Avaya Solution & Interoperability Test Lab

Application Notes for Configuring the M-net Premium SIP Trunk Service with Avaya Aura® Communication Manager Evolution Server 6.3, Avaya Aura® Session Manager 6.3 and Avaya Session Border Controller for Enterprise 7.0 – Issue 1.0

Abstract

These Application Notes describe the steps to configure Session Initiation Protocol (SIP) Trunking between the M-net Premium SIP Trunk 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 and various Avaya endpoints. M-net is a member of the Avaya DevConnect Service Provider program.

Readers should pay attention to **Section 2**, in particular the scope of testing as outlined in **Section 2.1** as well as the observations noted in **Section 2.2**, to ensure that their own use cases are adequately covered by this scope and results.

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 M-net Premium SIP Trunk 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 and various Avaya endpoints. In addition, Avaya Aura® System Manager 6.3 is used to configure Avaya Aura® Session Manager.

Customers using this Avaya SIP-enabled enterprise solution with the M-net Premium SIP Trunk 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 M-net Premium SIP Trunk Service via a broadband connection and exercise the features and functionality listed in **Section 2.1**. The simulated enterprise site was comprised of Communication Manager, Session Manager and Avaya Session Border Controller for Enterprise (Avaya SBCE).

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 for 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.

- Registration of the SIP Trunk with the service provider
- Sending and receiving SIP OPTIONS queries to the service provider
- Inbound and outbound PSTN calls (via the SIP trunk) to/from SIP and H.323 telephones at the enterprise
- Inbound and outbound PSTN calls to/from Avaya one-X® Communicator (soft client) using multiple protocols (H.323 and SIP) and multiple modes (Local Computer and Other Phone mode)
- Inbound and outbound PSTN calls to/from Avaya Communicator for Windows
- Various call types including: local, long distance, international, outbound toll-free, and local directory assistance
- Codecs G.711A and G.729A
- 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 forwarding and mobility (Extension to cellular – EC500)
- G.711 Fax
- Network Call Redirection using REFER and a 302 response
- Remote Worker

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

The following item is not supported:
- T.38 Fax

2.2. Test Results

Interoperability testing of the M-net Premium SIP Trunk Service was completed with successful results for all test cases with the exception of the observations and/or limitations described below.

- **Cut-through times on outbound calls** – During the testing, cut-through times varied widely from 6 – 30 seconds depending on the back-end carrier that the call was routed to from M-net to the PSTN. Testing was conducted using international trunks between Germany (M-net) and the United States (Avaya). These delays are believed to be a function of these trunks as oppose to indicating an interoperability issue between M-net and Avaya.
- **Call forward call display** – Inbound calls from the PSTN to the enterprise which are then call forwarded to another PSTN endpoint, show an incorrect caller ID display at the destination. The destination show the enterprise account DDI instead of the originating PSTN caller DDI. The Avaya SBCE was used to modify the PAI and Contact headers at the request of M-net but without success. Even though these changes did not have the desired effect, they are believed to be correct for interoperability and are retained in the configuration.
- **Mismatch codec on inbound call** – If an inbound call from the PSTN to the enterprise contains only codecs that are not supported by the enterprise, then the enterprise will return a "488 Not Acceptable Here" response. M-net converts this SIP error message to a SS7 error message and sends it to the PSTN carrier. This should cause some error indication (e.g., fast busy) to be presented to the PSTN caller. However, during the testing no error indication was provided and the call was silently dropped. This issue is not critical since it should only occur if the enterprise and/or M-net have misconfigured codecs.
- **G.711 fax failures** – G.711 fax calls from the PSTN to the enterprise (inbound) routinely failed or had significant errors. Outbound faxes worked more reliably. Communication Manager does not officially support G.711 fax on SIP trunks so there is no guarantee as to its success. Only T.38 fax is officially supported on SIP trunks by Communication Manager, but T.38 fax is not supported by M-net. G.711 fax usually works if there is minimal delay or jitter so a customer may use G.711 fax at their own risk. It is assumed that the international trunks used for testing had too much delay for reliable fax transmission.

- **One digit detected as two** – A call is established from the enterprise to a PSTN destination that requires user input (e.g., a voicemail system). When data is entered, a single digit entered by the user may be detected by the far-end as 2 digits (e.g., 8 is detected as 88, etc.) even though the correct digits were passed from the enterprise to M-net. This behavior was intermittent and usually a second attempt at entering the data was successful. This occurred with various types of enterprise users (local and remote). During troubleshooting, M-net determined that the root cause was a problem on the trunk to a specific PSTN carrier. M-net raised a trouble ticket with the carrier to resolve the issue. Thus, this problem is not an interoperability issue between M-net and Avaya.
- **Call transfer with REFER** – When the SIP REFER method was used for call transfer of an active PSTN call to another PSTN destination, then after the transfer was complete, unnecessary messaging (in the form of BYE message retransmissions) continued between the enterprise and M-net. The retransmissions from the enterprise continued until a timeout was reached. This behavior did not impact the call and the call was successful.
- **Vector redirect with REFER** – Inbound PSTN calls to a Communication Manager vector which are redirected by the vector to another PSTN destination fail. Communication Manager performs the redirection by sending a SIP REFER message to M-net with the new destination in the Refer-To header. The expectation is that M-net will initiate a new connection to the number in the Refer-To header. However, after the REFER message is sent, M-net sends a NOTIFY message containing 503 Service Unavailable and the call is not redirected.

2.3. Support

For technical support on the M-net Premium SIP Trunk Service, please contact M-net at www.m-net.de.

Avaya customers may obtain documentation and support for Avaya products by visiting http://support.avaya.com. Alternatively, in the United States, (866) GO-AVAYA (866-462-8292) provides access to overall sales and service support menus.

3. Reference Configuration

Figure 1 illustrates a sample Avaya SIP-enabled enterprise solution connected to the M-net Premium SIP Trunk Service.

The components used to create the simulated customer site included:

- System Manager
- Session Manager
- Communication Manager
- Avaya G450 Media Gateway
- Avaya Session Border Controller for Enterprise
- Avaya 1600 Series IP Deskphones (H.323)
- Avaya 9600 Series IP Deskphones (H.323 and SIP)
- Avaya one-X® Communicator (H.323 and SIP)
- Avaya Communicator for Windows

Located at the edge of the enterprise is the Avaya SBCE. It has a public side that connects to the external network and a private side that 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 this document. Similarly, any references to real routable PSTN numbers have been masked so as not to display PSTN routable numbers.

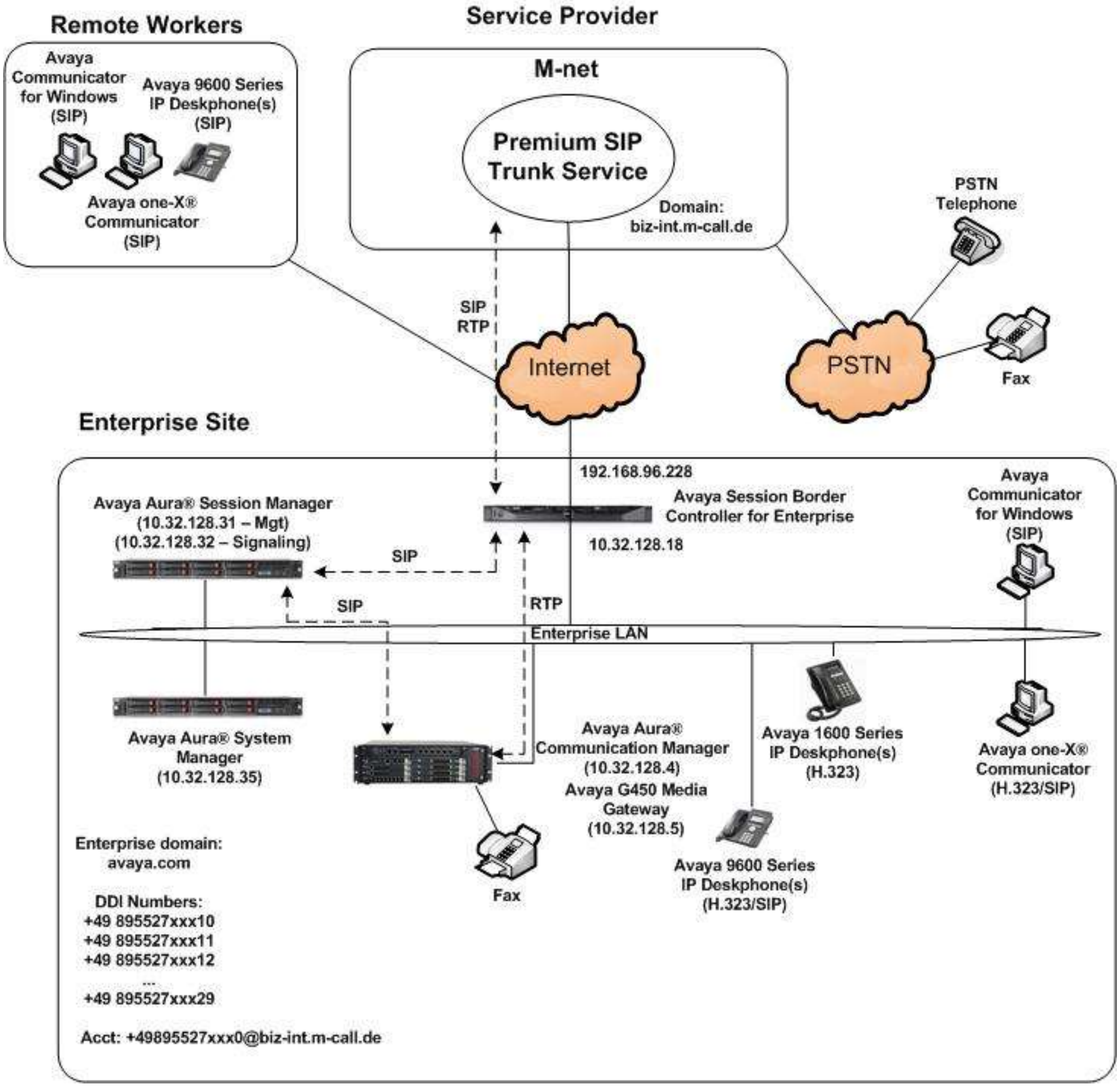

Remote Workers
Avaya Communicator for Windows (SIP)
Avaya 9600 Series IP Deskphone(s) (SIP)
Avaya one-X® Communicator (SIP)
Service Provider
M-net
Premium SIP Trunk Service
Domain: biz-int.m-call.de
PSTN Telephone
SIP
RTP
Internet
PSTN
Fax
Enterprise Site
192.168.96.228
Avaya Aura® Session Manager
(10.32.128.31 – Mgt)
(10.32.128.32 – Signaling)
Avaya Session Border Controller for Enterprise
10.32.128.18
Avaya Communicator for Windows (SIP)
SIP
SIP
RTP
Enterprise LAN
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 one-X® Communicator (H.323/SIP)
Fax
Avaya 9600 Series IP Deskphone(s) (H.323/SIP)
Enterprise domain: avaya.com
DDI Numbers:
+49 895527xxx10
+49 895527xxx11
+49 895527xxx12
...
+49 895527xxx29
Acct: +49895527xxx0@biz-int.m-call.de

Figure 1: Avaya Compliance Test Configuration

A separate 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 and 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 features 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 M-net Premium SIP Trunk Service.

M-net is a German service provider and requires the Request URI and To headers to contain the destination party in one of the following formats: local (e.g., 452xx0), national (e.g., 089452xx0) or international (e.g., 004989452xx0). The From, PAI, and Contact headers must contain the full DDI number in international format with a leading + sign (e.g., +498946226xxx10).

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 a HP ProLiant DL360 G7 Server	6.3 SP16 (Software Update Revision 6.3.16.13.4210) System Platform 6.3.7.0.05001
Avaya Aura® Session Manager running on a HP ProLiant DL360 G7 Server	6.3 SP16 (Build 6.3.16.0.631601)
Avaya Aura® Communication Manager running on an Avaya S8300 Server	6.3 SP13 (R016x.03.0.124.0-22619) System Platform 6.3.7.0.05001
Avaya G450 Media Gateway	36.16.0
Avaya Session Border Controller for Enterprise	7.0 (7.0.0-21-6602)
Avaya 1616 IP Deskphone (H.323) running Avaya one-X® Deskphone Value Edition	1.3 SP5 (1.3.50B)
Avaya 9641G IP Deskphone (H.323) running Avaya one-X® Deskphone Edition	6.6.0 (6.6029U)
Avaya 9611G IP Deskphone (SIP) running Avaya one-X® Deskphone SIP Edition	7.0.0 (7.0.0.39)
Avaya one-X® Communicator (H.323 or SIP)	6.2 SP10 (Build 6.2.10.03-FP10)
Avaya Communicator for Windows	2.1.2.75
M-net Premium SIP Trunk Service Components	
Equipment/Software	Release/Version
Oracle Acme Packet Net-Net SD 4500 Session Border Controller (SBC)	SCX6.4
Nokia Siemens Networks HiQ4200 Telephone Application Server (TAS)	R14
Nokia Siemens Networks CFX5000 IP Multimedia Subsystem (IMS)	IMS 7.2

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 M-net Premium SIP Trunk Service. A SIP trunk is established between Communication Manager and Session Manager for use by traffic to and from M-net. It is assumed the general installation of Communication Manager, the 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 and phone numbers shown throughout these Application Notes have been edited so that the actual public IP addresses of the network elements and public PSTN numbers 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 **70** 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  70
  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 transfer 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. To configure the codecs, enter the codecs in the **Audio Codec** column of the table in the order of preference defined by the service provider. For the compliance test, codec set 3 was configured with codecs G.711A and G.729A. Default values can be used for all other fields.

```
change ip-codec-set 3                                          Page   1 of   2

                          IP Codec Set

    Codec Set: 3

    Audio        Silence      Frames   Packet
    Codec        Suppression  Per Pkt  Size(ms)
 1: G.711A           n          2        20
 2: G.729A           n          2        20
 3:
```

M-net does not support T.38 fax. Thus, on **Page 2**, set the **FAX Mode** to **off**.

```
change ip-codec-set 3                                          Page   2 of   2

                          IP CODEC SET

                              Allow Direct-IP Multimedia? n
                                                                   Packet
                          Mode                   Redundancy        Size(ms)
    FAX                   off                     0           ECM: y
    Modem                 off                     0
    TDD/TTY               US                      3
    H.323 Clear-channel   n                       0
```

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 3 was chosen for the service provider trunk. Use the **change ip-network-region 3** command to configure region 3 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 3                                      Page   1 of  20
                               IP NETWORK REGION
  Region: 3
Location:         Authoritative Domain: avaya.com
    Name: SP Region              Stub Network Region: n
MEDIA PARAMETERS                 Intra-region IP-IP Direct Audio: yes
      Codec Set: 3               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 3 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 3 will be used for calls between region 3 (the service provider region) and region 1 (the rest of the enterprise). Creating this table entry for IP network region 3 will automatically create a complementary table entry on the IP network region 1 form for destination region 3. 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 3                                     Page   4 of  20

 Source Region: 3     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    3     y    NoLimit                                            n       t
 2
 3    3                                                               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 3 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, some of 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 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 the service provider. As a result, any signaling group or trunk group settings (**Section 5.6** and **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 **5063**.

- 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 the **DTMF over IP** field to **rtp-payload**. This value enables Communication Manager to send DTMF transmissions using RFC 2833.
- 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 from the Avaya Media Gateway and allow it to flow directly between the SIP trunk and the enterprise endpoint.
- Set the **Alternate Route Timer** to **30**. 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. This value was set to 30 to accommodate some carriers used by M-net which had long cut-through times. See **Section 2.2** for details.
- Default values may be used for all other fields.

```
add signaling-group 3                                           Page   1 of   3
                                SIGNALING GROUP

 Group Number: 3              Group Type: sip
  IMS Enabled? n        Transport Method: tls
        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
Alert Incoming SIP Crisis Calls? n
   Near-end Node Name: procr                 Far-end Node Name: sessionMgr
 Near-end Listen Port: 5063                Far-end Listen Port: 5063
                                        Far-end Network Region: 3

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): 30
```

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 3 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 shown in the previous section.
- 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 3                                             Page   1 of  21
                                TRUNK GROUP

Group Number: 3                   Group Type: sip           CDR Reports: y
  Group Name: SP Trunk                   COR: 1        TN: 1        TAC: 1003
   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: 3
                                                    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 (in milliseconds) should be equal to the time interval defined by 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 **900** seconds was used.

```
add trunk-group 3                                               Page   2 of  21
      Group Type: sip

TRUNK PARAMETERS

     Unicode Name: auto

                                            Redirect On OPTIM Failure: 30000

            SCCAN? n                                   Digital Loss Group: 18
                      Preferred Minimum Session Refresh Interval(sec): 900

 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 **public**. This field specifies the format of the calling party number (CPN) sent to the far-end. Public numbers are automatically preceded with a + sign (E.164 numbering format) when passed in the SIP From, Contact and P-Asserted Identity headers.

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 3                                                 Page   3 of  21
TRUNK FEATURES
          ACA Assignment? n            Measured: none
                                                          Maintenance Tests? y


                     Numbering Format: public
                                                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 **Network Call Redirection** field may be set to **y** or **n**. Setting the **Network Call Redirection** flag to **y** enables use of the SIP REFER message for call transfer; otherwise the SIP INVITE message will be used for call transfer. Both approaches are supported with this solution. However, be aware of the observation described in **Section 2.2** when using REFER with vectors.

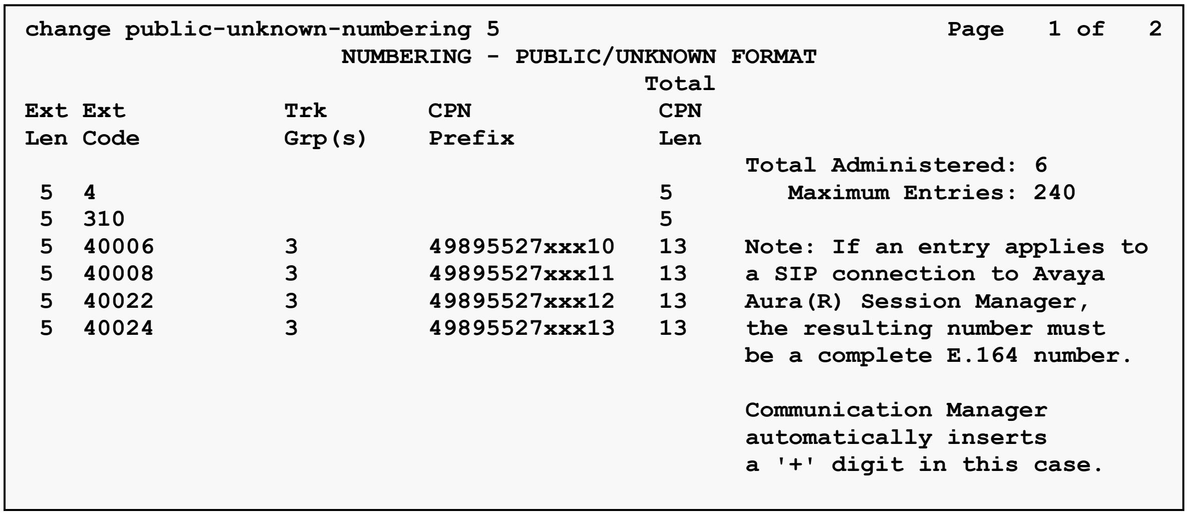
Set the **Send Diversion Header** field to **y** and the **Support Request History** field to **n**. The **Send Diversion Header** field provides additional information to the network if the call has been redirected. M-net does not directly support the Diversion header; however, the contents of this header will be used by the Avaya SBCE to modify the PAI and Contact headers for M-net. These header modifications are needed to support the call display for call forwarding of inbound calls back to the PSTN and some Extension to Cellular (EC500) call scenarios. See **Section 2.2** for details and **Section 7.6.1** for the Avaya SBCE configuration.

```
add trunk-group 3                                                 Page   4 of  21
                              PROTOCOL VARIATIONS

                                       Mark Users as Phone? n
Prepend '+' to Calling/Alerting/Diverting/Connected Number? n
                       Send Transferring Party Information? n
                                  Network Call Redirection? y
          Build Refer-To URI of REFER From Contact For NCR? n
                                     Send Diversion Header? y
                                   Support Request History? n
                              Telephone Event Payload Type:


                        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

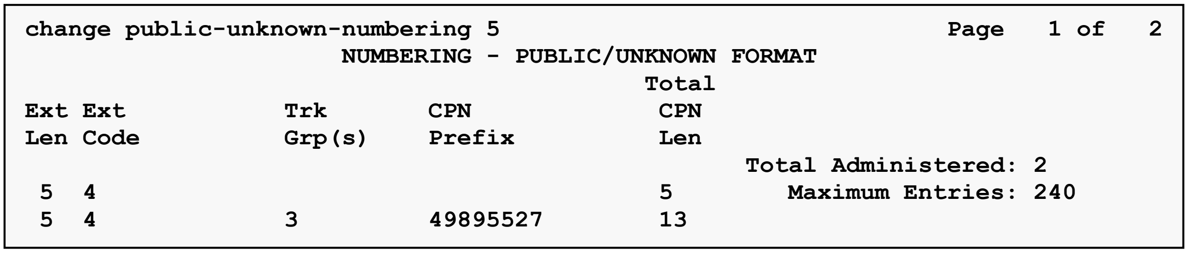
The calling party number is sent in the SIP “From”, “Contact” and “PAI” headers. Use the **change public-unknown-numbering** command to create an entry for each extension which has a DDI assigned. The DDI number will be assigned by the SIP service provider. It is used to authenticate the caller.

In the sample configuration, the first four DDI numbers provided for testing were assigned to the four extensions 40006, 40008, 40022, and 40024. Thus, these same DDI numbers were used in the outbound calling party information on the service provider trunk when calls were originated from these extensions. In the screenshot below, part of the DDIs are replaced with xxx for security reasons. However, the full DDI was entered on the form during testing.



```
change public-unknown-numbering 5                               Page   1 of   2
                      NUMBERING - PUBLIC/UNKNOWN FORMAT
                                           Total
Ext Ext            Trk       CPN            CPN
Len Code           Grp(s)    Prefix         Len
                                                 Total Administered: 6
 5  4                                       5       Maximum Entries: 240
 5  310                                     5
 5  40006          3         49895527xxx10  13   Note: If an entry applies to
 5  40008          3         49895527xxx11  13   a SIP connection to Avaya
 5  40022          3         49895527xxx12  13   Aura(R) Session Manager,
 5  40024          3         49895527xxx13  13   the resulting number must
                                                 be a complete E.164 number.

                                                 Communication Manager
                                                 automatically inserts
                                                 a '+' digit in this case.
```

In a real customer environment, normally the DDI number is comprised of the local extension plus a prefix. If this is true, then a single public numbering entry can be applied for all extensions. In the example below, all stations with a 5-digit extension beginning with 4 will send the calling party number as the **CPN Prefix** plus the extension number.



```
change public-unknown-numbering 5                               Page   1 of   2
                      NUMBERING - PUBLIC/UNKNOWN FORMAT
                                           Total
Ext Ext            Trk       CPN            CPN
Len Code           Grp(s)    Prefix         Len
                                                 Total Administered: 2
 5  4                                       5       Maximum Entries: 240
 5  4              3         49895527       13
```

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 **2** 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
    00                    10   18     2       intl         n
    0895527               12   12     2       natl         n
    1183                  4    4      2       svcl         n
```

The route pattern defines which trunk group will be used for an outgoing 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 2 during 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 **3** 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.
- **LAR**: **next**

```
change route-pattern 2                                          Page   1 of   3
                    Pattern Number: 4   Pattern Name: 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: 3    0                                                            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                                         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
```

Use the **save translation** command to save all Communication Manager configuration described in **Section 5**.

6. Configure Avaya Aura® Session Manager

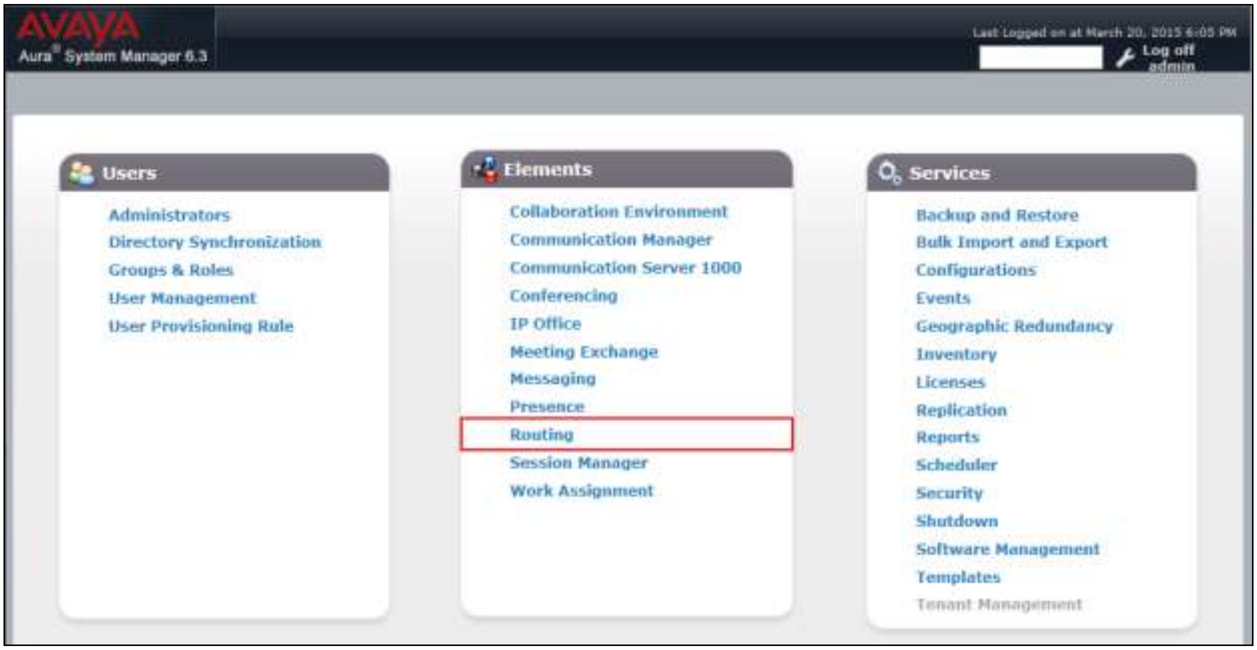
This section provides the procedures for configuring Session Manager. The procedures include configuring the following items:

- SIP Domain
- Location
- Adaptation Modules
- SIP Entities
- Entity Links
- Routing Policies
- Dial Patterns
- Session Manager

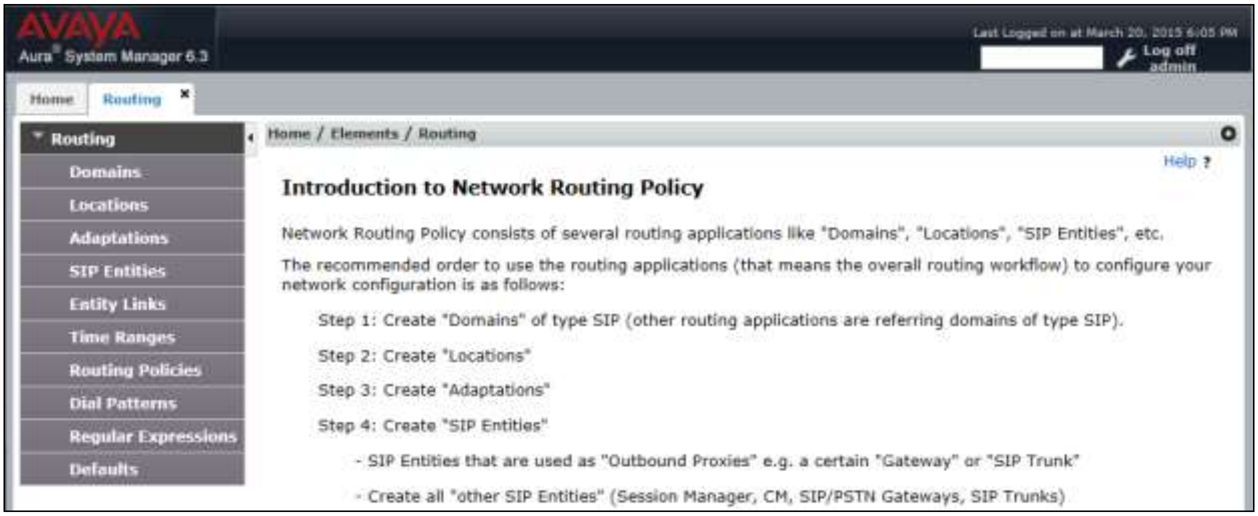
It may not be necessary to create all the items above when creating a connection to the service provider since some of these items would have already been defined as part of the initial Session Manager installation. This includes items such as certain SIP Domains, Locations, SIP Entities, and Session 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 and click on **Login** (not shown). The following 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"

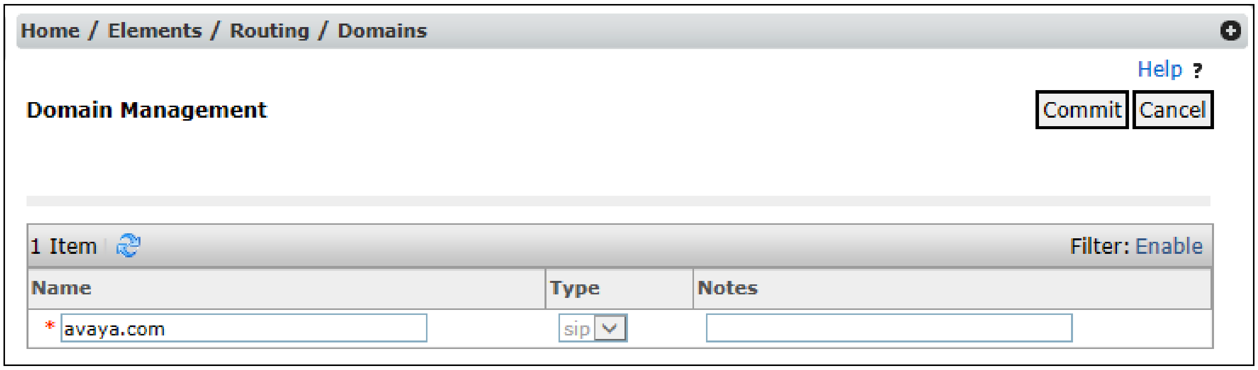
- SIP Entities that are used as "Outbound Proxies" e.g. a certain "Gateway" or "SIP Trunk"
- Create all "other SIP Entities" (Session Manager, CM, SIP/PSTN Gateways, SIP Trunks)

6.2. Specify SIP Domain

Create a SIP Domain for each domain for which Session Manager will need to be aware in order to route calls. For the compliance test, this includes the enterprise domain (**avaya.com**) as defined in **Section 5.5**. 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**. The screen below shows the entry for the enterprise domain.



Name	Type	Notes
* avaya.com	sip	

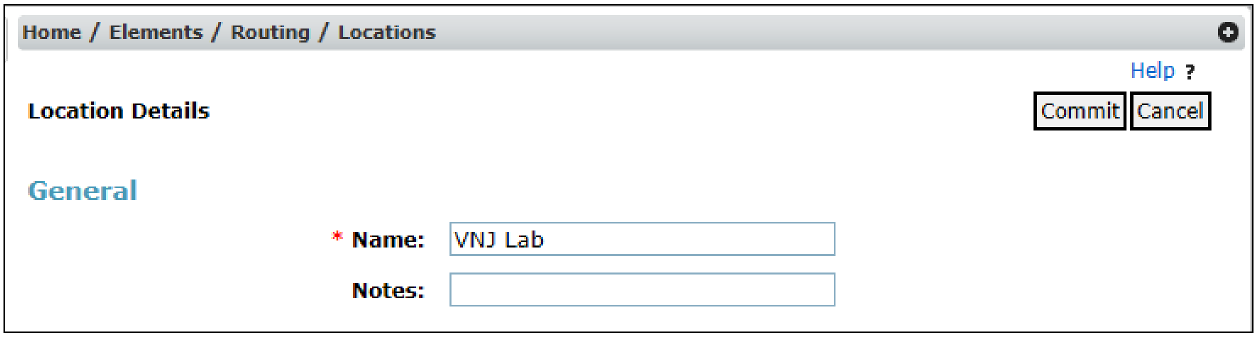
6.3. Add Location

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 at 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

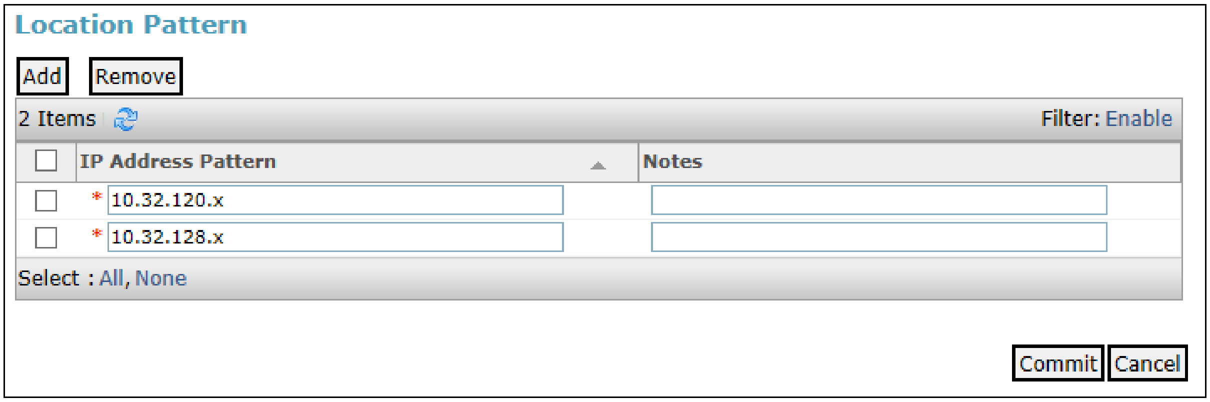
* Name: VNJ Lab

Notes:

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

2 Items

☐	IP Address Pattern	Notes
☐	* 10.32.120.x	
☐	* 10.32.128.x	

6.4. Add Adaptation

Session Manager can be configured with Adaptations that can modify SIP messages before or after routing decisions have been made or perform digit manipulation. The Adaptation **DigitConversionAdapter** supports digit conversion of telephone numbers in specific headers of SIP messages.

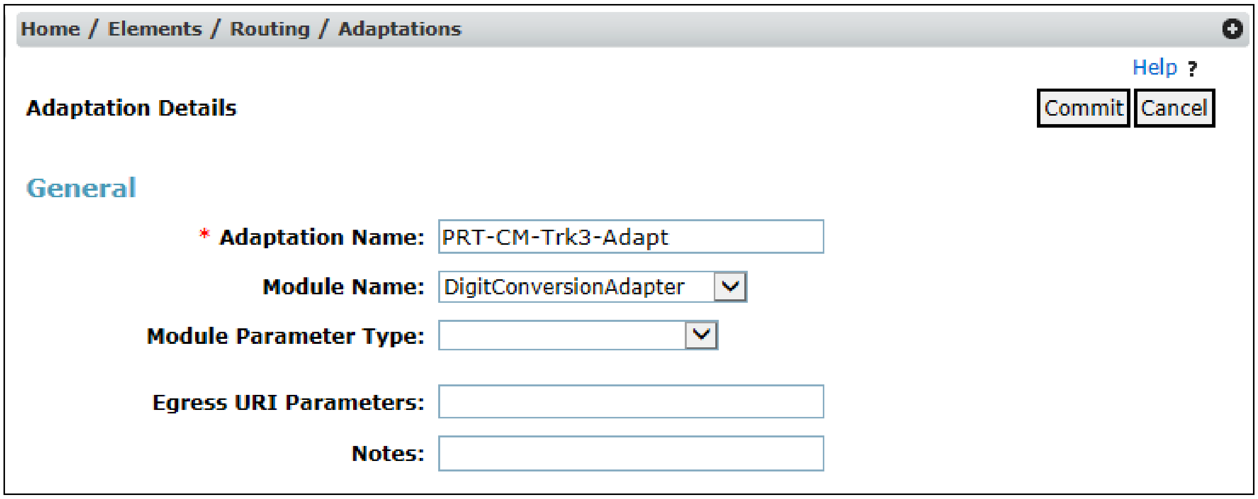
For the compliance test, one Adaptation was used. This Adaptation is applied to the Communication Manager SIP Entity and performs the following:

- Mapping inbound DDI numbers from M-net 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 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:	Select **DigitConversionAdapter** from the drop-down menu.
Module Parameter Type:	Leave blank.
Notes:	Enter a description (optional).



Adaptation Details

General

* Adaptation Name: PRT-CM-Trk3-Adapt

Module Name: DigitConversionAdapter

Module Parameter Type:

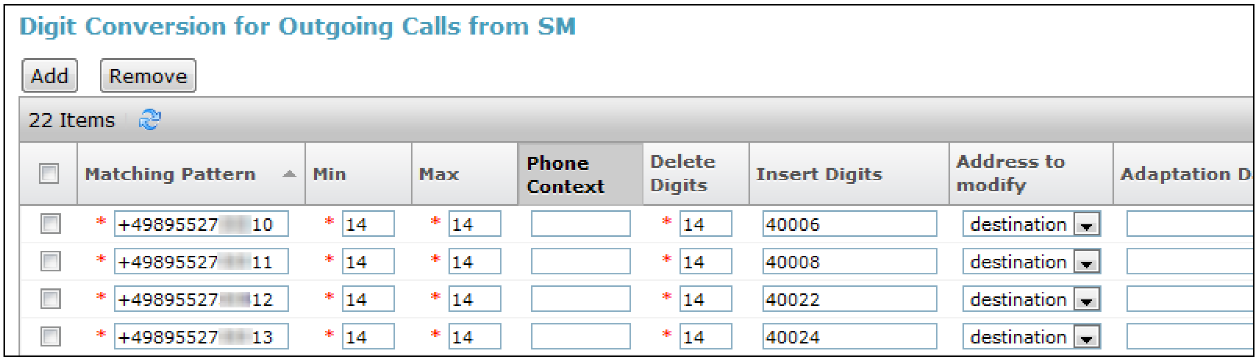
Egress URI Parameters:

Notes:

To map inbound DDI numbers from M-net to Communication Manager extensions, scroll down to the **Digit Conversion for Outgoing Calls from SM** section. Create an entry for each DDI 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 DDI 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 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.

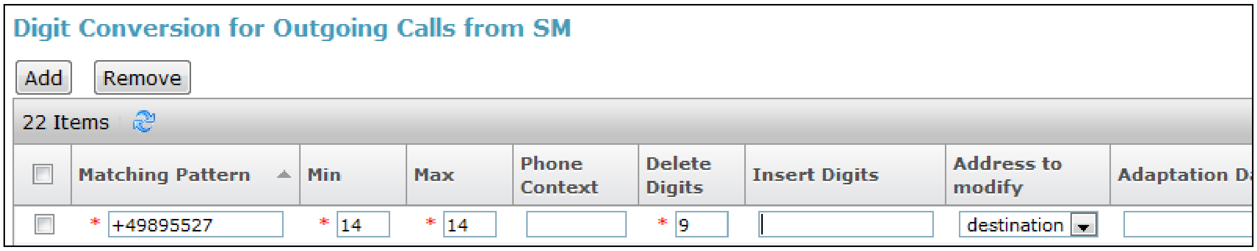
Click **Commit** to save.



Digit Conversion for Outgoing Calls from SM

☐	Matching Pattern	Min	Max	Phone Context	Delete Digits	Insert Digits	Address to modify	Adaptation D
☐	* +49895527[redacted]10	* 14	* 14		* 14	40006	destination	
☐	* +49895527[redacted]11	* 14	* 14		* 14	40008	destination	
☐	* +49895527[redacted]12	* 14	* 14		* 14	40022	destination	
☐	* +49895527[redacted]13	* 14	* 14		* 14	40024	destination	

In a real customer environment, often the DDI 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 9 digit prefix is deleted from each incoming DDI 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 D
☐	* +49895527	* 14	* 14		* 9		destination	

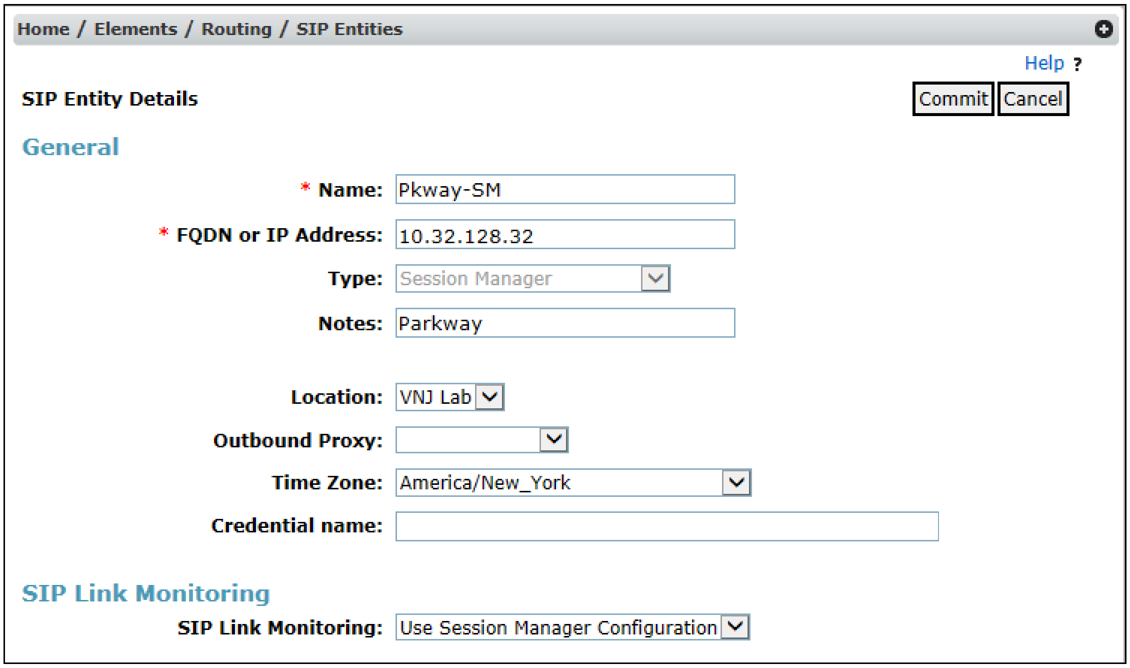
6.5. Add SIP Entity

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** created in **Section 6.3**.
- **Time Zone:**	Select the time zone for the Location above.

The following screen shows the addition of Session Manager. The IP address of the virtual SM-100 Security Module 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

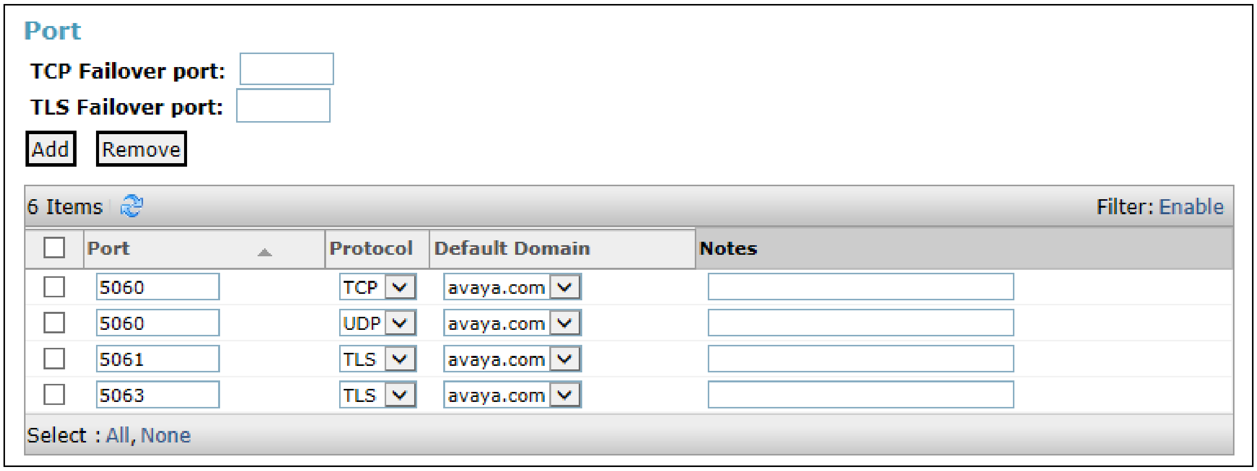
To define the ports used by Session Manager, scroll down to the **Port** section of the **SIP Entity Details** screen. This section is only present for **Session Manager** SIP Entities.

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

- **Port:** Port number on which 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. These ports were provisioned as part of the Session Manager installation not covered by this document. In addition, port 5063 defined in **Section 5.6** for use with service provider SIP traffic between Communication Manager and Session Manager was added to the list.



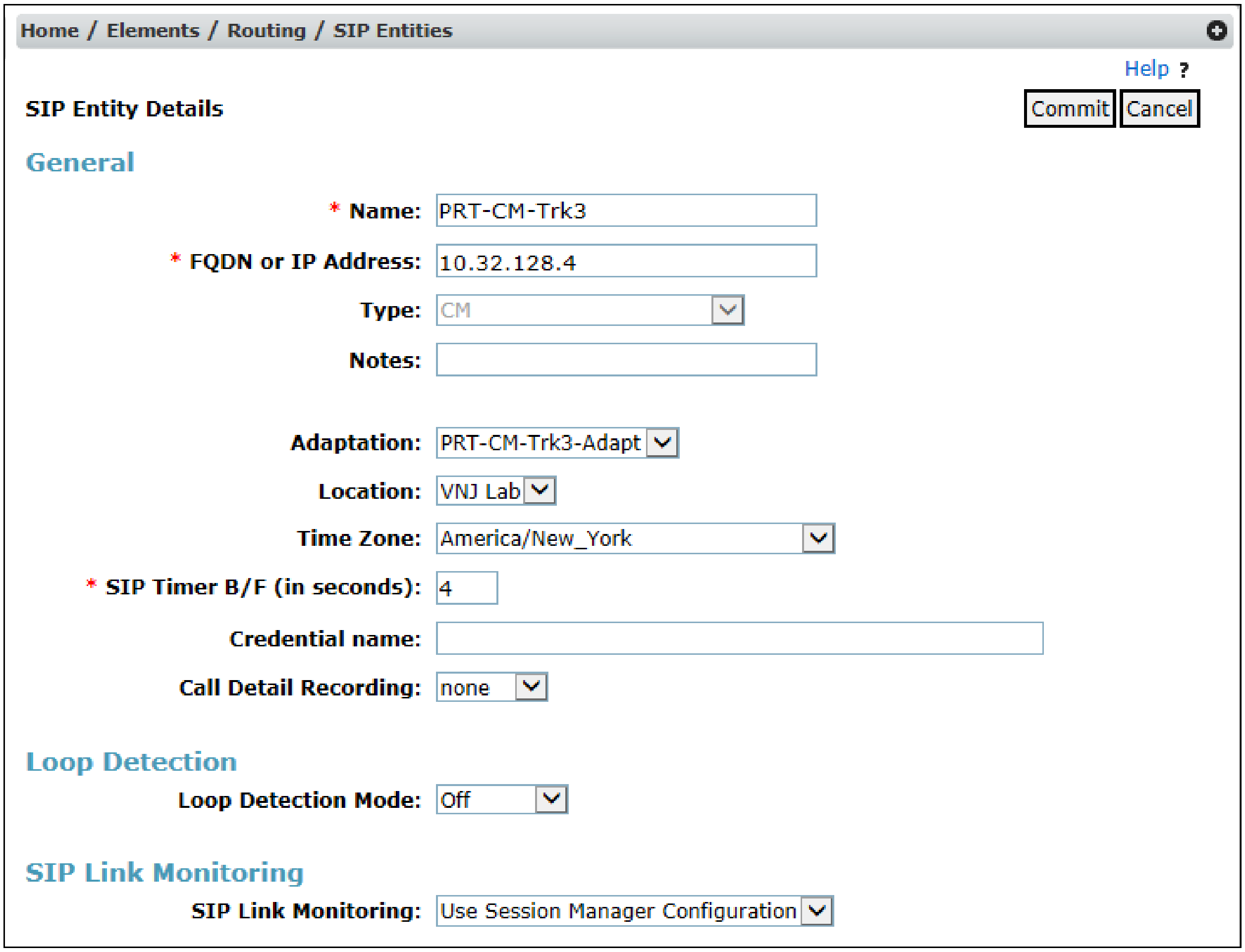
Port

TCP Failover port:

TLS Failover port:

☐	Port	Protocol	Default Domain	Notes
☐	5060	TCP	avaya.com	
☐	5060	UDP	avaya.com	
☐	5061	TLS	avaya.com	
☐	5063	TLS	avaya.com	

The following screen shows the addition of Communication Manager. Typically, when Session Manager is first installed, a SIP Entity and Entity Link is created for Communication Manager to carry intra-enterprise SIP traffic. In order for Session Manager to separate SIP service provider traffic on a separate Entity Link to Communication Manager, the creation of a second SIP Entity for Communication Manager is needed. The **FQDN or IP Address** field is set to the IP address of Communication Manager. For the **Adaptation** field, select the Adaptation previously defined for dial plan 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 (**Section 6.3**).



SIP Entity Details

General

* Name: PRT-CM-Trk3
* FQDN or IP Address: 10.32.128.4
Type: CM
Notes:
Adaptation: PRT-CM-Trk3-Adapt
Location: VNJ Lab
Time Zone: America/New_York
* SIP Timer B/F (in seconds): 4
Credential name:
Call Detail Recording: none

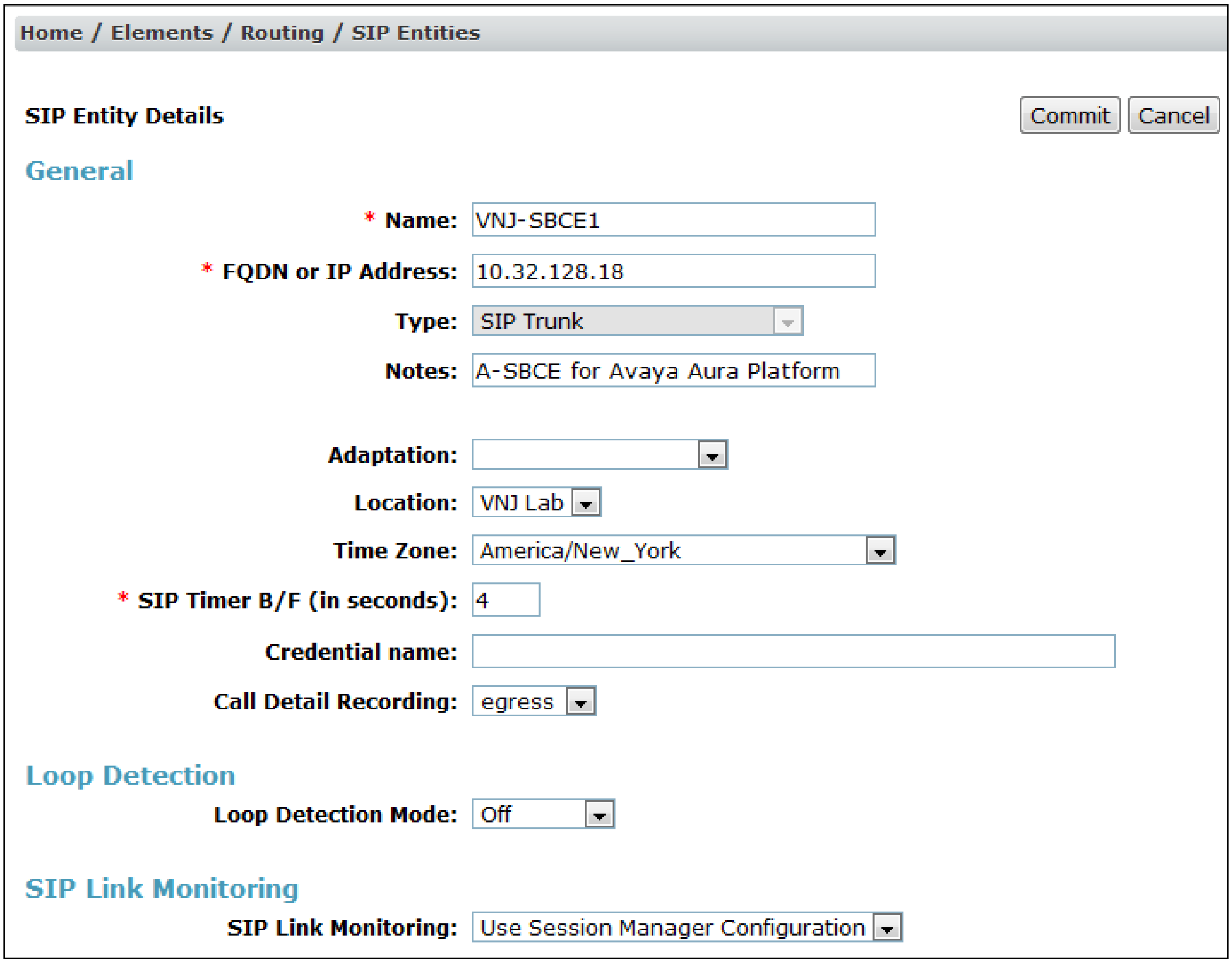
Loop Detection

Loop Detection Mode: Off

SIP Link Monitoring

SIP Link Monitoring: Use Session Manager Configuration

The following screen shows the addition of the Avaya SBCE. 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

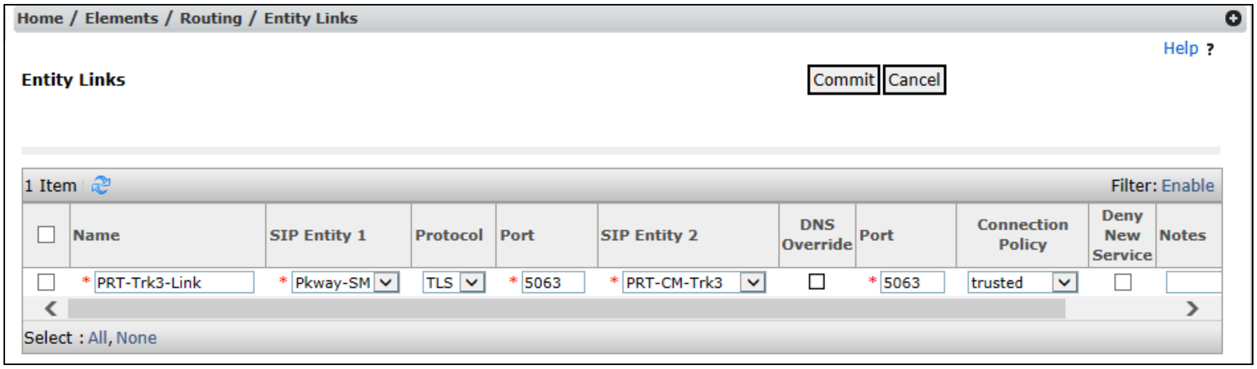
A SIP trunk between Session Manager and a telephony system is described by an Entity Link. Two Entity Links were created: one to Communication Manager for use only by service provider traffic and one to the Avaya SBCE. To add an Entity Link, navigate to **Routing → Entity Links** in the left-hand navigation 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 SIP Entity.
• **Protocol:**	Select the transport protocol used for this link.
• **Port:**	Port number on which Session Manager will receive SIP requests from the far-end.
• **SIP Entity 2:**	Select the name of the other system using the SIP Entity name defined in **Section 6.5**.
• **Port:**	Port number on which the other system receives SIP requests from Session Manager.
• **Connection Policy:**	Select **trusted** from pull-down menu.

Click **Commit** to save. The following screen illustrates the Entity Link to Communication Manager (**PRT-Trk3-Link**). The protocol and ports defined here must match the values used on the Communication Manager signaling group form in **Section 5.6**. Specifically, the following fields must match:

- **Protocol** must match the **Transport Method** from **Section 5.6**.
- SIP Entity 1 **Port** must match the **Far-end Listen Port** from **Section 5.6**.
- **SIP Entity 2** must match the SIP Entity defined for Communication Manager in **Section 6.5**.
- SIP Entity 2 **Port** must match the **Near-End Listen Port** from **Section 5.6**.

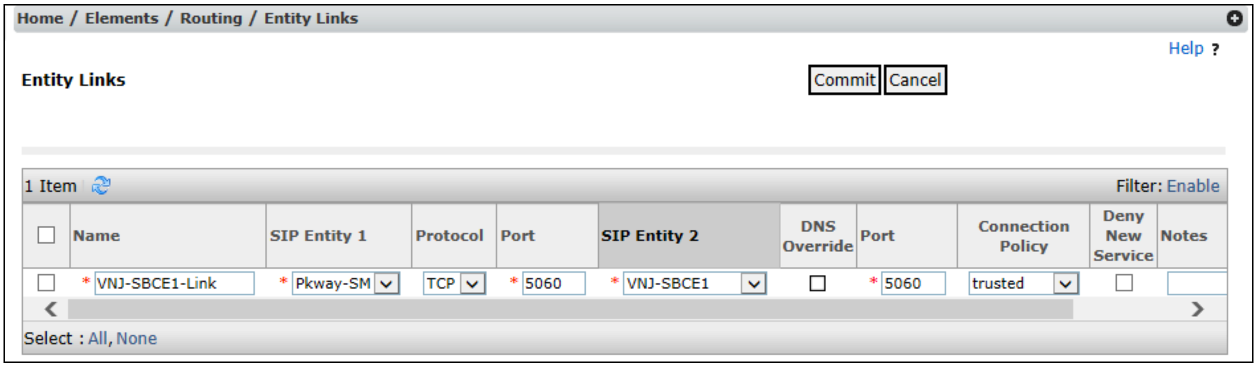
For part of the compliance test, the TCP protocol was used but the recommended configuration is to use TLS.



☐	Name	SIP Entity 1	Protocol	Port	SIP Entity 2	DNS Override	Port	Connection Policy	Deny New Service	Notes
☐	* PRT-Trk3-Link	* Pkway-SM	TLS	* 5063	* PRT-CM-Trk3	☐	* 5063	trusted	☐	

The following screen illustrates the Entity Link to the Avaya SBCE (**VNJ-SBCE1-Link**). The protocol and ports defined here must match the values used on the Avaya SBCE in **Section 7**. Specifically, the following fields must match:

- **Protocol** must match the protocol used by the Avaya SBCE Routing profile to reach Session Manager. This value is shown in the **Next Hop Address** in **Section 7.12.1**.
- SIP Entity 1 **Port** must match the port value used by the Avaya SBCE Routing profile to reach Session Manager. This value is shown in the **Next Hop Address** in **Section 7.12.1**.
- **SIP Entity 2** must match the SIP Entity defined for the Avaya SBCE in **Section 6.5**.
- SIP Entity 2 **Port** must match the port value defined in the Avaya SBCE internal signaling interface in **Section 7.3** for the selected protocol.



☐	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

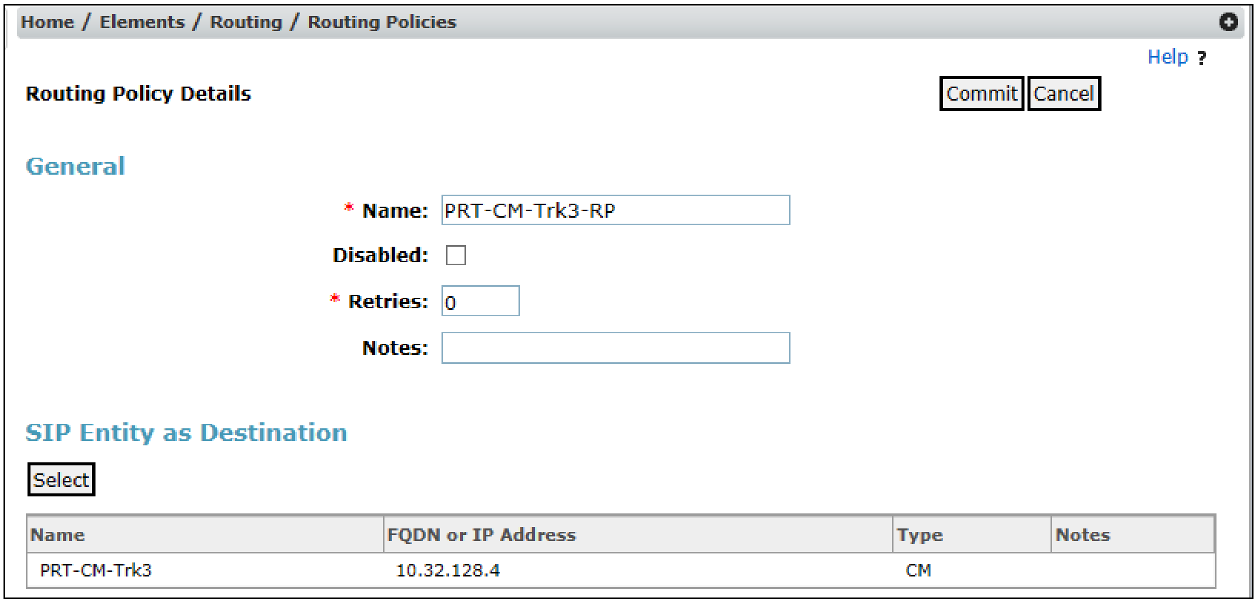
Routing Policies describe the conditions under which calls will be routed to the SIP Entities specified in **Section 6.5**. Two Routing Policies must be added: one for Communication Manager and one for the Avaya SBCE. To add a Routing Policy, navigate to **Routing → Routing Policies** in the left-hand 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-Trk3-RP

Disabled: ☐

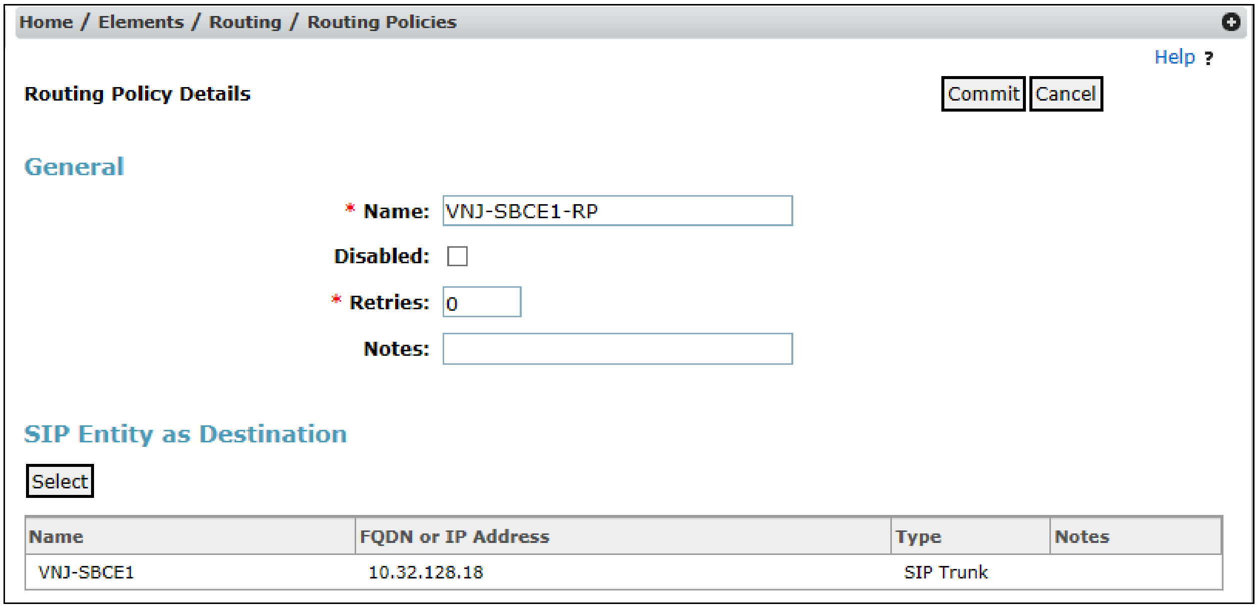
* Retries: 0

Notes:

SIP Entity as Destination

Name	FQDN or IP Address	Type	Notes
PRT-CM-Trk3	10.32.128.4	CM	

The following screen shows the Routing Policy for the Avaya SBCE.



Routing Policy Details

General

* Name: VNJ-SBCE1-RP

Disabled: ☐

* Retries: 0

Notes:

SIP Entity as Destination

Name	FQDN or IP Address	Type	Notes
VNJ-SBCE1	10.32.128.18	SIP Trunk	

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 M-net 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:

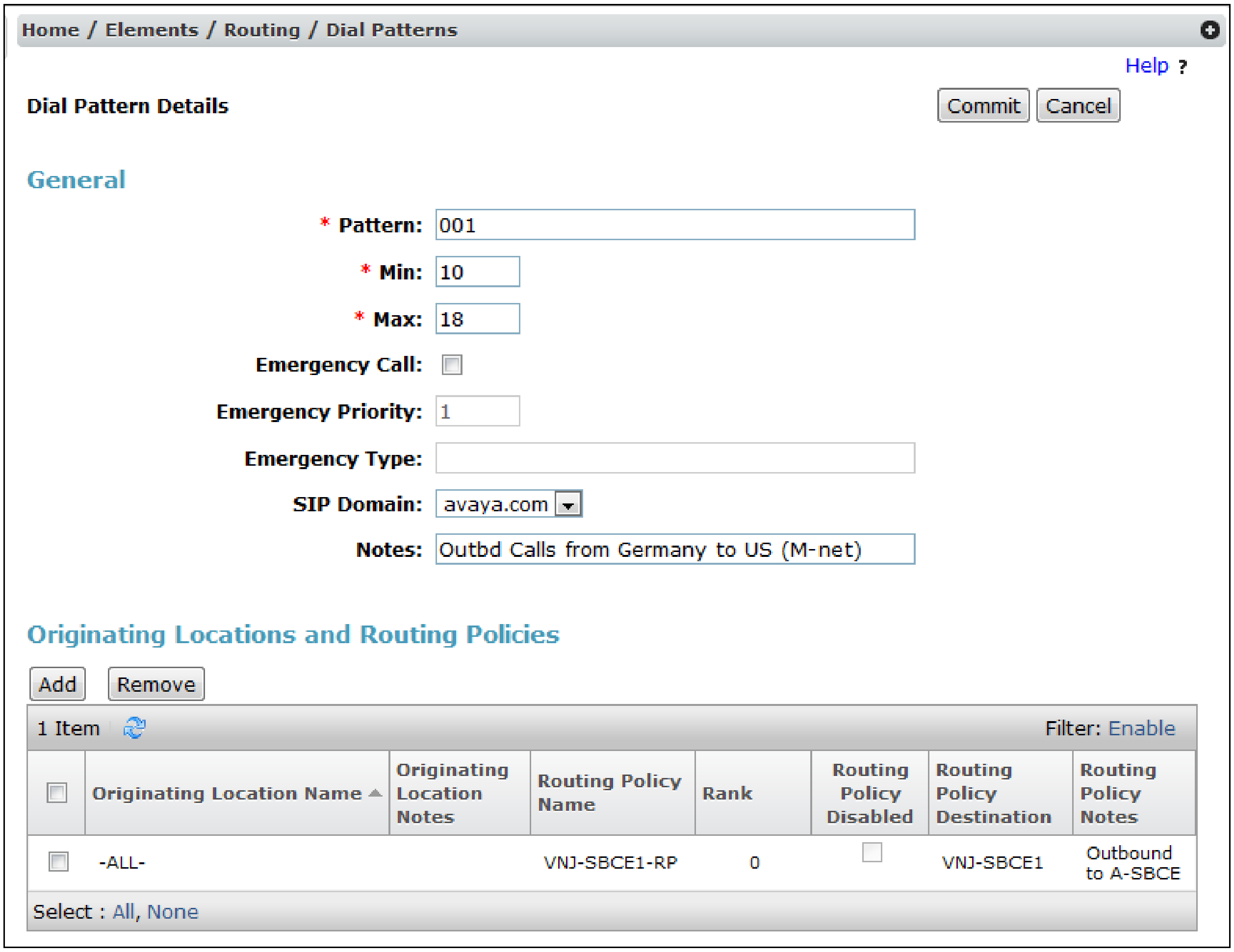
In the **General** section, enter the following values. Use default values for all remaining fields.

- **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.

Three examples of the Dial Patterns used for the compliance test are shown below. The first example shows that outbound international numbers (with between 10 - 18 digits) that begin with **001** and have a destination domain of **avaya.com** from **ALL** locations use route policy **VNJ-SBCE1-RP**.



Dial Pattern Details

General

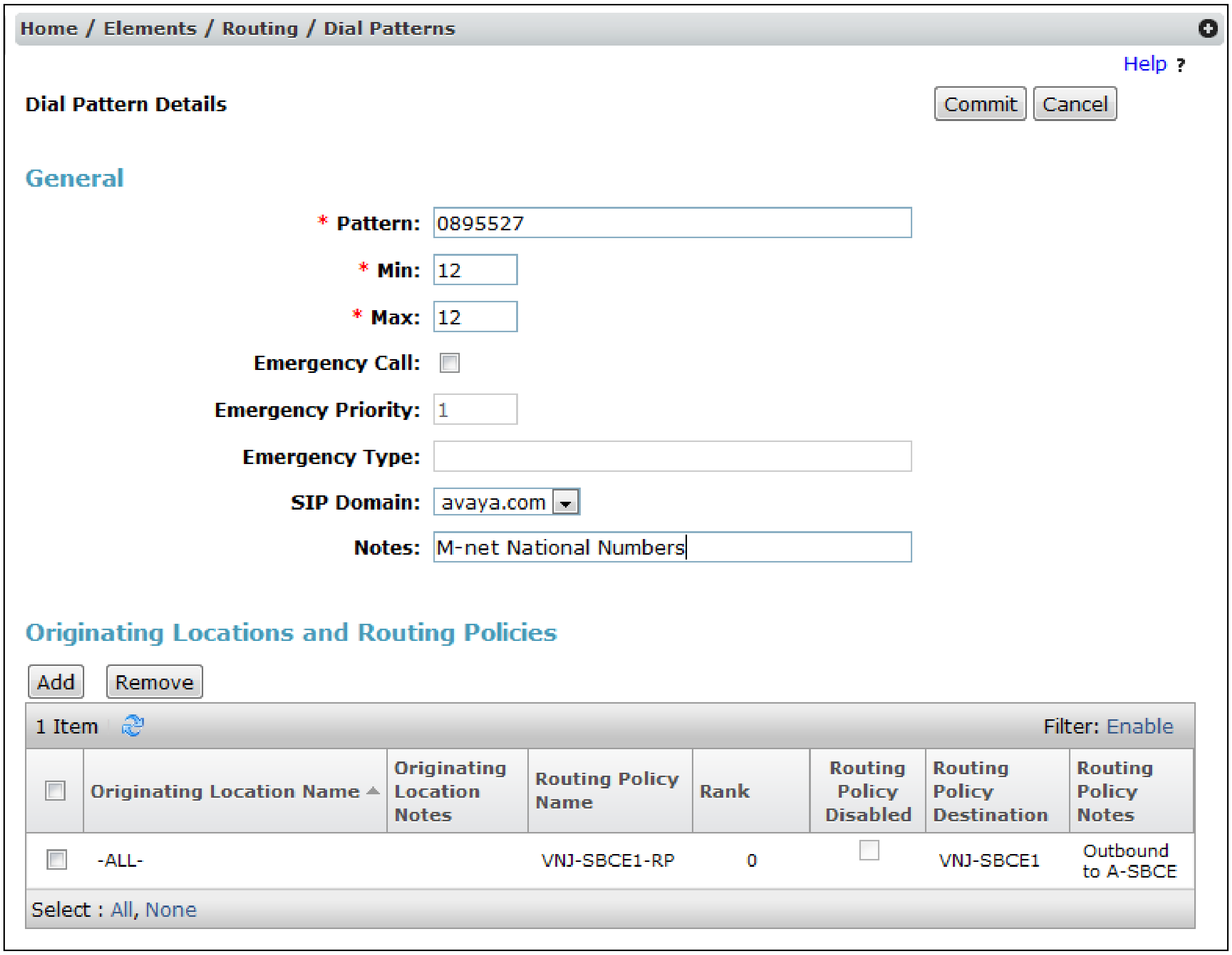
* Pattern:	001
* Min:	10
* Max:	18
Emergency Call:	☐
Emergency Priority:	1
Emergency Type:	
SIP Domain:	avaya.com
Notes:	Outbd Calls from Germany to US (M-net)

Originating Locations and Routing Policies

1 Item

☐	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

The second example shows that outbound national numbers that start with **08955527** to domain **avaya.com** and originating from **ALL** locations use route policy **VNJ-SBCE1-RP**.



Dial Pattern Details

General

* Pattern:	0895527
* Min:	12
* Max:	12
Emergency Call:	☐
Emergency Priority:	1
Emergency Type:	
SIP Domain:	avaya.com
Notes:	M-net National Numbers

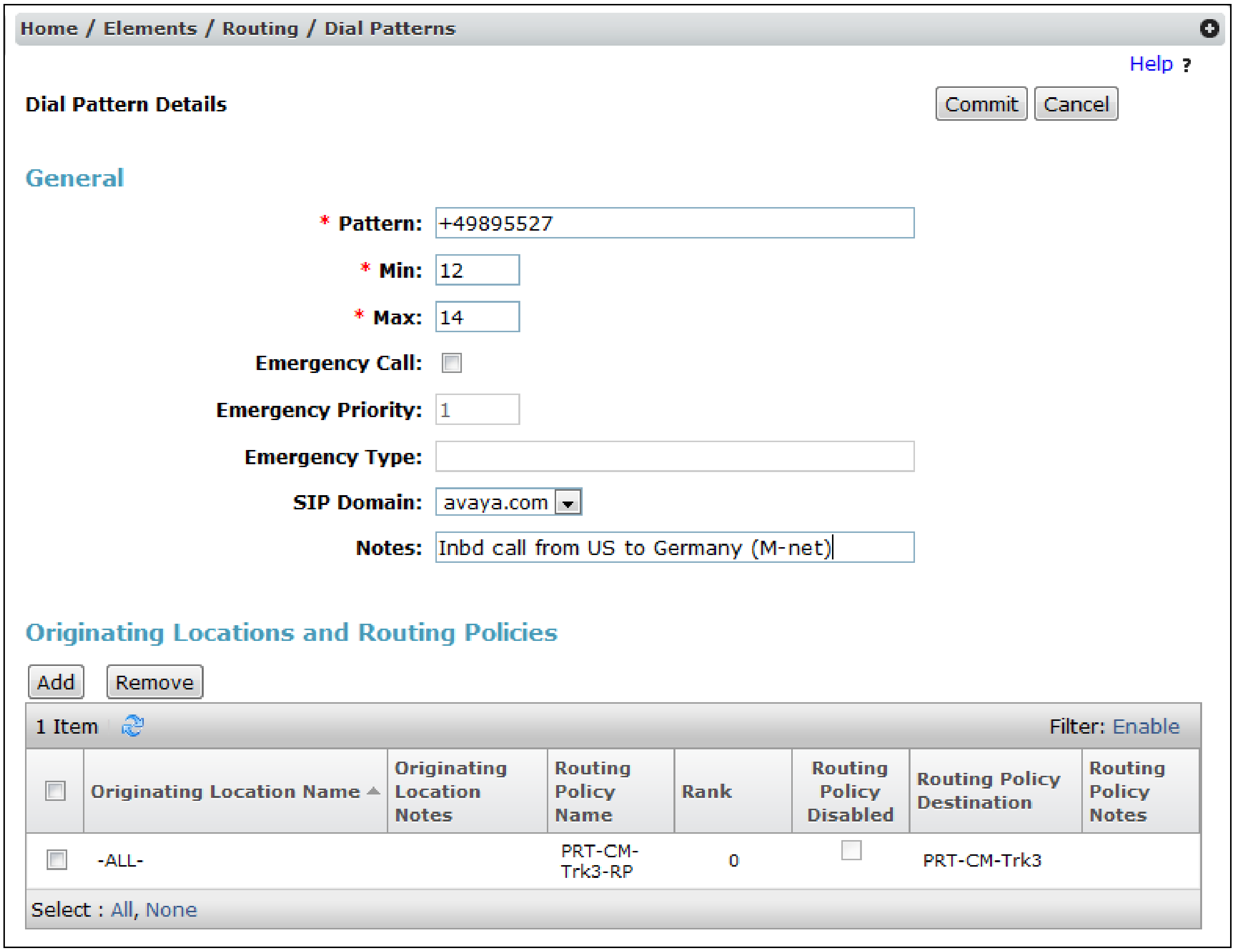
Originating Locations and Routing Policies

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 third example shows that incoming DDI numbers that start with +**49895527** to domain **avaya.com** and originating from **ALL** locations use route policy **PRT-CM-Trk3-RP**. These are the DDI numbers assigned to the enterprise from M-net. All other Dial Patterns used as part of the compliance test were configured in a similar manner.



Dial Pattern Details

General

* **Pattern:** +49895527

* **Min:** 12

* **Max:** 14

Emergency Call: ☐

Emergency Priority: 1

Emergency Type:

SIP Domain: avaya.com

Notes: Inbd call from US to Germany (M-net)

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-		PRT-CM-Trk3-RP	0	☐	PRT-CM-Trk3	

Select : All, None

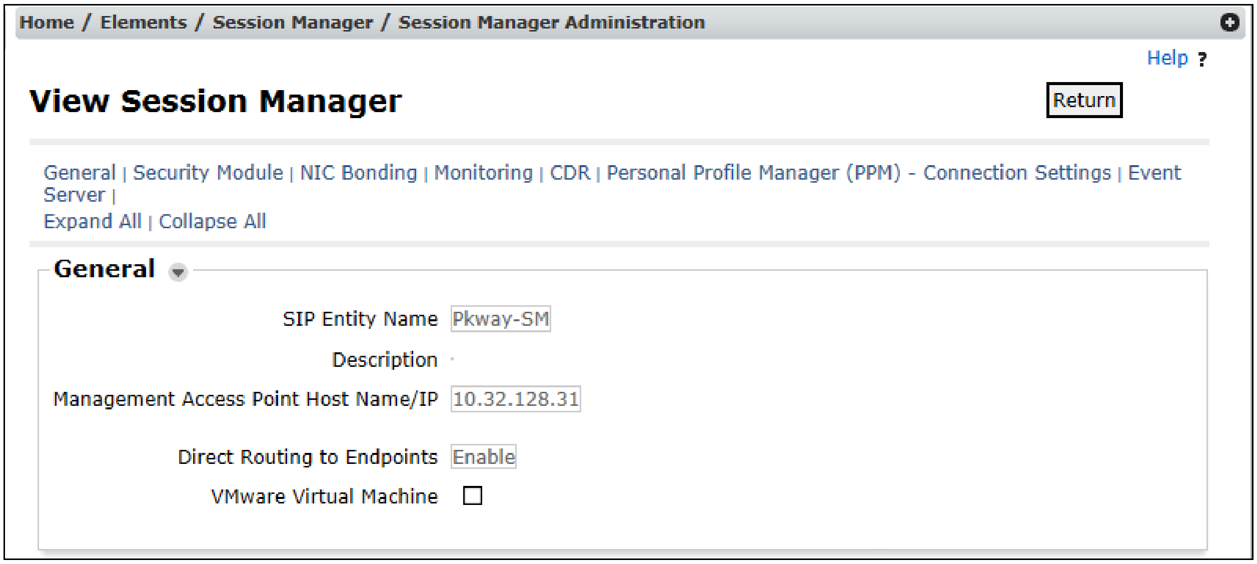
6.9. Add/View Session Manager

The creation of a Session Manager element provides the linkage between System Manager and Session Manager. This is 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 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

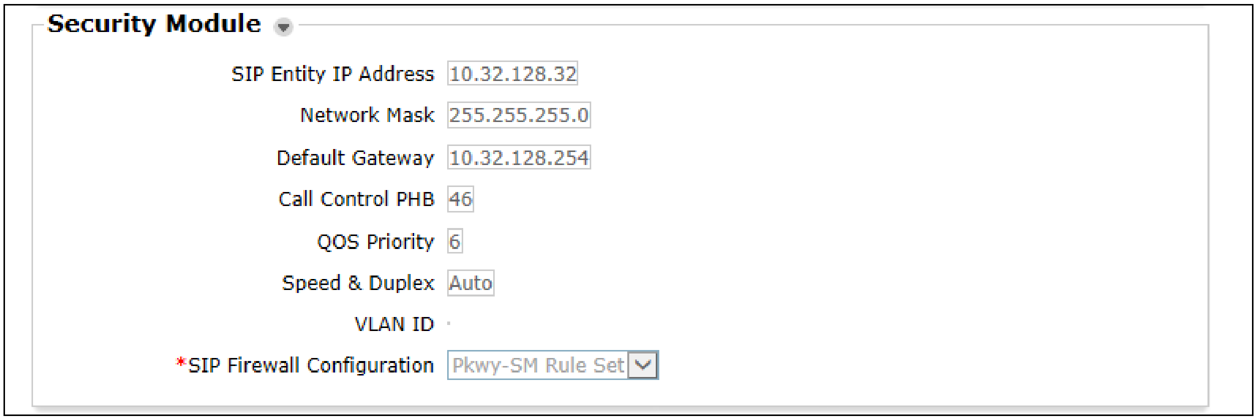
Direct Routing to Endpoints Enable

VMware Virtual Machine ☐

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

- **SIP Entity IP Address:** Should be filled in automatically based on the SIP Entity Name. Otherwise, enter the 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

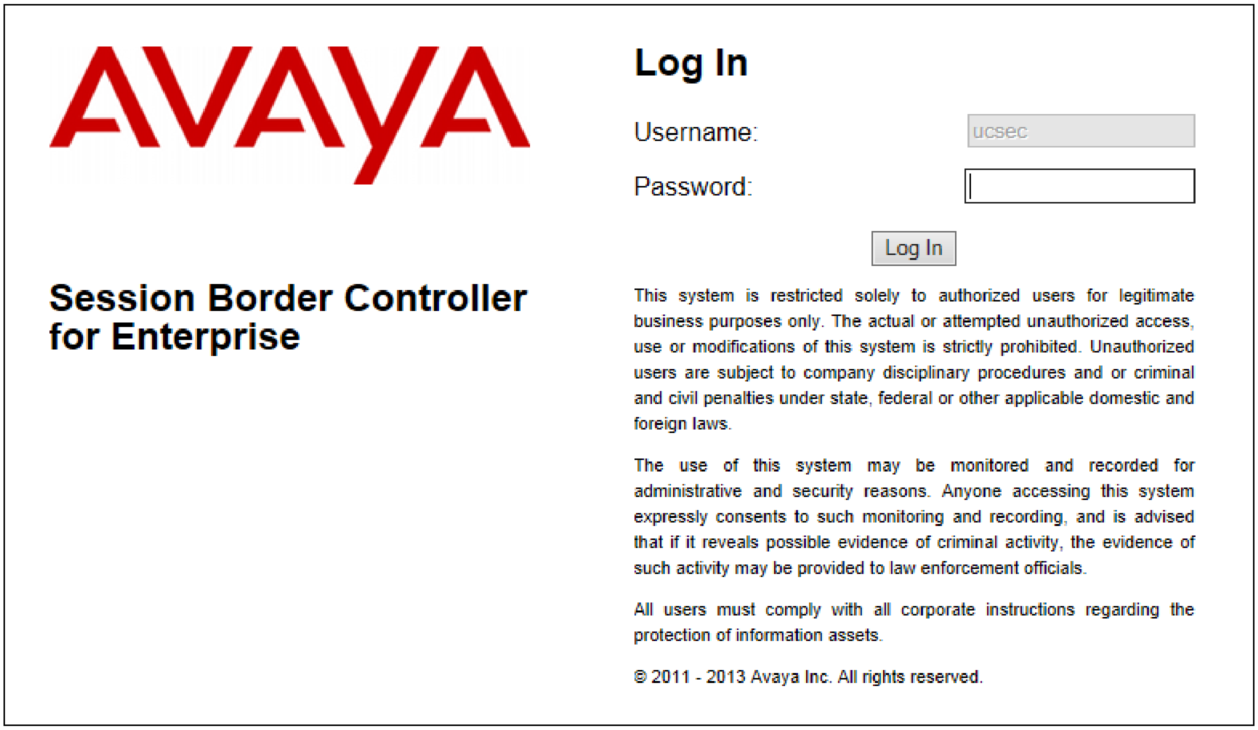
7. Configure Avaya Session Border Controller for Enterprise

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).

On all screens described in this section, it is 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.



Username: ucsec

Password:

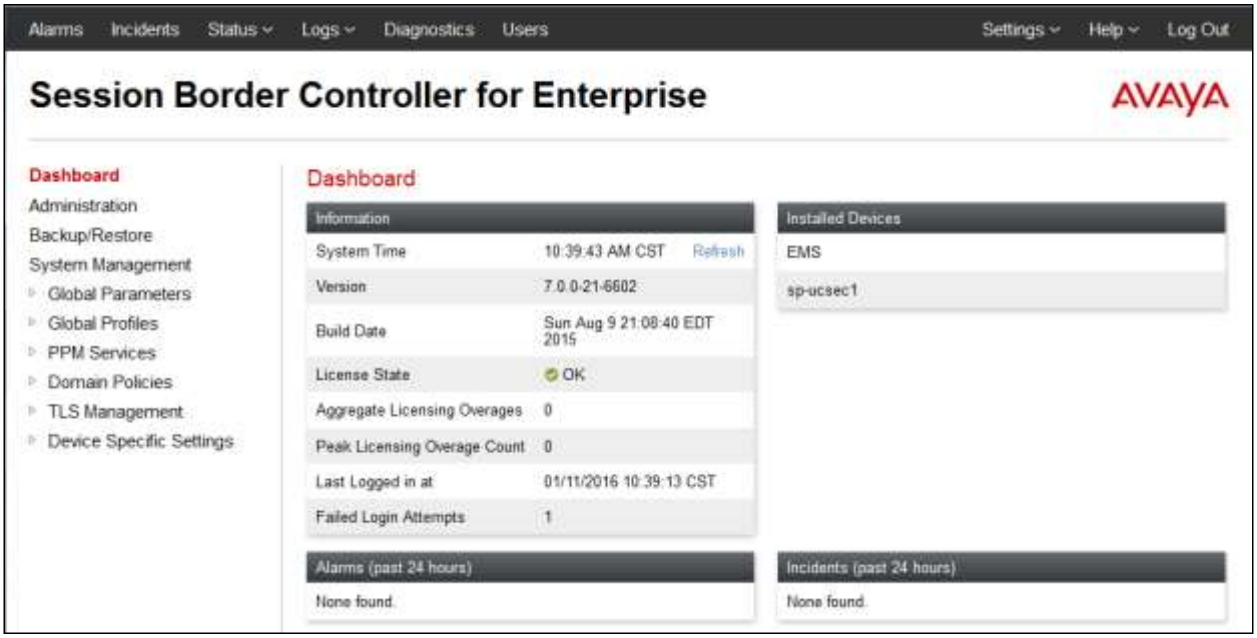
This system is restricted solely to authorized users for legitimate business purposes only. The actual or attempted unauthorized access, use or modifications of this system is strictly prohibited. Unauthorized users are subject to company disciplinary procedures and or criminal and civil penalties under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



Dashboard

Information	
System Time	10:39:43 AM CST
Version	7.0.0-21-6602
Build Date	Sun Aug 9 21:08:40 EDT 2015
License State	OK
Aggregate Licensing Overages	0
Peak Licensing Overage Count	0
Last Logged in at	01/11/2016 10:39:13 CST
Failed Login Attempts	1

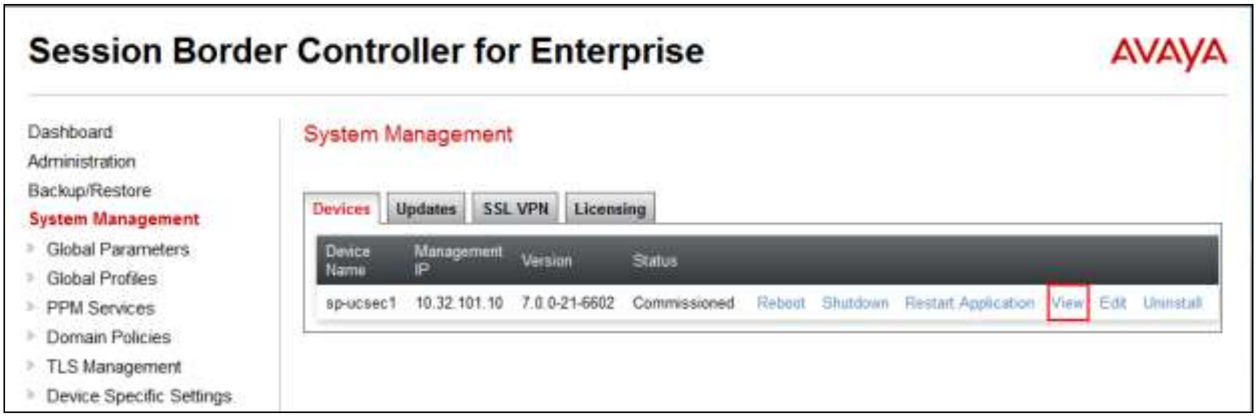
Installed Devices
EMS
sp-ucsec1

Alarms (past 24 hours)
None found.

Incidents (past 24 hours)
None found.

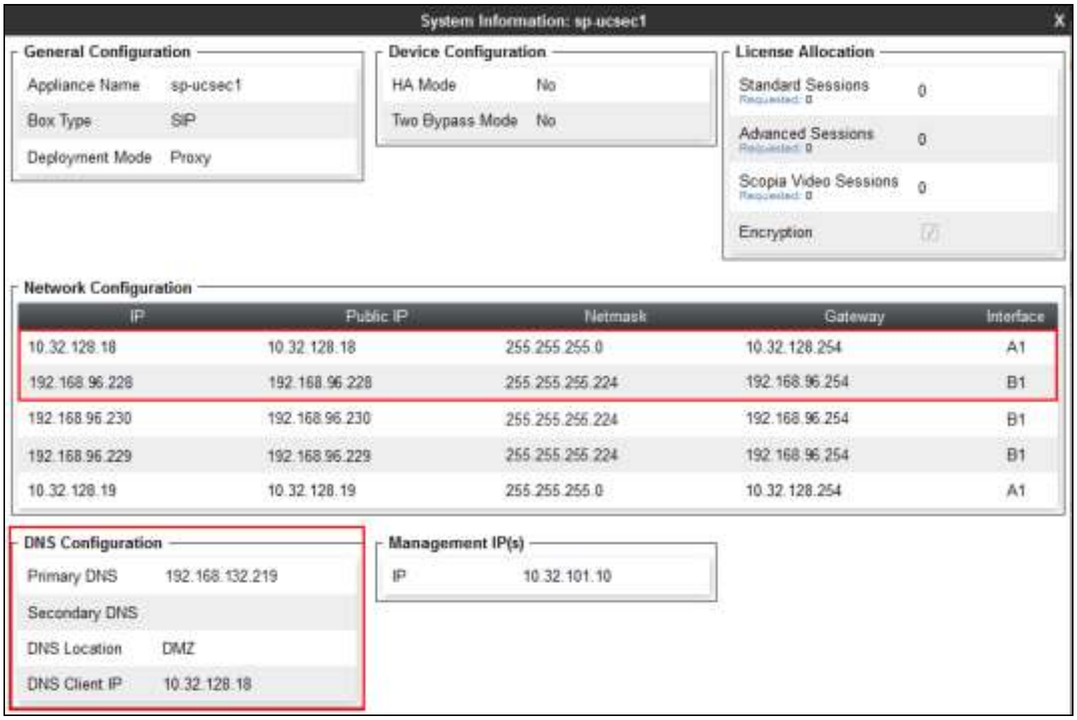
7.2. Verify Network Configuration and Enable Interfaces

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



Device Name	Management IP	Version	Status						
sp-ucsec1	10.32.101.10	7.0.0-21-6602	Commissioned	Reboot	Shutdown	Restart Application	View	Edit	Uninstall

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 respectively. Each of these interfaces must be enabled after installation. Lastly, the **DNS Configuration** must be configured since DNS will be used to resolve the M-net domain to an IP address.



General Configuration

Appliance Name	sp-ucsec1
Box Type	SIP
Deployment Mode	Proxy

Device Configuration

HA Mode	No
Two Bypass Mode	No

License Allocation

Standard Sessions Requested: 0	0
Advanced Sessions Requested: 0	0
Scopia Video Sessions Requested: 0	0
Encryption	☑

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
192.168.96.228	192.168.96.228	255.255.255.224	192.168.96.254	B1
192.168.96.230	192.168.96.230	255.255.255.224	192.168.96.254	B1
192.168.96.229	192.168.96.229	255.255.255.224	192.168.96.254	B1
10.32.128.19	10.32.128.19	255.255.255.0	10.32.128.254	A1

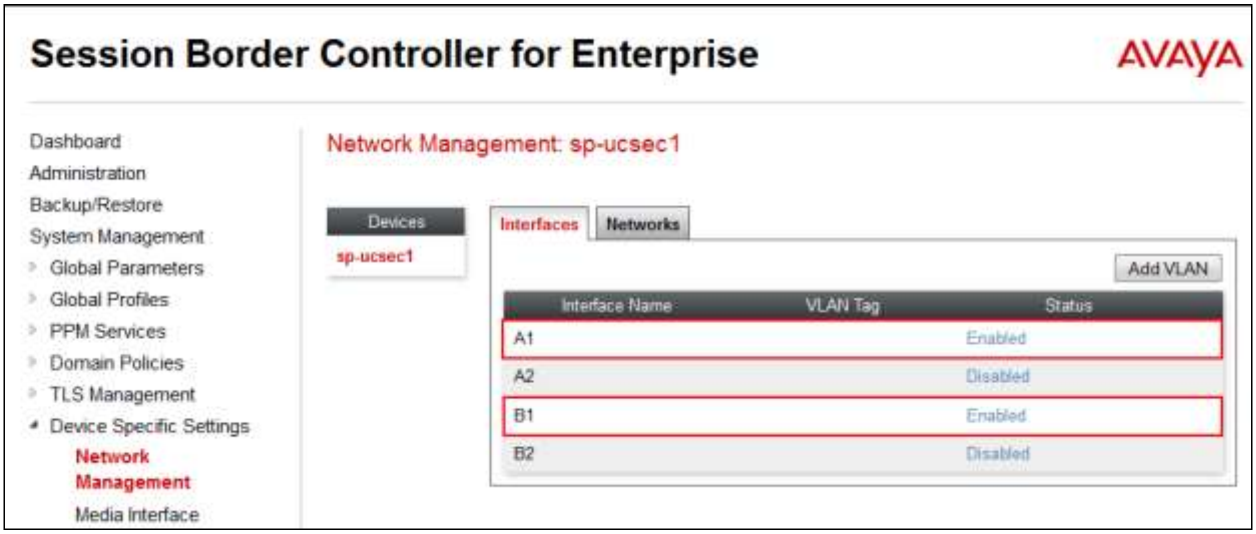
DNS Configuration

Primary DNS	192.168.132.219
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 **Interfaces** tab. Verify the **Status** is **Enabled** for both the **A1** and **B1** interfaces. If not, click the status **Enabled/Disabled** to toggle the state of the interface.



Interface Name	VLAN Tag	Status
A1		Enabled
A2		Disabled
B1		Enabled
B2		Disabled

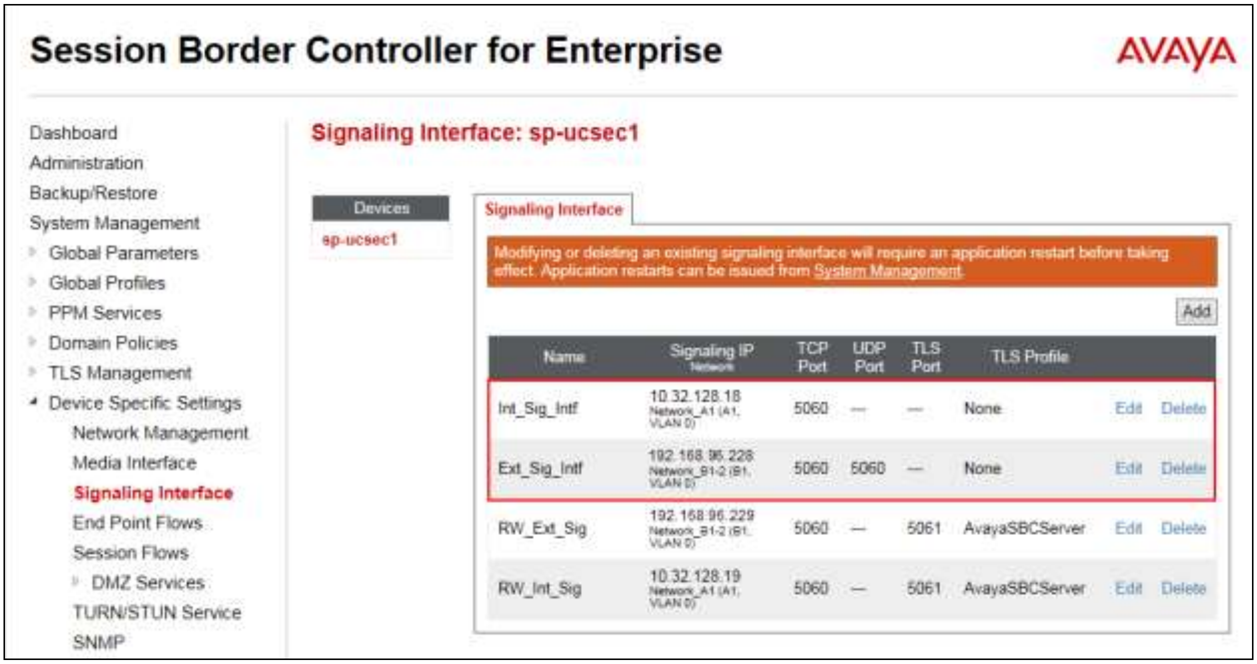
7.3. Signaling Interface

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 one or more 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 M-net will send messages using UDP on port 5060, it would have been sufficient to simply configure the Avaya SBCE for UDP.



Signaling Interface: sp-ucsec1

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

Name	Signaling IP Network	TCP Port	UDP Port	TLS Port	TLS Profile
Int_Sig_Intf	10.32.128.18 Network_A1 (A1, VLAN 0)	5060	—	—	None
Ext_Sig_Intf	192.168.96.228 Network_B1-2 (B1, VLAN 0)	5060	5060	—	None
RW_Ext_Sig	192.168.96.229 Network_B1-2 (B1, VLAN 0)	5060	—	5061	AvayaSBCServer
RW_Int_Sig	10.32.128.19 Network_A1 (A1, VLAN 0)	5060	—	5061	AvayaSBCServer

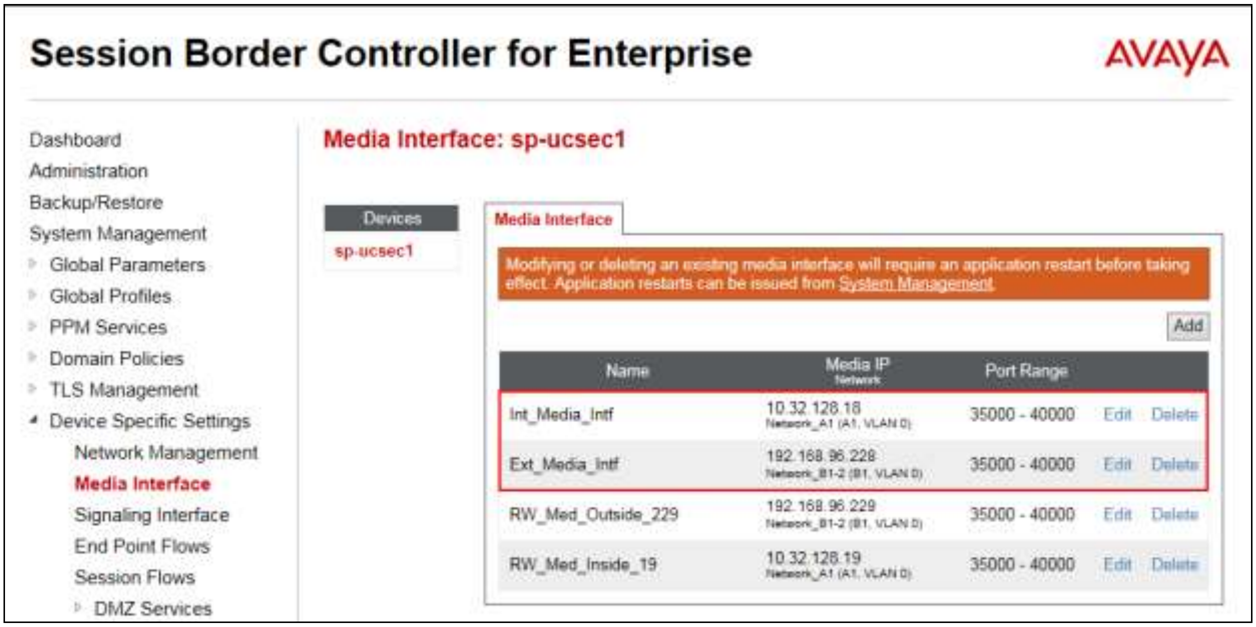
7.4. Media Interface

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 one or more 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

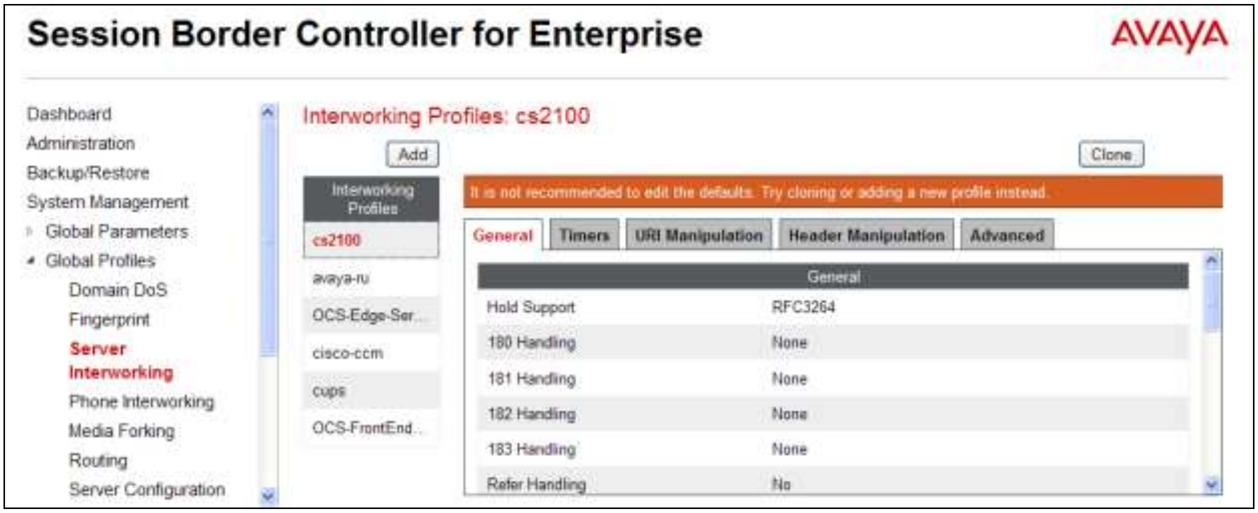
Modifying or deleting an existing media interface will require an application restart before taking effect. Application restarts can be issued from System Management.

Name	Media IP Network	Port Range		
Int_Media_Intf	10.32.128.18 Network_A1 (A1, VLAN 0)	35000 - 40000	Edit	Delete
Ext_Media_Intf	192.168.96.228 Network_B1-2 (B1, VLAN 0)	35000 - 40000	Edit	Delete
RW_Med_Outside_229	192.168.96.229 Network_B1-2 (B1, VLAN 0)	35000 - 40000	Edit	Delete
RW_Med_Inside_19	10.32.128.19 Network_A1 (A1, VLAN 0)	35000 - 40000	Edit	Delete

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 a server interworking profile for Session Manager and the service provider SIP server. These profiles will be applied to the appropriate server in **Sections 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 one or more 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.



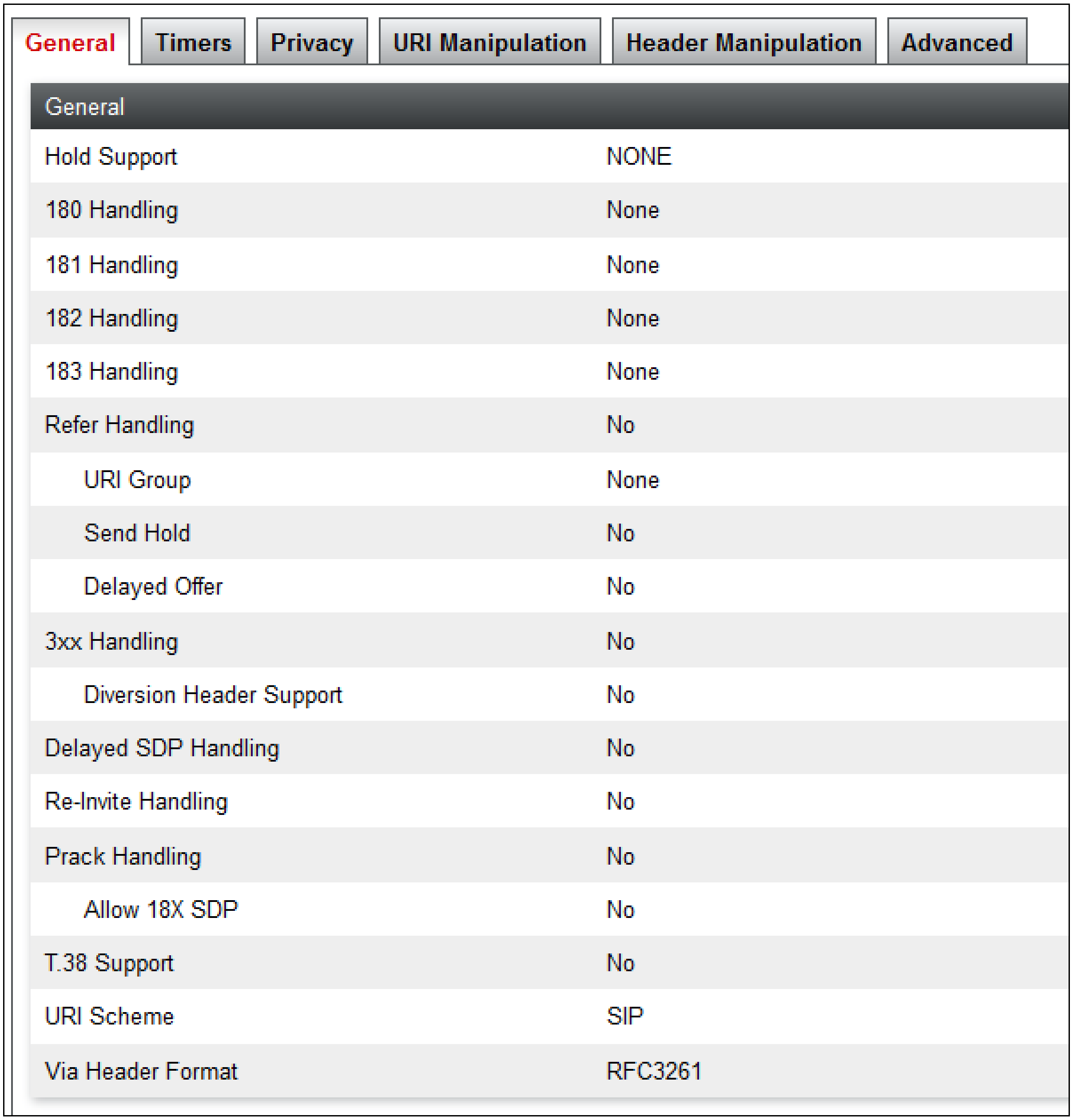
Interworking Profiles: cs2100

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

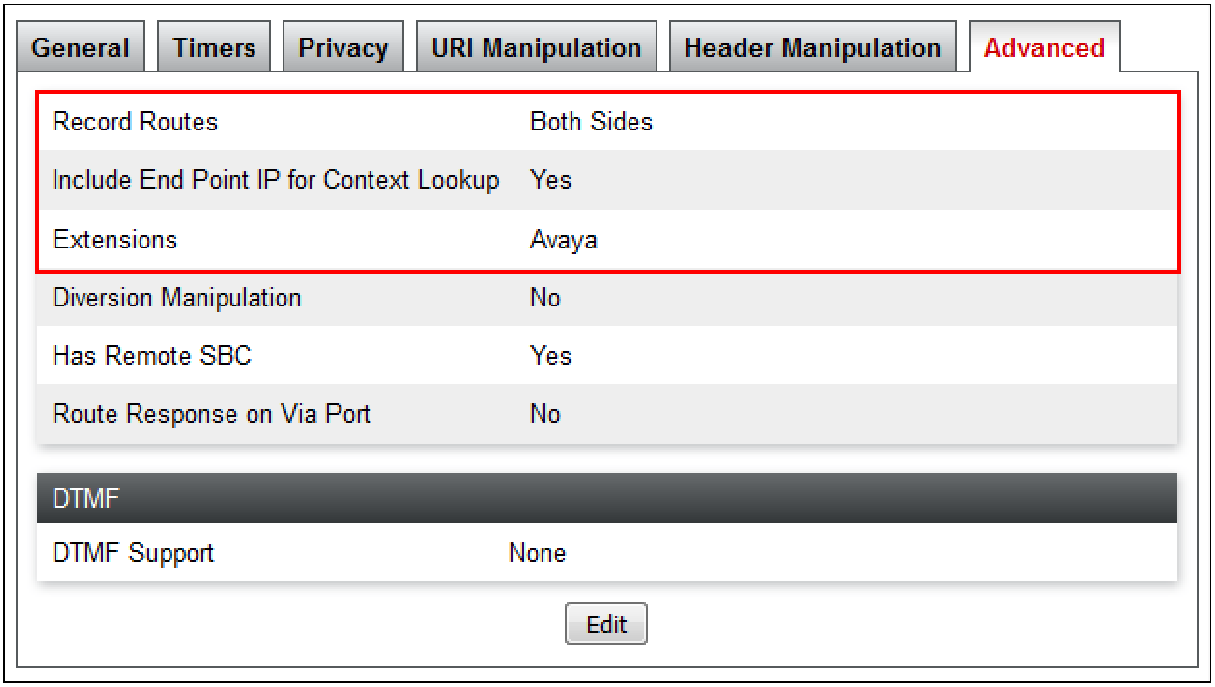
For the compliance test, server interworking profile **Avaya-SM** was created for Session Manager by cloning the existing profile **avaya-ru**. Highlighted values in this section indicate changes from the cloned profile or the default value. The **General** tab parameters are shown below.



General	
Hold Support	NONE
180 Handling	None
181 Handling	None
182 Handling	None
183 Handling	None
Refer Handling	No
URI Group	None
Send Hold	No
Delayed Offer	No
3xx Handling	No
Diversion Header Support	No
Delayed SDP Handling	No
Re-Invite Handling	No
Prack Handling	No
Allow 18X SDP	No
T.38 Support	No
URI Scheme	SIP
Via Header Format	RFC3261

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

The **Advanced** tab parameters are shown below.



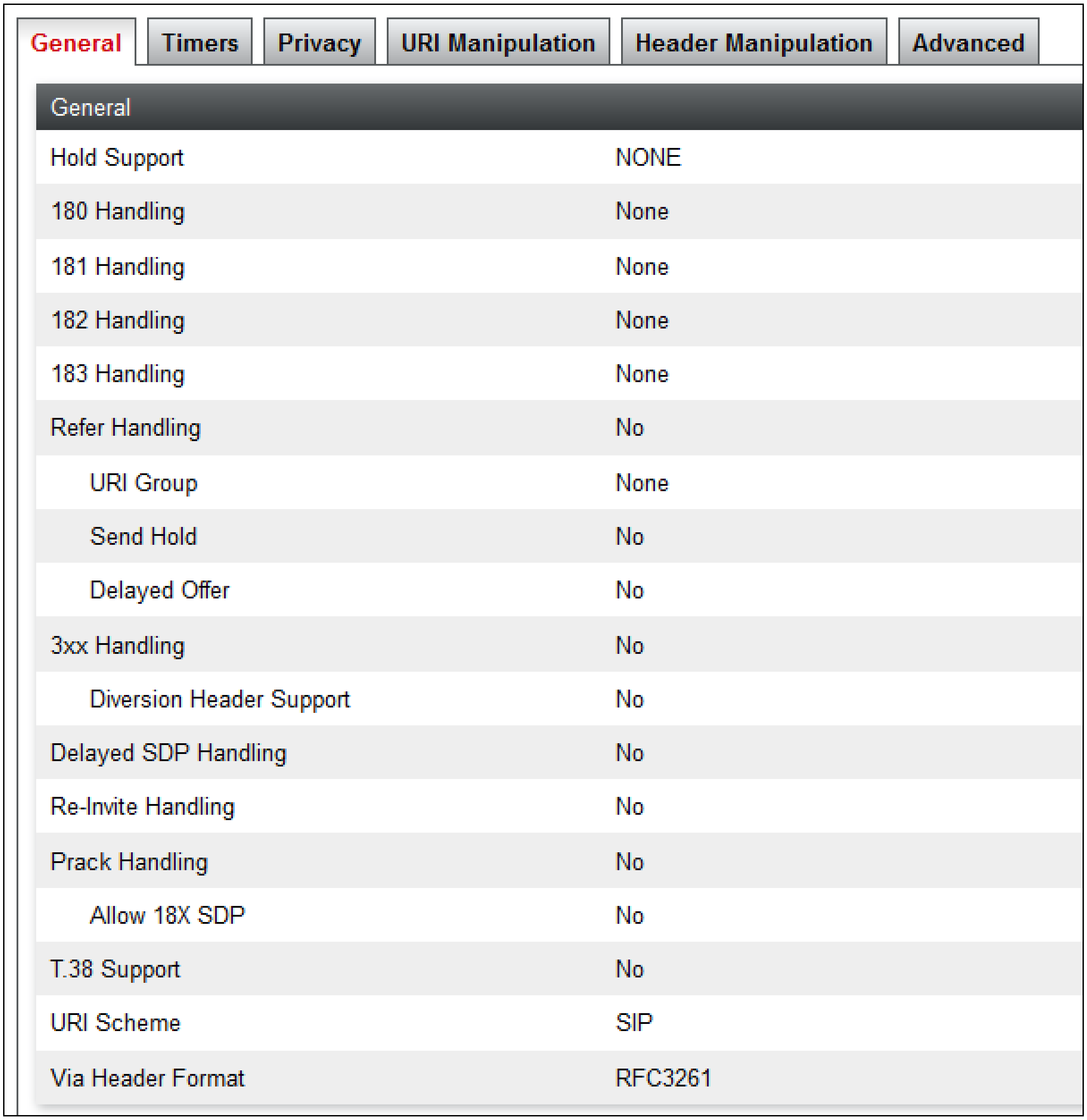
Record Routes	Both Sides
Include End Point IP for Context Lookup	Yes
Extensions	Avaya
Diversion Manipulation	No
Has Remote SBC	Yes
Route Response on Via Port	No

DTMF

DTMF Support	None

7.5.2. Server Interworking – M-net

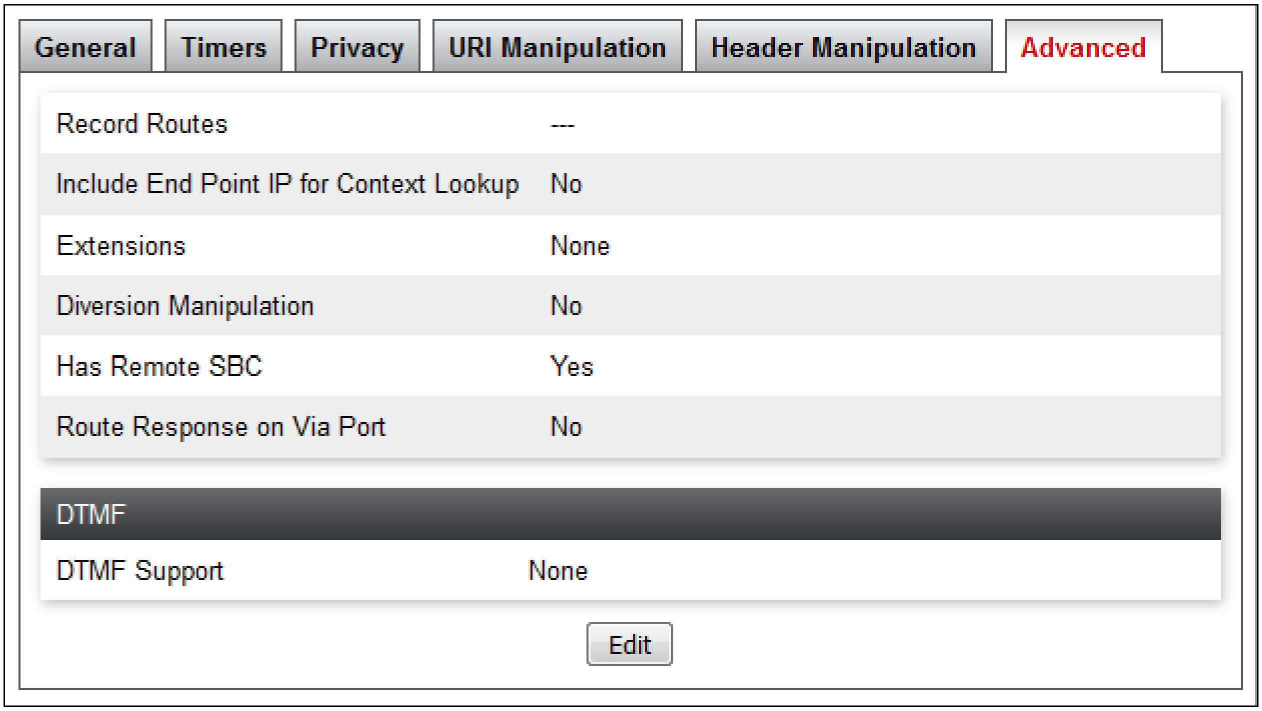
For the compliance test, server interworking profile **SP-General** was created for the M-net SIP server. When creating the profile, the default values were used for all parameters. The **General** tab parameters are shown below.



General	
Hold Support	NONE
180 Handling	None
181 Handling	None
182 Handling	None
183 Handling	None
Refer Handling	No
URI Group	None
Send Hold	No
Delayed Offer	No
3xx Handling	No
Diversion Header Support	No
Delayed SDP Handling	No
Re-Invite Handling	No
Prack Handling	No
Allow 18X SDP	No
T.38 Support	No
URI Scheme	SIP
Via Header Format	RFC3261

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

The **Advanced** tab parameters are shown below.



Record Routes	---
Include End Point IP for Context Lookup	No
Extensions	None
Diversion Manipulation	No
Has Remote SBC	Yes
Route Response on Via Port	No

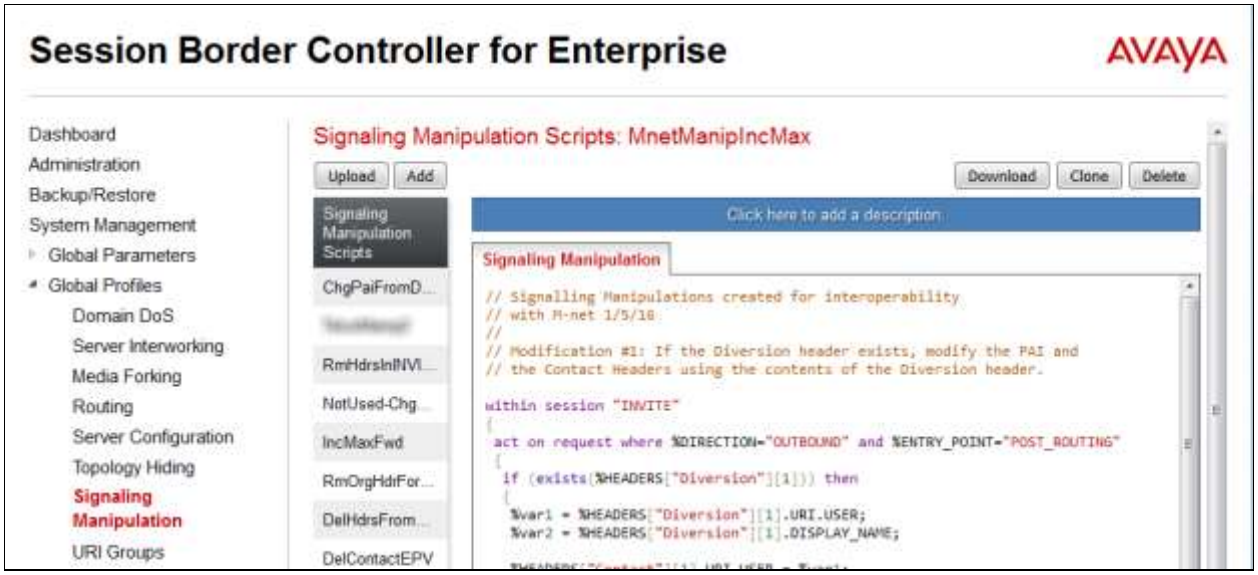
DTMF

DTMF Support	None

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. M-net required the signaling manipulation script defined in **Section 7.6.1**. It is applied to the M-net SIP server in **Section 7.7.2**.

To create a script, navigate to **Global Profiles → Signaling Manipulation** in the left pane. In the center pane, select **Add**. A script editor window (not shown) will appear in which the script can be entered line by line. The **Title** box at the top of the editor window (not shown) is where the name of the script is entered. Once complete, the script is shown in the far right pane. To view an existing script, select the script from the center pane. The settings will appear in the right pane as shown in the example below.

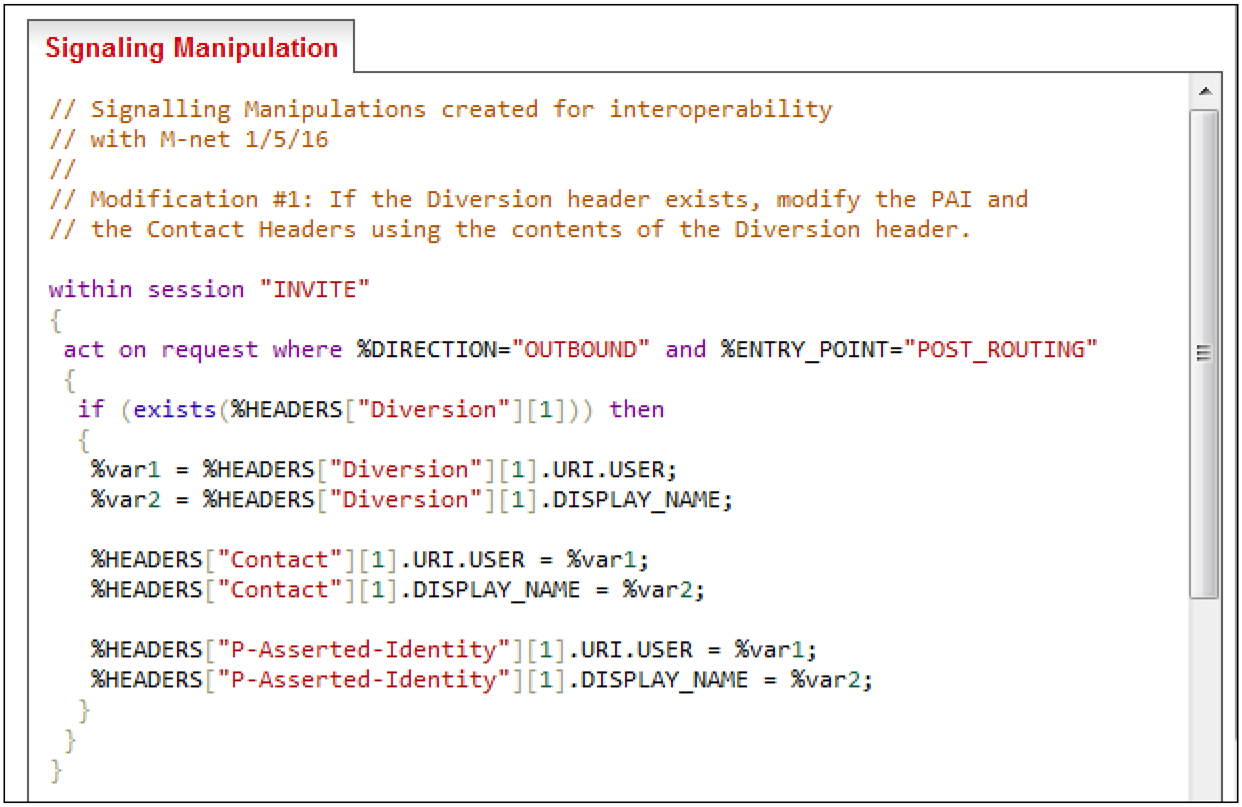


```
// Signalling Manipulations created for interoperability
// with M-net 1/5/16
//
// Modification #1: If the Diversion header exists, modify the PAI and
// the Contact Headers using the contents of the Diversion header.

within session "INVITE"
{
 act on request where %DIRECTION="OUTBOUND" and %ENTRY_POINT="POST_ROUTING"
 {
  if (exists(%HEADERS["Diversion"][1])) then
  {
   %var1 = %HEADERS["Diversion"][1].URI.USER;
   %var2 = %HEADERS["Diversion"][1].DISPLAY_NAME;
```

7.6.1. Signaling Manipulation Script – M-net

For the compliance test, signaling manipulation script **MnetManipIncMax** was created for the M-net SIP server. The script contains three manipulations.

The first manipulation checks to see if a Diversion header is present in the outbound INVITE, and if so it will overwrite the user and display name in the PAI and Contact headers with the contents of the Diversion Header. This is necessary for call forwarding and EC500. This manipulation was requested by M-net in order to correct the call display on the destination phone. See **Section 2.2** for details. Unfortunately, performing these header changes did not correct the call display; however, they are believed to be correct for interoperability and are retained in the configuration. The script instructions to perform these manipulations are shown below and in **Appendix A**.



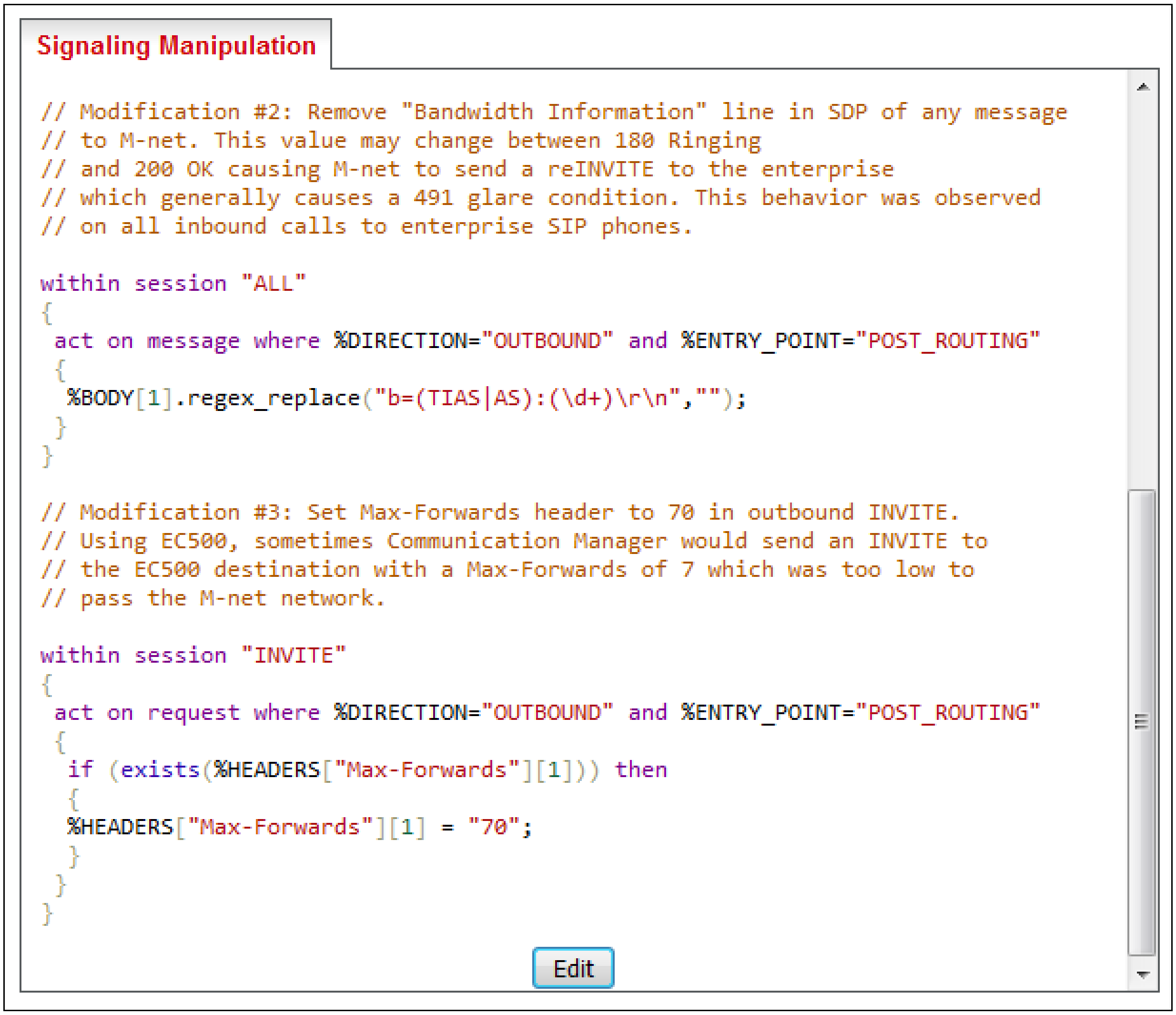
```
// Signalling Manipulations created for interoperability
// with M-net 1/5/16
//
// Modification #1: If the Diversion header exists, modify the PAI and
// the Contact Headers using the contents of the Diversion header.

within session "INVITE"
{
 act on request where %DIRECTION="OUTBOUND" and %ENTRY_POINT="POST_ROUTING"
 {
  if (exists(%HEADERS["Diversion"][1])) then
  {
   %var1 = %HEADERS["Diversion"][1].URI.USER;
   %var2 = %HEADERS["Diversion"][1].DISPLAY_NAME;

   %HEADERS["Contact"][1].URI.USER = %var1;
   %HEADERS["Contact"][1].DISPLAY_NAME = %var2;

   %HEADERS["P-Asserted-Identity"][1].URI.USER = %var1;
   %HEADERS["P-Asserted-Identity"][1].DISPLAY_NAME = %var2;
  }
 }
}
```

The second and third manipulations are in the same script file and are shown below.

The second manipulation removes the optional bandwidth parameter (b) in the SDP in all messages from the enterprise to M-net. In some call scenarios, this parameter changed between the 180 Ringing message and the 200 OK message sent from the enterprise during call set-up. This caused M-net to send a reINVITE which often resulted in a 491 error indicating a glare condition which in turn had to be resolved through additional signaling. To avoid this unwanted additional messaging, the bandwidth parameter was removed from the SDP.

The third manipulation sets the Max-Forwards value to 70 in outbound INVITE messages. In some EC500 call scenarios, Communication Manager would send an INVITE to the EC500 destination with a Max-Forwards value of 7 which was too low to pass through the M-net network, thus causing the call to fail. By ensuring that the Max-Forwards value is set high enough to transverse the M-net network, the calls were made to pass.

The complete file is shown in **Appendix A**.

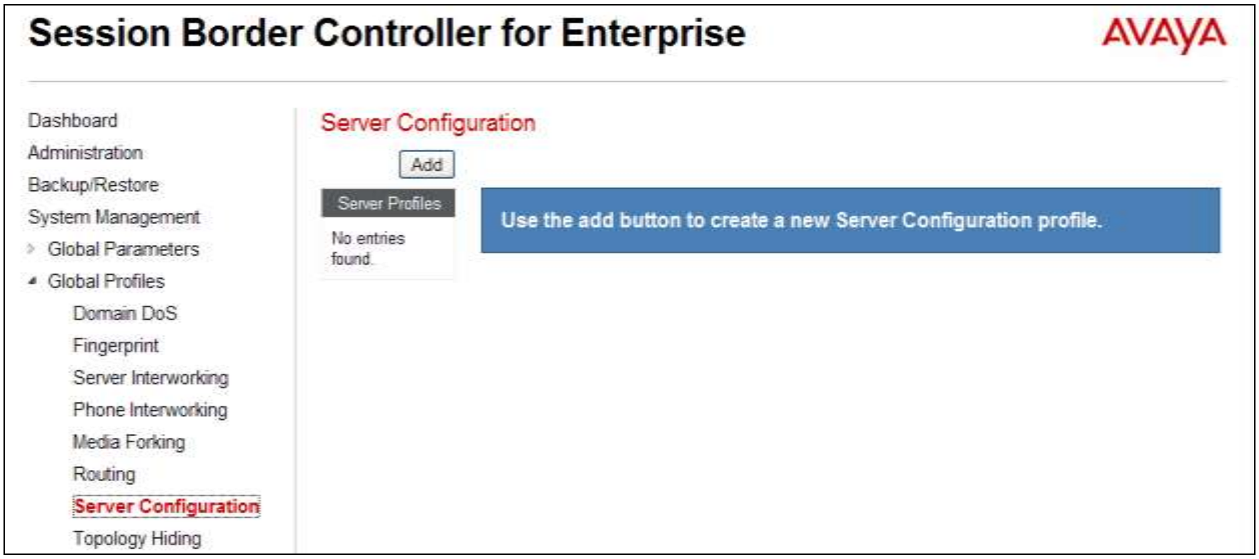


```
// Modification #2: Remove "Bandwidth Information" line in SDP of any message
// to M-net. This value may change between 180 Ringing
// and 200 OK causing M-net to send a reINVITE to the enterprise
// which generally causes a 491 glare condition. This behavior was observed
// on all inbound calls to enterprise SIP phones.

within session "ALL"
{
 act on message where %DIRECTION="OUTBOUND" and %ENTRY_POINT="POST_ROUTING"
 {
  %BODY[1].regex_replace("b=(TIAS|AS):(\d+)\r\n","");
 }
}

// Modification #3: Set Max-Forwards header to 70 in outbound INVITE.
// Using EC500, sometimes Communication Manager would send an INVITE to
// the EC500 destination with a Max-Forwards of 7 which was too low to
// pass the M-net network.

within session "INVITE"
{
 act on request where %DIRECTION="OUTBOUND" and %ENTRY_POINT="POST_ROUTING"
 {
  if (exists(%HEADERS["Max-Forwards"][1])) then
  {
  %HEADERS["Max-Forwards"][1] = "70";
  }
 }
}
```

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 one or more pop-up windows in which the profile parameters can be configured. Once complete, the profile name will appear under **Server Profiles** in the center pane and the settings will be shown in the far right pane. If a profile already exists, then the settings of the existing profile may be viewed by selecting the profile from the center pane. The settings will appear in the right pane.



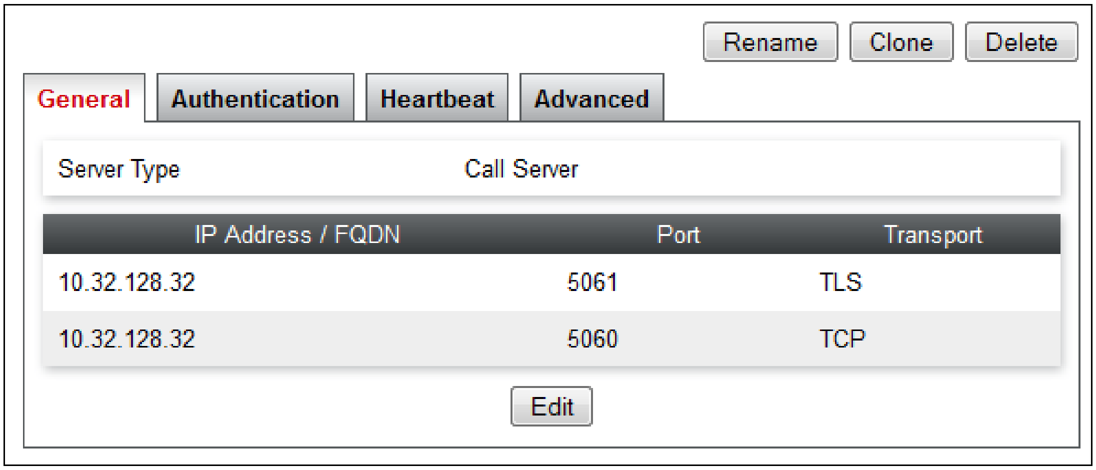
No entries found.

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**.
- Enter a valid combination of **IP Address / FQDN**, **Port** and **Transport** that Session Manager will use to listen for SIP requests. The standard SIP UDP/TCP port is 5060. The standard SIP TLS port is 5061. Additional combinations can be entered by clicking the **Add** button (not shown).

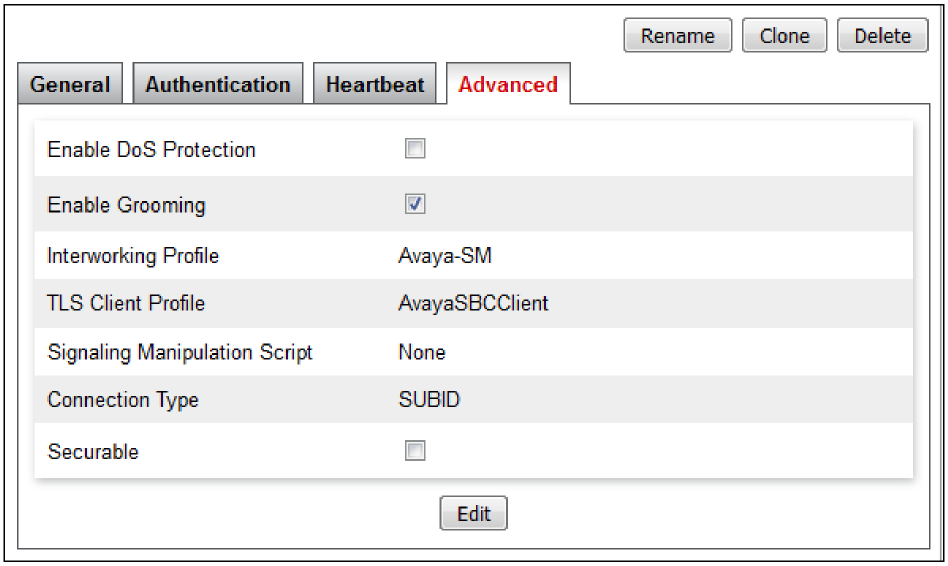


Server Type	Call Server

IP Address / FQDN	Port	Transport
10.32.128.32	5061	TLS
10.32.128.32	5060	TCP

The **Authentication** and **Heartbeat** tabs have no entries.

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**. Set the **TLS Client Profile** to **AvayaSBCClient**.

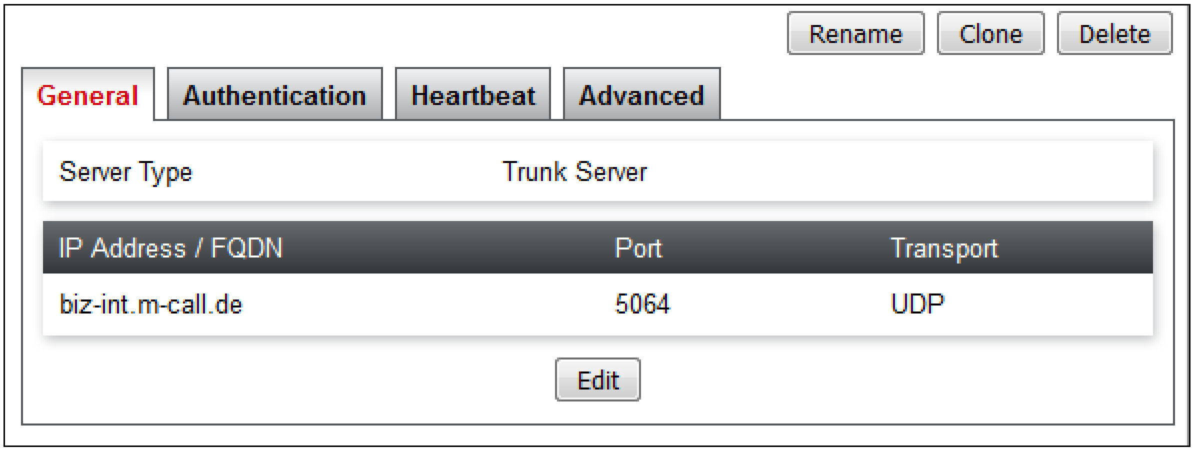


Enable DoS Protection	☐
Enable Grooming	☑
Interworking Profile	Avaya-SM
TLS Client Profile	AvayaSBCClient
Signaling Manipulation Script	None
Connection Type	SUBID
Securable	☐

7.7.2. Server Configuration – M-net

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

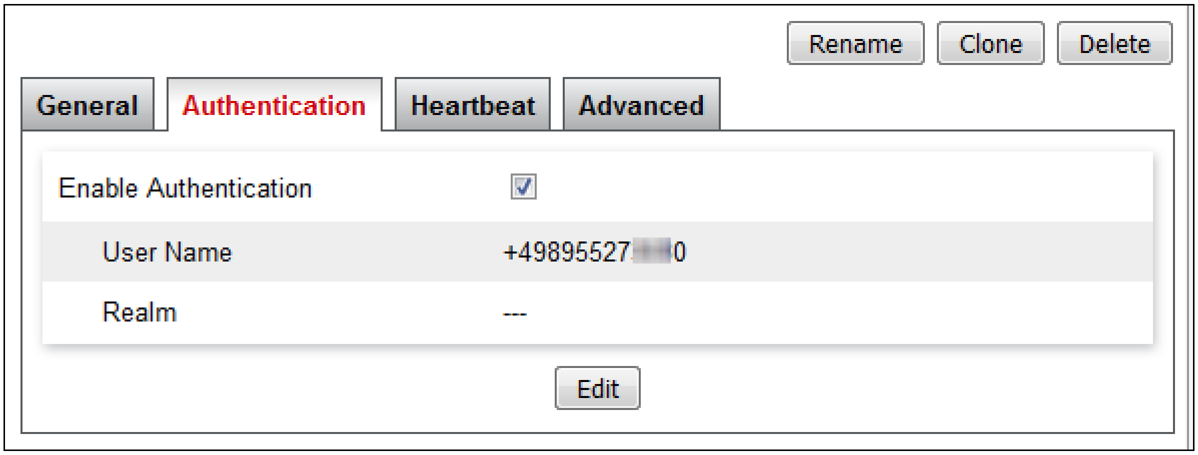
- Set **Server Type** to **Trunk Server**.
- Enter a valid combination of **IP Address / FQDN**, **Port** and **Transport** that the M-net SIP proxy will use to listen for SIP requests. This information is provided by M-net. The standard SIP UDP/TCP port is 5060 but for the purposes of the compliance test, port **5064** was used. Additional combinations can be entered by clicking the **Add** button (not shown). The Avaya SBCE will perform a DNS lookup on the FQDN provided by M-net to determine the IP address of the server.



Server Type: Trunk Server

IP Address / FQDN	Port	Transport
biz-int.m-call.de	5064	UDP

The Avaya SBCE will be registering to M-net on behalf of Communication Manager. On the **Authentication** tab, check the **Enable Authentication** box. Enter the **User Name** and **Password** (not shown) provided by M-net.



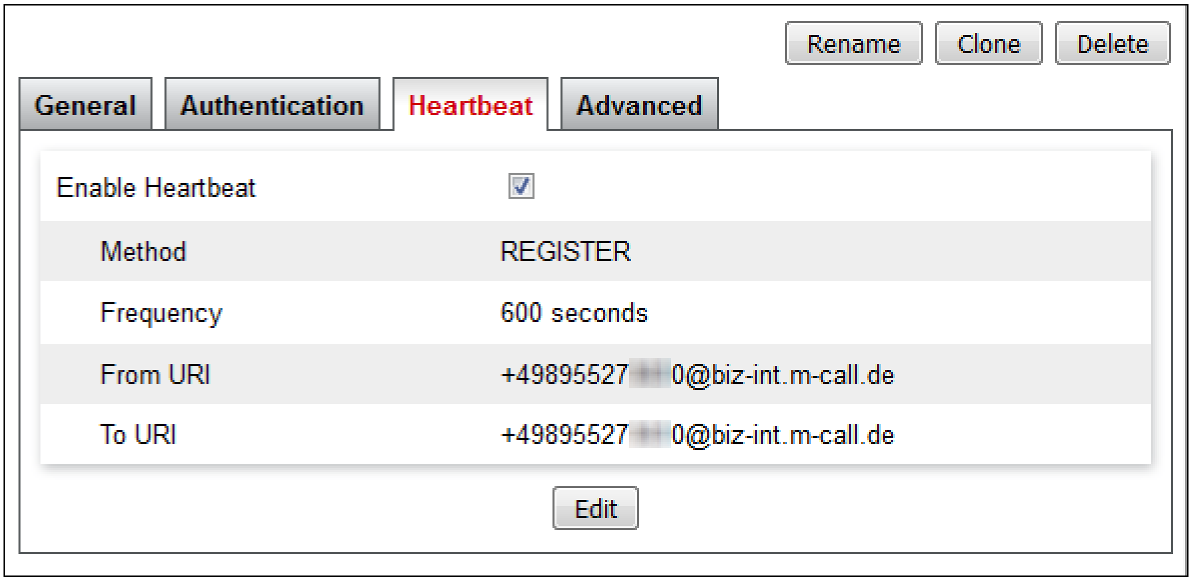
Enable Authentication ☑

User Name +49895527[redacted]0

Realm ---

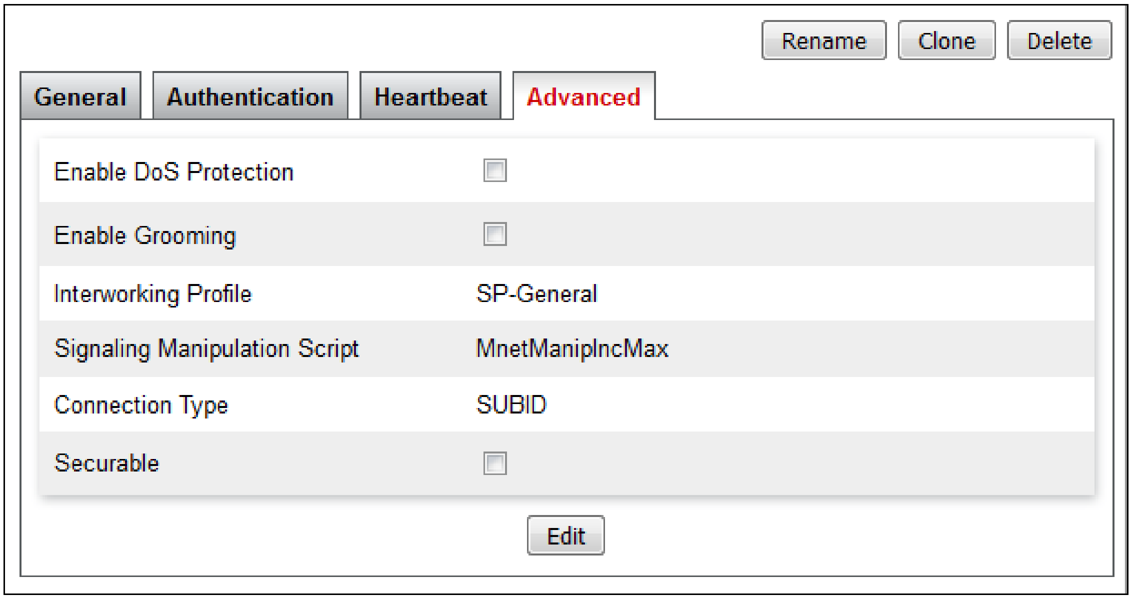
On the **Heartbeat** tab, configure the following:

- Check the **Enable Heartbeat** box.
- For the **Method**, select **REGISTER**.
- Set the **Frequency** to the value provided by M-net. The compliance test used the value of **600** seconds.
- Set the **From URI** field to the *user@domain* name that should appear in the REGISTER message. In the case of M-net, the *user* is the user name provided by M-net and used on the **Authentication** tab. The *domain* is the fully qualified domain name of the M-net SIP proxy provided by M-net.
- Set the **To URI** to the same value used for the **From URI**.



Enable Heartbeat	☑
Method	REGISTER
Frequency	600 seconds
From URI	+49895527[redacted]0@biz-int.m-call.de
To URI	+49895527[redacted]0@biz-int.m-call.de

On the **Advanced** tab, set the **Interworking Profile** field to the interworking profile for M-net defined in **Section 7.5.2**. Set the **Signaling Manipulation Script** field to the script created for M-net in **Section 7.6.1**.

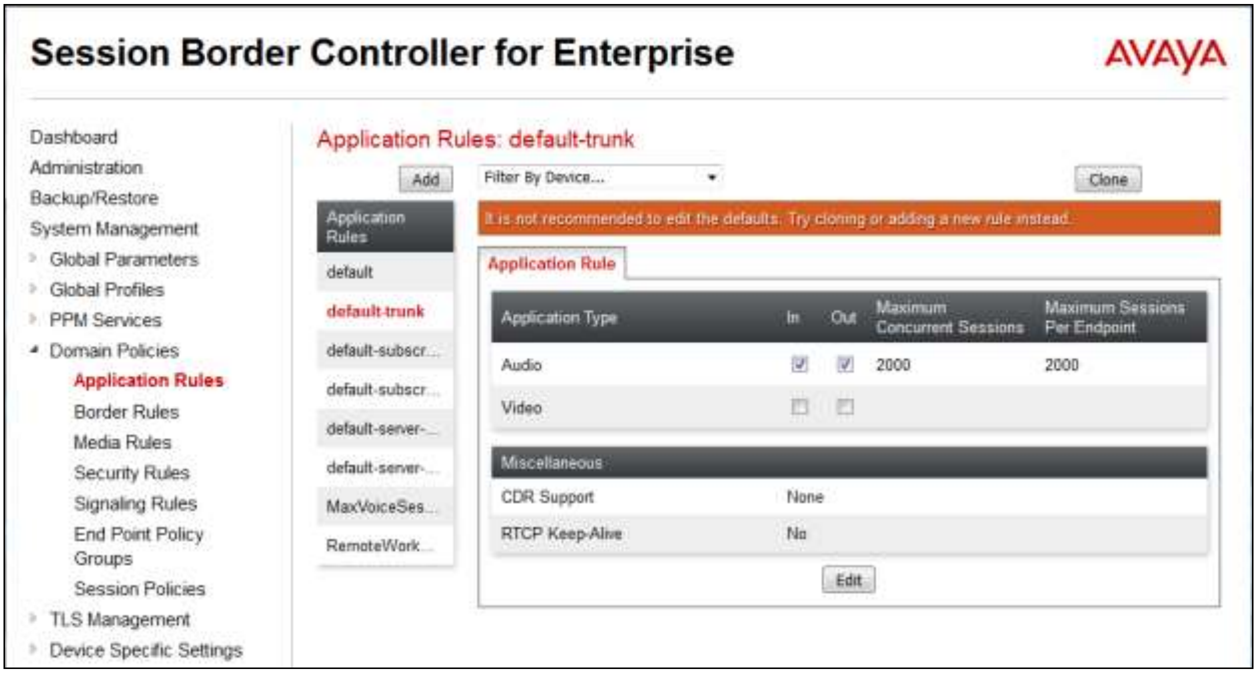


Enable DoS Protection	☐
Enable Grooming	☐
Interworking Profile	SP-General
Signaling Manipulation Script	MnetManipIncMax
Connection Type	SUBID
Securable	☐

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 M-net 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
Audio	☑	☑	2000	2000
Video	☐	☐		

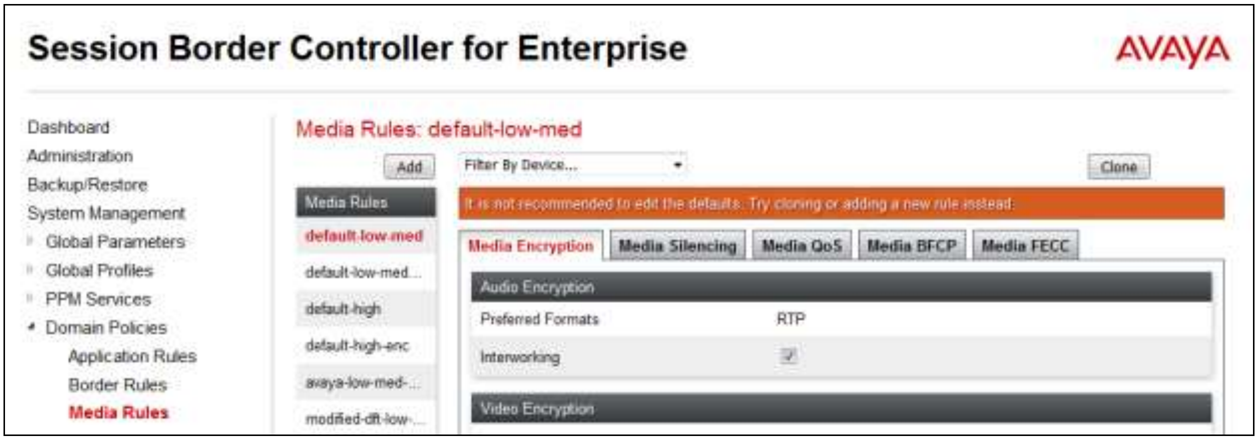
Miscellaneous	
CDR Support	None
RTCP Keep-Alive	No

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 M-net 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.

The contents of the **default-low-med** media rule are described below.



Media Rules: default-low-med

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

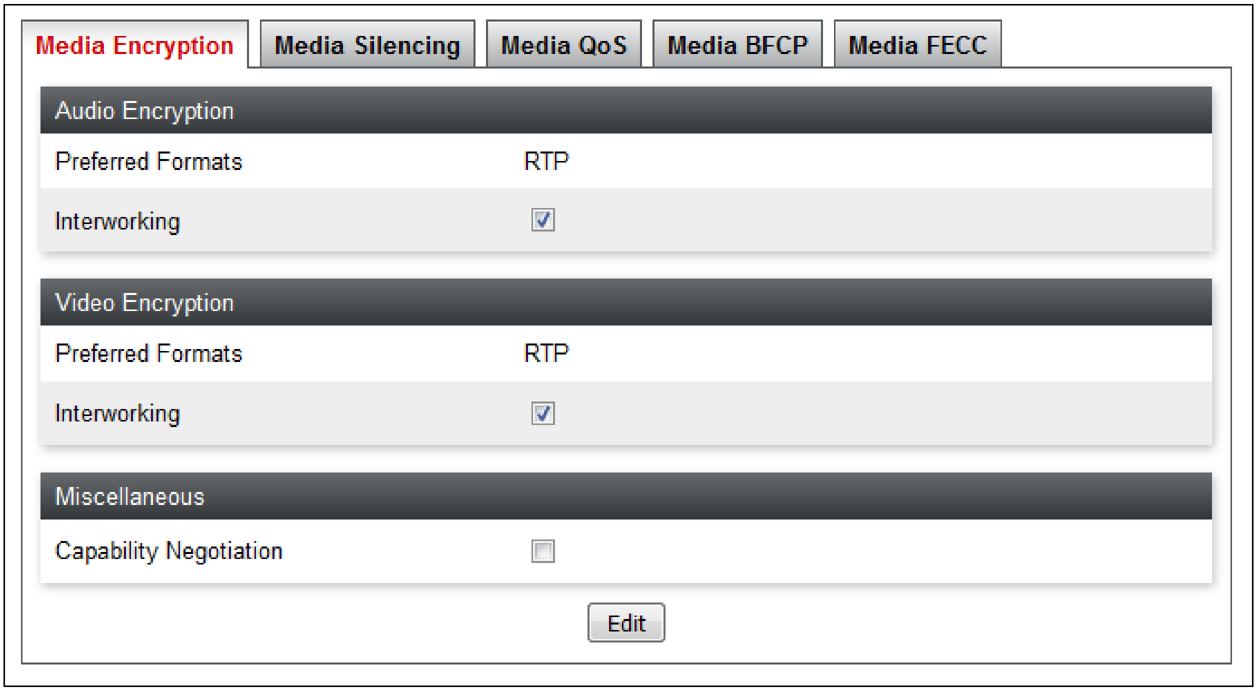
Audio Encryption

Preferred Formats RTP

Interworking ☑

Video Encryption

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



Audio Encryption

Preferred Formats RTP

Interworking ☑

Video Encryption

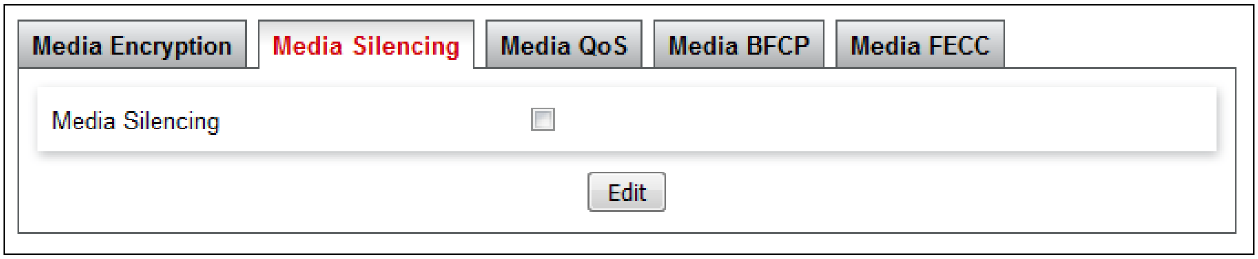
Preferred Formats RTP

Interworking ☑

Miscellaneous

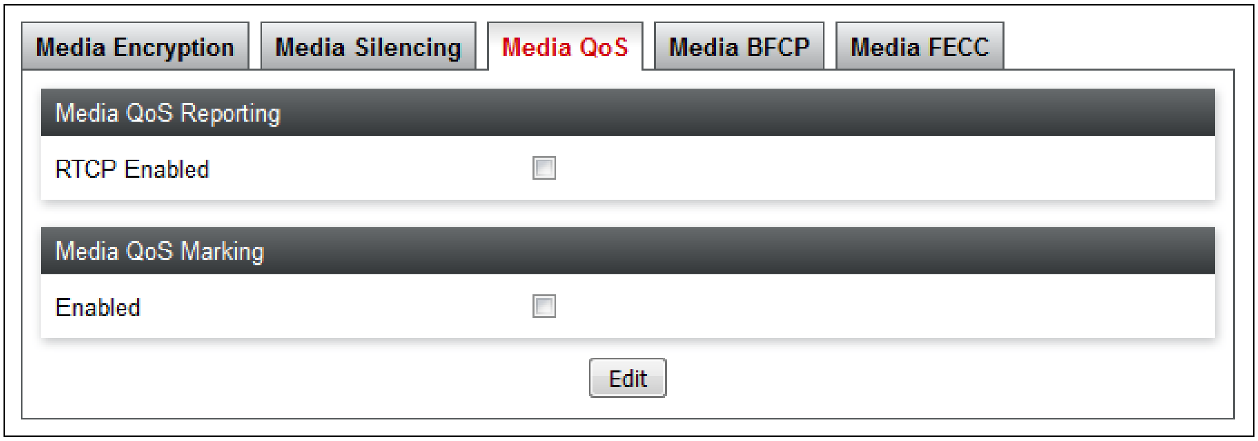
Capability Negotiation ☐

On the **Media Silencing** tab, **Media Silencing** is disabled.



Media Silencing ☐

The **Media QoS** settings are shown below.



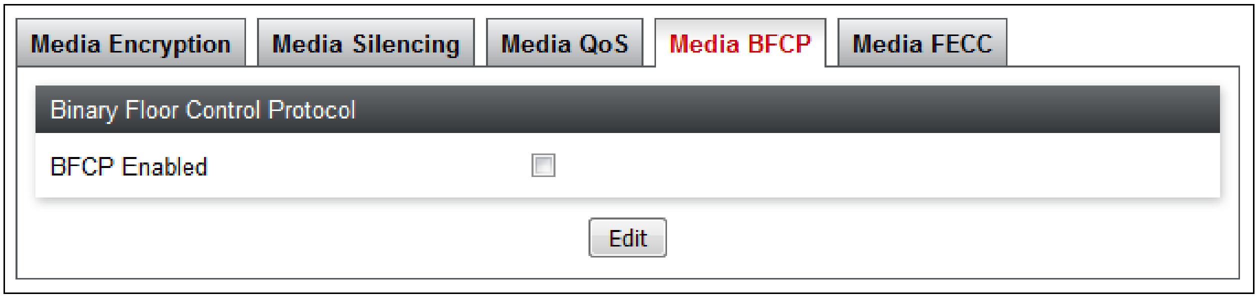
Media QoS Reporting

RTCP Enabled ☐

Media QoS Marking

Enabled ☐

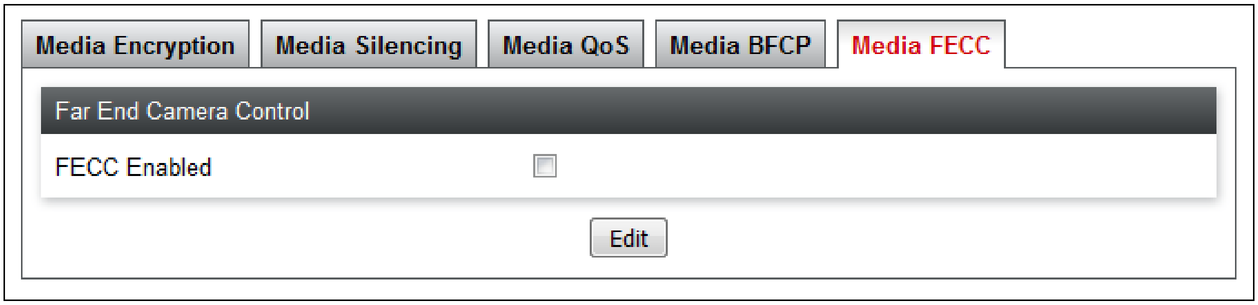
On the **Media BFCP** tab, BFCP is disabled.



Binary Floor Control Protocol

BFCP Enabled ☐

On the **Media FECC** tab, FECC is disabled.



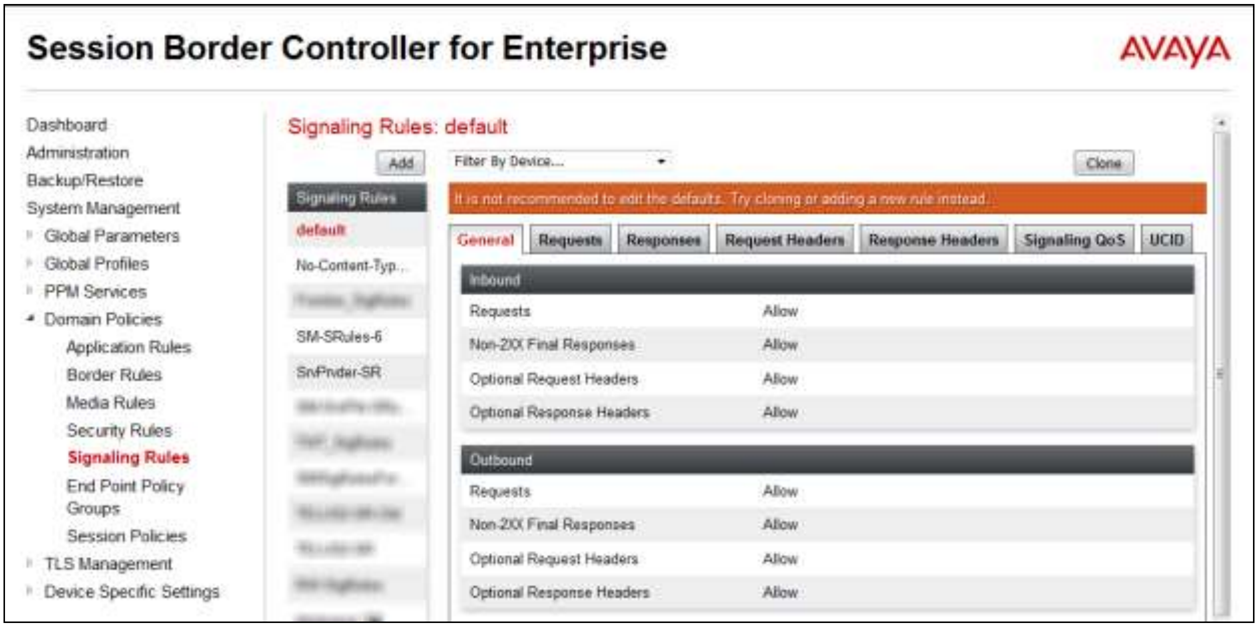
Far End Camera Control

FECC 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 and the M-net SIP server.

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 one or more 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.



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

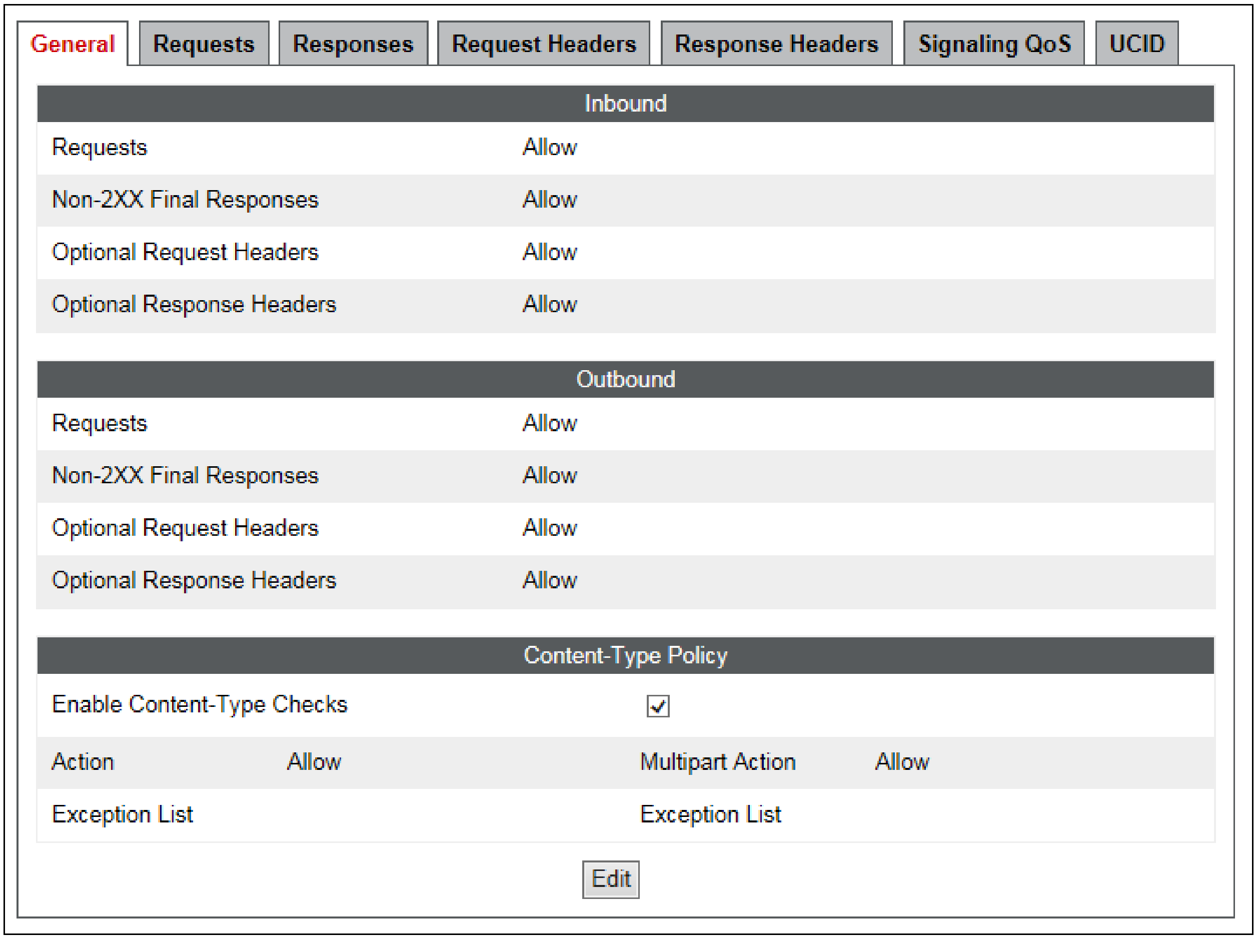
Inbound	
Requests	Allow
Non-2XX Final Responses	Allow
Optional Request Headers	Allow
Optional Response Headers	Allow

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

7.10.1. Signaling Rules – Session Manager

For the compliance test, signaling rule **SM-SRules-6** was created for Session Manager to prevent some proprietary headers in the SIP messages, sent from the Session Manager, from being propagated to M-net. A header was blocked if it contained internal addresses or other information about the internal network.

SM-SRules-6 was created using the default values on all tabs except the **Request Headers**, **Response Headers**, and **Signaling QoS** tabs. The **General** tab settings are shown below.



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

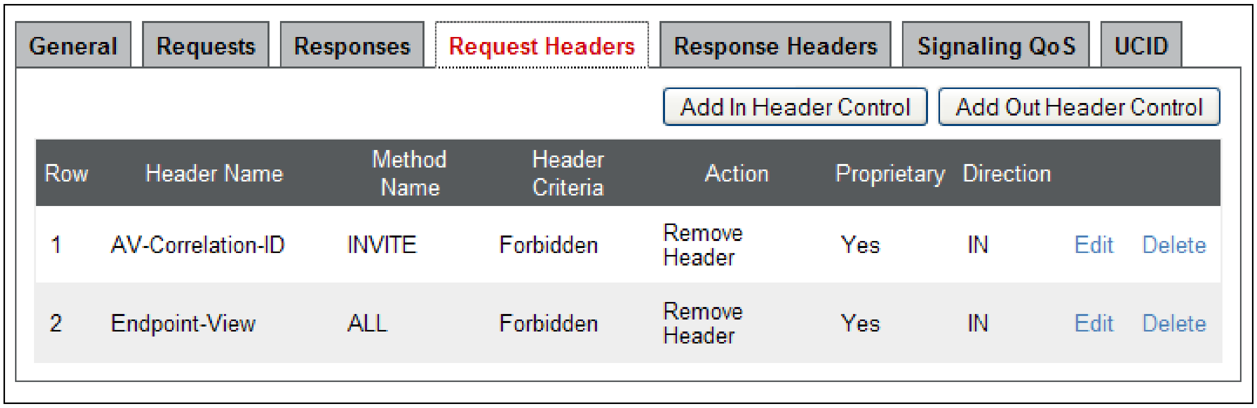
Outbound	
Requests	Allow
Non-2XX Final Responses	Allow
Optional Request Headers	Allow
Optional Response Headers	Allow

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

The **Requests** and **Responses** tabs have no entries.

The **Request Headers** tab shows the manipulations performed on the headers of request messages such as the initial INVITE or UPDATE message. 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:

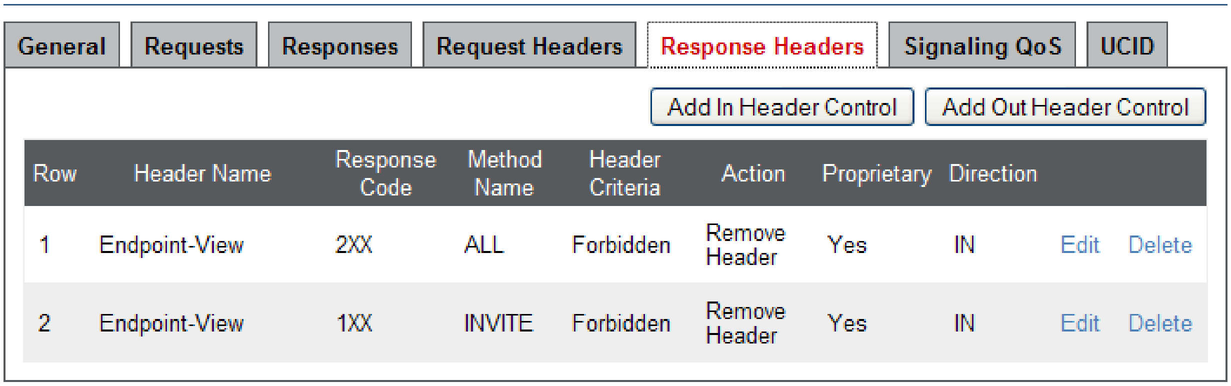
1. Removes the **AV-Correlation-ID** header from **INVITE** messages in the **IN** direction (Session Manager to Avaya SBCE).
2. Removes the **Endpoint-View** header from **ALL** messages in the **IN** direction.



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

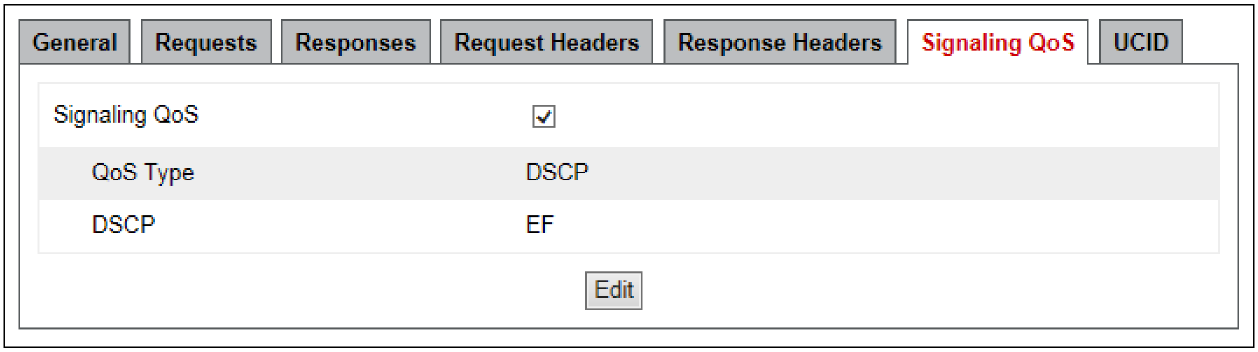
Similarly, manipulations can be performed on the headers of SIP response messages. These can be viewed by selecting the **Response Header** tab as shown below. Entries were created in the same manner as was done on the **Request Headers** tab. The entries shown perform the following actions:

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.



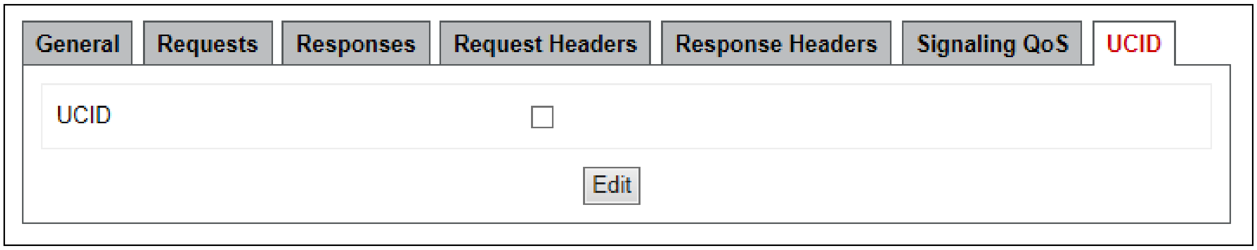
Row	Header Name	Response Code	Method Name	Header Criteria	Action	Proprietary	Direction		
1	Endpoint-View	2XX	ALL	Forbidden	Remove Header	Yes	IN	Edit	Delete
2	Endpoint-View	1XX	INVITE	Forbidden	Remove Header	Yes	IN	Edit	Delete

The **Signaling QoS** settings are shown below.



Signaling QoS	☑
QoS Type	DSCP
DSCP	EF

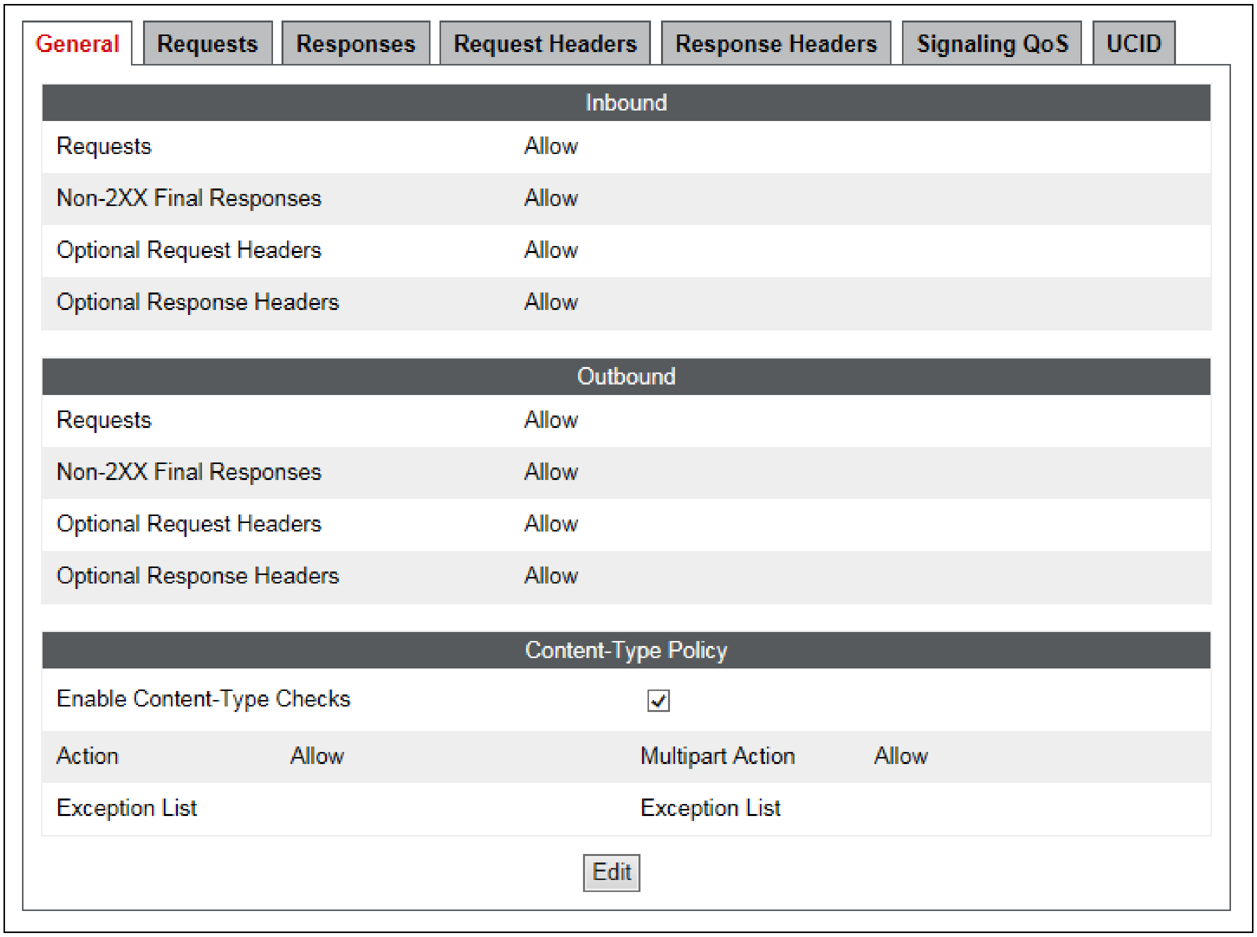
The **UCID** settings are shown below.



UCID	☐

7.10.2. Signaling Rules – M-net

The **SrvPrvder-SR** signaling rule (shown below) was used for the M-net SIP server. The **General** tab settings use the default values and are shown below.



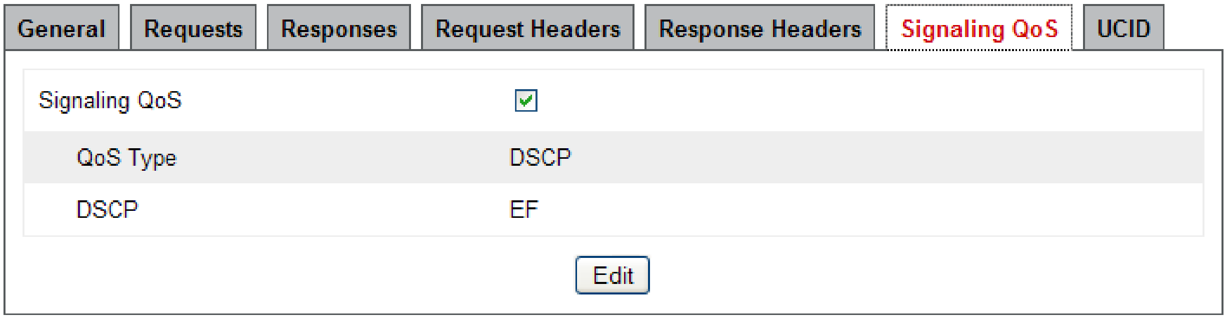
Inbound	
Requests	Allow
Non-2XX Final Responses	Allow
Optional Request Headers	Allow
Optional Response Headers	Allow

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	

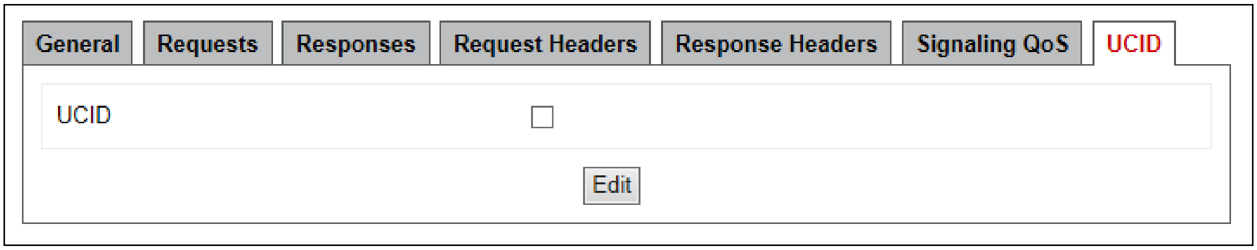
The **Requests**, **Responses**, **Requests Headers** and **Response Headers** tabs have no entries.

The **Signaling QoS** settings are shown below. This QoS setting is not a requirement for interoperability and QoS was not tested as part of the compliance test. If the QoS setting shown here does not meet the needs of the customer then it should be set as per customer requirements.



Signaling QoS	☑
QoS Type	DSCP
DSCP	EF

The **UCID** settings are shown below.

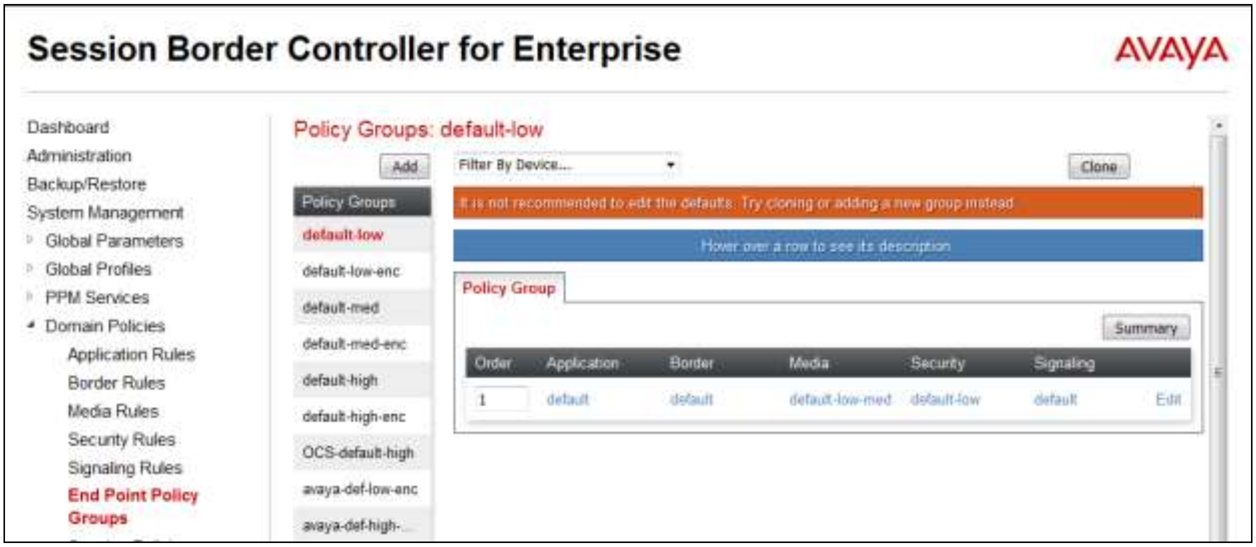


UCID ☐

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 an 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 one or more 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.



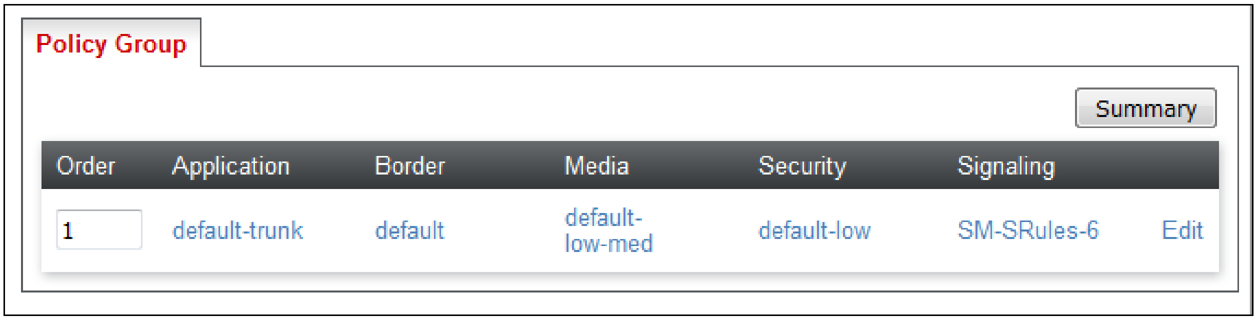
It is not recommended to edit the defaults. Try cloning or adding a new group instead.

Hover over a row to see its description

Order	Application	Border	Media	Security	Signaling	
1	default	default	default-low-med	default-low	default	Edit

7.11.1. Endpoint Policy Group – Session Manager

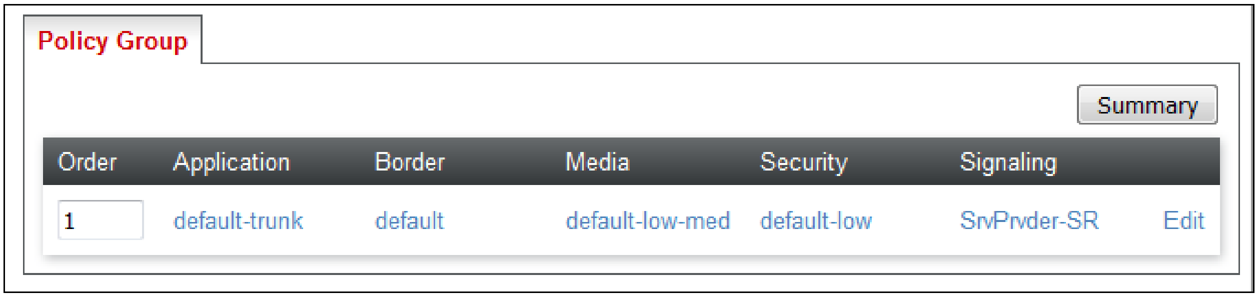
For the compliance test, endpoint policy group **SM-6.x** was created for Session Manager. Default values were used for each of the rules which comprise the group with the exception of **Application** and **Signaling**. For **Application**, enter the application rule created in **Section 7.8**. For **Signaling**, enter the signaling rule created in **Section 7.10.1**. The details of the default settings for **Media** are showed in **Section 7.9**.



Order	Application	Border	Media	Security	Signaling	
1	default-trunk	default	default-low-med	default-low	SM-SRules-6	Edit

7.11.2. Endpoint Policy Group – M-net

For the compliance test, endpoint policy group **General-SP** was created for the M-net SIP server. Default values were used for each of the rules which comprise the group with the exception of **Application** and **Signaling**. For **Application**, enter the application rule created in **Section 7.8**. For **Signaling**, enter the signaling rule created in **Section 7.10.2**. The details of the default settings for **Media** are showed in **Section 7.9**.

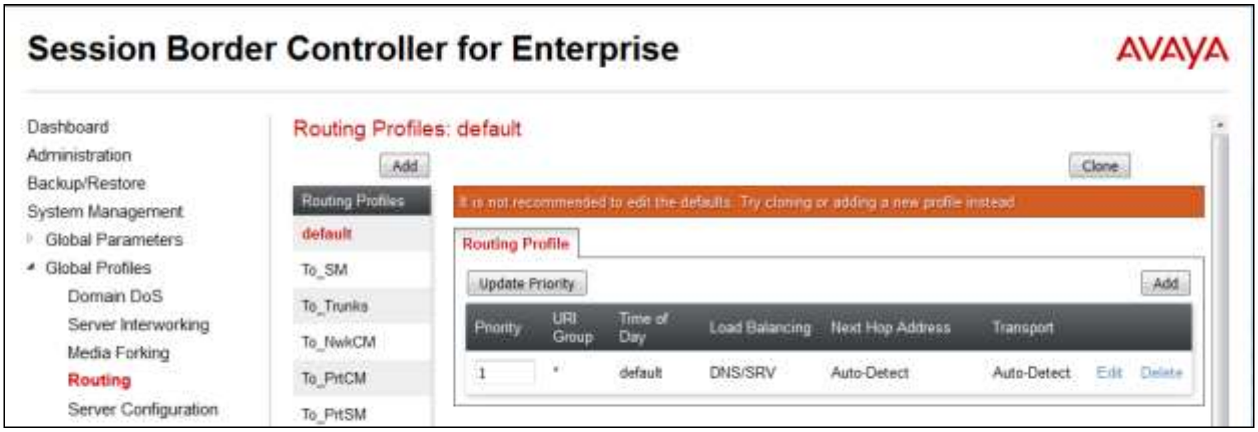


Order	Application	Border	Media	Security	Signaling	
1	default-trunk	default	default-low-med	default-low	SrvPrvder-SR	Edit

7.12. Routing

A routing profile defines where traffic will be directed based on the contents of the Request-URI. A routing profile is applied only after the traffic has matched an endpoint server flow defined in **Section 7.14**. Create a routing profile 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 one or more 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.



Routing Profiles: default

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

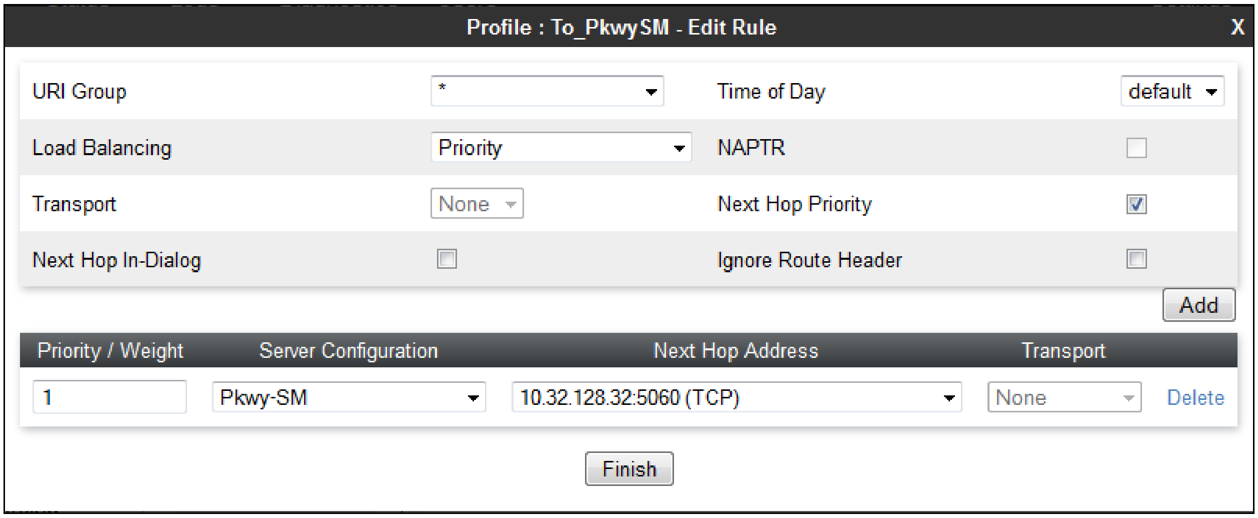
Priority	URI Group	Time of Day	Load Balancing	Next Hop Address	Transport		
1	*	default	DNS/SRV	Auto-Detect	Auto-Detect	Edit	Delete

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 **Load Balancing** to **Priority** from the pull-down menu.
- Enable **Next Hop Priority**.
- Click **Add** to enter the following for the Next Hop Address:
  - Set **Priority/Weight** to **1**.
  - For **Server Configuration**, select **Pkwy-SM** (**Section 7.7.1**) from the pull-down menu. The **Next Hop Address** will be filled-in automatically.

Click **Finish**.



Profile : To_PkwySM - Edit Rule

URI Group	*	Time of Day	default
Load Balancing	Priority	NAPTR	☐
Transport	None	Next Hop Priority	☑
Next Hop In-Dialog	☐	Ignore Route Header	☐

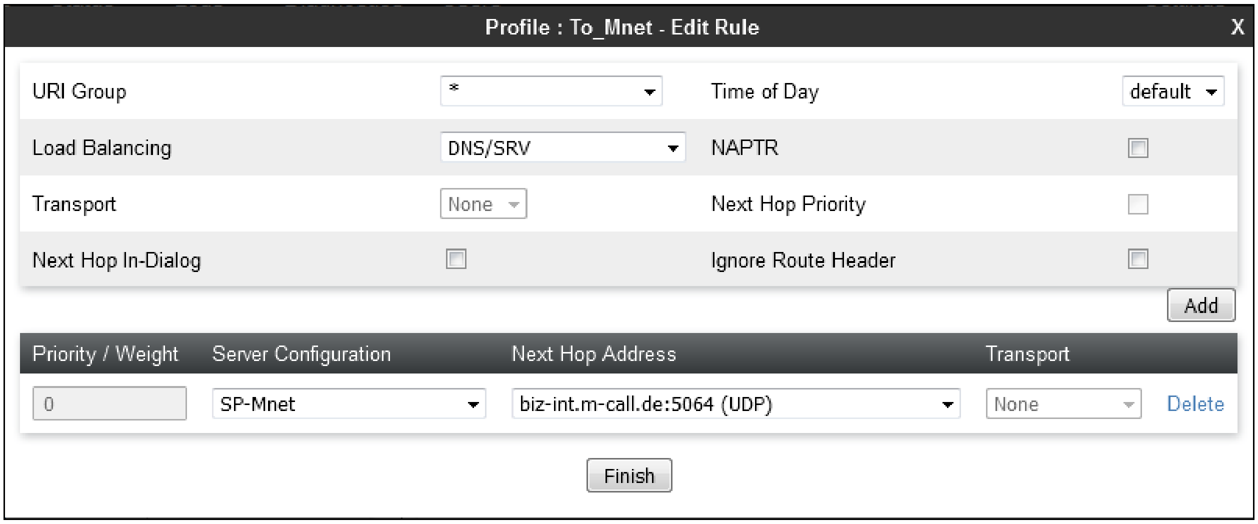
Priority / Weight	Server Configuration	Next Hop Address	Transport
1	Pkwy-SM	10.32.128.32:5060 (TCP)	None

7.12.2. Routing – M-net

For the compliance test, routing profile **To_Mnet** was created for M-net. When creating the profile, configure the parameters as follows:

- Set the **URI Group** to the wild card ***** to match on any URI.
- Set **Load Balancing** to **DNS/SRV** from the pull-down menu.
- Click **Add** to enter the following for the Next Hop Address:
  - For **Server Configuration**, select **SP-Mnet** (**Section 7.7.2**) from the pull-down menu. The **Next Hop Address** will be filled-in automatically.

Click **Finish**.



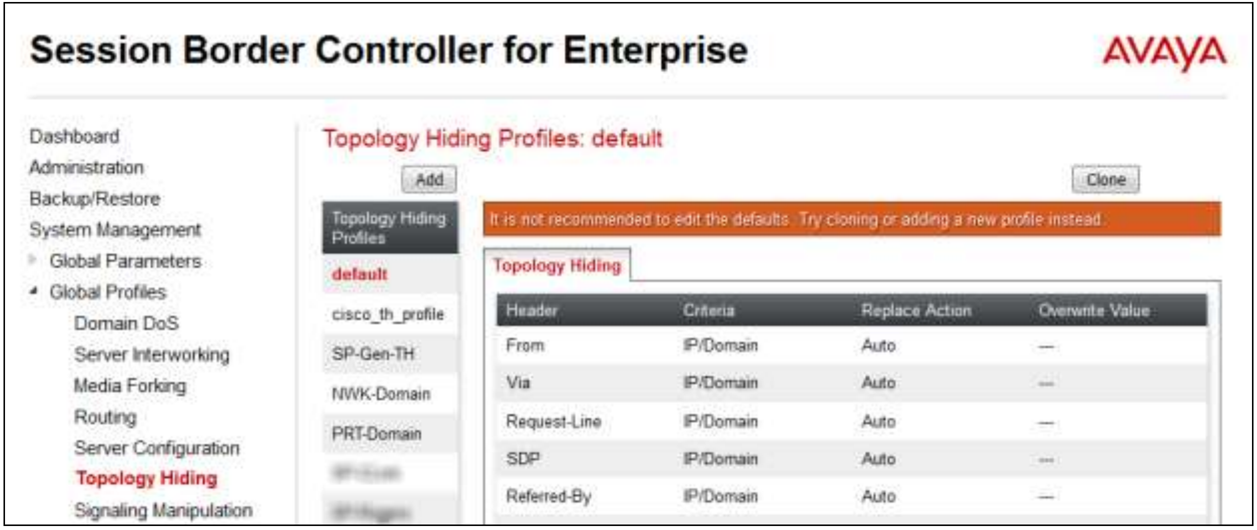
URI Group: *
Time of Day: default
Load Balancing: DNS/SRV
NAPTR: ☐
Transport: None
Next Hop Priority: ☐
Next Hop In-Dialog: ☐
Ignore Route Header: ☐

Priority / Weight	Server Configuration	Next Hop Address	Transport
0	SP-Mnet	biz-int.m-call.de:5064 (UDP)	None

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.



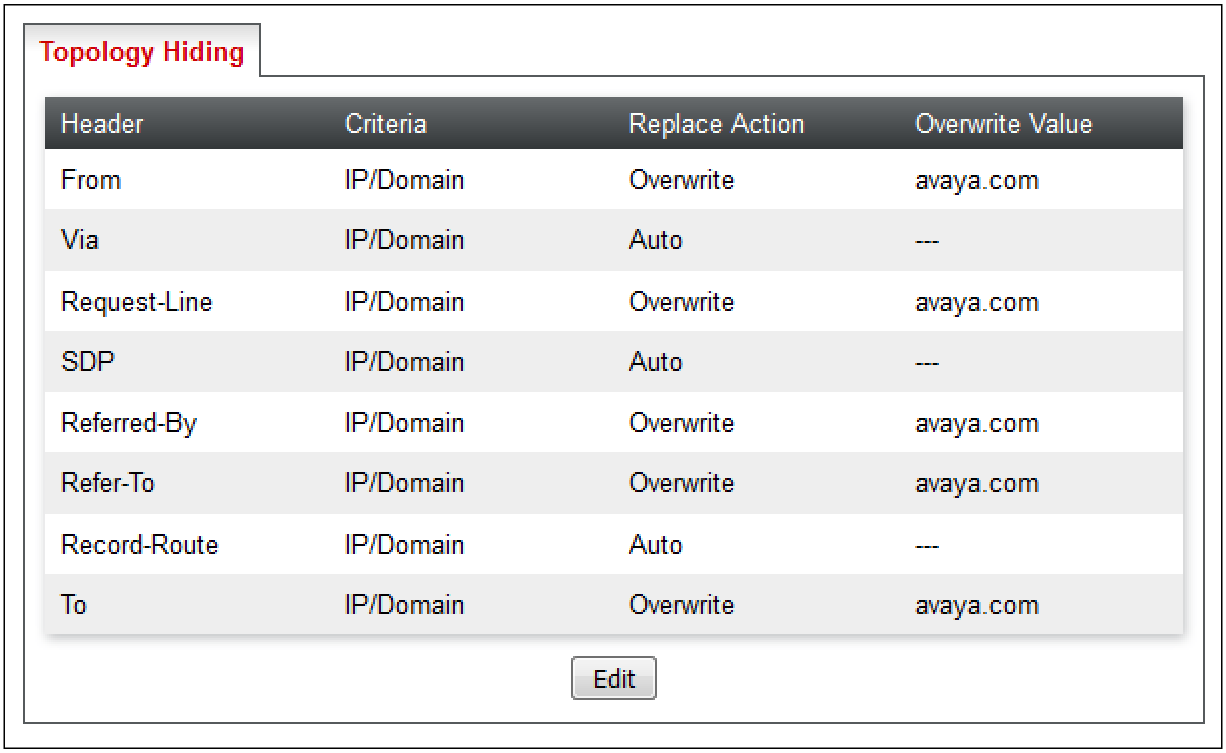
It is not recommended to edit the defaults. Try cloning or adding a new profile instead.

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

7.13.1. Topology Hiding – Session Manager

For the compliance test, topology hiding profile **PRT-Domain2** 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**, **Referred-By**, **Refer-To**, **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**).

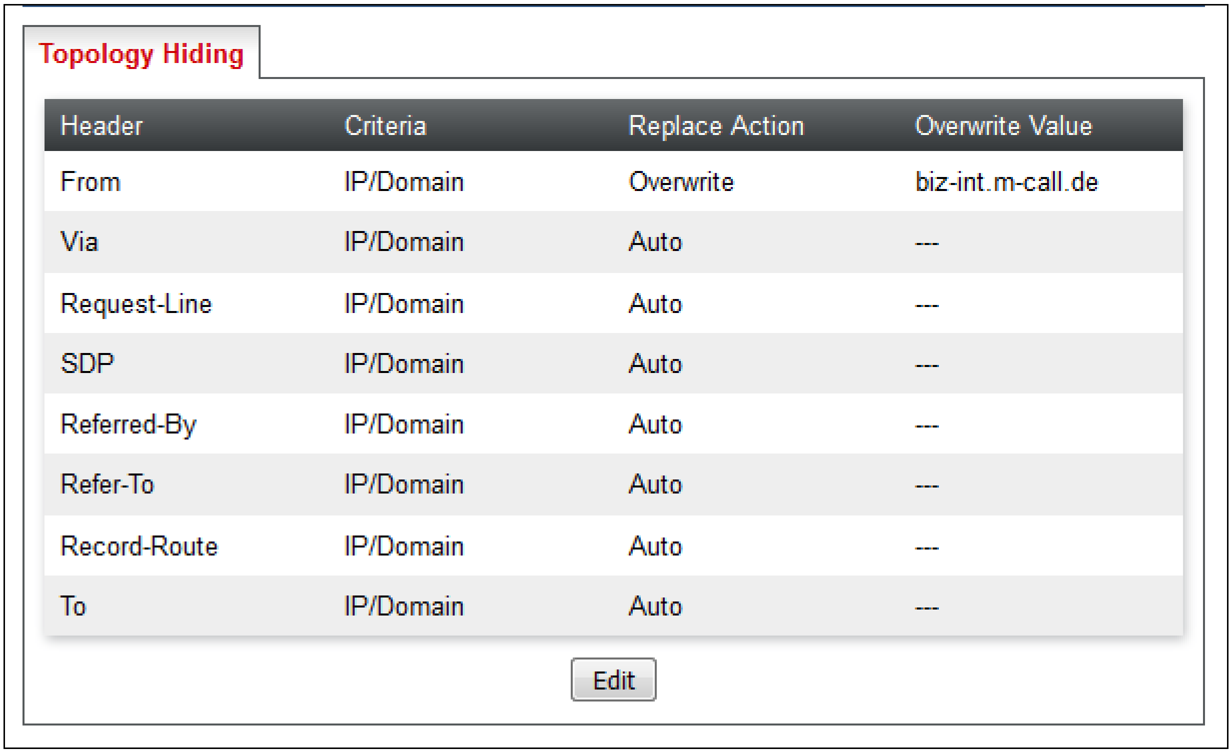


Header	Criteria	Replace Action	Overwrite Value
From	IP/Domain	Overwrite	avaya.com
Via	IP/Domain	Auto	---
Request-Line	IP/Domain	Overwrite	avaya.com
SDP	IP/Domain	Auto	---
Referred-By	IP/Domain	Overwrite	avaya.com
Refer-To	IP/Domain	Overwrite	avaya.com
Record-Route	IP/Domain	Auto	---
To	IP/Domain	Overwrite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

7.13.2. Topology Hiding – M-net

For the compliance test, topology hiding profile **SP-Mnet-TH** was created for M-net. This profile will be applied to traffic from the Avaya SBCE to M-net. 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 **From** which should be set to **Overwrite**. It was necessary to overwrite the From header for registration to work properly. The **Replace Action** of **Auto** puts the public IP of the SBCE in the From header which causes the REGISTER message to return an error.
- For those headers to be overwritten, the **Overwrite Value** is set to the M-net domain (**biz-int.m-call.de**).

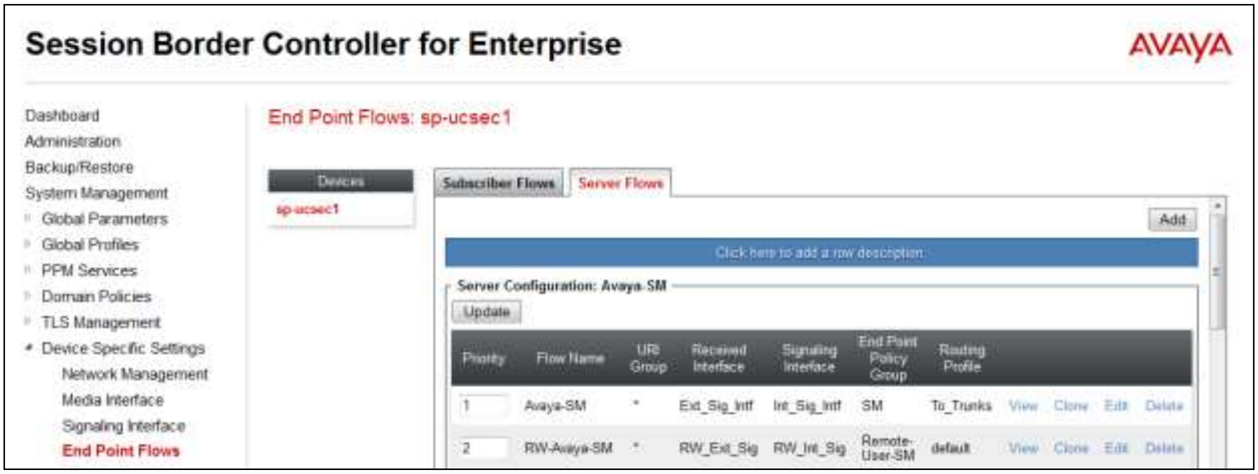


Header	Criteria	Replace Action	Overwrite Value
From	IP/Domain	Overwrite	biz-int.m-call.de
Via	IP/Domain	Auto	---
Request-Line	IP/Domain	Auto	---
SDP	IP/Domain	Auto	---
Referred-By	IP/Domain	Auto	---
Refer-To	IP/Domain	Auto	---
Record-Route	IP/Domain	Auto	---
To	IP/Domain	Auto	---

7.14. End Point Flows

Endpoint flows are used to determine the endpoints (connected servers) 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 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.



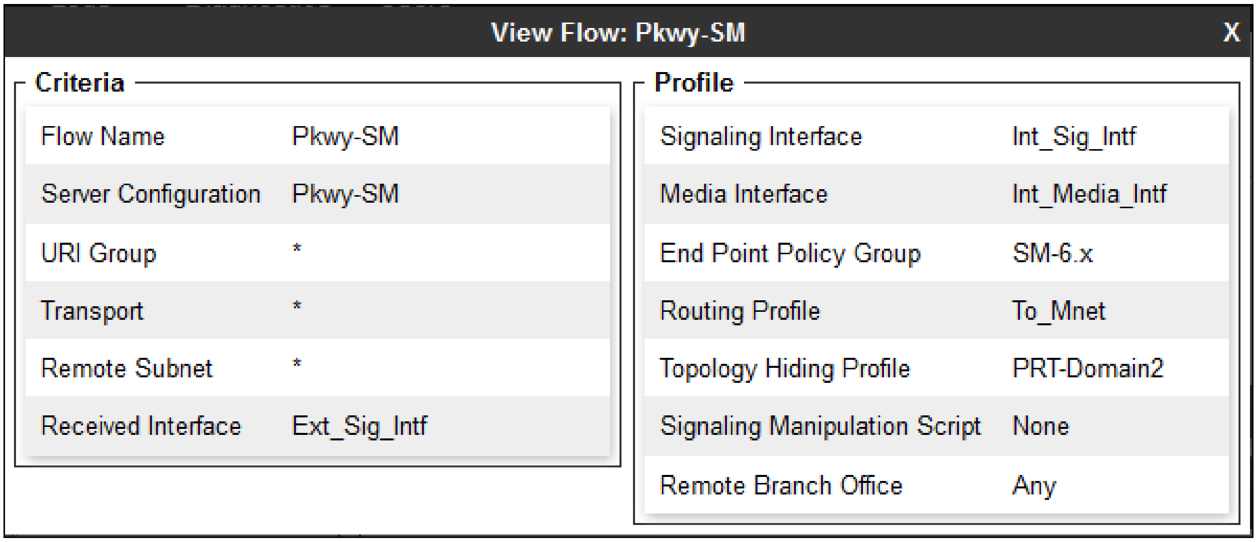
Server Configuration: Avaya-SM

Priority	Flow Name	URI Group	Received Interface	Signaling Interface	End Point Policy Group	Routing Profile				
1	Avaya-SM	*	Ext_Sig_Intf	Int_Sig_Intf	SM	To_Trunks	View	Clone	Edit	Delete
2	RW-Avaya-SM	*	RW_Ext_Sig	RW_Int_Sig	Remote-User-SM	default	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_Mnet** 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 the **Received Interface** to the external signaling interface (**Section 7.3**).
- Set the **Signaling Interface** to the internal signaling interface (**Section 7.3**).
- Set the **Media Interface** to the internal media interface (**Section 7.4**).
- 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 M-net SIP server.
- Set the **Topology Hiding Profile** to the topology hiding profile defined for Session Manager in **Section 7.13.1**.



Criteria

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

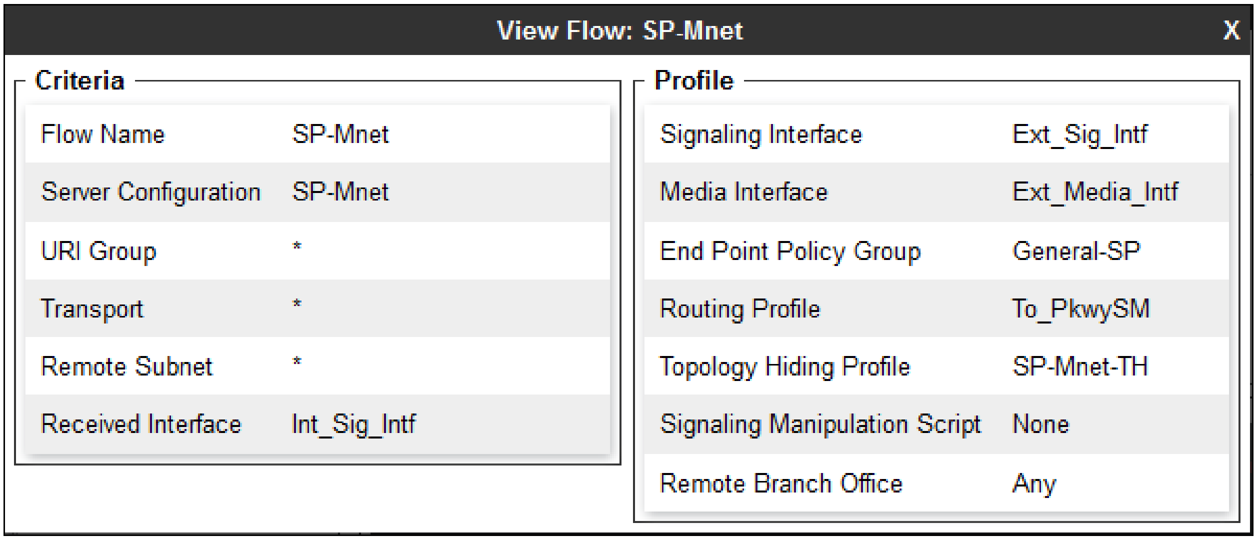
Profile

Signaling Interface	Int_Sig_Intf
Media Interface	Int_Media_Intf
End Point Policy Group	SM-6.x
Routing Profile	To_Mnet
Topology Hiding Profile	PRT-Domain2
Signaling Manipulation Script	None
Remote Branch Office	Any

7.14.2. End Point Flow – M-net

For the compliance test, endpoint flow **SP-Mnet** was created for the M-net SIP server. All traffic from M-net will match this flow as the source flow and use the specified **Routing Profile To_PkwySM** 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 M-net SIP server created in **Section 7.7.2**.
- To match all traffic, set the **URI Group**, **Transport**, and **Remote Subnet** to *.
- Set the **Received Interface** to the internal signaling interface (**Section 7.3**).
- Set the **Signaling Interface** to the external signaling interface (**Section 7.3**).
- Set the **Media Interface** to the external media interface (**Section 7.4**).
- Set the **End Point Policy Group** to the endpoint policy group defined for M-net in **Section 7.11.2**.
- Set the **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 M-net in **Section 7.13.2**.



View Flow: SP-Mnet

Criteria

Flow Name	SP-Mnet
Server Configuration	SP-Mnet
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	General-SP
Routing Profile	To_PkwySM
Topology Hiding Profile	SP-Mnet-TH
Signaling Manipulation Script	None
Remote Branch Office	Any

8. M-net Premium SIP Trunk Service Configuration

M-net is responsible for the network configuration and deployment of the M-net Premium SIP Trunk Service.

M-net will require that the customer provide the IP address and port number used to reach the Avaya SBCE at the edge of the enterprise. M-net will provide the FQDN and port number of the M-net SIP proxy/SBC, IP addresses/ports of media sources, SIP credentials and DDI numbers assigned to the enterprise. This information is used to complete the Communication Manager, Session Manager and 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 a 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.

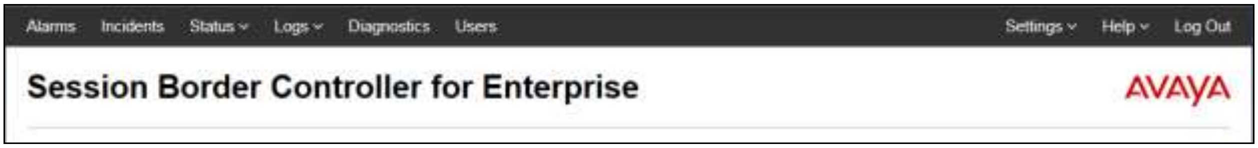
Troubleshooting:

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 access code number> - Displays real-time trunk group information.
    - **status trunk** <trunk access code number/channel number> - Displays real-time 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. Avaya Session Border Controller for Enterprise:
   There are several links and menus located on the taskbar at the top of the screen of the web interface that can provide useful diagnostic or troubleshooting information.

   - **Alarms**: This option provides information about active alarms.
   - **Incidents**: This option provides detailed reports of anomalies, errors, policies violations, etc.
   - **Status**: This option provides statistical and current status information.
   - **Diagnostics**: This option provides a variety of tools to test and troubleshoot the Avaya SBCE network connectivity.



10. Conclusion

These Application Notes describe the configuration necessary to connect Avaya Aura® Communication Manager, Avaya Aura® Session Manager and the Avaya Session Border Controller for Enterprise to the M-net Premium SIP Trunk Service. The M-net Premium SIP Trunk Service provides businesses a flexible, cost-saving alternative to traditional hardwired telephony trunks. Please refer to **Section 2.2** for 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.

[1] *Installing and Configuring Avaya Aura® System Platform*, Release 6.3, Issue 5, June 2015.

[2] *Administering Avaya Aura® System Platform*, Release 6.3, Issue 5, June 2015.

[3] *Administering Avaya Aura® Communication Manager*, Release 6.3, Document Number 03-300509, Issue 10, June 2015.

[4] *Avaya Aura® Communication Manager Feature Description and Implementation*, Release 6.3, Document Number 555-245-205, Issue 13, January 2016.

[5] *Upgrading Avaya Aura® System Manager on System Platform*, Release 6.3, Issue 5, October 2015.

[6] *Administering Avaya Aura® System Manager*, Release 6.3, Issue 8, December 2015.

[7] *Upgrading Avaya Aura® Session Manager*, Release 6.3, Issue 5, August 2014.

[8] *Administering Avaya Aura® Session Manager*, Release 6.3, Issue 7, September 2014.

[9] *Deploying Avaya Session Border Controller for Enterprise*, Release 7.0, Issue 1, August 2015.

[10] *Administering Avaya Session Border Controller for Enterprise*, Release 7.0, Issue 3, January 2016

[11] *Avaya 1600 Series IP Deskphones Administrator Guide Release*, Document Number 16-601438, Issue 7, May 2015.

[12] *Administering 9608/9808G/9611G/9621G/9641G/9641GS IP Deskphones Edition H.323*, Issue 1, April 2015.

[13] *Administering 9608/9808G/9611G/9621G/9641G/9641GS IP Deskphones Edition SIP*, Issue 2, August 2015.

[14] *Administering Avaya one-X® Communicator*, November 2015.

[15] *Administering Avaya Communicator for Android, iPad, iPhone, and Windows*, Release 2.1, Issue 5, September 2015.

[16] RFC 3261 *SIP: Session Initiation Protocol*, http://www.ietf.org/

[17] RFC 2833 *RTP Payload for DTMF Digits, Telephony Tones and Telephony Signals*, http://www.ietf.org/

12. Appendix A: M-net SIP Manipulation Script

```
// Signalling Manipulations created for interoperability
// with M-net 1/5/16
//
// Modification #1: If the Diversion header exists, modify the PAI and
// the Contact Headers using the contents of the Diversion header.

within session "INVITE"
{
 act on request where %DIRECTION="OUTBOUND" and %ENTRY_POINT="POST_ROUTING"
 {
  if (exists(%HEADERS["Diversion"][1])) then
  {
   %var1 = %HEADERS["Diversion"][1].URI.USER;
   %var2 = %HEADERS["Diversion"][1].DISPLAY_NAME;

   %HEADERS["Contact"][1].URI.USER = %var1;
   %HEADERS["Contact"][1].DISPLAY_NAME = %var2;

   %HEADERS["P-Asserted-Identity"][1].URI.USER = %var1;
   %HEADERS["P-Asserted-Identity"][1].DISPLAY_NAME = %var2;
  }
 }
}

// Modification #2: Remove "Bandwidth Information" line in SDP of any message
// to M-net. This value may change between 180 Ringing
// and 200 OK causing M-net to send a reINVITE to the enterprise
// which generally causes a 491 glare condition. This behavior was observed
// on all inbound calls to enterprise SIP phones.

within session "ALL"
{
 act on message where %DIRECTION="OUTBOUND" and %ENTRY_POINT="POST_ROUTING"
 {
  %BODY[1].regex_replace("b=(TIAS|AS):(\d+)\r\n","");
 }
}

// Modification #3: Set Max-Forwards header to 70 in outbound INVITE.
// Using EC500, sometimes Communication Manager would send an INVITE to
// the EC500 destination with a Max-Forwards of 7 which was too low to
// pass the M-net network.

within session "INVITE"
{
 act on request where %DIRECTION="OUTBOUND" and %ENTRY_POINT="POST_ROUTING"
 {
  if (exists(%HEADERS["Max-Forwards"][1])) then
  {
  %HEADERS["Max-Forwards"][1] = "70";
  }
 }
}
```

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.