



Avaya Solution & Interoperability Test Lab

Configuring Cisco Catalyst 3750E-24P to provide Quality of Service to Avaya 9600, 1600 and 4600 Series IP and SIP Telephones with Avaya Aura™ Communication Manager and Avaya Aura™ SIP Enablement Services running on Avaya Aura™ Midsize Enterprise Single Server – Issue 1.0

Abstract

These Application Notes describe the configuration steps required to connect Avaya 9600, 1600, and 4600 Series IP and SIP Telephones to a Cisco Catalyst 3750E-24P Power over Ethernet Switch for communication with Avaya Aura™ Communication Manager and Avaya Aura™ SIP Enablement Services running on Avaya Aura™ Midsize Enterprise Single Server. The Application Notes identify how to configure voice and data VLANs in a Cisco Catalyst 3750E Switch. Quality of Service is configured within Avaya Aura™ Communication Manager and the Cisco Catalyst 3750E Switch to support a SIP Trunk within Avaya Aura™ Communication Manager to carry voice calls between Avaya IP and SIP endpoints.

1. Introduction

In the field of computer networking and other packet-switched telecommunication networks, the traffic engineering term quality of service refers to resource reservation control mechanisms rather than the achieved service quality. Quality of service is the ability to provide different priority to different applications, users, or data flows, or to guarantee a certain level of performance to a data flow. For example, a required bit rate, delay, jitter, packet dropping probability and or bit error rate may be guaranteed. Quality of service guarantees are important for applications that require fixed bit rate and are delay sensitive. They are especially important if the network capacity is insufficient, for real-time streaming multimedia applications such as voice over IP, and in networks where the capacity is a limited resource, for example in cellular data communication. A network or protocol that supports quality of service may agree on a traffic contract with the application software and reserve capacity in the network nodes, for example during a session establishment phase. During the session it may monitor the achieved level of performance, for example the data rate and delay, and dynamically control scheduling priorities in the network nodes. It may release the reserved capacity during a tear down phase. A best-effort network or service does not support quality of service. An alternative to complex quality of service control mechanisms is to provide high quality communication over a best-effort network by over-provisioning the capacity so that it is sufficient for the expected peak traffic load. This eliminates network congestion and quality of service mechanisms are not required. In the field of telephony, quality of service was defined in the ITU standard X.902 as a set of quality requirements on the collective behavior of one or more objects. Quality of service comprises requirements on all the aspects of a connection, such as service response time, loss, signal-to-noise ratio, cross-talk, echo, interrupts, frequency response, loudness levels, and so on. A subset of telephony quality of service is Grade of Service requirements, which comprises aspects of a connection relating to capacity and coverage of a network, for example guaranteed maximum blocking probability and outage probability. Quality of service is sometimes used as a quality measure, with many alternative definitions, rather than referring to the ability to reserve resources. Quality of service sometimes refers to the level of quality of service, i.e. the guaranteed service quality. High quality of service is often confused with a high level of performance or achieved service quality, for example high bit rate, low latency and low bit error probability.

Networks operate on a best-effort delivery basis, which means that all traffic has equal priority and an equal chance of being delivered in a timely manner. When congestion occurs, all traffic has an equal chance of being dropped. When you configure the quality of service feature, you can select specific network traffic, prioritize it according to its relative importance, and use congestion management and congestion avoidance techniques to provide preferential treatment. Implementing quality of service in your network makes network performance more predictable and bandwidth utilization more effective. The quality of service implementation is based on the Differentiated Services architecture, an emerging standard from the Internet Engineering Task Force. This architecture specifies that each packet is classified upon entry into the network. The classification is carried in the IP packet header, using 6 bits from the deprecated IP Type of Service field to carry the classification information. Classification can also be carried in the Layer 2 frame.

1.1. Interoperability Compliance Testing

The objective of this interoperability test is to verify that Cisco Catalyst 3750E-24P can provide Quality of Service capability to Avaya 9600, 4600 and 1600 Series IP and SIP telephones and interoperate with Avaya Aura™ Communication Manager 5.2.1 and Avaya Aura™ SIP Enablement Services 5.2.1 running on Avaya Aura™ Midsize Enterprise Single Server. It also includes configuration of voice and data VLANs within the Cisco Catalyst 3750E-24P switch and Extreme Summit x450 router. Testing was carried out on codec support and negotiation supported by Avaya 9600, 1600 and 4600 Series IP and SIP telephones and as well as supplementary features such as Call Hold, Forward, Transfer and Conference between the Avaya IP and SIP endpoints.

1.2. Configuration

The configuration used in these Application Notes is shown in **Figure 1**. The Avaya Aura™ Midsize Enterprise software is installed and configured on Avaya System Platform on a S8500C Media Server. The Avaya Aura™ Midsize Enterprise Single Server is a template running software applications. These software applications include Avaya Aura™ Communication Manager, Avaya Aura™ SIP Enablement Services and Avaya Aura™ Application Enablement Services. The Avaya Aura™ Midsize Enterprise Media Server is connected to an Extreme Summit x250e 24P Switch and is configured in a separate VLAN. All IP and SIP telephones are physically connected to a single Cisco Catalyst 3750E-24P Switch and are administered in two separate voice VLANs. The PCs are configured in a single data VLAN. The 9600, 1600 and 4600 Series IP telephones register to Avaya Aura™ Communication Manager running on the Avaya Aura™ Midsize Enterprise Single Server and are administered as H.323 stations. The 9600 SIP telephones register to Avaya Aura™ SIP Enablement Services running on the Avaya Aura™ Midsize Enterprise Single Server and are administered as an OPS station on Avaya Aura™ Communication Manager. Both the Extreme Summit x250e 24P Switch and the Cisco Catalyst 3750E-24P Switch are connected to an Extreme Summit x450e 48P Router. Each of the switches was configured with uplink trunks to connect to the Extreme Summit x450 router.

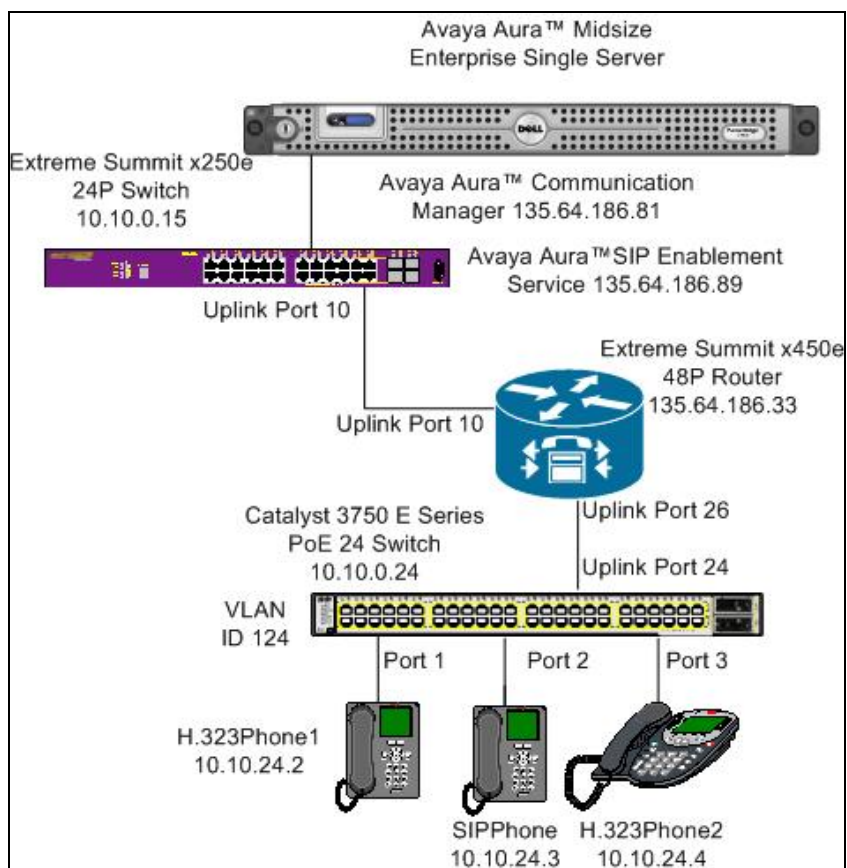


Figure 1: Avaya Aura™ Midsize Enterprise Single Server with Cisco Catalyst 3750E Switch

2. Equipment and Software Validated

The following equipment and software were used for the sample configuration provided:

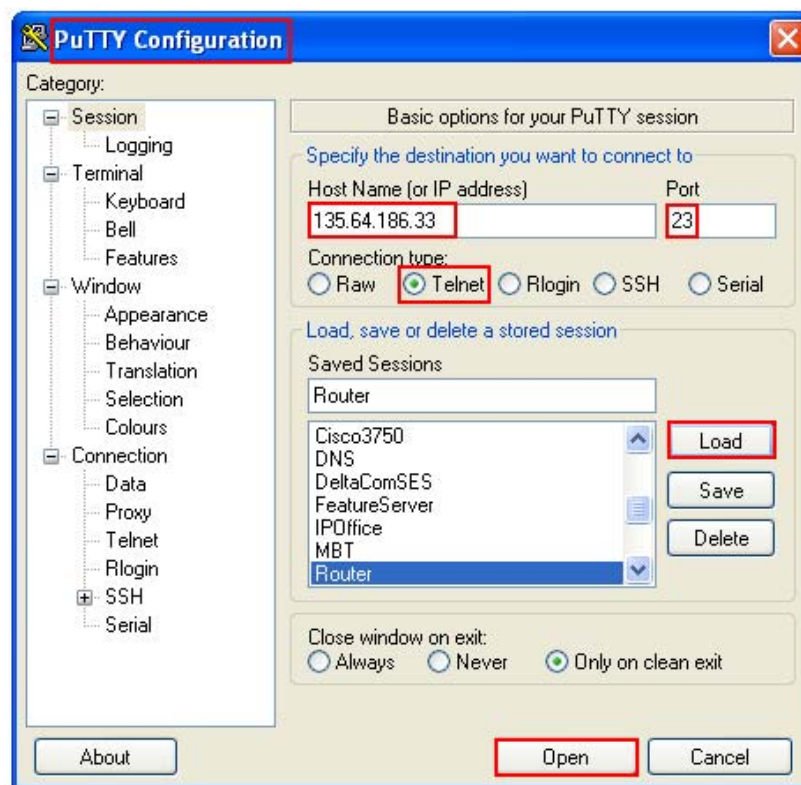
Avaya Aura™	Software
Avaya Aura™ Midsize Enterprise Single Server on a S8500C Media Server	Avaya Aura™ Midsize Enterprise Release 5.2.1.2.5 Avaya Aura™ Communication Manager Release 5.2.1 R15x.02.1.016.4 Avaya Aura™ SIP Enablement Services Release 5.2.1 SES05.2.1.016.4 Avaya Aura™ Application Enablement Services Release 5.2.0.98
Avaya one-X® 9600 Series IP Telephones (SIP)	Release 2.5
Avaya one-X® 9600 Series IP Telephones (H.323)	Release 3.1
Avaya one-X® 4600 Series IP Telephones (H.323)	Release 2.9
Avaya one-X® 1600 Series IP Telephones (H.323)	Release 1.22
Non Avaya Aura™	Software
Cisco Catalyst 3750 PoE 24P Switch	SW Ver. 12.2(35)SE5
Extreme Summit x250 24P Switch	Release 12.0.3.16
Extreme Summit x450 48P Router	Release 12.0.3.16
File Transfer Protocol Server	Microsoft Windows XP Professional Workstation Version 2002 Update: Service Pack 2

3. Configure Voice and Data VLANs in Extreme Summit x450e Router

This section describes the steps needed to configure voice and data VLANs in the Extreme Summit x450e router. It was decided to use two voice VLANs with IP address range 10.10.24.1/24 for voice VLAN 124 and IP address range 10.10.25.1/24 for voice VLAN 125. IP address range 10.10.26.1/24 was used for the data VLAN 126.

3.1. Access Extreme Summit x450e Router

To access the Extreme Summit x450e router open **PuTTY Configuration** and input the IP Address of the Extreme Summit x450e router and use the **Telnet** Connection type with **port 23**. The **IP Address** of the Extreme Summit x450e router was **135.64.186.33**. Load the following information and press the **Open** button.



Enter the router **Login : admin** and **password** and hit the return key. This brings the user to the command line interface of the Extreme Summit x450e router shown as **X450e-48p.1 #**.

```
telnet session telnet0 on /dev/ptyb2
```

```
login: admin
```

```
password:
```

```
ExtremeXOS
```

```
Copyright (C) 2000-2008 Extreme Networks. All rights reserved.
```

```
Protected by US Patent Nos: 6,678,248; 6,104,700; 6,766,482; 6,618,388; 6,034,957;  
6,859,438; 6,912,592; 6,954,436; 6,977,891; 6,980,550; 6,981,174; 7,003,705;  
7,017,082; 7,046,665; 7,126,923; 7,142,509; 7,149,217; 7,152,124; 7,154,861.  
=====
```

```
Press the <tab> or '?' key at any time for completions.  
Remember to save your configuration changes.
```

```
X450e-48p.1 #
```

3.2. Create Voice VLAN 124

To create VLAN 124, **create vlan p124** was issued from the command line interface of the router. To configure voice VLAN 124 and assign VLAN tag 124 to the VLAN the command **configure vlan p124 tag 124** was issued. The sample configuration uses the subnet range 10.10.24.1/24 for voice VLAN 124. From the command line interface, **configure vlan p124 ip address 10.10.24.1/24** was issued to assign this range to VLAN 124. When new IP interfaces are added to the router, IP forwarding is disabled by default and must be enabled. To enable IP forwarding on voice VLAN p124 the command **enable ip forwarding vlan p124** was issued from the command line interface of the router. This is to allow the voice VLAN 124 to communicate with the other voice and data VLANs.

```
X450e-48p.1 #create vlan p124
```

```
X450e-48p.1 #configure vlan p124 tag 124
```

```
X450e-48p.1 #configure vlan p124 ip address 10.10.24.1/24
```

```
X450e-48p.1 #enable ip forwarding vlan p124
```

3.3. Create Voice VLAN 125

To create voice VLAN p125, **create vlan p125** was issued from the command line interface of the router. To configure voice VLAN 125 and assign VLAN tag 125 to the VLAN the command **configure vlan p125 tag 125** was run. The sample configuration uses the subnet range 10.10.25.1/24 for voice VLAN 125. From the command line interface, **configure vlan p125 ip address 10.10.25.1/24** was issued. To enable IP forwarding on voice VLAN p125 the command **enable ip forwarding vlan p125** was issued.

```
X450e-48p.1 #create vlan p125
X450e-48p.1 #configure vlan p125 tag 125
X450e-48p.1 #configure vlan p125 ip address 10.10.25.1/24
X450e-48p.1 #enable ip forwarding vlan p125
```

3.4. Create Data VLAN 126

To create data VLAN p126, **create vlan p126** was issued from the command line interface of the router. To configure data VLAN 126 and assign VLAN tag 126 to the VLAN the command **configure vlan p126 tag 126** was run. The sample configuration uses the subnet range 10.10.26.1/24 for data VLAN 126. From the command line interface, **configure vlan p126 ip address 10.10.26.1/24** was issued. To enable IP forwarding on data VLAN p126 the command **enable ip forwarding vlan p126** was used.

```
X450e-48p.1 #create vlan p126
X450e-48p.1 #configure vlan p126 tag 126
X450e-48p.1 #configure vlan p126 ip address 10.10.26.1/24
X450e-48p.1 #enable ip forwarding vlan p126
```

3.5. Add Uplink Interface to Voice and Data VLANs

In this sample configuration **port 26** was used on the Extreme Summit x450e router as the uplink interface that would connect to the Cisco Catalyst 3750 switch. This port needed to be added to voice VLAN 124 so voice VLAN 124 could communicate with the other voice and data VLANs. From the command line interface of the Extreme Summit x450e router, **configure vlan p124 add port 26 tagged** performed this function. Similarly the same needed to be completed for voice VLAN 125 and data VLAN 126 with the commands **configure vlan p125 add port 26 tagged** and **configure vlan p126 add port 26 tagged**. This enabled all three VLANs to communicate with each other.

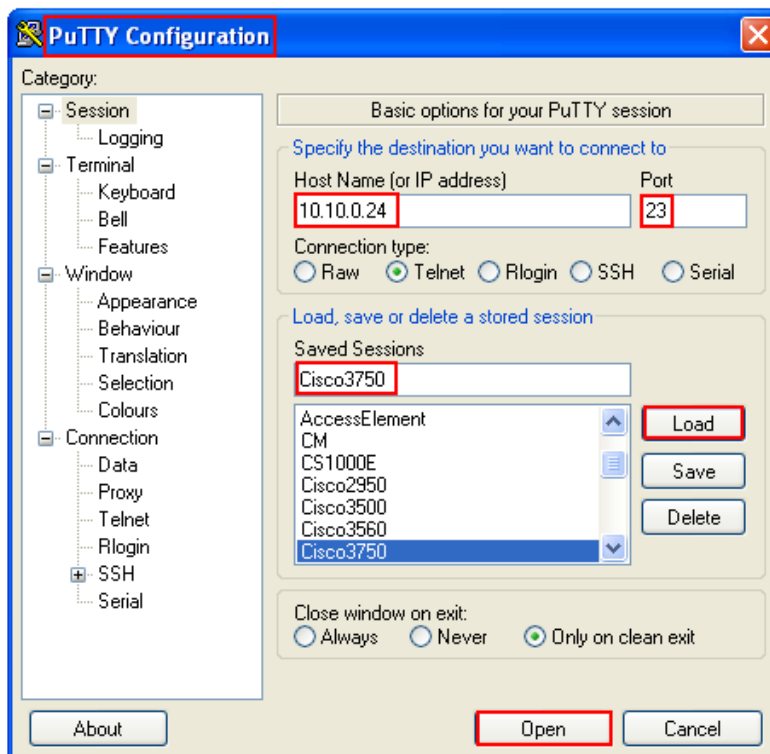
```
X450e-48p.1 #configure vlan p124 add port 26 tagged
X450e-48p.1 #Configure vlan p125 add port 26 tagged
X450e-48p.1 #Configure vlan p126 add port 26 tagged
```


4. Configure Voice and Data VLANs in Cisco Catalyst 3750E Switch

This section describes steps needed to configure voice and data VLANs in the Cisco Catalyst 3750E switch. It was decided to use two voice VLANs with IP address range 10.10.24.1/24 for voice VLAN 124 and IP address range 10.10.25.1/24 for voice VLAN 125. IP address range 10.10.26.1/24 was used for the data VLAN 126.

4.1. Access Cisco Catalyst 3750E Switch

To access the Cisco Catalyst 3750E switch open **PuTTY Configuration** and input the IP Address of the Cisco Catalyst 3750E switch and use the **Telnet** Connection type with **port 23**. The **IP Address** of the Cisco Catalyst 3750E switch was **10.10.0.24**. Load the following information and press the **Open** button.



Type **enable** at the command line interface. The user is then prompted to enter a password. Type the password and the user is brought to the hash prompt of the command line interface known as privileged mode.

```
cisco3750>enable
Password:
cisco3750#
```

4.2. Create Voice VLAN 124

To create voice VLAN 124 in the Cisco Catalyst 3750E switch the user must enter VLAN database configuration mode from privileged mode in the Cisco Catalyst 3750E switch. This is completed by typing **VLAN database** from privileged mode. From VLAN database configuration mode the user can assign a **Vlan id** and a **Vlan name** to the VLAN. **Vlan id 124** with **Vlan name p124** were created below.

```
cisco3750#vlan database
cisco3750(vlan)#vlan 124 name p124
cisco3750(vlan)#exit
```

4.3. Assign IP Address to Voice VLAN 124

In order to make changes to the Cisco Catalyst 3750E switch the user needs to be in global configuration mode of the Switch. This is achieved by entering the command **configure terminal** from privileged mode of the switch. The IP address range 10.10.24.0/24 was assigned to VLAN 124 by issuing the following command **ip address 10.10.24.1 255.255.255.0** from configuration mode of the Cisco Catalyst 3750E switch. The user must then enter configuration interface mode by issuing the command **interface vlan 124** from configuration mode and then assign the address ranges to the desired VLAN ID.

```
cisco3750#configure terminal
cisco3750(config)#interface vlan 124
cisco3750(config-if)#ip address 10.10.24.1 255.255.255.0
```

4.4. Assign Interface to Voice VLAN 124

In order to allow communication between multiple VLANs it was decided to configure the interface ports in trunk mode. Again the user enters configuration mode and enters the command **interface gigabitethernet1/0/1**. This means the user is selecting port 1 as the interface on the Cisco Catalyst 3750E switch to configure as a trunk link. This is the interface the IP telephone was connected to. To put the interface into permanent trunking mode the following command **switchport mode trunk** was issued from the command line interface. The **switchport trunk encapsulation dot1q** specifies 802.1q encapsulation on the trunk link. The **switchport voice vlan 124** command makes VLAN 124 a voice VLAN. The **switchport trunk allowed vlan 124-126** configures the list of VLANs allowed on the trunk link. Since we are using Avaya IP and SIP telephones cisco discovery protocol was disabled using the following command **no cdp enable**.

```
cisco3750#configure terminal
cisco3750(config)#interface gigabitethernet1/0/1
cisco3750(config-if)#switchport mode trunk
cisco3750(config-if)#switchport trunk encapsulation dot1q
cisco3750(config-if)#switchport voice vlan 124
cisco3750(config-if)#switchport trunk allowed vlan 124-126
cisco3750(config-if)#switchport trunk native vlan 126
cisco3750(config-if)#no cdp enable
```

The sample configuration in **Section 4.4** was used to configure interface 2 on the Cisco Catalyst 3750E switch. The SIP telephone was connected to interface 2 on the Cisco Catalyst switch.

4.5. Assign Interface to Data VLAN 126

To assign port 3 on the Cisco Catalyst 3750E switch the user must enter configuration mode from privileged mode by entering the **configure terminal** command at the command line interface. By issuing the **interface gigabitethernet1/0/3** the user is selecting port 3 of the Cisco Catalyst 3750E switch to configure this interface. To put the interface into permanent trunking mode the following command was issue from the command line interface **switchport mode trunk**. The **switchport trunk encapsulation dot1q** specifies 802.1q encapsulation on the trunk link. For switches running 802.1q as the trunking mechanism, the native VLAN of each port on the trunk must match This is achieved by entering the **switchport trunk native vlan 126** command.

```
cisco3750#configure terminal
cisco3750(config)#interface gigabitethernet1/0/3
cisco3750(config-if)#switchport mode trunk
cisco3750(config-if)#switchport trunk encapsulation dot1q
cisco3750(config-if)#switchport trunk allowed vlan 124-126
cisco3750(config-if)#switchport trunk native vlan 126
```

4.6. Configure Uplink Interface on Cisco Catalyst 3750E Switch

Port 24 on the Cisco Catalyst 3750E switch was used as the uplink interface to the Extreme Summit x450e router. It was configured as a trunking port to carry traffic between the Cisco Catalyst 3750E switch and the Extreme Summit x450e router. Enter configuration mode by issuing the command **configure terminal** at the command line interface. The command **Interface gigabitethernet1/0/24** was issued as port 24 was used as the interface port to the Extreme summit x450 router. Permanent trunking was set on port 24 with the command **switchport trunk mode** with 802.1q encapsulation with the command **switchport trunk encapsulation dot1q**. Allow traffic from the following VLANs 124, 125 and 126 across the interface to the Extreme Summit x450 router with the command **switchport trunk allowed vlan 124-126**.

```
cisco3750#configure terminal
cisco3750(config)#interface gigabitethernet1/0/24
cisco3750(config-if)#switchport mode trunk
cisco3750(config-if)#switchport trunk encapsulation dot1q
cisco3750(config-if)#switchport trunk allowed vlan 124-126
```

5. Configure Quality of Service on Extreme Summit x450 Router and Cisco Catalyst 3750E Switch

This section describes the steps needed to configure Quality of Service settings in the Extreme Summit x450e router and Cisco Catalyst 3750E switch. It documents configuring priority queues in the router and assigning DSCP and 802.1q values to these priority queues on the Extreme Summit x450e router and configuring autoqos and assigning COS values to the interfaces on the Cisco Catalyst 3750E switch.

5.1. Configure Priority Queues in Extreme Summit x450e Router

Depending on the model of the Extreme Networks switch being used, there are differences as to the number of default priority queues available. Two default priority queues, QP1 and QP8, are available for the Summit X450e router. By default, most traffic types are assigned to QP1, the lowest priority queue. Instead of using the default priority queue QP8 which is normally reserved for network control traffic, create a new priority queue. The configuration created priority queue QP7 by issuing the **create qosprofile qp7** command at the command line interface of the Extreme Summit x450e router.

```
X450e-48p.1 #create qosprofile qp7
```

5.2. Assign DSCP and 802.1q Values in Extreme Summit x450e Router

Assign DSCP and 802.1q values to the newly created QP7. According to the **display ip-network-region 1** form in Communication Manager as shown in **Section 6.6**, Avaya VoIP traffic uses **DIFFSERV/TOS PARAMETERS** of **46** and **802.1P/Q PARAMETERS** of **6** so those values are used here. To assign DSCP value of 46 to qosprofile 7 issue the following command **configure diffserv examination code-point 46 qp7** from the command line interface of the router and to assign 802.1q value of 6 to qosprofile 7 enter the following command **configure dot1q type 6 qp7** from the command line interface of the router.

```
X450e-48p.1 #configure diffserv examination code-point 46 qp7
X450e-48p.1 #configure dot1q type 6 qp7
```

5.3. Configure AutoQoS on Cisco Catalyst 3750E Switch

The Catalyst 3750E switch can prioritize the VoIP traffic based on the incoming packet's COS value. The AutoQoS feature is enabled at the interface level. The auto quality of service feature is used to simplify the deployment of existing quality of service features. Auto quality of service makes assumptions about the network design, and as a result, the switch can prioritize different traffic flows and appropriately use the ingress and egress queues instead of using the default quality of service behavior. The default is that quality of service is disabled. The switch then offers best effort service to each packet, regardless of the packet contents or size, and sends it from a single queue. When auto quality of service is enabled, it automatically classifies traffic based on the traffic type and ingress packet label. The switch uses the resulting classification to choose the appropriate egress queue. Auto quality of service commands are used to identify ports that receive trusted traffic through an uplink. When auto quality of service is enabled, the **auto qos voip trust** interface configuration command and the generated configuration are added to the running configuration. This additional running configuration of **mls qos** cli commands is shown in **Appendix A**. The switch applies the auto quality of service generated commands as if the commands were entered from the command line interface. An existing user configuration can

cause the application of the generated commands to fail or to be overridden by the generated commands. These actions occur without warning. If all the generated commands are successfully applied, any user-entered configuration that was not overridden remains in the running configuration. Any user-entered configuration that was overridden can be retrieved by reloading the switch without saving the current configuration to memory. If the generated commands fail to be applied, the previous running configuration is restored.

5.4. Configure the COS Value for Interface Gigabitethernet1/0/1 Vlan 124

Quality of service assigns the COS value specified with the **mls qos cos** interface configuration command to untagged frames received on trusted and untrusted ports. As mentioned above the **mls qos** applies automatically generated quality of service commands as shown below. A **trusted COS** value of **6** was assigned to **interface gigabitethernet1/0/1** to give the voice VLAN interface a high priority value. **auto qos voip trust** was enabled at the interface level also.

```
cisco3750#configure terminal
cisco3750(config)#interface gigabitethernet1/0/1
cisco3750(config-if)#switchport mode trunk
cisco3750(config-if)#switchport trunk encapsulation dot1q
cisco3750(config-if)#switchport trunk voice vlan 124
cisco3750(config-if)#switchport trunk allowed vlan 124-126
cisco3750(config-if)#switchport trunk native vlan 126
cisco3750(config-if)#no cdp enable
cisco3750(config-if)#srr-queue bandwidth share 10 10 60 20
cisco3750(config-if)#srr-queue bandwidth shape 10 0 0 0
cisco3750(config-if)#queue-set 2
cisco3750(config-if)#mls qos cos 6
cisco3750(config-if)#mls qos trust cos
cisco3750(config-if)#auto qos voip trust
cisco3750(config-if)#spanning-tree portfast
```

5.5. Configure the COS Value for Interface Gigabitethernet1/0/3 VLAN 126

A trusted COS value of **5** was assigned to **interface gigabitethernet1/0/3** to give the data VLAN interface a low priority value. The **auto qos voip trust** was enabled at the interface level also.

```
cisco3750#configure terminal
cisco3750(config)#interface gigabitethernet1/0/3
cisco3750(config-if)#switchport mode trunk
cisco3750(config-if)#switchport trunk encapsulation dot1q
cisco3750(config-if)#switchport trunk allowed vlan 124-126
cisco3750(config-if)#switchport trunk native vlan 126
cisco3750(config-if)#no cdp enable
cisco3750(config-if)#srr-queue bandwidth share 10 10 60 20
cisco3750(config-if)#srr-queue bandwidth shape 10 0 0 0
cisco3750(config-if)#queue-set 2
cisco3750(config-if)#mls qos cos 5
cisco3750(config-if)#mls qos trust cos
cisco3750(config-if)#auto qos voip trust
cisco3750(config-if)#spanning-tree portfast
```

6. Administer Avaya Aura™ Communication Manager

This section highlights the important commands for registering Avaya IP telephones as H.323 stations in Communication Manager and administering IP network-region and IP codec forms to carry calls between Avaya IP endpoints in separate VLANs. It also highlights the important commands for defining Avaya SIP telephones as an Off-PBX Station (OPS) and administering a SIP Trunk and Signaling Group to carry calls between Avaya IP and SIP telephones.

6.1. Verify OPS Capacity

Use the **display system-parameters customer-options** command to verify that **Maximum Off-PBX Telephones OPS** has been set to the value that has been licensed, and that this value will accommodate addition of SIP telephones. If a required feature is not enabled or there is insufficient capacity, contact an authorized Avaya Sales representative to obtain additional capacity.

```
display system-parameters customer-options                                     Page 1 of 11
                                OPTIONAL FEATURES

G3 Version: V15                               Software Package: Standard
Location: 2                                   RFA System ID (SID): 1
Platform: 25                                 RFA Module ID (MID): 1

                                USED
Platform Maximum Ports: 44000 113
Maximum Stations: 2400 21
Maximum XMOBILE Stations: 2400 0
Maximum Off-PBX Telephones - EC500: 2400 2
Maximum Off-PBX Telephones - OPS: 2400 11
Maximum Off-PBX Telephones - PBFMC: 2400 2
Maximum Off-PBX Telephones - PVFMC: 2400 0
Maximum Off-PBX Telephones - SCCAN: 0 0
```

Verify that **Maximum Concurrently Registered IP Stations** has been set to the value that has been licensed, and that this value will accommodate addition of IP telephones. Verify that **Maximum Administered SIP Trunks** has been set to accommodate addition of SIP Trunks.

display system-parameters customer-options		Page 2 of 11
OPTIONAL FEATURES		
IP PORT CAPACITIES		USED
	Maximum Administered H.323 Trunks: 8000	12
	Maximum Concurrently Registered IP Stations: 18000	3
	Maximum Administered Remote Office Trunks: 8000	0
	Maximum Concurrently Registered Remote Office Stations: 18000	0
	Maximum Concurrently Registered IP eCons: 128	0
	Max Concur Registered Unauthenticated H.323 Stations: 100	0
	Maximum Video Capable Stations: 2400	0
	Maximum Video Capable IP Softphones: 100	3
	Maximum Administered SIP Trunks: 5000	160
	Maximum Administered Ad-hoc Video Conferencing Ports: 8000	0
	Maximum Number of DS1 Boards with Echo Cancellation: 522	0
	Maximum TN2501 VAL Boards: 10	1
	Maximum Media Gateway VAL Sources: 250	0

6.2. Administer Dial Plan Analysis

This section describes the **Dial Plan Analysis** screen. This is Communication Manager's way of translating digits dialed by the user. The user can determine the beginning digits and total length for each type of call that Communication Manager needs to interpret. The **Dialed String** beginning with the number **4** and with a **Total Length** of **5** digits will be used to administer the **extension** range used for the IP telephones. The dialed string beginning with the number 5 and with a total length of 5 was also used in the dial plan analysis for configuration of the test IP telephones.

display dialplan analysis						Page 1 of 12		
DIAL PLAN ANALYSIS TABLE								
Location: all						Percent Full: 0		
Dialed String	Total Length	Call Type	Dialed String	Total Length	Call Type	Dialed String	Total Length	Call Type
0	1	fac						
1	5	ext						
2	5	aar						
3	5	aar						
4	5	ext						
5	5	ext						

6.3. Administer IP Node-Name

This section describes the **IP Node-Names form**. This is where Communication Manager assigns the IP Address and node-name to the SIP Enablement Server. The node-name of the SIP Enablement Server is **ses1** and the IP Address of the SIP Enablement Server is **135.64.186.89** within Communication Manager. Communication Manager automatically populates a processor node name to the IP Address of Communication Manager. This node name is **procr** with IP Address **135.64.186.81**.

```
list node-names all
```

NODE NAMES		
Type	Name	IP Address
IP	procr	135.64.186.81
IP	ses1	135.64.186.89

6.4. Administer Signaling Group

This section describes the **Signaling Group** screen. The **Group Type** was set to **sip** and the **Transport Method** was set to **tls**. Since the sip trunk is between Communication Manager and SIP Enablement Services the **Near-end Node Name** is the node name of Communication Manager, **procr**. The **Far-end Node Name** is the node name of SIP Enablement Services. This is **ses1**. The **Near-end Listen Port** and **Far-end Listen Port** are both set to port number **5061**. The **Far-end Network-Region** was set to **1**. The **Far-end Domain** is **silstack.com**, the domain name of the SIP Enablement Server.

```
display signaling-group 3
```

SIGNALING GROUP	
Group Number: 3	Group Type: sip
	Transport Method: tls
IMS Enabled? n	
IP Video? n	
Near-end Node Name: procr	Far-end Node Name: ses1
Near-end Listen Port: 5061	Far-end Listen Port: 5061
	Far-end Network Region: 1
Far-end Domain: silstack.com	
Incoming Dialog Loopbacks: eliminate	Bypass If IP Threshold Exceeded? n
DTMF over IP: rtp-payload	RFC 3389 Comfort Noise? n
Session Establishment Timer(min): 3	Direct IP-IP Audio Connections? y
Enable Layer 3 Test? n	IP Audio Hairpinning? n
	Direct IP-IP Early Media? n

6.5. Administer Trunk Group

This section describes the **Trunk Group** used to carry calls between the Avaya IP and SIP telephones. Trunk Group 3 was configured as a SIP Trunk with the **Group Type** set as **sip**. The trunk **Group Name** was set to **SIP Trunk to SES**. The **Direction** of the calls was set to **two-**

way as there will be calls to and from the Avaya IP and SIP telephones. The **Service Type** was set to **tie** since the trunk is configured as an internal trunk between Communication Manager and SIP Enablement Services. The **Signaling Group** number assigned to this trunk is **3**. The **Number of Members** assigned to this trunk group is **100**. All other fields on this page are left as default.

```
display trunk-group 3                                     Page 1 of 21
                                     TRUNK GROUP
Group Number: 3                      Group Type: sip      CDR Reports: y
  Group Name: SIP Trunk to SES        COR: 1             TN: 1       TAC: *03
  Direction: two-way                 Outgoing Display? n
Dial Access? n                       Night Service:
Queue Length: 0
Service Type: tie                    Auth Code? n

                                     Signaling Group: 3
                                     Number of Members: 100
```

6.6. Administer IP Network Region

This section describes **IP Network Region** screen. It was decided to place all IP and SIP endpoints in the one network region. The **Authoritative Domain** must mirror the domain name of the SIP Enablement Server. This was **silstack.com**. The codecs used on the IP and SIP endpoints were placed in **Codec Set 1**. IP Shuffling was turned on so both **Intra-region IP-IP Direct Audio** and **Inter-region IP-IP Direct Audio** were set to **yes**.

```
display ip-network-region 1                               Page 1 of 19
                                     IP NETWORK REGION
Region: 1
Location: 1      Authoritative Domain: silstack.com
Name:
MEDIA PARAMETERS      Intra-region IP-IP Direct Audio: yes
  Codec Set: 1        Inter-region IP-IP Direct Audio: yes
  UDP Port Min: 2048   IP Audio Hairpinning? n
  UDP Port Max: 3329
DIFFSERV/TOS PARAMETERS      RTCP Reporting Enabled? y
  Call Control PHB Value: 46   RTCP MONITOR SERVER PARAMETERS
  Audio PHB Value: 46         Use Default Server Parameters? y
  Video PHB Value: 26
802.1P/Q PARAMETERS
  Call Control 802.1p Priority: 6
  Audio 802.1p Priority: 6
  Video 802.1p Priority: 5     AUDIO RESOURCE RESERVATION PARAMETERS
H.323 IP ENDPOINTS      RSVP Enabled? n
  H.323 Link Bounce Recovery? y
  Idle Traffic Interval (sec): 20
  Keep-Alive Interval (sec): 5
  Keep-Alive Count: 5
```

6.7. Administer IP Codec Set

This section describes the **IP Codec Set** screen. It was decided to use IP Codec **G.711MU**, **G.711A** and **G.729** for testing purposes with the IP and SIP endpoints.

display ip-codec-set 1				Page	1 of	2
IP Codec Set						
Codec Set: 1						
Audio	Silence	Frames	Packet			
Codec	Suppression	Per Pkt	Size(ms)			
1: G.711MU	n	2	20			
2: G.711A	n	2	20			
3: G.729	n	2	20			
4:						

6.8. Administer Station Screen

This screen describes the **station** form setup for the Avaya SIP telephone on Communication Manager as shown. The **Extension** used was **40126** with phone **Type 9630**. The phone type would correspond to the particular phone type being tested for the Avaya IP telephone Series. The **Name** of the phone was set to **QoS SIP** and all other values on **Page 1** of the station form were left as default.

display station 40126		Page	1 of	5
STATION				
Extension: 40126	Lock Messages? n	BCC: 0		
Type: 9630	Security Code:	TN: 1		
Port: S00010	Coverage Path 1:	COR: 1		
Name: QoS SIP	Coverage Path 2:	COS: 1		
	Hunt-to Station:			
STATION OPTIONS				
	Time of Day Lock Table:			
Loss Group: 19	Personalized Ringing Pattern: 1			
	Message Lamp Ext: 40030			
Speakerphone: 2-way	Mute Button Enabled? y			
Display Language: english	Expansion Module? n			
Survivable GK Node Name:				
Survivable COR: internal	Media Complex Ext:			
Survivable Trunk Dest? y	IP SoftPhone? n			
	IP Video? n			

6.9. Administer Off PBX Telephone Station Mapping

This section show the **off-pbx-telephone station-mapping**. The Avaya SIP telephone extension **40126** uses off pbx **Application OPS** which is used for SIP enabled telephones. The SIP **Trunk Selection** is **3** as Trunk Group 3 was configured. The **Config Set** which is the desired call treatment was set to **1**.

display off-pbx-telephone station-mapping 40030							Page	1 of	3
STATIONS WITH OFF-PBX TELEPHONE INTEGRATION									
Station	Application	Dial	CC	Phone Number	Trunk	Config	Dual		
Extension		Prefix			Selection	Set	Mode		
40126	OPS	-		40126	3	1			

The **Call Limit** is set to **6** as shown below. This is the maximum amount of simultaneous calls for extension 40126. The **Mapping Mode** field was set to **both** in this configuration setup. This is used to control the degree of integration between SIP telephones. The **Calls Allowed** field was set to **all**. This identifies the call filter type for a SIP Phone. The **Bridged Calls** field was set to **none** as it was not needed for testing purposes.

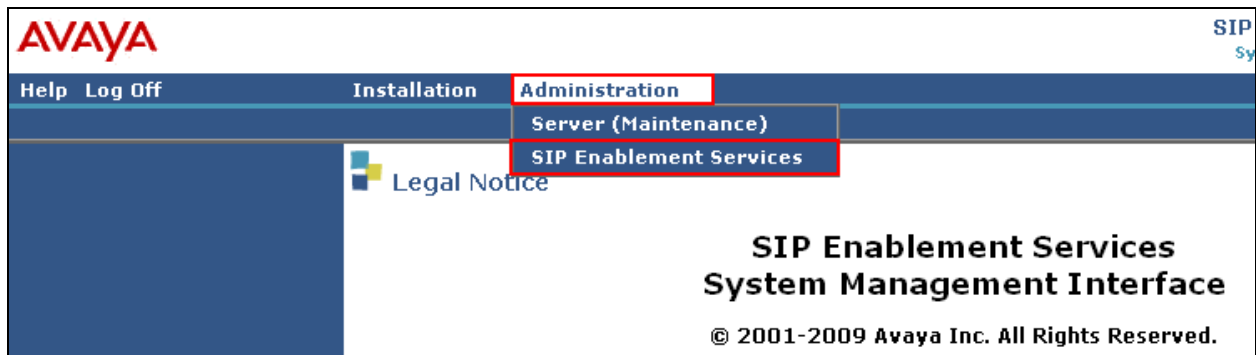
display off-pbx-telephone station-mapping 40030							Page	2 of	3
STATIONS WITH OFF-PBX TELEPHONE INTEGRATION									
Station	Appl	Call	Mapping	Calls	Bridged	Location			
Extension	Name	Limit	Mode	Allowed	Calls				
40126	OPS	3	both	all	none				

7. Administer Avaya Aura™ SIP Enablement Services

The following steps describe configuration of SIP Enablement Services to allow Avaya SIP telephones to register to SIP Enablement Services. .

7.1. Access Avaya Aura™ SIP Enablement Services

Access the SES Administration web interface, by entering **http://<ip-addr>/admin** as the URL in Internet browser, where <ip-addr> is the IP address of the SIP Enablement Services server. Log in with the appropriate credentials and then select the **Administration** link and then **SIP Enablement Services** from the main screen.



7.2. System Properties

On the left hand side of the System Management Interface access **Server Configuration** and then access **System Properties**. The **View System Properties** screen defines the server's type and domain. This **SES Version** field displays the release number, the current load and build number of the Avaya software that is running on this SES server. The **System Configuration** field identifies the SES server as being a **Simplex** machine. The **Host Type** field identifies the SES server as a home/edge type server. The **SIP Domain** field indicates the domain name assigned to the SIP Enablement Services Configuration. This was set to **silstack.com**. The **SIP License Host** field requires the IP address of the SES server that is running the WebLM application and has the associated license file installed. This entry shows the IP address of the SIP Enablement Server was entered as **135.64.186.89**.

Top

- Users
- Address Map Priorities
- Adjunct Systems
- Aggregator
- Certificate Management
- Conferences
- Emergency Contacts
- Export/Import to ProVision
- Hosts
- IM logs
- Communication Manager Servers
- Communication Manager Extensions
- Server Configuration**
 - Admin Setup
 - IM Log Settings
 - License
 - SNMP Configuration
 - System Properties**

View System Properties

SES Version: **SES-5.2.1.0-016.4**

System Configuration: Simplex

Host Type: SES combined home-edge

SIP Domain*: **silstack.com**

Note that the DNS domain is silstack.com

If you are unsure about this field, most often the SIP domain should be the root level DNS domain. For example, for a DNS domain of eastcoast.example.com, the SIP domain would likely be configured to example.com. This allows SIP calls and instant messages to users with handles of the format handle@example.com

SIP License Host*: **135.64.186.89**

DiffServ/TOS Parameters

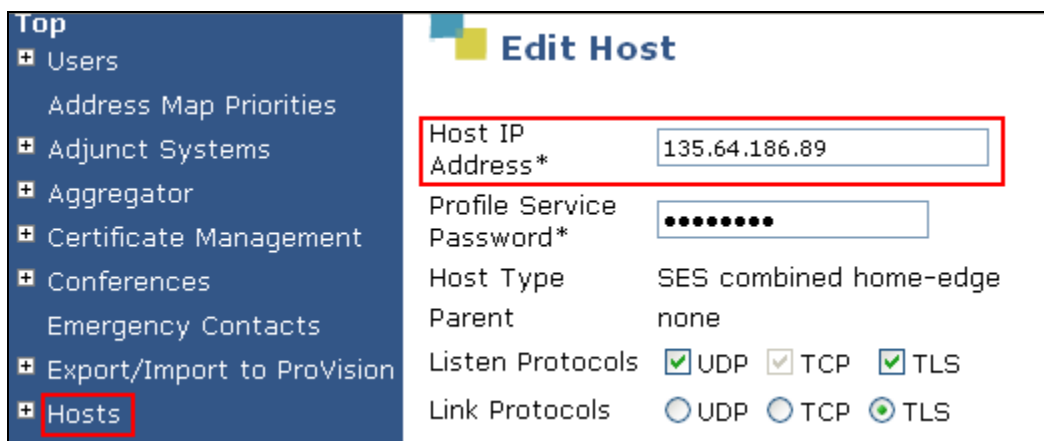
Call Control PHB Value*: 46

802.1 Parameters

Priority Value*: 6

7.3. Add Host Screen

On the System Management Interface access the **Hosts** section. The **Host IP Address** field contains the IP address for this combined home/edge server. This was **135.64.186.89**. The **Profile Service Password** is for permissions between SES hosts. This is not used by the administrator; it is used by internal software components for secure communication between SES servers and the master administration system. The **Host Type** functions as a **CM combined home-edge** server. In the **Listen Protocol** fields **UDP** and **TLS** were selected. The **Link Protocols** field refers to the trunk signaling between SIP Enablement Services and Communication Manager. Typically, the selection here matches the Signal Group value on Communication Manager. This was **TLS**. For third-party proxy servers you may select to link to SES with TLS, TCP or UDP.



Top

- Users
- Address Map Priorities
- Adjunct Systems
- Aggregator
- Certificate Management
- Conferences
- Emergency Contacts
- Export/Import to ProVision
- Hosts**

Edit Host

Host IP Address* 135.64.186.89

Profile Service Password*

Host Type SES combined home-edge

Parent none

Listen Protocols ☒ UDP ☒ TCP ☒ TLS

Link Protocols ☐ UDP ☐ TCP ☒ TLS

7.4. Administer Avaya SIP Telephones on SES

This screen allows the Avaya SIP telephone users to be added to the SES. Users are added one at a time with this screen. A handle identifies the user on the SES system. In this example the **Primary Handle** and **User ID** is **40126**. The **Password** needs to be six characters long and was set to **123456**. This password is needed when the Avaya SIP telephone registers to SIP Enablement Services after the extension of the SIP phone is input. The **Host IP** address is populated automatically to **135.64.186.89**. The name of the Avaya SIP telephone was **QoS SIP** (**First Name, Last Name**). Check the **Add Communication Manager Extension**. Press the **Add** button at the bottom of the screen. The SIP Phone extension 40126 must be added to Communication Manager also as described in **Sections 6.8** and **6.9**.

Address Map Priorities	Primary Handle*	40126
+ Adjunct Systems	User ID	40126
+ Aggregator	Password*	••••••
+ Certificate Management	Confirm Password*	••••••
+ Conferences	Host*	135.64.186.89 ▼
Emergency Contacts	First Name*	QoS
+ Export/Import to ProVision	Last Name*	SIP
+ Hosts	Address 1	
IM logs	Address 2	
+ Communication Manager Servers	Office	
+ Communication Manager Extensions	City	
+ Server Configuration	State	
+ SIP Phone Settings	Country	
+ Survivable Call Processors	Zip	
System Status	Survivable Call Processor	none ▼
+ Trace Logger	Add Communication Manager Extension	<input checked="" type="checkbox"/>
+ Trusted Hosts	Fields marked * are required.	
	Add	

When the **Add Communication Manager Extension** field is checked, the screen below appears. Confirm that extension **40126** is the **Communication Manager Extension** and press **Add**.

Add Communication Manager Extension

Extension: 40126

Communication Manager: CM

Fields marked * are required.

Add

8. Verification Steps

The following verification steps were tested using the sample configuration. The following steps can be used to verify installation in the field. It was verified that the PC in VLAN 126 with IP address 10.10.26.2 could ping the phone in VLAN 124 with IP address 10.10.24.2. This verified communication between source VLAN 124 and destination VLAN 126. A capture of the **ping results** are shown in **Figure 2**.

Filter: icmp Expression... Clear Apply					
No. -	Time	Source	Destination	Protocol	Info
15	13.766493	10.10.26.2	10.10.24.2	ICMP	Echo (ping) request
16	13.766647	10.10.24.2	10.10.26.2	ICMP	Echo (ping) reply
17	14.767614	10.10.26.2	10.10.24.2	ICMP	Echo (ping) request
18	14.767774	10.10.24.2	10.10.26.2	ICMP	Echo (ping) reply
20	15.768467	10.10.26.2	10.10.24.2	ICMP	Echo (ping) request
21	15.768624	10.10.24.2	10.10.26.2	ICMP	Echo (ping) reply
22	16.769169	10.10.26.2	10.10.24.2	ICMP	Echo (ping) request
23	16.769439	10.10.24.2	10.10.26.2	ICMP	Echo (ping) reply
25	17.770451	10.10.26.2	10.10.24.2	ICMP	Echo (ping) request
26	17.770608	10.10.24.2	10.10.26.2	ICMP	Echo (ping) reply
28	18.771362	10.10.26.2	10.10.24.2	ICMP	Echo (ping) request
29	18.771658	10.10.24.2	10.10.26.2	ICMP	Echo (ping) reply
30	19.772392	10.10.26.2	10.10.24.2	ICMP	Echo (ping) request
31	19.772578	10.10.24.2	10.10.26.2	ICMP	Echo (ping) reply
32	20.773380	10.10.26.2	10.10.24.2	ICMP	Echo (ping) request
33	20.773484	10.10.24.2	10.10.26.2	ICMP	Echo (ping) reply

Frame 9 (74 bytes on wire, 74 bytes captured)
Ethernet II, Src: ExtremeN_36:25:e7 (00:04:96:36:25:e7), Dst: Avaya_2a:9d:8e (00:1b:4f:2a:9d:8e)
Internet Protocol, Src: 10.10.26.2 (10.10.26.2), Dst: 10.10.24.2 (10.10.24.2)
Internet Control Message Protocol

Figure 2: Ping Results

It was verified that the PC in VLAN 126 with IP address 10.10.26.2 could ping the phone in VLAN 125 with IP address 10.10.25.2. This verified communication between source VLAN 125 and destination VLAN 126. A capture of the **ping results** are shown in **Figure 3**.

Filter: icmp		Expression... Clear Apply			
No. -	Time	Source	Destination	Protocol	Info
65	106.742973	10.10.26.2	10.10.25.2	ICMP	Echo (ping) request
66	106.743911	10.10.25.2	10.10.26.2	ICMP	Echo (ping) reply
67	107.743509	10.10.26.2	10.10.25.2	ICMP	Echo (ping) request
68	107.744320	10.10.25.2	10.10.26.2	ICMP	Echo (ping) reply
69	108.744504	10.10.26.2	10.10.25.2	ICMP	Echo (ping) request
70	108.745477	10.10.25.2	10.10.26.2	ICMP	Echo (ping) reply
72	109.745611	10.10.26.2	10.10.25.2	ICMP	Echo (ping) request
73	109.746426	10.10.25.2	10.10.26.2	ICMP	Echo (ping) reply
76	110.747437	10.10.26.2	10.10.25.2	ICMP	Echo (ping) request
77	110.748260	10.10.25.2	10.10.26.2	ICMP	Echo (ping) reply
80	111.748259	10.10.26.2	10.10.25.2	ICMP	Echo (ping) request
81	111.749115	10.10.25.2	10.10.26.2	ICMP	Echo (ping) reply
83	112.748315	10.10.26.2	10.10.25.2	ICMP	Echo (ping) request
84	112.749232	10.10.25.2	10.10.26.2	ICMP	Echo (ping) reply
86	113.749350	10.10.26.2	10.10.25.2	ICMP	Echo (ping) request
87	113.750412	10.10.25.2	10.10.26.2	ICMP	Echo (ping) reply

Frame 65 (74 bytes on wire, 74 bytes captured)
 Ethernet II, Src: ExtremeN_36:25:e7 (00:04:96:36:25:e7), Dst: Avaya_9e:22:31 (00:04:0d:9e:22:31)
 Internet Protocol, Src: 10.10.26.2 (10.10.26.2), Dst: 10.10.25.2 (10.10.25.2)
 Internet Control Message Protocol

Figure 3: Ping Results

It was verified that the VLAN 124 was seen from the Cisco Catalyst 3750E switch.. This was seen in the Wireshark trace in **Figure 4**.

Filter:		Expression... Clear Apply			
No. -	Time	Source	Destination	Protocol	Info
151	12.028476	Cisco_7a:b1:81	PVST+	STP	Conf. Root = 32768/124
152	12.035547	Cisco_7a:b1:81	PVST+	STP	Conf. Root = 32768/124
153	12.035710	10.10.26.10	135.64.21.5	DNS	Standard query SOA 249
154	12.045933	135.64.186.86	10.10.24.2	UDP	Source port: powerexcl
155	12.065944	135.64.186.86	10.10.24.2	UDP	Source port: powerexcl
156	12.085923	135.64.186.86	10.10.24.2	UDP	Source port: powerexcl
157	12.098164	10.10.26.10	135.64.21.5	DNS	Standard query A 3069
158	12.103856	Cisco_7a:b1:81	PVST+	STP	Conf. Root = 32768/124
159	12.105877	135.64.186.86	10.10.24.2	UDP	Source port: powerexcl
160	12.125942	135.64.186.86	10.10.24.2	UDP	Source port: powerexcl
161	12.145951	135.64.186.86	10.10.24.2	UDP	Source port: powerexcl
162	12.165965	135.64.186.86	10.10.24.2	UDP	Source port: powerexcl
163	12.185909	135.64.186.86	10.10.24.2	UDP	Source port: powerexcl
164	12.205943	135.64.186.86	10.10.24.2	UDP	Source port: powerexcl
165	12.225953	135.64.186.86	10.10.24.2	UDP	Source port: powerexcl
166	12.245928	135.64.186.86	10.10.24.2	UDP	Source port: powerexcl

Root Identifier: 32768 / 124 / 00:23:ab:1c:d1:80
 Root Path Cost: 4
 Bridge Identifier: 32768 / 124 / 00:23:ab:7a:b1:80
 Port identifier: 0x8001
 Message Age: 1

Figure 4: Vlan ID

Verified calls can be made with clear audio from the Avaya IP telephone to the Avaya SIP telephone. Verified the calls are seen to be active within Communication Manager.

status station 40126		Page 1 of 8
GENERAL STATUS		
Administered Type: 9640	Service State: in-service/off-hook	
Connected Type: 9640	TCP Signal Status: connected	
Extension: 40124		
status station 40124		Page 4 of 8
CALL CONTROL SIGNALING		
Port: S00025	Switch-End IP Signaling Loc: PROCR	H.245 Port:
IP Address	Port	Node Name Rgn
Switch-End: 135.64.186.81	61444	1
Set End: 10.10.24.4	1720	1
H.245 Near:		
H.245 Set:		
status station 40124		Page 5 of 8
AUDIO CHANNEL Port: S00025		
G.711MU	Switch-End Audio Location:	
IP Address	Port	Node Name Rgn
Other-End: 10.10.24.2	2192	1
Set-End: 10.10.24.4	3034	1
Audio Connection Type: ip-direct		

Figure 5 shows the Avaya IP Telephones registered to Communication Manager.

list registered-ip-stations					
REGISTERED IP STATIONS					
Station Ext or Orig Port	Set Type/ Net Rgn	Prod ID/ Release	TCP Skt	Station IP Address/ Gatekeeper	IP Address

40020	9640	IP_Phone	y	10.10.99.11	
	1	3.1000		135.64.186.81	
40124	9640	IP_Phone	y	10.10.24.2	
	1	3.1000		135.64.186.81	
40125	4621	IP_Phone	y	10.10.25.2	
	1	2.9		135.64.186.81	
50124	1608	IP_Phone	y	10.10.24.3	
	1	1.2200		135.64.186.81	
50125	9630	IP_Phone	y	10.10.25.3	
	1	3.1000		135.64.186.81	

Figure 5: IP Telephone Registration

To see what endpoints are registered to the SIP Enablement Server access the **Search Registered Users** on the left hand side of the System Management Interface menu. **Figure 6** shows the Avaya SIP telephone **40126** registered to SIP Enablement Services.

Top

Users

Add

Default Profile

Delete

Edit

List

Password

Search

Manage All Registered Users

Search Registered Devices

Search Registered Users

Address Map Priorities

Adjunct Systems

Registered Devices on 135.64.186.89

Registered and Provisioned Devices

Registered Devices

Provisioned Devices

Search

Refresh

Showing 1 to 2 of 2 registered contacts.

Handle	Program Version	MAC Address	Phone Type	Timestamp
<input type="checkbox"/> 40001	R5.2100-SP1-19397	00:00:00:00:00:00	one-X Communicator	2010-03-31 17:08:17
	2.5.0	00:04:0d:ec:a6:9e	one-X Deskphone	2010-04-15 16:59:35
<input type="checkbox"/> 40126	2.5.0	00:04:0d:ec:a3:ec	one-X Deskphone	2010-04-16 16:33:27

Figure 6: SIP Telephone Registration

It was verified that supplementary features such as Call Hold, Call Forward, Conference and Transfer could be completed between the Avaya endpoints. This was successful.

9. Conclusion

These Application Notes have described the administration steps required to configure:

- voice and data vlans on an Extreme Summit x450e router and Cisco Catalyst 3750E switch.
- Administration of Avaya IP and SIP telephones within Avaya Aura™ Communication Manager and Avaya Aura™ SIP Enablement Services to support H.323 and SIP telephones.
- Configuration of IP network-region and IP codecs and administration of a SIP Trunk and Signaling Group to carry calls between Avaya IP and SIP endpoints.

10. Additional References

This section references the Avaya documentation relevant to these Application Notes. Additional Avaya product documentation is available at <http://support.avaya.com>.

- [1] Administering Avaya Aura™ Communication Manager, Document Number 03-300509
- [2] Avaya Aura™ SIP Enablement Services (SES) Implementation Guide, May 2009, Document Number 16-300140
- [3] Administering Network Connectivity on Avaya Aura™ Communication Manager, Issue 14, May 2009, Document Number 555-233-504
- [4] SIP Support in Avaya Aura™ Communication Manager Running on Avaya S8xxx Servers, Issue 9, May 2009, Document Number 555-245-206
- [5] ExtremeXOS Command Reference Guide, May 2007, Document Number 100261-00 available at www.xtremenetworks.com
- [6] Catalyst 3750 Switch Software Configuration Guide 12.2(35)SE Configuring Voice VLANs, available at www.cisco.com
- [7] Catalyst 3750 Switch Software Configuration Guide 12.2(35)SE Configuring Quality of Service, available at www.cisco.com
- [8] Configuring 802.1Q Trunking between a Catalyst 3550/3560/3570 and Catalyst Switches that run Cisco IOS software, available at www.cisco.com

Appendix A

Sample default configuration file for Cisco Catalyst 3750E

Using 5942 out of 524288 bytes

```
version 12.2
no service pad
service timestamps debug uptime
service timestamps log uptime
no service password-encryption

hostname cisco3750

enable secret 5 $1$Pb8u$/RR6UVRFCcPMMqZ2WAVkt.
enable password cisco

no aaa new-model
switch 1 provision ws-c3750e-24pd
system mtu routing 1500
ip subnet-zero

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

mls qos queue-set output 1 threshold 2 138 138 92 400
mls qos queue-set output 1 threshold 3 36 77 100 318
mls qos queue-set output 1 threshold 4 20 50 67 400
mls qos queue-set output 2 threshold 1 149 149 100 149
mls qos queue-set output 2 threshold 2 118 118 100 235
mls qos queue-set output 2 threshold 3 41 68 100 272
mls qos queue-set output 2 threshold 4 42 72 100 242
mls qos queue-set output 1 buffers 10 10 26 54
mls qos queue-set output 2 buffers 16 6 17 61
mls qos

no file verify auto
spanning-tree mode pvst
spanning-tree extend system-id

vlan internal allocation policy ascending

interface FastEthernet0
no ip address
no ip route-cache
shutdown

interface GigabitEthernet1/0/1
switchport trunk encapsulation dot1q
switchport trunk native vlan 126
switchport trunk allowed vlan 124-126
switchport mode trunk
switchport voice vlan 124
srr-queue bandwidth share 10 10 60 20
srr-queue bandwidth shape 10 0 0 0
queue-set 2
mls qos cos 6
mls qos trust cos
auto qos voip trust
no cdp enable
spanning-tree portfast

interface GigabitEthernet1/0/2
switchport trunk encapsulation dot1q
switchport trunk allowed vlan 124-126
switchport mode trunk
switchport voice vlan 125
srr-queue bandwidth share 10 10 60 20
srr-queue bandwidth shape 10 0 0 0
queue-set 2
mls qos cos 6
mls qos trust cos
auto qos voip trust
no cdp enable
spanning-tree portfast

```
interface GigabitEthernet1/0/3  
switchport access vlan 126  
switchport mode access  
srr-queue bandwidth share 10 10 60 20  
srr-queue bandwidth shape 10 0 0 0  
queue-set 2  
mls qos cos 5  
mls qos trust cos  
auto qos voip trust
```

interface GigabitEthernet1/0/4

interface GigabitEthernet1/0/5

interface GigabitEthernet1/0/6

interface GigabitEthernet1/0/7

interface GigabitEthernet1/0/8

interface GigabitEthernet1/0/9

interface GigabitEthernet1/0/10

interface GigabitEthernet1/0/11

interface GigabitEthernet1/0/12

interface GigabitEthernet1/0/13

interface GigabitEthernet1/0/14

interface GigabitEthernet1/0/15

interface GigabitEthernet1/0/16

interface GigabitEthernet1/0/17

interface GigabitEthernet1/0/18

interface GigabitEthernet1/0/19

interface GigabitEthernet1/0/20

interface GigabitEthernet1/0/21

interface GigabitEthernet1/0/22
switchport access vlan 100

interface GigabitEthernet1/0/23

```
interface GigabitEthernet1/0/24
switchport trunk encapsulation dot1q
switchport trunk allowed vlan 124-126
switchport mode trunk
srr-queue bandwidth share 10 10 60 20
srr-queue bandwidth shape 10 0 0 0
queue-set 2
mls qos cos 6
mls qos trust cos
auto qos voip trust
no cdp enable
spanning-tree portfast
```

```
interface GigabitEthernet1/0/25
```

```
interface GigabitEthernet1/0/26
```

```
interface GigabitEthernet1/0/27
```

```
interface GigabitEthernet1/0/28
```

```
interface TenGigabitEthernet1/0/1
```

```
interface TenGigabitEthernet1/0/2
```

```
interface Vlan1
no ip address
no ip route-cache
shutdown
```

```
interface Vlan100
ip address 10.10.0.23 255.255.255.0
no ip route-cache
```

```
ip default-gateway 10.10.0.1
ip classless
ip http server
```

```
control-plane
```

```
line con 0
line vty 0 4
password cisco
login
length 0
line vty 5 15
password cisco
login
```

```
monitor session 1 source interface Gi1/0/1
monitor session 1 destination interface Gi1/0/4 encapsulation replicate
monitor session 2 source interface Gi1/0/2
monitor session 2 destination interface Gi1/0/5
end
```

©2010 Avaya Inc. All Rights Reserved.

Avaya and the Avaya Logo are trademarks of Avaya Inc. All trademarks identified by ® and ™ are registered trademarks or trademarks, respectively, of Avaya Inc. All other trademarks are the property of their respective owners. The information provided in these Application Notes is subject to change without notice. The configurations, technical data, and recommendations provided in these Application Notes are believed to be accurate and dependable, but are presented without express or implied warranty. Users are responsible for their application of any products specified in these Application Notes.

Please e-mail any questions or comments pertaining to these Application Notes along with the full title name and filename, located in the lower right corner, directly to the Avaya Solution & Interoperability Test Lab at interoplabinotes@list.avaya.com