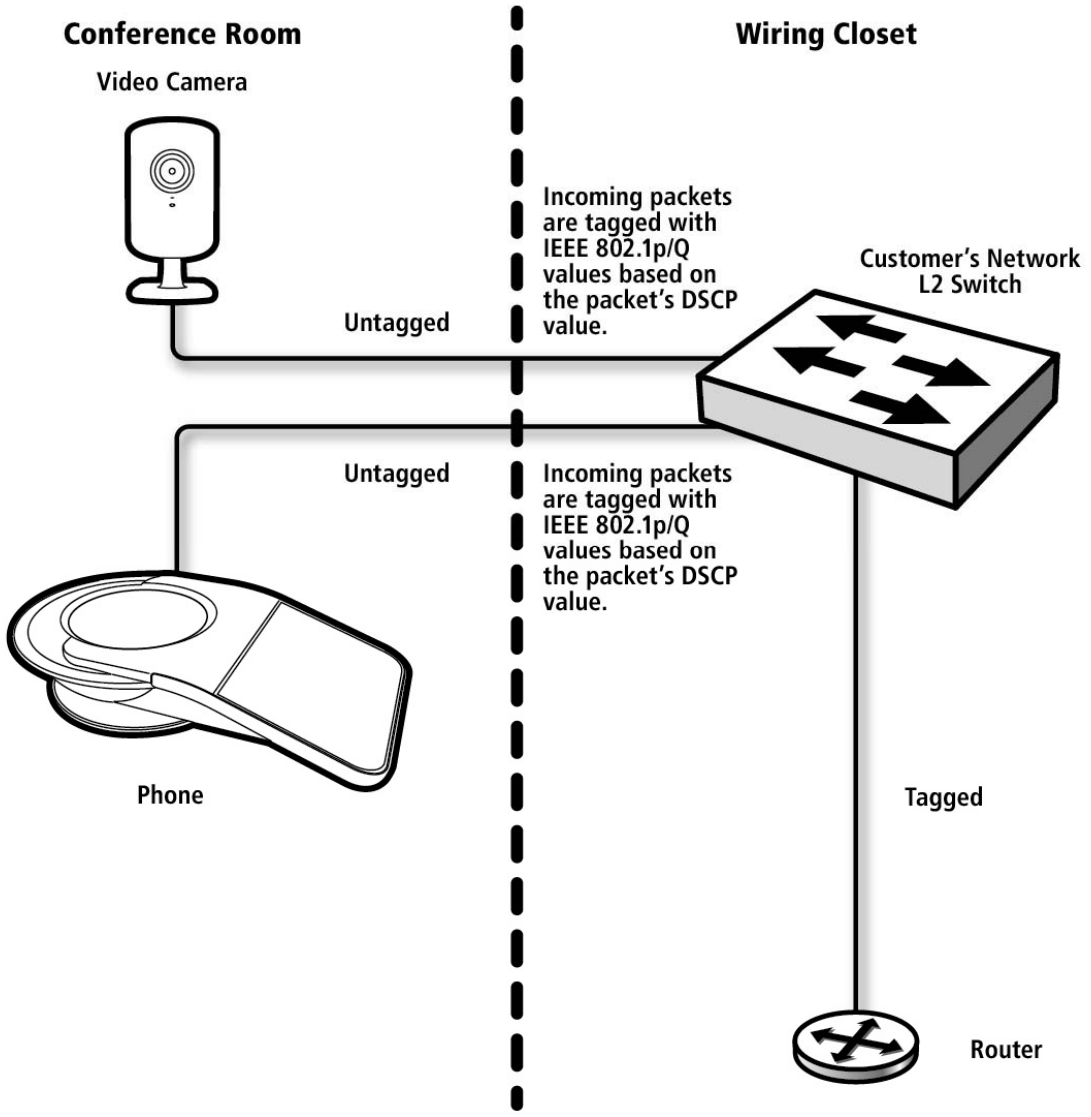

Figure 13. Configuration for Using Customer's L2 Switch, Release 1.0, SP1 and SP2

Configuration for Using the Customer's L2 Switch (Release 2.0)

For Release 2.0, the following diagram Figure 14. Configuration for Using Customer's L2 Switch, Release 2.0 shows the preferred configuration to use if the Administrator wishes to connect the phone and the Ethernet camera directly to the Customer's LAN.

Compared to the preceding configurations for earlier UC360 Releases, this configuration requires the least amount of manual programming by the Administrator.

> **Note:** As a safeguard, DSCP values should be correctly set on the ethernet camera, for details see the Section called phone Quality of Service Settings and the Section called Ethernet Camera QoS Settings. At Release 2.0, the phone has default L2 and L3 QoS values that should be appropriate for most networks.

> **Note:** The Camera Discovery Protocol is a non-routable protocol; it will only work when the camera and the phone are located in the same subnet. For additional details see the section called IP Networking Requirements for Ethernet Cameras.

The phone should have VLAN tagging enabled. This setting is found under the **Tools and Features** menu. When VLAN tagging is enabled, the phone will make use of VLAN information that might be provided by Default Settings, DHCP, LLDP-MED and CDP. As a result, the phone will transmit packets with L2 tagging on a particular VLAN.

Operational Description

As the following diagram illustrates

- For Release 2.0, the phone supports default L2 and L3 QoS values that are appropriate for most networks.
- Ensure that DSCP values are correctly set on both the Camera and the phone.
- The ethernet camera will transmit packets without L2 tagging.
- The Customer's Network L2 Switch must be programmed to tag packets arriving from the ethernet camera to the correct IEEE 802.1 p/Q values based on the packet's DSCP value and the L2 Switch should also be programmed to place the user's traffic on the same VLAN as the phone.
- The camera traffic will be locally switched by the Customer's Network L2 Switch and sent only to the phone, this traffic will not be sent to the Customer's router.
- The phone will transmit packets with L2 tagging.
- Traffic from the phone will sent to the Customer's Network L2 Switch, which in turn will send the traffic to the Customer's router.
- The ethernet camera will typically require a 100 Mb/s connection into the LAN.
- It is recommended that a 1 Gb/s connection be used to connect the phone into the LAN. If a 1 Gb/s connection is not supported, the use of a 100 Mb/s connection may work satisfactorily. However, use of a 100Mb/s connection may cause intermittent packet loss which will degrade the video quality.

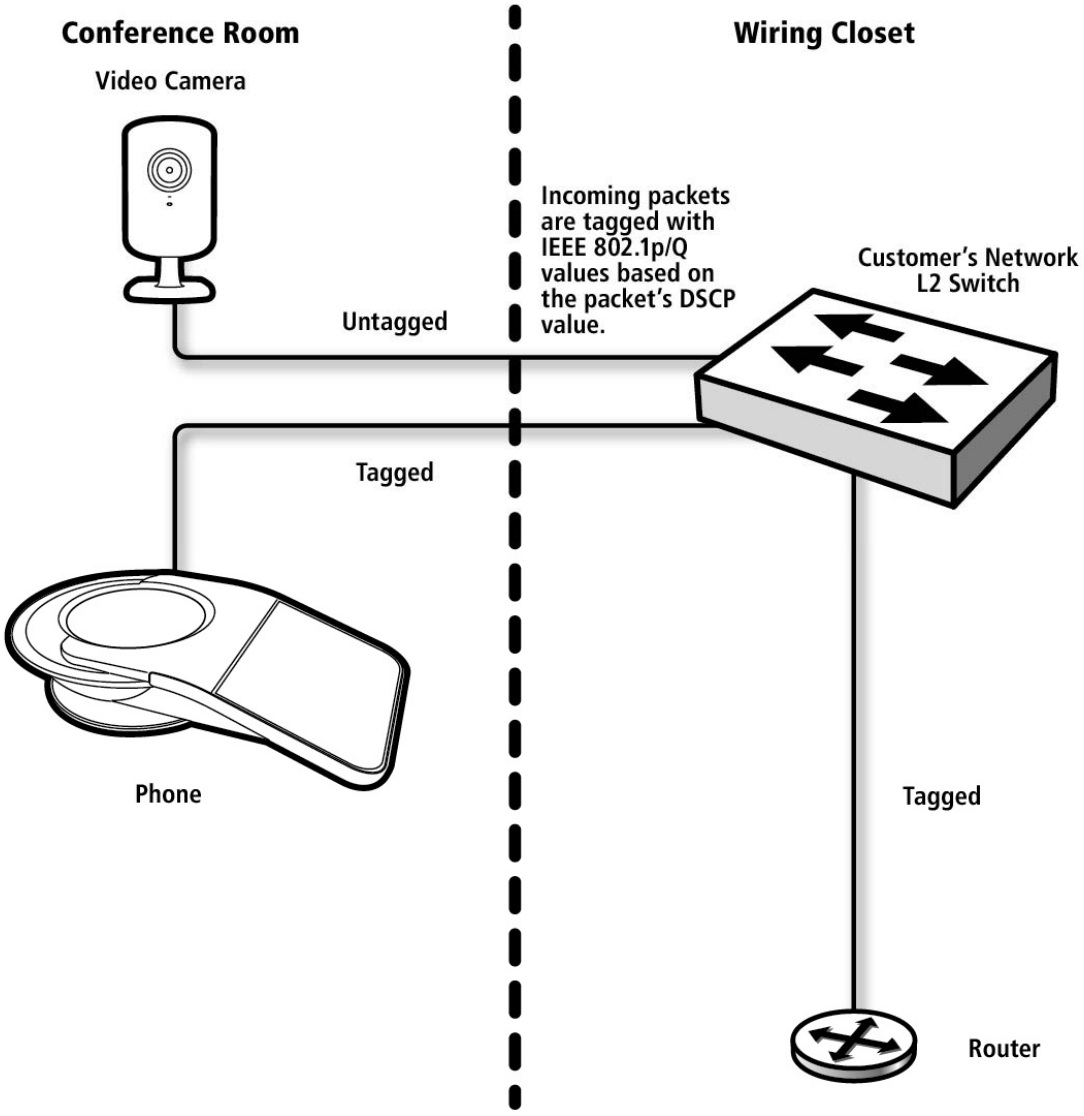

Figure 14. Configuration for Using Customer's L2 Switch, Release 2.0

WAN Guidelines

A WAN link is generally a point-to-point connection between routers and is always a full duplex link. The WAN link is typically used for connecting a remote office to the head office. The link speed for access WAN connections is usually slower than the typical LAN, which means the WAN link presents a potential bandwidth bottle neck.

When a WAN link is shared with other data devices there are other considerations, including the introduction of waiting delay. The end device sees this as jitter, resulting in potential packet loss, and the user experiences degraded voice and video quality.

The queuing techniques and the weightings given to the DSCP values become important considerations. For instance, the use of Expedited Queuing will give better advantage to voice traffic.

WAN QoS and SLA's

The best Quality of Service is obtained when the customer has control of the external WAN connections. This can be achieved by using dedicated leased lines between sites, or by ensuring a guaranteed service-level agreement (SLA) from the external network provider (ISP).

When specifying an SLA it is important that the guaranteed committed information rate (CIR) is specified and includes a guard band. Data sent in excess of the CIR is likely to be discarded during congestion periods in order to maintain guarantees on the SLA.

Also, consider that if the CIR (Committed Information Rate) is based exclusively on the voice and video requirements, additional data above this limit will be marked for "Eligible Discard." This applies to all packets, including voice and video traffic.

Ideally, the SLA should specify a CIR for voice traffic, video traffic and standard traffic.

Some carriers may also offer an SLA that honors and provides queuing for incoming (download to the customer) data as well. There may be an additional charge, but this will provide the added queuing on the far end of the often bandwidth limited connection between the customer and the carrier. With the customer providing priority queuing on the outgoing (uplink from the customer), this link will then have priority queuing at both ends of the connection, to ensure priority for voice and video traffic.

If a WAN connection provides data, voice and video traffic on a common path, then priority schemes need to be employed. The phone uses the appropriate DiffServ field settings. Priority queuing should be enabled on the end routers, even if priority is not used within a separate voice and video network.

Appropriate router MTU settings may be used to reduce WAN serialization delay for connections that carry voice. However, applying an MTU setting for video is not recommended. Video data also requires additional bandwidth and is therefore less likely to be subject to serialization delay and the requirement to adjust the MTU value.

Multiple Internet Service Providers

In many situations there might be more than one ISP involved in establishing a WAN connection between two particular locations.

Internet Service Providers use the Border Gateway Protocol (BGP) to establish routing of traffic between each other's networks. BPG runs on the ISP's router that is used as a gateway to connect to a different ISP's network.

To ensure that QoS markings are honoured end-to end across a WAN connection, it is imperative that the SLAs from all the ISPs involved be correctly defined and use the same definitions, and that all BGP routers be configured according to the SLAs.

Maintaining Availability

This section provides the Administrator with guidelines on maintaining phone availability. For information related to maintaining availability of SIP servers, consult the SIP Server documentation.

SIP Resiliency

To provide increased availability, the phone is able to register with two different SIP Servers. This means that in the event that the primary SIP Server fails, the secondary SIP Server will take over and process calls for the phone.

The phone is also able to address up to two DNS Servers.

To set up the phone for SIP resiliency, the Administrator needs to first do one of the following:

- The Administrator needs to program the DHCP server using DHCP Option 6. DHCP option 6 allows a list of two DNS Server IPv4 addresses to be made available to the phone.

  Or

- The Administrator needs to enter the IPv4 addresses of both DNS servers in the fields provided under the phone Network Settings menu.

Next, the Administrator needs to program the DHCP server using DHCP option 120. DHCP option 120 allows the Administrator to specify the Fully Qualified Domain Name (FQDN) of the SIP server.

When the phone queries the DNS server, the DNS server will return two IP addresses, one address is for the primary SIP server and the other address is for the secondary SIP server.

The phone will then attempt to register with the primary SIP server; if unsuccessful, it will then attempt to register with the secondary SIP server.

The following figure depicts the phone registration sequence using a DNS lookup.

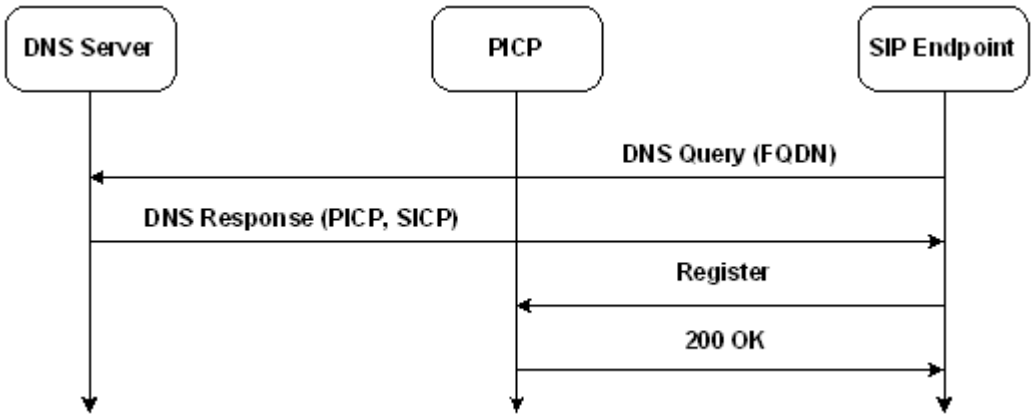

Figure 15. Conference/Video Phone Registration with DNS Lookup

Failover Behavior

Once the phone has successfully registered with a SIP server, it will attempt to re-register with this SIP server on an ongoing basis. The registration time-out period is programmable on the phone, but it is recommended to leave this at the default value of 300 seconds. If the phone fails to re-register with this current SIP server, it will then attempt to register (failover) with the alternate SIP server.

However, even though it is recommended to leave the registration timer at 300 seconds (5 minutes), it does not mean that the phone user will need to wait 5 minutes to learn of a SIP server failure.

In the event that the primary SIP server is unreachable, the phone will failover to the secondary SIP server as soon as the user tries to place a call the phone.

Also, when the primary SIP server is not functioning, an incoming call will be delivered from the secondary SIP server to the phone.

Failback Behavior

If the phone is registered with the secondary SIP server, and health checks between the secondary and primary SIP servers indicate that the primary SIP server has now recovered, then the next time the phone registers with the secondary SIP server it will be instructed by the secondary SIP server to failback (return) to the primary SIP server and register with the primary SIP server.

Network Availability

There are a number of things that can be done to improve network availability and these are typically discussed in depth in networking equipment documentation for L2 switches, routers and SIP servers. In general if increased network availability is required the Administrator should consider the following:

- The use of primary and secondary L2 switches and routers
- Resilient connections between devices in the access network
- Resilient connections between devices in the distribution network
- The use of Spanning Tree Protocols at L2 of the network
- The use of the Virtual Router Redundancy Protocol at L3 of the network
- The use of a back up DHCP server
- If DHCP server are in different subnets than the phone, then ensure that routers are configured to support DHCP forwarding

Power Considerations

If a resilient network has a single power source (not recommended), and if that source fails, all devices stop working. Ideally, the critical elements of the network should retain power in the event of failure of main power feed. This can be through an alternative power source such as a secondary main supply, local UPS or local generator.

Primary network devices (SIP servers, L2 switches, DNS servers and DHCP servers) should be powered from a different branch circuit than the branch circuit that is used for powering the secondary network devices. This will require special attention if the primary and secondary network devices are co-located in the same wiring closet.

Deployment with MiVoice Business

In the past, the MiVoice Business (formerly MCD) used a device registration model where each phone or end point was associated with a unique Device Type identifier that was used during product configuration to control product behavior and define licensing limitations. The phone employs a new device registration model where a single device type is used to support a number of different devices that have similar characteristics.

The phone uses a device type called UC Endpoint. This can be selected from the drop down list of supported devices on the MiVoice Business.

For detailed information, refer to the *Guide* and the MiVoice Business System Administrator's On-Line Help files, specifically the section called Deployment with SIP Servers and End Points.

Additionally, the administrator should consult the MiVoice Business documentation for specific information on the MiVoice Business operation with the phone and for network engineering guidelines.

Teleworker and MiVoice Border Gateway Deployments

MBG (MiVoice Border Gateway) is a Session Border Controller. The MBG is usually installed at the demarcation point between the customer's LAN and the Service Provider's Network, or the demarcation point between the Customer's LAN and a residential/Teleworker user. The MBG is a SIP aware firewall and provides security for the Customer's LAN.

The MBG also provides the following functionality:

- NAT Traversal
- Quality of Service
- Bandwidth Management
- Call Admission Control

In cases where the phone is connecting to the MiVoice Business or a SIP server via an internet DSL or DOCSIS connection, for security and NAT traversal reasons it is recommended that the phone be connected first to a MBG and the MBG in turn be connected to the MiVoice Business or SIP server.

From the MBG's perspective, the phone appears as an end point for both voice and video. The Administrator should register the phone with the MBG as a Mitel-UC-Endpoint.

The phone connects to the MBG on TCP port number 35010 to securely access an Active Directory server on the Customer's LAN.

Minimum MBG Software Requirement

For correct operation with the phone, the MBG must be running a minimum of MBG 7.1 SP1 software.

Teleworker Physical Connectivity and Power

Depending on the installation environment, there are a number of different options available for physically connecting and powering the phone and the IP camera, for details refer to the section called Power.

Teleworker IP Connectivity

It is recommended that a phone and its associated IP Camera be on the same subnet.

This allows for traffic between the IP camera and the phone to be locally switched rather than having to be routed from one subnet to another. Installing the IP camera and the phone on the same subnet also allows the phone to auto-discover the IP Camera using the ONVIF broadcast protocol.

For additional details refer to the section called LAN Connection Guidelines.

Conference/Video Phone Settings

SIP Settings

The SIP Settings menu, found under the System Settings menu, requires a few SIP settings to so the phone can operate with the MBG.

For details, refer to the *MiVoice Conference/Video Phone Administration Guide*.

- The MBG IP Address must be entered into the SIP Server Address field.
- The SIP Keep Alive Interval should be set to 10 seconds to keep the MBG's NAT mapping refreshed.
- The H.264 Baseline Profile CODEC is the preferred CODEC for use with Teleworker applications. It is recommended that the Administrator access the Video CODEC List and place the H.264 Baseline Profile CODEC at the top of the Video CODEC List.

> **Note:** When using URI dialing, only the H.264 Base Line CODEC is supported

H.264 High Profile CODEC Considerations

The High Profile H.264 CODEC may be less tolerant of network packet loss and network delays compared to the Baseline Profile H.264 CODEC, and Teleworker connections might incur higher packet loss than corporate LANs.

Packet loss may degrade a video image using a High Profile CODEC more than a video image using a Baseline Profile CODEC.

Due to the large variations in network quality in different locations and regions, the system Administrator and the Teleworker end user will need to determine which video CODEC setting is appropriate for their particular installation.

It is recommended to disable the H.264 High Profile CODEC when operating in Teleworker mode over an unmanaged network (internet).

Dynamic Bandwidth Allocation

When the phone is connected to an MBG, the Administrator should disable the Dynamic Bandwidth Allocation option on the phone. For further information see the section called Dynamic Bandwidth Allocation and the *MiVoice Conference/Video Phone Administration Guide*.

Bandwidth Settings

In some regions Teleworkers may have limited bandwidth to and from their ISP. While this bandwidth limitation may not present an issue when transferring data files or supporting a single VoIP call, it could potentially be an issue when supporting a video call due to the high bandwidth required for video transport.

To ensure good video quality on bandwidth, constrained links such as a Teleworker link, it will be necessary to configure the phone so that bandwidth consumption will be limited to prevent link from being overutilized.

The Administrator can choose to limit the phone bandwidth usage based on a detailed analysis of the ISP link or the Administrator can simply limit the phone bandwidth consumption to the absolute minimum amount. These two methods are described in the following sections.

Minimum Bandwidth Settings

In cases where the Administrator does not know what the bandwidth capabilities of the ISP link are, or the Administrator does not want to perform a detailed analysis of the communication link, then the phone should be configured to use the minimum bandwidth setting.

This is accomplished by using the video bandwidth limiting option to limit the phone bandwidth to the minimum settings of 512 kb/s in the uplink direction and 512 kb/s in the downlink direction. This will ensure that the Teleworker ISP connection's bandwidth capabilities will not be exceeded.

It should be noted that optimal video quality may not be achieved when bandwidth is limited to 512 kb/s in the uplink direction and 512 kb/s in the downlink direction. to obtain optimum video quality the Administrator may want to consider configuring the bandwidth settings based on an analysis of the communication link.

Bandwidth Settings Based on Analysis

In cases where the Administrator would like to find the bandwidth limit setting that provides optimal video quality without oversubscribing the communication link, the following procedure should be used

The best way to determine the amount of available bandwidth is to use a speed test tool, preferably one provided by a third party rather than the ISP themselves – buyer beware.

Once the bandwidth capabilities have been determined the Administrator must take into consideration the bandwidth requirements of the.

The Administrator should be aware that

- When a phone initiates a video conference it will also serve as the video bridge for the conference.
- A phone that is acting as a video bridge for a 3 party conference will require twice the video bandwidth and twice the audio bandwidth required by a phone that is only a participant in the conference.
- A phone that is acting as a video bridge for a 4 party conference will require three times the video bandwidth and three times the audio bandwidth required by a phone that is only a participant in the conference.
- Release 1.0 requires 2.1 Mb/s of video bandwidth in each direction to be a participant (not an initiator) in a video call.
- Release 2.0 has some new settings that can be used to reduce the video bandwidth requirements for a phone that is a participant or an initiator in a video conference. For details see the section called Bandwidth Limiting or the System Administrators Guide.

With the new video bandwidth limiting capabilities introduced in Release 2.0, the phone can now be configured to operate on bandwidth limited connections such as a Teleworker might encounter.

The new video bandwidth limiting options in Release 2.0 allow the Administrator to limit the video bandwidth requirements to:

- 1.5 Mb/s in the uplink direction
- 1.5 Mb/s in the downlink direction
- 1 Mb/s in the uplink direction
- 1 Mb/s in the downlink direction
- 512 kb/s in the uplink direction
- 512 kb/s in the downlink direction

Worked Example

For example, the Administrator has determined via actual measurements that a Teleworker to ISP connection supports a download bandwidth of 25 Mb/s and an upload bandwidth of 3 Mb/s.

The Teleworker location phone is running Release 2.0 software which allows for video bandwidth limiting.

The audio portion of the conference will be using G.711 CODECs and a 20 ms packet rate; this requires 100 kb/s of bandwidth in each direction for a single call. For details, see Voice Bandwidth Requirements.

Downlink Analysis

If the Teleworker phone were to initiate a 4 party video conference with the video bandwidth limit set to 1.5 Mb/s, then the required downlink bandwidth would be:

- Video Bandwidth = 3 x 1.5 Mb/s = 4.5 Mb/s
- Audio Bandwidth = 3 x 100 kb/s = 300 kb/s
- Total Bandwidth = 4.8 Mb/s

Since the total downlink bandwidth requirement is 4.8 Mb/s there will be no bandwidth restriction issues on a 25 Mb/s connection.

Uplink Analysis

If the Teleworker phone were to initiate a 4 party video conference with the video bandwidth limit set to 1.5 Mb/s it is obvious that the required video bandwidth (3 x 1.5 Mb/s = 4.5 Mb/s) will exceed the capabilities of a 3 Mb/s connection. As a result the Administrator will need to select an appropriate bandwidth limit for the uplink connection.

If the Administrator sets the video bandwidth limit for the upload direction to 512 kb/s, the required upload bandwidth would be:

- Video Bandwidth = 3 x 512 kb/s = 1.536 Mb/s
- Audio Bandwidth = 3 x 100 kb/s = 300 kb/s
- Total Bandwidth = 1.836 Mb/s

Since the total uplink bandwidth requirement is 1.836 Mb/s there will be no bandwidth restriction issues on a 3 Mb/s connection.

Notes

- These calculations do not take into account any other data transactions, such as web browsing or file transfers that might be taking place on this connection.
- As a rule of thumb the bandwidth utilization of a given connection should not exceed 70% of the available bandwidth.

Network Settings

The phone's Network parameters may be programmed manually or acquired automatically via DHCP. Teleworker users will generally need to manually supplement the parameters given by their DHCP server such as the MBG (SIP Server) IP address and the DNS IP address, for details refer to the section called IP Network Configuration for the phone

MBG Settings

The Administrator should configure the MBG for media pass through. If the software version of MBG deployed does not support media pass through mode, then the Administrator should configure the MBG so that media packets are assigned a DSCP value of 34 (AF41).

For details on how to configure the MBG, refer to the MBG On line Help files.

> **Note:** The current MBG software cannot differentiate between voice and video packets; it recognizes both packet types as 'media' packets. Assigning the normally recommended voice DSCP value to video packets could cause voice quality issues on the Customer's LAN and it could also violate Service Level Agreements in place with the ISP and incur unexpected costs, a DSCP value of 34 (AF41) is recommended.

MBG Transcoding Support

At this time the MBG does not provide transcoding support for SIP devices, including the phone.

However, the MBG does support pass-through mode for G.711, G.729a, and G.722.1 CODECs. That is, if one of these CODEC types is enabled on both endpoints and both of the endpoints want to use the same CODEC, then no transcoding is required and the call will be supported via the MBG pass-through mode.

Note that the MBG does not support either transcoding or pass-through mode for the G.722 CODEC.

Software Loads for Remote Phones

For most phones, the MBG packages and provides phone software loads; however, in the case of the phone this is not done.

If a remotely located phone requires a firmware update, the Administrator can either use an SD card at the remote site to upgrade the phone or use Secure Copy (SCP) to copy the firmware to the following directory on the MBG server for the phone to access.

/home/e-smith/files/ibays/Primary/html directory

For details on phone firmware upgrades, refer to the *MiVoice Conference/Video Phone Administration Guide*.

Deployment with SIP Servers and End Points

The Conference/Video Phone supports the SIP protocol. As a result, it is capable of operating with a number of third-party SIP Servers and SIP end points such as SIP phones, Audio Conference Units and Video Conference Units.

Mitel maintains a SIP Centre of Excellence (SIP CoE); the CoE performs interoperability testing between third-party devices and Mitel SIP devices. The CoE generates documents that cover the results of the interoperability tests and how the devices should be configured for successful interoperation.

For the complete list of devices that phone can interoperate with, please refer to the Knowledge Base article called Mitel Technical Reference Guide: Mitel Compatibility and Third-Party Certification Reference Guide for Mitel Products, 08-5159-00014.

This Reference Guide can be found on Mitel On-Line under **Support -> Technical Support -> SIP Centre of Excellence**.

A number of Knowledge Base articles exist that are referred to as *SIP Configuration Guides*. These guides provide configuration recommendations for the phone, SIP servers and SIP end points

The Mitel Technical Reference Guide lists the available SIP Configuration Guides and where to find them.

The *SIP Configuration Guides* provide the Administrator with the following type of information:

- Configuration recommendations for the phone and the MiVoice Business.
- Configuration recommendations for the phone and third-party SIP Servers and SIP end points.
- A list of potential interoperability and/or feature limitations.

SIP URI Dialing

Release 2.0 SP1 introduces a new feature called SIP URI Dialing.

A SIP URI (Uniform Resource Identifier) is an addressing mechanism that is used to place a phone call to a SIP-based service; this could be another SIP end point or a SIP conferencing service.

The SIP URI is essentially a user's or service's SIP phone number. The SIP URI looks similar to an email address and uses the following format:

SIP URI = sip:x@y:Port

Where x=Username and y=host (domain or IP): port

Example: John.Smith@Mitel.Com:5060

For more information on using SIP URI's for placing phone calls, see the *MiVoice Conference/Video Phone User Guide*.

Installation Guidelines

If SIP URI dialing is used, the Administrator needs to configure the phone and the network to allow for this capability.

Typically, the phone will be installed behind a corporate firewall. If the phone is behind a firewall, the phone cannot determine a public IP address to use for SIP signaling purposes. As a result, the Administrator must ensure that there is a mechanism in place that allows for firewall traversal.

The phone uses IP port 5060 (by default) for SIP URI signaling purpose. The URI itself provides a field for the IP port number, and if this field is populated, this port number will be used.

The Administrator should be aware that at Release 2.0 SP1, the phone does not support encryption for either signaling or for media.

The phone supports two deployment scenarios: deployment within the corporate network (on premise) and deployment in a SOHO (Teleworker) environment.

The two different methods of supporting firewall traversal are

- SIP outbound Proxy/SBC (Session Border Controller) – used for phone corporate or enterprise deployments
- SIP ALG (Application layer Gateway) – used for phone SOHO or Teleworker deployments.

The following sections describe these two different deployment scenarios and the two different firewall traversal methods in detail.

SIP Outbound Proxy/SBC Corporate and Enterprise Deployments

Enterprise class firewalls/routers are available that provide support for SIP URI dialing requests in the form of a SIP Outbound Proxy with SBC functionality. One company that offers such firewall solutions is Ingate Systems AB.

When the phone is deployed in an environment with a firewall that provides SIP URI dialing support, then all SIP requests from the phone will be routed via the proxy.

The phone must have the Proxy Server Address for Dial URI configured under **Advanced -> System Settings -> SIP Settings**. This is the internal IP address of the gateway or Outbound SIP Proxy server in the form FQDN | IP [:port]. (For additional details, refer to the *MiVoice Conference/Video Administration Guide*.)

With this configuration, non-SIP URI calls are handled by the MiVoice Business as they normally are, and media for local calls will stream directly between the devices on the LAN.

Calls using URI Dialing to an external conferencing service will be handled by proxy by the firewall, and media will be streamed through the proxy (firewall).

At the time of writing the following conferencing services are supported:

- Bluejeans
- Vidtel

For information on interoperation with additional conferencing services, see the Mitel SIP Centre of Excellence.

External Call Using SIP Outbound Proxy

The next diagram shows a call scenario where Phone (A) makes a call to an internet-based service that is off premise.

In this scenario, the signaling originating from Phone (A) is still proxied by the SBC, but the SBC modifies the signaling so that the media from Phone (A) is streamed to the internet-based service using public IP addresses.

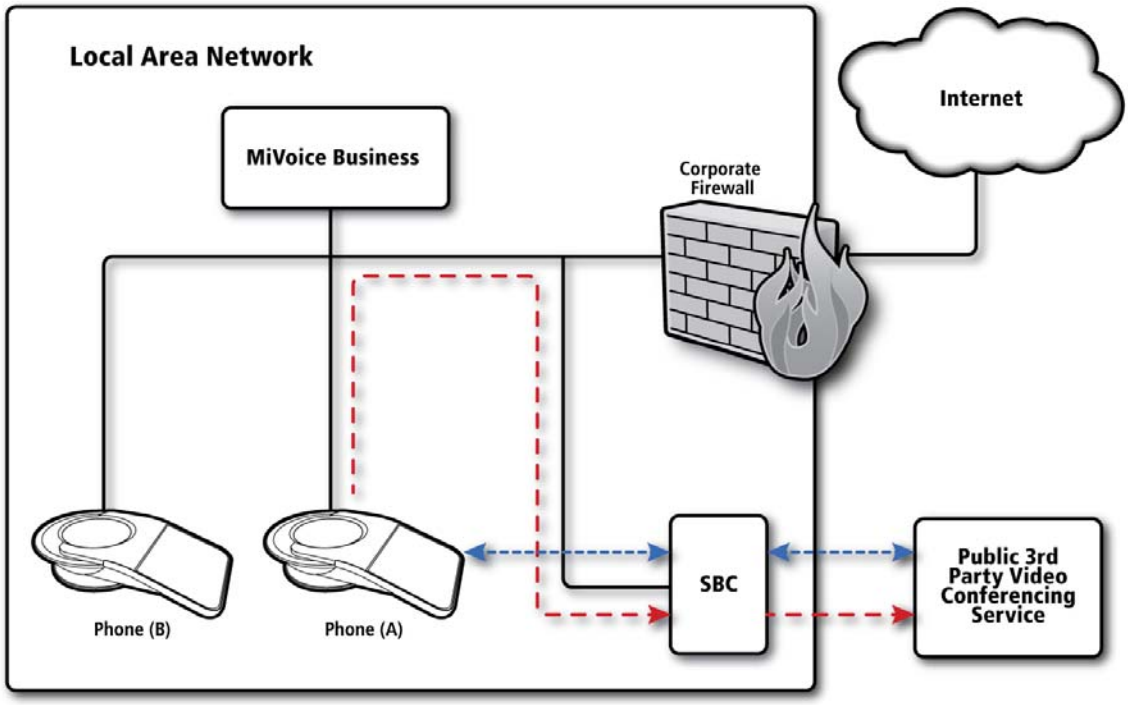

Figure 16. External SIP URI Call

SOHO Deployments

It is unlikely that a SOHO (residential) router will support SBC functionality. Many do, however, support SIP ALG (Application Layer Gateway).

If the router supports ALG, then the Administrator must first ensure that ALG is enabled on the router.

Once ALG is enabled, there is typically no further configuration required on the phone. ALGs usually require no special endpoint configuration.

When SIP ALG is enabled, the router will modify the outgoing SIP packets as required to allow for NAT traversal.

SIP ALG capabilities likely vary in effectiveness between different brands and models of routers. If you have additional questions about a router's capabilities, contact Mitel Professional Services

Voice Quality, Video Quality and Quality of Experience

When running IP traffic over the public internet, voice and video quality cannot be guaranteed. Unlike private WAN connections, the public internet does not support any form of quality of service (QoS) for different traffic classes. Additionally, it is not possible to put a Service Level Agreement in place when using public transmission facilities such as the internet.

Users may find some voice and/or video quality issues when operating over the internet due to unpredictable network latencies and potential packet loss due to network congestion.

Third-Party Video Conferencing Services

A number of third parties offer video conferencing services that are housed in the so called 'Cloud'. The phone user can access these services with SIP URI dialing.

Mitel maintains a SIP Centre of Excellence (SIP CoE); the CoE performs interoperability testing between third-party devices and services and Mitel SIP devices. The CoE generates documents that cover the results of the interoperability tests and how the phone and Cloud services should be configured for successful interoperation.

For the complete list of devices that phone can interoperate with, please refer to the Knowledge Base article called Mitel Technical Reference Guide: Mitel Compatibility and Third-Party Certification Reference Guide for Mitel Products, 08-5159-00014.

This Reference Guide can be found on Mitel On-Line under Support -> Technical Support -> SIP Centre of Excellence.

Conference/Video Phone Licensing

When installing the phone with a MiVoice Business, a license will be required. Phone licensing is the same as a regular IP phone. Depending on the particular configuration, the Administrator will need to obtain a MiVoice Business Standard License, a MiVoice Business Enterprise License or a Multi-Device License for each phone. Licenses may be obtained from the AMC server. No other licenses are required.

- A Standard License is required in a non-clustered environment.
- An Enterprise License is required in a clustered environment.
- For resilient operation, an Enterprise License is required on only one MiVoice Business (Primary MiVoice Business). The software indicates to the other MiVoice Business (Secondary MiVoice Business) that this device is licensed with an Enterprise class license.
- With a Multi-Device License, the users receives licenses for 8 devices, but only pays for 1, that is, the license is used by one user for multiple devices, desk phone, mobile phone, and so forth.

As described under the section called Product Variants, there are two variants of the phone, and each has its own customer orderable part number.

When installing the phone with a third party SIP Server, the Administrator will need to meet the licensing requirements for the third party equipment.

Conference/Video Phone Firmware Upgrades

The phone has a connector that accepts a Micro SDHC (Secure Digital High Capacity) memory card. The SDHC memory card format supports capacities of up to 32 Gigabytes. The SDHC connector is used to perform firmware upgrades on the phone. Firmware upgrades can also be performed from an HTTP(S) server. For details pertaining to firmware upgrades, refer to the *MiVoice Conference/Video Phone Administration Guide*.

Android O/S upgrades will occur when new versions of the phone software are delivered.

Emergency Services

The phone can be used to place an emergency call, however in the event of an emergency, placing an emergency call is likely going to be too time consuming and require too much thought from a caller who may not be thinking clearly.

For the above reasons, it is recommended that a conventional POTS phone or an IP phone that has been properly provisioned for emergency services be deployed in reasonably close proximity to the conference room.

The Administrator may want to post a sign in the conference room stating where the closest emergency response phone is located. The Administrator may also want to consider creating an Emergency Services Profile in the Active Directory for users that may need to place an emergency phone call from the phone.

Security and Authentication

The phone supports the IEEE 802.1x authentication protocol. Users are authenticated through the phone user interface by entering a username and password.

Authentication Protocol Support

Devices that authenticate through the IEEE 802.1x authentication protocol require an identification name and password before being allowed access to the network. The phone supports the EAP-MD5 protocol.

If the Administrator configures the network access L2 Switch for port access control, when the phone is connected to this port, it will prompt the user for an account name and password if one has not already been entered or if the information saved in the phone is invalid. Based on the response:

- The LAN port may be opened for access
- The VLAN settings may change
- The LAN port could be opened to a guest VLAN
- The port could be shut down

An 802.1x port may be configured to request authentication only at startup of the network port and this may include regular authentication retries.

Typically, 802.1x will only allow a single device to be authenticated and connected to a single LAN port. This restricts how devices can be connected into the network infrastructure.

- Where network ports only support a single connected device, for full authentication, the phone and the ethernet camera should be connected to separate LAN ports and the Mitel Multi-Port Gigabit switch should not be used.
- If it is a requirement that both the phone and the ethernet camera be connected to the same LAN switch port, then the phone and the ethernet camera should be connected to the Mitel Multi-Port Gigabit switch, which in turn allows for a single connection to be made to the LAN switch port.

> **Note:** Under these circumstances, if the LAN switch does not allow for multiple devices to be connected and authenticated on the same port, then the Administrator must ensure that 802.1x authentication is disabled on the LAN switch port.

Not all network LAN ports place single device restrictions on connected devices.

- HP switches allow multiple devices to be connected and authenticated on a single port and they also provide per device filtering. As an example, per device filtering would allow two devices to be connected and authenticated on a single LAN switch port. If a third device was connected and it failed to successfully authenticate, the third device would be denied access while the first two devices would remain connected.
- With Cisco switches, where the phone uses the Auxiliary VLAN setting, both the phone and the ethernet camera can operate on the same LAN port.

It is recommended that the Administrator enable the re-authentication response to regularly check access to the LAN switch port. The default time is often in the order of 3600 seconds.

The Network Settings Menu allows 802.1x to be enabled or disabled and a username and password to be assigned. For details, refer to the section on Network Configuration Menus.

Ethernet Camera

Most ethernet cameras support the IEEE 802.1x authentication protocol, access control lists and may offer the ability to disable firewall traversal capabilities. For details, refer to the Section on Ethernet Connected Cameras and the camera vendor's documentation.

SIP Security

SIP (Session Initiation Protocol) is an open standard signaling protocol used for establishing and terminating IP phone calls.

The phone uses SIP to communicate with the PBX and other IP end points. The phone is required to successfully go through an authentication process with the SIP server before access to system features is granted.

Troubleshooting

Troubleshooting Audio Quality Problems

Voice quality issues that users may experience can be varied. For example, users may complain of echo, buzzing, ticking, distortion, choppy audio, loudness issues, or delayed speech. The cause of voice quality problems can be associated with the TDM network, the analog network, the PSTN, the IP network, the user's environment, or due to equipment configuration errors. The following are areas where voice quality issues could originate:

- The Analog, TDM, or PSTN Networks
- Electrical Echo
- Positive Feedback
- The IP Network
- Delay
- Jitter
- Speech Compression
- Packet Loss
- Lack of WAN Bandwidth
- Lack of LAN Bandwidth
- Excessive number of transcoding hops
- The Environment
- Acoustic Echo
- Crosstalk
- Background Noise
- Side Tone (loud, quiet, or missing)
- Voltage Interference
- Improper Grounding
- Improper Use of Handset (breathing into microphone)
- Equipment Configuration Errors
- MiVoice Business Platforms, SIP Servers or PSTN Gateways
- IP phones and conference units
- Layer 2 Ethernet Switches and Routers
- Analog trunk and extension impedance and level settings
- Country settings

If the following questions can be answered, it will be easier to diagnose and correct the problem:

- What is the issue or complaint?
- What does it sound like? Do all parties on the call have the same complaint? If not, which call party (called, calling, Mitel user or external) is experiencing the voice quality issue?
- When does it occur?
- What is the call situation? For example, does it occur only on Loop Start to IP conference calls? Does it always occur at a certain time of day or at a specific phone?
- When did it start happening? For example, after a software upgrade, after new LAN equipment was installed, after there were changes in the IP network or after a new carrier was contracted?
- Where does the problem originate? For example, does it originate in Mitel equipment or in another vendor's customer premise equipment?
- Where is the problem occurring? For example, does it occur at a single IP phone, at multiple IP phones on the same Layer 2 switch, on analog phones connected to an Analog Service Unit, on a specific trunk, or on all trunks of a specific type?

Analog, TDM, or PSTN Network Issues

Echo

When echo is present on a call, users hear what they said tens or hundreds of milliseconds later. Users find echo annoying, particularly if it is loud or if the echo delay is long.

Echo occurs on a call when a portion of a signal is sent back towards the signal's source and there is significant delay in the call path. If the round-trip delay in the reflections is greater than 50 ms these reflections are perceived by users as echo. Reflection can be caused by line hybrids or by acoustic or mechanical audio coupling at the phone.

When reflection is occurring and the round trip delay is very short (less than 50 ms), the user of a handset will perceive the reflection as handset sidetone. Sidetone is reflection that has a very short delay. Sidetone is not a voice quality issue and is in fact beneficial because it has the effect of reassuring the user that the phone is not dead.

There are two types of echo, electrical echo and acoustic echo, and there are also cases of perceived echo.

Electrical Echo

In the case of electrical echo, the reflection is caused by impedance mismatches on the transmission line. The impedance mismatch causes energy from the signal to be reflected back to the source.

Electrical reflection usually occurs on analog trunks at hybrids where a 2-wire analog circuit is converted to a 4-wire analog circuit. Hybrids are not applicable to T1, PRI, or SIP trunks.

For more detailed trouble shooting information related to electrical echo, the Administrator should consult the vendor's documentation that is specific to the suspect analog gateway or PSTN gateway.

Acoustic Echo

In the case of acoustic echo, the signal reflection is the result of the sound from the telephone's ear piece or a speaker phone's speaker being picked up by the phone's microphone. The party on the far end hears both the caller's voice and, a few tens to hundreds of milliseconds later, the reflected version of his or her own voice. Acoustic echo is more likely to occur with:

- Hands free car phone systems
- Speakerphones or phones in hands free mode
- Standalone Conference Bridges
- Improperly designed phones where vibrations from the loudspeaker transfer to the microphone via the handset casing.

Perceived Echo

There are several conditions that can cause users to believe that they are hearing echo on a call.

Double Talk

Double talk occurs when both parties in a conversion talk at the same time. During double talk on a connection that uses an echo canceller, the echo canceller will be disabled during the period of time when double talk is occurring. This is necessary to allow the other speaker to be heard.

However, this also means that residual echo is not blocked. If the echo canceller filters are properly adapted, problems will not occur. However, double talk makes it difficult for the filters to maintain proper adaptation and sometimes it can cause the echo canceller to lose adaptation. In this case, the echo canceller quickly re-adapts when double talk is removed.

The type of double talk that occurs during a normal conversation should not degrade voice quality. However, it is possible to create echo, clipping, or a combination of the two, if users continuously talk over each other in an effort to stress the echo canceller. Echo that is artificially generated in this fashion should not be considered a voice quality issue.

Background Noise

In situations where there is significant background noise it may cause people to believe that they are experiencing echo. Essentially, this is another instance of double talk. Background noise can appear to the echo canceller as if someone were talking, thus causing the double-talk effect.

Cell Phones

It is possible for the user to hear when talking to a cell phone user; this usually occurs during double talk situations. This echo is due to a failure of the cell phone's acoustic echo canceller to cancel the echo. Because of the long delays and non-linear coding in the cellular network, only the echo canceller in the cell phone can cancel this echo. Cell phone calls can also exhibit symptoms similar to echo when a change in cell phone towers occurs. A change in cell phone towers can cause a brief disturbance in the signal that sounds like echo which stops after a few seconds or less.

Local Feedback

If the caller is talking to someone on a nearby phone that is using hands free mode, the caller may hear their own voice be transmitted through the air from the hands free phone's loud speaker. This sound is picked up by the caller's handset and the caller hears this through local side tone, but also in the ear without the handset.

Solving Echo Problems

Before you attempt to troubleshoot echo, you must understand the following points:

- The primary cause of echo is a combination of a significant delay plus a reflection. In order for echo to be heard by users, an echo canceller must fail to cancel or suppress the echo.
- Reflection causes echo if the round trip delay is long (greater that 50 ms round trip delay) and the reflections are not cancelled or suppressed. You must be able to identify the significant delays that are manifesting the reflections as echo. VoIP is a primary source of significant delay (amounting to several hundred milliseconds).
- Reflection sounds like handset sidetone when the round trip delay is short (for example, less than 50 ms).
- The two main causes of reflection are: 2-wire/4-wire interfaces, which are called hybrids, and acoustic feedback from phones
- You should be able to identify the types of echo:
- Electrical (line) echo originates at hybrids which are always located at both ends of any 2-wire segment
- Acoustic echo is caused by the failure of the echo canceller in the handset to suppress or cancel echo. It is more likely to occur when a phone, cell phone, or conference bridge is operating in hands free mode.
- Conditions such as double talk, background noise, two or more echo cancellers in series, signal level mismatch, and overload distortion that occurs during loud audio can reduce the effectiveness of echo cancellers and can sometimes result in noticeable voice quality issues.
- Customers should be made aware of the following facts:
- Reflections originating at IP phones that can cause echo must be cancelled by echo cancellers in the IP phone to prevent it from entering the long delay path of the IP network
- Reflections that originate in the short delay audio path of the PSTN must be prevented from entering the IP network by the echo cancellers in the PSTN gateway.

IP Network Issues

Conditions that can result in voice quality issues on IP Networks include:

- Latency (Delay)
- Packet Loss
- Excessive Speech Transcoding
- Jitter
- Lack of Bandwidth

Refer to the section called Network Measurement Criteria for recommendations on the acceptable amount of packet loss, jitter and latency.

Latency (Delay)

Latency in a call is the amount of time it takes for the caller's voice to reach the other end of the connection. As latency increases in a conversation, it becomes increasingly difficult for users to sustain a normal two-way conversation. The conversation rapidly deteriorates from an interactive exchange to an "over-to-you" radio-style form of communication. Severe latency in the network can result in dropped calls.

Latency becomes noticeable in a call at a 80 ms to 200 ms delay and is radio-style at 400 ms delay. Assuming that jitter and packet loss are not an issue, end-to-end delay is the most likely cause of voice quality issues on VoIP calls. From International Telecommunication Union -

Telecommunication Standardization Sector (ITU-T) recommendations, and based on practical experience, the one-way end-to-end delay for a voice call should not exceed 80 ms in the network.

Latency in the Data Network

Latency in the data network is a measure of the amount of time it takes for a data packet to travel through the network. Latency in the data network results in latency in calls. It's important to note that latency in the network can change significantly depending on the:

- Condition of the network
- Amount of available bandwidth
- Path that is being used through the network
- Amount of traffic

For example, latency may be high during the afternoon when network usage on the site peaks.

During the period of peak network usage, the IP phone user may experience poor voice quality on calls. Later, when network usage subsides, latency isn't a problem and voice quality on calls is good again. Therefore, you need to measure network latency when the voice quality issue is present to determine if latency is the cause.

You can use a ping test to determine if network latency is causing voice quality issues between two IP phones. The ping delay is the time it takes for a data packet to travel from one IP address across the network to another IP address and back again (round-trip delay). A ping utility allows you to send a data packet from a PC to an IP address on the network. If the packet reaches the IP address it is sent back, and the utility displays the round-trip delay. Typically, the send and receive paths have equal delays.

Jitter

Jitter is a measure of the variation in the packet delay. The major cause of jitter is network congestion. This occurs when the amount of data arriving at a node, including the source, destination, routers, and switches exceeds the capacity of the node to forward the data. In this case, data is stored in a buffer queue until the node is able to forward the data. The time that the data spends in this buffer before being forwarded is the major source of jitter.

While high quality network routers, switches, and Network Interface Cards (NICs) can generally forward packets at the network data rate; many routers, switches, and NICs are limited in the number packets they can forward per second. With short packets, such as VoIP packets, this can result in network congestion at data rates significantly lower than the network bandwidth.

High levels of jitter may result in packet loss and choppy voice quality on VoIP calls. To determine if jitter is the cause of voice quality issues a network analyzer should be employed to measure the network jitter. Network jitter should not exceed 60 ms.

Packet Loss

When packet loss occurs during a VoIP call, tiny fragments of the conversation are lost. Users may experience one or more of the following effects:

- Loss of words in a conversation
- Dropped calls (if packet loss is severe)
- Loss of intelligibility
- Fuzziness
- Choppy audio or clipping
- Common causes of packet loss within the network include:
- Congestion at a connection that results in buffer overflow and data loss.
- Highly variable jitter that causes packets to arrive too late at a gateway or IP phone. The packets arrive too late to be used for voice and are therefore discarded.
- Out-of-sequence packets being discarded on WAN connections.
- Incorrect duplex settings on LAN connections that results in data collisions and packet loss.
- Lack of network bandwidth.
- Network loss or temporary disconnection. This could occur if STP or RSTP network reconfiguration is occurring due to a network failure or change.

Although some packet loss can be handled on an ongoing basis, bursts of packet loss will be noticed by users. A network with 0.1% packet loss over time sounds much different than a network with the same loss but occurring in bursts of three or more packets. Network packet loss should not exceed 2%.

The phone display provides a Network Health icon that indicates when there is Network Congestion causing packet loss. This Icon, when active, is reporting that there is packet loss in the receive stream. In other words, a percentage of packets being transmitted from the far end to this phone are being lost somewhere in the network. For details refer to *the MiVoice Conference/Video Phone Administration Guide*.

Excessive Speech Transcoding

The phone supports a range of voice CODECs; these are described in the section called CODECS and Network Bandwidth Requirements.

A voice signal subjected to excessive compression or too many transcoding hops (for example, from G.711 standard to G.729.a and back to G.711) may sound like the voice is coming through a drain pipe. The Administrator should examine where compression is being used in the network, and try to minimize transcoding hops.

Lack of Network Bandwidth

Poor voice quality can result from a lack of network bandwidth. A lack of bandwidth can result in packet loss, excessive jitter and excessive latency. Ensure that there is sufficient bandwidth on the LAN and on the links to the WAN to support the amount of expected traffic.

Ensure that routers at bandwidth bottlenecks - such as at a WAN connection – have appropriate QoS settings and packet queuing mechanisms. Voice and video should have higher priority access to available bandwidth than regular or standard data traffic.

Background Noise

Background noise in a caller’s environment can cause the party at the other end to assume that they are hearing echo. Loud machinery, noisy crowds, a vibrating fan, or wind noise are all examples of background noise that can sound like echo to the caller on the other end.

Background noise on a call normally varies in strength as the noise level of the source fluctuates.

Background noise can also cause difficulties with conference phone performance if the conference phone mistakes background noise for an individual talking.

> **Note:** Wideband CODEC calls are more likely to pick up background noise than standard calls.

Configuration Errors on the Layer 2/3 Switches and Routers

The phone, the SIP Server, Layer 2 switches and network routers must be configured correctly to avoid voice quality issues. Consider the following recommendations:

- The LAN should be fully switched.
- Ensure that the phone and SIP end points are connected to the IP network only through layer 2 switches, not ethernet hubs.
- Ensure that the Network Layer 2 switch ports are also configured to auto-negotiate.
- Use full-duplex connections.
- Use VLANs to segregate voice and video packets from data traffic.
- Make proper use of Layer 2 and Layer 3 QoS mechanisms for wired LANs; make proper use of WMM QoS mechanisms for WiFi LANs.
- Provision extra bandwidth whenever possible, especially in the core of the backbone network.
- Provide appropriate bandwidth management, QoS settings and queuing for routers that connect over bandwidth restricted WAN links.

VLANs

- Configure L2 Switch ports to provide VLAN tagging to incoming untagged information and remove this tagging when passing out of the switch. This is used by the controller and associated applications.
- Configure ports to pass all active VLANs with tagging from one switch to another (there is no untagged information present in the connection). This maintains priority information between LAN switches.
- Configure ports to
  - Accept tagged information, and
  - Accept untagged information and pass it on to a specified VLAN.
- Do not use VLAN 0. The specification standard for VLAN 0 leaves room for interpretation. This can lead to incompatibility between different vendor units.
- Ensure that L2 and L3 priority recommendations for the phone are adhered to.
- Set Priority for untagged VLAN/native VLAN/default_vlan to 0.
- Some network vendors may already pre-define specific VLANs to identify other traffic, for example, Management. Do not use these existing VLANs for normal user traffic, voice or video.
- Do not share the voice or video VLAN with data devices.

WAN Layer 3 Routers

- Ensure that the packet per second (PPS) rating of routers and switches is adequate for the amount of traffic.
- Provide appropriate bandwidth management, QoS settings and queuing for routers that connect over bandwidth restricted WAN links.

Verifying Configuration of Network Switches and Routers

It is important to be able to verify that that network switches and routers are correctly configured to support QoS. There are a number of ways to do this remotely, one such method involves using Network Assessment software such as is offered by pathSolutions. Another method involves using a program called fping. For details on using this method, refer to *Appendix B fping.*

Troubleshooting Video Quality Problems

To solve video problems, the source of the problem needs to be identified and this is best done by determining where in the overall network the problem is occurring.

Once the area of the network where the problem is occurring has been determined, then the type of video problem being experienced needs to articulated.

Where in the Network is the Problem Occurring?

There are a number of questions that the administrator needs to ask in a sequential order to help isolate the source of the problem. The questions are

- Is the image transmitted from the ethernet camera to the local phone acceptable?

The phone should be put into preview mode by pressing the Show Camera button; alternately, the camera vendor's software could be used to view the ethernet camera's transmitted image.

Before proceeding to look at other areas where the problem may be located, it should be verified that the image received by the phone from the local camera is acceptable.

This testing must be performed for both the near end and far end parties. To answer this question, you will obviously need a person on the far end who can assist with the trouble shooting process.

If the local camera cannot transmit an image successfully to the local display for both the near end and far end parties, then the fault needs to be identified and resolved before proceeding.

- Can the far end party successfully receive an image transmitted from the near end?
- Can the near end party successfully receive an image transmitted from the far end?

Once all of the above questions have been answered, the Administrator will need to move onto identifying the type of video problem.

What Type of Video Problem is Occurring?

The Administrator now needs to classify the video problem into a particular category. Once the Administrator identified where the problem is occurring and what type of video problem is occurring, then the Administrator will be able to focus on what is causing this problem.

- Is the problem intermittent?

  It is important to determine if the problem is intermittent. If the problem is intermittent it could be related to other traffic loading down the network.

  If the problem is intermittent in nature, is there a pattern to when it occurs. This is important to understand because if there is a consistent time pattern it could be related to scheduled file transfer or back ups occurring on the network, or it could be related to a large number of video conferencing calls that occur on a regularly scheduled basis.

- Is audio quality affected at the same time that video problems are occurring?

  In a correctly engineered network audio and video packets will be treated differently because of different L2 and L3 QoS settings.

- Can you describe the video problems? You should be able to place a video problem into a particular category, such as:
- Audio and Video synchronization issues.

  The video looks like a poorly dubbed movie, the speaker's lips are moving but the audio is either leading or lagging the image.
- Unacceptable delays in the network.

  The image transmitted from the local camera to the local phone may have too much of a time lag.

  The image transmitted from one party to the other party may have too much of a time lag.
- The image becomes 'pixilated' or goes 'blocky'.

  Is this occurring all of the time, or only some of the time?

  Does this occur only when there is significant video motion occurring?

  Is the problem bi-directional or unidirectional?
- Is an unexpected image being received by one party?

  Is this occurring intermittently?

  Is there a pattern to when it occurs, i.e. when a party joins or leaves a conference?
- Does the received image have white sparkles or snow present in the image?

  Is this occurring intermittently or all of the time?

  Do the white pixels (sparkles) move around in the image?
- Lighting Issues

  Is there too little contrast - image is washed out?

  Is there too much contrast - there are no grey levels, image is comprised of very black and very white components.

  Is there a flicker - possibly due to fluorescent lights?

Probable Causes of Video Quality Problems

The previous exercises should have determined where in the network the problem is occurring and what type of problem is occurring. By combining this information the Administrator will now have far fewer points in the network to check for correct operation.

Synchronization Issues

Synchronization issues can be due to voice packets and video packets being received by the end point at significantly different times. Ensure that the guidelines for QoS have been followed and that at the network routers video and voice traffic streams are going into the recommended queues.

Unacceptable Network Delays

Excessive network latency can result in video packets being discarded due to their late arrival which may cause the video to be pixilated, see ‘Packet Loss’. Long network delays can also result in sluggish updates to the video stream which will appear as unnatural motion on the screen. Ensure that the guidelines for QoS have been followed and that at the network routers video and voice traffic streams are going into the recommended queues. Also ensure that network latency and network jitter does not exceed the recommended values.

Packet Loss and/or Packets out of Sequence

The following figure depicts an image that is pixilated; this type of image error is typically due to packet loss or packets being received out of sequence. Ensure that the guidelines for QoS have been followed and that at the network routers video and voice traffic streams are going into the recommended queues. Also ensure that network packet loss does not exceed the recommended values.

Figure 17. HDMI Video Pixilation

No Image being received on the HDMI Display

If the problem is related to a camera and phone in the same location, then it is likely attributed to a defective HDMI cable or an HDMI cable that is too long.

Substitute a known good cable to see if there is a change.

Flickering or Partial Image on the HDMI Display

When an HDMI display does not receive all of the video data that it should have, the image may appear with sparkles, the image may flicker or the display may only show a partial image.

When these faults are encountered, usually the HDMI cable is defective, of poor quality, routed too close to a source of electrical noise or it is too long.

Substitute a known good cable to see if there is a change.

Sparkles or Snow in Image

The signals carried in an HDMI cable are digital signals as opposed to analog signals, as a result at the pixel level the receiver either receives valid data to create a pixel or it does not receive valid data.

When valid pixel data is not received it usually causes the pixel to show up as a white pixel or a sparkle. In this case usually the HDMI cable is defective, of poor quality, routed too close to a source of electrical noise or it is too long. See the following Figure for an example of HDMI sparkle.

Substitute a known good cable to see if there is a change.

Figure 18. HDMI Sparkles or Snow

Lighting Issues

It is important to ensure that the conference room meets recommendations, such as no strong backlighting from electrical lights or sunlight coming in a window.

Often fluorescent lighting can cause either a 50 Hz or 60 Hz flicker to appear in the video image.

The Administrator should use Local Preview mode to ensure that the camera is correctly adjusted; items to consider are

- Position of the camera with respect to sources of light
- White Balance
- Brightness
- Contrast
- Exposure
- AGC
- 50 Hz & 60 Hz flicker compensation

Other Considerations Related to Video Quality Problems

HDMI Cable Quality

Contrary to some popular misconceptions, an HDMI cable either transmits the video data correctly or it does not. If the cable does not transmit the video data correctly the user will see the result on the HDMI display. If not enough video data is received by the HDMI display the user will see:

- Sparkles
- A partial image
- A flickering image
- A blank screen, and the display reporting that there is no signal

An HDMI cable will not cause:

- The colors in a display to be shifted
- Noise to appear in the image
- The image to be sharper
- The image to warmer
- The image to be softer

The above video artifacts and characteristics are valid when discussing RF and analog based video, but they are not valid parameters when discussing HDMI based video.

RF Interference Caused by HDMI Displays

It is possible that an HDMI display can radiate RF energy that will have a negative effect on analog radio and T.V. receivers. While analog receivers are unlikely to be found in a corporate or commercial setting, the administrator should be aware this possibility.

Installing HDMI Cables

It is always a good idea to test an HDMI cable's performance prior to routing the cable through walls, raceways and ceilings.

It is also good practice when routing HDMI cables to keep the cables away from power carrying cables, fluorescent light fixtures and other sources of electrical noise.

Make Use of Error Logs

The Administrator should make use of all available error logs, as they can contain helpful information.

Ethernet Camera Logs

Most ethernet camera vendors provide error logs that can be helpful with troubleshooting. The following is an example of typical error log information available from an ethernet camera.

- Parameter List: This lists how the camera's parameters have been configured.
- Access Log: This log provides information on all failed attempts to access the camera.
- Connection List: This lists all devices that are currently accessing the camera.
- Crash Report: This is an archive containing information that may be related to a camera failure.

Conference/Video Phone Logs

The phone produces error logs that the Administrator can copy to a memory card and provide to Customer Support. For details refer to the *MiVoice Conference/Video Phone Administration Guide*.

If the phne has been configured to operate with an IP Phone Analyzer (IPA) there could be useful logs available from the IPA. For details refer to the MiVoice phone System Administrator's Guide.

Network Equipment Logs

Network equipment such as L2 switches, routers and SIP Servers may have error logs that could be helpful with troubleshooting network related issues. Refer to the vendor's documentation for details.

Appendix A - Network Protocols

The phone supports the following network protocols.

Table 24. Network Protocols

Network Protocol	Supported in this Release	Version
ARP	Y	N/A
UDP	Y	IPv4
TCP I/P	Y	IPv4
ICMP	Y	
DHCP	Y	IPv4
IGMP		V1
HTTP(S)	Y	N/A
Ethernet II (DIX) frame support	Y	N/A
802.1Q priority tagging	Y	2005
802.1x with EAP-MD5	Y	v2
LLDP-MED	Y	v2009
CDPv1/v2 compliant	Y	v2
RTP for sequence checking	Y	N/A
SIP	Y	N/A
SSL	Y	N/A
NTP	Y	N/A
SNMP	N	N/A
802.3af (PoE)	Y	2003
TLS (Transport Layer Security)	Y – (The MiVoice Business will support this at Release 6.0)	N/A
ADB	Y	N/A
Remote Desktop	Y	N/A
LDAP	Y	N/A

Appendix B – Verifying Network QoS Setting with fping

> **Note:** The following procedure works only on Computers running the Windows XP Operating System, and the PC must not be a member of a network domain.

fping is a program that can be used to verify if a particular QoS setting is being honored by all of the network switches and routers involved in connecting two points.

The fping program can be used to transmit ping packets with a specific IP TOS (Type of Service) value. Since modern QoS Parameters such as DSCP make use of the 8 bit TOS field inside of an IP packet, picking the proper 8 bit value for TOS will also set a corresponding DSCP value.

fping's advantage is it displays the RETURNED value of the TOS field.

For more information on FPING and to get a copy of the program, please go to

http://www.kwakkelflap.com/fping.html

The premise of the test is to create a ping packet with a DSCP value of your choice.

Then ping the device or devices along the traceroute path, and see if the device returns the packet with an unchanged TOS (thus DSCP) value.

> **Note:** Windows operating systems by default do not allow DSCP values to be transmitted out of the network interface. To overcome this Windows restriction you have to set a registry entry called "DisableUserTOSSetting" so that Windows allows a non-zero DSCP value.

By default, most network devices will simply respond to a ping without altering the TOS value (thus DSCP). If the value comes back intact, then no device along the way in the network, or the end device has changed the value. If another value comes back, then some device along the network path has changed the value. If it comes back as zero (0) then chances are some network device in the path has a policy of not trusting TOS (or DSCP), or a device is actively setting it to zero (0) for a port or VLAN.

> **Note:** By default, when a Cisco device has any QoS enabled, any non-QoS provisioned port is set to zero out any packet's DSCP value (not trusted). If you want QOS to be transparent (Trusted) on the LAN, just turn QoS OFF (yes, OFF for the Cisco devices) and the Cisco equipment will simply ignore it and leave it alone so it gets passed on untouched.

Example # 1 of fping usage

The following example uses a decimal TOS value of 184. This sets the left-most 6 bits (this is DSCP) on the one byte TOS field to a value of 46 decimal. This is what is commonly referred to as "EF" (Expedited forwarding) for voice payloads.

C:\>fping 172.30.100.254 -v 184

Fast pinger version 2.22

(c) Wouter Dhondt (http://www.kwakkelflap.com)

Pinging 172.30.100.254 with 32 bytes of data every 1000 ms:

Reply[1] from 172.30.100.254: bytes=32 time=75.4 ms TTL=248 TOS=184
Reply[2] from 172.30.100.254: bytes=32 time=70.7 ms TTL=248 TOS=184
Reply[3] from 172.30.100.254: bytes=32 time=70.1 ms TTL=248 TOS=184
Reply[4] from 172.30.100.254: bytes=32 time=70.7 ms TTL=248 TOS=184

Ping statistics for 172.30.100.254:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss)
Approximate round trip times in milli-seconds:
Minimum = 70.1 ms, Maximum = 75.4 ms, Average = 71.7 ms

Note that in the above example we sent a 184 and get back a 184 so we can conclude that our QoS setting is being honored by all of the equipment in the network path to the end device.

Example # 2 of fping usage

The following example shows how fping can be used to detect a faulty network path where the DSCP value is forced to 0 somewhere along the path.

This example uses a decimal TOS value of 184.

C:\>fping 172.16.11.229 -v 184

Fast pinger version 2.22
(c) Wouter Dhondt (http://www.kwakkelflap.com)

Pinging 172.16.11.229 with 32 bytes of data every 1000 ms:

Reply[1] from 172.16.11.229: bytes=32 time=74.3 ms TTL=56 TOS=0
Reply[2] from 172.16.11.229: bytes=32 time=71.3 ms TTL=56 TOS=0
Reply[3] from 172.16.11.229: bytes=32 time=71.4 ms TTL=56 TOS=0
Reply[4] from 172.16.11.229: bytes=32 time=71.7 ms TTL=56 TOS=0

Ping statistics for 172.16.11.229:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss)
Approximate round trip times in milli-seconds:
Minimum = 71.3 ms, Maximum = 74.3 ms, Average = 72.2 ms

Additional details on TOS versus DSCP values

One Byte = 8 bits. The DSCP value is represented with the left-most 6 bits of the one-byte TOS field.

The right two bits are for ECN and can be safely ignored but ensure they are 00.

Therefore:

184 (decimal) = 10111000 (binary) = 101110 00 (6 bits of DSCP and the last 2 bits 00).

So, "101110" as an isolated value of 6 bits by themselves converts to 46 decimal).

Going the other way, Call Control signaling uses a decimal value of 26, this translates to 011010 so this equates to 01101000 as all 8 bits. Converting these 8 bits to decimal is: 104

So if you want to check that the Call Control signaling value of 26 is honored on a network, use 104 as the TOS value.

The other values and Class codes can be converted in a similar fashion.

A good reference is: http://www.tucny.com/Home/dscp-tos

Appendix C – Glossary

Term	Description
1080p	1080p refers to a HDTV mode that is comprised of 1080 horizontal lines of vertical resolution. The 1080p mode uses progressive scan rather than interlaced scan. 1080p uses a widescreen aspect ratio of 16:9 with a resolution of 1920 × 1080.
3300/MiVoice Business	3300 refers to the Mitel family of 3300 IP Communication Platform (ICP) controllers. These are hardware platforms that the MiVoice Business software can be deployed on.
720p	720p refers to a HDTV mode that is comprised of 720 horizontal lines of vertical resolution. The 720p mode uses progressive scan rather than interlaced scan. 720p uses a widescreen aspect ratio of 16:9 with a resolution of 1280 × 720.
AD	Active Directory (AD) is a directory service created by Microsoft for Windows domain networks. It is included in most Windows Server operating systems.
ADB	Android Debug Bridge is a versatile command line tool that lets you communicate with an emulator instance or connected Android-powered device.
Administrator	The Administrator is the person that is responsible for deployment, configuration and maintenance of networking hardware and software.
AMC	Applications Management Center. Used to activate new hardware and software licenses for Mitel products.
ARP	Address Resolution Protocol, a telecommunications protocol used for resolution of network layer addresses into link layer addresses.
Auto MDI/MDIX	MDI (Media Dependent Interface) defines the wiring standard and the standard wiring ethernet end points. MDIX (Media Dependent Interface with Crossover) defines the wiring standard for hubs and switches. Auto MDI/MDIX is a feature that automatically detects the interface type on the far end of a connection and, if necessary automatically adjusts the wiring so that the transmitter is connected to the receiver.
Auto Negotiation	A feature employed on some ethernet ports that is used to determine the speed and duplex settings that should be used based on the capabilities of both ports.
Auto Polarity	A feature employed on some ethernet ports that is used to automatically correct for wiring errors where the positive and negative leads have been reversed.
AVC	Advanced Video Coding (AVC) which is also know as H.264/MPEG-4 Part 10 is a standard for video compression, and is currently one of the most commonly used formats for the recording, compression, and distribution of high definition video. The final drafting work on the first version of the standard was completed in May 2003.
AWC	Audio and Web Conferencing is a Mitel product offering that allows you to schedule and manage conferences through a We-based interface.
BRI	Basic Rate Interface is an Integrated Services Digital Network (ISDN) configuration.

Term	Description
CAT-5	Category-5 is a twisted pair cable type that meets the specifications defined in ANSI/TIA/EIA-568-A.
CAT-5e	Category-5e is a twisted pair cable type that meets the specifications defined in TIA/EIA 568-5-A
CAT-6	Category 6 cable is a cable standard for Gigabit Ethernet and other network physical layers that is backward compatible with the Category 5/5e and Category 3 cable standards.
CAT-6a	Category 6a cable is a cable standard for Gigabit Ethernet that performs at improved specifications compared to CAT-6 cable.
CDP	Cisco Discovery Protocol is a proprietary Data Link Layer network protocol developed by Cisco Systems.
CIR	Committed Information Rate, in a Frame relay network is the average bandwidth for a virtual circuit guaranteed by an ISP to work under normal conditions. At any given time, the guaranteed bandwidth should not fall below this committed figure. The bandwidth is usually expressed in kilobits per second (kbit/s).
Coax	Coax or coaxial cable, has an inner conductor surrounded by a flexible, tubular insulating layer, surrounded by a tubular conducting shield.
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.
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.
DNS	Domain Name Server. A means of translating between typed names and actual IP addresses, for example, microsoft.com = 207.46.134.222
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.
DTMF	Dual Tone Multi-Frequency. In-voice-band tones used by telephones to signal a particular dialed digit. Also known as touch tone.
Duplex	A duplex communication system is a point-to-point system composed of two connected parties or devices that can communicate with one another in both directions simultaneously. An example of a duplex device is a telephone.
EAP-MD5	Extensible Authentication Protocol is an authentication framework frequently used in wireless networks and Point-to-Point connections. It is defined in RFC 3748.

Term	Description
F connector	The F connector is a coaxial RF connector commonly used on television, cable television and satellite television equipment.
FLASH Drive	A Flash Drive is a data storage device that includes flash memory with an integrated Universal Serial Bus (USB) interface.
fps	Frames Per Second
Gb/s	GigaBits Per Second. Billion bits per second is a measure of bandwidth on a telecommunications medium. May also be written as Gbits/s or Gb/s. Mb/s is not to be confused with GBps (megabytes per second).
GigE	Gigabit Ethernet, a high speed LAN technology defined by the Standard IEEE 802.3-2008.
H.264	H.264/MPEG-4 Part 10 or AVC (Advanced Video Coding) is a standard for video compression, and is currently one of the most commonly used formats for the recording, compression, and distribution of high definition video.
HDMI	High Definition Media Interface is an audio/video interface used for transferring digital audio/video data from a HDMI-compliant device to a compatible digital audio device, computer monitor, video projector or digital television.
HDTV	High Definition TeleVision is a standard which provides a higher resolution than standard-definition television.
HTTP	The Hypertext Transfer Protocol (HTTP) is an application protocol for distributed, collaborative, hypermedia information systems.
HTTPS	HTTPS is a communications protocol for secure communication over a computer network, with especially wide deployment on the Internet.
ICE	Interactive Connectivity Establishment is a technique used in computer networking involving network address translators (NATs) in Internet applications of Voice over Internet Protocol (VoIP), peer-to-peer communications, video, instant messaging and other interactive media.
ICMP	Internet Control Message Protocol is a protocol used to help identify when devices are present and create warnings when they fail.
IEEE 802.1p/Q	Refers to two IEEE standards 802.1P and 802.1Q that provide for eight traffic classes drawn from priority fields in the VLAN tags. These standards are used to apply QoS to specific packets.
IEEE 802.1x	IEEE 802.1X is an IEEE Standard for port-based Network Access Control. It provides an authentication mechanism to devices wishing to attach to a LAN or WLAN.
IEEE 802.3ab	Also know as 1000BASE-T. This is the standard for Gigabit Ethernet over twisted pair at 1 Gbit/s (125 MB/s).
IEEE 802.3af	This is the IEEE standard for supporting power over ethernet.
IEEE 802.3at	This is an IEEE standard for supporting power over ethernet with increased power ratings.

Term	Description
IGMP	The Internet Group Management Protocol is a communications protocol used by hosts and adjacent routers on IP networks to establish multicast group memberships.
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.
IPA	IP Phone Analyzer, a diagnostic tool produced by Mitel.
IPv4	Internet Protocol version 4 is the fourth revision in the development of the Internet Protocol (IP) and the first version of the protocol to be widely deployed.
ISP	An Internet service provider is an organization that provides access to the Internet.
ITU	International Telecommunication Union is the specialized agency of the United Nations which is responsible for information and communication technologies.
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.
LCD	Liquid Crystal Display refers to a flat panel display commonly used on telephones, calculators and Flat Panel Televisions.
LDAP	Lightweight Directory Access Protocol is a protocol that is used for accessing and maintaining distributed directory information services over an IP network.
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.
Mains	Mains is the general-purpose alternating-current (AC) electric power supply that is delivered over the power utility transmission grid.
Mb/s	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. Mb/s is not to be confused with Mb/s (megabytes per second).
MBG	MiVoice Border Gateway
MCD	Mitel Communications Director (now MiVoice Business)

Term	Description
MiVoice Conference Unit	The MiVoice Conference Unit is an Audio Conference Bridge with In-room Collaboration, Part Number 50006580
MiVoice Video Unit	The MiVoice Video Unit is a Video Conference Bridge with Remote Collaboration, Part Number 50006591
MDI/MDIX	See Auto MDI/MDIX
MOS	Mean Opinion Score, a scoring method used for evaluating the voice quality of telephone networks and equipment.
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.
NA	North America, a short form.
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.
NEMA	National Electrical Manufacturers Association is an American organization that provides a forum for the development of technical standards that are in the best interests of the industry and users.
NIC	Network Interface Card. Physical connection to the network. In a PC, this is often a plug-in card.
NTP	NTP (Network Time Protocol) allows the phone to set its time of day clock. The phone will access the default server at the URL - 2.android.pool.ntp.org - on the internet to obtain the current time of day.
Octet	An octet is a unit of digital information in computing and telecommunications that consists of eight bits.
ONVIF	Open Network Video Interface Forum is a global and open industry forum with the goal to facilitate the development and use of a global open standard for the interface of physical IP-based security products.
PBR	Policy Based Routing a technique used to make routing decisions based on policies set by the network administrator. A router will typically route a packet based on the packet's destination address. However, with PBR the router will forward the packet based on other criteria such as the packet's source address, the size of the packet, the protocol, the packet's payload or other information contained in the packet's header or payload.
PBX	Private Branch Exchange is a telephone exchange that serves a particular business or office.
PoE	Power over Ethernet is a method of delivering operating power to an IP device over the LAN cabling.
PoE Plus	The updated IEEE 802.3at-2009 PoE standard also known as PoE+ or PoE plus, provides up to 25.5 W of power.

Term	Description
PoE+	The updated IEEE 802.3at-2009 PoE standard also known as PoE+ or PoE plus, provides up to 25.5 W of power.
POTS	Plain Old Telephone Service is the voice-grade telephone service that remains the basic form of residential and small business service connection to the telephone network in many parts of the world.
PPP	Point-to-Point Protocol is a data link protocol commonly used in establishing a direct connection between two networking nodes.
PPS	Packets Per Second. In communication networks, such as Ethernet the throughput of the network or networking equipment is measured in packets per second.
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.
Proxy	A proxy server is a server (a computer system or an application) that acts as an intermediary for requests from clients seeking resources from other servers.
PSTN	Public Switched Telephone Network. The telephone network that provides local and long distance connections, e.g. Bell, AT&T, BT.
QoS	Quality of Service refers to several related aspects of telephony and computer networks that allow the transport of traffic with special requirements.
RCS	Redirection and Configuration Service (RCS) is a service that offers touchless deployment, firmware control, and branding of Mitel devices.
RF	Radio Frequency
RJ-45	A connector standard commonly used for terminating ethernet cables.
RSTP	Rapid Spanning Tree Protocol. A version of STP that will converge networks more rapidly than STP (see STP).
RTP	Real-time Transport Protocol defines a standardized packet format for delivering audio and video in real time over IP networks.
RTSP	Real Time Streaming Protocol is a network control protocol designed for use in entertainment and communications systems to control streaming media servers. The protocol is used for establishing and controlling media sessions between end points.
SD Card	Secure Digital Card is a non-volatile memory card format for use in portable devices.
SDHC Card	Secure Digital High Capacity Card is a format, defined in Version 2.0 of the SD specification which supports cards with capacities up to 32 GB. The SDHC trademark is licensed to ensure compatibility
SIP	Session Initiation Protocol. An IETF standard for signaling over IP.
SLA	Service Level Agreement is part of a service contract where the level of service is formally defined.

Term	Description
SNMP	Simple Network Management Protocol is a standardized protocol for managing devices on IP networks.
SNTP	Simple Network Time Protocol is a networking protocol used to synchronize clocks between computer systems over packet-switched, variable-latency data networks.
Soft Switch	A softswitch is a central device in a telecommunications network which connects telephone calls from one phone line to another, typically via the internet, entirely by means of software running on a general-purpose computer system.
SRTP	Secure Real-time Transport Protocol defines a profile of RTP (Real-time Transport Protocol), intended to provide encryption, message authentication and integrity, and replay protection to the RTP data in both unicast and multicast applications.
SSL	Secure Sockets Layer is a cryptographic protocol that provides communication security over the Internet
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.
STUN	Session Traversal Utilities for NAT is a network protocol that is used in NAT traversal for applications such as real-time voice and video IP communications, STUN is documented in RFC 5389.
T1	Primary Rate. Provides 23 or 24 channels of trunks per connection
TCP/IP	Transmission Control Protocol Internet 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.
Teleworker	A Mitel Solution that enables employees to work remotely with full access to voice mail, conferencing, and other features of the office phone system.
TLS	Transport Layer Security is cryptographic protocol that provides communication security over the Internet
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.
TRS	Tip Ring Sleeve is a common family of connector typically used for analog signals including audio, it is cylindrical in shape. It is also termed an audio jack, phone jack, phone plug, and jack plug.
UC Endpoint	Unified Communications is an application that provides a single access point for all your business communication and collaboration needs. A UC End Point is an end point such as a telephone or PC that is enabled for Unified Communications.
UDP	User Datagram Protocol. A layer 4 protocol with minimal handshaking and overhead. Used to stream voice. Considered connectionless.

Term	Description
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.
USB	Universal Serial Bus is an industry standard that defines the cables, connectors and communications protocols used on a bus for connection, communication and power supply between computers and electronic devices
UTP	Unshielded Twisted Pair. Cable that reduces emissions and maintains an impedance match through the twists per meter in the cable without resorting to shielding.
V	Volt is the SI derived unit for electric potential (voltage), electric potential difference, and electromotive force.
VAD	Voice Activity Detection, also known as speech activity detection, is a technique used in speech processing in which the presence or absence of human speech is detected.
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.
VoIP	Voice over IP, a technology used for transmitting and receiving voice over IP networks.
VPN	Virtual Private Network is a technology for using the Internet or another intermediate network to connect computers to isolated remote computer networks that would otherwise be inaccessible.
WAN	Wide Area Network. A network connection to a network that could be global, e.g. via Frame Relay.
Watt	The watt is a SI derived unit of power. The unit, defined as one joule per second, measures the rate of energy conversion or transfer.
Wi-Fi	Wi-Fi Alliance technology for Wireless LAN based on IEEE 802.11.
WUXGA	Widescreen Ultra Extended Graphics Array is a display resolution of 1920×1200 pixels with a 16:10 screen aspect ratio. It is a wide version of UXGA, and can be used for viewing high-definition television (HDTV) content.