Avaya Solution & Interoperability Test Lab

Configuring Juniper SRX210 Switch 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 Juniper SRX210 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 Juniper SRX210 Switch. Quality of Service is configured within Avaya Aura™ Communication Manager and the Juniper SRX210 Switch to support a SIP Trunk between Avaya Aura™ Communication Manager and SIP Enablement Services 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 Juniper SRX210 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. running on Avaya Aura™ Midsize Enterprise Single Server. It also includes configuration of voice and data VLANS within the Juniper SRX210 switch and 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 and Avaya Aura™ SIP Enablement Services. The Avaya Aura™ Midsize Enterprise Media Server is connected to an Data Switch and is configured in a separate VLAN. All IP and SIP telephones are physically connected to a single Juniper SRX210 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 Data Switch and the Juniper SRX210 Switch are connected to a Router. Each of the switches was configured with uplink trunks to connect to the router.

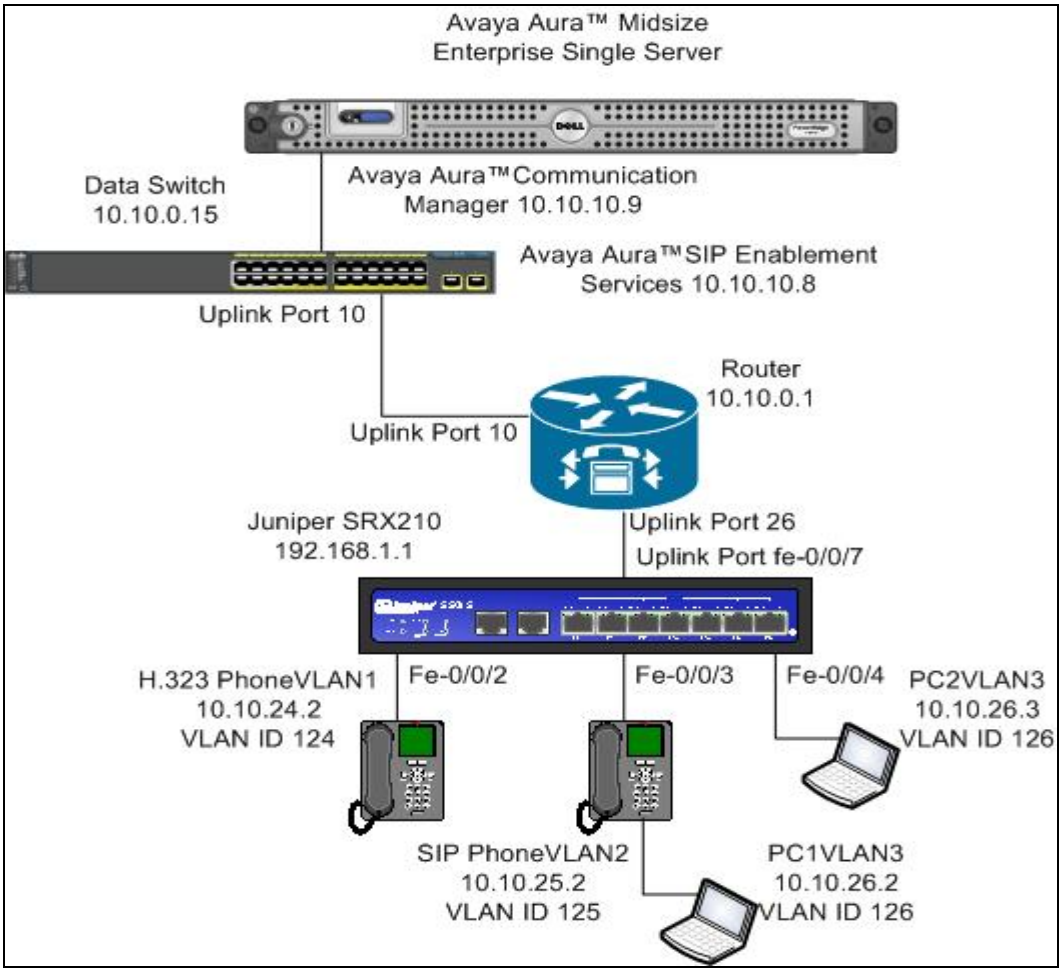


Figure 1: Avaya Aura™ Midsize Enterprise Single Server with Juniper SRX210 Switch

2. Equipment and Software Validated

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

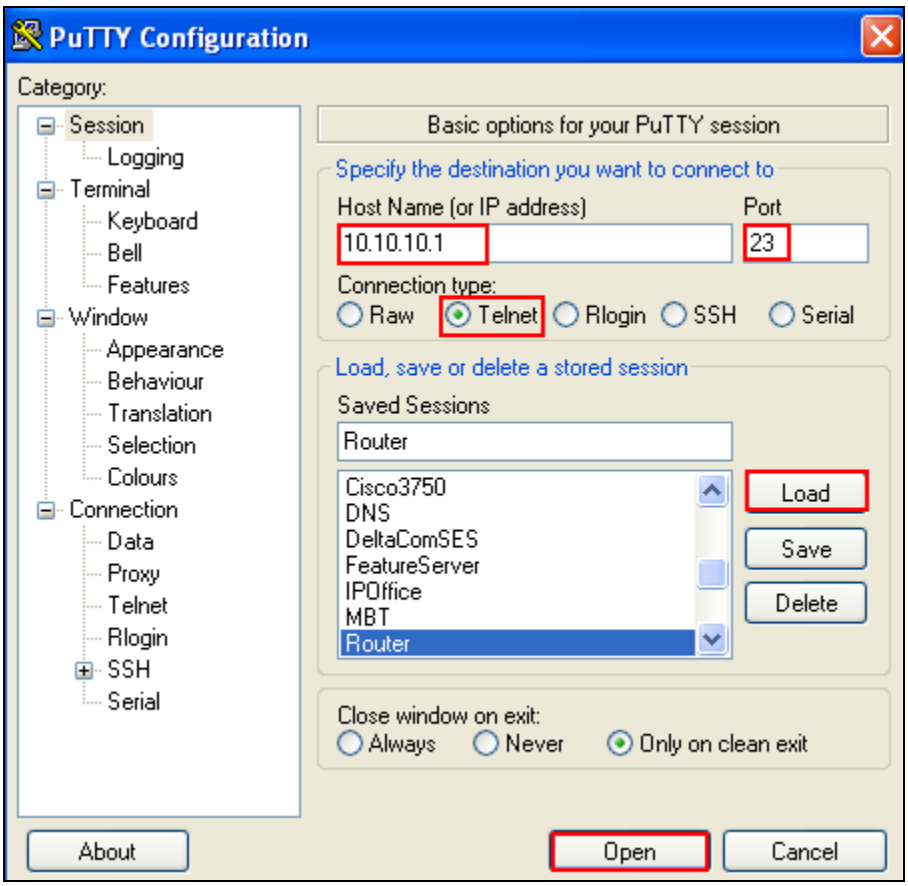
Avaya Aura™	Software
Avaya Aura™ Midsize Enterprise Single Server on a S8500C Media Server	Avaya Aura™ Midsize Enterprise Release 5.2.1.2.5 Avaya Aura™ Communication Manager Release 5.2.1 R15x.02.1.016.4 Avaya Aura™ SIP Enablement Services Release 5.2.1 SES05.2.1.016.4
Avaya one-X® 9600 Series IP Telephones (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
Juniper SRX210	Junos 10.0 R1
Data Switch	Release 12.0.3.16
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 the Router

This section describes the steps needed to configure voice and data VLANS in the 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 the Router

To access the router open **Putty Configuration** and input the IP Address of the router and use the **Telnet** Connection type with **port 23**. The **IP Address** of the router was **10.10.10.1**. 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 router shown as **X450e-48p.1 #.**

```
telnet session telnet0 on /dev/ptyb2

login: admin
password:

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

router #
```

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 intefaces 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.

```
router #create vlan p124
router #configure vlan p124 tag 124
router #configure vlan p124 ip address 10.10.24.1/24
router #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.

```
router #create vlan p125
router #configure vlan p125 tag 125
router #configure vlan p125 ip address 10.10.25.1/24
router #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.

```
router #create vlan p126
router #configure vlan p126 tag 126
router #configure vlan p126 ip address 10.10.26.1/24
router #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 router as the uplink interface that would connect to the Juniper SRX210 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 router, **configure vlan p124 add port 26 tagged** performed this function. Similiarly 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.

```
router #configure vlan p124 add port 26 tagged
router #Configure vlan p125 add port 26 tagged
router #Configure vlan p126 add port 26 tagged
```

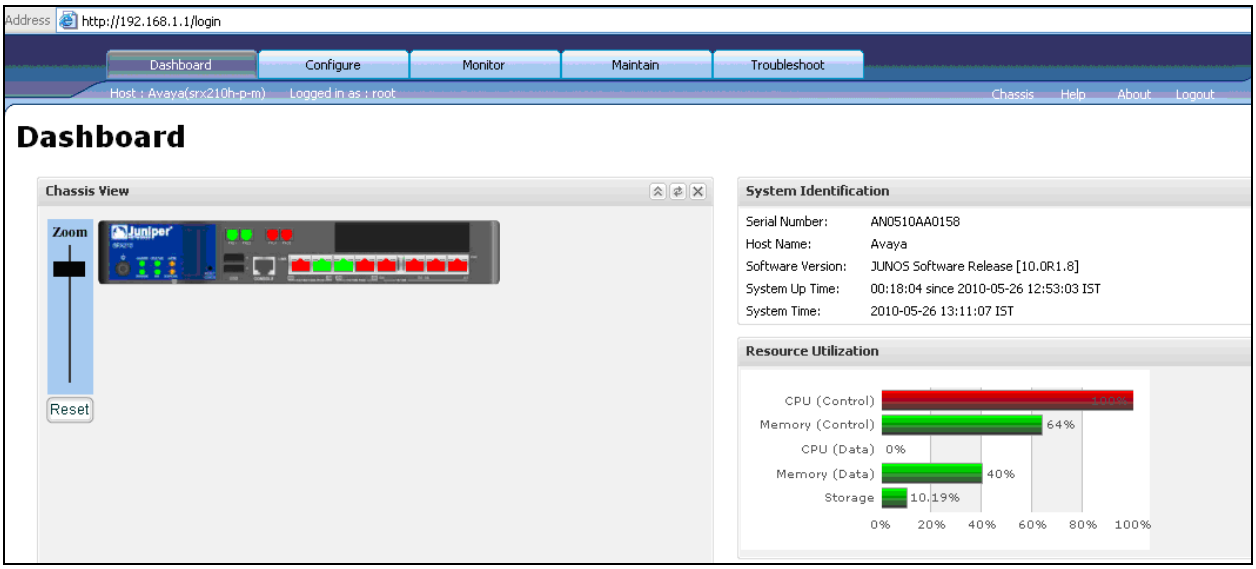
4. Configure Voice and Data VLANS in Juniper SRX210 Switch

This section describes steps needed to configure voice and data VLANS in the Juniper SRX210 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 Juniper SRX210 Switch

To access the Juniper SRX210 browse to the management IP Address of the Juniper SRX210 which was **192.168.1.1.** The following screenshot appears and enter the **username** and **password** and press the **Login** button.

The following screenshot is displayed showing the graphical user interface of the Juniper SRX210.



To access the command line interface again input the login and password for the Juniper SRX210. This brings the user to the command line interface. At the level **root@Avaya%** type **cli**. This takes the user to **the root@Avaya>** command line interface. Then type **configure** to enter configuration mode.

```
Login:
Password:
root@Avaya%cli
root@Avaya>configure
root@Avaya#
```

4.2. Assign Interfaces to VLAN 124

To create vlan 124 in the Juniper SRX210 switch the user must enter configuration mode from priviledged mode. It was decided to use interface fe-0/0/2 as the interface the Avaya 9600 IP telephone would plug into and interface fe-0/0/3 as the interface the Avaya 9600 SIP telephone would plug into. Create vlan124 with vlan-id 124 with the command **set vlans vlan124 vlan-id 124.** Assign vlan 124 to interface fe-0/0/2 with the command **set interfaces fe-0/0/2 unit 0 vlan-id 124.**

```
root@Avaya#set vlans vlan124 vlan-id 124
root@Avaya#set interfaces fe-0/0/2 unit 0 vlan-id 124
```

4.3. Assign Interfaces to VLAN 125

To create vlan 125 in the Juniper SRX210 switch the user must enter configuration mode from priviledged mode. It was decided to use interface fe-0/0/3 as the interface the Avaya 9600 IP telephone would plug into and interface fe-0/0/3 as the interface the Avaya 9600 SIP telephone would plug into. Create vlan125 with vlan-id 125 with the command **set vlans vlan125 vlan-id 125.** Assign vlan 125 to interface fe-0/0/3 with the command **set interfaces fe-0/0/3 unit 0 vlan-id 125.**

```
root@Avaya#set vlans vlan125 vlan-id 125
root@Avaya#set interfaces fe-0/0/3 unit 0 vlan-id 125
```

4.4. Assign IP Address to Interface fe-0/0/2

The IP address range 10.10.24.2 was assigned to interface fe-0/0/2 by issuing the following command **set interfaces fe-0/0/2 unit 0 family inet address 10.10.24.2** from the command line interface of the Juniper SRX210. The **set interfaces fe-0/0/2 unit 0 description voice vlan** command makes VLAN 124 a voice VLAN.

```
root@Avaya#set interfaces fe-0/0/2 unit 0 description voice vlan
root@Avaya#set interfaces fe-0/0/2 unit 0 family inet address 10.10.24.2
```

4.5. Assign IP Address to Interface fe-0/0/3

The IP address range 10.10.25.2 was assigned to interface fe-0/0/3 by issuing the following command **set interfaces fe-0/0/3 unit 0 family inet address 10.10.25.2** from the command line interface of the Juniper SRX210. The **set interfaces fe-0/0/3 unit 0 description voice vlan** command makes VLAN 125 a voice VLAN.

```
root@Avaya#set interfaces fe-0/0/3 unit 0 description voice vlan
root@Avaya#set interfaces fe-0/0/3 unit 0 family inet address 10.10.25.2
```

4.6. Assign Security Zones to Interfaces

In this sample configuration interfaces fe-0/0/2 and fe-0/0/3 were assigned to a trusted security zone using the command **set security zones security-zones trust interfaces fe-0/0/2** and **set security zones security-zones trust interfaces fe-0/0/3.**

```
root@Avaya#set security zones security-zone trust interfaces fe-0/0/2
root@Avaya#set security zones security-zone trust interfaces fe-0/0/3
```

4.7. Assign Interface to Data VLAN 126

To create vlan 126 in the Juniper SRX210 switch the user must enter configuration mode from priviledged mode. It was decided to use interface fe-0/0/4 as the interface the PC would plug into. Create vlan126 with vlan-id 126 with the command **set vlans vlan126 vlan-id 126.** Assign vlan 126 to interface fe-0/0/4 with the command **set interfaces fe-0/0/4 unit 0 vlan-id 126.** The IP address range 10.10.26.3 was assigned to interface fe-0/0/4 by issuing the following command **set interfaces fe-0/0/4 unit 0 family inet address 10.10.26.3** from the command line interface of the Juniper SRX210. The **set interfaces fe-0/0/4 unit 0 description data vlan** command makes VLAN 126 a data VLAN. The interface fe-0/0/4 was assigned to a trusted security zone using the command **set security zones security-zones trust interfaces fe-0/0/4**.

```
root@Avaya#set vlans vlan126 vlan-id 126
root@Avaya#set interfaces fe-0/0/4 unit 0 vlan-id 126
root@Avaya#set interfaces fe-0/0/4 unit 0 description data vlan
root@Avaya#set interfaces fe-0/0/4 unit 0 family inet address 10.10.26.3
root@Avaya#set security zones security-zone trust interfaces fe-0/0/4
```

4.8. Configure Uplink Interface on Juniper SRX210 Switch

Interface fe-0/0/7 on the Juniper SRX210 was used as the uplink interface to the router. It was configured as a trunking port to carry traffic between the Juniper SRX210 and the router. Enter configuration mode by issuing the command **configure** at the command line interface. The vlan124 was allowed across interface fe-0/0/7 with the command **set interfaces fe-0/0/7 unit 0 ethernet-switching vlan members vlan124**. The vlan125 was allowed across interface fe-0/0/7 with the command **set interfaces fe-0/0/7 unit 0 ethernet-switching vlan members vlan125.** The vlan126 was allowed across interface fe-0/0/7 with the command **set interfaces fe-0/0/7 unit 0 ethernet-switching vlan members vlan126.** The interface fe-0/0/7 was set to 802.1q trunk mode by issuing the command **set interfaces fe-0/0/7 unit 0 family ethernet-switching port-mode trunk.**

```
root@Avaya#configure
root@Avaya#set interfaces fe-0/0/7 unit 0 ethernet-switching vlan members vlan124
root@Avaya#set interfaces fe-0/0/7 unit 0 ethernet-switching vlan members vlan125
root@Avaya#set interfaces fe-0/0/7 unit 0 ethernet-switching vlan members vlan126
root@Avaya#set interfaces fe-0/0/7 unit 0 family ethernet-switching port-mode trunk
```

5. Configure Quality of Service on the Router and Juniper SRX210

This section describes the steps needed to configure Quality of Service settings in the router and Juniper SRX210 switch. It documents configuring priority queues in the router and assigning DSCP and 802.1q values to these priority queues on the router and assigning DSCP and 802.1q layer 2 values to the interfaces on the Juniper switch.

5.1. Configure Priority Queues in the Router

Depending on the model of the data 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 router.

```
router #create qosprofile qp7
```

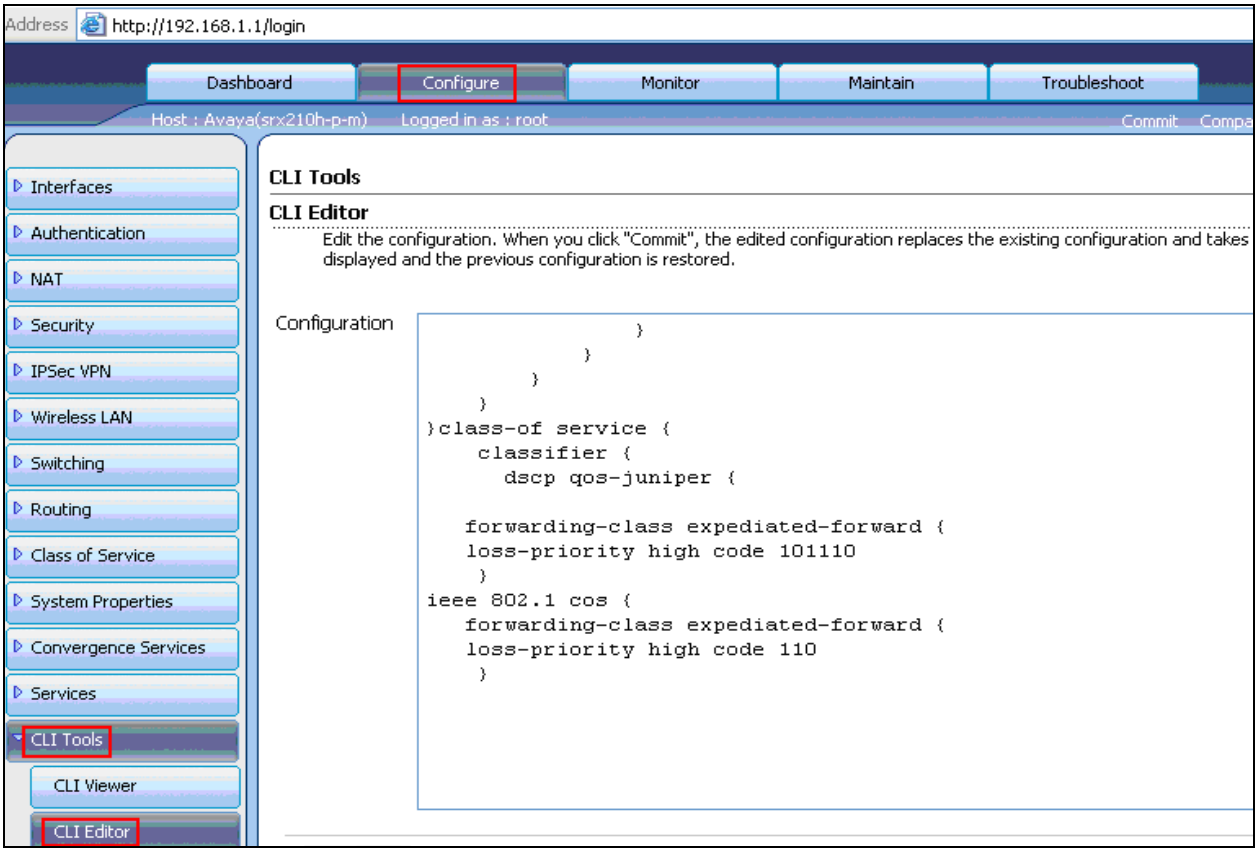
5.2. Assign DSCP and 802.1q Values in the Router

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.

```
router #configure diffserv examination code-point 46 qp7
router #configure dot1q type 6 qp7
```

5.3. Configure DSCP and 802.1q on Juniper SRX210 Switch

It was decided to create classifier rules to select voice traffic based on DSCP and COS values and use expediated forwarding for **DSCP value 46** (**101110**) and **COS value 6**(**110**). The classifier rule was named **dscp qos-juniper.** Access the **Configure** button on the system management interface. Access the **CLI Tools** on the left hand side of the SMI and then **CLI Editor.** The following classifier rule was added below.



5.4. Assign DSCP and 802.1q Values for Interfaces

A **scheduler-map** named **voip** was created and associated to interface **fe-0/0/2, fe-0/0/3** and **fe-0/0/4**. The classifier dscp qos-juniper was assigned to logical interfaces **unit 0** to identify ingress traffic based on the DSCP value.

```
interfaces {
  fe-0/0/2 {
 unit 0 {
      scheduler-map voip
   }
  classifiers {
    dscp qos-juniper
   }
interfaces {
  fe-0/0/3 {
 unit 0 {
      scheduler-map voip
   }
  classifiers {
    dscp qos-juniper
   }
interfaces {
  fe-0/0/4 {
 unit 0 {
      scheduler-map voip
   }
  classifiers {
    dscp qos-juniper
   }
```

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      Total  Call    Dialed   Total  Call     Dialed   Total  Call
    String      Length Type    String   Length Type     String   Length 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** 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

                                            Bypass If IP Threshold Exceeded? n
Incoming Dialog Loopbacks: eliminate                 RFC 3389 Comfort Noise? n
         DTMF over IP: rtp-payload            Direct IP-IP Audio Connections? y
Session Establishment Timer(min): 3                     IP Audio Hairpinning? n
         Enable Layer 3 Test? 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 used to define the Avaya SIP telephone on Communication Manager. 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 shows the **off-pbx-telephone station-mapping** form. 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 40126                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
```

On **Page 2**, 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.

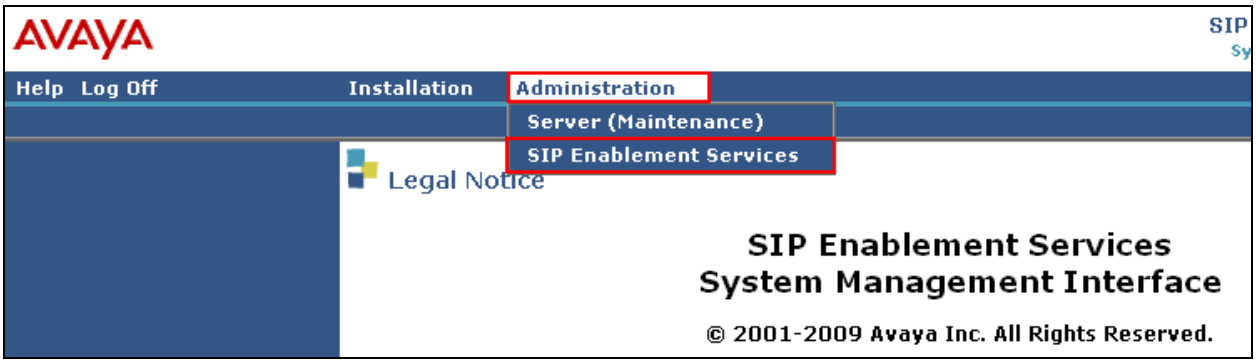
```
display off-pbx-telephone station-mapping 40126                 Page   2 of   3
                  STATIONS WITH OFF-PBX TELEPHONE INTEGRATION

 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.

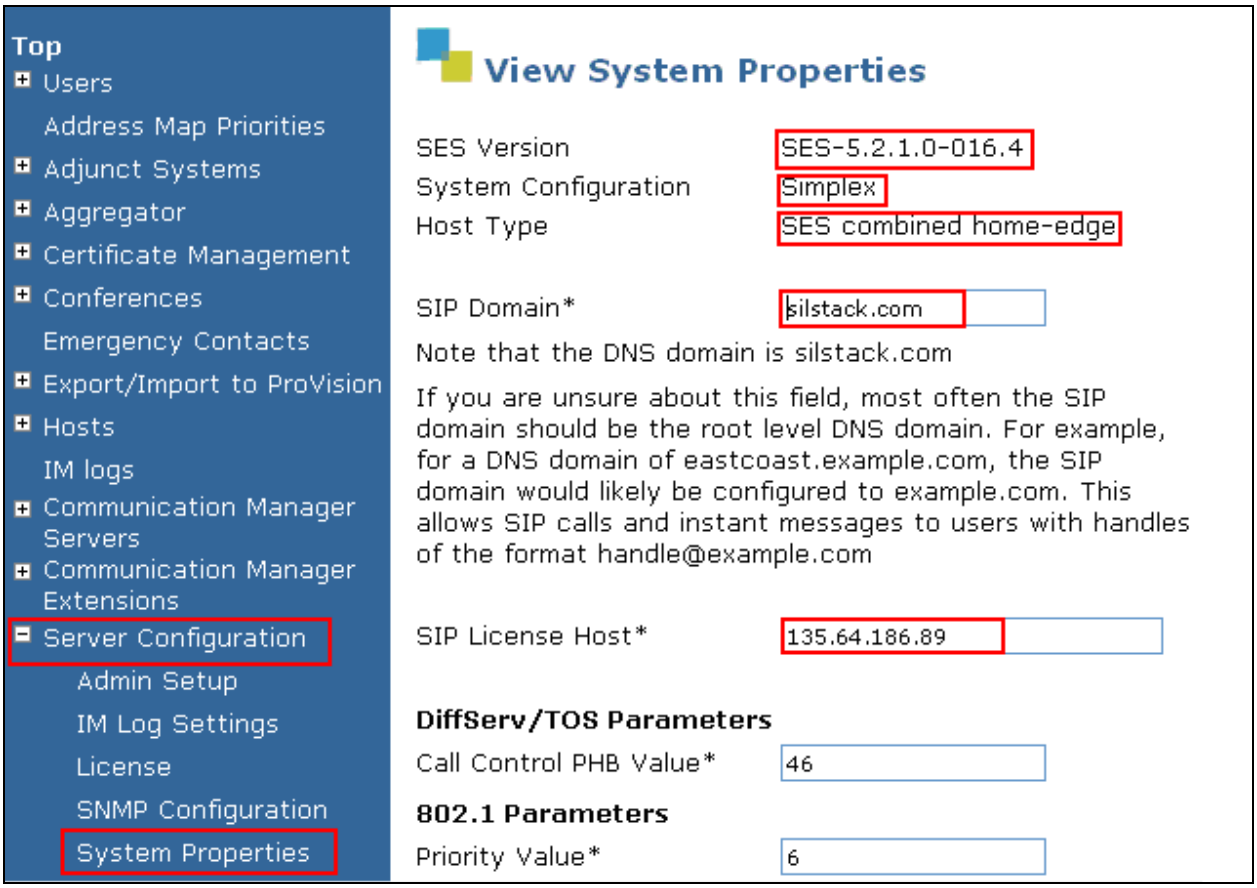
7.1. Access Avaya Aura™ SIP Enablement Services

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.



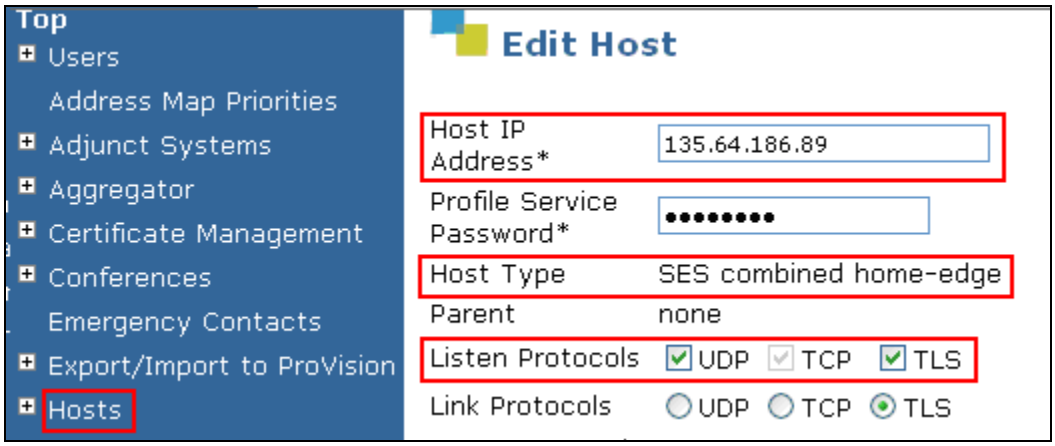
7.2. System Properties

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. The **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**.



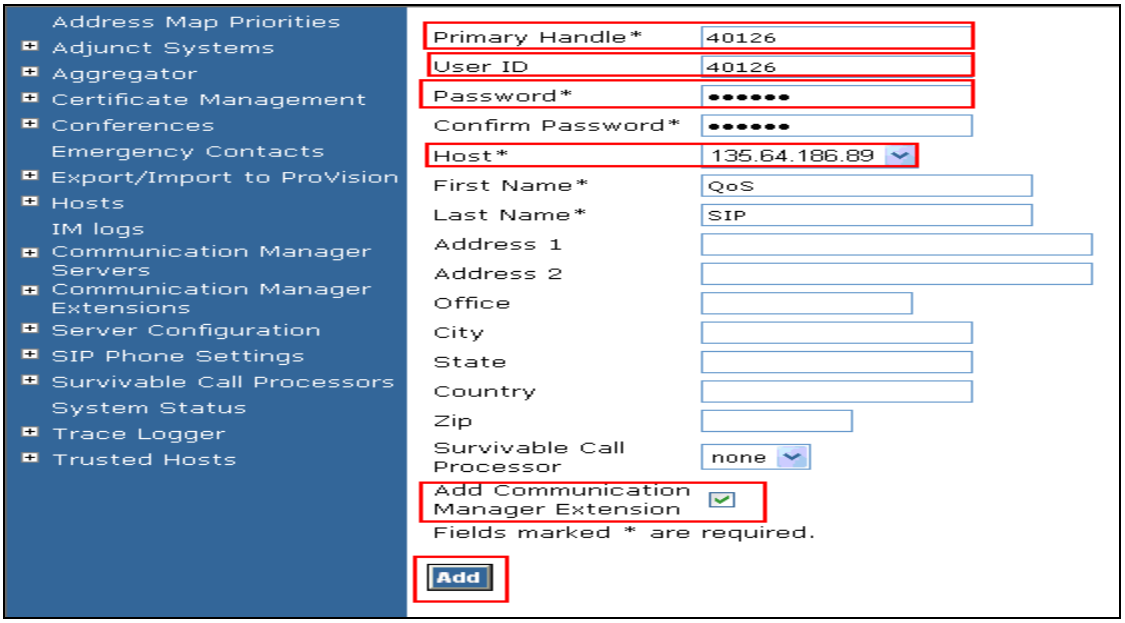
7.3. Add Host Screen

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 **SES 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.



7.4. Administer Avaya SIP Telephones on SIP Enablement Server

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**.



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**.

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.

From the Juniper SRX web interface, access the **Configure** tab, then the **Interfaces** heading on the left hand side of the graphical user interface. Verify the interfaces fe-0/0/2, fe-0/0/3 and fe-0/0/4are in service for the Juniper SRX210 as shown below.

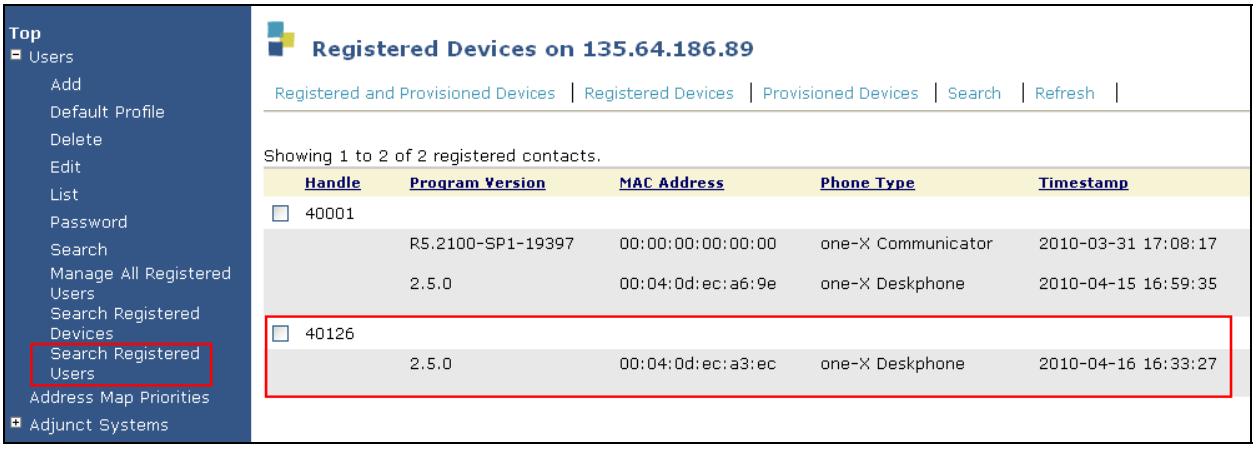
Verified calls can be made with clear audio from the Avaya IP telephone to the Avaya SIP telephone. Verified the calls are seen to be active within Communication Manager.

```
list trace station 40125

                                LIST TRACE

time            data

11:24:15     active station    40125 cid 0x473
11:24:15     G711MU ss:off ps:20
             rgn:1 [10.10.24.2]:2340
             rgn:1 [135.64.186.86]:2980
11:24:18     dial 40124
11:24:18     term station    40124 cid 0x473
11:24:20     active station    40124 cid 0x473
11:24:20     G711MU ss:off ps:20
             rgn:1 [10.10.25.2]:5004
             rgn:1 [10.10.24.2]:2340
11:24:20     G711MU ss:off ps:20
             rgn:1 [10.10.24.2]:2340
             rgn:1 [10.10.25.2]:5004
11:25:30     idle station    40125 cid 0x473
```

The screenshot below shows the Avaya IP Telephones registered to Communication Manager.

```
list registered-ip-stations

                            REGISTERED IP STATIONS

Station Ext   Set Type/ Prod ID/   TCP Station IP Address/
or Orig Port  Net Rgn   Release    Skt 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
```

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. The screenshot below shows the Avaya SIP telephone **40126** registered to SIP Enablement Services.



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

9. Conclusion

These Application Notes have described the administration steps required to configure: voice and data vlans on a router and Juniper SRX210 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 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] Juniper SRX210 Hardware Guide, Release 10.0, available at http://www.juniper.com

[6] Interface and Routing Configuration Guide for J-Series Services Routers and SRX–series Services Gateways, Release 10.0, available at http://www.juniper.com

[7] Network Policy and Service-Internet Engineering Task Forces RFC 2768 February 2000

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 interoplabnotes@list.avaya.com