Application Note

ST AppNote 10326 (AN 10326)
Dec 10, 2013

Data Network Best Practices for ShoreTel VoIP

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

Environment: ShoreTel UC versions 10.X – 14.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 ShoreTel UC Voice over IP versions 10.X – 14.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

UNDERSTANDING VLAN DESIGN *3*
CONFIGURING VLANS FOR SHORETEL IP PHONES *7*
CONFIGURING DHCP FOR SHORETEL IP PHONES *10*
AUTOMATIC IP PHONE VLAN ASSIGNMENT - DHCP *14*
AUTOMATIC IP PHONE VLAN ASSIGNMENT – LLDP-MED *15*
UNDERSTANDING QUALITY OF SERVICE (QOS) DESIGN *16*
CONFIGURING QUALITY OF SERVICE - LAN *19*
USING CISCO AUTO-QOS *23*
CONFIGURING QUALITY OF SERVICE - WAN *29*
PORT SECURITY ON DATA SWITCHES *37*
MTU CONSIDERATIONS FOR SITE TO SITE TUNNEL CONNECTIONS *37*
CONCLUSION *37*
REFERENCES *39*

Understanding VLAN Design

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 do so 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 help 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 have to store to communicate which is a more limited resource for IP phones. For example at a given site, create a data VLAN for PCs, a voice VLAN for all VoIP devices which should include ShoreGear switches, ShoreTel 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 benefits of placing data and voice traffic in separate VLANs and QoS strategies 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.

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 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 reaches over qty. 10 L2 switches at a

site or when all ports have been exhausted on the core L3 switch by access level L2 switch uplink connections.

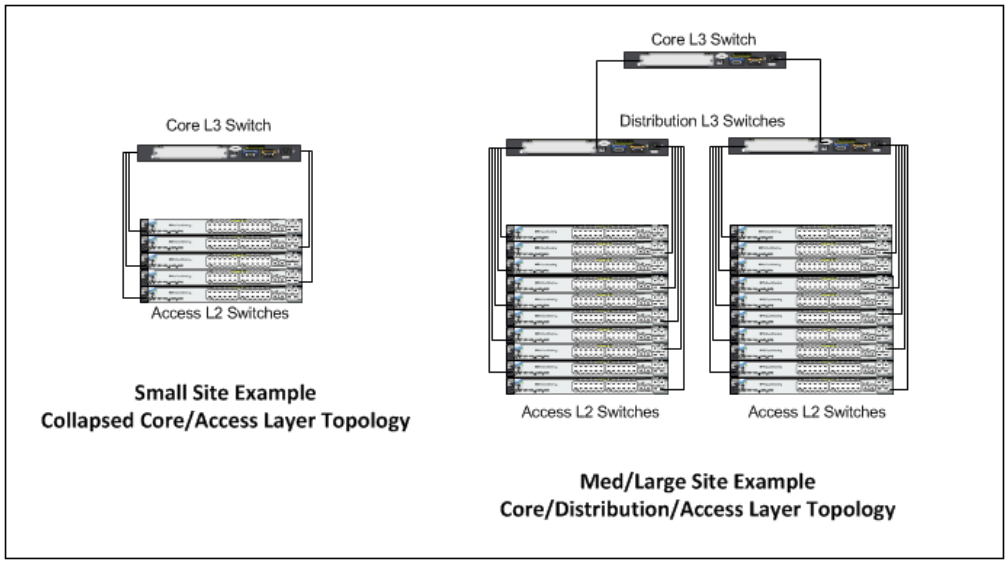

Figure 1

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 on each VLAN.

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 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.

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.

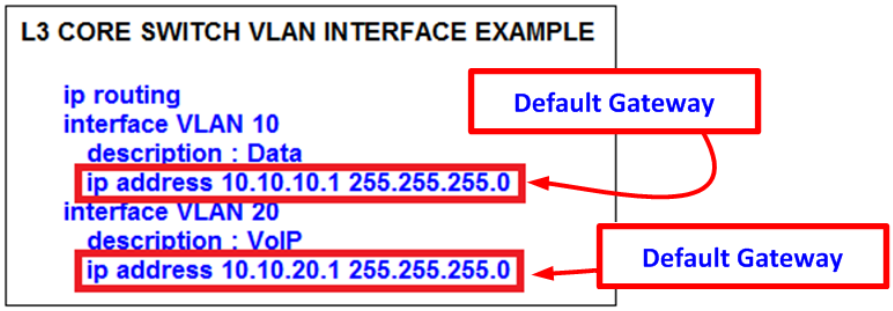

Figure 2

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***) directed at the firewall's next hop interface will only route Internet traffic to the firewall and keep local traffic on the L3 switch along with the directly connected VLAN routes or any other static or dynamic local routes.

> **IMPORTANT TIP**: Avoid hair-pining local traffic needlessly to the firewall and back to the L3 switch which causes port buffer overruns/tail drops, potential link congestion and voice quality issues if the firewall was configured with a subnet/VLAN as a default gateway(s).

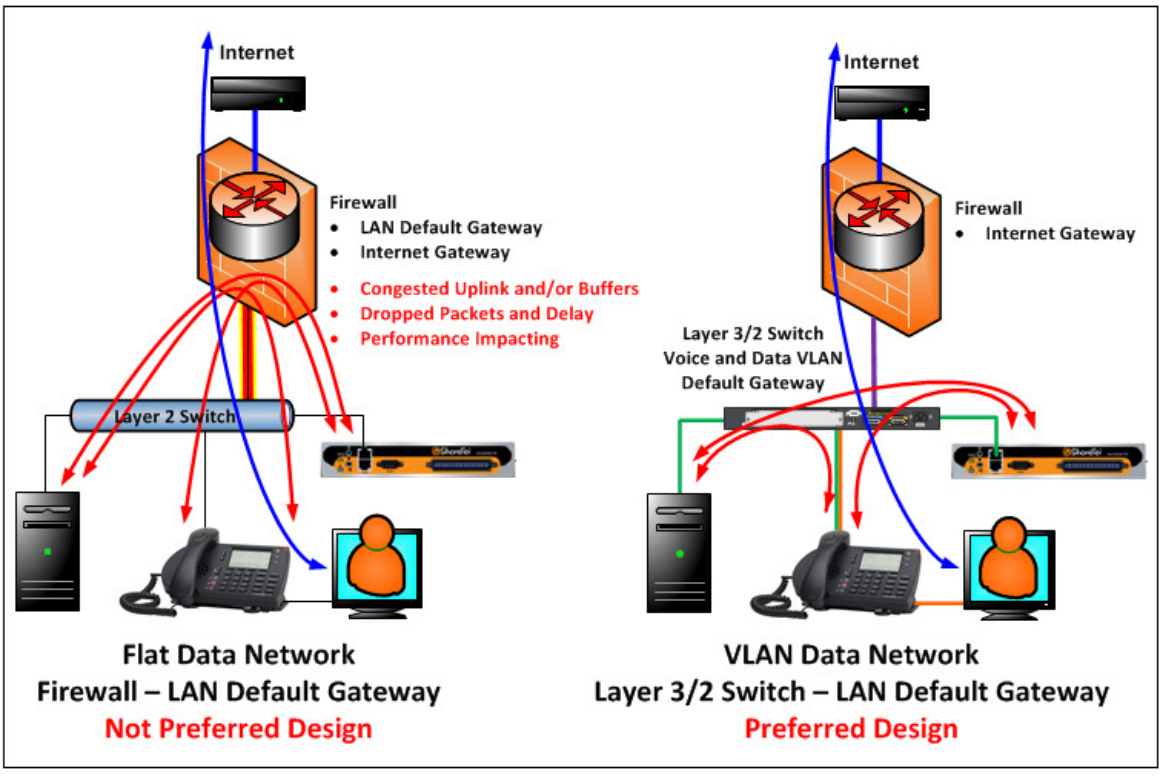

Figure 3

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 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 which 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 in Figure 3 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 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 only on each local LAN and for better IP address management.

> **IMPORTANT TIP**: Avoid trunking or tagging most local VLANs (i.e. Data and Voice VLANs) at a given site across a WAN connection to a remote site. In some cases, it is acceptable to trunk or tag a VLAN(s) across a WAN link, for example, a Guest Wi-Fi VLAN.

Each site will have its own Data and Voice VLAN(s) with separate IP addressing at each 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 from your other 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 ShoreTel. While adhering to the same design principles, to add hardware or link redundancy to any design (including Rapid Spanning Tree, 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 ShoreTel.

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 ShoreTel VoIP deployment.

The best practice summary of designing multiple VLANs into the data network design includes:

- 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 layer-2 switches across LAN uplinks to the site's layer-3 core switch or router.
- In most cases, 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.
- 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 functionality enabled to route IP traffic between local 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 "hub and spoke" WAN topology where all remote sites' layer-3 switch or router are the spokes connected via a WAN point-to-point uplink to the common "core" layer-3 switch or router at the hub site.
- Each VLAN will have its own VLAN interface IP address which 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 ShoreGear switches and ShoreTel 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.

Configuring VLANs for ShoreTel IP Phones

IP phones are a specialized device on the data network and have capabilities and requirements which need to be considered when designing the data network. For example, to help better utilize port capacity on data switches, a PC is allowed to piggy-back on an IP phone and share a single data switch port, utilizing VLAN trunking or tagging the Voice and Data VLANs for each device respectively.

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

Most data network equipment manufacturers have a voice VLAN feature either at the data switch access port or VLAN level that supports various VoIP capabilities (i.e. to mitigate deteriorating IP phone sound quality of a call if the data is unevenly sent due to lack of layer-2 output switch interface buffer prioritization). The Voice VLAN feature helps QoS use classification and scheduling to send network traffic from the switch in a predictable manner for IP phones. By default, the voice VLAN feature is disabled but when the voice VLAN feature is enabled, all

untagged traffic is sent according to the default CoS priority of the port and all 802.1P or 802.1Q tagged VLAN traffic's COS is trusted.

For further discussion how an IP phone is automatically assigned to the Voice VLAN when the Voice and Data VLANs are both assigned to the data switch port, refer to the sections below, *Automatic IP Phone VLAN Assignment - DHCP and Automatic IP Phone VLAN Assignment - LLDP-MED.*

Telecommuters that work remotely with a physical ShoreTel 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 ShoreTel VPN Concentrator located in the customer's corporate network to be able to register their ShoreTel IP phone as if it were in the office. Check with your ShoreTel administrator for the initial setup configuration on the IP Phone's VPN client to connect to your corporate ShoreTel VPN Concentrator and ShoreTel UC system. 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.

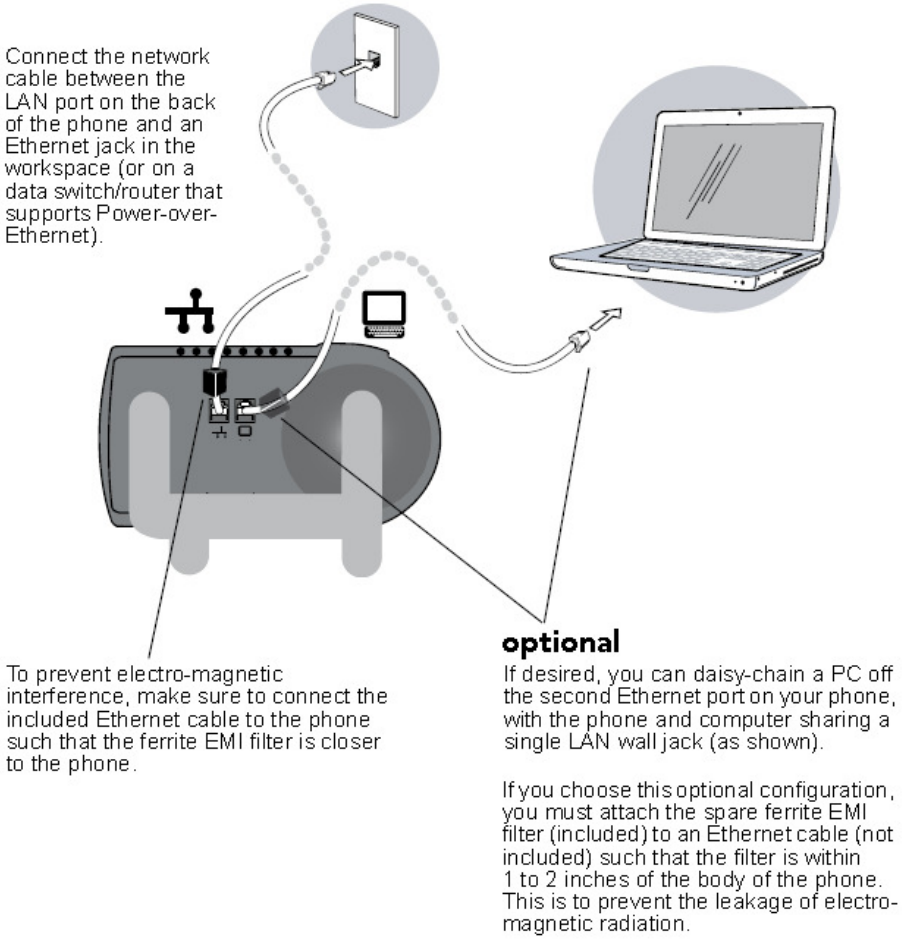

Figure 4

Figure 4 above demonstrates the physical connection of a PC connected to a ShoreTel IP phone in turn connected to the network connection on a single data switch access port.

Figure 5 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 ShoreTel IP phone. Figure 5 also shows the *access* port configuration when the Voice VLAN is the only VLAN (i.e. untagged VLAN) applied to the port for dedicated ShoreTel devices such as ShoreGear switches (e.g. SG-90, SG-220T1, SG-T1K, SG-90V, etc.), ShoreTel servers (e.g. HQ, DVS, ECC, etc.) and standalone ShoreTel IP phones.

IMPORTANT TIP: If the Voice VLAN feature is inadvertently applied to any ShoreGear switch or ShoreTel server, they may not be able to route to other VLANs on the data network.

```
L3 SWITCH CONFIGURATION
interface FastEthernet1    (and port 4)
  description : These ports have BOTH phone + PC
  switchport mode access
  switchport access vlan 10
  switchport voice vlan 20
  spanning-tree portfast
  no cdp enable
interface FastEthernet2    (and ports 5,11,12)
  description : These ports have ONLY voice devices
  switchport mode access
  switchport access vlan 20
  spanning-tree portfast
  no cdp enable
interface FastEthernet3    (and ports 6 & 10)
  description : These ports have ONLY data devices
  switchport mode access
  switchport access vlan 10
  spanning-tree portfast
  no cdp enable
```

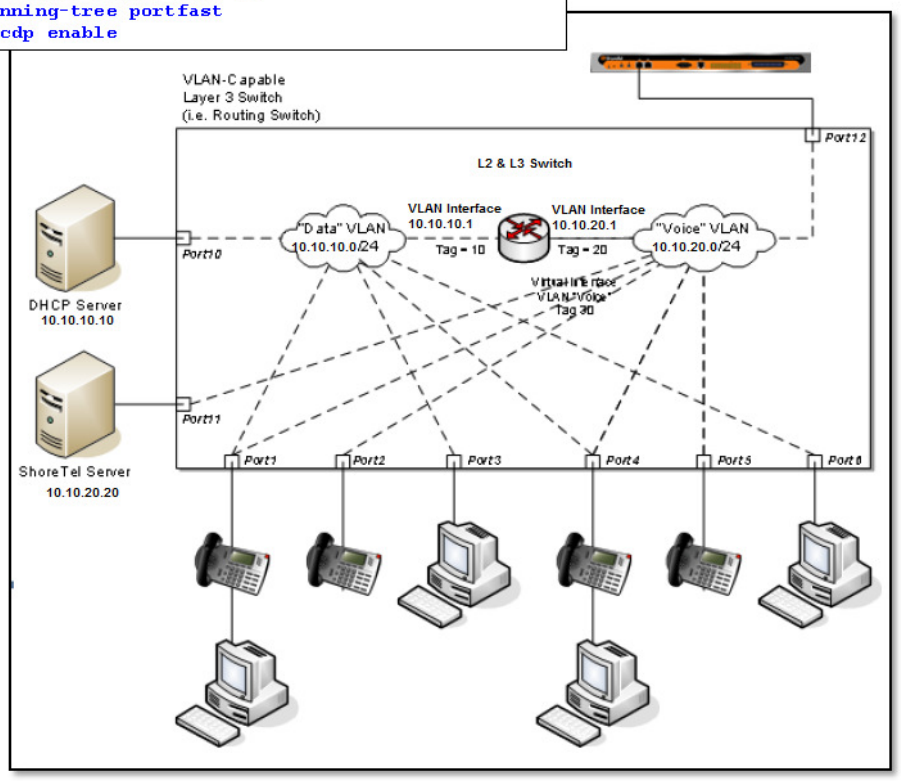

Figure 5

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

spanning-tree portfast

no cdp enable

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

In summary, ShoreTel 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. ShoreTel does not require nor dictate that you use a specific vendor's equipment for your LAN edge, core, WAN, switches, routers, operating systems, etc. as long as your data hardware supports the minimum recommended requirements presented in this document.

Configuring DHCP for ShoreTel 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 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. ShoreTel 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 ShoreTel "vendor-specific" DHCP option (i.e. Option 156) with the required parameters.

See Figure 6 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 6

Figures 7, 8 and 9 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 ShoreTel 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 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 an additional tagged VLAN(s), which will cause DHCP assignment issues.

```
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, country=1, language=1, layer2tagging=1, vlandid=20"
   option 4 ip 10.10.10.10
   lease infinite
```

Figure 7

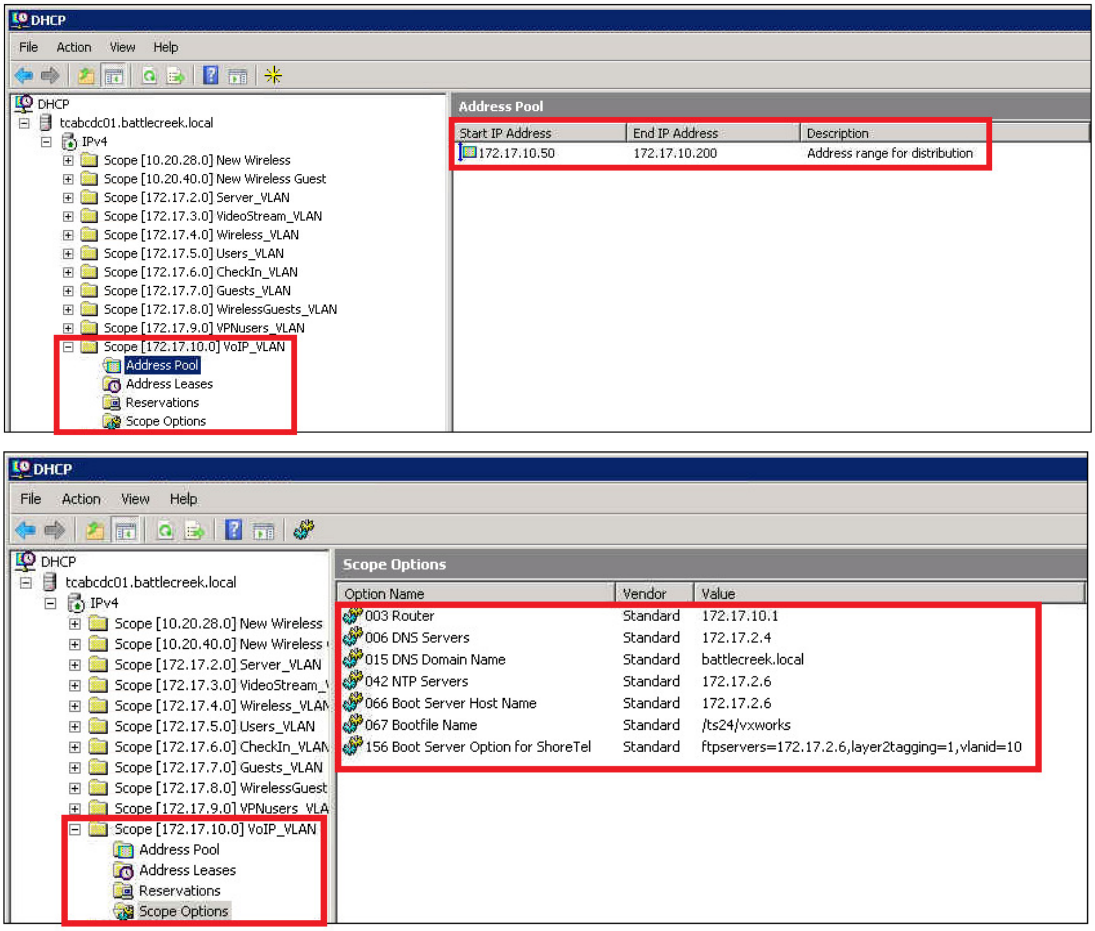

Figure 8

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 9

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 ShoreGear switches and ShoreTel servers 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.

ShoreTel IP Phones have a built-in configuration to seek the ShoreTel server's address with the Vendor Specific DHCP option 156. If this option is not available, ShoreTel's 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 ShoreTel 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,country=1, language=1, 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",country=1, language=1, Layer2Tagging=1,VlanId=20*

The maximum length of the supplied string is 160 characters.

For additional information, refer to the ShoreTel Planning and Installation Guide for details under the section *Configuring DHCP for ShoreTel 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.ShoreTel.Server* *(e.g. FtpServers= 10.10.20.20)*

In order for any ShoreTel 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 ShoreTel 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 ShoreTel 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.

Automatic IP Phone VLAN Assignment - DHCP

The Automatic VLAN Assignment feature using DHCP is not configured through ShoreTel Director. Configuration changes are performed on the appropriate DHCP Server. In the previous section, the DHCP Scope and related ShoreTel 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,country=1, language=1, Layer2Tagging=1,VlanId=20

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

1. As the ShoreTel 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" 10.10.10.10 to the DHCP server and the Data VLAN.
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 settings 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 Phone registers successfully and is ready for service.

For more detailed information on configuring Option 156 on your DHCP server, refer to article KB10966 or the appropriate ShoreTel Planning and Installation Guide for your system under sections *Configuring DHCP for ShoreTel IP Phones* and *Configuring Automatic VLAN Assignment via DHCP*.

Automatic IP Phone VLAN Assignment – LLDP-MED

LLDP (IEEE 802.1AB) is a vendor agnostic Layer 2 protocol designed to be used by network devices for advertising their identity, capabilities, and neighbors on a IEEE 802 Ethernet LAN. LLDP performs similar functions as several proprietary protocols such as the Cisco Discovery Protocol (CDP), Extreme Discovery Protocol, Nortel Discovery Protocol and Microsoft's Link Layer Topology Discovery. An enhancement to LLDP is LLDP-MED, Link Layer Discovery Protocol-Media Endpoint Discovery. For further information on LLDP-MED, refer to the appropriate ShoreTel 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 Phone powers up, the Ethernet switch sends LLDP Data Units defined as LLDP_Multicast packets to the Phone.
2. The 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 10 below).

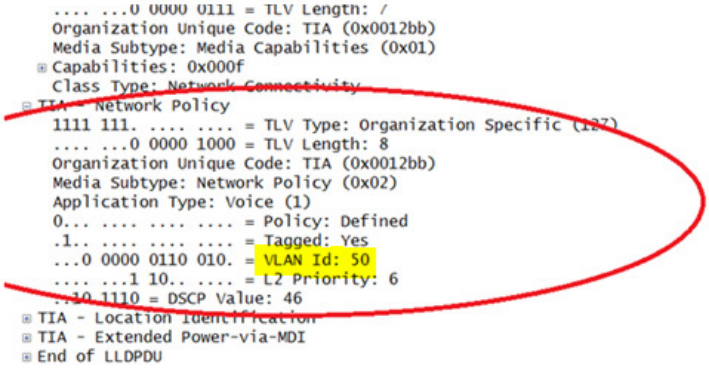

Figure 10

4. The 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 Phone via FTP downloads its configuration file, upgrades the Boot Image if needed as well as other required files and finally reboots.
6. The 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.

For more detailed information on configuring and troubleshooting Automatic VLAN assignment via LLDP please refer to the Knowledge Base article KB16607 and the ShoreTel System Administration Guide.

Understanding Quality of Service (QoS) Design

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. Data networks were not originally designed to support Voice traffic so special configuration is required for VoIP to achieve Toll quality on a data network. The voice configuration should comply with universally accepted standards for latency, jitter, and packet loss for VoIP. No part of the VoIP data networking infrastructure should have more than 150 msec one-way (or 300 msec round-trip) propagation delay between any two VoIP end-points, ShoreTel servers or ShoreGear switches, no more than 50 msec of jitter between VoIP media packets, and no more than 1% of packet loss for VoIP RTP media stream packets. QoS allows voice RTP media and signaling traffic to be prioritized higher than less time-sensitive data traffic on the network. Video is another time-sensitive traffic class that needs to be prioritized like Voice but typically not as high.

Even in a well-designed and segmented data network, congestion issues typically still arise in two general areas, links (i.e. between switches/routers) and output port buffers (i.e. on switches/routers). While many VoIP administrators think link congestion is the only trigger for QoS, output memory buffers actually trigger QoS more often and are built into every data network interface port. Input and output port buffers are a more limited memory resource compared to link speed and are used by every single packet whether links are congested or not. Most data hardware equipment manufacturers allocate both shared and dedicated memory buffer resources which can be managed manually as needed; however, the amount of memory used for output port buffer space does not increase exponentially compared to when link speeds increase exponentially on a particular switch or router. For example, when a switch port configured with a 1 Gbps connection speed is changed to a 10 Gbps connection speed or 100 Mbps connection speed is changed to a 1 Gbps connection speed, the speed mismatches between internal switch/router ports and the high ratio of access ports switching traffic to a single uplink port can put considerable contention or strain on the output memory buffers of a switch or router. When a particular output buffer fills up for a queue on a port, usually long before the link bandwidth is fully used, packets are tail-dropped with impunity according to the port's queue congestion-management and congestion-avoidance methods configured. Each switch/router port has multiple queues for sending packets more efficiently over a connection depending on the data equipment capabilities (i.e. the default queue - typical data traffic, priority queue - time-sensitive RTP traffic and other queues used for signaling and video traffic as needed). Without QoS configured, all traffic uses the default queue on each switch/router port. Default queues and classic data traffic congestion-avoidance methods are detrimental to all VoIP traffic! VoIP RTP media traffic needs to be sent in consistent intervals by mapping the traffic to the priority queue (separate from the default queue) on any given switch output port. Regardless of

available bandwidth, data and voice devices compete for available bandwidth in a survival of the fittest, best-effort manner. VoIP requires preferential and predictable bandwidth utilization, data traffic does not. This competition becomes more ruthless when bandwidth becomes scarcer on slower WAN links where bandwidth is typically 1 Mbps - 10 Mbps vs. a LAN, 100Mbps - 1000 Mbps.

> **IMPORTANT TIP**: The VoIP queues' bandwidth percentages for RTP and signaling traffic should be adjusted for the WAN compared to the LAN. The WAN queue bandwidth percentages should be based on what was purchased from the WAN Service Provider (e.g. MPLS). This will prevent the provider from demoting oversubscribed "platinum/gold" EF or AF31 traffic to a lower priority queue to be potentially delayed or dropped. Additionally, to ensure ShoreTel also doesn't attempt to oversubscribe the WAN link's EF bandwidth value, set the Admission Control Bandwidth appropriately for each site in Director.

To level the playing field or fields in this case, VoIP implementations require QoS at layer 2 (i.e. MAC) and also sometimes at layer 3 (i.e. IP). 802.1p is the standard defined by the Internet Engineering Task Force (IETF) that provides a mechanism for implementing QoS at the media access control (i.e. MAC) level or layer 2. QoS at layer 2 is also called CoS, Class of Service. CoS only exists at layer 2, where MAC addresses rule, within each VLAN. When all IP phones, ShoreTel servers, and ShoreGear switches are all on the same Voice VLAN (i.e. single site, one Voice VLAN, and no WAN), only layer 2 CoS needs to be implemented. When IP phones, ShoreTel servers and SG switches are on separate VLANs (e.g. IP Phones and SG switches on the Voice VLAN and ST server(s) on the Data VLAN), layer 3 QoS also needs to be applied otherwise when CoS marked traffic crosses between VLANs at layer 3, layer 2 CoS is lost (i.e. single or multiple sites, VoIP on multiple VLANs, or WAN is present). Layer 2 CoS values have to be mapped to corresponding layer 3 QoS values to work end-to-end on the appropriate switches/routers.

Layer 3 QoS is based on the Differentiated Services Code Point (i.e. DSCP or DiffServ) standard defined by the Internet Engineering Task Force (IETF) which specifies that each packet be marked or classified with a priority value in the 6-bit DS (i.e. Differentiated Services) field in the IP header. The DS field and ECN (i.e. Explicit Congestion Notification) field replaces the outdated IPv4 TOS field. The DiffServ Code Point is often set by the originating device, such as an IP Phone or assigned to packets as they enter a network device such as by data switch or router. Layer 2 CoS values are shown in Figure 11 below in the "Precedence" column while the corresponding layer 3 QoS values are also show in the "DSCP Values" columns.

QoS Class	Name (Used in ACL)	DSCP byte (Binary) DSCP in Blue	Hex (Hex) (used in ext ping)	DSCP 6-bits (Dec) (show cmd)	CoS (L2)	PHB (Alpha + number)	DSCP 8-bits (Dec)
Best Effort	routine	0000 0000	0x00	0	0	CS0	0 (0 – 7)
Less than Best Effort	priority	0010 0000 0010 1000	0x20 0x28	32 40	1	CS1 AF11 AF12 – 3	8 10 11, 12 (8 – 15)
Critical Data	immediate	0100 0000 0100 1000 0101 0000 0101 1000	0x40 0x48 0x50 0x58	64 72 80 88	2	CS2 AF21 AF22 AF23	16 18 20 22 (16 – 23)
Call Signaling	flash	0110 0000 0110 1000 0111 0000 0111 1000	0x60 0x68	96 **104**	**3**	CS3 **AF31** AF32 AF33	24 **26** 28 30 (24 – 31)
Video	flash-override	1000 0000 1000 1000	0x80 0x88	128 136	4	CS4 AF41 - 3	32 34, 36, 38 (32 – 39)
Voice Bearer	critical	1010 0000 1011 1000	0xA0 0xB8	160 **184**	**5**	CS5 **EF**	40 **46** (40 – 47)
Control Plane (Routing)	internet	1100 0000	0xC0	192	6	CS6	48 (48 – 55)
Control Plane (Routing)	network	1110 0000	0xE0	224	7	CS7	56 (56 – 63)

Figure 11

To summarize the most important QoS Design Principles;

1. All switches and routers must participate in the QoS infrastructure without exception to guarantee VoIP Toll quality end-to-end.
2. QoS is designed to handle congestion in two general areas, links (i.e. between switches/routers) and output port buffers (i.e. on switches/routers).
3. Default queues and classic data traffic congestion-avoidance methods are detrimental to all VoIP traffic!
4. Each switch/router port has multiple queues for sending packets more efficiently over a single link/connection via QoS depending on the data equipment capabilities (i.e. the default queue - typical data traffic, priority queue - time-sensitive RTP VoIP traffic and other queues used for VoIP signaling and video traffic as needed).
5. VoIP implementations require QoS/CoS at layer 2 (i.e. MAC) and also sometimes at layer 3 (i.e. IP).
6. When layer 2 CoS marked traffic crosses between VLANs at layer 3 (without layer 3 QoS), layer 2 CoS is lost.
7. Layer 2 CoS values have to be mapped to corresponding layer 3 QoS values to work end-to-end on the appropriate switches/routers.

The following sections offer recommendations and basic guidelines for implementing Quality of Service for the LAN and WAN when deploying a ShoreTel UC system on your network. Please use these examples as guidelines for discussion with network and security professionals to ensure implementation is in accordance with your corporate security and network policies and standards.

The following examples are taken from common layer 3 switches and routers such as Cisco, Juniper, HP Procurve, and Adtran to name a few. Actual commands and syntax may be different for your particular model, operating system, version and/or manufacturer. Please consult the manufacturer of your network equipment or an experienced network administrator for detailed instructions on configuring Quality of Service in your specific environment.

Configuring Quality of Service - LAN

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. This section will attempt to highlight the methods and basic configuration examples required to configure LAN based QoS/CoS using various common data hardware manufacturers.

In regards to Cisco LAN QoS/CoS configuration examples, the next section below, *Using Cisco Auto-QoS,* adequately covers how to use their automatic QoS configuration tools for layer 2 CoS and 3 QoS configuration. The follow on section, *Configuring Quality of Service – WAN,* will cover all layer 3 QoS configuration requirements and examples.

Cisco – 3750 (IOS) Example

```
!
mls qos map cos-dscp 0 8 16 26 34 46 48 56
mls qos srr-queue input priority-queue 1 bandwidth 10
mls qos srr-queue input cos-map queue 1 threshold 3 5 6
mls qos srr-queue input dscp-map queue 1 threshold 3 46 48
mls qos srr-queue output cos-map queue 1 threshold 3 5 6
mls qos srr-queue output cos-map queue 2 threshold 1 2 4
mls qos srr-queue output cos-map queue 2 threshold 2 3
mls qos srr-queue output cos-map queue 2 threshold 3 7
mls qos srr-queue output cos-map queue 3 threshold 3 0
mls qos srr-queue output cos-map queue 4 threshold 3 1
mls qos srr-queue output dscp-map queue 1 threshold 3 46 48
mls qos srr-queue output dscp-map queue 2 threshold 1 16 18 20 22 25 32 34 36
mls qos srr-queue output dscp-map queue 2 threshold 1 38
mls qos srr-queue output dscp-map queue 2 threshold 2 24 26
mls qos srr-queue output dscp-map queue 2 threshold 3 56
mls qos srr-queue output dscp-map queue 3 threshold 3 0
mls qos srr-queue output dscp-map queue 4 threshold 1 8
mls qos srr-queue output dscp-map queue 4 threshold 3 10 12 14
mls qos queue-set output 1 threshold 2 70 80 100 100
mls qos queue-set output 1 threshold 4 40 100 100 100
mls qos
!
```

```
!
vlan 110
 name Voice
!
!
!
interface FastEthernet1/0/1
 description N1 - Sue Fesler
 switchport access vlan 3
 switchport mode access
 switchport voice vlan 110
 srr-queue bandwidth share 1 70 25 5
 srr-queue bandwidth shape 3 0 0 0
 priority-queue out
 mls qos trust cos
 spanning-tree portfast
!
interface FastEthernet1/0/2
 description N25
 switchport access vlan 101
 switchport mode access
 switchport voice vlan 110
 srr-queue bandwidth share 1 70 25 5
 srr-queue bandwidth shape 3 0 0 0
 priority-queue out
 mls qos trust cos
 spanning-tree portfast
!
```

HP Procurve – 2520G-24-POE Example

```
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
```

```
vlan 10
   name "VoIP_VLAN"
   untagged 5
   tagged 13-14,17,23-24
   voice
   no ip address
   exit
```

Juniper – EX4200 Example

Create forwarding classes mapped to specific queues, video optional

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, video optional

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 af31

Create schedulers with buffer size, queue priority etc. , video optional

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), video optional

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), video optional

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 Default Forwarding Class to EF for each IP Phone Interface on the Voice VLAN

set ethernet-switching-options voip interface ge-0/0/0.0 vlan vlan_voice

set ethernet-switching-options voip interface ge-0/0/0.0 forwarding-class expedited-forwarding

set ethernet-switching-options voip interface ge-0/0/1.0 vlan vlan_voice

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

Set "Port Fast" using EDGE command on connected ShoreTel 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.)

Adtran - NetVanta 1335 PoE Example

```
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 24 32 40 48 56 to 0 1 2 3 4 5 6 7
!
!
vlan 20
name "VOICE_VLAN"

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

Any data hardware manufacturers not covered above can easily find similar configuration syntax by comparing the multiple examples to their data hardware manufacturer's respective QoS Implementation Guides to see the common configuration requirements in order to practically apply them to any switch/router QoS platform in a similar manner.

Every data hardware manufacture will include the same essential components implicitly or explicitly in their LAN QoS/CoS configuration such as;

- 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 map layer 2 CoS values to layer 3 DSCP values.
- Bind CoS configuration to all VoIP switch/router interfaces.
- Validate configurations.

Using Cisco Auto-QoS

Cisco has a somewhat automatic or scripted QoS configuration feature with various options that generate automatic 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 and Cisco CatOS firmware trains. This can save you from manually configuring the entire QoS configuration on each switch or router as well as trying to figure out what Cisco QoS best practices to implement based on your production data network design and configurations.

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. 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.

After Auto-QoS has finished, compare the generated QoS configuration in each switch or router to the QoS requirements for ShoreTel VoIP in all QoS sections and manually change or add any needed configuration 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.

The following examples show how to enable "Auto-QoS" on most Cisco CatOS and IOS based switches on the enterprise data network.

Cisco Catalyst OS	Cisco IOS Software
Enable QoS Globally	
set qos enable	mls qos
Enable Auto-QoS Globally	
set qos autoqos	auto qos or auto qos srnd4
Configuring Interface QoS	
set qos wrr 1p2q2t 30 70	srr-queue bandwidth share 10 10 60 20
	priority-queue out
set port qos <mod/ports> autoqos trust dscp	mls qos trust dscp
set port qos <mod/ports> autoqos trust cos	auto qos voip trust
Configuring Interface for Shoretel Voice	
	switchport mode access
set vlan XX <mod/ports>	switchport access vlan 10
set port auxiliaryvlan <mod/ports> XX	switchport voice vlan 20
set cdp disable <mod/ports>	no enable cdp
set spantree portfast <mod/ports> enable	spanning-tree portfast

Figure 12

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

mls 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.)

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.

Interface level QoS commands add configuration lines to each Ethernet interface. The lines added to each interface determine how the switch will handle marked traffic from the ShoreTel phones as well as ShoreGear switches and ShoreTel 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 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 different syntax and/or some commands that might be hidden in the show running configuration output because they are default.

Shown in Figure 13, output highlighted in blue is the typical Cisco IOS switch/router Ethernet port QoS commands for connected ShoreTel IP Phones, SG-Switches and ST Servers.

QoS Cisco IOS Interface Commands

```
interface FastEthernet1
  switchport mode access
  switchport access vlan 10
  switchport voice vlan 100
  srr-queue bandwidth share 10 10 60 20
  priority-queue out
  mls qos trust dscp
  auto qos voip trust
  no cdp enable
  spanning-tree portfast
```

Figure 13

srr-queue bandwidth share 10 10 60 20 - Enables Shaped Round Robin (SRR) egress queuing and assigns 10%, 10%, 60% and 20% 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.

```
!
mls qos map cos-dscp 0 8 16 26 34 46 48 56
mls qos srr-queue input priority-queue 1 bandwidth 10
mls qos srr-queue input cos-map queue 1 threshold 3 5 6
mls qos srr-queue input dscp-map queue 1 threshold 3 46 48
mls qos srr-queue output cos-map queue 1 threshold 3 5 6
mls qos srr-queue output cos-map queue 2 threshold 1 2 4
mls qos srr-queue output cos-map queue 2 threshold 2 3
mls qos srr-queue output cos-map queue 2 threshold 3 7
mls qos srr-queue output cos-map queue 3 threshold 3 0
mls qos srr-queue output cos-map queue 4 threshold 3 1
mls qos srr-queue output dscp-map queue 1 threshold 3 46 48
mls qos srr-queue output dscp-map queue 2 threshold 1 16 18 20 22 25 32 34 36
mls qos srr-queue output dscp-map queue 2 threshold 1 38
mls qos srr-queue output dscp-map queue 2 threshold 2 24 26
mls qos srr-queue output dscp-map queue 2 threshold 3 56
mls qos srr-queue output dscp-map queue 3 threshold 3 0
mls qos srr-queue output dscp-map queue 4 threshold 1 8
mls qos srr-queue output dscp-map queue 4 threshold 3 10 12 14
mls qos queue-set output 1 threshold 2 70 80 100 100
mls qos queue-set output 1 threshold 4 40 100 100 100
mls qos
!
```

Example Global QoS Queue Mappings

Figure 14

Queue Share %	Queue Mapped	QoS CoS Value	QoS DSCP Decimal Value
10	1	5	46
10	2	3	26
60	3	0	0
20	4	1	8

Example Queue Information Matrix

Figure 15

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.

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

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

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

show 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.

QoS Cisco CatOS Global Commands

set qos enable - enables QoS on the Catalyst switch.

set qos autoqos - executes global Auto-QoS on a Catalyst switch.

The global Auto-QoS commands with CatOS are functionally the equivalent to its IOS command counterparts.

QoS Cisco CatOS Interface Commands

```
interface fastethernet 5/10
  set qos wrr 1p2q2t 30 70
  set port qos 5/10 autoqos trust dscp
  set port qos 5/10 autoqos trust cos
  set vlan 10 5/10
  set port auxilaryvlan 5/10 20
  set cdp disable 5/10
  set spantree portfast 5/10 enable
```

Figure 16

set qos wrr 1p2q2t 30 70 - Enables Weighted Round Robin (WRR) scheduler egress queuing and in this case assigns 30% and 70% to the 2 WRR egress queues (i.e. 2q), each with two configurable WRED-drop thresholds (i.e. 2t), on the port for egress traffic. Each of the 2 queues is guaranteed that percentage and can burst above that if other queues are idle. Low Latency Queuing used with the strict priority queue (i.e. 1p) allows delay-sensitive content, such as voice over IP packets, to be sent before other categories of packets are sent. This gives delay-sensitive data preferential treatment over other traffic.

The percentages used are just an example and need to be adjusted for your network requirements that will not drop VoIP packets. Different Catalyst switch models and modules support various quantities of queues per port.

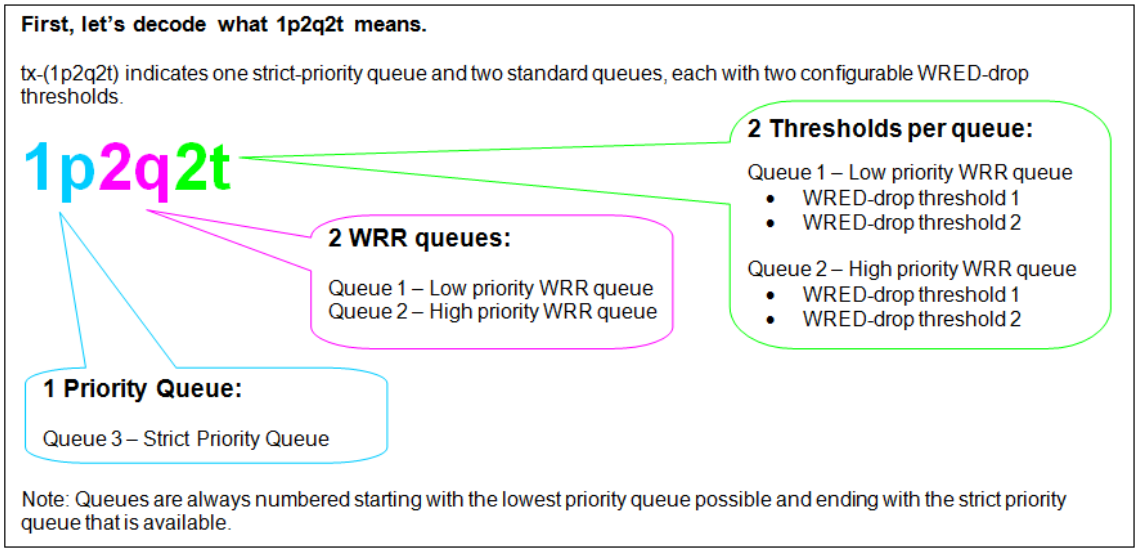

Figure 17

set port qos <mod/ports> autoqos trust-dscp - Sets the interface to trust DSCP values received from the phone.

set port qos <mod/ports> autoqos trust-cos - Sets the interface to trust VLAN-tagged Class of Service (CoS) values received from the phone.

Figure 18 shows a CatOS example with explanation how CoS is mapped to the respective queues with thresholds.

Default assignment for each CoS in a 1p2q2t port:

Command:
set qos map 1p2q2t tx q# thr# cos coslist

Also, CoS 5 (voice traffic) is assigned to the strict priority queue.

Default is as follows:

Frames with CoS 0, 1, 2 and 3 go to the low-priority transmit queue (queue 1)
Queue 1 has CoS 0 and 1 assigned to its first threshold, and CoS 2 and 3 assigned to its second threshold.

```
set qos map 1p2q2t tx 1 1 cos 0
set qos map 1p2q2t tx 1 1 cos 1
set qos map 1p2q2t tx 1 2 cos 2
set qos map 1p2q2t tx 1 2 cos 3
```

Frames with CoS 4, 6 and 7 go to the high-priority transmit queue (queue 2)
Queue 2 has CoS 4 and 6 assigned to its first threshold, and CoS 7 is assigned to its second threshold.

```
set qos map 1p2q2t tx 2 1 cos 4
set qos map 1p2q2t tx 2 1 cos 6
set qos map 1p2q2t tx 2 2 cos 7
```

Frames with CoS 5 go to the strict-priority transmit queue (queue 3) where the switch drops frames only when the buffer is 100 % full.

```
set qos map 1p2q2t tx 3 1 cos 5
```

Figure 18

Displaying Auto-QoS CatOS Information

show qos status

show port auxiliaryvlan <vlan number>

show port qos <mod/port>

show queueing int <interface name> (displays packets dropped per queue) [*clear qos statistics*]

sh qos info run <interface name>

sh qos statistics <interface name>

show qos info config <interface name>

When you enable Auto-QoS, traffic is automatically classified based on the traffic type and ingress packet label. The switch uses the resulting classification to set and choose the appropriate egress queue.

Please consult with your network professional or the Cisco Technical Assistance Center for further details or questions regarding the configuration of Cisco Auto QoS on Cisco LAN switches.

Configuring Quality of Service - WAN

A WAN data connection is required to connect each remote site L3 switch or router to the headquarter site L3 switch or router. Certain WAN connections as well as redundant WAN connections require a router at each site but other WAN connections with an Ethernet handoff only require a layer-3 switch. 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, 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 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 sites together. Because layer 3 IP routing is required to route traffic between VLANs or essentially between a LAN and WAN, layer 3 QoS is also required to maintain layer 2 QoS/CoS beyond its original VLAN.

This section will highlight the methods and basic configuration examples required to configure WAN based QoS policies using Cisco for example with ShoreTel.

First, ShoreTel allows you to set the DSCP values for all voice traffic using the web-based administration tool in Director. These DSCP settings are used for all Real-Time Protocol (i.e. RTP) packets that are sent from all ShoreTel IP phones, ShoreGear switches, and ShoreTel servers. ShoreTel Call Control and Video DSCP self marking values were introduced as of ShoreTel 13.1 and ShoreTel 14.1.

In 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 19.

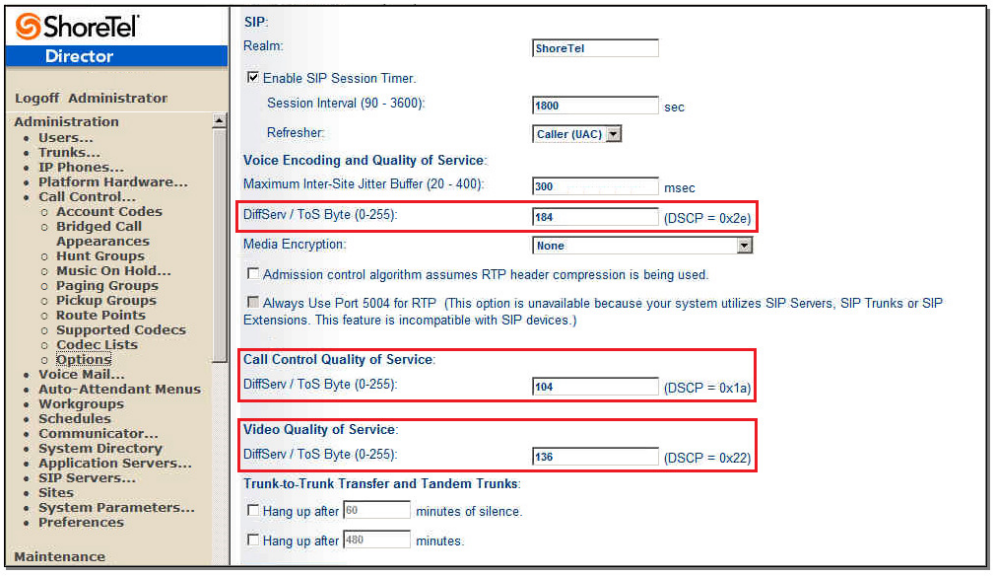

Figure 19

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 104 which equates to the Assured Forwarding 31 DSCP setting (i.e. AF31). *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 ShoreTel deployment as it requires a one-time reboot of all ShoreTel servers, ShoreGear switches and ShoreTel IP Phones in your organization to take effect.

Mechanisms to generally create and enforce QoS policies include:

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

TIP: A complete discussion of QoS policies for WAN technologies such as MPLS, Frame-Relay, Asynchronous Transfer Mode (ATM), Point-to-Point and Multilink over PPP (MLPPP) are beyond the scope of this document.

In addition to voice and video media ports, ShoreTel 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 following TCP and UDP ports are listed by ShoreTel release to ensure the right QoS policies are created on your data network for the version of ShoreTel installed. Prior to ShoreTel 13.1 and 14.1, all ShoreTel IPBX 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. To mark the signaling traffic, the data network administrator needs to create a policy map to manually mark the appropriate ports with DSCP AF31 for proper prioritization. Starting with ShoreTel 13.1 and 14.1, ShoreTel self-marks the appropriate signaling ports with DSCP AF31 so data network administrators simply trust and map the traffic appropriately. Refer to Figure 20 below for the updated ShoreTel port map for each ShoreTel release listed below. There are certain scenarios where with ShoreTel 13.1 and 14.1 or newer, a service policy matching and marking signaling traffic is required on L3 switch interfaces when there are multiple VLANs that carry VoIP traffic. In order for the QoS marking to be preserved across L3, one of the policies below will need to be applied and built using the ports in the figure below for the respective ShoreTel Release.

ShoreTel Port Usage - UDP Signalling VoIP Traffic (AF31)	ShoreTel 10	ShoreTel 11	ShoreTel 12	ShoreTel 13	ShoreTel 14
UDP 2427: MGCP Call Control	Ω	Ω	Ω	α	α
UDP 2727: MGCP Call Control	Ω	Ω	Ω	α	α
UDP 5060: SIP	Ω	Ω	Ω	α	α
UDP 5440: Location Service (LSP)	Ω	Ω	Ω	α	α
UDP 5441: Call Control (ShoreSIP)	Ω	Ω	Ω	α	α
UDP 5442: Switch Call Control – DRS	Ω	Ω	Ω	α	α
UDP 5443: Bandwidth Manager (BWM)	Ω	Ω	Ω	α	α
UDP 5445: Admission Control (ADM)	Ω	Ω	Ω	α	α
UDP 5446: Switch Call Control – DRS Keepalive	Ω	Ω	Ω	α	α
UDP 5450: SA-100/400 CMCA Web Share - PING Sync			Ω	α	α
ShoreTel Port Usage - TCP Signalling VoIP Traffic (AF31)	**ShoreTel 10**	**ShoreTel 11**	**ShoreTel 12**	**ShoreTel 13**	**ShoreTel 14**
TCP 5060: SIP (and all related/accepted TCP connections UDP 1024-65535 RTP)	Ω	Ω	Ω	α	α
TCP 5061: SIPS Call Control					α
TCP 5430: ShoreTAPI (DTAS to remote TMS)				α	α
TCP 5447: Client Application Server i.e. CAS (SSL)		Ω	Ω	α	α
TCP 5448: IP Phone to CAS over https					α
TCP 5452: TMS to Switch NCC			Ω	α	α
ShoreTel Port Usage - TCP & UDP Signalling VoIP Traffic (AF31)	**ShoreTel 10**	**ShoreTel 11**	**ShoreTel 12**	**ShoreTel 13**	**ShoreTel 14**
TCP & UDP 31453: Used by ShoreTel ECC for Client Server Communication	Ω	Ω	Ω	√**	√**
ShoreTel Port Usage - RTP VoIP Traffic (EF)	**ShoreTel 10**	**ShoreTel 11**	**ShoreTel 12**	**ShoreTel 13**	**ShoreTel 14**
UDP 5004: Media Port if not dynamic or SIP enabled, ST Director Configurable	Ω	Ω	Ω	α	
UDP 10000 – 10550: Default Media Port Range, ST Director Configurable	∞	∞	∞	α	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.					
∞ = unlimited dynamic port range used (1024-65535)					
α = Valid port used in ST release. Required QoS AUTOMATICALLY marked by ShoreTel device or server.					
Ω = Valid port used in ST release. Required QoS MANUALLY marked on data network for ShoreTel device and server.					

Figure 20

The step by step example below represents the general configuration commands to build a layer 3 QoS policy configuration on a L3 switch or router to be applied on the appropriate output interfaces.

Cisco

Step 1: Define the classes of traffic on your network

(** comments are not part of the configuration)

ShoreTel 12 and older (ST13.1, 14.1 and newer - apply to LAN interfaces if multiple VLANs carry VoIP traffic)

```
class-map match-any VoIP_AUDIO          ** Defines the VoIP_AUDIO class of traffic
match ip dscp ef                        ** Tells it to match anything already marked as EF (184)
match protocol rtp audio                ** Tells it to also match any other RTP/Audio traffic
class-map match-any CALL_CONTROL        ** Defines the CALL_CONTROL class of traffic
match ip dscp af31                      ** Match anything already set to DSCP AF31
match access-group 103                  ** Match anything in access list 103 (below)
```

ShoreTel 13.1, 14.1 and newer (apply to WAN interface(s) or connections to managed WAN router)

```
class-map match-any VoIP_AUDIO          ** Defines the VoIP_AUDIO class of traffic
match ip dscp ef                        ** Tells it to match anything already marked as EF (184)
match protocol rtp audio                ** Tells it to also match any other RTP/Audio traffic
class-map match-any CALL_CONTROL        ** Defines the CALL_CONTROL class of traffic
match ip dscp af31                      ** Match anything already set to DSCP AF31
```

Step 2: Apply a Policy to the classes of traffic defined above

```
policy-map VOIP                    ** Define a policy map and give it the name VOIP
class VoIP_AUDIO                   ** Assigns the VoIP_AUDIO class the following
  priority percent 20              ** Reserves 20% of the bandwidth for VoIP in the highest priority queue
  set ip dscp ef                   ** Makes sure priority traffic is marked EF as it goes through the WAN
class CALL_CONTROL                 ** Assigns the AF31-CLASS class to the following
  bandwidth 20                     ** Reserve 20% of the bandwidth for signalling in a medium queue higher than default
  set ip dscp af31                 ** Makes sure signalling traffic is marked AF31 as it goes through the WAN
class class-default                ** States all traffic not matching the above use the default queue
  set dscp default                 ** Make sure it is marked with DSCP 0 (best effort) to the WAN
  fair-queue                       ** Use Cisco's recommended fair queuing policy for best effort traffic
```

Step 3: Define ACL, ports and protocols to be treated as call control traffic

ShoreTel 12 Example (refer to Figure 20 for other ShoreTel Release specific port usage to include)

```
access-list 103 remark : ShoreTel VoIP Call and System Control (AF31) ST12
access-list 103 permit udp any any eq 2427
access-list 103 permit udp any any eq 2727
access-list 103 permit udp any any eq 5060
access-list 103 permit udp any any range 5440 5443
access-list 103 permit udp any any range 5445 5446
access-list 103 permit udp any any eq 5450
access-list 103 permit tcp any any eq 5060
access-list 103 permit tcp any any eq 5447
access-list 103 permit tcp any any eq 5452
access-list 103 permit tcp any any eq 31453 ** Only for Contact Center
access-list 103 permit udp any any eq 31453 ** Only for Contact Center
```

Step 4: Apply the policy map to the outgoing interface on the router or L3 switch

Router Example (apply to WAN ingress/egress interfaces)

```
interface serial0/0
description : T1 to MPLS WAN
bandwidth 1536
ip address 209.191.1.1 255.255.255.0
service-policy output VOIP
```

L3 Switch Example (apply to LAN interfaces if multiple VLANs carry VoIP traffic)

```
interface GigabitEthernet 1/1
service-policy output VOIP
```

Step 5: Confirm the QoS policy is applied to the WAN 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 priority queue configuration or that you may have too much non-voice traffic being placed in the priority queue. Make the necessary adjustments as needed and continue to monitor.

One command below shows the policy applied to the interface and any drops associated with the queues.

show policy-map interface serial0/0

```
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
```

Juniper

Step 1: Create firewall filter VOIP to match and map ShoreTel RTP and Signaling traffic to correct forwarding classes

ShoreTel 13 Example (refer to Figure 20 for other ShoreTel 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

Step 2: 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 high code-point af31

Step 3: Bind Rewrite Rules to "VLAN" interfaces where VoIP traffic exists including Communicator

set class-of-service interfaces vlan unit 5 rewrite-rules dscp v4rw

set class-of-service interfaces vlan unit 2 rewrite-rules dscp v4rw

set class-of-service interfaces vlan unit 10 rewrite-rules dscp v4rw

Step 4: Only create "Interface" Rewrite Rules to mark or remark traffic on untrusted uplinks/downlinks (typically from other non-Juniper switches that cannot mark QoS traffic if VLAN Rewrite Rules cannot)

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 af31

Step 5: Only bind Interface Rewrite Rules to core/edge interfaces from an untrusted source, not phones!

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

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. ShoreTel 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.

ShoreTel'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 ShoreTel 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 ShoreTel 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 ShoreTel 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 ShoreTel switches set the Do Not Fragment bit by default. A network using IPsec tunnels as VPN transport between sites will drop ShoreTel 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 ShoreTel, please contact ShoreTel 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.

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 ShoreTel 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"

IEEE 802.1Q Tagging:

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

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

Cisco Configuration Guides and References:

Cisco Medianet Campus QoS Design 4.0 (SRND4)

http://www.cisco.com/en/US/docs/solutions/Enterprise/WAN_and_MAN/QoS_SRND_40/QoSCampus_40.html#wp1104132

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

Appendix A: Juniper CoS/QoS

For information regarding a validated Juniper QoS Configuration Example with a LAN only configuration that works with ShoreTel VoIP on the Voice VLAN, refer to the Knowledge Base article KB16850 - Juniper EX Series Switches CoS-QoS ShoreTel VoIP Configuration Example that can be found on the ShoreTel Support website.

Document and Software Copyrights

Trademarks

Disclaimer

ShoreTel tests and validates the interoperability of the Member's solution with ShoreTel's published software interfaces. ShoreTel 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). ShoreTel 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 ShoreTel's published interfaces.

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

Company Information

ShoreTel, Inc.
960 Stewart Drive
Sunnyvale, California 94085 USA
+1.408.331.3300
+1.408.331.3333 fax

Author

CHAD HORTON
Technical Account Manager
chorton@ShoreTel.com
+1 (512) 551-7185 Tel/Fax/Cell