Application Note

AN3269

February 4, 2016

Network Best Practices for ShoreTel Sky

NOTE: The purpose of maintaining this older document is to provide information about data network best practices to ShoreTel Sky customers. The current document no longer provides the same level of detail about ShoreTel Sky. The information in this article about the Mitel Connect CLOUD Phone System is outdated. If you are looking for information for Mitel Connect CLOUD, please see the Network Best Practices for Mitel Connect CLOUD article.

Description: The purpose of this document is to summarize the requirements for the Mitel hosted local customer network environment.

Environment: ShoreTel Sky Phone System

Abstract

This application note discusses the use of data networking best practices in conjunction with ShoreTel Sky Call Conductor – ST Connect CLOUD 1.X. Network Administrators must consider a multitude of complex configuration tools and networking parameters when designing a small or large-scale local area network (LAN) and also remotely connected sites over a wide area network (WAN). With regard to VoIP, essential tools include the use of Virtual LANs (VLANs) and Quality of Service (QoS) configurations to virtually guarantee voice quality over a "best effort" data network, originally developed without voice in mind until several years later. Please refer to your network equipment

manufacturer's documentation in order to apply the ideas and concepts presented in this document to your specific equipment and environment.

Table of Contents

Selecting Data Networking Equipment for a Mitel Connect Deployment....3
Customer Site Cable Plant Requirements....3
Designing VLANs for VoIP....5
Configuring VLANs for ShoreTel IP Phones....8
Configuring Automatic IP Phone VLAN Assignment – LLDP-MED....11
Designing Quality of Service....12
Configuring Quality of Service – Single Site....14
Configuring Quality of Service – Multiple Sites....19
Using Cisco Auto-QoS....20
Packet Captures....24
What About Disaster Recovery?....24
Off-Net Firewall Best Practices....25
3rd Party MPLS DHCP Scope and QoS Best Practice....28
Power Over Ethernet....31
Configuring Cisco SB Switch Settings – Auto Smartport & EEE....31
Conclusion....32
References....33

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 Innovation Network 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 a Mitel Connect 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. In the event that 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 (edge data 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 & 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. Mitel approved and managed 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 technically used in some cases, they are NEVER recommended and void the Mitel managed SLA, because they don't provide any error statistics, which are extremely valuable when troubleshooting QOS related problems.

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, at minimum, and can cause packets to be discarded when excessive collisions occur.

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 carrying RTP-voice traffic to operate in full-duplex mode. This is a mandatory requirement for RTP traffic aggregation points, such as (switch-to) router, firewall, gateway, streaming server, and other-switch interfaces that carry numerous RTP flows simultaneously.

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 actually 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 particular 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. Therefore, if either device is forced to operate in full-duplex, the other device must also be forced to operate in full-duplex as well.

Half Duplex Configuration

Some low-end IP-phone and small-port IAD devices (1 or 2 analog ports) may not support full-duplex operation and can only operate in half-duplex mode. These are the only devices that should be allowed to operate half-duplex.

Summary of Valid Duplex Configurations

The following table summarizes all of the different 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	Can be used to connect a single IP phone or low-port IAD device to a switch. Should never be used at RTP aggregation points.

Figure 1

Mitel®
Powering connections

Designing VLANs for VoIP

What is a VLAN?

Virtual LANs (i.e. VLANs) are a data networking design construct by which more than one logical layer-2 (i.e. 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.

Ethernet uses Carrier Sense Multiple Access with Collision Detection protocol (i.e. CSMA/CD) to determine when a single Ethernet device on a layer-2 subnet/VLAN can access the media similar to how a polite conversation works where one speaks and everyone else listening does not speak. In a non-switched network, when multiple devices on the subnet need to "speak", they have to wait their turn until the one speaking or transmitting packets on the subnet is finished. In a switched network, this is less of a problem except for broadcast traffic. Transmitting voice traffic is time sensitive and the media access delay could become too great or too random at times, causing issues with voice. Smaller VLANs also control the quantity of MAC addresses that ARP tables, which is a more limited resource for IP phones, have to store to communicate properly. For example at a given site, create a data VLAN for PCs, a separate voice VLAN for all VoIP devices which should include Voice switches, servers and all IP phones, create a Wi-Fi VLAN for wireless devices, a Printer VLAN for printers, a Server VLAN for all other servers and 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 to design VLANs into your 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 has to 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 hub in a "hub and spoke" LAN topology where the layer-2 VLANs are the spokes on the same core switch or are connected to other layer-2 spoke switches via uplinks back to the layer-3 core switch. In the latter mentioned hub and spoke network topology design with multiple layer-2 switches, the VLANs on each layer-2 switch (i.e. the data VLAN and voice VLAN) are "trunked" or "tagged" back to the core layer-3 switch via its uplink.

> **IMPORTANT TIP**: Avoid "daisy chaining" switches or sites together across the network to keep from creating potential congestion bottle necks. In other words, L2 switches should connect using a hierarchal layer, "many-to-one", directly to the core L3 switch, not "one-to-one-to-one". An additional distribution hierarchal layer can be added when the number of layer 2 switches reach beyond qty. 10 of L2 switches at a site or when all ports have been exhausted on the core L3 switch by access level L2 switch uplink connections.

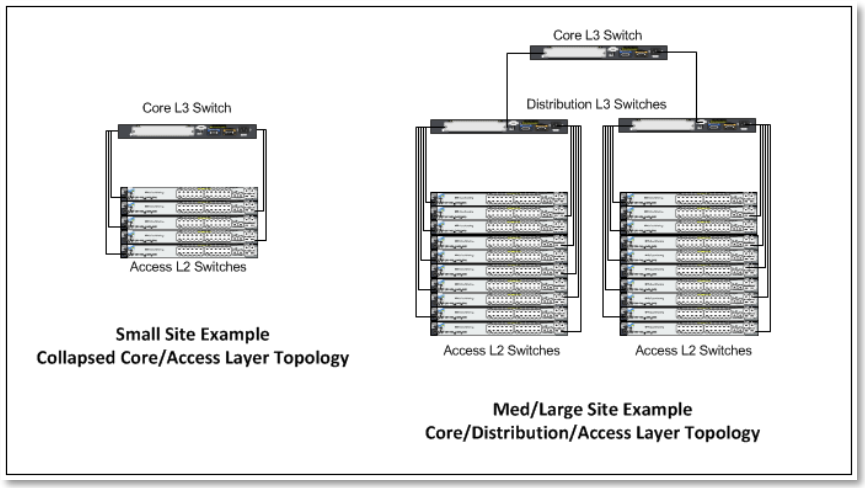

Figure 2

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 of 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 it's 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 imperative 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. Avoid configuring any default gateway for a site on any firewall, server, or any other data switching/routing device/appliance other than the designated "core" layer-3 data switch at each site. Refrain from using the core layer-3 switch's *ip default-gateway* global Cisco command as any subnet's default gateway. The *ip default-gateway* global Cisco command is intended to give administrators an IP address for Telnet administration when not using a loopback IP address.

How is the VLAN Default Gateway created?

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.

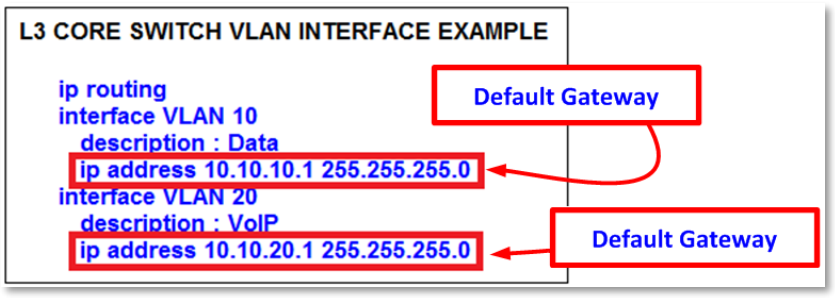

Figure 3

Firewall's are for security, NOT for LAN routing or switching

When connecting a firewall to the "core" L3 switch for Internet access, a default (static) IP route (e.g. *ip route 0.0.0.0 0.0.0.0 192.168.100.1*) in the core switch directed at the firewall's next hop interface will only route Internet traffic to the firewall and keep LAN traffic on the L3 data switch along with the directly connected VLAN routes or any other static or dynamic local IP routes.

> **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.

If the site 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.

> **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.

If the firewall doesn't support the creation of a point-to-point VLAN with the L3 switch, follow the firewall manufacturer configuration documentation for connecting to a LAN but DO NOT make the configured inside IP address of the firewall a default gateway for any connected VLAN between the firewall and L3 switch.

When connecting multiple remote sites to a headquarter site, the same "hub and spoke" model applies with the HQ site being the hub and each remote site being a spoke. Regardless of the type of WAN connectivity product chosen, which will be discussed in more detail in the following sections, a /30 point-to-point VLAN across each customer WAN connection is the ideal configuration to keep layer-2 traffic limited to each local LAN and for better IP address management.

> **IMPORTANT TIP**: Avoid trunking or tagging any local VLANs (i.e. Data and Voice VLANs) at a given site across any WAN connection to a remote site. This will eliminate any unnecessary L2 broadcast traffic across the WAN like ARP requests among others.

Each site will have its own Data and Voice VLAN(s) with separate IP addressing at each site. While IP addressing has to be unique for each VLAN, VLAN ID numbering can be reused from site to site. When using private IP address ranges to address the VLANs, typically the class A 10.X.X.X range is used for most devices on the LAN. To help make /30 point-to-point VLANs easily recognizable, it is recommended to use a different private IP address range to distinguish them from your other types of VLANs such as class C 192.168.X.X.

On each site's core L3 switch or router, the appropriate static IP routing or dynamic IP routing protocol(s) will need to

be configured to route traffic appropriately between sites. Refer to the appropriate data hardware manufacturer's configuration guide documentation on how to implement routing correctly as it is outside the scope of this document. While adhering to the same design principles, to add hardware or link redundancy to any design (including Rapid Spanning Tree, VTP, BGP, HSRP, VRRP, etc.), follow the appropriate data hardware manufacturer's configuration guide documentation to properly implement which is also outside the scope of this document and Mitel.

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 Connect CLOUD 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.
- Use a "hub and spoke" LAN topology where all layer-2 access level switches are the spokes connected via uplinks to the common "core" layer-3 switch.
- Use a WAN topology where all remote sites' layer-3 switch or router uses a WAN point-to-point uplink to the hub or point-to-multi-point uplink to all sites.
- Any private MPLS WAN circuits should bypass the firewall and connect directly to the L3 core switch. The firewall is an unnecessary single point of failure for a private network.
- 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.
- Connect all Voice switches and servers at a given site directly to the layer-3 data switch and only assign the local Voice VLAN as an untagged VLAN port for each.
- Use a separate /30 point-to-point VLAN to address each uplink/downlink to a remote site or to a firewall from the hub site's layer-3 switch, when appropriate.
- If expanding an existing VLAN subnet, change subnet mask on all devices on the subnet.

Configuring VLANs for ShoreTel 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, which need to be considered when designing the data network. For example, to help better utilize port capacity on data switches, a PC is allowed to 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.

ShoreTel 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. ShoreTel 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 (i.e. to mitigate deteriorating IP phone sound quality of a call if the data is unevenly sent due to lack of layer-2 output switch interface buffer prioritization). The Voice VLAN feature helps QoS use 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 but when the voice VLAN feature is enabled, all untagged traffic is sent according to the default CoS priority of the port and all 802.1P or 802.1Q tagged VLAN traffic's COS is trusted.

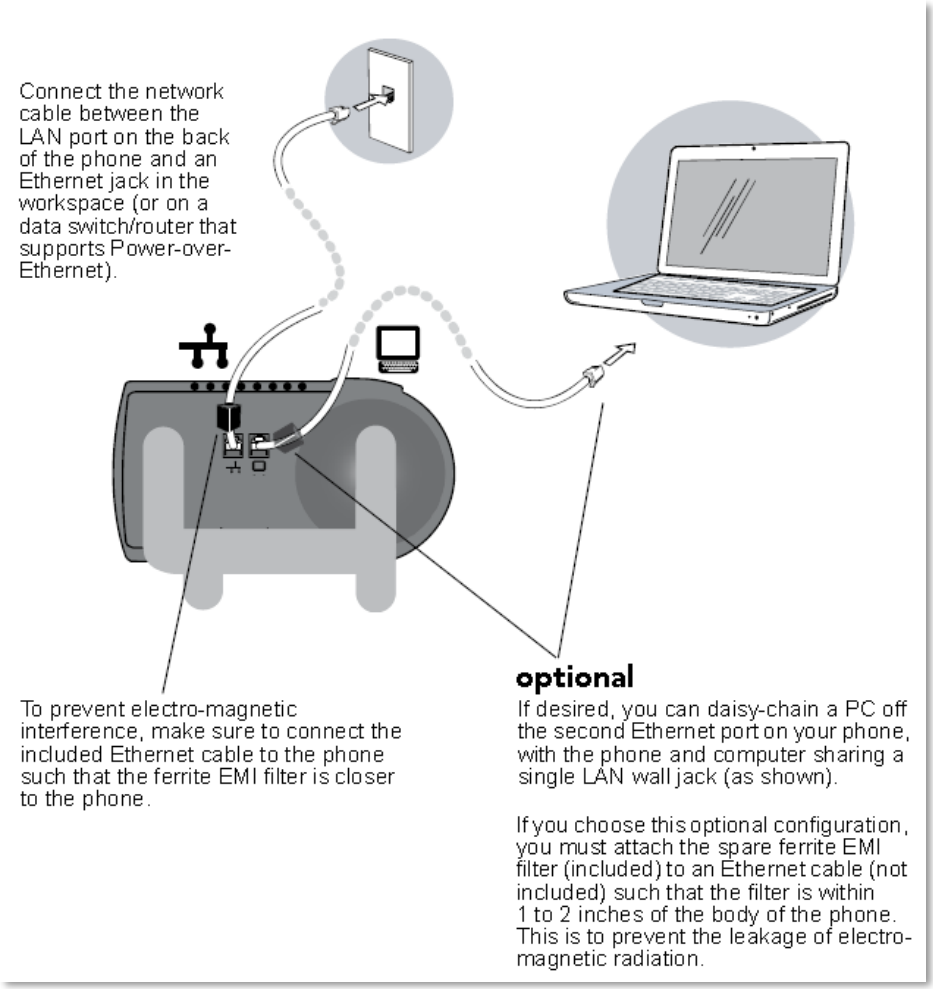

Figure 4

Figure 4 above demonstrates the physical connection of a PC connected to a ShoreTel 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 the section below, *Configuring Automatic IP Phone VLAN Assignment - LLDP-MED.*

The phone connected PC or laptop only has access to the local data network for normal Internet access so Voice and Data are still on separate virtual networks. While piggy-packed to the phone, the PC or laptop can start its own VPN client to connect separately to the corporate data network without any conflict or issue with the phone.

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 ShoreTel 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 ShoreTel IP Phone.

```
L2SWITCH 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 IP 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 ShoreTel 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.

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 a IEEE 802 Ethernet LAN. LLDP performs similar functions as several proprietary protocols such as the Cisco Discovery Protocol (CDP), Extreme Discovery Protocol, Nortel Discovery Protocol and Microsoft's Link Layer Topology Discovery. An enhancement to LLDP is LLDP-MED, Link Layer Discovery Protocol-Media Endpoint Discovery. LLDP eliminates the phone from using the untagged Data VLAN and allows only one DHCP request directly on the Voice VLAN.

The Automatic VLAN Assignment using LLDP-MED during the ShoreTel IP Phone standard boot process is as follows:

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 LLDP-MED TLV's such as "TIA – Network Policy" with "VLAN Id: 0" among many other TLV extensions. "VLAN Id: 0" is the request from the phone asking the Ethernet switch for the Voice VLAN ID as well as L2 Priority, DSCP value, and 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. See Figure 5 below).

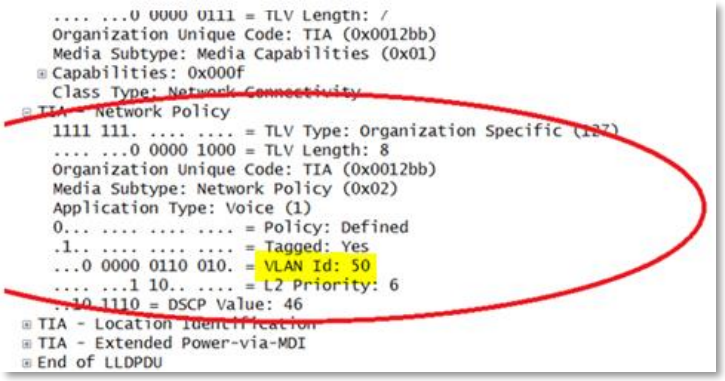

Figure 6

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 as well as other required files and finally reboots.
6. The IP Phone registers successfully and is ready for service.

LLDP is enabled by default on all supported ShoreTel IP phones starting with build version "SEV.3.3.0". All Ethernet switches in the data network intended to support IP phones should be configured for LLDP if not enabled by default with the appropriate TLVs enabled and configured per the Ethernet switch manufacturer's documentation and with the appropriate LLDP supported Ethernet switch firmware releases.

ShoreTel 400-series IP Phones

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

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 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 due to packet buffer memory queue limitations used on each transmitting data switch interface.

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 end-points, servers or switches.
- **Jitter** - No more than 50 msec of spacing between VoIP media packets
- **Loss** - No more than 1% of packet loss for VoIP RTP media stream packets
    - No standard has been set to measure signaling loss but while RTP is primarily time-sensitive, signaling is primarily drop-sensitive.

Why is the Interface Packet Buffer Memory the real QoS bottleneck and not the link bandwidth?

In most cases, before a packet is transmitted out any data switch/router interface, it is stored for a very brief amount of time in memory before the interface transmit queue sends the packet down the connected link. This memory is referred to as *packet buffer memory*. This memory is used differently depending on if the switch is a 'store & forward' or 'cut-thru' switch. Store & Forward switches buffer packets 100% of the time to a single, default queue when QoS is not enabled. This is like going through one checkout line at the grocery store for all shoppers. Cut-thru switches only buffer packets when interfaces are congested or busy also to a single, default queue when QoS is not enabled. When QoS is enabled, traffic is no longer sent to one transmit queue for an interface but multiple queues with reserved packet buffer memory for each queue where QoS classifies and maps marked traffic to a specific queue's packet buffer memory. This is like opening the express lane and self-checkout lane to better handle customers that can't wait with fewer groceries like VoIP traffic. Each queue activates distinct queuing algorithms designed to preserve VoIP traffic over other non-time sensitive or drop-sensitive traffic when transmitted. QoS exists at multiple OSI model layers where the queuing occurs at layer 3 and also layer 2 depending on whether the traffic is being routed and/or switched. Regarding Cisco, all IOS switches are 'Store & Forward'. Fixed S&F models include 3750X, 3560X, 2960 and 2960S for example. Nexus switches are Cut-Thru by default but can be changed to Store & Forward. ASICs have sped up switches so much that any gains today from cut-thru switching are small compared to store & forward. Layer 3 queues in layer-3 switches and routers are activated when layer-2 egress interfaces are congested or busy for traffic routing from different VLANs in the IP Routing Module. Packet Buffer memory is a limited resource and depending on the flow of traffic, can fill up more quickly compared to the connected link it supports. When the packet buffer is full, packets are tail-dropped or shaped and increment various drop counters.

QoS Traffic Marking Standard Recommendation

- RTP Traffic – Expedited Forwarding or PHB - **EF** i.e. **DSCP 46** or 184 (i.e. ToS (dec) value set in ST Director)
- Signaling Traffic – Class Selector 3 or PHB - **CS3** i.e. **DSCP 24** or 96 (i.e. ToS (dec) value set in ST Director)
    - AF31 – legacy signaling QoS traffic marking standard. It will still be supported during the transition to CS3.

QoS traffic marking standard is being updated to change the default signaling traffic DSCP value from AF31 to CS3 to better comply with industry standards. AF31 will still be supported during the transition period. RTP traffic will

continue to be marked with DSCP value EF. VoIP devices mark traffic at layer 3 using the appropriate DSCP value. Switches automatically map the layer 3 DSCP marking down to layer 2 for QoS at layer-2. The figure below offers the appropriate DSCP value in all necessary formats.

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

RFCs 2474, 2597 and 3246

Considering many customer data networks are built with Cisco networking equipment, per the Cisco QoS SRND (i.e. Cisco Enterprise QoS Solution Reference Network Design Guide), "Call-Signaling traffic should be marked as DSCP CS3 per the QoS Baseline. Call-Signaling traffic was originally marked by Cisco IP Telephony equipment to DSCP AF31 [circa early/mid 2000's]. However, the Assured Forwarding Classes, as defined in RFC 2597, were intended for flows that could be subject to markdown and subsequently the aggressive dropping of marked-down values. Marking down and aggressively dropping Call-Signaling could result in noticeable delay-to-dial-tone (DDT) and lengthy call setup times, both of which generally translate to poor quality experiences. Thus, the QoS Baseline changed the marking recommendation for Call-Signaling traffic to DSCP CS3 because Class Selector code points, as defined in RFC 2474, were not subject to markdown/aggressive dropping. Critical applications such as VoIP require service guarantees regardless of network conditions. The only way to provide service guarantees is to enable queuing at any node that has the potential for congestion, regardless of how rarely this may occur. This principle applies not only to Campus-to-WAN/VPN edges, where speed mismatches are most pronounced, but also to Campus Access-to-Distribution (typical 20:1) or Distribution-to-Core links (typical 4:1), where oversubscription ratios create the potential for congestion. There is simply no other way to guarantee service levels than by enabling [QoS] queuing wherever a speed mismatch exists. Not only does the Best Effort class of traffic require special bandwidth provisioning consideration, so does the highest class of traffic, sometimes referred to as the "Real-time" or "Strict Priority" class (which corresponds to RFC 3246 "An Expedited Forwarding Per-Hop Behavior"). The amount of bandwidth assigned to the Real-time queuing class is variable. However, if you assign too much traffic for strict priority queuing, then the overall effect is a dampening of QoS functionality."

Mechanisms to generally create and enforce QoS policies include:

- Queuing
- Shaping
- Selective-dropping
- Link-specific policies

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

The Most Important QoS Design Principles for Mitel

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

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 – Single Site

Single Site, Single Voice VLAN Deployment

QoS exists at multiple OSI model layers where the queuing occurs at layer 3 and also layer 2 depending on whether the traffic is being routed and/or switched. With a single site, single Voice VLAN deployment, layer 2 QoS is the only configuration that is required for prioritization.

Implicitly or Explicitly Universal LAN QoS/CoS Configuration Steps

- Enable QoS
- Configure queues, identifying priority queue, type, congestion-avoidance, bandwidth, buffer size, etc.
- Map CoS values to ingress and/or egress port queues and thresholds.
- Map DSCP values to ingress and/or egress port queues and thresholds.
- Configure DSCP map, which maps layer-2 CoS values to layer-3 DSCP values or visa versa.
- Bind QoS configuration to all VoIP switch interfaces.
- Validate configurations.

Cisco MLS-based vs. MQC-based QoS Configuration

Cisco's QoS configuration has evolved into two schools of configuration; Multi-Layer Switching (i.e. MLS) based QoS

and Modular QoS CLI (i.e. MQC) based QoS. Different Cisco switch models have adopted one of the 2 QoS configuration methods. Routers use MQC based QoS configuration. Once you have identified which method is used on a particular Cisco switch model, use the following examples that will work best with the Mitel Connect CLOUD system. To briefly summarize the main differences, MLS based-QoS only configures layer-2 QoS on switches. Layer-3 MLS-based switches need an additional policy-map manually configured for layer-3 QoS when needed for multiple Voice VLANs. MQC based QoS configures both layer-2 and layer-3 QoS, using a series of policy-maps on certain switches and all routers. The figure below quickly shows the difference between needed MLS-based and MQC-based QoS configurations. This is not a complete list of all commands but shows the primary commands issued at the interface level to get started.

Cisco IOS Software (MLS-based)	Cisco IOS Software (MQC-based)
mls qos or qos	qos
auto qos or auto qos srnd4	auto qos voip trust or auto qos trust (first interface)
srr-queue bandwidth share 10 10 60 20	auto qos voip trust or auto qos trust (> first interface)
priority-queue out	service-policy input AutoQos-4.0-Input-Policy (auto generated)
mls qos trust dscp	service-policy output AutoQos-4.0-Output-Policy (auto generated)
auto qos voip trust	
switchport mode access	switchport mode access
switchport access vlan 10	switchport access vlan 10
switchport voice vlan 20	switchport voice vlan 20
no cdp enable	no cdp enable
spanning-tree portfast	spanning-tree portfast

Figure 8

QoS Cisco IOS Interface MLS-based Commands Example

```
mls qos map cos-dscp 0 8 16 24 32 46 48 56
mls qos srr-queue input bandwidth 90 10
mls qos srr-queue input threshold 1 8 16
mls qos srr-queue input threshold 2 34 66
mls qos srr-queue input buffers 67 33
mls qos srr-queue input cos-map queue 1 threshold 2 1
mls qos srr-queue input cos-map queue 1 threshold 3 0
mls qos srr-queue input cos-map queue 2 threshold 1 2
mls qos srr-queue input cos-map queue 2 threshold 2 4 6 7
mls qos srr-queue input cos-map queue 2 threshold 3 3 5
mls qos srr-queue input dscp-map queue 1 threshold 2 9 10 11 12 13 14 15
mls qos srr-queue input dscp-map queue 1 threshold 3 0 1 2 3 4 5 6 7
mls qos srr-queue input dscp-map queue 1 threshold 3 32
mls qos srr-queue input dscp-map queue 2 threshold 1 16 17 18 19 20 21 22 23
mls qos srr-queue input dscp-map queue 2 threshold 2 33 34 35 36 37 38 39 48
mls qos srr-queue input dscp-map queue 2 threshold 2 49 50 51 52 53 54 55 56
mls qos srr-queue input dscp-map queue 2 threshold 2 57 58 59 60 61 62 63
mls qos srr-queue input dscp-map queue 2 threshold 3 24 25 26 27 28 29 30 31
mls qos srr-queue input dscp-map queue 2 threshold 3 40 41 42 43 44 45 46 47
mls qos srr-queue output cos-map queue 1 threshold 3 5
mls qos srr-queue output cos-map queue 2 threshold 3 3 6 7
mls qos srr-queue output cos-map queue 3 threshold 3 2 4
mls qos srr-queue output cos-map queue 4 threshold 2 1
mls qos srr-queue output cos-map queue 4 threshold 3 0
mls qos srr-queue output dscp-map queue 1 threshold 3 40 41 42 43 44 45 46 47
mls qos srr-queue output dscp-map queue 2 threshold 3 24 25 26 27 28 29 30 31
mls qos srr-queue output dscp-map queue 2 threshold 3 48 49 50 51 52 53 54 55
mls qos srr-queue output dscp-map queue 2 threshold 3 56 57 58 59 60 61 62 63
mls qos srr-queue output dscp-map queue 3 threshold 3 16 17 18 19 20 21 22 23
mls qos srr-queue output dscp-map queue 3 threshold 3 32 33 34 35 36 37 38 39
mls qos srr-queue output dscp-map queue 4 threshold 1 8
mls qos srr-queue output dscp-map queue 4 threshold 2 9 10 11 12 13 14 15
mls qos srr-queue output dscp-map queue 4 threshold 3 0 1 2 3 4 5 6 7
mls qos queue-set output 1 threshold 1 138 138 92 138
mls qos queue-set output 1 threshold 2 138 138 92 400
mls qos queue-set output 1 threshold 3 36 77 100 318
mls qos queue-set output 1 threshold 4 20 50 67 400
mls qos queue-set output 2 threshold 1 149 149 100 149
mls qos queue-set output 2 threshold 2 118 118 100 235
mls qos queue-set output 2 threshold 3 41 68 100 272
mls qos queue-set output 2 threshold 4 42 72 100 242
mls qos queue-set output 1 buffers 10 10 26 54
mls qos queue-set output 2 buffers 16 6 17 61
mls qos
```

```
interface GigabitEthernet1/0/1
 description uplink-ports
 switchport trunk encapsulation dot1q
 switchport mode trunk
 srr-queue bandwidth share 20 15 5 60
 priority-queue out
 mls qos trust dscp
 auto qos trust


interface GigabitEthernet1/0/5
 description pc-and-phone ports
 switchport access vlan 39
 switchport mode access
 switchport voice vlan 75
 srr-queue bandwidth share 1 2 7 90
 priority-queue out
 mls qos trust dscp
 auto qos trust
 no cdp enable
 spanning-tree portfast
```

Figure 9

srr-queue bandwidth share 20 15 5 60 - Enables Shaped Round Robin (SRR) egress queuing and assigns 20%, 15%, 5%

and 60% to the four egress queues, respectively, on the port for egress traffic. Each of the four queues (1, 2, 3, and 4) is guaranteed that percentage and can burst above that if other queues are idle. The percentages used are just an example and need to be adjusted for your network requirements that will not drop VoIP packets as needed.

The MLS generated map and queue commands map the appropriate queue to a COS value using the cos-map command and to a DSCP value using the dscp-map command. Notice the red highlighted output queues and the corresponding COS and DSCP values. Not all Cisco switches or non-Cisco switches map to the same queues every time. When customizing the srr-queue bandwidth command for the appropriate queue, check to see which DSCP values are mapped to which queue to customize each queue to the correct percentage desired relative to the speed of the interface and traffic volume expected.

priority-queue out - typically Queue 1, establishes a strict priority queue for traffic that is marked with highest priority – typically differentiated service code point (DSCP) value 184/EF (46) and above.

mls qos trust dscp - Sets the interface to trust DSCP values received from the phone or self-marking endpoint.

auto qos voip trust - Sets the interface to trust VLAN-tagged Class of Service (CoS) values received from the phone.

QoS Cisco IOS Interface MQC-based Commands Example

```
ip access-list extended acl-qos-shortel-RTP
remark shoretel-voip-media
permit udp any any range 10000 14500

ip access-list extended acl-qos-shortel-voip
remark shoretel-voip-call-and-system-control
permit udp any any eq 2427
permit udp any any eq 2727
permit udp any any eq 5060
permit udp any any range 5440 5443
permit udp any any range 5445 5446
permit udp any any eq 5450
permit tcp any any range 5060 5061
permit tcp any any eq 5430
permit tcp any any range 5447 5448
permit tcp any any eq 5452
permit tcp any any eq 31453
permit udp any any eq 31453


class-map match-any class-shoretel-media-input
  match access-group name acl-qos-shortel-RTP
  match  dscp ef

class-map match-any class-shoretel-signaling-input
  match access-group name acl-qos-shortel-voip
  match ip dscp cs3

class-map match-any class-shoretel-media-output
    match access-group name acl-qos-shortel-RTP
    match  dscp ef

class-map match-any class-shoretel-signaling-output
  match access-group name acl-qos-shortel-voip
  match ip dscp cs3
```

```
policy-map ShoreTel-Output-Policy
class class-shoretel-media-output
    set dscp ef
    priority
class class-shoretel-signaling-output
    set dscp cs3
    bandwidth remaining percent 15
class class-default
    set dscp default
    bandwidth remaining percent 60


policy-map ShoreTel-Input-Policy
class class-shoretel-media-input
   set dscp ef
class class-shoretel-signaling-input
   set dscp cs3
class class-default
   set dscp default


service-policy input ShoreTel-Input-Policy
service-policy output ShoreTel-Output-Policy
```

```
interface GigabitEthernet1/45
 description Trunk_Ports
 switchport trunk native vlan 1000
 switchport trunk allowed vlan 30,140,240,340,440,540
 switchport trunk allowed vlan add 940,1000
 switchport mode trunk
 qos trust dscp
 auto qos trust
 service-policy input ShoreTel-Input-Policy
 service-policy output ShoreTel-Output-Policy
```

```
interface GigabitEthernet8/47
 description PC-and-Phone Ports
 switchport access vlan 340
 switchport mode access
 switchport voice vlan 740
 qos trust dscp
 auto qos trust
 no cdp enable
 spanning-tree portfast
 service-policy input ShoreTel-Input-Policy
 service-policy output ShoreTel-Output-Policy
```

Figure 10

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.

Confirm the MQC-based QoS policy or MLS-based Policy-Map is applied to the Voice VLAN interface and monitor

It is important, on a routine basis, 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 signalling 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

Configuring Quality of Service – Multiple Sites

Multi-Site, Multi-Voice VLAN Deployment

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 or combination thereof. A single-site, multi-Voice VLAN deployment does not have a WAN but it shares the same concept of the multi-site, multi-Voice VLAN, which is that voice traffic does not stay on a single Voice VLAN but crosses the layer-3 boundary. 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 left off of 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.

A WAN data connection is required to connect each remote site L3 switch or router to the headquarter site's L3 switch or router. Certain WAN connections as well as redundant WAN connections require a customer provided router at each site but other WAN connections with an Ethernet handoff only require a layer-3 switch from the managed service provider hand-off. Consult your Service Provider and Data Hardware Vendor on which WAN connection product is appropriate for your bandwidth requirements between sites.

There are multiple WAN connectivity products; however, 2 common types represent the 2 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, which during high traffic periods will certainly cause voice quality issues. 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. Whether using MPLS or VPN tunnels, it is also recommended that the same type of point-to-point VLAN /30 subnet addressing be used to connect any two point-to-point sites together. Because layer-3 IP routing is required to route traffic between two VLANs or essentially between a LAN and a WAN, layer-3 QoS is also required to maintain layer 2 QoS/CoS beyond its original VLAN or while passing through a given layer-3 routing module.

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 queue-for-queue.

- Q1 – Expedited Forwarding (EF) strict priority traffic for RTP media ONLY
- Q2 – 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

While bandwidth/packet buffer percentages are assigned to each queue to guarantee resources during congestion, actual percentage assignment depends on traffic engineering calculations. Simply designed, based on the bandwidth of the MPLS service, calculate how many simultaneous calls respective to the chosen call codec during the busy call hour and allocate that percentage of traffic for Q1/EF traffic with some capacity to spare. A smaller percentage can be assigned to Q2 for prioritized signaling traffic based on the features, services and overall system design that controls how much signaling traffic will cross the WAN. This can be fine-tuned but there are signaling calculation charts in the Mitel Connect Planning and Install Guide to assist. The rest of the bandwidth and packet buffer allocation can be assigned to one of the remaining queues for best effort data traffic. To ensure that the WAN MPLS Service Provider is honoring and prioritizing your QoS markings, request to see the Ingress/Egress QoS Queue configuration on the WAN connection(s) for your connected sites as well as SHOW POLICY-MAP INTERFACE output for the Ingress and Egress Service Provider managed routers for the connected sites to confirm traffic is matching properly to each queue and no packet drops are occurring with Q1 or Q2 traffic.

Using Cisco Auto-QoS

Cisco uses an automated QoS configuration-scripting feature with various options that generate global QoS configurations on switches and/or routers. There are global Auto-QoS commands as well as interface specific Auto-QoS commands and they vary between Cisco IOS firmware trains. This can save you from manually configuring the entire QoS configuration on each switch or router. In fact, it is recommended to use AutoQoS when possible. The new DSCP marking standard will work with the default AutoQos configuration and should not require any customization of the auto-generated configuration once applied to all interfaces related to Mitel Connect traffic.

AutoQoS works for both MLS-based and MQC-based QoS configuration.

Auto-QoS needs to be run separately on every Cisco switch or router that participates in the VoIP QoS infrastructure. Some Cisco switches or routers may need to have their IOS firmware upgraded to support the Auto-QoS feature. Nexus switches do not support AutoQos and will require a manual configuration based on the MQC-based QoS commands described in the previous section. Check Cisco's documentation for specific Auto-QoS firmware version support. Auto-QoS interface commands specific to Cisco's IP Phone endpoints are not necessary, only Auto-QoS Support for Marked Traffic. Auto-QoS will never completely configure any switch or router with "ready to use" QoS but essentially acts as a QoS template that configures the majority of needed functionality in most cases.

After Auto-QoS has finished running, confirmed with a SH RUN command, compare the generated QoS configuration in each switch or router to the QoS requirements for Mitel VoIP in all QoS sections and manually apply to the VoIP related interfaces for full QoS functionality. To take advantage of the Auto-QoS defaults, you should enable Auto-QoS before you configure other QoS commands. If you are repurposing a Cisco switch or router that already had a QoS configuration applied, be sure to remove all existing QoS before applying your new QoS configuration.

> **IMPORTANT TIP**: It is a good practice to always back up your switch or router configurations before running Auto-QoS or before any other major configuration changes. Adjusting network settings should be performed after hours during a scheduled maintenance window. The switch/router may require a reboot to fully enact all changes.

In "enable" mode on the Cisco IOS L2 switch or L3 switch/router, type the following global commands:

mls qos or *qos* (enables QoS on the switch or router)

auto qos (executes global Auto-QoS) or *auto qos srnd4* (supported by certain models. *Auto qos srnd4* global configuration command is generated as a result of enhanced Auto-QoS configuration) or *auto qos voip trust* applied to the first physical interface generates the qos configuration for that interface as well as run the autoqos script for the applicable global commands. All commands are dependent of the Cisco model and IOS version so refer to Cisco documentation for more detail.

The global Auto-QoS command generates ingress and egress queuing, maps CoS values to DSCP values, and maps DSCP markings to queues among other configuration. Other models create only default policy-maps for all QoS.

Interface level QoS commands add configuration lines to each Ethernet interface. The lines added to each interface determine how the switch will handle marked traffic from the ShoreTel phones as well as switches and servers. At the interface level, by specifically using the *auto qos voip trust* command, no other commands on the interface will be automatically added thus will subsequently need to be added manually. Sometimes the commands can be entered in ranges for multiple interfaces at a time on a switch.

Depending on the IOS version and switch model, you may have differing syntax and/or some commands might be hidden in the show running configuration output because they are default and require other Show commands to view.

Displaying Auto-QoS Information on most Cisco IOS based switches and/or routers

The following Show commands are a list of the most common QoS verification output commands for QoS on multiple Cisco IOS platforms. Use the commands available to your particular equipment model as appropriate.

show run

show mls qos

show mls qos maps cos-dscp

show mls qos interface <mod/ports> [buffers | queueing]

show mls qos maps [cos-dscp | cos-input-q | cos-output-q | dscp-cos | dscp-input-q | dscp-output-q]

show mls qos input-queue

show auto qos interface <mod/ports>

show class-map

show policy-map

show policy-map interface <mod/ports>

show int <mod/ports> capabilities

show mls qos interface interface <mod/ports> statistics

show rmon [alarms | events] to display any LLQ drops.

> **TIP**: Auto-QoS also activates thresholds in the RMON alarm table to monitor drops in the voice LLQ in models that are supported.

In Figure 12 below, A SH RUN command after AutoQos has successfully completed, will show a similar group of MQC-based QoS commands. Highlighted with red outlined boxes, these specific commands will be used by Mitel Connect by default.

```
class-map match-all AutoQos-4.0-Scavenger-Classify
 match access-group name AutoQos-4.0-ACL-Scavenger
class-map match-all AutoQos-4.0-Signaling-Classify
 match access-group name AutoQos-4.0-ACL-Signaling
class-map match-any AutoQos-4.0-Priority-Queue
 match cos  5
 match dscp ef
 match dscp cs5
 match dscp cs4
class-map match-any AutoQos-4.0-Multimedia-Stream-Queue
 match dscp af31
 match dscp af32
 match dscp af33
class-map match-all AutoQos-4.0-Network-Mgmt
 match dscp cs2
class-map match-all AutoQos-4.0-Default-Classify
 match access-group name AutoQos-4.0-ACL-Default
class-map match-any AutoQos-4.0-Signaling
 match dscp cs3
 match cos  3
class-map match-any AutoQos-4.0-VoIP
 match dscp ef
 match cos  5
class-map match-any AutoQos-4.0-Control-Mgmt-Queue
 match cos  3
 match dscp cs7
 match dscp cs6
 match dscp cs3
 match dscp cs2
 match access-group name AutoQos-4.0-ACL-Signaling
class-map match-all AutoQos-4.0-Bulk-Data-Classify
 match access-group name AutoQos-4.0-ACL-Bulk-Data
class-map match-any AutoQos-4.0-Multimedia-Stream
 match dscp af31
 match dscp af32
```

```
policy-map AutoQos-4.0-Input-Policy
 class AutoQos-4.0-VoIP
 class AutoQos-4.0-Broadcast-Vid
 class AutoQos-4.0-Realtime-Interact
 class AutoQos-4.0-Network-Ctrl
 class AutoQos-4.0-Internetwork-Ctrl
 class AutoQos-4.0-Signaling
 class AutoQos-4.0-Network-Mgmt
 class AutoQos-4.0-Multimedia-Conf
 class AutoQos-4.0-Multimedia-Stream
 class AutoQos-4.0-Transaction-Data
 class AutoQos-4.0-Bulk-Data
 class AutoQos-4.0-Scavenger
policy-map AutoQos-4.0-Output-Policy
 class AutoQos-4.0-Scavenger-Queue
  bandwidth remaining percent 1
 class AutoQos-4.0-Priority-Queue
  priority
  police cir percent 30 bc 33 ms
 class AutoQos-4.0-Control-Mgmt-Queue
  bandwidth remaining percent 10
 class AutoQos-4.0-Multimedia-Conf-Queue
  bandwidth remaining percent 10
 class AutoQos-4.0-Multimedia-Stream-Queue
  bandwidth remaining percent 10
 class AutoQos-4.0-Trans-Data-Queue
  bandwidth remaining percent 10
    dbl
 class AutoQos-4.0-Bulk-Data-Queue
  bandwidth remaining percent 4
    dbl
 class AutoQos-4.0-Output-Control-Mgmt-Queue
 class class-default
  bandwidth remaining percent 25
    dbl
```

```
interface GigabitEthernet1/48
 description Trunk_Ports
 switchport trunk native vlan 1000
 switchport trunk allowed vlan 30,140,240,340
 switchport trunk allowed vlan add 940,1000
 switchport mode trunk
 qos trust dscp
 auto qos trust
 service-policy input AutoQos-4.0-Input-Policy
 service-policy output AutoQos-4.0-Output-Policy
!
interface GigabitEthernet2/1
 description PC_and_Phone_Ports
 switchport access vlan 540
 switchport mode access
 switchport voice vlan 740
 qos trust dscp
 auto qos trust
 no cdp enable
 spanning-tree portfast
 service-policy input AutoQos-4.0-Input-Policy
 service-policy output AutoQos-4.0-Output-Policy
!
interface Port-channel7
 description Port_Channel_Trunk_Ports
 switchport
 switchport trunk native vlan 1000
 switchport trunk allowed vlan 30,100,140,240,340
 switchport trunk allowed vlan add 841,940,1000
 switchport mode trunk
 switchport nonegotiate
 qos trust dscp
 auto qos trust
 service-policy input AutoQos-4.0-Input-Policy
```

Figure 12

Packet Captures

How do I verify the packets are marked with the right DSCP value?

Once you have incorporated all of the best practices in this document, one of the final steps is to verify that thel packets are marked correctly in order to be honored by the QoS configuration on the data network. The two figures below show where to look in a packet to see the DSCP value that is marked for QoS. If the RTP packets are not marked as Expedited Forwarding and the signaling packets per Figure 12 are not marked as CS3, revisit the previous sections to find the issue and retest until the packets are marked correctly. It is a best practice to check as many different sources of traffic on the data network to ensure individual segments were not missed.

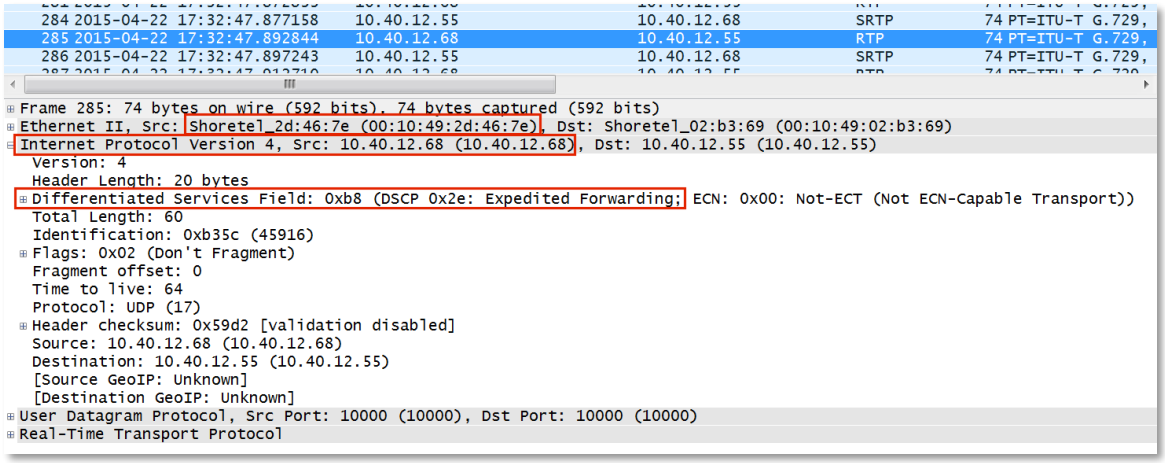

Figure 13

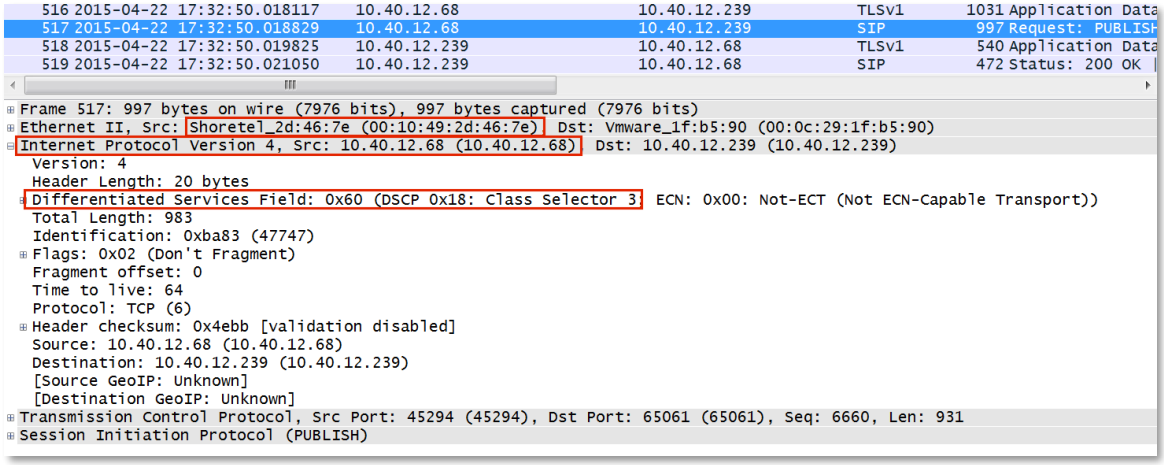

Figure 14

What About Disaster Recovery?

Every enterprise, whether large or small, places a heavy reliance on their communication infrastructure to conduct and grow their business. It is imperative that your Mitel Connect CLOUD system provides extremely high levels of reliability, survivability and functionality, even when faced with outages, faults and unforeseen disasters.

The cloud based architecture of the Mitel Connect CLOUD solution is uniquely tailored to exceed these expectations

and is built with reliability, resiliency, survivability and fault tolerance in mind. Like any advanced system, proper planning, deployment strategies and best practice configurations are necessary keys to installing and maintaining a fully survivable and high-availability Mitel Connect CLOUD system.

NOTE: Your backup connection may NOT be on a private network. The speed of the network may be slower and voice calls could be affected compared to the primary network connectivity.

Without redundancy, if you lose power to the Mitel provided router, all incoming calls will go to voicemail or any other pre-determined find-me-follow-me settings. You will NOT lose any incoming calls since it is a hosted service.

Take into account the following redundancy layers when considering how best to mitigate issues in your data network converged with Mitel Connect CLOUD:

Redundant Services – Which services need High Availability?

- Voice
- Internal Data (i.e. site to site)
- Internet

Redundant Links – Which connectivity options are possible based on available HA services?

- Mitel provided backup MPLS circuit (e.g. into a CUG) - Will support current voice, data and backhauled Internet.
- GRE VPN Tunnel - Will support voice but not data or backhauled Internet.
- NAT (i.e. Network Address Translation) over local Internet (i.e. assumes a local Internet connection) - Will support voice and Internet but not internal site-to-site data.

Redundant Hardware – What hardware is needed for more redundancy and security based on above selections?

- Backup Mitel provided router for backup MPLS circuit into carrier CUG.
- Local Internet connection(s) per site.
- Local firewall with a Layer-3 switch per site.

Once the customer decides on the necessary redundancy requirements, a Mitel data network engineer will help design the specific network topology per the HA requirements. Redundant configurations and designs are additional cost from the typical deployment and will be quoted per the customer requirements and environment designed.

Off-Net 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 Network Services does configure firewalls per a Network Delivery billable engagement. Mitel does not make recommendations on what firewalls to use other than what capabilities are required.

Firewalls requirements for any relevant Mitel Connect CLOUD configuration includes the following features:

- Stateful Inspection
- NAT
- DHCP server
- AV Antivirus Enforcement
- Spam filter
- Intrusion Detection System (IDS)
- Virtual Private Network (VPN)

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 (i.e. NAT) or a dedicated NAT device. In these cases, the firewall configuration needs to be considered for Mitel Connect Cloud services and features. The following ports for the Sky or Mitel Connect Cloud platform need to be opened with a policy on the firewall when configuring the NAT for the appropriate traffic to pass through.

NOTE: The firewall policy configuration to open the appropriate ports for the Mitel services should be limited

to the destination IP address of the given Mitel server(s). Consult your Mitel representative for the needed IP address information.

ShoreTel Sky DNS and Port Usage

For ShoreTel Sky IP Phones to work over a broadband Internet connection, firewalls must be configured to allow outbound and inbound traffic from/to the following ports to the appropriate URL or IP Address:

ShoreTel Sky Phones and Phone Assistant

- TCP 12000 SCCP
- TCP 12001 SCCP/HTTP
- TCP/UDP 5060 SIP
- TCP 5061 SIPS
- TCP/UDP 15061 SIP
- TCP 5443, 5448 CAS
- Proxy.m5net.com:8XXX (TCP**)
- UDP 69 TFTP
- UDP 16384-37000 RTP Media Server
- TCP 80
- TCP/UDP 443

**Note - 8XXX is the Server/API Port Number in the TFTP/Config Server article available at: http://support.shoretel.com/kb/view.php?t=TFTP

ShoreTel Sky DNS Servers – VoIP DHCP Scope

- 64.242.250.6 and 64.242.250.7

Mitel Connect Cloud Destination IP Addresses, DNS and Port Usage

For Mitel Connect Cloud IP Phones to work over a broadband Internet connection, firewalls must be configured to allow outbound and inbound traffic from/to the following ports to all the appropriate Mitel URL(s) or IP Address(es):

Mitel Destination IP Addresses

- 66.11.214.44 and 66.11.214.48 - IP phones
- 66.11.214.46 and 66.11.214.56 - softphones

Mitel DNS Servers – VoIP DHCP Scope

- 66.11.195.11 and 199.101.107.6

Ports

- TCP/UDP 5060 SIP
- TCP 5061 SIPS
- TCP 80 HTTP
- TCP/UDP 443
- TCP 8001 Admin
- TCP 31451-31471 (ECC Supervisor)
- UDP 10000-65535 RTP Media Stream

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, as long as 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 3600 seconds (6 minutes), so configuring the firewall/NAT device with TCP timeouts greater than 6 minutes will maintain the connection.
- Note that Mitel uses this relatively long registration interval because the client SIP softphone is

temporarily unavailable during the re-register process. Many NAT devices by default forget port mappings after 30 seconds, so this is an important area to troubleshoot.

- Stateless firewall/NAT configuration - port forwarding method
- This method works for single users on SOHO networks, as it eliminates the need to adjust the port timeout settings for their NAT/firewall device.
- It is required for users using less common stateless firewalls (firewalls that do not automatically map inbound ports based on outbound connections).
- In these cases, one can configure the NAT device (e.g., home router) to forward connections from the SIP signaling port (TCP port 15061) and real-time (RTP) audio port range (UDP ports 27000 - 29047) to the computer on the user's local area network.

Troubleshooting Connectivity

The eyeBeam application can be configured to generate a diagnostic log of varying detail. This can be used in combination with packet sniffing to isolate a problem. GUI software such as Ethereal/Wireshark or CLI programs such as tcpdump on Unix or Unix-like OS's (e.g. Mac OS X) can be helpful. EyeBeam does not provide a meaningful error, although, errors identified with a packet dump are likely caused by the client computer typically.

NOTE: Mitel uses non-standard SIP signaling and RTP ports.

In Summary:

- A lack of sent packets in a packet dump indicates a local computer problem outside of Mitel's control, for example, in the TCP stack.
- A lack of RECEIVED SIP messages in the X-Lite diagnostic log from "Catch 9 Communications" indicates a problem connecting to Mitel that may be caused by local computer, NAT, or Internet routing problems outside of Mitel's control.
- Other symptoms can be diagnosed in the eyeBeam client display or diagnostic log based on the type of RECEIVED SIP messages from "Catch 9 Communications."
- A "service unavailable" message on the client, accompanied by errors in the diagnostic log without any packets sent or received by the client computer indicate a problem with the client PC's network configuration or a bug in the SIP softphone client, e.g., a WINSOCK error. Mitel may not be able to resolve this issue; the client may have to reinstall the networking components of his or her operating system or perform a full re-installation.
- A login timeout when placing an outbound call, accompanied by repeated SENT SIP messages without any RECEIVED SIP messages in the diagnostic log and packets sent to (e.g. 66.11.207.75, pat1.212803.m5net.net) via UDP or TCP with a response from e.g. pat1212803.m5net.net, indicating that the port is "unavailable for IP" suggests a misconfigured SIP softphone (e.g., one that is trying to register or communicate on the wrong port). Note that Mitel does not use registered SIP ports.
- A busy signal when attempting to place an outgoing call accompanied by a RECEIVED SIP message in the diagnostic log stating "Proxy Authentication Required" indicates that the softphone is misconfigured and is not set to register. Incoming calls will fail to ring in this scenario. Set the softphone to register.
- An "unauthorized" message on the client accompanied by a RECEIVED SIP message in the diagnostic log stating "Unauthorized" when attempting to register indicates that the password or authorization name is incorrect. Incoming calls will fail to ring in this scenario.

SCCP Phones: Cisco Pix Firewall

When running a SCCP phone behind a Cisco PIX Firewall or routers configured for NAT can cause SCCP (Skinny) IP

phones to freeze or not work.

SCCP phone behind a Cisco PIX Firewall

By default, a PIX firewall inspects the content of TCP-SCCP packets and will discard any packet it doesn't understand. If a SCCP message becomes segmented into two separate TCP packets, the 2nd packet won't be understood by the PIX and will be discarded. Subsequent re-transmissions of the packet are likewise discarded, causing the phone to freeze. It must then be power-cycled to recover.

The solution is to add the following line to the PIX configuration and then reset all SCCP phones to make them open a new SCCP session.

no fixup protocol skinny 2000

SCCP phone behind a router configured for NAT

A Cisco router at a customer site configured for NAT will detect TCP-SCCP messages and translate the network address information inside the SCCP messages. Although this process is necessary for operation with Cisco Call Manager, it interferes with translations performed by the Call Manager and can also cause the phone to 'freeze'. The solution is to add the following line to the NAT router configuration and then reset all SCCP phones to make them open a new SCCP session.

no ip nat service skinny tcp port 2000

3rd Party MPLS DHCP Scope and QoS Best Practice

3rd Party MPLS DHCP Scope Customer Router Configuration Examples

Customers that order their own 3rd party MPLS circuit(s) and deploy a customer provided router(s) in a Mitel Data Center would also have to configure their own Voice DHCP scope for the Mitel VoIP service. The following examples show the options and parameters that are required for ShoreTel IP Phones with ShoreTel Sky vs. Mitel Connect CLOUD services.

ShoreTel Sky - Cisco DHCP Scope Example

```
!
ip dhcp pool voip
  network [voice subnet] [subnet mask]
  default-router [first usable voice subnet IP]
  dns-server 64.242.250.6 64.242.250.7
  option 150 ip [ST tftp 1] [ST tftp 2]
  option 156 ascii "ftpservers=[ST tftp 1], [ST tftp 2]"
```

ShoreTel Sky - HP DHCP Scope Example

```
#
dhcp server ip-pool voip
  network [voice subnet] mask [subnet mask]
  gateway-list [first usable voice subnet IP]
  dns-list 64.242.250.6 64.242.250.7
  option 150 ip-address [ST tftp 1] [ST tftp 2]
  option 156 ascii “ftpservers=[ST tftp 1], [ST tftp 2]”
```

ShoreTel Connect Cloud - Cisco DHCP Scope Example

```
!
ip dhcp pool voip
  network [voice subnet] [subnet mask]
  default-router [first usable voice subnet IP]
  dns-server 208.103.94.230 199.101.107.70
  option 156 ascii "configservers=update.sky.shoretel.com"
  option 42 ip [first usable = default-router]
!
ntp server 208.103.94.225 prefer
ntp server 199.101.107.67
!
```

ShoreTel Connect Cloud - HP DHCP Scope Example

```
#
dhcp server ip-pool voip
  network [voice subnet] mask [subnet mask]
  gateway-list [first usable voice subnet IP]
  dns-list 208.103.94.230 199.101.107.70
  option 156 ascii “configservers=update.sky.shoretel.com”
  option 42 ip-address [first usable = gateway-list]
#
ntp-service unicast-peer 208.103.94.225 priority
ntp-service unicast-peer 199.101.107.67
#
```

Figure 15

Notice the primary difference is the use of the *option 156 ftpServers* vs. the *configServers* parameter tag. With ShoreTel Sky, the *ftpServers* tag is directed to the appropriate server IP address. With ST Connect CLOUD, the *configServers* tag is used in order to direct the IP Phone to one of three URLs used to update the firmware via HTTP. If the IP Phone firmware needs automatic updating, the URL, *update.sky.shoretel.com*, will be used. Once updated, the bootstrap process contains all three URLs within the firmware and option 156 is no longer needed. However, keep the *option 156 configServers* tag configured on the DHCP server's voice VLAN DHCP scope in case any older ST IP Phones are ever used without manually configuring the URL into the IP Phone's CLI display.

> **Note:** The *ftpServers* and *configServers* parameters are case sensitive if manually changed in the phone CLI. They are not case sensitive when received from any DHCP server.

Do not simultaneously use both the ftpServers and configServers tags with option 156, considering each will boot the IP Phone differently with the hosted services. The ftpServers tag is intended for the ShoreTel Sky service and the configServers tag is intended for the ST Connect CLOUD service. If the ftpservers tag is used on the ST Connect CLOUD service, the ShoreTel IP Phone will likely not boot properly and will continually request for service. The same is true for the configServers tag if used on the ShoreTel Sky service.

3rd Party MPLS QoS Customer Router Configuration Examples

Every hop in the QoS construct needs to be configured including the customer provided 3rd party MPLS router. The following examples show how to properly mark traffic in the appropriate direction to match the LAN and WAN DSCP markings for ShoreTel Sky vs. Mitel Connect. The WAN facing policy marks all VoIP traffic as DSCP EF and the LAN facing policy remarks signaling traffic as CS3 and RTP traffic as EF to maintain DSCP compatibility in each direction.

ShoreTel Sky - Cisco IOS 15 QoS Example

```
!
class-map match-all Voice
 match access-group name VoiceSubnet
class-map match-all ShoreTel-VoIP-RTP
 match ip dscp ef
 match access-group 101
class-map match-all ShoreTel-VoIP-Control
 match access-group 100
!
policy-map lan_voip
 class ShoreTel-VoIP-RTP
  set dscp ef
 class ShoreTel-VoIP-Signaling
  set dscp cs3
 class class-default
  set dscp default
policy-map wan_voip
 class Voice
  set ip dscp ef
!
ip access-list extended VoiceSubnet
 permit ip [voice subnet] [wildcard mask] any
!
access-list 100 remark ShoreTel Sky Signaling Traffic
access-list 100 permit tcp any eq 2000 any
access-list 100 permit udp any eq 2000 any
access-list 100 permit tcp any eq 5060 any
access-list 100 permit udp any eq 5060 any
access-list 100 permit tcp any eq 5061 any
access-list 100 permit udp any eq 5061 any
access-list 100 permit tcp any eq 12000 any
access-list 100 permit tcp any eq 12001 any
access-list 100 permit tcp any eq 15061 any
access-list 101 remark ShoreTel Sky RTP Traffic
access-list 101 permit udp any any range 10000 11999
access-list 101 permit udp any any range 12002 15060
access-list 101 permit udp any any range 15062 33000
!
interface [ST Router facing port]
description WAN
```

```
service-policy output wan_voip
!
interface [Customer MPLS facing port]
description LAN
service-policy output lan_voip
```

```
!
```

ShoreTel Connect Cloud - Cisco IOS 15 QoS Example

```
!
class-map match-all Voice
 match access-group name VoiceSubnet
class-map match-all ShoreTel-VoIP-RTP
 match ip dscp ef
 match access-group 101
class-map match-all ShoreTel-VoIP-Control
 match access-group 100
!
policy-map lan_voip
 class ShoreTel-VoIP-RTP
  set dscp ef
 class ShoreTel-VoIP-Signaling
  set dscp cs3
 class class-default
  set dscp default
policy-map wan_voip
 class Voice
  set ip dscp ef
!
ip access-list extended VoiceSubnet
 permit ip [voice subnet] [wildcard mask] any
!
access-list 100 remark ShoreTel Cloud Signaling Traffic
access-list 100 permit tcp any eq 5060 any
access-list 100 permit udp any eq 5060 any
access-list 100 permit tcp any eq 5061 any
access-list 100 permit udp any eq 5061 any
access-list 101 remark ShoreTel Sky RTP Traffic
access-list 101 permit udp any any range 10000 65535
!
interface [ST Router facing port]
description WAN
service-policy output wan_voip
!
interface [Customer MPLS facing port]
description LAN
service-policy output lan_voip
```

ShoreTel Sky - HP Comware 7.0 QoS Ex

```
acl number 3001 name QOS
rule 0 permit ip source [ voice block ] [wc mask ] logging
#
acl number 3002 name LAN_QOS_SIGNALING
 rule 5 permit tcp source-port eq 2000
 rule 10 permit udp source-port eq 2000
 rule 15 permit tcp source-port eq 5060
 rule 20 permit udp source-port eq 5060
 rule 25 permit tcp source-port eq 5061
 rule 30 permit tcp source-port eq 12000
 rule 35 permit tcp source-port eq 12001
 rule 40 permit tcp source-port eq 15061
#
acl number 3003 name LAN_QOS_RTP
 rule 5 permit udp source-port range 10000 11999
 rule 10 permit udp source-port range 12002 15060
 rule 15 permit udp source-port range 15062 33000
#
traffic classifier voice operator or
 if-match acl 3001
#
traffic classifier call_signaling operator AND
 if-match acl 3002
#
traffic classifier rtp operator AND
 if-match acl 3003
#
traffic behavior mark_rtp
 remark dscp ef
#
traffic behavior mark_signaling
 remark dscp cs3
#
traffic behavior mark-voice
 remark dscp ef
 queue ef bandwidth pct 80 cbs-ratio 25
#
qos policy lan_voip
```

```
 classifier call_signaling behavior mark_signaling
 classifier rtp behavior mark_rtp
#
qos policy wan_voip
 classifier voice behavior mark-voice
#
interface [ST Router facing port]
desc WAN
qos apply policy wan_voip outbound
#
interface [Customer MPLS facing port]
desc LAN
qos apply policy lan_voip outbound
```

ShoreTel Connect Cloud - HP Comware 7.0 QoS Ex

```
acl number 3001 name QOS
rule 0 permit ip source [ voice block ] [wc mask ] logging
#
acl number 3002 name LAN_QOS_SIGNALING
 rule 5 permit tcp source-port eq 5060
 rule 10 permit udp source-port eq 5060
 rule 15 permit tcp source-port eq 5061
 rule 20 permit udp source-port eq 5061
#
acl number 3003 name LAN_QOS_RTP
 rule 5 permit udp source-port range 10000 65535
#
traffic classifier voice operator or
if-match acl 3001
#
traffic classifier call_signaling operator AND
 if-match acl 3002
#
traffic classifier rtp operator AND
 if-match acl 3003
#
traffic behavior mark_rtp
 remark dscp ef
#
traffic behavior mark_signaling
 remark dscp cs3
#
traffic behavior mark-voice
 remark dscp ef
 queue ef bandwidth pct 80 cbs-ratio 25
#
qos policy lan_voip
 classifier call_signaling behavior mark_signaling
 classifier rtp behavior mark_rtp
#
qos policy wan_voip
 classifier voice behavior mark-voice
#
interface [ST Router facing port]
desc WAN
qos apply policy wan_voip outbound
#
interface [Customer MPLS facing port]
desc LAN
qos apply policy lan_voip outbound
```

Power Over Ethernet

Typically, most VoIP deployments will utilize 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. A few things to consider is the power consumption of a group of IP phones vs. the amount of power a data switch can actually support at one time. When the power consumption is exceeded, the data switch turns off the POE to protect the switch and all of 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, a ShoreTel 485G 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 of 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 of the phones.

Configuring Cisco SB Switch Settings – Auto Smartport & EEE

When using ShoreTel 400-series IP Phones with Cisco Small Business switches (i.e. SG series), 2 port management features, Administrative Auto Smartport and Energy Efficient Ethernet (i.e. EEE), need to be disabled. This will ensure that the phone service will not be inadvertently interrupted due to the features' behavior. Issues with these features enabled typically experience IP Phone service recycling at a regular interval such as every 15 minutes or so.

Figure 16

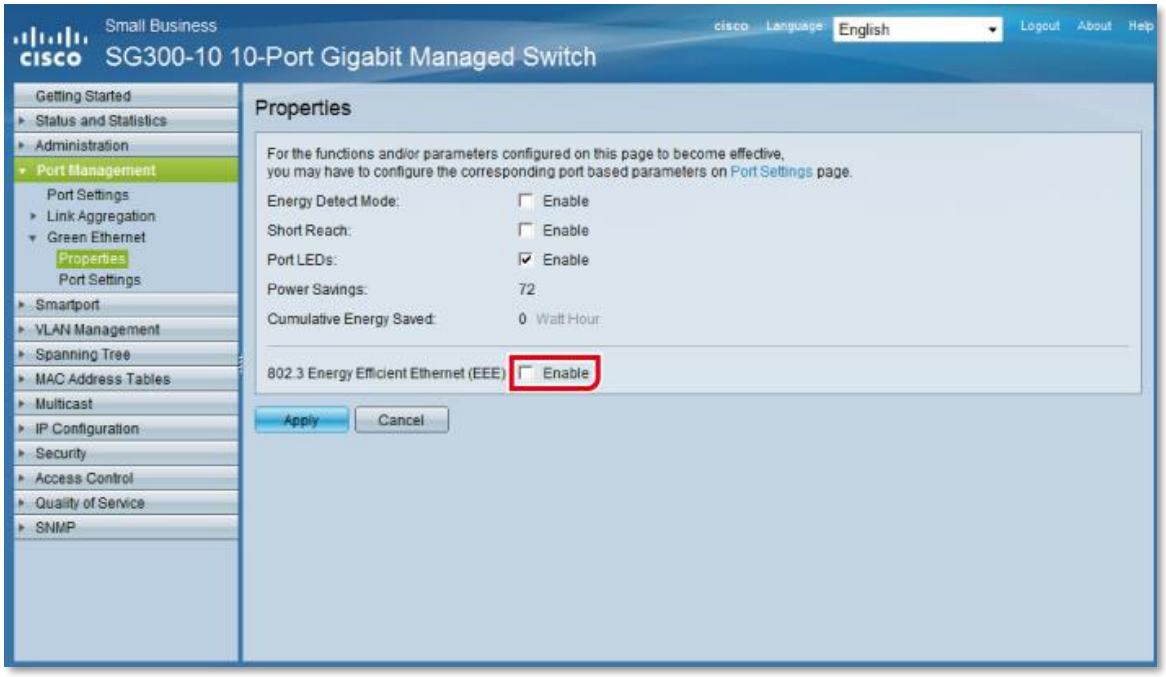

Figure 17

Conclusion

There are many different specialized QoS configuration options that were not discussed in this document; however, the most common were highlighted in a mid-level manner to help any IT administrator or Data Network Administrator with limited VoIP QoS background easily understand how best to deploy Mitel VoIP with the highest degree of success.

Other topics are very pertinent but are beyond the scope of this document, such as:

- Private VLANs
- MAC address locking/filtering

- Denial of Service (DOS) / Distributed DOS (DDOS) attack prevention
- Voice encryption
- Security best practices

References

IEEE 802.1Q Tagging:

http://www.ieee802.org/1/pages/802.1Q.html

http://ieeexplore.ieee.org/xpl/standardstoc.jsp?isnumber=27089&isYear=2003

Mitel Guides and References:

Mitel Planning and Installation Guide, Chapter 9: “Understanding Toll-Quality Voice”

Cisco Configuration Guides and References:

Cisco Medianet Quality of Service Design – Main Menu

http://www.cisco.com/en/US/solutions/ns340/ns414/ns742/ns1127/landing_cVideo.html

Cisco AutoQoS for Voice over IP (White Paper)

http://www.cisco.com/en/US/tech/tk543/tk759/technologies_white_paper09186a00801348bc.shtml

Configure CatOS Catalyst Switches to Connect Cisco IP Phones Configuration Example

http://www.cisco.com/en/US/products/hw/switches/ps708/products_configuration_example09186a00808a4a41.shtml

Configuring Auto-QoS

http://www.cisco.com/en/US/docs/switches/lan/catalyst3750/software/release/12.2_58_se/configuration/guide/swqos.html#wp1231112

Cisco AutoQoS Q&A

http://www.cisco.com/en/US/technologies/tk543/tk879/technologies_qas0900aecd8020a589.html

Troubleshooting Output Drops with Priority Queueing
http://www.cisco.com/en/US/tech/tk39/tk51/technologies_tech_note09186a0080103e8a.shtml

Considerations, Caveats, and Restrictions for AutoQoS VoIP
http://www.cisco.com/en/US/tech/tk543/tk759/technologies_white_paper09186a00801348bc.shtml#wp39556

Cisco QoS SRND

http://www.cisco.com/c/en/us/td/docs/solutions/Enterprise/WAN_and_MAN/QoS_SRND/QoS-SRND-Book/QoSIntro.html#pgfId-46102

Document and Software Copyrights

Trademarks

Disclaimer

Mitel tests and validates the interoperability of the Member's solution with Mitel's published software interfaces. Mitel does not test, nor vouch for the Member's development and/or quality assurance process, nor the overall feature functionality of the Member's solution(s). Mitel does not test the Member's solution under load or assess the scalability of the Member's solution. It is the responsibility of the Member to ensure their solution is current with Mitel's published interfaces.

The Mitel Technical Support organization will provide Customers with support of Mitel's published software interfaces. This does not imply any support for the Member's solution directly. Customers or reseller partners will need to work directly with the Member to obtain support for their solution.

Company Information

Mitel Inc.

960 Stewart Drive

Sunnyvale, California 94085 USA

+1.408.331.3300

+1.408.331.3333 fax

Author

CHAD HORTON
Manager, Innovation and Network Services
chorton@shoretel.com
+1 (512) 551-7185 Tel
+1 (408) 242-0195 Cell
www.shoretel.com