Avaya Solution & Interoperability Test Lab

Application Notes for Configuring Cox Communications SIP Trunking Service with Avaya Aura® Communication Manager 6.3, Avaya Aura® Session Manager 6.3 and Avaya Session Border Controller for Enterprise 6.2 – Issue 1.0

Abstract

These Application Notes describe the steps to configure Session Initiation Protocol (SIP) Trunking between the Cox Communications SIP Trunking Service and an Avaya SIP-enabled enterprise solution. The Avaya solution consists of Avaya Aura® Session Manager 6.3, Avaya Aura® Communication Manager Evolution Server 6.3, Avaya Session Border Controller for Enterprise 6.2 and various Avaya endpoints. The Avaya solution connects to the Cox SIP Trunking Service via an on-site EdgeMarc 4550 WAN access router managed by Cox Communications. Cox Communications is a member of the Avaya DevConnect Service Provider program.

Information in these Application Notes has been obtained through DevConnect compliance testing and additional technical discussions. Testing was conducted via the DevConnect Program at the Avaya Solution and Interoperability Test Lab.

1. Introduction

These Application Notes describe the steps to configure Session Initiation Protocol (SIP) Trunking between the Cox Communications SIP Trunking Service and an Avaya SIP-enabled enterprise solution. The Avaya solution consists of Avaya Aura® Session Manager 6.3, Avaya Aura® Communication Manager Evolution Server 6.3, Avaya Session Border Controller for Enterprise 6.2 (Avaya SBCE) and various Avaya endpoints. In addition, Avaya Aura® System Manager 6.3 is used to configure Avaya Aura® Session Manager. This Avaya solution connects to the Cox Communications SIP Trunking Service via an on-site EdgeMarc 4550 WAN access router (EdgeMarc) managed by Cox Communications as the demarcation point for the service.

Customers using this Avaya SIP-enabled enterprise solution with the Cox Communications SIP Trunking Service are able to place and receive PSTN calls via a broadband WAN connection with SIP. This converged network solution is an alternative to traditional PSTN trunks such as ISDN-PRI.

2. General Test Approach and Test Results

The general test approach was to connect a simulated enterprise site to the Cox Communications SIP Trunking Service and exercise the features and functionality listed in **Section 2.1**. It should be noted that the connection between the enterprise and Cox Communications is via a Cox-managed network IP connection which includes the on-site EdgeMarc connected to the public Internet. The simulated enterprise site was comprised of Communication Manager, Session Manager and Avaya Session Border Controller for Enterprise.

DevConnect Compliance Testing is conducted jointly by Avaya and DevConnect members. The jointly-defined test plan focuses on exercising APIs and/or standards-based interfaces pertinent to the interoperability of the tested products and their functionalities. DevConnect Compliance Testing is not intended to substitute full product performance or feature testing performed by DevConnect members, nor is it to be construed as an endorsement by Avaya of the suitability or completeness of a DevConnect member’s solution.

2.1. Interoperability Compliance Testing

To verify SIP trunking interoperability, the following features and functionality were covered during the interoperability compliance test.

- Sending SIP OPTIONS queries to and receiving responses from the service provider.
- Incoming calls from the PSTN to H.323 and SIP telephones at the enterprise. All inbound PSTN calls were routed from the service provider across the SIP trunk to the enterprise.
- Outgoing calls to the PSTN from H.323 and SIP telephones at the enterprise. All outbound calls to the PSTN were routed from the enterprise across the SIP trunk to the service provider.
- Inbound and outbound PSTN calls to/from one-X Communicator (soft client).
  Avaya one-X® Communicator can place calls from the local computer or control a remote phone. Both of these modes were tested. one-X Communicator also supports two

Voice Over IP (VoIP) protocols: H.323 and SIP. Each protocol version of one-X Communicator was also tested.
- Inbound and outbound calls to Flare Experience for Windows.
- Various call types including: local, long distance, international, outbound toll-free, operator, operator-assisted and local directory assistance (411).
- G.711MU codec.
- DTMF transmission using RFC 2833.
- Caller ID presentation and Caller ID restriction.
- Response to incomplete call attempts and trunk errors.
- Voicemail navigation for inbound and outbound calls.
- Voicemail Message Waiting Indicator (MWI)
- User features such as hold and resume, internal call forwarding, transfer, and conference.
- Off-net call transfer, conference, forwarding and mobility (extension to cellular – EC500).

Emergency 911 and inbound toll-free calls are supported but were not tested as part of the compliance test.

2.2. Test Results

Interoperability testing of the Cox Communications SIP Trunking Service was completed with successful results for all test cases with the exception of the observations or limitations described below.

- **Call-ID in UPDATE**: The Cox on-site EdgeMarc changes/tracks Call-ID in messages from the Avaya SBCE with the exception of the UPDATE message, in which case the EdgeMarc just passes along the same Call-ID from Avaya. This could cause the following problems:
  - When Communication Manager used UPDATE for display update after an off-net call redirection (transfer or forward), Cox would reject the UPDATE with a "481 Unknown Dialog" status message, therefore failing the call redirection.
  - When Communication Manager issued UPDATE to refresh an active call session, Cox would reject the UPDATE with a "481 Unknown Dialog" status message, causing Communication Manager to drop the call.
  - The Call-ID in UPDATE passed along by the EdgeMarc could expose enterprise internal network IP addresses over the public Internet.

  Cox investigated this issue and opened a ticket to Edgewater Networks (EdgeMarc vendor). During compliance testing, Communication Manager was configured to use re-INVITE instead of UPDATE for display update (**see Section 5.7**). Also see **Section 5.7** for details on session refresh initiated from Communication Manager.

- **411 Call**: Outbound call to 411 Local Directory Assistance got connected but the caller received no audio, and after about 30 seconds Cox would drop the call by sending a BYE message. Cox investigated this issue and traced it to the enterprise WAN IP address not being whitelisted on the media gateway used by the service for the 411 call.

- **Calling Party Number (PSTN transfers)**: The calling party number displayed on the PSTN phone is not updated to reflect the true connected party on calls that are transferred to the PSTN. After the call transfer is complete, the calling party number displays the number of the transferring party and not the actual connected party. Communication Manager provides the new connected party information by updating the Contact header in an re-INVITE message but the far-end phone display is not updated. The PSTN phone display is ultimately controlled by the PSTN carrier, thus this behavior is not necessarily indicative of a limitation of the combined Avaya/Cox solution. It is listed here simply as an observation.

- **Session Refresh**: No message headers for session refresh handshake were contained in SIP messages from Cox, but Cox issued session-refresh re-INVITE messages at 10-minute intervals during the compliance test.

- **Remote Worker**: Remote Worker (phones connected directly to the public Internet function as enterprise local extensions) is not supported by the combined Avaya/Cox solution as documented in these Application Notes since its setup requires Avaya SBCE be directly connected to the public Internet via its public interface, whereas in the tested solution Avaya SBCE was connected to the on-site EdgeMarc via a network internal to the enterprise. Conceptually, Remote Worker can be implemented using a second and dedicated Avaya SBCE connected directly to the public Internet, but this setup was beyond the scope of the compliance test.

Items not supported by the Cox Communications SIP Trunking Service included the following:

- G.729 codec
- T.38 fax
- REFER with replaces – Cox does not support REFER with replaces but does support REFER without replaces. However, it is not possible to enable use of REFER on Communication Manager (e.g., Network Call Redirection) for just those scenarios that use REFER without replaces. Thus, this solution will not use REFER (i.e., disable Network Call Redirection on Communication Manager).

In addition, the Cox Communications SIP Trunking Service requires the following behavior in SIP messaging:

- Eleven (1+10) digits must be sent in the Request URI and To headers of an outbound SIP INVITE message. The 1+10 digits dialed by the user are passed unaltered through all enterprise components. See related routing **Sections 5.9**, **6.8** and **7.12.2**.
- The **user=phone** parameter must be set in the Request URI. See Communication Manager trunk group settings in **Section 5.7**.

2.3. Support

For technical support on the Cox Communications SIP Trunking Service, please contact Cox Communications via the following:

- Web: http://www.cox.com - follow the support links for particular service areas.
- Phone: 1-800-620-6196

Avaya customers may obtain documentation and support for Avaya products by visiting http://support.avaya.com.

3. Reference Configuration

Figure 1 illustrates a sample Avaya SIP-enabled enterprise solution connected to the Cox Communications SIP Trunking Service. This is the configuration used for compliance testing.

The components used to create the simulated customer site included:

- System Manager
- Session Manager
- Communication Manager
- Avaya G450 Media Gateway
- Avaya SBCE
- Avaya 1600-Series IP telephones (H.323)
- Avaya 9600-Series IP telephones (H.323 and SIP)
- Avaya 1100/1200-Series IP telephones (SIP)
- Avaya A175 Desktop Video Device (SIP)
- One-X Communicator softphone (H.323 and SIP)
- Flare Experience for Windows softphone (SIP)

The Cox Communications SIP Trunking Service deploys a WAN access router doubled as a session border controller (EdgeMarc 4550) at the enterprise site which is managed by Cox Communications and serves as the demarcation point for the service. The public side of the Avaya SBCE connects to the EdgeMarc and the private side connects to the enterprise network. All SIP and RTP traffic entering or leaving the enterprise flows through the Avaya SBCE. In this way, the Avaya SBCE can protect the enterprise against any SIP-based attacks. The Avaya SBCE provides network address translation at both the IP and SIP layers.

For security reasons, any actual public IP addresses used in the configuration have been replaced with private IP addresses in these Application Notes.

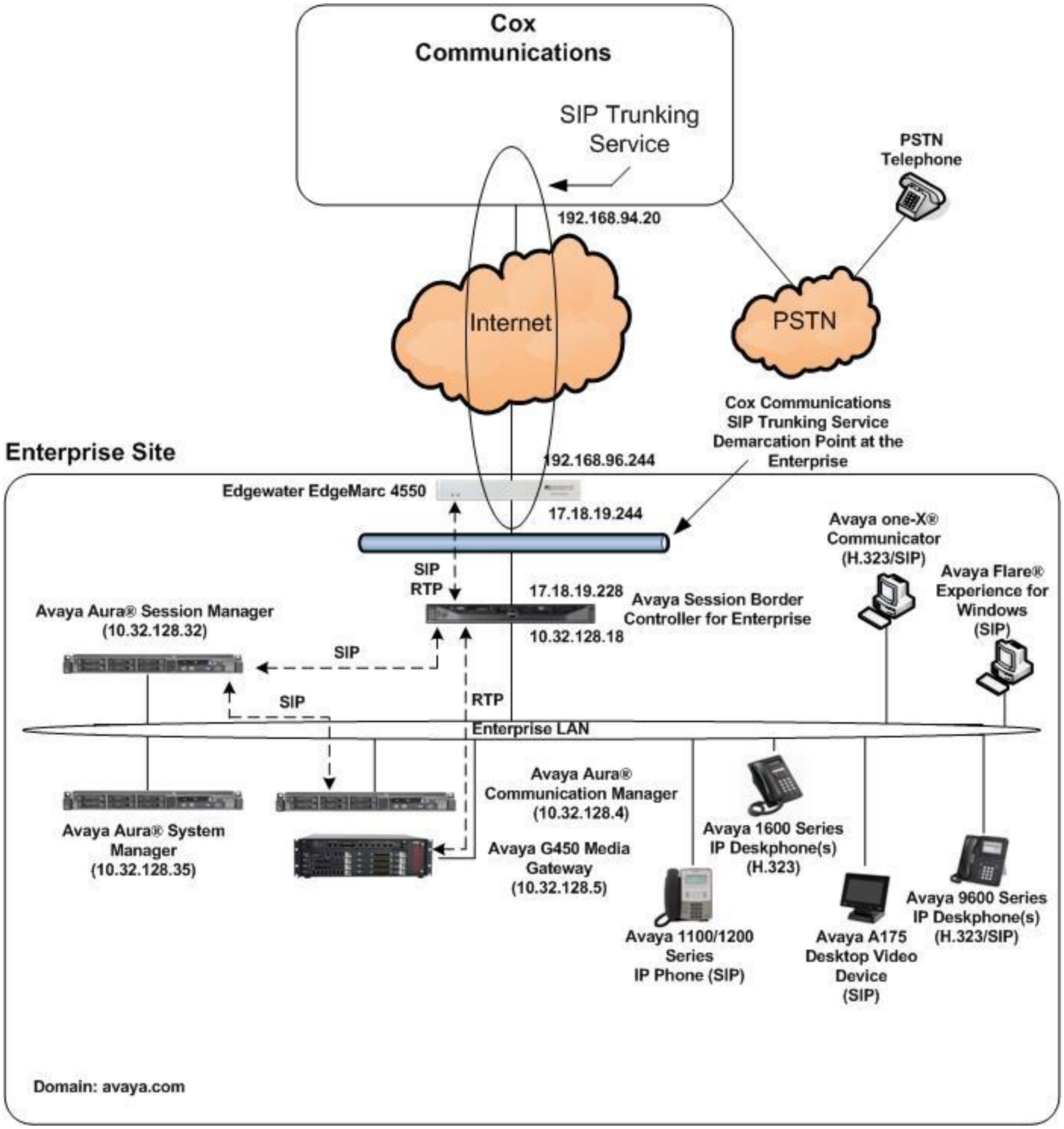

Cox Communications
SIP Trunking Service
PSTN Telephone
192.168.94.20
Internet
PSTN
Cox Communications SIP Trunking Service Demarcation Point at the Enterprise
Enterprise Site
192.168.96.244
Edgewater EdgeMarc 4550
17.18.19.244
SIP
RTP
17.18.19.228
Avaya Session Border Controller for Enterprise
10.32.128.18
Avaya Aura® Session Manager (10.32.128.32)
SIP
SIP
RTP
Enterprise LAN
Avaya one-X® Communicator (H.323/SIP)
Avaya Flare® Experience for Windows (SIP)
Avaya Aura® System Manager (10.32.128.35)
Avaya Aura® Communication Manager (10.32.128.4)
Avaya G450 Media Gateway (10.32.128.5)
Avaya 1600 Series IP Deskphone(s) (H.323)
Avaya 1100/1200 Series IP Phone (SIP)
Avaya A175 Desktop Video Device (SIP)
Avaya 9600 Series IP Deskphone(s) (H.323/SIP)
Domain: avaya.com

Figure 1: Avaya IP Telephony Network with the Cox Communications SIP Trunking Service

A dedicated trunk was created between Communication Manager and Session Manager to carry the service provider traffic. This was done so that any trunk or codec setting required by the service provider could be applied only to this trunk and not affect other enterprise SIP traffic. In addition, this trunk carried both inbound and outbound traffic.

For inbound calls, the calls flow from the service provider to the Avaya SBCE then to Session Manager. Session Manager uses the configured dial patterns (or regular expressions) and routing policies to determine the recipient (in this case Communication Manager) and on which link to send the call. Once the call arrives at Communication Manager, further incoming call treatment, such as incoming digit translations and class of service restrictions may be performed.

Outbound calls to the PSTN are first processed by Communication Manager and may be subject to outbound feature treatment such as automatic route selection, digit manipulation and class of service restrictions. Once Communication Manager selects the proper SIP trunk, the call is routed to Session Manager. Session Manager once again uses the configured dial patterns (or regular expressions) to determine the route to the Avaya SBCE. From the Avaya SBCE, the call is sent to the Cox Communications SIP Trunking Service.

For outbound calls, the Cox Communications SIP Trunking Service requires the enterprise send 11 (1+10) digits in the SIP destination headers (Request URI and To). In the SIP source headers (i.e., From, Contact, and P-Asserted-Identity), the enterprise sends 10 digits. For inbound calls, Cox Communications sends 10 digits in both the source headers and destination headers.

4. Equipment and Software Validated

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

Avaya IP Telephony Solution Components	
Equipment/Software	Release/Version
Avaya Aura® System Manager running on an HP® DL360 Server	6.3.8 (Build 6.3.0.8.5682-6.3.8.4219) (Software Update Revision 6.3.8.5.2376) System Platform 6.3.4.08007.0
Avaya Aura® Session Manager running on an HP® DL360 Server Server	6.3.8 (Build 6.3.8.0.638018)
Avaya Aura® Communication Manager running on an Avaya S8300 Server	6.3 SP6 (R016x.03.0.124.0-21591) System Platform 6.3.4.08007.0
Avaya G450 Media Gateway	34.5.1 /1
Avaya Session Border Controller for Enterprise running on a Dell R210 V2 server	6.2.1.Q18
Avaya 1616 IP Deskphone (H.323) running Avaya one-X® Deskphone Value Edition	1.3 SP4
Avaya 9611G IP Deskphone (H.323) running Avaya one-X® Deskphone Edition	6.3.1
Avaya 9621G IP Deskphone (SIP) running Avaya one-X® Deskphone SIP Edition	6.3.1
Avaya 1140E IP Telephone (SIP)	4.04.14.00s
Avaya A175 Desktop Video Device with Avaya Flare® Experience	SIP Version 1.1.3 (SIP_A175_1_1_3_021913)
Avaya one-X® Communicator (H.323 or SIP)	6.2.3.05-FP3
Avaya Flare® Experience for Windows	1.1.4.23
Cox Communications SIP Trunking Service Solution Components	
Equipment/Software	Release/Version
Edgewater EdgeMarc 4550	11.6.14
Acme Packet Net-Net 9200 Session Border Controller	nnSD710m4p2
Broadsoft SIP Application Server	AS, NS = R19

Table 1: Equipment and Software Tested

The specific configuration above was used for the compliance testing. Note that this solution will be compatible with other Avaya Server and Media Gateway platforms running similar versions of Communication Manager and Session Manager.

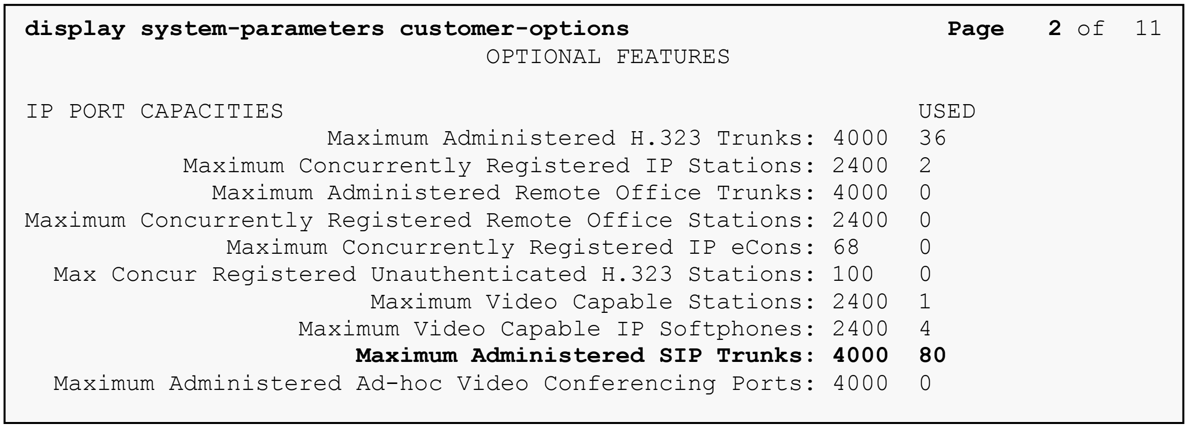
5. Configure Avaya Aura® Communication Manager

This section describes the procedure for configuring Communication Manager for the Cox Communications SIP Trunking Service. A SIP trunk is established between Communication Manager and Session Manager for use by traffic to and from Cox Communications. It is assumed the general installation of Communication Manager, Avaya Media Gateway and Session Manager has been previously completed and is not discussed here.

The Communication Manager configuration was performed using the System Access Terminal (SAT). Some screens in this section have been abridged and highlighted for brevity and clarity in presentation. Note that the IP addresses shown throughout these Application Notes have been edited so that the actual public IP addresses of the network elements are not revealed.

5.1. Licensing and Capacity

Use the **display system-parameters customer-options** command to verify that the **Maximum Administered SIP Trunks** value on **Page 2** is sufficient to support the desired number of simultaneous SIP calls across all SIP trunks at the enterprise including any trunks to the service provider. The example shows that **4000** SIP trunks are available and **80** are in use. The license file installed on the system controls the maximum values for these attributes. If a required feature is not enabled or there is insufficient capacity, contact an authorized Avaya sales representative to add additional capacity.



```
display system-parameters customer-options                    Page   2 of  11
                                OPTIONAL FEATURES

IP PORT CAPACITIES                                              USED
                     Maximum Administered H.323 Trunks: 4000  36
           Maximum Concurrently Registered IP Stations: 2400  2
             Maximum Administered Remote Office Trunks: 4000  0
Maximum Concurrently Registered Remote Office Stations: 2400  0
              Maximum Concurrently Registered IP eCons: 68    0
  Max Concur Registered Unauthenticated H.323 Stations: 100   0
                        Maximum Video Capable Stations: 2400  1
                   Maximum Video Capable IP Softphones: 2400  4
                       Maximum Administered SIP Trunks: 4000  80
  Maximum Administered Ad-hoc Video Conferencing Ports: 4000  0
```

5.2. System Features

Use the **change system-parameters features** command to set the **Trunk-to-Trunk Transfer** field to **all** to allow incoming calls from the PSTN to be transferred to another PSTN endpoint. If for security reasons, incoming calls should not be allowed to be transferred back to the PSTN then leave the field set to **none**.

```
change system-parameters features                               Page   1 of  20
                            FEATURE-RELATED SYSTEM PARAMETERS
                               Self Station Display Enabled? n
                                    Trunk-to-Trunk Transfer: all
               Automatic Callback with Called Party Queuing? n
    Automatic Callback - No Answer Timeout Interval (rings): 3
                       Call Park Timeout Interval (minutes): 10
        Off-Premises Tone Detect Timeout Interval (seconds): 20
                                 AAR/ARS Dial Tone Required? y
```

On **Page 9**, verify that a text string has been defined to replace the Calling Party Number (CPN) for restricted or unavailable calls. This text string is entered in the two fields highlighted below. The compliance test used the value of **anonymous** for both.

```
change system-parameters features                               Page   9 of  20
                        FEATURE-RELATED SYSTEM PARAMETERS

CPN/ANI/ICLID PARAMETERS
   CPN/ANI/ICLID Replacement for Restricted Calls: anonymous
  CPN/ANI/ICLID Replacement for Unavailable Calls: anonymous

DISPLAY TEXT
                                       Identity When Bridging: principal
                                        User Guidance Display? n
 Extension only label for Team button on 96xx H.323 terminals? n

INTERNATIONAL CALL ROUTING PARAMETERS
                 Local Country Code:
          International Access Code:

SCCAN PARAMETERS
   Enable Enbloc Dialing without ARS FAC? n

CALLER ID ON CALL WAITING PARAMETERS
     Caller ID on Call Waiting Delay Timer (msec): 200
```

5.3. IP Node Names

Use the **change node-names ip** command to verify that node names have been previously defined for the IP addresses of the server running Communication Manager **(procr**) and for Session Manager (**sessionMgr**). These node names will be needed for defining the service provider signaling group in **Section 5.6**.

```
change node-names ip                                              Page   1 of   2
                                  IP NODE NAMES
    Name              IP Address
cmm                 10.32.128.4
default             0.0.0.0
procr               10.32.128.4
procr6              ::
sessionMgr          10.32.128.32
```

5.4. Codecs

Use the **change ip-codec-set** command to define a list of codecs to use for calls between the enterprise and the service provider. The list should include the codecs and preferred order defined by the service provider. For the compliance test, codec G.711MU was tested using ip-codec-set 5. To configure the codecs, enter the codecs in the **Audio Codec** column of the table in the order of preference. Default values can be used for all other fields.

```
change ip-codec-set 5                                             Page   1 of   2

                          IP Codec Set

    Codec Set: 5

    Audio        Silence      Frames   Packet
    Codec        Suppression  Per Pkt  Size(ms)
 1: G.711MU           n         2        20
 2:
 3:
```

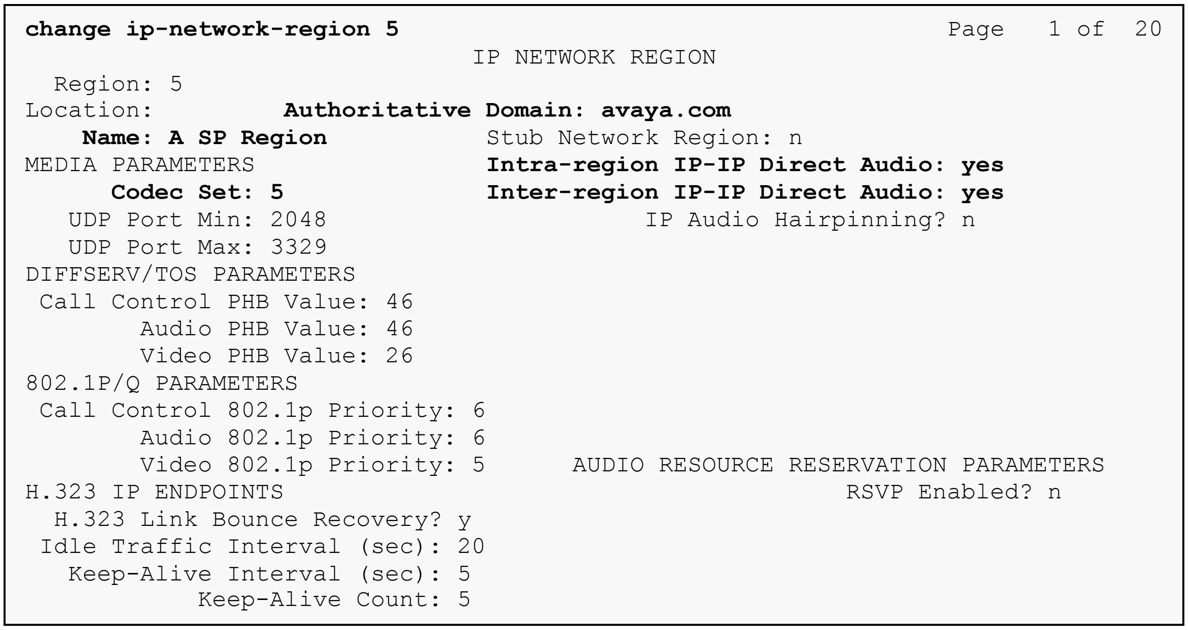
On **Page 2**, set the **Fax Mode** to **off** since T.38 fax calls are not supported with this solution.

```
change ip-codec-set 5                                             Page   2 of   2

                          IP Codec Set

                              Allow Direct-IP Multimedia? n

                    Mode                Redundancy
    FAX             off                  0
    Modem           off                  0
    TDD/TTY         US                   3
```

5.5. IP Network Region

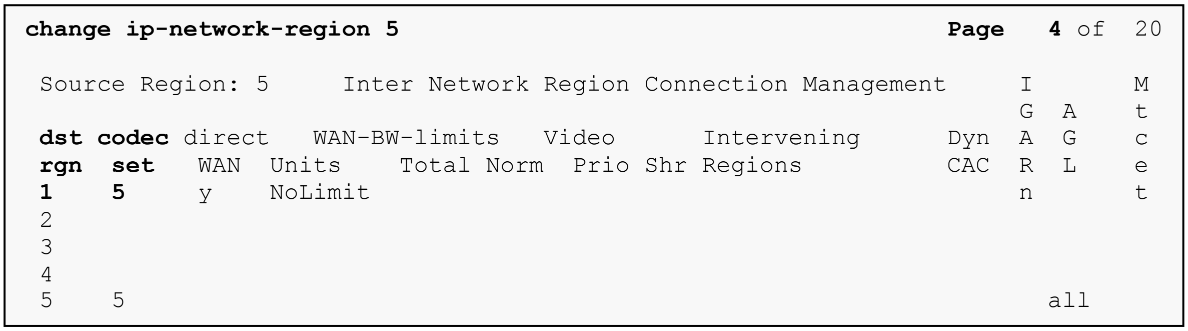
Create a separate IP network region for the service provider trunk. This allows for separate codec or quality of service settings to be used (if necessary) for calls between the enterprise and the service provider versus calls within the enterprise or elsewhere. For the compliance test, IP network region 5 was chosen for the service provider trunk. Use the **change ip-network-region 5** command to configure region 5 with the following parameters:

- Set the **Authoritative Domain** field to match the SIP domain of the enterprise. In this configuration, the domain name is **avaya.com**. This name appears in the "From" header of SIP messages originating from this IP region.
- Enter a descriptive name in the **Name** field.
- Enable **IP-IP Direct Audio** (shuffling) to allow audio traffic to be sent directly between IP endpoints without using media resources in the Avaya Media Gateway. Set both **Intra-region** and **Inter-region IP-IP Direct Audio** to **yes.** This is the default setting. Shuffling can be further restricted at the trunk level on the Signaling Group form.
- Set the **Codec Set** field to the IP codec set defined in **Section 5.4**.
- Default values can be used for all other fields.



```
change ip-network-region 5                                      Page   1 of  20
                               IP NETWORK REGION
  Region: 5
Location:         Authoritative Domain: avaya.com
    Name: A SP Region           Stub Network Region: n
MEDIA PARAMETERS                Intra-region IP-IP Direct Audio: yes
      Codec Set: 5              Inter-region IP-IP Direct Audio: yes
   UDP Port Min: 2048                      IP Audio Hairpinning? n
   UDP Port Max: 3329
DIFFSERV/TOS PARAMETERS
 Call Control PHB Value: 46
        Audio PHB Value: 46
        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
```

On **Page 4**, define the IP codec set to be used for traffic between region 5 and region 1. Enter the desired IP codec set in the **codec set** column of the row with destination region (**dst rgn**) **1**. Default values may be used for all other fields. The example below shows the settings used for the compliance test. It indicates that codec set 5 will be used for calls between region 5 (the service provider region) and region 1 (the rest of the enterprise). Creating this table entry for IP network region 5 will automatically create a complementary table entry on the IP network region 1 form for destination region 5. This complementary table entry can be viewed using the **display ip-network-region 1** command and navigating to **Page 4** (not shown).



```
change ip-network-region 5                                Page   4 of  20

 Source Region: 5     Inter Network Region Connection Management     I       M
                                                                      G  A    t
 dst codec direct   WAN-BW-limits   Video      Intervening      Dyn  A  G    c
 rgn  set   WAN  Units    Total Norm  Prio Shr Regions          CAC  R  L    e
 1    5     y    NoLimit                                              n       t
 2
 3
 4
 5    5                                                                 all
```

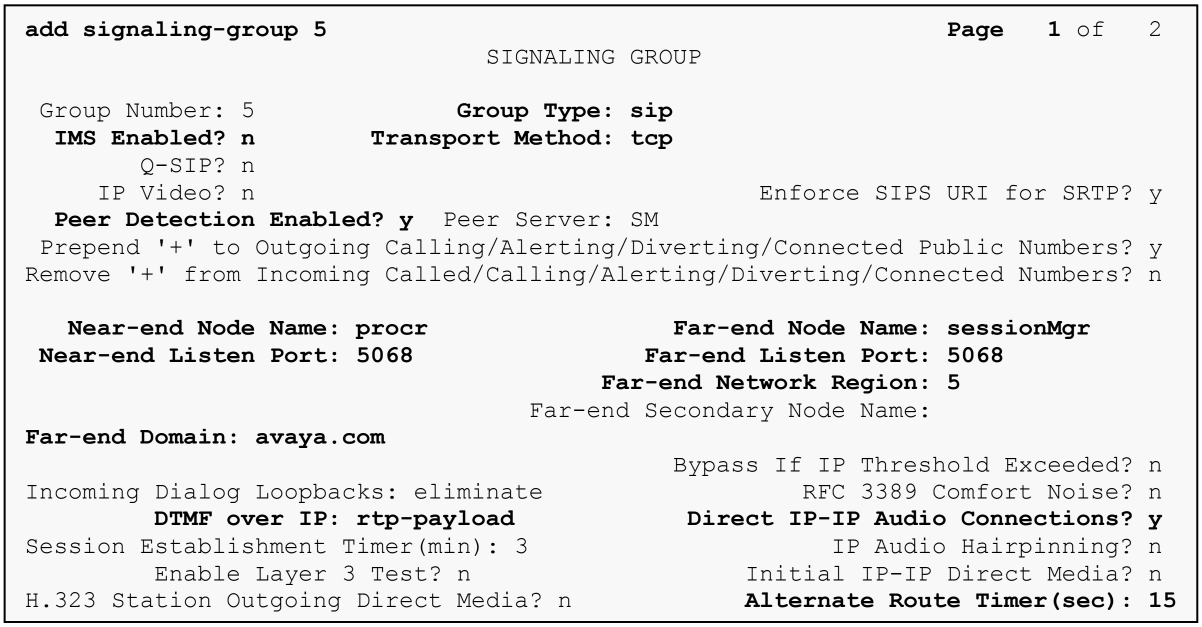
5.6. Signaling Group

Use the **add signaling-group** command to create a signaling group between Communication Manager and Session Manager for use by the service provider trunk. This signaling group is used for inbound and outbound calls between the service provider and the enterprise. For the compliance test, signaling group 5 was used for this purpose and was configured using the parameters highlighted below.

- Set the **Group Type** field to **sip**.
- Set the **Transport Method** to the recommended default value of **tls** (Transport Layer Security). For ease of troubleshooting during testing, the compliance test was conducted with the **Transport Method** set to **tcp**. The transport method specified here is used between Communication Manager and Session Manager. If TLS is used here, it must also be used on the Session Manager entity link defined in **Section 6.6**.
- Set the **IMS Enabled** field to **n**. This specifies Communication Manager will serve as an Evolution Server for Session Manager.
- Set the **Peer Detection Enabled** field to **y**. The **Peer-Server** field will initially be set to **Others** and cannot be changed via administration. Later, the **Peer-Server** field will automatically change to **SM** once Communication Manager detects its peer as a Session Manager.
- Set the **Near-end Node Name** to **procr**. This node name maps to the IP address of the Communication Manager as defined in **Section 5.3**.
- Set the **Far-end Node Name** to **sessionMgr**. This node name maps to the IP address of Session Manager as defined in **Section 5.3**.
- Set the **Near-end Listen Port** and **Far-end Listen Port** to a valid unused port instead of the default well-known port value. (For TLS, the well-known port value is 5061 and for TCP the well-known port value is 5060). At the time of Session Manager installation, a

SIP connection between Communication Manager and Session Manager would have been established for use by all Communication Manager SIP traffic using the well-known port value for TLS or TCP. By creating a new signaling group with a separate port value, a separate SIP connection is created between Communication Manager and Session Manager for SIP traffic to and from the service provider. As a result, any signaling group or trunk group settings (**Section 5.7**) will only affect the service provider traffic and not other SIP traffic at the enterprise. The compliance test was conducted with the **Near-end Listen Port** and **Far-end Listen Port** set to **5068**.

- Set the **Far-end Network Region** to the IP network region defined for the service provider in **Section 5.5**.
- Set the **Far-end Domain** to the domain of the enterprise.
- Set **Direct IP-IP Audio Connections** to **y**. This field will enable media shuffling on the SIP trunk allowing Communication Manager to redirect media traffic directly between the SIP trunk and the enterprise endpoint.
- Set the **DTMF over IP** field to **rtp-payload**. This value enables Communication Manager to send DTMF transmissions using RFC 2833.
- Set the **Alternate Route Timer** to **15**. This defines the number of seconds that Communication Manager will wait for a response (other than "100 Trying") to an outbound INVITE before selecting another route. If an alternate route is not defined, then the call is cancelled after this interval.
- Default values may be used for all other fields.



```
add signaling-group 5                                           Page   1 of   2
                                SIGNALING GROUP

 Group Number: 5             Group Type: sip
  IMS Enabled? n        Transport Method: tcp
        Q-SIP? n
     IP Video? n                                   Enforce SIPS URI for SRTP? y
  Peer Detection Enabled? y  Peer Server: SM
 Prepend '+' to Outgoing Calling/Alerting/Diverting/Connected Public Numbers? y
Remove '+' from Incoming Called/Calling/Alerting/Diverting/Connected Numbers? n

   Near-end Node Name: procr                 Far-end Node Name: sessionMgr
 Near-end Listen Port: 5068                Far-end Listen Port: 5068
                                        Far-end Network Region: 5
                                   Far-end Secondary Node Name:
Far-end Domain: avaya.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                   Initial IP-IP Direct Media? n
H.323 Station Outgoing Direct Media? n           Alternate Route Timer(sec): 15
```

5.7. Trunk Group

Use the **add trunk-group** command to create a trunk group for the signaling group created in **Section 5.6**. For the compliance test, trunk group 5 was configured using the parameters highlighted below.

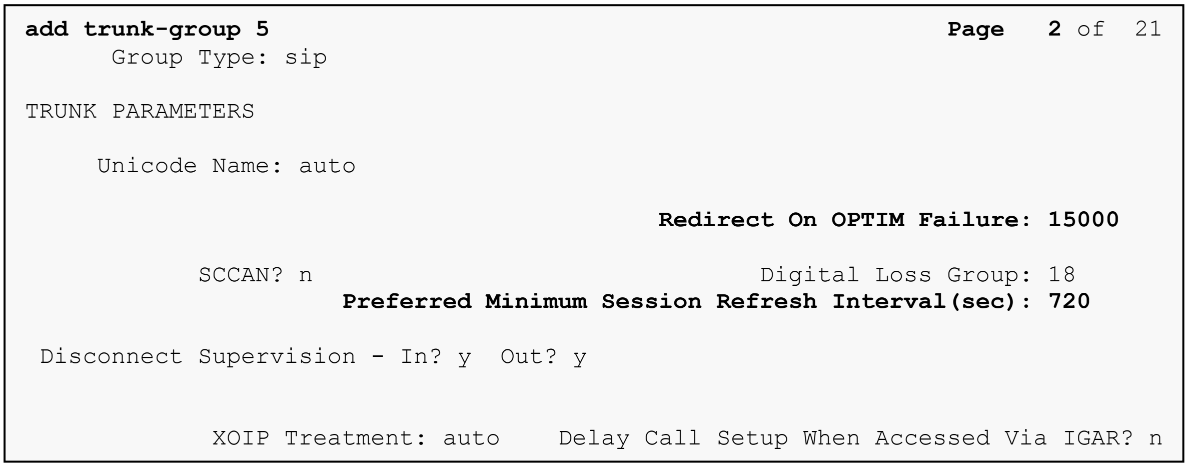
- Set the **Group Type** field to **sip**.
- Enter a descriptive name for the **Group Name**.
- Enter an available trunk access code (TAC) that is consistent with the existing dial plan in the **TAC** field.
- Set the **Service Type** field to **public-ntwrk**.
- Set **Member Assignment Method** to **auto**.
- Set the **Signaling Group** to the signaling group defined in **Section 5.6**.
- Set the **Number of Members** field to the number of trunk members in the SIP trunk group. This value determines how many simultaneous SIP calls can be supported by this trunk.
- Default values were used for all other fields.

```
add trunk-group 5                                                Page   1 of  21
                                TRUNK GROUP

Group Number: 5                   Group Type: sip           CDR Reports: y
  Group Name: A-SP-Trunk                 COR: 1        TN: 1        TAC: 1005
   Direction: two-way        Outgoing Display? n
 Dial Access? n                                Night Service:
Queue Length: 0
Service Type: public-ntwrk          Auth Code? n
                                             Member Assignment Method: auto
                                                      Signaling Group: 5
                                                    Number of Members: 10
```

On **Page 2**, the **Redirect On OPTIM Failure** value is the amount of time (in milliseconds) that Communication Manager will wait for a response (other than “100 Trying”) to a pending INVITE sent to an EC500 remote endpoint before selecting another route. If another route is not defined, then the call is cancelled after this interval. This time interval should be set to a value equal to the **Alternate Route Timer** on the signaling group form described in **Section 5.6**.

Verify that the **Preferred Minimum Session Refresh Interval** is set to a value acceptable to the service provider. This value defines the interval that re-INVITEs must be sent to keep the active session alive. For the compliance test, the value of **720** seconds was used.

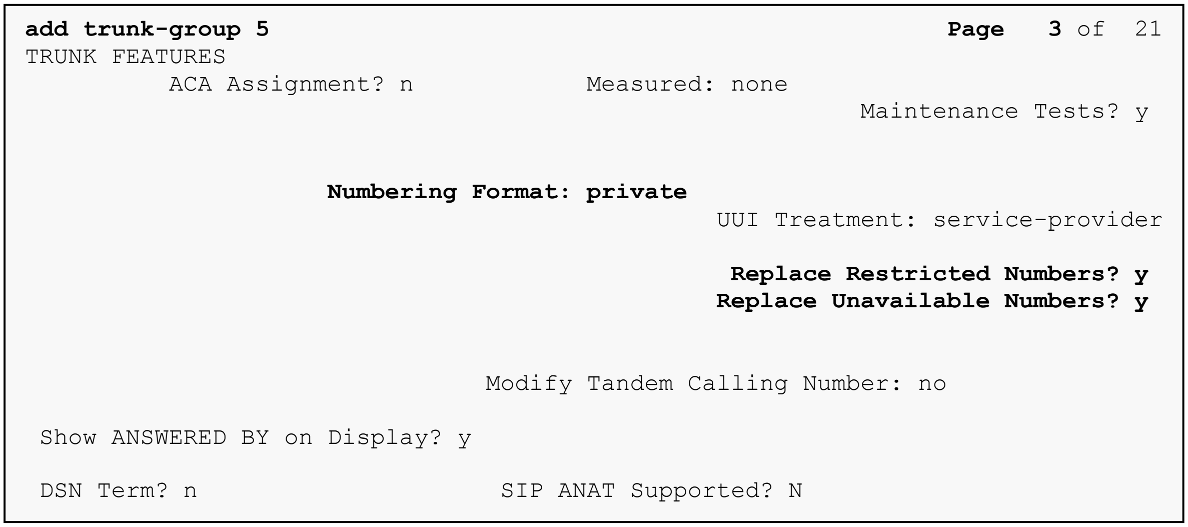
Communication Manager determines whether to use UPDATE or re-INVITE for session refresh based on whether UPDATE is supported by the remote end (i.e., whether the Allow header in messages from the remote end includes UPDATE). However, the Cox on-site EdgeMarc strips out the Allow header in messages it passes along to the enterprise, therefore Communication Manager could issue either message for session refresh depending on specific implementations in different versions of Communication Manager. The Communication Manager used for the compliance test (Release 6.3 SP6) uses re-INVITE for session refresh in the situation of seeing no Allow header in messages from the remote end, but there is no guarantee that other versions of Communication Manager or patches will do the same. To be on the safe side, the value of **720** seconds (or any value larger than 600 seconds) was used for **Preferred Minimum Session Refresh Interval**. This setting effectively disables session refresh initiated from Communication Manager since it resets the session-refresh timer each time it receives a session refresh message from the remote end (Cox initiates session refresh re-INVITEs at 10-minite intervals). This setting is related to the items **Call-ID in UPDATE** and **Session Refresh** in the limitation/observation list in **Section 2.2**).



```
add trunk-group 5                                               Page   2 of  21
      Group Type: sip

TRUNK PARAMETERS

     Unicode Name: auto

                                            Redirect On OPTIM Failure: 15000

            SCCAN? n                                   Digital Loss Group: 18
                      Preferred Minimum Session Refresh Interval(sec): 720

 Disconnect Supervision - In? y  Out? y


             XOIP Treatment: auto    Delay Call Setup When Accessed Via IGAR? n
```

On **Page 3**, set the **Numbering Format** field to **private**. This field specifies the format of the calling party number (CPN) sent to the far-end. Beginning with Communication Manager 6.0, public numbers are automatically preceded with a + sign (E.164 numbering format) when passed in the SIP From, Contact and P-Asserted Identity headers. To remove the + sign, the **Numbering Format** was set to **private** and the **Numbering Format** in the route pattern was set to **unk-unk** (see **Section 5.9**).

Set the **Replace Restricted Numbers** and **Replace Unavailable Numbers** fields to **y**. This will allow the CPN displayed on local endpoints to be replaced with the value set in **Section 5.2**, if the inbound call enabled CPN block. For outbound calls, these same settings request that CPN block be activated on the far-end destination if a local user requests CPN block on a particular call routed out this trunk. Default values were used for all other fields.

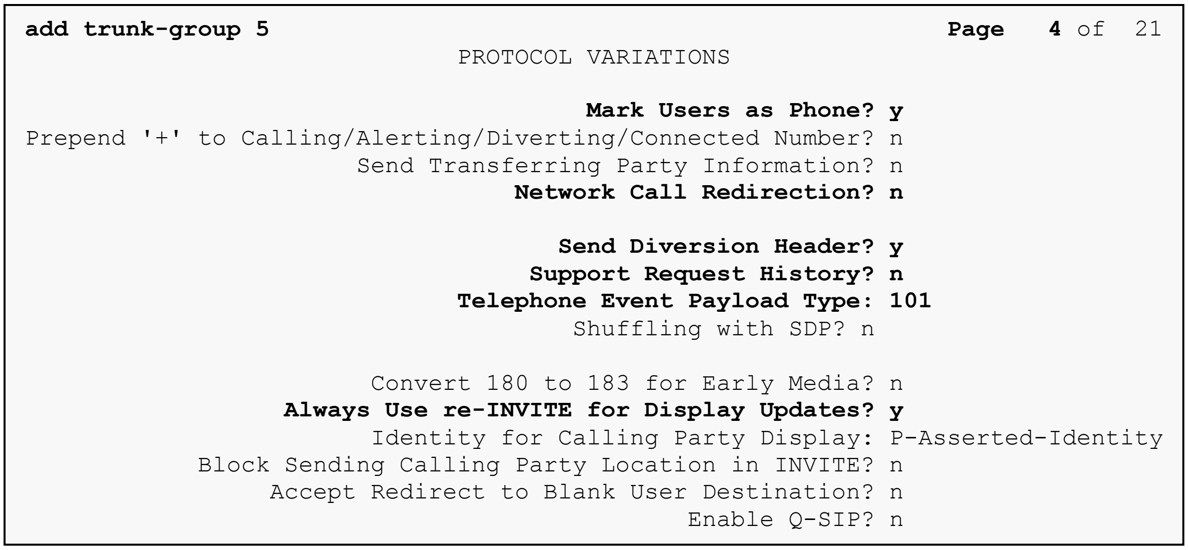


```
add trunk-group 5                                               Page   3 of  21
TRUNK FEATURES
          ACA Assignment? n            Measured: none
                                                          Maintenance Tests? y


                     Numbering Format: private
                                                UUI Treatment: service-provider

                                                 Replace Restricted Numbers? y
                                                Replace Unavailable Numbers? y


                                Modify Tandem Calling Number: no

 Show ANSWERED BY on Display? y

 DSN Term? n                     SIP ANAT Supported? N
```

On **Page 4**, set the **Mark Users as Phone** field to **y** which is required by Cox Communications. Since Cox Communications does not support all REFER scenarios (e.g., REFER with replaces) then the **Network Call Redirection** field must be set to **n**. Set the **Send Diversion Header** field to **y** and the **Support Request History** field to **n**. The **Send Diversion Header** field provides additional information to the network if the call has been redirected. These settings are needed to support call forwarding of inbound calls back to the PSTN and some Extension to Cellular (EC500) call scenarios.

Set **Telephone Event Payload Type** to **101**, the value used by Cox Communications.

Set **Always Use re-INVITE for Display Updates** to **y**. This setting directs Communication Manager to use re-INVITE instead of UPDATE (if supported by the remote end) for phone display update in off-net call re-directions (forward and transfer). See the item **Call-ID in UPDATE** in **Section 2.2** for details.



```
add trunk-group 5                                               Page   4 of  21
                              PROTOCOL VARIATIONS

                                       Mark Users as Phone? y
Prepend '+' to Calling/Alerting/Diverting/Connected Number? n
                       Send Transferring Party Information? n
                                  Network Call Redirection? n

                                     Send Diversion Header? y
                                   Support Request History? n
                              Telephone Event Payload Type: 101
                                      Shuffling with SDP? n

                        Convert 180 to 183 for Early Media? n
                  Always Use re-INVITE for Display Updates? y
                        Identity for Calling Party Display: P-Asserted-Identity
            Block Sending Calling Party Location in INVITE? n
                 Accept Redirect to Blank User Destination? n
                                              Enable Q-SIP? n
```

To ensure interoperability with Avaya SIP endpoints, the **Mark Users as Phone** field must also be set to **y** on the SIP trunk used by the SIP endpoints to register and communicate with the Session Manager. In most cases, this will be the trunk created during the initial installation of the Session Manager. In the case of the compliance test, this was trunk-group 1.

```
change trunk-group 1                                            Page   4 of  21
                              PROTOCOL VARIATIONS

                                       Mark Users as Phone? y
Prepend '+' to Calling/Alerting/Diverting/Connected Number? n
                       Send Transferring Party Information? n
                                  Network Call Redirection? n

                                     Send Diversion Header? n
                                   Support Request History? y
                              Telephone Event Payload Type:
                                      Shuffling with SDP? n

                        Convert 180 to 183 for Early Media? n
                  Always Use re-INVITE for Display Updates? n
                        Identity for Calling Party Display: P-Asserted-Identity
            Block Sending Calling Party Location in INVITE? n
                 Accept Redirect to Blank User Destination? n
                                              Enable Q-SIP? n
```

5.8. Calling Party Information

The calling party number is sent in the SIP "From", "Contact" and "PAI" headers. Since private numbering was selected to define the format of this number (**Section 5.7**), use the **change private-numbering** command to create an entry for each extension which has a DID assigned. The DID number will be assigned by the SIP service provider. It is used to authenticate the caller.

The screen below shows a subset of the DID numbers assigned for testing. These numbers were assigned to the five extensions 41012, 41016, 41018, 41020 and 41024. Thus, these same 10-digit numbers were used in the outbound calling party information on the service provider trunk when calls were originated from these extensions.

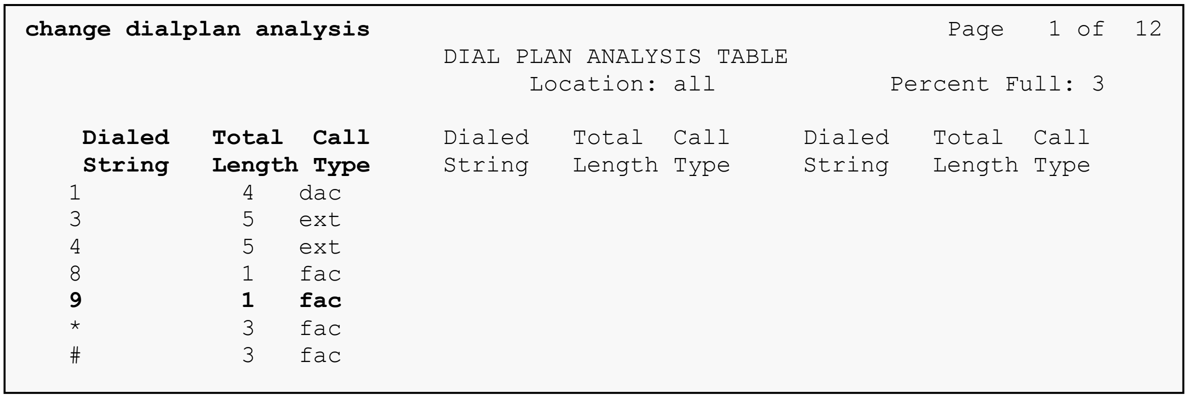
```
change private-numbering 5                                      Page   1 of   2
                           NUMBERING - PRIVATE FORMAT

Ext Ext               Trk        Private          Total
Len Code              Grp(s)     Prefix           Len
 5  4                                             5     Total Administered: 6
 5  41012             5          7036638122       10       Maximum Entries: 540
 5  41016             5          7036638126       10
 5  41018             5          7036638143       10
 5  41020             3          7036638150       10
 5  40024             3          7036638133       10
```

In a real customer environment, normally the DID number is comprised of the local extension plus a prefix. If this is true, then a single private numbering entry can be applied for all extensions. In the example below, all stations with a 5-digit extension beginning with 3 will send the calling party number as the **Private Prefix** plus the extension number.

```
change private-numbering 5                                      Page   1 of   2
                           NUMBERING - PRIVATE FORMAT

Ext Ext               Trk        Private      Total
Len Code              Grp(s)     Prefix        Len
 5  3                                          5     Total Administered: 2
 5  3                 3          70366         10       Maximum Entries: 540
```

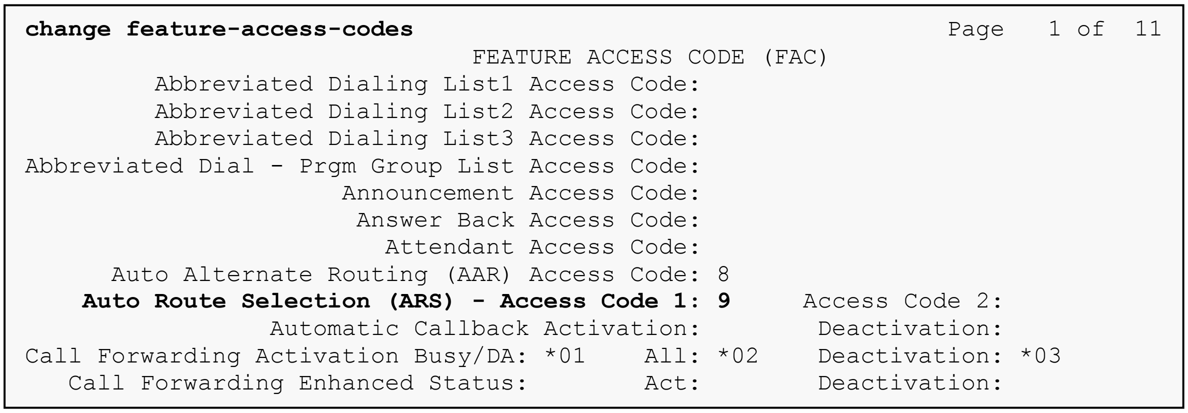
5.9. Outbound Routing

In these Application Notes, the Automatic Route Selection (ARS) feature is used to route outbound calls via the SIP trunk to the service provider. In the sample configuration, the single digit 9 is used as the ARS access code. Enterprise callers will dial 9 to reach an “outside line”. This common configuration is illustrated below with little elaboration. Use the **change dialplan analysis** command to define a dialed string beginning with 9 of length 1 as a feature access code (**fac**).



```
change dialplan analysis                                        Page   1 of  12
                             DIAL PLAN ANALYSIS TABLE
                                   Location: all           Percent Full: 3

    Dialed   Total  Call     Dialed   Total  Call      Dialed   Total  Call
    String   Length Type     String   Length Type      String   Length Type
   1           4   dac
   3           5   ext
   4           5   ext
   8           1   fac
   9           1   fac
   *           3   fac
   #           3   fac
```

Use the **change feature-access-codes** command to configure **9** as the **Auto Route Selection (ARS) – Access Code 1**.



```
change feature-access-codes                                     Page   1 of  11
                               FEATURE ACCESS CODE (FAC)
         Abbreviated Dialing List1 Access Code:
         Abbreviated Dialing List2 Access Code:
         Abbreviated Dialing List3 Access Code:
Abbreviated Dial - Prgm Group List Access Code:
                      Announcement Access Code:
                       Answer Back Access Code:
                         Attendant Access Code:
      Auto Alternate Routing (AAR) Access Code: 8
    Auto Route Selection (ARS) - Access Code 1: 9     Access Code 2:
                 Automatic Callback Activation:        Deactivation:
Call Forwarding Activation Busy/DA: *01    All: *02    Deactivation: *03
   Call Forwarding Enhanced Status:        Act:        Deactivation:
```

Use the **change ars analysis** command to configure the routing of dialed digits following the first digit 9. The example below shows a subset of the dialed strings tested as part of the compliance test. See **Section 2.1** for the complete list of call types tested. All dialed strings are mapped to route pattern **55** which contains the SIP trunk to the service provider (as defined next).

```
change ars analysis 0                                          Page   1 of   2
                             ARS DIGIT ANALYSIS TABLE
                                   Location: all            Percent Full: 1

          Dialed           Total     Route    Call   Node  ANI
          String          Min  Max  Pattern   Type   Num   Reqd
    0                     1    1     55       op           n
    0                     11   11    55       op           n
    011                   10   18    55       intl         n
    1703                  11   11    55       fnpa         n
    1732                  11   11    55       fnpa         n
    1800                  11   11    55       fnpa         n
    1877                  11   11    55       fnpa         n
    1908                  11   11    55       fnpa         n
    411                   3    3     55       svcl         n
```

The route pattern defines which trunk group will be used for the call and performs any necessary digit manipulation. Use the **change route-pattern** command to configure the parameters for the service provider route pattern in the following manner. The example below shows the values used for route pattern 55 configured for the compliance test.

- **Pattern Name**: Enter a descriptive name.
- **Grp No**: Enter the outbound trunk group for the SIP service provider. For the compliance test, trunk group **5** was used.
- **FRL**: Set the Facility Restriction Level (**FRL**) field to a level that allows access to this trunk for all users that require it. The value of **0** is the least restrictive level.
- **Pfx Mrk**: **1** The prefix mark (**Pfx Mrk**) of one will prefix any FNPA 10-digit number with a 1 and leave numbers of any other length unchanged. This will ensure 1 + 10 digits are sent to the Session Manager for long distance North American Numbering Plan (NANP) numbers.
- **Numbering Format**: **unk-unk** All calls using this route pattern will use the private numbering table. See setting of the **Numbering Format** in the trunk group form for full details in **Section 5.7**.
- **LAR**: **next**

```
change route-pattern 55                                         Page   1 of   3
                    Pattern Number: 4   Pattern Name: A-SP Route
                             SCCAN? n     Secure SIP? n
    Grp FRL NPA Pfx Hop Toll No. Inserted                            DCS/ IXC
    No          Mrk Lmt List Del  Digits                              QSIG
                             Dgts                                     Intw
 1: 5    0       1                                                    n   user
 2:                                                                   n   user
 3:                                                                   n   user
 4:                                                                   n   user
 5:                                                                   n   user
 6:                                                                   n   user

     BCC VALUE  TSC CA-TSC    ITC BCIE Service/Feature PARM  No. Numbering LAR
    0 1 2 M 4 W     Request                                 Dgts Format
                                                         Subaddress
 1: y y y y y n  n            rest                               unk-unk   next
 2: y y y y y n  n            rest                                         none
 3: y y y y y n  n            rest                                         none
 4: y y y y y n  n            rest                                         none
 5: y y y y y n  n            rest                                         none
 6: y y y y y n  n            rest                                         none
```

6. Configure Avaya Aura® Session Manager

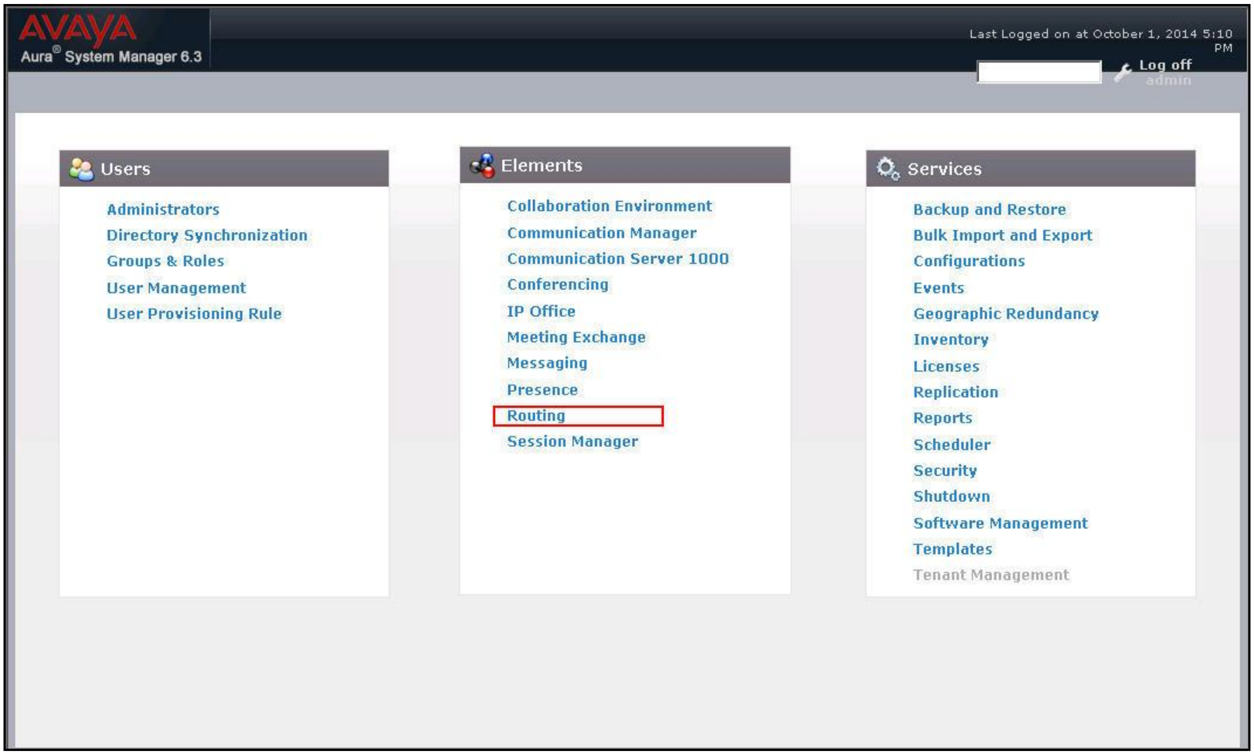
This section provides the procedures for configuring Session Manager. The procedures include configuring the following items:

- SIP domain
- Logical/physical Location that can be occupied by SIP Entities
- Adaptation module to perform dial plan manipulation
- SIP Entities corresponding to Communication Manager, the Avaya SBCE and Session Manager
- Entity Links, which define the SIP trunk parameters used by Session Manager when routing calls to/from SIP Entities
- Routing Policies, which control call routing between the SIP Entities
- Dial Patterns, which governs which Routing Policy is used to service a call.
- Session Manager, corresponding to the Session Manager Server to be managed by System Manager.

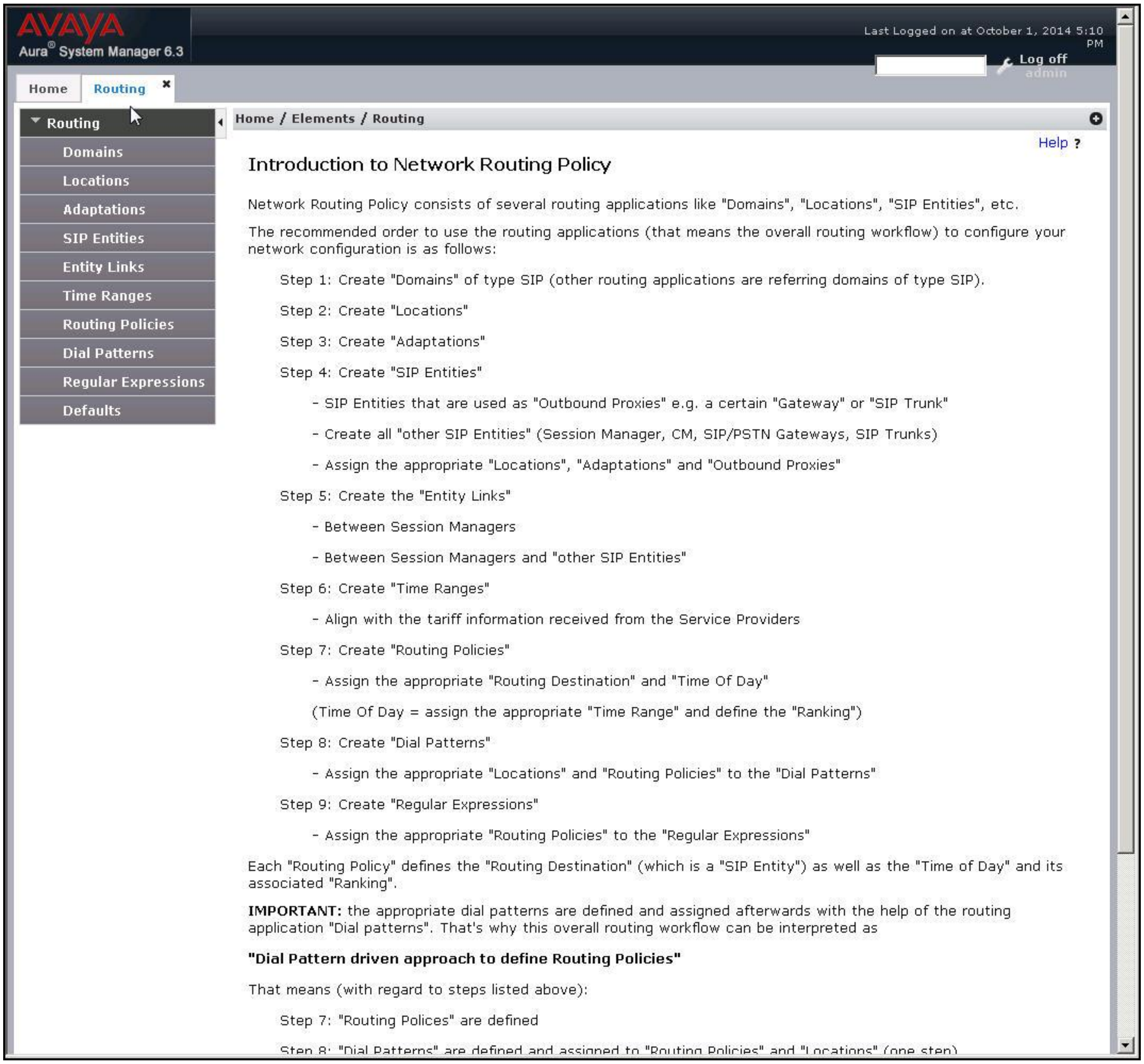
It may not be necessary to create all the items above when creating a connection to the service provider since some of these items would have already been defined as part of the initial Session Manager installation. This includes items such as certain SIP domains, locations, SIP entities, and Session Manager itself. However, each item should be reviewed to verify the configuration.

6.1. Avaya Aura® System Manager Login and Navigation

Session Manager configuration is accomplished by accessing the browser-based GUI of System Manager, using the URL **https://<ip-address>/SMGR**, where **<ip-address>** is the IP address of System Manager. Log in with the appropriate credentials. The **Home** page is displayed. The links displayed below will be referenced in subsequent sections to navigate to items requiring configuration. Most items will be located under the **Elements → Routing** link highlighted below.



Clicking the **Elements → Routing** link, displays the **Introduction to Network Routing Policy** page. In the left-hand pane is a navigation tree containing many of the items to be configured in the following sections.



Introduction to Network Routing Policy

Network Routing Policy consists of several routing applications like "Domains", "Locations", "SIP Entities", etc.

The recommended order to use the routing applications (that means the overall routing workflow) to configure your network configuration is as follows:

Step 1: Create "Domains" of type SIP (other routing applications are referring domains of type SIP).

Step 2: Create "Locations"

Step 3: Create "Adaptations"

Step 4: Create "SIP Entities"

- SIP Entities that are used as "Outbound Proxies" e.g. a certain "Gateway" or "SIP Trunk"
- Create all "other SIP Entities" (Session Manager, CM, SIP/PSTN Gateways, SIP Trunks)
- Assign the appropriate "Locations", "Adaptations" and "Outbound Proxies"

Step 5: Create the "Entity Links"

- Between Session Managers
- Between Session Managers and "other SIP Entities"

Step 6: Create "Time Ranges"

- Align with the tariff information received from the Service Providers

Step 7: Create "Routing Policies"

- Assign the appropriate "Routing Destination" and "Time Of Day"

(Time Of Day = assign the appropriate "Time Range" and define the "Ranking")

Step 8: Create "Dial Patterns"

- Assign the appropriate "Locations" and "Routing Policies" to the "Dial Patterns"

Step 9: Create "Regular Expressions"

- Assign the appropriate "Routing Policies" to the "Regular Expressions"

Each "Routing Policy" defines the "Routing Destination" (which is a "SIP Entity") as well as the "Time of Day" and its associated "Ranking".

IMPORTANT: the appropriate dial patterns are defined and assigned afterwards with the help of the routing application "Dial patterns". That's why this overall routing workflow can be interpreted as

"Dial Pattern driven approach to define Routing Policies"

That means (with regard to steps listed above):

Step 7: "Routing Polices" are defined

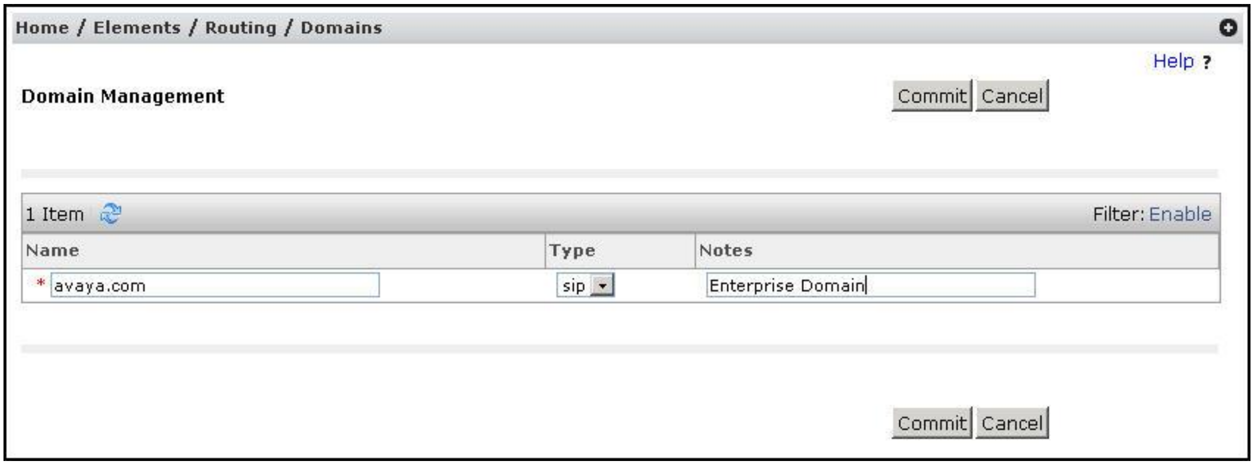
Step 8: "Dial Patterns" are defined and assigned to "Routing Policies" and "Locations" (one step)

6.2. Specify SIP Domain

Create a SIP domain for each domain of which Session Manager will need to be aware in order to route calls. For the compliance test, this includes the enterprise domain (**avaya.com**). Navigate to **Routing → Domains** in the left-hand navigation pane (**Section 6.1**) and click the **New** button in the right pane (not shown). In the new right pane that appears (shown below), fill in the following:

- **Name:** Enter the domain name.
- **Type:** Select **sip** from the pull-down menu.
- **Notes:** Add a brief description (optional).

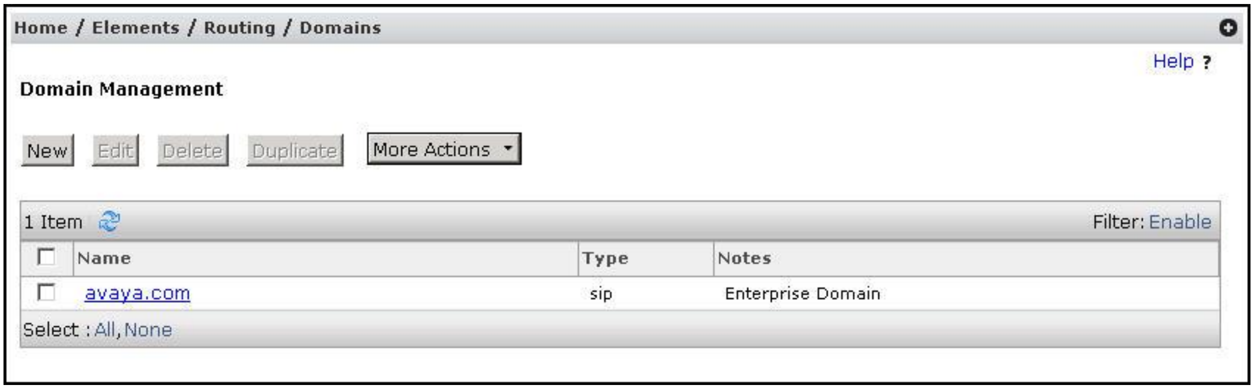
Click **Commit** to save.



Domain Management

Name	Type	Notes
* avaya.com	sip	Enterprise Domain

The screen below shows the configured entry for the enterprise domain.



Domain Management

□	Name	Type	Notes
□	avaya.com	sip	Enterprise Domain

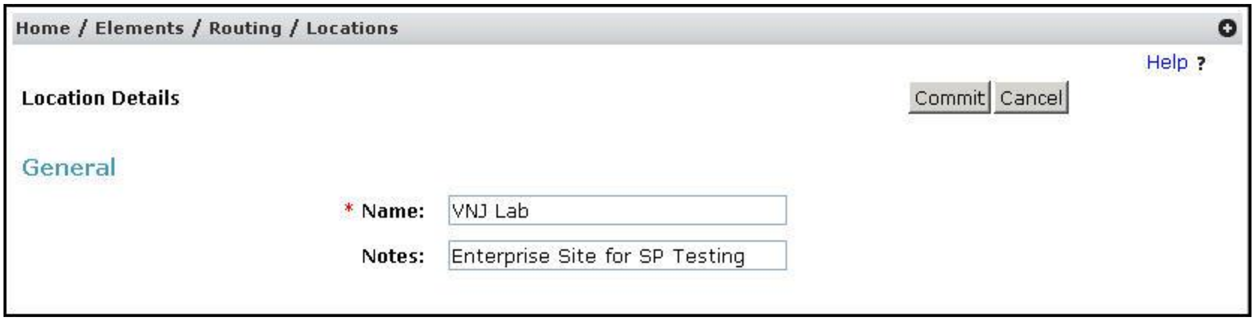
6.3. Add Location

Locations can be used to identify logical and/or physical locations where SIP Entities reside for purposes of bandwidth management and call admission control. A single location was defined for the enterprise even though multiple subnets were used. The screens below show the addition of the location named **VNJ Lab**, which includes all equipment on the enterprise including Communication Manager, Session Manager and the Avaya SBCE.

To add a location, navigate to **Routing → Locations** in the left-hand navigation pane (**Section 6.1**) and click the **New** button in the right pane (not shown). In the new right pane that appears (shown below), fill in the following:

In the **General** section, enter the following values. Use default values for all remaining fields.

- **Name:** Enter a descriptive name for the location.
- **Notes:** Add a brief description (optional).



Location Details

General

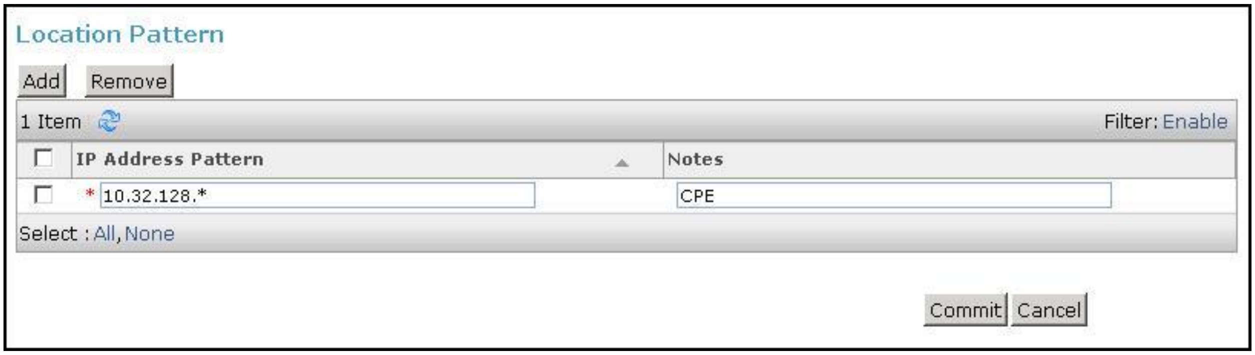
* Name: VNJ Lab

Notes: Enterprise Site for SP Testing

Scroll down to the **Location Pattern** section. Click **Add** and enter the following values. Use default values for all remaining fields.

- **IP Address Pattern:** Add all IP address patterns used to identify the location.
- **Notes:** Add a brief description (optional).

Click **Commit** to save.



Location Pattern

1 Item

□	IP Address Pattern	Notes
□	* 10.32.128.*	CPE

6.4. Add Adaptation Module

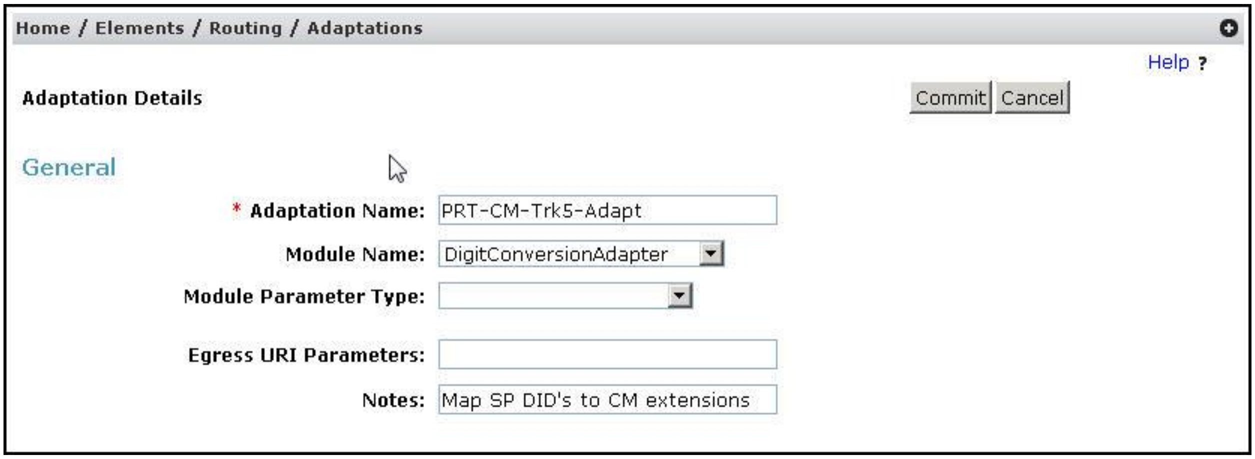
Session Manager can be configured with adaptation modules that can modify SIP messages before or after routing decisions have been made. A generic adaptation module **DigitConversionAdapter** supports digit conversion of telephone numbers in specific headers of SIP messages. Other adaptation modules are built on this generic, and can modify other headers to permit interoperability with third party SIP products.

For the compliance test, one adaptation was created for Communication Manager. The adaptation mapped inbound DID numbers from Cox Communications to local Communication Manager extensions.

To create the adaptation that will be applied to the Communication Manager SIP entity, navigate to **Routing → Adaptations** in the left-hand navigation pane (**Section 6.1**) and click on the **New** button in the right pane (not shown). In the new right pane that appears (shown below), fill in the following:

In the **General** section, enter the following values. Use default values for all remaining fields.

- **Adaptation name:** Enter a descriptive name for the adaptation.
- **Module name:** Enter **DigitConversionAdapter**.
- **Notes:** Enter a description (optional).



Adaptation Details

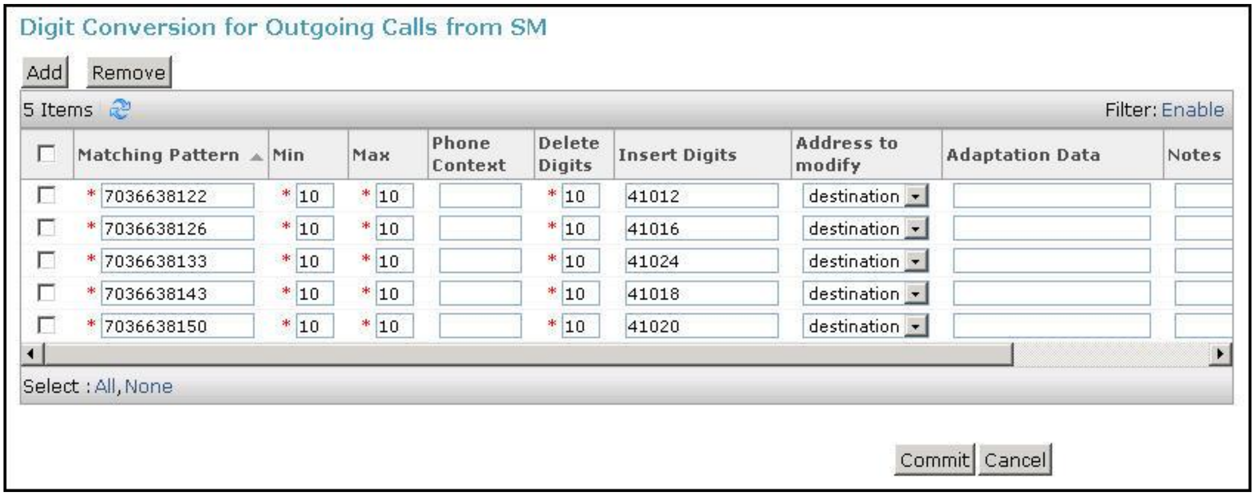
General

* Adaptation Name: PRT-CM-Trk5-Adapt
Module Name: DigitConversionAdapter
Module Parameter Type:
Egress URI Parameters:
Notes: Map SP DID's to CM extensions

To map inbound DID numbers from Cox Communications to Communication Manager extensions, scroll down to the **Digit Conversion for Outgoing Calls from SM** section. Create an entry for each DID to be mapped. Click **Add** and enter the following values for each mapping. Use default values for all remaining fields.

- **Matching Pattern:** Enter a digit string used to match the inbound DID number.
- **Min:** Enter a minimum dialed number length used in the match criteria.
- **Max:** Enter a maximum dialed number length used in the match criteria.
- **Delete Digits** Enter the number of digits to delete from the beginning of the received number.
- **Insert Digits:** Enter the number of digits to insert at the beginning of the received number.
- **Address to modify:** Select **destination** since this digit conversion only applies to the destination number.

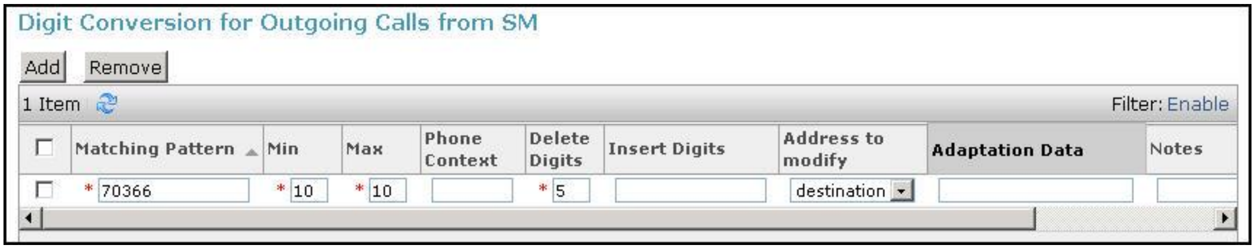
Click **Commit** to save.



Digit Conversion for Outgoing Calls from SM

□	Matching Pattern	Min	Max	Phone Context	Delete Digits	Insert Digits	Address to modify	Adaptation Data	Notes
□	* 7036638122	* 10	* 10		* 10	41012	destination		
□	* 7036638126	* 10	* 10		* 10	41016	destination		
□	* 7036638133	* 10	* 10		* 10	41024	destination		
□	* 7036638143	* 10	* 10		* 10	41018	destination		
□	* 7036638150	* 10	* 10		* 10	41020	destination		

In a real customer environment, often the DID number is comprised of the local extension plus a prefix. If this is true, then a single digit conversion entry can be created for all extensions. In the example below, a 5 digit prefix is deleted from each incoming DID number leaving a 5 digit extension to be routed by Session Manager.



Digit Conversion for Outgoing Calls from SM

□	Matching Pattern	Min	Max	Phone Context	Delete Digits	Insert Digits	Address to modify	Adaptation Data	Notes
□	* 70366	* 10	* 10		* 5		destination		

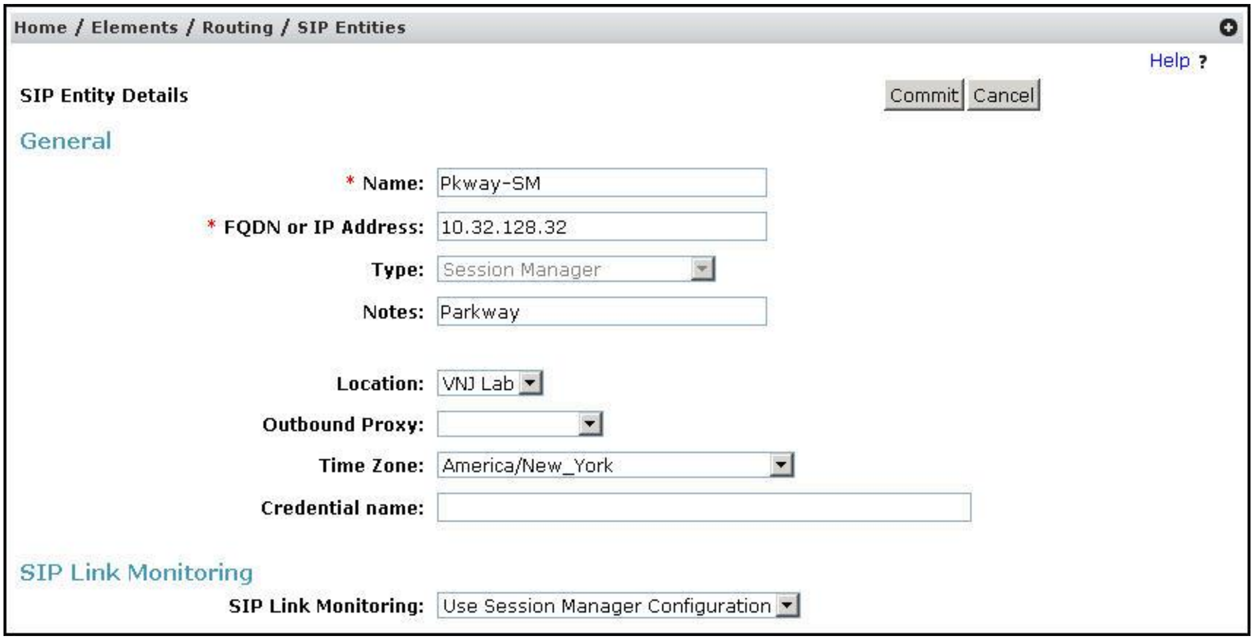
6.5. Add SIP Entities

A SIP Entity must be added for Session Manager and for each SIP telephony system connected to Session Manager which includes Communication Manager and the Avaya SBCE. Navigate to **Routing → SIP Entities** in the left-hand navigation pane (**Section 6.1**) and click on the **New** button in the right pane (not shown). In the new right pane that appears (shown below), fill in the following:

In the **General** section, enter the following values. Use default values for all remaining fields.

- **Name:** Enter a descriptive name.
- **FQDN or IP Address:** Enter the FQDN or IP address of the SIP Entity that is used for SIP signaling.
- **Type:** Enter **Session Manager** for Session Manager, **CM** for Communication Manager and **SIP Trunk** for the Avaya SBCE.
- **Adaptation:** This field is only present if **Type** is not set to **Session Manager**. If applicable, select the appropriate **Adaptation name** created in **Section 6.4** that will be applied to this entity.
- **Location:** Select the location that applies to the SIP entity being created. For the compliance test, all components were located in location **VNJ Lab**.
- **Time Zone:** Select the time zone for the location above.

The following screen shows the addition of Session Manager. The IP address of the Session Manager signaling interface is entered for **FQDN or IP Address**.



SIP Entity Details

General

* Name: Pkway-SM

* FQDN or IP Address: 10.32.128.32

Type: Session Manager

Notes: Parkway

Location: VNJ Lab

Outbound Proxy:

Time Zone: America/New_York

Credential name:

SIP Link Monitoring

SIP Link Monitoring: Use Session Manager Configuration

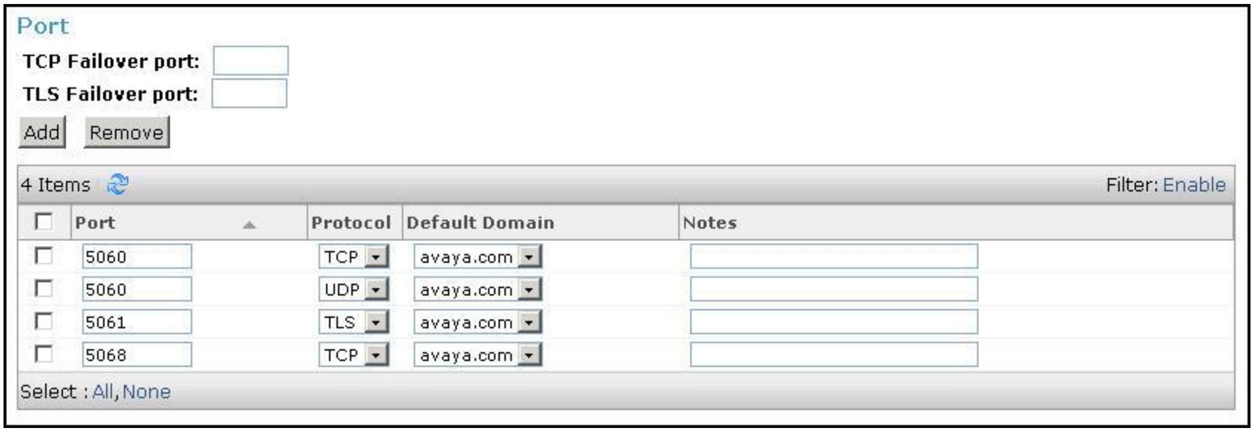
To define the ports used by Session Manager, scroll down to the **Port** section of the **SIP Entity Details** screen. This section is only present for **Session Manager** SIP entities.

In the **Port** section, click **Add** and enter the following values. Use default values for all remaining fields:

- **Port:** Port number on which the Session Manager can listen for SIP requests.
- **Protocol:** Transport protocol to be used with this port.
- **Default Domain:** The default domain associated with this port. For the compliance test, this was the enterprise SIP domain.

Defaults can be used for the remaining fields. Click **Commit** to save.

For the compliance test, four port entries were used. The first three are the standard ports used for SIP traffic: port 5060 for UDP/TCP and port 5061 for TLS. In addition, port 5068 defined in **Section 5.6** for use with service provider SIP traffic between Communication Manager and Session Manager was added to the list.



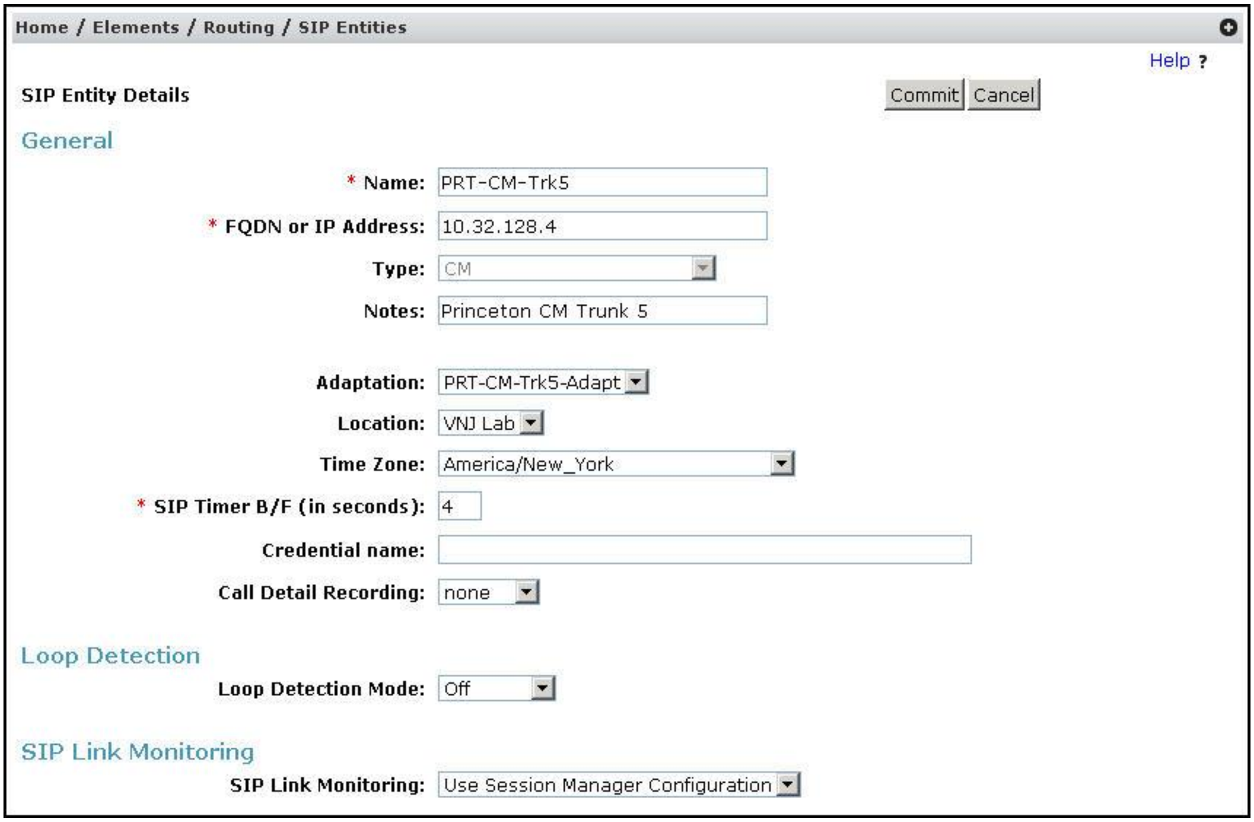
Port

TCP Failover port:

TLS Failover port:

□	Port	Protocol	Default Domain	Notes
□	5060	TCP	avaya.com	
□	5060	UDP	avaya.com	
□	5061	TLS	avaya.com	
□	5068	TCP	avaya.com	

The following screen shows the addition of Communication Manager SIP entity. In order for Session Manager to send SIP service provider traffic on a separate entity link to Communication Manager, this requires the creation of a separate SIP entity for Communication Manager other than the one created at Session Manager installation for use with all other SIP traffic. The **FQDN or IP Address** field is set to the IP address of Communication Manager. For the **Adaptation** field, select the adaptation module previously defined for dial digit manipulation in **Section 6.4**. The **Location** field is set to **VNJ Lab** which is the location defined for the subnet where Communication Manager resides.



SIP Entity Details

General

* Name: PRT-CM-Trk5

* FQDN or IP Address: 10.32.128.4

Type: CM

Notes: Princeton CM Trunk 5

Adaptation: PRT-CM-Trk5-Adapt

Location: VNJ Lab

Time Zone: America/New_York

* SIP Timer B/F (in seconds): 4

Credential name:

Call Detail Recording: none

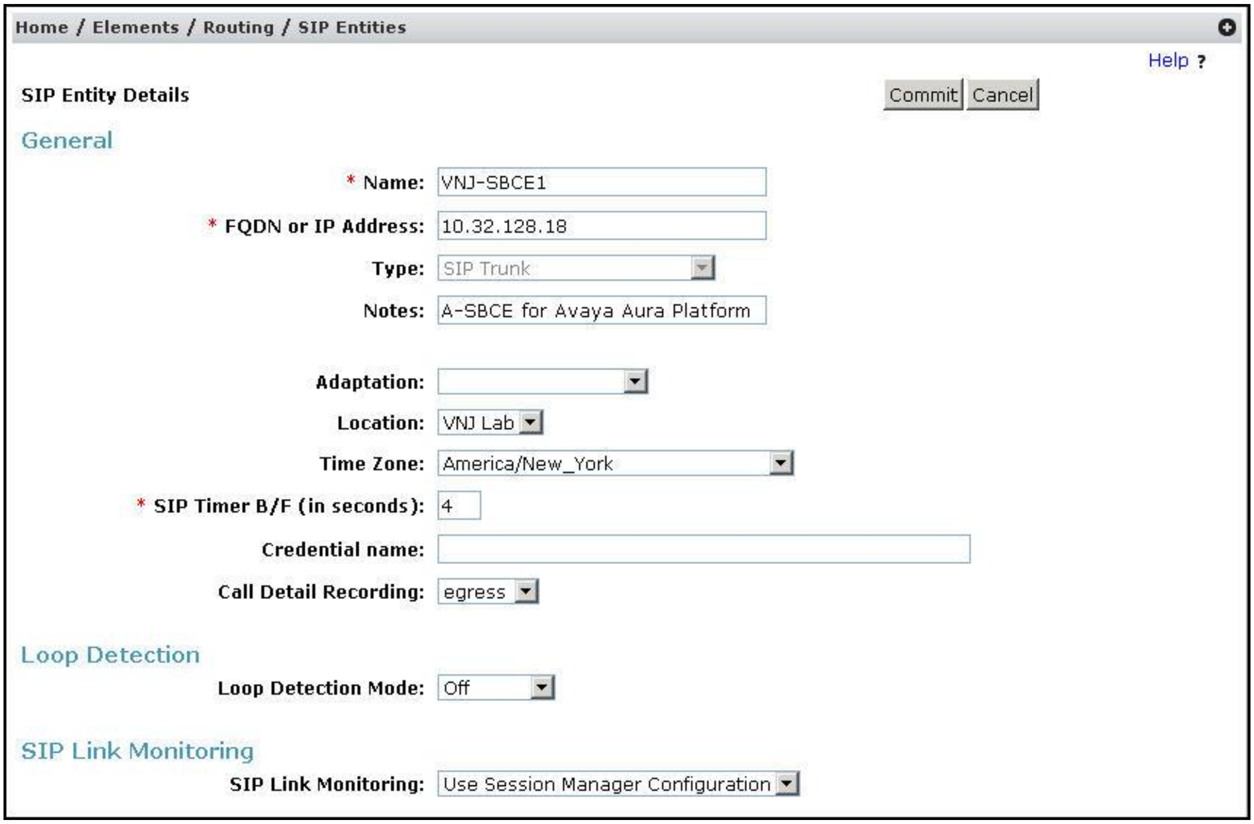
Loop Detection

Loop Detection Mode: Off

SIP Link Monitoring

SIP Link Monitoring: Use Session Manager Configuration

The following screen shows the addition of the Avaya SBCE SIP entity. The **FQDN or IP Address** field is set to the IP address of its private network interface (see **Figure 1**). The **Location** field is set to **VNJ Lab** which is the location defined for the subnet where the Avaya SBCE resides.



SIP Entity Details

General

* Name:	VNJ-SBCE1
* FQDN or IP Address:	10.32.128.18
Type:	SIP Trunk
Notes:	A-SBCE for Avaya Aura Platform
Adaptation:	
Location:	VNJ Lab
Time Zone:	America/New_York
* SIP Timer B/F (in seconds):	4
Credential name:	
Call Detail Recording:	egress

Loop Detection

Loop Detection Mode:	Off

SIP Link Monitoring

SIP Link Monitoring:	Use Session Manager Configuration

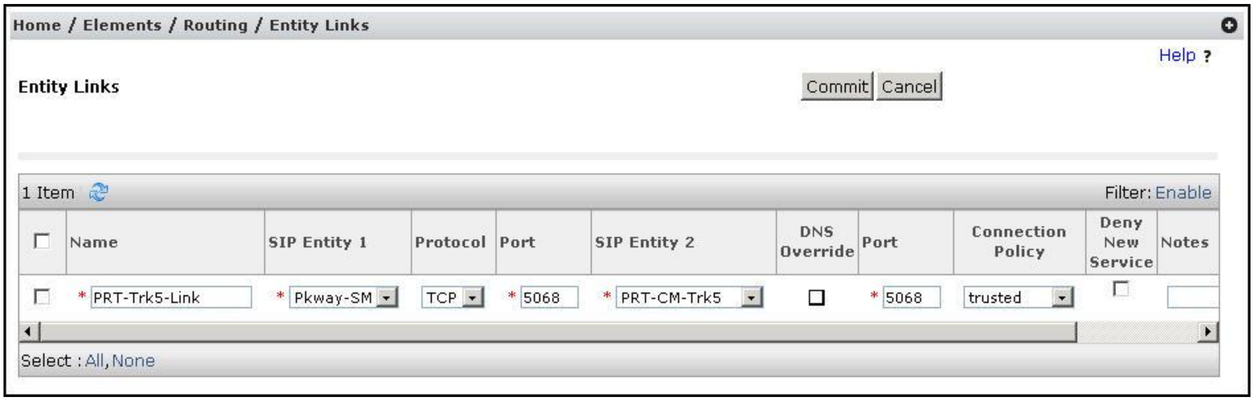
6.6. Add Entity Links

A SIP trunk between Session Manager and a telephony system is described by an Entity Link. Two entity links were created: one to Communication Manager for use only by service provider traffic and one to the Avaya SBCE. To add an entity link, navigate to **Routing → Entity Links** in the left-hand navigation pane (**Section 6.1**) and click on the **New** button in the right pane (not shown). In the new right pane that appears (shown below), fill in the following:

- **Name:** Enter a descriptive name.
- **SIP Entity 1:** Select the Session Manager.
- **Protocol:** Select the transport protocol used for this link. This must match the protocol used in the Communication Manager signaling group in **Section 5.6**.
- **Port:** Port number on which Session Manager will receive SIP requests from the far-end. For the Communication Manager entity link, this must match the **Far-end Listen Port** defined on the Communication Manager signaling group in **Section 5.6**.
- **SIP Entity 2:** Select the name of the other system. For the Communication Manager entity link, select the Communication Manager SIP entity defined in **Section 6.5**.
- **Port:** Port number on which the other system receives SIP requests from the Session Manager. For the Communication Manager Entity Link, this must match the **Near-end Listen Port** defined on the Communication Manager signaling group in **Section 5.6**.
- **Connection Policy:** Select **Trusted** from pull-down menu.

Click **Commit** to save.

The following screen illustrates the Entity Link to Communication Manager. The protocol and ports defined here must match the values used on the Communication Manager signaling group form in **Section 5.6**. For the compliance test, the TCP protocol was used (for ease in troubleshooting traces) but the recommended configuration is to use TLS.



Home / Elements / Routing / Entity Links

Help ?

Entity Links

Commit Cancel

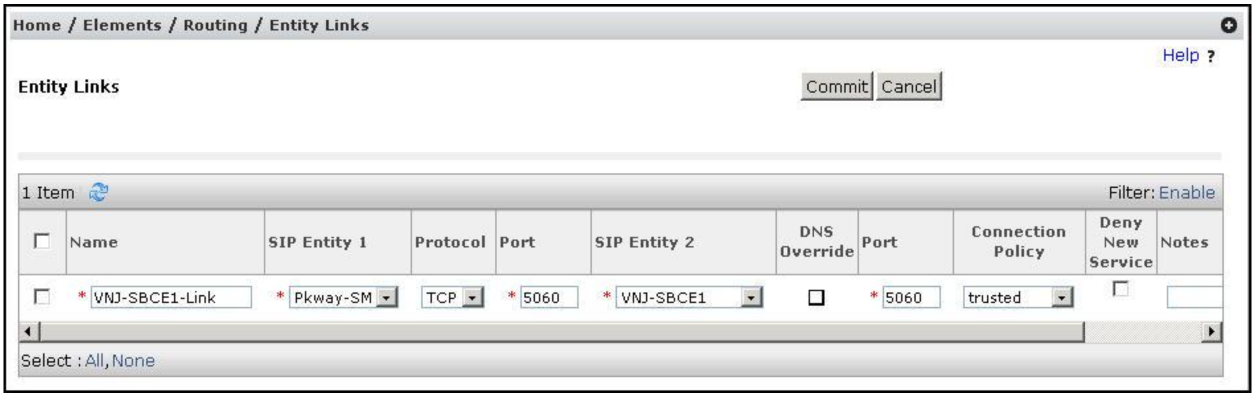
1 Item

Filter: Enable

□	Name	SIP Entity 1	Protocol	Port	SIP Entity 2	DNS Override	Port	Connection Policy	Deny New Service	Notes
□	* PRT-Trk5-Link	* Pkway-SM	TCP	* 5068	* PRT-CM-Trk5	□	* 5068	trusted	□	

Select : All, None

The following screen illustrates the Entity Link to the Avaya SBCE.



Entity Links

□	Name	SIP Entity 1	Protocol	Port	SIP Entity 2	DNS Override	Port	Connection Policy	Deny New Service	Notes
□	* VNJ-SBCE1-Link	* Pkway-SM	TCP	* 5060	* VNJ-SBCE1	□	* 5060	trusted	□	

6.7. Add Routing Policies

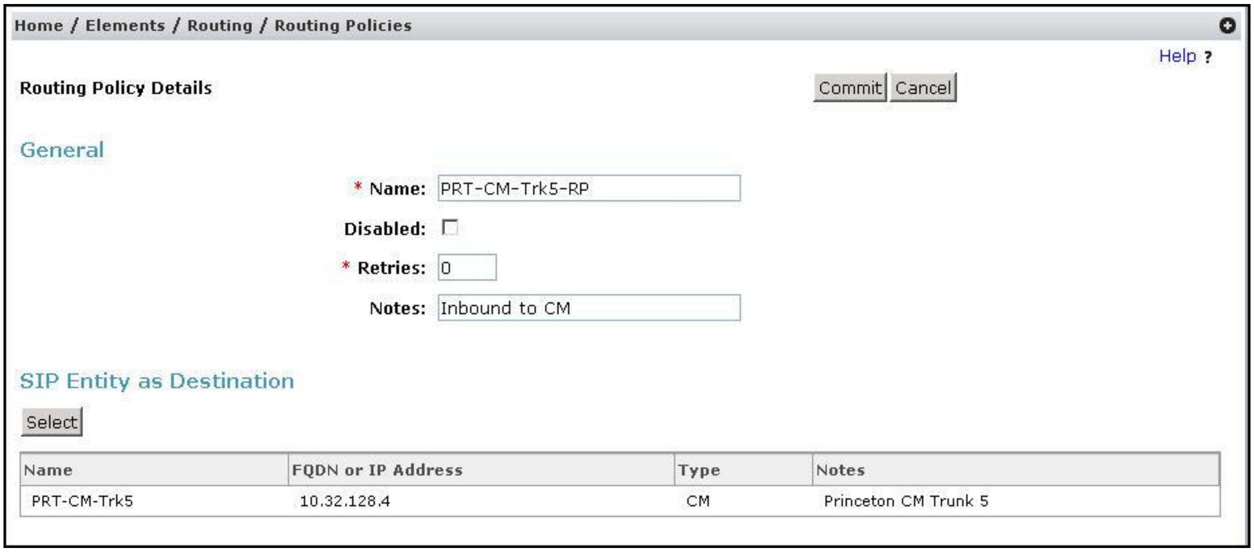
Routing Policies describe the conditions under which calls will be routed to the SIP entities specified in **Section 6.5**. Two routing policies must be added: one for Communication Manager and one for the Avaya SBCE. To add a routing policy, navigate to **Routing → Routing Policies** in the left-hand navigation pane (**Section 6.1**) and click on the **New** button in the right pane (not shown). In the new right pane that appears (shown below), fill in the following:

In the **General** section, enter the following values. Use default values for all remaining fields.

- **Name:** Enter a descriptive name.
- **Notes:** Add a brief description (optional).

In the **SIP Entity as Destination** section, click **Select.** The **SIP Entity List** page opens (not shown). Select the appropriate SIP entity to which this routing policy applies and click **Select.** The selected SIP entity displays on the Routing Policy Details page as shown below. Use default values for remaining fields. Click **Commit** to save.

The following screen shows the routing policy for Communication Manager.



Routing Policy Details

General

* Name: PRT-CM-Trk5-RP

Disabled: □

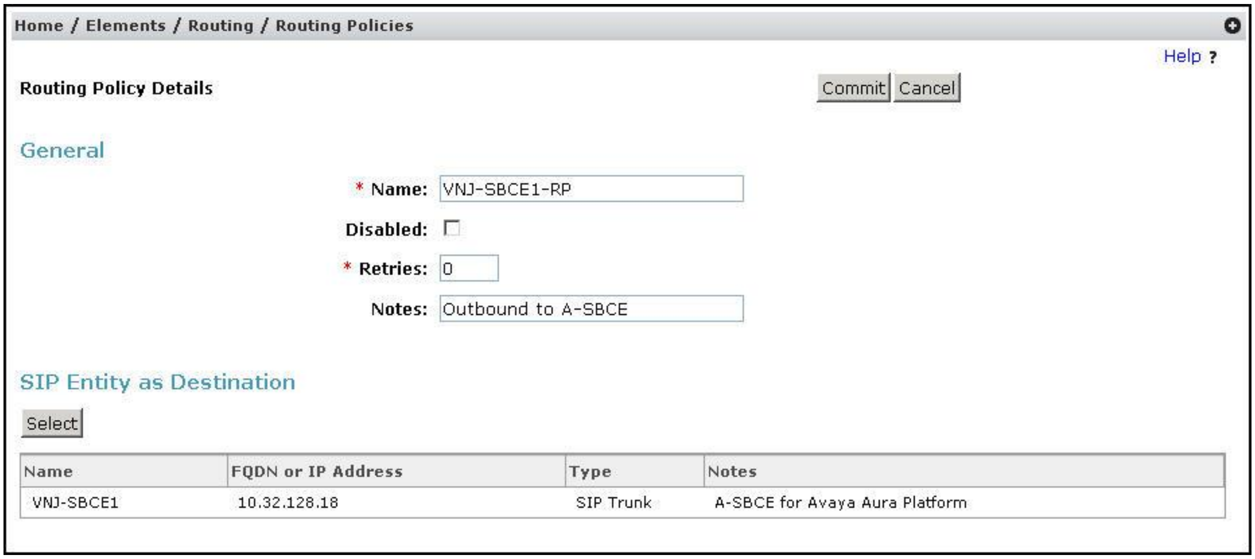
* Retries: 0

Notes: Inbound to CM

SIP Entity as Destination

Name	FQDN or IP Address	Type	Notes
PRT-CM-Trk5	10.32.128.4	CM	Princeton CM Trunk 5

The following screen shows the routing policy for the Avaya SBCE.



Routing Policy Details

General

* Name: VNJ-SBCE1-RP

Disabled: □

* Retries: 0

Notes: Outbound to A-SBCE

SIP Entity as Destination

Name	FQDN or IP Address	Type	Notes
VNJ-SBCE1	10.32.128.18	SIP Trunk	A-SBCE for Avaya Aura Platform

6.8. Add Dial Patterns

Dial Patterns are needed to route calls through Session Manager. For the compliance test, dial patterns were needed to route calls from Communication Manager to Cox Communications and vice versa. Dial patterns define which route policy will be selected for a particular call based on the dialed digits, destination domain and originating location. To add a dial pattern, navigate to **Routing → Dial Patterns** in the left-hand navigation pane (**Section 6.1**) and click on the **New** button in the right pane (not shown). In the new right pane that appears (shown below), fill in the following:

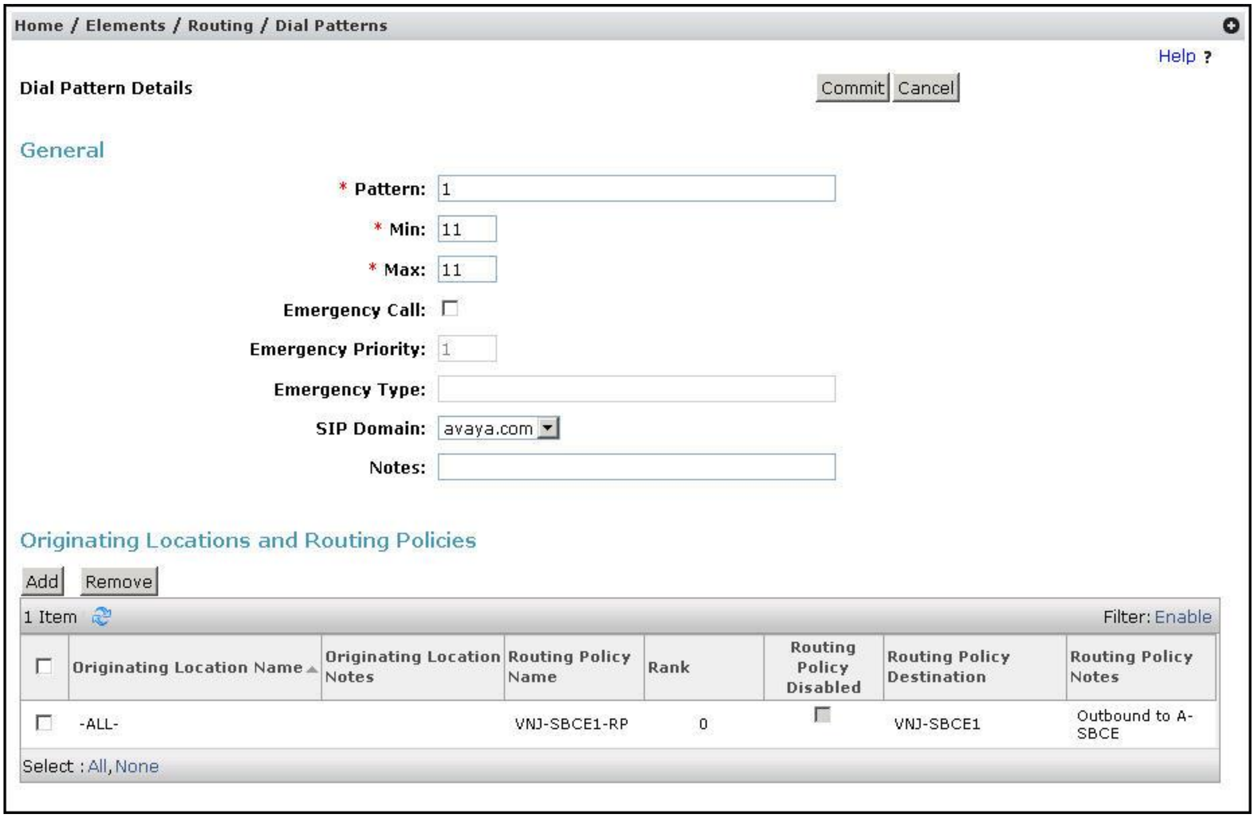
In the **General** section, enter the following values. Use default values for all remaining fields.

- **Pattern:** Enter a dial string that will be matched against the Request-URI of the call.
- **Min:** Enter a minimum length used in the match criteria.
- **Max:** Enter a maximum length used in the match criteria.
- **SIP Domain:** Enter the destination domain used in the match criteria.
- **Notes:** Add a brief description (optional).

In the **Originating Locations and Routing Policies** section, click **Add**. From the **Originating Locations and Routing Policy List** that appears (not shown), select the appropriate originating location for use in the match criteria. Lastly, select the routing policy from the list that will be used to route all calls that match the specified criteria. Click **Select**.

Default values can be used for the remaining fields. Click **Commit** to save.

Two examples of the dial patterns used for the compliance test are shown below. The first example is for outbound calls and shows that numbers that begin with 1 and have a destination domain of **avaya.com** from **ALL** locations use route policy **VNJ-SBCE1-RP**.



Dial Pattern Details

General

* Pattern:	1
* Min:	11
* Max:	11
Emergency Call:	□
Emergency Priority:	1
Emergency Type:	
SIP Domain:	avaya.com
Notes:	

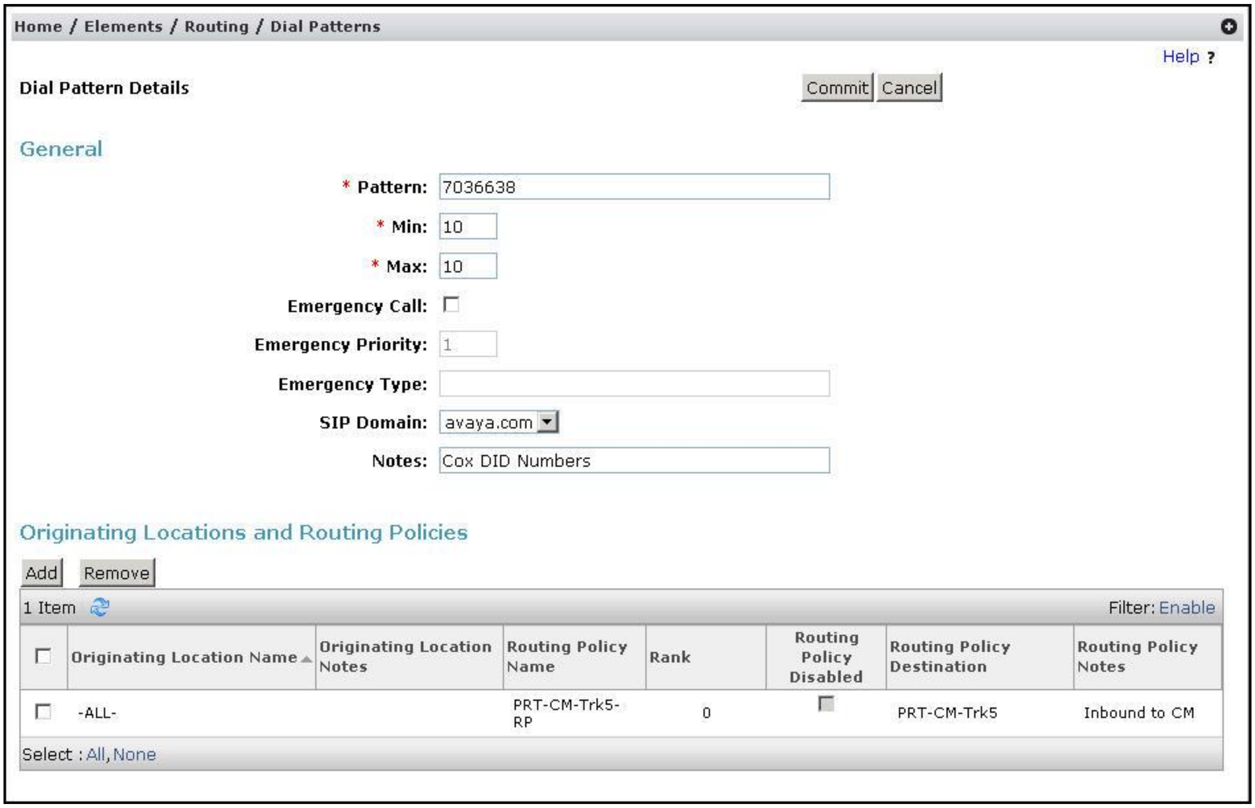
Originating Locations and Routing Policies

1 Item Filter: Enable

□	Originating Location Name	Originating Location Notes	Routing Policy Name	Rank	Routing Policy Disabled	Routing Policy Destination	Routing Policy Notes
□	-ALL-		VNJ-SBCE1-RP	0	□	VNJ-SBCE1	Outbound to A-SBCE

Select : All, None

The second example is for inbound calls and shows that 10 digit numbers that start with **7036638** to domain **avaya.com** and originating from **ALL** locations use route policy **PRT-CM-Trk5-RP**. These are the DID numbers assigned to the enterprise from Cox Communications. All other dial patterns used as part of the compliance test were configured in a similar manner.



Dial Pattern Details

General

* Pattern:	7036638
* Min:	10
* Max:	10
Emergency Call:	□
Emergency Priority:	1
Emergency Type:	
SIP Domain:	avaya.com
Notes:	Cox DID Numbers

Originating Locations and Routing Policies

□	Originating Location Name	Originating Location Notes	Routing Policy Name	Rank	Routing Policy Disabled	Routing Policy Destination	Routing Policy Notes
□	-ALL-		PRT-CM-Trk5-RP	0	□	PRT-CM-Trk5	Inbound to CM

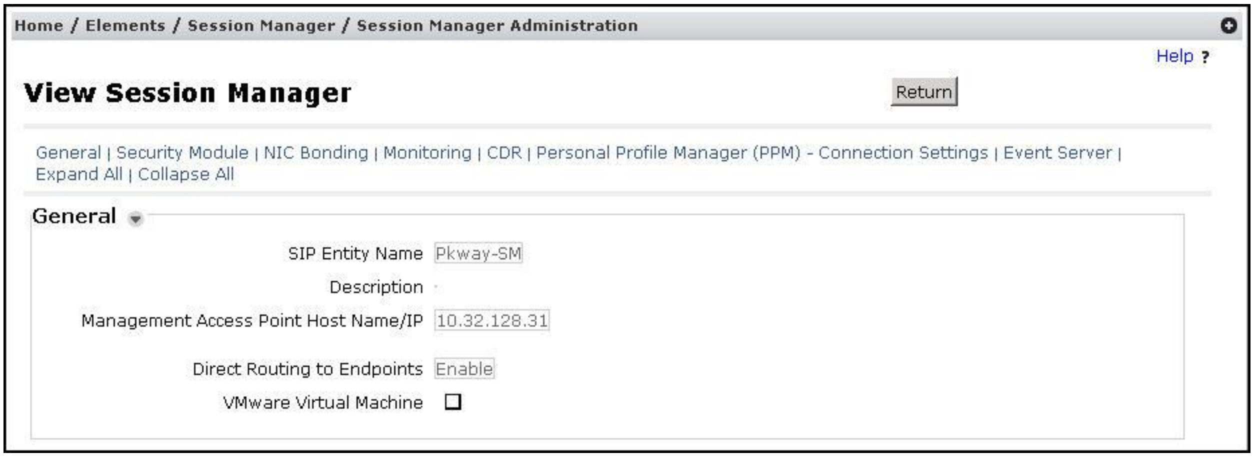
6.9. Add/View Avaya Aura® Session Manager

The creation of a Session Manager element provides the linkage between System Manager and Session Manager. This was most likely done as part of the initial Session Manager installation. To add a Session Manager, from the **Home** page, navigate to **Elements → Session Manager → Session Manager Administration** in the left-hand navigation pane (**Section 6.1**) and click on the **New** button in the right pane (not shown). If the Session Manager already exists, select the appropriate Session Manager and click **View** (not shown) to view the configuration. Enter/verify the data as described below and shown in the following screen:

In the **General** section, enter/verify the following values:

- **SIP Entity Name:** Select the SIP Entity created for Session Manager.
- **Description**: Add a brief description (optional).
- **Management Access Point Host Name/IP:** Enter the host name or IP address of the Session Manager management interface.

The screen below shows the Session Manager values used for the compliance test.

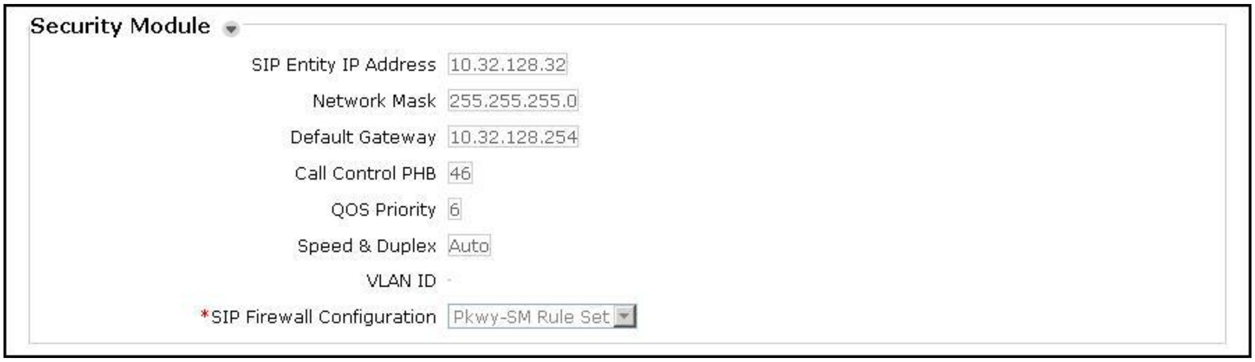

Home / Elements / Session Manager / Session Manager Administration
Help ?
View Session Manager
Return
General | Security Module | NIC Bonding | Monitoring | CDR | Personal Profile Manager (PPM) - Connection Settings | Event Server | Expand All | Collapse All
General

SIP Entity Name: Pkway-SM
Description:
Management Access Point Host Name/IP: 10.32.128.31
Direct Routing to Endpoints: Enable
VMware Virtual Machine: □

In the **Security Module** section, enter/verify the following values:

- **SIP Entity IP Address:** Should be filled in automatically based on the SIP Entity Name. Otherwise, enter IP address of the Session Manager signaling interface.
- **Network Mask:** Enter the network mask corresponding to the IP address of Session Manager.
- **Default Gateway**: Enter the IP address of the default gateway for Session Manager.

Use default values for the remaining fields. Click **Save** (not shown) to add this Session Manager. The screen below shows the remaining Session Manager values used for the compliance test.



Security Module

SIP Entity IP Address	10.32.128.32
Network Mask	255.255.255.0
Default Gateway	10.32.128.254
Call Control PHB	46
QOS Priority	6
Speed & Duplex	Auto
VLAN ID	
*SIP Firewall Configuration	Pkwy-SM Rule Set

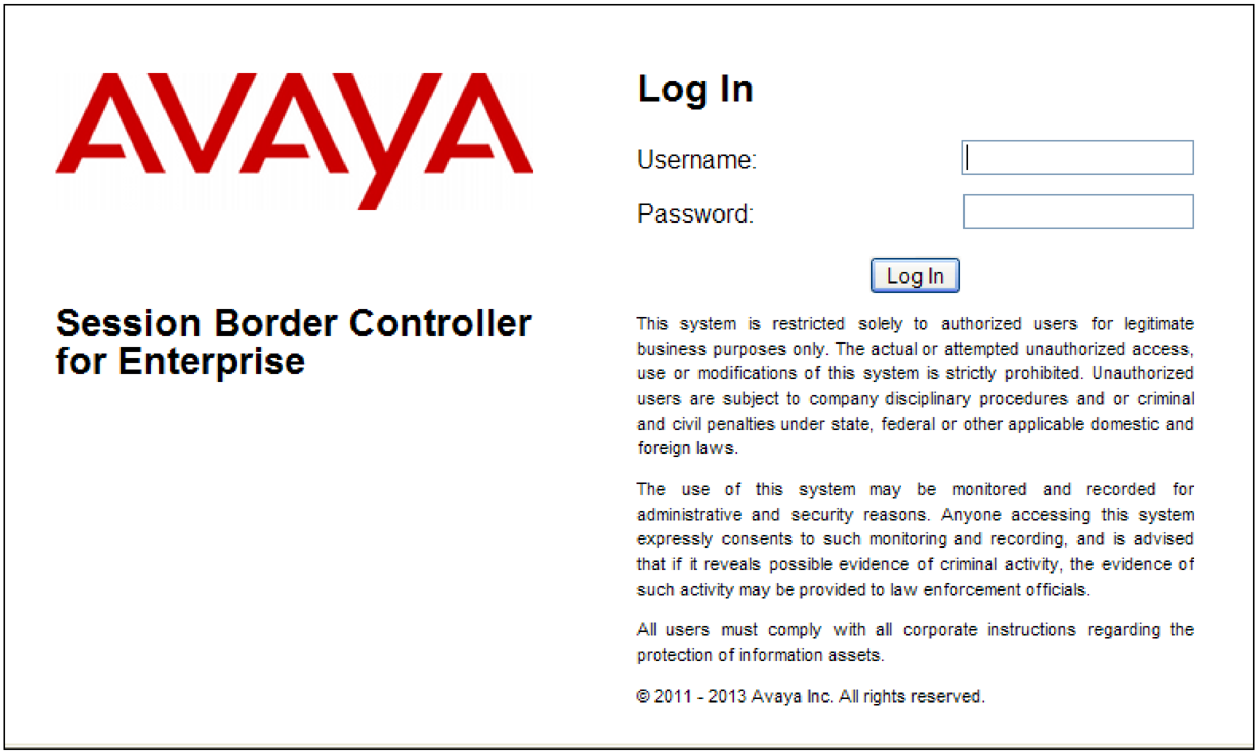
7. Configure Avaya Session Border Controller for Enterprise

This section describes the configuration of the Avaya SBCE. It is assumed that the initial installation of the Avaya SBCE has been completed including the assignment of a management IP address. The management interface **must** be provisioned on a different subnet than either the Avaya SBCE private or public network interfaces (e.g., A1 and B1). If the management interface has not been configured on a separate subnet, then contact your Avaya representative for guidance in correcting the configuration.

On all screens described in this section, it is to be assumed that parameters are left at their default values unless specified otherwise.

7.1. Access the Management Interface

Use a web browser to access the web interface by entering the URL **https://<ip-addr>**, where **<ip-addr>** is the management IP address assigned during installation. The Avaya SBCE login page will appear as shown below. Log in with appropriate credentials.



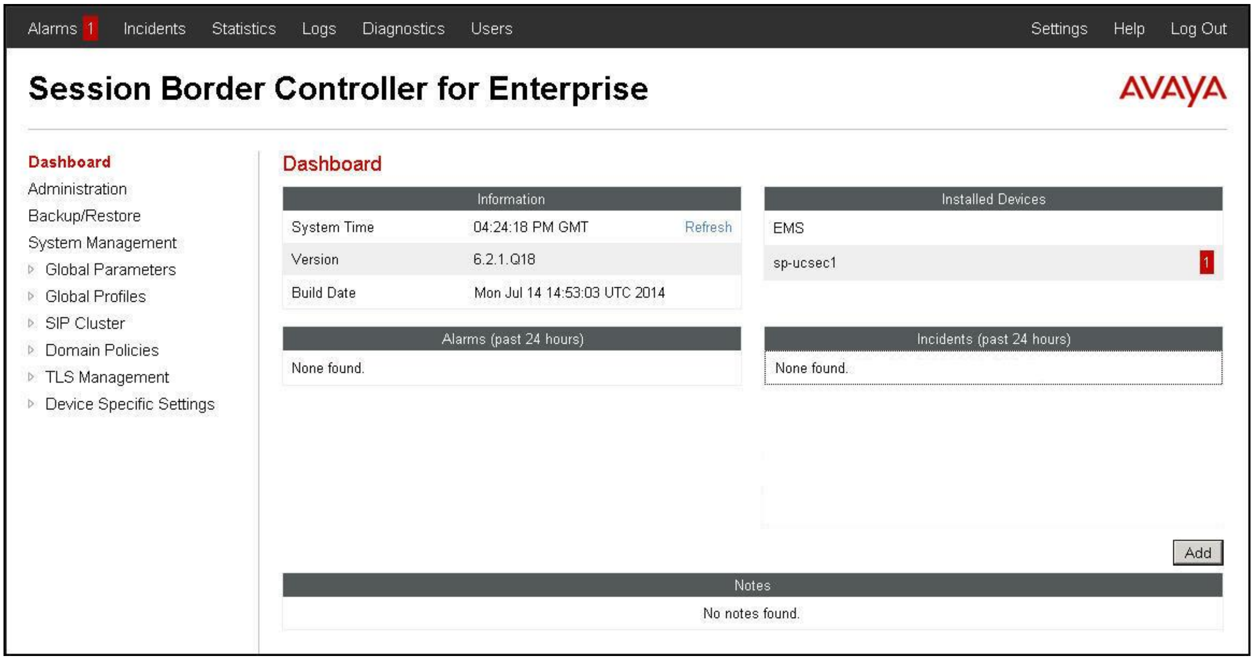
This system is restricted solely to authorized users for legitimate business purposes only. The actual or attempted unauthorized access, use or modifications of this system is strictly prohibited. Unauthorized users are subject to company disciplinary procedures and or criminal and civil penalties under state, federal or other applicable domestic and foreign laws.

The use of this system may be monitored and recorded for administrative and security reasons. Anyone accessing this system expressly consents to such monitoring and recording, and is advised that if it reveals possible evidence of criminal activity, the evidence of such activity may be provided to law enforcement officials.

All users must comply with all corporate instructions regarding the protection of information assets.

© 2011 - 2013 Avaya Inc. All rights reserved.

After logging in, the Dashboard screen will appear as shown below. All configuration screens of the Avaya SBCE are accessed by navigating the menu tree in the left pane.



Information		
System Time	04:24:18 PM GMT	Refresh
Version	6.2.1.Q18	
Build Date	Mon Jul 14 14:53:03 UTC 2014	

Installed Devices
EMS
sp-ucsec1 1

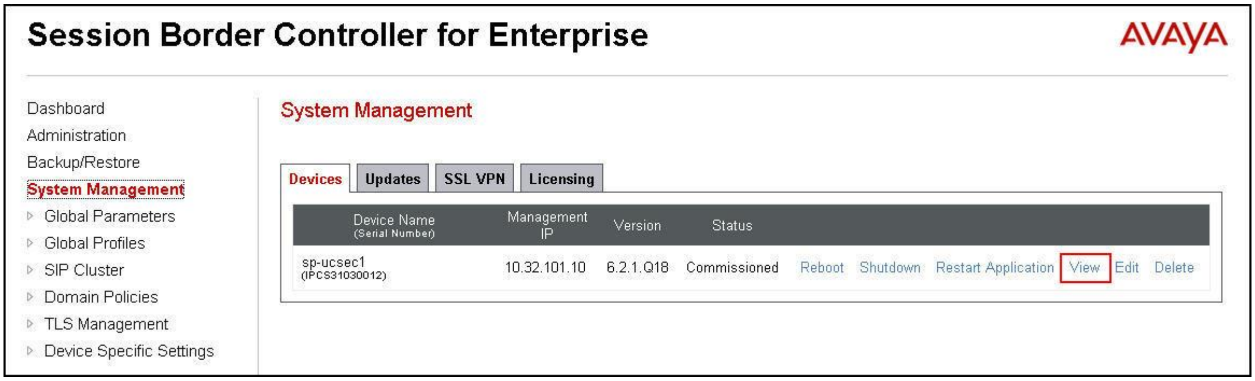
Alarms (past 24 hours)
None found.

Incidents (past 24 hours)
None found.

Notes
No notes found.

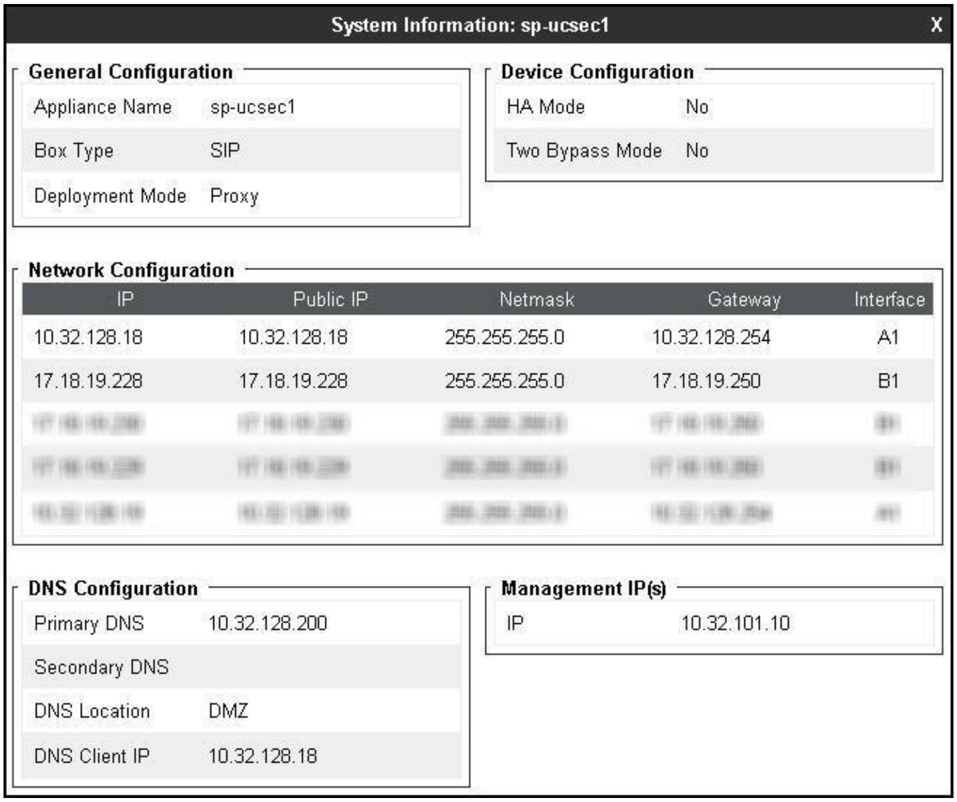
7.2. Verify Network Configuration and Enable Interfaces

To view the network information provided during installation, navigate to **System Management**. In the right pane, click **View** highlighted below.



Device Name (Serial Number)	Management IP	Version	Status						
sp-ucsec1 (IPCS31030012)	10.32.101.10	6.2.1.Q18	Commissioned	Reboot	Shutdown	Restart Application	View	Edit	Delete

A System Information page will appear showing the information provided during installation. In the **Appliance Name** field is the name of the device (**sp-ucsec1**). This name will be referenced in other configuration screens. The two **Network Configuration** entries highlighted below are the only two IP addresses that are directly related to the SIP trunking solution described in these Application Notes. Interfaces **A1** and **B1** represent the private and public interfaces of the Avaya SBCE. Each of these interfaces must be enabled after installation.



System Information: sp-ucsec1

General Configuration

Appliance Name	sp-ucsec1
Box Type	SIP
Deployment Mode	Proxy

Device Configuration

HA Mode	No
Two Bypass Mode	No

Network Configuration

IP	Public IP	Netmask	Gateway	Interface
10.32.128.18	10.32.128.18	255.255.255.0	10.32.128.254	A1
17.18.19.228	17.18.19.228	255.255.255.0	17.18.19.250	B1
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]

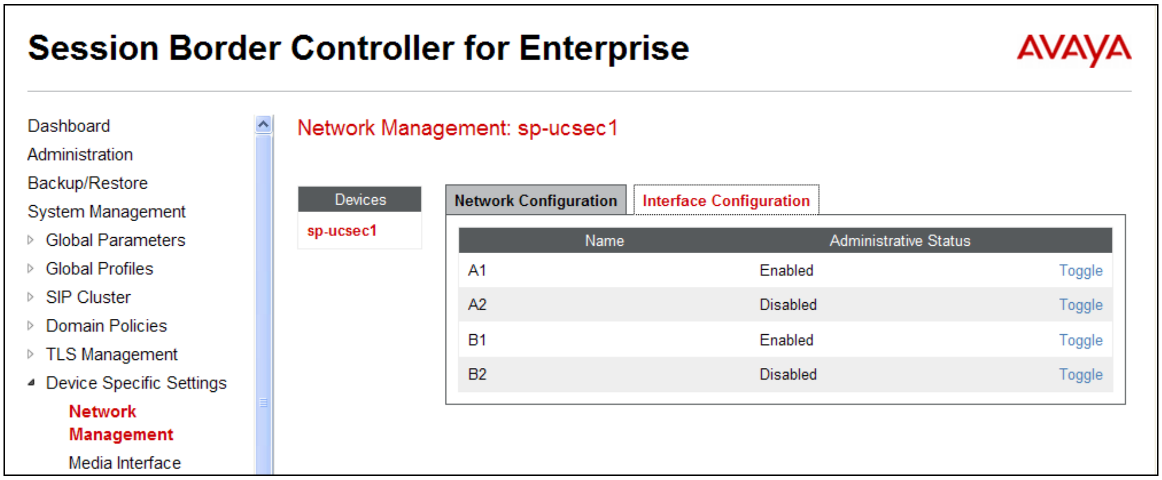
DNS Configuration

Primary DNS	10.32.128.200
Secondary DNS	
DNS Location	DMZ
DNS Client IP	10.32.128.18

Management IP(s)

IP	10.32.101.10

To enable the interfaces, first navigate to **Device Specific Settings → Network Management** in the left pane and select the device being managed in the center pane. In the right pane, click on the **Interface Configuration** tab. Verify the **Administrative Status** is **Enabled** for both the **A1** and **B1** interfaces. If not, click **Toggle** to enable the interface.



Network Management: sp-ucsec1

Name	Administrative Status	
A1	Enabled	Toggle
A2	Disabled	Toggle
B1	Enabled	Toggle
B2	Disabled	Toggle

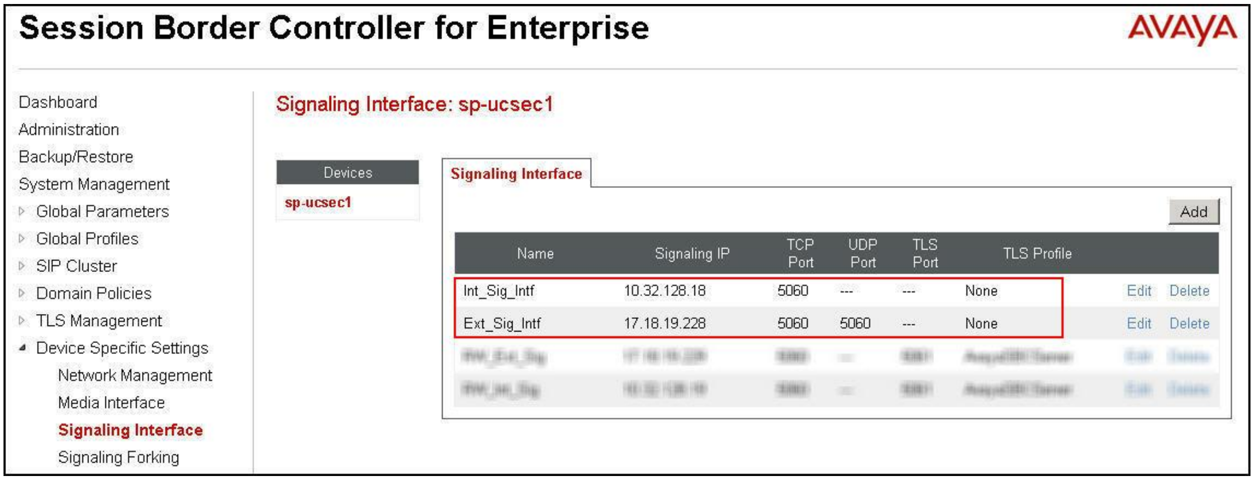
7.3. Signaling Interface

A signaling interface defines an IP address, protocols and listen ports that the Avaya SBCE can use for signaling. Create a signaling interface for both the internal and external sides of the Avaya SBCE.

To create a new interface, navigate to **Device Specific Settings → Signaling Interface** in the left pane. In the center pane, select the Avaya SBCE device (**sp-ucsec1**) to be managed. In the right pane, select **Add**. A pop-up window (not shown) will appear requesting the name of the new interface, followed by a series of pop-up windows in which the interface parameters can be configured. Once complete, the settings are shown in the far right pane.

For the compliance test, signaling interface **Int_Sig_Intf** was created for the Avaya SBCE internal interface and signaling interface **Ext_Sig_Intf** was created for the Avaya SBCE external interface. Each is highlighted below. When configuring the interfaces, configure the parameters as follows:

- Set **Name** to a descriptive name.
- For the internal interface, set the **Signaling IP** to the IP address associated with the private interface (A1) defined in **Section 7.2**. For the external interface, set the **Signaling IP** to the IP address associated with the public interface (B1) defined in **Section 7.2**.
- In the **UDP Port**, **TCP Port** and **TLS Port** fields, enter the port the Avaya SBCE will listen on for each transport protocol. For the internal interface, the Avaya SBCE was configured to listen for TCP on port 5060. For the external interface, the Avaya SBCE was configured to listen for UDP or TCP on port 5060. Since Cox Communications uses UDP on port 5060, it would have been sufficient to simply configure the Avaya SBCE for UDP.



Signaling Interface: sp-ucsec1

Name	Signaling IP	TCP Port	UDP Port	TLS Port	TLS Profile		
Int_Sig_Intf	10.32.128.18	5060	---	---	None	Edit	Delete
Ext_Sig_Intf	17.18.19.228	5060	5060	---	None	Edit	Delete
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]

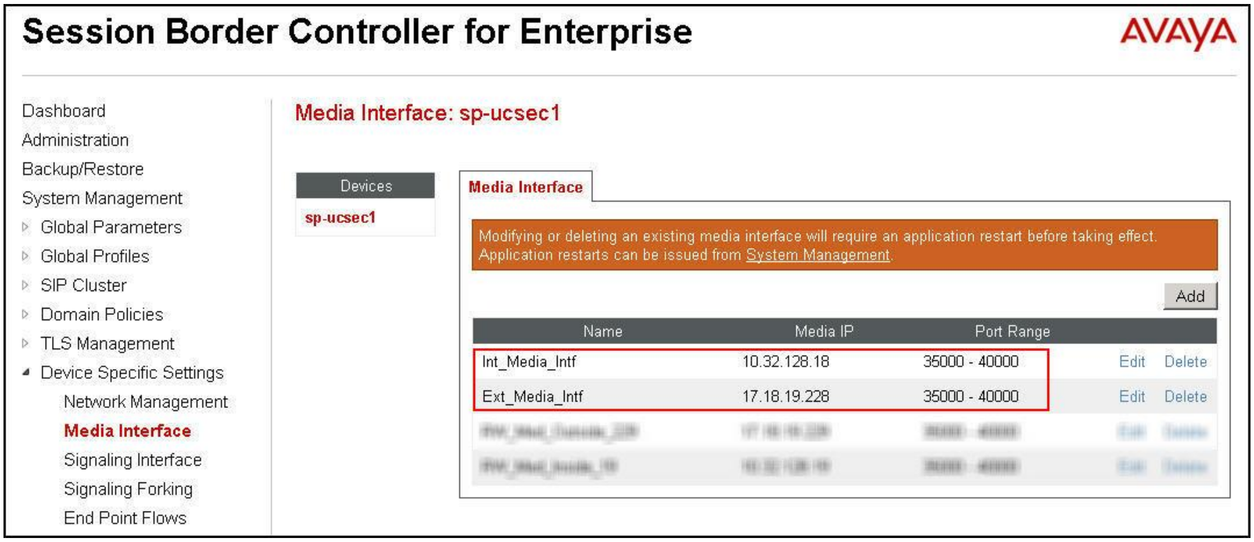
7.4. Media Interface

A media interface defines an IP address and port range for transmitting media. Create a media interface for both the internal and external sides of the Avaya SBCE.

To create a new interface, navigate to **Device Specific Settings → Media Interface** in the left pane. In the center pane, select the Avaya SBCE device (**sp-ucsec1**) to be managed. In the right pane, select **Add**. A pop-up window (not shown) will appear requesting the name of the new interface, followed by a series of pop-up windows in which the interface parameters can be configured. Once complete, the settings are shown in the far right pane.

For the compliance test, media interface **Int_Media_Intf** was created for the Avaya SBCE internal interface and media interface **Ext_Media_Intf** was created for the Avaya SBCE external interface. Each is highlighted below. When configuring the interfaces, configure the parameters as follows:

- Set **Name** to a descriptive name.
- For the internal interface, set the **Media IP** to the IP address associated with the private interface (A1) defined in **Section 7.2**. For the external interface, set the **Media IP** to the IP address associated with the public interface (B1) defined in **Section 7.2**.
- Set **Port Range** to a range of ports acceptable to both the Avaya SBCE and the far-end. For the compliance test, the default port range was used for both interfaces.



Media Interface: sp-ucsec1

Modifying or deleting an existing media interface will require an application restart before taking effect. Application restarts can be issued from System Management.

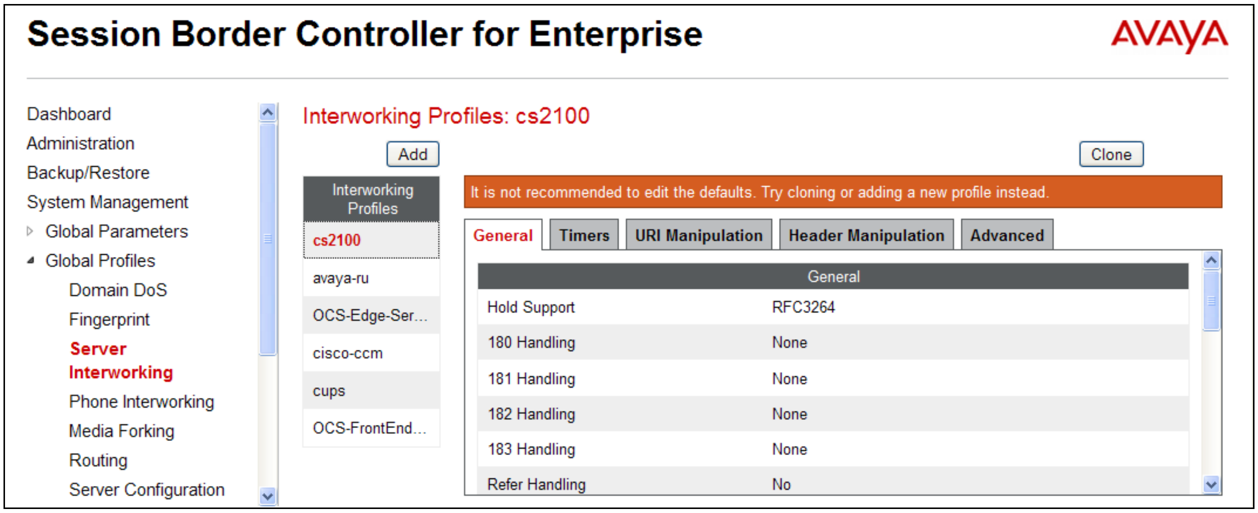
Name	Media IP	Port Range		
Int_Media_Intf	10.32.128.18	35000 - 40000	Edit	Delete
Ext_Media_Intf	17.18.19.228	35000 - 40000	Edit	Delete
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]

7.5. Server Interworking

A server interworking profile defines a set of parameters that aid in interworking between the Avaya SBCE and a connected server. Create separate server interworking profiles for Session Manager and the service provider SIP server. These profiles will be applied to the appropriate server in **Section 7.7.1** and **7.7.2**.

To create a new profile, navigate to **Global Profiles → Server Interworking** in the left pane. In the center pane, select **Add**. A pop-up window (not shown) will appear requesting the name of the new profile, followed by a series of pop-up windows in which the profile parameters can be configured. Once complete, the settings are shown in the far right pane. Alternatively, a new profile may be created by selecting an existing profile in the center pane and clicking the **Clone** button in the right pane. This will create a copy of the selected profile which can then be edited as needed. To view the settings of an existing profile, select the profile from the center pane. The settings will appear in the right pane.

The screen below shows the GUI elements described above before the server interworking profiles were added for the compliance test.

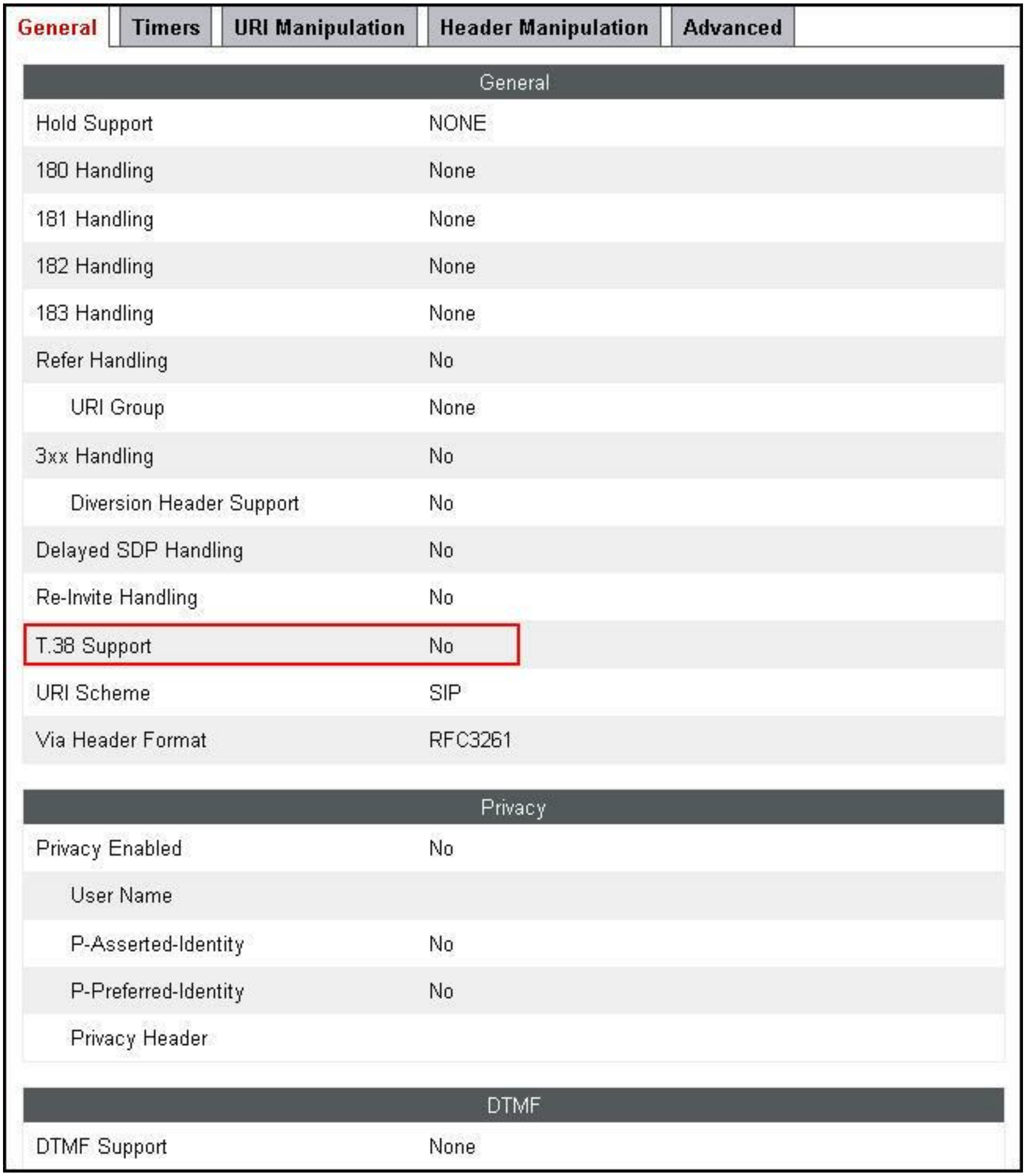


It is not recommended to edit the defaults. Try cloning or adding a new profile instead.

General	
Hold Support	RFC3264
180 Handling	None
181 Handling	None
182 Handling	None
183 Handling	None
Refer Handling	No

7.5.1. Server Interworking – Session Manager

For the compliance test, server interworking profile **PkwySM** was created for Session Manager by cloning the existing profile **avaya-ru**. The **General** tab parameters are shown below. Note that **T.38 Support** is set to **No** since Cox Communications does not support T.38 fax



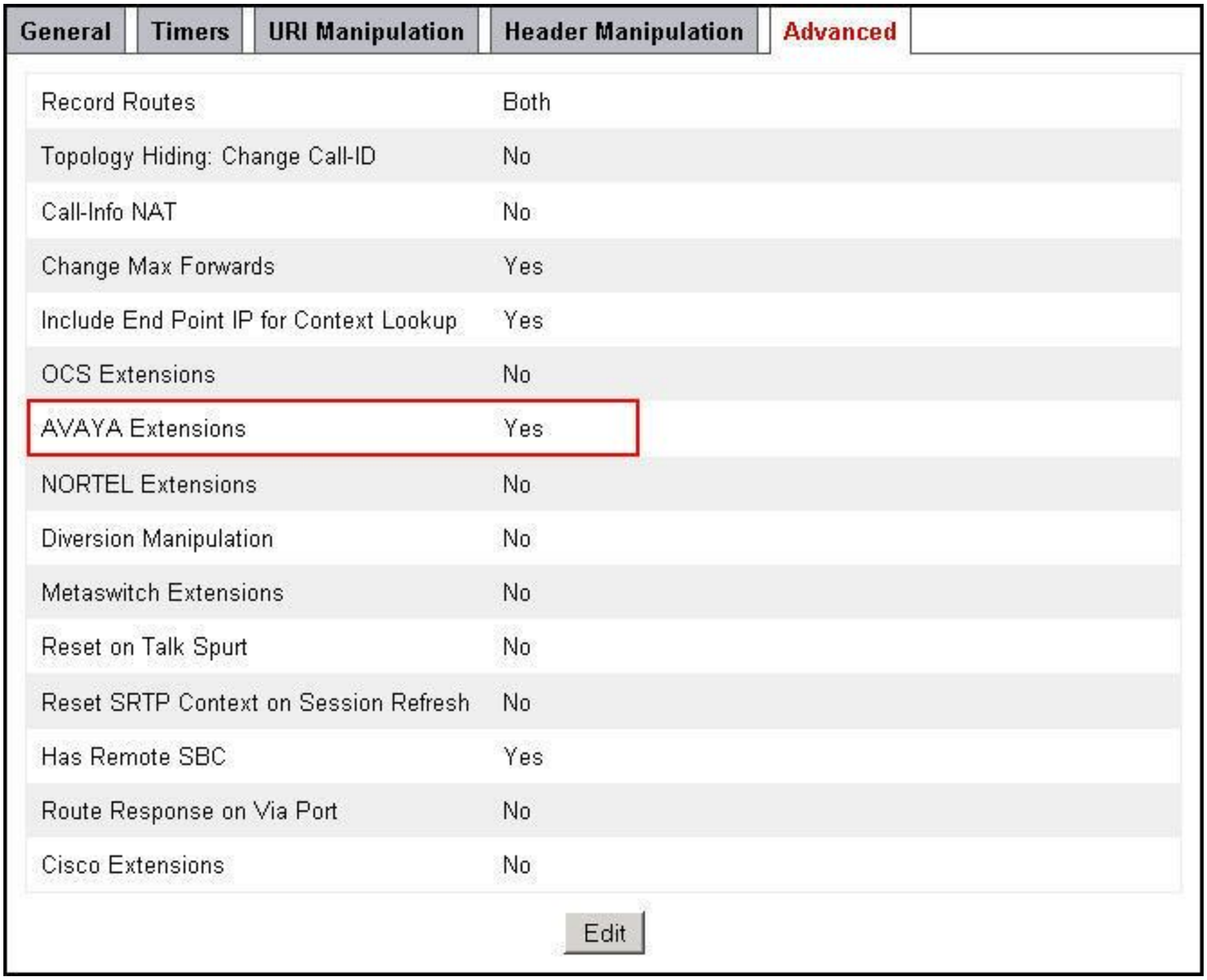
General	
Hold Support	NONE
180 Handling	None
181 Handling	None
182 Handling	None
183 Handling	None
Refer Handling	No
URI Group	None
3xx Handling	No
Diversion Header Support	No
Delayed SDP Handling	No
Re-Invite Handling	No
T.38 Support	No
URI Scheme	SIP
Via Header Format	RFC3261

Privacy	
Privacy Enabled	No
User Name	
P-Asserted-Identity	No
P-Preferred-Identity	No
Privacy Header	

DTMF	
DTMF Support	None

The **Timers**, **URI Manipulation** and **Header Manipulation** tabs have no entries.

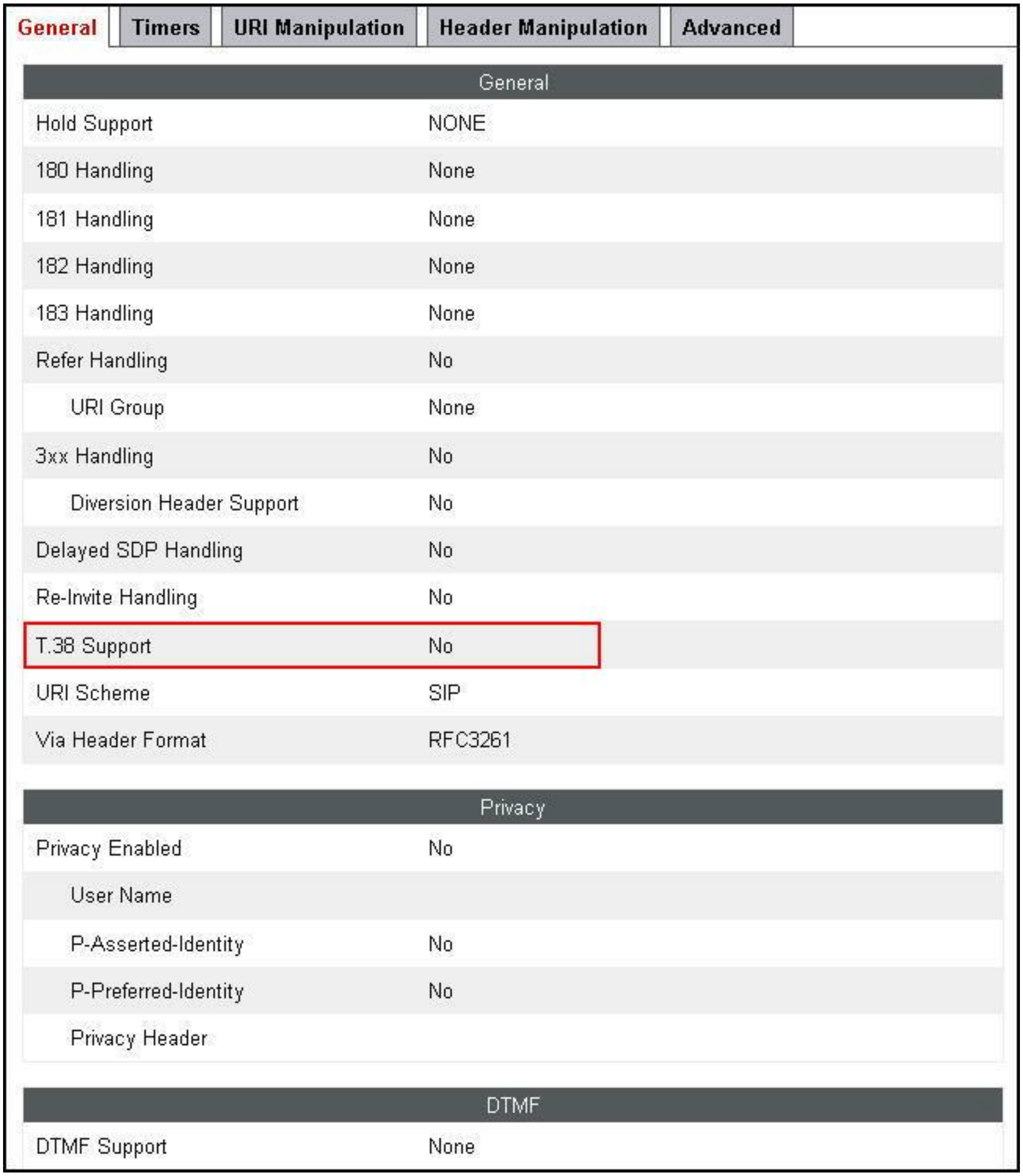
The **Advanced** tab parameters are shown below. Note that **AVAYA Extensions** is set to **Yes**.



Record Routes	Both
Topology Hiding: Change Call-ID	No
Call-Info NAT	No
Change Max Forwards	Yes
Include End Point IP for Context Lookup	Yes
OCS Extensions	No
AVAYA Extensions	Yes
NORTEL Extensions	No
Diversion Manipulation	No
Metaswitch Extensions	No
Reset on Talk Spurt	No
Reset SRTP Context on Session Refresh	No
Has Remote SBC	Yes
Route Response on Via Port	No
Cisco Extensions	No

7.5.2. Server Interworking – Cox Communications

For the compliance test, server interworking profile **SP-General** was created for the Cox Communications SIP server. When creating the profile, the default values were used for all parameters including the setting of **No** for **T.38 Support**. The **General** tab parameters are shown below.



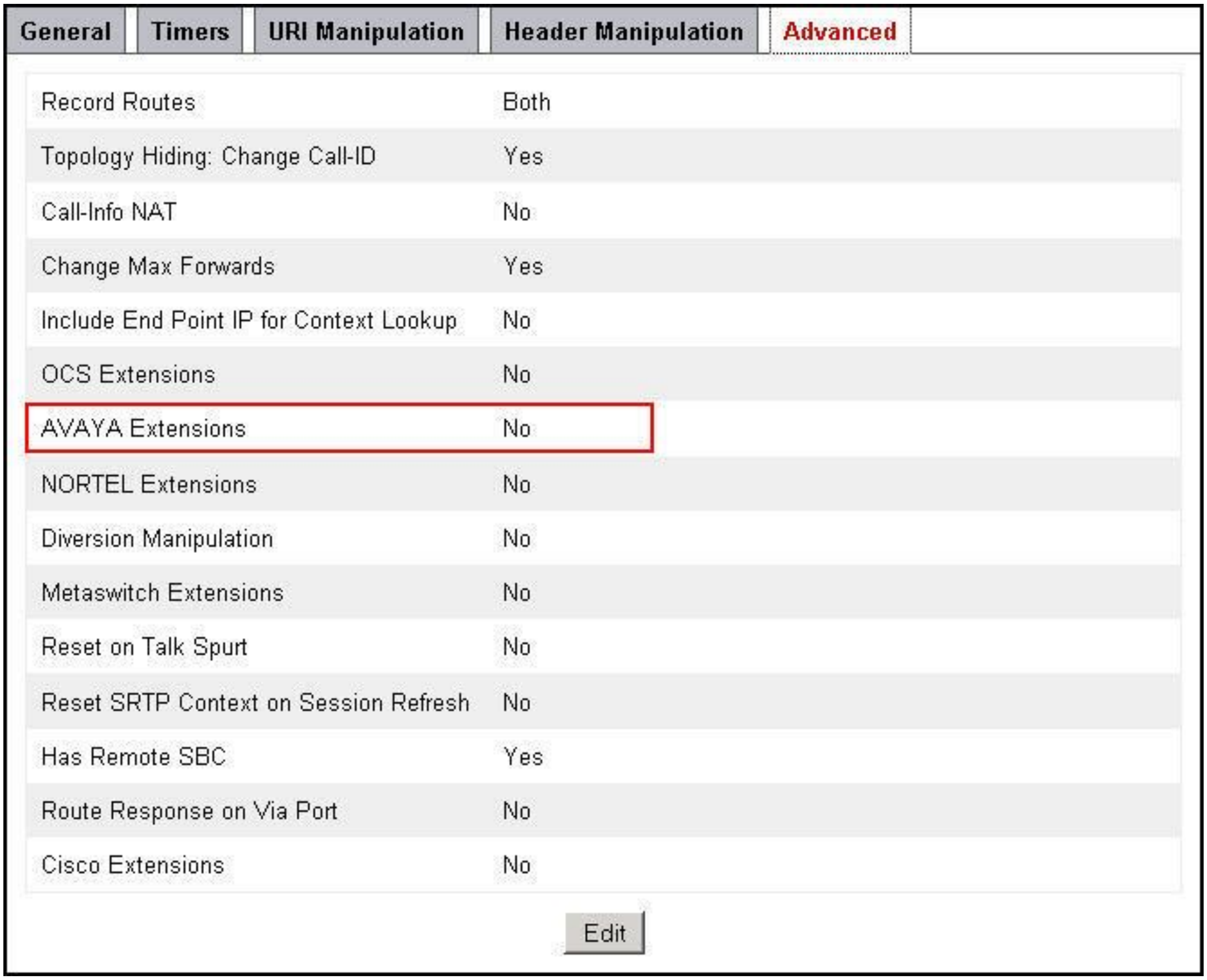
General	
Hold Support	NONE
180 Handling	None
181 Handling	None
182 Handling	None
183 Handling	None
Refer Handling	No
URI Group	None
3xx Handling	No
Diversion Header Support	No
Delayed SDP Handling	No
Re-Invite Handling	No
T.38 Support	No
URI Scheme	SIP
Via Header Format	RFC3261

Privacy	
Privacy Enabled	No
User Name	
P-Asserted-Identity	No
P-Preferred-Identity	No
Privacy Header	

DTMF	
DTMF Support	None

The **Timers**, **URI Manipulation**, **Header Manipulation** tabs have no entries.

The **Advanced** tab parameters are shown below. Note that **AVAYA Extensions** is set to **No**.



Record Routes	Both
Topology Hiding: Change Call-ID	Yes
Call-Info NAT	No
Change Max Forwards	Yes
Include End Point IP for Context Lookup	No
OCS Extensions	No
AVAYA Extensions	No
NORTEL Extensions	No
Diversion Manipulation	No
Metaswitch Extensions	No
Reset on Talk Spurt	No
Reset SRTP Context on Session Refresh	No
Has Remote SBC	Yes
Route Response on Via Port	No
Cisco Extensions	No

7.6. Signaling Manipulation

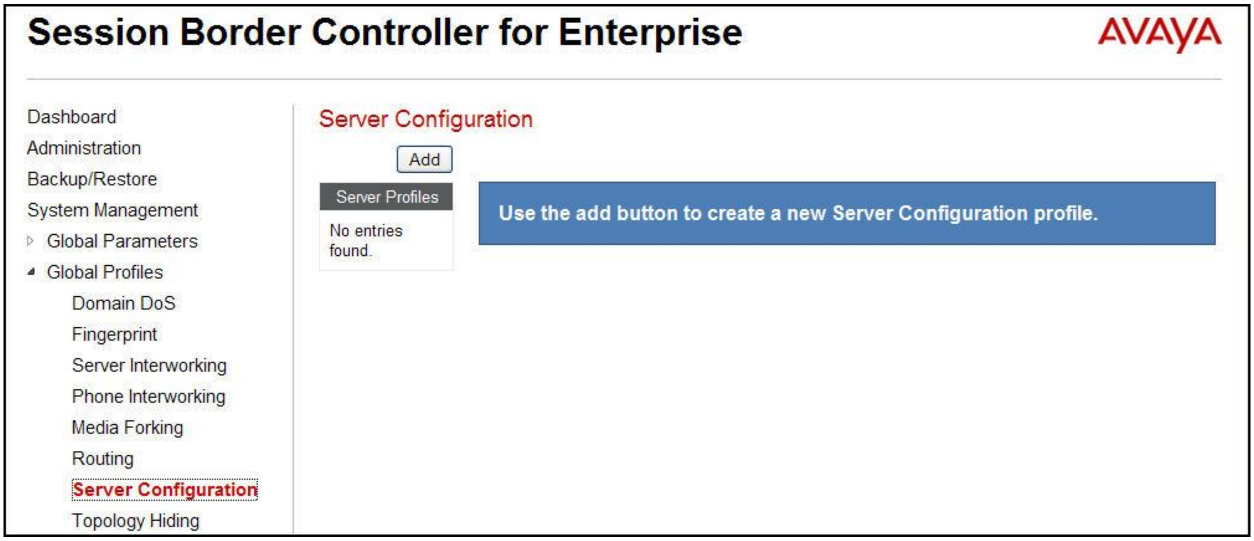
Signaling manipulation scripts provides for the manipulation of SIP messages which cannot be done by other configuration within the Avaya SBCE. It was not necessary to create any signaling manipulation scripts for interoperability with Cox Communications.

7.7. Server Configuration

A server configuration profile defines the attributes of the physical server. Create a server configuration profile for Session Manager and the service provider SIP server.

To create a new profile, navigate to **Global Profiles → Server Configuration** in the left pane. In the center pane, select **Add**. A pop-up window (not shown) will appear requesting the name of the new profile, followed by a series of pop-up windows in which the profile parameters can be configured. Once complete, the settings are shown in the far right pane. To view the settings of an existing profile, select the profile from the center pane. The settings will appear in the right pane.

The screen below shows the GUI elements described above before the servers profiles were added for the compliance test.



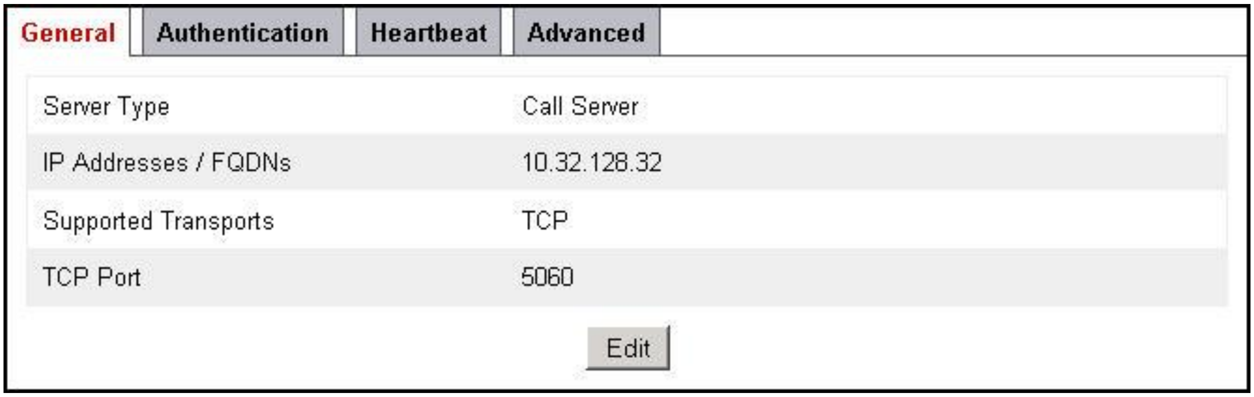
No entries found.

Use the add button to create a new Server Configuration profile.

7.7.1. Server Configuration – Session Manager

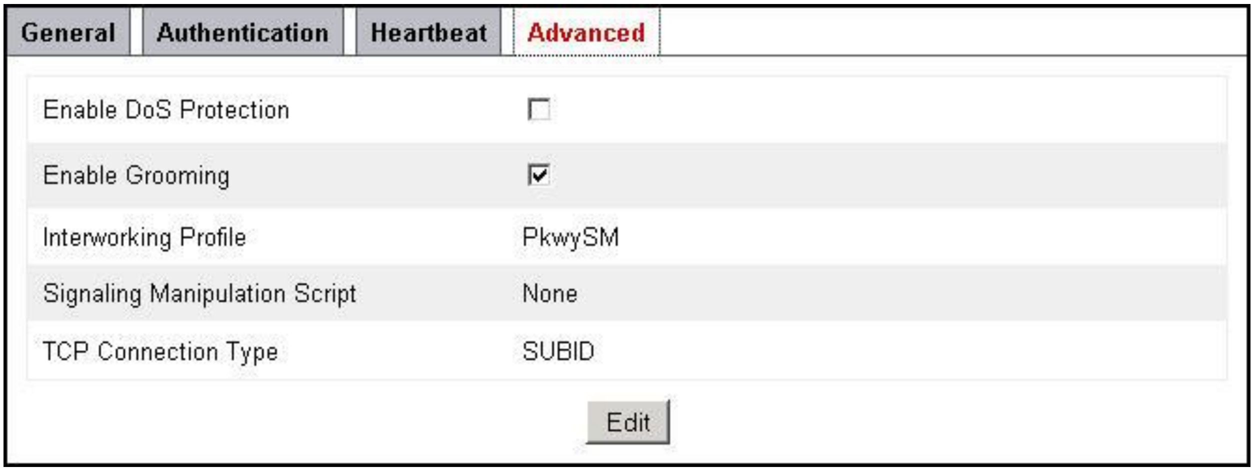
For the compliance test, server configuration profile **Pkwy-SM** was created for Session Manager. When creating the profile, configure the **General** tab parameters as follows:

- Set **Server Type** to **Call Server.**
- Set **IP Addresses / FQDNs** to the IP address of the Session Manager signaling interface.
- Set **Supported Transports** to the transport protocol used for SIP signaling between Session Manager and the Avaya SBCE.
- Set the **TCP Port** to the port Session Manager will listen on for SIP requests from the Avaya SBCE.



Server Type	Call Server
IP Addresses / FQDNs	10.32.128.32
Supported Transports	TCP
TCP Port	5060

On the **Advanced** tab, check **Enable Grooming** and set the **Interworking Profile** field to the interworking profile for Session Manager defined in **Section 7.5.1**.

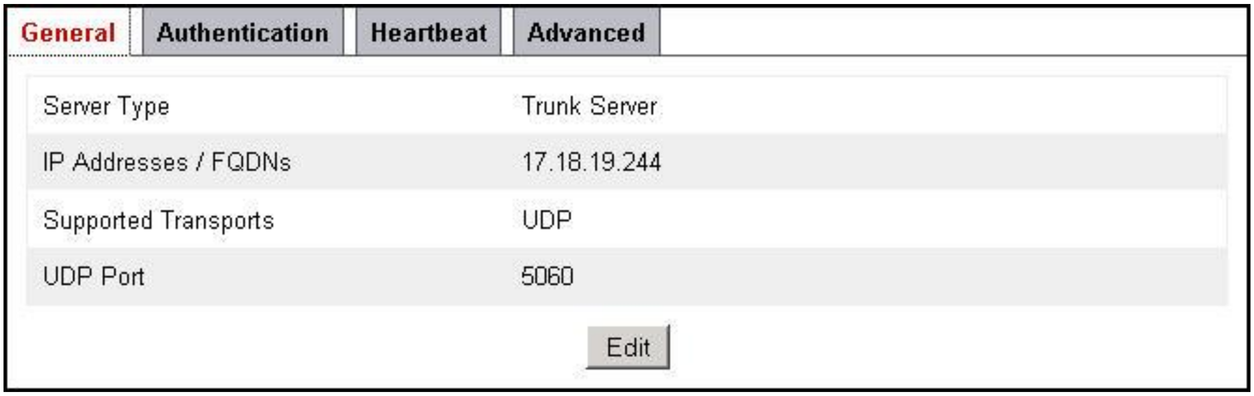


Enable DoS Protection	□
Enable Grooming	☑
Interworking Profile	PkwySM
Signaling Manipulation Script	None
TCP Connection Type	SUBID

7.7.2. Server Configuration – Cox Communications

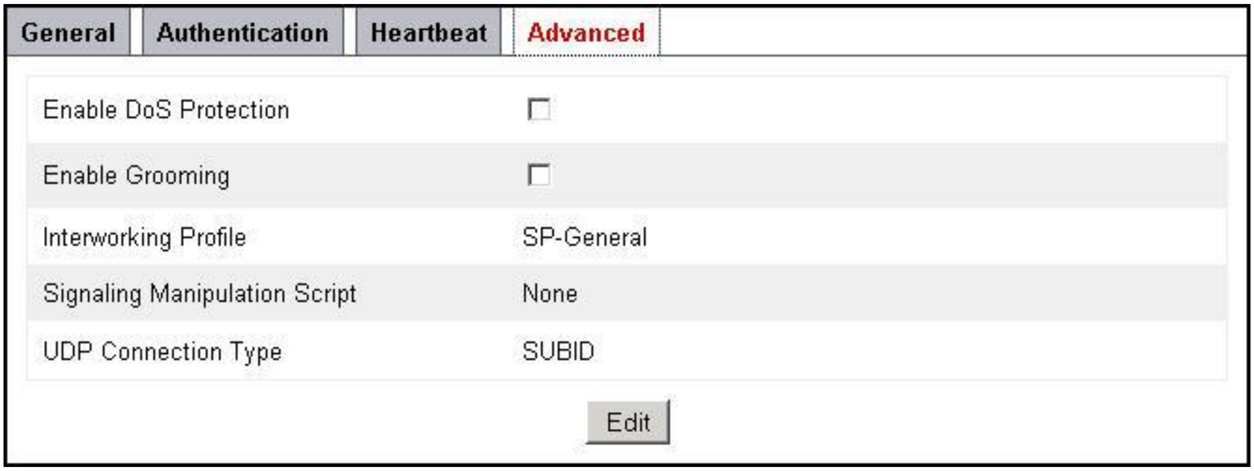
For the compliance test, server configuration profile **SP-Cox** was created for Cox Communications. When creating the profile, configure the **General** tab parameters as follows:

- Set **Server Type** to **Trunk Server.**
- Set **IP Addresses / FQDNs** to the IP address of the connected LAN port on EdgeMarc 4550 as shown in **Figure 1** in **Section 3**.
- Set **Supported Transports** to the transport protocol used for SIP signaling between EdgeMarc 4550 and the Avaya SBCE. In the compliance test, UDP was tested.
- Set the **UDP Port** to the standard SIP port of 5060. This is the port EdgeMarc 4550 will listen on for SIP requests from the Avaya SBCE.



Server Type	Trunk Server
IP Addresses / FQDNs	17.18.19.244
Supported Transports	UDP
UDP Port	5060

On the **Advanced** tab, set the **Interworking Profile** field to the interworking profile for Cox Communications defined in **Section 7.5.2**.

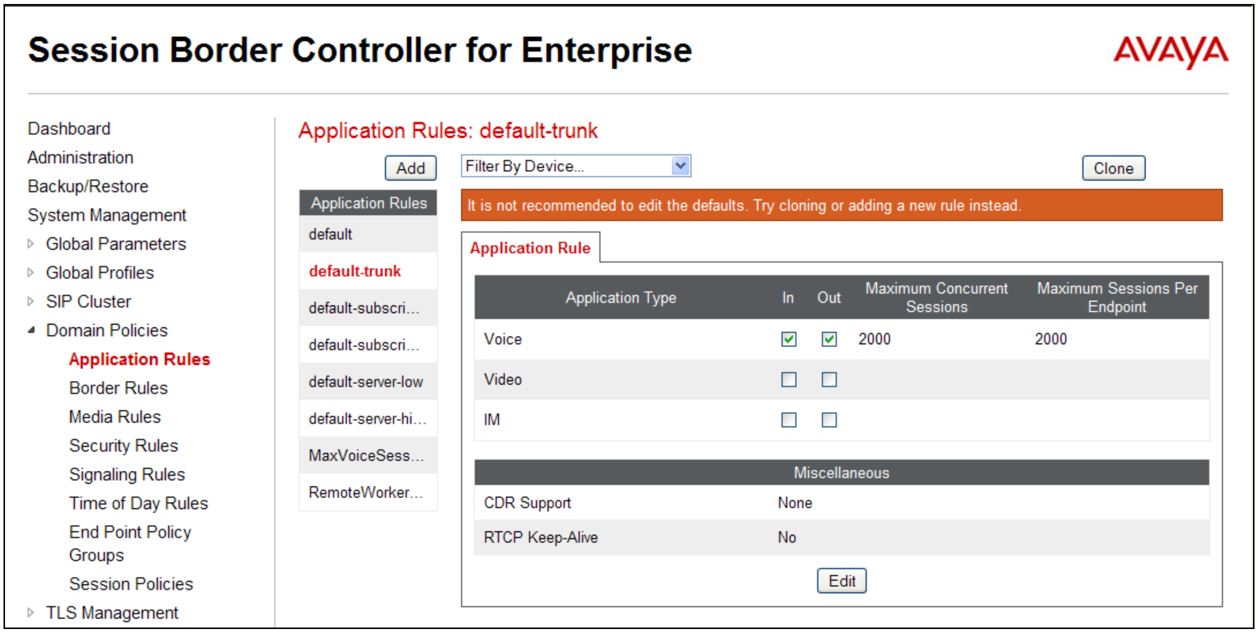


Enable DoS Protection	☐
Enable Grooming	☐
Interworking Profile	SP-General
Signaling Manipulation Script	None
UDP Connection Type	SUBID

7.8. Application Rules

An application rule defines the allowable SIP applications and associated parameters. An application rule is one component of the larger endpoint policy group defined in **Section 7.11**. For the compliance test, the predefined **default-trunk** application rule (shown below) was used for both Session Manager and the Cox Communications SIP server.

To view an existing rule, navigate to **Domain Policies → Application Rules** in the left pane. In the center pane, select the rule (e.g., **default-trunk**) to be viewed.



Application Rules: default-trunk

It is not recommended to edit the defaults. Try cloning or adding a new rule instead.

Application Type	In	Out	Maximum Concurrent Sessions	Maximum Sessions Per Endpoint
Voice	☑	☑	2000	2000
Video	□	□		
IM	□	□		

Miscellaneous	
CDR Support	None
RTCP Keep-Alive	No

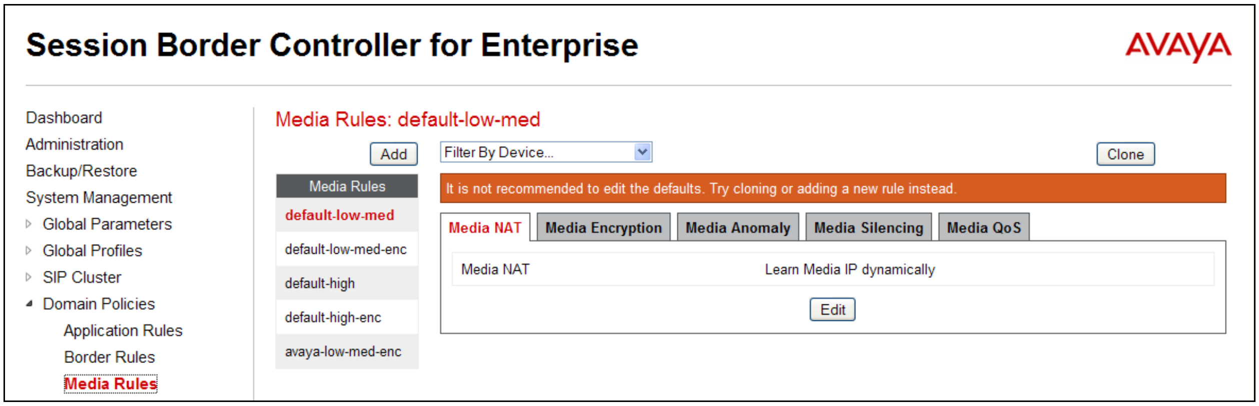
7.9. Media Rules

A media rule defines the processing to be applied to the selected media. A media rule is one component of the larger endpoint policy group defined in **Section 7.11**. For the compliance test, the predefined **default-low-med** media rule (shown below) was used for both Session Manager and the Cox Communications SIP server.

To view an existing rule, navigate to **Domain Policies → Media Rules** in the left pane. In the center pane, select the rule (e.g., **default-low-med**) to be viewed.

Each of the tabs of the **default-low-med** media rule containing data is shown below.

The **Media NAT** tab has no entries.



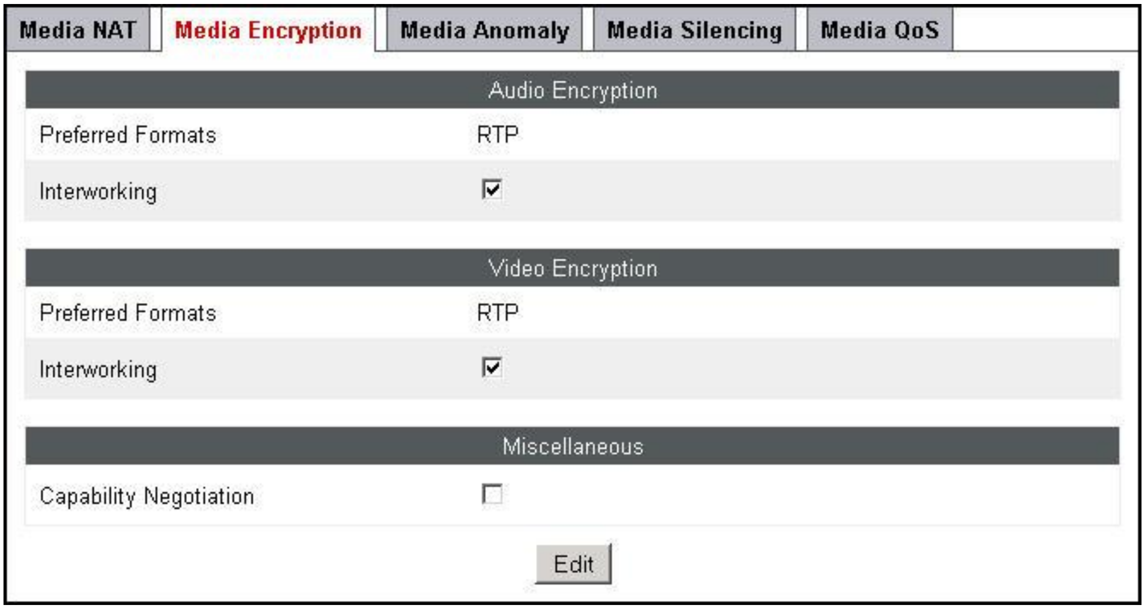
Session Border Controller for Enterprise

Media Rules: default-low-med

It is not recommended to edit the defaults. Try cloning or adding a new rule instead.

Media NAT	Learn Media IP dynamically

The **Media Encryption** tab indicates that no encryption was used.

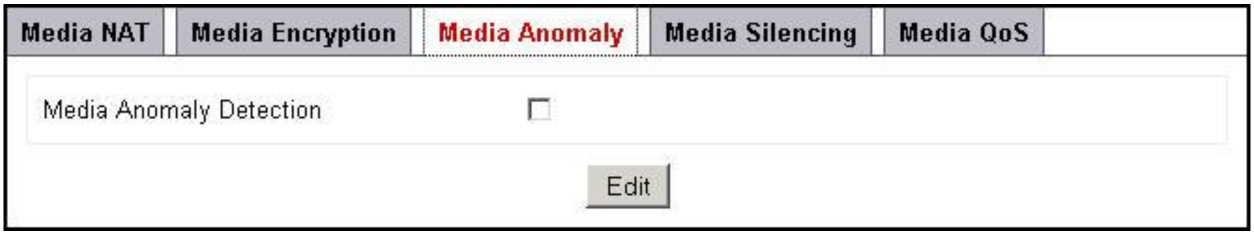


Audio Encryption	
Preferred Formats	RTP
Interworking	☑

Video Encryption	
Preferred Formats	RTP
Interworking	☑

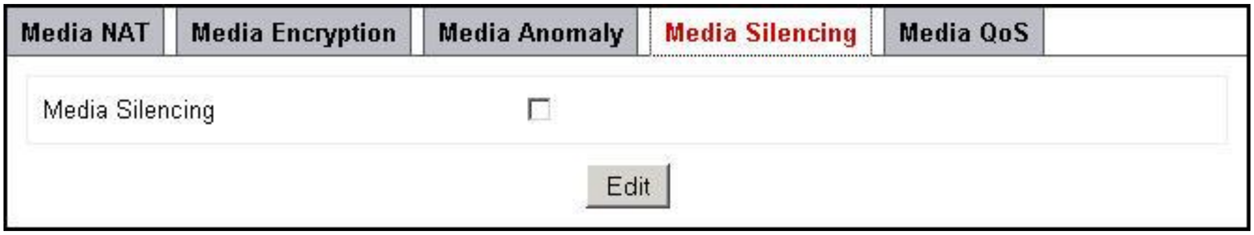
Miscellaneous	
Capability Negotiation	□

The **Media Anomaly** tab shows **Media Anomaly Detection** was disabled.



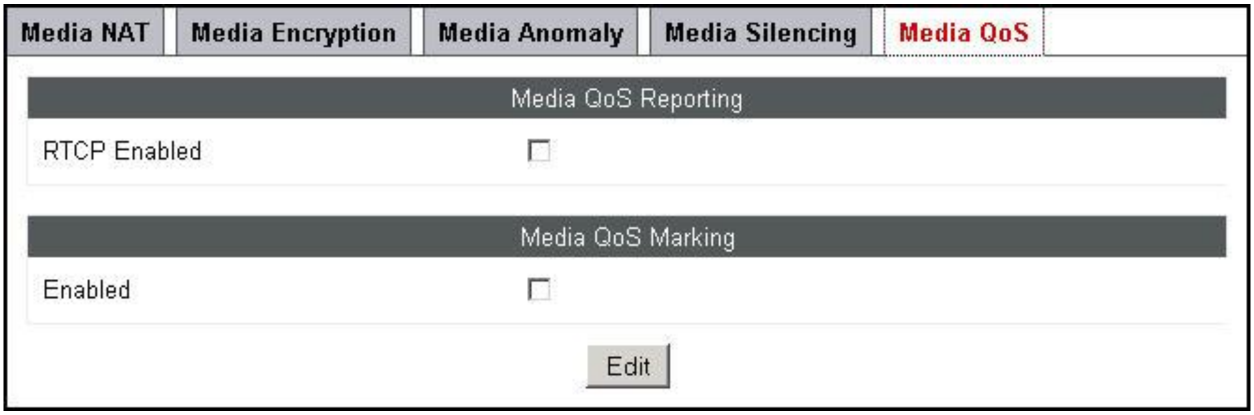
Media Anomaly Detection □

The **Media Silencing** tab shows Media Silencing was disabled.



Media Silencing □

The settings in the **Media QoS** tab are shown below.



Media QoS Reporting

RTCP Enabled □

Media QoS Marking

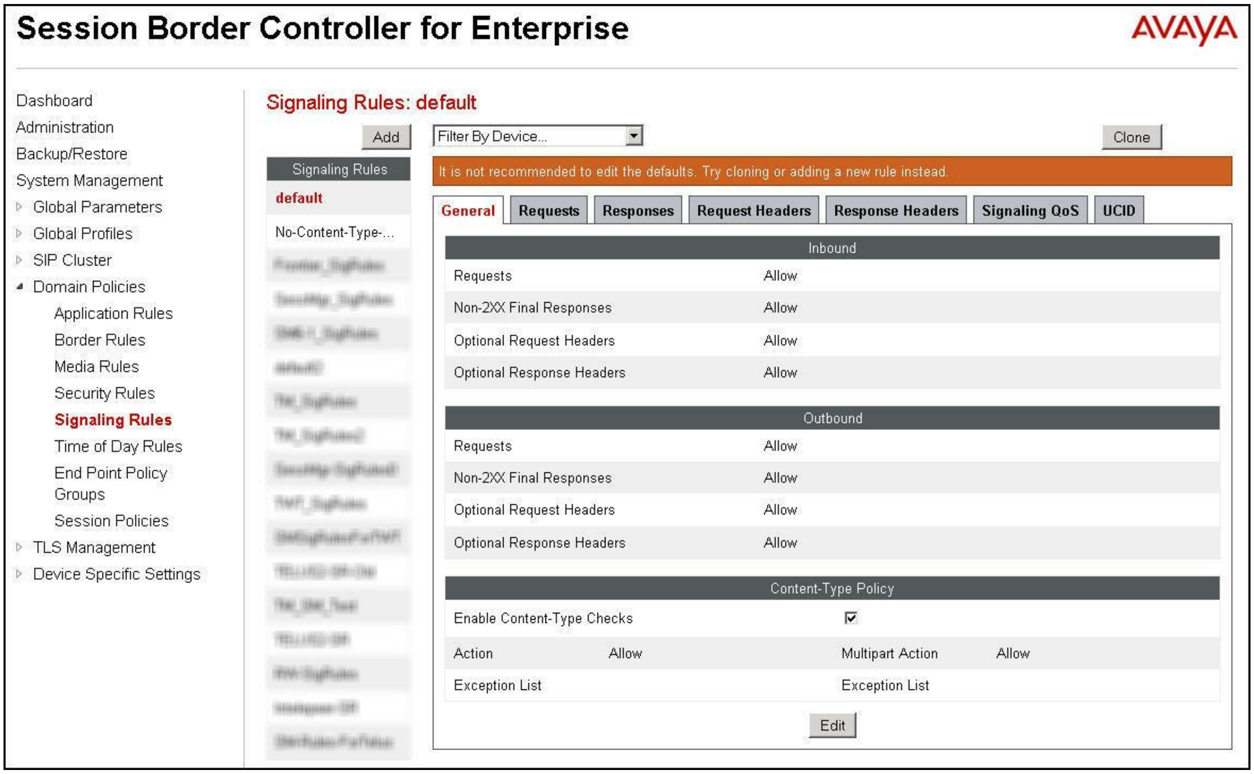
Enabled □

7.10. Signaling Rules

A signaling rule defines the processing to be applied to the selected signaling traffic. A signaling rule is one component of the larger endpoint policy group defined in **Section 7.11**. A specific signaling rule was created for Session Manager. The Cox Communications SIP server used the **default** rule.

To create a new rule, navigate to **Domain Policies → Signaling Rules** in the left pane. In the center pane, select **Add**. A pop-up window (not shown) will appear requesting the name of the new rule, followed by a series of pop-up windows in which the rule parameters can be configured. Once complete, the settings are shown in the far right pane. To view the settings of an existing rule, select the rule from the center pane. The settings will appear in the right pane.

The screen below shows the GUI elements described above.



Signaling Rules: default

It is not recommended to edit the defaults. Try cloning or adding a new rule instead.

Inbound	
Requests	Allow
Non-2XX Final Responses	Allow
Optional Request Headers	Allow
Optional Response Headers	Allow

Outbound	
Requests	Allow
Non-2XX Final Responses	Allow
Optional Request Headers	Allow
Optional Response Headers	Allow

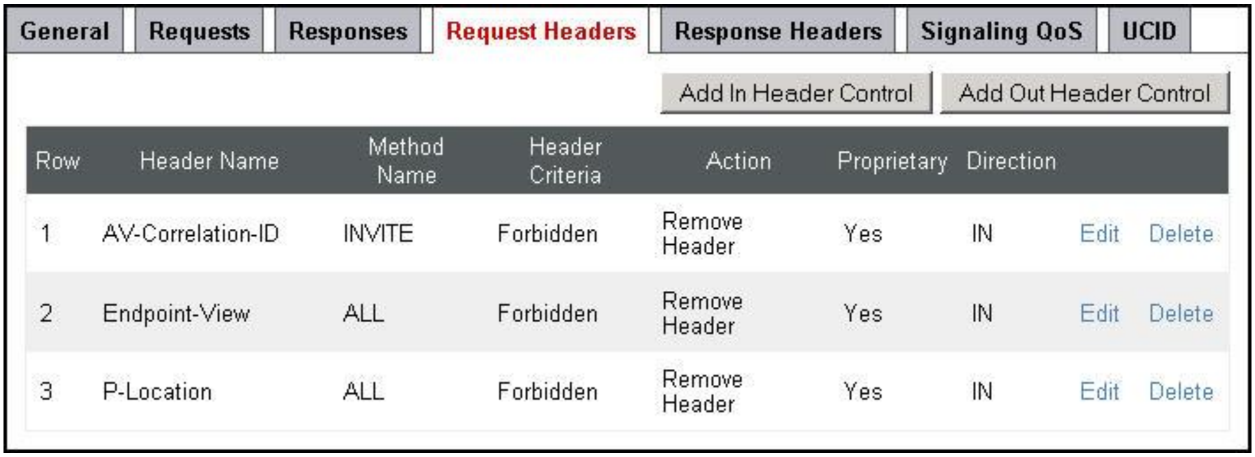
Content-Type Policy			
Enable Content-Type Checks	☑		
Action	Allow	Multipart Action	Allow
Exception List		Exception List	

7.10.1. Signaling Rules – Session Manager

For the compliance test, signaling rule **SessMgr_SigRules** was created for Session Manager to prevent proprietary headers in the SIP messages sent from the Session Manager from being propagated to Cox Communications. These headers may contain internal addresses or other information about the internal network. Select this rule in the center pane, then select the **Request Headers** tab to view the manipulations performed on request messages such as the initial INVITE or UPDATE message.

Click **Add** to create the rule. Keep the default values on all tabs except the **Request Headers** and **Response Headers** tabs. Select the **Request Headers** tab to create the manipulations performed on request messages such as INVITE or UPDATE. An entry is created by clicking the **Add In Header Control** or **Add Out Header Control** button depending on the direction (relative to the Avaya SBCE) of the message to be modified. Entries were created to perform the following actions:

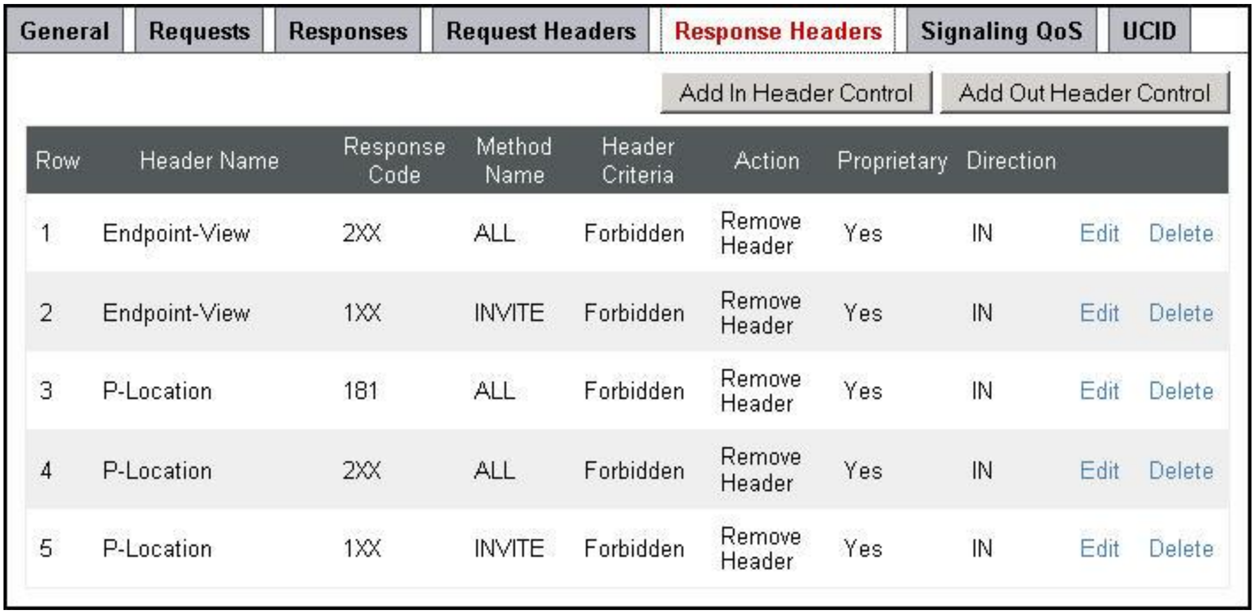
1. Removes the **AV-Correlation-ID** header from **INVITE** messages in the **IN** direction (Session Manager to Avaya SBCE).
2. Removes the **Endpoint-View** header from **ALL** messages in the **IN** direction.
3. Removes the **P-Location** header from **ALL** messages in the **IN** direction.



Row	Header Name	Method Name	Header Criteria	Action	Proprietary	Direction		
1	AV-Correlation-ID	INVITE	Forbidden	Remove Header	Yes	IN	Edit	Delete
2	Endpoint-View	ALL	Forbidden	Remove Header	Yes	IN	Edit	Delete
3	P-Location	ALL	Forbidden	Remove Header	Yes	IN	Edit	Delete

Similarly, manipulations can be performed on SIP response messages. These can be created by selecting the **Response Headers** tab as shown below. Entries were created in the same manner as was done on the **Request Headers** tab. The entries shown perform the following actions:

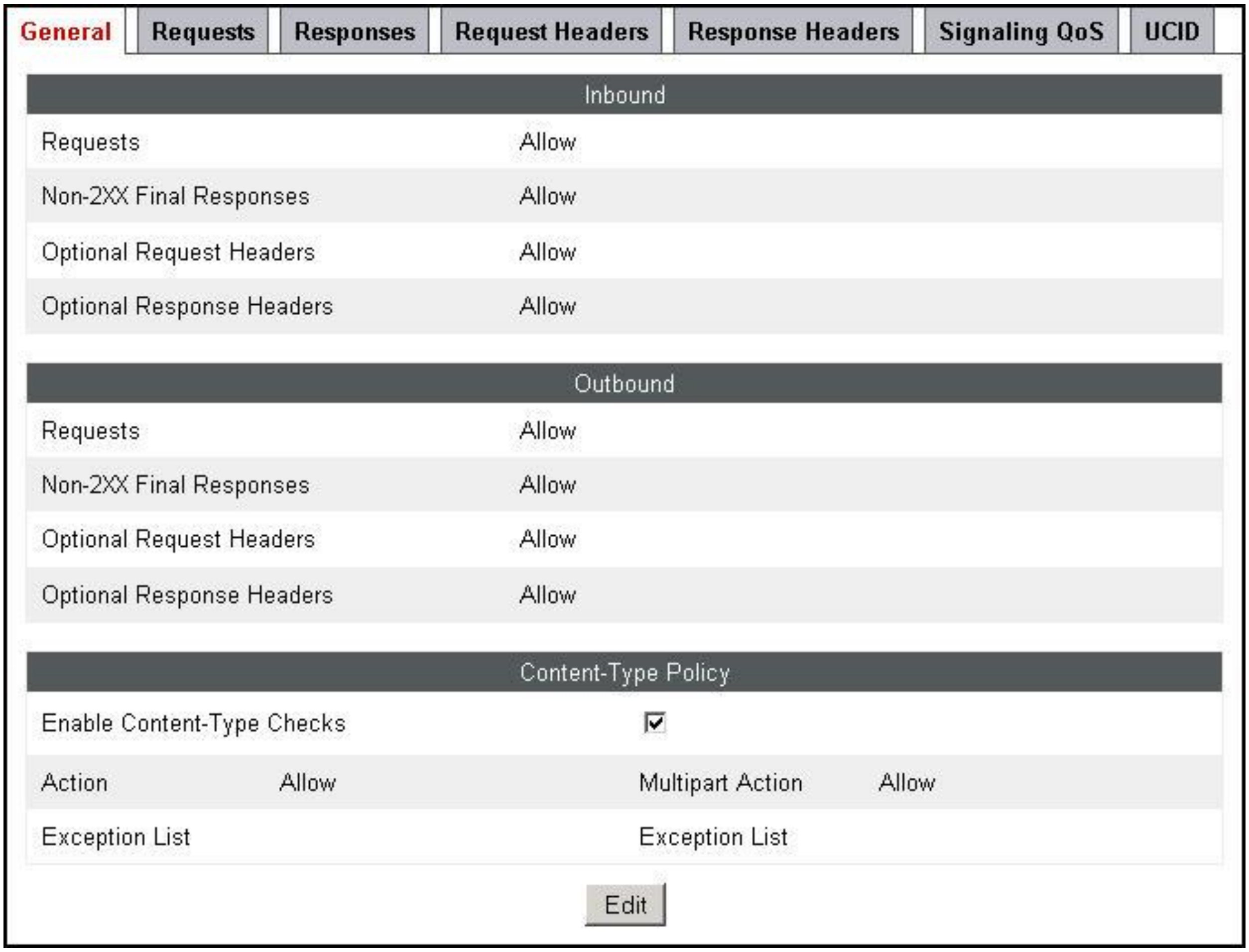
1. Removes the **Endpoint-View** header from any **2XX** response to **ALL** messages in the **IN** direction (Session Manager to Avaya SBCE).
2. Removes the **Endpoint-View** header from any **1XX** response to an **INVITE** message in the **IN** direction.
3. Removes the **P-Location** header from any **2XX** or a specific 181 response to **ALL** messages in the **IN** direction.
4. Removes the **P-Location** header from any **1XX** response to an **INVITE** message in the **IN** direction.



Row	Header Name	Response Code	Method Name	Header Criteria	Action	Proprietary	Direction		
1	Endpoint-View	2XX	ALL	Forbidden	Remove Header	Yes	IN	Edit	Delete
2	Endpoint-View	1XX	INVITE	Forbidden	Remove Header	Yes	IN	Edit	Delete
3	P-Location	181	ALL	Forbidden	Remove Header	Yes	IN	Edit	Delete
4	P-Location	2XX	ALL	Forbidden	Remove Header	Yes	IN	Edit	Delete
5	P-Location	1XX	INVITE	Forbidden	Remove Header	Yes	IN	Edit	Delete

7.10.2. Signaling Rules – Cox Communications

The predefined **default** signaling rule (shown below) was used for the Cox Communications SIP server. The **General** tab settings are shown below.

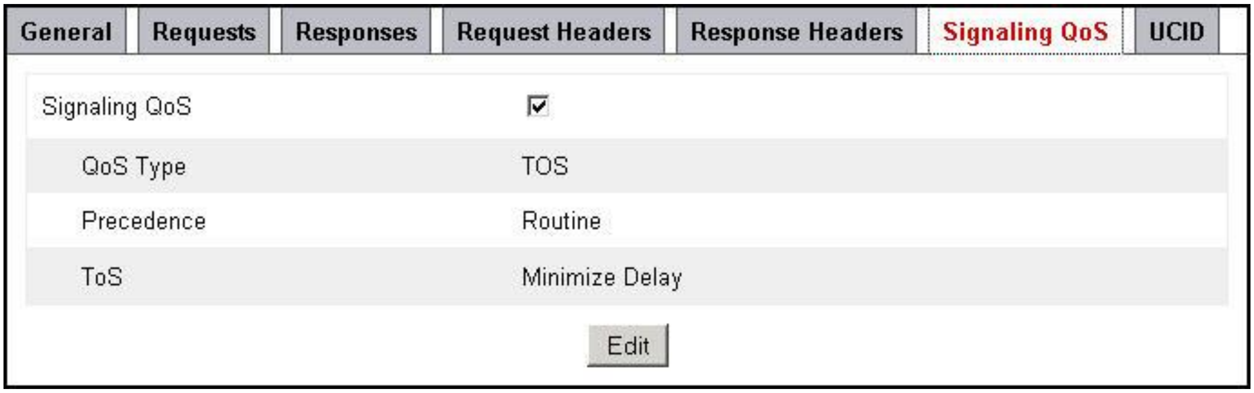


Inbound	
Requests	Allow
Non-2XX Final Responses	Allow
Optional Request Headers	Allow
Optional Response Headers	Allow

Outbound	
Requests	Allow
Non-2XX Final Responses	Allow
Optional Request Headers	Allow
Optional Response Headers	Allow

Content-Type Policy			
Enable Content-Type Checks		☑	
Action	Allow	Multipart Action	Allow
Exception List		Exception List	

The **Requests**, **Responses**, **Request Headers**, and **Response Headers** and **UCID** tabs have no entries. The **Signaling QoS** tab is shown below.



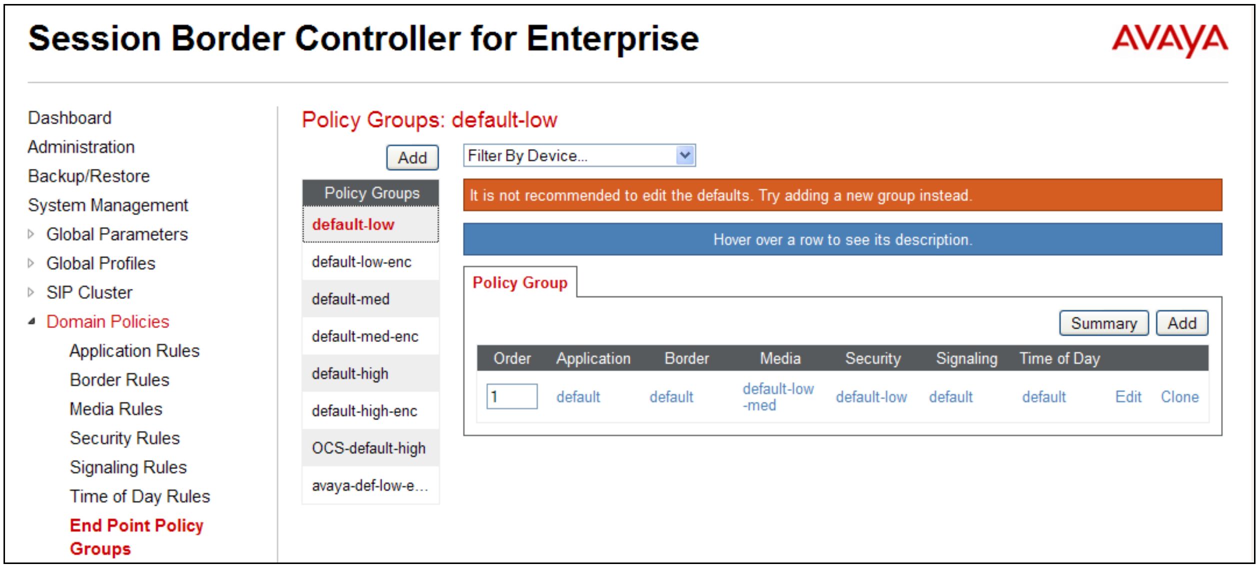
Signaling QoS	☑
QoS Type	TOS
Precedence	Routine
ToS	Minimize Delay

7.11. Endpoint Policy Groups

An endpoint policy group is a set of policies that will be applied to traffic between the Avaya SBCE and a signaling endpoint (connected server). Thus, an endpoint policy group must be created for Session Manager and the service provider SIP server. The endpoint policy group is applied to the traffic as part of the endpoint flow defined in **Section 7.14**.

To create a new group, navigate to **Domain Policies → End Point Policy Groups** in the left pane. In the center pane, select **Add**. A pop-up window (not shown) will appear requesting the name of the new group, followed by a series of pop-up windows in which the group parameters can be configured. Once complete, the settings are shown in the far right pane. To view the settings of an existing group, select the group from the center pane. The settings will appear in the right pane.

The screen below shows the GUI elements described above before specific endpoint policy groups were added for the compliance test.



Policy Groups: default-low

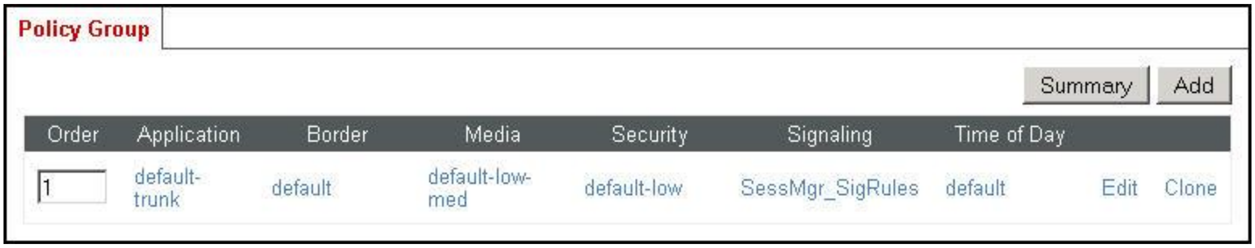
It is not recommended to edit the defaults. Try adding a new group instead.

Hover over a row to see its description.

Order	Application	Border	Media	Security	Signaling	Time of Day		
1	default	default	default-low-med	default-low	default	default	Edit	Clone

7.11.1. Endpoint Policy Group – Session Manager

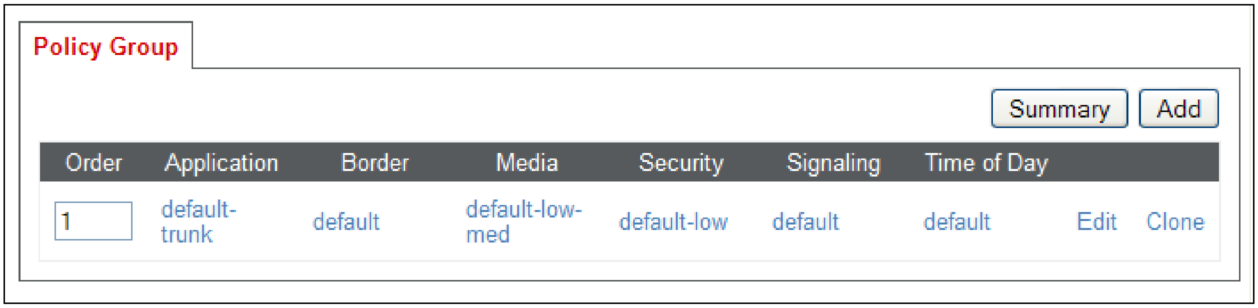
For the compliance test, endpoint policy group **SM** was created for Session Manager as shown below. For **Application**, enter the application rule described in **Section 7.8**. For **Signaling**, enter the signaling rule created in **Section 7.10.1**. For **Media**, enter the media rule described in **Section 7.9**.



Order	Application	Border	Media	Security	Signaling	Time of Day		
1	default-trunk	default	default-low-med	default-low	SessMgr_SigRules	default	Edit	Clone

7.11.2. Endpoint Policy Group – Cox Communications

For the compliance test, endpoint policy group **Cox-Policy-Grp** was created for the Cox Communications SIP server as shown below. For **Application**, enter the application rule described in **Section 7.8**. The details of the default settings for **Media** and **Signaling** are showed in **Section 7.9** and **Section 7.10.2** respectively.



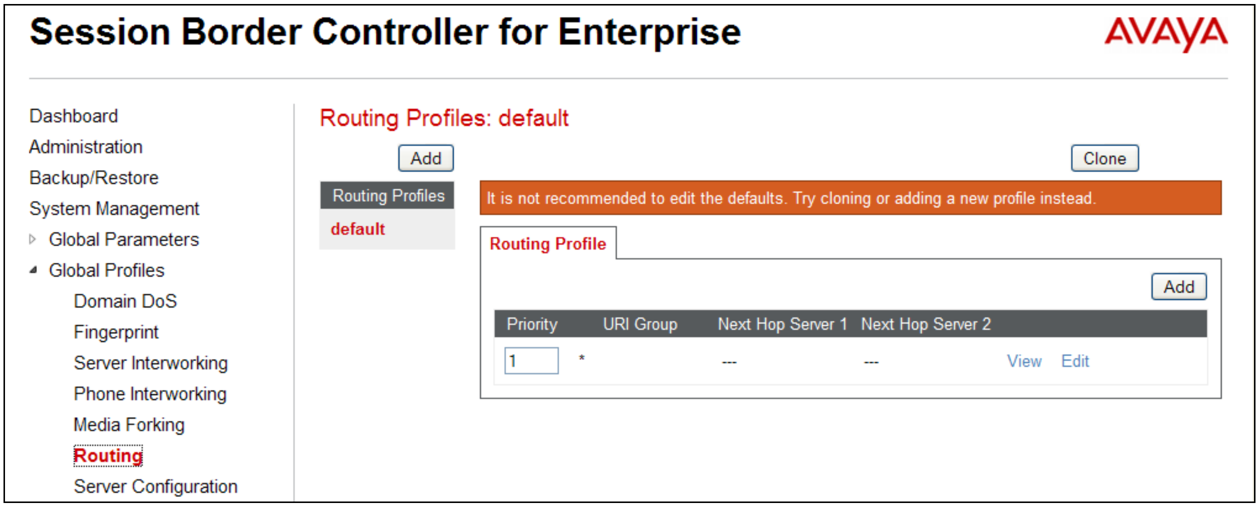
Order	Application	Border	Media	Security	Signaling	Time of Day		
1	default-trunk	default	default-low-med	default-low	default	default	Edit	Clone

7.12. Routing

A routing profile defines where traffic will be directed based on the contents of the URI. A routing profile is applied only after the traffic has matched an endpoint server flow defined in **Section 7.14**. Create separate routing profiles for Session Manager and the service provider SIP server.

To create a new profile, navigate to **Global Profiles → Routing** in the left pane. In the center pane, select **Add**. A pop-up window (not shown) will appear requesting the name of the new profile, followed by a series of pop-up windows in which the profile parameters can be configured. Once complete, the settings are shown in the far right pane. To view the settings of an existing profile, select the profile from the center pane.

The screen below shows the GUI elements described above before specific routing profiles were added for the compliance test.



Routing Profiles: default

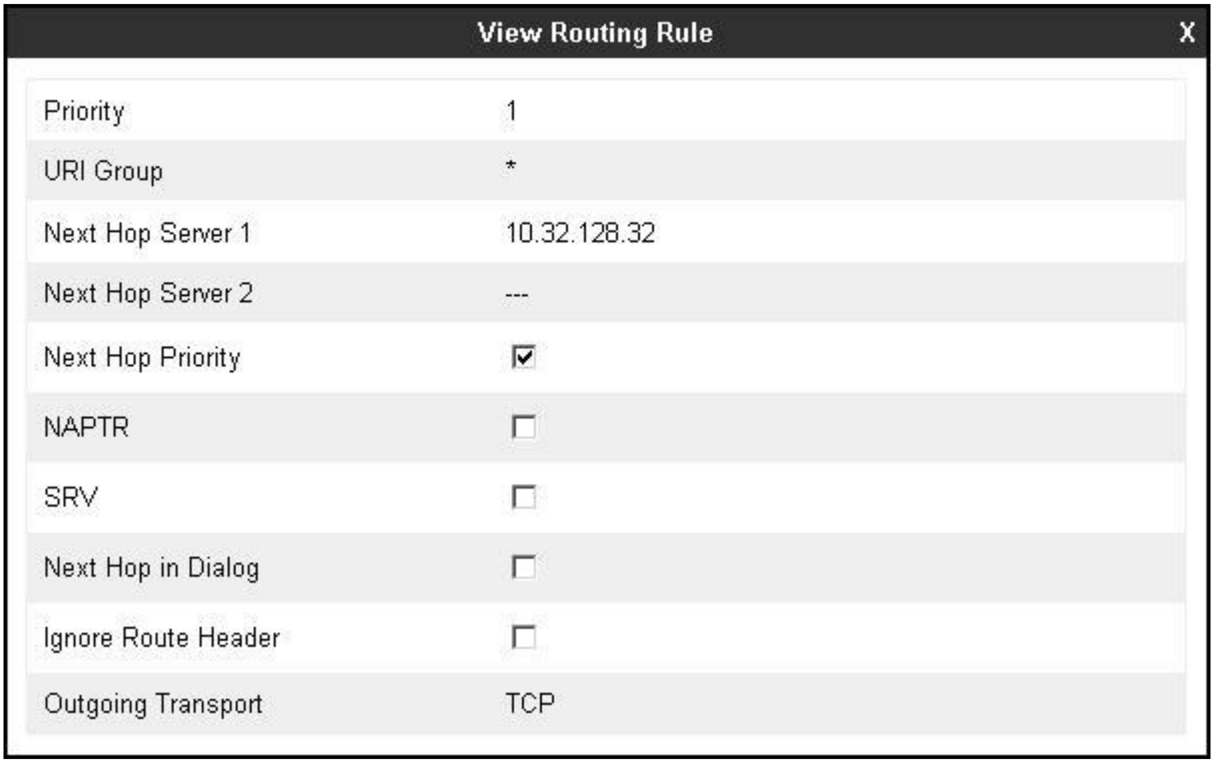
It is not recommended to edit the defaults. Try cloning or adding a new profile instead.

Priority	URI Group	Next Hop Server 1	Next Hop Server 2		
1	*	---	---	View	Edit

7.12.1. Routing – Session Manager

For the compliance test, routing profile **To-PkwySM** was created for Session Manager. When creating the profile, configure the parameters as follows:

- Set the **URI Group** to the wild card ***** to match on any URI.
- Set the **Next Hop Server 1** field to the IP address of Session Manager signaling interface.
- Enable **Next Hop Priority**.
- Set the **Outgoing Transport** field to **TCP**.

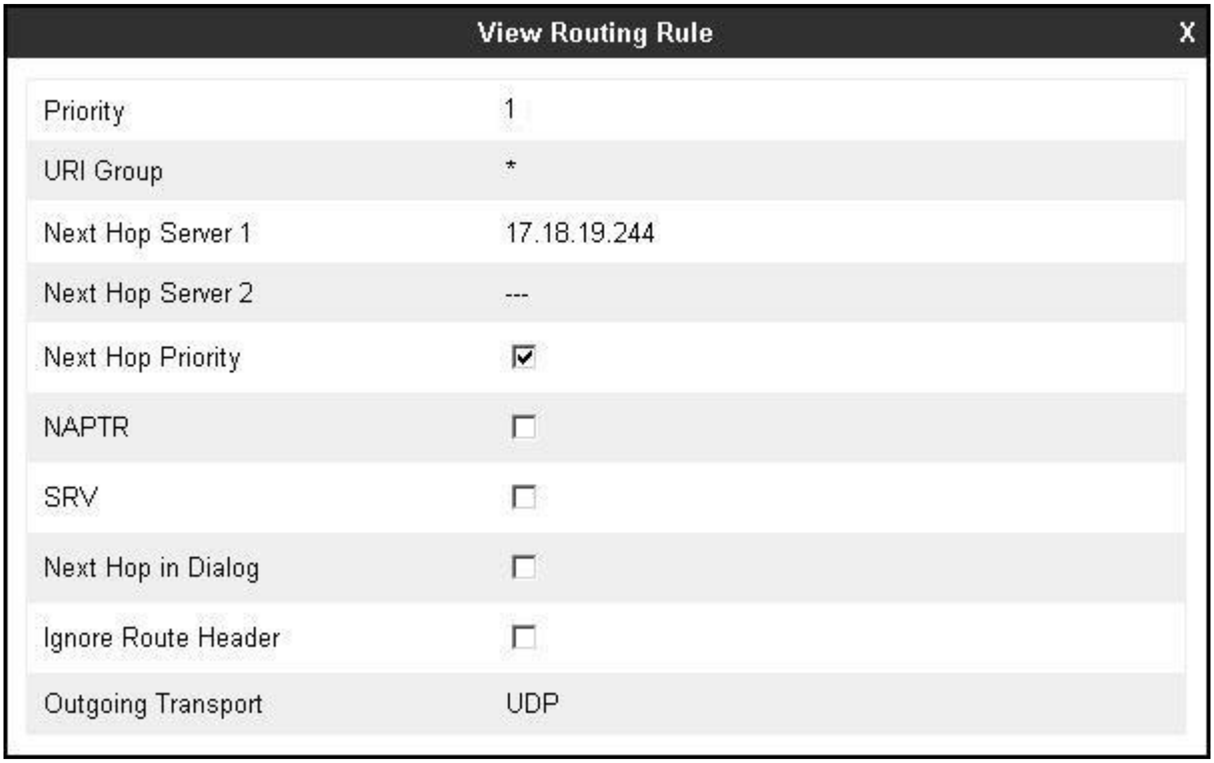


Priority	1
URI Group	*
Next Hop Server 1	10.32.128.32
Next Hop Server 2	---
Next Hop Priority	☑
NAPTR	□
SRV	□
Next Hop in Dialog	□
Ignore Route Header	□
Outgoing Transport	TCP

7.12.2. Routing – Cox Communications

For the compliance test, routing profile **To-Trunks** was created for Cox Communications. When creating the profile, configure the parameters as follows:

- Set the **URI Group** to the wild card ***** to match on any URI.
- Set the **Next Hop Server 1** field to the IP address of the connected LAN port on EdgeMarc 4550 as shown in **Figure 1** in **Section 3**.
- Enable **Next Hop Priority**.
- Set the **Outgoing Transport** field to **UDP**.



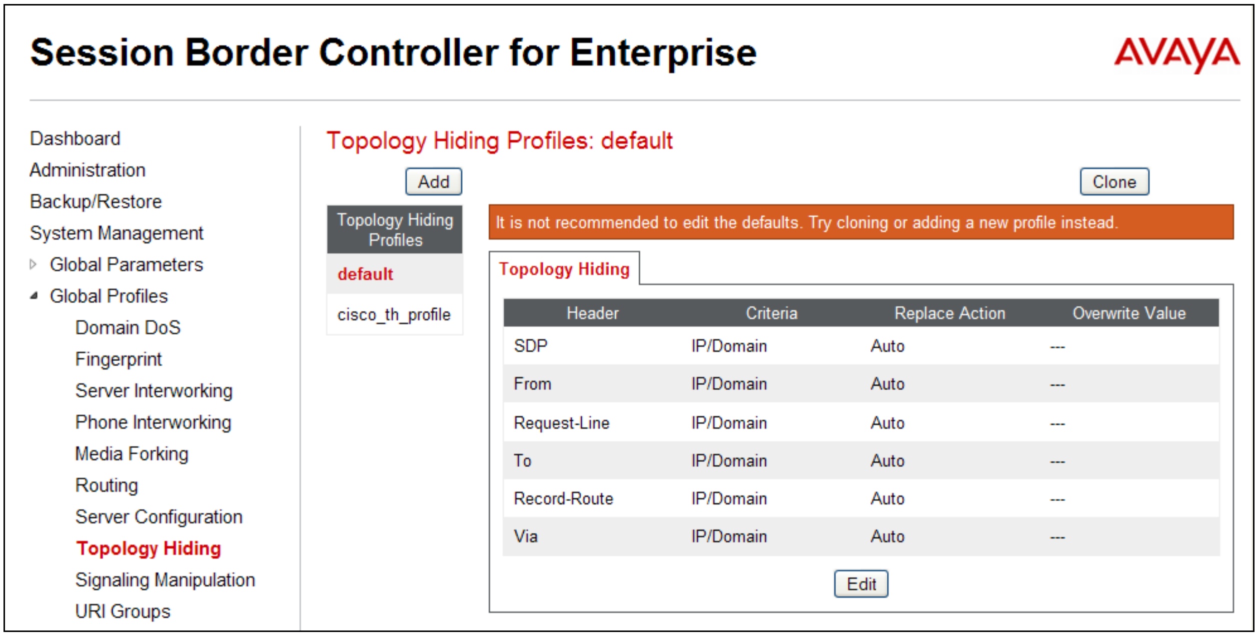
Priority	1
URI Group	*
Next Hop Server 1	17.18.19.244
Next Hop Server 2	---
Next Hop Priority	☑
NAPTR	□
SRV	□
Next Hop in Dialog	□
Ignore Route Header	□
Outgoing Transport	UDP

7.13. Topology Hiding

Topology hiding allows the host part of some SIP message headers to be modified in order to prevent private network information from being propagated to the untrusted public network. It can also be used as an interoperability tool to adapt the host portion of these same headers to meet the requirements of the connected servers. The topology hiding profile is applied as part of the endpoint flow in **Section 7.14**.

To create a new profile, navigate to **Global Profiles → Topology Hiding** in the left pane. In the center pane, select **Add**. A pop-up window (not shown) will appear requesting the name of the new profile, followed by a pop-up window in which a header can be selected and configured. Additional headers can be added in this window. Once complete, the settings are shown in the far right pane. To view the settings of an existing profile (e.g., **default**), select the profile from the center pane. The settings will appear in the right pane.

The screen below shows the GUI elements described above before specific topology hiding profiles were added for the compliance test.



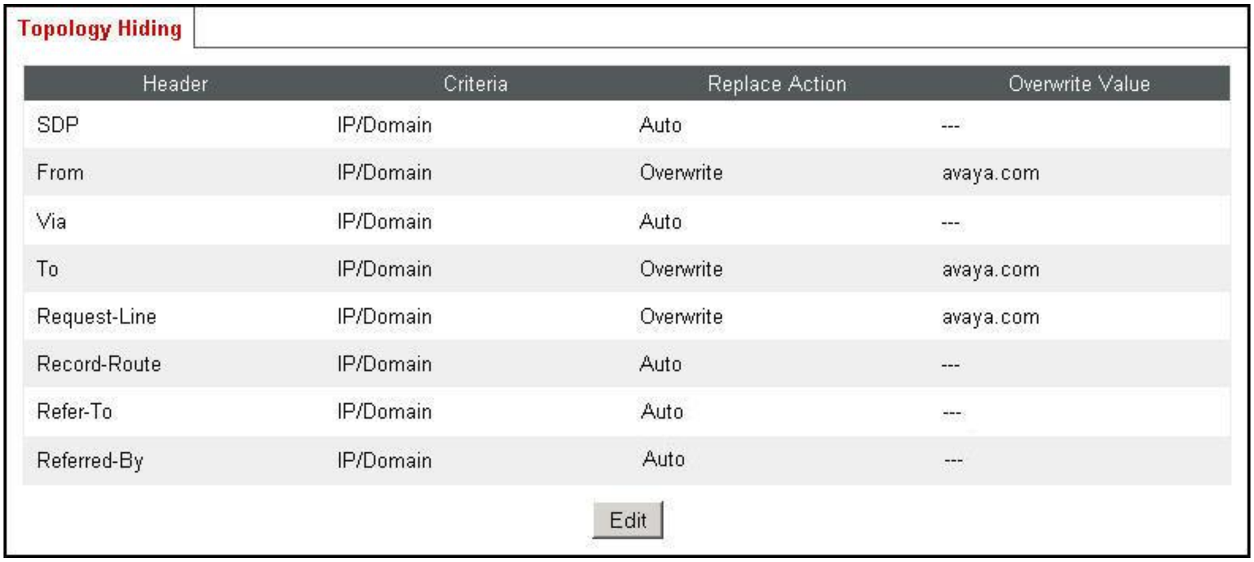
It is not recommended to edit the defaults. Try cloning or adding a new profile instead.

Header	Criteria	Replace Action	Overwrite Value
SDP	IP/Domain	Auto	---
From	IP/Domain	Auto	---
Request-Line	IP/Domain	Auto	---
To	IP/Domain	Auto	---
Record-Route	IP/Domain	Auto	---
Via	IP/Domain	Auto	---

7.13.1. Topology Hiding – Session Manager

For the compliance test, topology hiding profile **PRT-Domain** was created for Session Manager. This profile will be applied to traffic from the Avaya SBCE to Session Manager. When creating the profile, configure the parameters as follows:

- Set **Header** to the header whose host part of the URI is to be modified.
- Set **Criteria** to **IP/Domain** to indicate that the host part should be modified if it is an IP address or a domain.
- Set **Replace Action** to **Auto** for all headers except **Request-Line**, **From** and **To** which should be set to **Overwrite**.
- For those headers to be overwritten, the **Overwrite Value** is set to the enterprise domain (**avaya.com**).

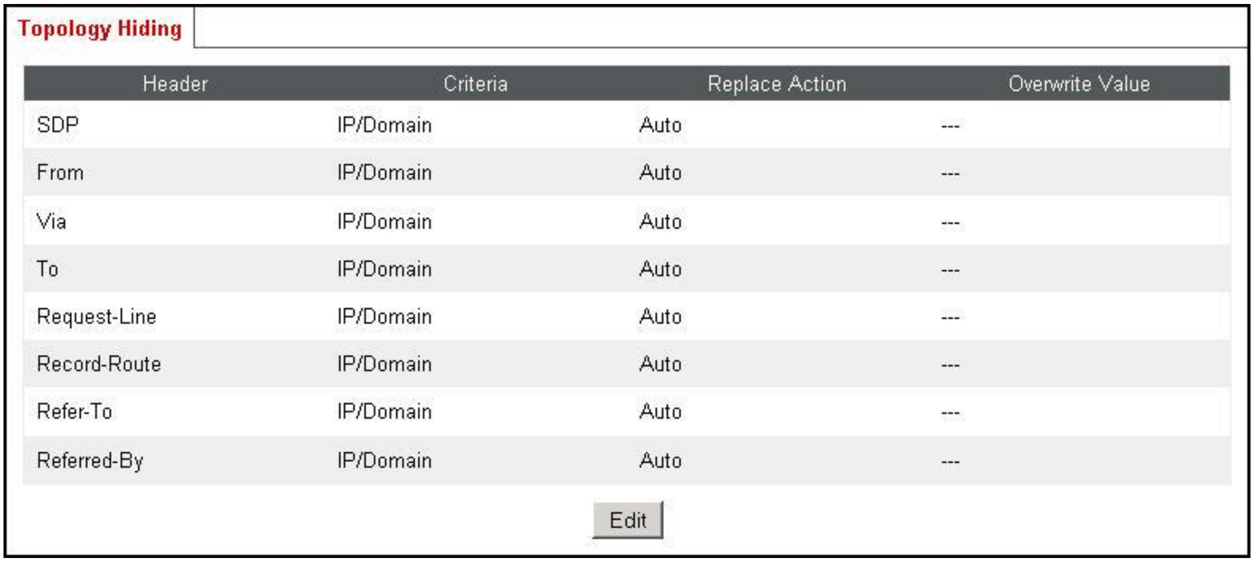


Header	Criteria	Replace Action	Overwrite Value
SDP	IP/Domain	Auto	---
From	IP/Domain	Overwrite	avaya.com
Via	IP/Domain	Auto	---
To	IP/Domain	Overwrite	avaya.com
Request-Line	IP/Domain	Overwrite	avaya.com
Record-Route	IP/Domain	Auto	---
Refer-To	IP/Domain	Auto	---
Referred-By	IP/Domain	Auto	---

7.13.2. Topology Hiding – Cox Communications

For the compliance test, topology hiding profile **SP-General** was created for Cox Communications. This profile will be applied to traffic from the Avaya SBCE to Cox Communications. When creating the profile, configure the parameters as follows:

- Set **Header** to the header whose host part of the URI is to be modified.
- Set **Criteria** to **IP/Domain** to indicate that the host part should be modified if it is an IP address or a domain.
- Set **Replace Action** to **Auto** for all headers.

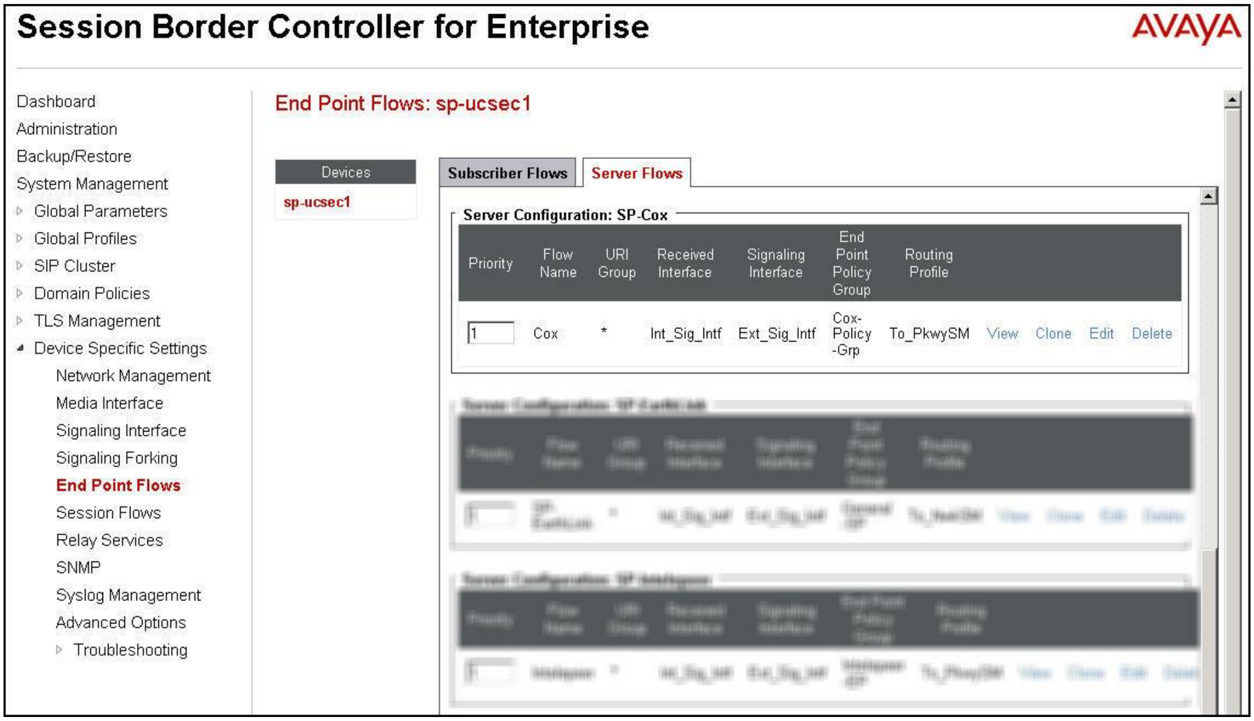


Header	Criteria	Replace Action	Overwrite Value
SDP	IP/Domain	Auto	---
From	IP/Domain	Auto	---
Via	IP/Domain	Auto	---
To	IP/Domain	Auto	---
Request-Line	IP/Domain	Auto	---
Record-Route	IP/Domain	Auto	---
Refer-To	IP/Domain	Auto	---
Referred-By	IP/Domain	Auto	---

7.14. End Point Flows

Endpoint flows are used to determine the signaling endpoints involved in a call in order to apply the appropriate policies. When a packet arrives at the Avaya SBCE, the content of the packet (IP addresses, URIs, etc.,) is used to determine which flow it matches. Once the flow is determined, the flow points to policies and profiles which control processing, privileges, authentication, routing, etc. Once routing is applied and the destination endpoint is determined, the policies for the destination endpoint are applied. Thus, two flows are involved in every call: the source endpoint flow and the destination endpoint flow. In the case of the compliance test, the signaling endpoints are Session Manager and the service provider SIP server.

To create a new flow for a server endpoint, navigate to **Device Specific Settings → End Point Flows** in the left pane. In the center pane, select the Avaya SBCE device (**sp-ucsec1**) to be managed. In the right pane, select the **Server Flows** tab and click the **Add** button. A pop-up window (not shown) will appear requesting the name of the new flow and the flow parameters. Once complete, the settings are shown in the far right pane.



End Point Flows: sp-ucsec1

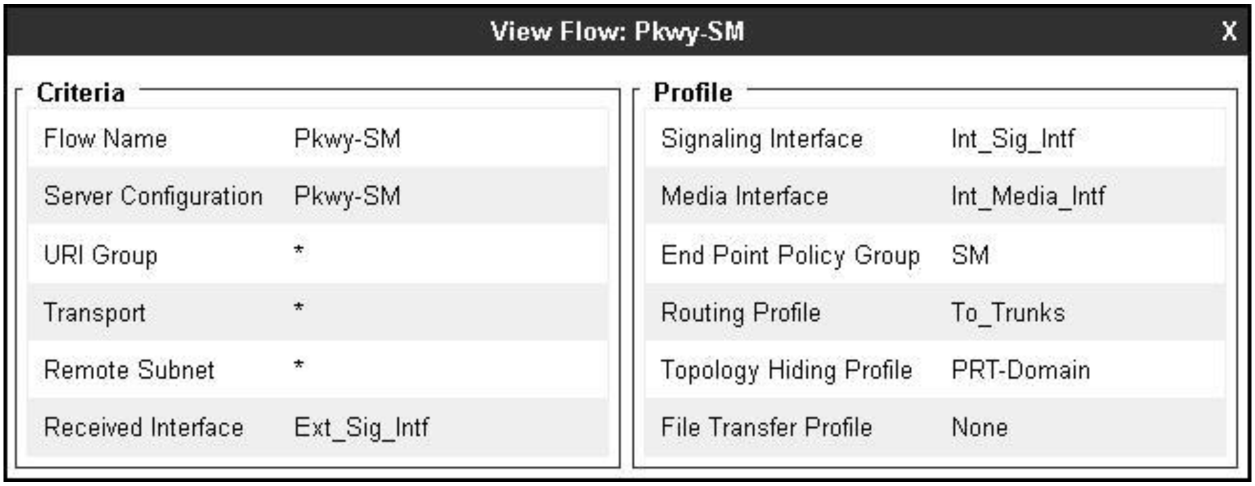
Server Configuration: SP-Cox

Priority	Flow Name	URI Group	Received Interface	Signaling Interface	End Point Policy Group	Routing Profile				
1	Cox	*	Int_Sig_Intf	Ext_Sig_Intf	Cox-Policy-Grp	To_PkwySM	View	Clone	Edit	Delete

7.14.1. End Point Flow – Session Manager

For the compliance test, endpoint flow **Pkwy-SM** was created for Session Manager. All traffic from Session Manager will match this flow as the source flow and use the specified **Routing Profile** to determine the destination server and corresponding destination flow. The **End Point Policy** and **Topology Hiding Profile** will be applied as appropriate. When creating the flow, configure the parameters as follows:

- For the **Flow Name**, enter a descriptive name.
- For **Server Configuration**, select the Session Manager server created in **Section 7.7.1**.
- To match all traffic, set the **URI Group**, **Transport**, and **Remote Subnet** to *****.
- Set **Received Interface** to the external signaling interface.
- Set **Signaling Interface** to the internal signaling interface.
- Set **Media Interface** to the internal media interface.
- Set the **End Point Policy Group** to the endpoint policy group defined for Session Manager in **Section 7.11.1**.
- Set the **Routing Profile** to the routing profile defined in **Section 7.12.2** used to direct traffic to the Cox Communications SIP server.
- Set the **Topology Hiding Profile** to the topology hiding profile defined for Session Manager in **Section 7.13.1**.



View Flow: Pkwy-SM

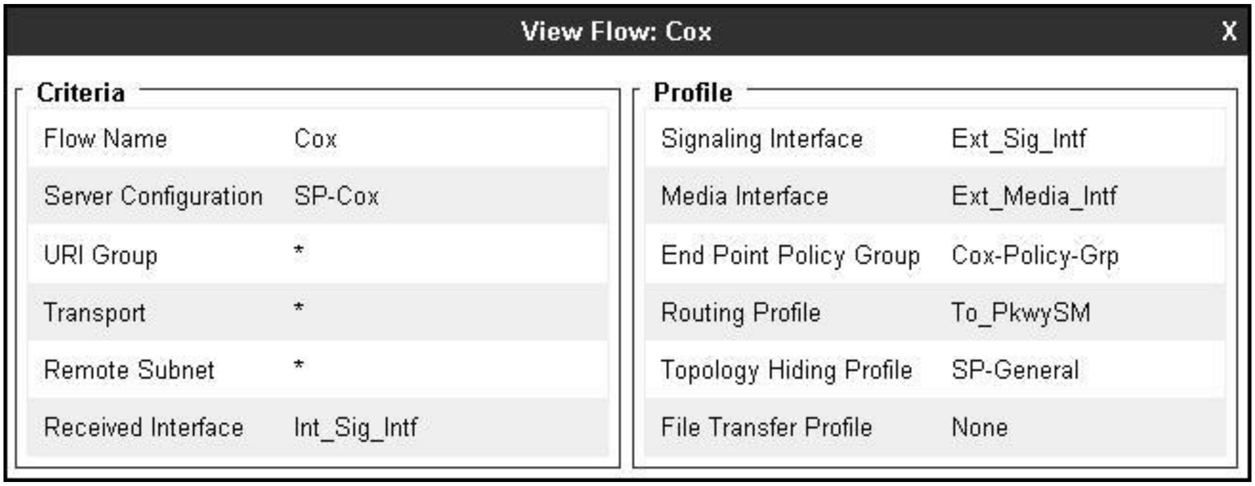
Criteria	
Flow Name	Pkwy-SM
Server Configuration	Pkwy-SM
URI Group	*
Transport	*
Remote Subnet	*
Received Interface	Ext_Sig_Intf

Profile	
Signaling Interface	Int_Sig_Intf
Media Interface	Int_Media_Intf
End Point Policy Group	SM
Routing Profile	To_Trunks
Topology Hiding Profile	PRT-Domain
File Transfer Profile	None

7.14.2. End Point Flow – Cox Communications

For the compliance test, endpoint flow **Cox** was created for the Cox Communications SIP server. All traffic from Cox Communications will match this flow as the source flow and use the specified **Routing Profile** to determine the destination server and corresponding destination flow. The **End Point Policy** and **Topology Hiding Profile** will be applied as appropriate. When creating the flow, configure the parameters as follows:

- For the **Flow Name**, enter a descriptive name.
- For **Server Configuration**, select the Cox Communications SIP server created in **Section 7.7.2**.
- To match all traffic, set the **URI Group**, **Transport**, and **Remote Subnet** to *.
- Set **Received Interface** to the internal signaling interface.
- Set **Signaling Interface** to the external signaling interface.
- Set **Media Interface** to the external media interface.
- Set **End Point Policy Group** to the endpoint policy group defined for Cox Communications in **Section 7.11.2**.
- Set **Routing Profile** to the routing profile defined in **Section 7.12.1** used to direct traffic to Session Manager.
- Set the **Topology Hiding Profile** to the topology hiding profile defined for Cox Communications in **Section 7.13.2**.



Criteria

Flow Name	Cox
Server Configuration	SP-Cox
URI Group	*
Transport	*
Remote Subnet	*
Received Interface	Int_Sig_Intf

Profile

Signaling Interface	Ext_Sig_Intf
Media Interface	Ext_Media_Intf
End Point Policy Group	Cox-Policy-Grp
Routing Profile	To_PkwySM
Topology Hiding Profile	SP-General
File Transfer Profile	None

8. Cox Communications SIP Trunking Service Configuration

Cox Communications is responsible for the configuration of its SIP Trunking Service including the network configuration and deployment/management of the on-site EdgeMarc 4550 WAN access router.

Cox Communications will require that the customer provide the public IP address and port number used to reach the on-site EdgeMarc at the edge of the enterprise as well as the internal IP address to be associated with the LAN port on the EdgeMarc. Cox Communications will provide Direct Inward Dialed (DID) numbers assigned to the enterprise. This information is used to complete the Communication Manager, Session Manager and the Avaya SBCE configuration discussed in the previous sections.

9. Verification Steps

This section provides verification steps that may be performed in the field to verify that the solution is configured properly. This section also provides a list of useful troubleshooting commands that can be used to troubleshoot the solution.

Verification Steps:

1. Verify that endpoints at the enterprise site can place calls to the PSTN and that the call remains active for more than 35 seconds. This time period is included to verify that proper routing of the SIP messaging has satisfied SIP protocol timers.
2. Verify that endpoints at the enterprise site can receive calls from the PSTN and that the call can remain active for more than 35 seconds.
3. Verify that the user on the PSTN can end an active call by hanging up.
4. Verify that an endpoint at the enterprise site can end an active call by hanging up.

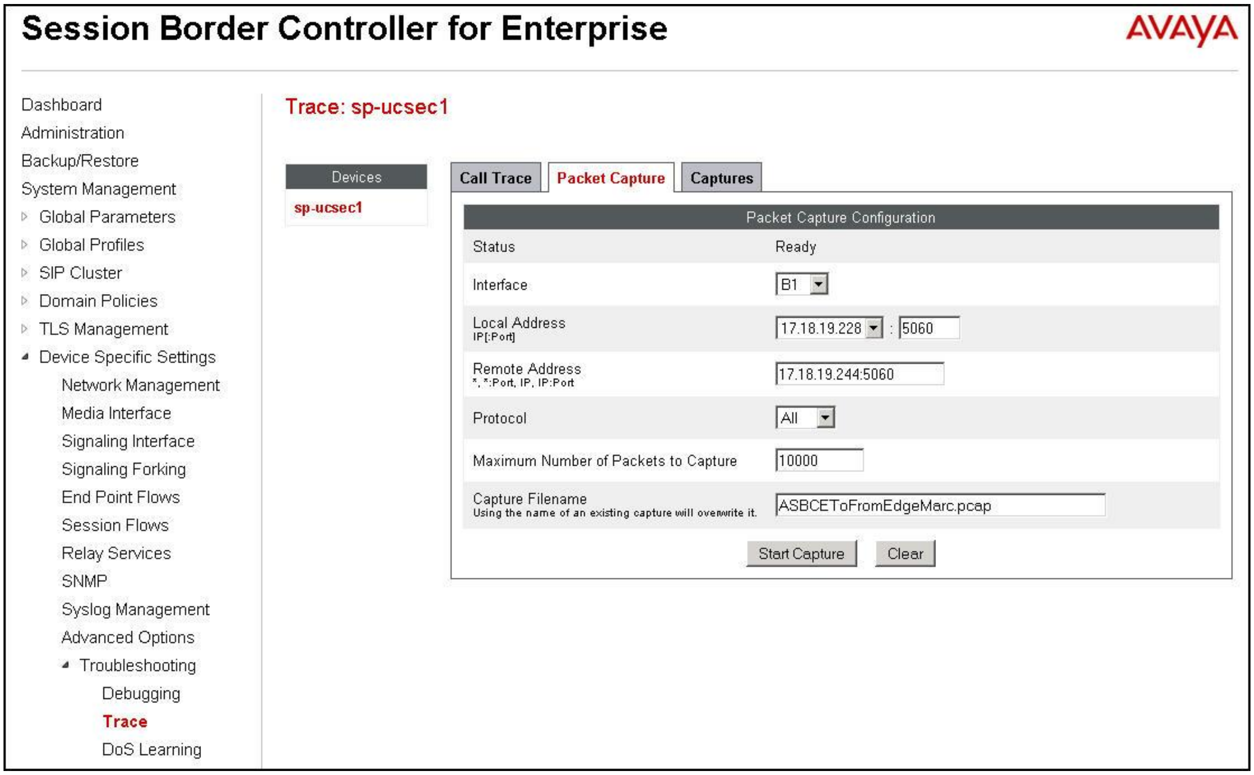
Troubleshooting:

1. Communication Manager:
   - **list trace station** <extension number> - Traces calls to and from a specific station.
   - **list trace tac** <trunk access code number> - Trace calls over a specific trunk group.
   - **status station** <extension number> - Displays signaling and media information for an active call on a specific station.
   - **status trunk** <trunk group number> - Displays trunk group information.
   - **status trunk** <trunk group number/channel number> - Displays signaling and media information for an active trunk channel.

2. Session Manager:
   - **Call Routing Test** - The Call Routing Test verifies the routing for a particular source and destination. To run the routing test, navigate to **Elements → Session Manager → System Tools → Call Routing Test**. Enter the requested data to run the test.

3. The Avaya SBCE:
   The Avaya SBCE can take internal traces on specified interfaces. SIP signaling crossing both interfaces A1 and B1 can be captured for troubleshooting. In the Avaya SBCE web interface, navigate to **Device Specific Settings → Troubleshooting → Trace** to invoke this facility. In the **Packet Capture** tab, select or supply the relevant information (e.g., A1 or B1 or any interfaces, IP/port, protocol, number of packets to capture, capture file name, etc.), then press the **Start Capture** button start the trace. The captured trace file can then be downloaded from the **Captures** tab for examination using a protocol sniffer application such as Wireshark.

   The screen below shows the setup for capturing packets between the public interface of the Avaya SBCE (**B1**) and the on-site EdgeMarc 4550 (**17.18.19.244:5060**).



Status	Ready
Interface	B1
Local Address IP[:Port]	17.18.19.228 : 5060
Remote Address *, *:Port, IP, IP:Port	17.18.19.244:5060
Protocol	All
Maximum Number of Packets to Capture	10000
Capture Filename Using the name of an existing capture will overwrite it.	ASBCEToFromEdgeMarc.pcap

10. Conclusion

These Application Notes describe the configuration necessary to connect Avaya Aura® Communication Manager 6.3, Avaya Aura® Session Manager 6.3 and Avaya Session Border Controller for Enterprise 6.2 to the Cox Communications SIP Trunking Service via an on-site EdgeMarc 4550 router managed by Cox Communications. The Cox Communications SIP Trunking Service provides businesses a flexible, cost-saving alternative to traditional hardwired telephony trunks. Please refer to **Section 2.2** for any exceptions or workarounds.

11. References

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

Avaya Aura® System Platform

[1] *Installing and Configuring Avaya Aura® System Platform*, Release 6.3.4, Issue 2, July 2014.
[2] *Administering Avaya Aura® System Platform*, Release 6.3.4, Issue 2, July 2014.
[3] *Upgrading Avaya Aura® System Manager*, Release 6.3.4, Issue 2, July 2014.

Avaya Aura® Session Manager/System Manager

[4] *Deploying Avaya Aura® Session Manager*, Release 6.3, Issue 5, September 2014.
[5] *Administering Avaya Aura® Session Manager,* Release 6.3, Issue 7, September 2014.
[6] *Deploying Avaya Aura® System Manager on System Platform*, Release 6.3, Issue 4, June 2014.
[7] *Administering Avaya Aura® System Manager for Release 6.3.8*, Release 6.3, August 2014.

Avaya Aura® Communication Manager

[8] *Administering Avaya Aura® Communication Manager*, Release 6.3, Issue 10, June 2014, Document Number 03-300509.
[9] *Programming Call Vectoring Features in Avaya Aura® Call Center Elite*, Release 6.3.6, June 2014.

Avaya Endpoints

[10] *Avaya 1600 Series IP Deskphones Administrator Guide*, Release 1.3.3, Issue 4, April 2013, Document Number 16-601443.
[11] *Administering Avaya IP Deskphone H.323 9608, 9611G, 9621G, and 9641G*, Release 6.3.1, Issue 17, January 2014, Document Number 16-300698.
[12] *Administering Avaya one-X® Deskphone SIP for 9601, 9608, 9611G, 9621G, and 9641G* Release 6.2.2, Issue 2, April 2013, Document Number 16-601944.
[13] *Avaya 1140E IP Deskphone with SIP Software on Avaya Aura® User Guide*, Release 4.4, November 2013, Document Number 16-604274.
[14] Using the Avaya A175 Desktop Video Device with the Avaya Flare® Experience, Document ID 16-603733, Issue 2, December 2011.
[15] *Administering Avaya one-X® Communicator*, July 2013.
[16] *Using Avaya Flare® Experience for Windows*, Release 1.1, Issue 2, Feburary 2013, Document Number 18-604158.

Avaya Session Border Controller for Enterprise

[1] *Administering Avaya Session Border Controller for Enterprise*, Release 6.2, Issue 3, June 2014.
[2] *Avaya Session Border Controller for Enterprise Overview and Specification*, Issue 2, December 2013

Internet Engineering Task Force (IETF®) SIP RFC

[1] RFC 3261 *SIP: Session Initiation Protocol*, http://www.ietf.org/
[2] RFC 2833 *RTP Payload for DTMF Digits, Telephony Tones and Telephony Signals*, http://www.ietf.org/

Product documentation for the Cox SIP Trunking Service is available from Cox Communications.

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 DevConnect Program at devconnect@avaya.com.