Avaya Solution & Interoperability Test Lab

Application Notes for Configuring Bell Canada SIP Trunking with Avaya Aura® Communication Manager Server Release 6.3, Avaya Aura® Session Manager Release 6.3, and Avaya Session Border Controller for Enterprise Release 6.2 – Issue 1.0

Abstract

These Application Notes describe the steps to configure Session Initiation Protocol (SIP) Trunking between Bell Canada SIP Trunking service and an Avaya SIP-enabled enterprise solution. The Avaya solution consists of Avaya Aura® Communication Manager Server 6.3, Avaya Aura® Session Manager 6.3, Avaya Session Border Controller For Enterprise 6.2 and various Avaya endpoints. This documented solution does not extend to configurations without Avaya Aura® Session Manager or Avaya Session Border Controller For Enterprise.

Bell Canada SIP Trunking service provides PSTN access via a SIP Trunk between the enterprise and Bell Canada networks as an alternative to legacy analog or ISDN/PRI trunks. This approach generally results in lower cost for the enterprise.

Bell Canada is a member of the Avaya DevConnect Service Provider Program. Information in these Application Notes has been obtained through DevConnect compliance testing and additional technical discussions. Testing was conducted via the DevConnect Program at the Avaya Solution and Interoperability Test Lab.

Table of Contents

1. Introduction....4
2. Test Scope and Results....5
2.1. Interoperability Compliance Testing....5
2.2. Test Results....6
2.3. Support....7
3. Reference Configuration....8
4. Equipment and Software Validated....11
5. Configure Avaya Aura® Communication Manager....12
5.1. Licensing and Capacity....12
5.2. System Features....13
5.3. IP Node Names....13
5.4. Codecs....14
5.5. IP Network Region....14
5.6. Signaling Group....16
5.7. Trunk Group....18
5.8. Calling Party Information....21
5.9. Outbound Routing....22
5.10. Vector Directory Numbers (VDN)....23
5.10.1. Pre-Answer Redirection to a PSTN Destination....24
5.10.2. Post-Answer Redirection to a PSTN Destination....25
5.11. Incoming Call Handling....25
5.12. Saving Communication Manager Configuration Changes....25
6. Configure Avaya Aura® Session Manager....26
6.1. System Manager Login and Navigation....27
6.2. Specify SIP Domain....28
6.3. Add Location....29
6.4. Add Adaptation Module....30
6.5. Add SIP Entities....31
6.6. Add Entity Links....34
6.7. Add Routing Policies....35
6.8. Add Dial Patterns....37
6.9. Add/View Session Manager....39
7. Configure Avaya Session Border Controller for Enterprise....40
7.1. Log into Avaya Session Border Controller for Enterprise....42
7.2. Global Profiles....44
7.2.1. Uniform Resource Identifier (URI) Groups....44
7.2.2. Routing Profiles....46
7.2.3. Topology Hiding....48
7.2.4. Server Interworking....50
7.2.5. Signaling Manipulation....56
7.2.6. Server Configuration....58
7.3. Domain Policies....62
7.3.1. Application Rules....62
7.3.2. Media Rules....64
7.3.3. Signaling Rules....67

7.3.4. Endpoint Policy Groups 70
7.3.5. Session Policy 71
7.4. Device Specific Settings 74
7.4.1. Network Management 74
7.4.2. Media Interface 75
7.4.3. Signaling Interface 76
7.4.4. End Point Flows - Server Flow 76
7.4.5. Session Flow 79
8. Bell Canada SIP Trunking Configuration 81
9. Verification and Troubleshooting 82
9.1. Verification Steps 82
9.2. Protocol Traces 82
9.3. Troubleshooting: 82
9.3.1. Avaya SBCE: 82
9.3.2. Communication Manager 87
9.3.3. Session Manager 87
10. Conclusion 88
11. References 89

1. Introduction

These Application Notes describe steps to configure Session Initiation Protocol (SIP) Trunking between Bell Canada SIP Trunking service and an Avaya SIP-enabled enterprise solution. The Avaya solution consists of Avaya Aura® Communication Manager (Communication Manager) 6.3, Avaya Aura® Session Manager (Session Manager) 6.3, Avaya SBC for Enterprise (Avaya SBCE) 6.2 and various Avaya endpoints. This documented solution does not extend to configurations without Session Manager or Avaya SBCE.

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

Bell Canada applies Digest Authentication for outgoing calls from the enterprise. It uses challenge-response authentication with “401 Unauthorized” response to each outgoing initial INVITE to Bell Canada. The subsequent INVITE from the enterprise provides the “Authorization” header with a configured user name and password. This credential is provided by Bell Canada and configured on Avaya SBCE. This call authentication scheme as specified in RFC 3261 provides authentication for SIP signaling.

2. Test Scope and Results

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

2.1. Interoperability Compliance Testing

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

- Incoming PSTN calls to various phone types including SIP, H.323, digital, and analog telephones at the enterprise. All incoming calls from PSTN are routed to the enterprise across the SIP Trunk from service provider.
- Outgoing PSTN calls from various phone types including SIP, H.323, digital, and analog telephones at the enterprise. All outgoing calls to PSTN are routed from the enterprise across the SIP Trunk to service provider.
- Incoming and outgoing PSTN calls to/ from Avaya one-X® Communicator soft phone. Both Computer Mode (where Avaya one-X® Communicator is used for call control as well as audio path) and Telecommuter Mode (where Avaya one-X® Communicator is used for call control and a separate telephone is used for audio path) are tested. Both SIP and H.323 protocols were tested.
- Incoming and outgoing PSTN calls to/ from Remote Worker which is an Avaya 96X1 IP phone that remotely registers over public internet to Session Manager via Avaya SBCE as Communication Manager SIP station.
- Dialing plans including local, long distance, international, outgoing toll-free, operator assisted, local directory assistance (411) calls, etc.
- Calling Party Name presentation and Calling Party Name restriction.
- Proper codec negotiation with G.711MU codec.
- Proper media transmission using G.711MU codec.
- Proper early media transmission using G.711MU codec.
- Incoming and outgoing fax over IP using G.711MU codec.
- DTMF tone transmission as out-of-band RTP events as per RFC 2833.
- Voicemail navigation for incoming and outgoing calls.
- User features such as hold and resume, transfer, forward and conference.
- Off-net call transfer using subsequent INVITE method.
- Off-net call tandem of incoming Vector Directory Number (VDN) calls using subsequent INVITE method.
- Off-net call forward using Diversion method.
- EC500 mobility (extension to cellular) using Diversion method.
- Routing incoming vector calls to call center agent queues.

- Response to OPTIONS heartbeat.
- Response to incomplete call attempts and trunk errors.
- Session Timers implementation.

Items that are not supported by Bell Canada in the test environment, or not tested as part of the compliance testing, are listed below:

- Inbound toll-free and outgoing emergency calls (E911) are supported but were not tested as part of the compliance testing because Bell Canada has not provided the necessary configuration.
- G.729 codec is not supported.
- Fax over IP with T.38 codec is not supported.
- Off-net call transfer using REFER method is not supported.
- Incoming call redirection on VDN before answer using “302 Moved Temporarily” method is not supported.
- Incoming call redirection after answer of incoming VDN calls using REFER method is not supported.
- Off-net call forward using History-Info method is not supported.

2.2. Test Results

Interoperability testing of Bell Canada SIP Trunking Service with the Avaya SIP-enabled enterprise solution was successfully completed with exception of the observations/limitations described below.

1. **Calling Party Number of incoming calls contains a "+" character that needs to be deleted**. Incoming calls from Bell Canada to the enterprise contains a "+" followed by 11-digit in the “From” header for Calling Party Number. EC500 mobility call feature does not work since EC500 mobile number configured on Communication Manager (in **off-pbx-telephone station-mapping** form) is not allowed to contain non-digit characters like “+” to match the number in the incoming “From” header. The workaround is to have Avaya SBCE normalize Calling Party Number in the “From” header to remove the plus sign then incoming calls work properly. For the detailed configuration, please refer to **Section Error! Reference source not found.**.

2. **Fax over IP using G.711MU codec is successful**. For fax over IP, a service provider is recommended to support T.38 in order to work properly with Communication Manager, because it does not support fax call using G.711MU codec. However, when **ip-codec-set** is set with “fax-off” as described in **Section Error! Reference source not found.**, Communication Manager handles the G.711 fax call as best effort, thus there is no guarantee of success. The fax call is handled like a regular voice call using G.711 codec. In the compliance testing, incoming and outgoing fax calls appeared to work with G.711MU codec. The fax document was transmitted successfully with acceptable quality.

3. **Communication Manager off-net redirects (by transferring or forwarding) an incoming or outgoing call back to PSTN, Calling Party Number is not updated**.

Before completing the off-net redirection, Communication Manager sends UPDATE to Bell Canada on both call legs with the “Contact” and “P-Asserted-Identity” headers containing Calling Party Number of true connected PTSN parties. However, Calling Party Number was not updated, both PSTN parties still display Calling Party Name of Communication Manager station. It depends on Bell Canada and the intermediate service providers that may route the call from Bell Canada to PSTN parties to support Calling Party Display update. This issue has low user impact, it is listed here simply as an observation.

2.3. Support

For technical support on Avaya products described in these Application Notes, visit http://support.avaya.com.

For technical support on Bell Canada SIP Trunking, contact Bell Canada at http://www.bell.ca/enterprise/EntPrd_SIP_Trunking.page.

3. Reference Configuration

Figure 1 illustrates a sample Avaya SIP-enabled enterprise solution connected to Bell Canada SIP Trunking Service through the public internet.

For confidentiality and privacy purposes, actual public IP address and PSTN routable phone number used in the compliance testing have been replaced with fictitious parameters throughout the Application Notes.

The Avaya components used to create the simulated customer site include:

- Avaya S8800 Server running Communication Manager
- Avaya G450 Media Gateway
- Avaya S8800 Server running Session Manager
- Avaya S8800 Server running System Manager
- Avaya S8800 Servers running Messaging
- Avaya Session Border Controller for Enterprise
- Avaya 9600-Series IP Telephones (H.323 and SIP)
- Avaya one-X® Communicator soft phones (H.323 and SIP)
- Avaya digital and analog telephones

Located at the edge of the enterprise is the Avaya SBCE. It has a public side that connects to the external network and a private side that connects to enterprise network. All SIP and RTP traffic entering or leaving the enterprise flows through Avaya SBCE. In this way, Avaya SBCE can protect the enterprise against any SIP-based attacks. Avaya SBCE provides network address translation at both the IP and SIP layers. Transport protocol between Avaya SBCE and Bell Canada across the public network is UDP; the same transport protocol was used for the connection between Avaya SBCE and Session Manager across the enterprise network.

In the compliance testing, Bell Canada provided the service provider public SIP domain as **sipxxxxxxxx.bell.ca** and enterprise public SIP domains as **cust6xxxx.xxxx.bell.ca**. These public SIP domains will be used for public SIP traffic between Avaya SBCE and Bell Canada.

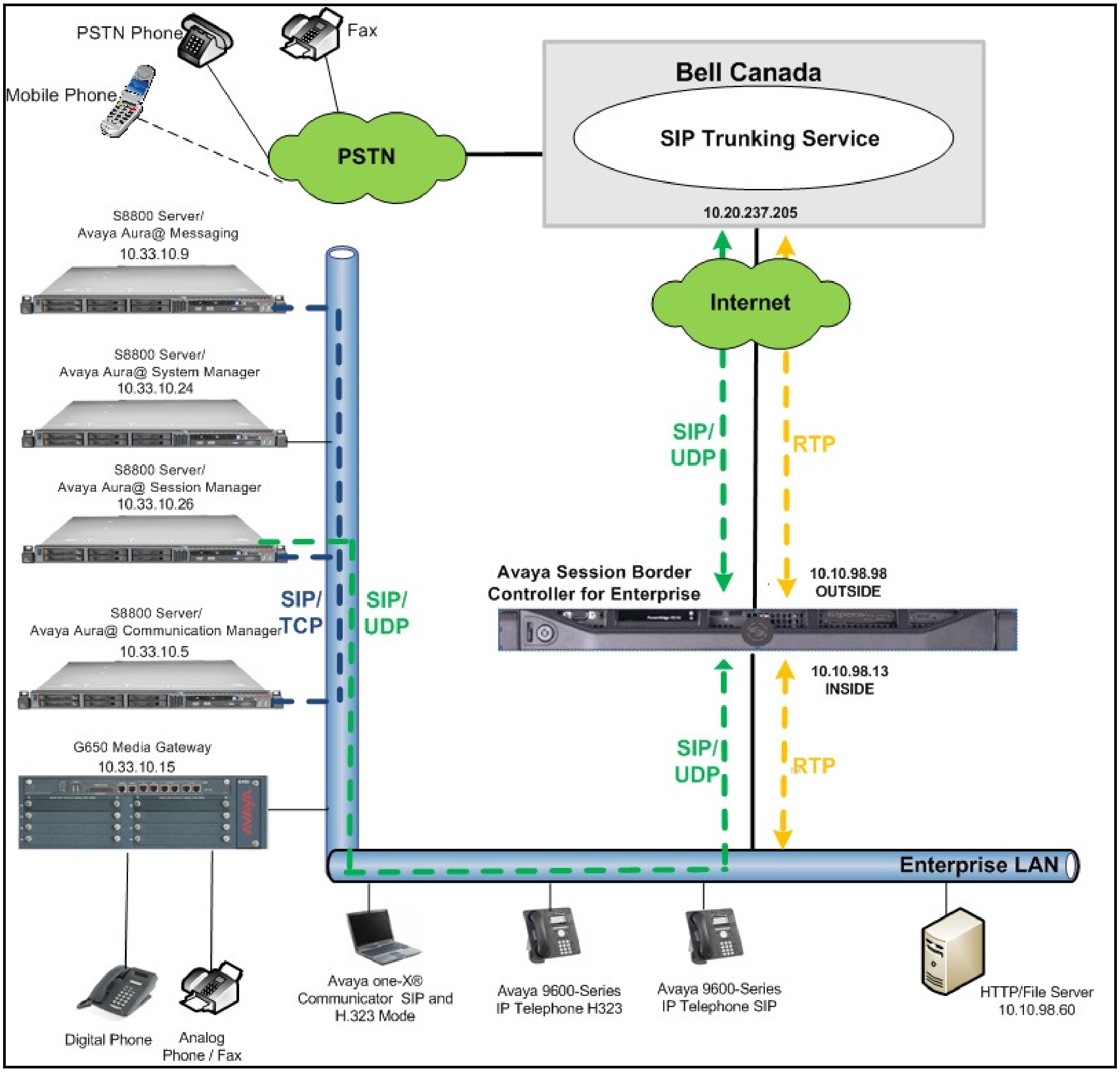


Figure 1: Avaya IP Telephony Network Connecting to Bell Canada SIP Trunking Service

Two separate SIP trunk groups were created between Communication Manager and Session Manager to carry traffic to and from service provider respectively. Any specific trunk or codec settings required by service provider were applied only to these dedicated trunks so as not to affect other enterprise SIP traffic.

Incoming calls flowed from service provider to 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 calls. Once the calls arrived at Communication Manager, further incoming call treatment, such as incoming digit translations and class of service restrictions could be performed.

Outgoing calls to 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 calls were routed to Session Manager to route to Avaya SBCE for egress to Bell Canada.

4. Equipment and Software Validated

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

Avaya IP Telephony Solution Components	
Component	Release
Avaya Aura® Communication Manager Evolution Server running on Avaya S8800 Server	6.3 (R016x.03.0.124.0)
Avaya G450 Media Gateway FW Version HW Vintage	 31 .22 .0 1
Avaya Aura® Session Manager running on Avaya S8800 Server	6.3.2.0.632023
Avaya Aura® System Manager running on Avaya S8800 Server	6.3.8.0 Patch 6.3.8.1627 Build Number 6.3.2.4.1399
Avaya Aura® Messaging running on Avaya S8800 Server	6.1-11.0
Avaya Session Border Controller For Enterprise	6.2 (6.2.0.Q36)
Avaya 96xx Series IP Telephone (H.323)	Avaya one-X® Deskphone Edition 6.0.1
Avaya 96xx Series IP Telephone (SIP)	Avaya one-X® Deskphone SIP Edition R6_0_3-120511 and Avaya one-X® Deskphone SIP Edition 6.2
Avaya one-X Communicator (H.323&SIP)	6.1.3.08-SP3-Patch2-35791
Avaya 1408 Digital Telephone	n/a
Avaya 6210 Analog Telephone	n/a
Bell Canada SIP Trunking Solution Components	
Component	Release
Bell Canada SIP Trunking Service	Version 1.3

Table 1: Equipment and Software Tested

The specific equipment and software above were used for the compliance testing. Note: This solution will be compatible with other Avaya Server and Media Gateway platforms running similar versions of Communication Manager and Session Manager.

5. Configure Avaya Aura® Communication Manager

This section describes procedures for configuring Communication Manager for inter-operating with Bell Canada. A SIP trunk was established between Communication Manager and Session Manager for use by signaling traffic to the enterprise from Bell Canada (for incoming calls to the enterprise from PSTN); similarly a separate SIP trunk was created for carrying signaling traffic to Bell Canada from the enterprise (for outgoing calls to PSTN from the enterprise). For outgoing calls, Bell Canada requires trunk group identification (tgrp) value in the "Contact" header. During the compliance testing, Bell Canada provided the "tgrp" value as **vsxx-416XXX1880-01a**.

It is assumed the general installation of Communication Manager has been previously completed.

The Communication Manager configuration was performed using System Access Terminal (SAT). Some screens in this section have been abridged for brevity and clarity in presentation.

5.1. Licensing and Capacity

Use **display system-parameters customer-options** command to verify that **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 service provider. The example shows that **24000** licenses are available and **96** are in use. The license file installed on the system controls the maximum values for these attributes. If a required feature is not enabled or there is insufficient capacity, contact an authorized Avaya sales representative to add additional capacity.

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

IP PORT CAPACITIES                                                  USED
                     Maximum Administered H.323 Trunks: 12000 0
           Maximum Concurrently Registered IP Stations: 18000 2
             Maximum Administered Remote Office Trunks: 12000 0
Maximum Concurrently Registered Remote Office Stations: 18000 0
              Maximum Concurrently Registered IP eCons: 414   0
  Max Concur Registered Unauthenticated H.323 Stations: 100   0
                        Maximum Video Capable Stations: 41000 0
                   Maximum Video Capable IP Softphones: 18000 0
                       Maximum Administered SIP Trunks: 24000 96
  Maximum Administered Ad-hoc Video Conferencing Ports: 24000 0
   Maximum Number of DS1 Boards with Echo Cancellation: 522   0
                             Maximum TN2501 VAL Boards: 128   0
                     Maximum Media Gateway VAL Sources: 250   1
           Maximum TN2602 Boards with 80 VoIP Channels: 128   0
          Maximum TN2602 Boards with 320 VoIP Channels: 128   0
   Maximum Number of Expanded Meet-me Conference Ports: 300   0

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

5.2. System Features

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

```
change system-parameters features                               Page   1 of  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
```

On **Page 9** verify that a text string has been defined to replace Calling Party Number (CPN) for restricted or unavailable calls. The compliance testing used the values of **AV-Restricted** for restricted calls and **AV-Unavailable** for unavailable calls.

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

CPN/ANI/ICLID PARAMETERS
   CPN/ANI/ICLID Replacement for Restricted Calls: AV-Restricted
  CPN/ANI/ICLID Replacement for Unavailable Calls: AV-Unavailable

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

5.3. IP Node Names

Use **change node-names ip** command to verify that node names have been previously defined for the IP addresses of Communication Manager (**procr**) and Session Manager (**SM63**). These node names will be needed for defining the service provider signaling groups in **Section 5.6**.

```
change node-names ip                                            Page   1 of   2
                                  IP NODE NAMES
    Name              IP Address
SM63                10.33.10.26
default             0.0.0.0
procr               10.33.10.5
procr6              ::
```

5.4. Codecs

Use **change ip-codec-set** command to define a list of codecs to use for calls between the enterprise and service provider. For the compliance testing, Bell Canada configured their network for G.711MU codec for voice calls. Thus, **ip-codec-set** was set to enable only G.711 codec in **Audio Codec** column of the table. Default values can be used for all other fields. The following screen shows codec set **1** configuration at the time of the compliance testing.

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

                          IP Codec Set

    Codec Set: 1

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

On **Page 2**, set **FAX Mode** to **off** to support G.711 fax calls as best effort. Incoming and outgoing G.711 fax calls appeared to work properly even though G.711 is not recommended for fax call on Communication Manager; it was treated like regular voice call using G.711 codec. For more information, see **Section** Error! Reference source not found., observation **2**.

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

                          IP Codec Set

                              Allow Direct-IP Multimedia? n



                    Mode              Redundancy
    FAX             off                0
    Modem           off                0
    TDD/TTY         US                 3
    Clear-channel   n                  0
```

5.5. IP Network Region

IP network region allows separate codec or quality of service settings to be used (if necessary) for calls between the enterprise and service provider versus calls within the enterprise or elsewhere. For the compliance testing, **ip-network-region 1** was created. Use **change ip-network-region 1** command to configure region **1** with following parameters:

- Set **Authoritative Domain** field to match the SIP domain of the enterprise. In this configuration, SIP domain name **avayalab.com** was assigned to Avaya lab. This domain name appears in the “From” header of SIP messages originating from this IP region. **Note**: Session Manager adaptation configuration (see **Section 6.4**) was used to convert this SIP domain name into **enterprise.com** to assist Avaya SBCE in distinguishing public PSTN traffic and private enterprise traffic in routing outgoing calls either to PSTN or to

Remote Worker station. Topology-Hiding feature on Avaya SBCE (see **Section 7.2.3.1**) will translate private SIP domain into public SIP domain that is known to Bell Canada.

- Enter a descriptive name in **Name** field.
- Enable **IP-IP Direct Audio** (shuffling) to allow audio traffic to be sent directly between IP endpoints without using media resources in Avaya Media Gateway. Keep both **Intra-region** and **Inter-region IP-IP Direct Audio** to **yes** to use the default setting.
- Set **Codec Set** field to IP codec set defined in **Section 5.4**.
- Default values can be used for all other fields.

```
change ip-network-region 1                                      Page   1 of  20
                               IP NETWORK REGION
  Region: 1
Location: 1       Authoritative Domain: avayalab.com
    Name: avayalab.com          Stub Network Region: n
MEDIA PARAMETERS                Intra-region IP-IP Direct Audio: yes
      Codec Set: 1              Inter-region IP-IP Direct Audio: yes
   UDP Port Min: 2048                      IP Audio Hairpinning? n
   UDP Port Max: 3329
```

On **Page 4**, define IP codec set to be used for traffic between region **1** and other regions. In this testing, Communication Manager, Session Manager, IP phone and Avaya SBCE were assigned to the same region **1**. Enter desired IP codec set in the **codec set** column of the row with destination region (**dst rgn**) **2**. Default values may be used for all other fields. The example below shows the settings used for the compliance testing. It indicates that codec set **1** will be used for calls between region **1** (the service provider region) and other regions.

```
change ip-network-region 1                                      Page   4 of  20

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

Non-IP telephones, e.g. analog, digital, derive network region from Avaya Media Gateway to which the device is connected. IP telephones can be assigned a network region based on an IP address mapping. The following screen illustrates a subset of IP network map used to verify these Application Notes.

For the compliance testing, devices with IP addresses in the **10.10.97.0/24** subnet and **10.33.0.0/16** subnet were assigned to network region **1**. These include Communication Manager, Session Managers and Avaya SBCEs that were set up for the test environment. IP telephones used for the compliance testing, including both Avaya 9600 IP Telephones and Avaya one-X® Communicator soft phones, were also assigned to network region **1** with IP addresses in the **10.33.0.0/16** subnet. In production environments, different sites will typically be on different networks and ranges of IP addresses assigned by the DHCP scope serving the site. These addresses can be entered as one entry in the network map, to assign all telephones in a range to a specific network region.

```
change ip-network-map                                              Page   1 of  63
                               IP ADDRESS MAPPING

                                                 Subnet Network      Emergency
 IP Address                                      Bits   Region VLAN Location Ext
 ----------------------------------------------- ------ ------ ---- -------------
 FROM: 10.33.0.0                                 /16    1       n
   TO: 10.33.255.255
 FROM: 10.10.97.0                                /24    1       n
   TO: 10.10.97.255
FROM:                                           /              n
   TO:
```

5.6. Signaling Group

Use **add signaling-group** command to create 2 signaling groups between Communication Manager and Session Manager for use by incoming and outgoing calls. The signaling group used for incoming calls is shown below. For the compliance testing, signaling group **2** was used and configured with parameters highlighted below.

- Set **Group Type** field to **sip**.
- Set **IMS Enabled** field to **n**. This specifies Communication Manager will serve as an Evolution Server for Session Manager.
- Set **Transport Method** to **tcp** for private SIP Trunk between Communication Manager and Session Manager.
- Set **Near-end Listen Port** and **Far-end Listen Port** to a valid unused port. This is necessary so Session Manager can distinguish this trunk from the trunk used for other enterprise SIP traffic. The compliance testing was conducted with **Near-end Listen Port** and **Far-end Listen Port** set to well-known port for **5060** for **TCP**.
- Set **Peer Detection Enabled** field to **y**. **Peer-Server** field will initially be set to **Others** but after, it will automatically change to **Session Manager** once Communication Manager detects its peer as Session Manager.
- Set **Near-end Node Name** to **procr** as shown in **Section 5.3**.
- Set **Far-end Node Name** to **SM63** as shown in **Section 5.3**.
- Set **Far-end Network Region** to the IP network region **1** defined for the service provider in **Section 5.5**.
- Set **Far-end Domain** to blank.
- Set **Direct IP-IP Audio Connections** to **y**. This field will enable media shuffling on the SIP Trunk allowing Communication Manager to redirect media traffic directly between the SIP Trunk and the enterprise station. If this value is set to **n**, then Avaya Media Gateway will remain in the media path of all calls between the SIP Trunk and the station. Depending on the number of media resources available on Avaya Media Gateway, these resources may be depleted during high call volume preventing additional calls from completing.
- Set **DTMF over IP** field to **rtp-payload**. This setting enables Communication Manager to send DTMF transmissions using RFC 2833.

- Verify that **Initial IP-IP Direct Media** was set to **n**.
- Change default setting of **6** for **Alternate Route Timer (sec)** to **30**. This allows more time for outgoing PSTN calls to complete through Bell Canada SIP Trunking Service.
- Set **Enable Layer 3 Test?** to **y** to allow Communication Manager to request and respond to OPTIONS heartbeat from Session Manager.
- Default values may be used for all other fields.

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

 Group Number: 2              Group Type: sip
  IMS Enabled? n        Transport Method: tcp
        Q-SIP? n
     IP Video? n                                   Enforce SIPS URI for SRTP? y
  Peer Detection Enabled? y  Peer Server: SM
 Prepend '+' to Outgoing Calling/Alerting/Diverting/Connected Public Numbers? n
Remove '+' from Incoming Called/Calling/Alerting/Diverting/Connected Numbers? y

   Near-end Node Name: procr                   Far-end Node Name: SM63
 Near-end Listen Port: 5060                  Far-end Listen Port: 5060
                                          Far-end Network Region: 1

Far-end Domain:
                                             Bypass If IP Threshold Exceeded? n
Incoming Dialog Loopbacks: eliminate                  RFC 3389 Comfort Noise? n
         DTMF over IP: rtp-payload             Direct IP-IP Audio Connections? y
Session Establishment Timer(min): 3                     IP Audio Hairpinning? n
         Enable Layer 3 Test? y                    Initial IP-IP Direct Media? n
H.323 Station Outgoing Direct Media? n             Alternate Route Timer(sec): 30
```

Signaling group for outgoing calls was similarly configured except that **Far-end Domain** was set to **avayalab.com** and **"**Enable Layer 3 Test?**"** was set to **n** to restrict Communication Manager from responding to incoming OPTIONS heartbeat from Session Manager because this SIP Trunk was dedicated to outgoing traffic only. For the compliance testing, signaling group **3** was used for this purpose and shown below:

```
add signaling-group 3                                          Page   1 of   2
                                SIGNALING GROUP

 Group Number: 3              Group Type: sip
  IMS Enabled? n        Transport Method: tcp
        Q-SIP? n
     IP Video? n                                  Enforce SIPS URI for SRTP? y
  Peer Detection Enabled? y  Peer Server: SM
 Prepend '+' to Outgoing Calling/Alerting/Diverting/Connected Public Numbers? n
Remove '+' from Incoming Called/Calling/Alerting/Diverting/Connected Numbers? y

   Near-end Node Name: procr                  Far-end Node Name: SM63
 Near-end Listen Port: 5060                 Far-end Listen Port: 5060
                                         Far-end Network Region: 1

Far-end Domain: avayalab.com
                                          Bypass If IP Threshold Exceeded? n
Incoming Dialog Loopbacks: eliminate               RFC 3389 Comfort Noise? n
         DTMF over IP: rtp-payload         Direct IP-IP Audio Connections? y
Session Establishment Timer(min): 3                  IP Audio Hairpinning? n
         Enable Layer 3 Test? n                Initial IP-IP Direct Media? n
H.323 Station Outgoing Direct Media? n         Alternate Route Timer(sec): 30
```

5.7. Trunk Group

Use **add trunk-group** command to create trunk group for the 2 signaling groups created in **Section 5.6**. For the compliance testing, trunk group **2** was configured for incoming calls and trunk group **3** was configured for outgoing calls using parameters highlighted below.

- Set **Group Type** field to **sip**.
- Enter a descriptive name for **Group Name**.
- Enter an available trunk access code (**TAC**) that is consistent with the existing dial plan in **TAC** field.
- Set **Direction** field to **incoming** for trunk group **2** and **outgoing** for trunk group **3**.
- Set **Outgoing Display** to **y** to enable name display on the SIP Trunk.
- Set **Service Type** field to **public-ntwrk**.
- Set **Member Assignment Method** to **auto**.
- Set **Signaling Group** to appropriate signaling group shown in **Section 5.6**, i.e. signaling group **2** for incoming trunk group **2** and signaling group **3** for outgoing trunk group **3**.
- Set **Number of Members** field to the number of trunk members of the trunk group. This value determines how many simultaneous SIP calls can be supported by this trunk.
- Default values were used for all other fields.

```
add trunk-group 2                                              Page   1 of  21
                                TRUNK GROUP

Group Number: 2                    Group Type: sip          CDR Reports: y
  Group Name: Bell_Incoming               COR: 1        TN: 1        TAC: *002
   Direction: incoming       Outgoing Display? y
 Dial Access? n                                  Night Service:

Service Type: public-ntwrk          Auth Code? n
                                              Member Assignment Method: auto
                                                       Signaling Group: 2
                                                     Number of Members: 32
```

On **Page 2**, verify that **Preferred Minimum Session Refresh Interval (sec)** is set to a value acceptable to the service provider. This value defines the interval that re-INVITEs must be sent to keep the active session alive. For the compliance test, the value of **300** seconds was used.

```
add trunk-group 2                                              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): 300

 Disconnect Supervision - In? y
```

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

Set **Replace Restricted Numbers** and **Replace Unavailable Numbers** fields to **y**. This will allow CPN displayed on local endpoints to be replaced with the value set in **Section 5.8**, if incoming calls enabled CPN block. For outbound calls, these same settings request that CPN block be activated on the far-end destination if a local user requests CPN block on a particular call routed out this trunk. Default values were used for all other fields.

```
add trunk-group 2                                                 Page   3 of  21
TRUNK FEATURES
          ACA Assignment? n            Measured: none
                                                               Maintenance Tests? y



                     Numbering Format: private
                                                         UUI Treatment: service-provider

                                                          Replace Restricted Numbers? y
                                                         Replace Unavailable Numbers? y

Show ANSWERED BY on Display? y
```

On **Page 4**, **Network Call Redirection** field can be set to **n**. This setting disable the use of the REFER method for call transfer because Bell Canada preferred to use subsequence INVITE method as an alternative.

- Set **User as Phone?** to **y**.
- Set **Send Diversion Header** field to **y**. This field provides additional information to the network if the call has been re-directed. This is needed to support call forwarding of inbound calls back to the PSTN and some Extension to Cellular (EC500) call scenarios.
- Set **Support Request History** field to **n**. This parameter determines whether the “History-Info” header will be included in the call-redirection INVITE from the enterprise.
- Set **Telephone Event Payload Type** to **101** which is the value Bell Canada preferred.
- Set **Convert 180 to 183 for Early Media** field to **y**.

```
add trunk-group 2                                                 Page   4 of  21
                              PROTOCOL VARIATIONS

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

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


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

Page 1 of trunk group **3** for outgoing calls as shown in the screenshot below, the **Direction** was set to “outgoing” and **Signaling Group** was set to 3.

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

Group Number: 3                    Group Type: sip          CDR Reports: y
  Group Name: Bell_Outgoing               COR: 1        TN: 1        TAC: *003
   Direction: outgoing       Outgoing Display? y
 Dial Access? n
Queue Length: 0
Service Type: public-ntwrk
                                              Member Assignment Method: auto
                                                       Signaling Group: 3
                                                     Number of Members: 32
```

The configurations on other pages of trunk group 3 are identical to trunk group 2.

5.8. Calling Party Information

Calling Party Number is sent in the "From", "Contact" and "PAI" headers. Since private numbering was selected to define the format of this number (**Section 5.7**), use **change private-numbering** command to create an entry for a range of extension starting with **18** which has DID numbers assigned. The DID numbers are provided by service provider to authenticate the caller.

The normal DID number is comprised of the local extension plus a prefix. A single private numbering entry can be applied for all extensions. In the example below, all stations with a 4-digit extension beginning with **18** will send Calling Party Number as **Private Prefix 416XXX** plus the extension number **18XX** for incoming and outgoing calls over trunk group **2** and **3**.

```
change private-numbering 0                                      Page   1 of   2
                            NUMBERING - PRIVATE FORMAT

Ext Ext              Trk         Private           Total
Len Code             Grp(s)      Prefix            Len
 4  18               2-3         416XXX            10    Total Administered: 2
 4  18               10                            4        Maximum Entries: 540
```

Even though private numbering was selected, currently the number used in the "Diversion" header is derived from the public unknown numbering table and not the private numbering table. As a workaround for this, the entries in the private numbering table must be repeated in the public unknown numbering table.

```
change public-unknown-numbering 0                               Page   1 of   2
                       NUMBERING - PUBLIC/UNKNOWN FORMAT
                                                  Total
Ext Ext             Trk        CPN                CPN
Len Code            Grp(s)     Prefix             Len
                                                        Total Administered: 3
 5  4               1                             5        Maximum Entries: 9999
 4  18              2-3        416XXX             10
 4  18              10                            4
```

5.9. Outbound Routing

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

```
change dialplan analysis                                        Page   1 of  12
                             DIAL PLAN ANALYSIS TABLE
                                   Location: all            Percent Full: 0

    Dialed   Total  Call      Dialed   Total  Call      Dialed   Total  Call
    String   Length Type      String   Length Type      String   Length Type
   18          4   ext
   9           1   dac
   *           4   dac
```

Use **change feature-access-codes** command to configure **9** as **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: *111
                       Answer Back Access Code:
                         Attendant Access Code:
      Auto Alternate Routing (AAR) Access Code: *100
    Auto Route Selection (ARS) - Access Code 1: 9     Access Code 2:
                 Automatic Callback Activation:        Deactivation:
Call Forwarding Activation Busy/DA:        All:        Deactivation:
   Call Forwarding Enhanced Status:        Act:        Deactivation:
```

Use **change ars analysis** command to configure 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 testing. See **Section 2.1** for complete list of call types tested. All dialed strings are mapped to route pattern **3** for outgoing calls and route pattern 3 for vector call redirection which contains the SIP Trunk to service provider (as defined next).

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

          Dialed           Total     Route    Call   Node  ANI
          String          Min  Max  Pattern   Type   Num   Reqd
    0                     1    28    3        pubu         n
    1                     11   11    3        pubu         n
    411                   3    3     3        svcl         n
```

The route pattern defines which trunk group will be used for outgoing calls and performs any necessary digit manipulation. Use **change route-pattern** command to configure the parameters for service provider trunk route pattern in the following manner.

The example below shows the values used for route pattern **3** for outgoing call.

- **Pattern Name**: Enter a descriptive name.
- **Grp No**: Enter outgoing trunk group **3** for service provider SIP Trunk. For the compliance testing, trunk group **3** was used.
- **FRL**: Set 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.
- **Numbering Format**: **unk-unk**. All calls using this route pattern will use the private numbering table. See setting of **Numbering Format** in the trunk group form for full details in **Section 5.7**.
- **LAR**: **next**.

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

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

5.10. Vector Directory Numbers (VDN)

This section describes basic commands used to configure Vector Directory Numbers (VDN) and corresponding vectors. These Application Notes provide rudimentary vector definitions to demonstrate and test the off-net redirection using a VDN. In general, call centers will use vector functionality that is more complex and tailored to individual needs. The definition and documentation of those complex applications and associated vectors are beyond the scope of these Application Notes.

This section provides a sample configuration of the VDN **1883** as shown in the following abridged screen. The originally dialed DID number may be mapped to VDN **1883** by the incoming call handling treatment for the incoming trunk group on Communication Manager. Incoming calls to VDN **1883** will be routed to destination vector number **1883**.

```
display vdn 1883                                                Page   1 of   3
                            VECTOR DIRECTORY NUMBER

                             Extension: 1883
                                 Name*: Bell VDN
                           Destination: Vector Number        1883
                   Attendant Vectoring? n
                  Meet-me Conferencing? n
                    Allow VDN Override? n
                                   COR: 1
                                   TN*: 1
                              Measured: none


        VDN of Origin Annc. Extension*:
                            1st Skill*:
                            2nd Skill*:
                            3rd Skill*:



* Follows VDN Override Rules
```

5.10.1. Pre-Answer Redirection to a PSTN Destination

VDN **1883** was associated with vector **1883**, which is shown below. For the pre-answer redirection, vector **1883** was configured to play ringback (step 01) then redirect off-net incoming calls back to the PSTN by **route-to number** (step 02) **91613XXX5279** where the digit 9 is the ARS feature access code as discussed in **Section 5.9** and the number **1613XXX5279** is a PSTN destination. As a result, a subsequent INVITE will be sent with the “Request-URI” header containing **1613XXX5279** as the URI-User parameter.

```
display vector 1883                                             Page   1 of   6
                                  CALL VECTOR

    Number: 1883             Name: Bell Canada
Multimedia? n      Attendant Vectoring? n    Meet-me Conf? n           Lock? n
     Basic? y   EAS? y   G3V4 Enhanced? y   ANI/II-digit? y   ASAI Routing? y
 Prompting? y   LAI? y  G3V4 Adv Route? y   CINFO? y   BSR? y   Holidays? y
 Variables? y   3.0 Enhanced? y
01 wait-time    10  secs hearing ringback
02 route-to     number 91613XXX5279     with cov n if unconditionally
03 stop
04
```

5.10.2. Post-Answer Redirection to a PSTN Destination

For post-answer redirection, vector **1883** was configured to play an announcement (step 02) after answering the call. After the announcement, **route-to number** (step 03) includes **91613XXX5279** where the digit **9** is the ARS feature access code as discussed in **Section 5.9** and the number **1613XXX5279** is a PSTN destination. As a result, a subsequent INVITE will be sent with the "Request-URI" header containing **1613XXX5279** as the URI-User parameter.

```
display vector 1883                                          Page   1 of   6
                                  CALL VECTOR

    Number: 1883             Name: Bell Canada
Multimedia? n      Attendant Vectoring? n    Meet-me Conf? n           Lock? n
     Basic? y   EAS? y   G3V4 Enhanced? y   ANI/II-Digits? y   ASAI Routing? y
 Prompting? y   LAI? y  G3V4 Adv Route? y   CINFO? y   BSR? y   Holidays? y
 Variables? y   3.0 Enhanced? y
01 wait-time    10  secs hearing silence
02 announcement 1884
03 route-to     number 91613XXX5279     with cov n if unconditionally
04 stop
```

5.11. Incoming Call Handling

When an incoming call arrives from Session Manager, Communication Manager applies incoming handling treatment on incoming trunk group 2 (the incoming trunk group is discussed in **Section 5.7**). Bell Canada sends 10 digits in the "Request-URI" and "To" headers to the assigned DID number. The incoming call handling treatment will translate the 10-digit DID number with prefix **416XXX18** to 4-digit based extensions. To do this, use **inc-call-handling-trmt trunk-group** command to define an incoming handling for Bell Canada. Following screenshot shows the configuration in detail on incoming trunk group 2.

```
change inc-call-handling-trmt trunk-group 2                     Page   1 of  30
                       INCOMING CALL HANDLING TREATMENT
 Service/      Number   Number      Del Insert
 Feature        Len      Digits
 public-ntwrk    10  416XXX18         6
 public-ntwrk
```

5.12. Saving Communication Manager Configuration Changes

The command "**save translation all**" can be used to save the configuration changes made on Communication Manager.

6. Configure Avaya Aura® Session Manager

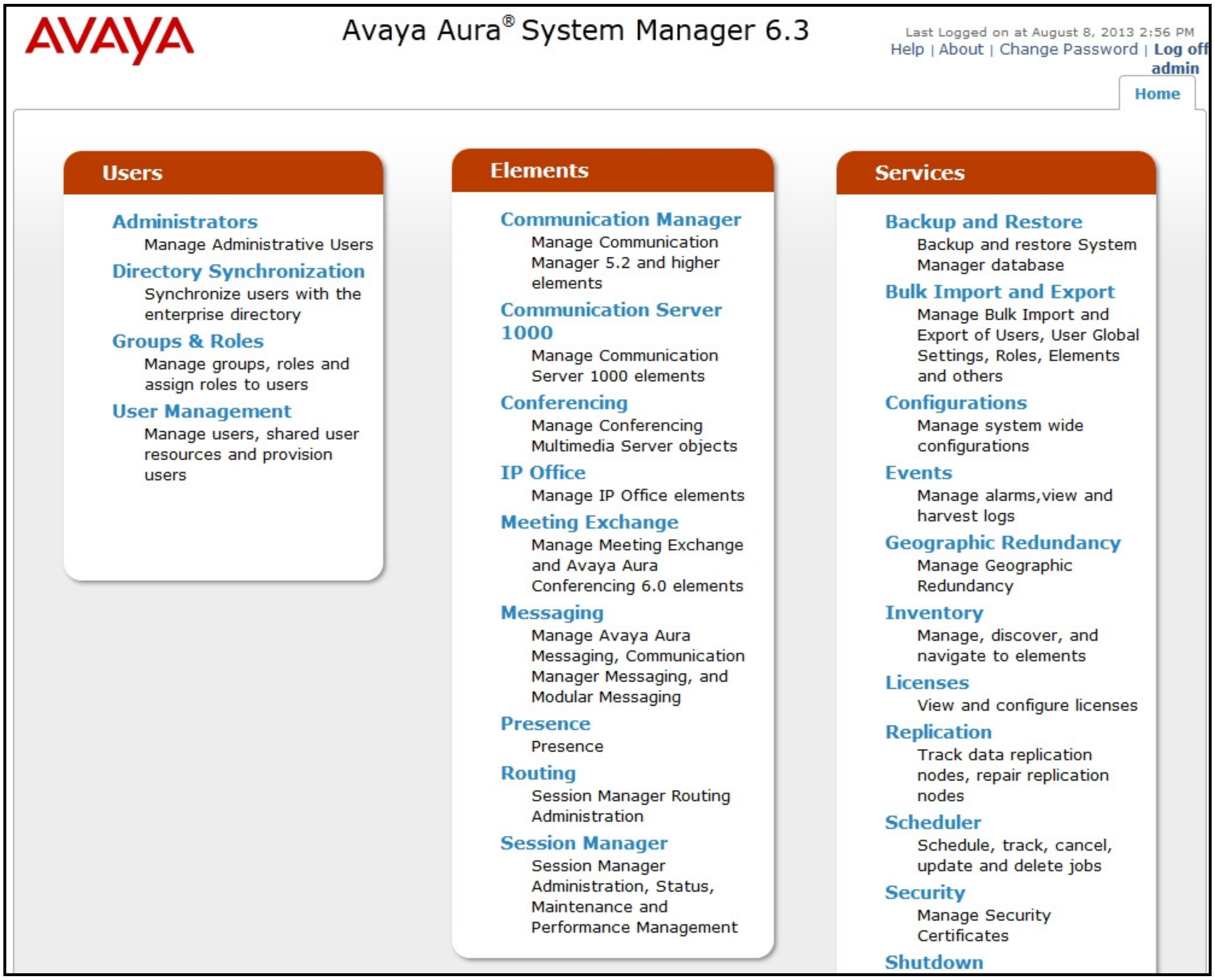
This section provides the procedures for configuring Session Manager. The procedures include adding the following items:

- SIP domain.
- Logical/physical Location that can be occupied by SIP Entities.
- Adaptation module to perform SIP domain manipulation.
- SIP Entities corresponding to Communication Manager, Session Manager and 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.
- Session Manager, corresponding to the Session Manager server to be managed by System Manager.

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

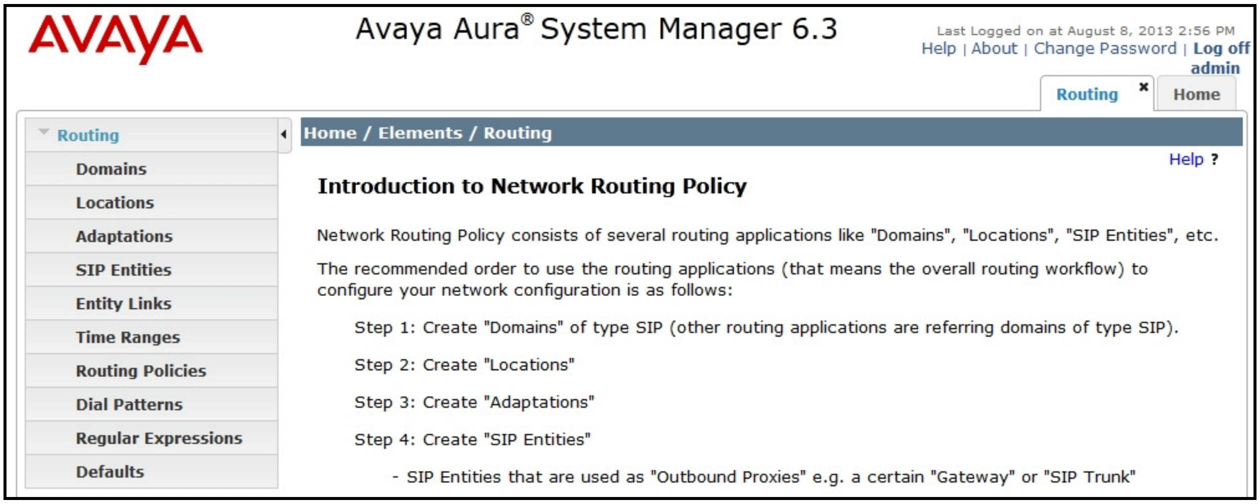
6.1. System Manager Login and Navigation

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. At the **System Manager Log On** screen, provide the appropriate credentials and click on **Login** (not shown). The initial screen shown below is then displayed.



Most of the configuration items are performed in the Routing Element. Click **Routing** in the **Elements** column to bring up the **Introduction to Network Routing Policy** screen.

The navigation tree displayed in the left pane will be referenced in subsequent sections to navigate to items requiring configuration.

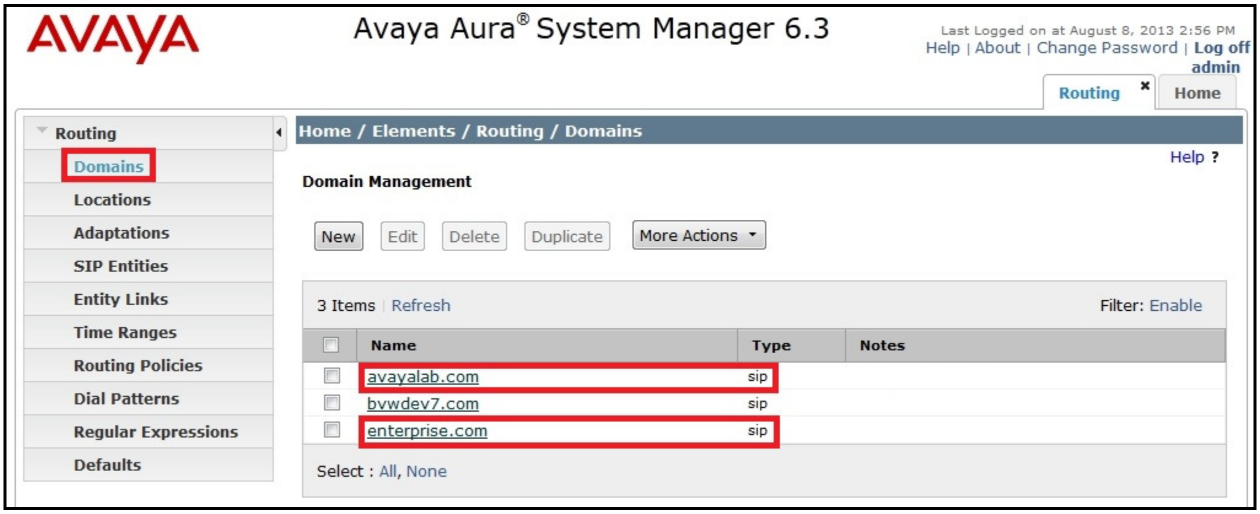


6.2. Specify SIP Domain

To view or change SIP domains, select **Routing → Domains**. Click the checkbox next to the name of SIP domain and **Edit** to edit an existing domain, or the **New** button to add a domain. Click **Commit** button (not shown) after changes are completed.

The following screen shows the list of configured SIP domains **avayalab.com** for public SIP Trunk between Communication Manger and Session Manager and **enterprise.com** for public SIP Trunk between Session Manger and Avaya SBCE. These SIP domains are not known to Bell Canada SIP Trunking Service.

Note: In these Application Notes, Avaya SBC was configured to support both SIP Trunking to service provider and Remote Worker for Avaya 96X1 SIP phone to register to Session Manager as Communication Manager station over the internet. Therefore, two separate SIP domains were defined to assist Avaya SBCE in distinguishing public SIP Trunk traffic that contains **enterprise.com** and Remote Worker traffic that contains **avayalab.com**. In the real deployment, it is recommended to have separate Avaya SBCE for SIP Trunking and Remote Worker. In this configuration, separate SIP domain name is not required on Session Manager for the public SIP Trunk.



6.3. Add Location

Locations can be used to identify logical and/or physical locations where SIP Entities reside for purposes of bandwidth management and call admission control. 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).

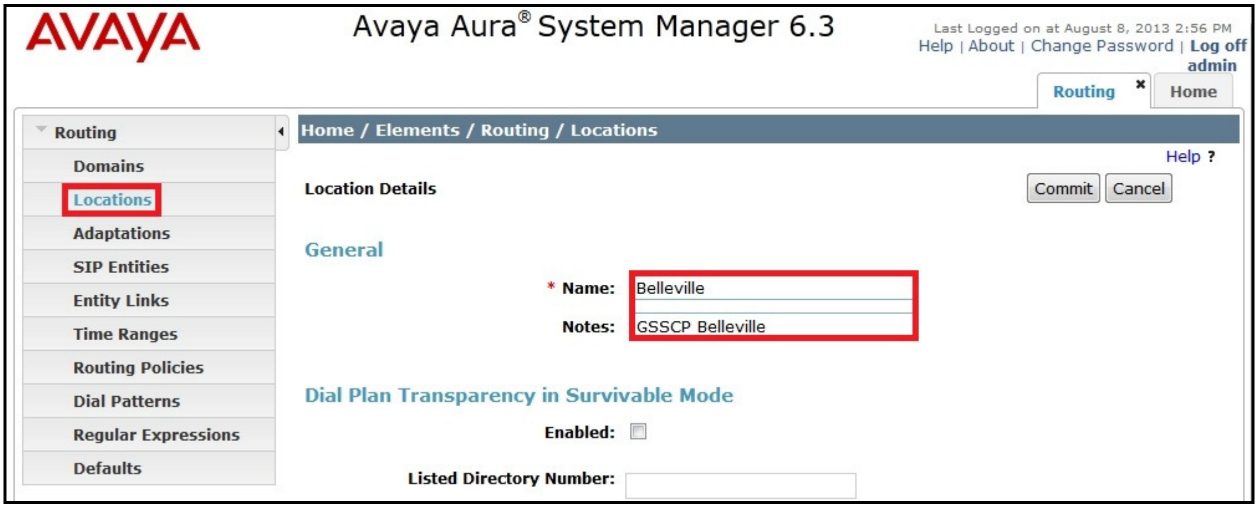
In **General** section, enter following values:

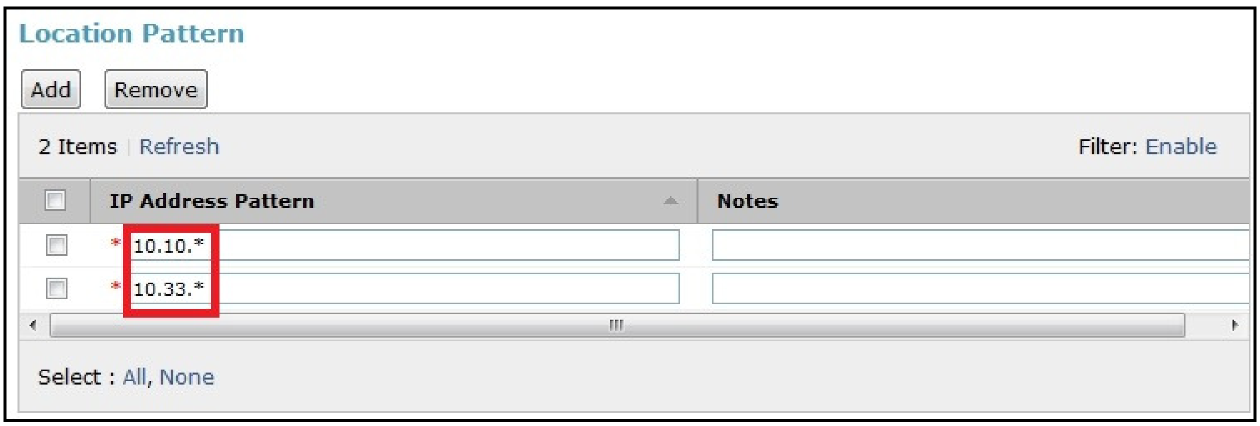
- **Name**: Enter a descriptive name for the location.
- **Notes**: Add a brief description (optional).

In **Location Pattern** section, click **Add** and enter following values:

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

Displayed below are the screenshot for **Belleville** location, which includes all equipment on the **10.10.X.X** and **10.33.X.X** subnet including Communication Manager, Session Manager and Avaya SBCE. Click **Commit** to save.



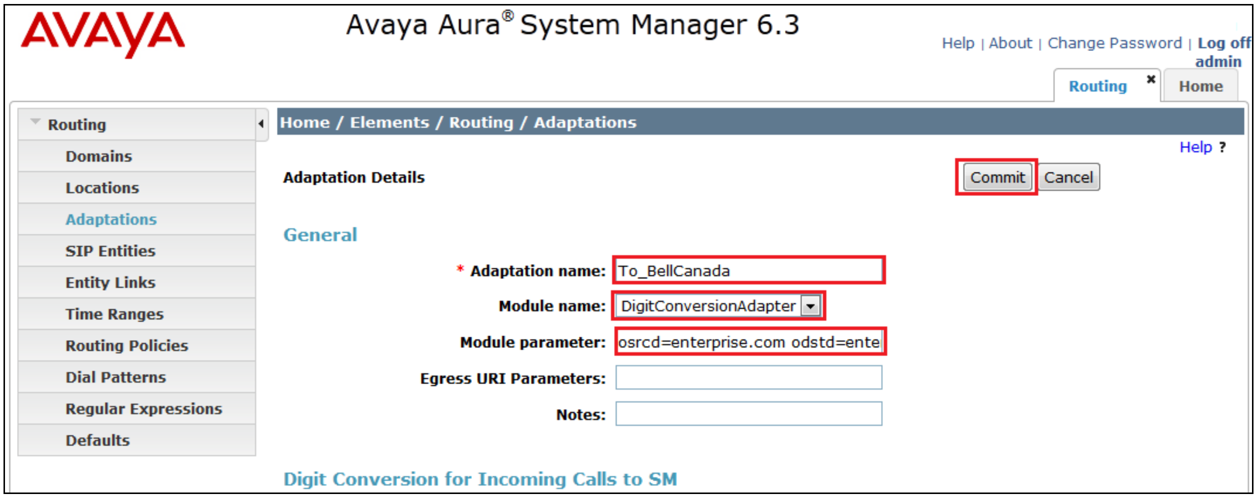


6.4. Add Adaptation Module

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

To view or change adaptations, select **Routing → Adaptations**. Click the checkbox corresponding to the name of an adaptation and **Edit** to edit an existing adaptation, or the **New** button to add an adaptation. Click the **Commit** button after changes are completed.

Adaptations **To_BellCanada** and **To_CM** were configured and used in the compliance testing. The **To_BellCanada** adaptation as show in the following screenshot, will later be assigned to Avaya SBCE SIP Entity. This adaptation uses **DigitConversionAdapter** and specifies **osrcd=enterprise.com odstd=enterprise.com fromto=true** to adapt the SIP domain from **avayalab.com** to **enterprise.com** for outgoing call to Avaya SBCE.



The adaptation **To_CM** shown below will later be assigned to Communication Manager SIP Entity. This adaptation uses **DigitConversionAdapter** specifies **osrcd=avayalab.com odstd=avayalab.com fromto=true** to adapt the SIP domain from **enterprise.com** to **avaya.com** for incoming calls from Bell Canada to Communication Manger.

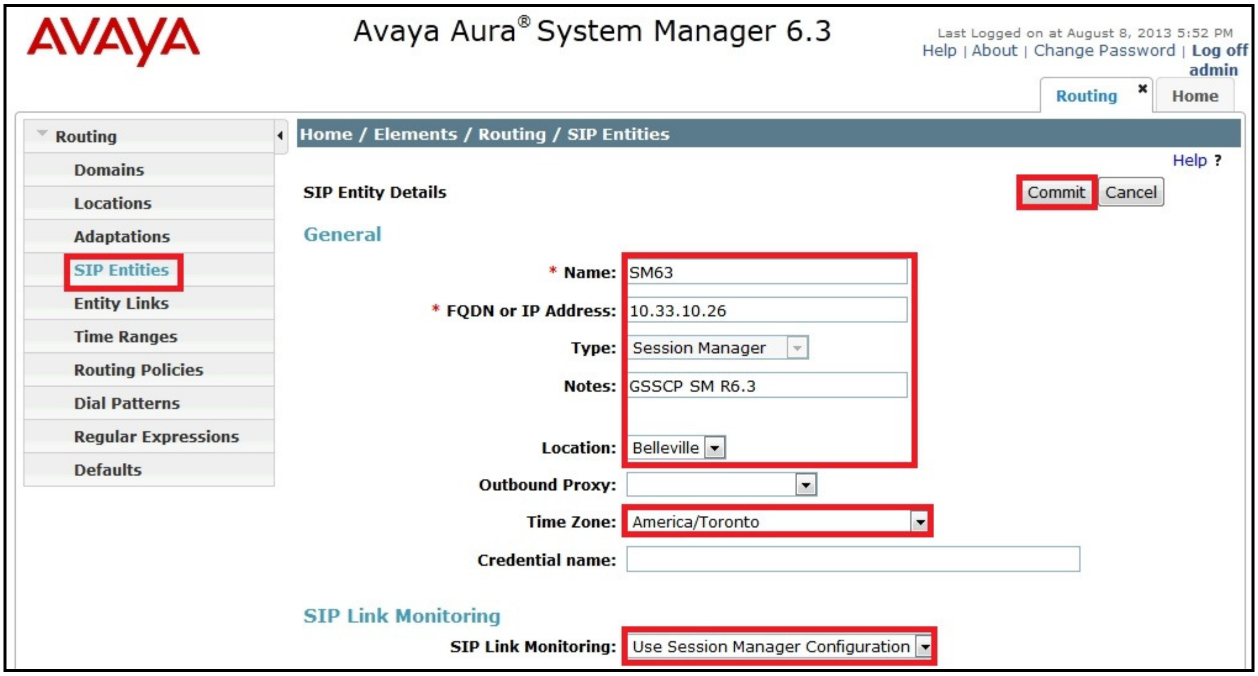
6.5. Add SIP Entities

A SIP Entity must be added for Session Manager and for each SIP telephony system connected to it which includes Communication Manager and Avaya SBCE. Navigate to **Routing → SIP Entities** in the left navigation pane and click the **New** button in the right pane (not shown).

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

- **Name**: Enter a descriptive name.
- **FQDN or IP Address**: Enter IP address of SIP Entity that is used for SIP signaling.
- **Type**: Select **Session Manager** for Session Manager, **CM** for Communication Manager and **Other** for Avaya SBCE.
- **Adaptation**: This field is only present if **Type** is not set to **Session Manager**. If applicable, select **Adaptation** name created in **Section 6.4** that will apply to this entity.
- **Location**: Select the locations defined previously in **Section 6.3**.
- **Time Zone**: Select time zone for the location above.
- **SIP Link Monitoring**: Select **Use Session Manager Configuration**.

The following screen shows the addition of Session Manager SIP Entity **SM63** with IP address of Session Manager signaling interface is entered for **FQDN or IP Address**.



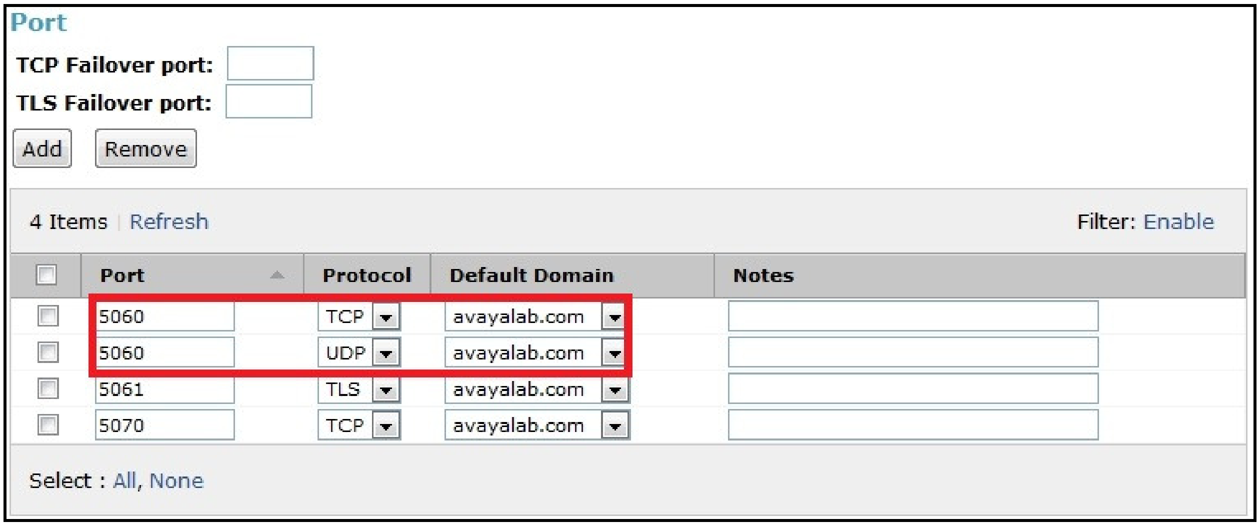
To define port used by Session Manager, scroll down to **Port** section of **SIP Entity Details** screen. This section is only present for **Session Manager** SIP Entity.

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

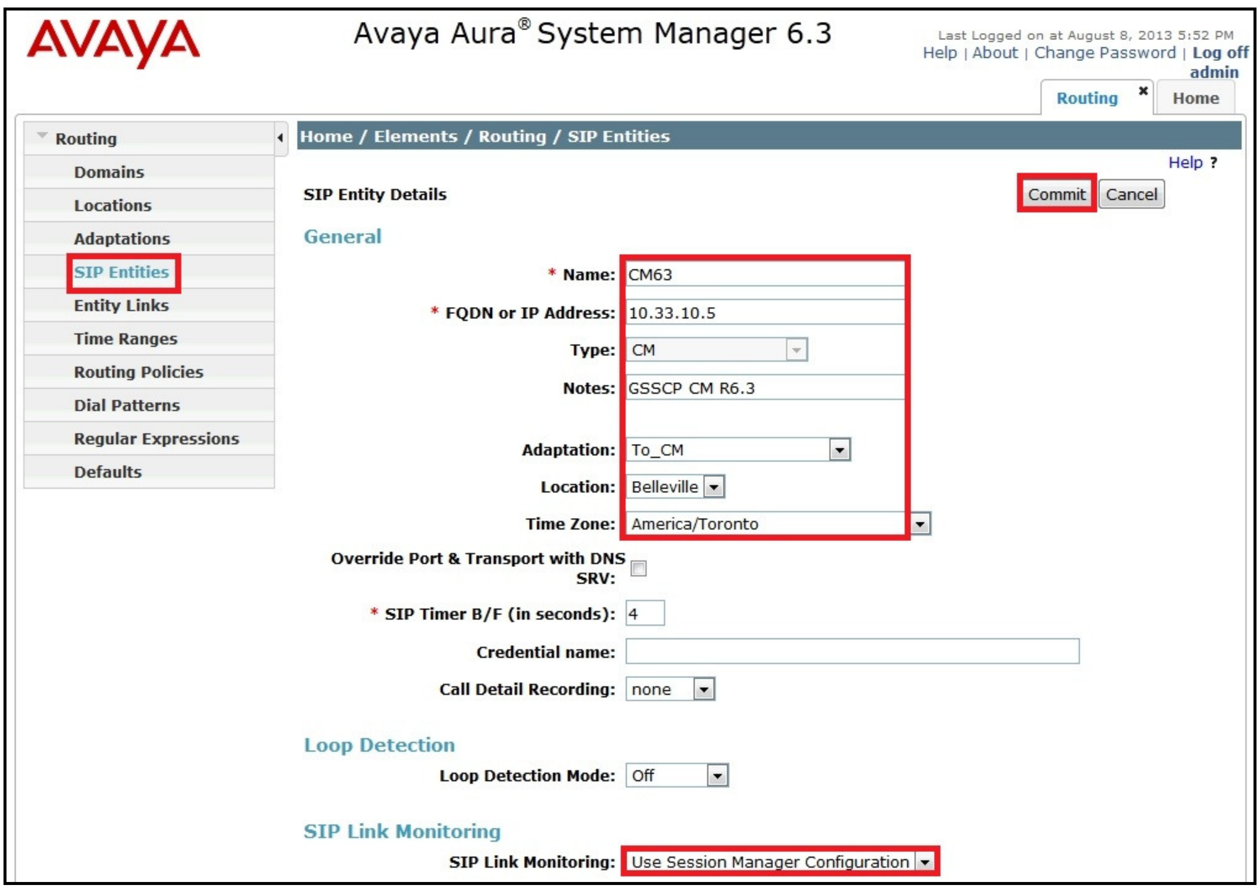
- **Port**: Port number on which Session Manager can listen for SIP requests.
- **Protocol**: Transport protocol to be used to send SIP requests.
- **Default Domain**: The domain used for the enterprise.

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

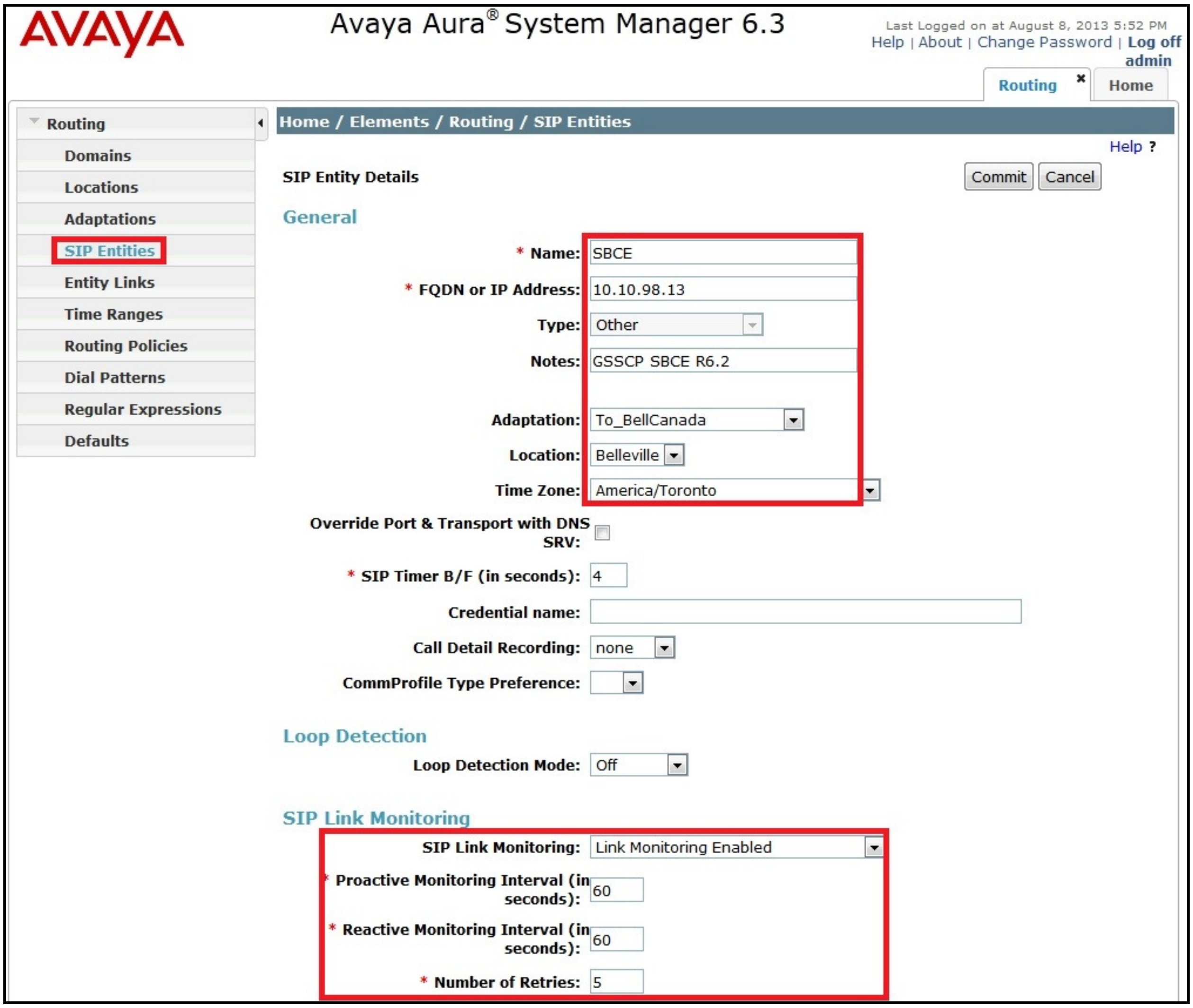
The compliance testing used **Port** entry **TCP/5060** for connection to Communication Manager and **Port** entry **UDP/5060** for connection to Avaya SBCE.



The following screen shows the addition of Communication Manager SIP Entity CM63. In order for Session Manager to send SIP signaling to Communication Manager, it is necessary to create a SIP Entity for Communication Manager. **FQDN or IP Address** field was set to IP address of Communication Manager. **Type** was selected as **CM**. For **Adaptation** field, select adaptation module **To_CM** previously defined for SIP domain manipulation in **Section 6.4**. **IP Link Monitoring** was set to **Use Session Manager Configuration**.



The following screen shows the addition of Avaya SBCE SIP Entity **SBCE**. **FQDN or IP Address** field was set to IP address of its private network interface **10.10.98.113** as shown in **Figure 1**. **Link Monitoring Enabled** was selected for **SIP Link Monitoring**. These time settings should be adjusted or left at their default values per customer needs and requirements.



6.6. Add Entity Links

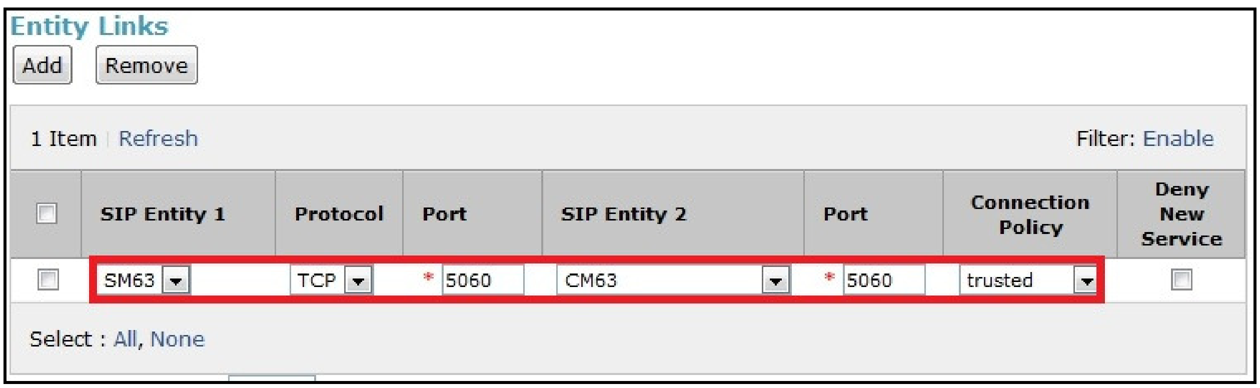
A SIP Trunk between Session Manager and a telephony system is described by an Entity Link. Two Entity Links were created; one to Communication Manager for use only by service provider traffic and another one to Avaya SBCE. To add an Entity Link, navigate to **Routing → Entity Links** in the left navigation pane and click on **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 Session Manager.
- **Protocol**: Select transport protocol used for this link.

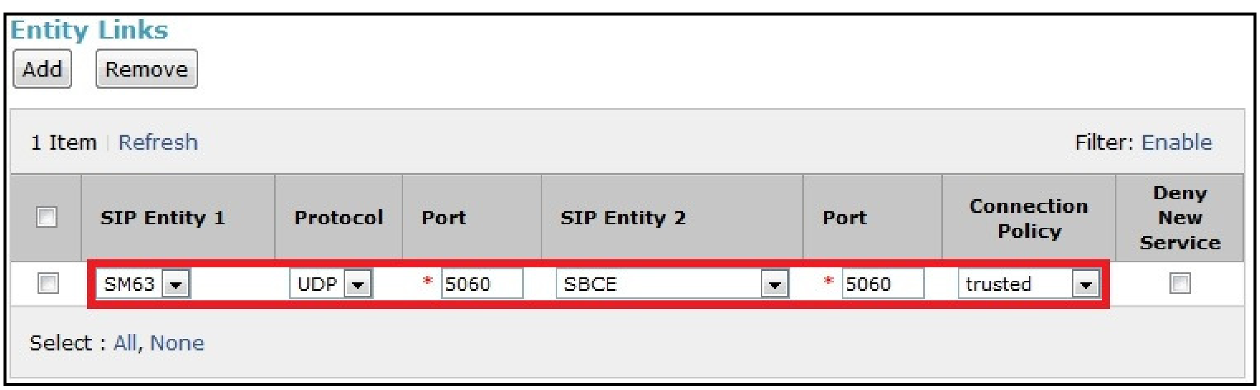
- **Port**: Port number on which Session Manager will receive SIP requests from the far-end. For Communication Manager, this must match **Far-end Listen Port** defined on the Communication Manager signaling group in **Section 5.6**.
- **SIP Entity 2**: Select name of the other system. For Communication Manager, select Communication Manager SIP Entity **CM63** defined in **Section 6.5**. For Avaya SBCE, select Avaya SBCE SIP Entity **SBCE** defined in **Section 6.5**.
- **Port**: Port number on which other system receives SIP requests from Session Manager. For Communication Manager, this must match **Near-end Listen Port** defined on the Communication Manager signaling group in **Section 5.6**.
- **Connection Polity**: Select **Trusted**.
- Click **Commit** to save.

The following screens illustrate Entity Links to Communication Manager and Avaya SBCE. For the compliance testing, **TCP/5060** was used for the connection to Communication Manger and UCP/5060 was used for the connection to Avaya SBCE.

Entity Link to Communication Manager:



Entity Link to Avaya SBCE:



6.7. Add Routing Policies

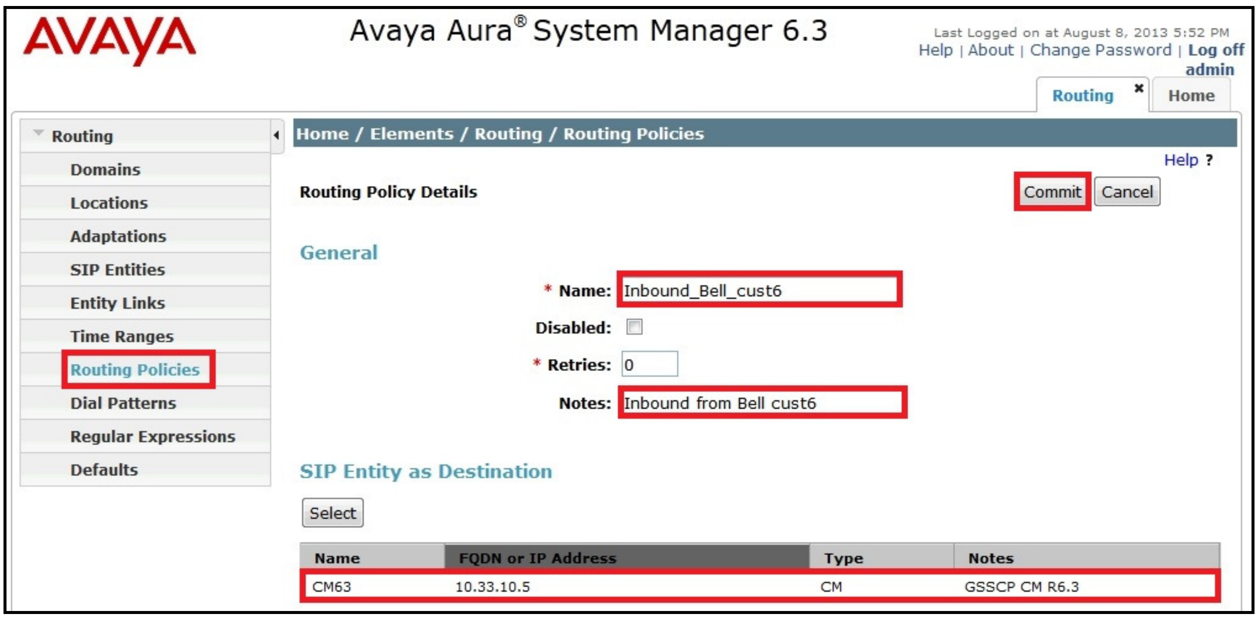
Routing policies describe the conditions under which calls will be routed to SIP Entities specified in **Section 6.5**. Two routing policies must be added: one for Communication Manager and one for Avaya SBCE. To add Routing Policy, navigate to **Routing → Routing Policies** in the left navigation pane and click on **New** button in the right pane (not shown). The following screen is displayed.

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

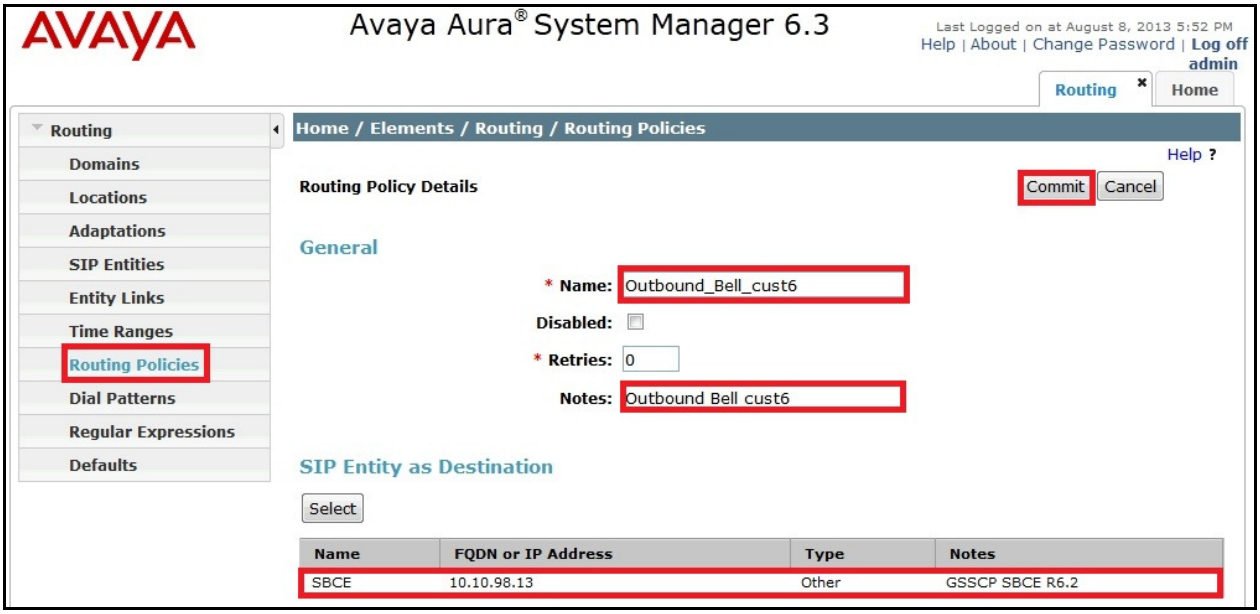
- **Name:** Enter a descriptive name.
- **Notes:** Add a brief description (optional).

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

The following screens show Routing Policy **Inbound_Bell_cust6** defined for incoming calls to Communication Manager.



The following screens show Routing Policy **Outbound_Bell_cust6** for outgoing calls to Avaya SBCE.



6.8. Add Dial Patterns

Dial Patterns are needed to route specific calls through Session Manager. For the compliance testing, dial patterns were needed to route calls from Communication Manager to Bell Canada 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 the **New** button in the right pane (not shown).

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

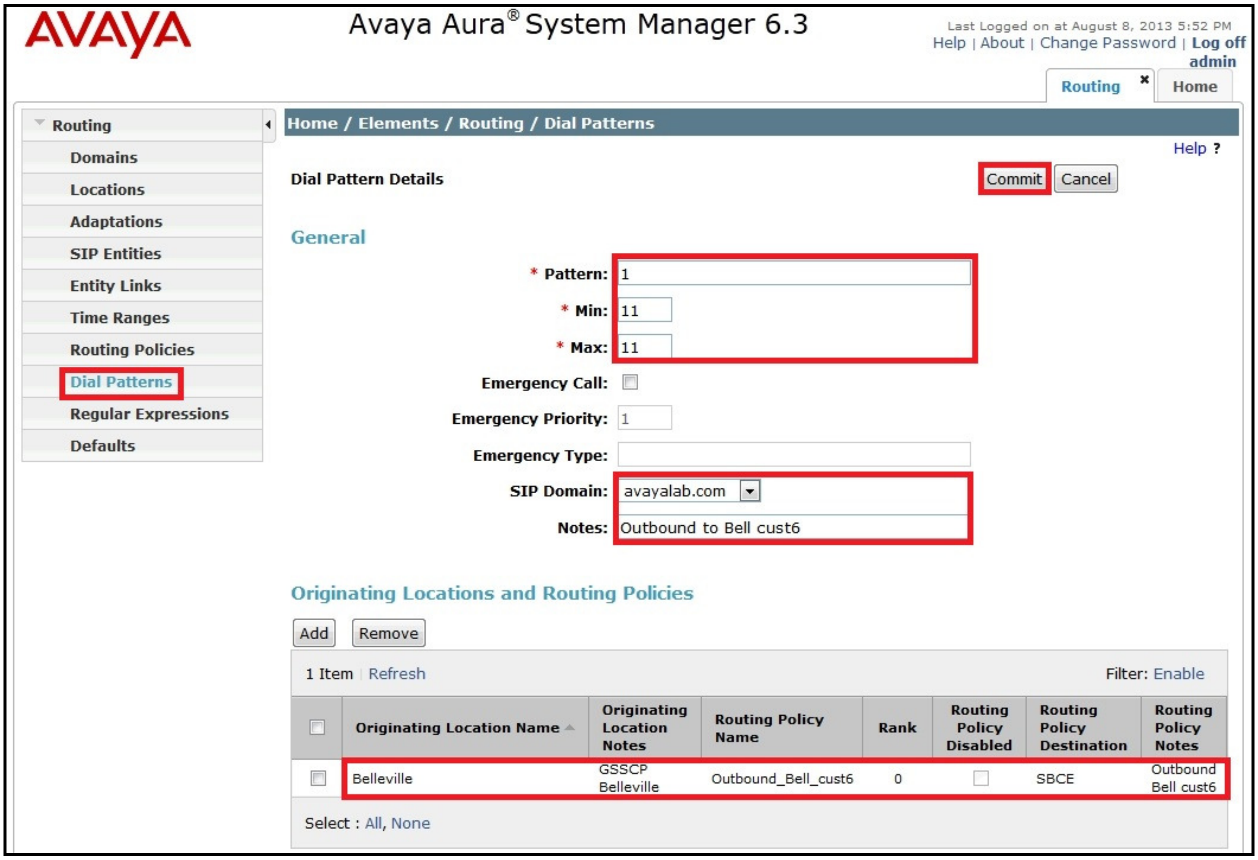
- **Pattern**: Enter a dial string that will be matched against the "Request-URI" of the call.
- **Min**: Enter a minimum length used in the match criteria.
- **Max**: Enter a maximum length used in the match criteria.
- **SIP Domain**: Enter the destination domain used in the match criteria.
- **Notes**: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

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

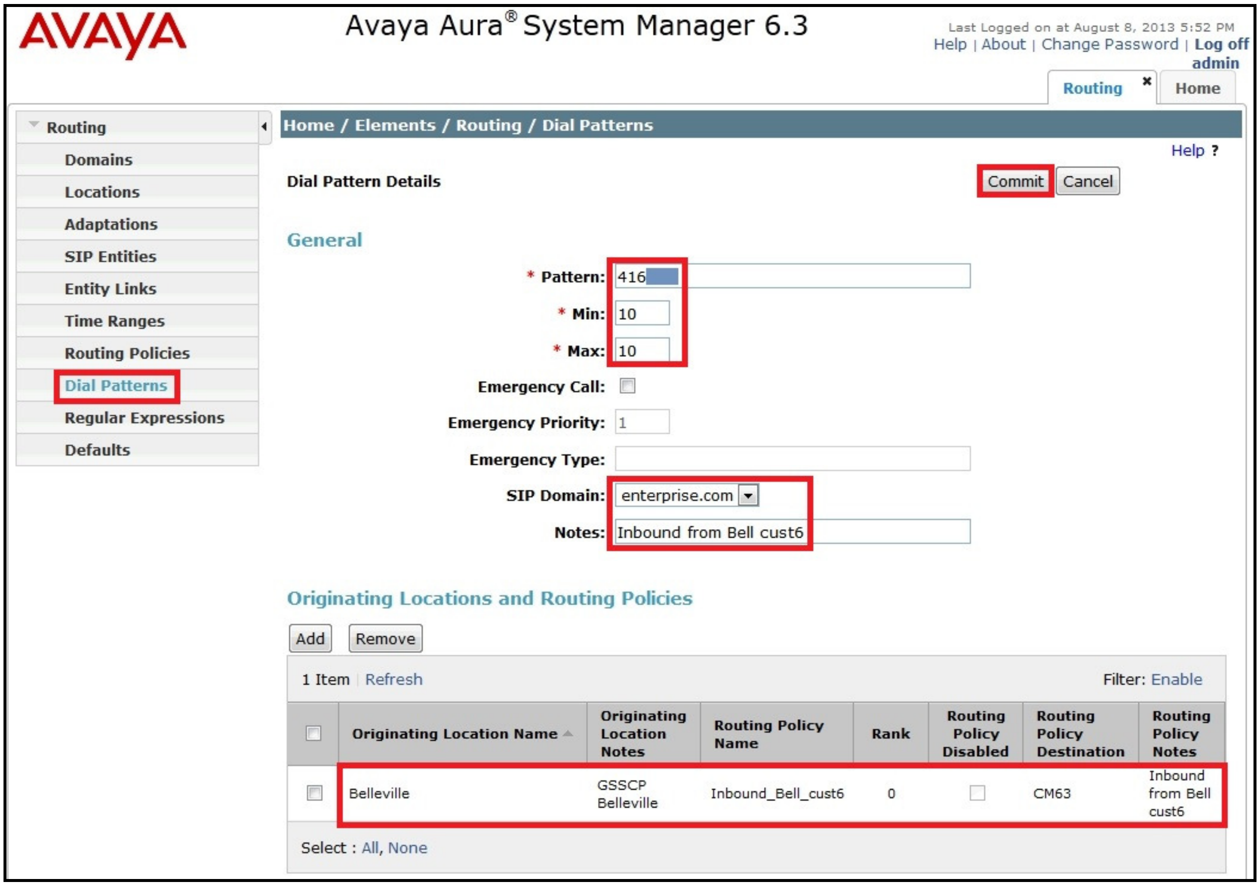
Default values can be used for the remaining fields. Click **Commit** to save.

Two examples of the dial patterns used for the compliance testing are shown below, one for outgoing calls with prefix **1** from the enterprise to the PSTN and one for incoming calls with prefix **416XXX** from PSTN to the enterprise. Other dial patterns, e.g. 011 international calls, 411 directory assistance calls, etc., were similarly defined.

The first example shows that 11-digit dialed numbers that begin with **1** and a destination domain **avayalab.com** uses route policy **Outbound_Bell_cust6** as defined in **Section 6.7**.



The second example shows that inbound 10-digit numbers that start with **416XXX** to domain **enterprise.com** uses route policy **Inbound_Bell_cust6** as defined in **Section 6.7**. These are the DID numbers assigned to the enterprise by Bell Canada.



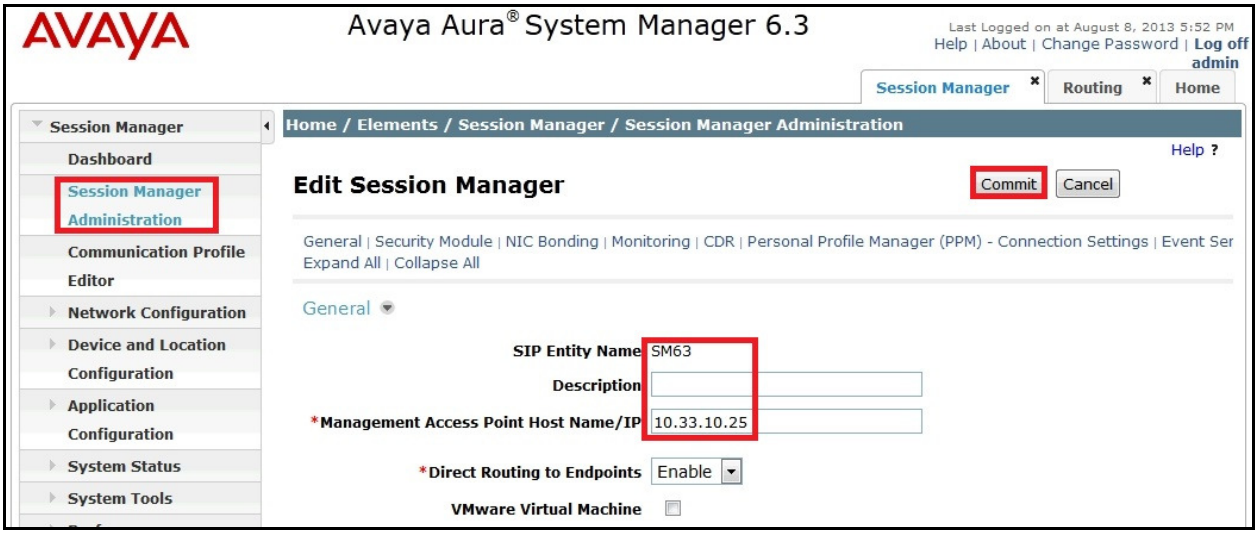
6.9. Add/View Session Manager

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

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

- **SIP Entity Name**: Select SIP Entity **SM63** created for Session Manager.
- **Description**: Add a brief description (optional).
- **Management Access Point Host Name/IP**: Enter IP address of the Session Manager management interface.

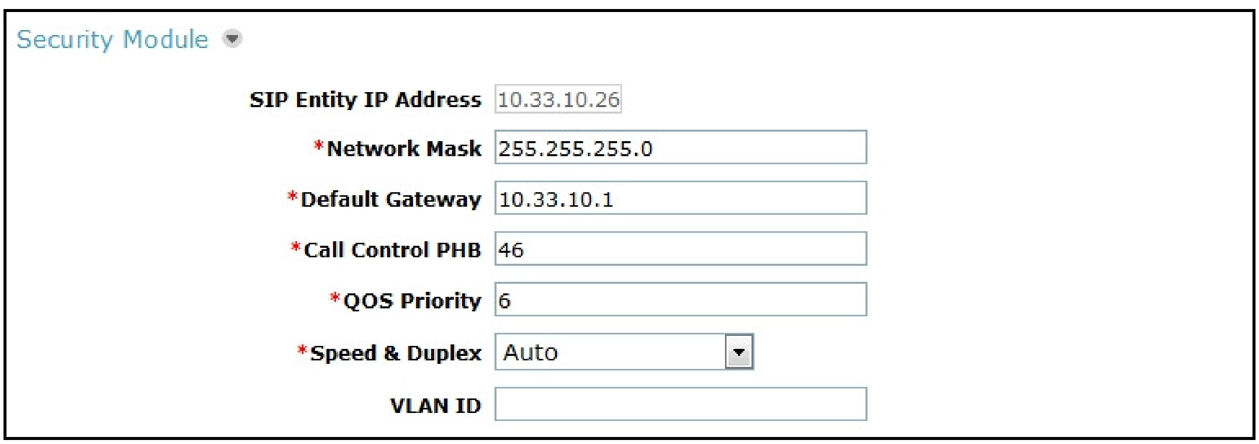
The screen below shows the Session Manager values used for the compliance testing.



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

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

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



7. Configure Avaya Session Border Controller for Enterprise

This section covers the configuration of Avaya SBCE. It is assumed that software has already been installed. For additional information on these configuration tasks, see Error! Reference source not found. **[9]**, **[10]** and **[11]**.

The compliance testing comprised configuration for two major components, Trunk Server for service provider and Call Server for the enterprise. Each component consists of a set of Global

Profiles, Domain Policies and Device Specific Settings. The configuration was defined in Avaya SBCE web user interface as described in following sections.

Trunk Server configuration elements for service provider – Bell Canada:

- Global Profiles:
  - URI Groups
  - Routing
  - Topology Hiding
  - Server Interworking
  - Signaling Manipulation
  - Server Configuration
- Domain Policies:
  - Application Rules
  - Media Rules
  - Signaling Rules
  - Endpoint Policy Group
  - Session Policy
- Device Specific Settings:
  - Network Management
  - Media Interface
  - Signaling Interface
  - End Point Flows → Server Flows
  - Session Flows

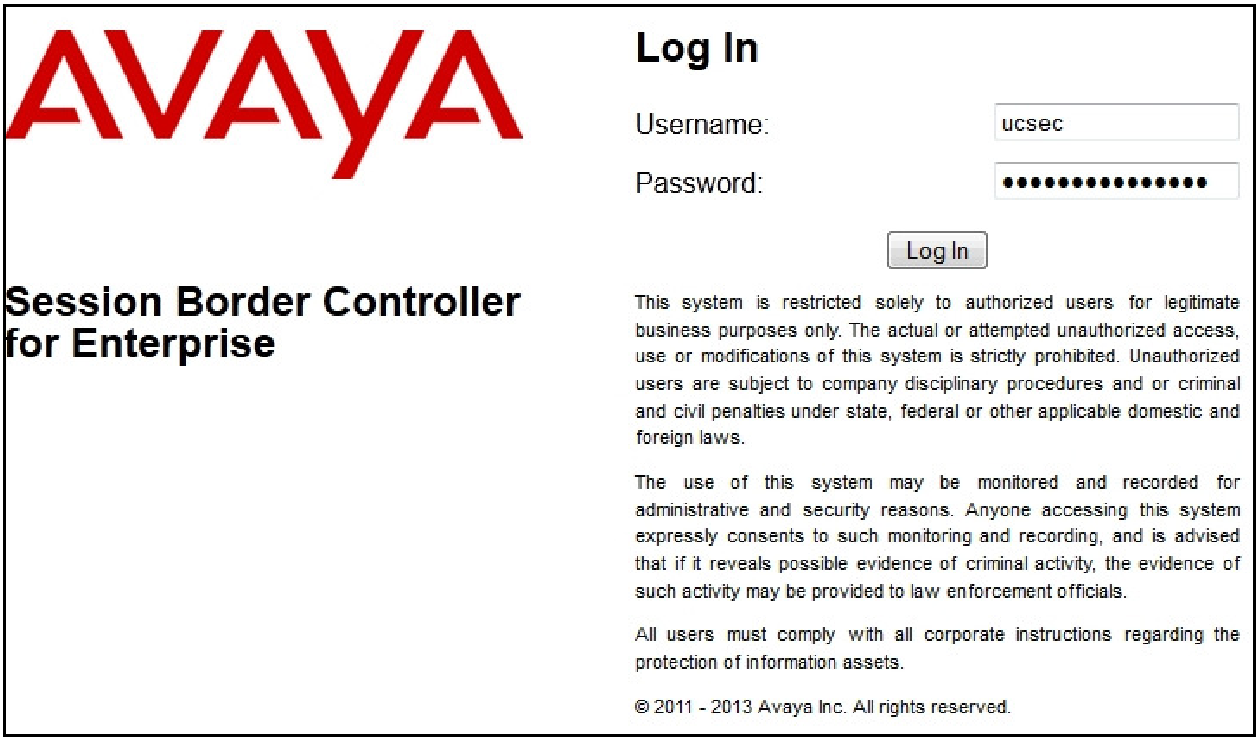
Call Server configuration elements for the enterprise – Session Manager:

- Global Profiles:
  - URI Groups
  - Routing
  - Topology Hiding
  - Server Interworking
  - Server Configuration
- Domain Policies:
  - Application Rules
  - Media Rules
  - Signaling Rules
  - Endpoint Policy Group
  - Session Policy
- Device Specific Settings:
  - Network Management
  - Media Interface
  - Signaling Interface
  - End Point Flows → Server Flows
  - Session Flows

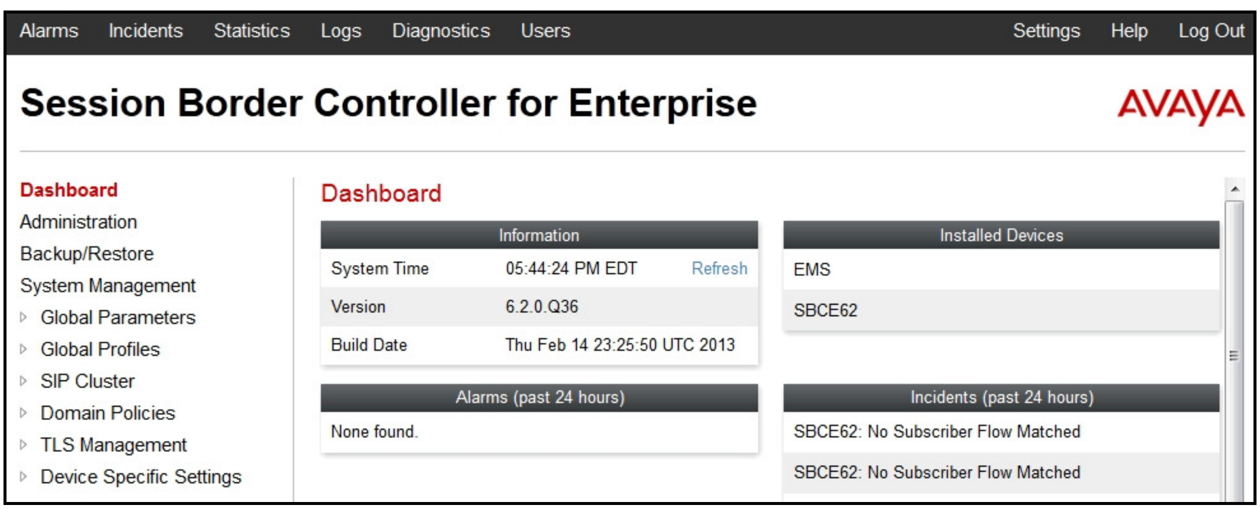
7.1. Log into Avaya Session Border Controller for Enterprise

Use a web browser to access Avaya SBCE web interface, enter https://<ip-addr>/sbc in the address field of web browser, where <ip-addr> is the management IP address.

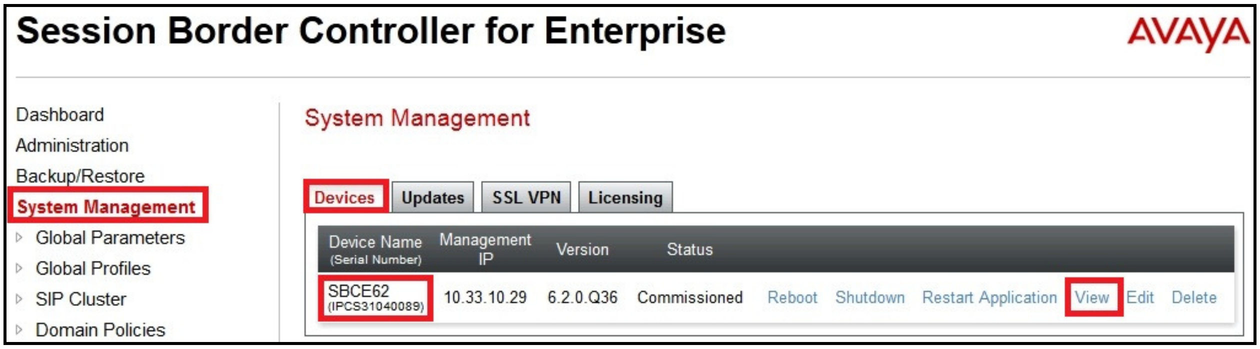
Enter appropriate credentials then click **Log In**.



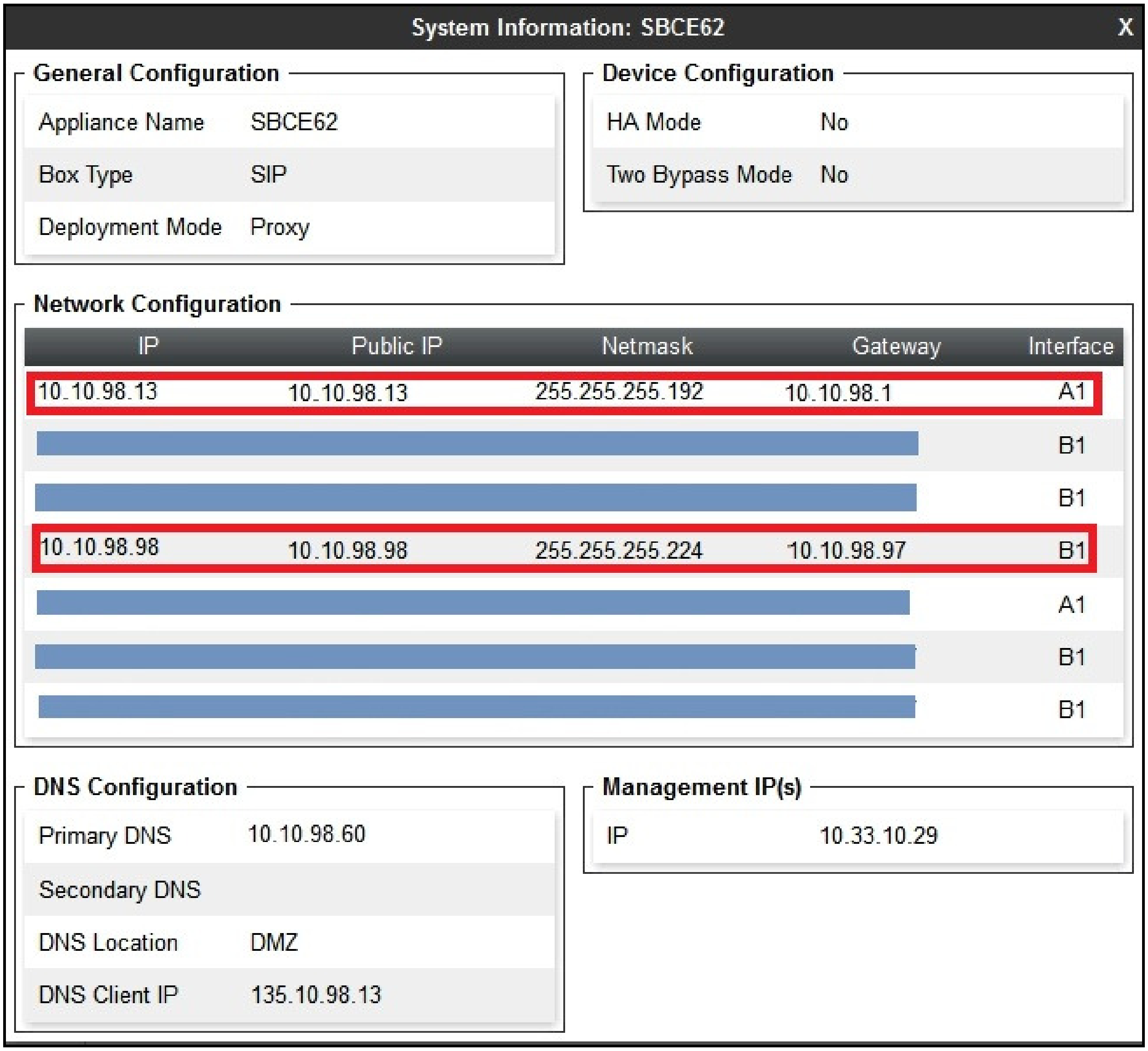
Dashboard main page will appear as shown below.



To view system information that has been configured during installation, navigate to **System Management**. A list of installed devices is shown in the right pane. In the compliance testing, a single Device Name **SBCE62** was already added. To view the configuration of this device, click **View** as shown in the screenshot below.



System Information screen shows **Network Settings**, **DNS Configuration** and **Management IP** information provided during installation and corresponded to **Figure 1**. **Box Type** was set to **SIP** and **Deployment Mode** was set to **Proxy**. Default values were used for all other fields.



7.2. Global Profiles

Global Profiles allows for configuration of parameters across all Avaya SBCE appliances.

7.2.1. Uniform Resource Identifier (URI) Groups

URI Group feature allows a user to create any number of logical URI groups that are comprised of individual SIP subscribers located in that particular domain or group. These groups are used by the various domain policies to determine which actions (Allow, Block, or Apply Policy) should be used for a given call flow.

To add URI Group, select **Global Profiles → URI Groups** then click **Add** button (not shown).

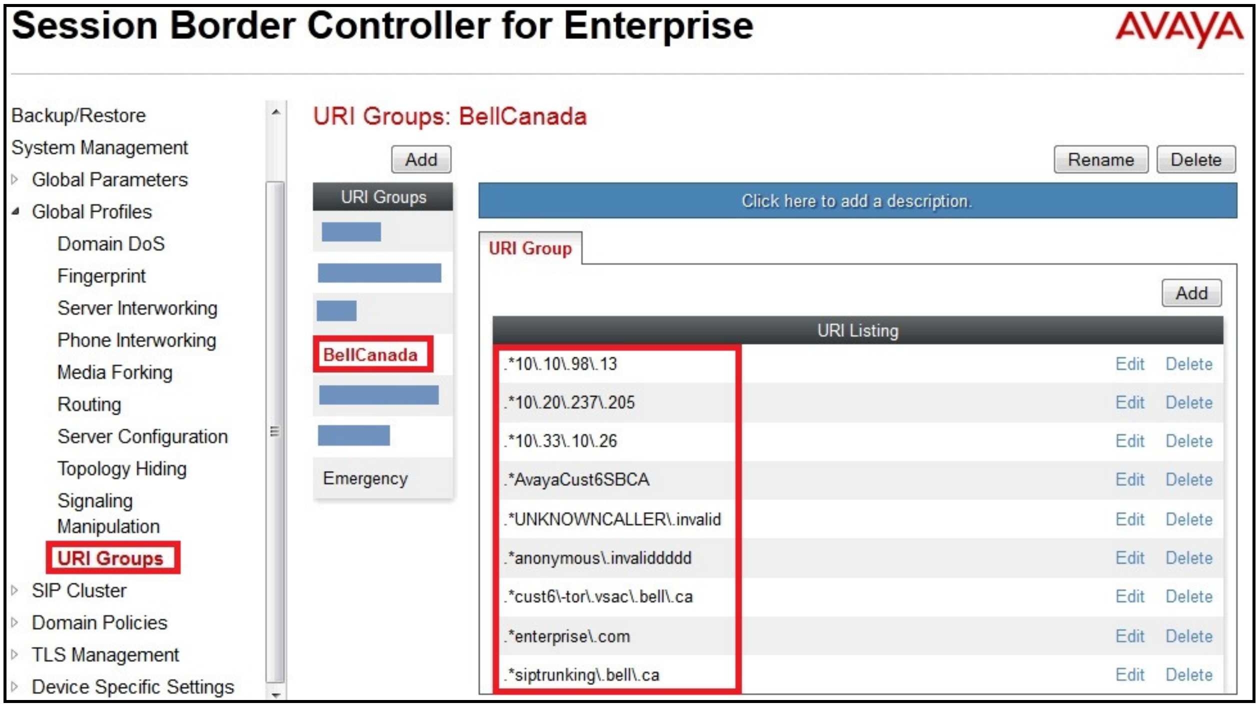
In the compliance testing, URI Group **BellCanada** was added with URI type as **Regular Expression**. It consists of enterprise SIP domains "**.*enterprise\.com**" for regular calls and "**.*nonymous\.invalid**", "**.*UNKNOWNCALLER\.invalid**" for private calls, service provider SIP domains "**.*cust6\xxxx\.xxxx\.bell\.ca**" and "**.*sipxxxxxxxx\.bell\.ca**", IP addresses based URI-Host of the OPTIONS heartbeat originated by Session Manager "**.*10\.33\.10\.26**" and "**.*10\.10\.98\.13**". The OPTIONS heartbeat originated by service provider has SIP domains as ".***AvayaCust6SBCA**".

SIP domain "**.*nonymous\.invalid**" was defined for private outgoing calls from Communication Manager which URI-Host was masked to **anonymous.invalid** while SIP domain "**.*UNKNOWNCALLER\.invalid**" was defined for private incoming call form Bell Canada with URI-Host was marked to **UNKNOWNCALLER.invalid**. The enterprise SIP domain "**.*enterprise\.com**" was defined as per description in **Section 6.2** for enterprise SIP traffic originated from Commutation Manager over the SIP Trunk. For the public SIP Trunk between Avaya SBCE and Bell Canada, the URI-Host in the "From", "PAI", and "Diversion" headers, presents SIP domain **cust6xxxx.xxxx.bell.ca** while the URI-Host in the "Request-URI" and "To" headers, will have SIP domain **sipxxxxxxxx.bell.ca**. These domains are assigned by Bell Canada. The IP addresses and value of URI-Host in OPTIONS heartbeat were also defined for routing incoming and outgoing OPTIONS between Session Manager and Bell Canada.

URI-Group **BellCanada** was used to match the "From" and "To" headers in a SIP call dialog received from both Session Manager and Bell Canada. If there is a match, Avaya SBCE will apply appropriate Routing profile (see **Section 7.2.2**) and Server Flow (see **Section 7.4.4**) to route incoming and outgoing calls to the right destinations.

Note: For the compliance testing, the addition of URI-Group is optional to isolate incoming and outgoing calls between Bell Canada and Avaya lab which is a shared testing environment. For the field deployment, the use of URI-Group may not be required.

The screenshot below illustrates the URI listing for URI Group **BellCanada**.



7.2.2. Routing Profiles

Routing profiles define a specific set of packet routing criteria that are used in conjunction with other types of domain policies to identify a particular call flow and thereby ascertain which security features will be applied to those packets. Parameters defined by Routing profiles include packet transport settings, name server addresses and resolution methods, next hop routing information and packet transport types.

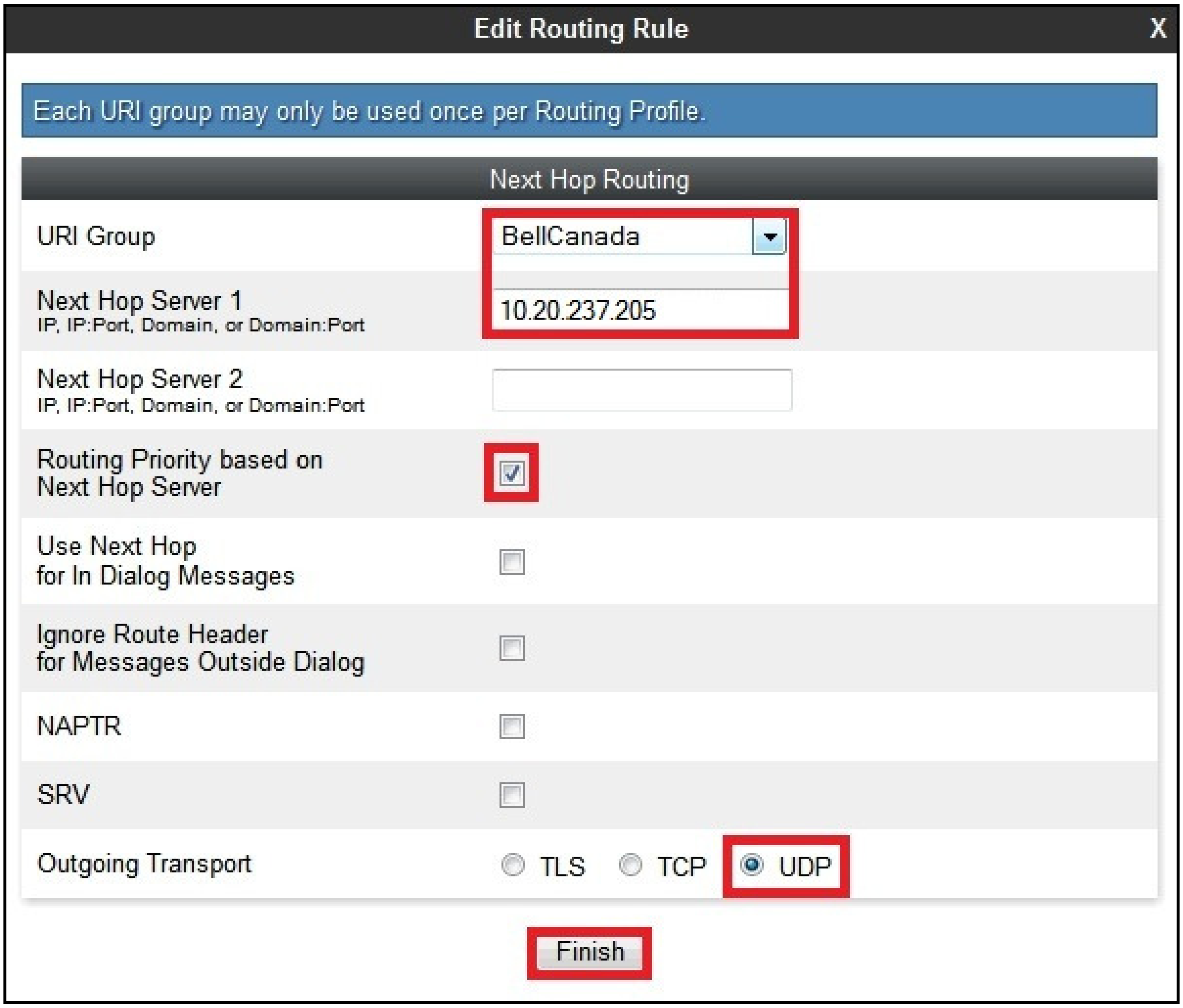
To create Routing profile, select **Global Profiles → Routing** then click **Add** button (not shown).

In the compliance testing, Routing Profile **To_BellCanada** was created to be used in conjunction with Server Flow (see **Section 7.4.4**) defined for Session Manager. This entry is to route outgoing calls from the enterprise to Bell Canada.

In the opposite direction, Routing profile **To_SM** was created to be used in conjunction with a Server Flow (see **Section 7.4.4**) defined for Bell Canada. This entry is to route incoming calls from Bell Canada to the enterprise.

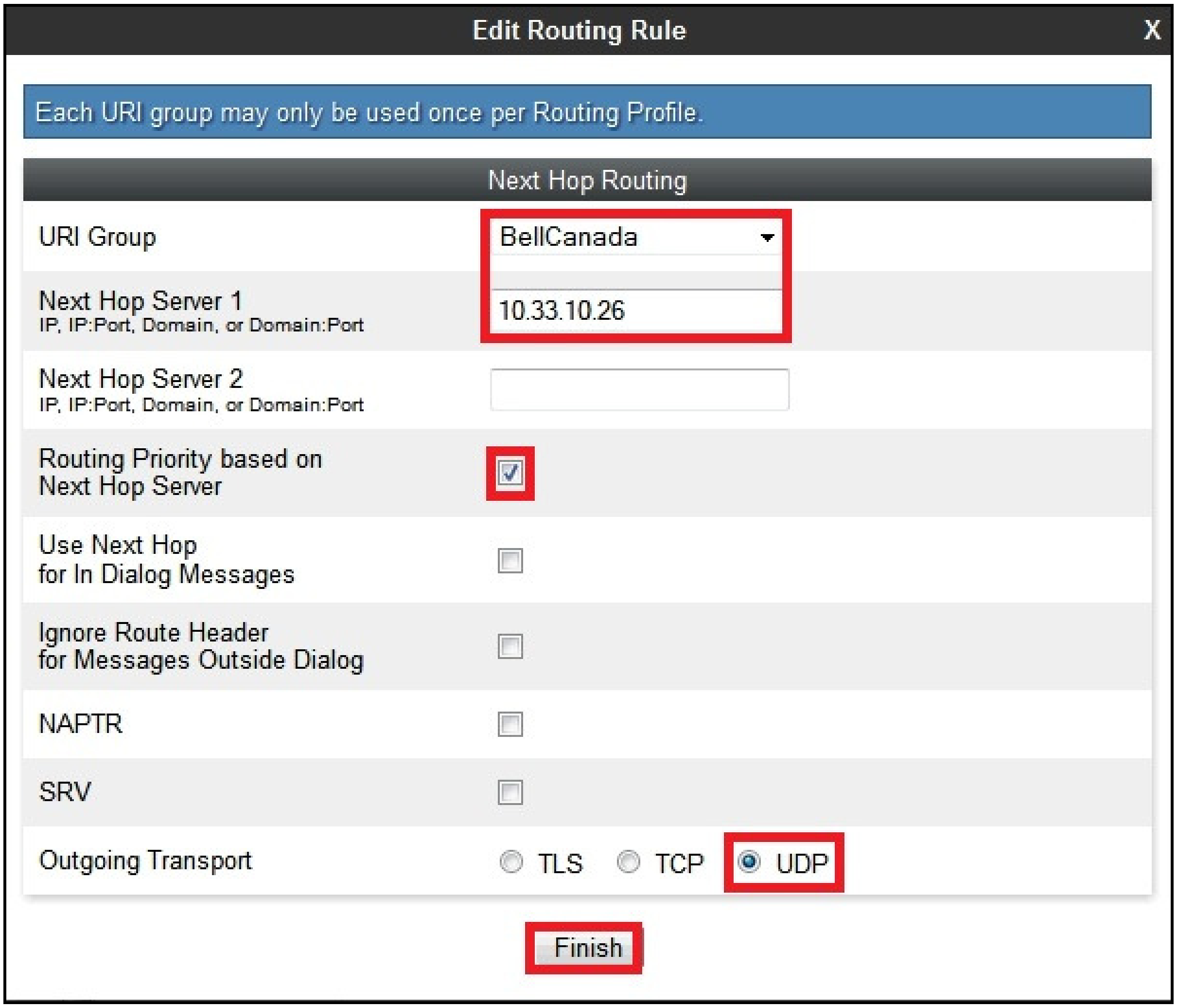
7.2.2.1 Routing Profile for Bell Canada

To display **Edit Routing Rule** dialog of Routing profile **To_BellCanada**, select **Global Profiles → Routing**: **To_BellCanada**. As shown in the screenshot below, if there is a match in the SIP domain of the "To" header with the URI Group **BellCanada** defined in **Section 7.2.1**, outgoing calls will be routed to **Next Hop Server 1** as defined as **10.20.237.205** which is the IP address of Bell Canada Trunk Server, on implied default port **5060**. As shown in **Figure 1**, Bell Canada SIP Trunking Service was connected with transportation protocol **UDP**. The other options were kept as default.



7.2.2.2 Routing Profile for Session Manager

Similarly, Routing profile **To_SM** was created to route incoming calls to the **Next Hop Server 1** as defined as **10.33.10.26** which is the IP address of Session Manager, on implied default port **5060** if there is a match on the SIP domain of the "To" header with the URI Group **BellCanada** defined in **Section 7.2.1**. As shown in **Figure 1**, Session Manager was connected with transportation protocol **UDP**. To display **Edit Routing Rule** dialog of Routing profile **To_SM**, select **Global Profiles → Routing**: **To_SM** then click **Edit** (not shown).



7.2.3. Topology Hiding

Topology Hiding is a security feature of Avaya SBCE which allows changing certain key SIP message parameters to 'hide' or 'mask' how the enterprise network may appear to an unauthorized or malicious user.

To create Topology Hiding profile, select **Global Profiles → Topology Hiding** then click **Add** button (not shown).

In the compliance testing, two Topology Hiding profiles were created: **To_BellCanada** and **To_SM**.

7.2.3.1 Topology Hiding Profile for Bell Canada

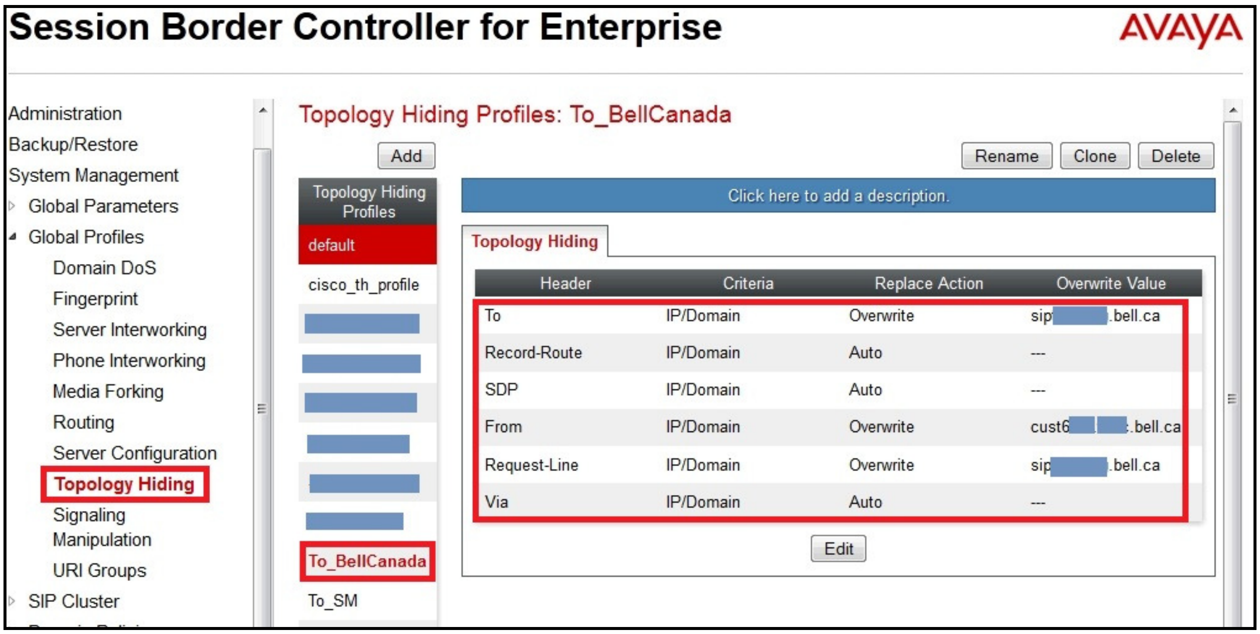
Topology Hiding profile **To_BellCanada** was defined for outgoing calls to Bell Canada to:

- Mask URI-Host of the "Request-URI" and "To" headers with service provider SIP domain **sipxxxxxxxx.bell.ca** to meet the requirements of Bell Canada. This can be done by selecting **Overwrite** for **Replace Action** setting.

- Mask URI-Host of the “From” header with service provider SIP domain **cust6xxxx.xxxx.bell.ca**. This can be done by selecting **Overwrite** for **Replace Action** setting.
- Change the “Record-Route”, “Via” headers and SDP added by Session Manager, with the outside IP address of Avaya SBCE which is known to Bell Canada.

This implementation is to secure the enterprise network topology and also to meet SIP requirements from service provider.

The screenshots below illustrate Topology Hiding profile **To_BellCanada**.

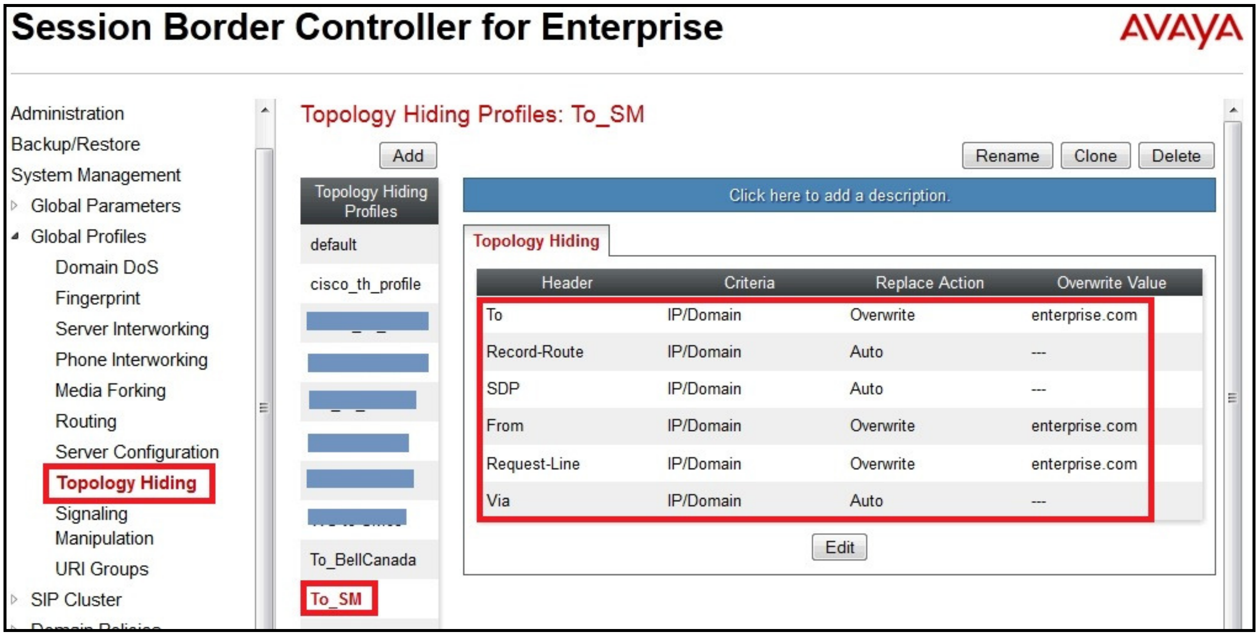


7.2.3.2 Topology Hiding Profile for Session Manager

Topology Hiding profile **To_SM** was defined for incoming calls to Session Manager to:

- Mask URI-Host of the “Request-URI”, “To”, and “From” headers with the enterprise SIP domain **enterprise.com**.
- Change the “Record-Route”, “Via” headers and SDP added by Bell Canada with the inside IP address of Avaya SBCE which is known to Communication Manager.

The screenshots below illustrate Topology Hiding profile **To_SM**.



Notes:

- **Criteria** should be **IP/Domain** to allow Avaya SBCE to mask both domain name and IP address presenting in the URI-Host.
- Masking applies to the “From” header also applies to the “Referred-By” and “P-Asserted-Identity” headers.
- Masking applies to the “To” header also applies to “Refer-To” headers.

7.2.4. Server Interworking

Server Interworking profile features are configured differently for Call Server and Trunk Server. To create Server Interworking profile, select **UC-Sec Control Center → Global Profiles → Server Interworking** then click **Add** button (not shown).

In the compliance testing, two Server Interworking profiles **BellCanada** and **SM** were created for Bell Canada (Trunk Server) and Communication Manager (Call Server).

7.2.4.1 Server Interworking profile for Bell Canada

Server Interworking profile **BellCanada** was defined to match SIP specification of Bell Canada. **General** and **Advanced** tabs were configured with following parameters while other tabs **Timers, URI Manipulation** and **Header Manipulation** were kept as default.

General settings:

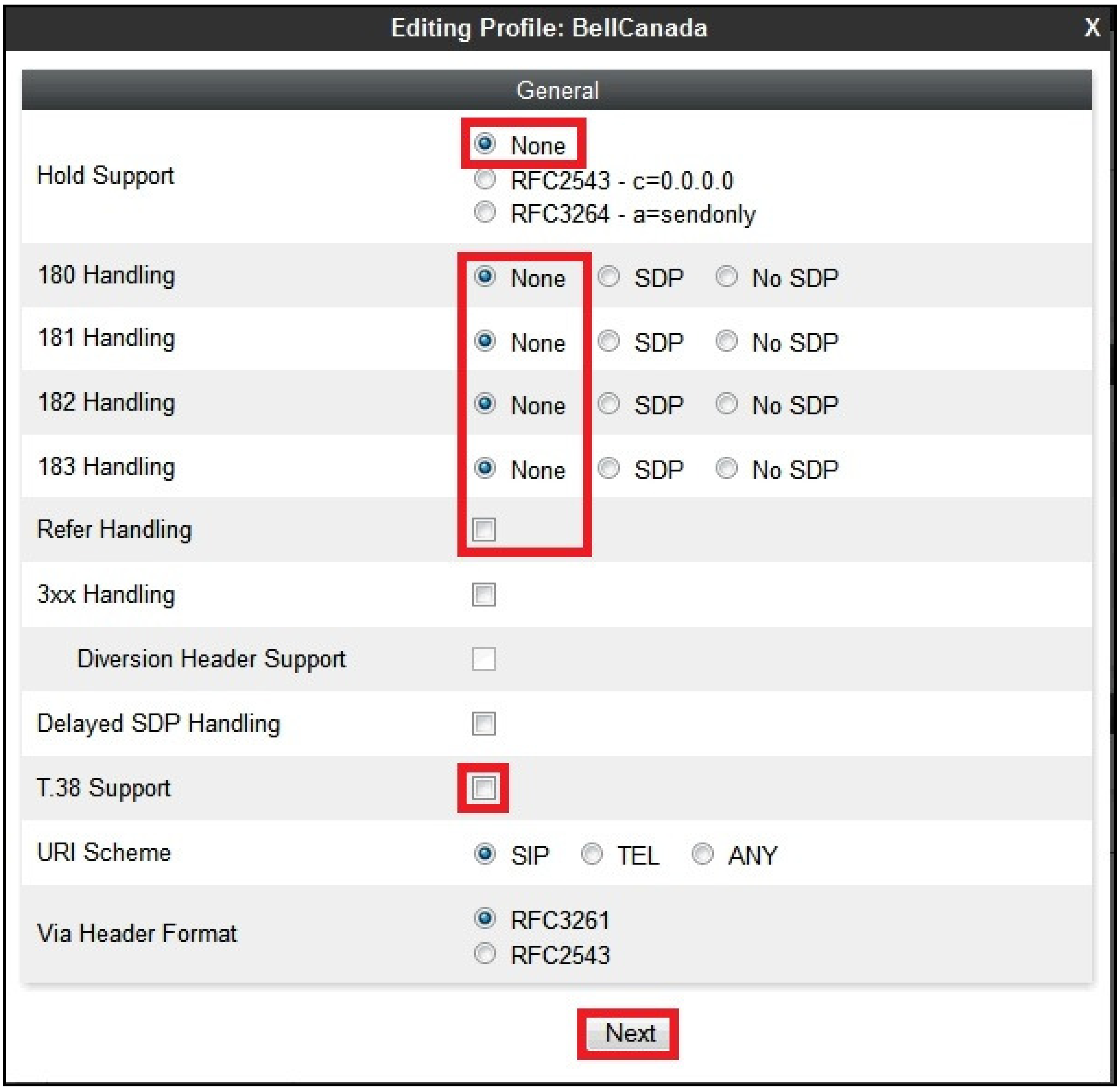
- **Hold Support** = **None**.
- **18X Handling** = **None**.
- **Refer Handling** = **Unchecked**.
- **T.38 Support** = **Unchecked**. Bell Canada did not supported T.38 fax in the compliance testing.

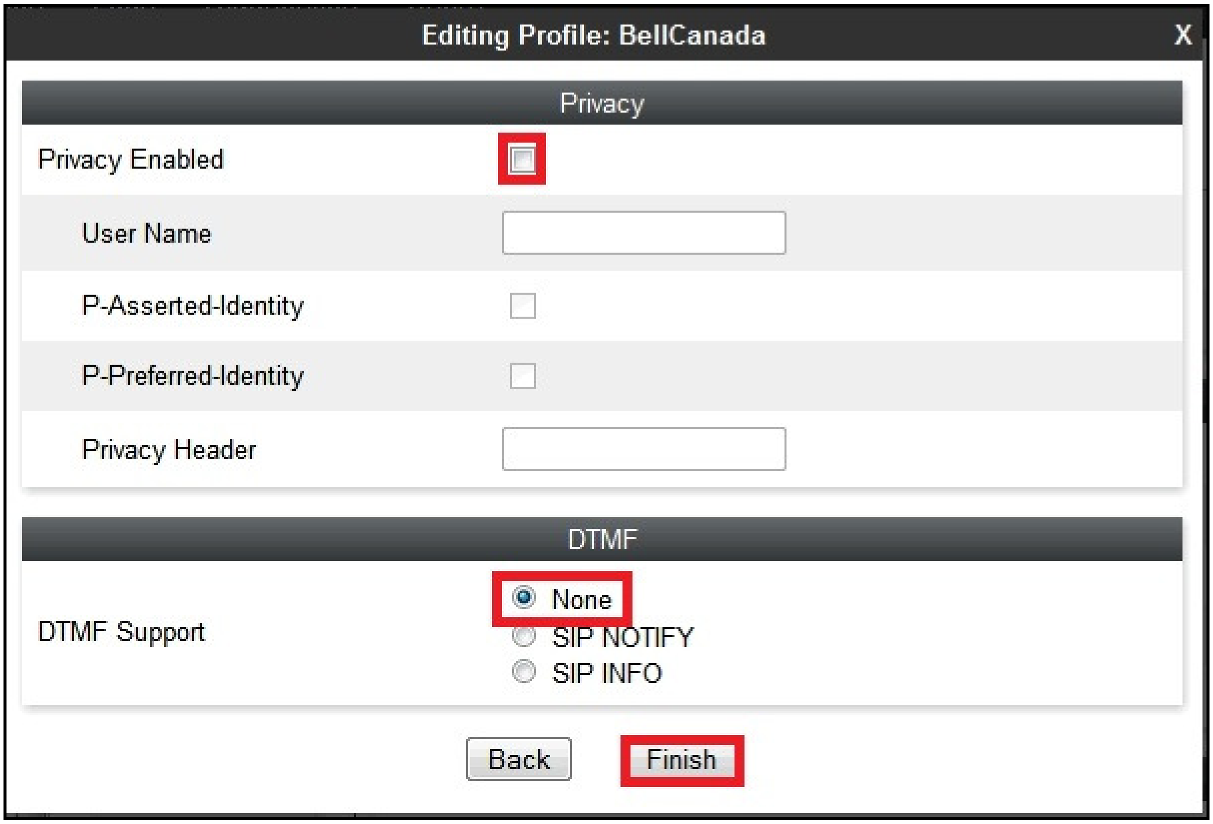
- **Privacy Enabled** = **Unchecked**.
- **DTMF Support** = **None**.

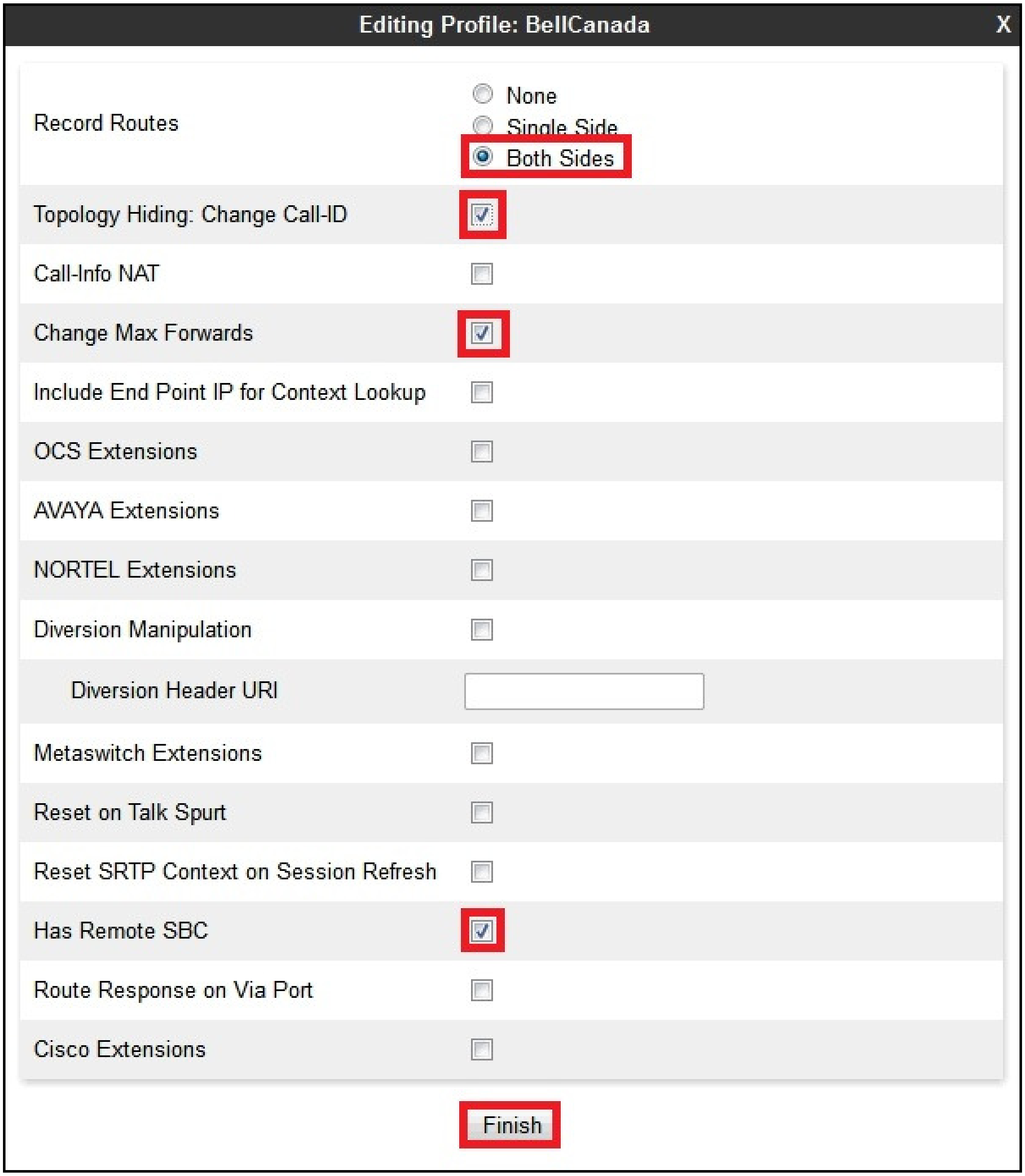
Advanced settings:

- **Record Routes** = **Both Sides**.
- **Topology-Hiding**: **Change Call-ID** = **Checked**.
- **Change Max-Forwards** = **Checked**.
- **Has Remote SBC** = **Checked**.

Server Interworking profile **BellCanada** is shown in the following screenshots.

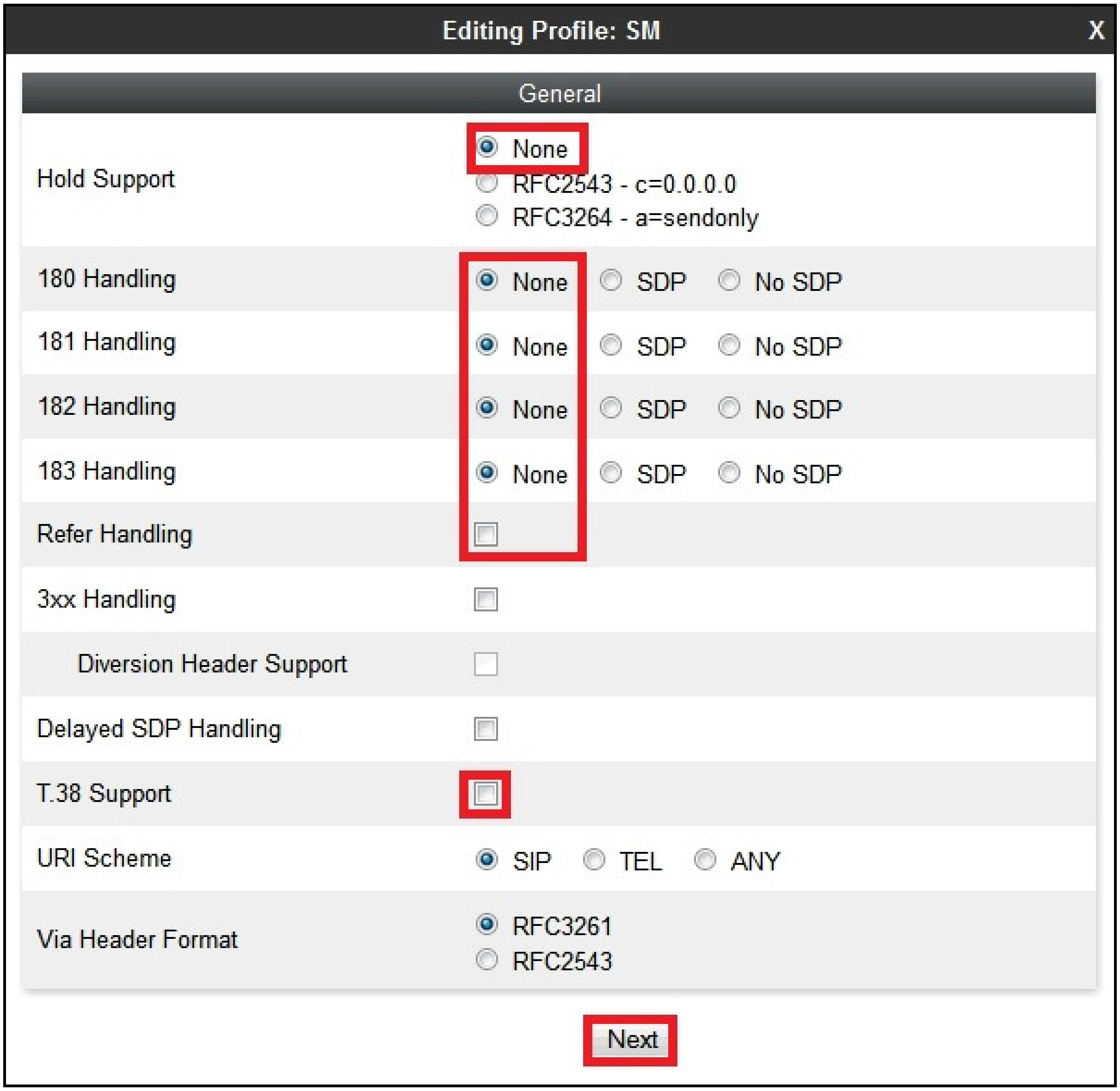


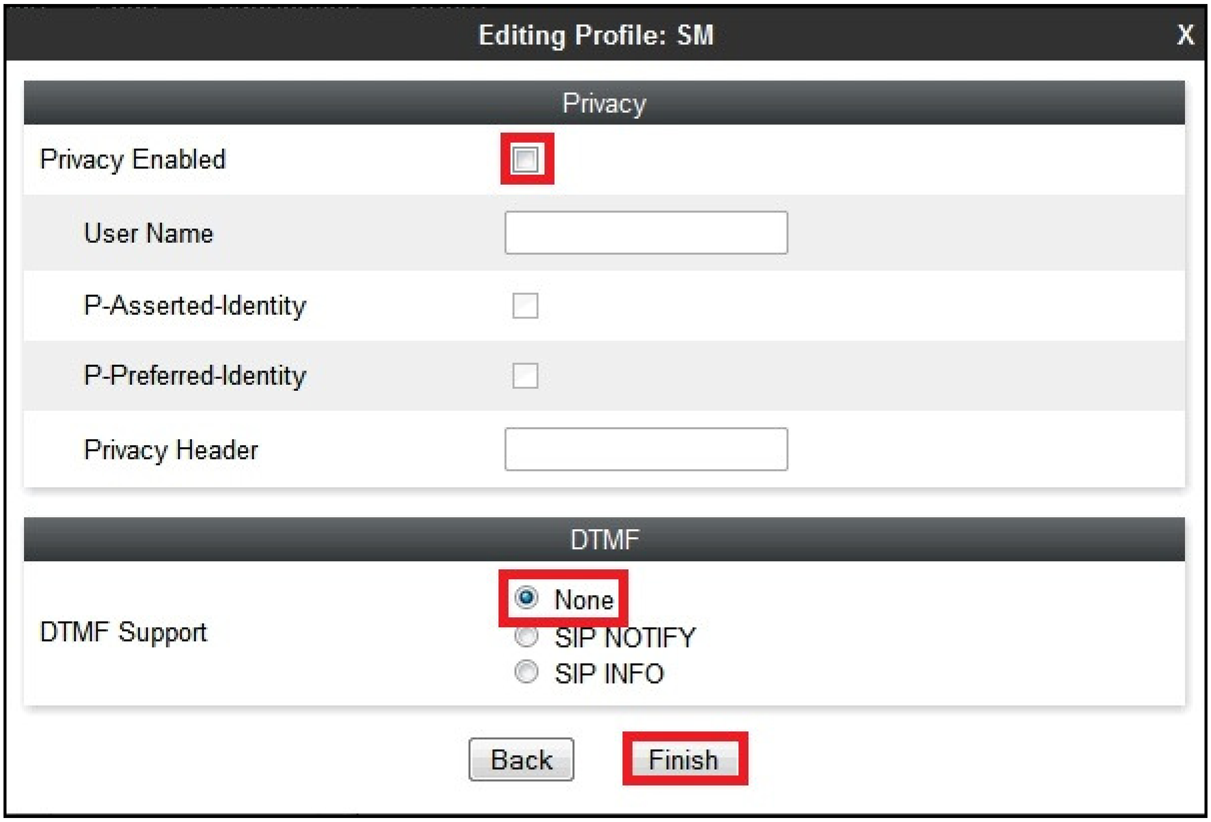

Editing Profile: BellCanada
X
Privacy
Privacy Enabled
User Name
P-Asserted-Identity
P-Preferred-Identity
Privacy Header
DTMF
DTMF Support
None
SIP NOTIFY
SIP INFO
Back
Finish

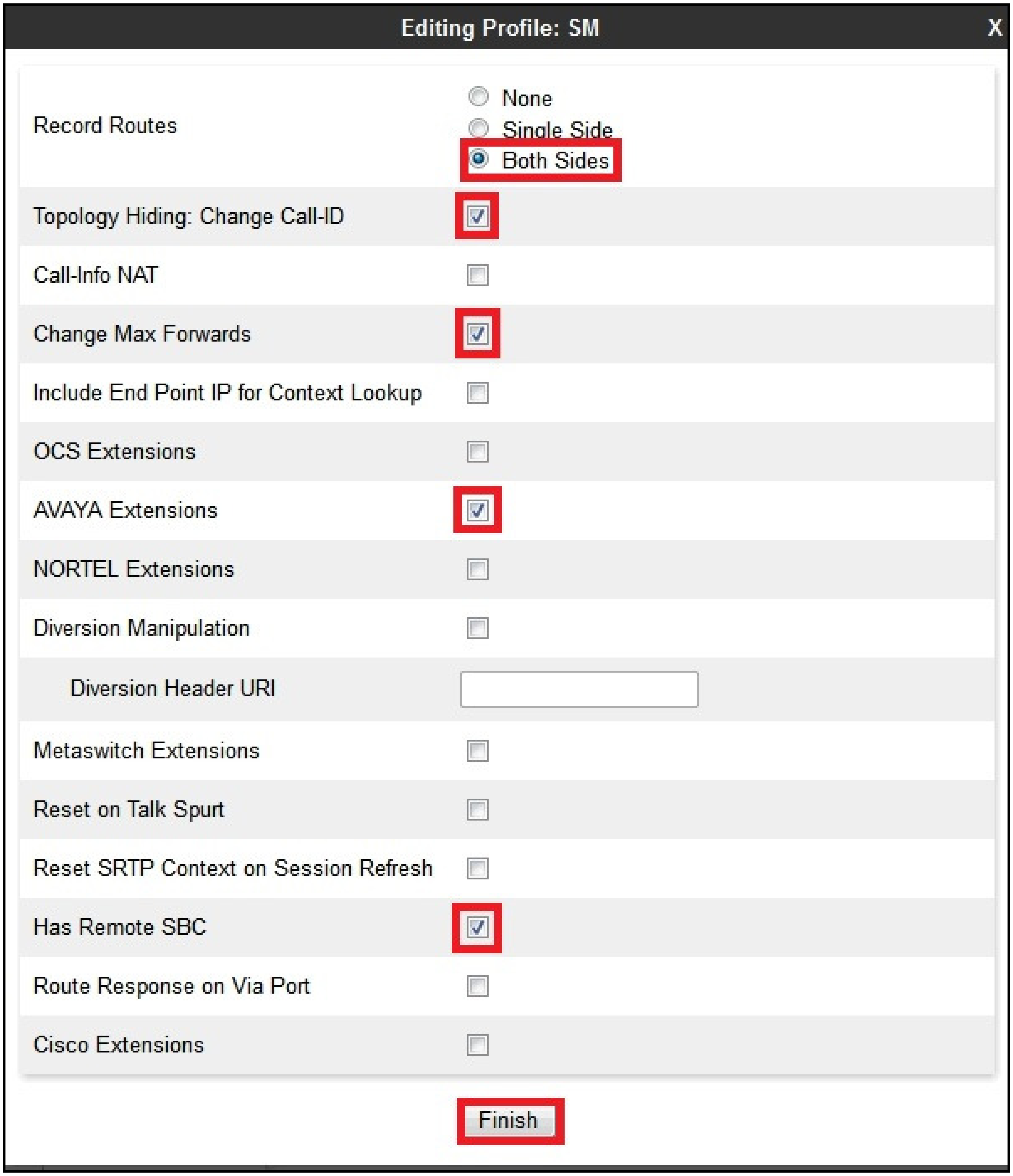


7.2.4.2 Server Interworking profile for Session Manager

Server Interworking profile **SM** shown in the screenshots below, was similarly defined to match the specification of Session Manager with the exception of the support for **Avaya Extensions** was enabled.


Editing Profile: SM
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
3xx Handling
Diversion Header Support
Delayed SDP Handling
T.38 Support
URI Scheme
SIP TEL ANY
Via Header Format
RFC3261
RFC2543
Next


Editing Profile: SM
X
Privacy
Privacy Enabled
User Name
P-Asserted-Identity
P-Preferred-Identity
Privacy Header
DTMF
DTMF Support
None
SIP NOTIFY
SIP INFO
Back
Finish



7.2.5. Signaling Manipulation

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

The SigMa scripting language is designed to express any of the SIP header manipulation operations to be done by Avaya SBCE. Using this language, a script can be written and tied to a given **Server Configuration** which will be configured in the next steps. Avaya SBCE appliance then interprets this script at the given entry point or "hook point".

These Application Notes will not discuss the full feature of **Signaling Manipulation** but will show an example of a script created during compliance testing to aid in **Topology Hiding**.

In this compliance testing, SigMa script **BellCanada** was created to apply to Bell Canada Server Configuration. The script has two portions to normalize the outgoing and incoming call respectively.

Note: the SigMa script for Session Manager is unnecessary since the signaling has already been normalized on the Bell Canada side.

To create **Signaling Manipulation** script, select **UC-Sec Control Center → Global Profiles → Signaling Manipulation**. Click the **Add Script** (not shown).

The detail of SigMa script **BellCanada** is as follows:

```
within session "ALL"
{
act on request where %DIRECTION="OUTBOUND" and %ENTRY_POINT="POST_ROUTING"
         {
          append(%HEADERS["Contact"][1].URI.USER,";tgrp=vsac_416XXX1880_01a;trunk-
context=siptrunking.bell.ca");
         }
 act on message where %DIRECTION="INBOUND" and %ENTRY_POINT="AFTER_NETWORK"
        {
         %HEADERS["From"][1].URI.USER.regex_replace("(\+)","");
         %HEADERS["Contact"][1].URI.USER.regex_replace("(\+)","");
        }
}
```

7.2.5.1 Signaling Manipulation rules for outgoing calls

In **Signaling Manipulation** script **BellCanada** above, the statement **`act on message where %DIRECTION="OUTBOUND" and %ENTRY_POINT="POST_ROUTING"`** is to specify the script will take effect on all type of SIP messages for outgoing calls and the manipulation will be done after routing. The manipulation will be according to the rules contained in this statement.

Bell Canada requires that the "Contact" header must include a pre-defined trunk group ID, this value is obtained by Bell Canada and it is assigned per individual SIP trunk basis. In the certification testing, the trunk group ID was inserted in the "Contact" header as shown the following rule.

```
append(%HEADERS["Contact"][1].URI.USER,";tgrp=vsac_416XXX1880_01a;trunk-
context=siptrunking.bell.ca");
```

7.2.5.2 Signaling Manipulation rules for incoming calls

In Signaling Manipulation script **BellCanada** above, the statement **`act on message where %DIRECTION="INBOUND" and %ENTRY_POINT="AFTER_NETWORK"`** is to specify the script will take effect on all type of SIP messages for incoming calls and the manipulation will be done before routing. The manipulation will be according to the rules contained in this statement.

In the compliance testing, Bell Canada sent “+” sign in URI-User of the “From” and “Contact” headers. Two rules as shown in the screenshot below are added to remove the “+” sign to make the dialing plan compliant to North America numbering.

```
%HEADERS["From"][1].URI.USER.regex_replace("(\+)","");
%HEADERS["Contact"][1].URI.USER.regex_replace("(\+)","");
```

7.2.6. Server Configuration

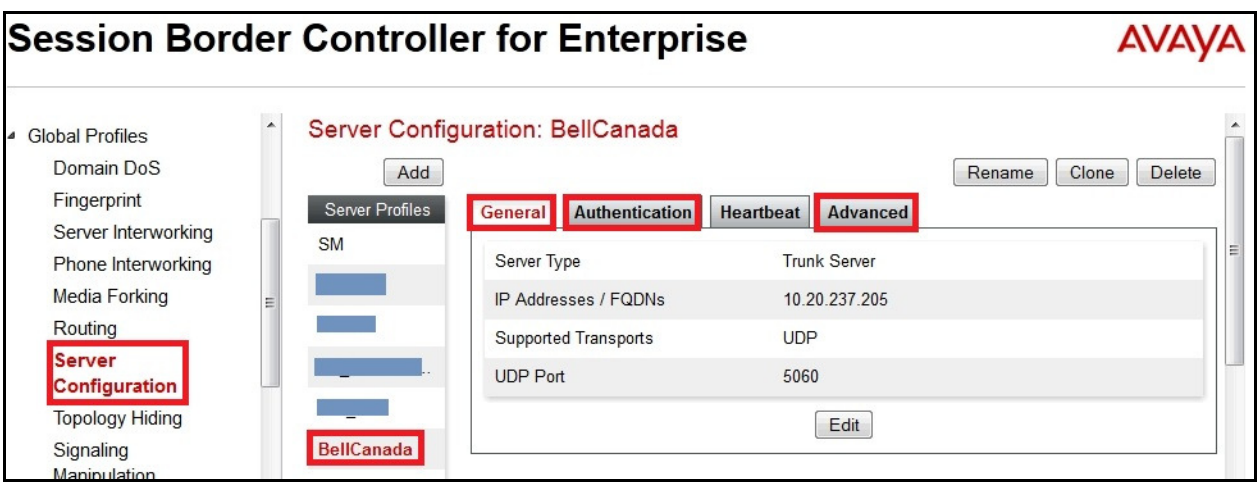
Server Configuration screen contains four tabs: **General**, **Authentication**, **Heartbeat**, and **Advanced**. These tabs are used to configure and manage various SIP Call Server specific parameters such as TCP and UDP port assignments, heartbeat signaling parameters, DoS security statistics and trusted domains.

To create Server Configuration, select **Global Profiles →Server Configuration** then click **Add** button (not shown).

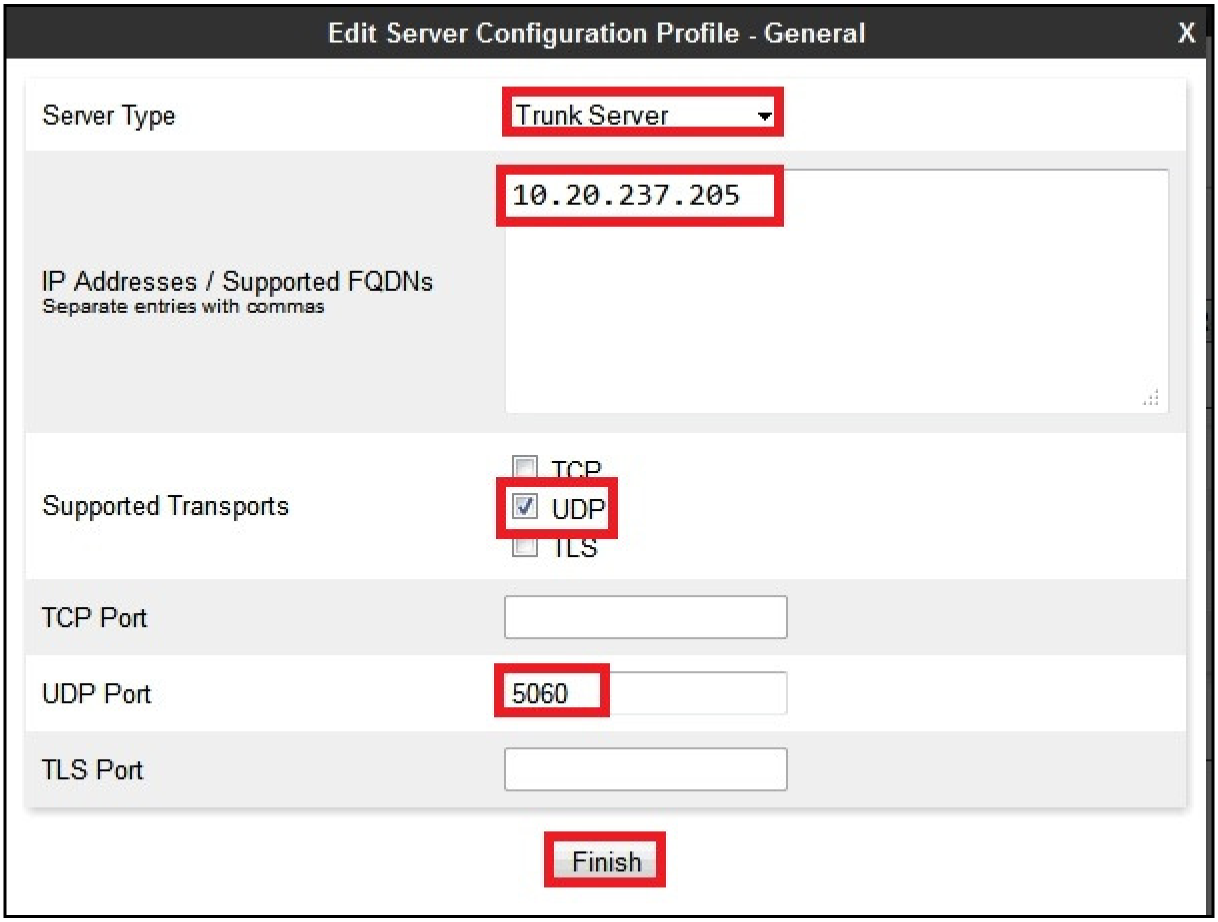
In the compliance testing, two separate Server Configurations were created, server entry **BellCanada** for Bell Canada and server entry **SM** for Session Manager.

7.2.6.1 Server Configuration for Bell Canada

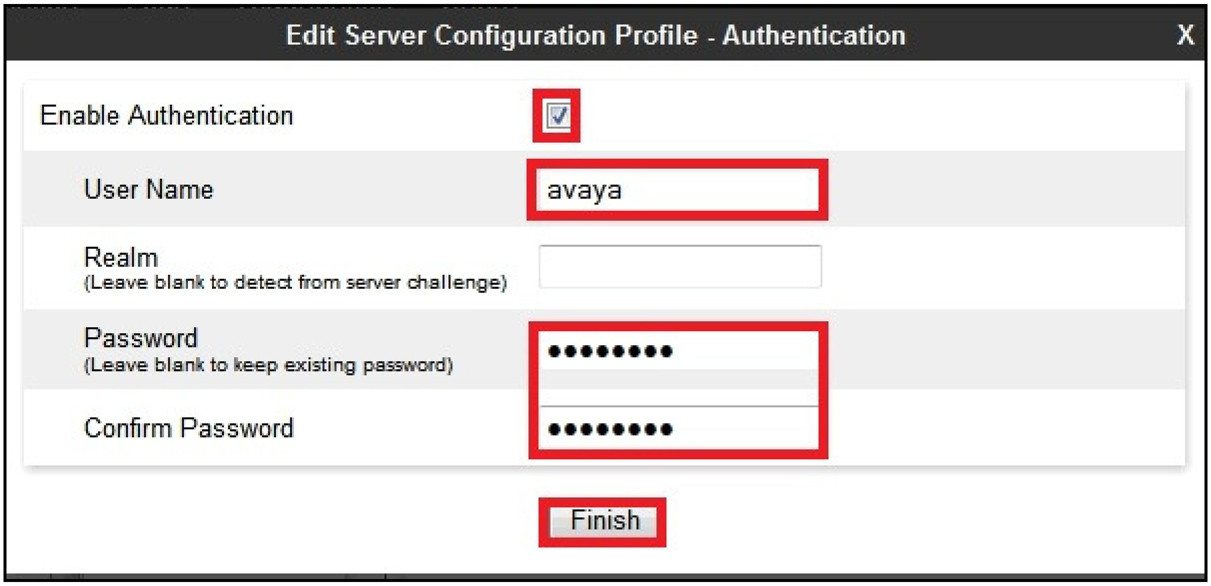
Server Configuration **BellCanada** was added for Bell Canada, it is discussed in detail below. **General**, **Authentication** and **Advanced** tabs were provisioned. **Heartbeat** tab, however, was disabled as default to allow Avaya SBCE to forward the OPTIONS heartbeat originated from Session Manager to Bell Canada (to query for the status of the SIP Trunk).



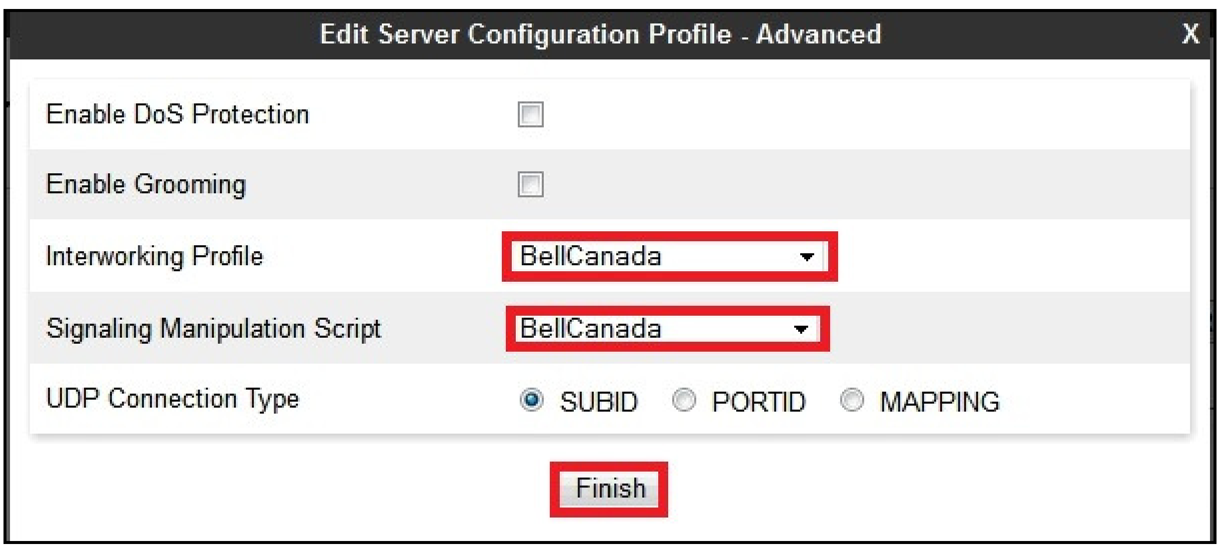
Under **General** tab, specify Server Type for Bell Canada as **Trunk Server**. IP connectivity has also been defined as shown in the screenshot below. In this compliance testing, Bell Canada supported transport protocol **UDP** on IP address **10.20.237.205** and listened on port **5060**.



Authentication tab was configured with **Enable Authentication** selected to allow Avaya SBCE to provide proper credential for Digest Authentication implemented by Bell Canada. Keep **Realm** field as blank as default, but configure the credential which was obtained from service provider, with **User Name avaya** and predefined **Password** for the compliance testing.

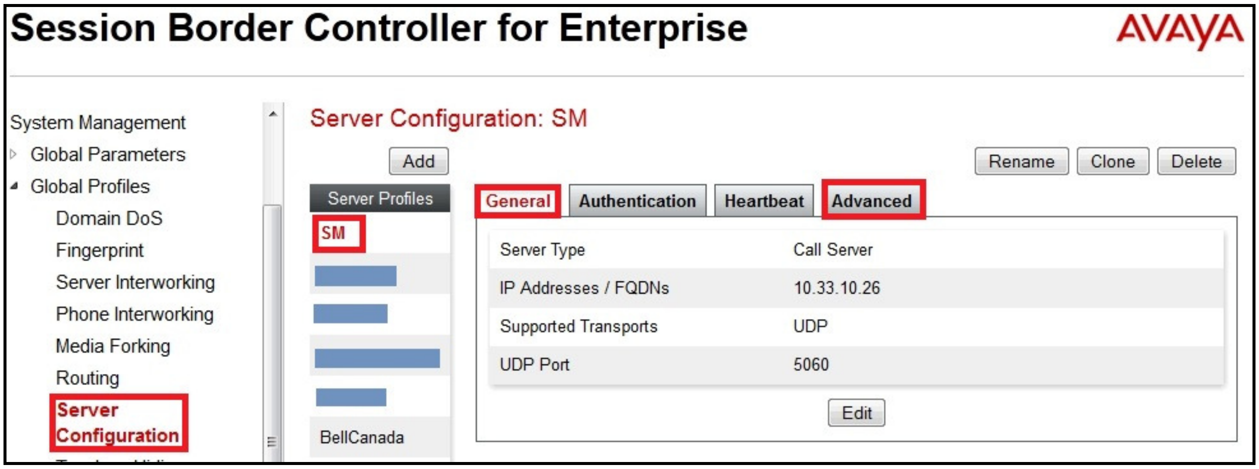


For **Advanced** tab, **Interworking Profile** was set to use **BellCanada** as defined in **Section 7.2.4** and **Signaling Manipulation Script** was set to **BellCanada** as defined in **Section 7.2.5**. Other settings were kept as default.

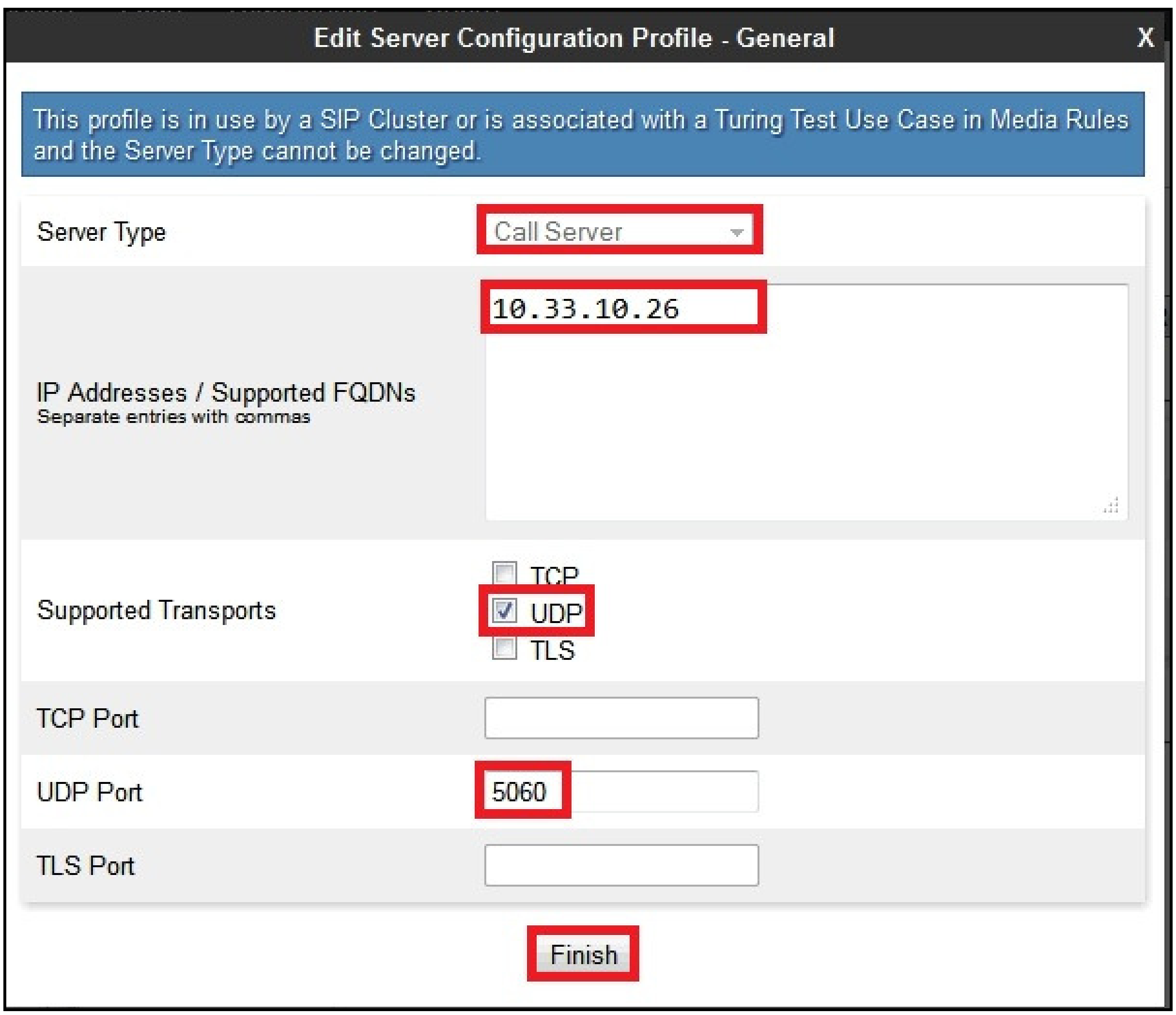


7.2.6.2 Server Configuration for Session Manager

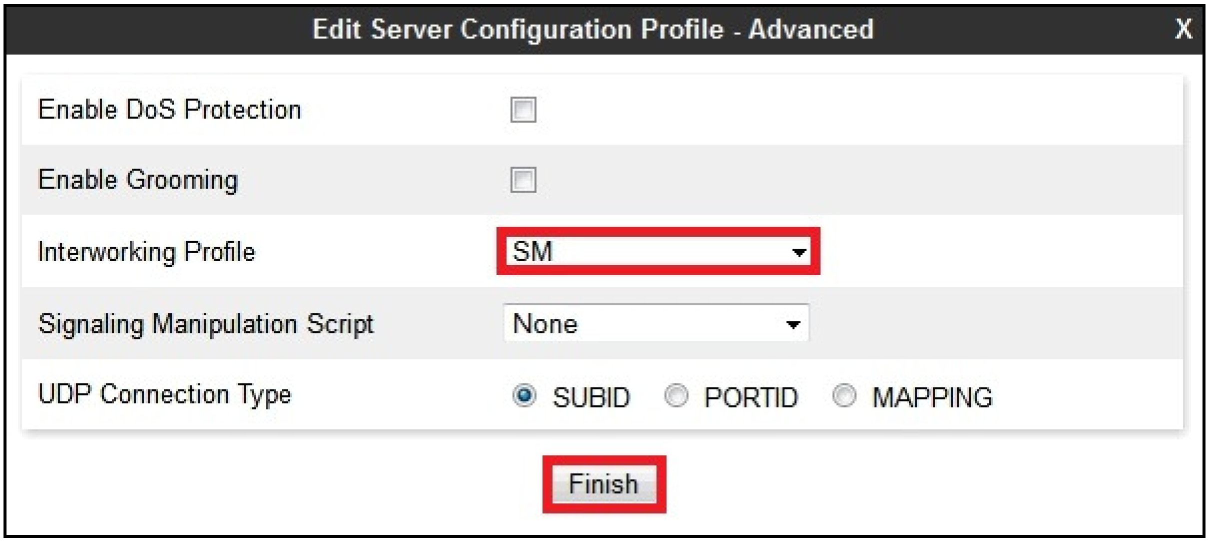
Server Configuration **SM** was similarly created for Session Manager, and is discussed in detail below. Only **General** and **Advanced** tabs required provisioning. **Heartbeat** tab was kept disabled as default to allow Avaya SBCE to forward the OPTIONS heartbeat from Bell Canada to Session Manager (to query for the status of the SIP Trunk).



Under **General** tab, specify Server Type as **Call Server**. IP connectivity has also been defined as shown in the screenshot below. In this compliance testing, Session Manager was configured with transport protocol **UDP** on IP address **10.33.10.26** and listens on port **5060**.



For **Advanced** tab, select Interworking Profile **SM** as defined in **Section 7.2.4**. Other settings were kept as default.



7.3. Domain Policies

Domain Policies feature configures various rule sets (policies) to control unified communications based upon criteria of communication sessions originating from or terminating at the enterprise. These criteria can be used to trigger policies which, in turn, activate various security features of Avaya SBCE security device to aggregate, monitor, control and normalize call flow. There are default policies available for use, or a custom domain policy can be created.

7.3.1. Application Rules

Application Rules define which types of SIP-based applications Avaya SBCE security device will protect: voice, video, and/or instant messaging (IM). In addition, it is possible to configure the maximum number of concurrent voice and video sessions the network will process in order to prevent resource exhaustion.

For the certification testing, Application Rule was created to set the number of concurrent voice traffic. The sample configuration cloned and modified the default application rule to increase the number of **Maximum Concurrent Session** and **Maximum Sessions Per Endpoint**.

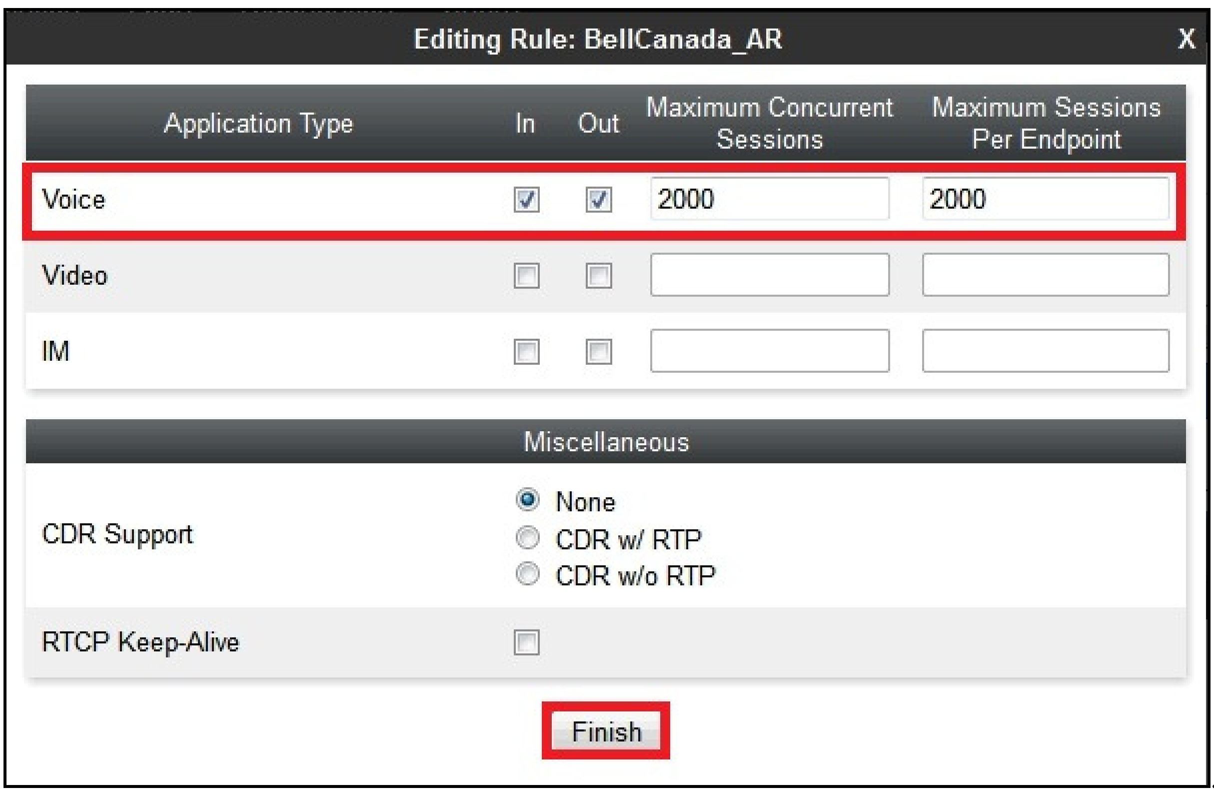
In the compliance testing, two **Application Rules** were created for BellCanada and Session Manager

7.3.1.1 Application Rule for Bell Canada

To clone Application Rule, navigate to **Domain Policies → Application Rules**, select **default** rule then click **Clone** button (not shown).

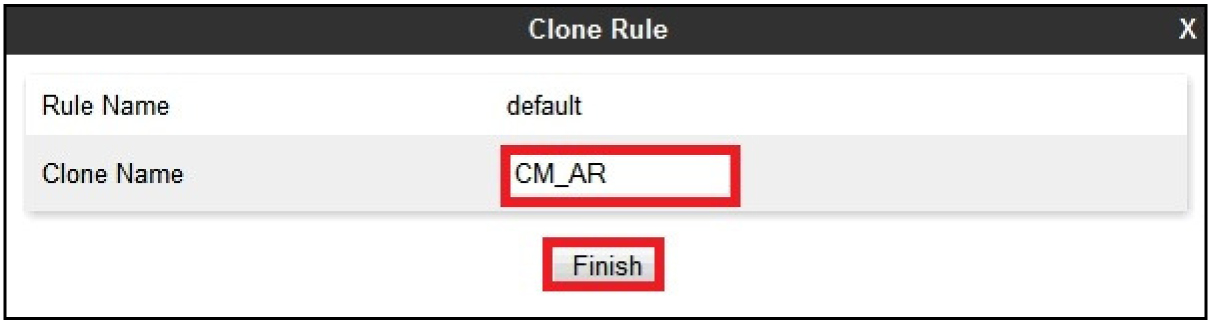
Enter a descriptive name, e.g. **BellCanada_AR** for the new rule then click **Finish** button.

Click **Edit** button (not shown) to modify the rule. Set **Maximum Concurrent Sessions** and **Maximum Session Per Endpoint** for **Voice** application to a value high enough for the amount of traffic the network is able process. The following screen shows the modified Application Rule with **Maximum Concurrent Sessions** and **Maximum Session Per Endpoint** set to **2000**. In the compliance testing, Communication Manager was programmed to control concurrent sessions by setting **Number of Members** (see **Section 5.7**) to the allotted number. Therefore, values in the Application Rule **BellCanada_AR** were set high enough to be considered non-blocking.

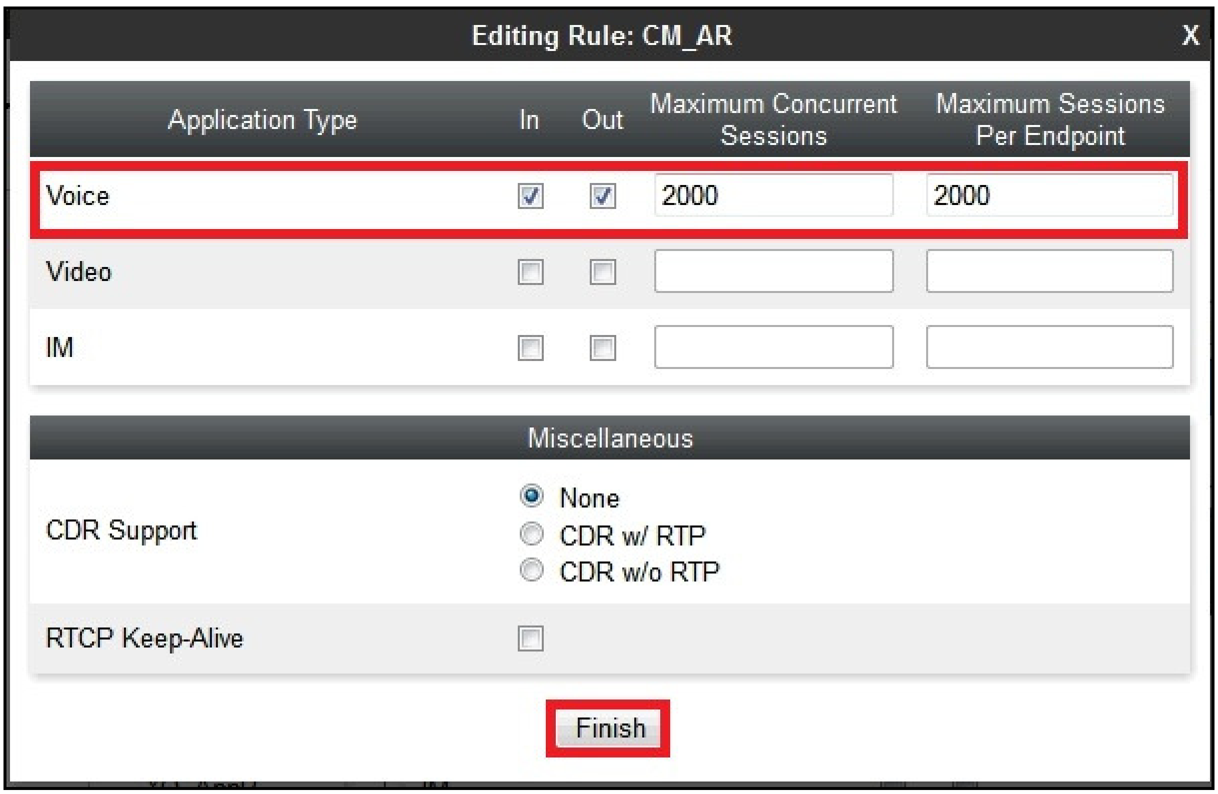


7.3.1.2 Application Rule for Communication Manager

Clone Application Rule with a descriptive name, e.g. **CM_AR** for Communication Manager and click **Finish** button.



The Application Rule **CM_AR** was similarly configured as shown in the screenshots below.



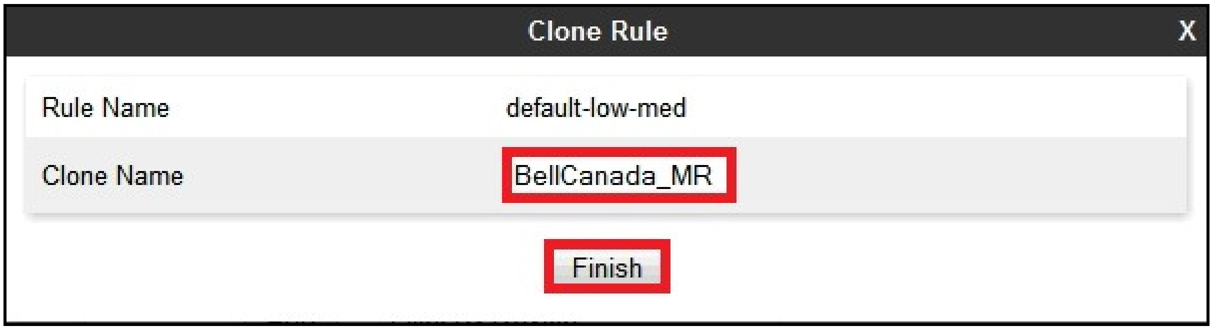
7.3.2. Media Rules

Media Rules 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 packet matching the criteria will be handled by Avaya SBCE security product.

7.3.2.1 Media Rule for Bell Canada

To create **Media Rule**, navigate to **Domain Policies → Media Rules**, select **default-low-med** rule then click **Clone** button (not shown).

Enter a descriptive name, e.g. **BellCanada_MR** for the new rule then click **Finish** button.



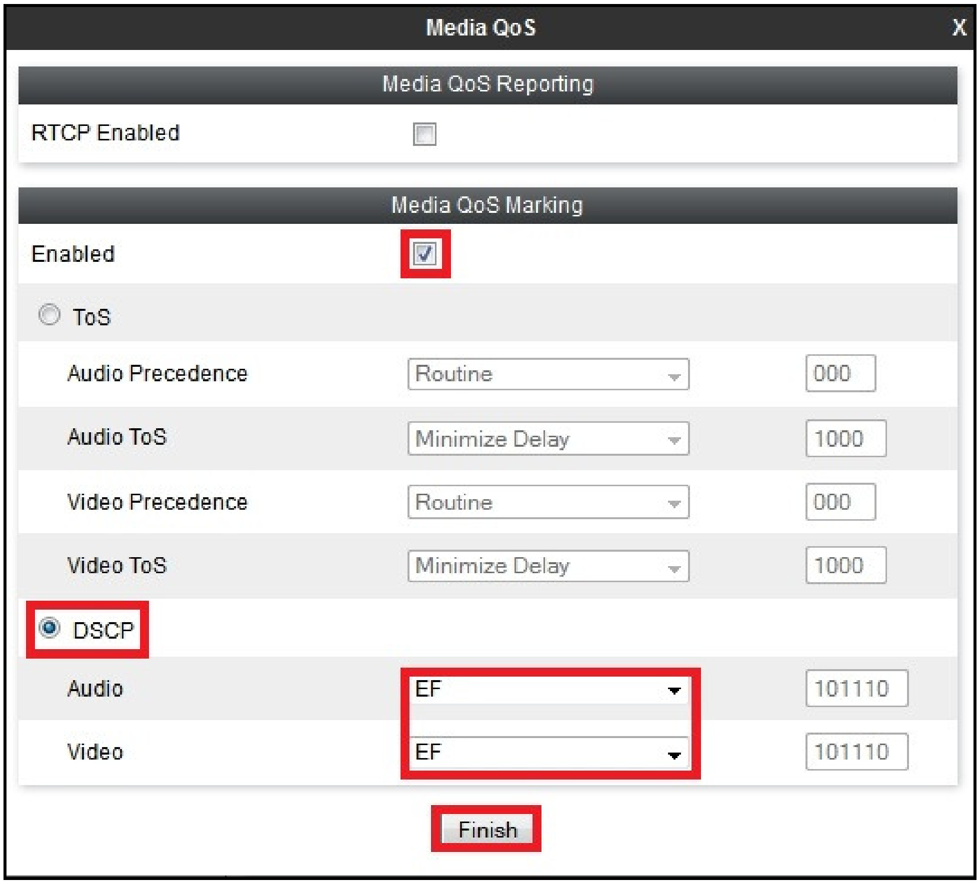
When RTP changes while active call is in progress, Avaya SBCE interprets this as an anomaly and alerts will be created in **Incidents Log**. Thus, disabling **Media Anomaly Detection** could prevent **RTP Injection Attack** alerts from being created in the log.

To modify Media Anomaly, select **Media Anomaly** tab and click **Edit** button (not shown). Then uncheck **Media Anomaly Detection** and click **Finish** button.

Media Silencing feature detects the silence while active call is in progress. If the silence is detected and exceeds an allowed duration, Avaya SBCE generates alerts in **Incidents Log**. In the compliance testing, Media Silencing detection was disabled to prevent the call from unexpectedly disconnected due to RTP packet lost on the public internet.

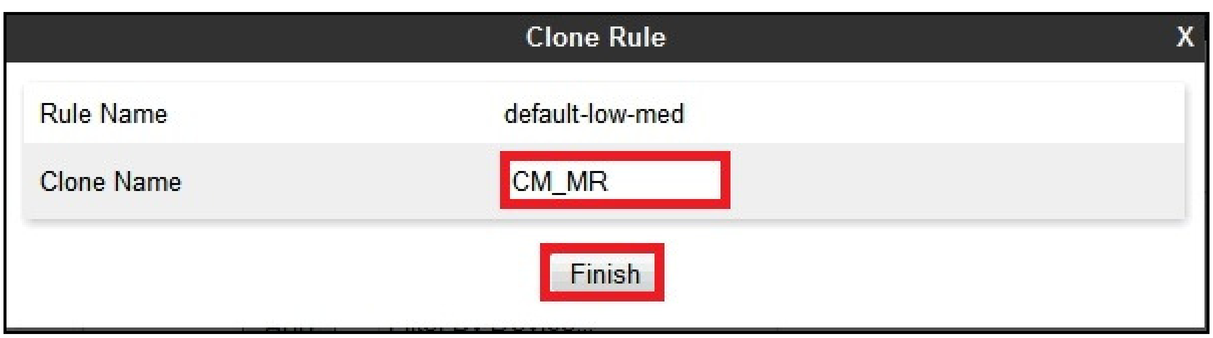
To modify Media Silencing, select **Media Silencing** tab and click **Edit** button (not shown). Then uncheck **Media Silencing** and click **Finish** button.

Under **Media QoS** tab, click **Edit** button (not shown) to configure Quality of Service (QoS). Avaya SBCE can be configured to mark Differentiated Services Code Point (DSCP) in IP packet header with specific values to support Quality of Services policy for media. The following screen shows QoS values used for the compliance testing.



7.3.2.2 Media Rule for Communication Manager

Clone a Media Rule with a descriptive name, e.g. **CM_MR** for Communication Manager then click **Finish** button.



Media Rule **CM_MR** was similarly configured for **Media Anomaly**, **Media Silencing** and **Media QoS** (not shown).

7.3.3. Signaling Rules

Signaling Rules define the action to be taken (Allow, Block, Block with Response, etc.) for each type of SIP-specific signaling request and response message. When SIP signaling packets are received by Avaya SBCE, they are parsed and "pattern-matched" against particular signaling criteria defined by these rules. Packets matching the criteria defined by the Signaling Rules are tagged for further policy matching.

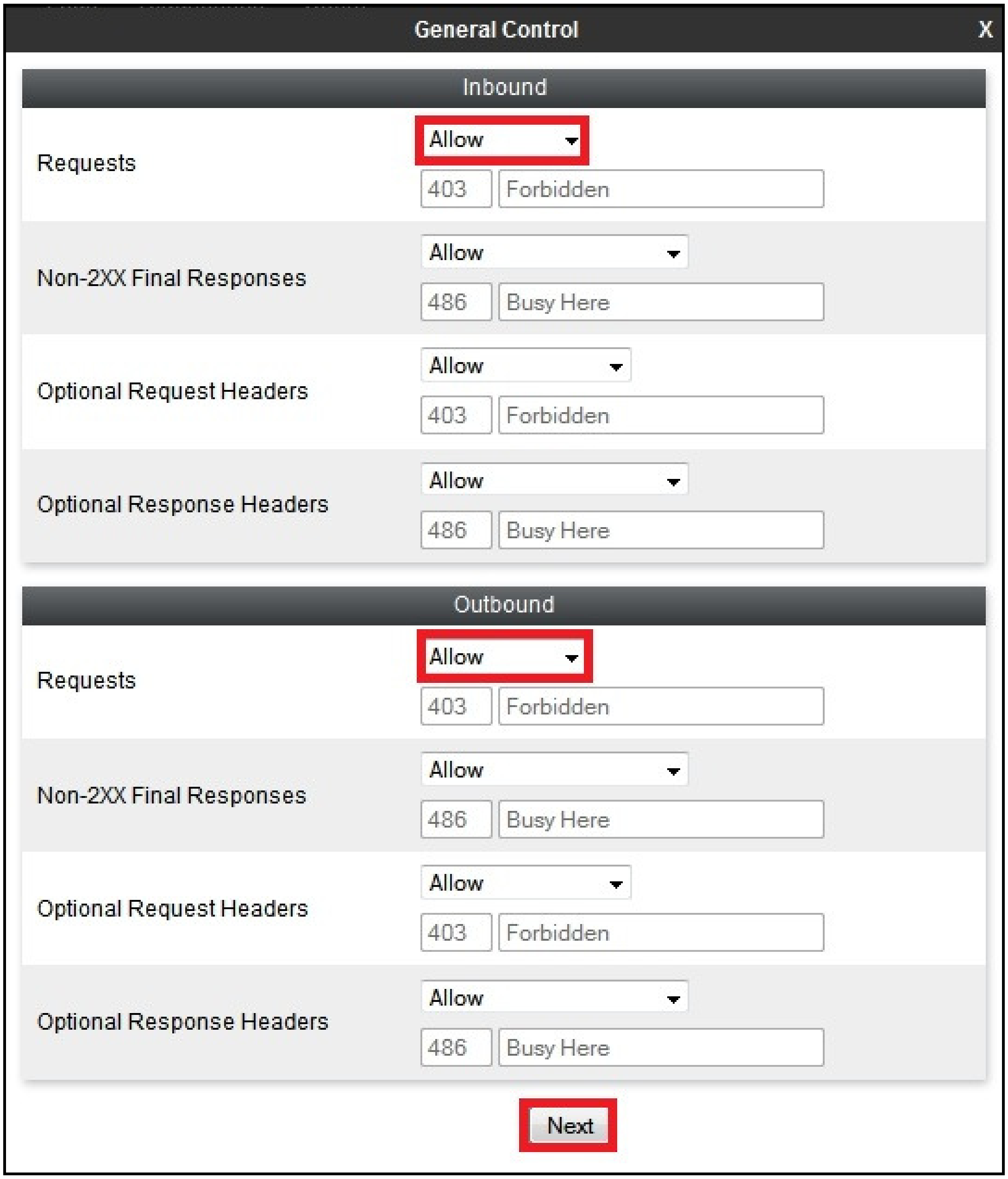
To clone Signaling Rule, navigate to **Domain Policies → Signaling Rules**, select **default** rule then click **Clone** button (not shown).

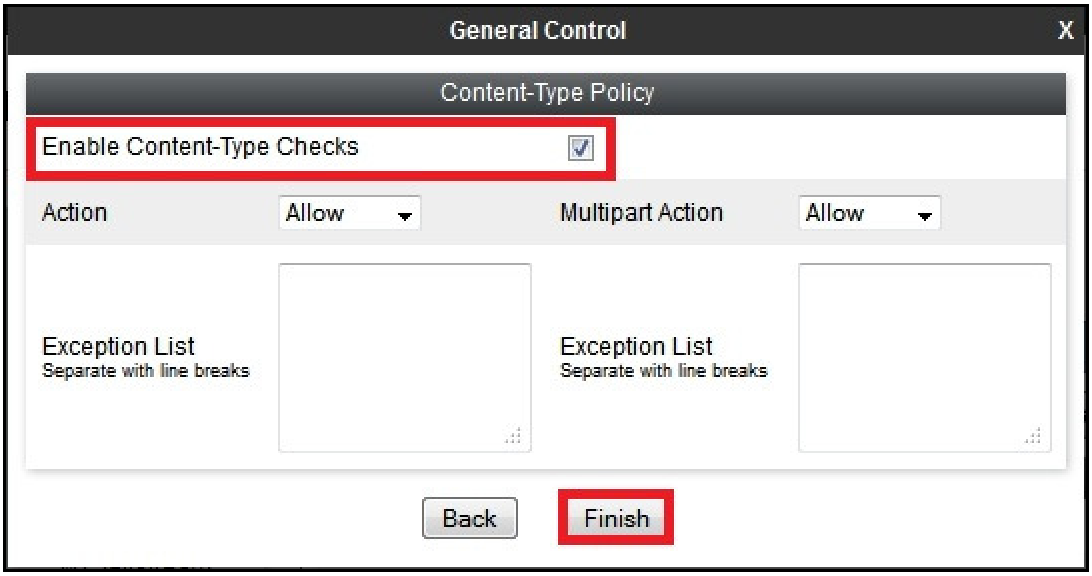
In the compliance testing, two **Signaling Rules** were created for Bell Canada and Communication Manager.

7.3.3.1 Signaling Rule for Bell Canada

Clone Signaling Rule with a descriptive name, e.g. **BellCanada_SR** and click **Finish** button.

Cloning from Signaling Rule default, verify that **General** settings of **BellCanada_SigR** with **Inbound** and **Outbound Request** were set to **Allow**, and **Enable Content-Type Checks** was enabled with **Action** and **Multipart-Action** were set to **Allow** as shown in the following screenshots.

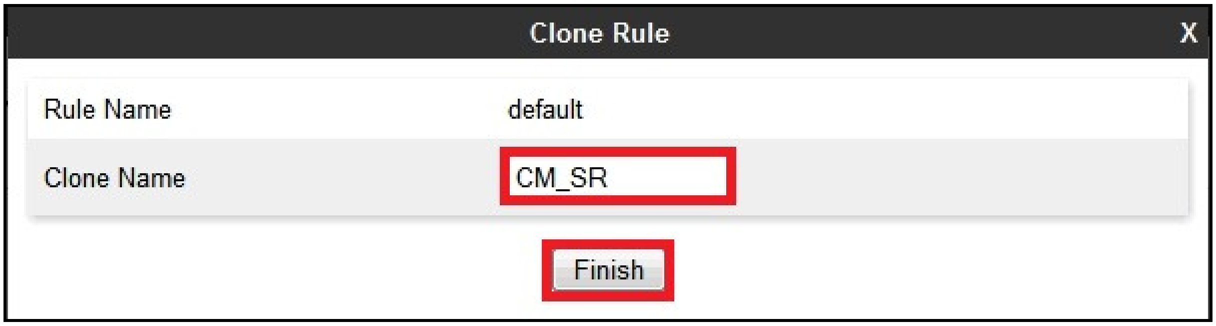

General Control
X
Inbound
Requests
Allow
403
Forbidden
Non-2XX Final Responses
Allow
486
Busy Here
Optional Request Headers
Allow
403
Forbidden
Optional Response Headers
Allow
486
Busy Here
Outbound
Requests
Allow
403
Forbidden
Non-2XX Final Responses
Allow
486
Busy Here
Optional Request Headers
Allow
403
Forbidden
Optional Response Headers
Allow
486
Busy Here
Next



For **Signaling QoS** tab, select proper Quality of Service (QoS). Avaya SBCE can be configured to mark Differentiated Services Code Point (DSCP) in IP packet header with specific values to support Quality of Services policies for signaling. The following screen shows QoS values used for the compliance testing.

7.3.3.2 Signaling Rule for Communication Manager

Clone Signaling Rule with a descriptive name, e.g. **CM_SR** for Communication Manager then click **Finish** button.



Signaling Rule **CM_SR** was similarly configured for **General** and **Signaling QoS** settings.

7.3.4. Endpoint Policy Groups

The rules created within Domain Policy section are assigned to Endpoint Policy Group which is then applied to Server Flow defined in **Section 7.4.4**

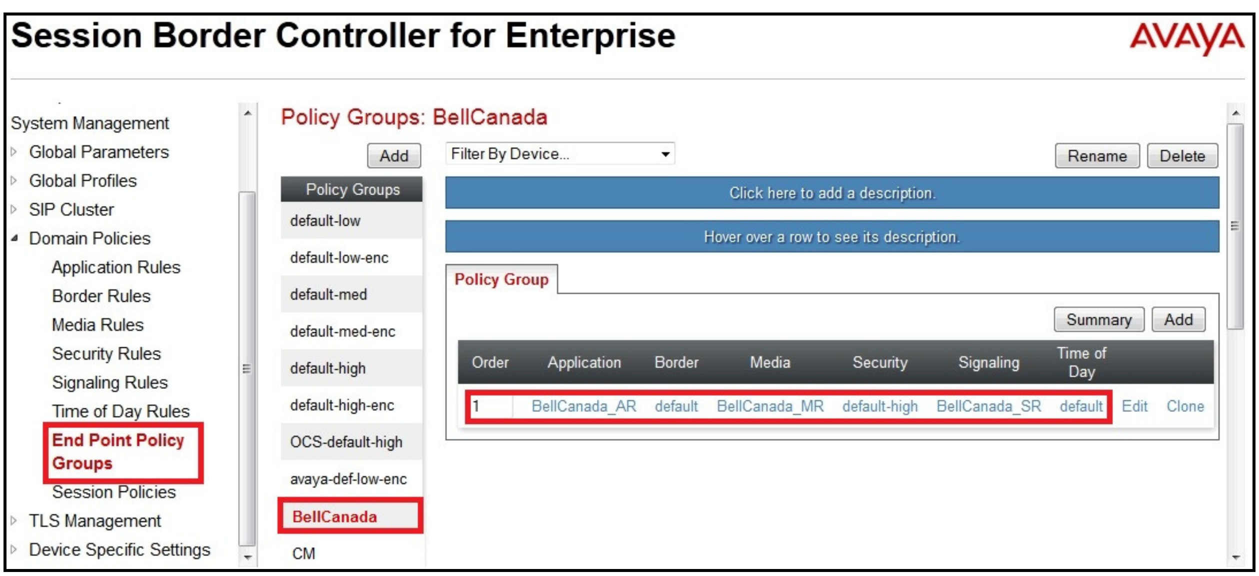
Endpoint Policy Groups were separately created for Bell Canada and Communication Manager.

To create Policy Group, navigate to **Domain Policies** → **Endpoint Policy Groups** and click **Add** button (not shown).

7.3.4.1 Endpoint Policy Group for Bell Canada

The following screen shows Endpoint Policy Group **BellCanada** created for Bell Canada.

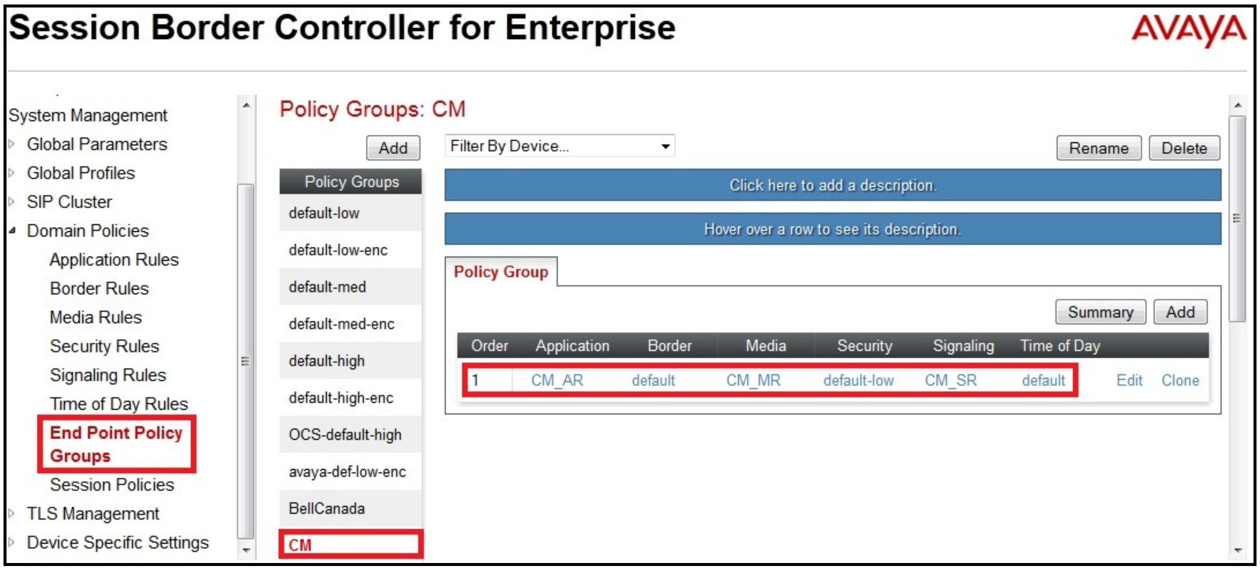
- Set Application Rule to **BellCanada_AR** which was created in **Section 7.3.1.1**.
- Set Media Rule to **BellCanada_MR** which was created in and **Section 7.3.2.1**.
- Set Signaling Rule to **BellCanada_SR** which was created in **Section 7.3.3.1**.
- Set **Border** and **Time of Day** rules to **default**.
- Set **Security** rule to **default-high**.



7.3.4.2 Endpoint Policy Group for Communication Manager

The following screen shows Endpoint Policy Group **CM** created for Communication Manager.

- Set Application Rule to **CM_AR** which was created in **Section 7.3.1.2**.
- Set Media Rule to **CM_MR** which was created in and **Section 7.3.2.2**.
- Set Signaling Rule **CM_SR** which was created in **Section 7.3.3.2**.
- Set the **Border** and **Time of Day** rules to **default**.
- Set the **Security** rule to **default-low**.



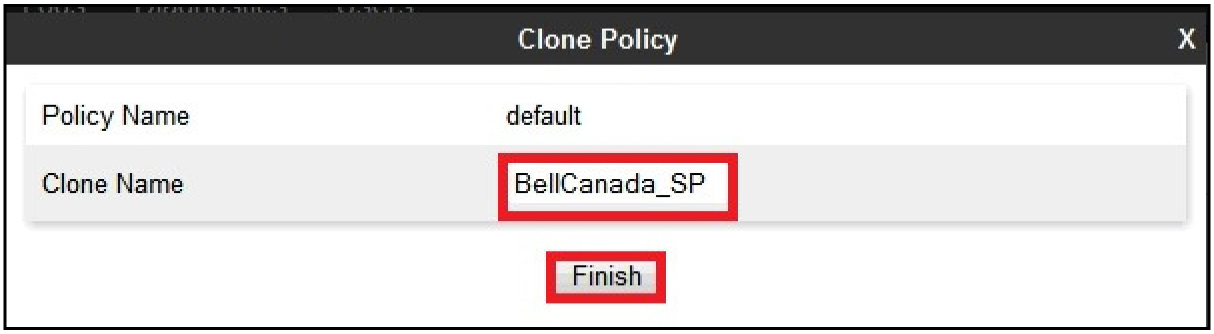
7.3.5. Session Policy

Session Policy is applied based on the source and destination of a media session, i.e. which codec is to be applied to the media session between its source and destination. The source and destination are defined in the URI Group shown in **Section 7.2.1**.

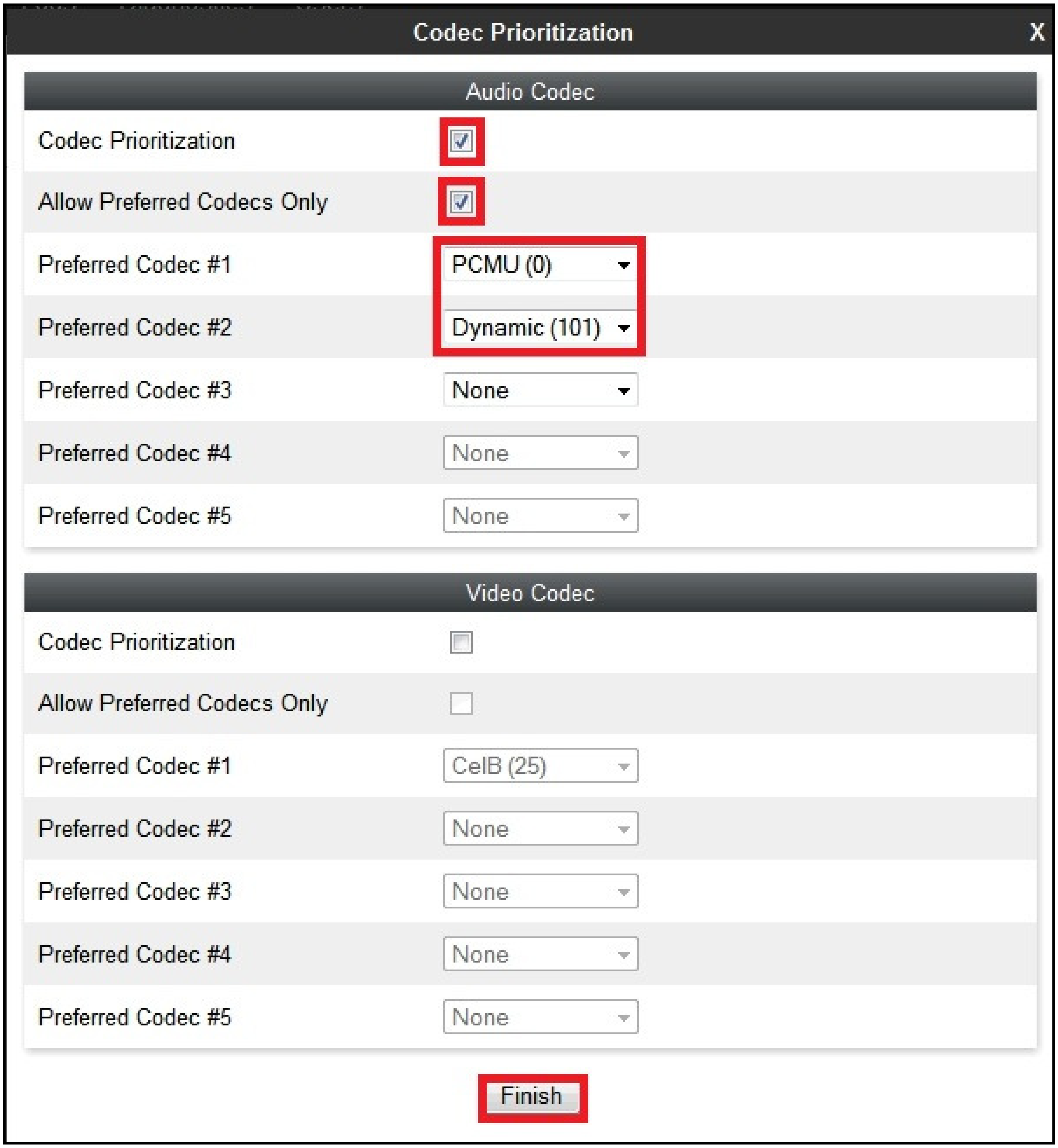
In the compliance testing, Session Policy **BellCanada_SP** was created to match codec configuration on Bell Canada. The policy also allows Avaya SBCE to anchor media in off-net call forward and call transfer scenarios.

To clone Session Policy which applies to both Bell Canada and Communication Manager, navigate to **Domain Policies → Session Policies**, select **default** rule then click **Clone** button (not shown).

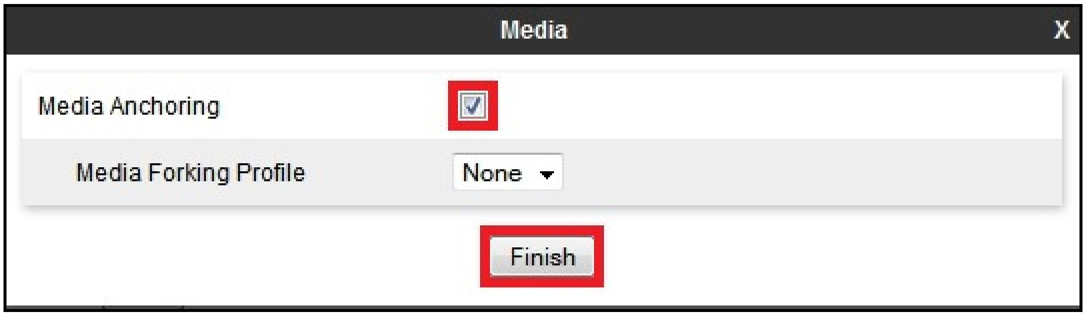
Enter a descriptive name, .e.g. **BellCanada_SP** for the new policy and click on the **Finish** button.



In the compliance testing, Bell Canada supported G.711MU only for RTP. To define **Codec Prioritization** for **Audio Codec**, select profile **BellCanada_SP** created above then click **Edit** button (not shown). Select **Preferred Codec #1** as **PCMU (0)**, **Preferred Codec #2** as **Dynamic (101)** for RFC2833/ DTMF. Check **Allow Preferred Codecs Only** to prevent the unsupported codec from being sent to both ends.



Under **Media** tab of Session Policy **BellCanada_SP** created above, click **Edit** button (not shown) then check **Media Anchoring** to allow Avaya SBCE to anchor media in off-net call forward and call transfer scenarios.



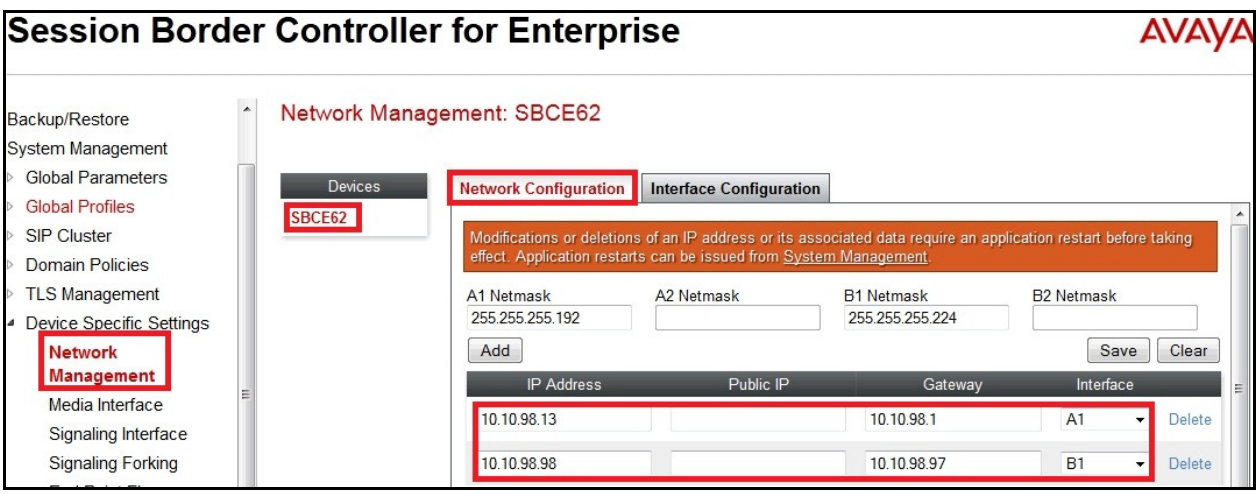
7.4. Device Specific Settings

Device Specific Settings feature allows aggregate system information to be viewed and various device-specific parameters to be managed to determine how a particular device will function when deployed in the network. Specifically, it gives the ability to define and administer various device-specific protection features such as Message Sequence Analysis (MSA) functionality and protocol scrubber rules, end-point and session call flows, as well as the ability to manage system logs and control security features.

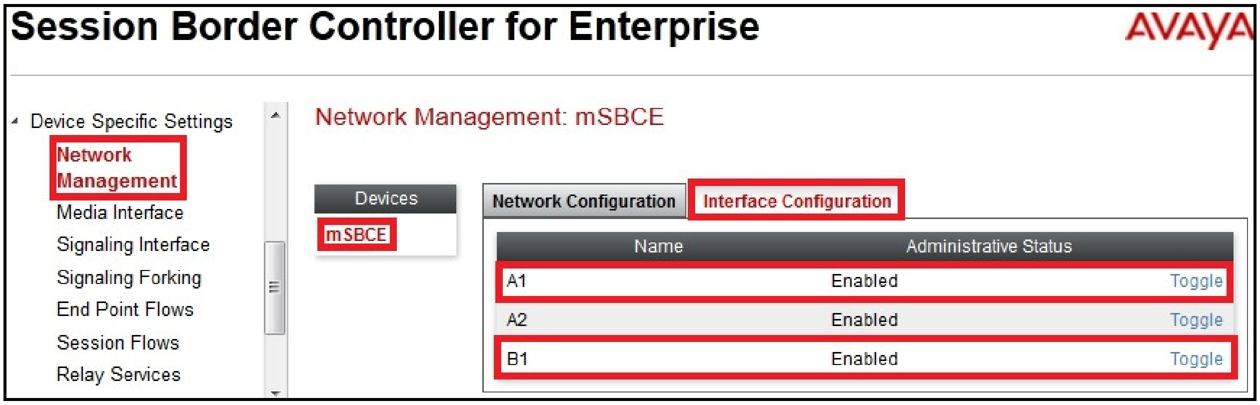
7.4.1. Network Management

Network Management page is where the network interface settings are configured and enabled. During the installation process of Avaya SBCE, certain network-specific information is defined such as device IP address, public IP address, subnet mask, gateway, etc. to interface the device to the networks. This information populates the various Network Management tabs which can be edited as needed to optimize device performance and network efficiency.

Navigate to **Device Specific Settings → Network Management**, under **Network Configuration** tab, verify IP addresses assigned to the interfaces and that the interfaces were enabled. The following screen shows private interface was assigned to **A1** and public interface was assigned to **B1** appropriate to the parameters shown in the **Figure 1**.



On **Interface Configuration** tab, enable the interfaces connecting to inside enterprise and outside service provider networks. To enable interface, click the appropriate **Toggle State** button. The following screen shows interface **A1** and **B1** were **Enabled**.



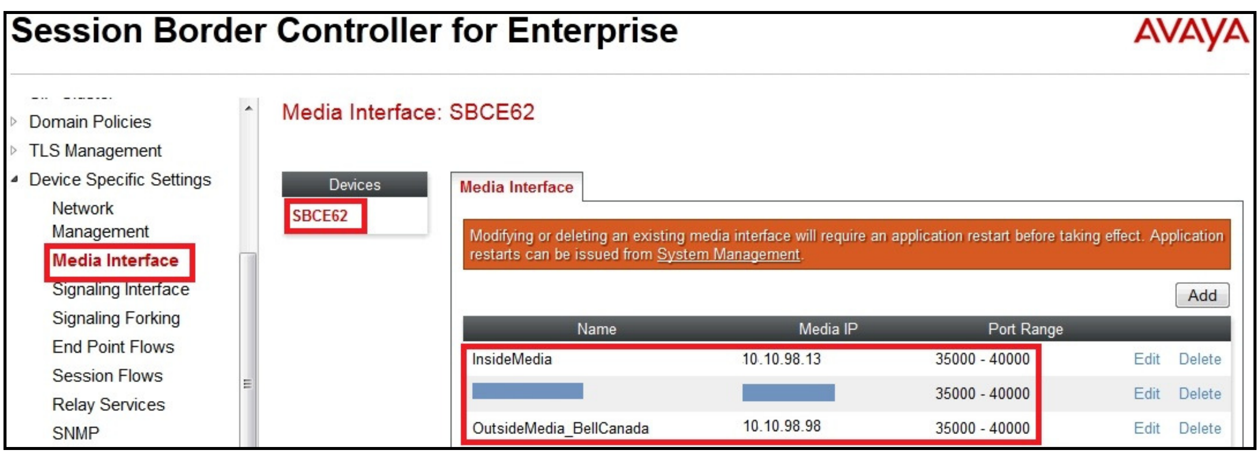
7.4.2. Media Interface

Media Interface screen is where media ports are defined. Avaya SBCE will open connection for RTP traffic on the defined ports.

To create **Media Interface**, navigate to **Device Specific Settings → Media Interface** and click **Add** button (not shown).

Two separate Media Interfaces were needed for inside and outside interfaces. The following screen shows Media Interfaces **InsideMedia** and **OutsideMedia** were created for the compliance testing.

Note: After media interfaces are created, an application restart is necessary before the changes will take effect.

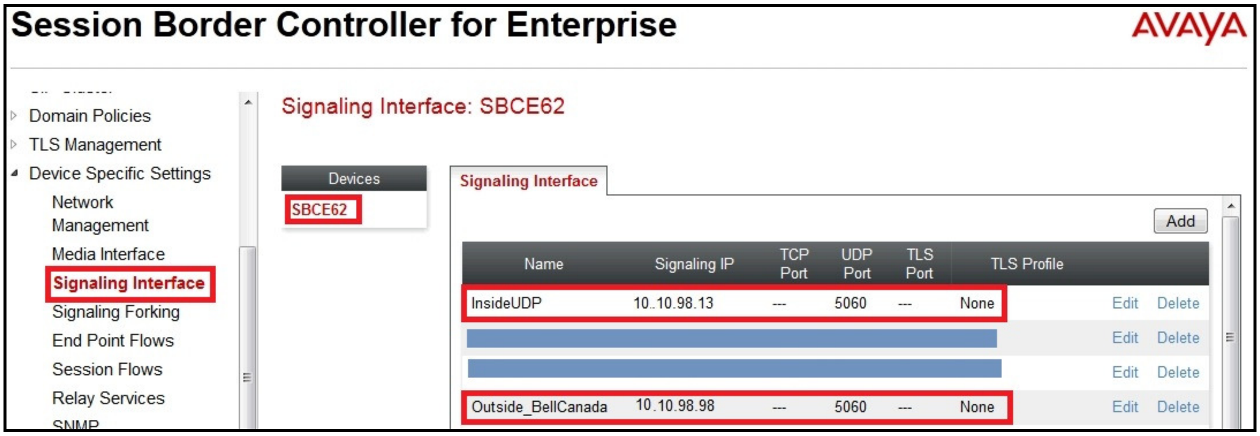


7.4.3. Signaling Interface

Signaling Interface screen is where SIP signaling port is defined. Avaya SBCE will listen for SIP request on the defined port.

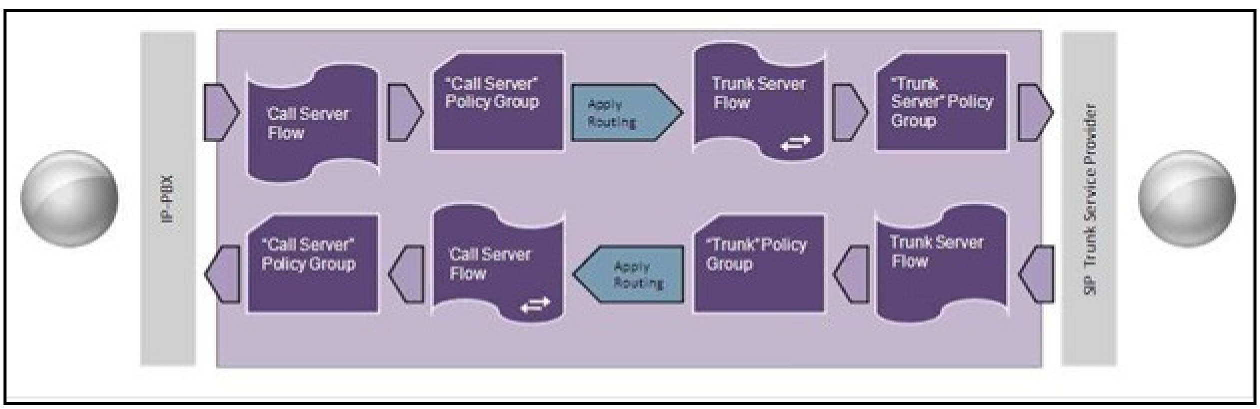
To create **Signaling Interface**, navigate to **Device Specific Settings → Signaling Interface** and click **Add** button (not shown).

Two separate Signaling Interfaces were needed for inside and outside interfaces. The following screen shows Signaling Interfaces **Inside_UDP** and **Outside_BellCanada** were created in the compliance testing with **UDP/5060** configured for both inside and outside interfaces.



7.4.4. End Point Flows - Server Flow

When a packet is received by Avaya SBCE, the content (IP addresses, URIs, etc.) is used to determine which flow it matches. Once the flow is determined, the flow points to a policy 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 Avaya SBCE to secure SIP Trunk calls.

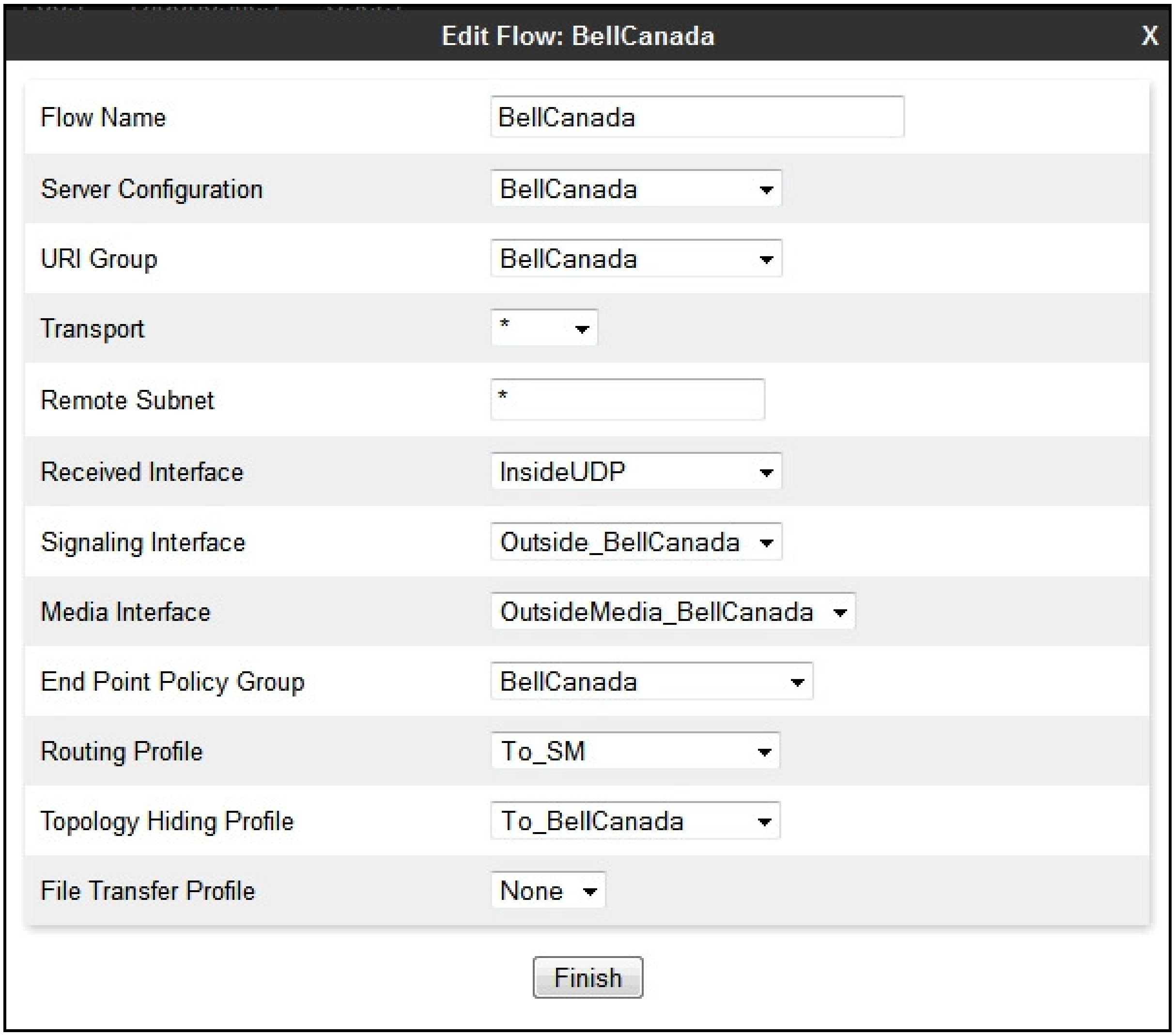


In the compliance testing, two separate Server Flows were created for Bell Canada and Session Manager.

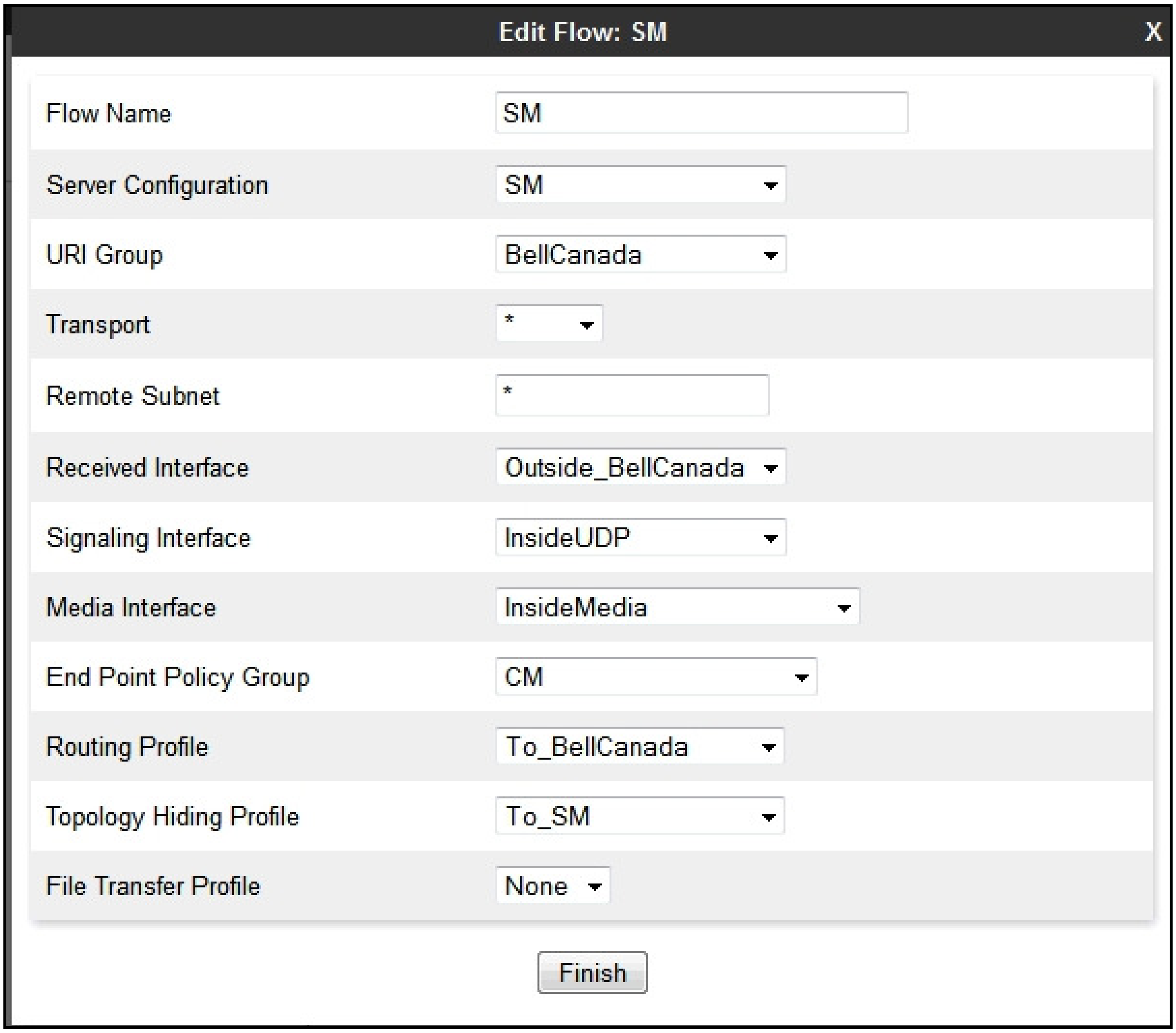
To create Server Flow, navigate to **Device Specific Settings → End Point Flows**, select the **Server Flows** tab and click **Add** button (not shown). In the new window that appears, enter following values while other fields were kept as default.

- **Flow Name**: Enter a descriptive name.
- **Server Configuration**: Select Server Configuration created in **Section 7.2.6** which the Server Flow associates to.
- **URI Group**: Select URI Group **BellCanada** created in **Section 7.2.1**.
- **Received Interface**: Select Signaling Interface created in **Section 7.4.3** which is Server Configuration designed to receive SIP signaling.
- **Signaling Interface**: Select Signaling Interface created in **Section 7.4.3** which is Server Configuration designed to send SIP signaling.
- **Media Interface**: Select Media Interface created in **Section 7.4.2** which is Server Configuration designed to send RTP.
- **End Point Policy Group**: Select End Point Policy Group created in **Section 7.3.4** which the Server Flow associates to.
- **Routing Profile**: Select Routing Profile created in **Section 7.2.2** which is Server Configuration is designed to route the calls to.
- **Topology Hiding Profile**: Select Topology Hiding profile created in **Section 7.2.3** to apply toward Server Configuration.
- Use default values for all remaining fields. Click **Finish** to save and exit.

The following screen shows Server Flow **BellCanada** created for Bell Canada.



The following screen shows Server Flow **SM** created for Session Manager.



7.4.5. Session Flow

Session Flows feature allows defining certain parameters that pertain to media portions of a call, whether it originates from the enterprise or outside the enterprise. This feature provides the complete and unparalleled flexibility to monitor, identify and control very specific types of calls based upon these user-definable parameters. Session Flows profiles SDP media parameters, to completely identify and characterize a call placed through the network.

A common Session Flow **BellCanada_SF** was created for both Bell Canada and Communication Manager.

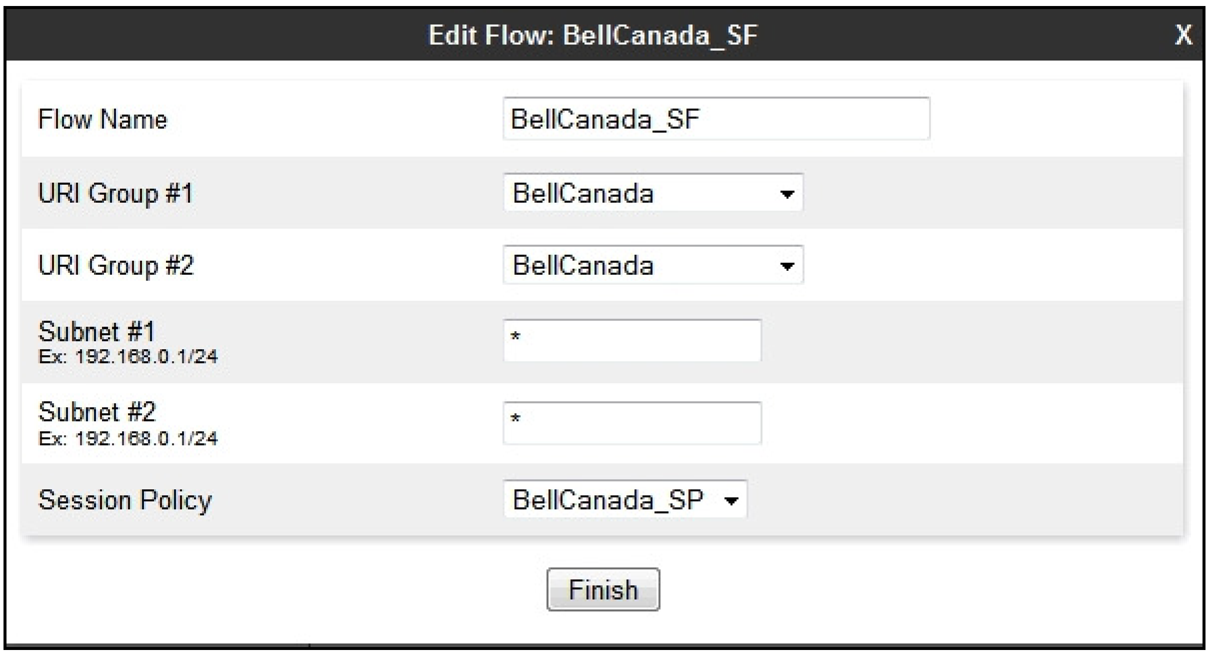
To create Session Flow, navigate to **Device Specific Settings → Session Flows** then click **Add** (not shown). In the new window that appears, enter following values while remaining fields were kept as default.

- **Flow Name**: Enter a descriptive name.

- **URI Group #1**: Select URI Group **BellCanada** created in **Section 7.2.1** to assign to the Session Flow as source URI Group.
- **URI Group #2**: Select URI Group **BellCanada** created in **Section 7.2.1** to assign to the Session Flow as destination URI Group.
- **Session Policy**: Select Session Policy **BellCanada_SP** created in **Section 7.3.5** to assign to the Session Flow.
- Click **Finish** button.

Note: A unique URI Group is used for source and destination, since it contains multiple URIs defined for source as well as for destination.

The following screen shows Session Flow **BellCanada_SF**.



8. Bell Canada SIP Trunking Configuration

Bell Canada is responsible for the configuration of Bell Canada SIP Trunking service. The customer will need to provide the IP address used to reach the Avaya SBCE at the enterprise. Bell Canada will provide the customer with the necessary information to configure the SIP connection from the enterprise site to the Bell Canada network. The provided information from Bell Canada includes:

- IP address of the Bell Canada SIP proxy.
- Bell Canada SIP domain.
- Enterprise SIP domain.
- Credentials for Digest Authentication.
- Supported codecs.
- DID numbers.
- A customer specific SIP signaling reference.

The sample configuration between Bell Canada and the enterprise for the compliance test is a static configuration. There is no registration of the SIP trunk or enterprise users to the Bell Canada network.

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 useful troubleshooting tips that can be used for troubleshooting.

9.1. Verification Steps

Following activities were made to each test scenario:

- Verify that endpoints at the enterprise site can place and receive calls to PSTN and that the call remains active for more than 35 seconds.
- Verify that user on both PSTN and the enterprise sides can end an active call by hanging up.

9.2. Protocol Traces

Following SIP message headers were inspected using sniffer trace analysis tool:

- Request-URI: Verify proper request number and SIP domain.
- From: Verify proper display name and display number.
- To: Verify proper display name and display number.
- P-Preferred-Identity: Verify proper display name and display number.
- Privacy: Verify privacy masking with "id".
- Diversion: Verify proper display name and display number.

Following attributes in SIP message body were inspected using sniffer trace analysis tool:

- Connection Information (c line): Verify correct IP addresses of near and far endpoints.
- Time Description (t line): Verify correct session timeout value of near and far endpoints.
- Media Description (m line): Verify correct audio port, codec, DTMF event description.
- Media Attribute (a line): Verify correct audio port, codec, ptime, send/ receive ability, DTMF event.

9.3. Troubleshooting:

9.3.1. Avaya SBCE:

Using network sniffing tool, e.g. Wireshark to monitor SIP signaling between the enterprise and Bell Canada. The sniffer traces are captured at the public interface of Avaya SBCE.

Following screenshots show an example incoming call from Bell Canada to the enterprise.

- Incoming INVITE request from Bell Canada.

```
INVITE sip:416XXX1880@cust6xxxx.xxxx.bell.ca;transport=udp SIP/2.0
Via: SIP/2.0/UDP 10.20.237.205:5060;branch=z9hG4bKjqtd6n301gugekc6d2k0.1
From: "Avaya
CS1K"<sip:+1647XXX1232@sipxxxxxxxx.bell.ca;user=phone>;tag=SDsafdb01-1632016891-
1372858841325-
```

```
To: "Bell Demo12345"<sip:416XXX1880@cust6xxxx.xxxx.bell.ca>
Call-ID: SDsafdb01-ebe347a4af13405e5d0c00828d4567d3-a0n8330
CSeq: 308395127 INVITE
Contact: <sip:+1647XXX1232@10.20.237.205:5060;transport=udp>
Supported: 100rel
Allow: ACK,BYE,CANCEL,INFO,INVITE,OPTIONS,PRACK,REFER,NOTIFY,UPDATE
Accept: application/media_control+xml,application/sdp,multipart/mixed
Max-Forwards: 18
Content-Type: application/sdp
Content-Length: 189

v=0
o=BroadWorks 38021480 1 IN IP4 10.20.237.205
s=-
c=IN IP4 10.20.237.205
t=0 0
m=audio 21806 RTP/AVP 0 8 18 101
a=ptime:20
a=rtpmap:101 telephone-event/8000
a=fmtp:101 0-15
```

- 200OK response from the enterprise.

```
SIP/2.0 200 OK
From: "Avaya CS1K"
<sip:1647XXX1232@sipxxxxxxxx.bell.ca;user=phone>;tag=SDsafdb01-1632016891-
1372858841325-
To: "Bell Demo12345"
<sip:416XXX1880@cust6xxxx.xxxx.bell.ca>;tag=80dc9cc369f7e212a451f6fab100
CSeq: 308395127 INVITE
Call-ID: SDsafdb01-ebe347a4af13405e5d0c00828d4567d3-a0n8330
Contact: <sip:416XXX1880;tgrp=vsac_416XXX1880_01a;trunk-
context=sipxxxxxxxx.bell.ca@10.10.98.98:5060;transport=udp;user=phone;gsid=65bc2
af0-e3e6-11e2-af59-e41f13b32ca8>
Record-Route: <sip:10.10.98.98:5060;ipcs-line=10038;lr;transport=udp>
Allow: INVITE, ACK, OPTIONS, BYE, CANCEL, NOTIFY, REFER, INFO, PRACK, UPDATE
Supported: 100rel, join, replaces, sdp-anat, timer
Via: SIP/2.0/UDP 10.20.237.205:5060;branch=z9hG4bKjqtd6n301gugekc6d2k0.1
Accept-Language: en
Server: Avaya CM/R016x.03.0.124.0 AVAYA-SM-6.3.2.0.632023
P-Asserted-Identity: "Bell x1880"
<sip:416XXX1880@cust6xxxx.xxxx.bell.ca;user=phone>
Session-Expires: 600;refresher=uas
Content-Type: application/sdp
P-Location:
SM;origlocname="Belleville";origsiglocname="Belleville";origmedialocname="Bellev
ille";termlocname="Belleville";termsiglocname="Belleville";termmedialocname="Bel
leville";smaccounting="true"
P-AV-Message-Id: 1_2
Av-Global-Session-ID: 65bc2af0-e3e6-11e2-af59-e41f13b32ca8
Content-Length: 173

v=0
o=- 1372858841 2 IN IP4 10.10.98.98
s=-
c=IN IP4 10.10.98.98
b=AS:64
t=0 0
m=audio 35038 RTP/AVP 0 101
a=rtpmap:0 PCMU/8000
a=rtpmap:101 telephone-event/8000
```

Following screenshots show an example outgoing call from the enterprise to Bell Canada.

- Outgoing INVITE request from the enterprise.

```
INVITE sip:1647XXX1232@sipxxxxxxxx.bell.ca;user=phone SIP/2.0
From: "Bell x1882"
<sip:416XXX1882@cust6xxxx.xxxx.bell.ca;user=phone>;tag=0ac25877af7e2116551f6fab1
00
To: <sip:1647XXX1232@sipxxxxxxxx.bell.ca;user=phone>
CSeq: 1 INVITE
Call-ID: 3e9fdc20d69d5748b838d376a1606b5a
Contact: <sip:416XXX1882;tgrp=vsac_416XXX1880_01a;trunk-
context=sipxxxxxxxx.bell.ca@10.10.98.98:5060;user=phone;gsid=264f61a0-e3f7-11e2-
af59-
e41f13b32ca8;epv=%3csip:1882%40avayalab.com%3bgr%3dc37c0d4e9da42a54640893bc78e52
008%3e>
Record-Route: <sip:10.10.98.98:5060;ipcs-line=11711;lr;transport=udp>
Allow: INVITE, ACK, OPTIONS, BYE, CANCEL, SUBSCRIBE, NOTIFY, REFER, INFO, PRACK,
PUBLISH, UPDATE
Supported: 100rel, join, replaces, sdp-anat, timer
User-Agent: Avaya one-X Deskphone 6.2.0.72 (38197) AVAYA-SM-6.3.2.0.632023 Avaya
CM/R016x.03.0.124.0 AVAYA-SM-6.3.2.0.632023
Max-Forwards: 60
Via: SIP/2.0/UDP 10.10.98.98:5060;branch=z9hG4bK-s1632-001196319850-1--s1632-
Accept-Language: en
Alert-Info: <cid:internal@avayalab.com>;avaya-cm-alert-type=internal
P-Asserted-Identity: "Bell x1882"
<sip:416XXX1882@cust6xxxx.xxxx.bell.ca;user=phone>
Session-Expires: 600;refresher=uac
Min-SE: 600
Content-Type: application/sdp
Endpoint-View:
<sip:1882@avayalab.com;gr=c37c0d4e9da42a54640893bc78e52008>;local-tag=-
1f60fe2c51d40e1d-5c57e340_F188210.33.5.51;call-id=39_51d40e1d-17524a7c-
5c57e3c0_I@10.33.5.51
P-AV-Message-Id: 1_2
P-Charging-Vector: icid-value="264f61a0-e3f7-11e2-af59-e41f13b32ca8"
Av-Global-Session-ID: 264f61a0-e3f7-11e2-af59-e41f13b32ca8
P-Location:
SM;origlocname="Belleville";origsiglocname="Belleville";origmedialocname="Bellev
ille";termlocname="Belleville";termsiglocname="Belleville";smaccounting="true"
Content-Length: 213

v=0
o=- 1372866042 1 IN IP4 10.10.98.98
s=-
c=IN IP4 10.10.98.98
b=TIAS:64000
t=0 0
a=avf:avc=n prio=n
a=csup:avf-v0
m=audio 35044 RTP/AVP 0 101
a=rtpmap:0 PCMU/8000
a=rtpmap:101 telephone-event/8000
```

- Incoming 401 from Bell Canada to request Digest Authentication.

```
SIP/2.0 401 Unauthorized
From: "Bell x1882"
```

```
<sip:416XXX1882@cust6xxxx.xxxx.bell.ca;user=phone>;tag=0ac25877af7e2116551f6fab1
00
To: <sip:1647XXX1232@sipxxxxxxxx.bell.ca;user=phone>;tag=SD501k999-718440725-
1372866042565
CSeq: 1 INVITE
Call-ID: 3e9fdc20d69d5748b838d376a1606b5a
Via: SIP/2.0/UDP 10.10.98.98:5060;branch=z9hG4bK-s1632-001196319850-1--s1632-
WWW-Authenticate: DIGEST
qop="auth",nonce="BroadWorksXhioozu11Tppznd2BW",realm="sipxxxxxxxx.bell.ca",algo
rithm=MD5
Content-Length: 0
```

- Outgoing re-INVITE from the enterprise with the Authorization header.

```
INVITE sip:1647XXX1232@sipxxxxxxxx.bell.ca;user=phone SIP/2.0
From: "Bell x1882"
<sip:416XXX1882@cust6xxxx.xxxx.bell.ca;user=phone>;tag=0ac25877af7e2116551f6fab1
00
To: <sip:1647XXX1232@sipxxxxxxxx.bell.ca;user=phone>
CSeq: 2 INVITE
Call-ID: 3e9fdc20d69d5748b838d376a1606b5a
Contact: <sip:416XXX1882;tgrp=vsac_416XXX1880_01a;trunk-
context=sipxxxxxxxx.bell.ca@10.10.98.98:5060;user=phone;gsid=264f61a0-e3f7-11e2-
af59-
e41f13b32ca8;epv=%3csip:1882%40avayalab.com%3bgr%3dc37c0d4e9da42a54640893bc78e52
008%3e>
Record-Route: <sip:10.10.98.98:5060;ipcs-line=11711;lr;transport=udp>
Allow: INVITE, ACK, OPTIONS, BYE, CANCEL, SUBSCRIBE, NOTIFY, REFER, INFO, PRACK,
PUBLISH, UPDATE
Supported: 100rel, join, replaces, sdp-anat, timer
User-Agent: Avaya one-X Deskphone 6.2.0.72 (38197) AVAYA-SM-6.3.2.0.632023 Avaya
CM/R016x.03.0.124.0 AVAYA-SM-6.3.2.0.632023
Max-Forwards: 60
Via: SIP/2.0/UDP 10.10.98.98:5060;branch=z9hG4bK-s1632-001196077393-1--s1632-
Accept-Language: en
Alert-Info: <cid:internal@avayalab.com>;avaya-cm-alert-type=internal
Authorization: Digest username="avaya", realm="sipxxxxxxxx.bell.ca",
nonce="BroadWorksXhioozu11Tppznd2BW", uri="sip:enterprise.com",
response="802953b823d5a09449f3f32fb8a46743", algorithm=MD5, cnonce="0a4f113b",
qop=auth, nc=00000001
P-Asserted-Identity: "Bell x1882"
<sip:416XXX1882@cust6xxxx.xxxx.bell.ca;user=phone>
Session-Expires: 600;refresher=uac
Min-SE: 600
Content-Type: application/sdp
Endpoint-View:
<sip:1882@avayalab.com;gr=c37c0d4e9da42a54640893bc78e52008>;local-tag=-
1f60fe2c51d40e1d-5c57e340_F188210.33.5.51;call-id=39_51d40e1d-17524a7c-
5c57e3c0_I@10.33.5.51
P-AV-Message-Id: 1_2
P-Charging-Vector: icid-value="264f61a0-e3f7-11e2-af59-e41f13b32ca8"
Av-Global-Session-ID: 264f61a0-e3f7-11e2-af59-e41f13b32ca8
P-Location:
SM;origlocname="Belleville";origsiglocname="Belleville";origmedialocname="Bellev
ille";termlocname="Belleville";termsiglocname="Belleville";smaccounting="true"
Content-Length: 213

v=0
o=- 1372866042 1 IN IP4 10.10.98.98
s=-
c=IN IP4 10.10.98.98
```

```
b=TIAS:64000
t=0 0
a=avf:avc=n prio=n
a=csup:avf-v0
m=audio 35044 RTP/AVP 0 101
a=rtpmap:0 PCMU/8000
a=rtpmap:101 telephone-event/8000
```

- Incoming 200OK response from Bell Canada.

```
SIP/2.0 200 OK
From: "Bell x1882"
<sip:416XXX1882@cust6xxxx.xxxx.bell.ca;user=phone>;tag=0ac25877af7e2116551f6fab1
00
To: <sip:1647XXX1232@sipxxxxxxxx.bell.ca;user=phone>;tag=SD501k999-1234136246-
1372866043627
CSeq: 2 INVITE
Call-ID: 3e9fdc20d69d5748b838d376a1606b5a
Via: SIP/2.0/UDP 10.10.98.98:5060;branch=z9hG4bK-s1632-001196077393-1--s1632-
Record-Route: <sip:10.10.98.98:5060;ipcs-line=11711;lr;transport=udp>
Supported:
Contact: <sip:1647XXX1232@10.20.237.205:5060;transport=udp>
Allow: ACK,BYE,CANCEL,INFO,INVITE,OPTIONS,PRACK,REFER,NOTIFY,UPDATE
Accept: application/media_control+xml,application/sdp
Content-Type: application/sdp
Content-Length: 189

v=0
o=BroadWorks 38304917 1 IN IP4 10.20.237.205
s=-
c=IN IP4 10.20.237.205
t=0 0
m=audio 21812 RTP/AVP 0 8 18 101
a=ptime:20
a=rtpmap:101 telephone-event/8000
a=fmtp:101 0-15
```

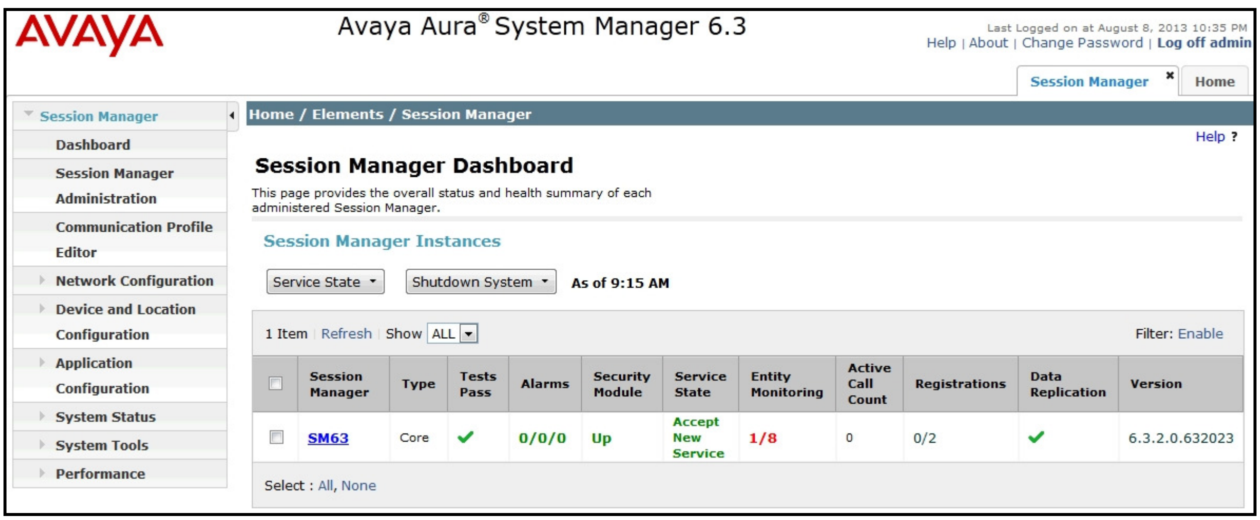
9.3.2. Communication Manager

Following is list of command for troubleshooting on Communication Manager.

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

9.3.3. Session Manager

System State – Navigate to **Home** → **Elements** → **Session Manager**, as shown below. Verify that a green check mark is placed under **Tests Pass** and the **Service State** is **Accept New Service**.



traceSM -x – Session Manager command line tool for traffic analysis. Log into the Session Manager 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, navigate to **Home** → **Elements** → **Session Manager** → **System Tools** → **Call Routing Test**. Enter the requested data to run the test.

10. Conclusion

These Application Notes describe the configuration necessary to connect Avaya Aura® Communication Manager 6.3, Avaya Aura® Session Manager 6.3 and Avaya Session Border Controller for Enterprise 6.2 to Bell Canada SIP Trunking Service. Bell Canada SIP Trunking is a SIP-based Voice over IP solution for customers ranging from small businesses to large enterprises. Bell Canada SIP Trunking provides a flexible, cost-saving alternative to traditional hardwired telephony trunks.

All of the test cases have been executed. The test results met the objectives outlined in **Section 2.1**, and a number of observations were noted in **Section 2.2**. Bell Canada SIP Trunking Service is considered **compliant** with Avaya Aura® Communication Manager 6.3, Avaya Aura® Session Manager 6.3 and Avaya Session Border Controller for Enterprise 6.2.

11. References

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

[1] *Implementing Avaya Aura® Communication Manager,* Doc ID 03-603558, Release 6.3.
[2] *Administering Avaya Aura® Communication Manager, Doc ID 03-300509, Release 6.3*
[3] *Implementing Avaya Aura® Session Manager,* Release 6.3
[4] *Installing Service Packs for Avaya Aura® Session Manager*, Release 6.3
[5] *Upgrading Avaya Aura® Session Manager,* Release 6.3
[6] *Maintaining and Troubleshooting Avaya Aura® Session Manager,* Release 6.3
[7] *Implementing Avaya Aura® System Manager,* Release 6.3
[8] *Installing Avaya Session Border Controller for Enterprise,* Release 6.2
[9] *Administering Avaya Session Border Controller for Enterprise,* Release 6.2, Issue 2, March 2013.
[10] *Installing Avaya Session Border Controller for Enterprise,* Release 6.2, Issue 2, March 2013.
[11] *Upgrading Avaya Session Border Controller for Enterprise,* Release 6.2, Issue 2, March 2013.
[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/*

Product documentation for Bell Canada SIP Trunking is available from Bell Canada.

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.