Mitel
Powering connections

Application Note AN3269

Sep 15, 2021

Network and Firewall Best Practices for MiCloud Connect (Customer Provided Connectivity Only)

Description: The purpose of this document is to summarize the requirements for the customer's local network and firewall. The information published in this document is focused specifically on customers who connect to the Mitel Cloud via the Internet. This guide does not apply to customers connected to Mitel via private connections such as MPLS, Ethernet or T1 circuits.

Environment: Mitel MiCloud Connect with Internet Connectivity Only

Summary: This application note discusses the use of data networking and customer firewall best practices in Mitel MiCloud Connect for ***only* those customers connecting via Internet.** Network Administrators must consider a multitude of complex configuration designs and networking parameters when designing a small or large-scale local area network (LAN) with or without remotely connected sites over a wide-area-network (WAN). Essential tools for VoIP include the use of Virtual LANs (VLANs), Quality of Service (QoS) and firewall configurations to provide excellent voice quality over a "best effort" Internet connection. Please refer to your network equipment manufacturer's documentation to apply the ideas and concepts presented in this document to your specific equipment and environment.

NOTE: Customers connecting to Mitel via dedicated circuits (T1) or MPLS should consult with Mitel Activations for specifics related to this type of connection. The majority of the concepts discussed in this document also apply to an "on-net" customer with some slight modifications to the WAN configuration.

Table of Contents

Selecting Data Networking Equipment for a Mitel Connect Deployment

Which Data Network Manufacturers Are Supported?

Mitel does not endorse any single data network manufacturer over another for use with a Mitel Connect deployment but compatible equipment manufacturers and models are any that have been certified through the Mitel TechConnect 3rd party technology partner program or any other major data network equipment provider that meets the following equipment requirements and deployment best practices.

What Are the Data Network Equipment Minimum Requirements for Deployment?

1. A “managed” switch or router with GUI or CLI administrative capabilities to configure the networking device. Mitel does not recommend connecting any non-managed switches or hubs to the network. If a non-managed switch must be connected, only the data VLAN should be configured on the port with proper duplex settings to avoid collisions on the network.
2. Supports PoE with enough power for all connected IP phones simultaneously (access-layer switches only)
3. Supports LLDP and LLDP-MED (edge data switches only)
4. Supports a minimum of 2 VLANs on all switches (1 for voice, 1 for data) and trunking with 802.1Q VLAN tagging.
5. Supports QoS at layer 2 for edge devices and layers 3 and 4 for core switches and routers, which include queuing, shaping, selective-dropping, DSCP trust and link-specific policies.
6. Optional high availability and advanced routing supports Rapid Spanning Tree, VTP, BGP, OSPF, HSRP, VRRP or similar protocols.
7. Supports auto speed and duplex negotiation by default, with option to force-configure individual port speed and duplex modes when necessary.
8. Provide individual-port speed and duplex mode indication, plus error & traffic statistics, which are useful in troubleshooting.

Ethernet (repeater) hubs are strictly half-duplex devices and therefore should **never be used** to connect any Mitel devices. Auto-negotiating full-duplex Ethernet switches should always be used.

Ethernet switches are available in two basic forms, managed and non-managed switches. Manageable switches cost more than non-manageable ones but provide several useful features such as manual port duplex configuration and statistics reporting as well as an administrator CLI or GUI. Non-manageable switches can only perform auto-negotiation and provide no statistics or CLI/GUI.

Although non-manageable switches can be used in some cases, such as a small office with less than 5 phones, they are **NOT** recommended and void the Mitel managed Service Agreement (SLA). Non-managed LAN switches don't provide traffic separation, traffic prioritization, queuing and error statistics required when VOIP is deployed in an office environment.

Customer Site Cable Plant Requirements

To avoid the possibility of lost packets due to corrupted electrical signals, the Ethernet wire plant and associated patch cables to each IP-phone, IAD, or network device, should be a minimum of CAT-5 UTP cable.

Ideally, each station-pull should be certified for conformance to IEEE 802.3 specifications with a commercially available CAT-5 cable tester. The tester should include conformance tests for DB insertion loss, cross talk, impedance, wire mapping, and capacitance.

Half/Full-Duplex

Ethernet interfaces operate in either half-duplex or full-duplex mode.

In half-duplex mode, only one Ethernet frame can be transmitted across the interface at a time in either direction. If both devices should begin transmitting frames at the same time, a collision is detected and both devices abort their transmissions and retry again later. This situation adds delay and can cause packets to be discarded when excessive collisions occur which will affect voice quality and overall VOIP performance.

In full-duplex mode, Ethernet frames can be sent in both directions simultaneously, thereby doubling the available bandwidth and eliminating the possibility of collisions and their associated delays and lost packets. With VoIP networks, it is desirable for all Ethernet interfaces to operate in full-duplex mode. This is a mandatory requirement for Real Time Protocol (RTP) traffic aggregation points, such as (switch-to) router, firewall, gateway, streaming server, and other-switch interfaces that carry VOIP traffic.

Auto (Duplex) Negotiation Configuration

Most Ethernet switches and station devices perform automatic duplex negotiation, and default to this mode of operation. When two auto-negotiating Ethernet devices are first connected, a set of "link code words" are transmitted by each device, advertising its own speed and duplex capabilities to the other device.

Assuming each device successfully receives and understands the link code words of its peer, the two devices will auto-configure themselves for the best duplex mode possible (e.g., full is preferred instead of half), and the highest speed possible (e.g., 10/100), that is supported by both. Full duplex via auto negotiation is the preferred mode of operation for all VOIP Ethernet devices and should be used wherever possible.

> **NOTE:** If either the switch or station device should fail to receive or understand the link code words from its peer, (a rare occurrence, but one that does occur) that device will default to operating in half-duplex mode. However, if the peer should successfully receive and understand the local devices link code words and the local device has advertised full-duplex capability, the peer will configure itself to full-duplex, thus resulting in a duplex mismatch situation. This condition always results in interface errors and dropped packets!

Forced Duplex Configuration

Some auto-negotiating interfaces that should be running full-duplex can fail to auto negotiate to full-duplex at both ends. The interface must be force-configured or manually configured to operate in full-duplex at both ends to work correctly.

> **NOTE:** Forcing a device to operate at a specific speed or duplex mode disables transmission of the auto-negotiation code words by that device when initially connected to another device. This prevents the other device from ever being able to auto-negotiate to full-duplex. If either device is forced to operate in full-duplex, the other device must also be forced to operate in full-duplex.

Summary of Valid Duplex Configurations

The table shown in Figure 1 below summarizes all the possible duplex configuration modes between connected Ethernet devices and their validity as applicable to VOIP applications.

Device 1	Device 2	Validity
Auto-full	Auto-full	Preferred for all devices
Auto-full	Auto-half	Invalid - duplex mismatch produces errors – Force both ends to full-duplex; or if both ends don't support force-full, try a different model of Ethernet switch.
Forced-full	Auto	Invalid – No code words sent by forced end, auto-end defaults to half-duplex. Mismatch produces errors.
Forced-full	Forced-full	Used as alternative when auto-auto fails to produce full-full.
Auto-half	Auto-half	Not recommended for any VOIP connected/aggregation devices.

Figure 1

Designing VLANs for VoIP

What Is a VLAN?

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

> **TIP:** Segmenting similar layer-2 traffic into separate subnets/VLANs helps mitigate propagating unnecessary traffic across too many data switch interfaces resulting in a more congested data network.

Data networks tend to be "noisy" and chatter endlessly throughout the day and night. This adversely impacts real-time devices such as phones, videophones, video conference systems etc. This can be exacerbated if a data device gets a virus causing increased "noise" on the network which drowns out the voice traffic. Some data devices (printers or servers) send and receive large amounts of data on a regular basis (images, database queries, presentations, emails with large attachments). To prevent real time voice and video from being "squeezed" out of the network, sites with VOIP should have data and voice separation using physical separation (cabling) or virtual separation with VLANs. A well-designed site will separate network traffic by function with a VLAN for phones and additional VLANs for PCs, printers, servers, Wi-Fi devices etc.

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

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

How Can I Design VLANs into my Network?

After understanding the importance of using multiple VLANs, particularly with voice, consider certain best practices on how to design multiple VLANs into your network topology effectively. When using multiple VLANs, at least one data switch at a given site must have layer-3 IP routing functionality enabled to route IP traffic between local VLANs. This layer-3 data switch is also referred to generally as the "core" switch and acts as a traffic cop for the LAN topology. Some Internet connected customers will use their firewall as the layer-3 gateway for each VLAN (this is an acceptable configuration but requires proper configuration of the firewall. See firewall section below).

> **IMPORTANT TIP:** Avoid "daisy chaining" switches together across the network to prevent potential congestion bottle necks. In other words, L2 switches should connect using a hierarchal layer, "many-to-one," directly to the core L3 switch. This is known as the Core→Distribution→Access network design topology. Example:

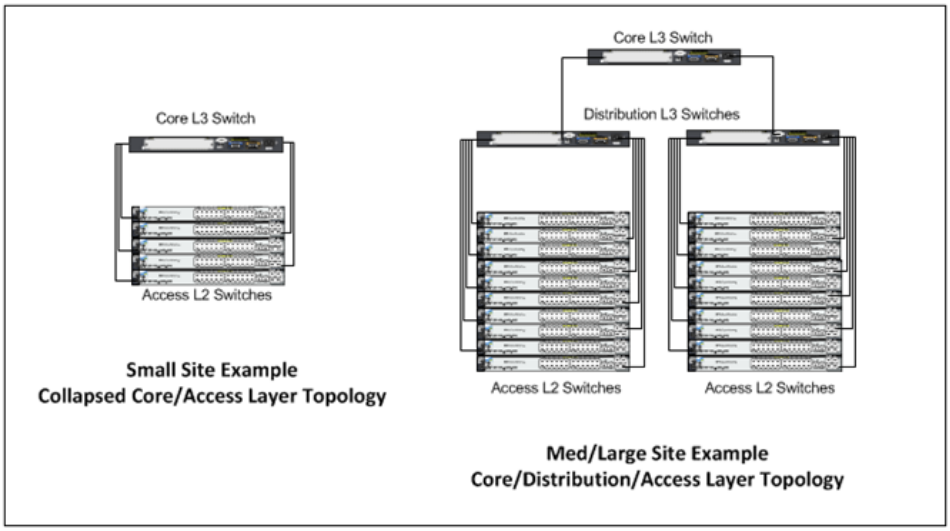


Figure 2

Now that the voice and data VLAN's are directly connected to the core layer-3 switch, IP routing can occur automatically between any 2 VLANs for all the trunked layer-2 switches with a properly configured default gateway or VLAN interface IP on each VLAN.

What Is a VLAN Tag or VLAN ID?

The industry standard for VLAN tagging is an IEEE specification called 802.1Q. The device connected to the VLAN-tagged port, in this case the L3 switch/router, must be capable of understanding 802.1Q tags and its network interface must be configured to have VLAN tagging enabled and have specific VLAN IDs assigned to it per the network hardware manufacturer's configuration guide documentation. Each packet is marked within a switch by a VLAN ID number called a VLAN tag (generally a number between 1 and 4096) to identify the VLAN. The tags are stripped off when the packets are transmitted to devices connected to standard ports on the switch. These standard ports connected to standard devices are called "untagged ports". When assigning more than one VLAN to a single data switch port, the first or default VLAN is the "untagged" VLAN, typically the data VLAN, and all additional VLANs on the same port are "tagged," typically the voice VLAN. Some switch manufacturers refer to a single VLAN on a port as "untagged" and multiple VLANs on the same port as all "tagged" VLANs. The devices within each VLAN still need to use a default gateway to be routed to another subnet/VLAN.

> **IMPORTANT TIP:** It is highly recommended that each VLAN's Default Gateway be the "VLAN interface IP address" configured on the layer-3 core switch or in some cases an actual router acting as the "core" layer-3 routing module. Using the site firewall as the default gateway for each VLAN can be done at smaller sites but is not recommended for sites with 30+ phones/PCs.

Example VLAN Default Gateway Assigned on Core Switch:

The proper way to set a default gateway for each VLAN on the layer-3 core switch is to assign one IP address in the VLAN's useable IP address range (e.g., 10.X.X.1) to the VLAN interface. When creating the DHCP scope for a given VLAN, the default router or default gateway for the associated VLAN will be the IP address of the corresponding 'VLAN interface' configured on the layer-3 switch. This allows routing to occur between VLANs on the layer-3 switch for a non-routing aware device like a PC, server, or IP phone.

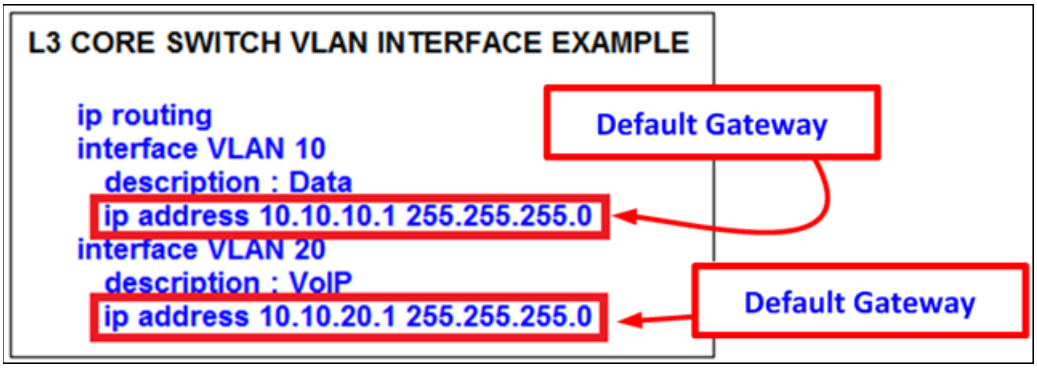


Figure 3

Firewall's Are for Security, not for LAN Routing or Switching

In general firewalls should not be used to route traffic between VLANs unless the firewall supports creating multiple VLANs with a L3 routing table, it is recommended to create a separate VLAN for the firewall uplink between the firewall and the L3 data switch as a point-to-point VLAN. The VLAN to the firewall should be setup to allow all tagged and untagged packets in order to not inadvertently drop tagged packets in certain configurations.

> **IMPORTANT TIP:** Avoid (1) hair-pining LAN traffic through the firewall, (2) using the firewall as the L3 LAN switch, or (3) configuring devices to use the firewall's inside IP address as the LAN's default gateway. This potentially causes inadvertently blocked ports, port buffer overruns/tail drops, link congestion, one-way audio in certain call scenarios and general voice quality issues.

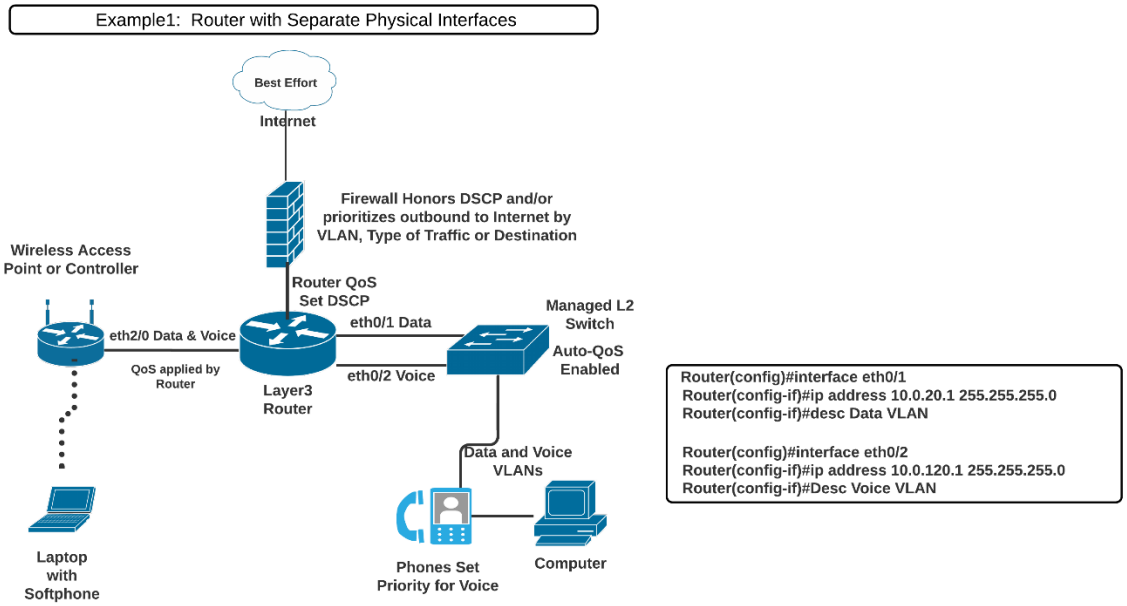
> **TIP:** The point-to-point VLAN is a common method to connect separate L3 routing devices that separates the layer-2 LAN traffic from the firewall for better firewall and LAN performance. It also better manages IP addressing by using a /30 subnet mask with only 2 useable IP addresses, one for each side of the point-to-point connection.

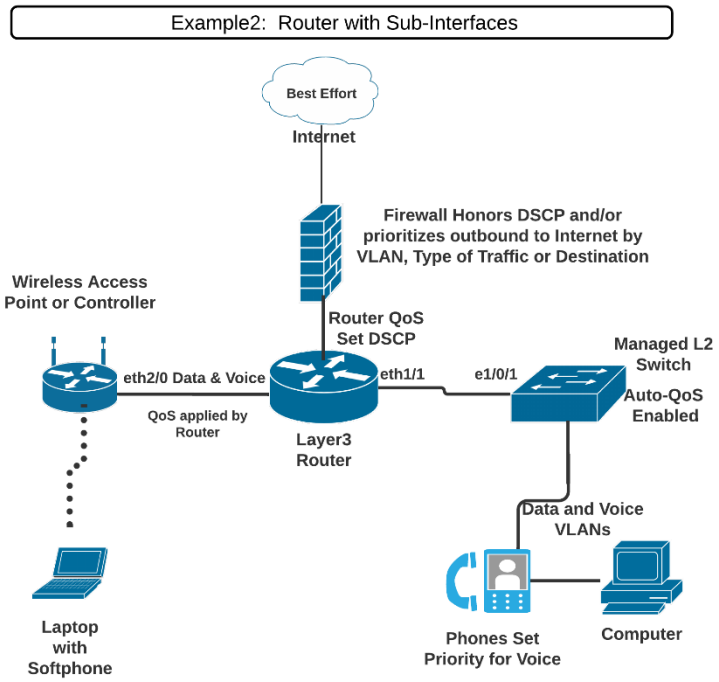
There are multiple ways to configure a data network for VoIP, especially in larger networks; however, if other preferred methods achieve the same design principles and outcomes discussed here then they are generally acceptable for a Mitel MiCloud Connect deployment.

Summary of Designing Multiple VLANs into the Data Network

- Create separate VLANs for VOICE and DATA as well as any other types of traffic that may need to be segregated similarly to enhance data network performance on a LAN.
- Trunk all Voice and Data VLANs on each layer-2 switch across the LAN uplink(s) to the site's layer-3 core switch or router.
- Avoid trunking any LAN VLANs across WAN links to/from other sites, particularly Voice.
- Each site will have its own set of Voice and Data VLANs with separate IP addressing per VLAN at each site. VLAN ID numbering can be reused from site to site.
- When using a single LAN switch for a site, ensure the switch supports both layer-2 and layer-3 routing functionality enabled to route IP traffic between local VLANs.
- When using multiple LAN switches for a site, ensure at least one "core" data switch has layer-3 IP routing enabled to route IP traffic between VLANs on all local layer-2 switches.
- Each VLAN will have its own VLAN interface IP address that also serves as that subnet/VLAN's Default Gateway. Avoid using a firewall, server, or any data switching device or appliance other than the designated "core" layer-3 switch at each site to address each VLAN interface with its respective Default Gateway.

The diagrams below show some common VOIP deployment examples:





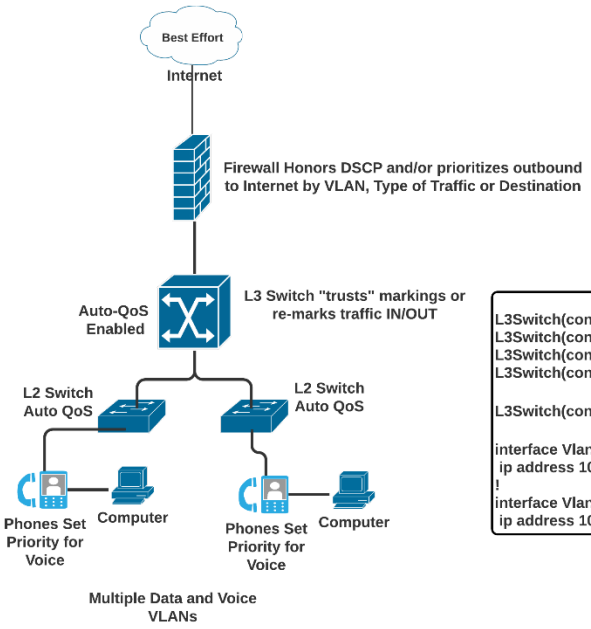

```
Switch(config)#interface Ethernet1/0/1
Switch(config-if)#switchport trunk encapsulation dot1q
Switch(config-if)#switchport mode trunk
Switch(config-if)#switchport trunk allow vlan 20,120

Router(config)# interface eth1/1
Router(config)# no shutdown
Router(config)# no ip address

Router(config)# interface eth1/1.20
Router(config)# desc Data VLAN 20
Router(config-subif)# encapsulation dot1Q 20
Router(config-subif)# ip address 10.0.20.1 255.255.255.0

Router(config)# interface eth1/1.120
Router(config)# desc Voice VLAN 120
Router(config-subif)# encapsulation dot1Q 120
Router(config-subif)# ip address 10.0.120.1 255.255.255.0
```

Example3: Layer 3 Switch

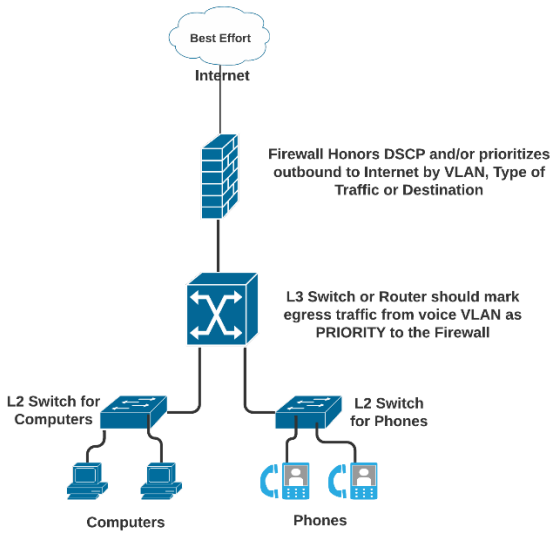



```
L3Switch(config)# vlan 20
L3Switch(config-vlan)# name Data
L3Switch(config)# vlan 120
L3Switch(config-vlan)# name Voice

L3Switch(config)# ip routing

interface Vlan20
 ip address 10.0.20.1 255.255.255.0
!
interface Vlan120
 ip address 10.0.120.1 255.255.255.0
```

Example4: Physical Separation "Old School - No VLANs"



Configuring VLANs for IP Phones

Piggy-back the PC to the IP Phone

IP phones are a specialized device on the data network and have capabilities and requirements that need to be considered when designing the data network. For example, to help better utilize port capacity on data switches, a PC can piggy-back on an IP phone and share a single data switch port, utilizing VLAN trunking or tagging the Voice and Data VLANs for each device respectively. This design avoids having 2 LAN connections or ”drops” at each desk (one for the phone and one for the computer).

IP phones have an internal 2-port switch on the back of the IP phone to connect it to the data network through the network port as well as a PC through the access port. Mitel IP phones prioritize voice, so the connected PC is unable to disrupt outbound voice quality.

Most data network equipment manufacturers have a voice VLAN feature either at the data switch access port or VLAN level that supports various VoIP capabilities. The Voice VLAN feature uses classification and scheduling to send network traffic from the switch in a predictable manner for IP phones. By default, the voice VLAN feature is disabled on most LAN switches. Once enabled the LAN switch will create queues and look at the priority of the traffic as marked by the phone. This ensures small, time-sensitive voice does not get stuck behind a large print job started by the connected PC.

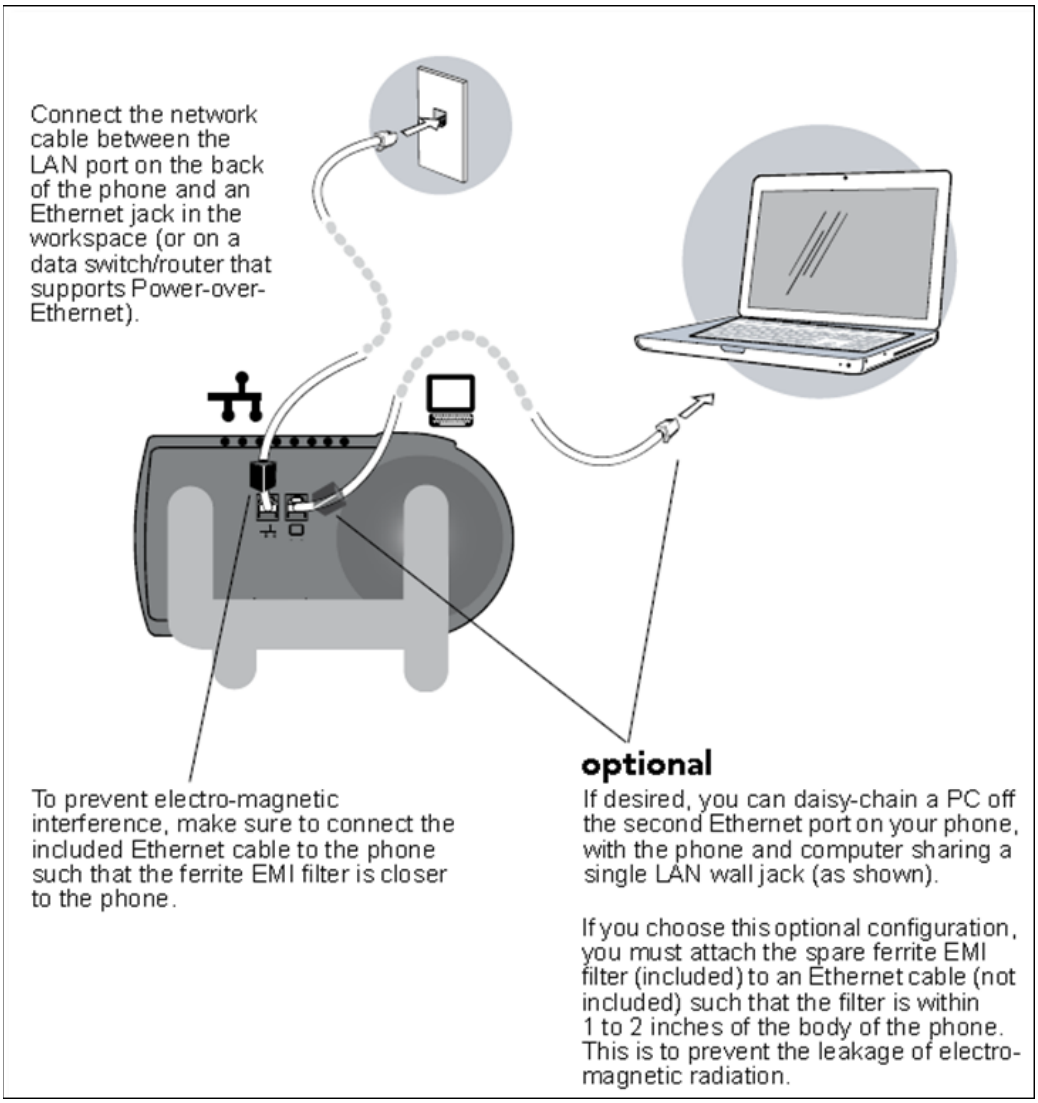


Figure 4

Figure 4 above demonstrates the physical connection of a PC connected to an IP phone in turn connected to the network connection on a single data switch access port. For further discussion, how an IP phone is automatically assigned to the Voice VLAN when the Voice and Data VLANs are both assigned to the data switch port, refer to “Configuring Automatic IP Phone VLAN Assignment – LLDP-MED” on page 14.

Figure 5 below demonstrates a Cisco data network example of how to configure the voice VLAN feature on the data switch access port to support both Voice and Data VLANs for each IP phone. Figure 5 also shows the access port configuration when the Voice VLAN is the only VLAN (i.e., untagged VLAN) applied to the port for each dedicated IP phone.

```
L2 SWITCH CONFIGURATION
interface FastEthernet1    (and port 4)
  description : These ports have BOTH phone + PC
  switchport mode access
  switchport access vlan 10
  switchport voice vlan 20
  spanning-tree portfast
  no cdp enable
interface FastEthernet2    (and ports 5,11,12)
  description : These ports have ONLY voice devices
  switchport mode access
  switchport access vlan 20
  spanning-tree portfast
  no cdp enable
interface FastEthernet3    (and ports 6 & 10)
  description : These ports have ONLY data devices
  switchport mode access
  switchport access vlan 10
  spanning-tree portfast
  no cdp enable
```

Figure 5

The different port configuration examples above include the following two commands on each Fast Ethernet port when our devices are present:

spanning-tree portfast

no cdp enable

Although these statements are not required, it is recommended that CDP (Cisco Discovery Protocol) be disabled on Ethernet ports not connected to Cisco devices to reduce unnecessary traffic. In addition, Spanning Tree should be set to either “portfast” or “rapid spanning tree” mode for Cisco switches or “edge” for Juniper switches. This will allow faster boot times and fewer network issues when connecting to IP phones.

Mitel leverages the use of VLANs to integrate into the network topology that you, the network administrator, have decided is most appropriate for your LAN topology. Mitel does not require nor dictate that you use a specific vendor’s equipment for your LAN edge, core, WAN, switches, routers, operating systems, etc., as long as your data hardware supports the minimum recommended requirements presented in this document.

Automatically assigning VLANs to a Mitel phone can be done via 2 methods as described in the next 2 sections:

1. LLDP-MED
2. DHCP Scope Option 156

IMPORTANT NOTE: Setting VLAN should be done by LLDP or DHCP—not both simultaneously.

Configuring Automatic IP Phone VLAN Assignment – LLDP-MED

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

Automatic VLAN Assignment Using LLDP-MED During IP Phone Standard Boot Process

1. As the IP phone powers up, the Ethernet switch sends LLDP Data Units defined as LLDP_Multicast packets to the Phone.
2. The IP phone responds in kind adding TIA Organizationally Specific Type-Length-Value (**TLV**) such as VLAN assignment, manufacturer, location, power requirements etc.
3. The Ethernet switch in turn responds to the phone with the same TIA LLDP-MED TLV extensions and in the "TIA – Network Policy" TLV, the designated VLAN Id of the Voice VLAN is offered to the phone (e.g., VLAN Id: 50 as shown in Figure 6 below).

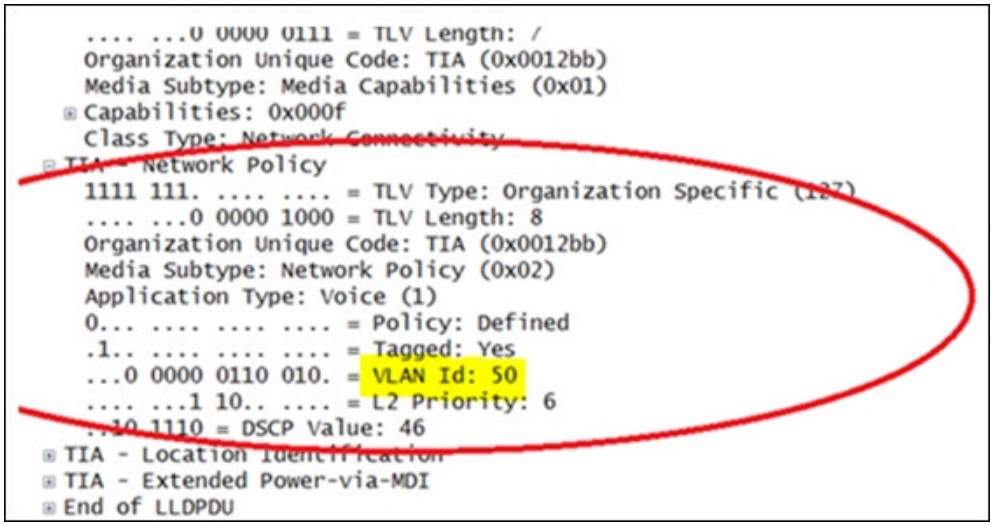


Figure 6

4. The IP phone performs a typical DHCP sequence of Discover, Offer, Request, Ack to get an IP address plus available DHCP Options from the Voice VLAN.
5. The IP phone via FTP downloads its configuration file, upgrades the Boot Image if needed and reboots
6. The IP phone registers successfully and is ready for service.

LLDP is enabled by default on all Mitel manufactured IP phones. All Ethernet switches in the data network intended to support IP phones via LLDP should be configured per the Ethernet switch manufacturer's documentation and appropriate

IP Phones for MiCloud Connect

LLDP-MED can also send a default DSCP value assignment to the IP phone for application type voice. To better understand the IP phone's inheritance behavior, in general, the last setting assigned wins unless some other logic prevails.

- LLDP OFF: ST DSCP used for RTP and Signaling
- LLDP-MED TLV ON with a default of 0: ST DSCP used for RTP and Signaling
- LLDP-MED TLV ON with a non-zero value: LLDP used for RTP. ST DSCP used for Signaling

Configuring Automatic IP Phone VLAN Assignment – DHCP

1. **Considerations for DHCP:** DHCP is a layer2 broadcast technology meaning it can't leave its assigned VLAN without help. DHCP automatically assigns several mandatory and some optional parameters to devices on the network. When VLANs are assigned and DHCP is used, you must configure a method for DHCP broadcasts to reach your DHCP server. The methods for doing this are:
    a. **BEST Method:** Utilize DHCP Helper or Forwarder. Most switch manufacturers will provide a configuration tool that will forward or "help" the DHCP broadcast reach the IP address of the DHCP server. The server will then respond directly (unicast) back to the DHCP requestor with an OFFER of an IP address. In the Cisco world, this is called an "ip-helper" address.
    b. **2nd Method:** Trunk port to the DHCP server. This is recommended only in cases where helper/forwarder is not available, and you have dedicated DHCP servers (servers not running other applications). The LAN connection to the DHCP server can be turned into a "trunk port" meaning it will be assigned all VLANs where DHCP devices exist. The server will then "listen" to everything put on the wire (including DHCP) and respond with an OFFER of an IP address to the device.

Creating Data and Voice DHCP Scopes on Microsoft Server (Example):

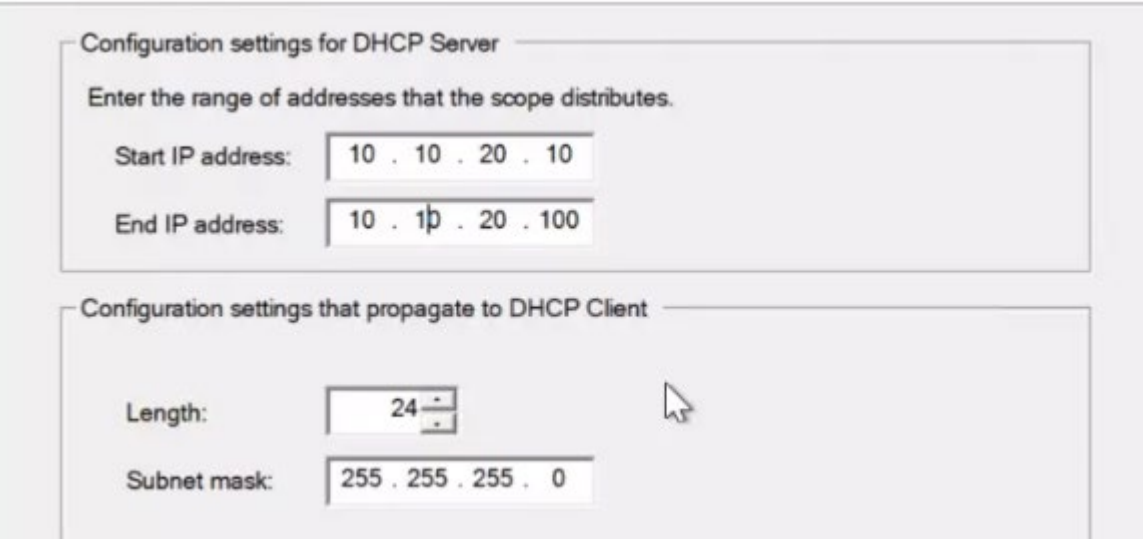
Step 1: Create 2 new scopes (IP ranges/subnets) on the DHCP server, one for data and one for voice. We will create the following 2 scopes:

DATA VLAN: 10.10.20.0/24 VLAN 20 (valid host range = 1 thru 254)

VOICE VLAN: 10.10.200.0/24 VLAN 200 (valid host range = 1 thru 254)

Step 2: Input the START and END of the IPs that you want to be automatically "OFFERED" to computers on the Data VLAN. The computer and phone will first boot to the data VLAN then the phone will see via OPTION 156 that it needs to reboot into the Voice VLAN and "tag" its traffic to get a voice IP address.

Note: You should not use the entire host range of 1 through 254 (for /24 subnet). In most cases its best to exclude the bottom or top of the IP range for things that do not use DHCP like routers, firewalls, or devices you don't want to ever change their IP (static IP devices).



Click NEXT →

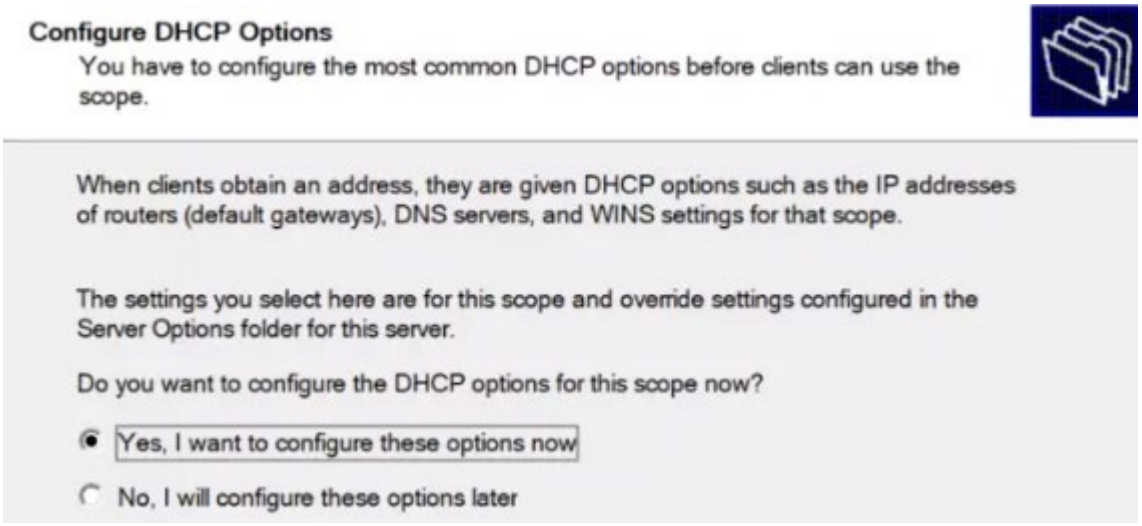
The next 2 items are described without screenshots for brevity.

DHCP EXCLUSIONS: This window allows you to select a subset of the IPs in the DHCP scope that you do not want the server to hand out. For example, we could have put the entire range above as 1 thru 254 and then put in an EXCLUSION for IPs 1 thru 10. This is somewhat user preference and can be skipped if you already excluded some IPs as seen above. At a minimum, 1 IP must be excluded per network to act as a gateway.

LEASE DURATION: Lease duration is the time DHCP Server will give a specific computer or client an IP before changing it or giving it another one when it logs-in again. The default of 8 days is usually acceptable.

Step 3: Configuring DHCP SCOPE Options

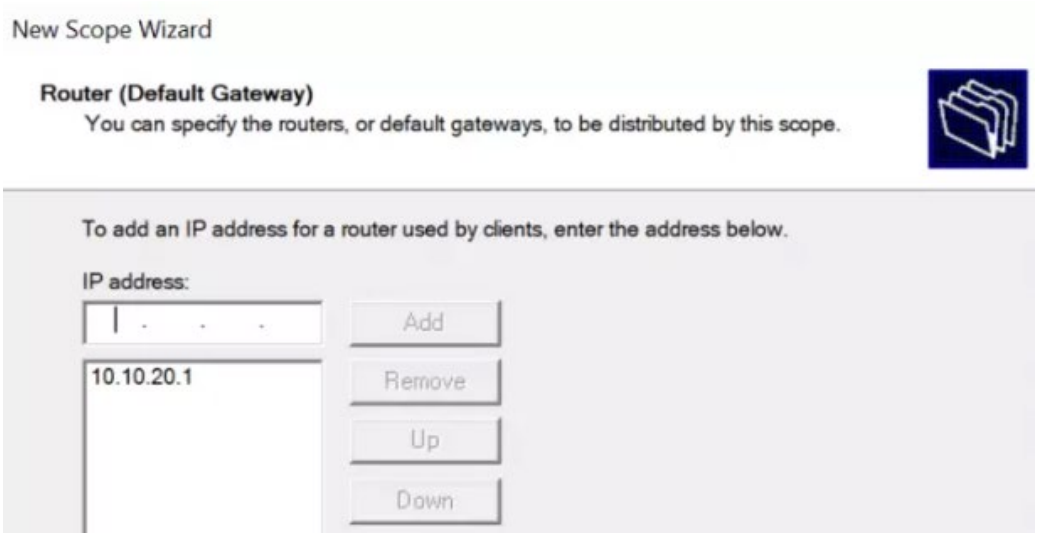
DHCP options allow routine network parameters and some manufacturer specific information to be sent to DHCP devices. In the case of Mitel phones, option 156 is used to "tell" the phone it needs to reboot into a voice VLAN and begin "tagging" its traffic with that VLAN number.



Several DHCP OPTIONS are required by all networks for them to function and are not specific to Mitel. The following items are required in each SCOPE created for DHCP devices to function in the network. You will run the wizard twice, once for the DATA VLAN SCOPE and again for the VOICE VLAN SCOPE.

Item 1: Default Gateway. On this page, key in the Default Gateway that the DHCP clients will be assigned during lease time. Key in and click "Add" beside it. After that, hit "Next". In most cases this IP will be .1 or .254 as most network administrators use those addresses as the gateway. The gateway allows computers in this VLAN to talk to computers in other VLANs or to get out to the Internet. The default gateway must ALWAYS be in the same subnet/range as the DHCP devices. In our example, we excluded IP addresses 1 to 10 in our SCOPE so that .1 can be used as the default gateway. Default Gateways are Layer3 devices capable of routing traffic between VLANs/Networks. They are typically Layer3 Switches, Routers, or in some cases Firewalls. In our example, we configured DHCP to hand out gateways per VLAN as follows:

- **Data VLAN Default Gateway = 10.10.20.1**
- **Voice VLAN Default Gateway = 10.10.200.1**



Item 2: DNS Servers DNS servers translate names (websites) to IP addresses on the network. For the Data VLAN, Mitel recommends entering either your internal company DNS server and parent domain (e.g. companyxyz.com/10.0.20.1), or you can use your ISP provided DNS server or a public DNS such as Google DNS (Googles DNS servers are 8.8.8.8 and 8.8.4.4).

FOR OFFICE VOICE DNS SCOPE: Mitel recommends using the company's DNS as primary for the voice VLAN and Google's DNS as secondary or tertiary backup. In some cases, the DNS server may be provided by your ISP in which case that is the DNS to use as secondary or tertiary DNS for voice VLANs.

Note: Unlike the DHCP server, the DNS server functions at layer3 and can be any IP and is not required to be in the same VLAN/subnet range. A typical VOICE VLAN SCOPE DNS OPTION would list the DNS in the following order: (the UP/DOWN buttons allow you to order them 1 to 3)

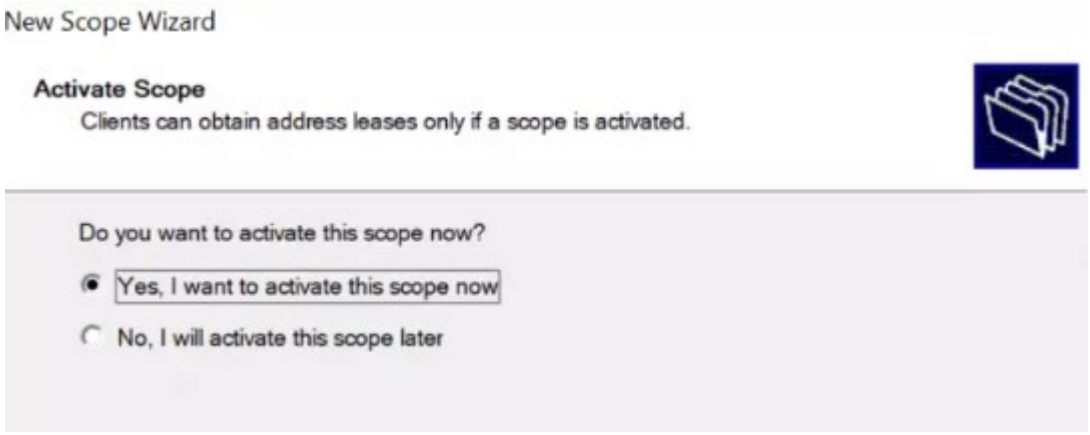
1. [Customer DNS or Customer ISP provided DNS]
2. Customer Backup DNS
3. Public DNS (8.8.8.8)

FOR HOME VOICE USERS: For home users with desk phones, Mitel recommends setting the desk phone to Google's DNS as primary/secondary (8.8.8.8/8.8.4.4) to avoid issues caused by DNS outages on your ISPs network.

NOTE: Mitel customers should never use a DNS provided by Mitel. Mitel internal DNS are used ONLY for customers with private network connections.

Step 4: Finish Scope Wizard and ACTIVATE the SCOPE.

On this Step, just click "Next" to activate the scope we have configured. If you would wish to activate it later, choose the second radio option.



IMPORTANT: You will run this WIZARD twice. Once to create the data VLAN with its unique SCOPE options and again with the voice VLAN with its unique SCOPE options. You will then proceed to add Option 156 to each SCOPE as described below.

Step 5: Add Mitel specific option 156 to the Data and Voice Scopes

This step creates the option to assign Mitel Connect phones to reboot into the VLAN assigned in the scope. This will need to be done in both the DATA and in the VOICE SCOPES.

Go back to the DHCP manager and locate the DATA and VOICE scopes created in Steps 1 to 4 above.

1. Open your DHCP manager.
2. Locate the Data subnet that your phones will initially boot into
3. Navigate to the scope options and add option 156.
4. Set the value of option 156 to the following based on your system setup:

The following is exclusive to Mitel U.S. Internet connected phones sending traffic over public Internet:

DATA SCOPE OPTION 156: **phone sees option 156 and reboots into VLAN 200

Option 156 will be set to type = STRING and the following text string can be pasted into the field.

configServers=update.sky.shoretel.com,cloudDomain=sky.shoretel.com,layer2tagging=1,VLANid=200

VOICE SCOPE OPTION 156: **phone sees its in VLAN 200 and continues boot process

Option 156 will be set to type = STRING and the following text string can be pasted into the field.

configServers=update.sky.shoretel.com,cloudDomain=sky.shoretel.com,layer2tagging=1,VLANid=200

For EU and AU DHCP servers the correct option 156 are:

- **configServers=update.sky.shoretel.eu,cloudDomain=sky.shoretel.eu,layer2tagging=1,VLANid=200**
- **configServers=update.sky.shoretel.com.au,cloudDomain=sky.shoretel.com.au,layer2tagging=1,VLANid=200**

6900 Phones versus IP400 Phones:

- IP400 series phones require the CONFIGSERVER and CLOUDDOMAIN in all configuration scenarios
- IP6900 series phones in North America can forgo CONFIGSERVER and CLOUDDOMAIN parameters and utilize the LAYER2TAGGING parameter only in option 156.
- IP6900 series phones in EU and AU require CONFIGSERVER and CLOUDDOMAIN in all configuration scenarios
- Connect customers with a mixture of IP400 and IP6900 phones should include CONFIGSERVER and CLOUDDOMAIN in all configuration scenarios

IMPORTANT NOTE:

Mitel 6900 Firmware version 5.2.0.307 and 5.2.0.1127 – 5.2.0.1148 the IP 6900 phones had limited support of DHCP Option 156 tags and only supported "CloudDomain" tag in the DHCP Option 156.

With firmware version 5.2.1.156, and newer, the IP 6900 series phones now support following DHCP Option 156 tags in addition to CloudDomain tag:

- configServers
- ftpServers
- VLANid
- layer2tagging

Workaround: Boot the phones on the default VLAN, register it, let it upgrade to latest version to support VLAN tag, then let it reboot, grab the VLAN tag and boot to the voice VLAN using the option 156.

How much Bandwidth do I need for Voice over the Internet?

Internet circuits are "best-effort" transport

Unlike Frame-Relay, Asynchronous Transfer Mode (ATM), and MPLS, a typical Internet connection has no mechanism to set a committed rate for voice or enforce prioritization for real-time traffic to ensure low-latency and minimal packet loss end-to-end. So why is voice over the Internet so popular?

1. Low cost (sometimes with no per minute charges) is the primary reason for choosing Voice over Internet
2. The reliability of the Internet worldwide has improved dramatically in the last 5 years
3. The ability to purchase large amounts of Internet bandwidth in the office and at home
4. Easy setup and speed of installation (order to install time often less than 14 days)
5. Ability to work in the office and remote (anywhere with "good" Internet)

Common pitfalls with Voice over Internet

A high-quality connection to the Internet results in less than 1% of calls (on average) experiencing drops or call quality complaints. However, there are some gotchas that should be considered:

1. **Synchronous vs Asynchronous Internet speeds:** A typical cable modem Internet connection provides more download bandwidth than upload bandwidth. Circuits are sold in varieties such as 10Down/1UP, 50Down/ 10UP, 100Down/20UP etc. The reason for this is in the past most users were pulling data down from the Internet versus pushing large amounts of data UP toward the Internet. As more data and applications migrate to the cloud there has been a dramatic surge in UPLOADED data from both offices and home users. Videoconferencing, Office365, a multitude of SaaS applications, VPN, and other bulk data is beginning to consume a majority of the Internet UPLOAD speed. The result is users complaining they can hear the outside person very clearly, but they sound garbled/choppy/tinny/underwater to the person on the far end. This is typically a result of bulk data delaying voice in the outbound direction.
2. **Competition for Internet Resources:** This often occurs with home users where the Internet quality seems to come and go throughout the day. This is attributed to other applications (home schooling, video streaming, video meetings) utilizing bandwidth at the same time. The same scenario can also occur in an office environment when large data transfers such as medical images, videoconferences, operating system updates, database synchronizations etc. monopolize the pipe. For the office, there are some mitigation strategies discussed in the firewall section later in this document. For home users, the first step is to have your Internet Service Provider (ISP) test your circuit using test equipment from your house and look at your overall utilization graphs. If nothing is found, try purchasing more bandwidth to see if the number of occurrences drop dramatically. Finally, in some cases the home user may need to switch to another Internet provider to get a more reliable or less congested pathway through the Internet.
3. **Microbursting:** Microbursting is a common phenomenon in all IP networks. Microbursts are the rapid bursts of data packets sent in quick succession leading to periods of full (or near full) line-rate transmission that can overflow packet buffers both in network endpoints, switches, routers, and firewalls. These bursts

often last only a few seconds or milliseconds. They typically will not show up on any utilization graph because most devices sample the data rate in terms of minutes (ISPs typically sample every 15 minutes meaning these microburst peaks get smoothed out over that period and will not show up on the utilization charts). A good rule of thumb is if your internet circuit runs for long periods of time in the 60% to 80% range, you are likely experiencing microbursts that can affect voice quality). If possible, ask the ISP or network administrator to modify your outbound Internet device to sample at faster rates such as every 5 minutes or 1 minute intervals to see if peaks rise above 80% utilization for several minutes throughout the day. In the office, there are some mitigation strategies discussed later in this document. For home users, increasing bandwidth or turning off streaming devices during the day might be your only options.

4. **Propagation Delay:** Modern fiber networks send data at the speed of light (186,000 miles per second). This is incredibly fast but in some cases it may not be fast enough. For example, a user on a computer softphone in the Philippines connecting back to a cloud PBX in the United States often cannot achieve the low latency necessary for a sustained high-quality voice or video call. Users will complain of audio problems and frequent disconnects due to the roundtrip time exceeding the 300-millisecond (ms) necessary for consistently clear speech quality. In these cases, the user may need to utilize a PSTN phone, cell phone or an IP phone registered to a cloud PBX in closer geographic proximity (such as Australia in our example case). A simple way to confirm this issue is to run a continuous PING test from the user's computer back to an Internet IP in the United States. If the round-trip-times exceed 300ms consistently, then propagation delay is the likely culprit for audio distortion.

5. **Double Firewalls:** Internet Service Providers (ISP) are increasingly enabling firewalls by default on the modems and routers deployed to customers. While this is good for home users, this can be bad for office environments where a dedicated firewall was purchased and installed by a customer, partner or vendor. This can create a scenario where VOIP traffic is slowed or dropped as it passes through both firewalls. Offices with their own dedicated firewalls should ensure the ISP modem or router is set to "pass through" mode (sometimes called "bridge-mode" or "pseudo-firewall" mode). Two ISP gateway devices where this issue is very common are Cisco Models DPC 3939b and DPC 3941b. Customers with a dedicated firewall should contact their ISP to confirm no additional firewall or inspection is being done by the ISP device.

6. **Wi-Fi:** In some cases, a user's home network device is located in another room from their office computer and/or Mitel telephone. In this case a home user may choose to use softphone on their Wi-Fi connected computer or connect a Mitel desk phone to a Wi-Fi extender (https://www.mitel.com/products/devices-accessories/ip-phones-peripherals/other/mitel-wlan-adapter) or other off-the-shelf wireless extender. The "gold standard" for voice is to be hard-wired via CAT5 cabling to your ISP device but in some cases this is not feasible. The Wi-Fi option will work keeping the following items in mind:

    a. Wi-Fi throughput varies by distance, interior walls, and other obstacles in the middle

    b. Wi-Fi extenders tend to need a reboot occasionally to prevent signal/channel interference

    c. Wi-Fi devices can be interfered with if other Wi-Fi or wireless emitters are in close proximity

    d. Wi-Fi throughput is reduced dramatically by shared streaming devices such as Smart TV's, Smart Phones, Tablets, Notebooks, and any other devices connected to the same wireless network

    IMPORTANT NOTE: Mitel WLAN Adapter/Extender (part#: 51304977) can be used in multi-device mode supporting up to 16 phones connected to an external ethernet switch. Key considerations for multi-device WLAN extender mode are:

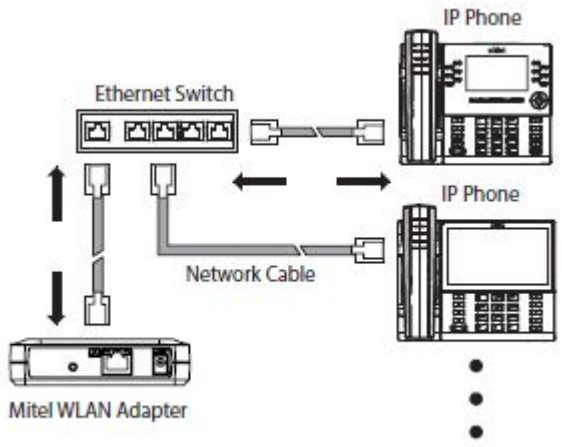
    1. WLAN adapters should be a minimum of 30ft (10 meters) apart to avoid Wi-Fi congestion

    2. Confirming and/or hard coding SPEED/DUPLEX between the Extender and LAN switch is recommended

    3. Mitel recommends plugging phones only into the Ethernet switch to avoid the need for VLANs

    4. WLAN adapters are simple repeaters requiring that the underlying Wi-Fi network, access points, firewall and Internet speeds be suitable for voice traffic. For multiple phones on wireless, the deployment requires VLAN separation for voice and data wireless devices, QoS for the voice VLAN, and the same general network best practice adoption outlined in this document.

    5. A diagram showing the typical setup for a multi-device WLAN adapter is shown below:



7. **The Computer/Laptop:** Occasionally an older model computer may not have the CPU, memory, or multi-threading capabilities to process real time voice or video due to other processes consuming its resources. In addition, anti-virus and other security programs can slow voice processing and cause audio issues or call disconnects. Monitoring the computer resources using Microsoft's PERFMON, TASK MANAGER or similar monitoring program is a good place to check for this issue. In general, if a computer is running a recent operating system (such as Windows 8/10 or MacOS 10.12+) and it runs smoothly without feeling sluggish to the user—it will generally work for voice applications/softphones. For further information please see: https://oneview.mitel.com/s/article/Connect-Client-Softphone-Best-Practices

So How much Internet Bandwidth is required?

There is no easy answer to this question because there are many factors to consider:

1. What other applications run at your location that need Internet bandwidth and how much bandwidth or how "bursty" are these applications?
2. Does your ISP have good peering relationships with Internet "Long-Haul" carriers to ensure your traffic isn't bottlenecking at the peering point or somewhere along the Internet path itself?
3. How oversubscribed is your ISP provider? Internet providers use algorithms to determine when to increase their aggregation circuit speeds to prevent congestion. Sometimes they underestimate usage in an area or at times their primary circuit fails causing them to re-route traffic over a smaller circuit. In these cases, users with smaller Internet circuits will experience congestion quicker and for longer periods as congestion, drops and retransmits occur. When it comes to Internet—your mileage may vary.
4. What Quality of Service mechanisms discussed in the next section can you deploy on your LAN, WAN, and firewall to prevent congestion on your Internet circuit?
5. Are you connecting to your cable modem over Wi-Fi or direct cable? Typically, direct cable connections get the highest priority in and out of the Internet device. Switching from wireless to wired is a good test to see if your Wi-Fi router or computer Wi-Fi port is the bottleneck.

Again, there is no easy answer to the question but in general when it comes to Internet bandwidth—more is better!

1. For office installs, a network assessment that includes baselining current Internet usage along with what applications are using the Internet is a great start. If there are bulky/bursty applications in use, set them to run after hours. Testing the CAT5/6 cabling with a cable tester and running a simulated voice analyzer (such as Mitel's Voice Readiness Test Tool) ***BEFORE*** deploying the phones is strongly recommended.
2. If using many wireless phones (Bluetooth/DECT) in close proximity, conducting a wireless site survey to rule out environmental interference or having a "heat" map generated to ensure full coverage for the desks in remote areas may be needed.

Typical bandwidth usage:

Typical Bandwidth	
MiCloud Connect Client	Bandwidth Use
Phone Only	.2kbps (idle / "on hook")
Connect Client	.2kbps (idle / "on hook")
Operator	.2kbps +1.5 kbps
Extension Monitor	1.5 kbps per monitored ext.
Audio call (G.722 / G.711)	87 kbps
Audio call (G.729)	31 kbps
Audio call (iLBC)	28 kbps
<150ms Latency one way, <1% Packet loss for RTP / Media traffic, Jitter <50ms between packets	

Although there are many factors involved, the following guidelines are provided based on feedback from Mitel Connect Internet customers running standard data applications alongside Mitel phones (note: a voice VLAN is required in the office but is not required for home users):

- Recommended Single Home User Speed: 30-50Mbps Down / 10Mbps (minimum) UP
- Recommended Small Office (<30 Users): 50Mbps Down / 20Mbps UP
- Recommended Medium Office (31 to 100 Users): 50-100Mbps (synchronous) up/down speeds are same
- Recommended Large Office (>100 Users): 100 to 500Mbps (synchronous) or SDWAN or MPLS

NOTE: The recommendations above are guidelines only. The variables discussed in the previous sections will cause some customers to need more bandwidth while others will report excellent results with less bandwidth. The most important aspect of a successful VOIP deployment is to understand the type of applications running on your network and utilize a voice simulation test tool at each location prior to VOIP deployment.

The following sections discuss best practices for LAN, WAN, and firewalls to ensure voice gets the proper Quality of Service at all points in your network leading up to the Internet circuit. Software Defined WAN (SDWAN) is discussed as a method to improve voice quality and provide additional redundancy for voice communication. The last section discusses the use of Virtual Private Networks (VPNs) for home users.

Designing Quality of Service

I Have Enough Bandwidth, Why Do I Need QoS?

When VoIP is introduced to any data network, all switches and routers within the environment must participate in the QoS infrastructure without exception to guarantee voice quality. Simply adding additional bandwidth does not always provide the necessary QoS guarantee given that Internet link speed is generally the last point of congestion on a data network. Speed does not always overcome jitter as random streams of data can commingle with VoIP media packets and increase the interval between media packets beyond acceptable standards since only one default queue is available. Data networks were not originally designed to support voice traffic so special configuration and multiple queues are required for VoIP to achieve "Toll Quality" on a best effort data network.

Data Network Design Universal Quality Standards to Support VoIP

- **Latency** - No part of the VoIP data network infrastructure should have more than 150 msec. one-way (or 300 msec. round-trip) propagation delay between any two VoIP endpoints.
- **Average Jitter** - No more than 50 milliseconds of spacing between VoIP media packets
- **Max Jitter** – Maximum or Peak jitter in a single interval should not exceed 200 milliseconds
    - **Note**: The occasional maximum jitter value between 200 and 800 likely will not affect voice quality however numerous peaks in these ranges on a consistent basis will result in garbled audio.

- **Loss** - No more than 1% of packet loss for VoIP RTP media stream packets No standard has been set to measure signaling loss but while RTP is primarily time-sensitive, signaling is primarily drop-sensitive.

Mitel's Phones Mark Traffic as follows

- Voice Traffic – Expedited Forwarding – EF / DSCP 46
- Signaling Traffic – Class Selector 3 or PHB - CS3 / DSCP 24

DSCP Class	DSCP (bin)	DSCP (hex)	ToS (bin)	ToS (hex)	CoS	DSCP (dec)	ToS (dec)	TOS String Format
default	**0000 00**	**0x00**	**0000 0000**	**0x00**	**0**	**0**	**0**	**Routine**
cs1	1000 00	0x08	0010 0000	0x20	1	8	32	Priority
af11	1010 00	0x0A	0010 1000	0x28	1	10	40	Priority
af12	1100 00	0x0C	0011 0000	0x30	1	12	48	Priority
af13	1110 00	0x0E	0011 1000	0x38	1	14	56	Priority
cs2	0100 00	0x10	0100 0000	0x40	2	16	64	Immediate
af21	0100 10	0x12	0100 1000	0x48	2	18	72	Immediate
af22	1010 00	0x14	0101 0000	0x50	2	20	80	Immediate
af23	1011 00	0x16	0101 1000	0x58	2	22	88	Immediate
cs3	0110 00	0x18	0110 0000	0x60	3	24	96	Flash
af31	**0110 10**	**0x1A**	**0110 1000**	**0x68**	**3**	**26**	**104**	**Flash**
af32	0111 00	0x1C	0111 0000	0x70	3	28	112	Flash
af33	0111 10	0x1E	0111 1000	0x78	3	30	120	Flash
cs4	1000 00	0x20	1000 0000	0x80	4	32	128	FlashOverride
af41	1000 10	0x22	1000 1000	0x88	4	34	136	FlashOverride
af42	1001 00	0x34	1001 0000	0x90	4	36	144	FlashOverride
af43	1001 10	0x26	1001 1000	0x98	4	38	152	FlashOverride
cs5	1010 00	0x28	1010 0000	0xA0	5	40	160	Critical
ef	1011 10	0x2E	1011 1000	0xB8	5	46	184	Critical
cs6	1100 00	0x30	1100 0000	0xC0	6	48	192	Internetworkcontrol
cs7	1110 00	0x38	1110 0000	0xE0	7	56	224	Networkcontrol

Figure 7

Methods to Create and Enforce QoS Policies

- Queuing
- Shaping
- Policing **normally done by carriers but can be enforced in customer router

IMPORTANT TIP: Although not as time-sensitive as voice media packets, voice signaling packets are more drop-sensitive.

The Most Important QoS Design Principles for Mitel

1. In a strictly Internet environment, QoS only comes into play on customer devices leading to or from the device connected to the Internet. Typical scenarios:
    a. Each site has their own dedicated Internet. In this scenario, enabling QoS on the LAN switch and configuring each LAN port connected to a Mitel phone to "TRUST" the phone markings is often the only configuration necessary. Note: We will discuss firewall strategies in a later section.
    b. Each site is connected via MPLS, Private Line, or Tunnel to a central location or datacenter with a large bandwidth connection to the Internet. In this scenario, you must go beyond enabling LAN QoS and enable QoS on every device/connection in the path to and from the Internet device. Failure to do this often results in users at the main site reporting no voice quality issues while users at remote sites report many phone audio issues due to congested voice traffic working its way toward the Internet device.
    c. Quality of Service is not configured by default on private lines or MPLS circuits. You must work with the provider of these internal WAN circuits to ensure the QoS configured on your internal

devices matches the policy configured on WAN provider devices. Failure to verify this will often result in the worst possible voice quality between sites and to the Internet egress device.

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

Configuring Quality of Service (QoS)

Single Site, Single Voice VLAN Deployment

QoS exists at multiple OSI model layers where the queuing occurs at layer 3 and layer 2 depending on whether the traffic is being routed and/or switched. With a single site, single Voice VLAN deployment, enabling QoS on the LAN switch and confirming voice gets egress priority outbound to the Internet is required.

Steps to enable LAN QoS/CoS (Class-of-Service) for Generic LAN Switch

- Enable QoS/CoS Globally on the LAN Switch
- Configure type and number of queues
- Map CoS values to ingress and/or egress port queues and thresholds (layer 2 devices)
- Map DSCP values to ingress and/or egress port queues and thresholds (layer 3 devices)
- Configure DSCP map, which maps layer-2 CoS values to layer-3 DSCP values or vice versa.
    - **IMPORTANT NOTE:** As traffic transitions from Layer2 to Layer3 network devices or from Layer3 back to Layer2 devices, the QoS tags are removed by default. A policy must be configured in many cases to re-mark, re-map or TRUST settings at each threshold.
- Many LAN manufacturers have automated the process above so that a single command (**auto-qos enable**) will generate default values for the items above that meet the needs of most VoIP implementations
- Bind QoS configuration to all VoIP switch interfaces and configure TRUST command
    - **IMPORTANT NOTE:** Configuring QoS or enabling Auto-QoS is only half the equation. You ***must*** configure the LAN switch ports, trunks, and uplinks to TRUST the markings from the phone.
- Confirm on the LAN port of the router, firewall or other device being used as the default gateway for voice traffic that voice packets are being marked at the appropriate classification when they “arrive.”

CAUTION: Failure to enable QoS on the LAN switch can lead to intermittent poor phone audio as switches become saturated with traffic from data devices and servers connected to the same switch.

Each data hardware manufacturer implements QoS on their LAN switches using slightly different command structures and tools; however, the resulting QoS functionality is essentially the same. Enabling QoS on the LAN allows the switch to distinguish packets or packet flows from each other, assign labels to indicate the priority of the packet, make the packets comply with configured resource limits and provide preferential treatment in situations when link or buffer resource contention exists. Any data hardware manufacturers not mentioned can easily find similar configuration syntax by comparing the given examples to their data hardware manufacturer’s respective QoS Implementation Guide to see the common configuration requirements in order to apply them to any switch/router QoS platform in a similar manner.

Example of auto-qos enabled on Cisco LAN switch with TRUST settings for Mitel phones:

```
Interface FastEthernt1/0/23
 description uplink to router
 no cdp enable
 ip address 10.10.20.1 255.255.255.252
 auto qos voip trust

interface GigabitEthernet1/0/12
 description ** Mitel Phone  **
 no cdp enable
```

```
 switchport access VLAN 20
 switchport mode access
 switchport voice VLAN 120
 auto qos voip trust
 spanning-tree portfast
end
```

Multi-Site, Single or Multi Voice VLAN at each Location

Customers with multiple sites will often use their private network/WAN to send data between sites and only send traffic to the Internet out 1 or 2 sites (primary and backup) with Internet connectivity. In this scenario, Quality of Service must be configured between all devices in the path leading to and from the Internet connection. Failure to configure QoS between sites over private links will result in phone users at remote locations complaining of poor quality audio while users at sites co-located with the Internet router state quality is good.

The multi-site, multi-Voice VLAN or even a single-site, multi-Voice VLAN deployment builds directly on the previous 'single-site, single VLAN' section. A multi-site deployment can be a series of single-site, single Voice VLAN deployments connected to each other via a private WAN, VPN over the Internet, a service provider WAN/private links or combination thereof. This is important because layer-2 QoS markings are lost or ignored when the QoS marked packet crosses a layer-3 routing boundary. Voice traffic that crosses the layer-3 boundary now requires QoS configuration at the networking devices that route between VLANs, which could be core or distribution layer-3 switches or routers. Firewalls are intentionally omitted from this list because they are not designed to be LAN routing or switching devices in a true enterprise environment. Firewalls are best used to protect and route traffic to and from the Internet or untrusted network sources.

There are multiple WAN connectivity products; however, two common types represent the two basic categories of WAN connectivity important to Voice, MPLS (i.e., QoS capable) and the VPN Tunnel over the Internet (i.e., not QoS capable). MPLS is a private WAN connection offered by many service providers which is designed for real-time traffic such as voice. MPLS with QoS enabled provides QoS at every hop across the service providers network for your circuit. MPLS can prioritize voice traffic and honor QoS markings across the service provider's network. However, VPN tunnels over an Internet connection cannot prioritize voice traffic and will not honor QoS markings across the ISP's Internet network, this can cause voice degradation during periods of high utilization. In some cases where MPLS or other similar private connectivity is not available or feasible at a site, VPN tunnels can be used but voice quality cannot be guaranteed.

When selecting an MPLS WAN Service Provider, be sure to specify or order the appropriate QoS Class of Service with the MPLS circuit because in many cases, it is not enabled automatically. MPLS without QoS enabled is no different than an Internet connection regarding prioritization of traffic classes. Most MPLS Service Providers provide standard QoS queues, which map the appropriate classified traffic into separate queues similar to a LAN QoS design. The recommended queues should match the following criteria, which should also match the LAN QoS traffic design in similar fashion.

- Queue1 – Expedited Forwarding (EF) strict priority traffic for RTP media ONLY
- Queue2 – Class Selector 3 (CS3) medium priority traffic for prioritized signaling ONLY
- Q3 or Q4 – Default, Best Effort traffic for all other data traffic and/or non-prioritized signaling ONLY

NOTE: Failure to confirm that QoS settings on your Layer3 routers match exactly with the queues, markings, and percentages on you provider's equipment will result in poor quality audio.

Example - QoS Cisco iOS Interface MQC-based Commands (Layer3 Router)

Most Manufacturers configure Layer3 QoS in 3 steps. Below is an example for Cisco routers where voice packets are placed in a priority queue utilizing 25% of circuit bandwidth. Please consult your manufacturers documentation or open a configuration assistance case as needed to determine the correct configuration for your equipment.

Example Steps to Configure QoS across a private WAN link toward Internet Router:

Step 1: Define which ports you want to prioritize into or out of an interface

```
ip access-list extended acl-qos-mitel-voicertp
remark Mitel-Voice-Media-Range
permit udp any any range 10000 65535

ip access-list extended acl-qos-mitel-callcontrol
 remark Mitel-Connect-Signalling
 permit tcp any any eq 5060
 permit tcp any any eq 5061
 permit tcp any any eq 80
 permit tcp any any eq 443
 permit tcp any any eq 8001
 permit tcp any any range 31450-31471  **Connect Contact Center Only
 permit udp any any eq 5060
 permit udp any any eq 443


class-map match-any class-mitel-voicertp-input
 match accesss-group name acl-qos-mitel-voicertp
 match dscp ef

class-map match-any class-mitel-callcontrol-input
 match access-group name acl-qos-mitel-callcontrol
 match dscp cs3

class-map match-any class-mitel-voicertp-output
 match accesss-group name acl-qos-mitel-voicertp
 match dscp ef

class-map match-any class-mitel-callcontrol-output
 match access-group name acl-qos-mitel-callcontrol
 match dscp cs3
```

Step 2: Create policies that dictate how to mark traffic or how much bandwidth to reserve for packets that match the criteria defined in step 1 above. The policy below reserves 25% bandwidth for voice.

```
policy-map Mitel-Output-Policy
 class class-mitel-voicertp-output
  set dscp ef
  priority
 class class-mitel-callcontrol-output
  set dscp cs3
  bandwidth remaining percent 15
 class class-default
  set dscp 0
  bandwidth remaining percent 60


policy-map Mitel-Input-Policy
 class class-mitel-voicertp-input
 set dscp ef
 class class-mitel-callcontrol-input
 set dscp cs3
 class class-default
 set dscp 0
```

Step 3: Apply the policies in Step 2 to the interfaces on your layer3 device

```
interface GigabitEthenet1/1
 description WAN Connect to HQ Primary Internet Site
 service-policy output Mitel-Output-Policy
 service-policy input Mitel-Input Policy
```

Confirm QoS Policy and Routinely Monitor for Output Drops

It is important to monitor the output queues to confirm traffic is matching the service policies and ensure that there are not any drops in the priority queue or medium priority queue(s) for signaling or video traffic, or more importantly, that the drops are not incrementing.

Queue drops are an indication that you need to increase the amount of bandwidth in the layer-3 priority queue configuration or that you may have too much non-RTP voice traffic being placed in the priority queue. Make the necessary adjustments as needed and continue to monitor.

```
WAN INTERFACE CONFIGURATION
# show policy-map interface ser0/0
...
 Serial0/0/0

  Service-policy output: voip

    Class-map: VoIP_AUDIO (match-any)
      29598783 packets, 5906874082 bytes
      5 minute offered rate 17000 bps, drop rate 0 bps
      Match: ip dscp ef (46)
        26411300 packets, 5531823810 bytes
        5 minute rate 17000 bps
      Queueing
        Strict Priority
        Output Queue: Conversation 264
        Bandwidth 20 (%)
        Bandwidth 750 (kbps) Burst 5000 (Bytes)
        (pkts matched/bytes matched) 2434250/1375653329
        (total drops/bytes drops) 770350/746146747          ** 32% drop rate BAD!!

    Class-map: CALL_CONTROL (match-any)
      148419 packets, 9504366 bytes
      5 minute offered rate 0 bps, drop rate 0 bps
      Match: ip dscp af31
        148419 packets, 9504366 bytes
        5 minute rate 0 bps
      Queueing
        Class-Based Weighted Fair Queue
        Output Queue: Conversation 264
        Bandwidth 20 (%)
        Bandwidth 500 (kbps) Burst 12500 (Bytes)
        (pkts matched/bytes matched) 11071/708974
        (total drops/bytes drops) 0/0                       ** 0 Drops is good!

      Class-map: class-default (match-any)
        84557179 packets, 14841300472 bytes
        5 minute offered rate 52000 bps, drop rate 0 bps
        Match: any
```

Figure 11

NOTE: A deep dive into enterprise class QoS is beyond the scope of this document. An older but well written document outlining traditional QoS design concepts can be found here:

https://www.cisco.com/c/en/us/td/docs/solutions/Enterprise/WAN_and_MAN/QoS_SRND/QoS-SRND-Book/QoSIntro.html

****CONSULT YOUR MANUFACTURERS LATEST DESIGN AND CONFIGURATION GUIDELINES**

Software Defined WAN (SD-WAN)

Competition for Internet bandwidth and congestion avoidance is a common theme when voice and video are deployed via "best-effort" Internet circuits. Voice traffic typically utilizes very little bandwidth, but it requires low latency, low packet loss, high reliability, and consistent timing between packets to ensure high quality voice. This can be difficult to achieve consistently with only a single Internet connection and especially if there is no prioritization of voice traffic over bulk application traffic which can cause delay/loss in voice transmission. SDWAN technology provides increased application performance across the WAN and Internet paths while at the same time providing redundancy between multiple paths and a more consistent voice experience over the Internet.

SDWAN provides increased performance for voice and can mitigate common Internet issues such as:

- Phone outages due to single circuit at each location
- Poor quality voice due to lack of voice prioritization between voice and bulk data
- Poor quality voice due to lack of traffic shaping or bandwidth reservation
- Ability to distribute applications across multiple circuits (1 ISP for voice and 1 ISP for data)
- Failover with voice prioritization between Internet circuits
- Better visibility and monitoring of throughput, loss, latency, and jitter

For more information about Mitel's approved SD-WAN partner for MiCloud Connect, please visit:

- https://www.cpitelecom.net/mitelsdwan

IMPORTANT NOTE: Load balancing of voice media traffic (RTP traffic) is not recommended. This is not to say it cannot be done but it requires in-depth knowledge of circuit parameters, stream reconstruction, and other concepts that are outside of the scope of this document. Keeping the design simple by sending voice, video, and other low latency applications out of your primary circuit while sending bulk data out of a secondary circuit (which can also be used in the event of primary circuit failure) is the recommended configuration for ease of setup and high quality voice.

Firewall Best Practices

A firewall is an information technology (IT) security device which is configured to permit, deny, or proxy data connections set and configured by the organization's security policy. Firewalls can either be hardware and/or software based. Mitel does not make recommendations on what firewalls to use other than what capabilities are required. Next generation firewalls often have some traffic prioritization and traffic shaping capabilities that can enhance the voice over Internet experience (some common firewall best practice links are provided at the end of this section).

Firewall Requirements

Firewall requirements for Mitel MiCloud Connect configuration include the following features:

- Stateful Inspection
- NAT
- Ability to modify firewall rules (permit or deny specific TCP/UDP ports, services, IPs, URLs)

Network Address Translation

A public IP address is generally not assigned directly to a user's computer. Computers are generally located on a private network behind a router or firewall providing network address translation (NAT) or a dedicated NAT device. In these cases, the firewall configuration needs to be considered for Mitel MiCloud Connect services and features. The following ports for the Mitel MiCloud Connect platform need to be opened with a policy on the firewall when configuring the NAT for the appropriate traffic to pass through.

Mitel MiCloud Connect Port Usage

For Mitel MiCloud Connect IP phones to work over a broadband Internet connection, firewalls must be configured to allow traffic to the following ports:

- TCP/UDP 5060 (SIP)
- TCP/UDP 5061 (SIPS)
- TCP 80 (HTTP) **legacy 3rd party devices only
- TCP/UDP 443 (HTTPS)
- TCP 8001 (Admin-Portal)
- TCP 31450-31666 (Enterprise Contact Center ECC only)
- UDP 10000-65535 (RTP Media Stream)

Firewall Policies/Features

In general, VoIP (RTP) traffic is very sensitive to any type of network delay, loss, or modification that might occur as it traverses a network. The local firewall could have policies or features that negatively impact RTP traffic and therefore need to be disabled. The following common features could negatively impact RTP traffic and should be disabled, modified, or selectively disabled for the voice networks only:

- SIP-ALG/SIP-NAT/SIP Transformation
- SIP Inspection/Deep Packet Threat Inspection for SIP
- UDP Flood Control (recommend disabling or setting this parameter to a very high value to prevent encrypted UDP voice drops – firewalls can mistake voice/UDP traffic as a flood and drop it)
- TCP Session timeout should be 6 minutes or greater (if configurable)

Traffic Prioritization by URL/Domain

Modern firewalls often allow prioritization to URLs and their associated IP ranges. To prioritize traffic outbound on the firewall interface connected to the ISP or ISP router, the following URLs can be used:

- ***.sky.shoretel.com**
- ***.mitel.com**
- ***.mitelcloud.com**
- ***.mitel.io** (for use with Mitel MiTeams Video Conferencing)

Note: For AU/EU customers see below:

- ***.sky.shoretel.com.au**
- ***.mitelcloud.com.au**
- ***.sky.shoretel.eu**
- ***.mitelcloud.eu**
- ***.mitelcloud.co.uk**

IP Permit Lists Are Not Supported

Mitel does not support or recommend prioritization by IP because IP ranges are subject to change. For the purposes of troubleshooting or investigation of voice quality issues, the following IP ranges are provided.

North America:

- 66.11.214.0/24
- 66.11.195.0/24
- 208.103.83.0/24
- 199.101.105.0/24 **Recently added for increased redundancy and failover
- 134.199.16.0/21 **Recently added for increased redundancy and failover

Australia:

- 103.15.177.0/24

Europe:

- 185.161.24.0/22

Note: In some cases, adding an explicit PERMIT OUTBOUND statement for the above IP and URLs in the firewall configuration will prevent false positive events in the firewall that might inadvertently drop returning voice traffic.

Explicit inbound permit policies are *not* required on a stateful firewall that allows outbound traffic to return by default. Note: Adding explicit inbound IP permit rules can be useful as a test to rule out firewall related issues but are not recommended for long term use. Consult with your network security for further understanding.

Stateful Firewall/NAT Configuration - Connection-Timeout-Adjusting Method

Single users can use this method, but it must be used on LANs where multiple SIP devices are traversing the same NAT.

- Stateful firewalls recognize inbound traffic that is part of an established connection and send it to the correct IP and ports on the client. With such a configuration, the NAT/firewall device handles port mapping provided the connection does not time out.
- Mitel requires that SIP softphones re-register (i.e., let the server know they are still available and connected) at least every 360 seconds (6 minutes), so configuring the firewall/NAT device with TCP timeouts greater than 6 minutes will maintain the connection.

Additional Resources

Each firewall manufacturer publishes their own unique configuration guidelines for real time voice and video over the Internet. The following resources are listed for convenience. Mitel recommends that a search for newer articles or a configuration assistance case be opened with your firewall manufacturer to ensure optimal configuration.

Palo Alto Firewall:

- https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000ClouCAC
- https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000ClS0CAK
- https://docs.paloaltonetworks.com/pan-os/9-1/pan-os-admin/quality-of-service/qos-use-cases/use-case-qos-for-voice-and-video-applications
- https://docs.paloaltonetworks.com/pan-os/8-1/pan-os-new-features/globalprotect-features/split-tunnel-for-public-applications.html

Cisco Meraki Firewall:

- https://documentation.meraki.com/General_Administration/Tools_and_Troubleshooting/VoIP_on_Cisco_Meraki%3A_F.A.Q._and_Troubleshooting_Tips
- https://www.cisco.com/c/dam/en/us/solutions/meraki-branch.pdf

SonicWall Firewall:

- https://www.sonicwall.com/support/knowledge-base/udp-and-icmp-flood-protection/170503279224098/
- https://www.sonicwall.com/support/knowledge-base/how-to-troubleshoot-common-voip-issues/170503552140480/
- http://help.sonicwall.com/help/sw/eng/7020/26/2/3/content/VoIP_voIPOptions.htm
- https://www.sonicwall.com/support/knowledge-base/how-can-i-make-wan-groupvpn-route-all-traffic-policy-for-one-user-s-gvc-policy/170503392435592/

FortiNet/FortiGate:

- https://kb.fortinet.com/kb/documentLink.do?externalID=FD36405
- https://docs.fortinet.com/document/fortigate/6.2.0/cookbook/858887/voip-solutions
- https://docs.fortinet.com/document/fortigate/5.6.0/cookbook/190566/traffic-shaping-for-voip

Sophos Firewall:

- https://docs.sophos.com/nsg/sophos-firewall/18.0/Help/en-us/webhelp/onlinehelp/nsg/sfos/troubleshooting/VoIPDoSSpoofProtection.html
- https://docs.sophos.com/nsg/sophos-firewall/18.0/Help/en-us/webhelp/onlinehelp/nsg/sfos/concepts/VoIPResolveCallIssues.html

Cisco FirePower:

- https://www.cisco.com/c/en/us/td/docs/security/firepower/620/configuration/guide/fpmc-config-guide-v62/quality_of_service_qos.pdf

VPN (Virtual Private Networks) with Voice over Internet

All Mitel MiCloud Connect telephony communication is encrypted by default which means a VPN is not required for security purposes. However, many users working from home are required to connect to a VPN for security when connected to internal servers, databases, and devices residing in the office or in a datacenter. Here are some items to consider when running Voice over VPN:

- **Forced Tunnel vs Split Tunnel VPN:** Mitel recommends using Split Tunnel VPN configurations for home telephony users (if allowed by your security manager). Split tunneling allows some traffic destined for the Internet to go straight out the user's home connection while forcing all other data to use the secure tunnel. As we've discussed, voice, video, and other real time traffic require the shortest path, lowest latency, and minimal interference as they go back and forth across the Internet. Forced Tunnel VPN (VPNs that require 100% of all traffic to traverse the tunnel) can cause voice issues by:
    - Adding propagation delay to the voice path. For example, a VPN user in San Antonio might send their voice to a VPN concentrator in San Francisco where it goes out the Internet back to Mitel servers hosted in Dallas. This adds 1000s of miles to what would normally be a 90 mile trip across the Internet.
    - Consuming additional bandwidth in the form of "overhead" when creating the secure tunnel
    - Causing more frequent call drops due to tunnel resets and key renegotiation
    - Adding additional security rules (similar to firewalls) that may cause adverse behavior with real time voice and video

To avoid common issues with home user VPN, voice users at home should be placed in a separate VPN group that allows them to send voice traffic directly to and from the user's home ISP. In most cases, this is accomplished by placing voice users in a unique group that allows split tunneling for Internet traffic or at a minimum allows split tunneling to Mitel domains:

- *.sky.shoretel.com
- *.mitel.com
- *.mitel.io **Mitel MiTeams Video Conferencing only

Another method to avoid VPN issues is to use a physical desk phone at home that is plugged directly into the home users cable modem (this will require a Mitel power adapter for the phone in most cases). This allows the desk phone to utilize the Internet directly without the need for computer VPN and has the added benefit of avoiding contention with other applications, anti-virus and firewalls running on the home computer.

What about home Contact Center Users with VPN?

This scenario presents a few additional items worth considering. If a contact center agent has a desk phone connected directly to the Internet but is utilizing the Mitel Agent Interaction Center (AIC) over VPN there is a possibility of network timing issues as VPN traffic may take the "long way" while the phone is taking the direct Internet route. In addition, there is an increased chance the AIC browser or the phone has a very brief drop that causes the two devices to momentary lose sync which may cause additional "forced release" notifications. The deployment scenarios in order of preference are:

1. **Best:** AIC installed on agent home machine with desk phone and VPN Split Tunnel
2. **Very Good:** AIC installed on agent home machine with softphone and VPN Split Tunnel
3. **Good:** AIC installed on agent home machine with softphone and VPN Forced Tunnel
4. **Fair:** AIC installed on computer in remote office using RDP and Mitel Desk phone at home
5. **Acceptable:** AIC installed on computer in remote office using RDP and Mitel softphone on home computer with Forced Tunnel VPN
6. **Tolerable:** AIC installed on computer in remote office using RDP and Mitel softphone on home computer with Split Tunnel VPN

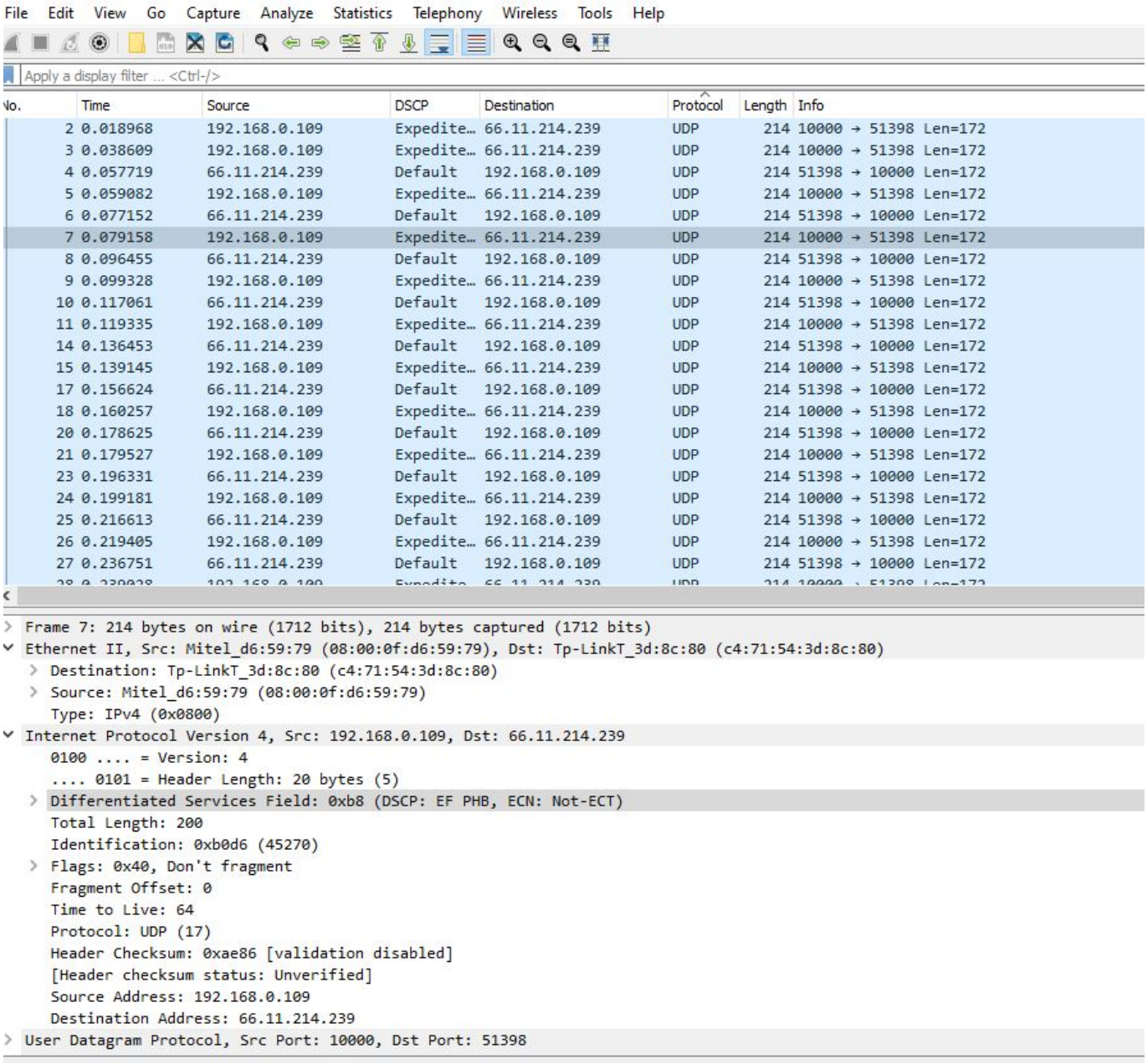
Packet Captures

How Do I Verify that Packets Are Marked with the Correct DSCP Value?

After you have incorporated all the best practices in this document, one of the final steps is to verify that the packets are marked correctly in order to be honored by the QoS configuration on the data network. At a minimum you must confirm voice packets are given priority as they traverse lower bandwidth links in your network. These are typically smaller site to site WAN links and the uplink to the Internet.

The two figures below show where to look in a packet to see the DSCP value that is marked for QoS. Because Mitel Connect traffic utilizes encryption, the real time voice traffic will show up as UDP packets in a Wireshark. The traffic is easy to spot because it will have a constant back and forth flow with the following characteristics:

- Mitel phones utilize source port 10000 and count up
- Length will be approximately 170 to 220 bytes (voice packets are small)
- Destination port will be in the high range (30000 to 65000)



Power Over Ethernet

Typically, most VoIP deployments use Power over Ethernet to power an IP Phone from the Ethernet connection rather than using a power supply plugged into the wall outlet. This makes for a simplified physical deployment of the IP Phone. If the POE LAN switch is underpowered or does not have dual power supplies and its primary power supply is beginning to fail users will report random occurrences of “phones all go dark and reboot”.

A few things to consider is the power consumption of a group of IP phones versus the amount of power a data switch can support at one time. When the power consumption is exceeded, the data switch turns off the PoE to protect the switch and all the phones on the switch power down. When designing a data network with edge/closet data switches, look for the total wattage of power that the data switch can support such as 370W for example. Also consider the power consumption of the IP phones that will be connected to the selected data switch. All IP phones identify idle, active, and max power consumption specifications. For example, an IP 485G phone lists the power specs as Power Class 2 PoE, 3.0W idle, 4.4W active, and 4.9W max. If a data switch cannot determine the PoE

Power Class of the connected device, it will instead send the max power to the phone, which is 15.4W either during the phone boot process and/or the idle or active states. Using LLDP, the data switch can automatically detect the Power Class and send the appropriate power levels to the phone so as not to max out at 15.4W and consume all the data switch's available PoE power supply for IP Phones. Use any data switch Show commands to display actual power consumption levels of IP Phones during or post deployment to ensure the data switch is adequately powering all the phones.

Note: Mitel recommends the use of dual power supplies whenever possible for all POE LAN switches supporting more than 12 POE connected phones. Dual power supplies are highly recommended to avoid losing all phones for an extended period of time due to a single power supply failure.

Ethernet over Power (EoP)

Ethernet over power works by using a building's copper electrical wiring as a giant shared broadcast hub for sending and receiving high frequency signals needed for the Ethernet protocol. These signals are layered on top of the electrical current so as not to interfere with power operations. The advantage is that you don't need any additional wiring. The disadvantage is that it is a shared medium. All devices have to fight to send data over the shared medium. Ethernet over power is the least preferred method to send voice throughout your home but will often work with the following caveats:

- Limit the number devices using the home wiring. Mitel recommends using it only for the desk phone itself.
- Never a plug a home laptop or computer into the back of a desk phone at home. This configuration is strictly reserved for office LAN designs.
- Never utilize Ethernet over Power in an apartment building where shared wiring and signals can not only compromise audio quality but also compromise your data security.
- Never utilize Ethernet over Power in homes build before 1990s—the wiring may not be of high enough quality to support EoP frequencies.

Port Scanning and Network Monitoring

Mitel recommends customers avoid any port scanning of the Voice VLAN for Mitel hardware phones during business hours. (This recommendation includes port scans with network/inventory or security vulnerability software such as Spiceworks, SolarWinds, Qualys etc.)

Port scanning can cause dropped calls or "frozen phones" due to the small amount of memory and processor available to the average phone. During business hours a phone could become overloaded trying to respond to the scanner while maintaining a live phone call. Often, only a complete phone reboot can resolve these issues when they arise so it's important to advise users/sites to reboot any "stuck phones" after an intensive scan of the voice VLAN is conducted. Scanning after hours reduces the risk of phone related issues.

Migrating from MiCloud Business to MiCloud Connect

When transitioning from MiCloud Business to MiCloud Connect there are some important aspects of the network that require attention and configuration changes. These items include:

1. Connectivity Differences to MiCloud Connect
2. Firewall Policies
3. DHCP Options

Connectivity to MiCloud Connect

While it is possible to reuse your existing Mitel provided circuit(s) for MiCloud Business be aware this circuit will not be a private connection to the MiCloud Connect data centers and therefore will have no SLA/QoS guarantees. The data centers for MiCloud Connect and MiCloud Business are separate entities and share no private network connectivity. It is recommended to route all MiCloud Connect traffic directly out public Internet whenever possible. Continuing to back-haul voice traffic to the MiCloud Business data centers (Seattle and Miami) only to be placed on the Internet from those locations will introduce additional latency that could impact voice quality. MiCloud Connect data centers are currently located in Carrollton, TX and Chicago, IL via public Internet connections. Sending VoIP traffic out of the local site/home Internet connection is a more direct and optimal path.

Firewall/QoS Policies

It is important to create new, or update, firewall policies for MiCloud Connect. MiCloud Connect uses an entirely different set of domains/subnets and port ranges from MiCloud Business. To ensure all proper configurations are in place, please reference the **Configuring Quality of Service (QoS)** and **Firewall Best Practice** sections of this document. It is extremely important to review these sections in their entirety.

DHCP Options

Confirming/updating DHCP options to match the MiCloud Connect requirements is of the upmost importance when activating service. This is especially important when transitioning from an existing Mitel (or ShoreTel) system because the DHCP server will most likely have options enabled that would impact the new phones. The most important DHCP option is option 156 (ascii). This option is used to set many different parameters of the MiCloud Connect phones (400 and 6900 series). These parameters are below:

- CloudDomain
- ConfigServers
- ftpServers
- VLANid
- layer2tagging

The above parameters are important to consider as it could render the phone inoperable if any parameter is misconfigured. The most common parameter that impacts the phones is *ftpServers* which is not needed by a Mitel Connect phone. Please refer to the section **Creating Data and Voice DHCP Scopes on Microsoft Server (Example)** in this document for more detail and examples of how to create DHCP scopes for MiCloud Connect.

Conclusion

There are many different specialized QoS, Firewall, Router, LAN and SDWAN configuration options that were not discussed in this document; however, the most common were highlighted to help any IT administrator or data network administrator with limited VoIP experience to easily understand how best to deploy Mitel VoIP with the highest degree of success. The last page of this document provides a VOIP checklist that summarizes the most important items discussed in a brief format that can be used prior to IP telephony deployment.

Voice over Internet Deployment Checklist

- Ensure all site cabling is CAT5 or better. Testing each Ethernet jack is also good practice using a common cable tester (see Amazon Fluke or Klein)
- Confirm Full Duplex on all aggregate connection points. (e.g. switch to switch, switch to router, router to firewall etc.)
- Confirm voice and data traffic is separated. This can be done with separate LAN switches or the more common method of installing a voice VLAN
- Mitel recommends automatic VLAN assignment using LLDP or DHCP. Manual VLAN assignment should only be used for testing/workaround
- Baseline the site's Internet usage and learn what applications are in use. Do any data applications "hog" the outbound or inbound bandwidth for several minutes at a time?
- The Internet is a best-effort/shared medium. When in doubt, buy more BW
- For larger sites, purchase the same amount of outbound and inbound bandwidth. Asynchronous Internet speeds will work for smaller sites if there are no bandwidth "hogs" or by using QoS/Traffic shaping
- If telephony users are geographically dispersed, confirm round trip ping times are not consistently exceeding 300ms to that location
- Wi-Fi adds additional points of network contention along with the possibility of wireless interference if phones are closer than 6ft apart
- Quality of Service is required for consistent end-to-end voice quality
- The most important place to prioritize voice traffic is on the LAN switch and at the aggregation points leading to and from your ISP
- Software Defined WANS provide better voice quality and increased redundancy over the Internet
- Ensure the Firewall is configured for VOIP per manufacturers specifications
- Home users with VPN utilizing Connect client, softphone, or AIC should utilize split-tunnel configuration for optimal results
- Port scanning of the Voice VLAN should be done after business hours