Application Notes for Configuring Avaya Aura® Communication Manager Rel. 7.1, Avaya Aura® Session Manager Rel. 7.1 and Avaya Session Border Controller for Enterprise Rel. 7.2 to support Bell MTS SIP Trunking Service – Issue 1.0

Abstract

These Application Notes describe the procedures for configuring Session Initiation Protocol (SIP) Trunking Service on an enterprise solution consisting of Avaya Aura® Communication Manager Rel. 7.1, Avaya Aura® Session Manager Rel. 7.1 and Avaya Session Border Controller for Enterprise Rel. 7.2, to interoperate with the Bell MTS Communications SIP Trunking service.

The Bell MTS SIP Trunking service provide customers with PSTN access via a SIP trunk between the enterprise and the service provider's network, as an alternative to legacy analog or digital trunks. This approach generally results in lower cost for the enterprise.

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.

Table of Contents

1. Introduction 4
2. General Test Approach and Test Results 4
   2.1. Interoperability Compliance Testing 6
   2.2. Test Results 8
   2.3. Support 9
3. Reference Configuration 10
4. Equipment and Software Validated 13
5. Configure Avaya Aura® Communication Manager 14
   5.1. Licensing and Capacity 14
   5.2. System Features 15
   5.3. IP Node Names 17
   5.4. Codecs 17
   5.5. IP Network Regions 19
   5.6. Signaling Group 20
   5.7. Trunk Group 22
   5.8. Calling Party Information 25
   5.9. Inbound Routing 26
   5.10. Outbound Routing 27
6. Configure Avaya Aura® Session Manager 31
   6.1. System Manager Login and Navigation 32
   6.2. SIP Domain 33
   6.3. Locations 33
   6.4. Adaptations 36
   6.5. SIP Entities 38
   6.6. Entity Links 41
   6.7. Routing Policies 42
   6.8. Dial Patterns 43
7. Configure Avaya Session Border Controller for Enterprise 46
   7.1. System Access 46
   7.2. System Management 47
   7.3. Network Management 50
   7.4. Media Interfaces 51
   7.5. Signaling Interfaces 53
   7.6. Server Interworking 55
      7.6.1. Server Interworking Profile – Enterprise 55
      7.6.2. Server Interworking Profile – Service Provider 58
   7.7. Signaling Manipulation 59
      7.7.1. Signaling Manipulation – Enterprise 59
      7.7.2. Signaling Manipulation – Service Provider 60
   7.8. Server Configuration 61
      7.8.1. Server Configuration Profile – Enterprise 61
      7.8.2. Server Configuration Profile – Service Provider 63

7.9. Routing ... 66

7.9.1. Routing Profile – Enterprise ... 66

7.9.2. Routing Profile – Service Provider ... 67

7.10. Topology Hiding ... 68

7.10.1. Topology Hiding Profile – Enterprise ... 69

7.10.2. Topology Hiding Profile – Service Provider ... 70

7.11. Domain Policies ... 71

7.11.1. Application Rules ... 71

7.11.2. Media Rules ... 72

7.11.3. Signaling Rules ... 75

7.12. End Point Policy Groups ... 76

7.12.1. End Point Policy Group – Enterprise ... 76

7.12.2. End Point Policy Group – Service Provider ... 77

7.13. End Point Flows ... 78

7.13.1. End Point Flow – Enterprise ... 79

7.13.2. End Point Flow – Service Provider ... 81

8. Bell MTS SIP Trunking Service Configuration ... 82

9. Verification and Troubleshooting ... 82

9.1. General Verification Steps ... 82

9.2. Communication Manager Verification ... 82

9.3. Session Manager Verification ... 83

9.4. Avaya SBCE Verification ... 84

10. Conclusion ... 88

11. References ... 88

1. Introduction

These Application Notes describe the procedures for configuring Session Initiation Protocol (SIP) Trunking Service between the Bell MTS network and an Avaya SIP-enabled enterprise solution. The Avaya solution consists of Avaya Aura® Communication Manager Rel. 7.1 (Communication Manager), Avaya Aura® Session Manager Rel. 7.1 (Session Manager), Avaya Session Border Controller for Enterprise Rel. 7.2 (Avaya SBCE) and various Avaya endpoints, listed in **Section 4**.

The Bell MTS SIP Trunking service referenced within these Application Notes is designed for business customers. Customers using this service with this Avaya enterprise solution are able to place and receive PSTN calls via a broadband WAN connection and the SIP protocol. This converged network solution is an alternative to traditional PSTN trunks such as analog and/or ISDN-PRI.

The terms “Service Provider”, “Bell MTS” or “MTS” will be used interchangeably throughout these Application Notes.

2. General Test Approach and Test Results

A simulated CPE site containing all the equipment for the Avaya SIP-enabled enterprise solution was installed at the Avaya Solution and Interoperability Lab. The enterprise site was configured to connect to the Bell MTS network via a broadband connection to the public Internet.

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

Avaya recommends our customers implement Avaya solutions using appropriate security and encryption capabilities enabled by our products. The testing referenced in this DevConnect Application Note included the enablement of supported encryption capabilities in the Avaya products only (private network side). Readers should consult the appropriate Avaya product documentation for further information regarding security and encryption capabilities supported by those Avaya products.

Support for these security and encryption capabilities in any non-Avaya solution component is the responsibility of each individual vendor. Readers should consult the appropriate vendor-supplied product documentation for more information regarding those products.

For the compliance testing associated with this Application Notes, the interface between the Avaya system and the MTS network did not include the use of any specific encryption features, UDP Transport for signaling and RTP for media was used between the Avaya system and the MTS network across the SIP trunk. TLS transport for signaling and SRTP for media was used inside of the enterprise (private network side, in between Avaya components).

2.1. Interoperability Compliance Testing

To verify SIP trunk interoperability, the following features and functionality were covered during the interoperability compliance test:

- SIP Trunk registration and response to SIP OPTIONS queries.
- Incoming calls from the PSTN were routed to DID numbers assigned by MTS. Incoming PSTN calls were terminated to the following endpoints: Avaya 96x1 Series IP Deskphones (H.323 and SIP), Avaya 9408 Digital Deskphones, Avaya one-X® Communicator softphone (H.323 and SIP), Avaya Equinox softphone (SIP) and analog Deskphones.
- Inbound and outbound PSTN calls to/from Remote Workers using Avaya 96x1 Deskphones (SIP).
- Outgoing calls to the PSTN were routed via MTS's network to various PSTN destinations.
- Proper disconnect when the caller abandons the call before the call is answered.
- Proper disconnect via normal call termination by the caller or the called parties.
- Proper disconnect by the network for calls that are not answered (with voicemail off).
- Proper response to busy endpoints.
- Proper response/error treatment when dialing invalid PSTN numbers.
- Proper Codec negotiation and two way speech-path. Testing was performed with codecs: G.711MU and G.729.
- No matching codecs.
- Voicemail and DTMF tone support (leaving and retrieving voice mail messages, etc.).
- Outbound Toll-Free calls, interacting with IVR (Interactive Voice Response systems).
- Calling number blocking (Privacy).
- Call Hold/Resume (long and short duration).
- Call Forward (unconditional, busy, no answer).
- Blind Call Transfers.
- Consultative Call Transfers.
- Station Conference.
- EC500 (Extension to Cellular) calls.
- T.38 fax.
- Simultaneous active calls.
- Long duration calls (over one hour).
- Proper response/error treatment to all trunks busy.
- Proper response/error treatment when disabling SIP connection.

Note – Remote Worker was tested as part of this solution. The configuration necessary to support remote workers is beyond the scope of these Application Notes and is not included in these Application Notes.

The following items were not tested:

- Inbound toll-free calls, 911 calls (emergency), “0” calls (Operator), 411 Directory Assistance, and 0+10 digits calls (Operator Assisted) were not tested.
- The SIP REFER method for call redirection is supported but is not preferred by Bell MTS, refer to **Section 2.2**.

2.2. Test Results

Interoperability testing of the Bell MTS SIP Trunking Service with the Avaya SIP-enabled enterprise solution was completed with successful results for all test cases with the observations/limitations noted below:

- **T.38 Fax**: With Communication Manager configured as "T.38-G711-fallback", on outgoing fax calls from Communication Manager to the PSTN, MTS did not send the re-INVITE message to Communication Manager to switch from G.711 audio to T.38 fax within the 4 seconds time-out interval expected by Communication Manager, this caused Communication Manager to send a re-INVITE message to MTS for G.711 pass-through, this resulted on the fax being sent via G.711 pass-through however in the middle of fax transmission MTS sent re-INVITE for T.38 fax Communication Manager responded with "488 Fax Request Rejected" and caused the fax was interrupted. It recommends configuring as "**T.38-standard**" for fax working in both ways (refer to **Section 5.4**).
- **SIP OPTIONS**: SIP OPTIONS messages sent by MTS to the enterprise having the format like "sip:ping@sipdomain.com" that causes Session Manager to respond with "404 Not Found (No route available)". Since the SIP OPTIONS messages sent by MTS to the enterprise were intended for link monitoring and to keep the SIP trunk UP. The signaling manipulation script was applied for the enterprise to address this issue (refer to **Section 7.7.1**).
- **Network Call Redirection**: Both REFER and re-INVITEs for the network call redirection are supported by MTS but re-INVITEs method is preferred by MTS and all the network call redirection test scenarios during the compliance test were configured with this method (Network Call Redirection set to N, refer to **Section 5.7**).
- **Incorrect Call Display on call transfers to the PSTN Phone**: Call display was not properly updated on PSTN phones involved in a call transfers. After successful call transfers to the PSTN, the PSTN phone did not display the actual connected party, instead the DID number assigned to the enterprise station that initiated the transfer was displayed.
- **SIP header optimization**: There are multiple SIP headers and parameters used by Communication Manager and Session Manager, some of them Avaya proprietary, that had no significance in the service provider's network. These headers were removed with the purpose of blocking enterprise information from being propagated outside of the enterprise boundaries, to reduce the size of the packets entering the service provider's network and to improve the solution interoperability in general. The following headers were removed from outbound messages using an Adaptation in Session Manager: AV-Global-Session-ID, AV-Correlation-ID, Alert-Info, Endpoint-View, P-AV-Message-id, P-Charging-Vector and P-Location (**Section 6.4**).
- **Inbound privacy call**: Inbound privacy call from PSTN to the enterprise station was established successfully but as the enterprise station hung up the PSTN phone was still in the call, this was because MTS added an internal IP address in the **Contact** header that caused Avaya SBCE sent **BYE** message to the MTS internal IP address instead of the MTS SIP proxy IP address. The signaling manipulation scrip was applied to remove the internal IP address of MTS to address this issue (refer to **Section 7.7.2**).
- **Outbound privacy call**: Outbound privacy call from the enterprise station to PSTN, Communication Manager used the Privacy header and sent the format like "

"Anonymous" sip:anonymous@anonymous.invalid" in the **From** header but MTS was not able to scan this for the outbound privacy call and it also could not scan the same in the P-Asserted-Identity header, this resulted in the calling number from the enterprise station still shown up in the PSTN phone. The signaling manipulation script was applied to keep only "Anonymous" for the caller name in the **From** header to address this issue (refer to **Section 7.7.2**).

- **Direct IP-IP Audio Connections**: The Direct IP-IP Audio Connections must be set to N in the signaling group in Communication Manager for the solution to work (refer to **Section 5.6**). The reason was that as the enterprise SIP station made outbound call to PSTN, Communication Manager is using re-INVITE without SDP to establish the direct media between the SIP station and internal media interface of Avaya SBCE. Since Avaya SBCE passes the re-INVITE message to MTS and MTS responds 200 OK with SDP having the two m lines for audio and T.38 fax, Communication Manager then used the SDP from the 200 OK to build a re-INVITE message and send it to the SIP station in process of negotiating the direct media but as soon as the SIP station sees the m line for T.38 fax it responds back with "488 Not Acceptable Here", at this point the call was established successfully but it obtained the media resource from either Media Gateway or Media Server for the call. This behavior happens on Avaya 96x1 Deskphones but it is different on Avaya Equinox and one-X Communicator SIP softphones. Below is the list of issues that are related to the T.38 fax included in INVITE message or 200 OK SDP from MTS and the Direct IP-IP Audio Connections is set to Y:
    - The outbound call to PSTN from Avaya Equinox was dropped as soon as the PSTN answered the call. As explained above, Avaya Equinox sent back 200 OK with SDP having only m line for audio while Communication Manager was expecting 200 SDP with T.38 fax and then Communication Manager sends BYE to Avaya Equinox and MTS.
    - The outbound call to PSTN from Avaya one-X Communicator had no audio. As explained above, Avaya one-X Communicator sends back "500 Internal Error (SDP Offer Mismatch)" for the re-INVITE message from Communication Manager. The call was established and took the media resource but there was no audio.
    - Incoming call from PSTN was blind transferred by an enterprise station to PSTN had no audio.
    - Incoming call from PSTN off-net forwarded by an enterprise station to PSTN number had no audio.
    - Extension to cellular had no audio for PSTN call to an enterprise and picked up by EC500 cellular phone.

2.3. Support

For support on Bell MTS SIP Trunking Service visit the corporate Web page at: https://MTS.com/enterprise

3. Reference Configuration

Figure 1 illustrates the sample Avaya SIP-enabled enterprise solution, connected to the Bell MTS SIP Trunking Service through a public Internet WAN connection.

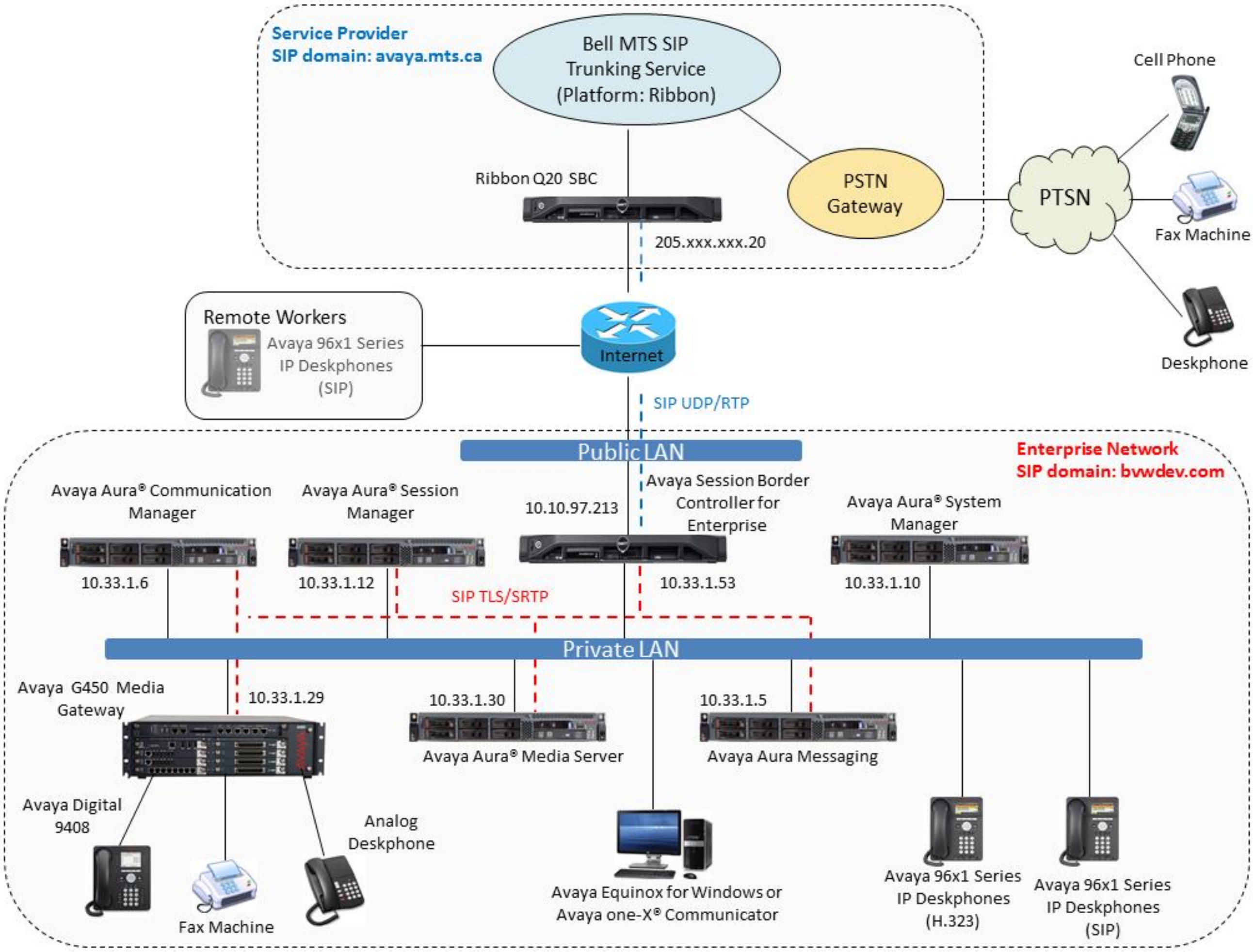


Figure 1: **Avaya SIP Enterprise Solution connected to Bell MTS SIP Trunking Service**

The Avaya components used to create the simulated enterprise customer site included:

- Avaya Aura® Communication Manager.
- Avaya Aura® Session Manager.
- Avaya Aura® System Manager.
- Avaya Session Border Controller for Enterprise.
- Avaya Aura® Messaging.
- Avaya Aura® Media Server.
- Avaya G450 Media Gateway.
- Avaya 96x1 Series IP Deskphones (H.323 and SIP).
- Avaya one-X® Communicator softphones (H.323 and SIP).
- Avaya Equinox softphone (SIP).
- Avaya digital and analog telephones.

Additionally, the reference configuration included remote worker functionality. A remote worker is a SIP endpoint that resides in the untrusted network, registered to Session Manager at the enterprise via the Avaya SBCE. Remote workers offer the same functionality as any other endpoint at the enterprise. This functionality was successfully tested during the compliance test using only the Avaya 96x1 SIP Deskphones. For signaling, Transport Layer Security (TLS) and for media, Secure Real-time Transport Protocol (SRTP) was used on Avaya 96x1 SIP Deskphones used to test remote worker functionality. Other Avaya SIP endpoints that are supported in a Remote Worker configuration deployment were not tested.

The configuration tasks required to support remote workers are beyond the scope of these Application Notes; hence they are not discussed in this document. Consult [**9**] in the **References** section for additional information on this topic.

The Avaya SBCE was located at the edge of the enterprise. Its public side was connected to the public Internet, while its private side was connected to the enterprise infrastructure. All signaling and media traffic entering or leaving the enterprise flowed through the Avaya SBCE, protecting in this way the enterprise against any SIP-based attacks. The Avaya SBCE also performed network address translation at both the IP and SIP layers.

For inbound calls, the calls flowed from the service provider to the Avaya SBCE then to Session Manager. Session Manager used 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 arrived at Communication Manager, further incoming call treatment, such as incoming digit translation was performed.

Outbound calls to the PSTN were first processed by Communication Manager for outbound feature treatment such as automatic route selection and class of service restrictions. Once Communication Manager selected the proper SIP trunk, the call was routed to Session Manager. Session Manager once again used the configured dial patterns (or regular expressions) and routing policies to determine the route to the Avaya SBCE for egress to the MTS network.

A separate SIP trunk was created between Communication Manager and Session Manager to carry the service provider traffic. This was done so that any trunk or codec settings required by the service provider could be applied only to this trunk without affecting other enterprise SIP traffic. This trunk carried both inbound and outbound traffic.

As part of the Avaya Aura® version 7.1 release, Communication Manager incorporates the ability to use the Avaya Aura® Media Sever (AAMS) as a media resource. The AAMS is a software-based, high density media server that provides DSP resources for IP-based sessions. Media resources from both the AAMS and a G450 Media Gateway were utilized during the compliance test. The configuration of the AAMS is not discussed in this document. For more information on the installation and administration of the AAMS in Communication Manager refer to the AAMS documentation listed in the **References** section.

Avaya Aura® Messaging was used during the compliance test to verify voice mail redirection and navigation, as well as the delivery of Message Waiting Indicator (MWI) messages to the enterprise telephones. Since the configuration tasks for Messaging are not directly related to the interoperability tests with the MTS network SIP Trunking service, they are not included in these Application Notes.

4. Equipment and Software Validated

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

Equipment/Software	Release/Version
Avaya	
Avaya Aura® Communication Manager	R017x.01.0.532.0 (01.0.532.0-24515)
Avaya Aura® Session Manager	7.1.3.0 (7.1.3.0.713014)
Avaya Aura® System Manager	7.1.3.0 Build No. 7.1.0.0.1125193 Software Update Rev. No. 7.1.3.0.037763
Avaya Session Border Controller for Enterprise	ASBCE 7.2 7.2.1.0-05-14222
Avaya Aura® Messaging	7.0 Service Pack 0 (MSG-00.0.441.0-017_0004)
Avaya Aura® Media Server	7.8.0.333 SP5 7.8.0.333_2017.07.17
Avaya G450 Media Gateway	G450_sw_39_12_0
Avaya 96x1 Series IP Deskphones (SIP)	Version 7.1.2.0.4
Avaya 96x1 Series IP Deskphones (H.323)	Version 6.6604
Avaya one-X® Communicator (H.323, SIP)	6.2.12.22-SP12
Avaya Equinox (SIP)	3.4.0.18
Avaya 2420 Series Digital Deskphones	N/A
Avaya 6210 Analog Deskphones	N/A
Bell MTS	
Ribbon Application Server	CVM17
Ribbon Q20 SBC	9.3

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

Note – The Avaya Aura® servers and the Avaya SBCE used in the reference configuration and shown on the previous table were deployed on a virtualized environment. These Avaya components ran as virtual machines over VMware® (ESXi 6.0.0) platforms. Consult the installation documentation on the **References** section for more information.

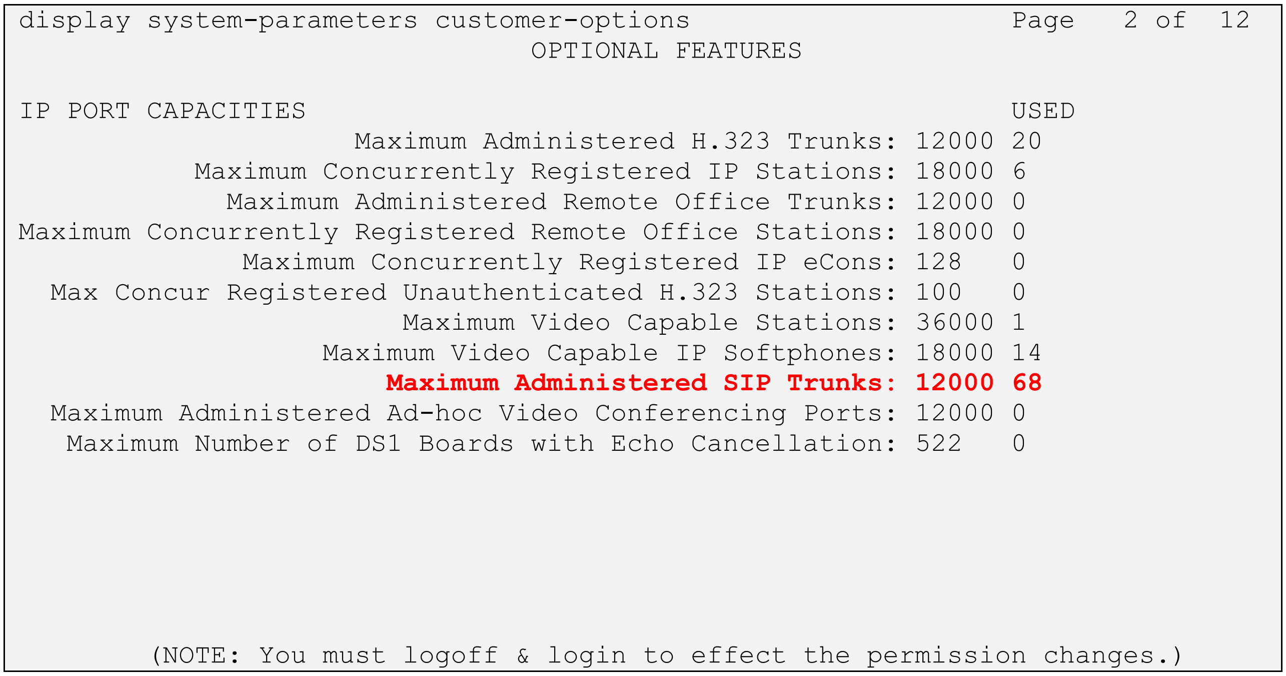
5. Configure Avaya Aura® Communication Manager

This section describes the procedure for configuring Communication Manager to work with the MTS network SIP Trunking service. A SIP trunk is established between Communication Manager and Session Manager for use by signaling traffic to and from the service provider. It is assumed that the general installation of Communication Manager, the Avaya G450 Media Gateway and the Avaya Aura® Media Server 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. Some screens captures will show the use of the **change** command instead of the **add** command, since the configuration used for the testing was previously added.

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 and from the service provider. The example shows that **12000** licenses are available and **68** 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.



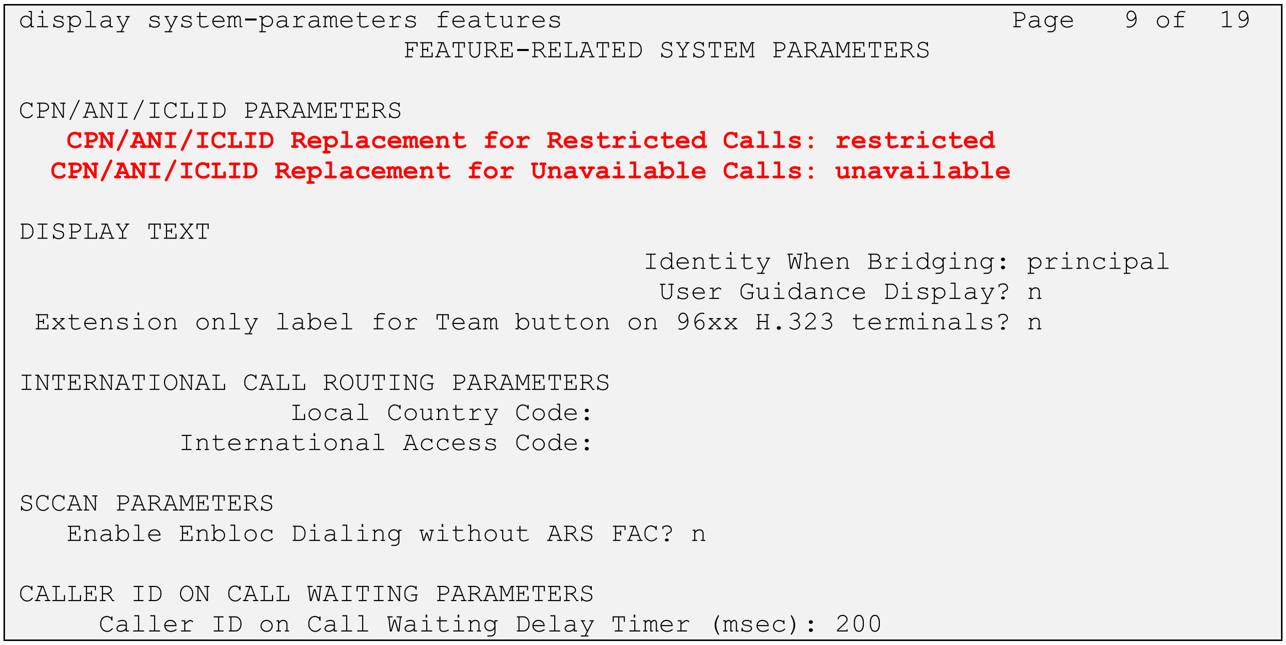
```
display system-parameters customer-options                      Page   2 of  12
                                OPTIONAL FEATURES

IP PORT CAPACITIES                                              USED
                     Maximum Administered H.323 Trunks: 12000 20
           Maximum Concurrently Registered IP Stations: 18000 6
             Maximum Administered Remote Office Trunks: 12000 0
Maximum Concurrently Registered Remote Office Stations: 18000 0
              Maximum Concurrently Registered IP eCons: 128   0
  Max Concur Registered Unauthenticated H.323 Stations: 100   0
                        Maximum Video Capable Stations: 36000 1
                   Maximum Video Capable IP Softphones: 18000 14
                       Maximum Administered SIP Trunks: 12000 68
  Maximum Administered Ad-hoc Video Conferencing Ports: 12000 0
   Maximum Number of DS1 Boards with Echo Cancellation: 522   0









        (NOTE: You must logoff & login to effect the permission changes.)
```

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***.

```
display system-parameters features                           Page   1 of  19
                            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
                             Music/Tone on Hold: music Type: ext    1104
              Music (or Silence) on Transferred Trunk Calls? no
              DID/Tie/ISDN/SIP Intercept Treatment: attendant
    Internal Auto-Answer of Attd-Extended/Transferred Calls: transferred
                  Automatic Circuit Assurance (ACA) Enabled? n




             Abbreviated Dial Programming by Assigned Lists? n
       Auto Abbreviated/Delayed Transition Interval (rings): 2
                    Protocol for Caller ID Analog Terminals: Bellcore
    Display Calling Number for Room to Room Caller ID Calls? n
```

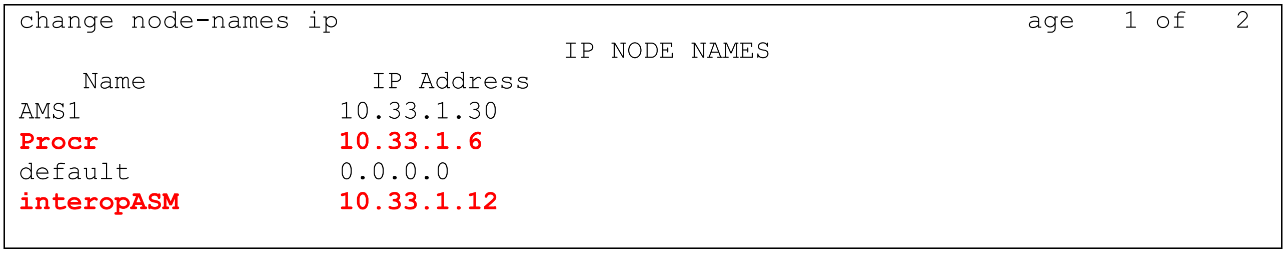
On **Page 9** verify that a text string has been defined to replace the Calling Party Number (CPN) for restricted or unavailable calls. This text string is entered in the two fields highlighted below. The compliance test used the value of ***restricted*** for restricted calls and ***unavailable*** for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



```
display system-parameters features                               Page   9 of  19
                        FEATURE-RELATED SYSTEM PARAMETERS

CPN/ANI/ICLID PARAMETERS
   CPN/ANI/ICLID Replacement for Restricted Calls: restricted
  CPN/ANI/ICLID Replacement for Unavailable Calls: unavailable

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

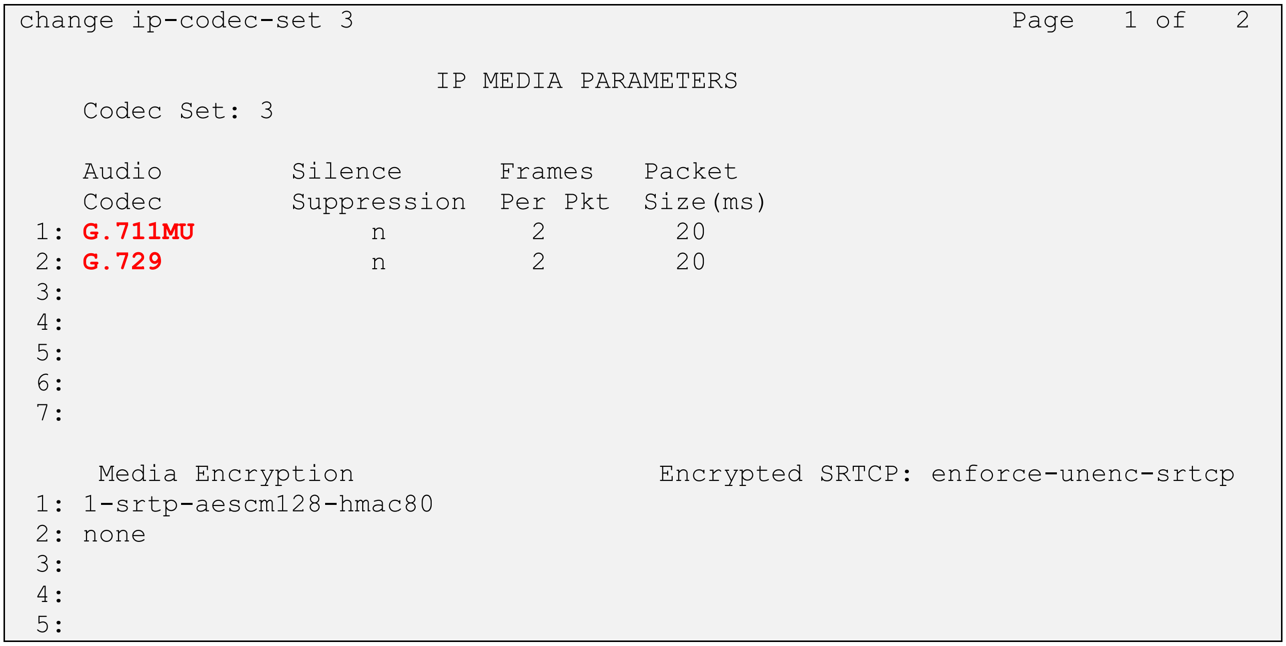
Use the **change node-names ip** command to verify that node names have been previously defined for the IP addresses of Communication Manager **(proc**r) and the Session Manager security module (**interopASM**). These node names will be needed for defining the service provider signaling group in **Section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



```
change node-names ip                                            age    1 of    2
                                  IP NODE NAMES
    Name                  IP Address
AMS1                    10.33.1.30
Procr                   10.33.1.6
default                 0.0.0.0
interopASM              10.33.1.12
```

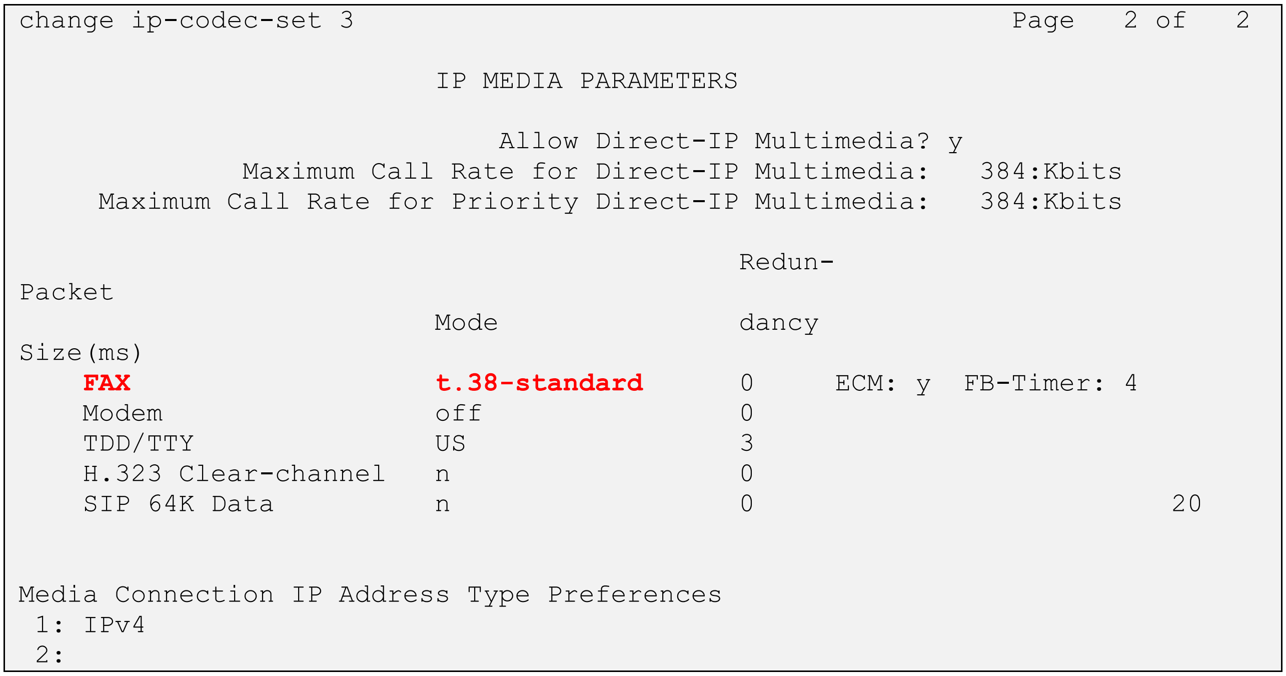
5.4. Codecs

Use the **change ip-codec-set** command to define a list of codecs to use for calls between the enterprise and the service provider. For the compliance test, ip-codec-set 3 was used for this purpose. Enter the corresponding codec in the **Audio Codec** column of the table. MTS supports audio codecs ***G.711MU*** and ***G.729***.



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

                          IP MEDIA PARAMETERS
    Codec Set: 3

    Audio        Silence      Frames   Packet
    Codec        Suppression  Per Pkt  Size(ms)
 1: G.711MU           n          2        20
 2: G.729             n          2        20
 3:
 4:
 5:
 6:
 7:

     Media Encryption                   Encrypted SRTCP: enforce-unenc-srtcp
 1: 1-srtp-aescm128-hmac80
 2: none
 3:
 4:
 5:
```

On **Page 2**, set the **Fax Mode** to ***t.38-standard*** (refer to **Section 2.2**).

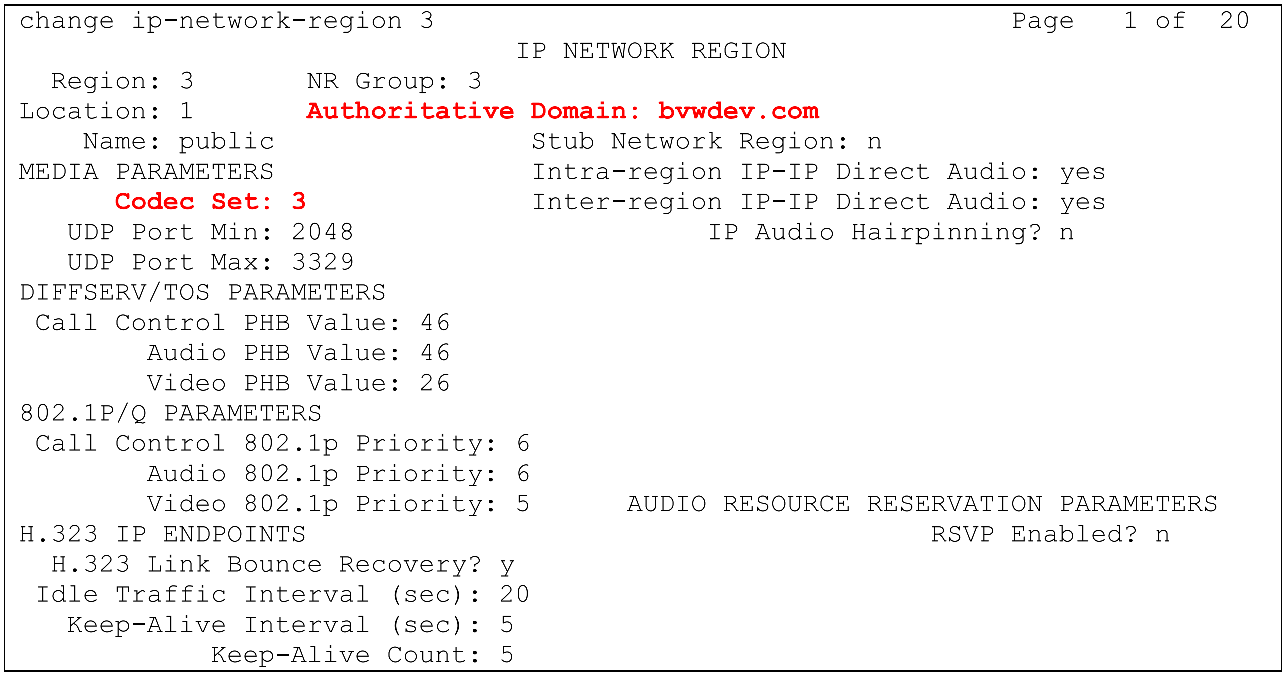


```
change ip-codec-set 3                                         Page    2 of    2

                          IP MEDIA PARAMETERS

                              Allow Direct-IP Multimedia? y
              Maximum Call Rate for Direct-IP Multimedia:   384:Kbits
     Maximum Call Rate for Priority Direct-IP Multimedia:   384:Kbits

                                             Redun-
Packet
                          Mode               dancy
Size(ms)
    FAX                   t.38-standard      0      ECM: y  FB-Timer: 4
    Modem                 off                0
    TDD/TTY               US                 3
    H.323 Clear-channel   n                  0
    SIP 64K Data          n                  0                          20


Media Connection IP Address Type Preferences
 1: IPv4
 2:
```

5.5. IP Network Regions

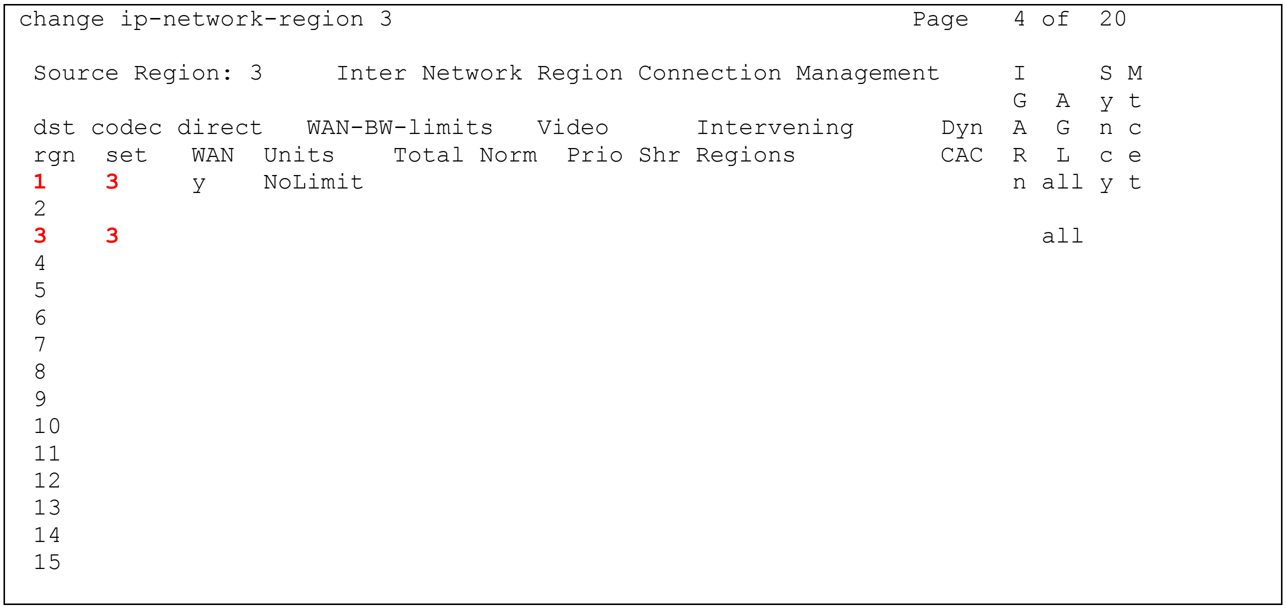
Create a separate IP network region for the service provider trunk group. This allows for separate codec or quality of service settings to be used (if necessary) for calls between the enterprise and the service provider versus calls within the enterprise or elsewhere. For the compliance test, IP Network 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 ***bvwdev.com*** as assigned to the shared test environment in the Avaya test lab. This domain name appears in the "From" header of SIP messages originating from this IP region.
- Enter a descriptive name in the **Name** field.
- Leave both **Intra-region** and **Inter-region IP-IP Direct Audio** set to ***yes***, the default setting. This will 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 and Media Server. Shuffling can be further restricted at the trunk level on the Signaling Group form if needed.
- Set the **Codec Set** field to the IP codec set defined in **Section 5.4**.
- Default values may be used for all other fields.



```
change ip-network-region 3                                    Page    1 of   20
                               IP NETWORK REGION
  Region: 3       NR Group: 3
Location: 1       Authoritative Domain: bvwdev.com
    Name: public                    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 (the rest of the enterprise). 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 following example 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).



```
change ip-network-region 3                                    Page   4 of  20

 Source Region: 3     Inter Network Region Connection Management     I     S M
                                                                     G  A  y t
 dst codec direct   WAN-BW-limits   Video      Intervening      Dyn  A  G  n c
 rgn  set   WAN  Units    Total Norm  Prio Shr Regions          CAC  R  L  c e
 1    3     y    NoLimit                                             n all y t
 2
 3    3                                                               all
 4
 5
 6
 7
 8
 9
 10
 11
 12
 13
 14
 15
```

5.6. Signaling Group

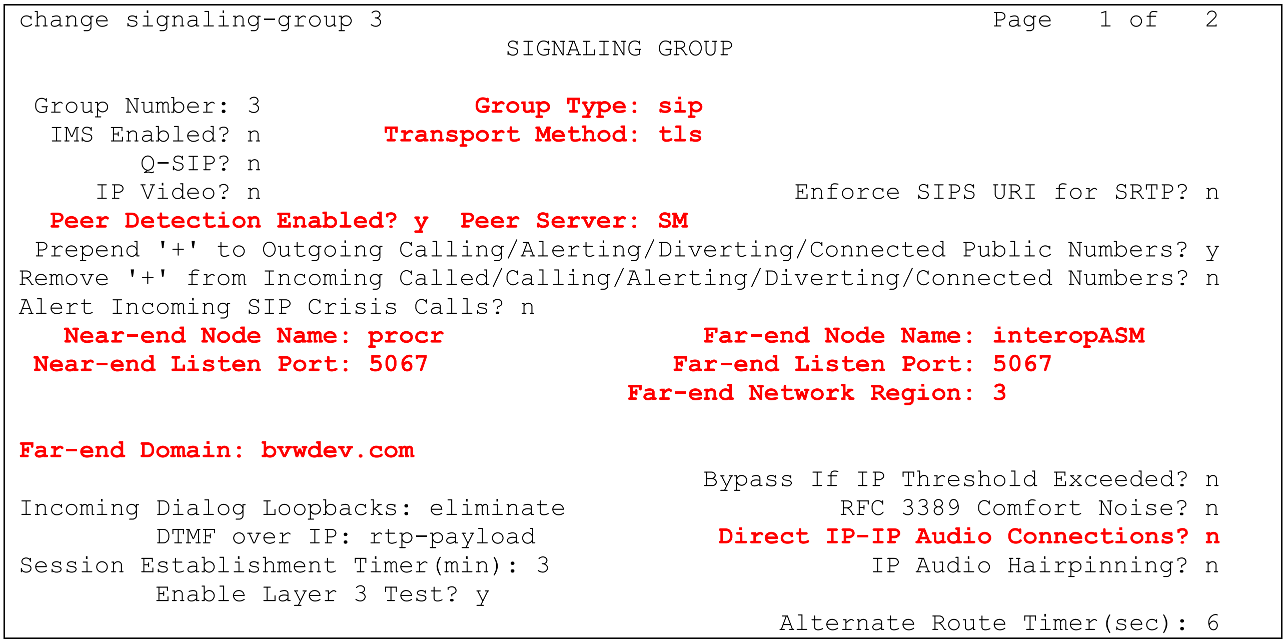
Use the **add signaling-group** command to create a signaling group between Communication Manager and Session Manager for use by the service provider trunk. This signaling group is used for inbound and outbound calls between the service provider and the enterprise. For the compliance test, signaling group 2 was used and was configured using the parameters highlighted below, shown on the screen on the next page:

- Set the **Group Type** field to ***sip***.
- Set the **IMS Enabled** field to ***n***. This specifies the Communication Manager will serve as an Evolution Server for the Session Manager.
- Set the **Transport Method** to the transport protocol to be used between Communication Manager and Session Manager. For the compliance test, ***tls*** was used.
- 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 is a Session Manager.

Note: Once the **Peer-Server** field is updated to ***SM***, the system changes the default values of the following fields, setting them to display–only:

- **Prepend '+' to Outgoing Calling/Alerting/Diverting/Connected Public Numbers?** is changed to ***y***.

- **Remove '+' from Incoming Called/Calling/Alerting/Diverting/Connected Numbers?** is changed to ***n***.
- Set the **Near-end Node Name** to ***procr***. This node name maps to the IP address of the Communication Manager as defined in **Section 5.3**.
- Set the **Far-end Node Name** to ***SM***. 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). This is necessary so Session Manager can distinguish this trunk from the trunk used for other enterprise SIP traffic. The compliance test was conducted with the **Near-end Listen Port** and **Far-end Listen Port** set to ***5067***.
- 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 ***n***. With this set to **n**, the Avaya Media Gateway or Media Server will remain in the media path of all calls between the SIP trunk and the endpoint. Depending on the number of media resources available in the Avaya Media Gateway and Media Server, these resources may be depleted during high call volume preventing additional calls from completing. Refer to **Section 2.2** for more detail.
- Default values may be used for all other fields.



```
change signaling-group 3                                        Page   1 of   2
                                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? n
  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: interopASM
 Near-end Listen Port: 5067                Far-end Listen Port: 5067
                                        Far-end Network Region: 3

Far-end Domain: bvwdev.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? n
Session Establishment Timer(min): 3                     IP Audio Hairpinning? n
         Enable Layer 3 Test? y
                                                  Alternate Route Timer(sec): 6
```

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 2 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 the **Signaling Group** to the signaling group shown in **Section 5.6**.
- Set the **Number of Members** field to the number of trunk members in the SIP trunk group. This value determines how many simultaneous SIP calls can be supported by this trunk.
- Default values were used for all other fields.

```
change trunk-group 3                                          Page   1 of  21
                                TRUNK GROUP

Group Number: 3                    Group Type: sip          CDR Reports: y
  Group Name: OUTSIDE CALL                COR: 1        TN: 1         TAC: #03
   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**, 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/UPDATE must be sent to keep the active session alive. The default value of **600** seconds was used.

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

TRUNK PARAMETERS

     Unicode Name: auto


                                          Redirect On OPTIM Failure: 5000

            SCCAN? n                             Digital Loss Group: 18
                     Preferred Minimum Session Refresh Interval(sec): 600

 Disconnect Supervision - In? y  Out? y


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

 Caller ID for Service Link Call to H.323 1xC: station-extension
```

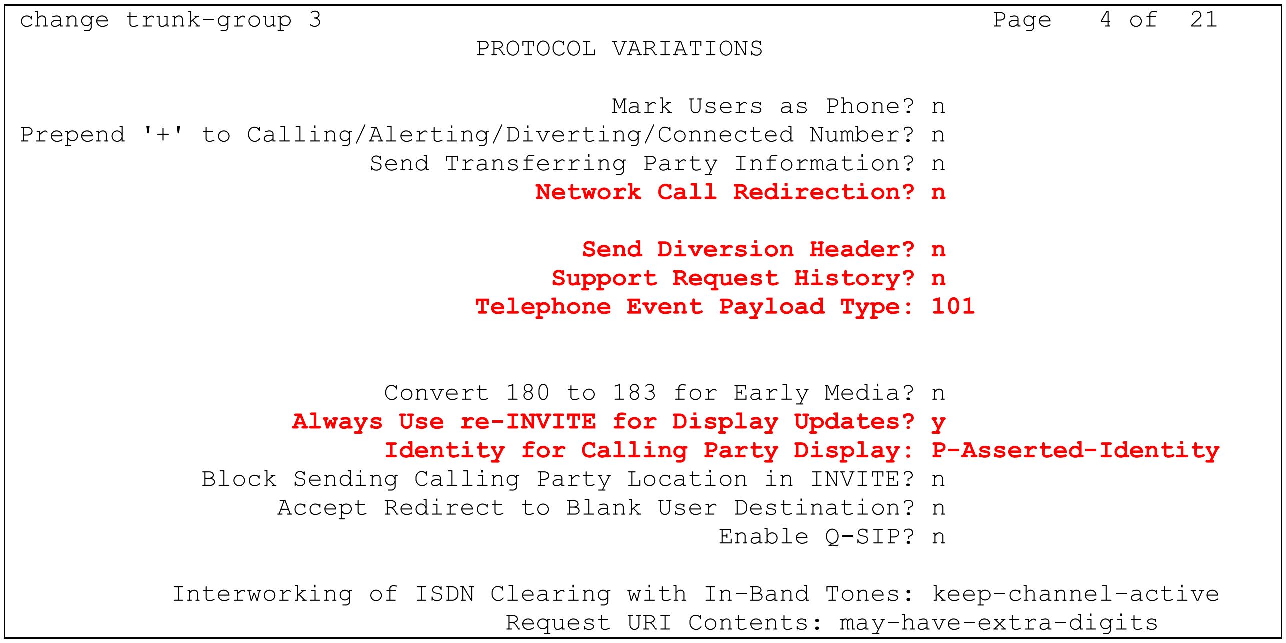
On **Page 3**:

- Set the **Numbering Format** field to ***private***. This field specifies the format of the calling party number (CPN) sent to the far-end. When ***public*** format is used, Communication Manager automatically inserts a "+" sign, preceding the numbers in the "From", "Contact" and "P-Asserted Identity" (PAI) headers. To keep uniformity with the format used by MTS, the **Numbering Format** was set to ***private*** and the **Numbering Format** in the route pattern was set to ***unk-unk*** (see **Section 5.10**).
- 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 has enabled CPN block.

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



   Suppress # Outpulsing? n  Numbering Format: private
                                                UUI Treatment: service-provider

                                                 Replace Restricted Numbers? y
                                                Replace Unavailable Numbers? y

                                                  Hold/Unhold Notifications? y
                                Modify Tandem Calling Number: no




 Show ANSWERED BY on Display? y
```

On **Page 4**:

- Set the **Network Call Redirection** field to ***n***. With this setting, Communication Manager will not use the REFER method, which is not recommended by MTS, for the redirection of PSTN calls that are transferred back to the SIP trunk (refer to **Section 2.1** and **2.2**).
- Set the **Send Diversion Header** field to ***n*** and **Support Request History** to ***n***.
- Set the **Telephone Event Payload Type** to **101**, the value preferred by MTS.
- Set the **Always Use re-INVITE for Display Updates?** to ***y***.
- Verify that **Identity for Calling Party Display** is set to ***P-Asserted-Identity***.
- Default values were used for all other fields.



```
change 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? n

                                     Send Diversion Header? n
                                   Support Request History? n
                              Telephone Event Payload Type: 101


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

          Interworking of ISDN Clearing with In-Band Tones: keep-channel-active
                                      Request URI Contents: may-have-extra-digits
```

5.8. Calling Party Information

The calling party number is sent in the SIP "From", "Contact" and "PAI" headers. Since private numbering was selected to define the format of this number (**Section 5.7**), use the **change private-numbering** command to create an entry for each extension which has a DID assigned. DID numbers are provided by the SIP service provider. Each DID number is assigned in this table to one enterprise internal extension or Vector Directory Numbers (VDNs). In the example below, three DID numbers were assigned by the service provider for testing. These DID numbers were used as the outbound calling party information on the service provider trunk when calls were originated from the mapped extensions.

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

Ext Ext                Trk         Private          Total
Len Code               Grp(s)      Prefix           Len
 4  33                 1                            4     Total Administered: 11
 4  34                 1                            4        Maximum Entries: 540
 4  3301               3           204xxx4610       10
 4  3304               3           204xxx4612       10
 4  3314               3           204xxx4613       10
 4  3400               3           204xxx4612       10
```

5.9. Inbound Routing

In general, the “incoming call handling treatment” form for a trunk group can be used to manipulate the digits received for an incoming call if necessary. Since Session Manager is present, Session Manager can be used to perform digit conversion using an Adaptation, and digit manipulation via the Communication Manager incoming call handling table may not be necessary. If the DID number sent by MTS is left unchanged by Session Manager, then the DID number can be mapped to an extension using the incoming call handling treatment of the receiving trunk group. Use the **change inc-call-handling-trmt** command to create an entry for each DID.

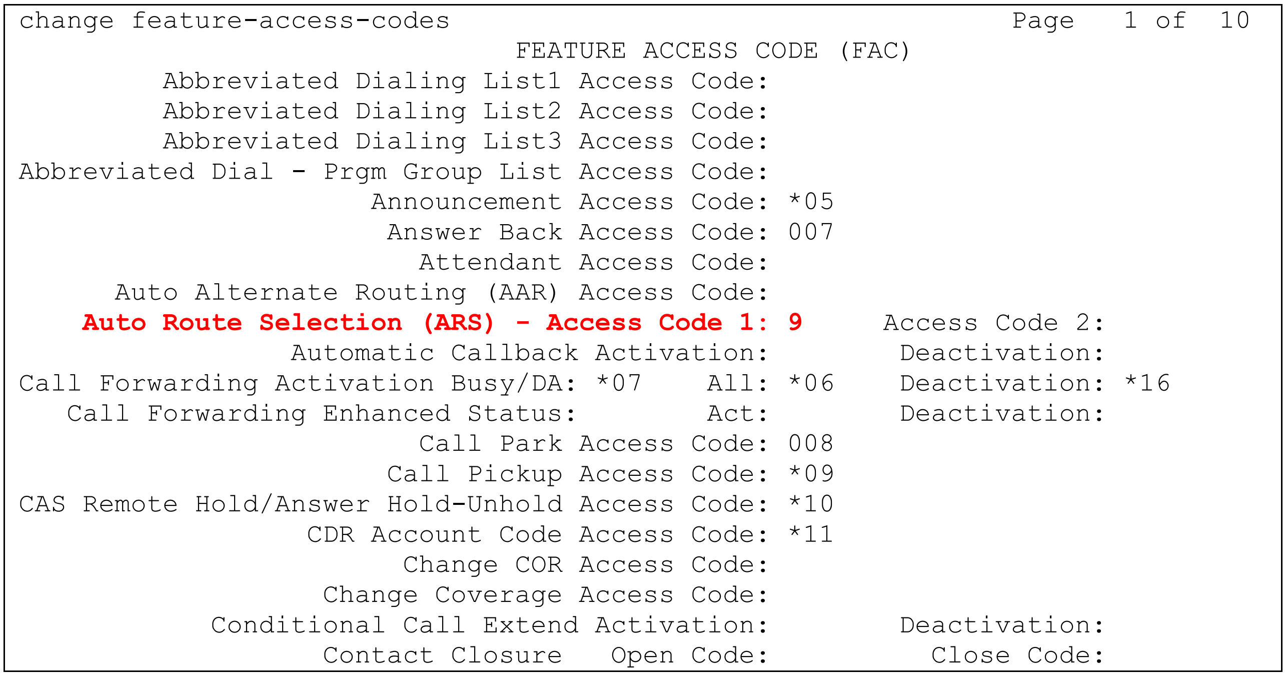
```
change inc-call-handling-trmt trunk-group 3                         age    1 of   30
                       INCOMING CALL HANDLING TREATMENT
 Service/      Number    Number       Del  Insert
 Feature        Len       Digits
 public-ntwrk    10  204xxx4610        10   3301
 public-ntwrk    10  204xxx4611        10   3401
 public-ntwrk    10  204xxx4612        10   3303
 public-ntwrk    10  204xxx4613        10   3315
```

5.10. 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: 5

    Dialed    Total  Call       Dialed    Total  Call       Dialed    Total  Call
    String    Length Type       String    Length Type       String    Length Type
   0            3    fac       4            4    aar       #            3    dac
   1            4    ext       43           4    aar
   1            11   udp       44           4    udp
   13           5    aar       45           4    aar
   14           5    aar       46           4    aar
   20           4    aar       50           4    aar
   23           5    aar       51           4    udp
   24           5    aar       54           4    udp
   28           5    aar       546          5    aar
   30           4    aar       56           5    udp
   33           4    ext       60           5    udp
   33           5    aar       608          10   udp
   34           4    ext       8            1    fac
   34           5    aar       9            1    fac
   35           4    udp       *            3    dac
```

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  10
                               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: *05
                       Answer Back Access Code: 007
                         Attendant Access Code:
      Auto Alternate Routing (AAR) Access Code:
    Auto Route Selection (ARS) - Access Code 1: 9     Access Code 2:
                 Automatic Callback Activation:        Deactivation:
Call Forwarding Activation Busy/DA: *07    All: *06    Deactivation: *16
   Call Forwarding Enhanced Status:        Act:        Deactivation:
                         Call Park Access Code: 008
                       Call Pickup Access Code: *09
CAS Remote Hold/Answer Hold-Unhold Access Code: *10
                  CDR Account Code Access Code: *11
                        Change COR Access Code:
                   Change Coverage Access Code:
            Conditional Call Extend Activation:        Deactivation:
                   Contact Closure   Open Code:          Close Code:
```

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 **3**, which contains the SIP trunk group to the service provider.

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

          Dialed               Total     Route     Call    Node   ANI
          String              Min  Max  Pattern    Type    Num    Reqd
    1                         11   14    3         pubu           n
    101xxxx0                  8    8     deny      op             n
    101xxxx0                  18   18    deny      op             n
    101xxxx01                 16   24    deny      iop            n
    101xxxx011                17   25    deny      intl           n
    101xxxx1                  18   18    deny      fnpa           n
    10xxx0                    6    6     deny      op             n
    10xxx0                    16   16    deny      op             n
    10xxx01                   14   22    deny      iop            n
    10xxx011                  15   23    deny      intl           n
    10xxx1                    16   16    deny      fnpa           n
    1200                      11   11    deny      fnpa           n
    121                       11   11    deny      fnpa           n
    122                       11   11    deny      fnpa           n
    123                       10   11    3         natl           n
```

The route pattern defines which trunk group will be used for the call and performs any necessary digit manipulation. Use the **change route-pattern** command to configure the parameters for the service provider trunk route pattern in the following manner. The example below shows the values used for route pattern 3 in the compliance test.

- **Pattern Name**: Enter a descriptive name.
- **Grp No**: Enter the outbound trunk group for the SIP service provider.
- **FRL**: Set the Facility Restriction Level (**FRL**) field to a level that allows access to this trunk for all users that require it. The value of **0** is the least restrictive level.
- **Pfx Mrk**: Set to **1** to ensure 1 + 10 digits are sent to the service provider for long distance numbers in the North American Numbering Plan (NANP).
- **Numbering Format**: Set to ***unk-unk***. All calls using this route pattern will use the private numbering table. See setting of the **Numbering Format** in the trunk group form for full details in **Section 5.7**.

```
change route-pattern 3                                          Page   1 of   3
                    Pattern Number: 3      Pattern Name: Public
    SCCAN? n     Secure SIP? n      Used for SIP stations? n

    Grp  FRL NPA Pfx Hop Toll No.  Inserted                                DCS/ IXC
    No           Mrk Lmt List Del  Digits                                  QSIG
                              Dgts                                         Intw
 1: 3    0         1                                                         n   user
 2:                                                                         n   user
 3:                                                                         n   user
 4:                                                                         n   user
 5:                                                                         n   user
 6:                                                                         n   user

     BCC VALUE  TSC CA-TSC    ITC BCIE Service/Feature PARM Sub  Numbering LAR
    0 1 2 M 4 W     Request                                 Dgts Format
 1: y y y y y n  n            rest                                  unk-unk   none
 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
```

Note - Enter the **save translation** command (not shown) to save all the changes made to the Communication Manager configuration in the previous sections.

6. Configure Avaya Aura® Session Manager

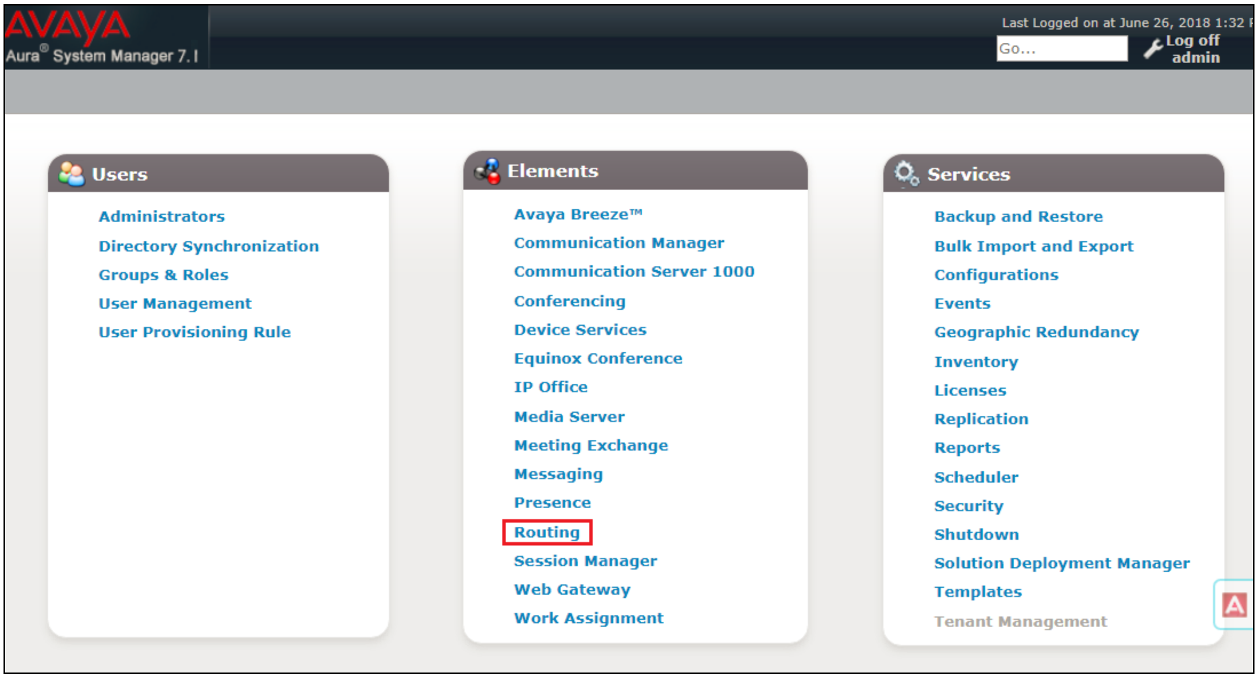
This section provides the procedures for configuring Session Manager. The procedures include adding the following items:

- SIP domain.
- Logical/physical Locations that can be occupied by SIP Entities.
- Adaptation module to perform header manipulations.
- SIP Entities corresponding to Communication Manager, Session Manager and the Avaya SBCE.
- Entity Links, which define the SIP trunk parameters used by Session Manager when routing calls to/from SIP Entities.
- Routing Policies, which control call routing between the SIP Entities.
- Dial Patterns, which govern to which SIP Entity a call is routed.

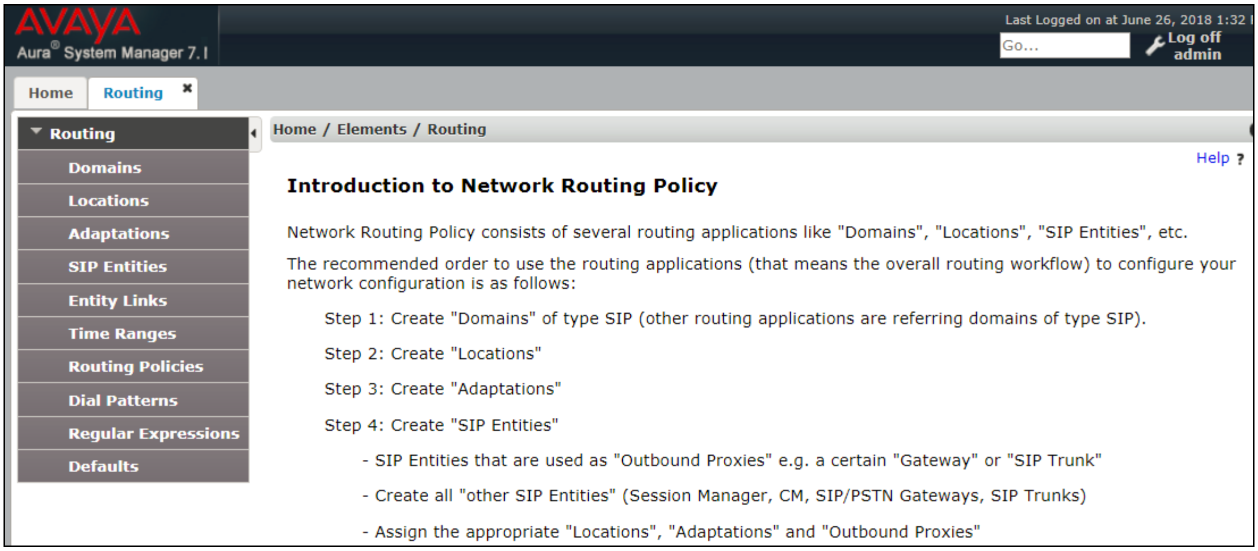
The following sections assume that the initial configuration of Session Manager and System Manager has already been completed, and that network connectivity exists between System Manager and Session Manager.

6.1. 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 **Log On** (not shown). The screen shown below is then displayed; click on **Routing**.



The navigation tree displayed in the left pane below will be referenced in subsequent sections to navigate to items requiring configuration. Most items discussed in this section will be located under the **Routing** link shown below.



Introduction to Network Routing Policy

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

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

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

Step 2: Create "Locations"

Step 3: Create "Adaptations"

Step 4: Create "SIP Entities"

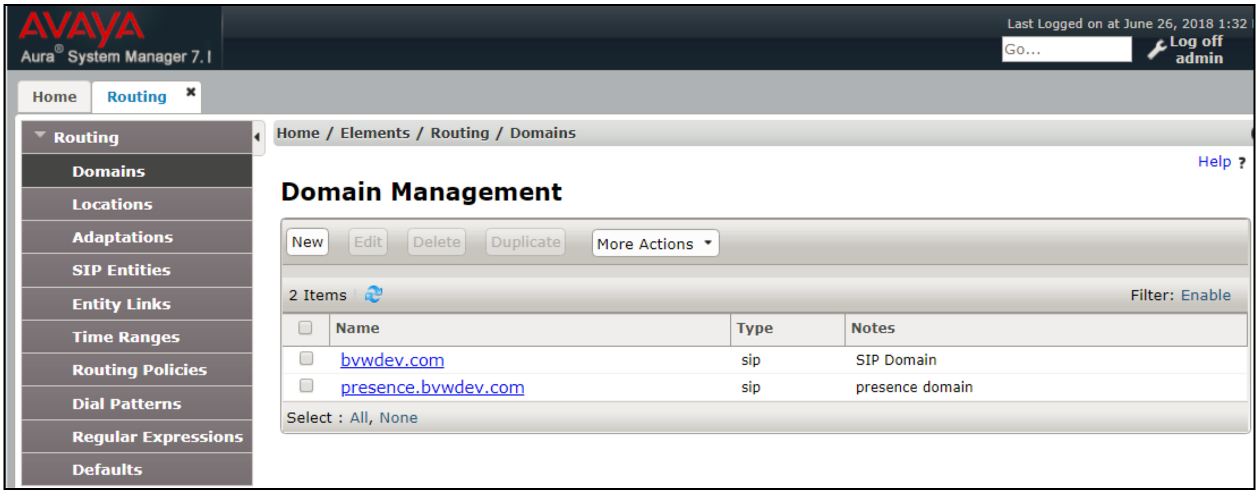
- SIP Entities that are used as "Outbound Proxies" e.g. a certain "Gateway" or "SIP Trunk"
- Create all "other SIP Entities" (Session Manager, CM, SIP/PSTN Gateways, SIP Trunks)
- Assign the appropriate "Locations", "Adaptations" and "Outbound Proxies"

6.2. SIP Domain

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

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

The screen below shows the entry for the enterprise domain.



Domain Management

2 Items

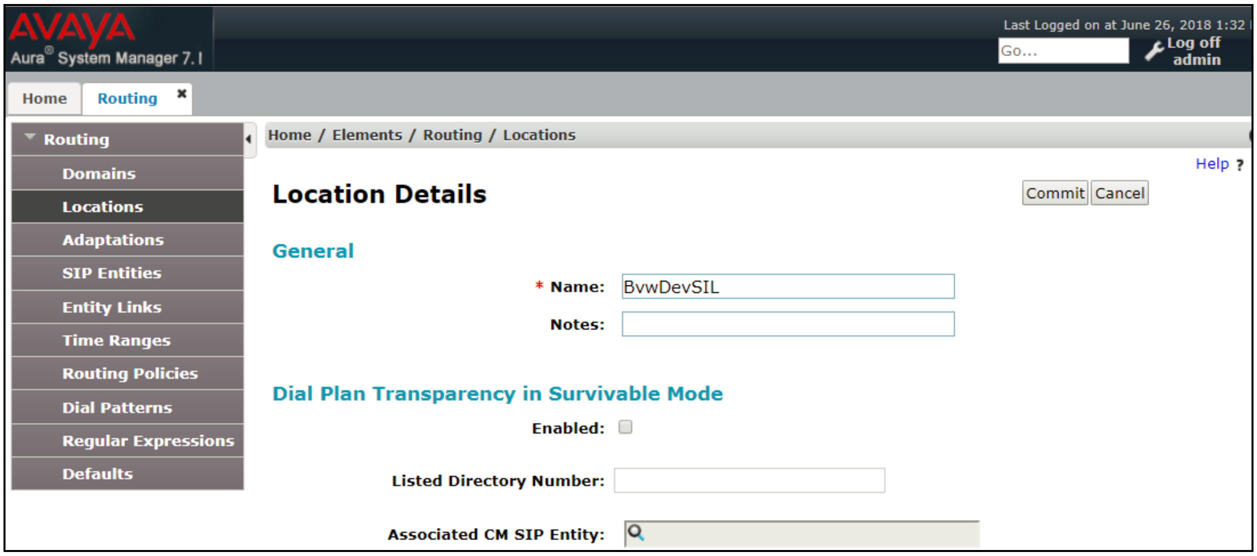
□	Name	Type	Notes
□	bvwdev.com	sip	SIP Domain
□	presence.bvwdev.com	sip	presence domain

6.3. Locations

Locations can be used to identify logical and/or physical locations where SIP Entities reside for purposes of bandwidth management, call admission control and location-based routing. To add a location, navigate to **Routing → Locations** in the left-hand navigation pane and click the **New** button in the right pane (not shown). In the **General** section, enter the following values:

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

The following screen shows the location details for the location named ***BvwDevSIL***. Later, this location will be assigned to the SIP Entity corresponding to Session Manager. Other location parameters (not shown) retained the default values.



Location Details

General

* Name: BvwDevSIL

Notes:

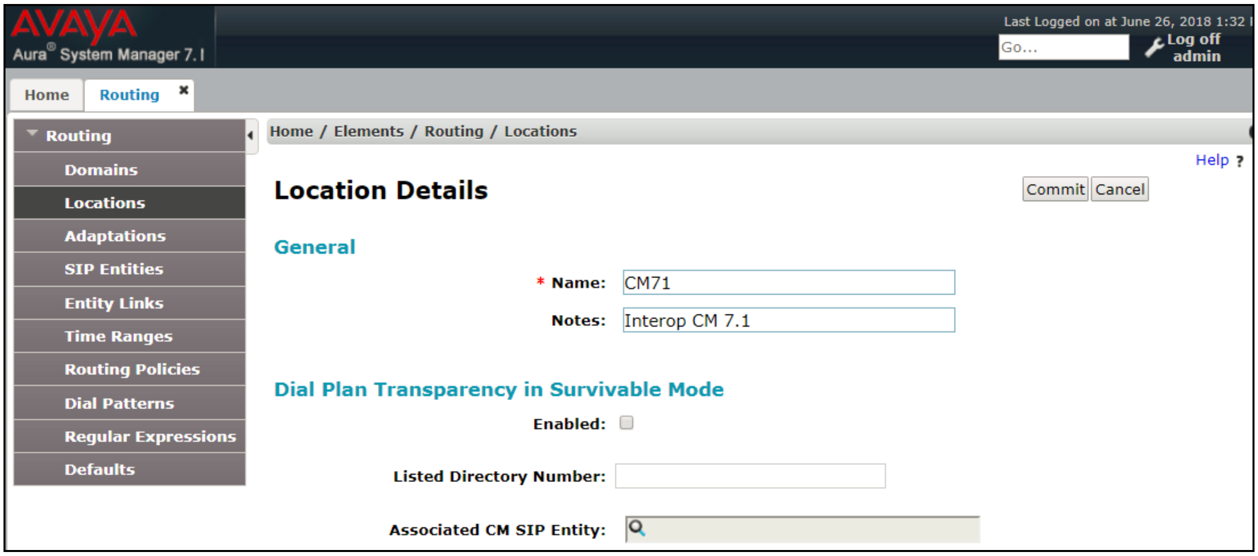
Dial Plan Transparency in Survivable Mode

Enabled: □

Listed Directory Number:

Associated CM SIP Entity:

The following screen shows the location details for the location named ***CM71***. Later, this location will be assigned to the SIP Entity corresponding to Communication Manager. Other location parameters (not shown) retained the default values.



Location Details

General

* Name: CM71

Notes: Interop CM 7.1

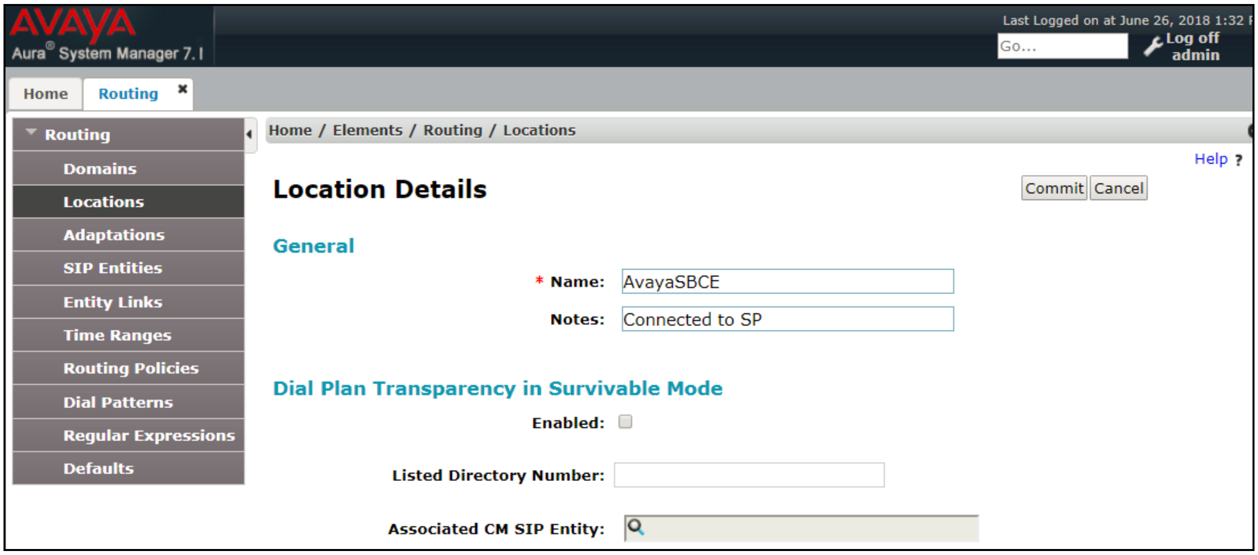
Dial Plan Transparency in Survivable Mode

Enabled: □

Listed Directory Number:

Associated CM SIP Entity:

The following screen shows the location details for the location named ***Avaya SBCE***. Later, this location will be assigned to the SIP Entity corresponding to the Avaya SBCE. Other location parameters (not shown) retained the default values.



Location Details

General

* Name: AvayaSBCE

Notes: Connected to SP

Dial Plan Transparency in Survivable Mode

Enabled: □

Listed Directory Number:

Associated CM SIP Entity:

6.4. Adaptations

In order to improve interoperability with third party elements, Session Manager 7.1 incorporates the ability to use Adaptation modules to remove specific headers that are either Avaya proprietary or deemed excessive/unnecessary for non-Avaya elements.

For the compliance test, an Adaptation named ***CM_Headers_Remove*** was created to block the following headers from outbound messages, before they were forwarded to the Avaya SBCE: AV-Global-Session-ID, AV-Correlation-ID, Alert-Info, Endpoint-View, P-AV-Message-ID, P-Charging-Vector and P-Location. These headers contain private information from the enterprise, which should not be propagated outside of the enterprise boundaries. They also add unnecessary size to outbound messages, while they have no significance to the service provider.

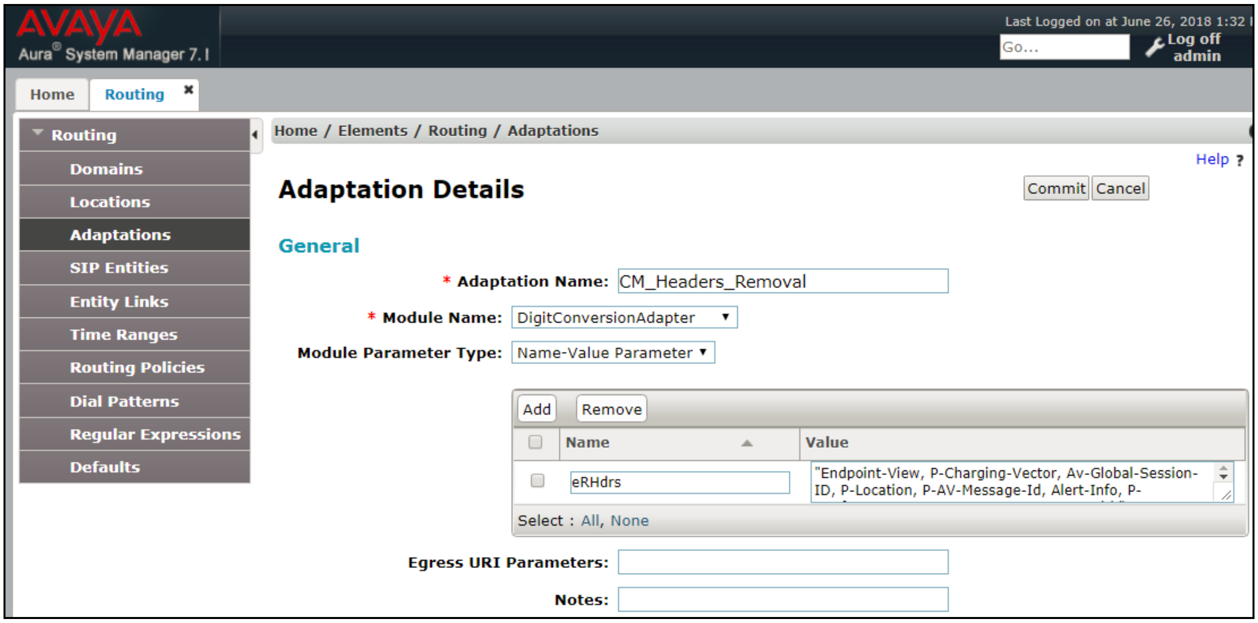
Navigate to **Routing → Adaptations** in the left-hand navigation pane and click the **New** button in the right pane (not shown). In the new right pane that appears (shown below), fill in the following:

- **Adaptation Name**: Enter an appropriate name.
- **Module Name**: Select the ***DigitConversionAdapter*** option.
- **Module Parameter Type**: Select ***Name-Value Parameter***.

Click **Add** to add the name and value parameters, as follows:

- **Name**: Enter ***eRHdrs***. This parameter will remove the specified headers from messages in the egress direction.
- **Value**: Enter ***"Alert-Info, P-Charging-Vector, AV-Global-Session-ID, AV-Correlation-ID, P-AV-Message-Id, P-Location, Endpoint-View"***
- Click **Commit** to save.

The screen below shows the adaptation created for the compliance test. This adaptation will later be applied to the SIP Entity corresponding to the Avaya SBCE. All other fields were left at their default values.



Adaptation Details

General

* Adaptation Name: CM_Headers_Removal

* Module Name: DigitConversionAdapter

Module Parameter Type: Name-Value Parameter

□	Name	Value
□	eRHdrs	"Endpoint-View, P-Charging-Vector, Av-Global-Session-ID, P-Location, P-AV-Message-Id, Alert-Info, P-

Egress URI Parameters:

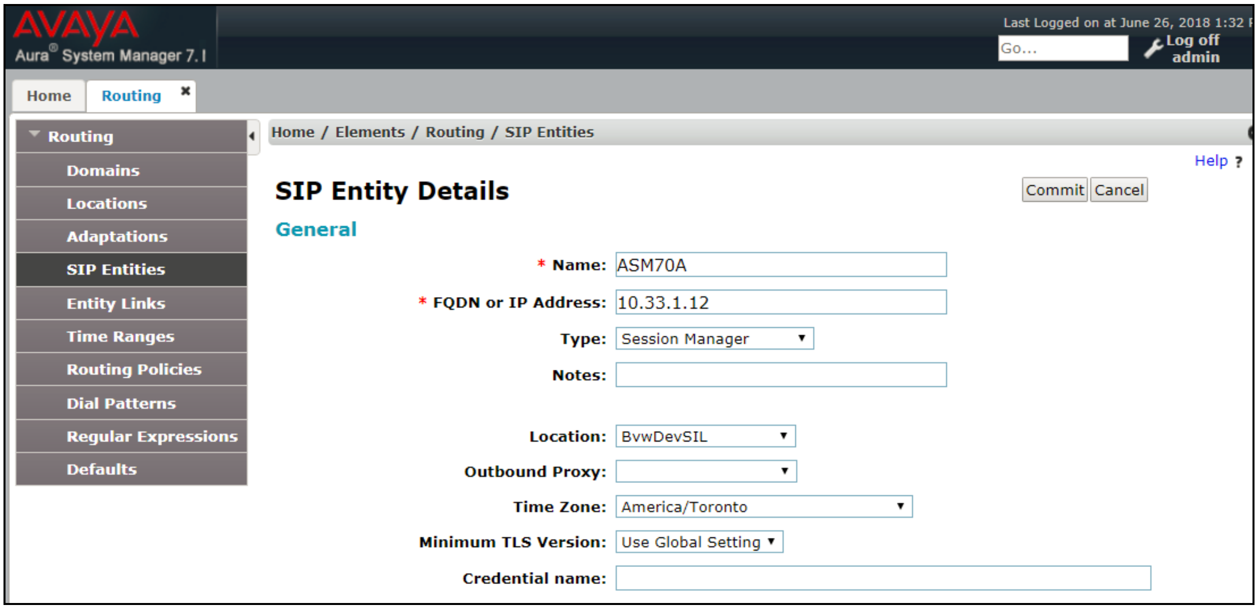
Notes:

6.5. SIP Entities

A SIP Entity must be added for Session Manager and for each SIP telephony system connected to it, which includes Communication Manager and the Avaya SBCE. Navigate to **Routing → SIP Entities** in the left navigation pane and click on the **New** button in the right pane (not shown). 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 (see **Figure 1**).
- **Type:** Select ***Session Manager*** for Session Manager, ***CM*** for Communication Manager and ***SIP Trunk*** (or ***Other***) for the Avaya SBCE.
- **Adaptation:** This field is only present if **Type** is not set to **Session Manager** If Adaptations were to be created, here is where they would be applied to the entity.
- **Location:** Select the location that applies to the SIP Entity being created, defined in **Section 6.3**.
- **Time Zone:** Select the time zone for the location above.
- Click **Commit** to save.

The following screen shows the addition of the ***Session Manager*** SIP Entity for Session Manager. The IP address of the Session Manager Security Module is entered in the **FQDN or IP Address** field.

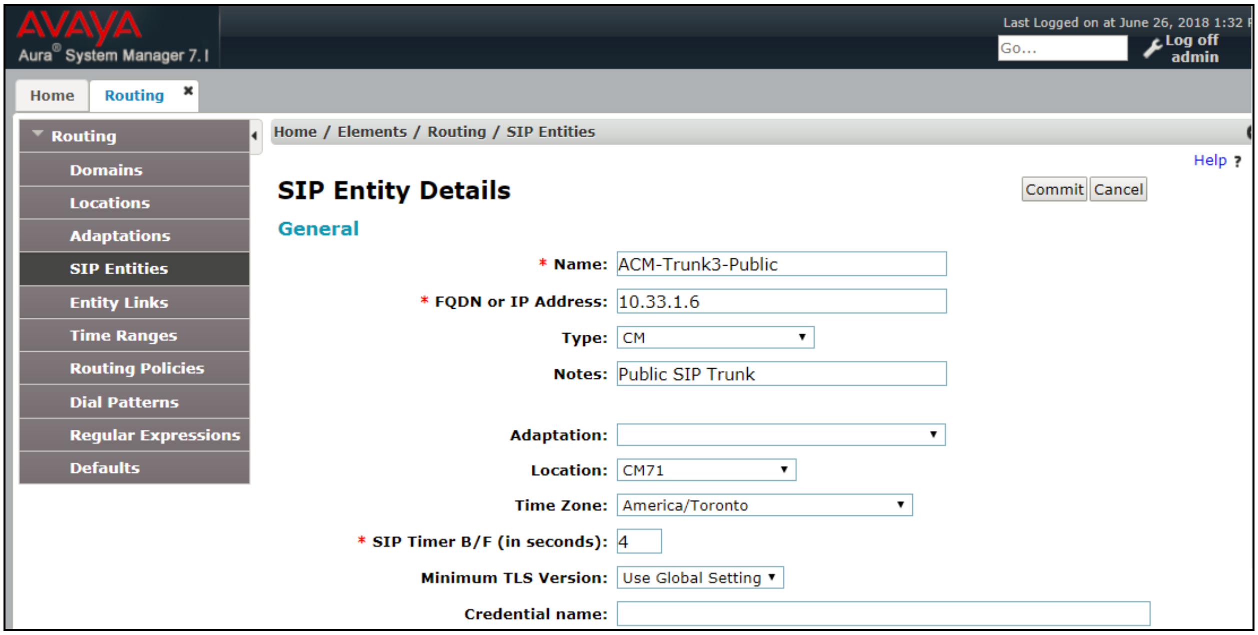


SIP Entity Details

General

* Name:	ASM70A
* FQDN or IP Address:	10.33.1.12
Type:	Session Manager
Notes:	
Location:	BvwDevSIL
Outbound Proxy:	
Time Zone:	America/Toronto
Minimum TLS Version:	Use Global Setting
Credential name:	

The following screen shows the addition of the ***ACM-Trunk3-Public*** SIP Entity for Communication Manager. In order for Session Manager to send SIP service provider traffic on a separate entity link to Communication Manager, the creation of a separate SIP entity for Communication Manager is required. This SIP Entity should be different than the one created during the Session Manager installation, used by all other enterprise SIP traffic. The **FQDN or IP Address** field is set to the IP address of the "**procr**" interface in Communication Manager, as seen in **Section 5.3**. Select the location that applies to the SIP Entity being created, defined in **Section 6.3**.



SIP Entity Details

General

* Name: ACM-Trunk3-Public

* FQDN or IP Address: 10.33.1.6

Type: CM

Notes: Public SIP Trunk

Adaptation:

Location: CM71

Time Zone: America/Toronto

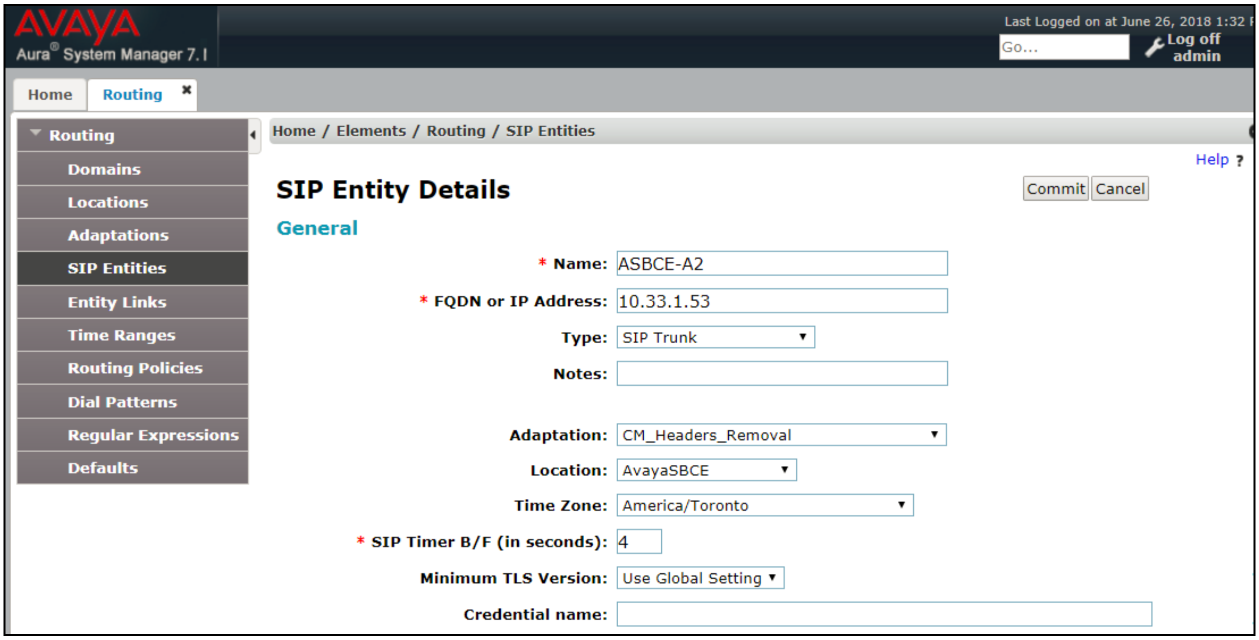
* SIP Timer B/F (in seconds): 4

Minimum TLS Version: Use Global Setting

Credential name:

The following screen shows the addition of the ***Avaya SBCE*** SIP Entity for the Avaya SBCE:

- The **FQDN or IP Address** field is set to the IP address of the SBC private network interface (see **Figure 1**).
- On the **Adaptation** field, the adaptation module ***CM_Headers_Removal*** previously defined in **Section 6.4** was selected.
- Select the location that applies to the SIP Entity being created, defined in **Section 6.3**.



SIP Entity Details

General

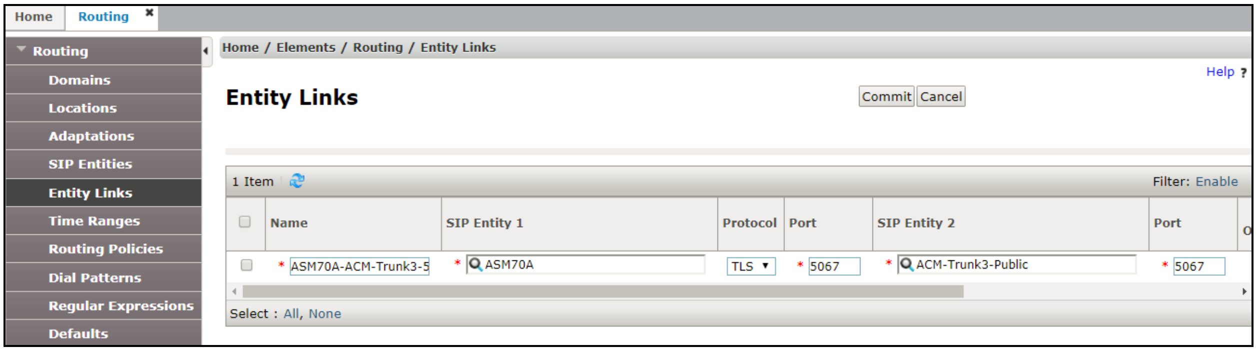
* Name:	ASBCE-A2
* FQDN or IP Address:	10.33.1.53
Type:	SIP Trunk
Notes:	
Adaptation:	CM_Headers_Removal
Location:	AvayaSBCE
Time Zone:	America/Toronto
* SIP Timer B/F (in seconds):	4
Minimum TLS Version:	Use Global Setting
Credential name:	

6.6. 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 the 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 navigation pane and click on the **New** button in the right pane (not shown). Fill in the following fields in the new row that is displayed:

- **Name:** Enter a descriptive name.
- **SIP Entity 1:** Select the Session Manager from the drop-down menu (**Section 6.5**).
- **Protocol:** Select the transport protocol used for this link (**Section 5.6**).
- **Port:** Port number on which Session Manager will receive SIP requests from the far-end (**Section 5.6**).
- **SIP Entity 2:** Select the name of the other system from the drop-down menu (**Section 6.5**).
- **Port:** Port number on which the other system receives SIP requests from Session Manager (**Section 5.6**).
- **Connection Policy:** Select **Trusted** to allow calls from the associated SIP Entity.
- Click **Commit** to save.

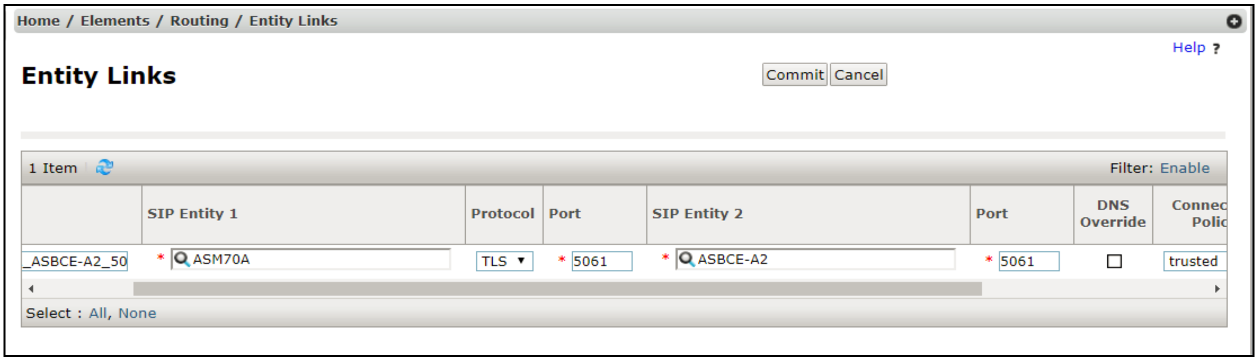
The screen below shows the Entity Link to Communication Manager. The protocol and ports defined here must match the values used on the Communication Manager signaling group form in **Section 5.6**. ***TLS*** transport and port ***5067*** were used.



Entity Links

□	Name	SIP Entity 1	Protocol	Port	SIP Entity 2	Port
□	* ASM70A-ACM-Trunk3-5	* ASM70A	TLS	* 5067	* ACM-Trunk3-Public	* 5067

The Entity Link to the Avaya SBCE is shown below; ***TLS*** transport and port ***5061*** were used.



Entity Links

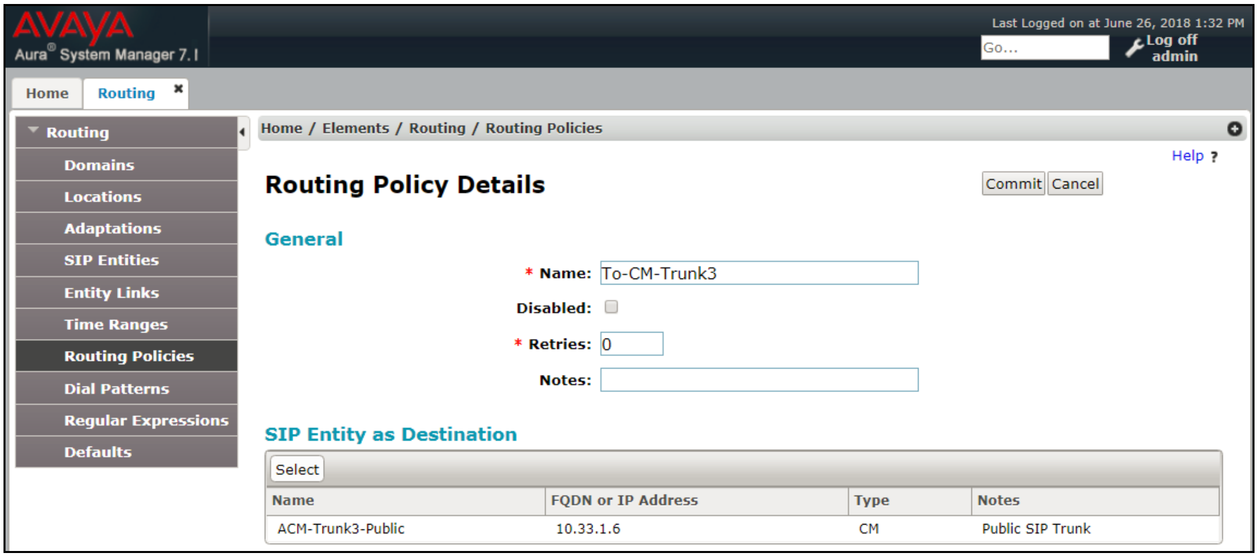
	SIP Entity 1	Protocol	Port	SIP Entity 2	Port	DNS Override	Connec Polic
_ASBCE-A2_50	* ASM70A	TLS	* 5061	* ASBCE-A2	* 5061	□	trusted

6.7. 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 were added: an incoming policy with Communication Manager as the destination, and an outbound policy to the Avaya SBCE. To add a routing policy, navigate to **Routing → Routing Policies** in the left navigation pane and click on the **New** button in the right pane (not shown). The following screen is displayed:

- In the **General** section, enter a descriptive **Name** and add a brief description under **Notes** (optional).
- In the **SIP Entity as Destination** section, click **Select**. The **SIP Entity List** page opens (not shown). Choose the appropriate SIP entity to which this routing policy applies (**Section 6.5**) 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 screens show the Routing Policies for Communication Manager.



Routing Policy Details

General

* Name: To-CM-Trunk3

Disabled: □

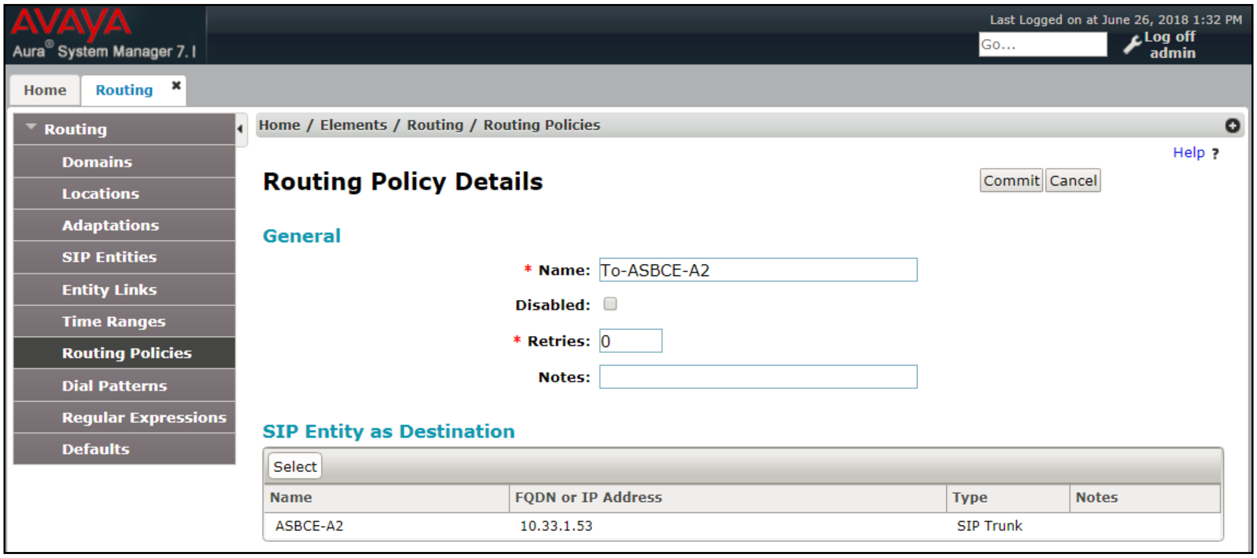
* Retries: 0

Notes:

SIP Entity as Destination

Name	FQDN or IP Address	Type	Notes
ACM-Trunk3-Public	10.33.1.6	CM	Public SIP Trunk

The following screens show the Routing Policies for the Avaya SBCE.



Routing Policy Details

General

* Name: To-ASBCE-A2

Disabled: □

* Retries: 0

Notes:

SIP Entity as Destination

Name	FQDN or IP Address	Type	Notes
ASBCE-A2	10.33.1.53	SIP Trunk	

6.8. Dial Patterns

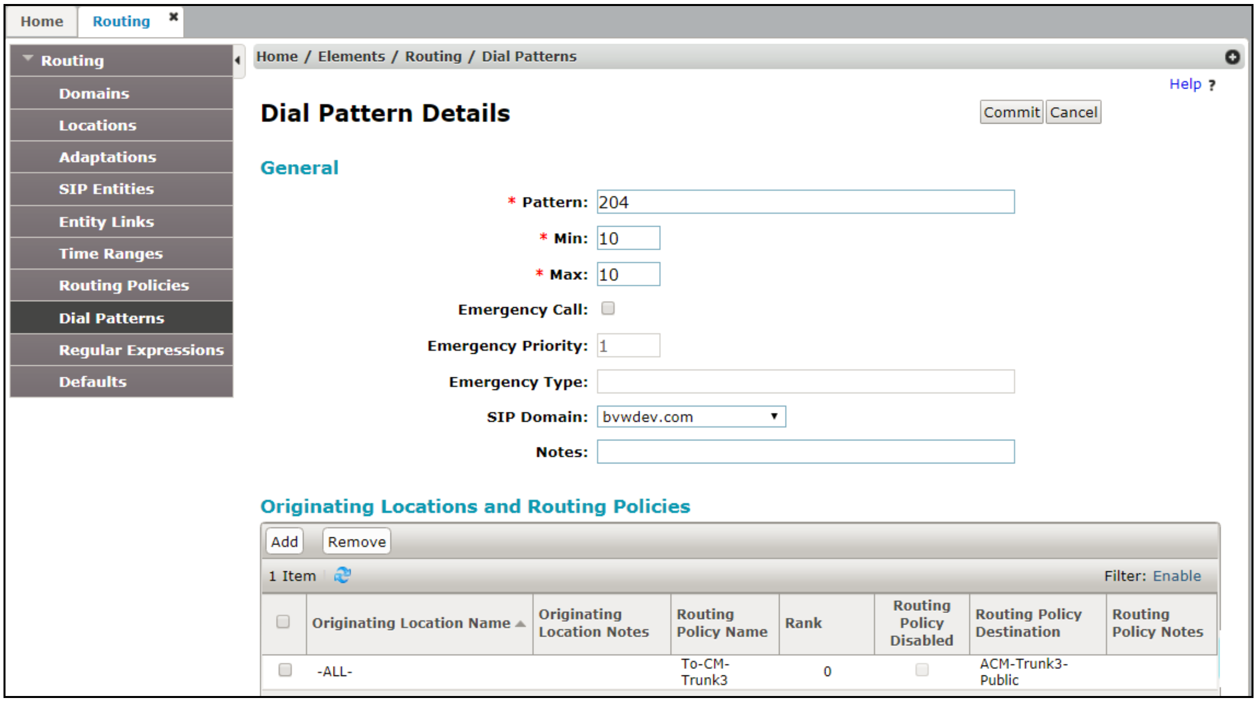
Dial Patterns are needed to route specific calls through Session Manager. For the compliance test, dial patterns were needed to route calls from Communication Manager to the service provider and vice versa. Dial Patterns define which route policy will be selected for a particular call based on the dialed digits, destination domain and originating location. To add a dial pattern, navigate to **Routing** → **Dial Patterns** in the left navigation pane and click on the **New** button in the right pane (not shown). Fill in the following, as shown in the screens below:

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

- **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, or select "**ALL**" to route incoming calls to all SIP domains.
- **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 (**Section 6.3**).
- Lastly, select the routing policy from the list that will be used to route all calls that match the specified criteria (**Section 6.7**). Click **Select** (not shown).
- Click **Commit** to save.

The following screen illustrates an example dial pattern used to verify inbound PSTN calls to the enterprise. In the example, calls to 10 digit numbers starting with ***204***, arriving from location ***Avaya SBCE***, used route policy ***To-CM-Trunk3*** to Communication Manager. The SIP Domain was set to ***bvwdev.com***.

Repeat this procedure as needed to define additional dial patterns for other range of numbers assigned by the service provider to the enterprise, to be routed to Communication Manager.



Dial Pattern Details

General

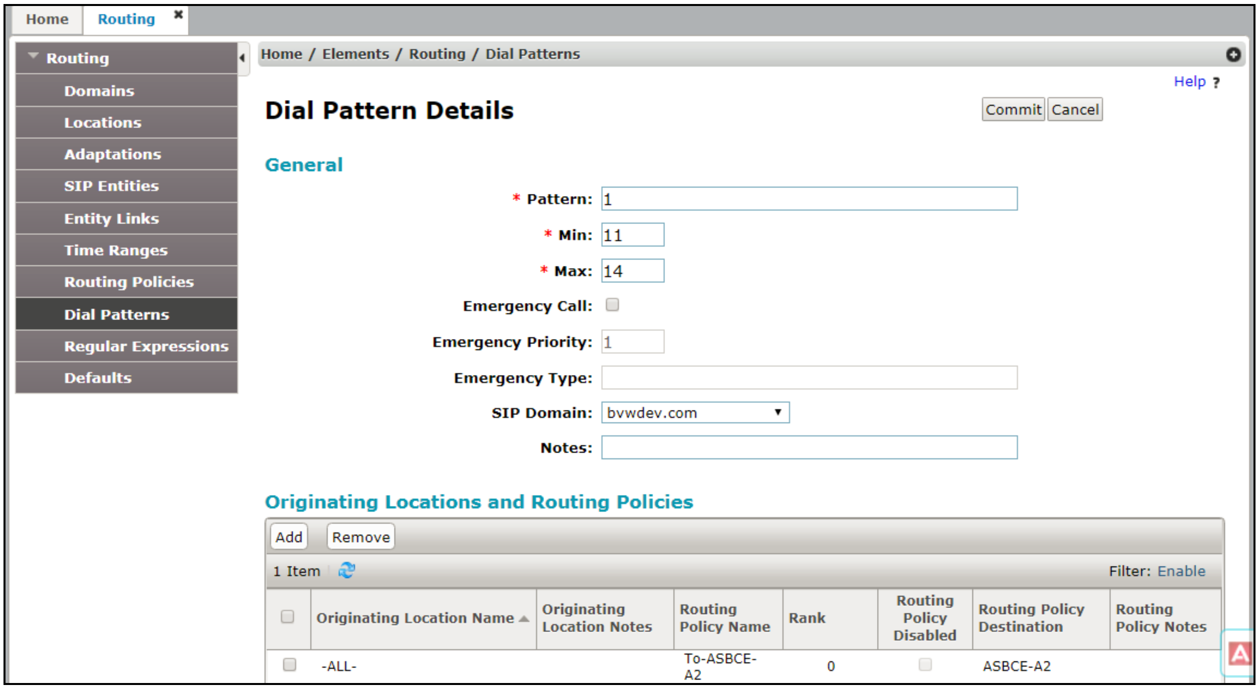
* Pattern:	204
* Min:	10
* Max:	10
Emergency Call:	□
Emergency Priority:	1
Emergency Type:	
SIP Domain:	bvwdev.com
Notes:	

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-		To-CM-Trunk3	0	□	ACM-Trunk3-Public	

The example in this screen shows the 11 digit dialed numbers for outbound international calls, beginning with ***1***, arriving from the ***All*** location, will use route policy ***Avaya SBCE***, which sends the call out to the PSTN via Avaya SBCE and the service provider SIP trunk. The SIP Domain was set to ***bvwdev.com***.



Dial Pattern Details

General

* Pattern:	1
* Min:	11
* Max:	14
Emergency Call:	□
Emergency Priority:	1
Emergency Type:	
SIP Domain:	bvwdev.com
Notes:	

Originating Locations and Routing Policies

□	Originating Location Name	Originating Location Notes	Routing Policy Name	Rank	Routing Policy Disabled	Routing Policy Destination	Routing Policy Notes
□	-ALL-		To-ASBCE-A2	0	□	ASBCE-A2	

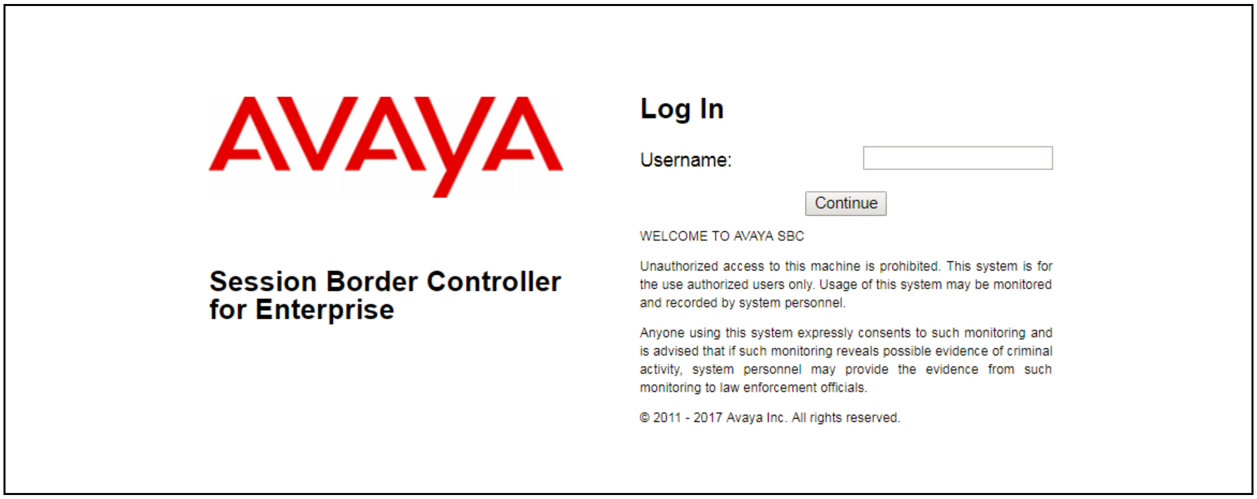
Repeat this procedure as needed, to define additional dial patterns for PSTN numbers to be routed to the service provider's network via the Avaya SBCE.

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, the assignment of the management interface IP Address and license installation have already been completed; hence these tasks are not covered in these Application Notes. For more information on the installation and initial provisioning of the Avaya SBCE consult the Avaya SBCE documentation in the **Additional References** section.

7.1. System Access

Access the Session Border Controller web management interface by using a web browser and entering the URL **https://<ip-address>**, where **<ip-address>** is the management IP address configured at installation. Log in using the appropriate credentials.



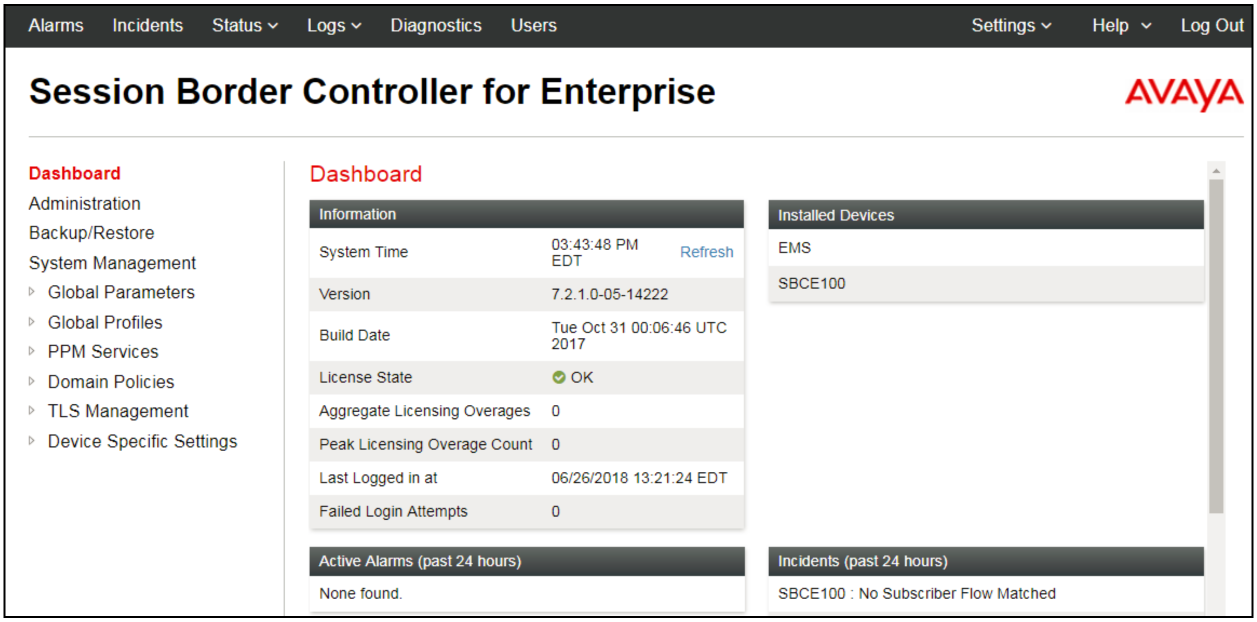
WELCOME TO AVAYA SBC

Unauthorized access to this machine is prohibited. This system is for the use authorized users only. Usage of this system may be monitored and recorded by system personnel.

Anyone using this system expressly consents to such monitoring and is advised that if such monitoring reveals possible evidence of criminal activity, system personnel may provide the evidence from such monitoring to law enforcement officials.

© 2011 - 2017 Avaya Inc. All rights reserved.

Once logged in, the Dashboard screen is presented. The left navigation pane contains the different available menu items used for the configuration of the Avaya SBCE. Verify that the status of the **License State** field is **OK**, indicating that a valid license is present. Contact an authorized Avaya sales representative if a license is needed.



Information	
System Time	03:43:48 PM EDT
Version	7.2.1.0-05-14222
Build Date	Tue Oct 31 00:06:46 UTC 2017
License State	✓ OK
Aggregate Licensing Overages	0
Peak Licensing Overage Count	0
Last Logged in at	06/26/2018 13:21:24 EDT
Failed Login Attempts	0

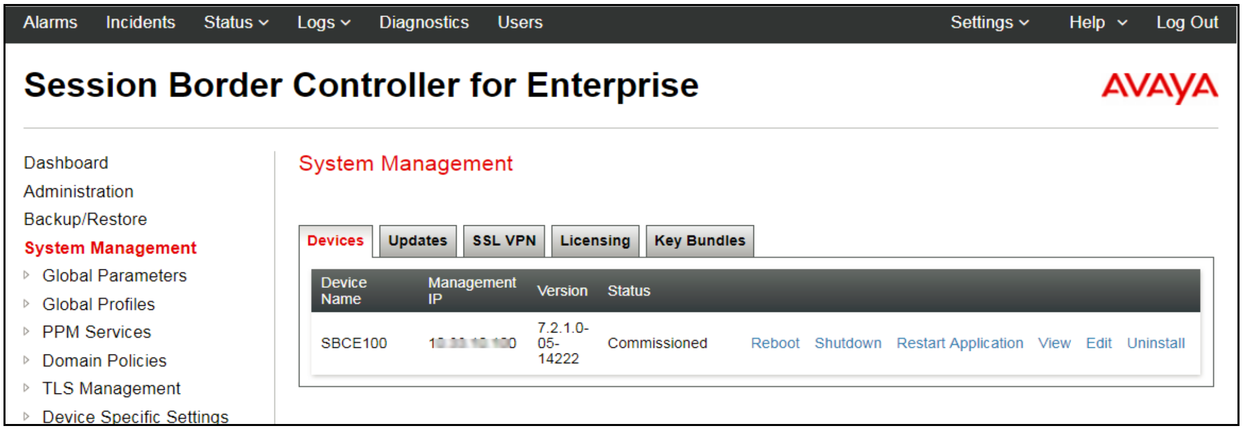
Installed Devices
EMS
SBCE100

Active Alarms (past 24 hours)
None found.

Incidents (past 24 hours)
SBCE100 : No Subscriber Flow Matched

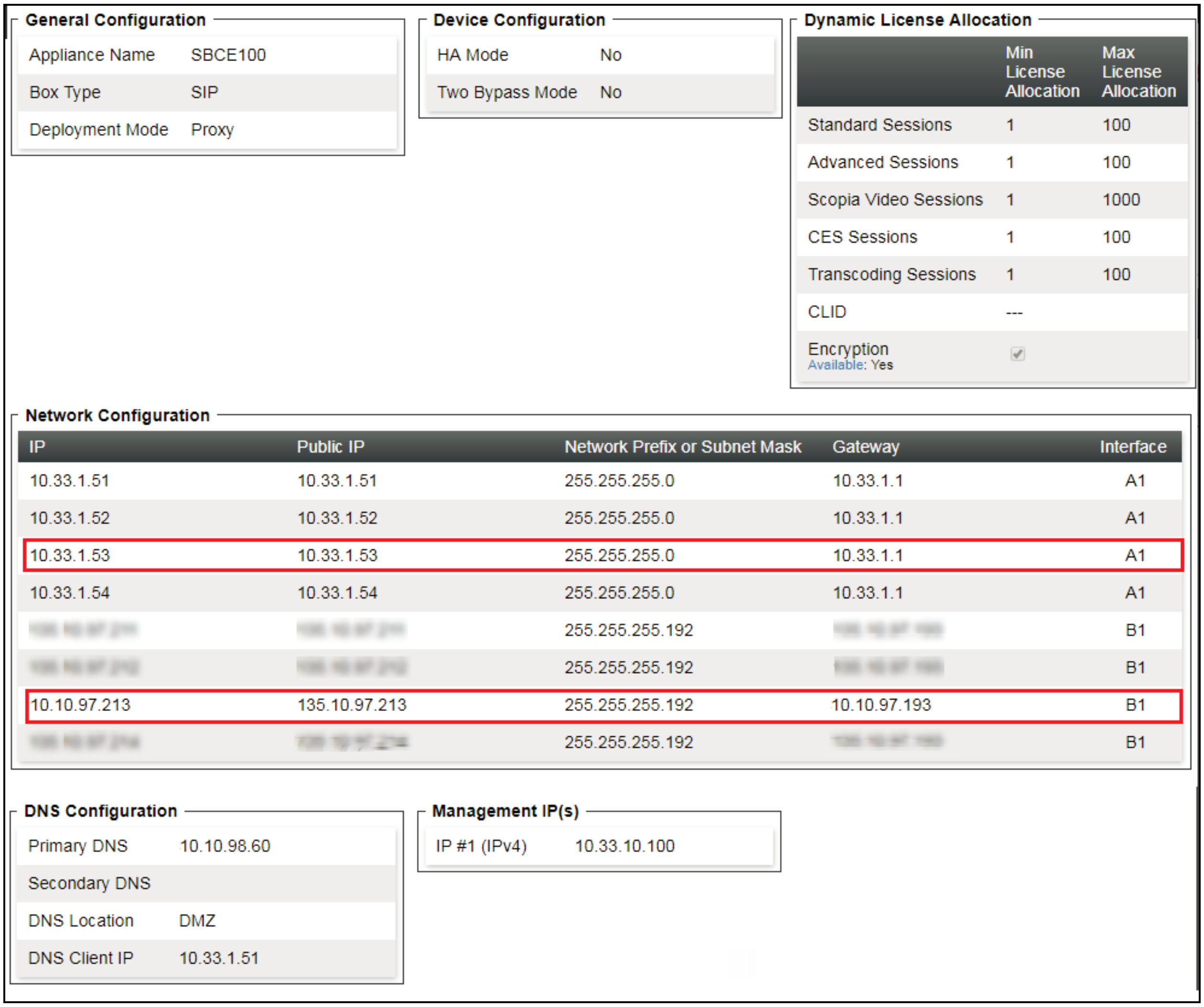
7.2. System Management

To view current system information, select **System Management** on the left navigation pane. A list of installed devices is shown in the **Devices** tab on the right pane. In the reference configuration, a single device named ***SBCE100*** is shown. The management IP address that was configured during installation is blurred out for security reasons, the current software version is shown. The management IP address needs to be on a subnet separate from the ones used in all other interfaces of the Avaya SBCE, segmented from all VoIP traffic. Verify that the **Status** is ***Commissioned***, indicating that the initial installation process of the device has been previously completed, as shown on the screen below.



Device Name	Management IP	Version	Status						
SBCE100	[redacted]	7.2.1.0-05-14222	Commissioned	Reboot	Shutdown	Restart Application	View	Edit	Uninstall

To view the network configuration assigned to the Avaya SBCE, click **View** on the previous screen. The **System Information** window is displayed, containing the current device configuration and network settings.



General Configuration

Appliance Name	SBCE100
Box Type	SIP
Deployment Mode	Proxy

Device Configuration

HA Mode	No
Two Bypass Mode	No

Dynamic License Allocation

	Min License Allocation	Max License Allocation
Standard Sessions	1	100
Advanced Sessions	1	100
Scopia Video Sessions	1	1000
CES Sessions	1	100
Transcoding Sessions	1	100
CLID	---	
Encryption Available: Yes	☑	

Network Configuration

IP	Public IP	Network Prefix or Subnet Mask	Gateway	Interface
10.33.1.51	10.33.1.51	255.255.255.0	10.33.1.1	A1
10.33.1.52	10.33.1.52	255.255.255.0	10.33.1.1	A1
10.33.1.53	10.33.1.53	255.255.255.0	10.33.1.1	A1
10.33.1.54	10.33.1.54	255.255.255.0	10.33.1.1	A1
[redacted]	[redacted]	255.255.255.192	[redacted]	B1
[redacted]	[redacted]	255.255.255.192	[redacted]	B1
10.10.97.213	135.10.97.213	255.255.255.192	10.10.97.193	B1
[redacted]	[redacted]	255.255.255.192	[redacted]	B1

DNS Configuration

Primary DNS	10.10.98.60
Secondary DNS	
DNS Location	DMZ
DNS Client IP	10.33.1.51

Management IP(s)

IP #1 (IPv4)	10.33.10.100

The highlighted IP addresses in the **System Information** screen are the ones used for the SIP trunk to MTS, and are the ones relevant to these Application Notes. Other IP addresses assigned to the Avaya SBCE **A1** and **B1** interfaces are used to support remote workers and other SIP trunks, and they are not discussed in this document. Also note that for security purposes, any public IP addresses used during the compliance test have been masked in this document.

In the reference configuration, the private interface of the Avaya SBCE (10.33.1.53) was used to connect to the enterprise network, while its public interface (10.10.97.213) was used to connect to the public network. See **Figure 1**.

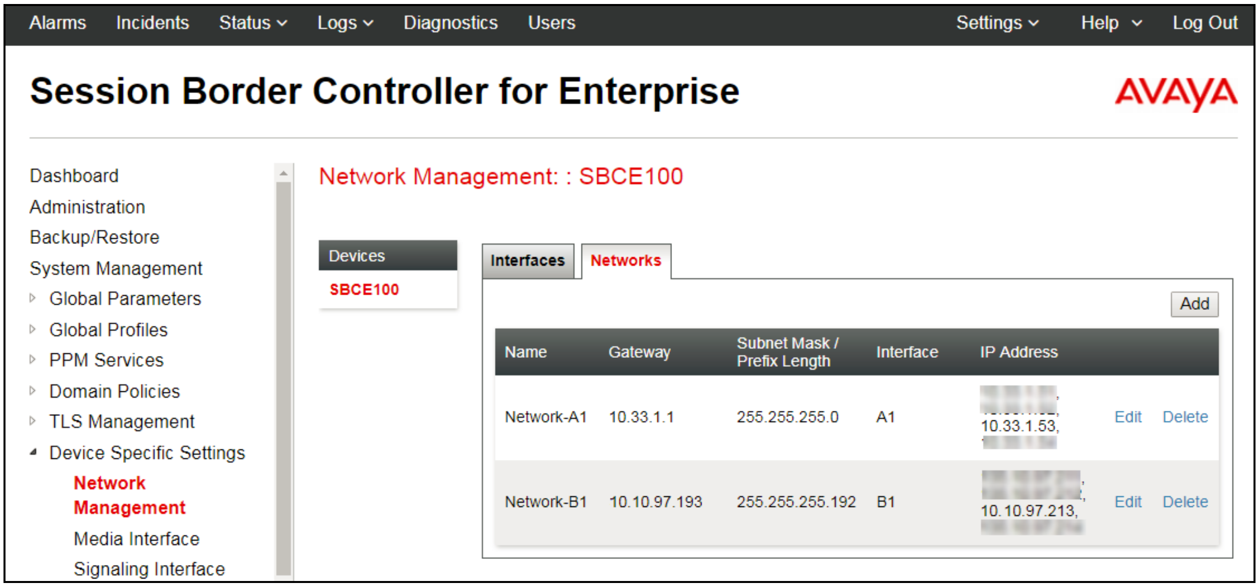
On the **License Allocation** area of the **System Information**, verify that the number of **Standard Sessions** is sufficient to support the desired number of simultaneous SIP calls across all SIP trunks at the enterprise. The number of sessions and encryption features are primarily controlled by the license file installed.

7.3. Network Management

The network configuration parameters should have been previously specified during installation of the Avaya SBCE. In the event that changes need to be made to the network configuration, they can be entered here.

Select **Network Management** from **Device Specific Settings** on the left-side menu. Under **Devices** in the center pane, select the device being managed, ***SBCE100*** in the sample configuration. On the **Networks** tab, verify or enter the network information as needed.

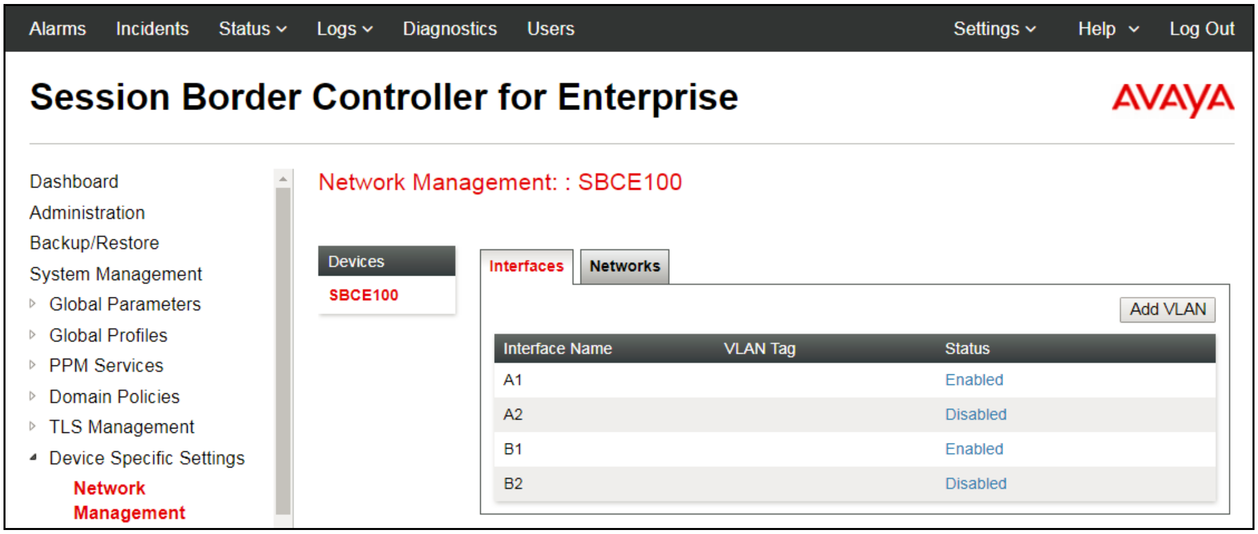
Note that in the configuration used during the compliance test, the IP addresses assigned to the private (***10.33.1.53***) and public (***10.10.97.213***) sides of the Avaya SBCE are the ones relevant to these Application Notes.



Network Management: : SBCE100

Name	Gateway	Subnet Mask / Prefix Length	Interface	IP Address		
Network-A1	10.33.1.1	255.255.255.0	A1	[redacted], 10.33.1.53, [redacted]	Edit	Delete
Network-B1	10.10.97.193	255.255.255.192	B1	[redacted], 10.10.97.213, [redacted]	Edit	Delete

On the **Interfaces** tab, verify the **Administrative Status** is **Enabled** for the **A1** and **B1** interfaces. Click the buttons under the **Status** column if necessary to enable the interfaces.



Network Management: : SBCE100

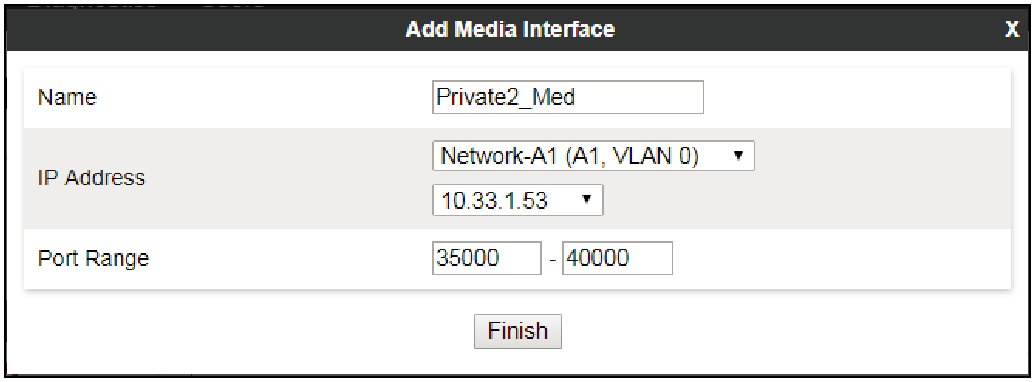
Interface Name	VLAN Tag	Status
A1		Enabled
A2		Disabled
B1		Enabled
B2		Disabled

7.4. Media Interfaces

Media Interfaces were created to specify the IP address and port range in which the Avaya SBCE will accept media streams on each interface. Packets leaving the interfaces of the Avaya SBCE will advertise this IP address, and one of the ports in this range as the listening IP address and port in which it will accept media from the Call Server or the trunk server.

To add the Media Interface in the enterprise direction, select **Media Interface** from the **Device Specific Settings** menu on the left-hand side, select the device being managed and click the **Add** button (not shown).

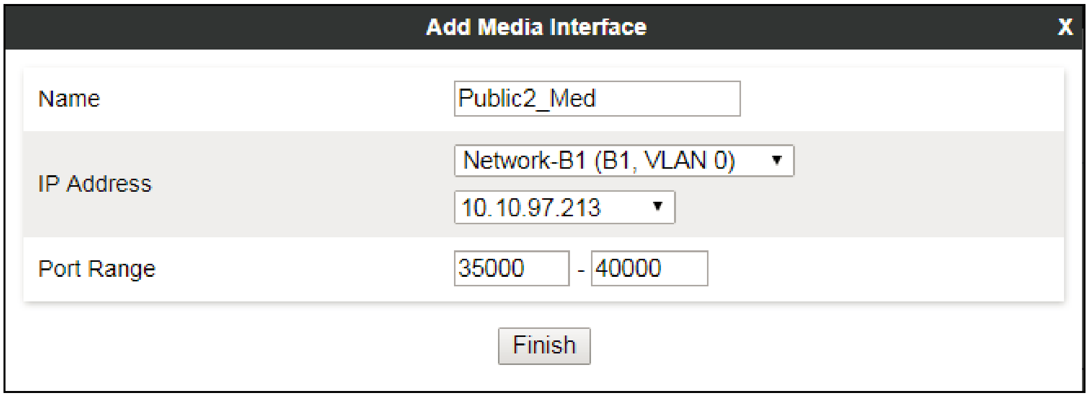
- On the **Add Media Interface** screen, enter an appropriate **Name** for the Media Interface.
- Under **IP Address**, select from the drop-down menus the network and IP address to be associated with this interface.
- The **Port Range** was left at the default values of ***35000-40000***.
- Click **Finish**.



Name	Private2_Med
IP Address	Network-A1 (A1, VLAN 0) 10.33.1.53
Port Range	35000 - 40000

A Media Interface facing the public side was similarly created with the name ***Public2_Med***, as shown below.

- Under **IP Address**, the network and IP address to be associated with this interface was selected.
- The **Port Range** was left at the default values.
- Click **Finish**.



Add Media Interface

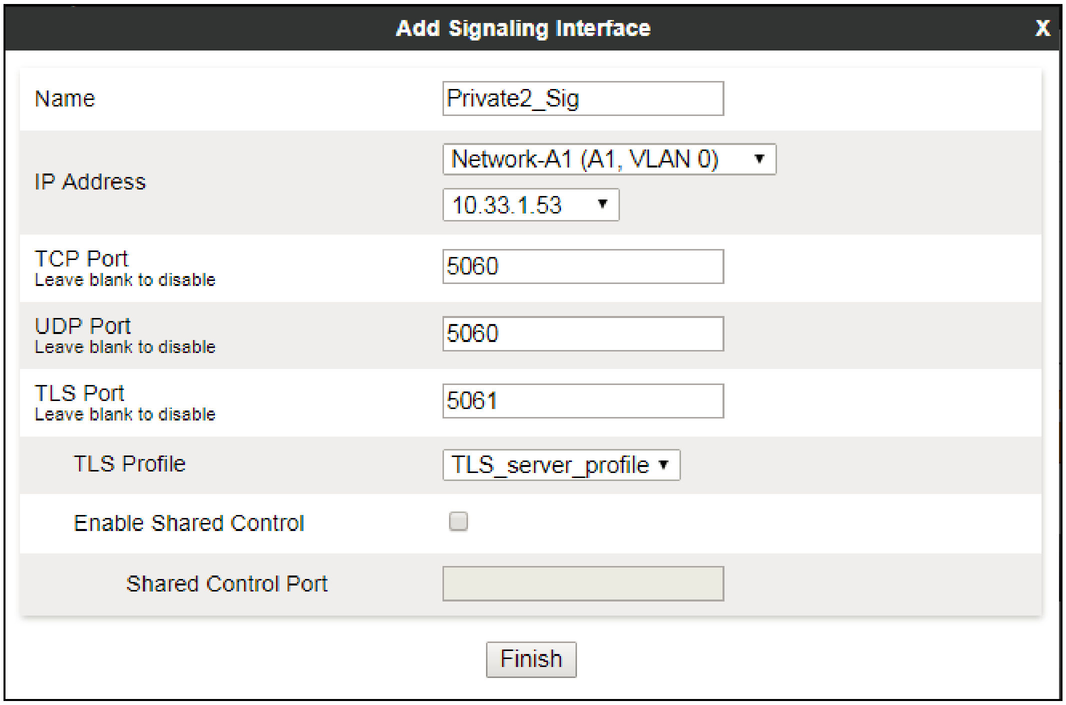
Name	Public2_Med
IP Address	Network-B1 (B1, VLAN 0) 10.10.97.213
Port Range	35000 - 40000

7.5. Signaling Interfaces

Signaling Interfaces are created to specify the IP addresses and ports in which the Avaya SBCE will listen for signaling traffic in the connected networks.

To add the Signaling Interface in the enterprise direction, select **Signaling Interface** from the **Device Specific Settings** menu on the left-hand side, select the device being managed and click the **Add** button (not shown).

- On the **Add Signaling Interface** screen, enter an appropriate **Name** for the interface.
- Under **IP Address**, select from the drop-down menus the network and IP address to be associated with this interface.
- Enter ***5061*** for **TLS Port**, since TLS port 5061 is used to listen for signaling traffic from Session Manager in the sample configuration, as defined in **Section 6.6**.
- Select a **TLS Profile** (See Note below).
- Click **Finish**.

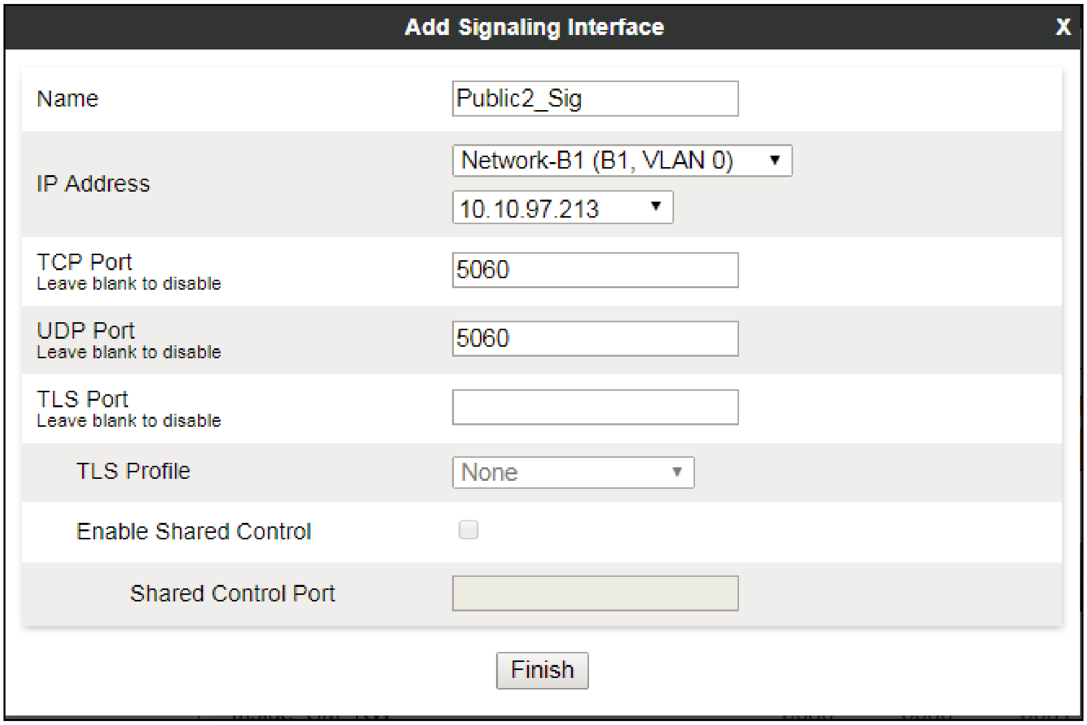


Name	Private2_Sig
IP Address	Network-A1 (A1, VLAN 0) ▾ 10.33.1.53 ▾
TCP Port Leave blank to disable	5060
UDP Port Leave blank to disable	5060
TLS Port Leave blank to disable	5061
TLS Profile	TLS_server_profile ▾
Enable Shared Control	□
Shared Control Port	

Note - The configuration tasks required to support TLS transport for signaling and SRTP for media inside of the enterprise (private network side) are beyond the scope of these Application Notes; hence they are not discussed in this document

A second Signaling Interface with the name ***Public2_Sig*** was similarly created in the service provider's direction.

- Under **IP Address**, select from the drop-down menus the network and IP address to be associated with this interface.
- Enter ***5060*** for **UDP Port**, since this is the protocol and port used by the Avaya SBCE to listen to the service provider's SIP traffic.
- Click **Finish**.



Add Signaling Interface

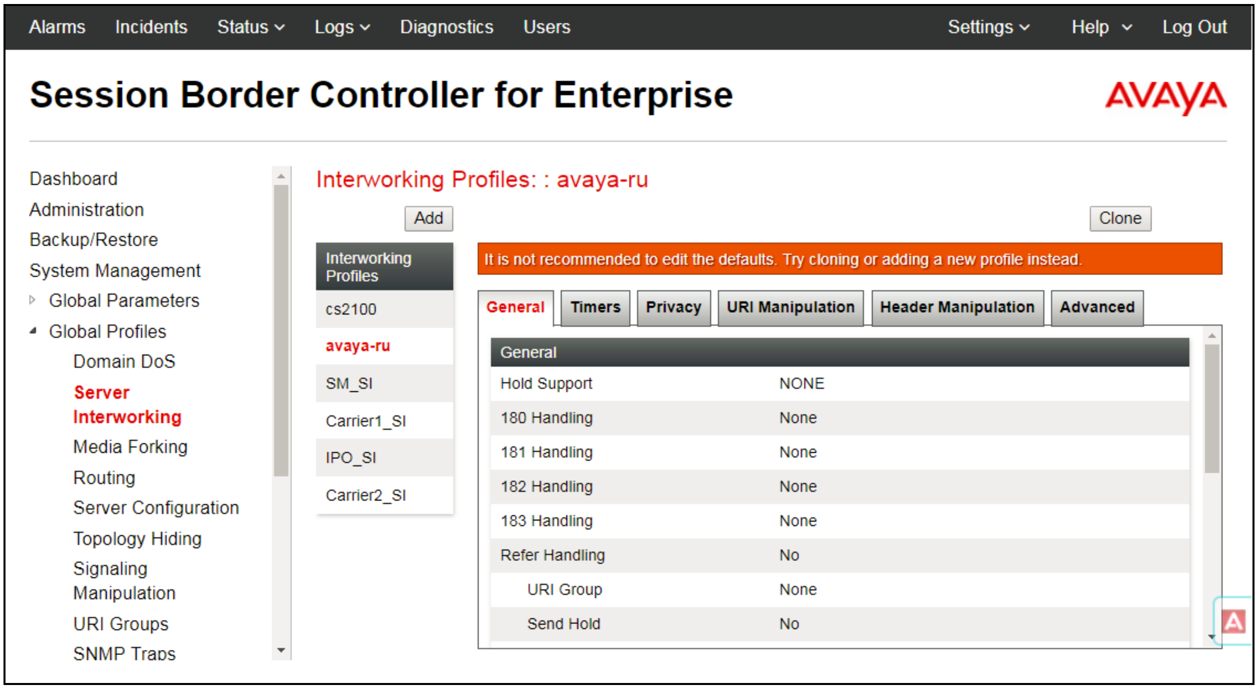
Name	Public2_Sig
IP Address	Network-B1 (B1, VLAN 0) ▼ 10.10.97.213 ▼
TCP Port Leave blank to disable	5060
UDP Port Leave blank to disable	5060
TLS Port Leave blank to disable	
TLS Profile	None ▼
Enable Shared Control	□
Shared Control Port	

7.6. Server Interworking

Interworking Profile features are configured to facilitate the interoperability between the enterprise SIP-enabled solution (Call Server) and the SIP trunk service provider (Trunk Server).

7.6.1. Server Interworking Profile – Enterprise

Interworking profiles can be created by cloning one of the pre-defined default profiles, or by adding a new profile. To configure the interworking profile in the enterprise direction, select **Global Profiles → Server Interworking** on the left navigation pane. Under **Interworking Profiles**, select ***avaya-ru*** from the list of pre-defined profiles. Click **Clone**.

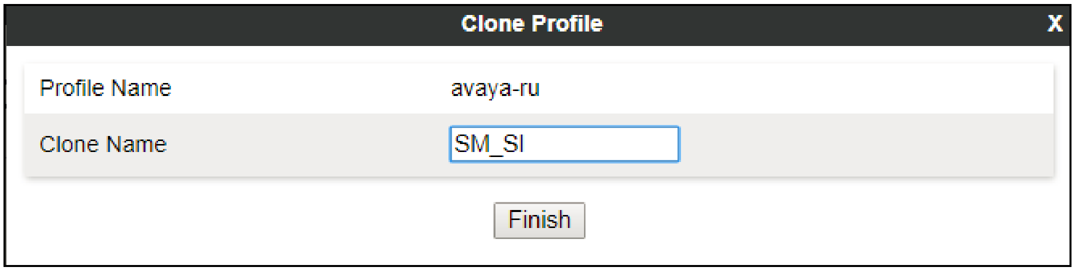


Interworking Profiles: : avaya-ru

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

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

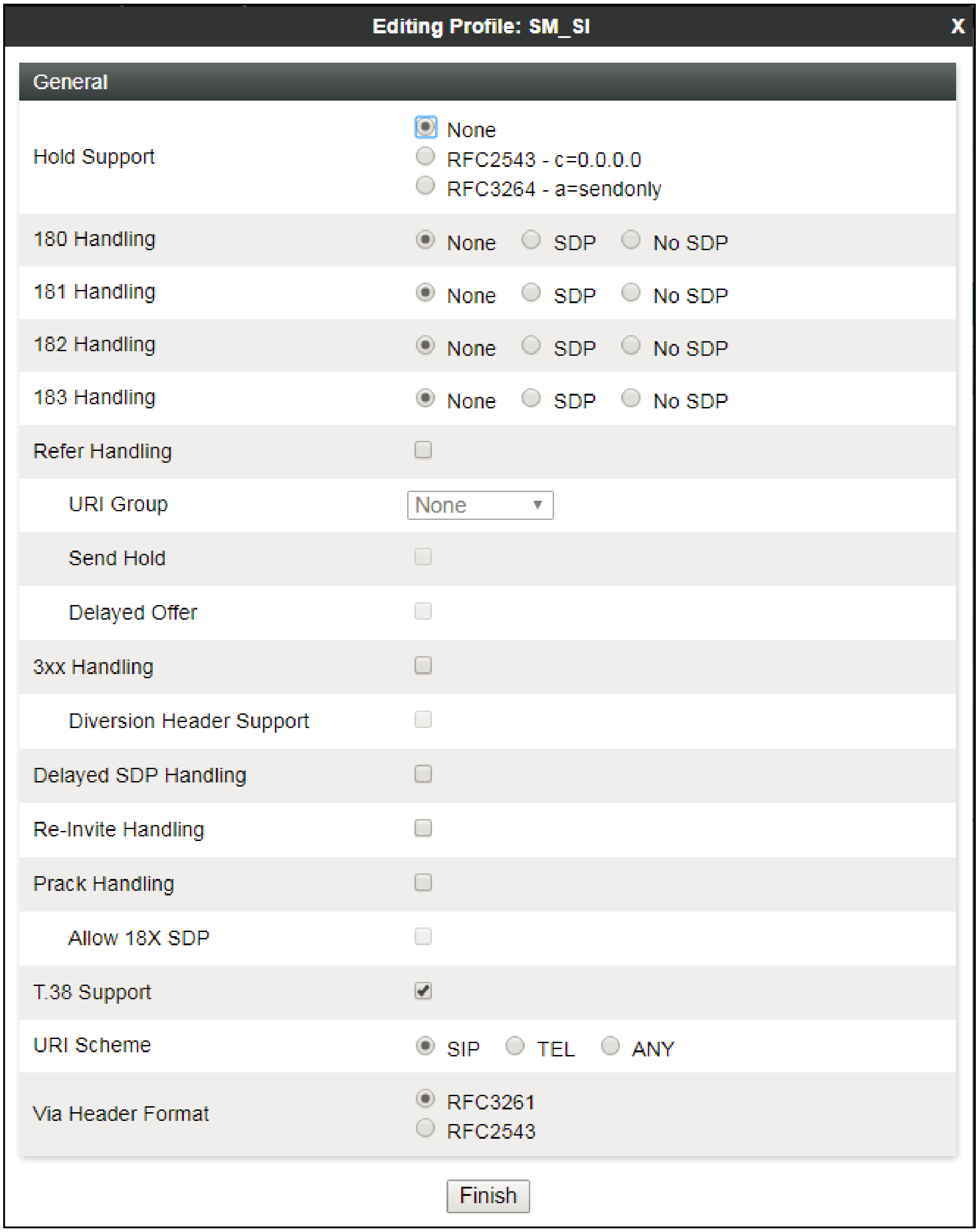
- Enter a descriptive name for the cloned profile.
- Click **Finish**.



Profile Name	avaya-ru
Clone Name	SM_SI

Click **Edit** on the newly cloned ***SM_SI*** interworking profile:

- On the **General** tab, check ***T.38 Support***.
- Leave remaining fields with default values.
- Click **Finish**.



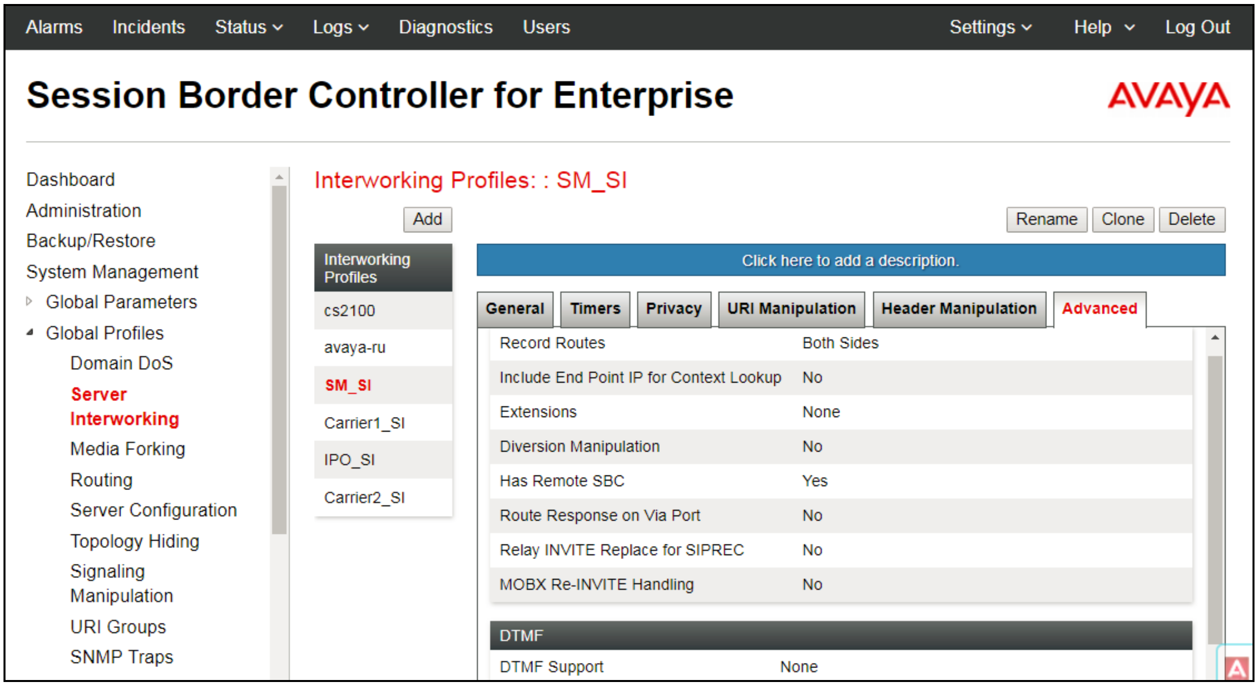
Editing Profile: SM_SI X

General

Hold Support	● None ○ RFC2543 - c=0.0.0.0 ○ RFC3264 - a=sendonly
180 Handling	● None ○ SDP ○ No SDP
181 Handling	● None ○ SDP ○ No SDP
182 Handling	● None ○ SDP ○ No SDP
183 Handling	● None ○ SDP ○ No SDP
Refer Handling	□
URI Group	None ▾
Send Hold	□
Delayed Offer	□
3xx Handling	□
Diversion Header Support	□
Delayed SDP Handling	□
Re-Invite Handling	□
Prack Handling	□
Allow 18X SDP	□
T.38 Support	☑
URI Scheme	● SIP ○ TEL ○ ANY
Via Header Format	● RFC3261 ○ RFC2543

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

The **Advanced** tab settings are shown on the screen below:



Record Routes	Both Sides
Include End Point IP for Context Lookup	No
Extensions	None
Diversion Manipulation	No
Has Remote SBC	Yes
Route Response on Via Port	No
Relay INVITE Replace for SIPREC	No
MOBX Re-INVITE Handling	No

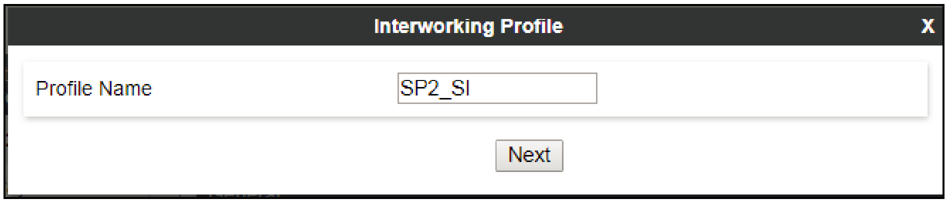
DTMF

DTMF Support	None

7.6.2. Server Interworking Profile – Service Provider

A second interworking profile in the direction of the SIP trunk was created, by adding a new profile in this case. Select **Global Profiles → Server Interworking** on the left navigation pane and click **Add** (not shown).

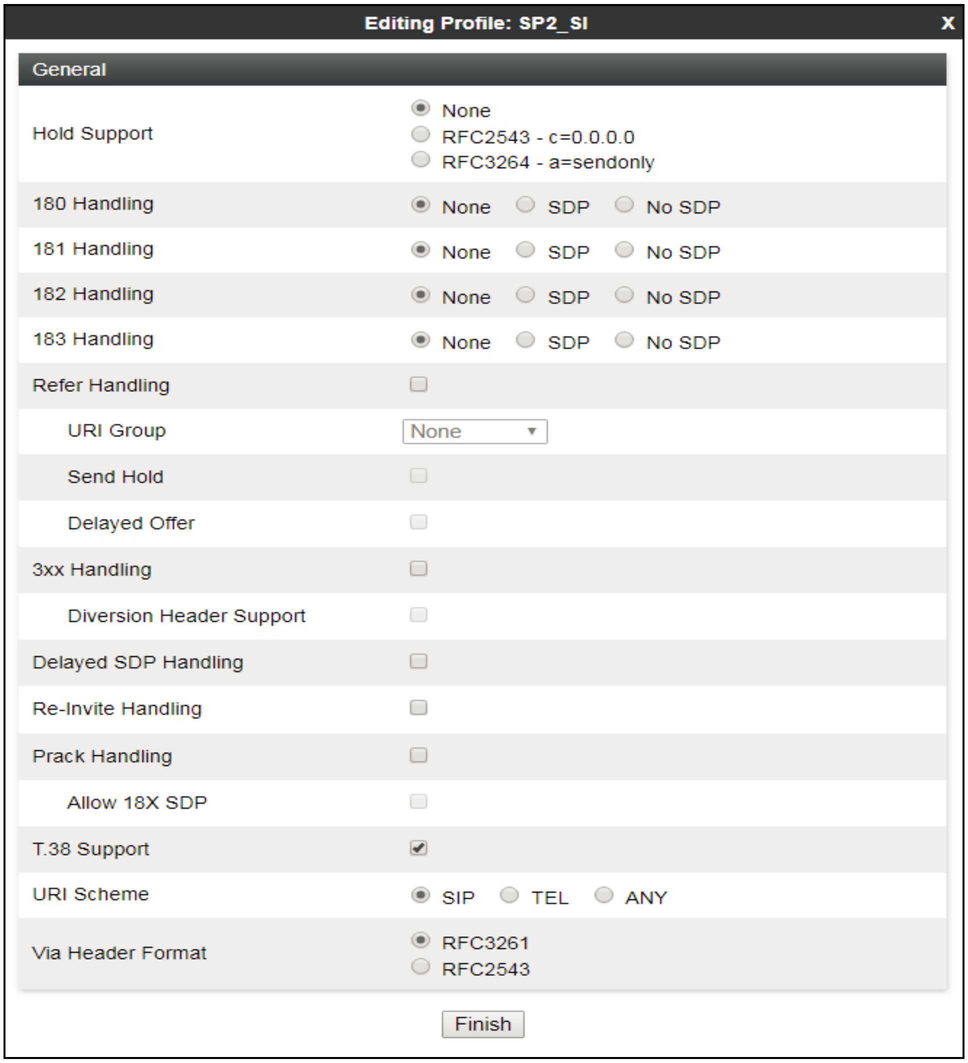
- Enter a descriptive name for the new profile.
- Click **Next**.



Interworking Profile

Profile Name	SP2_SI

On the **General** tab, check ***T.38 Support***. Click **Next**, then click **Finish** on the last tab leaving remaining fields with default values (not shown).



Editing Profile: SP2_SI

General

Hold Support	● None ○ RFC2543 - c=0.0.0.0 ○ RFC3264 - a=sendonly
180 Handling	● None ○ SDP ○ No SDP
181 Handling	● None ○ SDP ○ No SDP
182 Handling	● None ○ SDP ○ No SDP
183 Handling	● None ○ SDP ○ No SDP
Refer Handling	☐
URI Group	None
Send Hold	☐
Delayed Offer	☐
3xx Handling	☐
Diversion Header Support	☐
Delayed SDP Handling	☐
Re-Invite Handling	☐
Prack Handling	☐
Allow 18X SDP	☐
T.38 Support	☑
URI Scheme	● SIP ○ TEL ○ ANY
Via Header Format	● RFC3261 ○ RFC2543

7.7. Signaling Manipulation

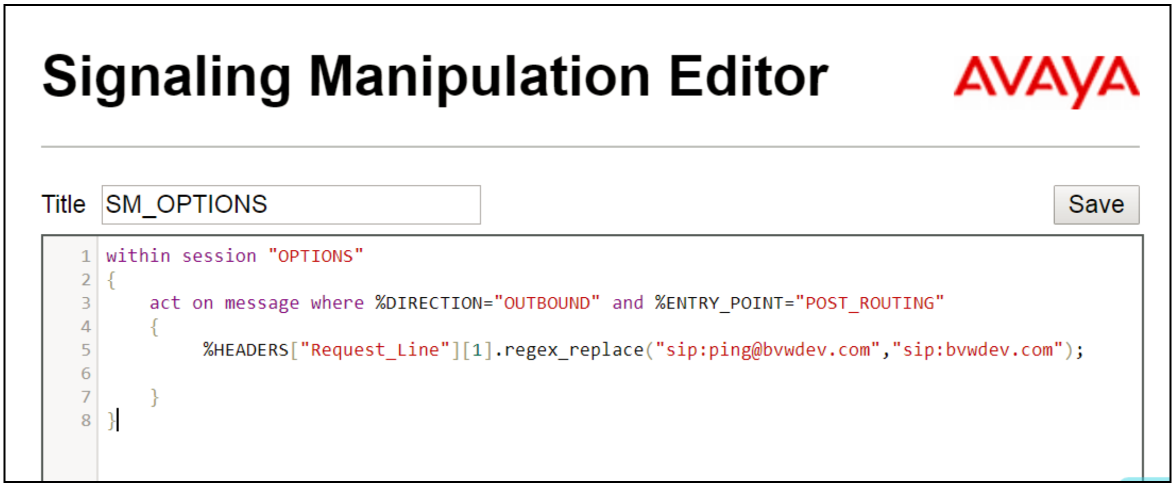
Signaling Manipulation feature allows the ability to add, change and delete any of the headers in a SIP message. This feature adds the ability to configure such manipulation in a highly flexible manner using a proprietary scripting language called **SigMa**.

7.7.1. Signaling Manipulation – Enterprise

To create a Signaling Manipulation script that will be applied for enterprise, select **Global Profiles → Signaling Manipulation**. Click **Add Script** (not shown).

The **Signaling Manipulation Editor** window is displayed; enter the ***SM_OPTIONS*** name in the ***Title*** and enter content of the script as shown below.

The purpose of the script is to remove the username ***ping*** in the URI of **Request_Line** header of OPTIONS message that is sent from MTS. If the username ***ping*** is not removed, Session Manager rejected the OPTIONS message with error ***404 Route Not Found***.



Title: SM_OPTIONS

```
within session "OPTIONS"
{
    act on message where %DIRECTION="OUTBOUND" and %ENTRY_POINT="POST_ROUTING"
    {
        %HEADERS["Request_Line"][1].regex_replace("sip:ping@bvwdev.com","sip:bvwdev.com");

    }
}
```

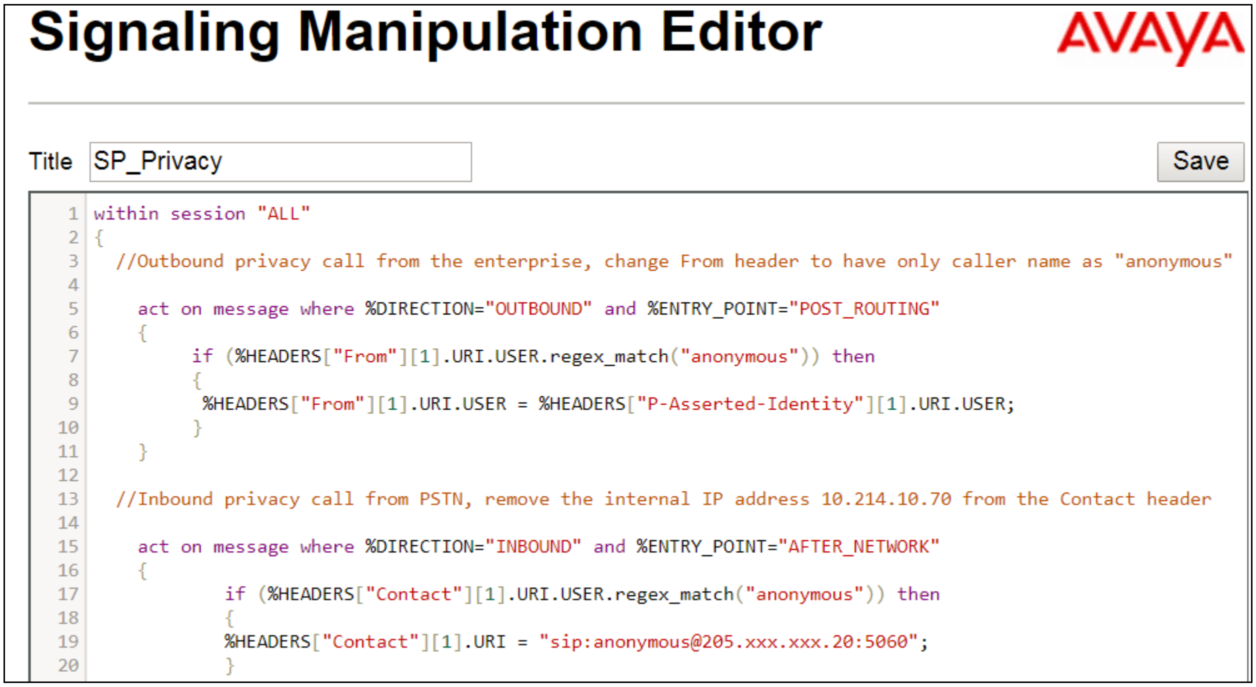
Below is the text version of the signaling manipulation script.

```
within session "OPTIONS"
{
    act on message where %DIRECTION="OUTBOUND" and %ENTRY_POINT="POST_ROUTING"
    {

%HEADERS["Request_Line"][1].regex_replace("sip:ping@bvwdev.com","sip:bvwdev.com");

    }
}
```

7.7.2. Signaling Manipulation – Service Provider

Repeat the same procedure above to create another signaling manipulation script for service provider and named it as ***SP_Privacy***.

The signaling manipulation script was applied to **Server Configuration** for service provider for privacy call.



Signaling Manipulation Editor

Title: SP_Privacy

```
within session "ALL"
{
  //Outbound privacy call from the enterprise, change From header to have only caller name as "anonymous"

    act on message where %DIRECTION="OUTBOUND" and %ENTRY_POINT="POST_ROUTING"
    {
         if (%HEADERS["From"][1].URI.USER.regex_match("anonymous")) then
         {
          %HEADERS["From"][1].URI.USER = %HEADERS["P-Asserted-Identity"][1].URI.USER;
         }
    }

  //Inbound privacy call from PSTN, remove the internal IP address 10.214.10.70 from the Contact header

    act on message where %DIRECTION="INBOUND" and %ENTRY_POINT="AFTER_NETWORK"
    {
            if (%HEADERS["Contact"][1].URI.USER.regex_match("anonymous")) then
            {
            %HEADERS["Contact"][1].URI = "sip:anonymous@205.xxx.xxx.20:5060";
            }
```

Below is the text version of the signaling manipulation for Enterprise.

```
within session "ALL"
{
    //Outbound privacy call from the enterprise, change From header to have only
caller name as "anonymous"
    act on message where %DIRECTION="OUTBOUND" and %ENTRY_POINT="POST_ROUTING"
    {
          if (%HEADERS["From"][1].URI.USER.regex_match("anonymous")) then
      {
          %HEADERS["From"][1].URI.USER = %HEADERS["P-Asserted-Identity"][1].URI.USER;
      }
    }
   //Inbound privacy call from PSTN, remove the internal IP address 10.214.10.70 from
the Contact header

    act on message where %DIRECTION="INBOUND" and %ENTRY_POINT="AFTER_NETWORK"
    {
            if (%HEADERS["Contact"][1].URI.USER.regex_match("anonymous")) then
            {
            %HEADERS["Contact"][1].URI = "sip:anonymous@205.xxx.xxx.20:5060";
            }
    }
}
```

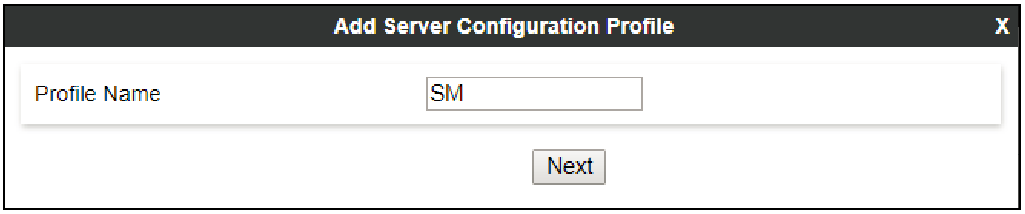
7.8. Server Configuration

Server Profiles are created to define the parameters for the Avaya SBCE peers; Session Manager (Call Server) at the enterprise and MTS SIP Proxy (Trunk Server).

7.8.1. Server Configuration Profile – Enterprise

From the **Global Profiles** menu on the left-hand navigation pane, select **Server Configuration** and click the **Add** button (not shown) to add a new profile for the Call Server.

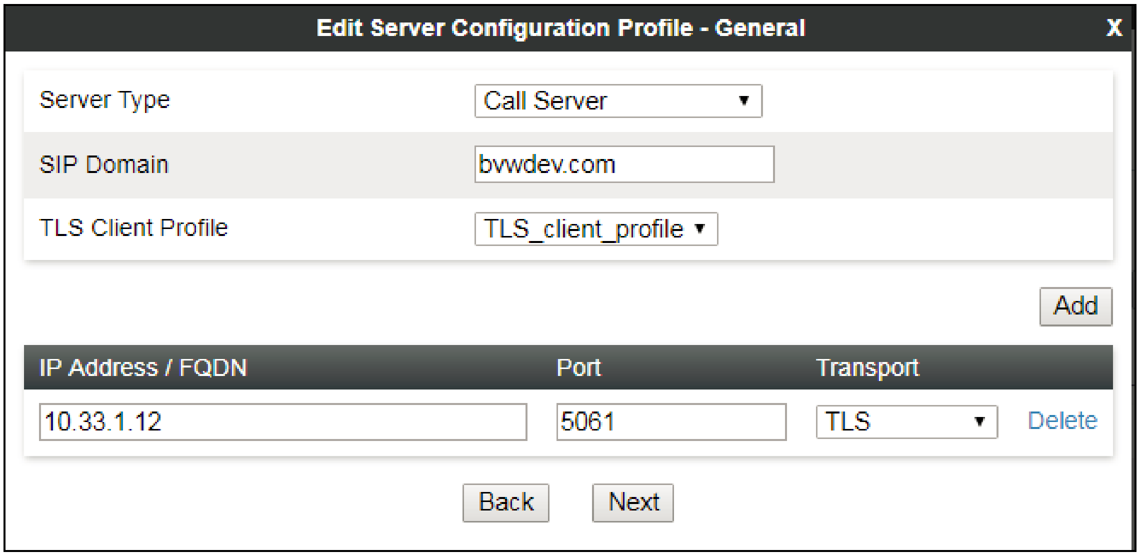
- Enter an appropriate **Profile Name** similar to the screen below.
- Click **Next**.



Add Server Configuration Profile

Profile Name	SM

- On the **Edit Server Configuration Profile – General** tab select ***Call Server*** from the drop-down menu under the **Server Type**.
- Select a **TLS Client Profile**.
- On the **IP Addresses / FQDN** field, enter the IP address of the Session Manager Security Module (**Section 6.5**).
- Enter ***5061*** under **Port** and select ***TLS*** for **Transport**. The transport protocol and port selected here must match the values defined for the Entity Link to the Session Manager previously created in **Section 6.6**.
- Click **Next**.

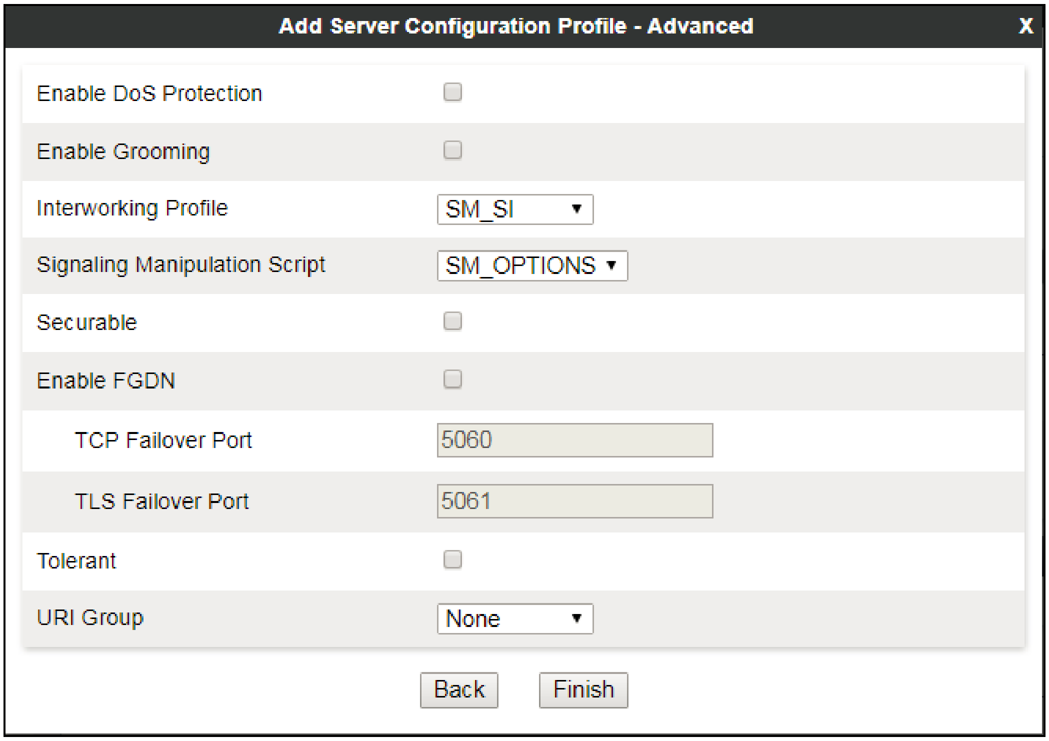


Edit Server Configuration Profile - General

Server Type	Call Server
SIP Domain	bvwdev.com
TLS Client Profile	TLS_client_profile

IP Address / FQDN	Port	Transport	
10.33.1.12	5061	TLS	Delete

- Click **Next** until the **Add Server Configuration Profile – Advanced** tab is reached (not shown).
- On the **Add Server Configuration Profile – Advanced** tab select ***SM_SI*** from the **Interworking Profile** drop-down menu (**Section 7.6.1**) and ***SM_OTIONS*** from the **Signaling Manipulation Script** drop-down menu (**Section 7.7.1**).
- Click **Finish**.



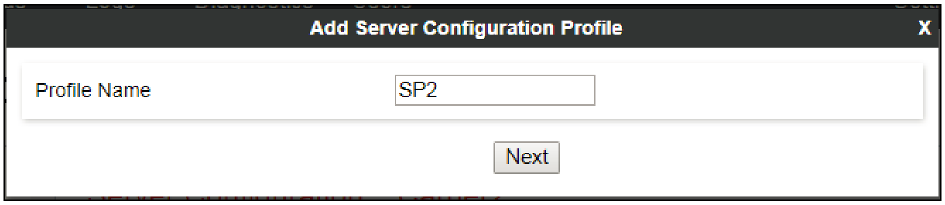
Add Server Configuration Profile - Advanced

Enable DoS Protection	□
Enable Grooming	□
Interworking Profile	SM_SI
Signaling Manipulation Script	SM_OPTIONS
Securable	□
Enable FGDN	□
TCP Failover Port	5060
TLS Failover Port	5061
Tolerant	□
URI Group	None

7.8.2. Server Configuration Profile – Service Provider

Similarly, to add the profile for the Trunk Server, click the **Add** button on the **Server Configuration** screen (not shown).

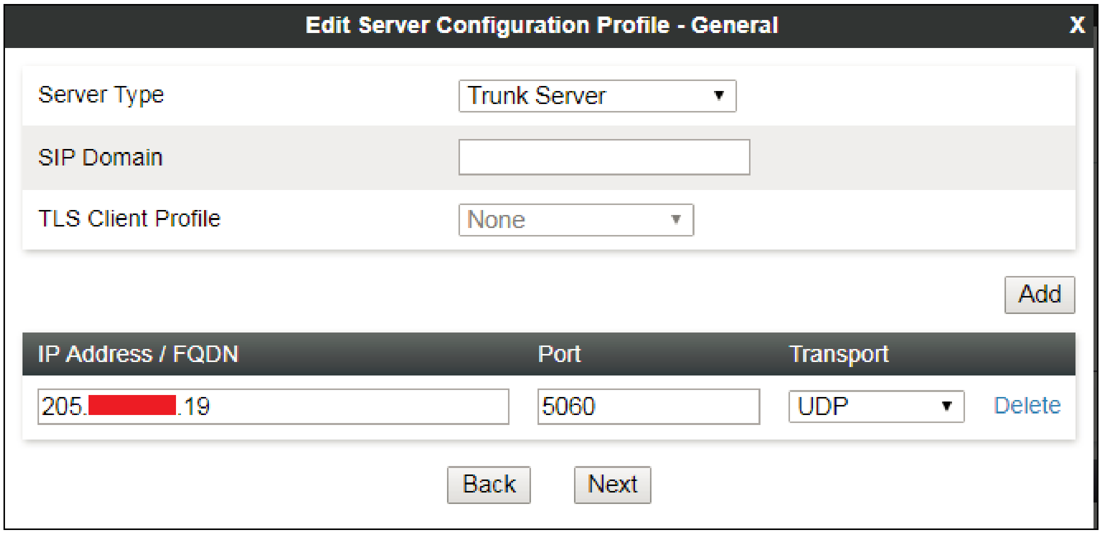
- Enter an appropriate **Profile Name** similar to the screen below.
- Click **Next**.



Add Server Configuration Profile

Profile Name	SP2

- On the **Edit Server Configuration Profile - General** Tab select ***Trunk Server*** from the drop-down menu for the **Server Type**.
- On the **IP Addresses / FQDN** field, enter the IP address of the MTS SIP proxy server. This information was provided by MTS.
- Enter ***5060*** under **Port**, and select **UDP** for **Transport** for both entries.
- Click **Next** until the **Add Server Configuration Profile – Advanced** tab is reached (not shown).

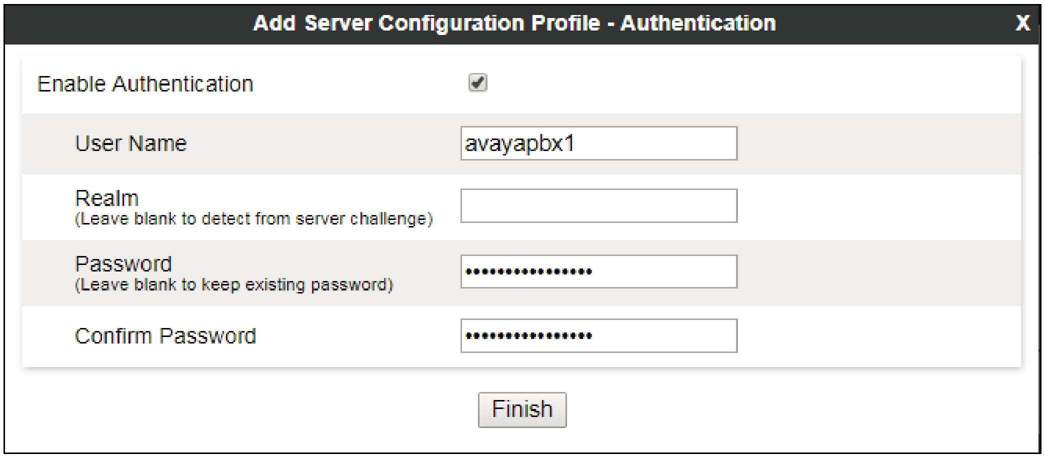


Edit Server Configuration Profile - General

Server Type	Trunk Server
SIP Domain	
TLS Client Profile	None

IP Address / FQDN	Port	Transport	
205.[redacted].19	5060	UDP	Delete

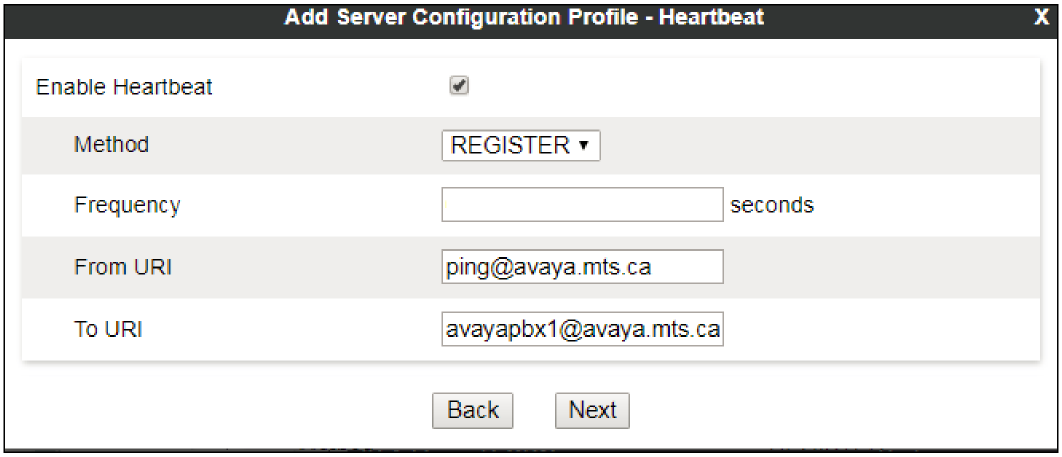
- On the **Add Server Configuration Profile – Authentication** tab, check the **Enable Authentication** checkbox; enter the username and password provided by MTS in the **Use Name** and **Password** and **Confirm Password** fields.



Add Server Configuration Profile - Authentication

Enable Authentication	☑
User Name	avayapbx1
Realm (Leave blank to detect from server challenge)	
Password (Leave blank to keep existing password)	••••••••••••••••
Confirm Password	••••••••••••••••

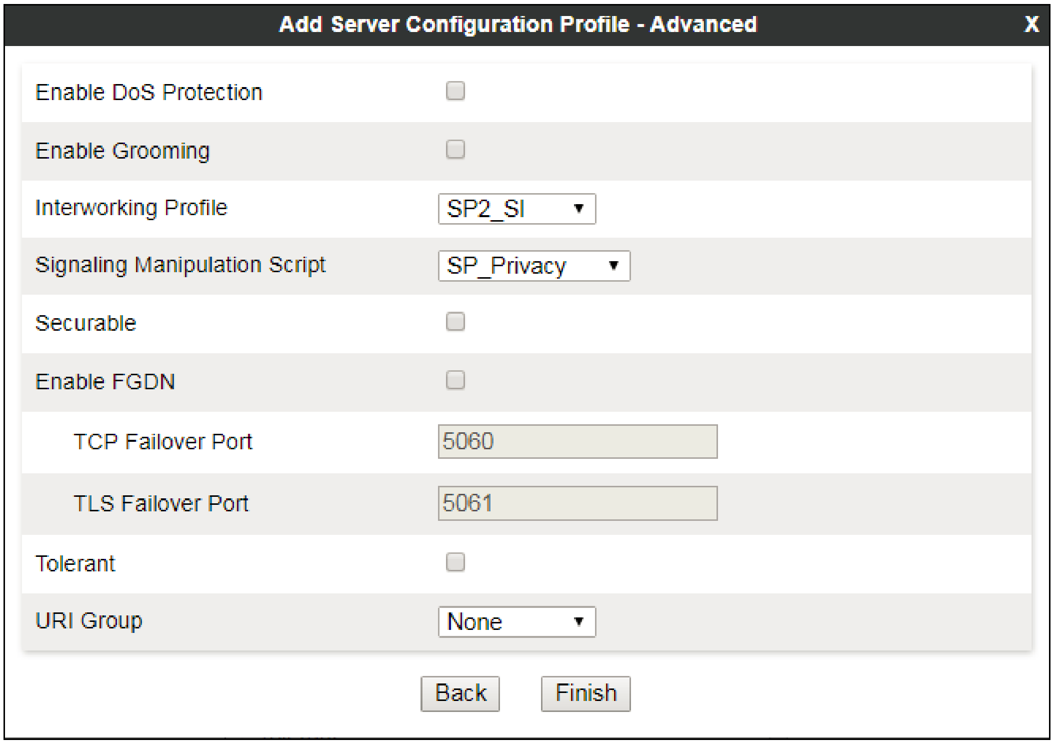
- On the **Add Server Configuration Profile – Heartbeat tab**, check the **Enable Heartbeat** checkbox and select **REGISTER** in the drop-down menu **Method**, enter the ***ping@avaya.mts.ca*** in the **From URI** field and ***avayapbx1@avaya.mts.ca*** in the **To URI** field. Note that the username part ***avayapbx1*** must be matched with the user name provided otherwise the REGISTER will be rejected by MST.



Add Server Configuration Profile - Heartbeat

Enable Heartbeat	☑
Method	REGISTER ▾
Frequency	seconds
From URI	ping@avaya.mts.ca
To URI	avayapbx1@avaya.mts.ca

- On the **Add Server Configuration Profile – Advanced** tab select ***SP2-SI*** from the **Interworking Profile** drop-down menu (**Section 7.6.2**) and ***SP_Privacy*** in the **Signaling Manipulation Script** drop-down menu (**Section 7.7.2**).
- Click **Finish**.



Add Server Configuration Profile - Advanced

Enable DoS Protection	□
Enable Grooming	□
Interworking Profile	SP2_SI
Signaling Manipulation Script	SP_Privacy
Securable	□
Enable FGDN	□
TCP Failover Port	5060
TLS Failover Port	5061
Tolerant	□
URI Group	None

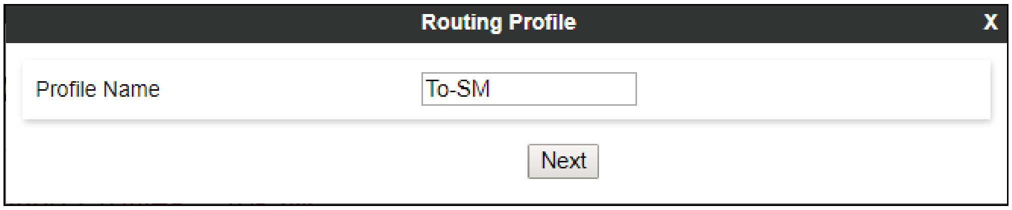
7.9. Routing

Routing profiles define a specific set of routing criteria that is used, in addition to other types of domain policies, to determine the path that the SIP traffic will follow as it flows through the Avaya SBCE interfaces. Two Routing Profiles were created in the test configuration, one for inbound calls, with Session Manager as the destination, and the second one for outbound calls, which are routed to the service provider SIP trunk.

7.9.1. Routing Profile – Enterprise

To create the inbound route, select the **Routing** tab from the **Global Profiles** menu on the left-hand side and select **Add** (not shown).

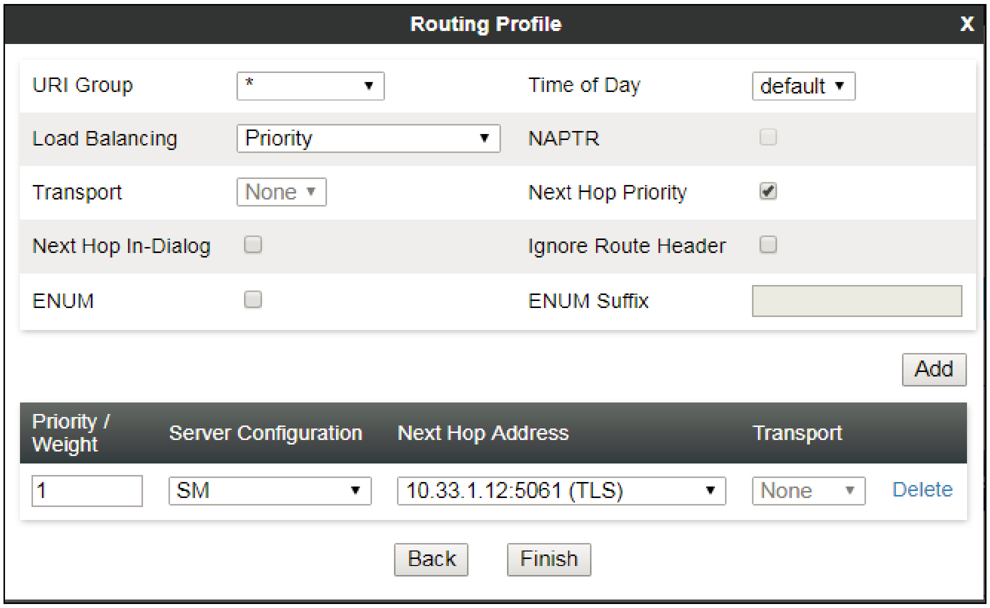
- Enter an appropriate **Profile Name** similar to the example below.
- Click **Next**.



Routing Profile

Profile Name	To-SM

- On the **Routing Profile** tab, click the **Add** button to enter the next-hop address.
- Under **Priority/Weight** enter ***1***.
- Under **Server Configuration**, select ***SM***. The **Next Hop Address** field will be populated with the IP address, port and protocol defined for the Session Manager Server Configuration Profile in **Section 7.8.1**.
- Defaults were used for all other parameters.
- Click **Finish**.



Routing Profile

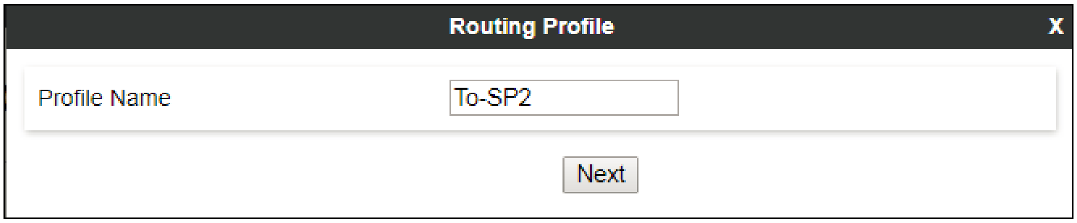
URI Group	*	Time of Day	default
Load Balancing	Priority	NAPTR	☐
Transport	None	Next Hop Priority	☑
Next Hop In-Dialog	☐	Ignore Route Header	☐
ENUM	☐	ENUM Suffix	

Priority / Weight	Server Configuration	Next Hop Address	Transport	
1	SM	10.33.1.12:5061 (TLS)	None	Delete

7.9.2. Routing Profile – Service Provider

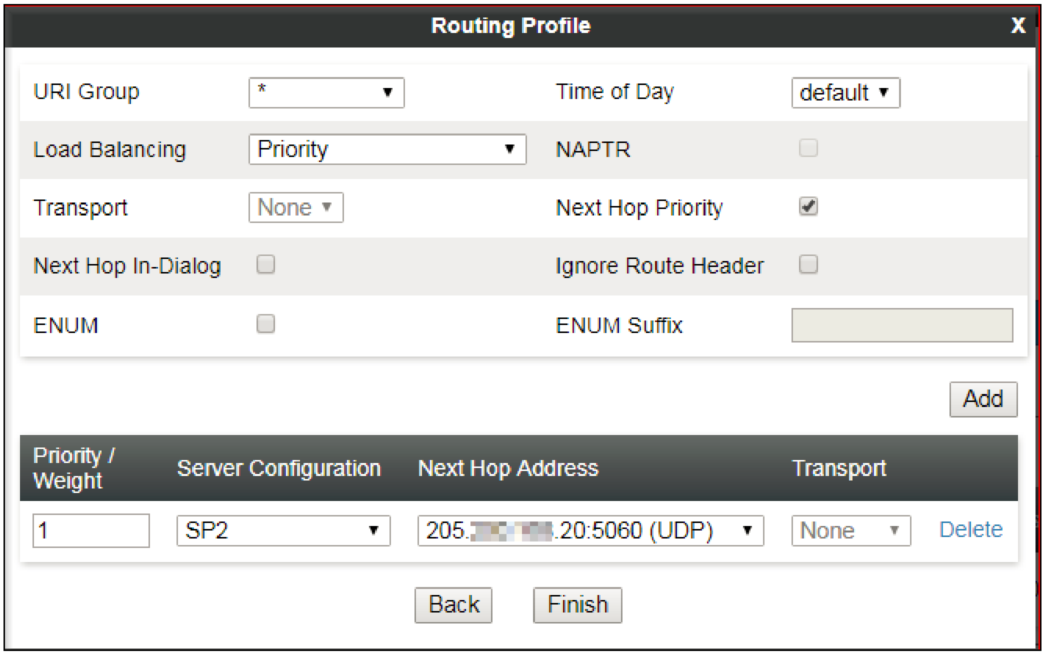
Back at the **Routing** tab, select **Add** (not shown) to repeat the process in order to create the outbound route.

- Enter an appropriate **Profile Name** similar to the example below.
- Click **Next**.



Profile Name	To-SP2

- On the **Routing Profile** tab, click the **Add** button to enter the next-hop address.
- Click on the **Add** button to add a **Next-Hop Address**.
- **Server Configuration**: Select ***SP2***.
- The **Next Hop Address** is populated automatically with ***205.xxx.xxx.20:5060 (UDP)*** MTS's SIP Proxy IP address, Port and Transport, Server Configuration Profile defined in **Section 7.8.2**
- Click **Finish**.



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

Priority / Weight	Server Configuration	Next Hop Address	Transport	
1	SP2 ▾	205.[redacted].20:5060 (UDP) ▾	None ▾	Delete

7.10. Topology Hiding

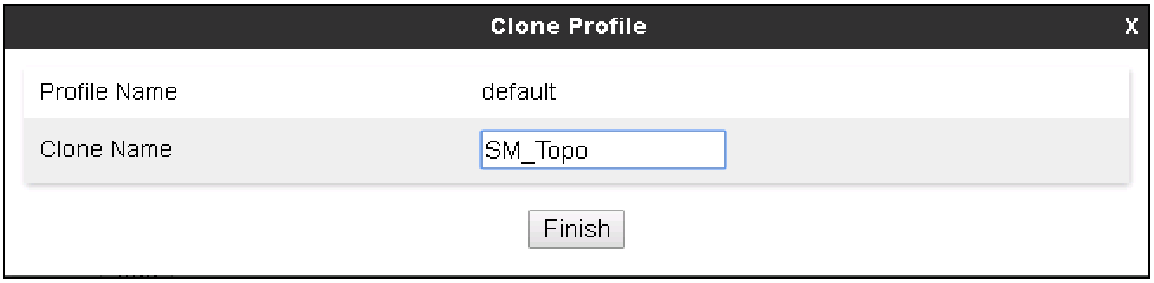
Topology Hiding is a security feature that allows the modification of several SIP headers, preventing private enterprise network information from being propagated to the untrusted public network.

Topology Hiding can also be used as an interoperability tool to adapt the host portion in the SIP headers to the IP addresses or domains expected on the service provider and the enterprise networks. For the compliance test, the default Topology Hiding Profile was cloned and modified accordingly. Only the minimum configuration required to achieve interoperability on the SIP trunk was performed. Additional steps can be taken in this section to further mask the information that is sent from the enterprise to the public network.

7.10.1. Topology Hiding Profile – Enterprise

To add the Topology Hiding Profile in the enterprise direction, select **Topology Hiding** from the **Global Profiles** menu on the left-hand side, select ***default*** from the list of pre-defined profiles and click the **Clone** button (not shown).

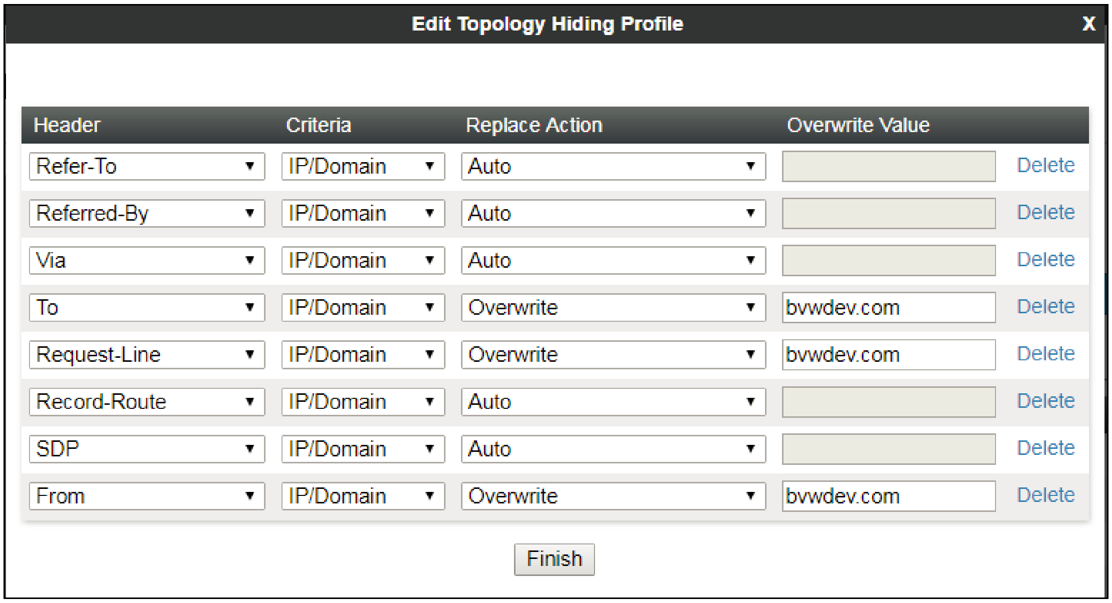
- Enter a **Clone Name** such as the one shown below.
- Click **Finish**.



Profile Name	default
Clone Name	SM_Topo

On the newly cloned ***SM_Topo*** profile screen, click the **Edit** button (not shown).

- For the, **From**, **To** and **Request-Line** headers, select ***Overwrite*** in the **Replace Action** column and enter the enterprise SIP domain ***bvwdev.com***, in the **Overwrite Value** column of these headers, as shown below. This is the domain known by Session Manager, defined in **Section 6.2**.
- Default values were used for all other fields.
- Click **Finish**.

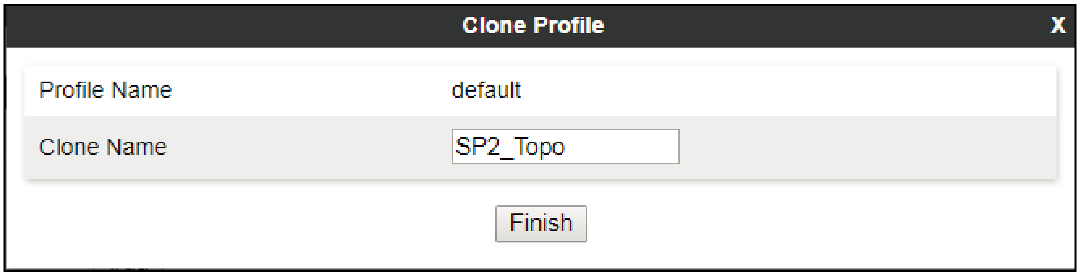


Header	Criteria	Replace Action	Overwrite Value	
Refer-To	IP/Domain	Auto		Delete
Referred-By	IP/Domain	Auto		Delete
Via	IP/Domain	Auto		Delete
To	IP/Domain	Overwrite	bvwdev.com	Delete
Request-Line	IP/Domain	Overwrite	bvwdev.com	Delete
Record-Route	IP/Domain	Auto		Delete
SDP	IP/Domain	Auto		Delete
From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

7.10.2. Topology Hiding Profile – Service Provider

To add the Topology Hiding Profile in the service provider direction, select **Topology Hiding** from the **Global Profiles** menu on the left-hand side, select ***default*** from the list of pre-defined profiles and click the **Clone** button (not shown).

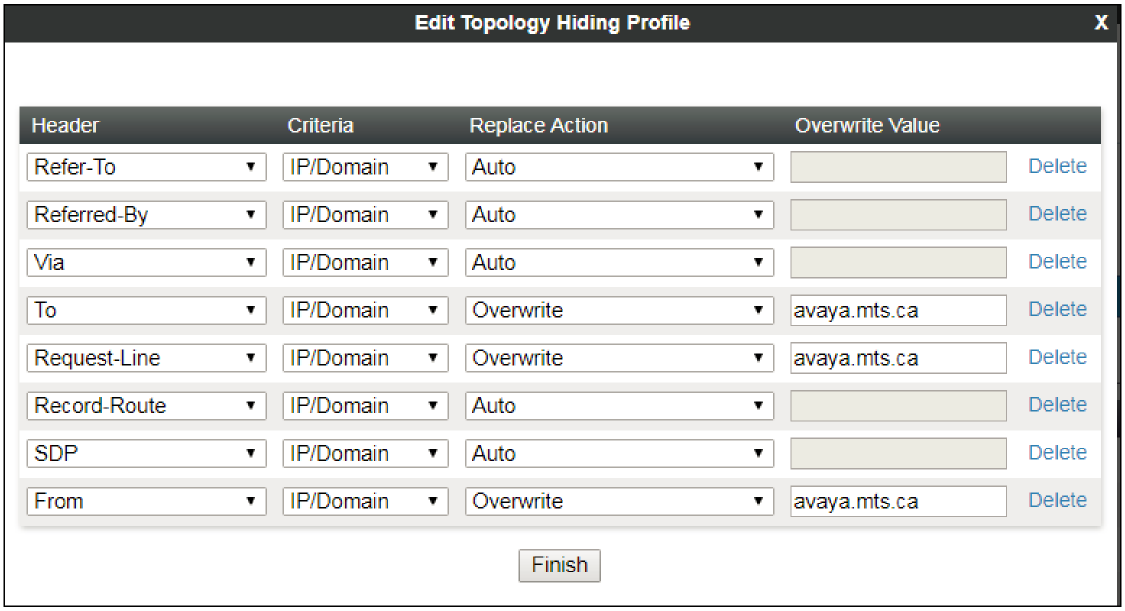
- Enter a **Clone Name** such as the one shown below.
- Click **Finish**.



Clone Profile

Profile Name	default
Clone Name	SP2_Topo

- On the newly cloned ***SP2_Topo*** profile screen, click the **Edit** button (not shown).
- For the, **From, To** and **Request-Line** headers, select ***Overwrite*** in the **Replace Action** column and enter the enterprise SIP domain ***avaya.mts.ca***, in the **Overwrite Value** column of these headers, as shown below. This is the domain provided by MTS.
- Default values were used for all other fields.
- Click **Finish**.



Edit Topology Hiding Profile

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

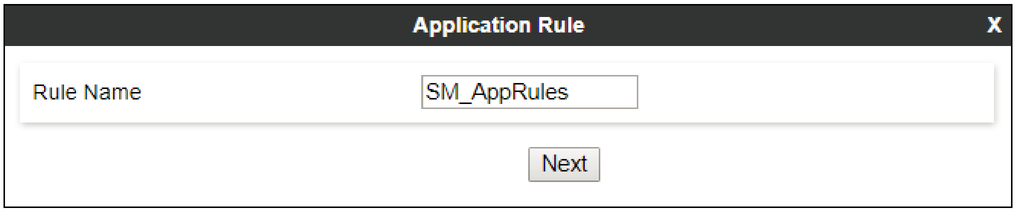
7.11. Domain Policies

Domain Policies allow the configuration of sets of rules designed to control and normalize the behavior of call flows, based upon various criteria of communication sessions originating from or terminating in the enterprise. Domain Policies include rules for Application, Media, Signaling, Security, etc.

7.11.1. Application Rules

Application Rules define which types of SIP-based Unified Communications (UC) applications the UC-Sec security device will protect: voice, video, and/or Instant Messaging (IM). In addition, Application Rules define the maximum number of concurrent voice and video sessions the network will process in order to prevent resource exhaustion. From the menu on the left-hand side, select **Domain Policies → Application Rules**, click on the **Add** button to add a new rule.

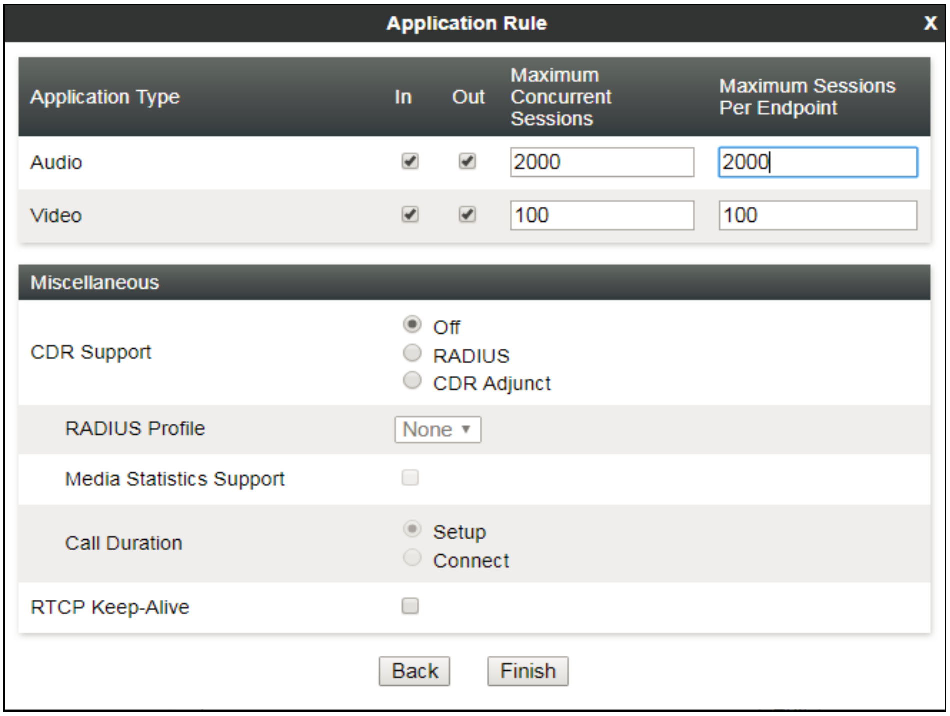
- Under **Rule Name** enter the name of the profile, e.g., ***SM_AppRules***.
- Click **Next**.



Application Rule

Rule Name: SM_AppRules

- Under **Audio** check ***In*** and ***Out*** and set the **Maximum Concurrent Sessions** and **Maximum Sessions Per Endpoint** to recommended values, the values of ***2000*** for Audio and ***100*** for Video were used in the sample configuration.
- Click **Finish**.



Application Rule

Application Type	In	Out	Maximum Concurrent Sessions	Maximum Sessions Per Endpoint
Audio	☑	☑	2000	2000
Video	☑	☑	100	100

Miscellaneous

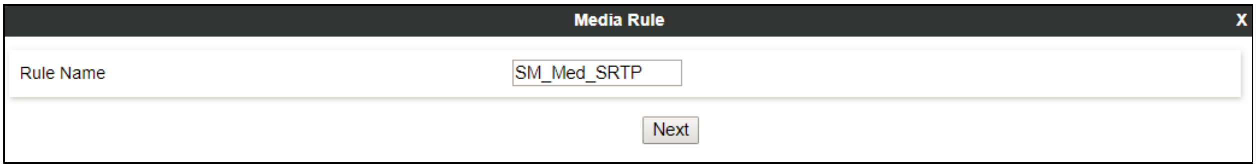
CDR Support	● Off ○ RADIUS ○ CDR Adjunct
RADIUS Profile	None
Media Statistics Support	□
Call Duration	● Setup ○ Connect
RTCP Keep-Alive	□

7.11.2. Media Rules

Media Rules allow one to define RTP media packet parameters such as prioritizing encryption techniques and packet encryption techniques. Together these media-related parameters define a strict profile that is associated with other SIP-specific policies to determine how media packets matching these criteria will be handled by the Avaya SBCE security product. For the compliance test, two media rules (shown below) were used; one toward Session Manager and one toward the Service Provider.

To add a media rule in the Session Manager direction, from the menu on the left-hand side, select **Domain Policies → Media Rules**.

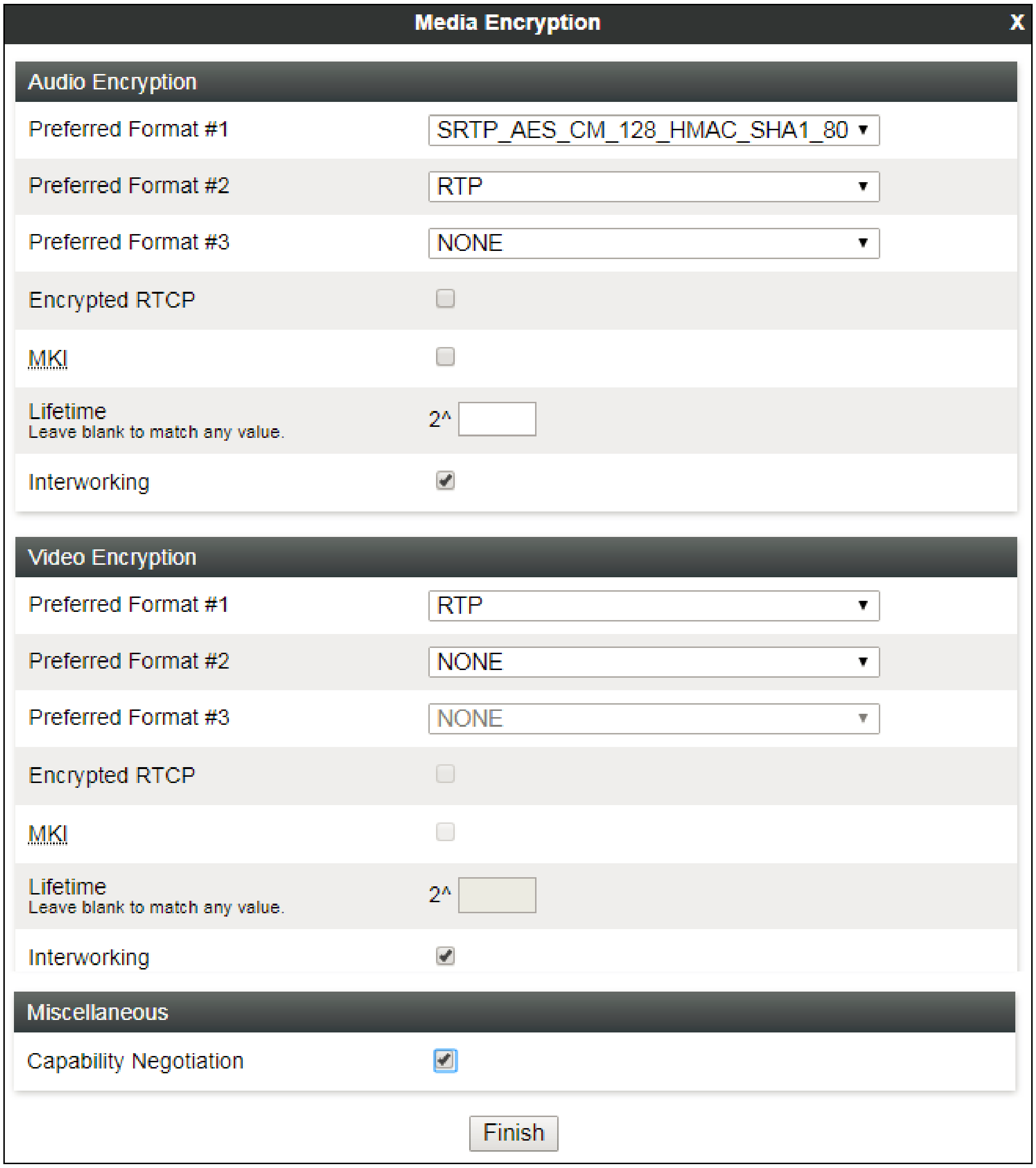
- Click on the **Add** button to add a new media rule (not shown).
- Under **Rule Name** enter ***SM_Med_SRTP***.
- Click **Next**.



Media Rule

Rule Name: SM_Med_SRTP

- Under Audio Encryption, **Preferred Format #1**, select ***SRTP_AES_CM_128_HMAC_SHA1_80***.
- Under Audio Encryption, **Preferred Format #2**, select **RTP**.
- Under Audio Encryption, uncheck ***Encrypted RTCP***.
- Under Audio Encryption, check ***Interworking***.
- Repeat the above steps under Video Encryption but only select RTP.
- Under Miscellaneous verify that ***Capability Negotiation*** is checked.
- Click **Next**.



Media Encryption

Audio Encryption

Preferred Format #1	SRTP_AES_CM_128_HMAC_SHA1_80 ▾
Preferred Format #2	RTP ▾
Preferred Format #3	NONE ▾
Encrypted RTCP	□
MKI	□
Lifetime Leave blank to match any value.	2^
Interworking	☑

Video Encryption

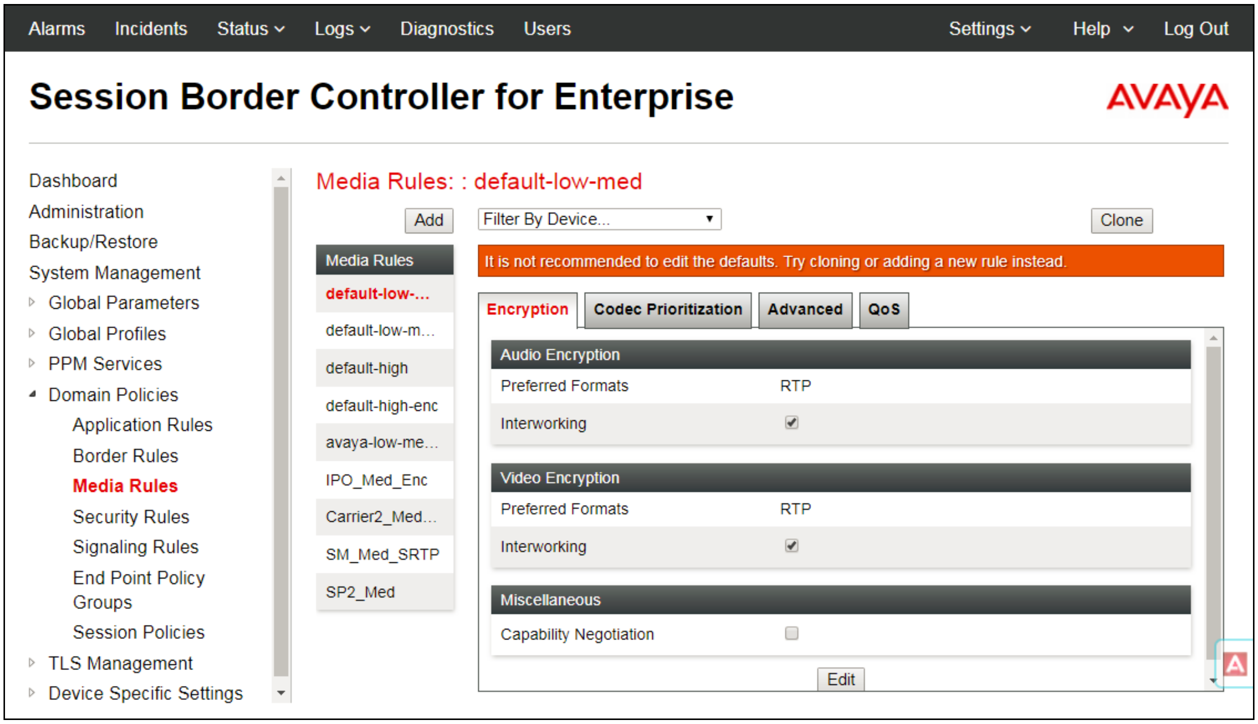
Preferred Format #1	RTP ▾
Preferred Format #2	NONE ▾
Preferred Format #3	NONE ▾
Encrypted RTCP	□
MKI	□
Lifetime Leave blank to match any value.	2^
Interworking	☑

Miscellaneous

Capability Negotiation	☑

- Accept default values in the remaining sections by clicking **Next** (not shown), and then click **Finish** (not shown).

For the compliance test, the **default-low-med** Media Rule was used in the Service Provider direction.



Media Rules: : default-low-med

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

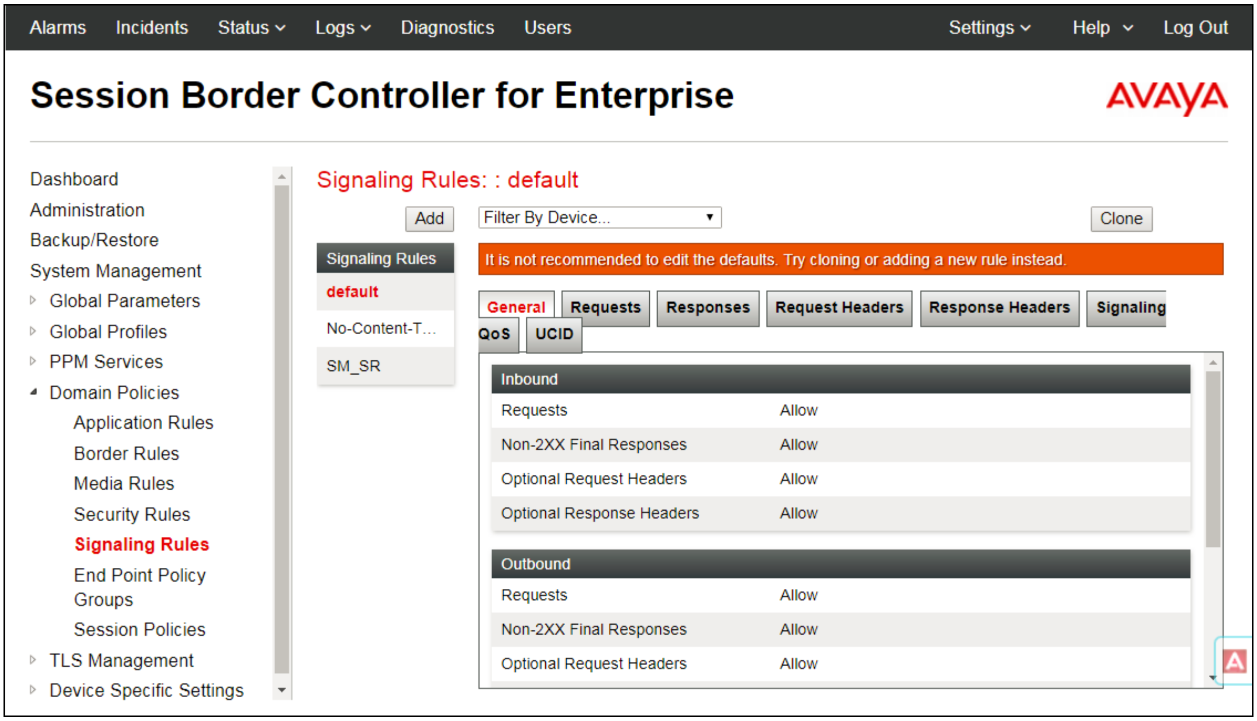
Audio Encryption	
Preferred Formats	RTP
Interworking	☑

Video Encryption	
Preferred Formats	RTP
Interworking	☑

Miscellaneous	
Capability Negotiation	□

7.11.3. Signaling Rules

For the compliance test, the **default** signaling rule was used.



Signaling Rules: : default

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

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

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

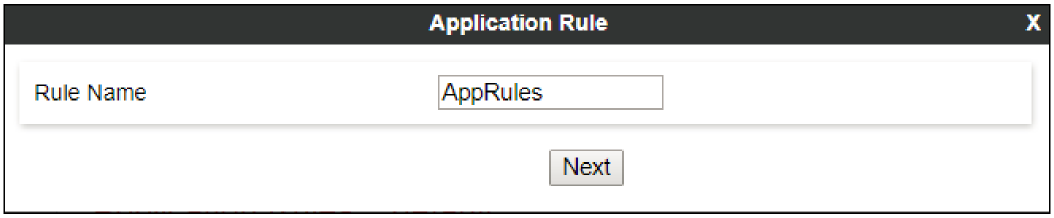
7.12. End Point Policy Groups

End Point Policy Groups associate the different sets of rules under Domain Policies (Media, Signaling, Security, etc.) to be applied to specific SIP messages traversing through the Avaya SBCE. Please note that changes should not be made to any of the default rules used in these End Point Policy Groups.

7.12.1. End Point Policy Group – Enterprise

To create an End Point Policy Group for the enterprise, select **End Point Policy Groups** under the **Domain Policies** menu and select **Add** (not shown).

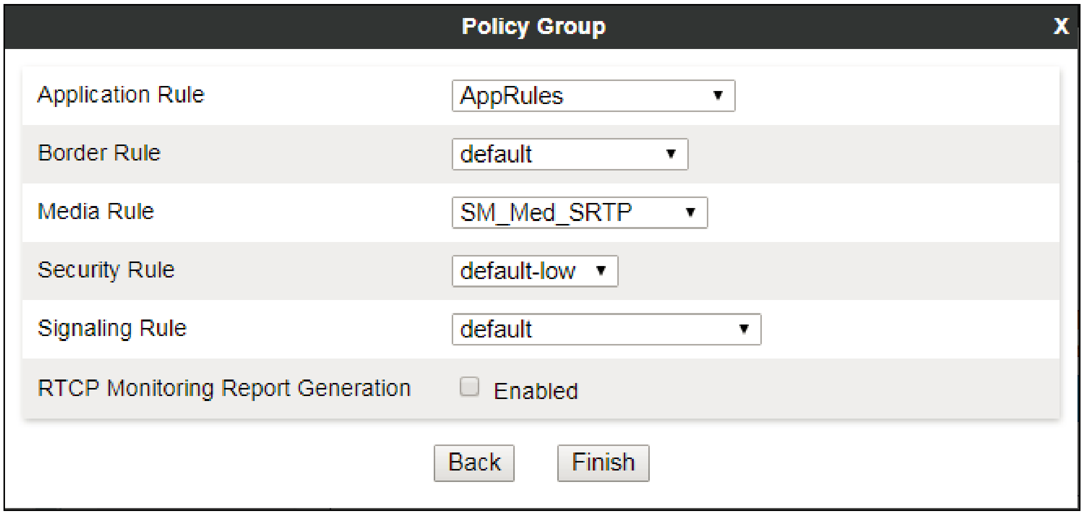
- Enter an appropriate name in the **Group Name** field.
- Click **Next**.



Rule Name	AppRules

Under the **Policy Group** tab enter the following:

- **Application Rule:** ***AppRules*** (**Section 7.11.1**).
- **Border Rule:** ***default***.
- **Media Rule:** ***SM_Med_SRTP*** (**Section 7.11.2**).
- **Security Rule:** ***default-low***.
- **Signaling Rule:** ***default*** (**Section 7.11.3**).
- Click **Finish**.

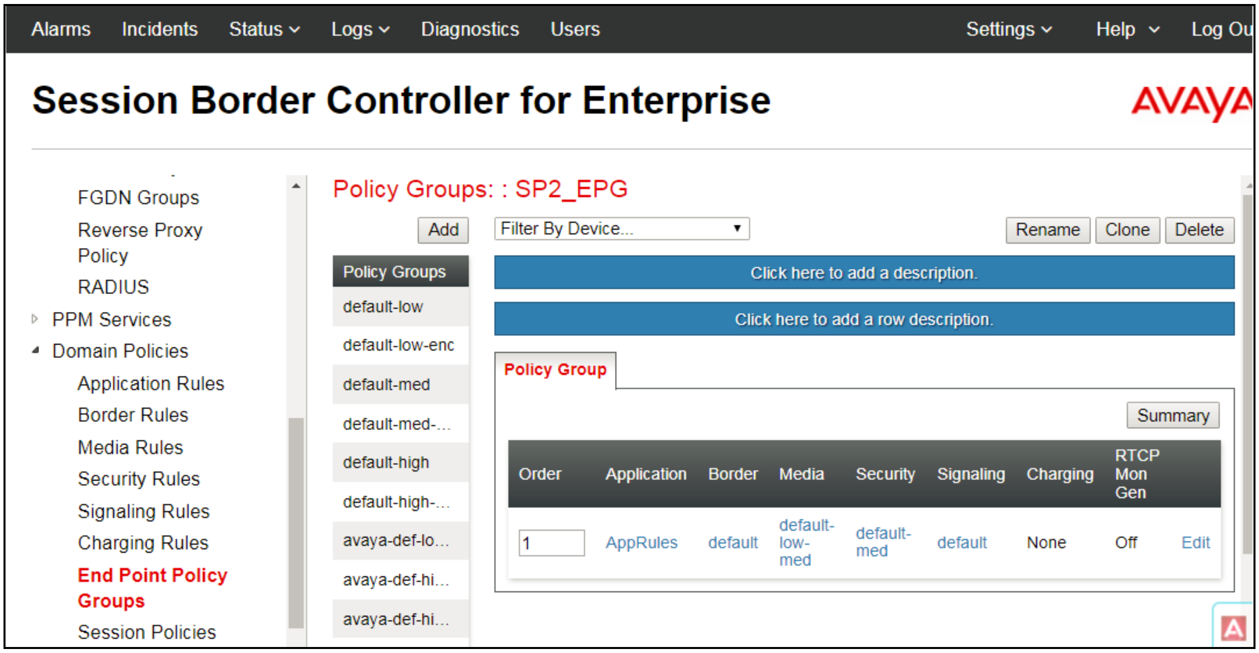


Application Rule	AppRules
Border Rule	default
Media Rule	SM_Med_SRTP
Security Rule	default-low
Signaling Rule	default
RTCP Monitoring Report Generation	□ Enabled

7.12.2. End Point Policy Group – Service Provider

A second End Point Policy Group was created for the service provider, repeating the steps previously described. In the Policy Group tab, all fields used one of the default sets already pre-defined in the configuration, except for the Application Rule, which was set to ***AppRules*** (**Section 7.11.1**).

The screen below shows the End Point Policy Group named ***SP2_EPG*** after the configuration was completed.

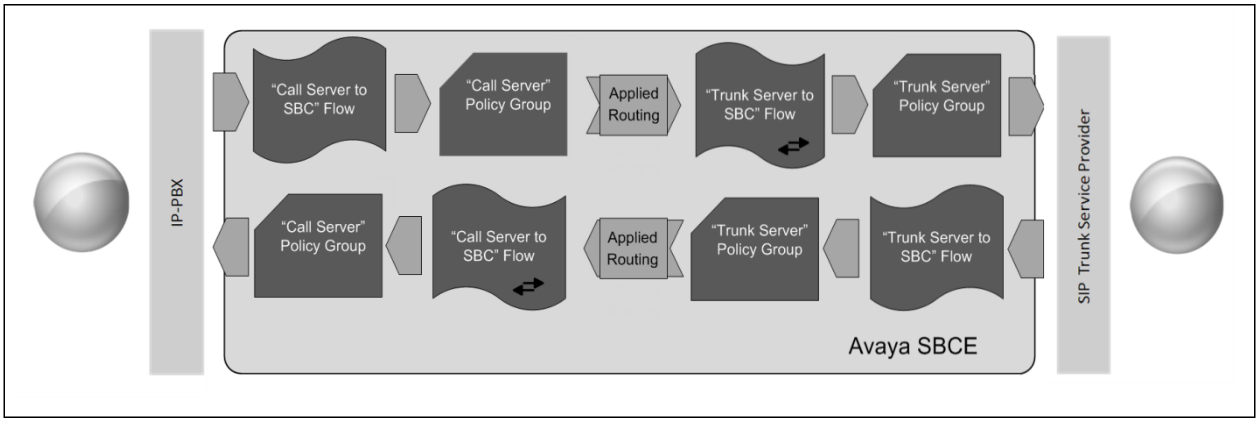


Policy Groups: : SP2_EPG

Order	Application	Border	Media	Security	Signaling	Charging	RTCP Mon Gen	
1	AppRules	default	default-low-med	default-med	default	None	Off	Edit

7.13. End Point Flows

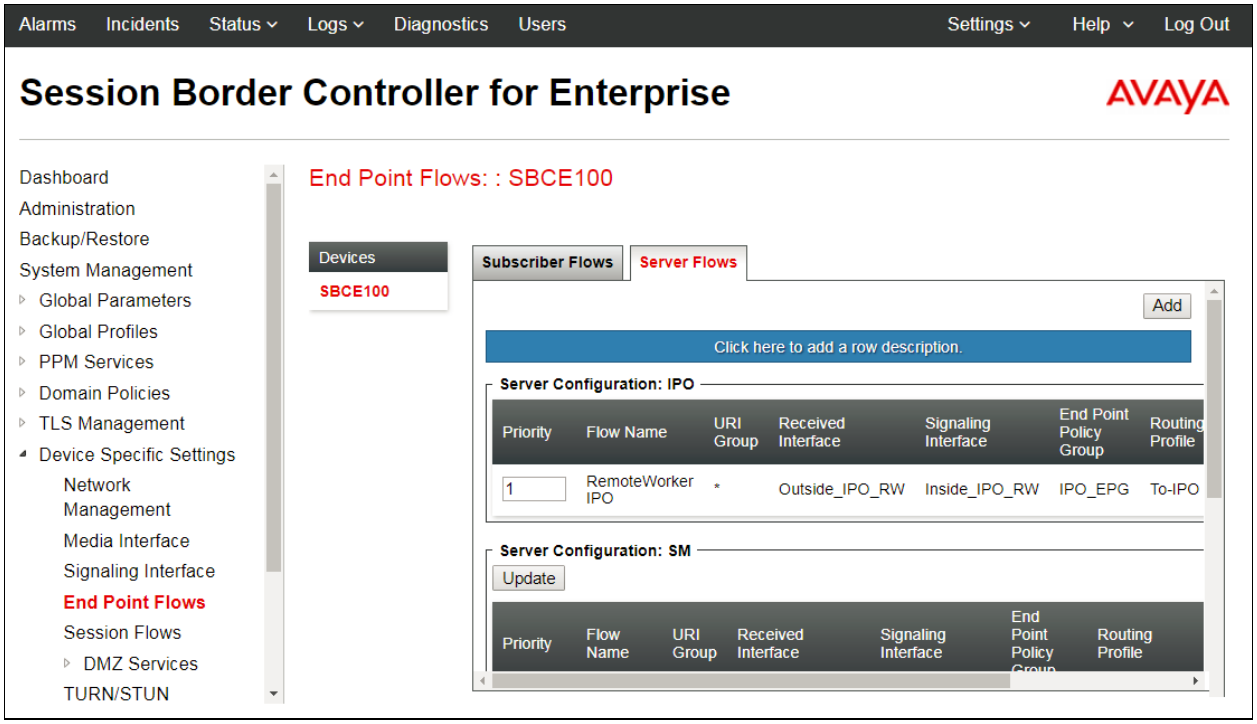
When a packet is received by Avaya SBCE, the content of the packet (IP addresses, URIs, etc.) is used to determine which flow it matches. Once the flow is determined, the flow points to a policy group which contains several rules concerning processing, privileges, authentication, routing, etc. Once routing is applied and the destination endpoint is determined, the policies for this destination endpoint are applied. The context is maintained, so as to be applied to future packets in the same flow. The following screen illustrates the flow through the Avaya SBCE to secure a SIP trunk call.


IP-PBX
"Call Server to SBC" Flow
"Call Server" Policy Group
Applied Routing
"Trunk Server to SBC" Flow
"Trunk Server" Policy Group
"Call Server" Policy Group
"Call Server to SBC" Flow
Applied Routing
"Trunk Server" Policy Group
"Trunk Server to SBC" Flow
Avaya SBCE
SIP Trunk Service Provider

The **End-Point Flows** defines certain parameters that pertain to the signaling and media portions of a call, whether it originates from within the enterprise or outside of the enterprise.

7.13.1. End Point Flow – Enterprise

To create the call flow toward the enterprise, from the left navigation menu, select Device **Specific Settings →End Point Flows**, then select the **Server Flows** tab. Click **Add**.



End Point Flows: : SBCE100

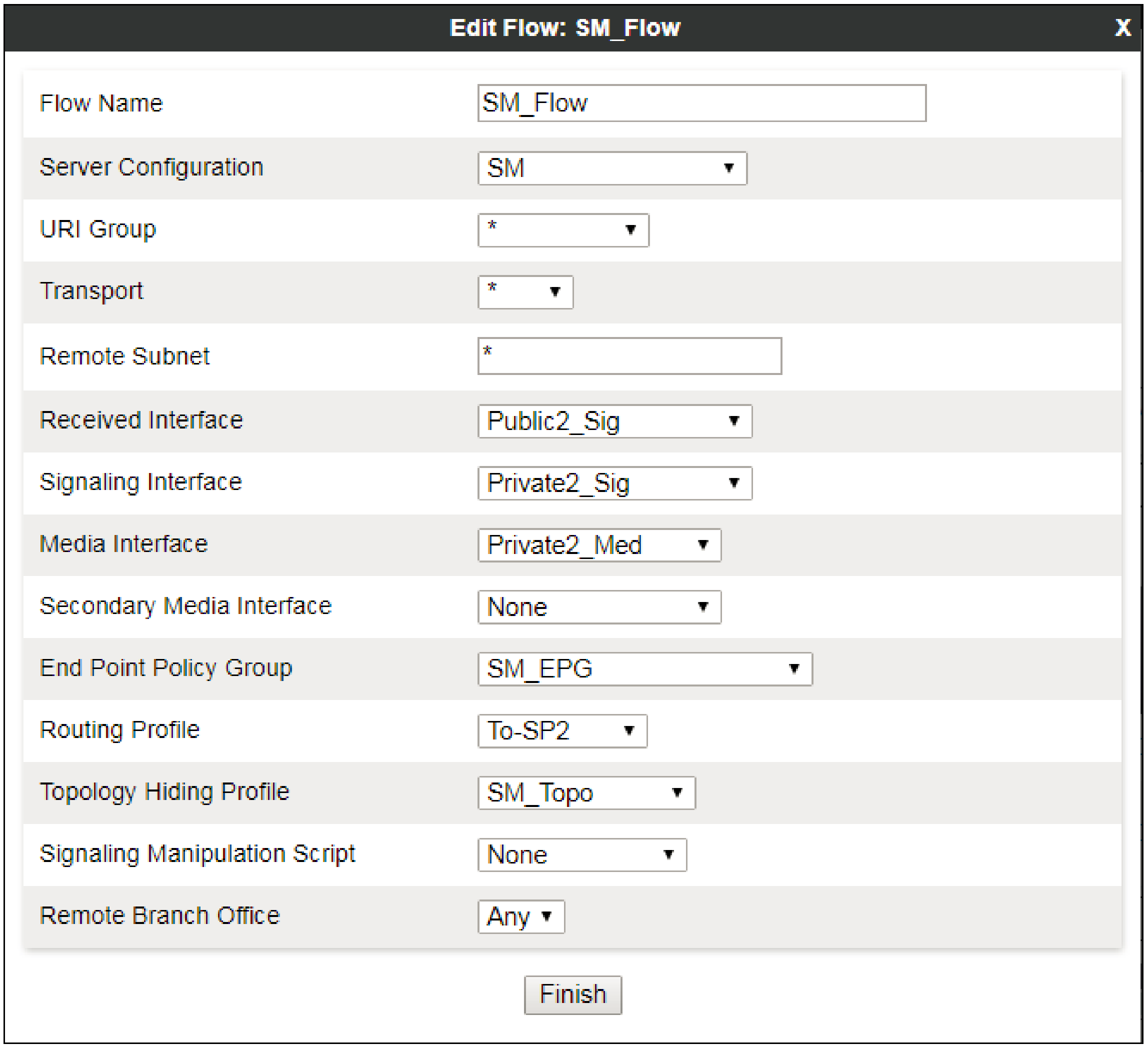
Server Configuration: IPO

Priority	Flow Name	URI Group	Received Interface	Signaling Interface	End Point Policy Group	Routing Profile
1	RemoteWorker IPO	*	Outside_IPO_RW	Inside_IPO_RW	IPO_EPG	To-IPO

Server Configuration: SM

Priority	Flow Name	URI Group	Received Interface	Signaling Interface	End Point Policy Group	Routing Profile

The screen below shows the flow named ***SM_Flow*** created in the sample configuration. The flow uses the interfaces, policies, and profiles defined in previous sections. Note that the **Routing Profile** selection is the profile created for the Service Provider in **Section 7.9.2**, which is the reverse route of the flow. Click **Finish**.

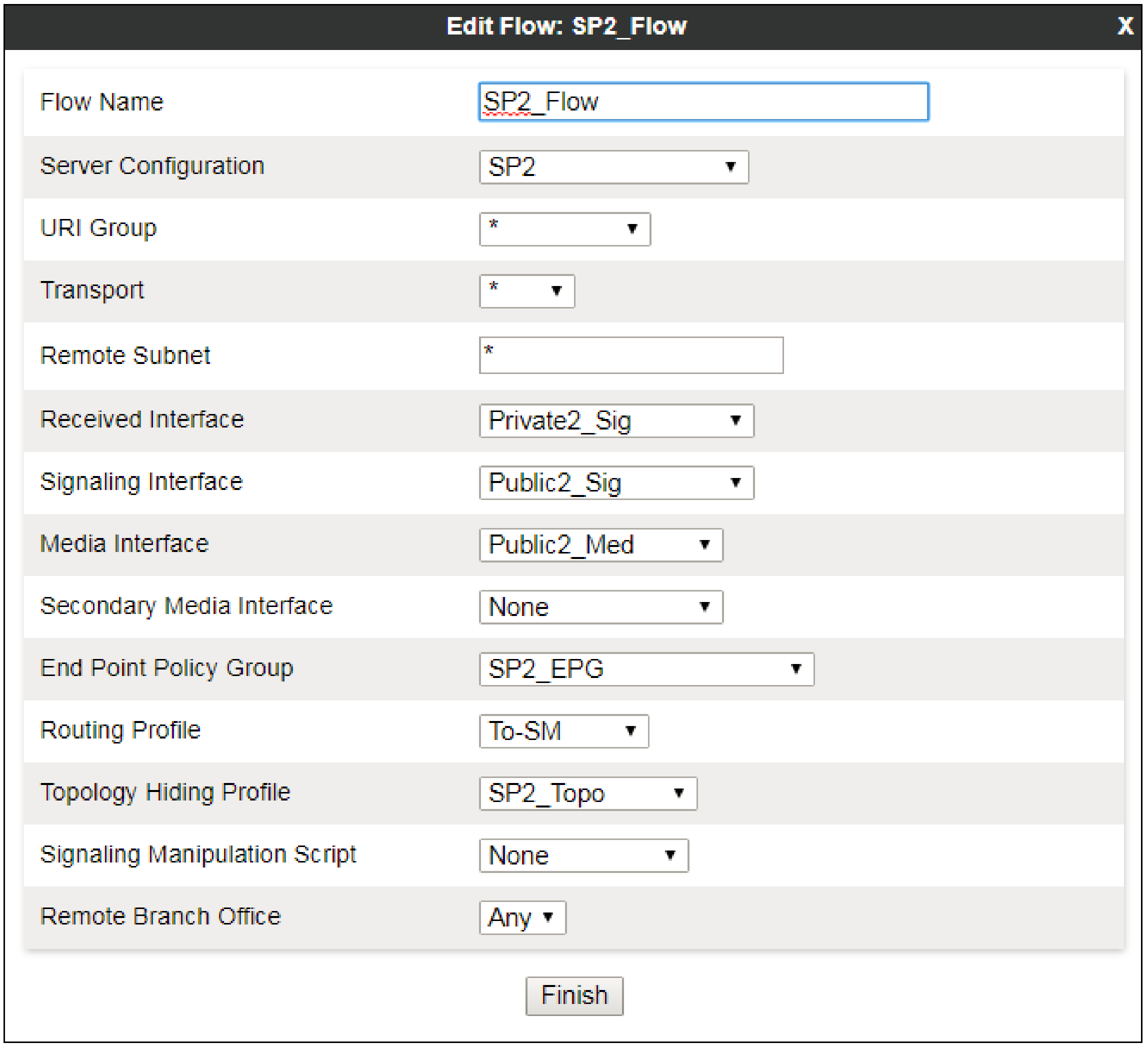


Edit Flow: SM_Flow

Flow Name	SM_Flow
Server Configuration	SM
URI Group	*
Transport	*
Remote Subnet	*
Received Interface	Public2_Sig
Signaling Interface	Private2_Sig
Media Interface	Private2_Med
Secondary Media Interface	None
End Point Policy Group	SM_EPG
Routing Profile	To-SP2
Topology Hiding Profile	SM_Topo
Signaling Manipulation Script	None
Remote Branch Office	Any

7.13.2. End Point Flow – Service Provider

A second Server Flow with the name ***SP2_Flow*** was similarly created in the Service Provider direction. The flow uses the interfaces, policies, and profiles defined in previous sections. Note that the **Routing Profile** selection is the profile created for Session Manager in **Section 7.9.1**, which is the reverse route of the flow. Click **Finish**.



Edit Flow: SP2_Flow

Flow Name	SP2_Flow
Server Configuration	SP2
URI Group	*
Transport	*
Remote Subnet	*
Received Interface	Private2_Sig
Signaling Interface	Public2_Sig
Media Interface	Public2_Med
Secondary Media Interface	None
End Point Policy Group	SP2_EPG
Routing Profile	To-SM
Topology Hiding Profile	SP2_Topo
Signaling Manipulation Script	None
Remote Branch Office	Any

8. Bell MTS SIP Trunking Service Configuration

To use Bell MTS SIP Trunking Service, a customer must request the service from MTS using the established sales processes. The process can be started by contacting MTS via the corporate web site at: https://BellMTS.ca

During the signup process, MTS and the customer will discuss details about the preferred method to be used to connect the customer's enterprise network to MTS's network.

MTS will provide the following information:

- MTS SIP proxy server IP address.
- SIP username and password for authentication and registration.
- DID numbers.
- Supported codecs and order of preference.
- Etc.

9. Verification and Troubleshooting

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 commands that can be used to troubleshoot the solution.

9.1. General Verification Steps

- 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.
- 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.
- Verify that the user on the PSTN can end an active call by hanging up.
- Verify that an endpoint at the enterprise site can end an active call by hanging up.

9.2. Communication Manager Verification

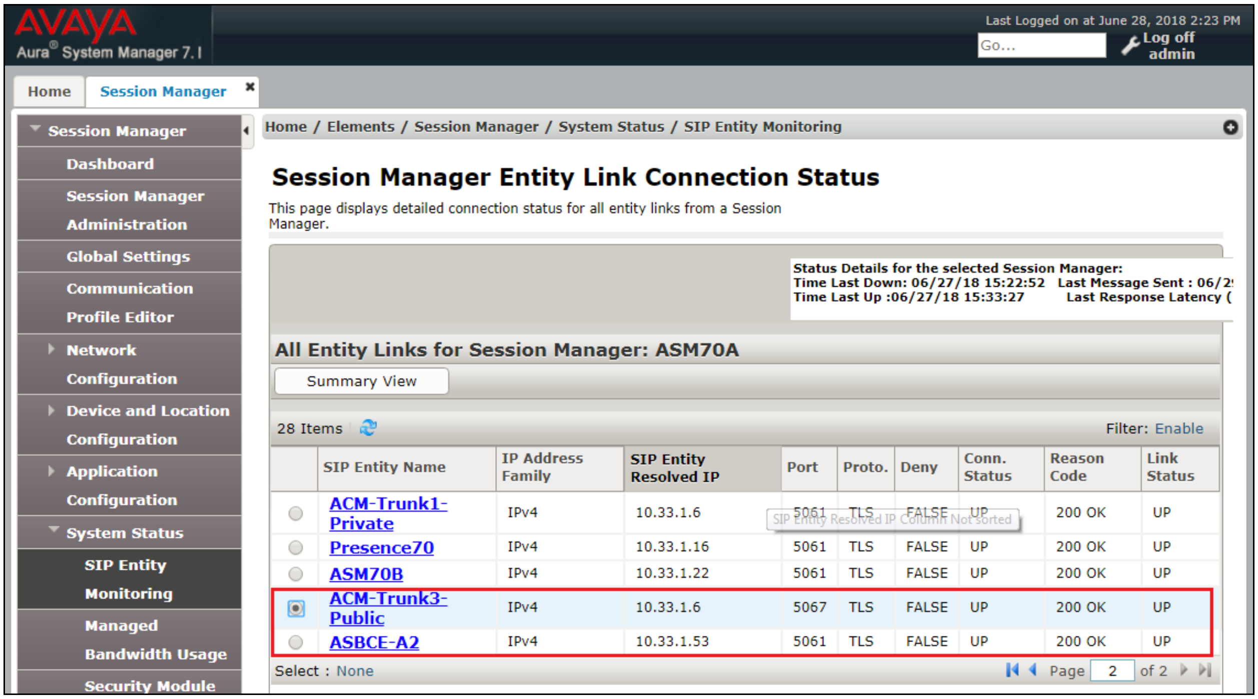
The following commands can be entered in the Communication Manager SAT terminal to verify the SIP trunk functionality:

- **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 signaling-group** <signaling group number>
  Displays signaling group service state.
- **status trunk** <trunk group number>
  Displays trunk group service state.
- **status station** <extension number>
  Displays signaling and media information for an active call on a specific station.

9.3. Session Manager Verification

Log in to System Manager. Under the **Elements** section, navigate to **Session Manager → System Status → SIP Entity Monitoring**. Click the Session Manager instance **ASM70A** (not shown).

Verify that the state of the Session Manager links to Communication Manager and the Avaya SBCE under the **Conn. Status** and **Link Status** columns is ***UP***, like shown on the screen below.


AVAYA
Aura® System Manager 7.1
Last Logged on at June 28, 2018 2:23 PM
Go...
Log off admin
Home
Session Manager
Session Manager
Dashboard
Session Manager Administration
Global Settings
Communication Profile Editor
Network Configuration
Device and Location Configuration
Application Configuration
System Status
SIP Entity Monitoring
Managed Bandwidth Usage
Security Module
Home / Elements / Session Manager / System Status / SIP Entity Monitoring
Summary View
Filter: Enable
SIP Entity Resolved IP Column Not sorted
Select : None
Page 2 of 2

Session Manager Entity Link Connection Status

This page displays detailed connection status for all entity links from a Session Manager.

Status Details for the selected Session Manager:
Time Last Down: 06/27/18 15:22:52 Last Message Sent : 06/2
Time Last Up :06/27/18 15:33:27 Last Response Latency (

All Entity Links for Session Manager: ASM70A

28 Items

	SIP Entity Name	IP Address Family	SIP Entity Resolved IP	Port	Proto.	Deny	Conn. Status	Reason Code	Link Status
○	ACM-Trunk1-Private	IPv4	10.33.1.6	5061	TLS	FALSE	UP	200 OK	UP
○	Presence70	IPv4	10.33.1.16	5061	TLS	FALSE	UP	200 OK	UP
○	ASM70B	IPv4	10.33.1.22	5061	TLS	FALSE	UP	200 OK	UP
●	ACM-Trunk3-Public	IPv4	10.33.1.6	5067	TLS	FALSE	UP	200 OK	UP
○	ASBCE-A2	IPv4	10.33.1.53	5061	TLS	FALSE	UP	200 OK	UP

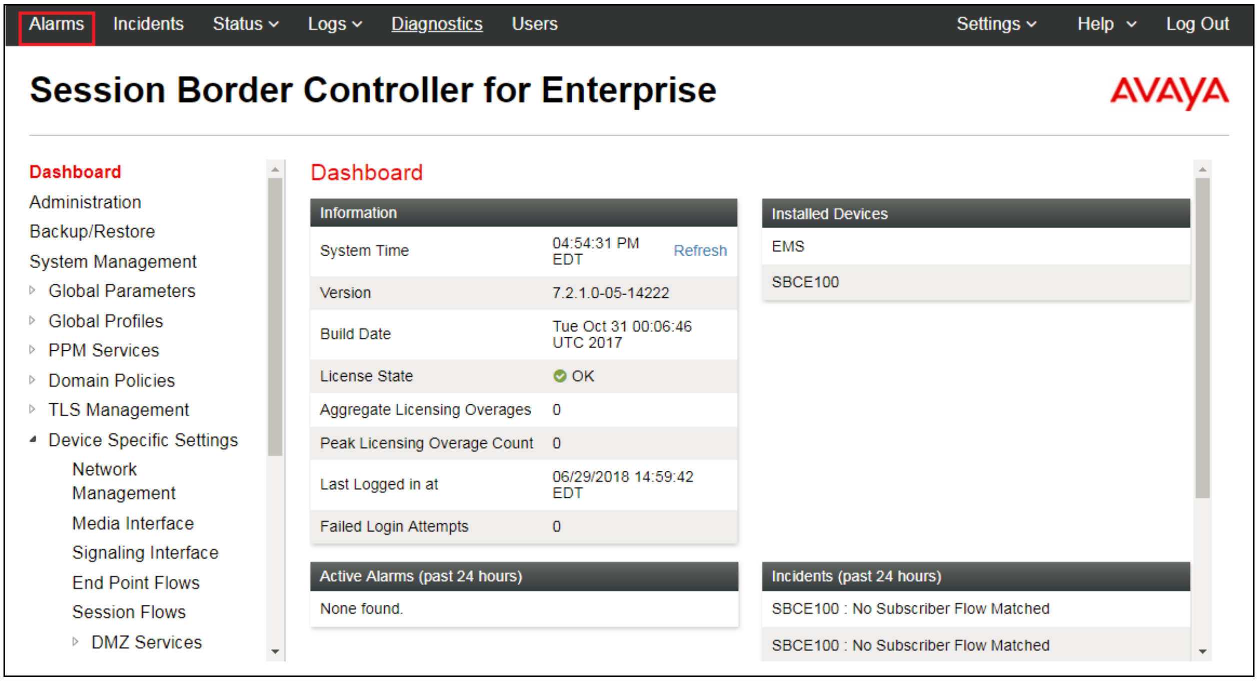
Other Session Manager useful verification and troubleshooting tools include:

- **traceSM** – Session Manager command line tool for traffic analysis. Login to the Session Manager command line management interface to run this command.
- **Call Routing Test** – The Call Routing Test verifies the routing for a particular source and destination. To run the routing test, from the System Manager Home screen navigate to **Elements → Session Manager →System Tools → Call Routing Test**. Enter the requested data to run the test.

9.4. Avaya SBCE Verification

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 screen provides information about the health of the SBC.



Session Border Controller for Enterprise

Dashboard

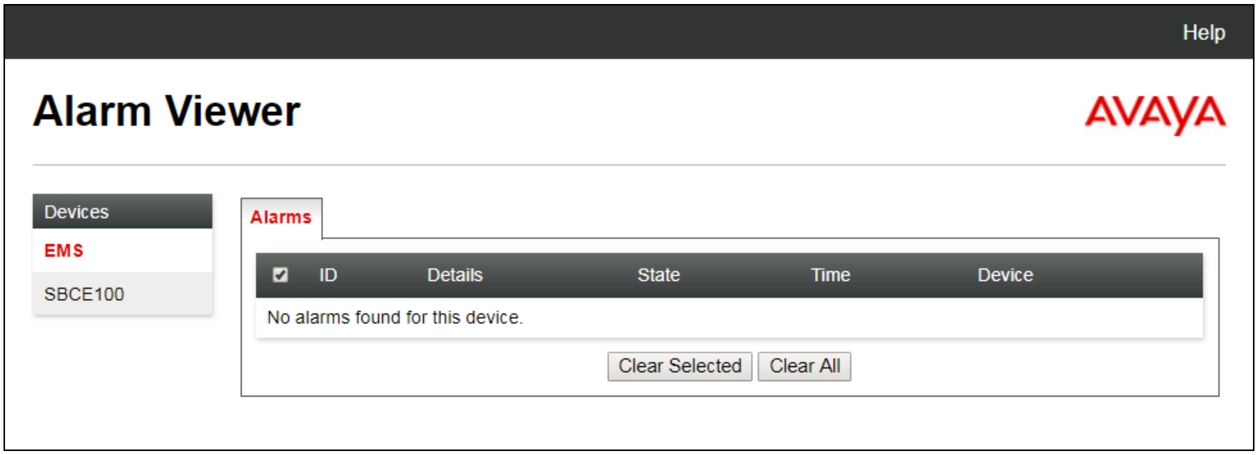
Information	
System Time	04:54:31 PM EDT
Version	7.2.1.0-05-14222
Build Date	Tue Oct 31 00:06:46 UTC 2017
License State	✓ OK
Aggregate Licensing Overages	0
Peak Licensing Overage Count	0
Last Logged in at	06/29/2018 14:59:42 EDT
Failed Login Attempts	0

Installed Devices
EMS
SBCE100

Active Alarms (past 24 hours)
None found.

Incidents (past 24 hours)
SBCE100 : No Subscriber Flow Matched
SBCE100 : No Subscriber Flow Matched

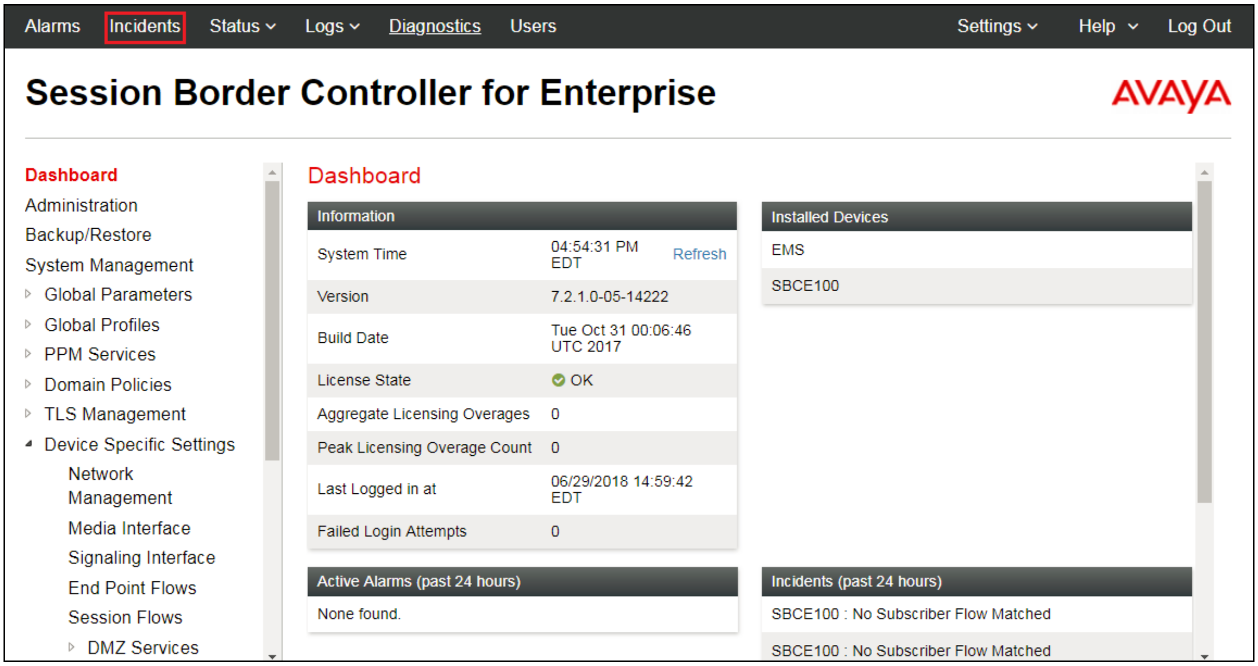
The following screen shows the **Alarm Viewer** page.



Alarm Viewer

☑	ID	Details	State	Time	Device
No alarms found for this device.					

Incidents: Providing detailed reports of anomalies, errors, policies violations, etc.



Session Border Controller for Enterprise

Dashboard

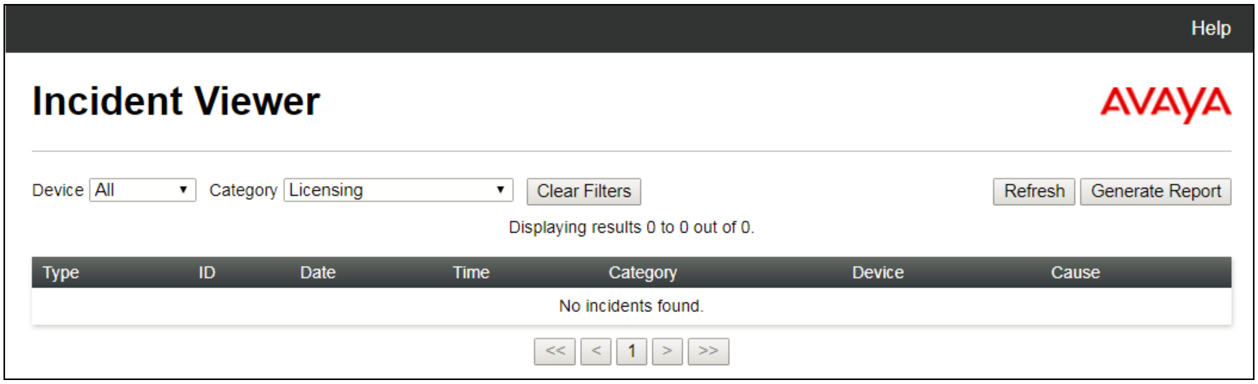
Information	
System Time	04:54:31 PM EDT
Version	7.2.1.0-05-14222
Build Date	Tue Oct 31 00:06:46 UTC 2017
License State	✓ OK
Aggregate Licensing Overages	0
Peak Licensing Overage Count	0
Last Logged in at	06/29/2018 14:59:42 EDT
Failed Login Attempts	0

Installed Devices
EMS
SBCE100

Active Alarms (past 24 hours)
None found.

Incidents (past 24 hours)
SBCE100 : No Subscriber Flow Matched
SBCE100 : No Subscriber Flow Matched

The following screen shows the Incident Viewer page.



Incident Viewer

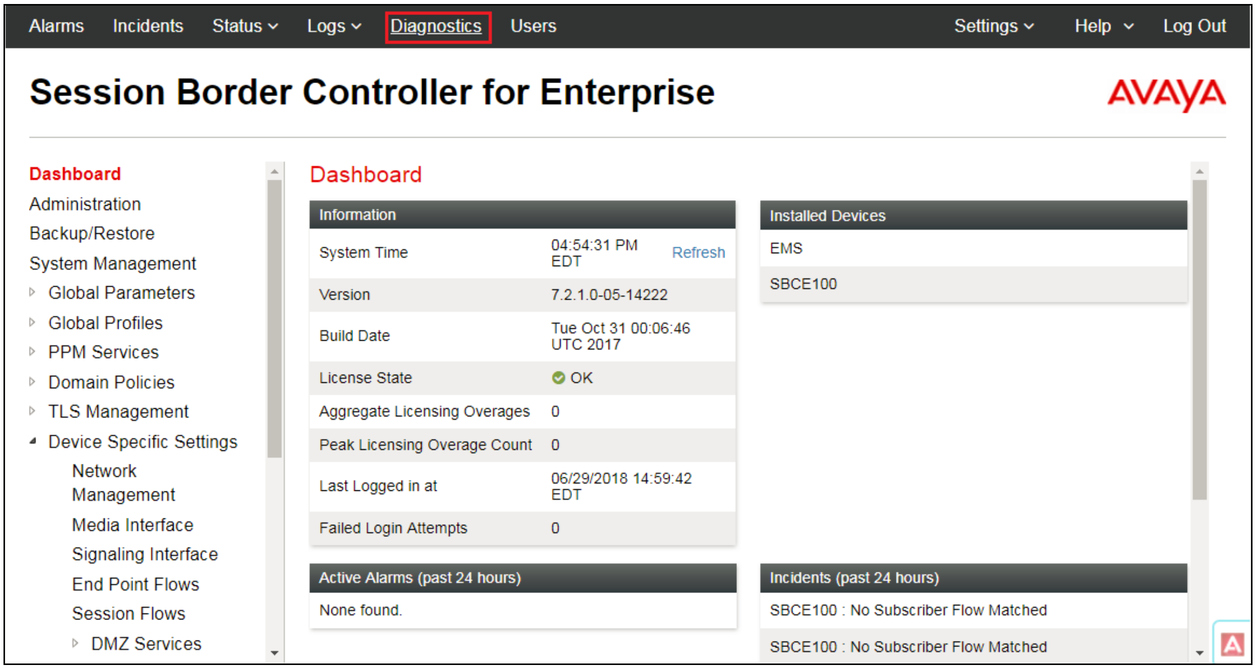
Device: All

Category: Licensing

Displaying results 0 to 0 out of 0.

Type	ID	Date	Time	Category	Device	Cause
No incidents found.						

Diagnostics: This screen provides a variety of tools to test and troubleshoot the Avaya SBCE network connectivity.



Session Border Controller for Enterprise

Dashboard

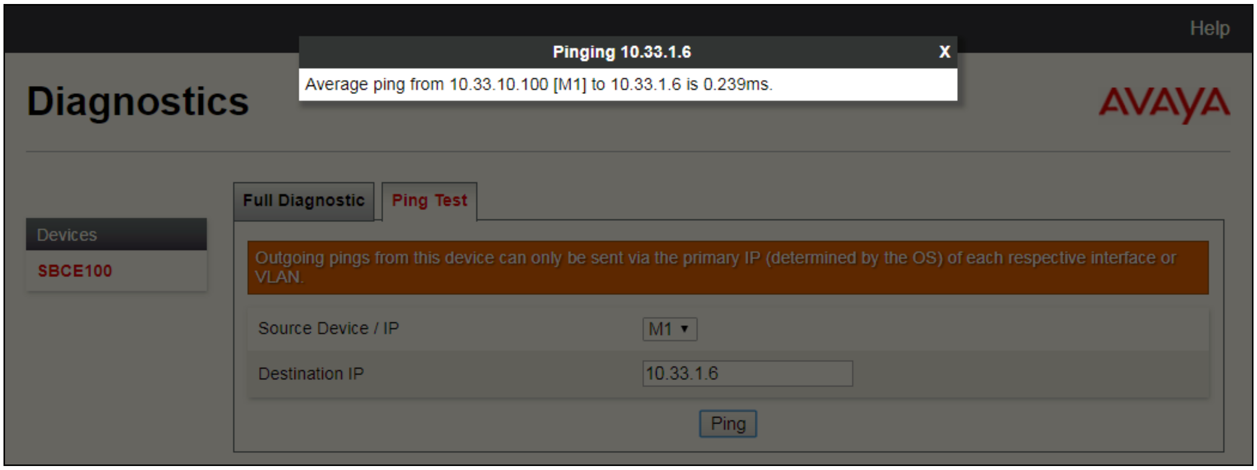
Information	
System Time	04:54:31 PM EDT
Version	7.2.1.0-05-14222
Build Date	Tue Oct 31 00:06:46 UTC 2017
License State	✓ OK
Aggregate Licensing Overages	0
Peak Licensing Overage Count	0
Last Logged in at	06/29/2018 14:59:42 EDT
Failed Login Attempts	0

Installed Devices
EMS
SBCE100

Active Alarms (past 24 hours)
None found.

Incidents (past 24 hours)
SBCE100 : No Subscriber Flow Matched
SBCE100 : No Subscriber Flow Matched

The following screen shows the Diagnostics page with the results of a ping test.



Diagnostics

Pinging 10.33.1.6

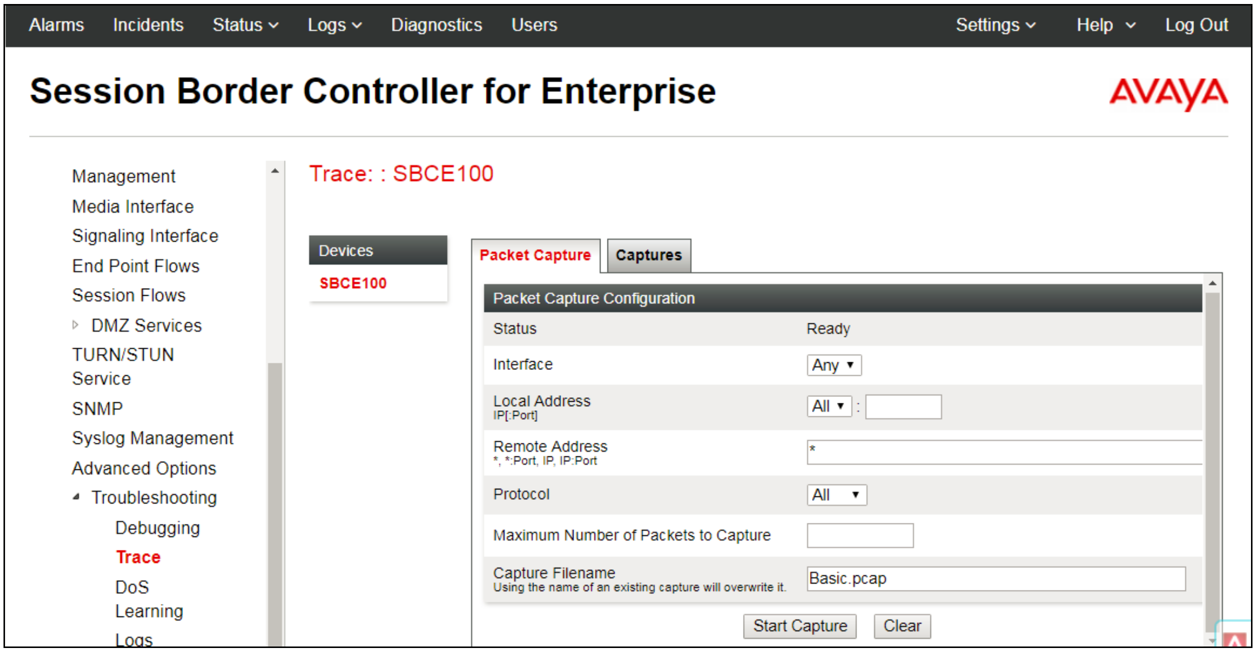
Average ping from 10.33.10.100 [M1] to 10.33.1.6 is 0.239ms.

Outgoing pings from this device can only be sent via the primary IP (determined by the OS) of each respective interface or VLAN.

Source Device / IP: M1

Destination IP: 10.33.1.6

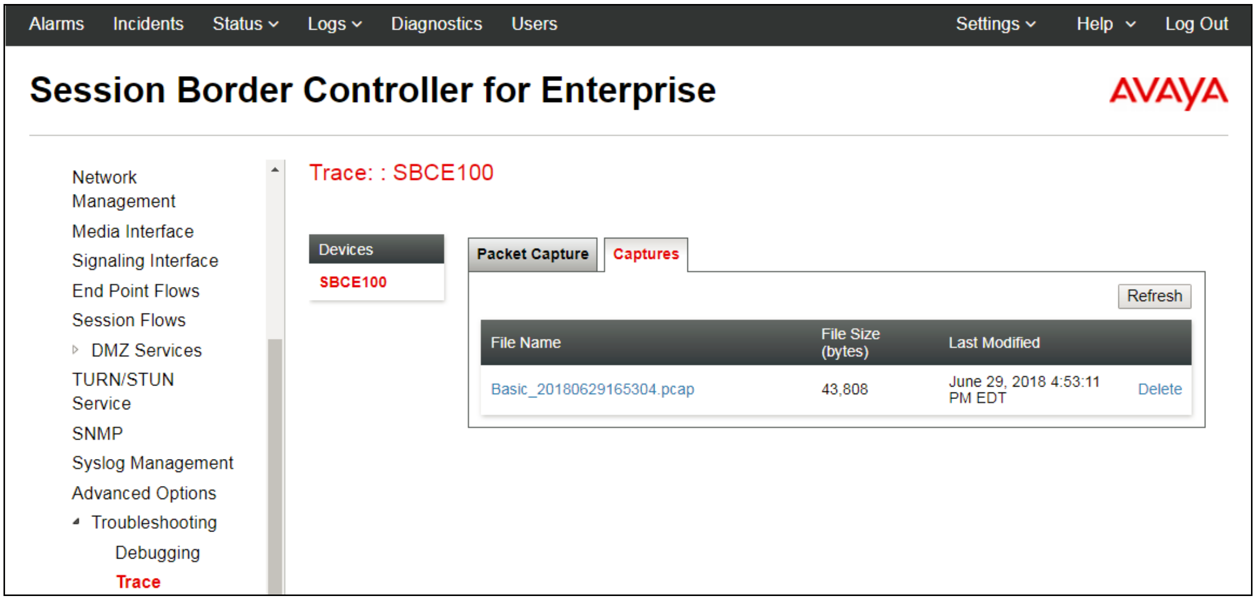
Additionally, the Avaya SBCE contains an internal packet capture tool that allows the capture of packets on any of its interfaces, saving them as *pcap* files. Navigate to **Device Specific Settings → Troubleshooting → Trace**. Select the **Packet Capture** tab, set the desired configuration for the trace and click **Start Capture**.



Packet Capture Configuration

Status	Ready
Interface	Any ▾
Local Address IP[:Port]	All ▾ :
Remote Address *, *:Port, IP, IP:Port	*
Protocol	All ▾
Maximum Number of Packets to Capture	
Capture Filename Using the name of an existing capture will overwrite it.	Basic.pcap

Once the capture is stopped, click the **Captures** tab and select the proper *pcap* file. Note that the date and time is appended to the filename specified previously. The file can now be saved to the local PC, where it can be opened with an application such as Wireshark.



File Name	File Size (bytes)	Last Modified	
Basic_20180629165304.pcap	43,808	June 29, 2018 4:53:11 PM EDT	Delete

10. Conclusion

These Application Notes describe the procedures required to configure Avaya Aura® Communication Manager 7.1, Avaya Aura® Session Manager 7.1 and Avaya Session Border Controller for Enterprise 7.2, to connect to the Bell MTS SIP Trunking service, as shown in **Figure 1**.

Interoperability testing of the sample configuration was completed with successful results for all test cases with the observations/limitations described in **Sections 2.1** and **2.2**.

11. References

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

[1] *Deploying Avaya Aura® Communication Manager*, Release 7.1.3, Issue 4, June 2018.

[2] *Administering Avaya Aura® Communication Manager*, Release 7.1.3, Issue 4, June 2018.

[3] *Administering Avaya Aura® System Manager* for Release 7.1.3, Issue 15, June 2018.

[4] *Deploying Avaya Aura® System Manager*, Release 7.1.3, Issue 8, May 2018.

[5] *Deploying Avaya Aura® Session Manager*, Release 7.1.3, Issue 5, May 2018.

[6] *Administering Avaya Aura® Session Manager*, Release 7.1.2, Issue 5, July 2018.

[7] *Deploying Avaya Session Border Controller for Enterprise*, Release 7.2.1, Issue 4, November 2017.

[8] *Administering Avaya Session Border Controller for Enterprise*, Release 7.2.1, Issue 4, November 2017.

[9] *Configuring Remote Workers with Avaya Session Border Controller for Enterprise Rel. 7.0, Avaya Aura® Communication Manager Rel. 7.0 and Avaya Aura® Session Managers Rel. 7.0 - Issue 1.0.*

[10] *Deploying and Updating Avaya Aura® Media Server Appliance*, Release 7.8, Issue 3, August 2017.

[11] *Implementing and Administering Avaya Aura® Media Server*. Release 7.8, Issue 5, October 2017.

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

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

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.