Application Note

AN2919

Nov 20, 2017

Network Best Practices for Mitel Connect ONSITE

Description: This application note discusses various Data Network VoIP topics such as Understanding VLAN Design, Configuring VLANs for IP Phones, DHCP, Automatic VLAN Assignment, QoS Design, Configuring LAN & WAN QoS, AutoQoS, Port Security and MTU Considerations.

Environment: ST14.2 and earlier – Mitel Connect ONSITE 1.X

Abstract

This application note discusses the use of VLAN's, DHCP scopes and Quality of Service among other data networking best practices in conjunction with our UC Voice over IP versions ST14.2 (and earlier) and Mitel Connect ONSITE 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

What Data Network Manufacturers are supported?

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

What are the Data Network Equipment minimum requirements for a Mitel Connect deployment?

1. A ‘managed’ switch or router with GUI or CLI administrative capabilities to configure the networking device
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 VLAN creation 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. Optional DHCP server which can configure option 156 with all necessary tags

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

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 ST 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.

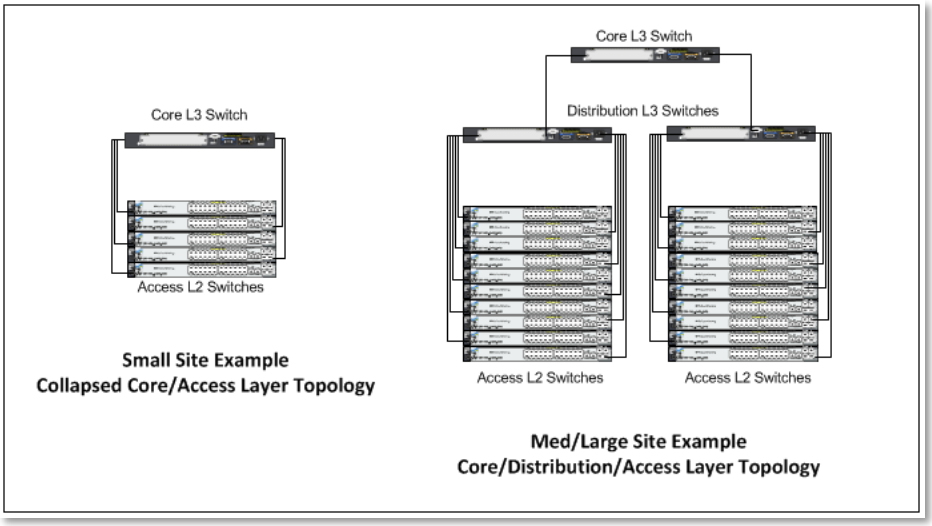

Figure 2

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.

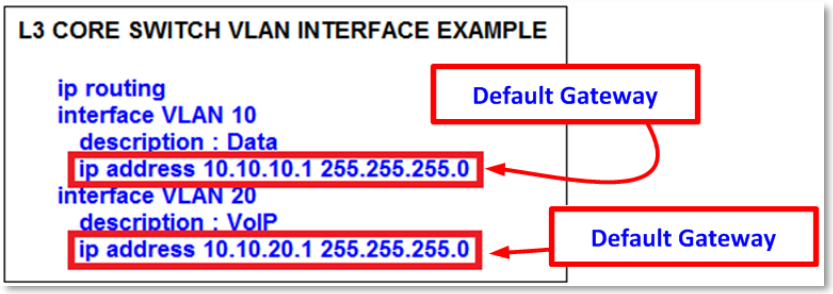

Figure 3

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.

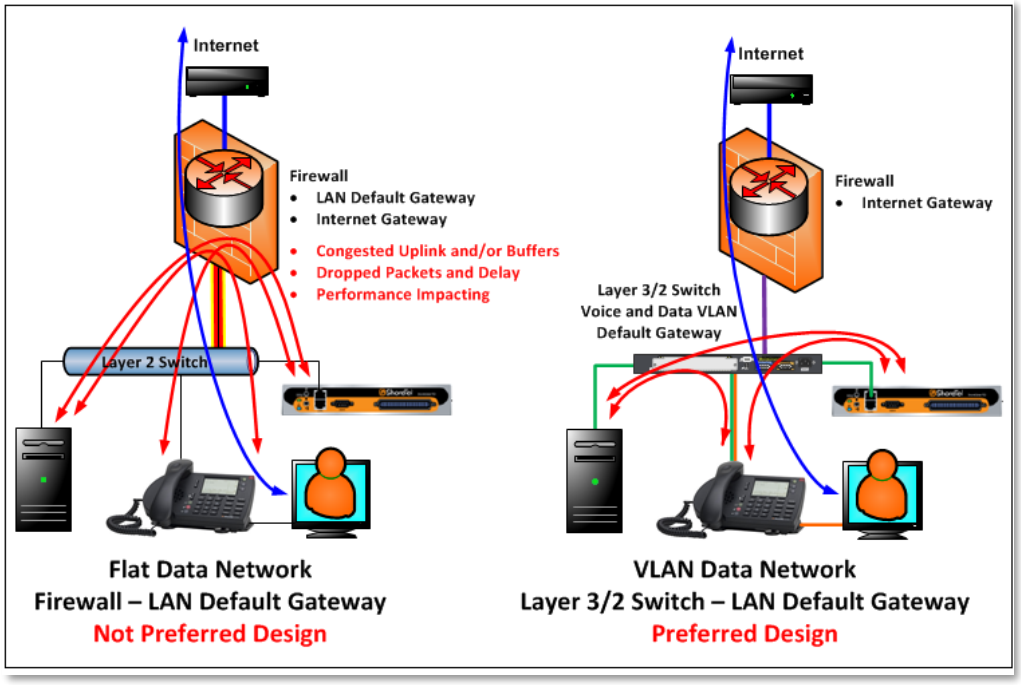

Figure 4

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 (shown above in Figure 4 as the purple link in the preferred design. The green and orange links also shown represent the voice and data VLANs respectively).

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 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 and Mitel. 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.

In summary, 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 ONSITE 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 ST 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.
- If expanding an existing VLAN subnet, change subnet mask on all devices on the subnet.

Configuring VLANs for IP Phones

Piggy-back the PC to the IP Phone

IP phones are a specialized device on the data network and have capabilities and requirements that need to be considered when designing the data network. For example, to help better utilize port capacity on data switches, a PC 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.

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. 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.

For further discussion of 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 sections below, Configuring *Automatic IP Phone VLAN Assignment - DHCP and Configuring Automatic IP Phone VLAN Assignment - LLDP-MED.*

Telecommuters

Telecommuters that work remotely with a physical IP Phone that supports a VPN client built into the phone (e.g. IP655, IP565g, IP560g and IP230g) can connect their phone's network port to their home office router (i.e. DSL or Cable Modem Router's LAN switch ports) and connect their PC or laptop to their phone's PC access port on the back of the IP phone just like in the office. The phone uses it's built in VPN client to automatically connect securely to a VPN Concentrator located in the customer's corporate network to be able to register their IP phone as if it were in the office. The PC or laptop does not have access to the Voice VLAN that the VPN IP phone uses with its VPN client. The phone connected PC or laptop 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.

Check with your Mitel administrator for the initial setup configuration on the IP Phone's VPN client to connect to your corporate VPN Concentrator and Mitel Connect ONSITE system. Also, new to Mitel Connect ONSITE is an Edge Gateway with RAST for VPN-less remote 400-series SIP IP Phones.

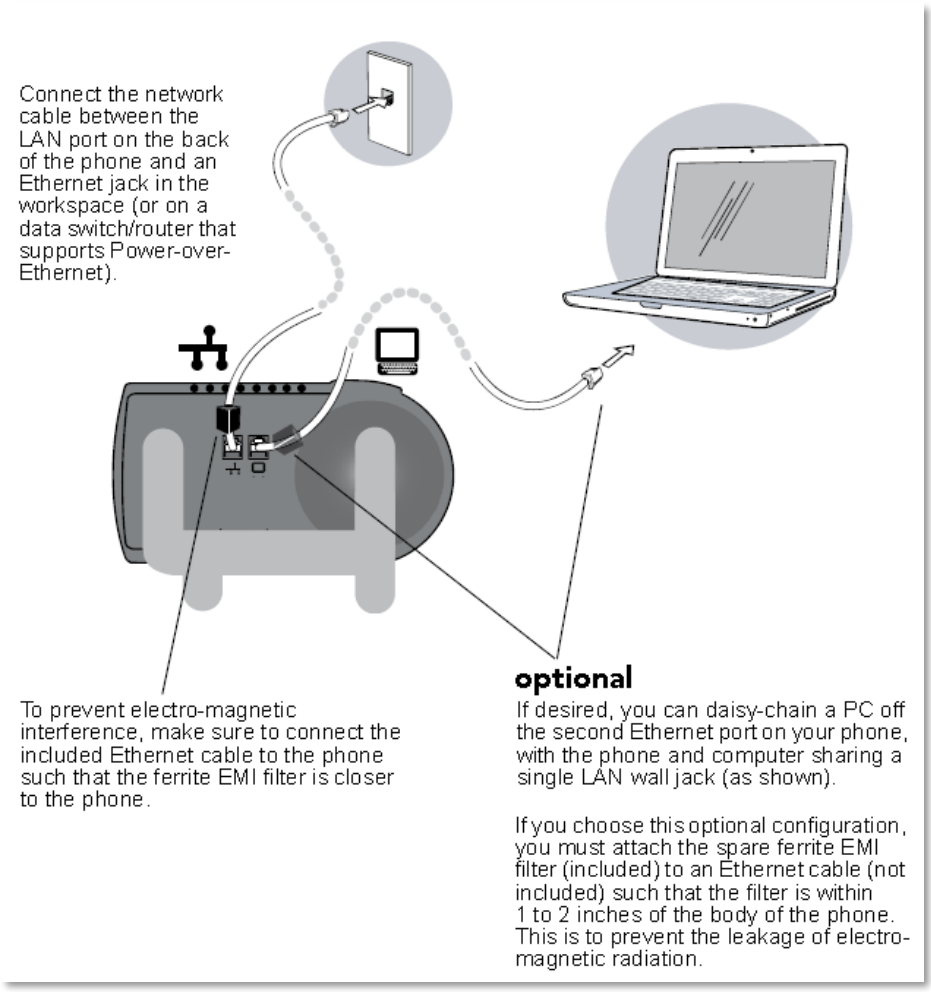

Figure 5

Figure 5 above demonstrates the physical connection of a PC connected to an IP phone in turn connected to the network connection on a single data switch access port.

How to configure the Voice and Data VLANs one the same data port

Figure 6 below demonstrates a Cisco example of how to configure the *voice* VLAN feature on the data switch access port to support both Voice and Data VLANs for each IP phone. Figure 6 below also shows the *access* port configuration when the Voice VLAN is the only VLAN (i.e. untagged VLAN) applied to the port for dedicated ST devices such as voice switches (e.g. SG-90, SG-220T1, SG-T1K, SG-90V, etc.), servers (e.g. HQ, DVS, ECC, etc.) and standalone IP phones.

IMPORTANT TIP: If the Voice VLAN feature (switchport voice) is inadvertently applied to any stand-alone ST voice switch or server e.g. switchport voice vlan xx without the corresponding data VLAN switchport access configured, the ST devices may not be able to route to other VLANs on the data network (as shown below in Figure 6). DO NOT daisy chain multiple PC's or an unmanaged switch or hub to an IP Phone's network port.

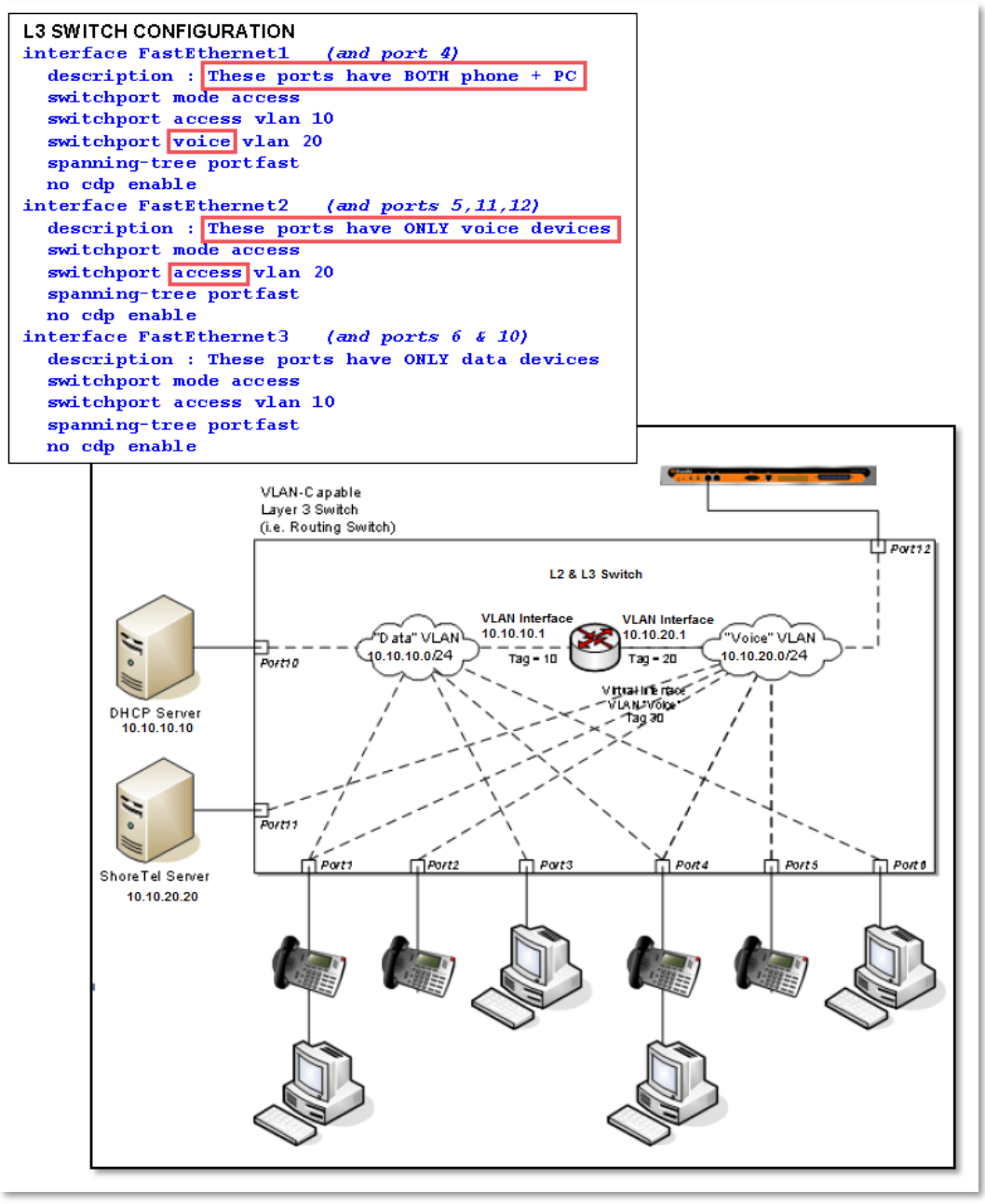

Figure 6

The different port configuration examples above include the following two commands on each Fast Ethernet port when ST 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 ST phones, voice switches or servers. 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.

Configuring DHCP for IP Phones

Typically, IP phones and PCs get their assigned IP address and other networking configuration information dynamically from a network DHCP server. This saves administrators a considerable amount of work from having to manually configure every IP phone or PC on their data network individually, especially when network parameters change across the entire network environment. DHCP packets are broadcast packets and by design are not transmitted beyond the layer-3 boundary of the VLAN that the DHCP request originated. If there is only one DHCP server and there are multiple VLANs, DHCP broadcast packets will not be able to reach the DHCP server on a different VLAN and will fail. Therefore, all foreign VLANs to the DHCP server VLAN need to have an *ip helper-address* statement included in each VLAN configuration on all L3 switches where VLAN interfaces are configured with an IP address (i.e. default gateway) in order to forward all DHCP requests to the DHCP server IP address. The DHCP server can be configured on many different vendor's switches, routers or servers. Mitel doesn't recommend any specific vendor or platform over another as long as the selected DHCP platform can assign an IP address, subnet mask, default gateway, DNS server(s), network time server(s), and a Mitel "vendor-specific" DHCP option (i.e. Option 156) with the required parameters. See Figure 7 below for a Cisco configuration example of the *ip helper-address* relay agent command. Most switch manufacturers' ip helper-address commands are very similar and basically work the same. The specific IP address targeted in the ip helper-address relay agent command will always be the IP address of the DHCP server handling DHCP requests for the given VLAN. Some data networks may have multiple DHCP servers but it is critical that no more than one DHCP server has one DHCP scope built for a given VLAN.

> IMPORTANT TIP: When multiple DHCP servers are configured to distribute the same IP address DHCP Scope (i.e. range) for a given VLAN, many issues with the DHCP scope leases will occur.

```
L3 CORE CISCO SWITCH DHCP HELPER EXAMPLE
#
interface VLAN20
  description : VoIP
  ip address 10.10.20.1 255.255.255.0
  ip helper-address 10.10.10.10
```

Figure 7

Figures 8, 9 and 10 demonstrate the configuration examples on how to simply build the Voice VLAN DHCP Scope in a Cisco L3 Switch, Microsoft Domain Controller or Unix DHCP Server respectively. In all examples, the Voice DHCP Scope contains the Address Pool and Scope Options for IP phones. Cisco defines the address pool from the given network subnet (i.e. network 10.10.20.0 255.255.255.0 which blocks out 254 assignable IP addresses - 10.10.20.1 thru 10.10.20.254) then specifies which part of that range to exclude from the address pool (i.e. ip dhcp exclude-address 10.10.20.1 10.10.20.99) which results in an DHCP Address Pool of 10.10.20.100 thru 10.10.20.254 for distribution to the IP phones. Microsoft takes the opposite approach. In this case, the DHCP Scope also contains the given network subnet like the Cisco example but instead of specifying what to exclude, Microsoft specifies the address range to include for distribution to the IP phones. The Unix Server DHCP configuration looks similar to the HP and Cisco example but the address pool inclusion typically works like the Microsoft example.

IMPORTANT TIP: Ensure that a DHCP server is connected to a data switch port with only one untagged VLAN assigned and not connected to a data switch port with a multiple tagged VLAN(s), which will cause DHCP assignment issues.

NOTE**:** The *ftpServers* parameter is provided for compatibility with sites running ST MGCP phones. 400-Series IP phones use HTTP to download configuration files from servers specified in the *ftpServers* parameter. For new installations, the *configServers* parameter is recommended over the *ftpServers* parameter.

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.

```
L3 HP PROCURVE 2920 SWITCH DHCP CONFIGURATION EXAMPLE

dhcp-server pool "ShoreTel_phone"
    authoritative
    network 10.10.20.0 255.255.255.0
    default-router "10.10.20.1”
    dns-server "10.10.10.10,10.10.10.11”
    option 156 ascii ftpservers=10.10.20.20, layer2tagging=1, vlanid=20
    option 4 ip 10.10.10.10
    range 10.10.20.100 10.10.10.254

L3 CORE CISCO SWITCH DHCP CONFIGURATION EXAMPLE

ip dhcp excluded-address 10.10.20.1 10.10.20.99
!
ip dhcp pool ShoreTel_phone
   network 10.10.20.0 255.255.255.0
   default-router 10.10.20.1
   dns-server 10.10.10.10 10.10.10.11
   option 156 ascii “ftpservers=10.10.20.20, layer2tagging=1, vlanid=20”
   option 4 ip 10.10.10.10
   lease infinite
```

Figure 8

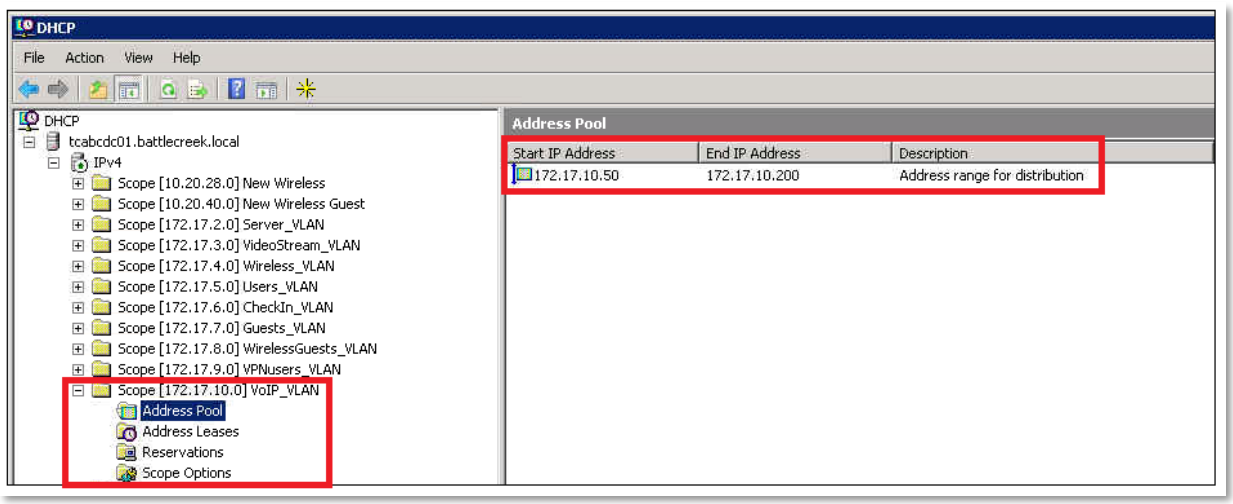

Figure 9 (part 1)

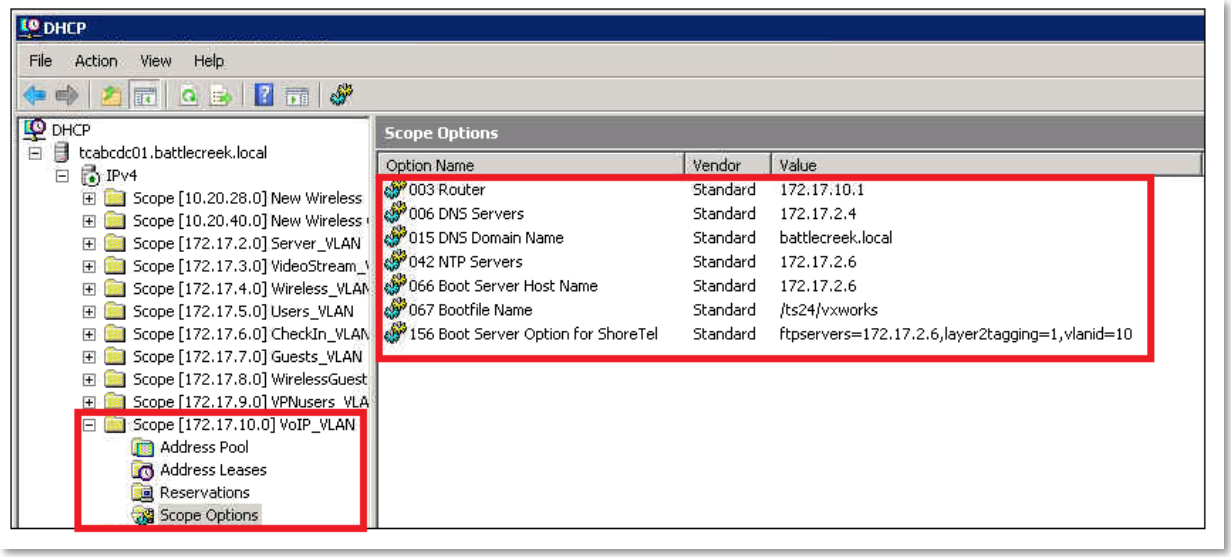

Figure 9 (part 2)

UNIX SERVER DHCP CONFIGURATION EXAMPLE

```
# Example Unix /etc/dhcpd.conf for ShoreTel VoIP
default-lease-time 600;
max-lease-time 7200;
option ntp-servers 10.10.10.10;
option routers 10.10.20.1;
option domain-name-servers 10.10.10.10, 10.10.10.11;
option shoretel-server code 156 = string;
option shoretel-server "ftpservers=10.10.20.20, country=1, language=1, layer2tagging=1, vlanid=20";

subnet 10.10.20.0 netmask 255.255.255.0 {
    range 10.10.20.100 10.10.20.254;
}
```

Figure 10

In all of the DHCP Scope configuration examples, the importance of excluding a relatively small portion of the Voice VLAN from the DHCP Address Pool is to allow a range of static IP addresses in the same VLAN that can be permanently assigned and never given to an IP phone dynamically. The static IP addresses are intended for ST voice switches, servers or other important devices on the same VLAN.

To properly calculate the Voice VLAN size and Voice DHCP Address Pool at a given site:

1. Add the quantity of required IP addresses plus projected growth together.
2. Take the previous result and double it.
3. Round up to the closest subnet size.
4. From the calculated subnet size, calculate the needed quantity of static IP addresses plus anticipated growth, double it and round to the nearest quantity of 10 or 100 as appropriate.
5. Subtract the static IP address quantity from the beginning or end of the useable IP address range of the VLAN.
6. The result is the Voice DHCP Address Pool for the Voice VLAN at the given site.
7. Repeat steps 1-6 for each additional VoIP site.

The IP Phones have a built-in configuration to seek the server's address with the Vendor Specific DHCP option 156. If this option is not available, IP phones use option 66. The specific parameters in option 156 are sent directly to each phone to automatically configure the phone that would otherwise need to be configured manually with the phone's keypad to connect to the Mitel Connect ONSITE HQ server (or local DVS in a multi-site deployment) and download phone firmware and other configuration files.

Also, you can have two ftp servers passed to the IP phones using option 156. This is especially important when using Doubletake redundancy for the Director server or a local DVS. For example:

One FTP Server (HQ Server)

(option 156) ftpServers= 10.10.20.20, layer2tagging=1,vlanId=20

Two FTP Servers (HQ Server with Doubletake Redundant Server or local DVS)

(option 156) ftpServers= "10.10.20.20,10.10.20.21", layer2tagging=1,vlanId=20

The maximum length of the supplied string is 160 characters.

For additional information, refer to the Mitel Connect Planning and Installation Guide for details under the section Configuring DHCP for IP Phones.

In some cases where DHCP isn't working properly with the full complement of parameters specified for Option 156, switch to the minimum amount of data that is required for option 156 to function;

(option 156) ftpServers=IP.Address.of.ST.Server (e.g. ftpServers= 10.10.20.20)

In order for any IP phone with a piggy-back PC to determine which VLAN (i.e. Voice or Data VLAN) on the connected data switch access port to boot and send its DHCP request, a mechanism has to be put in place to make the determination for the IP phone. There are 3 mechanisms used by our IP phones to automatically assign the appropriate DHCP site specific options during the phone's boot process;

1. IP Phone custom configuration file (i.e. refer to the Mitel Connect Maintenance Guide, section 6.4.4., *DHCP Site Specific Options*).
2. DHCP Server
3. LLDP-MED

Using the DHCP Server mechanism, the IP phone boots twice; first on the untagged data VLAN and after being redirected by DHCP, a second time on the Voice VLAN. Using the LLDP-MED mechanism, the IP phone boots only once for its Voice VLAN IP address. Certain environments favor one automatic assignment mechanism over the other. The following sections explain 2 mechanisms in detail to find which one works best on your network.

Configuring Automatic IP Phone VLAN Assignment - DHCP

The Automatic VLAN Assignment feature using DHCP is not configured through Mitel Connect Director. Configuration changes are performed on the appropriate DHCP Server. In the previous section, the DHCP Scope and related IP phone option 156 were configured properly for the Voice VLAN. Without a redirecting mechanism in the DHCP Server, the IP phone will always use the untagged Data VLAN to contact the DHCP Server during the boot process for the Data VLAN DHCP Scope Options and not find the Voice VLAN DHCP Scope Option 156. The DHCP Server however can be configured to redirect the DHCP request in the example below by adding a redirecting Option 156 on the Data VLAN 10 DHCP Scope using the VLAN ID field highlighted in red which is pointed to the configured Voice VLAN 20 DHCP Scope:

Data VLAN 10 DHCP Scope

(option 156) ftpServers=10.10.20.20,layer2tagging=1,vlanid=20

Voice VLAN 20 DHCP Scope

(option 156) ftpServers= 10.10.20.20, layer2tagging=1,vlanId=20

The Automatic VLAN Assignment using DHCP during the IP Phone standard boot process is as follows:

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

For more detailed information on configuring Option 156 on your DHCP server, refer to article 3031 or the appropriate Mitel Planning and Installation Guide for your system under sections *Configuring DHCP for ShoreTel IP Phones* and *Configuring Automatic VLAN Assignment via DHCP*.

Configuring Automatic IP Phone VLAN Assignment – LLDP-MED

LLDP (IEEE 802.1AB) is a vendor agnostic Layer-2 protocol designed to be used by network devices for advertising their identity, capabilities, and neighbors on an IEEE 802 Ethernet LAN. LLDP performs similar functions as several proprietary protocols such as the Cisco Discovery Protocol (CDP), Extreme Discovery Protocol, Nortel Discovery Protocol and Microsoft's Link Layer Topology Discovery. An enhancement to LLDP is LLDP-MED, Link Layer Discovery Protocol-Media Endpoint Discovery. For further information on LLDP-MED, refer to the appropriate Mitel System Administration Guide for your system under section *LLDP-MED and IEEE 802.1x Support*. 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 LLDP enabled 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 11 below).

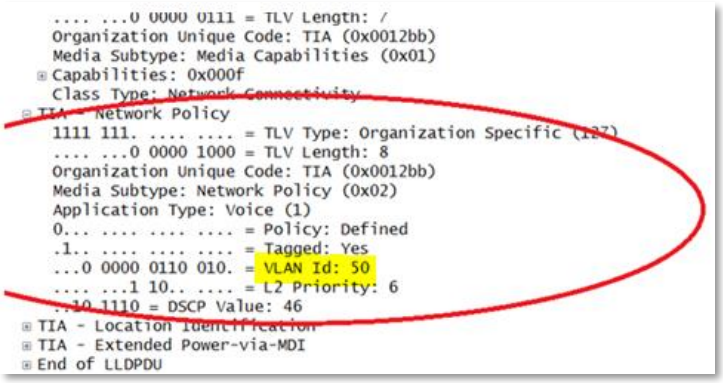

Figure 11

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.

To see the current phone firmware build version:

Press "<Mute> + INFO (4636) #" on the IP phone keypad to sequence through all info.

LLDP vs. Director DSCP IP Phone Assignment Precedence

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.

IP 400 Series Phones"

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

All other phone series:

- LLDP OFF**:** Director DSCP used for RTP and Signaling
- LLDP-MED TLV ON with a default of 0**:** Director DSCP used for RTP and Signaling
- LLDP-MED TLV ON with a non-zero value**:** Last setting wins, LLDP first, Director (config file) last

For more detailed information on configuring and troubleshooting Automatic VLAN assignment via LLDP please refer to the Knowledge Base article 3489 and the Mitel Connect System Administration Guide. For configuring base LLDP functionality for Juniper, refer to Juniper Knowledge Base article KB11308.

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, ST 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.

ST 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 ShoreTel signaling QoS traffic marking standard. It will still be supported during the transition to CS3.

The ST 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. ST 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 12

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

In addition to voice and video media ports, Mitel also uses a number of TCP and UDP ports for multiple signalling protocols related to call control and system control**.**

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

The TCP and UDP ports shown in Figure 13 below are listed by ST release to ensure the right QoS policies are created on your data network for the version of Mitel installed. Prior to ST13.1 and ST14.1, all ST UC systems set DSCP (i.e. DiffServ) fields for call control (i.e. signaling) traffic to zero by default. As a result call control traffic is treated as low priority by the network elements, which can result in latency and packet drops. This results in unpredictable call states under low or even medium levels of network congestion if not marked on the data network accordingly. Starting with ST13.1 and ST14.1, the appropriate signaling ports are self-marked with DSCP AF31 so data network administrators could simply trust and map the traffic appropriately. While Mitel has begun the transition to self-mark signaling traffic from AF31 to CS3, only new installations beginning with Mitel Connect ONSITE will automatically self-mark signaling traffic as CS3. All others, including upgrades to Connect, will have to manually change the default signaling traffic DSCP value from AF31 to CS3 in Director. Ensure that any other policy or configuration on the data network is simultaneously changed from AF31 to CS3. Figure 13 below shows the self-marking port map for each ST release.

ShoreTel Port Usage - UDP Signalling VoIP Traffic (CS3)	ShoreTel 13	ShoreTel 14	ShoreTel Connect
UDP 2427: MGCP Call Control	α	α	α
UDP 2727: MGCP Call Control	α	α	α
UDP 5060: SIP	α	α	α
UDP 5440: Location Service (LSP)	α	α	α
UDP 5441: Call Control (ShoreSIP)	α	α	α
UDP 5442: Switch Call Control – DRS	α	α	α
UDP 5443: Bandwidth Manager (BWM)	α	α	α
UDP 5445: Admission Control (ADM)	α	α	α
UDP 5446: Switch Call Control – DRS Keepalive	α	α	α
UDP 5450: SA-100/400 CMCA Web Share - PING Sync	α	α	α
ShoreTel Port Usage - TCP Signalling VoIP Traffic (CS3)	**ShoreTel 13**	**ShoreTel 14**	**ShoreTel Connect**
TCP 5060: SIP (and all related/accepted TCP connections UDP 1024-65535 RTP)	α	α	α
TCP 5061: SIPS Call Control		α	α
TCP 5430: ShoreTAPI (DTAS to remote TMS)	α	α	α
TCP 5447: Client Application Server i.e. CAS (SSL)	α	α	α
TCP 5448: IP Phone to CAS over https		α	α
TCP 5452: TMS to Switch NCC	α	α	α
ShoreTel Port Usage - TCP & UDP Signalling VoIP Traffic (CS3)	**ShoreTel 13**	**ShoreTel 14**	**ShoreTel Connect**
TCP & UDP 31453: Used by ShoreTel ECC for Client Server Communication	√**	√**	
TCP 31451-31471: Used by ShoreTel ECC for Client Server Communication			√**
ShoreTel Port Usage - RTP VoIP Traffic (EF)	**ShoreTel 13**	**ShoreTel 14**	**ShoreTel Connect**
UDP 10000 – 10550: Default Media Port Range, ST Director Configurable	α		
UDP 10000 – 14500: Default Media Port Range, ST Director Configurable		α***	
UDP 10000 – 20000: Default Media Port Range, ST Connect Director Configurable			α
√ ** = All outbound call control traffic from ECC terminates on local DTAS of DVS (via ShoreTapi). In case the local DTAS needs to forward the ECC call control traffic to the remote TMS, the DTAS will take care of marking the call control traffic with the configured DSCP value.			
α = Valid port used in ST release. Required QoS AUTOMATICALLY marked by ShoreTel device or server.			
α*** = Default RTP port range set in Director expanded in ST 14.2 from 10000-10550 to 10000-14500			

Figure 13

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. Also refer to the appendices below for some additional examples.

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.

First, Mitel allows you to set the DSCP values for all voice traffic using the web-based administration tool in Mitel Connect Director. These DSCP settings are used for all Real-Time Protocol (i.e. RTP) packets that are sent from all IP phones and ST voice switches and servers. ST Call Control and Video DSCP self marking values were introduced as of ST13.1 and ST14.1.

In Mitel Connect Director, navigate to *Call Control Options* and verify the values for *DiffServ /ToS Byte* under *Voice Encoding and Quality of Service* as well as *Call Control Quality of Service* and *Video Quality of Service* settings as shown below in Figure 14.

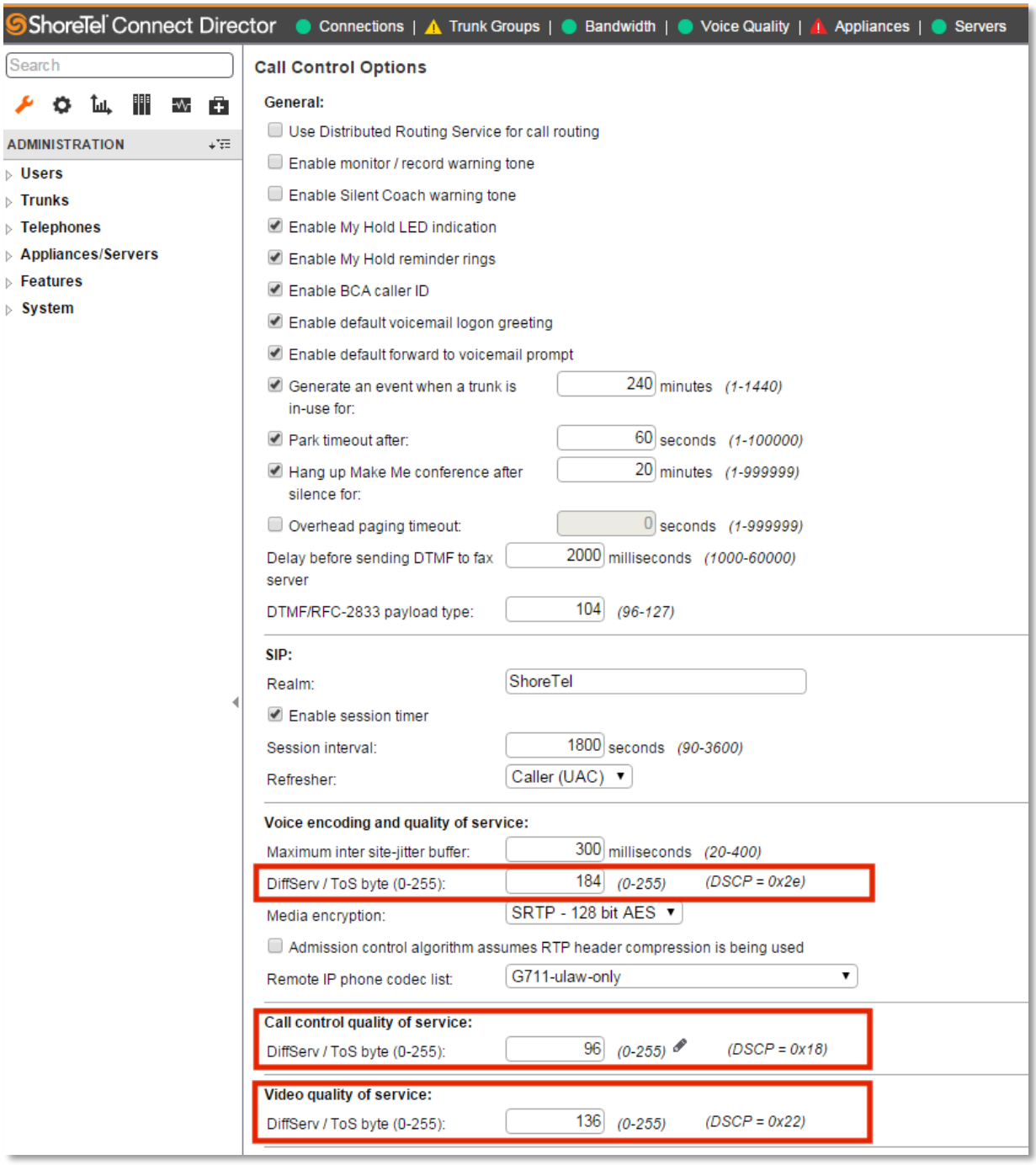

Figure 14

The recommended setting for *DiffServ/ToS Byte* is decimal 184 which equates to the Expedite Forwarding DSCP setting (i.e. EF). The recommended setting for *Call Control Quality of Service* is decimal 96 which equates to the Class Selector 3 or DSCP 24 setting (i.e. CS3). *Video Quality of Service* is set to decimal 136 which equates to Assured Forwarding 41 DSCP setting (i.e. AF41). If you change these values, change them early in your Mitel Connect deployment as it can require a one-time reboot depending on the release version of all ST servers, ST voice switches and IP Phones in the system to take effect.

The RTP port usage has also changed. In ST12.3, the default RTP port range was UDP ports 10000-10550. With version ST14.2, the default range was expanded to 10000-14500. Now with Mitel Connect ONSITE, the port range has been expanded to UDP 10000-20000 as shown in the figure below. Accounting for these ranges is imporant when building your QoS configuration.

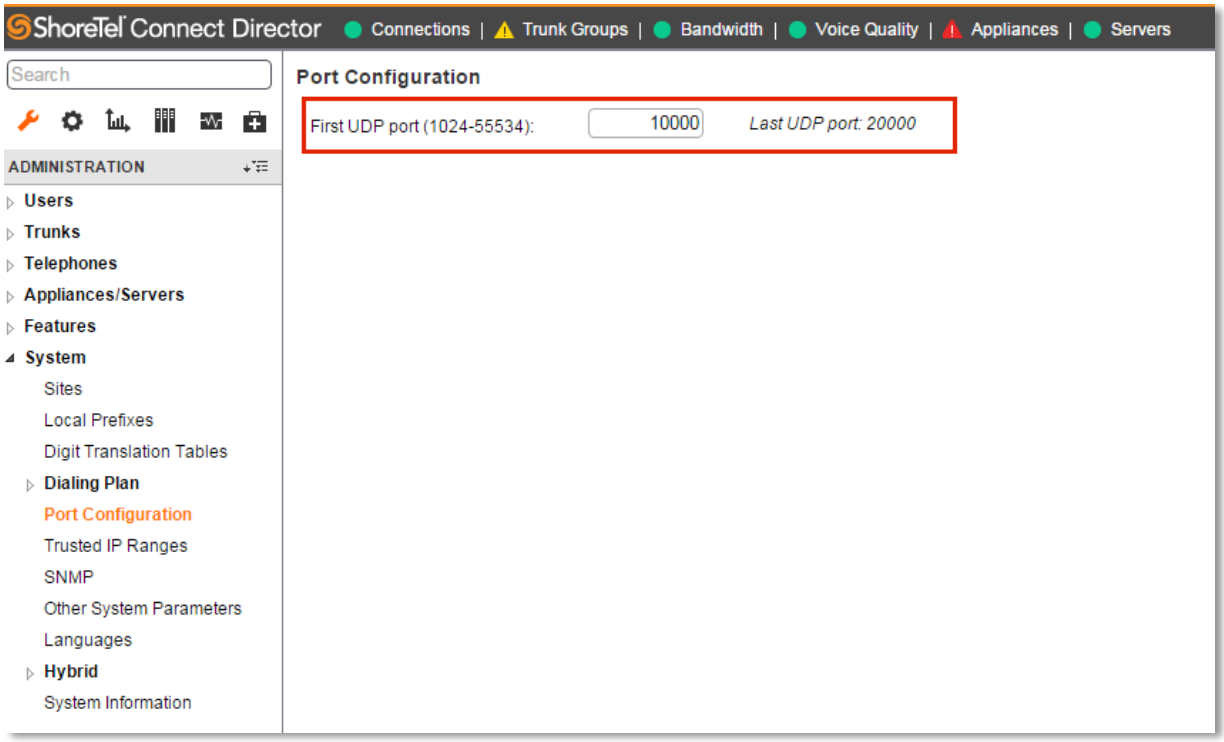

Figure 15

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 ONSITE 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. Figure 16 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 16

IMPORTANT TIP: The use of AutoQos as shown in the figure above works best with ST signaling DSCP default value changed from AF31 to CS3 in Mitel Connect Director. While AF31 will also work, CS3 is generally preferred by the AutoQoS configuration since it mirrors Cisco UC VoIP signaling self-marking recommendations.

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
```

Figure 17 (part 1)

```
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 17 (part 2)

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 18

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 19

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 or Low Latency Queuing 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 Mitel 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 Mitel 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.

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 20

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 ST phones as well as voice 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 appropriate commands available to your specific equipment model.

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 the three-part Figure 21 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
```

Figure 21 (part 1)

```
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
```

Figure 21 (part 2)

```
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 21 (part 3)

Configuring DSCP Policy on ST Servers with Windows Server 2008 & 2012

After MS Windows Server 2003, Microsoft no longer supports 3rd party applications (i.e. ST) marking traffic with a DSCP value using an API. The only alternative is to manually build the following QoS-policy. The procedure below details how to setup QoS - DSCP for RPT and signaling traffic on a ST HQ and any DVS servers running on a Windows 2008 or 2012 Server. Perform on each individual Windows 2008/2012 Server used by ST. The instructions below use a local Group Policy Object Editor on the local Windows server but if all of the ST servers are in a domain in their own OU, without inheriting any other group policies, the following policy-based QoS configuration can also be completed at the domain level for all participating ST servers such as HQ, DVS, ECC or any other 3rd party servers running the DVS software such as a Call Recording server. The Policy-based QoS simply marks all outbound VoIP traffic with a specific DSCP value for data networks enabled for QoS.

Configuration Steps

1. Click the Windows Start button and in the program search box type “gpedit.msc” to open the Local Group Policy Editor.

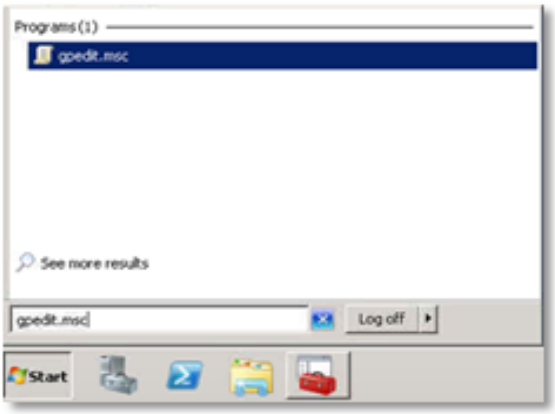

Figure 22

2. From the Local Group Policy, navigate to ‘Policy-based QoS’ under Windows Settings within Computer Configuration.

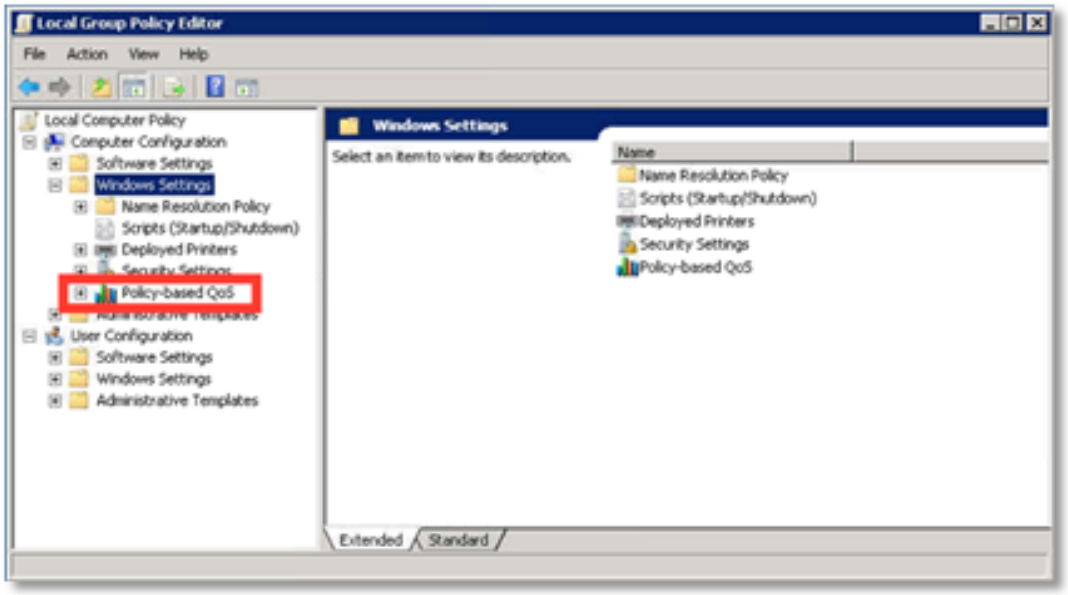

Figure 23

3. Right click policy-based QoS and select Advance QoS Settings then go to the DSCP Marking override tab. Check the Control DSCP marking checkbox and select Allowed and Click OK.

Figure 24

4. Right click ‘Policy-Based QoS’ to create each new policy for each needed UDP and TCP ports specified in Figure 13, for the appropriate ST version. Enter the name of the policy and specify the appropriate DSCP value, RTP - DSCP 46 and Signaling - DSCP 24 as shown in Figure 25 and 26. Make sure this value matches the default DSCP values set in ST Connect Director under Call Control > Options in Figure 14.

Click NEXT.

NOTE: Refer to Figure 12 to convert tfigurehe DSCP value to the format specified in ST Connect Director.

Signaling Example – DSCP 24

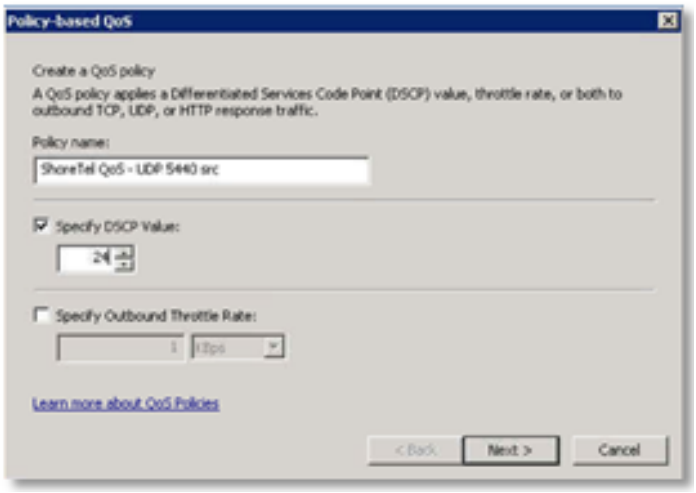

Figure 25

RTP Example – DSCP 46

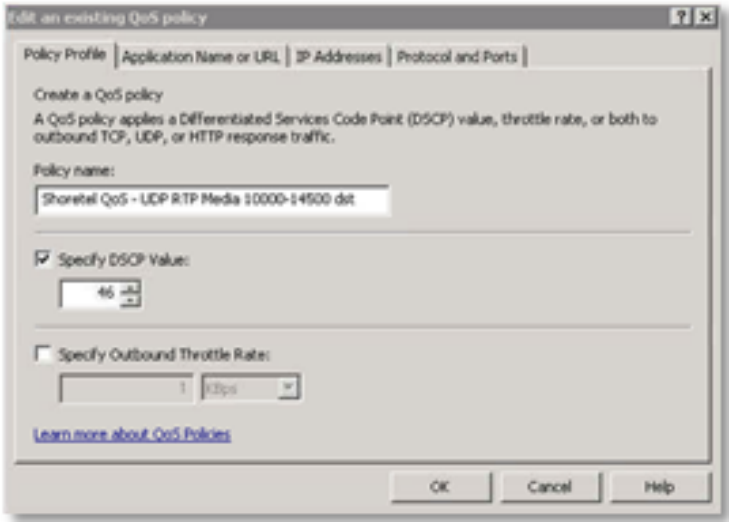

Figure 26

5. Leave the default “All applications” selected.

Click NEXT.

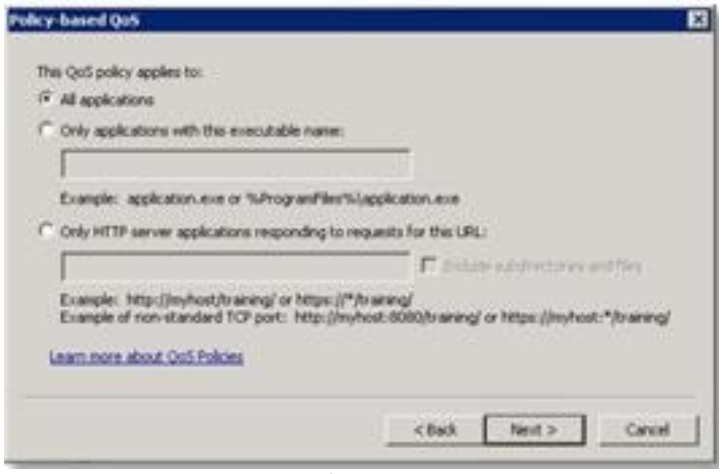

Figure 27

6. Select This QoS policy applies to “Only for the following source IP address or prefix” and enter the IP address with mask of the ST server you are applying the policy to specifically.

Click NEXT

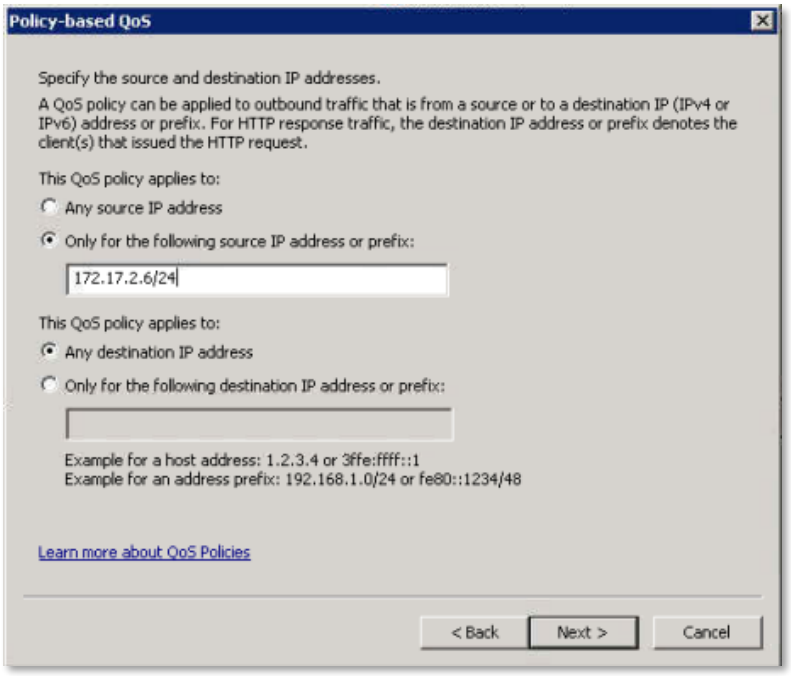

Figure 28

7. Select the protocol and either specify the appropriate source or destination port per policy created.

Click Finish.

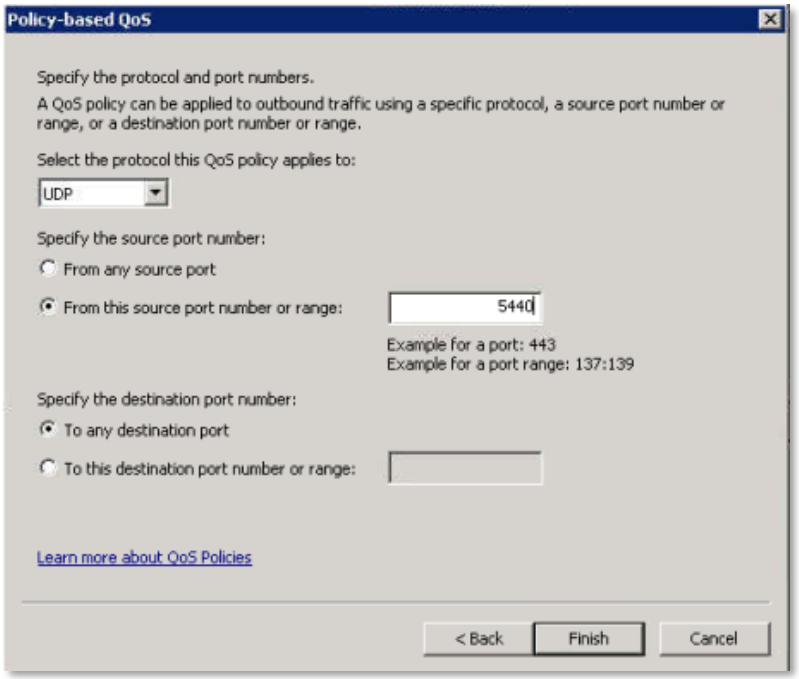

Figure 29

8. Repeat steps 4-7 for each port. The final set of QoS policies should look like the image on the next page.

NOTE: Ports may vary depending on the ST release referenced in Figure 13.

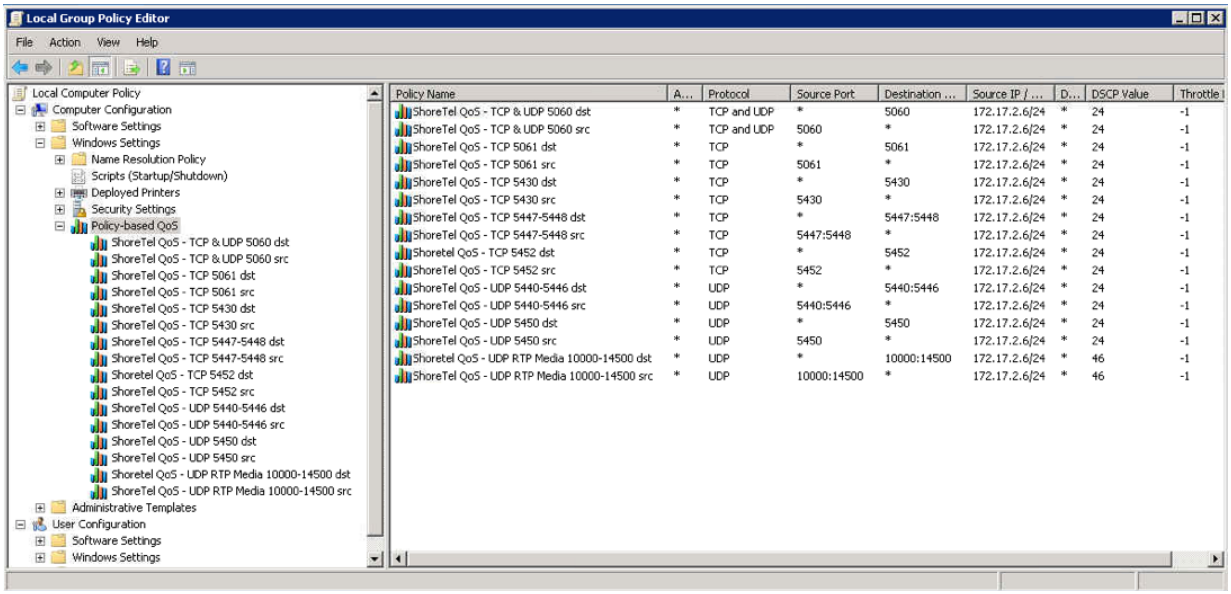

Figure 30

9. Run Wireshark on each ST server for approximately 5-10 minutes and filter on each port used in the policy to verify they are marked accordingly.

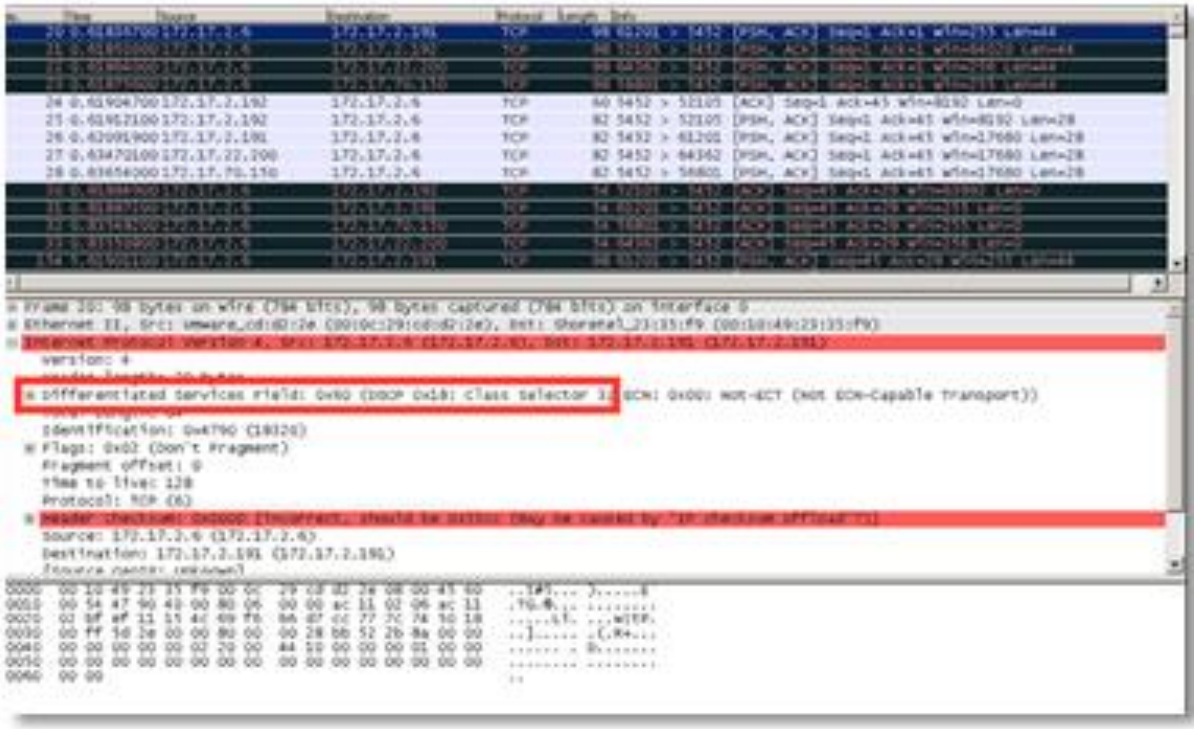

Figure 31

QoS Considerations for SIP Trunking Session Boarder Controller - Ingate

Traffic that routes through a Session Boarder Controller like the Ingate can impact QoS for the duration SIP trunk traffic is on the customer network. The following screen shots quickly show how to enable QoS on the Ingate is used and how to apply to QoS Eth0 and Eth1 interfaces. See bullets below for the following tabs that are configured.

- QoS Classes Tab – Set up QoS Classes for SIP Media and SIP signaling select Type of QoS to Priority Queues.
- QoS Eth0 Tab – Set incoming and outgoing QoS to Active. Ensure SIP Signaling and SIP media are classified as shown in the figures below.
- QoS Eth1 Tab – Set incoming and outgoing QoS to Active. Ensure SIP Signaling and SIP media are classified as shown in the figures below.
- ToS Modification Tab – Set SIP Signaling to DSCP 24 and SIP Media to DSCP 46.

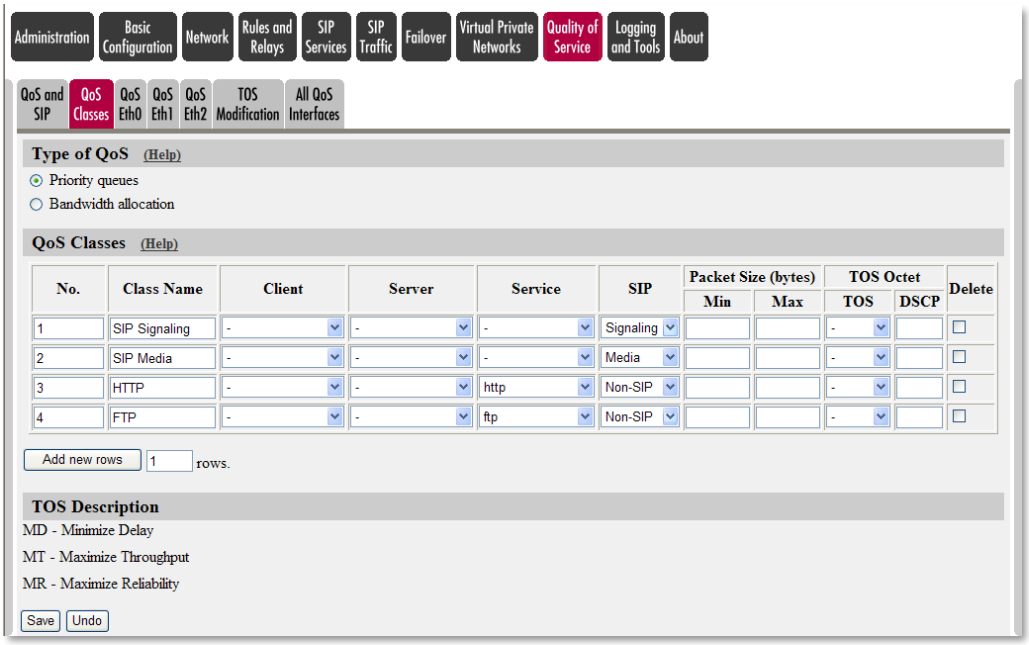

Figure 32

Figure 33

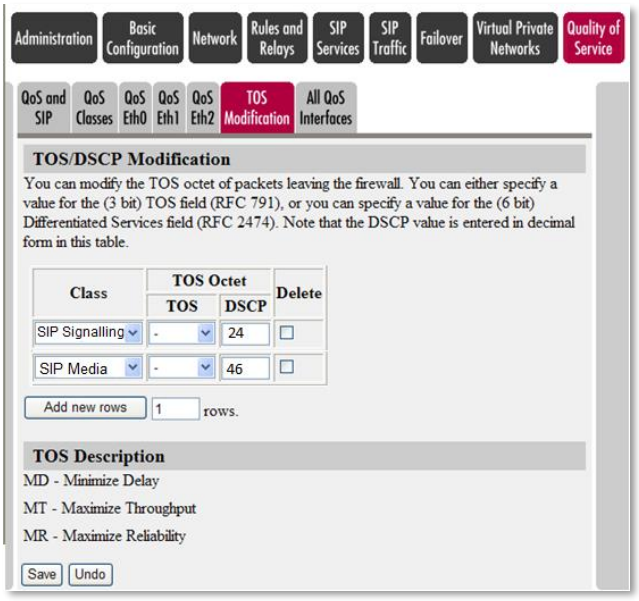

Figure 34

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, an IP 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.

Port Scanning on Network

It is recommended that using any typical port scanners like NMAP, IP Scanner, Nessus, IPS, IDS, etc. exempt all ports and IP's used by all Mitel system equipment. Port scanning any vendors' VoIP equipment is known to cause congestion, resets, packet drops of valid TCP connections and can have many more unforeseen effects that can lead to unexpected behavior in the UC VoIP environment. It is an industry best practice to not scan any UC VoIP equipment and to exempt those ports from scanning to not cause unintended behavior on the specific ST system.

Port Security on Data Switches

When you enable port security on a voice VLAN port, you must set the maximum allowed secure addresses on the port to at least two. When the port is connected to an IP phone, the IP phone requires two MAC addresses: one for the access VLAN and the other for the voice VLAN. Also, you cannot configure static secure MAC addresses in the voice VLAN. Unless port security is a requirement in your network, the best practice is to disable port security for ports connected to VoIP devices or servers.

MTU Considerations for Site to Site Tunnel Connections

While Tunnels for VoIP between sites are not ideal, there are scenarios where a tunnel such as VPN is the only connectivity option to allow VoIP at a remote site. IPsec (and GRE) can add considerable overhead to user packets. This overhead can cause large (possibly larger than the Path Maximum Transmission Unit, PMTU,) IPsec or GRE/IPsec packets to be dropped or fragmented (broken into smaller pieces). An interface MTU is the maximum packet size in bytes that can be transmitted out of an interface. The MTU between two devices over an intervening network is called the *path MTU*. This distinction is important because simply increasing the MTU on one device along the network path will not resolve a MTU issue unless every device in the path is increased or decreased to accommodate the MTU. Mitel supports MTU Discovery; however, if ICMP is being blocked along the path for any reason so that the MTU Discovery negotiation isn't communicated back to the other end or MTU Discovery is not supported anywhere along the same path, MTU Discovery won't work properly.

Mitel's default payload size for all of its VoIP protocols is 1400 bytes as of **ST11.2 Build 16.43.8500 or greater (does not include ST12.0 and ST12.1 builds)** and **ST 12.2 Build 17.41.7001 or greater** and if running ST Distributed Routing Service (DRS), **ST11.2 Build 16.43.8501 or greater** and **ST 12.2 Build 17.41.7003 or greater.** This payload size will generally allow Mitel to operate seamlessly over Virtual Private Networks (VPNs) and other topologies using common tunneling protocols. In some instances when a provider or VPN tunnel configuration inadvertently sets the path MTU too low, ideally, the WAN path MTU needs to be changed along the appropriate links to the appropriate size above the Mitel default payload size plus overhead (typically 28 bytes for IP/ICMP headers) up to 1500 bytes. If the MTU cannot be changed, worst case, the resolution must be to configure the network to *IGNORE* the Do Not Fragment (DNF) bit and allow Fragmentation and Reassembly by the VPN/Tunnel devices. While fragmentation causes some performance degradation on the receiving IPsec VPN gateway and a reduction in packet throughput, it is better in most cases than dropping larger than the allowed PMTU packets all together that violate the set PMTU so VoIP communication does not function properly. Newer ST switches set the Do Not Fragment bit by default. A network using IPsec tunnels as VPN transport between sites will drop ST packets unless they are configured to allow fragmentation over the VPN. For details on how to set the proper path MTU, fragmentation and drop configurations, please consult your firewall or router/switch manufacturer's documentation. For any other MTU considerations with Mitel, please contact Mitel TAC for further assistance.

To quickly assess a WAN path's PMTU, execute a series of ping tests using the following command at a Window's CDM prompt from the remote end of the WAN tunnel connection;

ping <HQ server IP> -f -l XXXX (e.g. ping <HQ server IP> -f -l 1400), where XXXX is the packet size.

Begin increasing or decreasing the packet size from this number in small increments until you find the largest allowable size that does not fragment and successfully pings.

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 the Mitel 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 13 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 Mitel traffic on the data network to ensure individual segments were not missed.

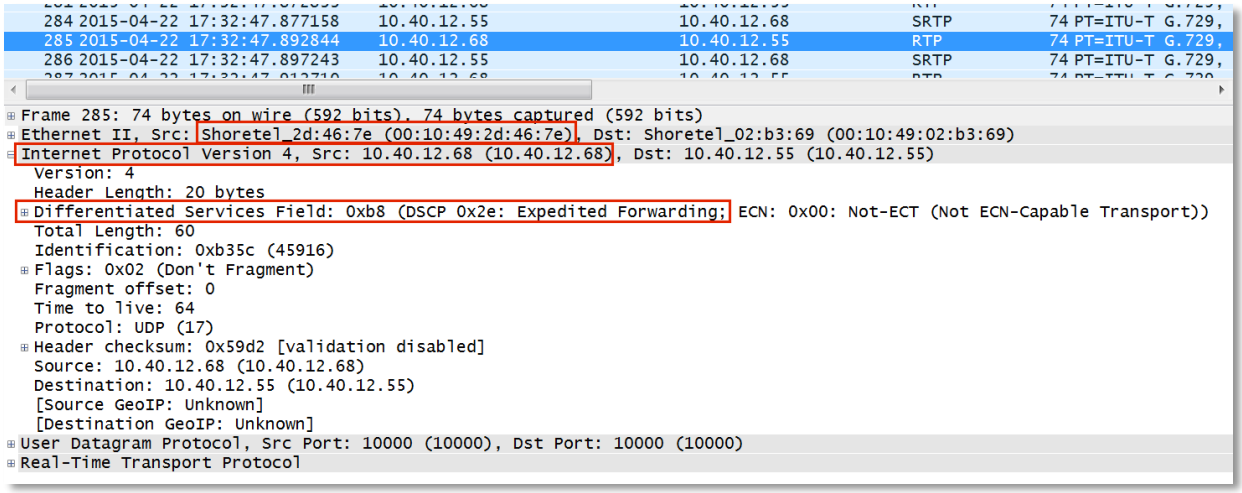

Figure 35

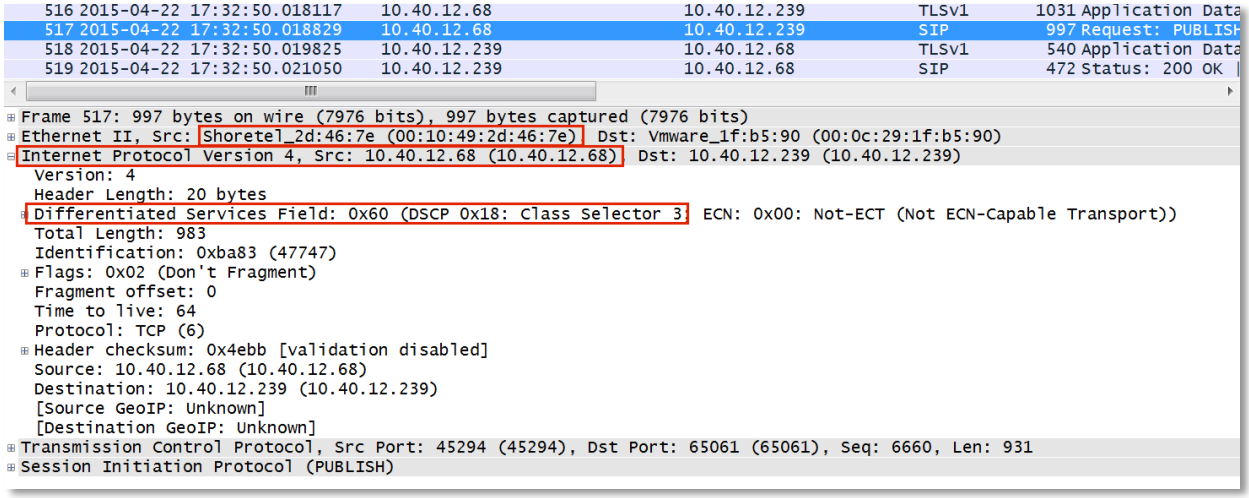

Figure 36

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

ShoreTel Guides and References:

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

ShoreTel Planning and Installation Guide, Chapter 9: “Configuring DHCP for ShoreTel IP Phones”

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

Appendix A: Avaya CoS/QoS Config Examples

Avaya ERS4500 – Enterprise Device Manager

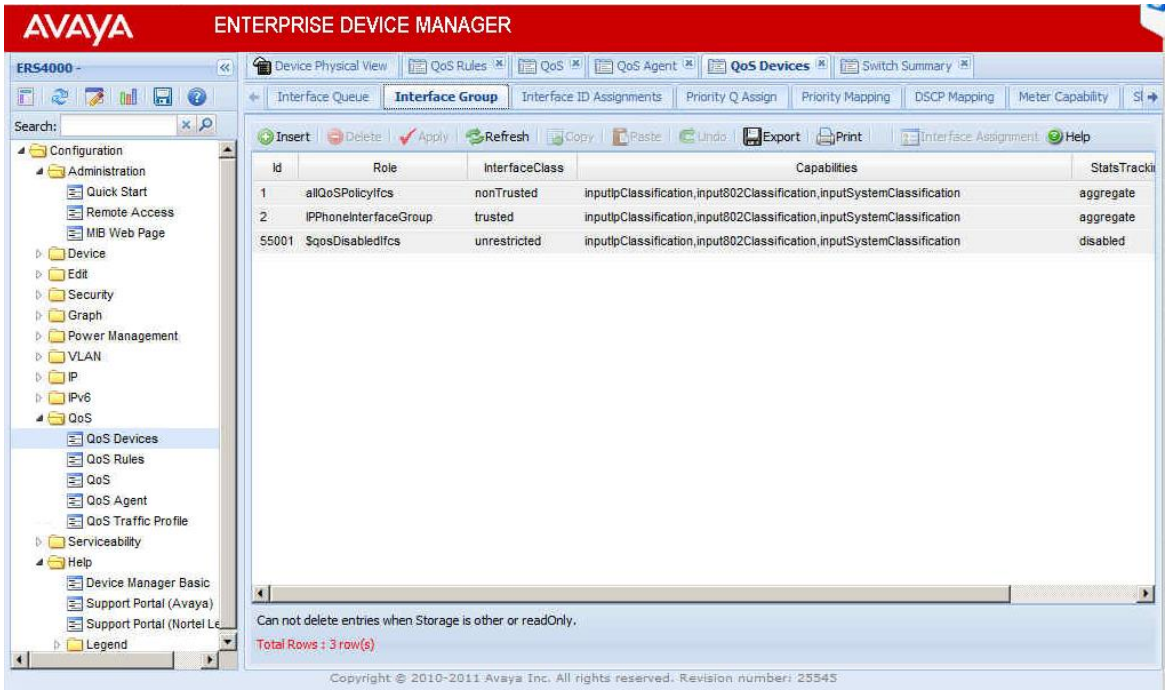

Figure A1

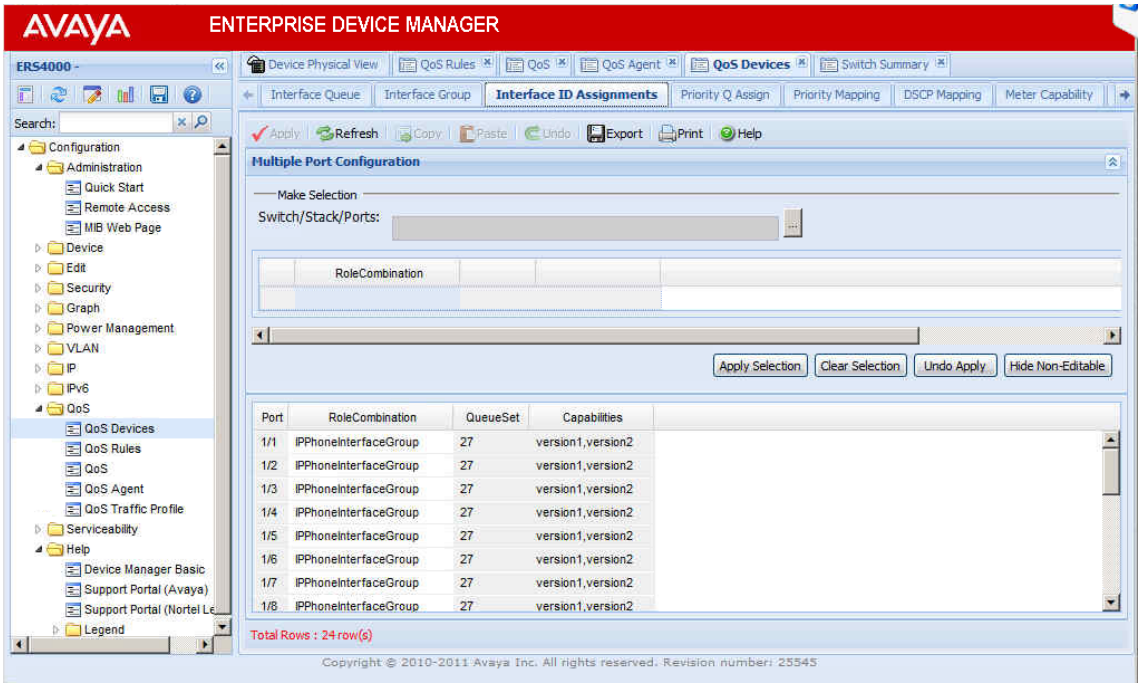

Figure A2

NOTE: Requires a reboot to change default QueueSet. Only 8 of 32 used. Chose 3, displays 27 which are same. Also Change default Queue Config (QueueSet) and Packet Buffer Allocation (Maximum).

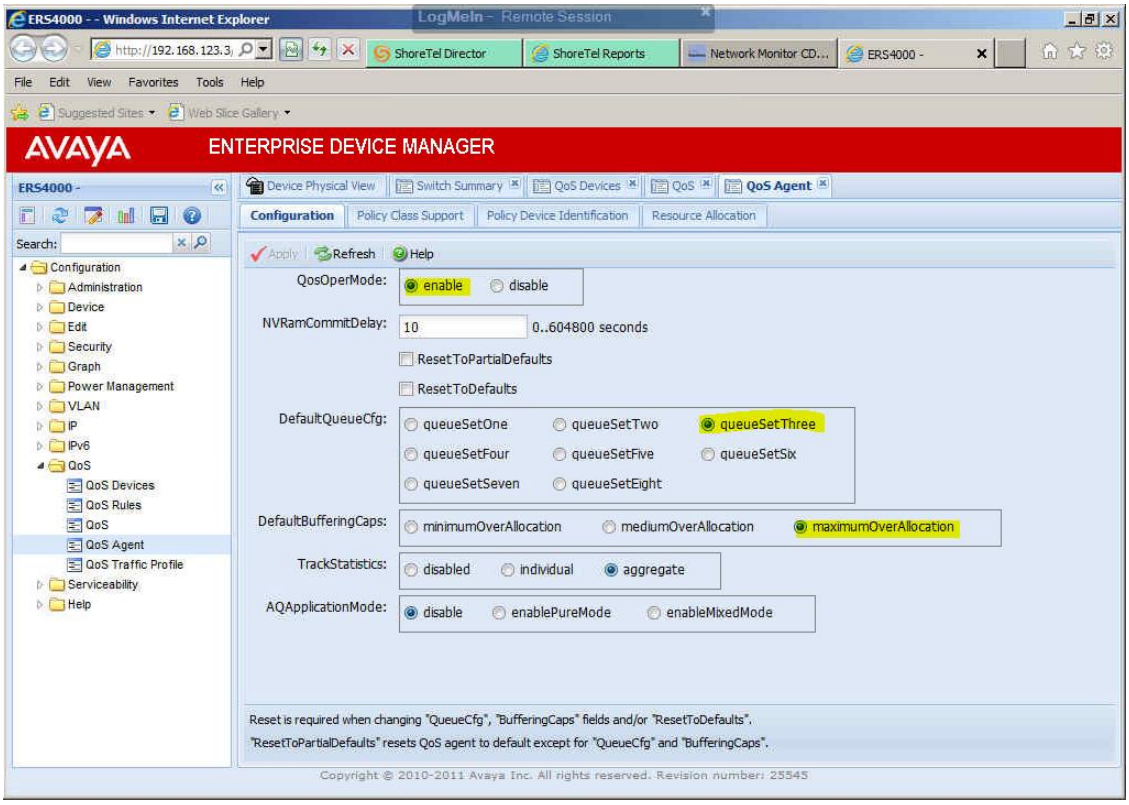

Figure A3

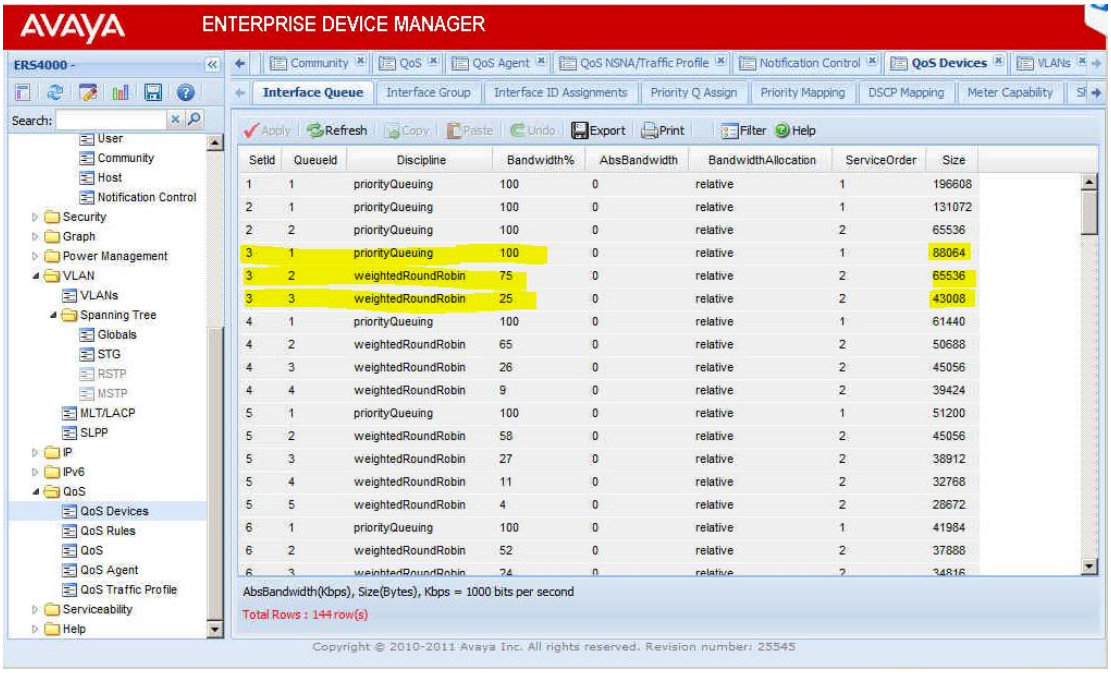

Figure A4

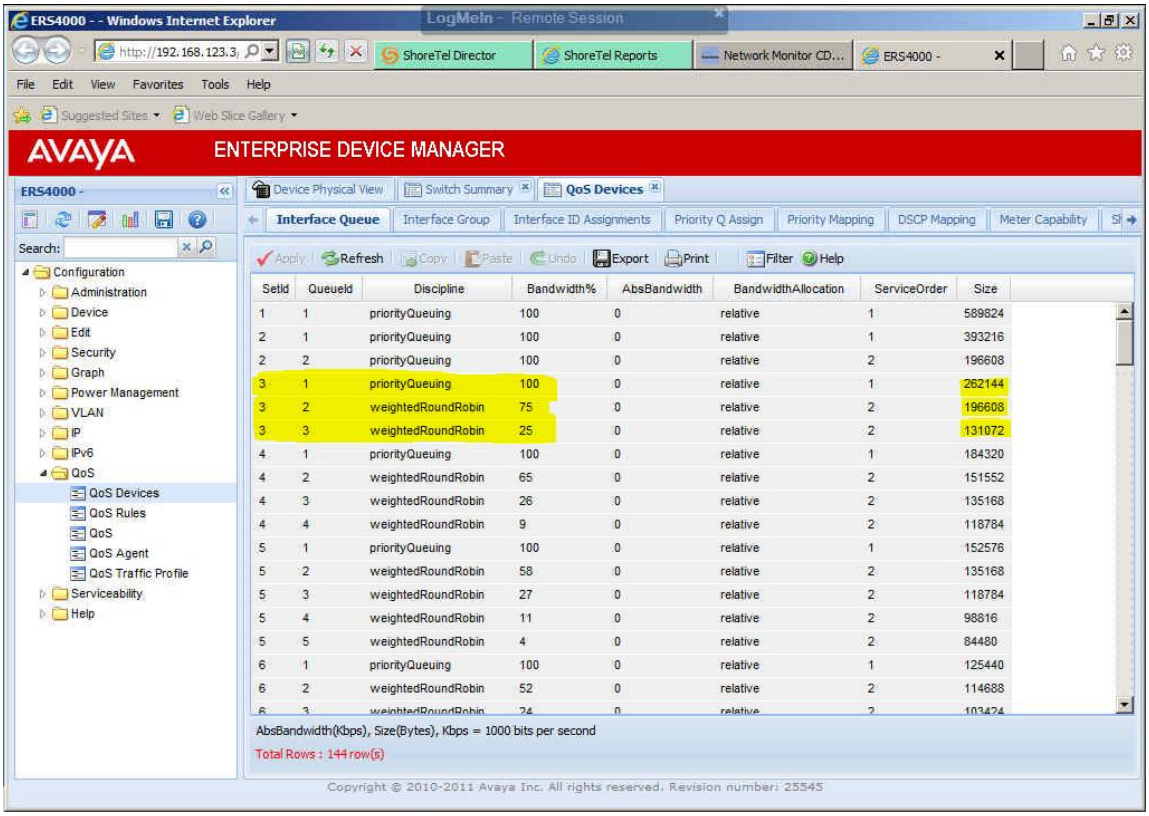

Figure A5

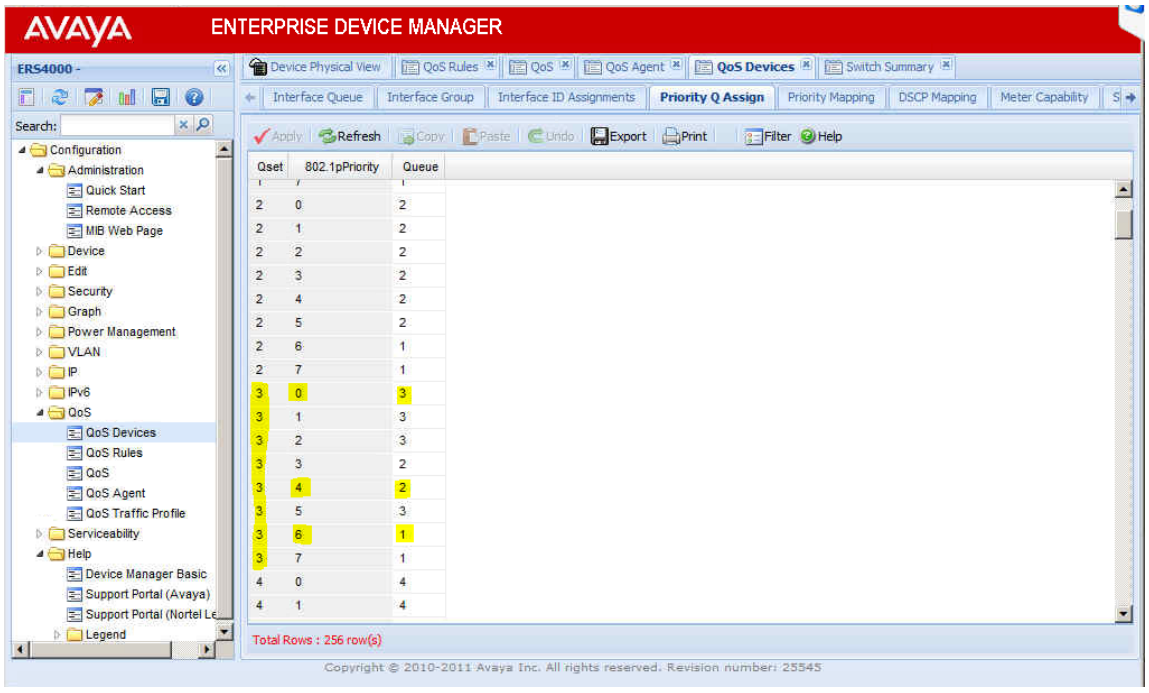

Figure A6

NOTE: Change DSCP 26 to 24 per the new ST Signaling DSCP standard recommendation.

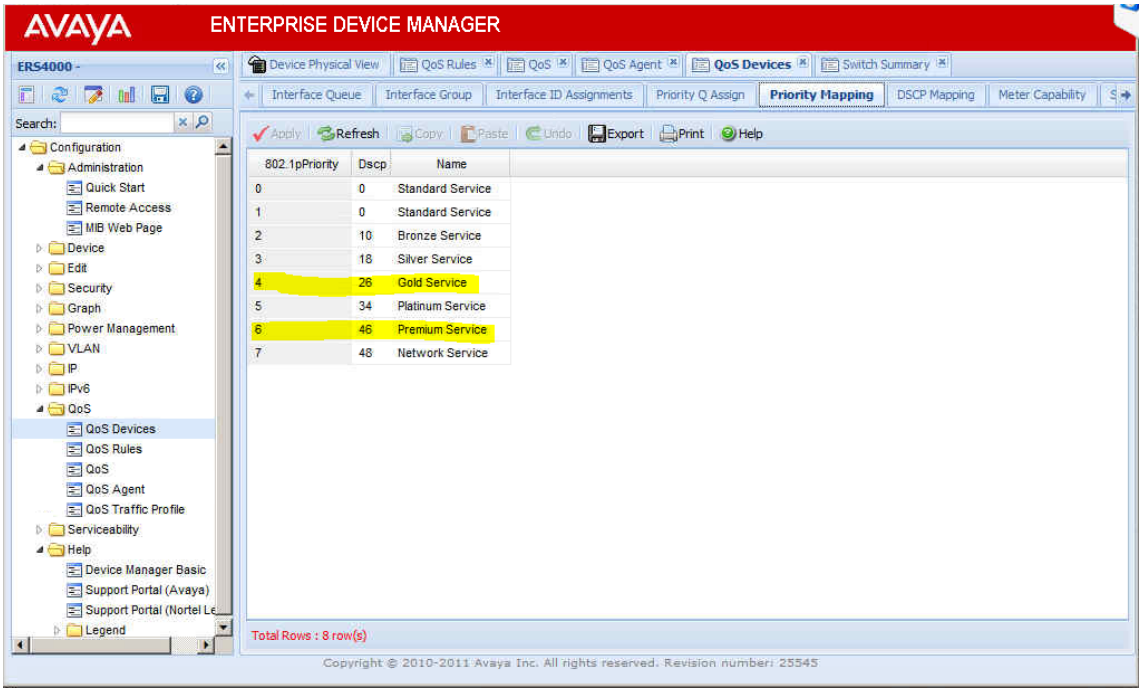

Figure A7

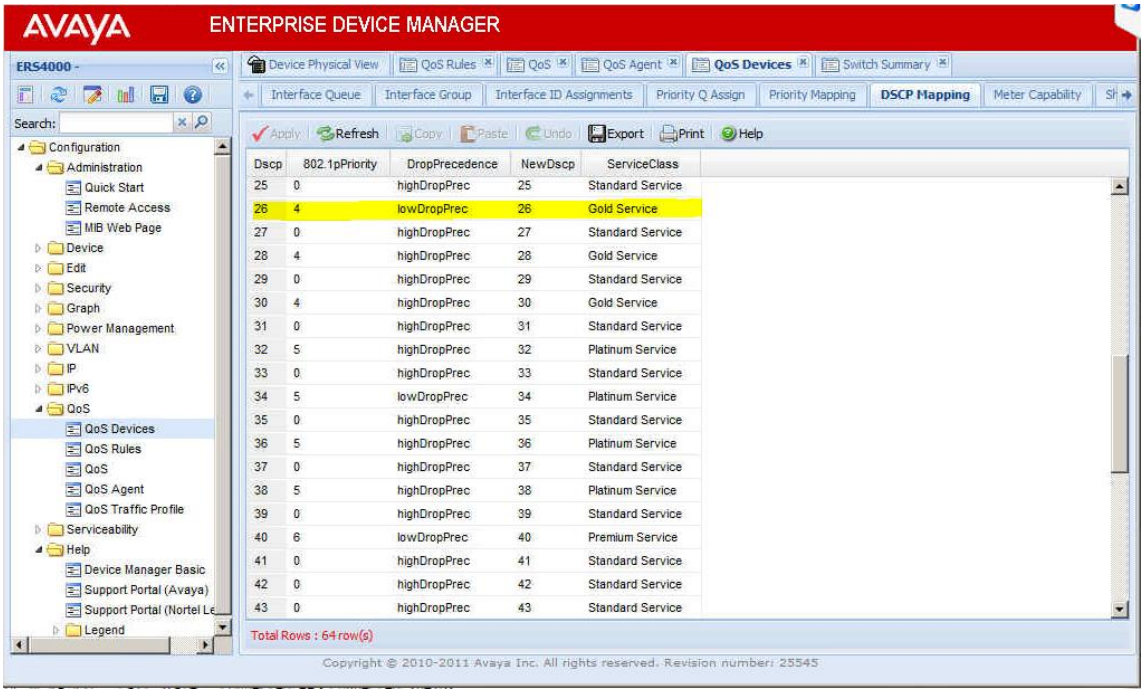

Figure A8

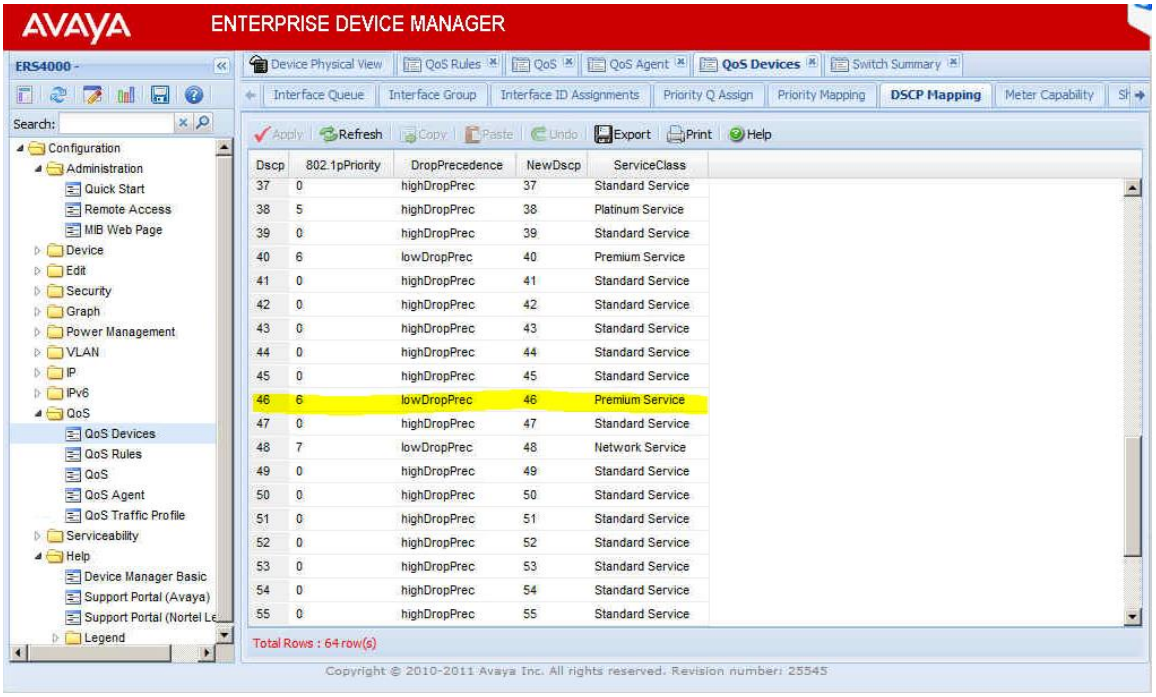

Figure A9

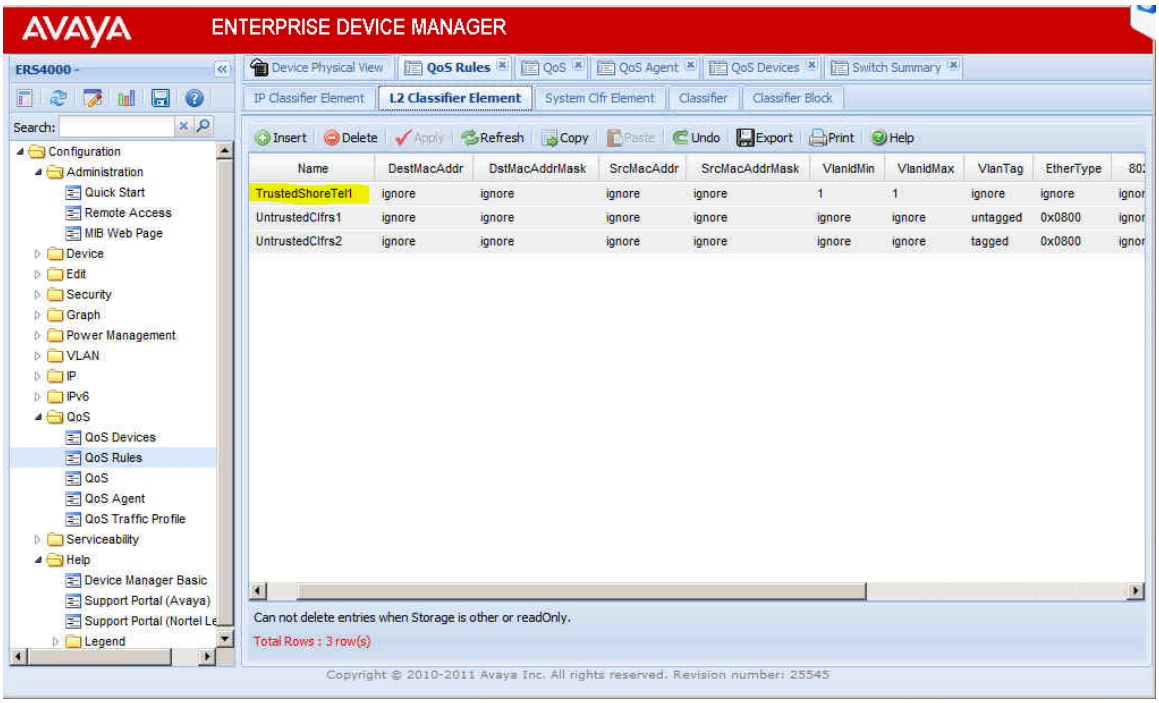

Figure A10

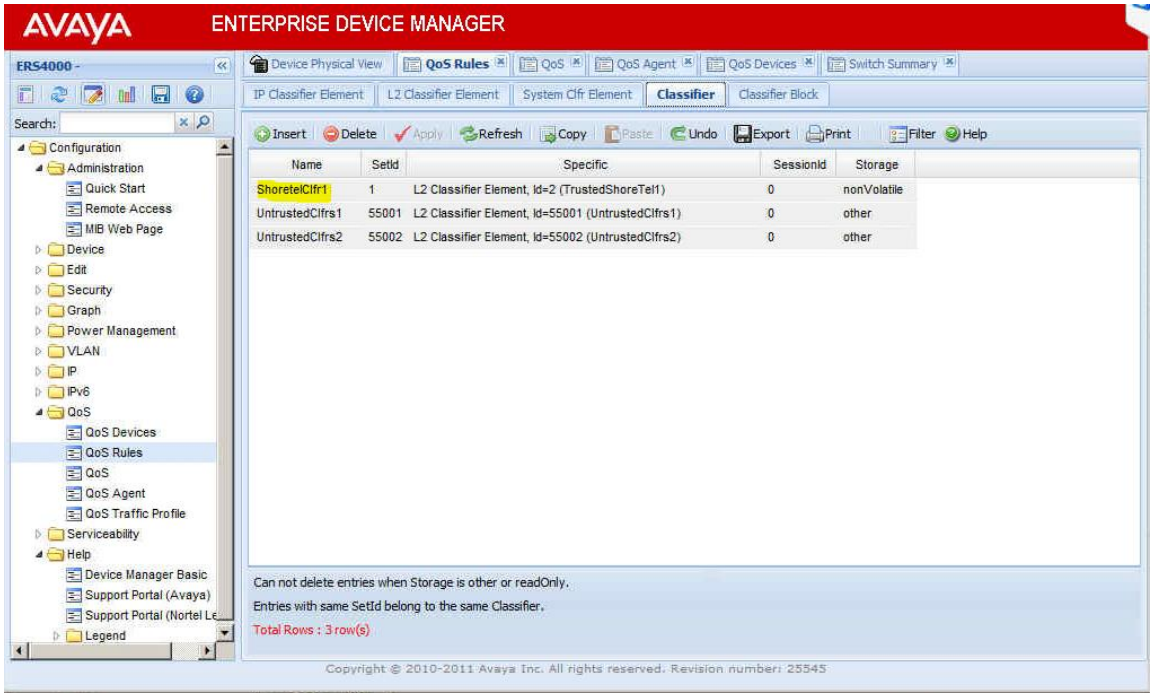

Figure A11

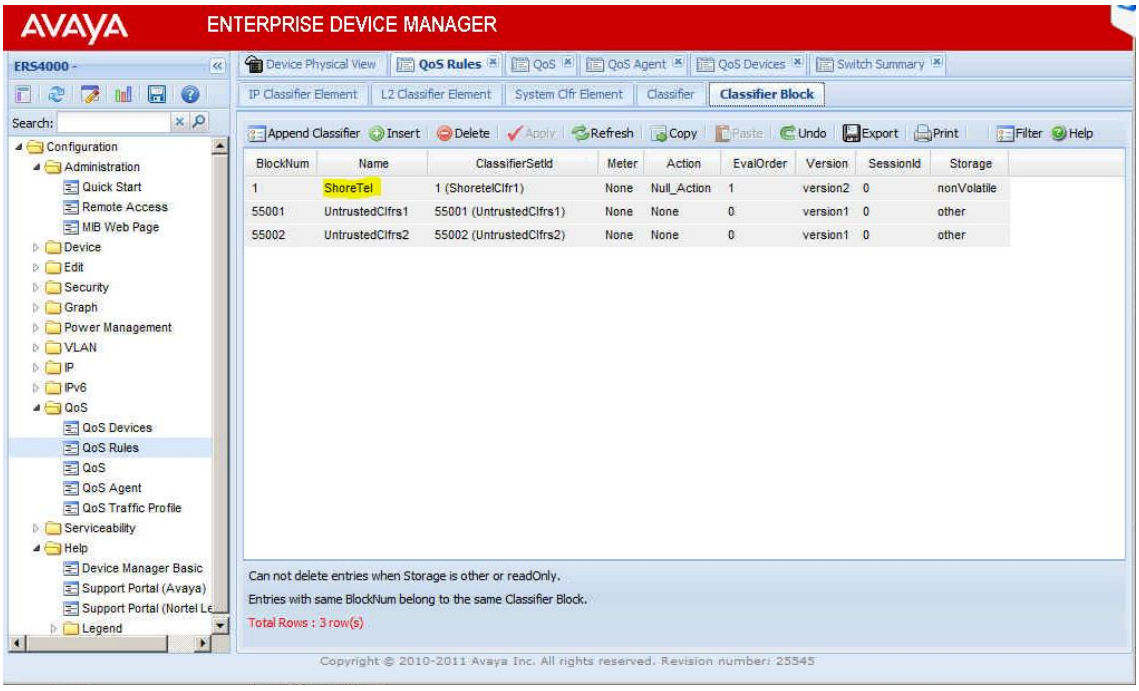

Figure A12

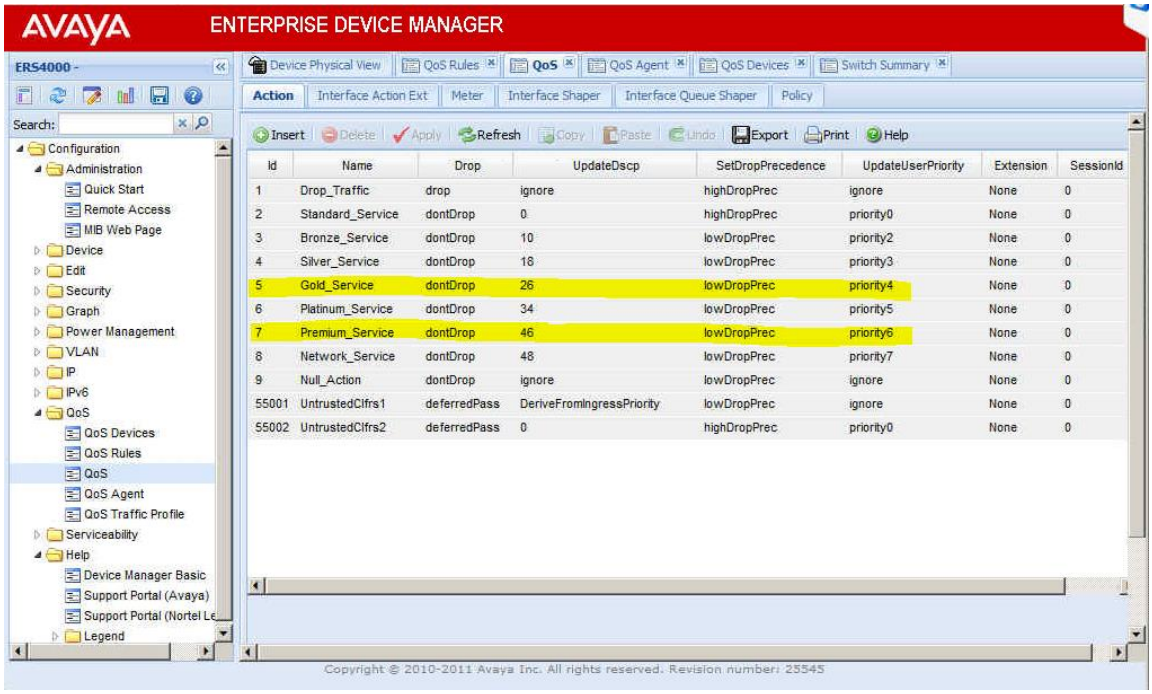

Figure A13

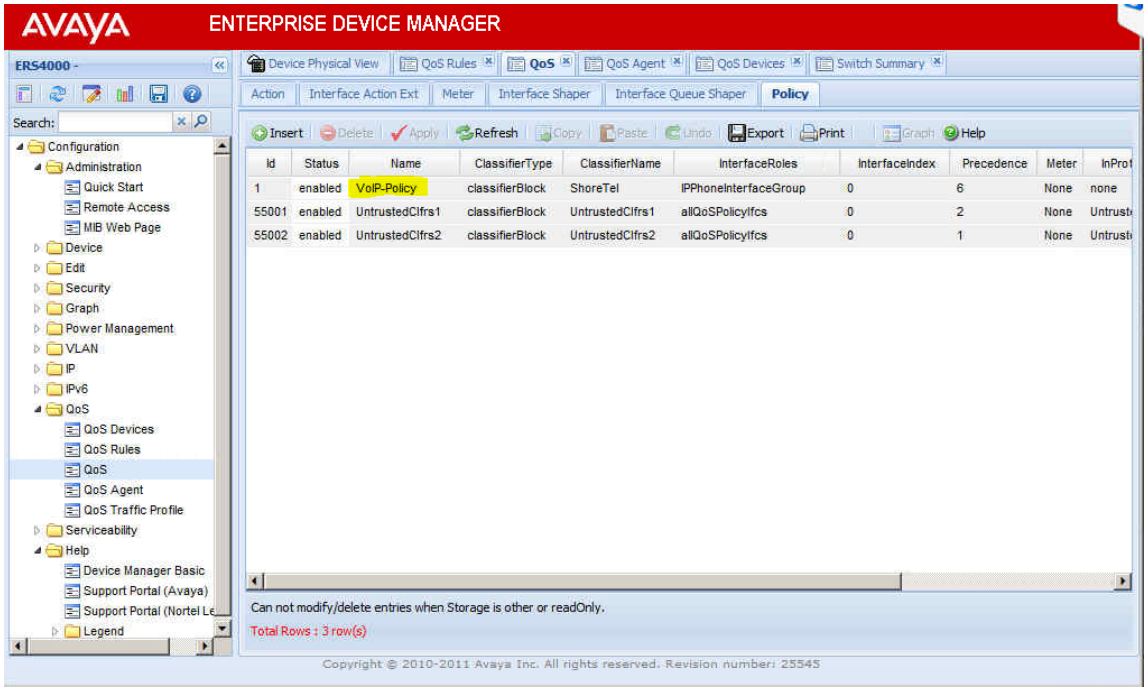

Figure A14

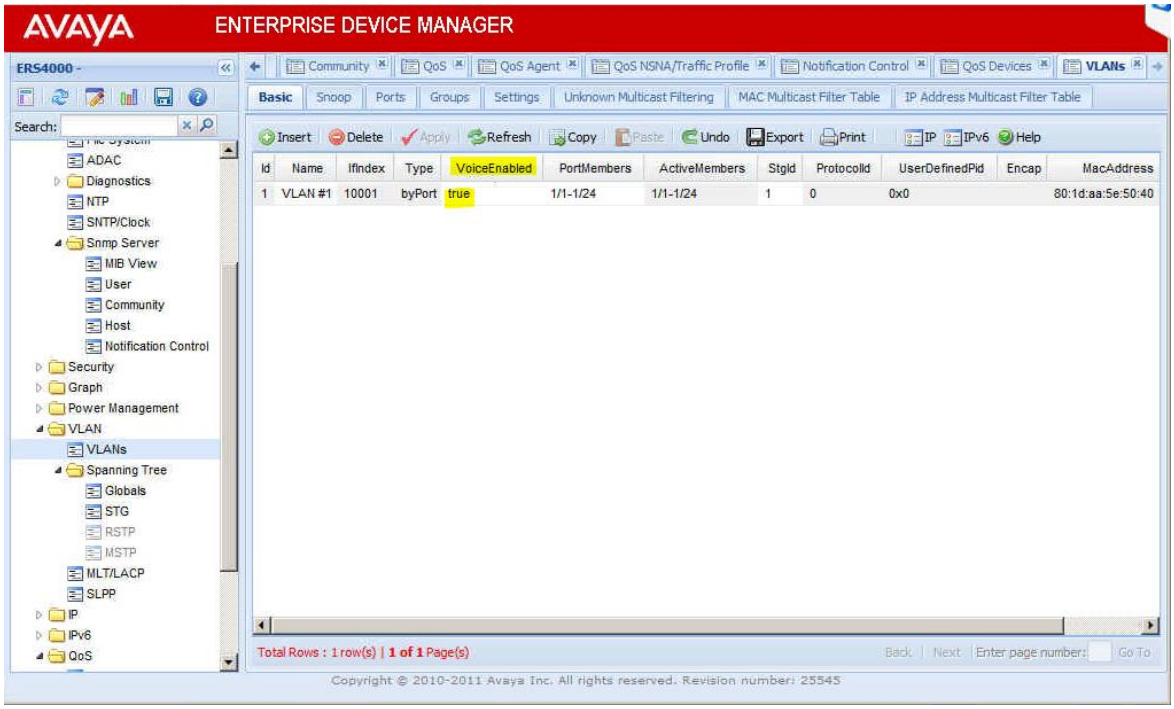

Figure A15

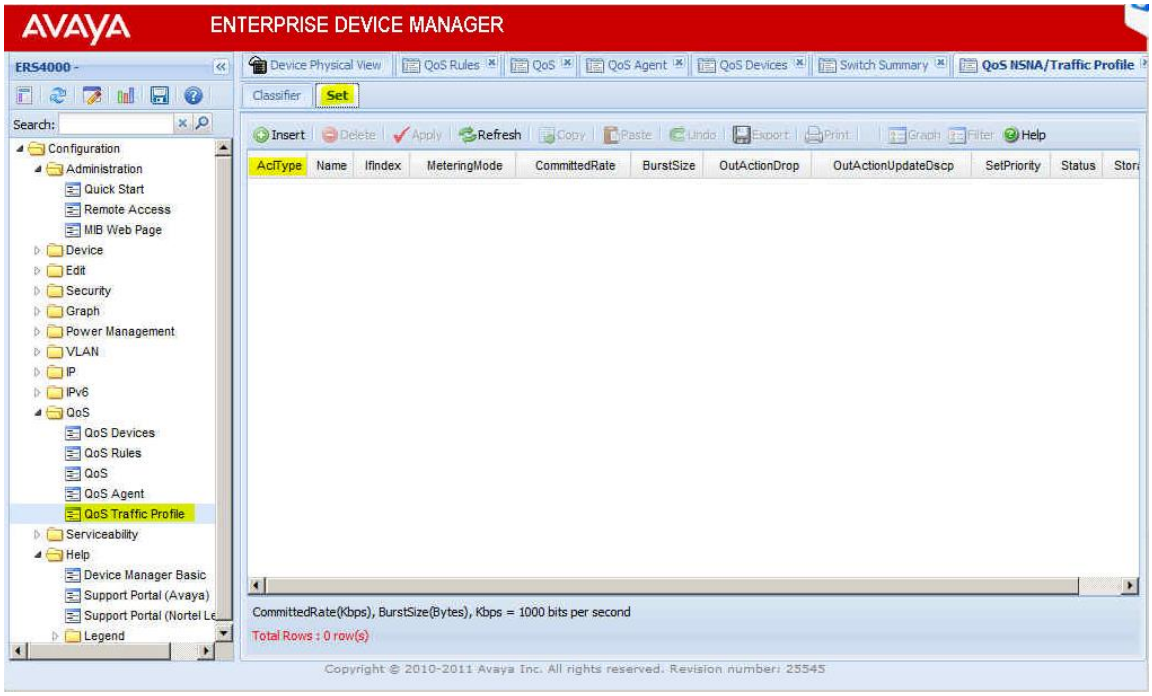

Figure A16

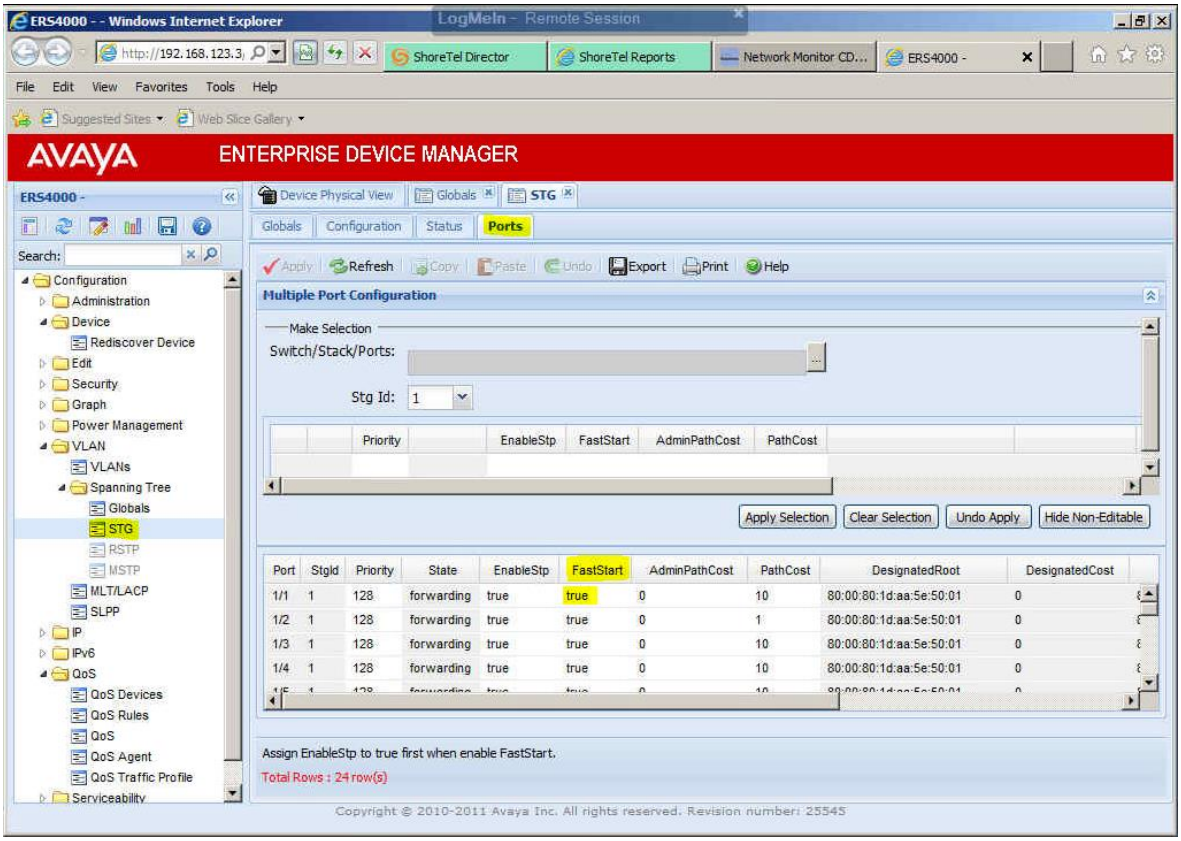
ERS4000 - - Windows Internet Explorer
LogMeIn - Remote Session
ShoreTel Director
ShoreTel Reports
Network Monitor CD...
ERS4000 -
File Edit View Favorites Tools Help
AVAYA
ENTERPRISE DEVICE MANAGER
ERS4000 -
Search:
Configuration
Administration
Device
Rediscover Device
Edit
Security
Graph
Power Management
VLAN
VLANs
Spanning Tree
Globals
STG
RSTP
MSTP
MLT/LACP
SLPP
IP
IPv6
QoS
QoS Devices
QoS Rules
QoS
QoS Agent
QoS Traffic Profile
Serviceability
Device Physical View
Globals
STG
Globals
Configuration
Status
Ports
Apply
Refresh
Copy
Paste
Undo
Export
Print
Help
Multiple Port Configuration
Make Selection
Switch/Stack/Ports:
Stg Id: 1
Priority
EnableStp
FastStart
AdminPathCost
PathCost
Apply Selection
Clear Selection
Undo Apply
Hide Non-Editable
Port StgId Priority State EnableStp FastStart AdminPathCost PathCost DesignatedRoot DesignatedCost
1/1 1 128 forwarding true true 0 10 80:00:80:1d:aa:5e:50:01 0
1/2 1 128 forwarding true true 0 1 80:00:80:1d:aa:5e:50:01 0
1/3 1 128 forwarding true true 0 10 80:00:80:1d:aa:5e:50:01 0
1/4 1 128 forwarding true true 0 10 80:00:80:1d:aa:5e:50:01 0
Assign EnableStp to true first when enable FastStart.
Total Rows : 24 row(s)
Copyright © 2010-2011 Avaya Inc. All rights reserved. Revision number: 25545

Figure A17

Appendix B: Adtran CoS/QoS Config Examples

Adtran - NetVanta 1335 PoE Example

NOTE: Change DSCP 26 to 24 per the new ST Signaling DSCP standard recommendation.

```
qos cos-map 1 0 1
qos cos-map 2 2
qos cos-map 3 3 4
qos cos-map 4 5 6 7
qos queue-type strict-priority
!
qos dscp-cos 0 8 16 26 34 46 48 56 to 0 1 2 3 4 5 6 7
!
!
vlan 20
name "VOICE_VLAN"
```

Figure B1

```
interface switchport 0/1
 description ***  VOICE ACCESS PORT  ***
 spanning-tree edgeport
 qos trust cos
 no shutdown
 switchport access vlan 20
!
interface switchport 0/2
 description ***  VOICE ACCESS PORT  ***
 spanning-tree edgeport
 qos trust cos
 no shutdown
 switchport access vlan 20
```

Figure B2

Appendix C: Cisco CoS/QoS Config Examples

If configuring MQC-based QoS for layer-2/3 network devices or MLS-based QoS for layer-2 network devices, use AutoQoS, add any interface specific commands listed in the sections above not configured by AutoQoS and apply the scripted policy-map QoS configuration to the appropriate interfaces that VoIP traffic will traverse where applicable. Applying the policy-map QoS configuration to a VLAN interface is much easier than to each physical interface. If configuring QoS for layer-3 MLS-based networking devices, see the example in Figure 17 of this document.

Appendix D: Dell CoS/QoS Config Examples

Dell – 3548 0 Example

```
qos

priority-queue out num-of-queues 4

wrr-queue cos-map 1 0
wrr-queue cos-map 2 3
wrr-queue cos-map 3 5

qos map dscp-queue 0 to 1
qos map dscp-queue 24 to 2
qos map dscp-queue 46 to 3

qos trust dscp
```

Appendix E: Juniper CoS/QoS Config Examples

For information regarding a validated Juniper QoS Configuration Example with a LAN only configuration that works with ST VoIP on the Voice VLAN, refer to the Knowledge Base article KB1002 - Juniper EX Series Switches CoS-QoS Mitel VoIP Configuration Example article.

Juniper

Create firewall filter VOIP to match and map RTP and Signaling traffic to correct forwarding classes

Juniper – EX4200 Example

Create forwarding classes mapped to specific queues

set class-of-service forwarding-classes class voice queue-num 5

set class-of-service forwarding-classes class voice-control queue-num 3

Create BA classifiers mapping forwarding classes to DSCP code points

set class-of-service classifiers dscp ezqos-dscp-classifier forwarding-class voice loss-priority low code-points ef

set class-of-service classifiers dscp ezqos-dscp-classifier forwarding-class voice-control loss-priority low code-points cs3

Create schedulers with buffer size, queue priority etc.

set class-of-service schedulers voice-sched transmit-rate percent 15

set class-of-service schedulers voice-sched buffer-size percent 5

set class-of-service schedulers voice-sched priority strict-high

set class-of-service schedulers voice-control-sched transmit-rate percent 10

set class-of-service schedulers voice-control-sched buffer-size percent 5

set class-of-service schedulers voice-control-sched priority low

Create scheduler maps to bind schedulers to forwarding classes (queues)

set class-of-service scheduler-maps ethernet-cos-map forwarding-class voice scheduler voice-sched

set class-of-service scheduler-maps ethernet-cos-map forwarding-class voice-control scheduler voice-control-sched

Bind CoS to interfaces (up/downlinks of core/edge switches)

set class-of-service interfaces ge-1/0/21 scheduler-map ethernet-cos-map

set class-of-service interfaces ge-1/0/21 unit 0 classifiers dscp ezqos-dscp-classifier

set class-of-service interfaces ge-1/0/22 scheduler-map ethernet-cos-map

set class-of-service interfaces ge-1/0/22 unit 0 classifiers dscp ezqos-dscp-classifier

Set interface(s) for IP phone and a user's PC connected to a single switch port

set vlans vlan_data vlan-id 10

set vlans vlan_voice vlan-id 20

set interface ge-0/0/0 unit 0 family ethernet-switching vlan members vlan_data

set ethernet-switching-options voip interface ge-0/0/0 vlan vlan_voice

set ethernet-switching-options voip interface ge-0/0/1.0 forwarding-class voice

Set “Port Fast” using EDGE command on connected ST devices (i.e. servers, SG switches, phones)

set protocols rstp interface ge-0/0/0.0 edge

set protocols rstp interface ge-0/0/1.0 edge

To validate configuration use the example commands for each switch and uplink interface

show configuration | *no-more* | *display set* (optional display formats to show running configuration)

show class-of-service (shows only the QoS configuration vs. all configuration)

show firewall (shows any advanced filter rules that may be used)

show interfaces queue ge-0/0/1 (checks all port queues for matched priority traffic and dropped packets.)

monitor interface ge-7/0/0 (check all uplink/downlink interfaces for drops, errors, discard, etc. If configured properly, they should all be 0 and not increment. Check phone interfaces as needed.)

TIP: ST13 Example (refer to Figure 12 for other ST release specific port usage to include)

set firewall family inet filter VOIP term VOIP_RTP1 from protocol udp

set firewall family inet filter VOIP term VOIP_RTP1 from source-port 10000-10550

set firewall family inet filter VOIP term VOIP_RTP1 then loss-priority low

set firewall family inet filter VOIP term VOIP_RTP1 then forwarding-class voice

set firewall family inet filter VOIP term VOIP_RTP1 then accept

set firewall family inet filter VOIP term VOIP_RTP2 from protocol udp

set firewall family inet filter VOIP term VOIP_RTP2 from destination-port 10000-10550

set firewall family inet filter VOIP term VOIP_RTP2 then loss-priority low

set firewall family inet filter VOIP term VOIP_RTP2 then forwarding-class voice

set firewall family inet filter VOIP term VOIP_RTP2 then accept

set firewall family inet filter VOIP term VOIP-SIGNALLING1 from protocol udp

set firewall family inet filter VOIP term VOIP-SIGNALLING1 from source-port 2427

set firewall family inet filter VOIP term VOIP-SIGNALLING1 then loss-priority low

set firewall family inet filter VOIP term VOIP-SIGNALLING1 then forwarding-class voice-control

set firewall family inet filter VOIP term VOIP-SIGNALLING1 then accept

set firewall family inet filter VOIP term VOIP-SIGNALLING2 from protocol udp

set firewall family inet filter VOIP term VOIP-SIGNALLING2 from source-port 2727

set firewall family inet filter VOIP term VOIP-SIGNALLING2 then loss-priority low

set firewall family inet filter VOIP term VOIP-SIGNALLING2 then forwarding-class voice-control

set firewall family inet filter VOIP term VOIP-SIGNALLING2 then accept

set firewall family inet filter VOIP term VOIP-SIGNALLING3 from protocol udp

set firewall family inet filter VOIP term VOIP-SIGNALLING3 from source-port 5440-5446

set firewall family inet filter VOIP term VOIP-SIGNALLING3 then loss-priority low

set firewall family inet filter VOIP term VOIP-SIGNALLING3 then forwarding-class voice-control

set firewall family inet filter VOIP term VOIP-SIGNALLING3 then accept

set firewall family inet filter VOIP term VOIP-SIGNALLING4 from protocol udp

set firewall family inet filter VOIP term VOIP-SIGNALLING4 from source-port 5450

set firewall family inet filter VOIP term VOIP-SIGNALLING4 then loss-priority low

set firewall family inet filter VOIP term VOIP-SIGNALLING4 then forwarding-class voice-control

set firewall family inet filter VOIP term VOIP-SIGNALLING4 then accept

set firewall family inet filter VOIP term VOIP-SIGNALLING5 from protocol udp

set firewall family inet filter VOIP term VOIP-SIGNALLING5 from source-port 5060

set firewall family inet filter VOIP term VOIP-SIGNALLING5 then loss-priority low

set firewall family inet filter VOIP term VOIP-SIGNALLING5 then forwarding-class voice-control

set firewall family inet filter VOIP term VOIP-SIGNALLING5 then accept

set firewall family inet filter VOIP term VOIP-SIGNALLING6 from protocol udp

set firewall family inet filter VOIP term VOIP-SIGNALLING6 from destination-port 2427

set firewall family inet filter VOIP term VOIP-SIGNALLING6 then loss-priority low

set firewall family inet filter VOIP term VOIP-SIGNALLING6 then forwarding-class voice-control

set firewall family inet filter VOIP term VOIP-SIGNALLING6 then accept

set firewall family inet filter VOIP term VOIP-SIGNALLING7 from protocol udp

set firewall family inet filter VOIP term VOIP-SIGNALLING7 from destination-port 2727

set firewall family inet filter VOIP term VOIP-SIGNALLING7 then loss-priority low

set firewall family inet filter VOIP term VOIP-SIGNALLING7 then forwarding-class voice-control

set firewall family inet filter VOIP term VOIP-SIGNALLING7 then accept

set firewall family inet filter VOIP term VOIP-SIGNALLING8 from protocol udp

set firewall family inet filter VOIP term VOIP-SIGNALLING8 from destination-port 5440-5446

set firewall family inet filter VOIP term VOIP-SIGNALLING8 then loss-priority low

set firewall family inet filter VOIP term VOIP-SIGNALLING8 then forwarding-class voice-control

set firewall family inet filter VOIP term VOIP-SIGNALLING8 then accept

set firewall family inet filter VOIP term VOIP-SIGNALLING9 from protocol udp

set firewall family inet filter VOIP term VOIP-SIGNALLING9 from destination-port 5450

set firewall family inet filter VOIP term VOIP-SIGNALLING9 then loss-priority low

set firewall family inet filter VOIP term VOIP-SIGNALLING9 then forwarding-class voice-control

set firewall family inet filter VOIP term VOIP-SIGNALLING9 then accept

set firewall family inet filter VOIP term VOIP-SIGNALLING10 from protocol udp

set firewall family inet filter VOIP term VOIP-SIGNALLING10 from destination-port 5060

set firewall family inet filter VOIP term VOIP-SIGNALLING10 then loss-priority low

set firewall family inet filter VOIP term VOIP-SIGNALLING10 then forwarding-class voice-control

set firewall family inet filter VOIP term VOIP-SIGNALLING10 then accept

set firewall family inet filter VOIP term VOIP-SIGNALLING11 from protocol tcp

set firewall family inet filter VOIP term VOIP-SIGNALLING11 from source-port 5430

set firewall family inet filter VOIP term VOIP-SIGNALLING11 then loss-priority low

set firewall family inet filter VOIP term VOIP-SIGNALLING11 then forwarding-class voice-control

set firewall family inet filter VOIP term VOIP-SIGNALLING11 then accept

set firewall family inet filter VOIP term VOIP-SIGNALLING12 from protocol tcp

set firewall family inet filter VOIP term VOIP-SIGNALLING12 from source-port 5447

set firewall family inet filter VOIP term VOIP-SIGNALLING12 then loss-priority low

set firewall family inet filter VOIP term VOIP-SIGNALLING12 then forwarding-class voice-control

set firewall family inet filter VOIP term VOIP-SIGNALLING12 then accept

set firewall family inet filter VOIP term VOIP-SIGNALLING13 from protocol tcp

set firewall family inet filter VOIP term VOIP-SIGNALLING13 from source-port 5452

set firewall family inet filter VOIP term VOIP-SIGNALLING13 then loss-priority low

set firewall family inet filter VOIP term VOIP-SIGNALLING13 then forwarding-class voice-control

set firewall family inet filter VOIP term VOIP-SIGNALLING13 then accept

set firewall family inet filter VOIP term VOIP-SIGNALLING14 from protocol tcp

set firewall family inet filter VOIP term VOIP-SIGNALLING14 from destination-port 5430

set firewall family inet filter VOIP term VOIP-SIGNALLING14 then loss-priority low

set firewall family inet filter VOIP term VOIP-SIGNALLING14 then forwarding-class voice-control

set firewall family inet filter VOIP term VOIP-SIGNALLING14 then accept

set firewall family inet filter VOIP term VOIP-SIGNALLING15 from protocol tcp

set firewall family inet filter VOIP term VOIP-SIGNALLING15 from destination-port 5447

set firewall family inet filter VOIP term VOIP-SIGNALLING15 then loss-priority low

set firewall family inet filter VOIP term VOIP-SIGNALLING15 then forwarding-class voice-control

set firewall family inet filter VOIP term VOIP-SIGNALLING15 then accept

set firewall family inet filter VOIP term VOIP-SIGNALLING16 from protocol tcp

set firewall family inet filter VOIP term VOIP-SIGNALLING16 from destination-port 5452

set firewall family inet filter VOIP term VOIP-SIGNALLING16 then loss-priority low

set firewall family inet filter VOIP term VOIP-SIGNALLING16 then forwarding-class voice-control

set firewall family inet filter VOIP term VOIP-SIGNALLING16 then accept

set firewall family inet filter VOIP term ACCEPT_ALL then accept

Option 1 - Bind firewall filter VOIP to the Voice VLAN interface (apply to any other VLANs as necessary)

set interfaces vlan unit 20 family inet filter input VOIP

Option 1a - Create VLAN Rewrite Rules to mark or remark traffic between VLANs

set class-of-service rewrite-rules dscp v4rw forwarding-class voice loss-priority low code-point ef

set class-of-service rewrite-rules dscp v4rw forwarding-class voice-control loss-priority low code-point cs3

Option 1b - Bind Rewrite Rules to “VLAN” interfaces where VoIP traffic exists

set class-of-service interfaces vlan unit 20 rewrite-rules dscp v4rw

Option 2 - Bind firewall filter VOIP to a physical interface (apply to any L3 up/down links or untrusted switches)

set interfaces ge-1/0/0 unit 0 family inet filter input VOIP

Option 2a - Create “Interface” Rewrite Rules for interfaces that can’t bind VLAN rewite rules

set class-of-service rewrite-rules dscp rewrite-dscp forwarding-class voice loss-priority low code-point ef

set class-of-service rewrite-rules dscp rewrite-dscp forwarding-class voice-control loss-priority low code-point cs3

Option 2b - Bind “Interface” Rewrite Rules to interfaces that can’t bind VLAN rewite rules

set class-of-service interfaces ge-1/0/18 unit 0 rewrite-rules dscp rewrite-dscp

set class-of-service interfaces ge-1/0/19 unit 0 rewrite-rules dscp rewrite-dscp

IMPORTANT TIP: Don’t mix commands from above example Options 1a-b with Options 2a-b on any overlapping physical/virtual interfaces as a one-way audio issue could occur.

Appendix F: HP CoS/QoS Config Examples

HP Procurve – 2520G-24-POE Examples

```
PC-2520G-24-PoE-SDF(config)# show run

Running configuration:

; J9299A Configuration Editor; Created on release #J.15.09.0014
; Ver #03:01.14.05:13
hostname "PC-2520G-24-PoE-SDF"
mirror-port 18
console inactivity-timer 120
fault-finder bad-driver sensitivity high
fault-finder bad-transceiver sensitivity high
fault-finder bad-cable sensitivity high
fault-finder too-long-cable sensitivity high
fault-finder over-bandwidth sensitivity high
fault-finder broadcast-storm sensitivity high
fault-finder loss-of-link sensitivity high
fault-finder duplex-mismatch-hdx sensitivity high
fault-finder duplex-mismatch-fdx sensitivity high
power-over-ethernet pre-std-detect
qos dscp-map 000000 priority 0
qos dscp-map 001000 priority 1
qos dscp-map 010000 priority 2
qos dscp-map 011000 priority 3
qos dscp-map 011010 priority 3
qos dscp-map 100000 priority 4
qos dscp-map 101000 priority 5
qos dscp-map 101110 priority 5
qos dscp-map 110000 priority 6
qos dscp-map 111000 priority 7
qos type-of-service diff-services
timesync sntp
sntp unicast
```

Figure F1

```
vlan 10
   name "VoIP_VLAN"
   tagged 1-21,23-24,27-28
   no ip address
   voice
   exit
vlan 20
   name "TRUST_WLAN"
   untagged 22-23
   tagged 27-28
   no ip address
   exit
vlan 40
   name "GUEST_WLAN"
   tagged 21-23,27-28
   no ip address
   qos priority 1
   exit
spanning-tree
spanning-tree 1 admin-edge-port
spanning-tree 1 bpdu-protection
spanning-tree 2 admin-edge-port
spanning-tree 2 bpdu-protection
spanning-tree 3 admin-edge-port
spanning-tree 3 bpdu-protection
spanning-tree 4 admin-edge-port
spanning-tree 4 bpdu-protection
spanning-tree 5 admin-edge-port
spanning-tree 5 bpdu-protection
spanning-tree 6 admin-edge-port
spanning-tree 6 bpdu-protection
spanning-tree 7 admin-edge-port
spanning-tree 7 bpdu-protection
spanning-tree 8 admin-edge-port
spanning-tree 8 bpdu-protection
spanning-tree 9 admin-edge-port
spanning-tree 9 bpdu-protection
spanning-tree 10 admin-edge-port
spanning-tree 10 bpdu-protection
```

Figure F2

HP Procurve – 2920G-24G Example

HP-2920-24G# sh run

Running configuration:

; J9726A Configuration Editor; Created on release #WB.15.11.0007

; Ver #03:12.15.0d:09

hostname "HP-2920-24G"

module 1 type j9726a

class ipv4 "All_Other"

10 ignore ip 0.0.0.0 255.255.255.255 0.0.0.0 255.255.255.255 ip-dscp ef

20 ignore udp 0.0.0.0 255.255.255.255 0.0.0.0 255.255.255.255 range 10000 10550

30 ignore ip 0.0.0.0 255.255.255.255 0.0.0.0 255.255.255.255 ip-dscp cs3

40 ignore udp 0.0.0.0 255.255.255.255 0.0.0.0 255.255.255.255 eq 2427

```
    50 ignore udp 0.0.0.0 255.255.255.255 0.0.0.0 255.255.255.255 eq 2727
    60 ignore udp 0.0.0.0 255.255.255.255 0.0.0.0 255.255.255.255 eq 5060
    70 ignore udp 0.0.0.0 255.255.255.255 0.0.0.0 255.255.255.255 range 5440 5446
    80 ignore udp 0.0.0.0 255.255.255.255 0.0.0.0 255.255.255.255 eq 5450
    90 ignore tcp 0.0.0.0 255.255.255.255 0.0.0.0 255.255.255.255 range 5060 5061
    100 ignore tcp 0.0.0.0 255.255.255.255 0.0.0.0 255.255.255.255 eq 5430
    110 ignore tcp 0.0.0.0 255.255.255.255 0.0.0.0 255.255.255.255 range 5447 5448
    120 ignore tcp 0.0.0.0 255.255.255.255 0.0.0.0 255.255.255.255 eq 5452
  exit
class ipv4 "VoIP_Audio"
    10 match ip 0.0.0.0 255.255.255.255 0.0.0.0 255.255.255.255 ip-dscp ef
    20 match udp 0.0.0.0 255.255.255.255 0.0.0.0 255.255.255.255 range 10000 10550
  exit
class ipv4 "Call_Control"
    10 match ip 0.0.0.0 255.255.255.255 0.0.0.0 255.255.255.255 ip-dscp cs3
    20 match udp 0.0.0.0 255.255.255.255 0.0.0.0 255.255.255.255 eq 2427
    30 match udp 0.0.0.0 255.255.255.255 0.0.0.0 255.255.255.255 eq 2727
    40 match udp 0.0.0.0 255.255.255.255 0.0.0.0 255.255.255.255 eq 5060
    50 match udp 0.0.0.0 255.255.255.255 0.0.0.0 255.255.255.255 range 5440 5446
    60 match udp 0.0.0.0 255.255.255.255 0.0.0.0 255.255.255.255 eq 5450
    70 match tcp 0.0.0.0 255.255.255.255 0.0.0.0 255.255.255.255 range 5060 5061
    80 match tcp 0.0.0.0 255.255.255.255 0.0.0.0 255.255.255.255 eq 5430
    90 match tcp 0.0.0.0 255.255.255.255 0.0.0.0 255.255.255.255 range 5447 5448
    100 match tcp 0.0.0.0 255.255.255.255 0.0.0.0 255.255.255.255 eq 5452
  exit
policy qos "VOIP"
    10 class ipv4 "VoIP_Audio" action dscp ef action priority 5
    20 class ipv4 "Call_Control" action dscp af31 action priority 3
    30 class ipv4 "All_Other" action dscp default action priority 0
  exit
qos dscp-map 011010 priority 3
qos dscp-map 101110 priority 5
qos type-of-service diff-services
vlan 52 service-policy VOIP in
vlan 51 service-policy VOIP in
```

Document and Software Copyrights

Mitel Networks Corporation reserves the right to make changes without notice to the specifications and materials contained herein and shall not be responsible for any damage (including consequential) caused by reliance on the materials presented, including, but not limited to typographical, arithmetic or listing errors.

Trademarks

The Mitel word and logo are trademarks of Mitel Networks Corporation. Any reference to third-party trademarks is for reference only and Mitel makes no representation of ownership of these marks.

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.