Application Note

ShoreTel™

ST-0131 April 28, 2006

Best Practice Recommendations for Implementing VLANs in a ShoreTel VoIP Environment with IP Phones

This application note discusses the use of Virtual LANs and DHCP scopes in a ShoreTel Voice over IP environment, particularly with the use of IP Phones.

Introduction

Network Administrators must consider a multitude of complex configuration options and networking parameters when designing a large local area network (LAN). Those options can include the use of Virtual LANs.

This document will briefly describe the use and purpose of VLANs and then explain, in detail, several implementation strategies for VLANs in a Voice over IP (VoIP) network. Configuration samples are included. For simplicity sake all configuration examples are given using Cisco IOS command structures. Please refer to your networking hardware's documentation in order to apply the ideas and concepts presented in this document rather than using these exact configuration examples.

Defining VLANs

Virtual LANs (VLANs) are a networking design construct by which more than one layer-2 (L2) network can exist on a single network segment while still separating broadcast domains.

Consider the design differences between the following two networks: The first diagram (figure 1) illustrates a campus network with two physical layer-2 Ethernet switches. These switches are layer-2 only and do not support VLANs. All devices on a single switch must therefore be in the same layer-2 broadcast domain and must be assigned IP addresses in the same IP subnet.

In this first network, each switch has its own unique IP subnet and its own broadcast domain. All ports on the switch are assigned to (that is, are members of) a single subnet/broadcast domain and devices on that switch can only communicate to devices on another subnet by sending traffic to an external, layer-3 device (e.g. a router) which acts as the default gateway for the devices on each subnet.

In figure 1, if a device needs to be reassigned from one network to the other (say, an employee is reassigned from the QA department to the HR department) the device needs to be physically disconnected from the original switch, configured with a new IP address and default gateway and physically reconnected to the other switch.

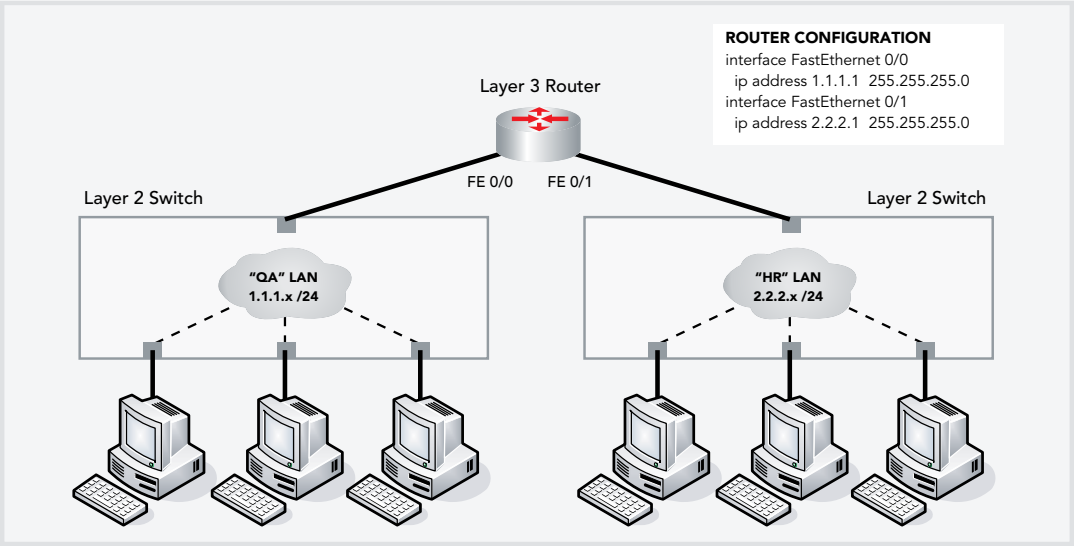
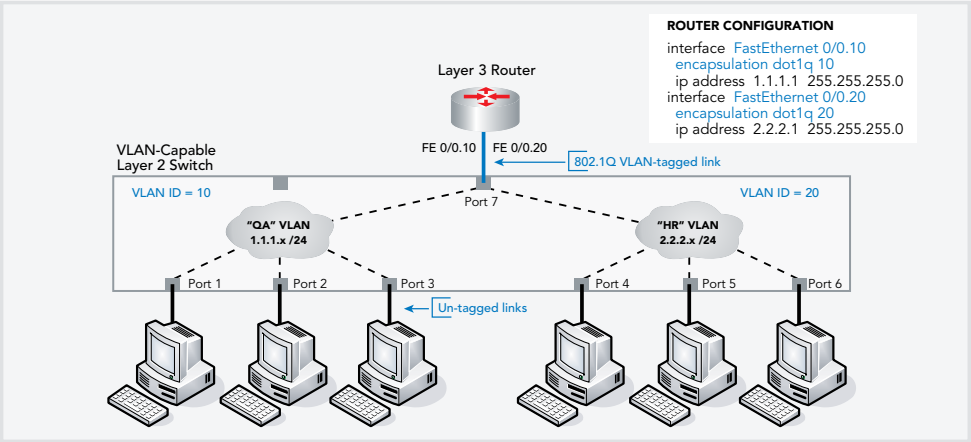


Figure 1



LAYER 2 SWITCH CONFIGURATION

```
vlan 10 name QA
interface FastEthernet1
 switchport mode access (the default)
 switchport access vlan 10
interface FastEthernet2
 switchport access vlan 10
interface FastEthernet3
 switchport access vlan 10
vlan 20 name HR
interface FastEthernet4
 switchport access vlan 20
 interface FastEthernet5
 switchport access vlan 20
interface FastEthernet6
 switchport access vlan 20
interface FastEthernet7
 switchport mode trunk
 switchport trunk encapsulation dot1q
```

Figure 2.

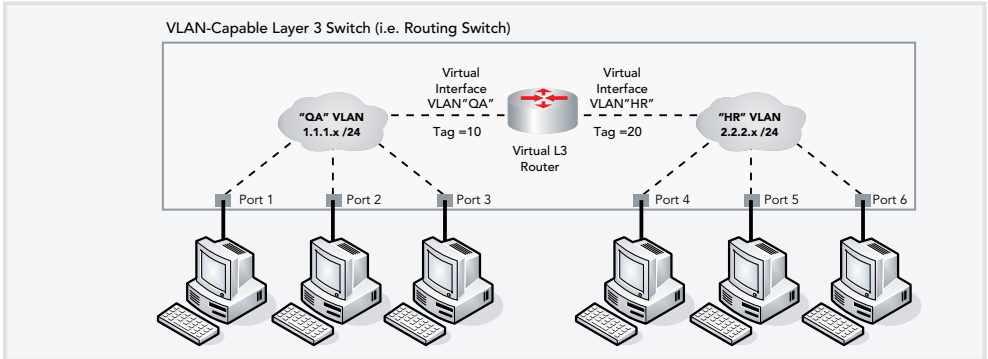
In the second diagram (figure 2) the two non-VLAN-capable L2 switches have been replaced by a single VLAN-capable L2 switch. (Note: newly added configuration settings have been colored in BLUE.)

Ports in the switch now must be configured by the administrator to be assigned to one particular VLAN or the other. Ports in the switch are now no longer physically restricted to being in a single LAN but can be logically, or virtually, assigned to a logical LAN, called a Virtual LAN (VLAN). All ports in this new network can now be dynamically assigned to either the QA VLAN or the HR VLAN and the broadcast domains for the two "virtual" networks are contained and isolated by the software running on the switch. Packets sent within one virtual network stay within the VLAN. Each packet is marked, internally within the switch, by a VLAN ID number called a VLAN tag (generally a number between 1 and 4096) to identify which VLAN it belongs to. The tags, though used internally, 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."

The devices within one VLAN still need to send packets to a default gateway to be routed to another subnet. And since the switch in this example is a layer-2 only switch (and therefore has no ability to route packets, only switch packets) an external router is still required. But we can now take advantage of a mechanism of VLANs called "VLAN tagging." VLAN tagging can be configured when the administrator desires traffic from more than one VLAN to be carried on a single Ethernet cable. By configuring a switch port to be a "VLAN-tagged" switch port, and by assigning that port to carry traffic for more than one VLAN, each packet that exits on the switch will have an additional 4-byte VLAN tag inserted into the Ethernet packet. 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 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 tags assigned to it.

In this example, packets that are sent from the QA subnet to the router leave the switch on port 7 tagged with a VLAN ID of 10 (the administrator's chosen ID for that VLAN). The router will route the packet from one of its sub-interfaces to its other sub-interface and resend the new packet out the same physical interface back to the switch; but this time the packet will have a VLAN ID tag of 20. The switch will deliver the received packet to the proper destination device in VLAN 20 (on the HR VLAN).

In the third diagram (figure 3) we have upgraded from a Layer-2, non-routing switch to a Layer-3, routing switch, often called an "L3 switch." Layer-3 switches have built-in routing capabilities and can route packets between VLANS without the need for an external router.



LAYER 3 SWITCH CONFIGURATION

```
. . . . . .
ip routing
interface VLAN_10
 description : QA Network
 ip address 1.1.1.1 255.255.255.0
interface VLAN_20
 description : HR Network
 ip address 2.2.2.1 255.255.255.0
. . . . . .
```

Figure 3.

In summary, VLANs can offer several advantages to a network administrator. By adding VLANs and VLAN tagging to a network design a network administrator can purchase fewer switches, relocate users from one VLAN to another far easier and can conserve on total port usage and expense on both the Ethernet switches and the routers by sending traffic for more than VLAN on a single port.

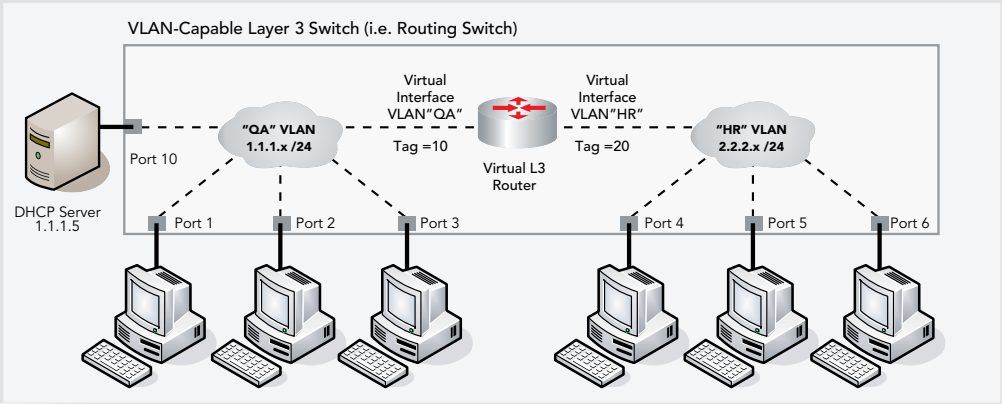
Conversely, adding VLANs to a network design greatly increases its complexity and should only be done when the IT staff controlling a network has a thorough understanding of networking, IP subnetting, VLANs and the specific configuration tools and options their network equipment provides

DHCP

A Dynamic Host Configuration Protocol (DHCP) Server provides an automated way for devices on a network to be assigned IP address information without an administrator having to manually edit configuration settings on each and every network device. This is commonly used for assigning network addresses and information to workstations and IP phones.

Figure 4 adds a DHCP server to our sample network topology. There is a single DHCP server on the QA VLAN which is configured with settings for both VLANs (each group of setting is called a "scope"). When a station on the QA VLAN makes a broadcast request for an IP address, the DHCP server will respond with IP address and network information directly to the requesting station. When a device on the HR network makes a broadcast DHCP request for an IP address, the router on that network (in this case, an internal virtual router inside the L3 switch) needs to forward that request to the DHCP server in the QA VLAN. This concept is called "DHCP relay" (also called "BootP Relay" or an "IP Helper Address" by some vendors).

Please note that, as of this writing, ShoreTel does not support the use of "Super Scopes" on Microsoft DHCP Server software. Please use traditional scopes and scope options when using a Microsoft DHCP server to avoid potential problems which can result in IP Phones that do not receive proper IP addresses when they renew their DHCP address, usually done at ½ the lease interval.



LAYER 3 SWITCH CONFIGURATION

```
interface FastEthernet10
 switchport access vlan 10

interface VLAN20
 description : HR Network
 ip address 2.2.2.1  255.255.255.0
 ip helper-address 1.1.1.5
```

DHCP SERVER CONFIGURATION

```
Scope "QA"
 Address Range: 1.1.1.100 – 1.1.1.199
 Subnet Mask:  255.255.255.0
 Default Router: 1.1.1.1
Scope "HR"
 Address Range: 2.2.2.100 – 2.2.2.199
 Subnet Mask:  255.255.255.0
 Default Router: 2.2.2.1
```

Figure 4.

Voice over IP, VLANs and QoS Considerations

Finally we add IP Phones and Voice over IP (VoIP) to our network topology.

In many cases it is completely unnecessary to add VLANs to your network in order to support ShoreTel VoIP. Some vendors have a difficult time guaranteeing adequate latency minimums and quality of service (QoS) without forcing every implementation to deploy VLANs. Also, this often means that their VoIP solution will not work on network equipment (e.g. switches, routers, access points, etc.) from other vendors, trapping you into a single vendor for every component of your network infrastructure regardless of it's quality or suitability to your needs.

ShoreTel has one of the best voice sampling, audio digitizing and packetization processing in the VoIP industry. It is common to deploy several hundred ShoreTel IP phones intermixed with several hundred general-use workstations in the same campus LAN environment and have no need to deploy VLANs or implement QoS on the LAN. This is true even when using ShoreTel's high quality, Linear Broadband codec for intra-site calls on the LAN.

The ShoreTel Linear Broadband codec generates a digitized voice payload of about 256Kbps. When you add in the overhead for RTP & UDP encapsulation, IP packetization and Ethernet framing, a single voice conversation generates a stream of real-time audio packets of approximately 309Kbps in each direction.

If that IP phone is using a 10Mbps Ethernet link, an active VoIP call consumes approximately 3% (309K/10M) of the available bandwidth on that link. If that IP phone is

connected with a 100Mb, full-duplex Ethernet link the conversation equates to about 0.3% of the link bandwidth. Clearly, bandwidth consumption is not an issue for delivering high-quality voice in a ShoreTel IP phone deployment.

Next, consider the potential degradation in voice quality caused by added delay. All ShoreTel IP phones have a dual-port, full-duplex, 10/100Mb, auto-sensing Ethernet switch embedded into the hardware of the phones. This allows a computer's Network Interface Card (NIC) to be daisy-chained through the phone enabling a "single cable to the desktop" environment. This can produce considerable savings on the number of Ethernet switch ports needed as well as savings on cabling costs. But what if the PC is performing a large file transfer? We don't want our small voice packets getting stuck behind a queue of large data packets as they traverse through the phone and are transmitted upstream to the Ethernet switch. To remedy this, each ShoreTel IP phone has built in priority queuing mechanisms to place all outbound voice packets ahead of the outbound data packets. Cleary delay, specifically serialization delay caused by daisy-chaining PCs through IP phones, will not cause degraded voice quality on a ShoreTel IP phone deployment.

Next, consider packet loss on the LAN and the flow of packets once they are received by the Ethernet switch. ShoreTel requires a mid-tier to enterprise-class Ethernet switching infrastructure. This means that your switches should have the following features:

- IP manageable (i.e. have an IP address that you can telnet or web-browse to for administration)
- Be able to report on errors such as CRC errors, runts, jumbos and interface resets
- Have a non-blocking, or near-non-blocking backplane (often called the "switching fabric")
- Have high speed uplinks for inter-switch connections (i.e. copper Gb or fiber Gb uplink ports)

If your topology includes older switches that are not near-wire-speed, includes hubs, includes consumer-grade switches that provide no statistics or error reporting, or if you use 10 or 100Mb connections for uplinks you need to consider upgrading to newer switches. Additional optional features that are not required but may be beneficial when looking for a new Ethernet switches include:

- Ability to support VLANs (VLAN capable)
- Ability to route internally (L3 switch)
- Power over Ethernet Support (IEEE 802.3af)
- Ability to do bi-directional port mirroring (for troubleshooting)
- Ability to configure QoS settings (based on VLAN, physical port, UDP port, DCSP value, etc.)

If your switched network topology uses 100Mb full duplex links to your stations and IP phones; is comprised of near-non-blocking switches at the edge; uses managed switches that report errors and provide statistics; and use Gb uplinks to connect to core switches … then every IP voice packet that is received in an edge switch will have nearly 100% chance of reaching its destination anywhere on your entire LAN without the need to configure advanced QoS, prioritization, queuing strategies or complex VLAN topologies.

In summary, adding voice to your data network should not be the single guiding factor for moving to a VLAN-architecture on your network. But—if you have other, legitimate, well-considered reasons for moving to a VLAN-based topology (such as security reasons, administrative reasons, traffic isolation reasons, etc.) then the ShoreTel components will conform very nicely to your desired topology. Each ShoreTel IP phone can be dynamically configured to support VLANs and VLAN tagging which we will discuss in the next section.

ShoreTel IP Phones in a VLAN Environment

ShoreTel leverages the use of VLANs and DHCP servers to integrate into the network topology that you, the network administrator, have decided is most appropriate for your LAN topology. We do 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 hardware supports the minimum recommended requirements you are free to deploy the equipment and network topology that works best for you.

In the final diagram (figure 5) we have added a mixture of ShoreTel IP phones connected by themselves as well as phones with PC workstations daisy-chained through them, and a VLAN dedicated for voice.

In this topology the PCs need to get proper information for the IP subnet they are in and need to communicate to the switch using untagged Ethernet packets. The stand-alone ShoreTel IP phones need to dynamically discover the ShoreTel server information as well as details about the Voice VLAN to connect to and what VLAN tag to insert into their Ethernet packets. In addition to tagging their own voice packets with the Voice VLAN tag ID, the IP phones with PCs connected behind them need to be able to pass data packets destined to and from the PCs NIC through the phone. These "pass-through" data packets need to be left entirely untagged.

You start by creating a new VLAN on the L3 switch:

LAYER 3 SWITCH CONFIGURATION

```
interface VLAN30
 description : Voice Network
 ip address 3.3.3.1 255.255.255.0
 ip helper-address 1.1.1.5
```

Then you modify the switch ports to allow them to accept VLAN tags and assign any untagged packets the port receives to the correct VLAN for the PC workstation connected behind the IP phone. Finally you add a switch port for the ShoreTel server on the Voice VLAN:

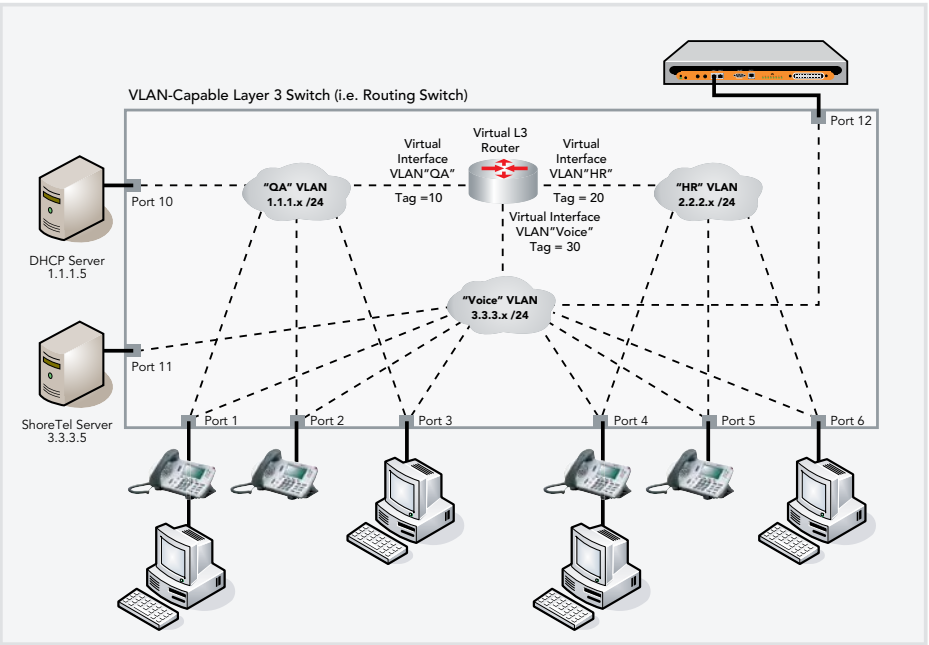
LAYER 3 SWITCH CONFIGURATION

```
interface FastEthernet1
 switchport mode trunk
 switchport trunk encapsulation dot1q
 switchport trunk native vlan 10
interface FastEthernet2  (and port 3)
 switchport mode trunk
 switchport trunk encapsulation dot1q
 switchport trunk native vlan 10
 . . . . . .
interface FastEthernet4  (and ports 5,6)
 switchport mode trunk
 switchport trunk encapsulation dot1q
 switchport trunk native vlan 20
 . . . . . .
interface FastEthernet11  (and port 12)
 switchport access vlan 30
```

Next, modify your DHCP scope information. The ShoreTel IP phones need to have a ShoreTel "vendor-specific" DHCP option (Option 156) included in the offer they receive from the DHCP server. The text string within this option needs to identify the IP address of the ShoreTel server and can optionally specify whether VLAN tagging should be enabled and, if so, what VLAN tag ID should be used.

When an IP phone first boots up it will send an untagged DHCP broadcast packet. This packet will be seen by the Ethernet switch on the "native," untagged VLAN configured for that port. In our sample topology this may be either the QA VLAN or the HR VLAN. Via the DHCP relay configuration (IP helper address) the IP phones on both subnets will get an IP address that is correct for the native subnet they are connected to and will also be given the necessary information for both the ShoreTel server's IP address and the Voice VLAN tag ID. The IP phones will next contact the ShoreTel server, download any necessary firmware updates.

Lastly, the IP phones will issue a DHCP RELEASE on the native VLAN (an untagged packet) and will then issue an immediate DHCP RENEW on the Voice VLAN (as an 802.1Q tagged packet using the VLAN ID of 30). Through the DHCP relay configuration on the Voice VLAN the DHCP request will be received by the DHCP server which will offer a new IP address in the Voice VLAN's IP subnet. Any PC data packets that pass through the IP phone (from the switch to the PC or from the PC to the switch) will be passed unaltered and untagged.



DHCP SERVER CONFIGURATION

```
Scope "QA"
 Address Range:  1.1.1.100 – 1.1.1.199
 Subnet Mask:  255.255.255.0
 Default Router: 1.1.1.1
 Option 156:  ftpservers=3.3.3.5,  layer2tagging=1, vlanid=30
Scope "HR"
 Address Range:  2.2.2.100 – 2.2.2.199
 Subnet Mask:  255.255.255.0
 Default Router: 2.2.2.1
 Option 156:  ftpservers=3.3.3.5, layer2tagging=1, vlanid=30
Scope "Voice"
 Address Range:  3.3.3.100 – 3.3.3.199
 Subnet Mask:  255.255.255.0
 Default Router: 3.3.3.1
 Option 156:  ftpservers=3.3.3.5, layer2tagging=1, vlanid=30
```

Figure 5.

Sample VLAN Switch Configuration

Below is a sample configuration from a Cisco Catalyst 3650 Layer-3 switch. This configuration emulates the exact design of the network topology in figure 5.

```
C3560_Switch#show running-config
!
version 12.1
!
ip routing
!
interface FastEthernet0/1
 description : Link to PC on QA VLAN + ShoreTel IP Phone
 switchport mode trunk
                                  ! Allows the port to receive tagged and untagged packets
 switchport trunk encapsulation dot1q
                                  ! Sets the tagging mode to the IEEE 802.1Q specification
 switchport trunk native vlan 10
                                  ! Any untagged packets received will be placed in this VLAN
                                  ! Without this cmd the default native VLAN is used (VLAN ID=1)
!
interface FastEthernet0/2
 description : Link to Stand-Alone ShoreTel IP Phone (VLAN 30, tagged)
 switchport mode trunk
 switchport trunk encapsulation dot1q
!
interface FastEthernet0/3
 description : Link to Stand-Alone PC on QA VLAN (VLAN 10, untagged)
 switchport mode access           ! (this is the default and will not display)
 switchport access vlan 10
!
interface FastEthernet0/4
 description : Link to PC on HR VLAN + ShoreTel IP Phone
 switchport mode trunk
 switchport trunk encapsulation dot1q
 switchport trunk native vlan 20
!
interface FastEthernet0/5
 description : Link to Stand-Alone ShoreTel IP Phone (VLAN 30, tagged)
 switchport mode trunk
 switchport trunk encapsulation dot1q
!
interface FastEthernet0/6
 description : Link to Stand-Alone PC on HR VLAN (VLAN 20, untagged)
 switchport mode access           ! (this is the default and will not display)
 switchport access vlan 20
!
interface FastEthernet0/10
 description : Link to DHCP Server (VLAN 10, untagged)
 switchport mode access
 switchport access vlan 10
!
interface FastEthernet0/11
 description : Link to ShoreTel Server (VLAN 30, untagged)
 switchport mode access
 switchport access vlan 30
!
interface FastEthernet0/12
 description : Link to ShoreTel ShoreGear Switch (VLAN 30, untagged)
 switchport mode access
 switchport access vlan 30
!
```

```
! CONFIGURATION FOR ALL OTHER PORTS.
! THE FOLLOWING STANDARD PORT CONFIGURATION CAN BE USED FOR
! ALL THREE TYPES OF PORTS: PC-Only, IP Phone-Only, or PC+IPPhone daisy-chained
!
! interface FastEthernet0/xx
!  description : Generic VoIP Network Port Configuration
!  switchport mode trunk
!  switchport trunk encapsulation dot1q
!  switchport trunk native vlan xx  ! If you want other than the 'native' vlan
!  switchport nonegotiate           ! Stops unnecessary DTP auto-negot'tion
!
interface VLAN10
 description : QA VLAN/Network
 ip address 1.1.1.1 255.255.255.0
!
interface VLAN20
 description : HR VLAN/Network
 ip address 2.2.2.1 255.255.255.0
 ip helper-address 1.1.1.5
!
interface VLAN30
 description : Voice VLAN/Network
 ip address 3.3.3.1 255.255.255.0
 ip helper-address 1.1.1.5
!
end
```

Epilogue

There are many different configuration options that were not discussed in this document. Some of them were left out for brevity sake (such as multi-netting). Some were left out because they are discussed in other ShoreTel White Papers (such as WAN QoS configuration guidelines) or the ShoreTel Documentation (such as detailed IP phone configuration options and additional DHCP scope parameters such as NTP servers, and GMT offset).

Others topics were left out because they are not needed, do not improve the voice-quality in a VoIP network, are unnecessarily complex or provide little or no added value. These include:

- Cisco's AutoQOS
- Cisco's proprietary Voice VLAN using CDP

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

- Port security
- Private VLANs
- MAC address locking/filtering
- Denial of Service (DOS) / Distributed DOS (DDOS) attack prevention
- Voice encryption (added in ShoreTel 6)
- Security best practices

References

- IEEE 802.1Q Tagging:
  http://www.ieee802.org/1/pages/802.1Q.html
  http://ieeexplore.ieee.org/xpl/standardstoc.jsp?isnumber=27089&isYear=2003
- Cisco Catalyst 3560 VLAN documentation:
  http://www.cisco.com/en/US/products/hw/switches/ps5528/products_configuration_guide_chapter-09186a00802b7cc8.html
- ShoreTel6 Planning and Installation Guide, Chapter 9: "Understanding Toll-Quality Voice"
- ShoreTel6 Planning and Installation Guide, Chapter 9: "Configuring DHCP for ShoreTel IP Phones"

Record of Change

This application note is subject to change. Updates and corrections are always welcome. Please submit any updates or corrections to ProServices@ShoreTel.com.

Issue	Author	Reason for Change	Date
1.0	J. Rowley	Initial Release	April 28, 2006

ShoreTel™

960 Stewart Drive Sunnyvale, CA 94085 USA Phone +1.408.331.3300 +1.877.80SHORE Fax +1.408.331.3333 www.shoretel.com