Application Notes for Bell Canada SIP Trunking Service using Least Cost Routing with Avaya Aura® Communication Manager R6.0.1, Geographic Redundant Avaya Aura® Session Managers R6.1 and Avaya Session Border Controllers for Enterprise R4.0.5 – Issue 1.0

Abstract

These Application Notes describe the steps to configure Session Initiation Protocol (SIP) Trunking between Bell Canada SIP Trunking Service which features Least Cost Routing at the Central Office and an Avaya SIP-enabled enterprise solution. The Avaya solution consists of Avaya Aura® Communication Manager Evolution Server 6.0.1, geographic redundant Avaya Aura® Session Managers 6.1, geographic redundant Avaya Session Border Controllers for Enterprise 4.0.5 and various Avaya endpoints.

The Avaya SIP-enabled enterprise solution implements geographic redundancy on Avaya Aura® Session Managers and Avaya Session Border Controllers for Enterprise to ensure the high availability of the enterprise SIP Trunk.

Bell Canada SIP Trunking Service features Least Cost Routing on outgoing calls from the enterprise. This feature uses a trunk group identification predefined by Bell Canada to route outgoing calls to PSTN call parties on the designed virtual routes within Bell Canada's networks. This approach generally results in lower cost for the enterprise and supports the billing strategy at Bell Canada.

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

These Application Notes describe the steps to configure Session Initiation Protocol (SIP) Trunking between Bell Canada SIP Trunking Service (Bell Canada) which features Least Cost Routing at Bell Canada Central Office (Bell Canada CO) and an Avaya SIP-enabled enterprise solution. The Avaya solution consists of Avaya Aura® Communication Manager Evolution Server (Communication Manager) 6.0.1, geographic redundant Avaya Aura® Session Managers (Session Manager) 6.1, geographic redundant Avaya Session Border Controllers for Enterprise (Avaya SBCE) 4.0.5 and various Avaya endpoints. This documented solution does not extend to configurations without Session Manager or the Avaya SBCE.

The Avaya SIP-enabled enterprise solution implements geographic redundancy on Session Managers and the Avaya SBCEs to ensure the high availability of the enterprise SIP Trunk. For normal operation, the enterprise SIP Trunk is established between Communication Manager, the primary Session Manager and the primary Avaya SBCE. When the primary Session Manager is out-of-service, the SIP Trunk shall failover to the secondary Session Manager. The same approach also applies when the primary Avaya SBCE is out-of-service, the SIP Trunk shall failover to the secondary Avaya SBCE. At a certain state of network failover, all the incoming and outgoing calls will be carried over the newly established SIP Trunk. When the failed enterprise server is back to in-service state, the OPTIONS heartbeat can detect the state changes then automatically recover the SIP Trunk to normal operation state.

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 the 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 a “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 the Avaya SBCE. This call authentication scheme as specified in RFC 3261 provides authentication for the SIP signaling.

Bell Canada also features Least Cost Routing for outgoing calls from the enterprise. The feature requires the “Contact” header of the SIP traffic from the enterprise in a specific format to contain the trunk group identification (tgrp) parameter. The “tgrp” is predefined by Bell Canada, it will be used by Bell Canada CO to route the call to the PSTN on designed virtual routes within Bell Canada networks. This approach generally results in lower cost for the enterprise and supports the billing strategy at Bell Canada.

2. Test Scope and Results

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.

Bell Canada is a member of the Avaya DevConnect Service Provider Program. The general test approach is to connect a simulated enterprise to the Vendor Validation Circuit through the Internet and exercise the features and functionalities listed in **Section 2.1**.

2.1 Interoperability Compliance testing

To verify the Least Cost Routing feature in combination with the geographic redundancy implementation on Session Manager and the Avaya SBCE, the following features and functionalities were covered during the interoperability compliance testing:

- Incoming and outgoing calls with network failover at the Avaya SBCE level.
- Incoming and outgoing calls with network failover at Session Manager level.
- Proactively overflowed outgoing calls by Communication Manager with Least Cost Routing enabled.
- Reactively overflowed outgoing calls by Communication Manager with Least Cost Routing enabled.

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

- Incoming PSTN calls to various phone types including SIP, H.323, digital and analog telephones at the enterprise. All incoming calls from the PSTN are routed to the enterprise across the SIP Trunk from the service provider.
- Outgoing PSTN calls from various phone types including SIP, H.323, digital and analog telephones at the enterprise. All outgoing calls to the PSTN are routed from the enterprise across the SIP Trunk to the service provider.
- Incoming and outgoing PSTN calls to/ from Avaya one-X® Communicator soft phone. Both the Avaya one-X® Communicator Computer Mode (where the Avaya one-X® Communicator is used for call control as well as audio path) and the Avaya one-X® Communicator Telecommuter Mode (where the 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 on the 1XC are tested.
- 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 on the test environment or not tested as part of the compliance testing, are listed as following:

- 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 calls 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 with the Avaya SIP-enabled enterprise solution was successfully completed with the exception of the observations/ limitations described below.

1. **The Calling Party Number of incoming calls contains a "+" character that needs to be deleted**. The incoming call from Bell Canada to the enterprise contains a "+" followed by 11-digit in the “From” header for the Calling Party Number. The EC500 mobility call feature does not work since the 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 the Avaya SBCE normalize the Calling Party Number in the “From” header to remove the plus sign then the calls work properly. For the detail configuration, please refer to **Section 7.2.5**.

2. **Fax over IP using G.711MU codec is successful**. For fax over IP, the service provider is recommended to support T.38 in order to work properly with Communication Manager. Communication Manager does not support fax call using G.711MU codec. However, when the **ip-codec-set** is set with "fax-off" as described in **Section 5.4**, 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. **When a SIP station consultative transfers an incoming call to a local H.323 station, the Calling Party Display is not correct**. The local H.323 station displays the Trunk-group Name and Trunk-group Access Code (TAC) instead of the Calling Party Name and Number of PSTN party. This is a known behavior of Communication Manager with no available resolution at this time. This issue has low user impact, it is listed here simply as an observation.

4. **When Communication Manager off-net redirects (by transferring or forwarding) an incoming or outgoing call back to PSTN, the 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 contain the Calling Party Number of the true connected PTSN parties. However, the Calling Party Number was not updated, both PSTN parties still display the Calling Party Name of the 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 the Calling Party Display update. This issue has low user impact, it is listed here simply as an observation.

5. **Perform an "Application Restart" on the Ayaya SBCE may cause the SigMa script and Authentication to stop working**. If the SigMa script and Authentication do not work after an "Application Restart", please contact Avaya for support on the Avaya SBCE. Note: The password for Authentication should not contain special characters (e.g., "!"). This is a known limitation of the Avaya SBCE with no available resolution at this time.

2.3 Support

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

For technical support on Bell Canada SIP Trunking Service, 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 Vendor Validation Circuit through the Internet.

For confidentiality and privacy purposes, the actual public IP addresses and PSTN routable phone numbers 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 System Manager
- Avaya S8800 Server running Session 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 Softphones (H.323 and SIP)
- Avaya Digital Telephones
- Avaya Analog Telephones

Located at the edge of the enterprise is the primary and secondary Avaya SBCE. Each Avaya SBCE has a public side that connects to Bell Canada networks and a private side that connects to the enterprise networks. All SIP and RTP traffic entering or leaving the enterprise flow through the Avaya SBCE. In this way, the Avaya SBCE can protect the enterprise against any SIP-based attacks. The Avaya SBCE provides Network Address Translation (NAT) at both the IP and SIP layers. The transport protocol between the Avaya SBCE and Bell Canada across the public networks is UDP, the same transport protocol UDP is also used between the 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 two enterprise public SIP domains as **cust2xxxx.xxxx.bell.ca** and **cust6xxxx.xxxx.bell.ca**. These public SIP domains will be used for the public SIP traffic between the primary and secondary Avaya SBCE and Bell Canada.

For Least Cost Routing feature, Bell Canada requires the outgoing SIP traffic from the enterprise with the "Contact" header has to be in a specific format. It should contain one of the two predefined "tgrp" values **vsxx_416XXX1396_01a** or **vsxx_416XXX1880_01a**. Each particular "tgrp" will assist Bell Canada CO in routing the calls to the PSTN on the designed virtual routes. Following are two examples of a proper "Contact" header with the "tgrp" set to **vsxx_416XXX1396_01a** and **vsxx_416XXX1880_01a**.

```
Contact: "Bell SIP x1882" <sip:416XXX1882;tgrp=vsxx_416XXX1396_01a;trunk-
context=sipxxxxxxxx.bell.ca@10.10.98.116:5060;user=phone>
```

```
Contact: "Bell SIP x1882" <sip:416XXX1882;tgrp=vsxx_416XXX1880_01a;trunk-
context=sipxxxxxxxx.bell.ca@10.10.98.116:5060;user=phone>
```

The Avaya Customer Premises Equipment (CPE) environment was configured with separate SIP Trunk groups between Communication Manager and Session Manager to carry traffic to and from the service provider. Any specific trunk or codec settings required by the service provider were applied only to these dedicated trunks so as not to affect other enterprise SIP traffic. An enterprise private SIP domain **avayalab.com** was created for the incoming trunk group and multiple enterprise private SIP subdomains were created for the outgoing trunk groups. Each enterprise private SIP subdomain was defined appropriately to each "tgrp" value obtained from Bell Canada. In the compliance testing, two outgoing trunk groups were defined appropriately to two "tgrp" values **vsxx_416XXX1396_01a** and **vsxx_416XXX1880_01a**. Therefore, two enterprise private SIP subdomains are defined for two outgoing trunk groups as **vsxx-416XXX1396-01a.avayalab.com** and **vsxx-416XXX1880-01a.avayalab.com** under the signaling group form on Communication Manager (see **Section 5.6**) and the SIP Domain on Session Manager (see **Section 6.2**).

Notes:

- Communication Manager and Session Manager do not allow special characters in the SIP domain name as per RFC 1035, thus the special character underscore "_" is replace with the dash "-" in the enterprise private SIP subdomains.
- In the real deployment, the enterprise may be assigned more than two "tgrp" values by Bell Canada. With each "tgrp", an outgoing trunk group will be created with an appropriate enterprise private SIP subdomain. Therefore, there may be more than two outgoing trunk groups need to be created. The sample configuration is just for two outgoing trunk groups, but it is also applicable to multiple outgoing trunk group deployments.

For incoming calls, the Topology-Hiding feature of the Avaya SBCE (see **Section 7.2.3**) will change all public service provider public SIP domains into the enterprise private SIP domain **avayalab.com** before forwarding the SIP traffic over the incoming trunk group to Communication Manager via Session Manager. Session Manager uses the configured Dial Patterns (see **Section 6.7**) and Routing Policies (see **Section 6.6**) to determine the recipient as Communication Manager and on which link to send the call. Once the call arrives at Communication Manager, further incoming call treatments, such as incoming digit translations (see **Section 5.11**) and class of service restrictions are performed.

For outgoing calls, the SIP traffic will be first processed by Communication Manager for outgoing feature treatment such as Automatic Route Selection (ARS) (see **Section 5.9**) to select the outgoing trunk groups and class of service restrictions. Once Communication Manager selects the proper SIP Trunk, the call will be routed to Session Manager. Session Manager uses the configured Dial Patterns (see **Section 6.7**) and Routing Policies (see **Section 6.6**) to determine the route to the Avaya SBCE for the egress traffic to Bell Canada networks. The SigMa script on the Avaya SBCE (see **Section 7.2.5**) extracts the "tgrp" value from the enterprise subdomains by deleting the suffix **.avayalab.com**, then constructs the real “tgrp” by replacing the dash “-“ with the underscore “_”. The SigMa script uses the “tgrp” value to normalize the “Contact” header as described above. Subsequently, the Avaya SBCE applies the Topology Hiding profile to change all enterprise private SIP domains into the service provider public SIP domains which are known to Bell Canada.

Two outgoing trunk groups were created to carry outgoing calls to Bell Canada. To do so, both trunk groups are tied to the same route pattern which is defined for the Alternate Route Selection (ARS) for outgoing calls (see **Section 5.9**). With two trunk groups in a route pattern, outgoing calls may be overflowed in the proactive mode or reactive mode to the next available trunk group. In the proactive mode, Communication Manager will proactively overflow the outgoing call to the next available trunk group when it detects the current trunk group is fully used. While in the reactive mode, it will overflows outgoing calls to the next available trunk group when the current trunk group is still available but outgoing calls on that trunk group are rejected by Bell Canada due to its capacity limit at Bell Canada CO.

In the compliance testing, geographic redundancy was implemented on Session Manager and the Avaya SBC. When the primary Session Manager is out of service, the SIP Trunk will be established between Communication Manager and the secondary Session Manager which will connect to the primary Avaya SBCE. If the primary Avaya SBCE is also out of service, then the SIP Trunk will be established between Communication Manager and the secondary Session Manager which will connect to the secondary Avaya SBCE. The detailed configuration for geographic redundancy will be discussed in **Section 6** for Session Manager and **Section 7** for the Avaya SBCE.

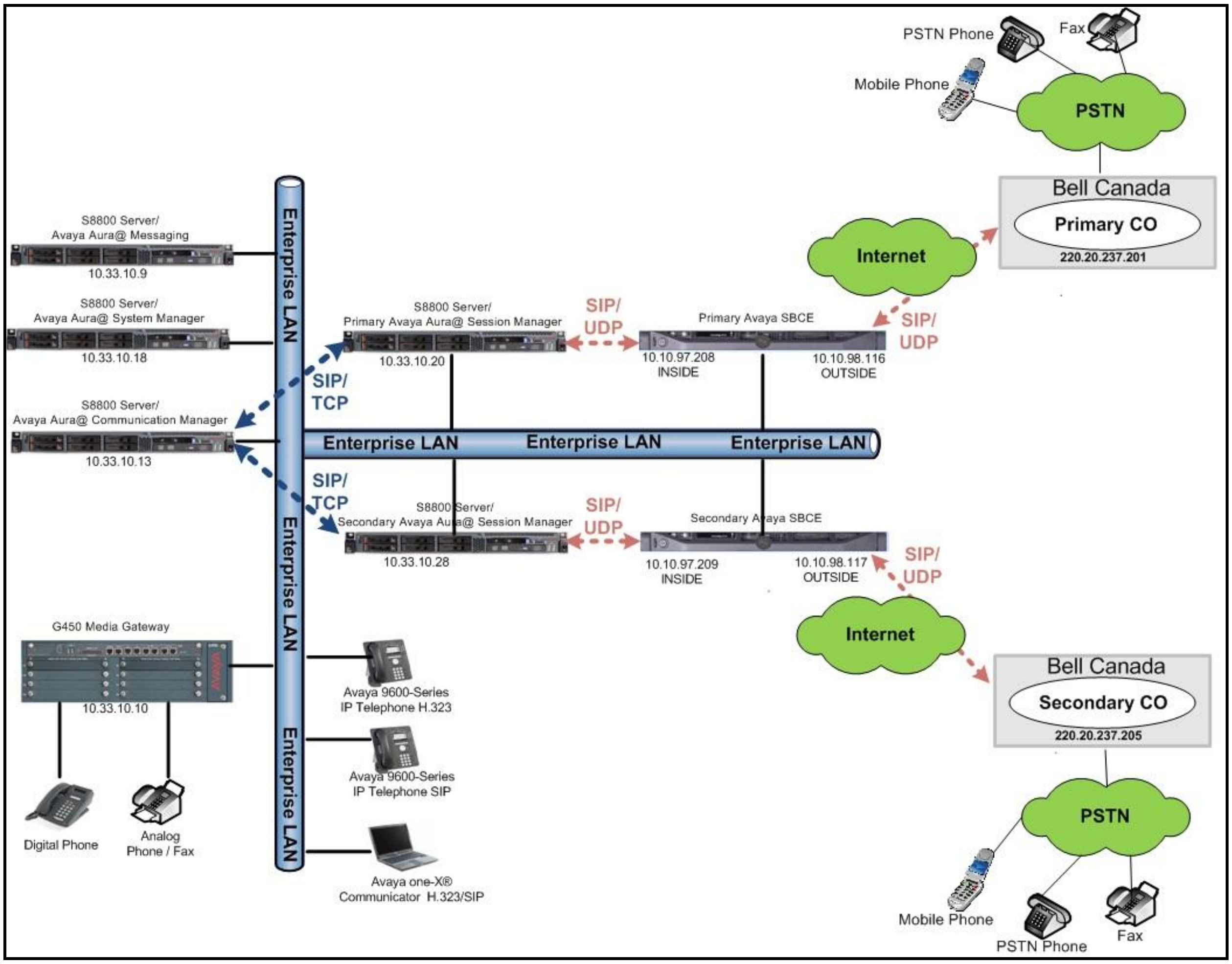


Figure 1: **Avaya IP Telephony Network Connecting to Bell Canada SIP Trunking Service**.

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 running on Avaya S8800 Server	6.0.1 (R016x.00.1.510.1-19940)
Avaya G450 Media Gateway FW Version HW Vintage	 31 .22 .0 1
Avaya Aura® Session Manager running on Avaya S8800 Server	6.1.7.0.617012
Avaya Aura® System Manager running on Avaya S8800 Server	6.1.5.0 (6.1.12.1.1960)
Avaya Aura® Messaging running on Avaya S8800 Server	6.1-11.0 (MSG-00.1.510.1-115_0205)
Avaya Session Border Controller for Enterprise	4.0.5 Q19
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
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 Service 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 the procedure for configuring Communication Manager for inter-operating with Bell Canada SIP Trunking Service. A SIP Trunk was created between Communication Manager and each Session Manager to be used for incoming signaling traffic from Bell Canada to the enterprise (for incoming calls to the enterprise from PSTN). For outgoing calls, Bell Canada requires the trunk group identification (tgrp) value in the "Contact" header. The "tgrp" is predefined to assist with Bell Canada Least Cost Routing feature. To achieve this, multiple SIP Trunks were created to carry outgoing signaling traffic to Bell Canada networks from the enterprise (for outgoing calls to the PSTN from the enterprise) with each SIP Trunk carrying a unique "tgrp" embedded as part of the enterprise private SIP domains. This implementation is used in combination with the SigMa scripts on the Avaya SBCE to extract the "tgrp" from the SIP domains then construct the "Contact" header as per the requirement from Bell Canada. During the compliance testing, Bell Canada provided two "tgrp" values as **vsxx-416XXX1396-01a** and **vsxx-416XXX1880-01a**.

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

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

5.1 Licensing and Capacity

Use the **display system-parameters customer-options** command to verify that the **Maximum Administered SIP Trunks** value on **Page 2** is sufficient to support the desired number of simultaneous SIP calls across all SIP Trunks at the enterprise including any trunks to and from the service provider. The example shows that **24000** licenses are available and **224** 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 4
             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: 18000 0
                   Maximum Video Capable IP Softphones: 18000 0
                       Maximum Administered SIP Trunks: 24000 224
  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 the **change system-parameters features** command to set the **Trunk-to-Trunk Transfer** field to **all** to allow incoming calls from the PSTN to be transferred to another PSTN endpoint. If for security reasons, incoming calls should not be allowed to transfer back to the PSTN then leave the field set to **none**.

```
display system-parameters features                              Page   1 of  19
                            FEATURE-RELATED SYSTEM PARAMETERS
                               Self Station Display Enabled? n
                                    Trunk-to-Trunk Transfer: all
               Automatic Callback with Called Party Queuing? n
    Automatic Callback - No Answer Timeout Interval (rings): 3
                       Call Park Timeout Interval (minutes): 10
        Off-Premises Tone Detect Timeout Interval (seconds): 20
                                 AAR/ARS Dial Tone Required? Y
```

On **Page 9** verify that a text string has been defined to replace the 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.

```
display 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
```

5.3 IP Node Names

Use the **change node-names ip** command to verify that node names have been previously defined for the IP addresses of Communication Manager (**procr**), the primary Session Manager

(**SM61A**) and the secondary Session Manager (**SM61B**). These node names will be used to define the signaling groups in **Section 5.6**.

```
change node-names ip                                            Page   1 of   2
                                  IP NODE NAMES
    Name              IP Address
AAM                 10.33.10.9
SBCE                10.10.97.189
SM61A               10.33.10.20
SM61B               10.33.10.28
default             0.0.0.0
procr               10.33.10.13
procr6              ::
```

5.4 Codecs

Use the **change ip-codec-set** command to define a list of codecs to use for calls between the enterprise and the service provider. For the compliance testing, Bell Canada configured their network for G.711MU codec for voice calls. Thus, the **ip-codec-set** is set to enable only G.711 codec in the **Audio Codec** column of the table. Default values can be used for all other fields. The following screen shows the codec set 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 the **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 calls on Communication Manager, they are treated like regular voice calls using G.711 codec. For more information, see **Section 2.2**, observation 2.

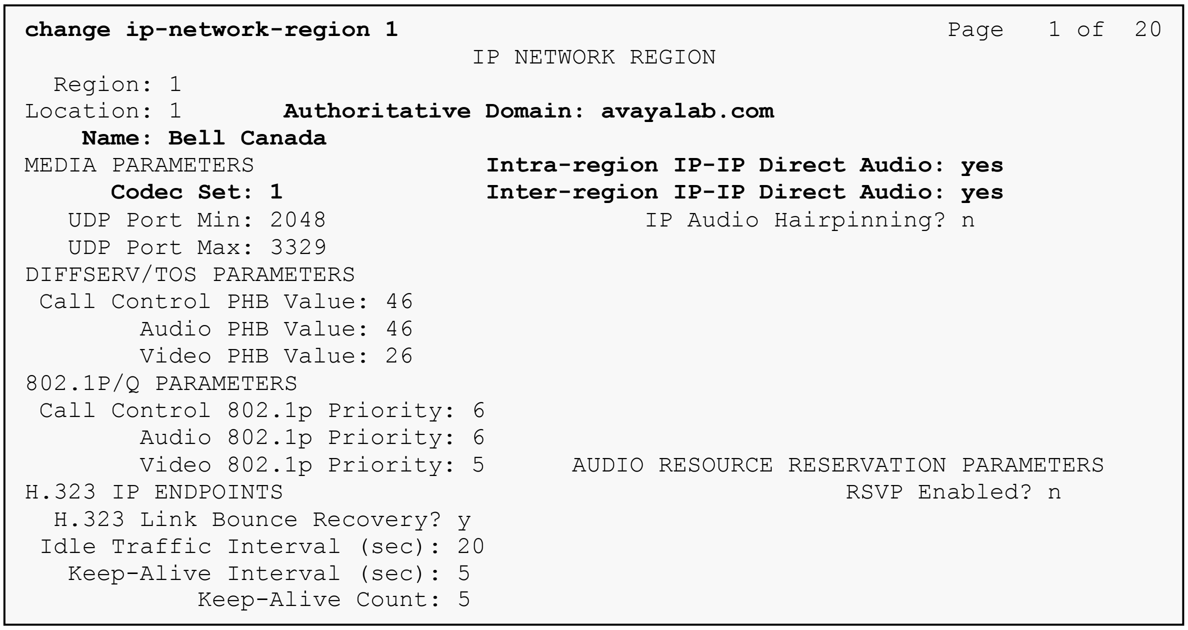
```
change ip-codec-set 1                                           Page   2 of   2

                          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

Create a separate IP network region for the service provider trunk groups. This allows for separate codec or quality of service settings to be used (if necessary) for calls between the enterprise and the service provider versus calls within the enterprise or elsewhere.

For the compliance testing, **ip-network-region 1** was created. Use the **change ip-network-region 1** command to configure region 1 with the following parameters:

- Set the **Authoritative Domain** field to match the SIP domain of the enterprise. In this configuration, the domain name **avayalab.com** is assigned to the test environment in the Avaya test lab. This domain name appears in the "From", "P-Asserted-Identity" and "Diversion" headers of SIP messages originating from this IP network region.
- Enter a descriptive name in the **Name** field.
- Enable **IP-IP Direct Audio** (shuffling) to allow audio traffic to be sent directly between IP endpoints without using media resources in the Media Gateway. Set both **Intra-region** and **Inter-region IP-IP Direct Audio** to **yes.** This is the default setting. Shuffling can be further restricted at the trunk level on the Signaling Group forms in **Section 5.6**.
- Set the **Codec Set** field to the IP codec set defined in **Section 5.4**.
- Default values can be used for all other fields.



```
change ip-network-region 1                                      Page   1 of  20
                               IP NETWORK REGION
  Region: 1
Location: 1       Authoritative Domain: avayalab.com
    Name: Bell Canada
MEDIA PARAMETERS                Intra-region IP-IP Direct Audio: yes
      Codec Set: 1              Inter-region IP-IP Direct Audio: yes
   UDP Port Min: 2048                      IP Audio Hairpinning? n
   UDP Port Max: 3329
DIFFSERV/TOS PARAMETERS
 Call Control PHB Value: 46
        Audio PHB Value: 46
        Video PHB Value: 26
802.1P/Q PARAMETERS
 Call Control 802.1p Priority: 6
        Audio 802.1p Priority: 6
        Video 802.1p Priority: 5      AUDIO RESOURCE RESERVATION PARAMETERS
H.323 IP ENDPOINTS                                       RSVP Enabled? n
  H.323 Link Bounce Recovery? y
 Idle Traffic Interval (sec): 20
   Keep-Alive Interval (sec): 5
            Keep-Alive Count: 5
```

On **Page 4**, define the IP codec set to be used for traffic between region 1 and other regions. Enter the desired IP codec set in the **codec set** column of the row with destination region (**dst rgn**) 1. Default values may be used for all other fields. In the compliance testing, Communication Manager, Session Managers, the Avaya SBCEs and IP phones were assigned to the same region 1. The screenshot below 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
```

Non-IP telephones (e.g., analog, digital) derive network region from the 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 the IP network map configuration 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 are assigned to network region 1. These include Communication Manager, Session Managers and the Avaya SBCEs that were set up for the test environment. IP telephones used for the compliance testing, including both the Avaya 9600 IP Telephones and the Avaya one-X® Communicator soft phones, are assigned to network region 1 with IP addresses in the **10.10.98.0/24** 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: 10.10.98.0                              /24    1      n
   TO: 10.10.98.255
 FROM:                                         /             n
   TO:
```

5.6 Signaling Group

Use the **add signaling-group** command to create a single signaling group for incoming calls and multiple signaling groups for outgoing calls between Communication Manager and each Session Manager. While the incoming signaling group is used to receive calls with SIP domain **avayalab.com**, the outgoing signaling groups are used to originate calls with a SIP domain containing the “tgrp” as part of the FQDN. This implementation on outgoing calls is to meet the requirement from Bell Canada for Least Cost Routing feature.

In the compliance testing, geographic redundancy was implemented on Session Manager. Therefore, the signaling groups configured for the primary Session Manager (as described in

Section 5.6.1 below) will be duplicated to the secondary Session Manager (as described in **Section 5.6.2** below).

5.6.1 Signaling Group for the Primary Avaya Aura® Session Manager

For the compliance testing, the signaling group 1 was established between Communication Manager and the primary Session Manager for incoming calls. It was configured using the parameters highlighted below:

- Set the **Group Type** field to **sip**.
- Set the **IMS Enabled** field to **n**. This specifies Communication Manager will serve as an Evolution Server.
- Set the **Transport Method** to the value of **tcp**. The transport method specified here is used between Communication Manager and the primary Session Manager.
- Set the **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 the **Near-end Listen Port** and **Far-end Listen Port** set to **5160**.
- Set the **Peer Detection Enabled** field to **n** and the **Peer Server** field to **SM**.
- Set the **Near-end Node Name** to **procr**. This node name maps to the IP address of Communication Manager as defined in **Section 5.3**.
- Set the **Far-end Node Name** to **SM601A**. This node name maps to the IP address of the primary Session Manager as defined in **Section 5.3**.
- Set the **Far-end Network Region** to the IP network region defined for the service provider in **Section 5.5**.
- Set the **Far-end Domain** to **avayalab.com**.
- Set **Direct IP-IP Audio Connections** to **y**. This field will enable media shuffling on the SIP Trunk allowing Communication Manager to redirect media traffic directly between the SIP Trunk and the enterprise endpoint.
- Set the **DTMF over IP** field to **rtp-payload**. This setting enables Communication Manager to send out-of-band DTMF as per RFC 2833.
- Set the **Enable Layer 3 Test?** to **y** to allow Communication Manager to send OPTIONS heartbeat to monitor the status of SIP Trunk connecting to Session Manager.
- Verify that the **Initial IP-IP Direct Media** is set to **n**, this is the default value.
- Change default setting of **6** for **Alternate Route Timer (sec)** to **30**. This allows more time for a PSTN call to complete through Bell Canada networks.
- Default values may be used for all other fields.

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

 Group Number: 1             Group Type: sip
  IMS Enabled? n       Transport Method: tcp
        Q-SIP? n                                               SIP Enabled LSP? n
     IP Video? n                                    Enforce SIPS URI for SRTP? y
  Peer Detection Enabled? n  Peer Server: SM



   Near-end Node Name: procr                   Far-end Node Name: SM61A
 Near-end Listen Port: 5160                  Far-end Listen Port: 5160
                                          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? y                   Initial IP-IP Direct Media? n
H.323 Station Outgoing Direct Media? n            Alternate Route Timer(sec): 30
```

For outgoing calls, Bell Canada provides two “tgrp” values **vsxx_416XXX1396_01a** and **vsxx_416XXX1880_01a** that need to be sent in the “Contact” header. This manipulation is achieved by the SigMa script on the Avaya SBCE. To assist the SigMa script, the trunk group for outgoing calls, however, will be configured with **Far-end Domain** containing the predefined “tgrp”. In appropriate to two “tgrp” values, there were two signaling groups created for the primary Session Manager. The signaling groups were similarly configured as signaling group 1 as described above except the **Far-end Domain** was set to **vsxx-416XXX1396-01a.avayalab.com** or **vsxx-416XXX1880-01a.avayalab.com**. For the compliance testing, signaling group 2 and 3 were created for this purpose and are shown below:

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

 Group Number: 2             Group Type: sip
  IMS Enabled? n       Transport Method: tcp
        Q-SIP? n                                               SIP Enabled LSP? n
     IP Video? n                                    Enforce SIPS URI for SRTP? y
  Peer Detection Enabled? n  Peer Server: SM



   Near-end Node Name: procr                   Far-end Node Name: SM61A
 Near-end Listen Port: 5260                  Far-end Listen Port: 5260
                                          Far-end Network Region: 1

Far-end Domain: vsxx-416XXX1396-01a.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? y                   Initial IP-IP Direct Media? n
H.323 Station Outgoing Direct Media? n            Alternate Route Timer(sec): 30
```

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

 Group Number: 3             Group Type: sip
  IMS Enabled? n       Transport Method: tcp
        Q-SIP? n                                               SIP Enabled LSP? n
     IP Video? n                                     Enforce SIPS URI for SRTP? y
  Peer Detection Enabled? n  Peer Server: SM



   Near-end Node Name: procr                  Far-end Node Name: SM61A
 Near-end Listen Port: 5360                 Far-end Listen Port: 5360
                                         Far-end Network Region: 1

Far-end Domain: vsxx-416XXX1880-01a.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? y                   Initial IP-IP Direct Media? n
H.323 Station Outgoing Direct Media? n            Alternate Route Timer(sec): 30
```

Note: The sample configuration was for 2 outgoing trunk groups. If the deployment in the field requires more outgoing trunk groups then more signaling groups for outgoing calls will need to be appropriately created.

5.6.2 Signaling Group for the Secondary Avaya Aura® Session Manager

For the compliance testing, signaling group 11 was established between Communication Manager and the secondary Session Manager for incoming calls. It was similarly configured as signaling group 1 in **Section 5.6.1**.

```
add signaling-group 11                                         Page   1 of   1
                                SIGNALING GROUP

 Group Number: 11            Group Type: sip
  IMS Enabled? n       Transport Method: tcp
        Q-SIP? n                                               SIP Enabled LSP? n
     IP Video? n                                     Enforce SIPS URI for SRTP? y
  Peer Detection Enabled? n  Peer Server: SM



   Near-end Node Name: procr                  Far-end Node Name: SM61B
 Near-end Listen Port: 5160                 Far-end Listen Port: 5160
                                         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? y                   Initial IP-IP Direct Media? n
H.323 Station Outgoing Direct Media? n            Alternate Route Timer(sec): 30
```

For outgoing calls, signaling group 12 and 13 were created to connect Communication Manager with the secondary Session Manager. They were similarly configured as signaling group 2 and 3 as described in **Section 5.6.1**.

```
add signaling-group 12                                         Page   1 of   1
                                SIGNALING GROUP

 Group Number: 12             Group Type: sip
  IMS Enabled? n        Transport Method: tcp
        Q-SIP? n                                               SIP Enabled LSP? n
     IP Video? n                                     Enforce SIPS URI for SRTP? y
  Peer Detection Enabled? n  Peer Server: SM



   Near-end Node Name: procr                 Far-end Node Name: SM61B
 Near-end Listen Port: 5260                Far-end Listen Port: 5260
                                        Far-end Network Region: 1

Far-end Domain: vsxx-416XXX1396-01a.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? y                       Initial IP-IP Direct Media? n
H.323 Station Outgoing Direct Media? n                Alternate Route Timer(sec): 30
```

```
add signaling-group 13                                         Page   1 of   1
                                SIGNALING GROUP

 Group Number: 3              Group Type: sip
  IMS Enabled? n        Transport Method: tcp
        Q-SIP? n                                               SIP Enabled LSP? n
     IP Video? n                                     Enforce SIPS URI for SRTP? y
  Peer Detection Enabled? n  Peer Server: SM



   Near-end Node Name: procr                 Far-end Node Name: SM61B
 Near-end Listen Port: 5360                Far-end Listen Port: 5360
                                        Far-end Network Region: 1

Far-end Domain: vsxx-416XXX1880-01a.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? y                       Initial IP-IP Direct Media? n
H.323 Station Outgoing Direct Media? n                Alternate Route Timer(sec): 30
```

5.7 Trunk Group

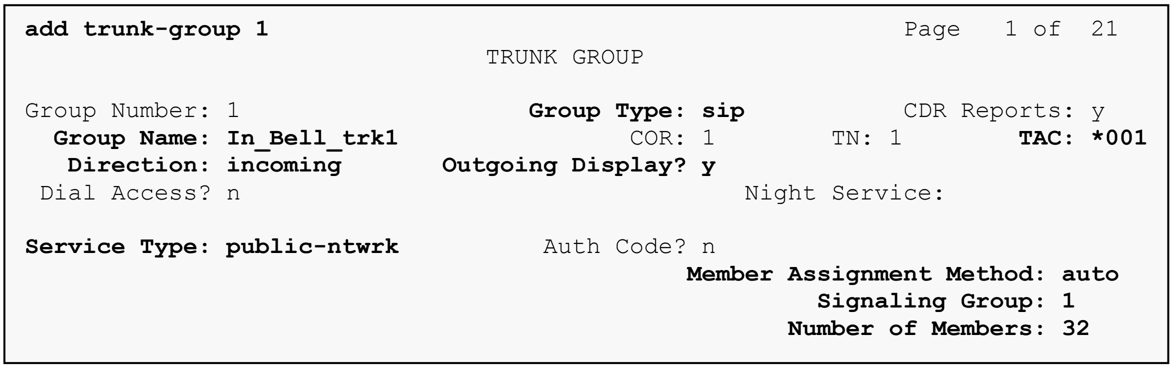
Use the **add trunk-group** command to create a single trunk group for incoming calls and multiple trunk groups for outgoing calls between Communication Manager and each Session Manager. The trunk groups were created for each of the signaling groups created in **Section 5.6**.

In the compliance testing, geographic redundancy was implemented on Session Manager. Therefore, the trunk groups configured for the primary Session Manager (as described in **Section 5.7.1** below) will be replicated to the secondary Session Manager (as described in **Section 5.7.2** below).

5.7.1 Trunk Group for the Primary Avaya Aura® Session Manager

For the compliance testing, the trunk group 1 was configured for incoming calls and trunk group 2 and 3 were configured for outgoing calls through the primary Session Manager. The trunk groups were created using the parameters highlighted below.

- Set the **Group Type** field to **sip**.
- Enter a descriptive name for the **Group Name**.
- Enter an available trunk access code (**TAC**) that is consistent with the existing dial plan in the **TAC** field.
- Set the **Direction** field to **incoming** for trunk group 1 and **outgoing** for trunk group 2 and 3.
- Set the **Outgoing Display** to **y** to enable name display on the trunk.
- Set the **Service Type** field to **public-ntwrk**.
- Set **Member Assignment Method** to **auto**.
- Set the **Signaling Group** to the appropriate signaling group shown in **Section 5.6.1**, (i.e., signaling group 1 for incoming trunk group 1 and signaling group 2 and 3 for outgoing trunk group 2 and 3).
- Set the **Number of Members** field to **32**. It is the number of trunk members in the SIP Trunk group. This value determines how many simultaneous SIP calls can be supported by this trunk.
- Default values were used for all other fields.



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

Group Number: 1                    Group Type: sip          CDR Reports: y
  Group Name: In_Bell_trk1                COR: 1        TN: 1        TAC: *001
   Direction: incoming      Outgoing Display? y
 Dial Access? n                                   Night Service:

Service Type: public-ntwrk          Auth Code? n
                                               Member Assignment Method: auto
                                                        Signaling Group: 1
                                                      Number of Members: 32
```

On **Page 2**, verify that the **Preferred Minimum Session Refresh Interval (sec)** is set to a value acceptable to the service provider. This value defines the interval that subsequent INVITEs must be sent to keep the active session alive. For the compliance testing, the value of **300** seconds was used. Set the **Disconnect Supervision** to **y**, this setting is to enable the incoming call redirection using Vector Directory Number as discussed in **Section 5.10**.

```
add trunk-group 1                                            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 the **Numbering Format** field to **private**. This field specifies the format of the calling party number (CPN) sent to the far-end. On Communication Manager, public numbers are automatically preceded with a + sign when passed in the “From”, “Contact” and “P-Asserted Identity” headers. The addition of the + sign impacted interoperability with Bell Canada. Thus, the **Numbering Format** was set to **private** and the **Numbering Format** in the route pattern 2 was set to **unk-unk** (see **Section 5.9**).

Set the **Replace Restricted Numbers** and **Replace Unavailable Numbers** fields to **y**. This will allow the CPN displayed on local endpoints to be replaced with the value set in **Section 5.2**, if incoming calls enabled CPN blocking.

```
add trunk-group 1                                            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
```

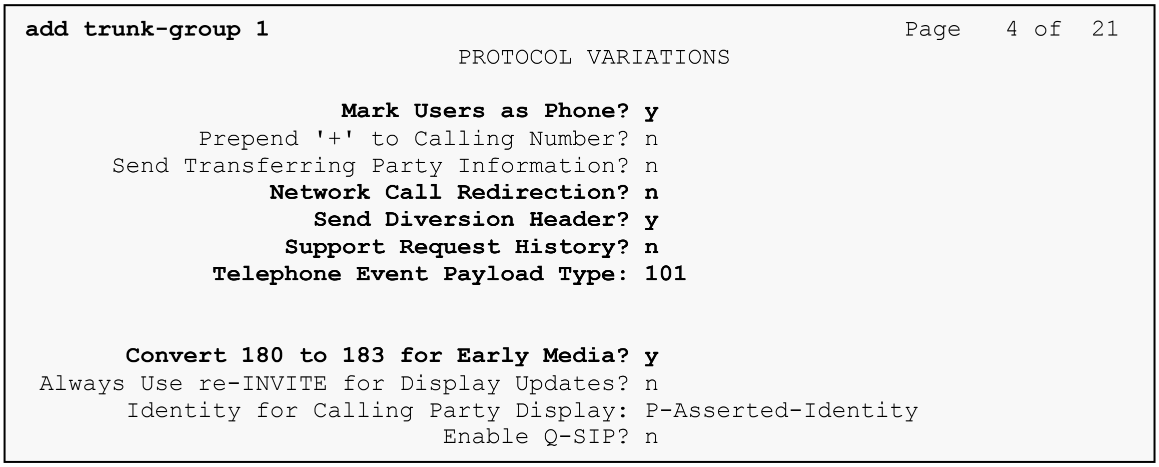
On **Page 4**, set the **Network Call Redirection** field to **n**. This setting is to use subsequent INVITE to off-net transfer an incoming call back to PSTN instead of using REFER method. Note: REFER is not supported by Bell Canada in the compliance testing.

Set the **Mark Users as Phones** field to **y**. This field indicates the calls are made by the telephone set. Note: If the **Mark Users as Phones** field is set to **n**, Bell Canada will reject outgoing calls.

Set the **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 incoming calls back to the PSTN and Extension to Cellular (EC500) call scenarios.

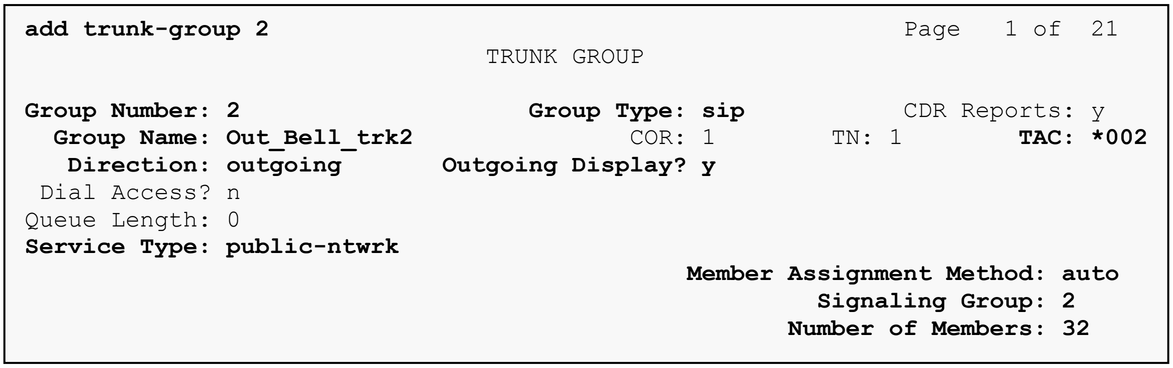
Set the **Support Request History** field to **n**. This setting disables the “History-Info” header in the call-redirection INVITE from the enterprise.

Set the **Telephone Event Payload Type** to **101**, the value preferred by Bell Canada. Set the **Convert 180 to 183 for Early Media** field to **y**.

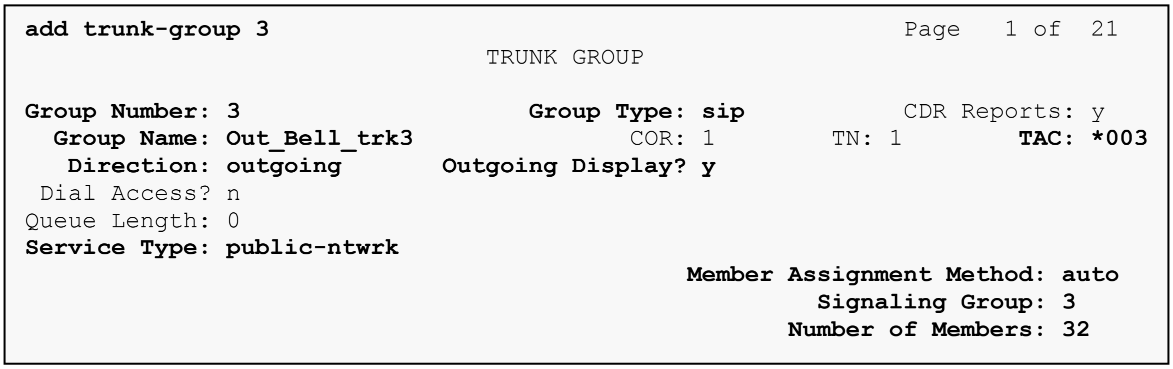


```
add trunk-group 1                                            Page   4 of  21
                              PROTOCOL VARIATIONS

                      Mark Users as Phone? y
            Prepend '+' to Calling 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
                             Enable Q-SIP? n
```

The outgoing trunk group 2 and 3 were similarly configured except the **Direction** was set to “outgoing” and **Signaling Group** was set to 2 and 3 appropriately. The screens below show **Page 1** of trunk group 2 and 3 for outgoing calls from the enterprise.



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

Group Number: 2                    Group Type: sip           CDR Reports: y
  Group Name: Out_Bell_trk2               COR: 1        TN: 1        TAC: *002
   Direction: outgoing       Outgoing Display? y
 Dial Access? n
Queue Length: 0
Service Type: public-ntwrk
                                              Member Assignment Method: auto
                                                       Signaling Group: 2
                                                     Number of Members: 32
```

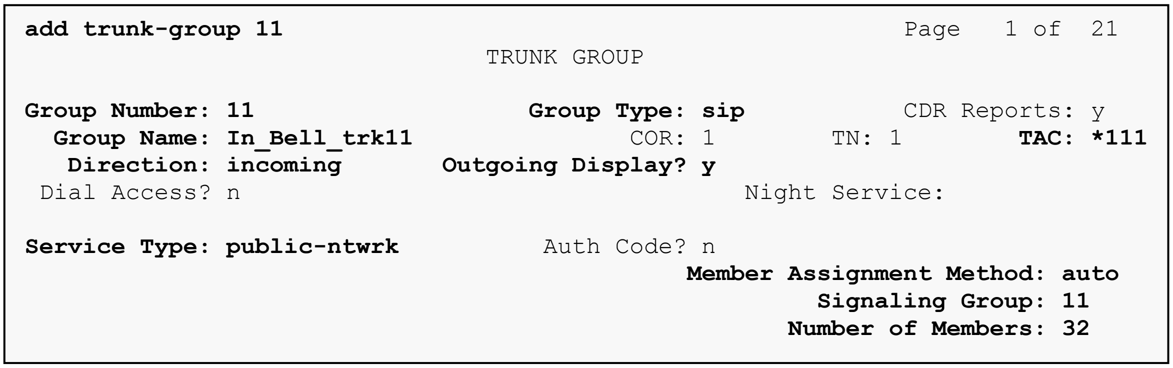


```
add trunk-group 3                                            Page   1 of  21
                                TRUNK GROUP

Group Number: 3                    Group Type: sip           CDR Reports: y
  Group Name: Out_Bell_trk3               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
```

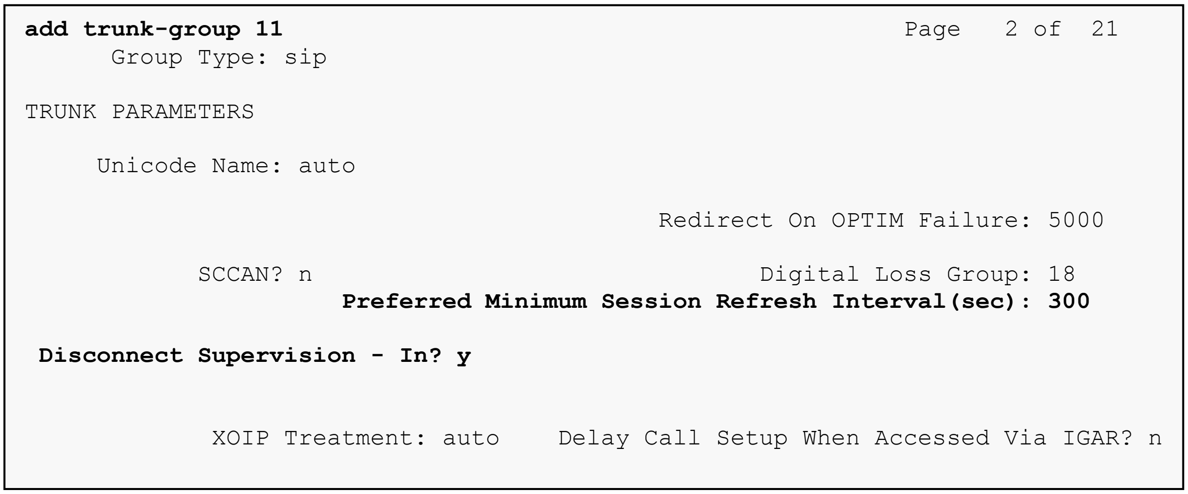
The configurations on other pages of trunk group 2 and 3 are identical to trunk group 1.

5.7.2 Trunk Group for the Secondary Avaya Aura® Session Manager

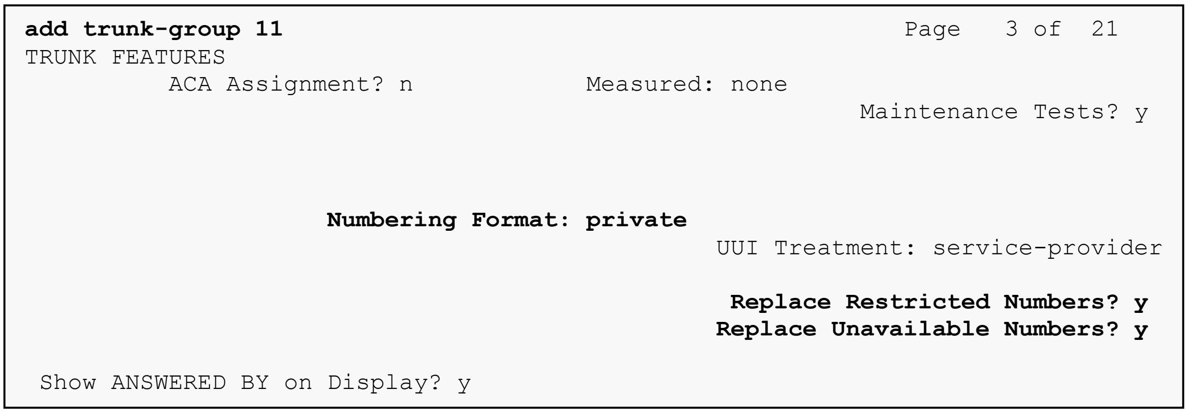
For the compliance testing, trunk group 11 was configured for incoming calls and trunk group 12 and 13 were configured for outgoing calls through the secondary Session Manager. The trunk groups were similarly configured as the trunk groups created for the primary Session Manager as described in **Section 5.7.1**. The screenshots below show the configuration of the incoming trunk group 11.



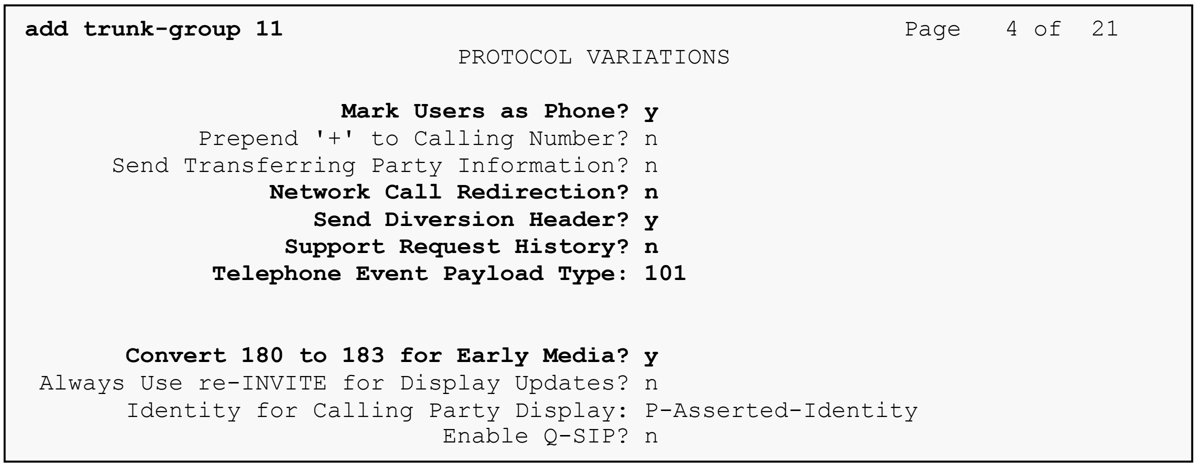
```
add trunk-group 11                                           Page   1 of  21
                                TRUNK GROUP

Group Number: 11                   Group Type: sip           CDR Reports: y
  Group Name: In_Bell_trk11               COR: 1        TN: 1        TAC: *111
   Direction: incoming       Outgoing Display? y
 Dial Access? n                                    Night Service:

Service Type: public-ntwrk          Auth Code? n
                                              Member Assignment Method: auto
                                                       Signaling Group: 11
                                                     Number of Members: 32
```



```
add trunk-group 11                                           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


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

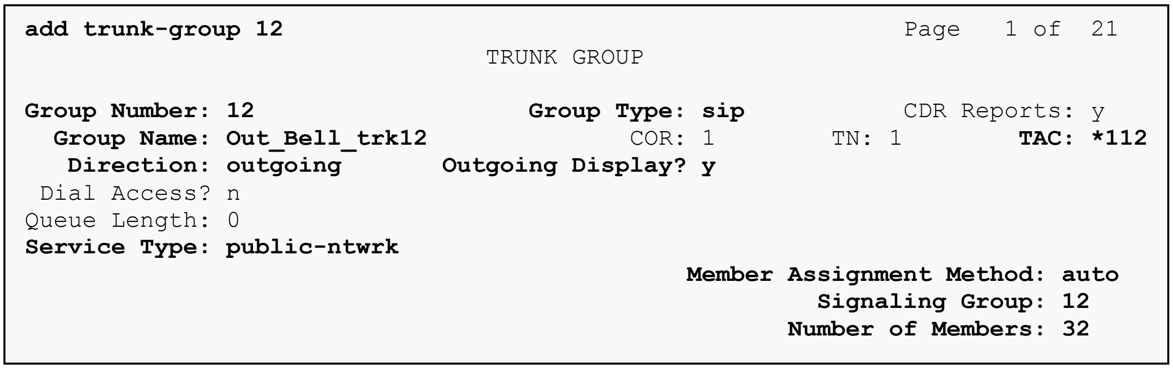


```
add trunk-group 11                                           Page   3 of  21
TRUNK FEATURES
          ACA Assignment? n            Measured: none
                                                          Maintenance Tests? y



                     Numbering Format: private
                                                UUI Treatment: service-provider

                                                 Replace Restricted Numbers? y
                                                Replace Unavailable Numbers? y

 Show ANSWERED BY on Display? y
```

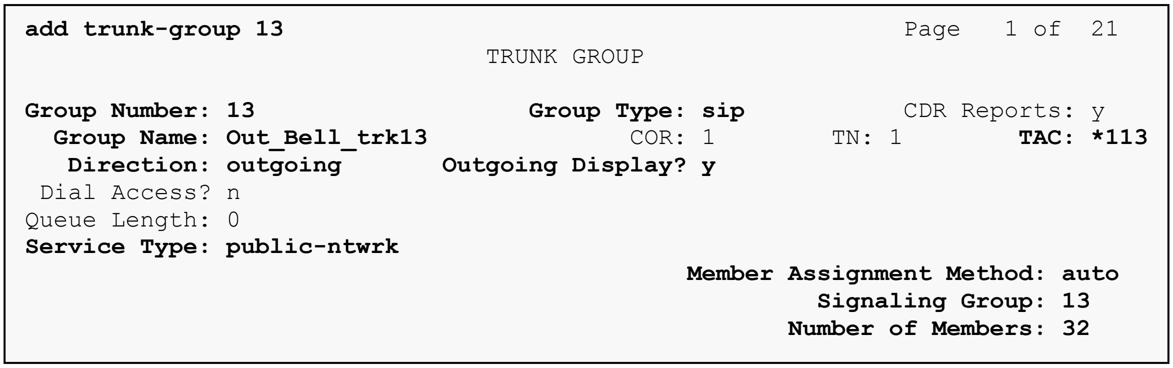


```
add trunk-group 11                                              Page   4 of  21
                                 PROTOCOL VARIATIONS

                      Mark Users as Phone? y
            Prepend '+' to Calling 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
                           Enable Q-SIP? n
```

The outgoing trunk group 12 and 13 were similarly configured except the **Direction** was set to "outgoing" and **Signaling Group** was set to 12 and 13 appropriately. The screens below show **Page 1** of trunk group 12 and 13 for outgoing calls from the enterprise.



```
add trunk-group 12                                              Page   1 of  21
                                   TRUNK GROUP

Group Number: 12                   Group Type: sip          CDR Reports: y
  Group Name: Out_Bell_trk12              COR: 1        TN: 1        TAC: *112
   Direction: outgoing       Outgoing Display? y
 Dial Access? n
Queue Length: 0
Service Type: public-ntwrk
                                              Member Assignment Method: auto
                                                       Signaling Group: 12
                                                     Number of Members: 32
```



```
add trunk-group 13                                              Page   1 of  21
                                   TRUNK GROUP

Group Number: 13                   Group Type: sip          CDR Reports: y
  Group Name: Out_Bell_trk13              COR: 1        TN: 1        TAC: *113
   Direction: outgoing       Outgoing Display? y
 Dial Access? n
Queue Length: 0
Service Type: public-ntwrk
                                              Member Assignment Method: auto
                                                       Signaling Group: 13
                                                     Number of Members: 32
```

The configurations on other pages of trunk group 12 and 13 are identical to the trunk group 11.

5.8 Calling Party Information

The 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 the **change**

private-numbering command to create an entry for each extension which has a DID assigned. The DID numbers are provided by the service provider. It is used 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 compliance testing, all stations with a 4-digit extension beginning with 13 or 18 will send the Calling Party Number as the **Private Prefix** plus the extension number on the trunk groups created in **Section 5.7**.

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

Ext Ext            Trk        Private          Total
Len Code           Grp(s)     Prefix           Len
 4  13             1-3        416XXX           10    Total Administered: 4
 4  13             11-13      416XXX           10       Maximum Entries: 540
 4  18             1-3        416XXX           10
 4  18             11-13      416XXX           10
```

Even though private numbering was selected, currently the number used in the SIP 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: 4
 4  13            1-3       416XXX           10       Maximum Entries: 9999
 4  13            11-13     416XXX           10
 4  18            1-3       416XXX           10     Note: If an entry applies to
 4  18            11-13     416XXX           10    a SIP connection to Avaya
                                                    Aura(tm) Session Manager,
                                                     the resulting number must
                                                   be a complete E.164 number.
```

5.9 Outbound Routing

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

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

    Dialed   Total  Call      Dialed   Total  Call      Dialed   Total  Call
    String   Length Type      String   Length Type      String   Length Type
   13          4   ext
   18          4   ext
   6           1   dac
   9           1   dac
   *           4   dac
```

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

```
change feature-access-codes                                Page   1 of  10
                               FEATURE ACCESS CODE (FAC)
         Abbreviated Dialing List1 Access Code:
         Abbreviated Dialing List2 Access Code:
         Abbreviated Dialing List3 Access Code:
Abbreviated Dial - Prgm Group List Access Code:
                      Announcement Access Code: *007
                       Answer Back Access Code:
                         Attendant Access Code:
      Auto Alternate Routing (AAR) Access Code: 6
    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:
                         Call Park Access Code:
                       Call Pickup Access Code:
CAS Remote Hold/Answer Hold-Unhold Access Code:
                  CDR Account Code Access Code:
                        Change COR Access Code:
                   Change Coverage Access Code:
            Conditional Call Extend Activation:        Deactivation:
                   Contact Closure   Open Code:          Close Code:
```

Use the **change ars analysis** command to configure the routing of dialed digits following the first digit 9. The example below shows a subset of the dialed strings tested as part of the compliance testing. See **Section 2.1** for the complete list of call types tested. All dialed strings are mapped to route pattern 2 (as defined next) for outgoing calls and for the vector call redirection on the SIP Trunk to the service provider.

```
change ars analysis 0                                      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    2        pubu         n
    1                     11   11    2        pubu         n
    411                   3    3     2        svcl         n
    416                   10   10    2        pubu         n
    613                   10   10    2        pubu         n
```

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

The example below shows the values used for route pattern 2 for outgoing calls.

- **Pattern Name**: Enter a descriptive name.
- **Grp No**: Enter the outgoing trunk group for the service provider. For the compliance testing, trunk group 2, 3, 12 and 13 were used.
- **FRL**: Set the Facility Restriction Level (**FRL**) field to a level that allows access to this trunk for all users that require it. The value of **0** is the least restrictive level.
- **Numbering Format**: **unk-unk**. All calls using this route pattern will use the private numbering table. See setting of the **Numbering Format** in the trunk group form for full details in **Section 5.7**.
- **LAR**: **next**

For the geographic redundancy implementation on Session Manager, outgoing calls are firstly routed to the primary Session Manager then to the secondary Session Manager. To achieve this, the route pattern 2 will be configured with trunk group 2 and 3 to the primary Session Manager at the order 1 and 2 which are higher priority than trunk group 12 and 13 to the secondary Session Manager at the order 3 and 4.

```
change route-pattern 2                                         Page   1 of   3
                    Pattern Number: 2   Pattern Name: Bell_cust6
                             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: 2    0                                                             n   user
 2: 3    0                                                             n   user
 3: 12   0                                                             n   user
 4: 13   0                                                             n   user
 5:                                                                    n   user
 6:                                                                    n   user

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

5.10 Vector Directory Numbers (VDNs)

This section describes the basic commands used to configure Vector Directory Numbers (VDNs) 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
```

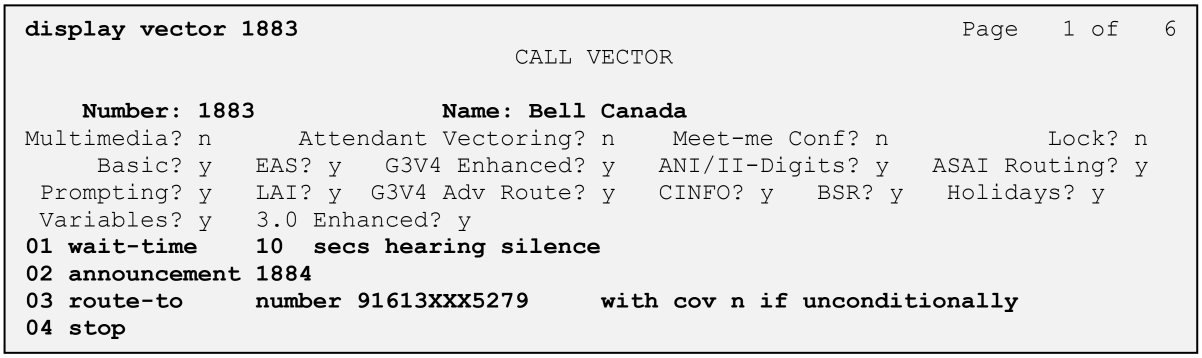
5.10.1 Pre-Answer Redirection to a PSTN Destination

The VDN 1883 was associated with vector 1883, which is shown below. For the pre-answer redirection, the 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

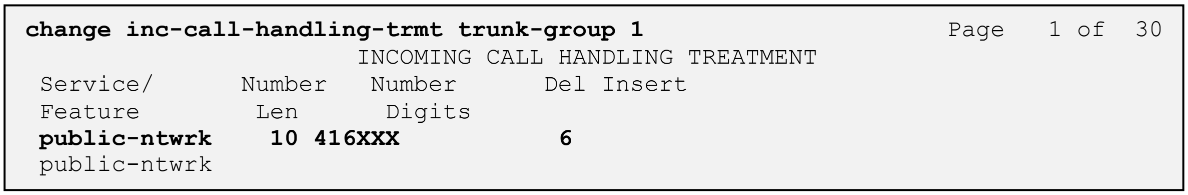
For post-answer redirection, the vector 1883 was configured to play an announcement (step 02) after answering the call. After the announcement, the **route-to number** (step 03) includes 91613XXX5279 where the digit 9 is the ARS feature access code as discussed in **Section 5.9** and the number 1613XXX5279 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.



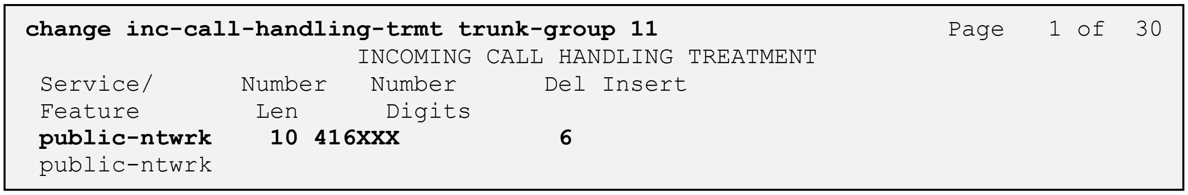
```
display vector 1883                                                Page   1 of   6
                                  CALL VECTOR

    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 either the primary Session Manager or the secondary Session Manager, Communication Manager applies incoming handling treatment on incoming trunk group 1 or trunk group 11 (the incoming trunk groups are discussed in **Section 5.7**). Bell Canada sends 10 digits in “Request-URI” and “To” headers to the assigned DID number. The incoming call handling treatment will translate the 10-digit DID number with prefix **416XXX** to 4-digit based extensions. To do this, use the **inc-call-handling-trmt trunk-group** command to define an incoming handling for Bell Canada. Following screenshots show the configuration in detail on incoming trunk group 1 and 11.



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



```
change inc-call-handling-trmt trunk-group 11                      Page   1 of  30
                       INCOMING CALL HANDLING TREATMENT
 Service/      Number   Number      Del Insert
 Feature        Len      Digits
 public-ntwrk    10 416XXX           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:

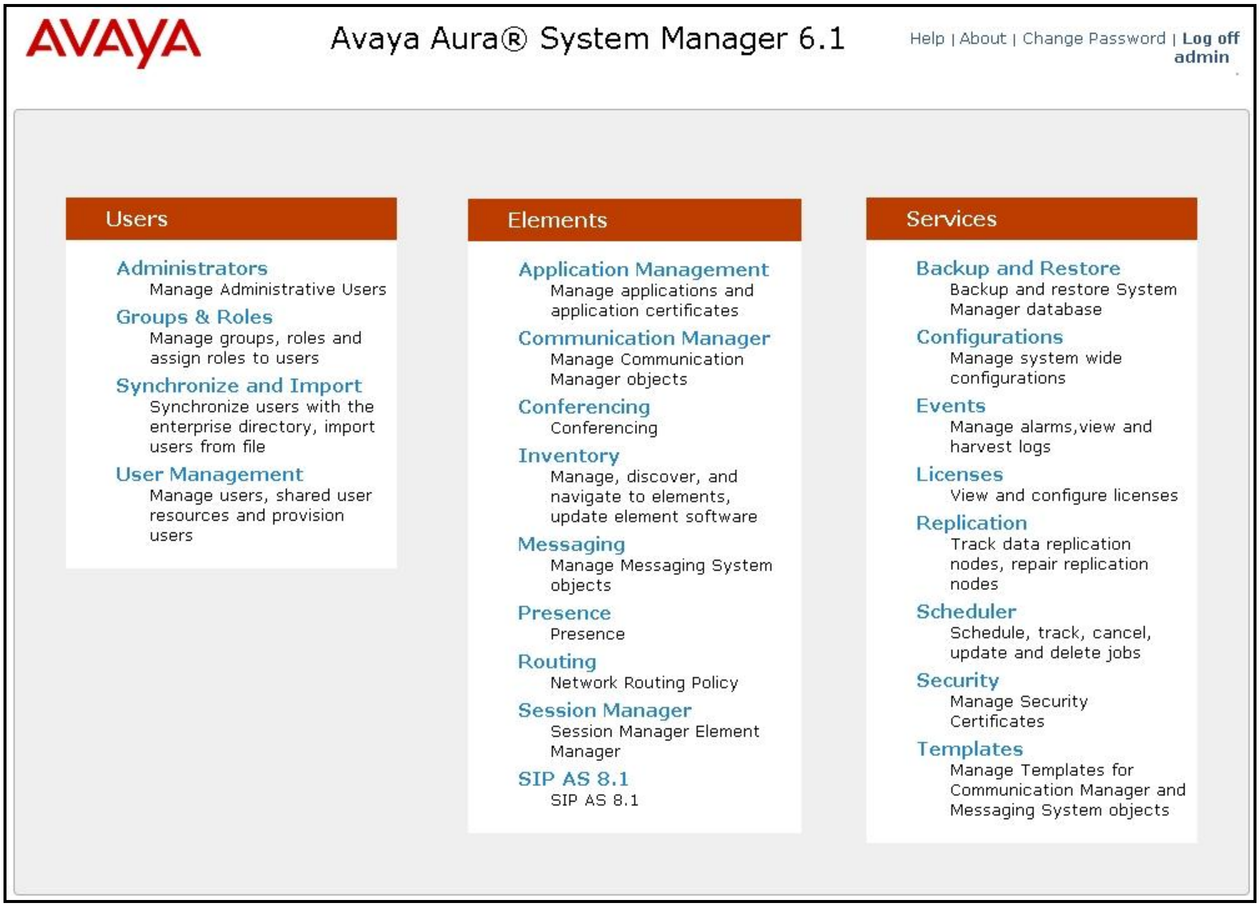
- SIP domain.
- Logical/physical Location that can be occupied by SIP Entities.
- SIP Entities corresponding to Communication Manager, Session Manager and the Avaya SBCE.
- Entity Links, which define the SIP Trunk parameters used by Session Manager when routing calls to/from SIP Entities.
- Routing Policies, which control call routing between the SIP Entities.
- Dial Patterns, which govern to which SIP Entity a call is routed.
- 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, Location, SIP entities, and Session Manager itself. However, each item should be reviewed to verify the configuration.

In the compliance testing, geographic redundancy was implemented on Session Manager. When the primary Session Manager is out of service, the SIP Trunk will be established between Communication Manager and the secondary Session Manager. Therefore, the configuration for the primary Session Manager needs to be replicated to the secondary Session Manager.

6.1 System Manager Login and Navigation

Session Manager configuration is accomplished by accessing the browser-based GUI of System Manager, using the URL “https://<ip-address>/SMGR”, where “<ip-address>” is the IP address of System Manager. 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.


AVAYA
Avaya Aura® System Manager 6.1
Help | About | Change Password | Log off admin

Users

Administrators
Manage Administrative Users

Groups & Roles
Manage groups, roles and assign roles to users

Synchronize and Import
Synchronize users with the enterprise directory, import users from file

User Management
Manage users, shared user resources and provision users

Elements

Application Management
Manage applications and application certificates

Communication Manager
Manage Communication Manager objects

Conferencing
Conferencing

Inventory
Manage, discover, and navigate to elements, update element software

Messaging
Manage Messaging System objects

Presence
Presence

Routing
Network Routing Policy

Session Manager
Session Manager Element Manager

SIP AS 8.1
SIP AS 8.1

Services

Backup and Restore
Backup and restore System Manager database

Configurations
Manage system wide configurations

Events
Manage alarms,view and harvest logs

Licenses
View and configure licenses

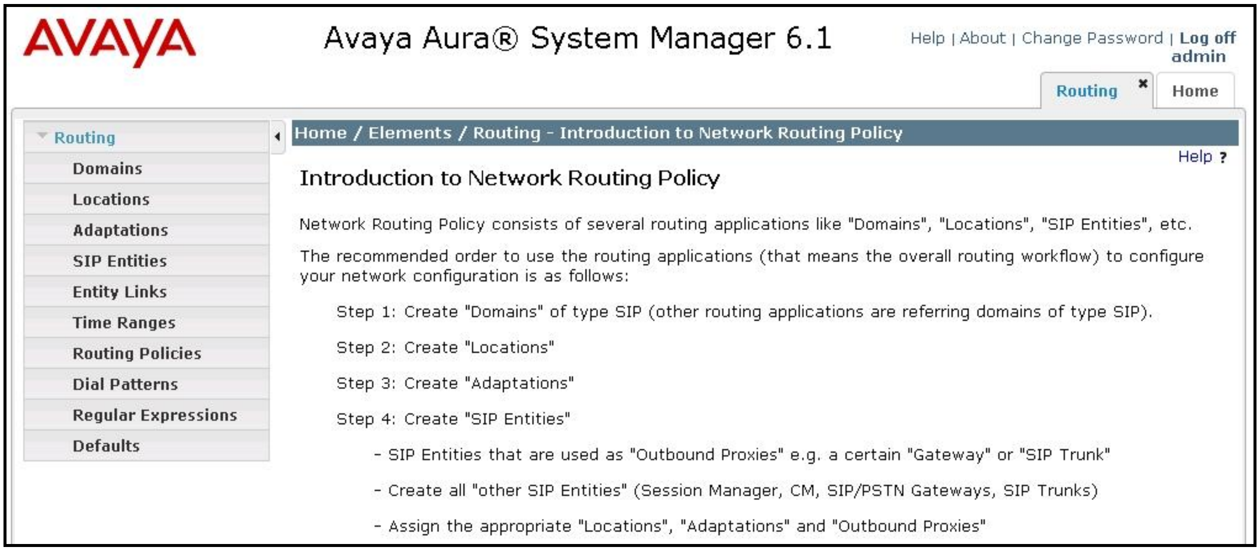
Replication
Track data replication nodes, repair replication nodes

Scheduler
Schedule, track, cancel, update and delete jobs

Security
Manage Security Certificates

Templates
Manage Templates for Communication Manager and Messaging System objects

Most of the configuration items are performed in the Routing Element. Click on **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.



Introduction to Network Routing Policy

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

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

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

Step 2: Create "Locations"

Step 3: Create "Adaptations"

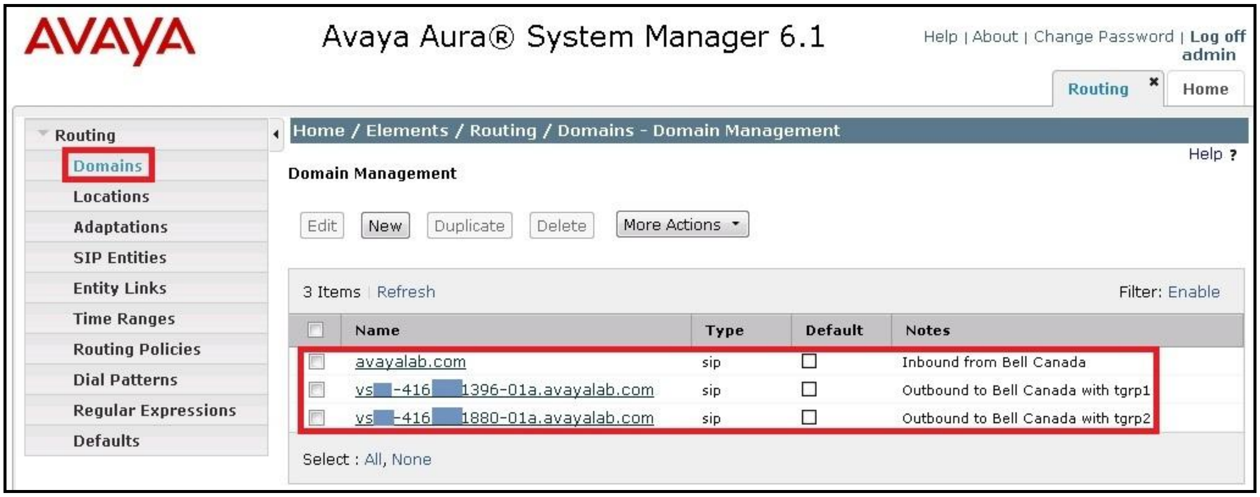
Step 4: Create "SIP Entities"

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

6.2 Specify SIP Domain

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

The following screen shows the list of configured SIP domains. The domain **avayalab.com** is an enterprise private SIP domain, it was defined to route incoming calls to Communication Manager. Incoming calls were received with service provider public SIP domain **cust2xxxx.xxxx.bell.ca** or **cust6xxxx.xxxx.bell.ca** which will be translated by the Avaya SBCE to **avayalab.com** to route to Session Manager. The other SIP domains **vsxx-416XXX1396-01a.avayalab.com** and **vsxx-416XXX1880-01a.avayalab.com** were used for outgoing calls containing the "tgrp" as **vsxx-416XXX1396-01a** and **vsxx-416XXX1880-01a**. The "tgrp" assists the Avaya SBCE to construct the "Contact" header as per the requirement from Bell Canada to support the Least Cost Routing feature implemented by Bell Canada CO. These outgoing SIP domains will be translated by the Avaya SBCE to **sipxxxxxxxx.bell.ca** to route to Bell Canada networks.



Home / Elements / Routing / Domains - Domain Management

Domain Management

☐	Name	Type	Default	Notes
☐	avayalab.com	sip	☐	Inbound from Bell Canada
☐	vs[redacted]-416[redacted]1396-01a.avayalab.com	sip	☐	Outbound to Bell Canada with tgrp1
☐	vs[redacted]-416[redacted]1880-01a.avayalab.com	sip	☐	Outbound to Bell Canada with tgrp2

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

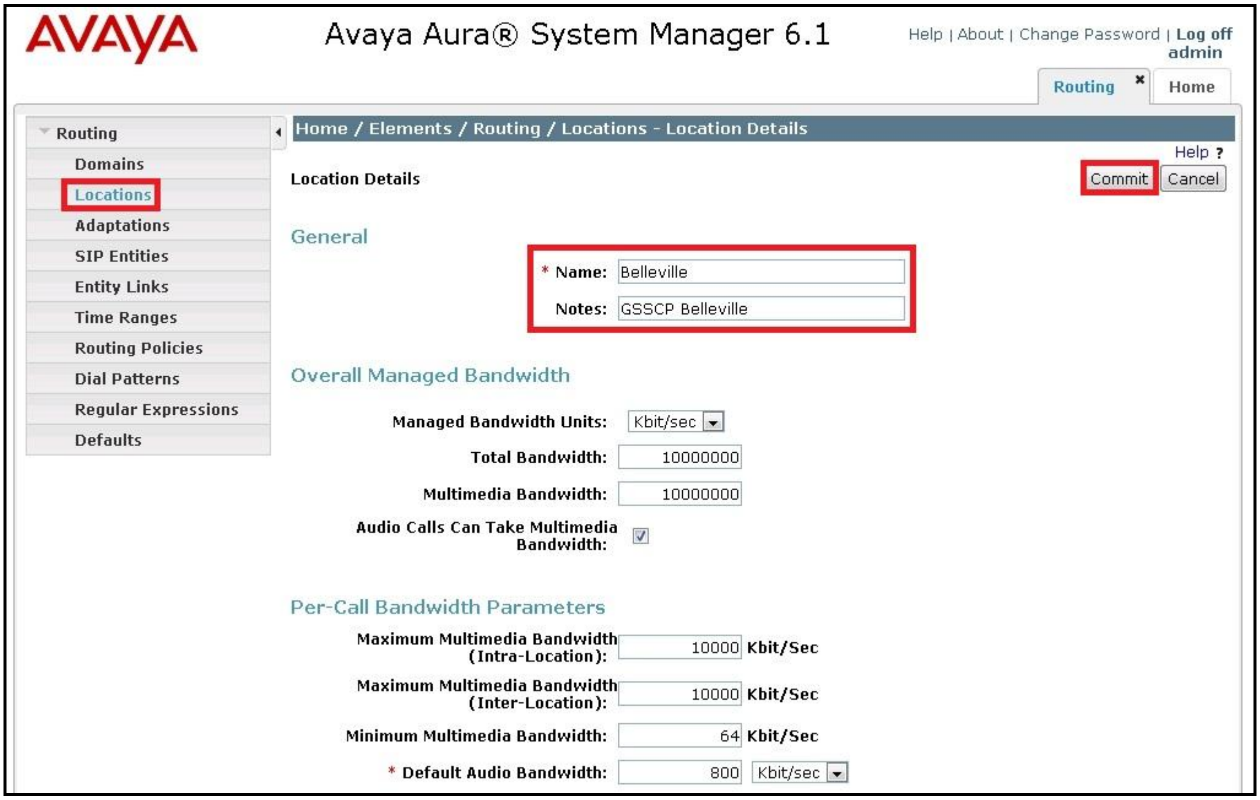
- **Name:** Enter a descriptive name for the location.
- **Notes:** Add a brief description (optional).

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

- **IP Address Pattern:** An IP address pattern used to identify the location.

- **Notes:** Add a brief description (optional).

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



Location Details

General

* Name: Belleville

Notes: GSSCP Belleville

Overall Managed Bandwidth

Managed Bandwidth Units: Kbit/sec

Total Bandwidth: 10000000

Multimedia Bandwidth: 10000000

Audio Calls Can Take Multimedia Bandwidth: ☑

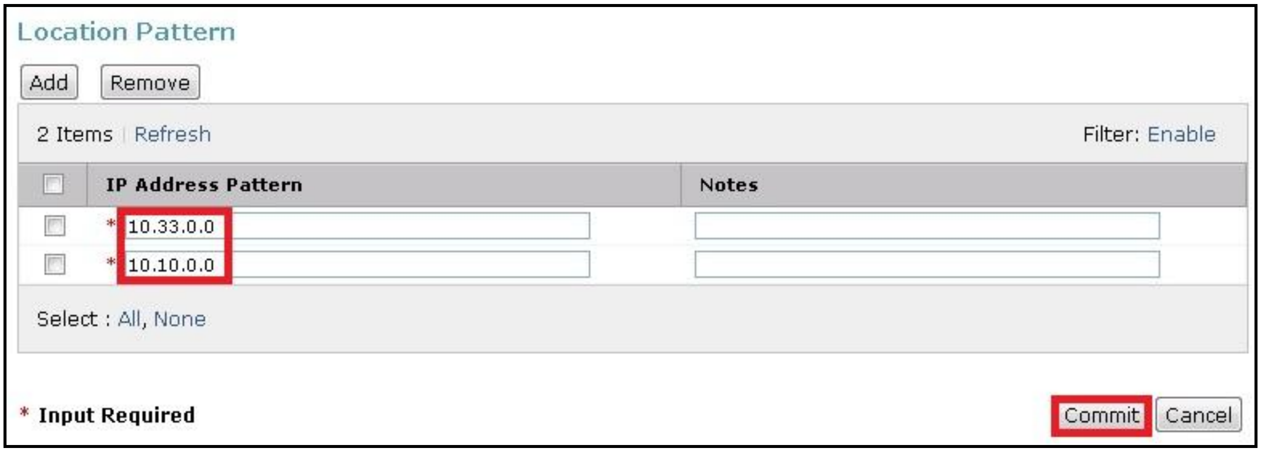
Per-Call Bandwidth Parameters

Maximum Multimedia Bandwidth (Intra-Location): 10000 Kbit/Sec

Maximum Multimedia Bandwidth (Inter-Location): 10000 Kbit/Sec

Minimum Multimedia Bandwidth: 64 Kbit/Sec

* Default Audio Bandwidth: 800 Kbit/sec



Location Pattern

□	IP Address Pattern	Notes
□	* 10.33.0.0	
□	* 10.10.0.0	

* Input Required

6.4 Add SIP Entities

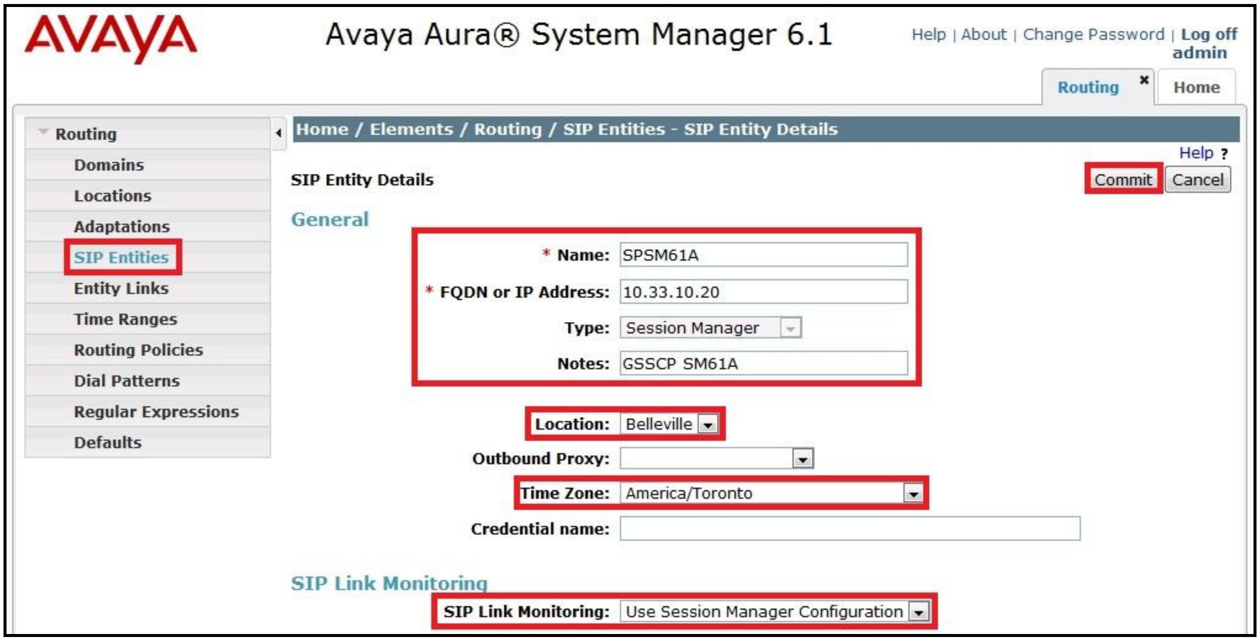
A SIP Entity must be added for Session Manager and for each SIP telephony system connected to it which includes Communication Manager and the Avaya SBCE. Navigate to **Routing →**

SIP Entities in the left navigation pane and click on the **New** button in the right pane (not shown).

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

- **Name:** Enter a descriptive name.
- **FQDN or IP Address:** Enter the FQDN or IP address of the SIP Entity that is used for SIP signaling.
- **Type:** Select **Session Manager** for Session Manager, **Communication Manager** for Communication Manager and **Other** for the Avaya SBCE.
- **Location:** Select one of the locations defined previously.
- **Time Zone:** Select the time zone for the location above.

The following screen shows the addition of SIP Entity for the primary Session Manager. The IP address of the primary Session Manager signaling interface is entered for **FQDN or IP Address**. **The SIP Link Monitoring** is kept as default **Use Session Manager Configuration**.



SIP Entity Details

General

* Name: SPSM61A

* FQDN or IP Address: 10.33.10.20

Type: Session Manager

Notes: GSSCP SM61A

Location: Belleville

Outbound Proxy:

Time Zone: America/Toronto

Credential name:

SIP Link Monitoring

SIP Link Monitoring: Use Session Manager Configuration

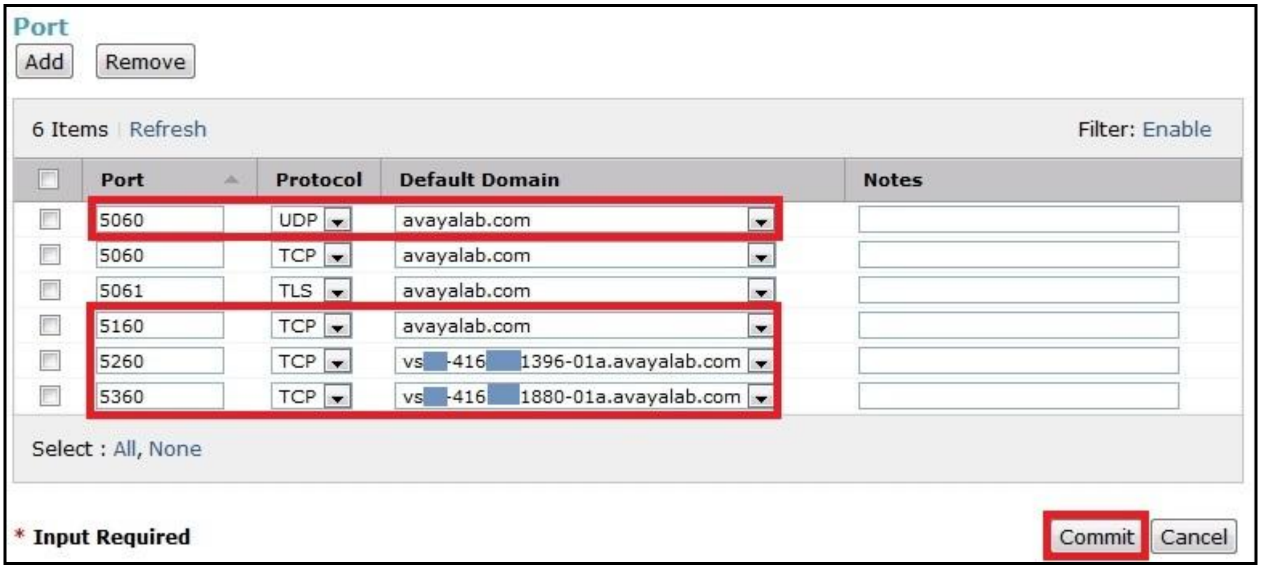
To define the ports used by the primary Session Manager, scroll down to the **Port** section of the **SIP Entity Details** screen. This section is only present for the **Session Manager** SIP Entity.

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

- **Port**: Port number on which the Session Manager can listen for SIP requests.
- **Protocol**: Transport protocol to be used 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/5160** connecting to Communication Manager for incoming calls, **Port** entry **TCP/5260** and **TCP/5360** for outgoing calls with "tgrp" **vsxx-416XXX1396-01a** and **vsxx-416XXX1880-01a**. The **Port** entry **UDP/5060** is for connecting to the primary and secondary Avaya SBCE.



Port

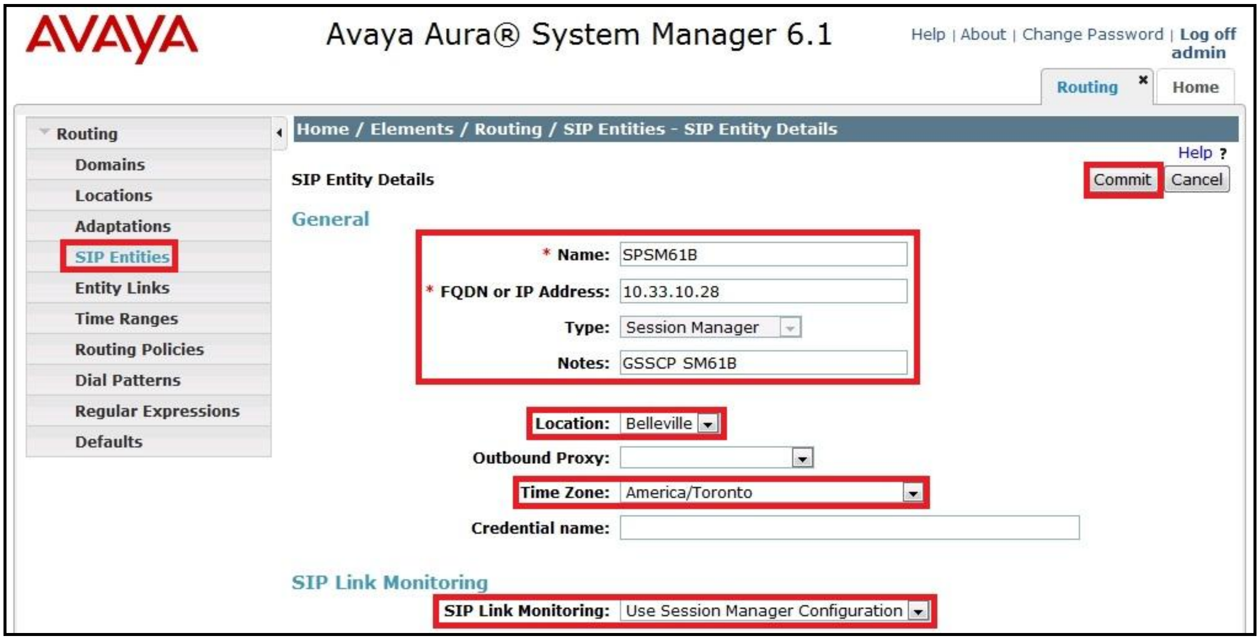
6 Items | Refresh Filter: Enable

□	Port	Protocol	Default Domain	Notes
□	5060	UDP	avayalab.com	
□	5060	TCP	avayalab.com	
□	5061	TLS	avayalab.com	
□	5160	TCP	avayalab.com	
□	5260	TCP	vs[redacted]-416[redacted]1396-01a.avayalab.com	
□	5360	TCP	vs[redacted]-416[redacted]1880-01a.avayalab.com	

Select : All, None

* Input Required

The SIP Entity for the secondary Session Manager was similarly created except the **FQDN or IP Address** field is set to the signaling interface of the secondary Session Manager. It is shown in the following screenshots.



Home / Elements / Routing / SIP Entities - SIP Entity Details

SIP Entity Details

General

* Name: SPSM61B

* FQDN or IP Address: 10.33.10.28

Type: Session Manager

Notes: GSSCP SM61B

Location: Belleville

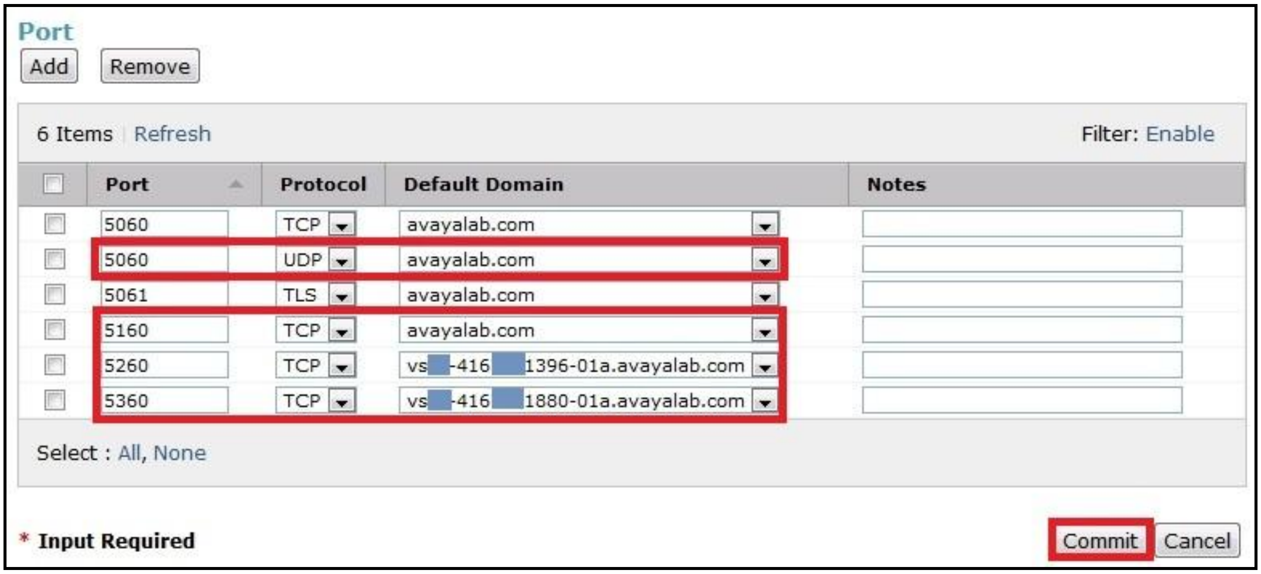
Outbound Proxy:

Time Zone: America/Toronto

Credential name:

SIP Link Monitoring

SIP Link Monitoring: Use Session Manager Configuration



Port

6 Items | Refresh Filter: Enable

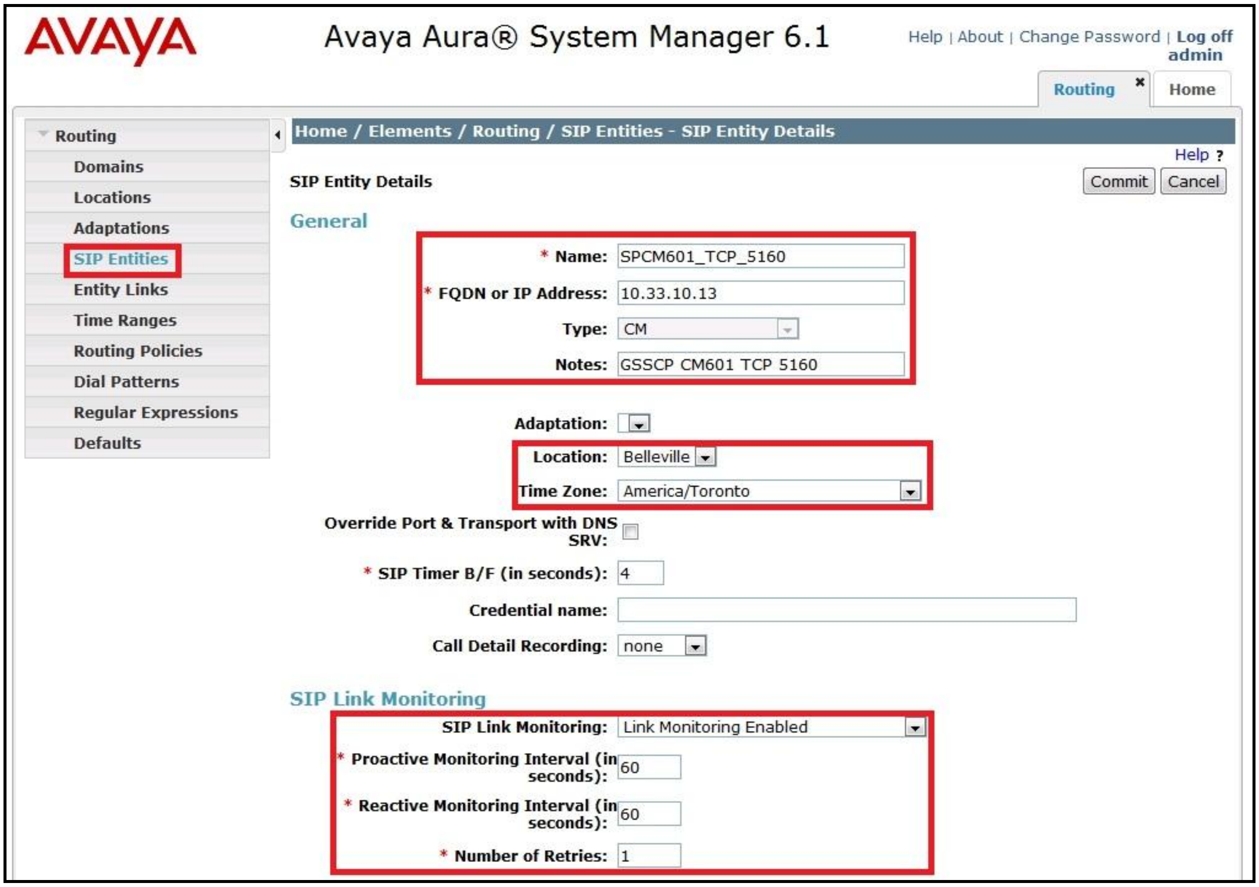
□	Port	Protocol	Default Domain	Notes
□	5060	TCP	avayalab.com	
□	5060	UDP	avayalab.com	
□	5061	TLS	avayalab.com	
□	5160	TCP	avayalab.com	
□	5260	TCP	vs[redacted]-416[redacted]1396-01a.avayalab.com	
□	5360	TCP	vs[redacted]-416[redacted]1880-01a.avayalab.com	

Select : All, None

* Input Required

The following section shows the addition of the Communication Manager SIP Entity. The **FQDN or IP Address** field is set to the IP address of Communication Manager. Select **Type** is **CM**. In the compliance testing, a single SIP Entity was created to for incoming calls and multiple SIP Entities were created for outgoing calls for each of the signaling groups created on Communication Manager in **Section 5.6**. Each SIP Entity will be used to create the Entity Link which will be discussed next in the **Section 6.5**.

The SIP Entity for incoming calls to Communication Manager on **Port** entry **TCP/5160** is shown in the screenshot below. The **SIP Link Monitoring** was set to **Link Monitoring Enabled** with **Proactive Monitoring Interval** and **Reactive Monitoring Intervals** were set to 60 seconds. This setting allows Session Manager to send OPTIONS heartbeat to check for the status of the SIP Trunk every 60 seconds.



SIP Entity Details

General

* Name: SPCM601_TCP_5160

* FQDN or IP Address: 10.33.10.13

Type: CM

Notes: GSSCP CM601 TCP 5160

Adaptation:

Location: Belleville

Time Zone: America/Toronto

Override Port & Transport with DNS SRV: □

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

Credential name:

Call Detail Recording: none

SIP Link Monitoring

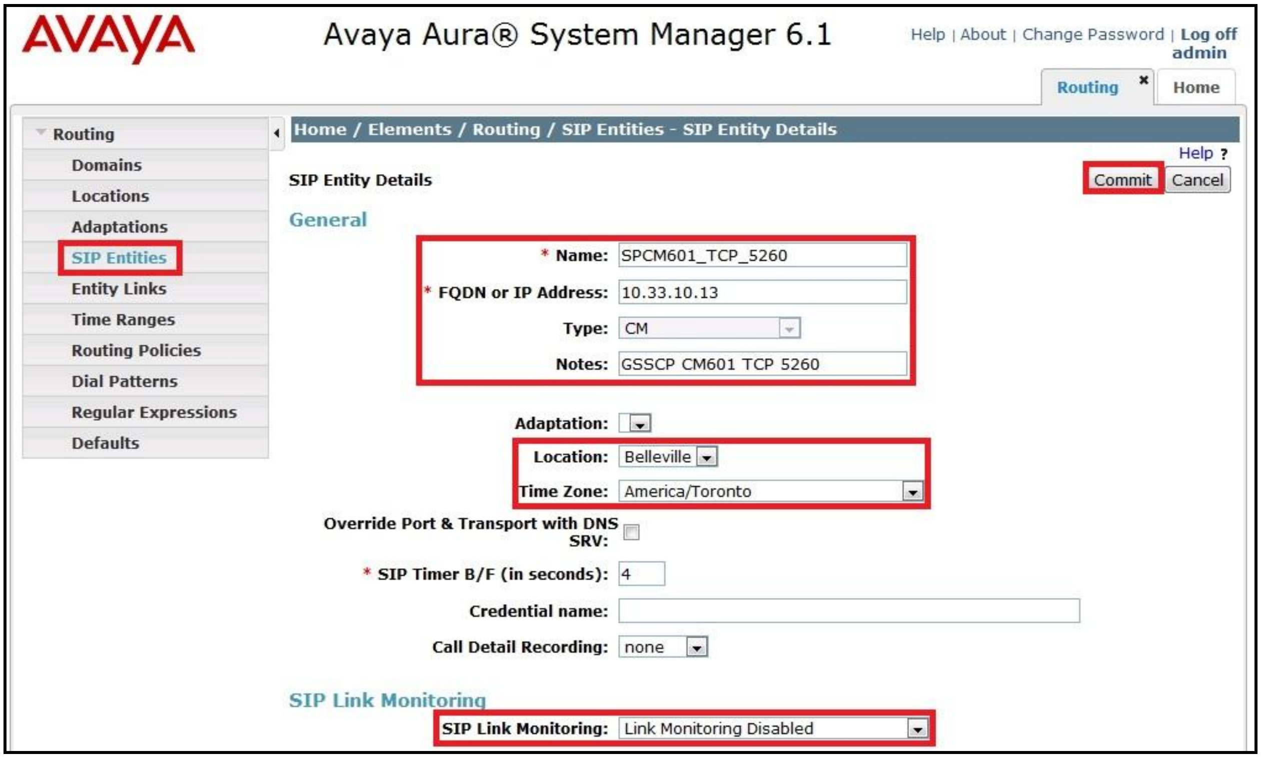
SIP Link Monitoring: Link Monitoring Enabled

* Proactive Monitoring Interval (in seconds): 60

* Reactive Monitoring Interval (in seconds): 60

* Number of Retries: 1

The following screens show the SIP Entities for outgoing calls from Communication Manager on **Port** entry **TCP/5260** with “trgp” **vsxx-416XXX1396-01a** and **Port** entry **TCP/5360** with “tgrp” **vsxx-416XXX1880-01a**. The **SIP Link Monitoring** was set to **Link Monitoring Disabled**. This setting restricts Session Manager from sending OPTIONS heartbeat to check for the status of the SIP Trunk. If enabled, the incoming OPTIONS request from Session Manager to Communication Manager will be rejected because the traffic comes in the trunk groups which were designed for outgoing traffic. Otherwise, the OPTIONS heartbeat will monitored by Communication Manager under the setting for signaling groups for outgoing calls in **Section 5.6**.



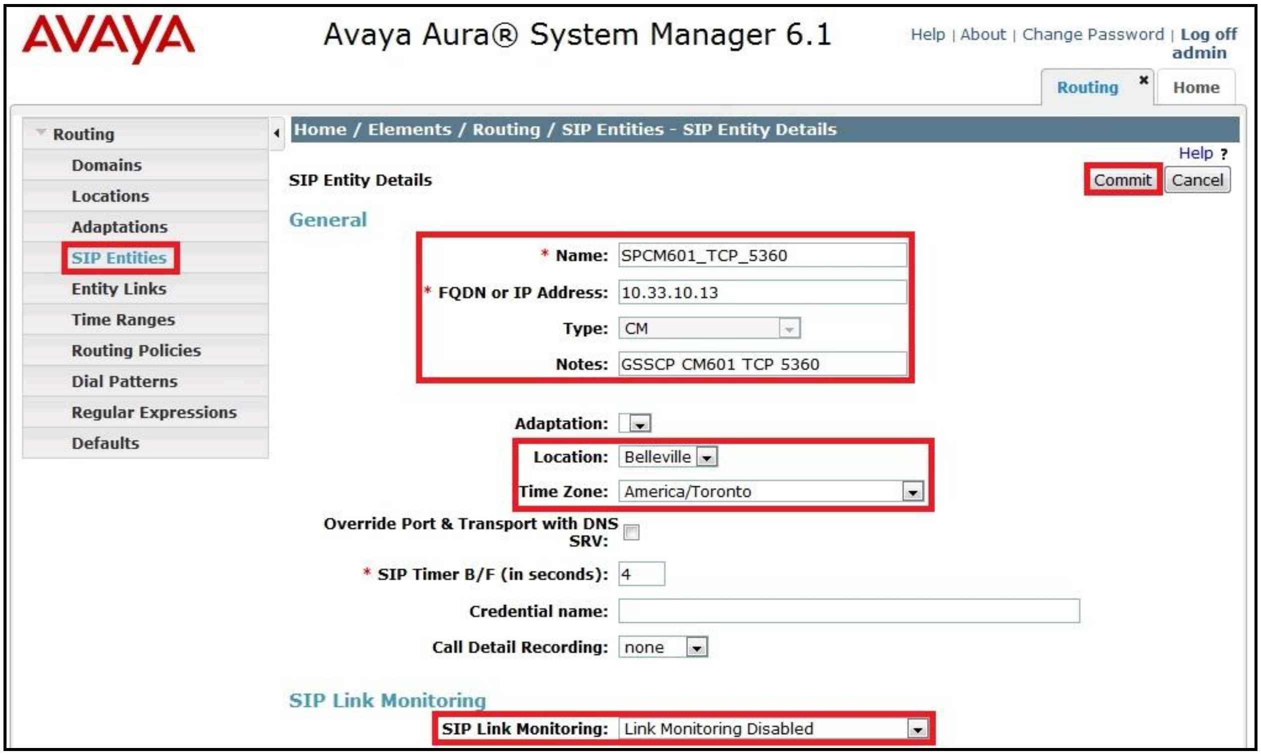
SIP Entity Details

General

* Name:	SPCM601_TCP_5260
* FQDN or IP Address:	10.33.10.13
Type:	CM
Notes:	GSSCP CM601 TCP 5260
Adaptation:	
Location:	Belleville
Time Zone:	America/Toronto
Override Port & Transport with DNS SRV:	□
* SIP Timer B/F (in seconds):	4
Credential name:	
Call Detail Recording:	none

SIP Link Monitoring

SIP Link Monitoring:	Link Monitoring Disabled



SIP Entity Details

General

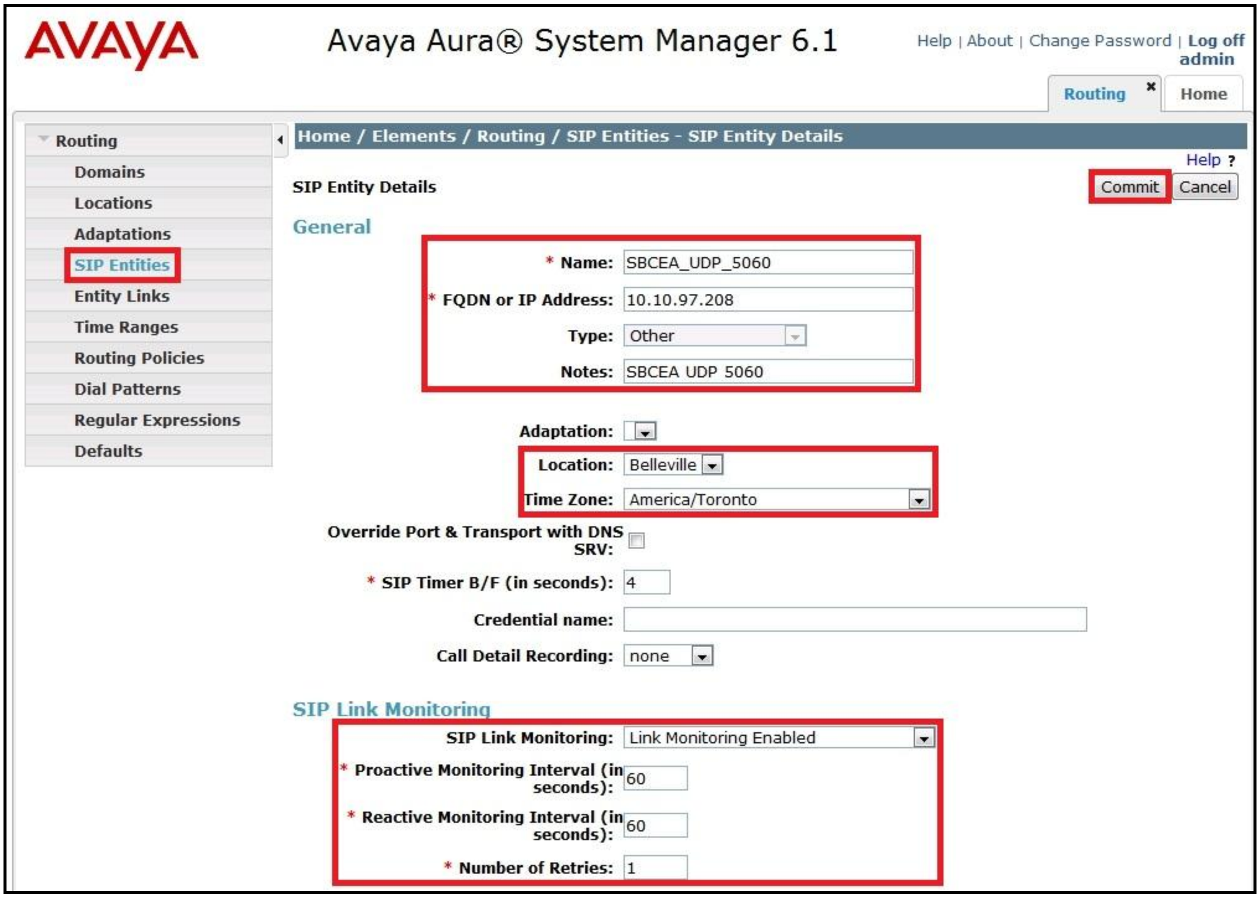
* Name:	SPCM601_TCP_5360
* FQDN or IP Address:	10.33.10.13
Type:	CM
Notes:	GSSCP CM601 TCP 5360
Adaptation:	
Location:	Belleville
Time Zone:	America/Toronto
Override Port & Transport with DNS SRV:	□
* SIP Timer B/F (in seconds):	4
Credential name:	
Call Detail Recording:	none

SIP Link Monitoring

SIP Link Monitoring:	Link Monitoring Disabled

Note: The sample configuration was created with two outgoing trunk groups. If the deployment in the field requires more outgoing trunk groups then more SIP Entities for outgoing calls will need to be created appropriately.

The following screens show the addition of the SIP Entities for the primary Avaya SBCE **10.10.97.208** and the secondary Avaya SBCE **10.10.97.209**. The **FQDN or IP Address** field is set to the IP address of the private network interfaces. The **SIP Link Monitoring** was set to **Link Monitoring Enabled** with **Proactive Monitoring Interval** and **Reactive Monitoring Intervals** were set to 60 seconds. This setting allows Session Manager to send OPTIONS heartbeat to check for the status of the SIP Trunk every 60 seconds. It means if the primary Avaya SBCE fails, it will take the Session Manager 60 seconds to detect and then failover to the secondary Avaya SBCE. In the meantime, Session Manager will also reactively check for the status of the failed link every 60 seconds to resume the connection to the primary Avaya SBCE.



SIP Entity Details

General

* Name: SBCEA_UDP_5060

* FQDN or IP Address: 10.10.97.208

Type: Other

Notes: SBCEA UDP 5060

Adaptation:

Location: Belleville

Time Zone: America/Toronto

Override Port & Transport with DNS SRV: □

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

Credential name:

Call Detail Recording: none

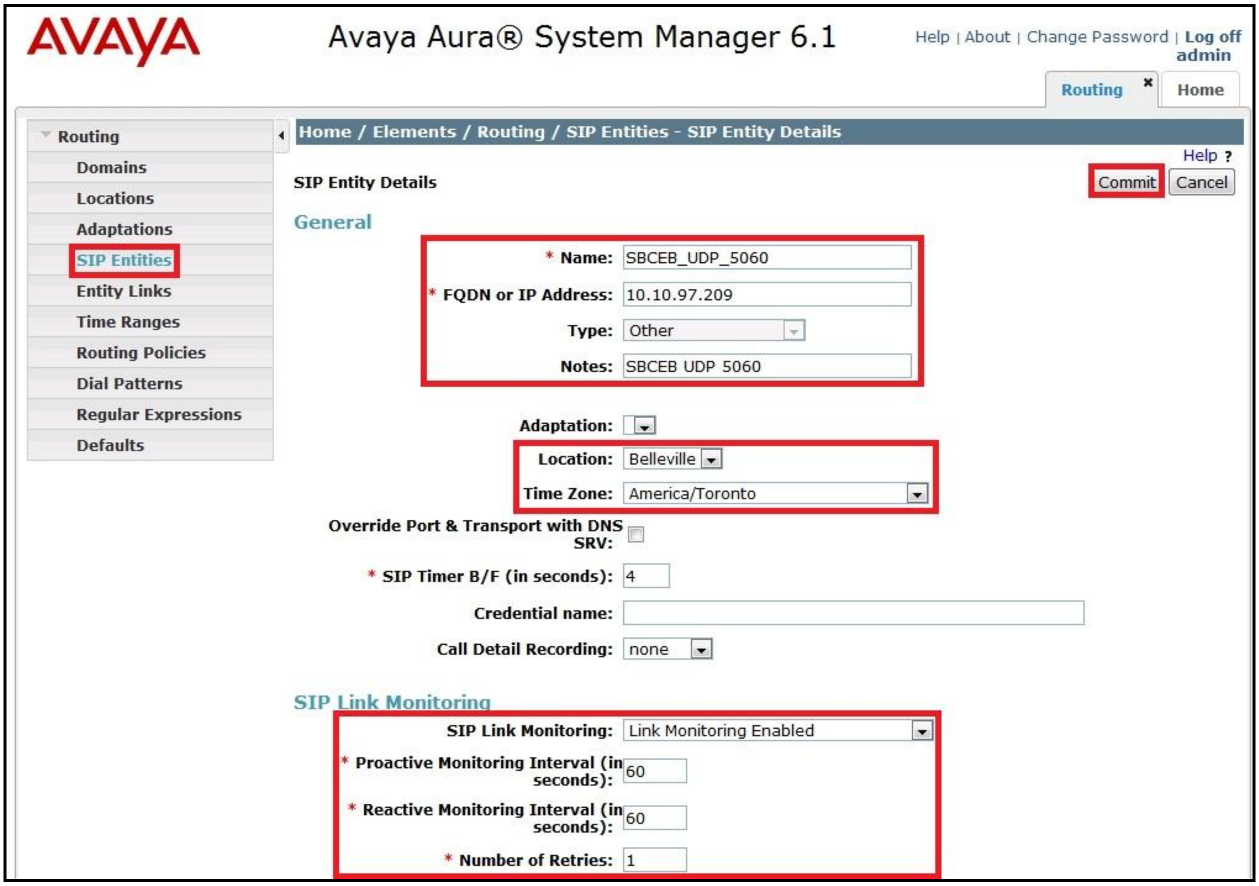
SIP Link Monitoring

SIP Link Monitoring: Link Monitoring Enabled

* Proactive Monitoring Interval (in seconds): 60

* Reactive Monitoring Interval (in seconds): 60

* Number of Retries: 1



SIP Entity Details

General

* Name: SBCEB_UDP_5060

* FQDN or IP Address: 10.10.97.209

Type: Other

Notes: SBCEB UDP 5060

Adaptation:

Location: Belleville

Time Zone: America/Toronto

Override Port & Transport with DNS SRV: □

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

Credential name:

Call Detail Recording: none

SIP Link Monitoring

SIP Link Monitoring: Link Monitoring Enabled

* Proactive Monitoring Interval (in seconds): 60

* Reactive Monitoring Interval (in seconds): 60

* Number of Retries: 1

6.5 Add Entity Links

A SIP Trunk between Session Manager and a telephony system is described by an Entity Link. From each Session Manager to Communication Manager, one Entity Link was created to carry incoming calls and multiple Entities Links were created to for outgoing calls. Each Session Manager will also have one Entity Link to each Avaya SBCE for service provider traffic.

To add an Entity Link, navigate to **Routing → Entity Links** in the left navigation pane and click on the **New** button in the right pane (not shown). Fill in the following fields in the new row that is displayed:

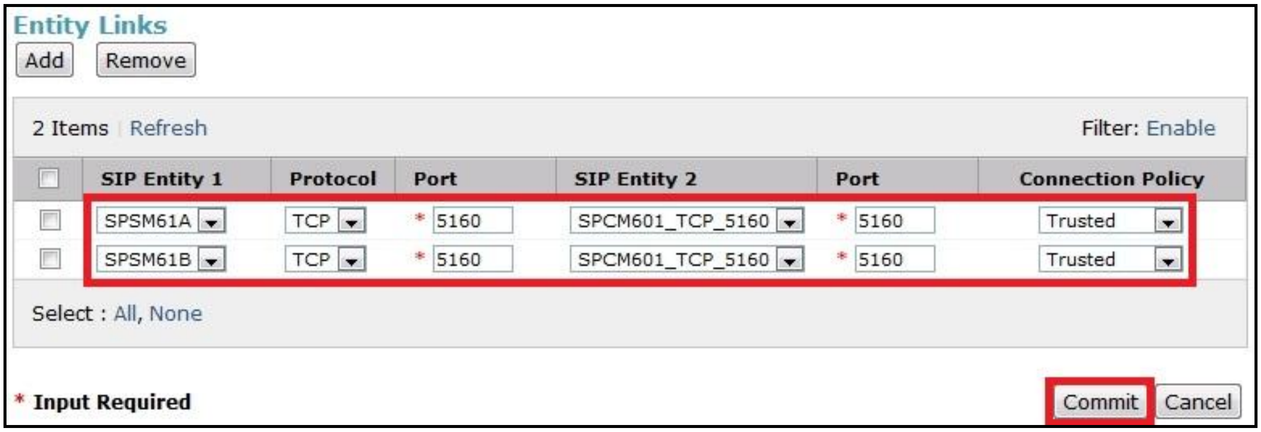
- **Name**: Enter a descriptive name.
- **SIP Entity 1**: Select the Session Manager.
- **Protocol**: Select the transport protocol used for this link.
- **Port**: Port number on which Session Manager will receive SIP requests from the far-end. For Communication Manager, this must match the **Far-end Listen Port** defined for signaling group in **Section 5.6**.
- **SIP Entity 2**: Select the name of the other system. For Communication Manager, select the Communication Manager SIP Entities defined in **Section 6.4**. For the Avaya SBCE, select the Avaya SBCE SIP Entities defined in **Section 6.4**.

- **Port**: Port number on which the other system receives SIP requests from Session Manager. For Communication Manager, this must match the **Near-end Listen Port** defined for signaling group in **Section 5.6**.
- **Connection Policy**: Select **Trusted**. **Note**: If **Trusted** is not selected, all calls from the associated SIP Entity specified in **Section 6.4** will be requested to process authentication.

Click **Commit** to save.

The following screenshots illustrate the Entity Links from both primary and secondary Session Manager to Communication Manager and both primary and secondary Avaya SBCE.

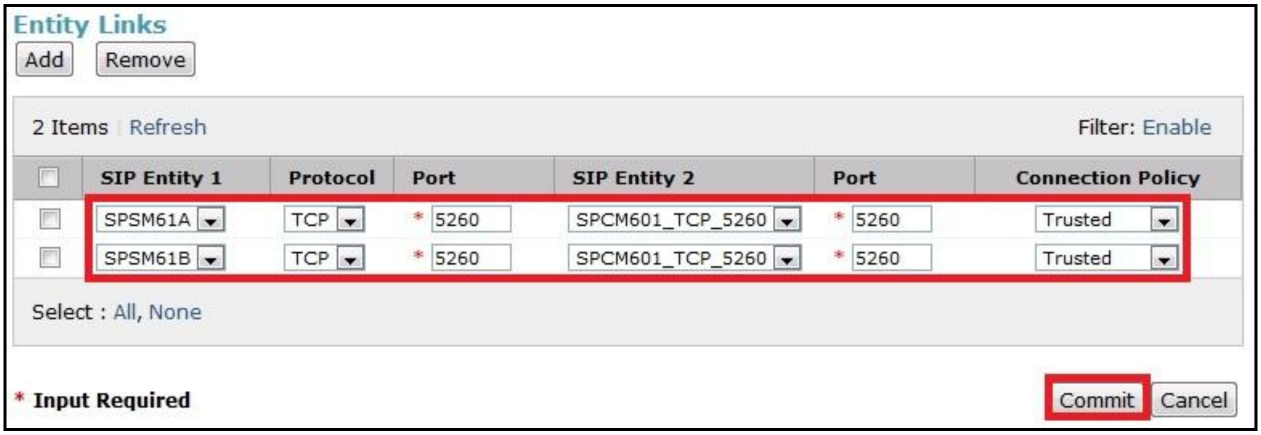
Entity Links between the primary and secondary Session Manager and Communication Manager for incoming calls on **Port** entry **TCP/5160**:



☐	SIP Entity 1	Protocol	Port	SIP Entity 2	Port	Connection Policy
☐	SPSM61A	TCP	* 5160	SPCM601_TCP_5160	* 5160	Trusted
☐	SPSM61B	TCP	* 5160	SPCM601_TCP_5160	* 5160	Trusted

* Input Required

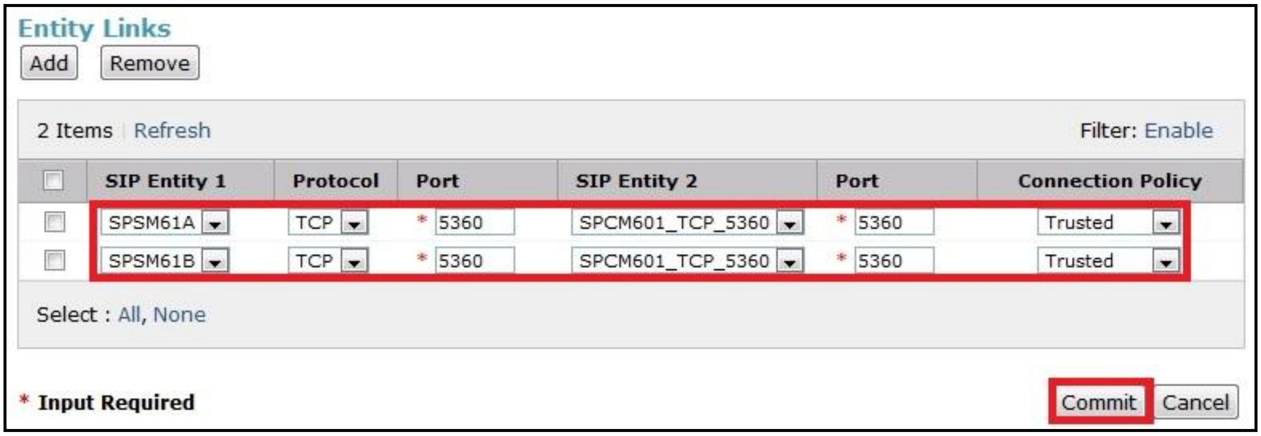
Entity Links between the primary and secondary Session Manager and Communication Manager for outgoing calls with "tgrp" **vsxx-416XXX1396-01a** on **Port** entry **TCP/5260**:



☐	SIP Entity 1	Protocol	Port	SIP Entity 2	Port	Connection Policy
☐	SPSM61A	TCP	* 5260	SPCM601_TCP_5260	* 5260	Trusted
☐	SPSM61B	TCP	* 5260	SPCM601_TCP_5260	* 5260	Trusted

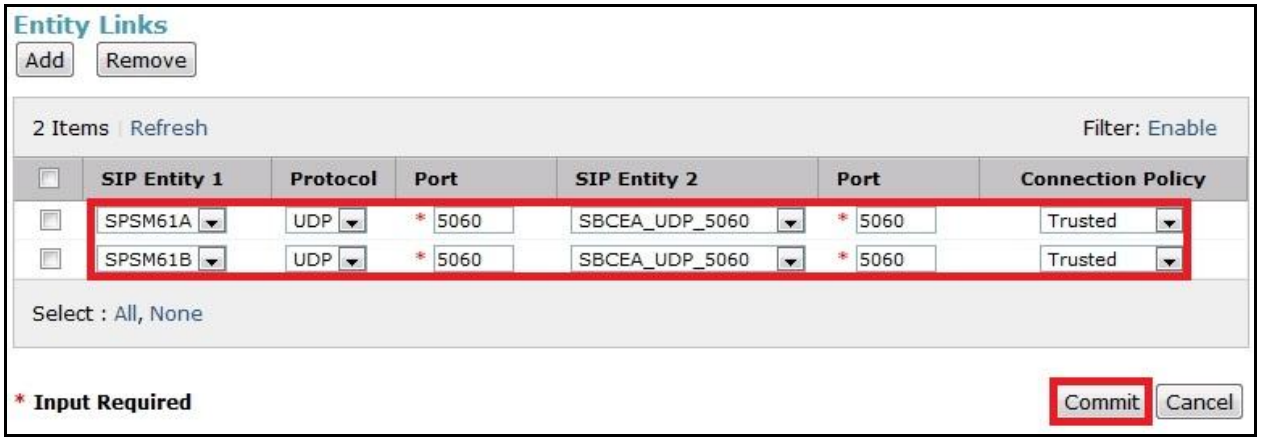
* Input Required

Entity Links between the primary and secondary Session Manager and Communication Manager for outgoing calls with "tgrp" **vsxx-416XXX1880-01a** on **Port** entry **TCP/5360**:



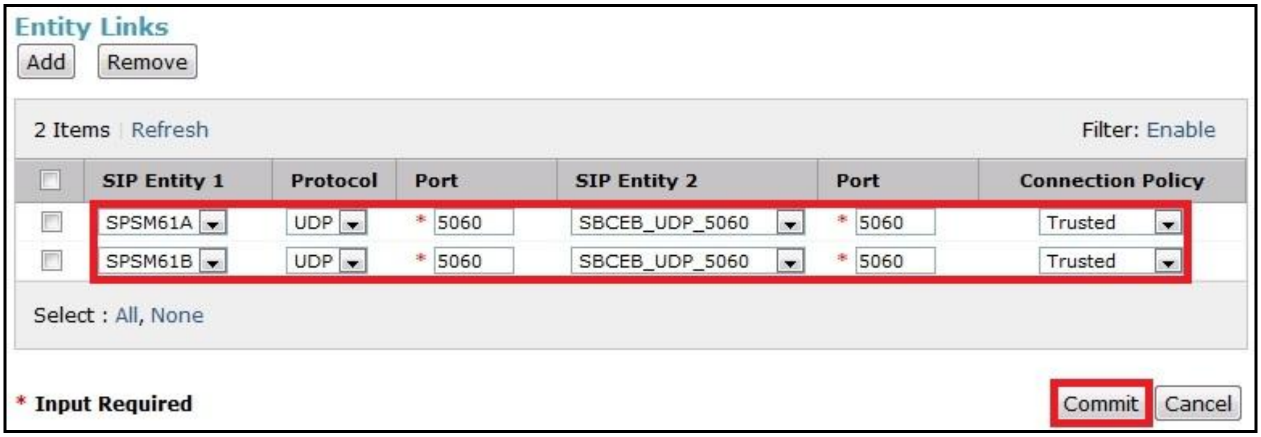
□	SIP Entity 1	Protocol	Port	SIP Entity 2	Port	Connection Policy
□	SPSM61A	TCP	* 5360	SPCM601_TCP_5360	* 5360	Trusted
□	SPSM61B	TCP	* 5360	SPCM601_TCP_5360	* 5360	Trusted

Entity Links between the primary and secondary Session Manager and the primary Avaya SBCE for service provider calls on **Port** entry **UDP/5060**:



□	SIP Entity 1	Protocol	Port	SIP Entity 2	Port	Connection Policy
□	SPSM61A	UDP	* 5060	SBCEA_UDP_5060	* 5060	Trusted
□	SPSM61B	UDP	* 5060	SBCEA_UDP_5060	* 5060	Trusted

Entity Links between the primary and secondary Session Manager and the secondary Avaya SBCE for service provider calls on **Port** entry **UDP/5060**:



□	SIP Entity 1	Protocol	Port	SIP Entity 2	Port	Connection Policy
□	SPSM61A	UDP	* 5060	SBCEB_UDP_5060	* 5060	Trusted
□	SPSM61B	UDP	* 5060	SBCEB_UDP_5060	* 5060	Trusted

6.6 Add Routing Policies

Routing Policies describe the conditions under which calls will be routed to the SIP Entities specified in **Section 6.4**. A single Routing Policy was added to route incoming calls to Communication Manager and multiple Routing Policies were also appropriately added to route outgoing calls to the primary and secondary Avaya SBCE.

To add a Routing Policy, navigate to **Routing → Routing Policies** in the left navigation pane and click on the **New** button in the right pane (not shown). The following screen is displayed then fills in the following:

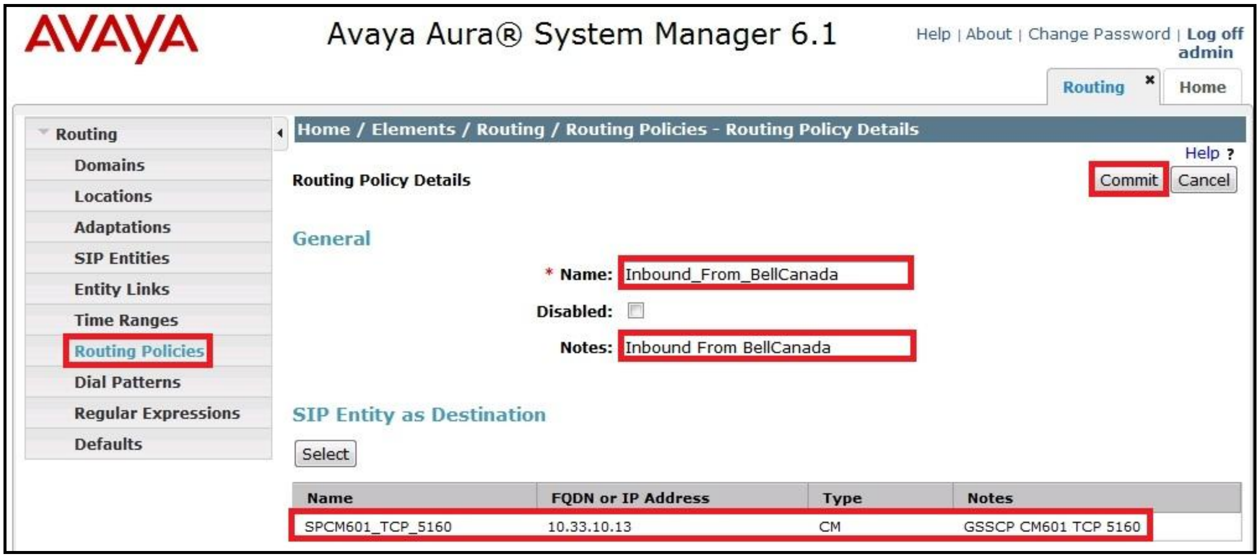
In the **General** section, enter the following values:

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

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

The following screens show the Routing Policies used in the compliance testing.

Routing Policy **Inbound_From_BellCanada** for incoming calls to Communication Manager:



Routing Policy Details

General

* Name: Inbound_From_BellCanada

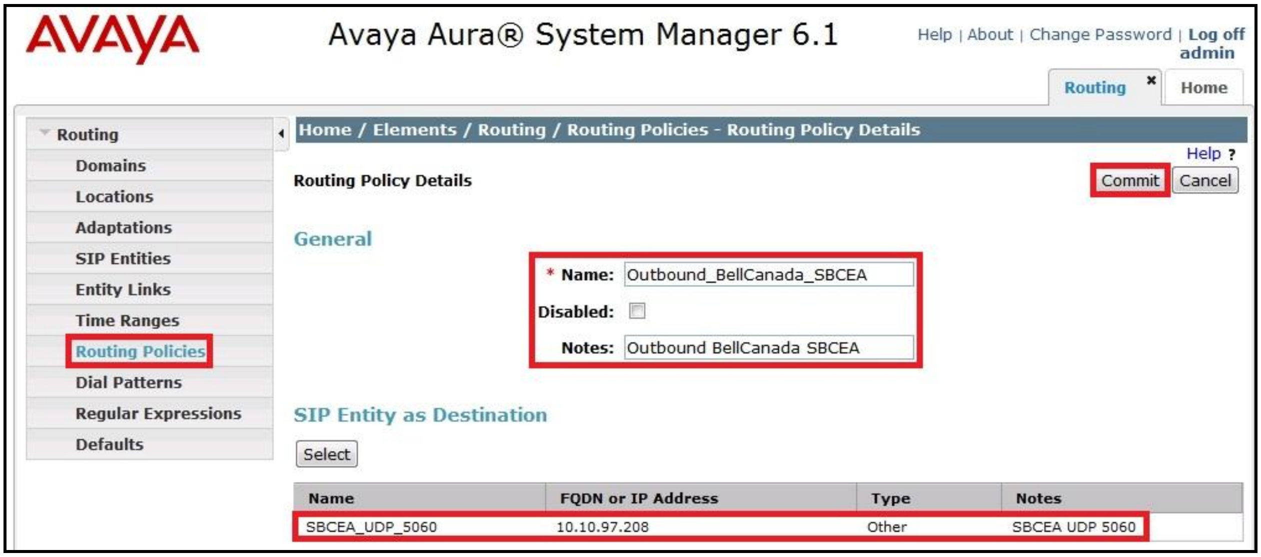
Disabled: □

Notes: Inbound From BellCanada

SIP Entity as Destination

Name	FQDN or IP Address	Type	Notes
SPCM601_TCP_5160	10.33.10.13	CM	GSSCP CM601 TCP 5160

Routing Policy **Out_BellCanada_SBCEA** for outgoing calls to the primary Avaya SBCE:



Routing Policy Details

General

* Name: Outbound_BellCanada_SBCEA

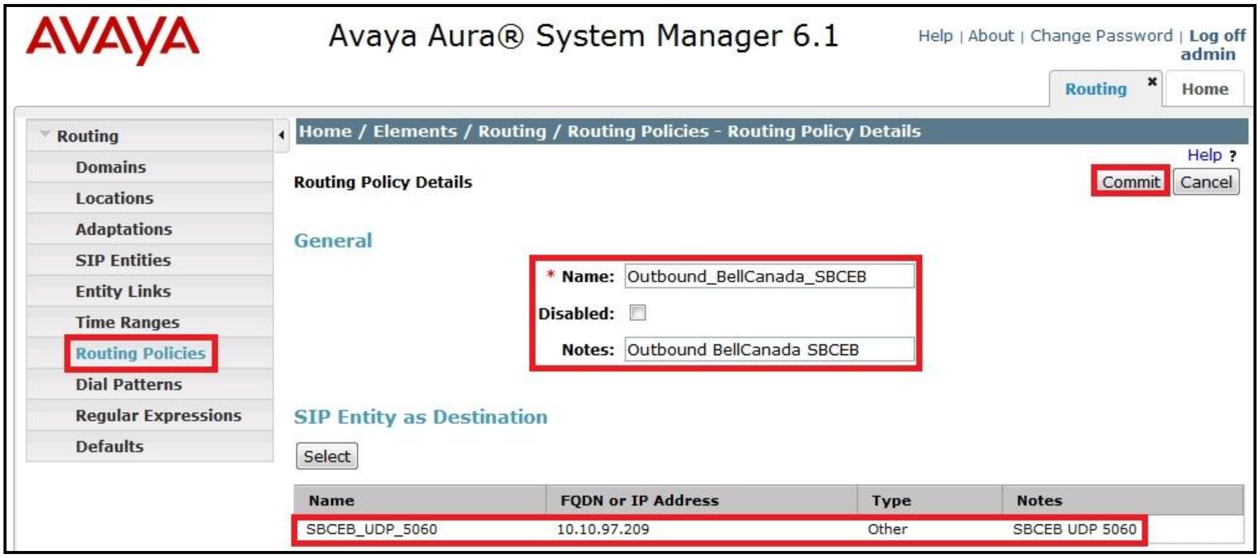
Disabled: □

Notes: Outbound BellCanada SBCEA

SIP Entity as Destination

Name	FQDN or IP Address	Type	Notes
SBCEA_UDP_5060	10.10.97.208	Other	SBCEA UDP 5060

Routing Policy **Out_BellCanada_SBCEB** for outgoing calls to the secondary Avaya SBCE:



Routing Policy Details

General

* Name: Outbound_BellCanada_SBCEB

Disabled: □

Notes: Outbound BellCanada SBCEB

SIP Entity as Destination

Name	FQDN or IP Address	Type	Notes
SBCEB_UDP_5060	10.10.97.209	Other	SBCEB UDP 5060

6.7 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 on the **New** button in the right pane (not shown). Fill in the following, as shown in the screens below:

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

- **Pattern**: Enter a dial string that will be matched against the “Request-URI” of the call.
- **Min**: Enter a minimum length used in the match criteria.

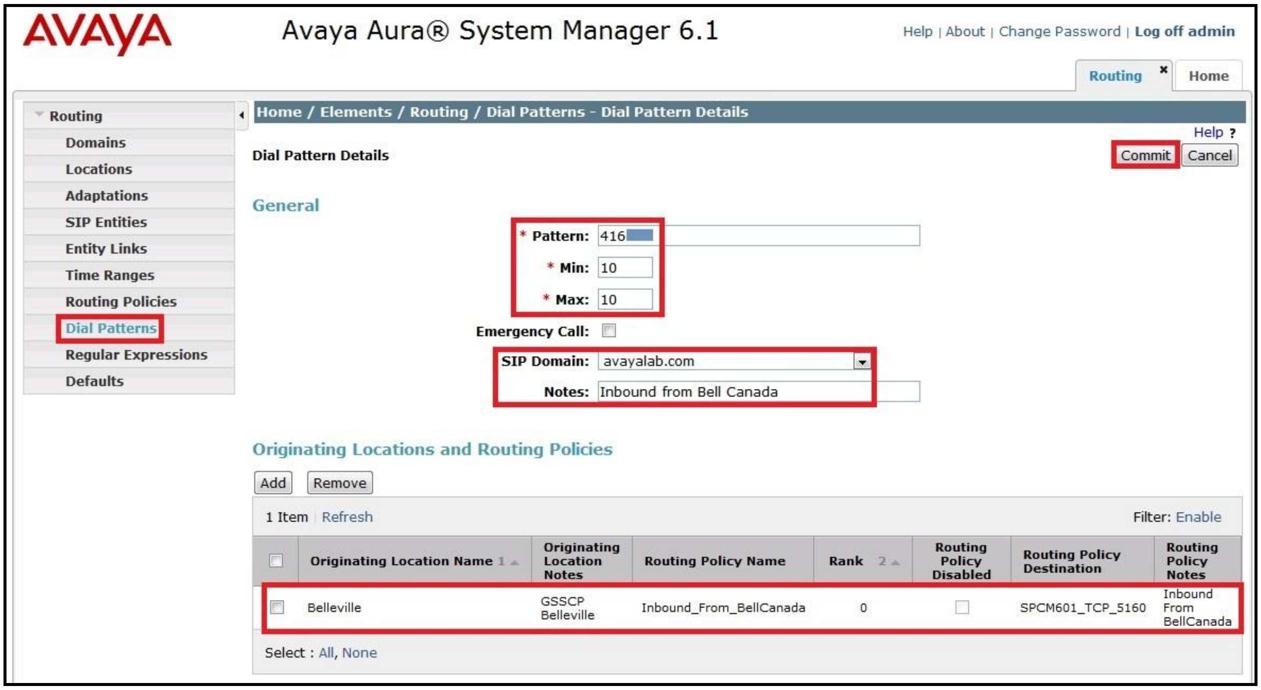
- **Max**: Enter a maximum length used in the match criteria.
- **SIP Domain**: Enter the destination domain used in the match criteria.
- **Notes**: Add a brief description (optional).

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

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

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

The first example shows a Dial Pattern for incoming calls that 10-digit DID numbers start with **416XXX** to SIP domain **avayalab.com** (after being translated by the Avaya SBCE from the service provider public SIP domain **cust2xxxx.xxxx.bell.ca** or **cust6xxxx.xxxx.bell.ca**). The Dial Pattern uses the Route Policy **Inbound_From_BellCanada** as defined in **Section 6.6**. These DID numbers are assigned to the enterprise by Bell Canada.



Dial Pattern Details

General

* Pattern: 416

* Min: 10

* Max: 10

Emergency Call: □

SIP Domain: avayalab.com

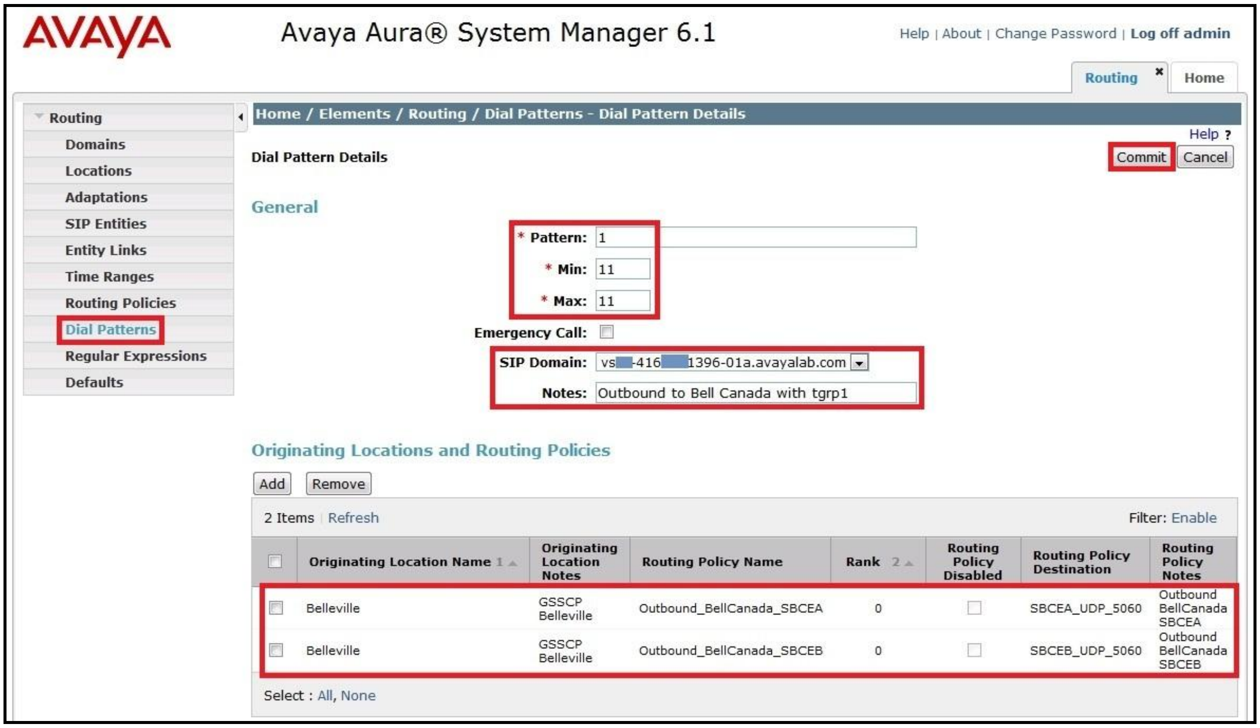
Notes: Inbound from Bell Canada

Originating Locations and Routing Policies

□	Originating Location Name	Originating Location Notes	Routing Policy Name	Rank	Routing Policy Disabled	Routing Policy Destination	Routing Policy Notes
□	Belleville	GSSCP Belleville	Inbound_From_BellCanada	0	□	SPCM601_TCP_5160	Inbound From BellCanada

The second example shows 2 Dial Patterns for outgoing calls that 11-digit dialed numbers begin with digit **1** and possibly have a destination SIP domain **vsxx-416XXX1396-01a.avayalab.com** (which contains “tgrp” **vsxx-416XXX1396-01a)** or SIP domain **vsxx-416XXX1880-01a.avayalab.com** (which contains “tgrp” **vsxx-416XXX1880-01a)**. Each Dial Pattern uses

Routing Policy **Outbound_BellCanada_SBCEA** and **Outbound_BellCanada_SBCEB** as defined in **Section 6.6** to "round-robin" route outgoing calls to the primary and secondary Avaya SBCE. It also ensures that if the primary Avaya SBCE is out of service, Session Manager shall failover to the secondary Avaya SBCE.



Dial Pattern Details

General

* Pattern: 1

* Min: 11

* Max: 11

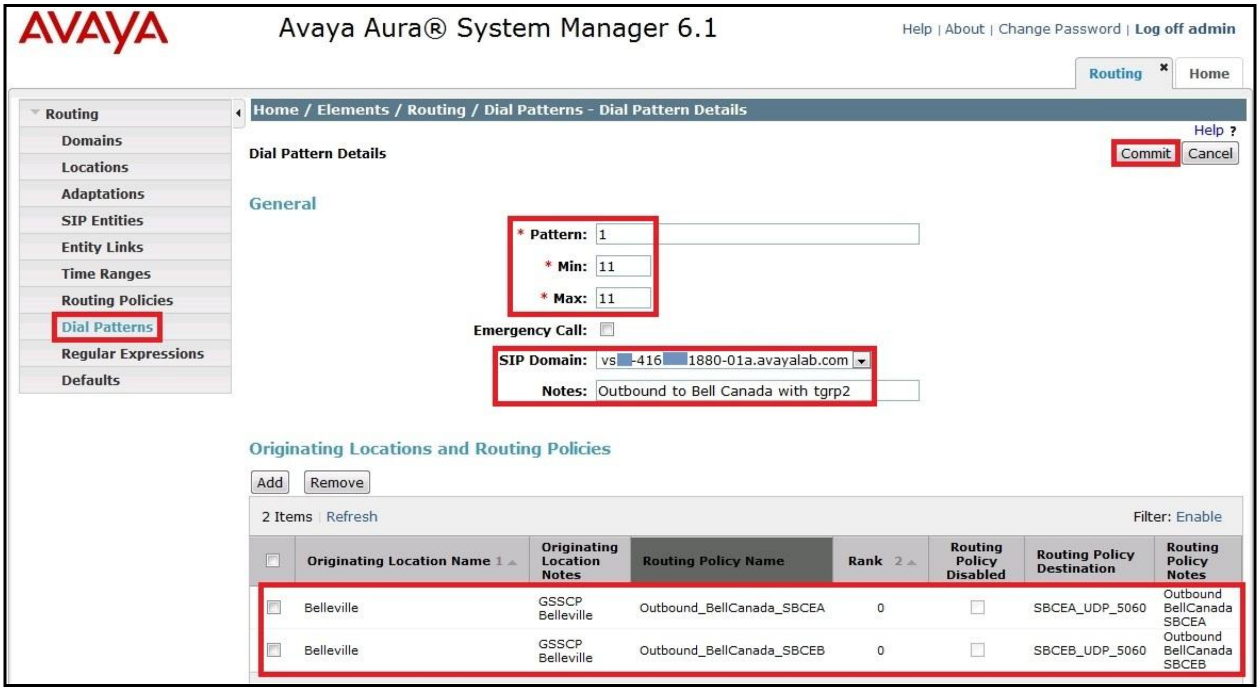
Emergency Call: □

SIP Domain: vs[redacted]-416[redacted]1396-01a.avayalab.com

Notes: Outbound to Bell Canada with tgrp1

Originating Locations and Routing Policies

□	Originating Location Name	Originating Location Notes	Routing Policy Name	Rank	Routing Policy Disabled	Routing Policy Destination	Routing Policy Notes
□	Belleville	GSSCP Belleville	Outbound_BellCanada_SBCEA	0	□	SBCEA_UDP_5060	Outbound BellCanada SBCEA
□	Belleville	GSSCP Belleville	Outbound_BellCanada_SBCEB	0	□	SBCEB_UDP_5060	Outbound BellCanada SBCEB



Dial Pattern Details

General

* Pattern: 1

* Min: 11

* Max: 11

Emergency Call: □

SIP Domain: vs[redacted]-416[redacted]1880-01a.avayalab.com

Notes: Outbound to Bell Canada with tgrp2

Originating Locations and Routing Policies

□	Originating Location Name	Originating Location Notes	Routing Policy Name	Rank	Routing Policy Disabled	Routing Policy Destination	Routing Policy Notes
□	Belleville	GSSCP Belleville	Outbound_BellCanada_SBCEA	0	□	SBCEA_UDP_5060	Outbound BellCanada SBCEA
□	Belleville	GSSCP Belleville	Outbound_BellCanada_SBCEB	0	□	SBCEB_UDP_5060	Outbound BellCanada SBCEB

Note: The SIP Domain can be simply selected as **-ALL-**. It will apply to all outgoing calls with a specific Dial Pattern regardless the destination SIP Domains.

6.8 Add/View Avaya Aura® Session Manager

The creation of a Session Manager element provides the linkage between System Manager and Session Manager. This was most likely done as part of the initial Session Manager installation. To add a Session Manager, navigate to **Home → Elements → Session Manager → Session Manager Administration** in the left navigation pane and click on the **New** button in the right pane (not shown). If the 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 the **General** section, enter the following values:

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

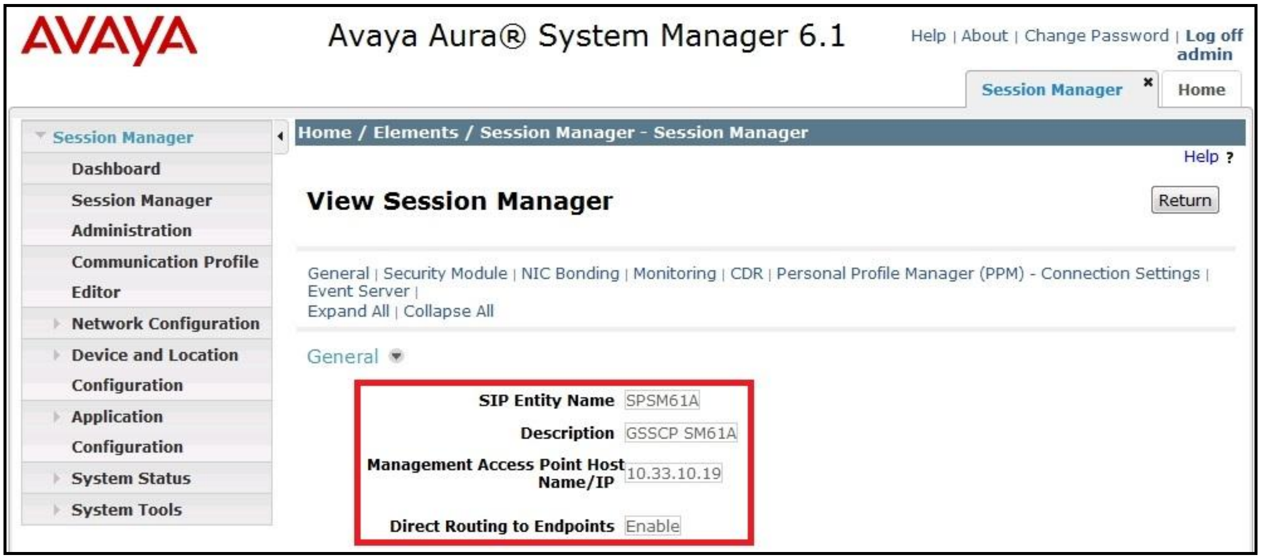
In the **Security Module** section, enter the following values:

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

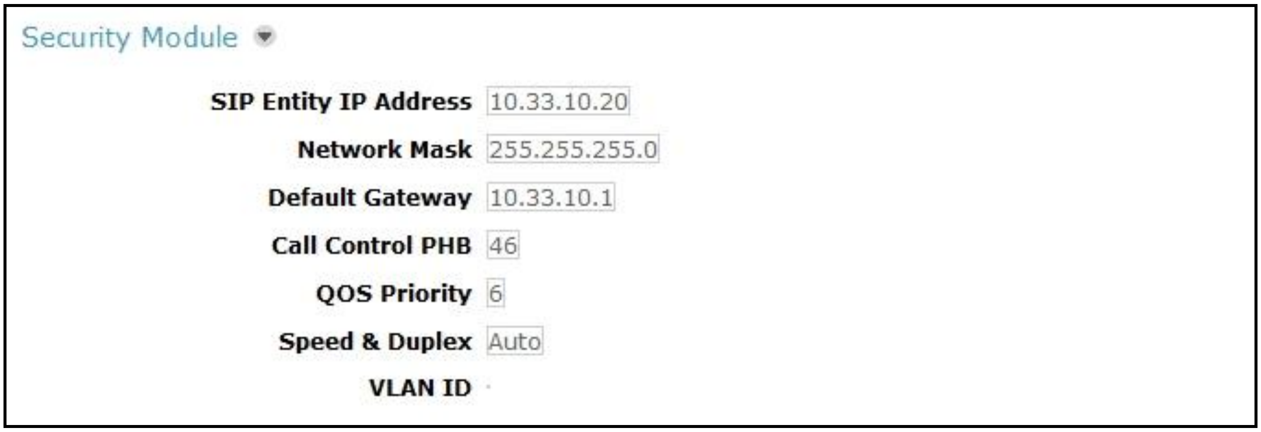
In **Monitoring** section, verify **Enable Monitoring** is checked.

Use default values for the remaining fields. Then click **Save** (not shown).

The screenshots below show the primary Session Manager values.


AVAYA
Avaya Aura® System Manager 6.1
Help | About | Change Password | Log off admin
Session Manager
Home
Session Manager
Dashboard
Session Manager Administration
Communication Profile Editor
Network Configuration
Device and Location Configuration
Application Configuration
System Status
System Tools
Home / Elements / Session Manager - Session Manager
Help ?
View Session Manager
Return
General | Security Module | NIC Bonding | Monitoring | CDR | Personal Profile Manager (PPM) - Connection Settings | Event Server |
Expand All | Collapse All
General

SIP Entity Name: SPSM61A
Description: GSSCP SM61A
Management Access Point Host Name/IP: 10.33.10.19
Direct Routing to Endpoints: Enable


Security Module

SIP Entity IP Address 10.33.10.20

Network Mask 255.255.255.0

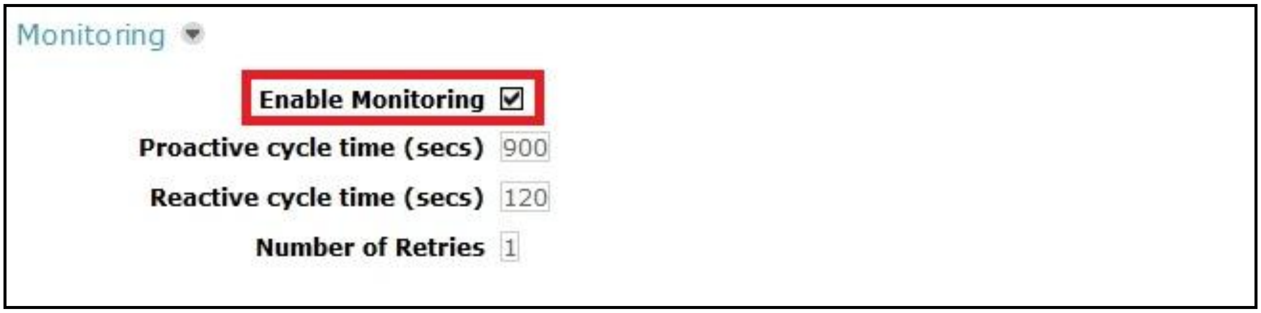
Default Gateway 10.33.10.1

Call Control PHB 46

QOS Priority 6

Speed & Duplex Auto

VLAN ID


Monitoring

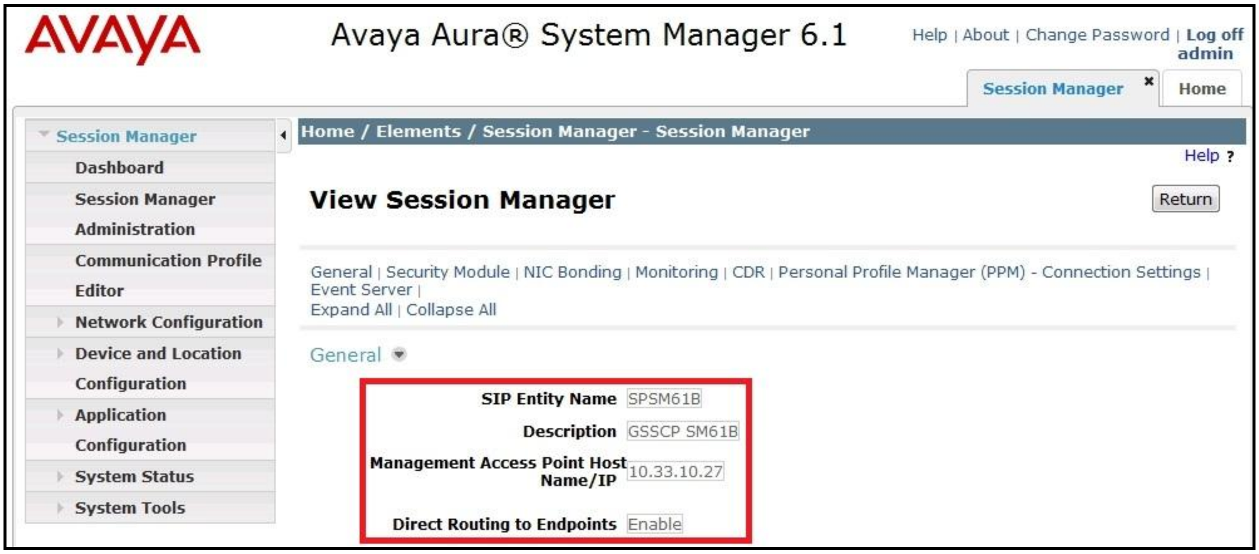
Enable Monitoring ☑

Proactive cycle time (secs) 900

Reactive cycle time (secs) 120

Number of Retries 1

The screenshots below show the secondary Session Manager values.


AVAYA
Avaya Aura® System Manager 6.1
Help | About | Change Password | Log off
admin
Session Manager
Home
Session Manager
Dashboard
Session Manager Administration
Communication Profile Editor
Network Configuration
Device and Location Configuration
Application Configuration
System Status
System Tools
Home / Elements / Session Manager - Session Manager
Help ?
Return
General | Security Module | NIC Bonding | Monitoring | CDR | Personal Profile Manager (PPM) - Connection Settings | Event Server |
Expand All | Collapse All

View Session Manager

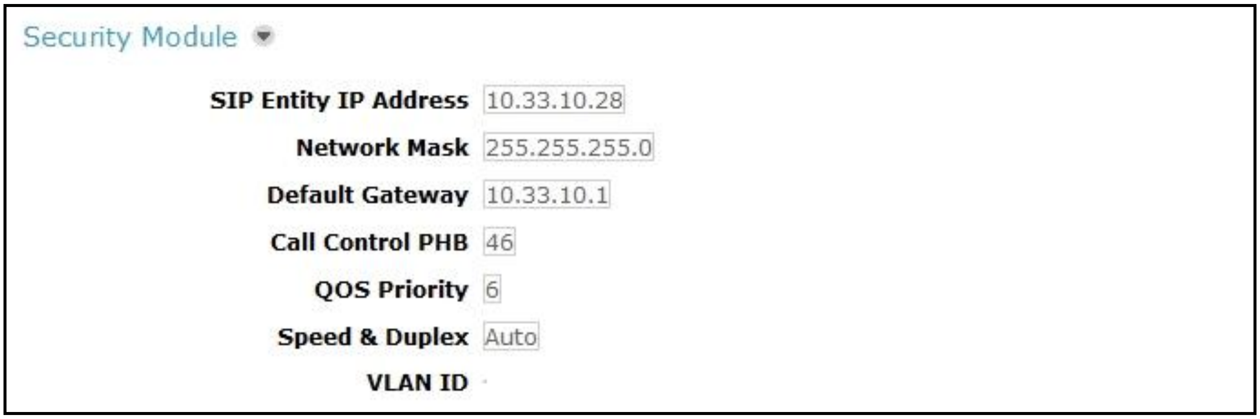
General

SIP Entity Name SPSM61B

Description GSSCP SM61B

Management Access Point Host Name/IP 10.33.10.27

Direct Routing to Endpoints Enable



Security Module

SIP Entity IP Address 10.33.10.28

Network Mask 255.255.255.0

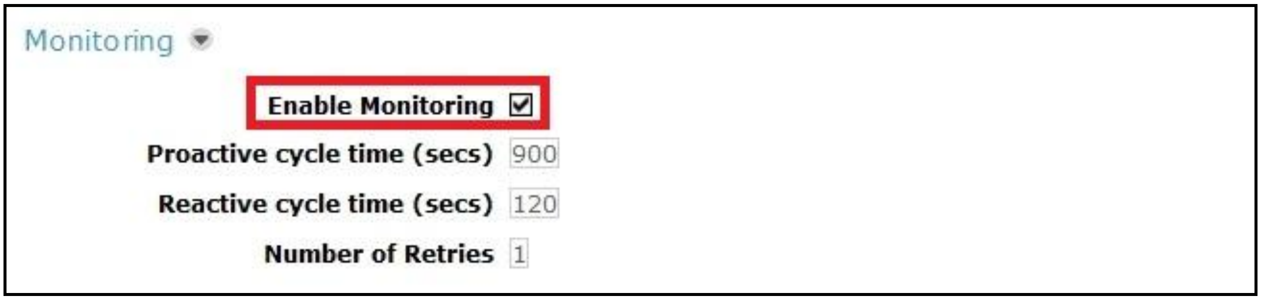
Default Gateway 10.33.10.1

Call Control PHB 46

QOS Priority 6

Speed & Duplex Auto

VLAN ID



Monitoring

Enable Monitoring ☑

Proactive cycle time (secs) 900

Reactive cycle time (secs) 120

Number of Retries 1

7. Configure Avaya Session Border Controller for Enterprise

This section covers the configuration of the Avaya SBCE. It is assumed that the software has already been installed. For additional information on these configuration tasks, see **References [12]** and **[13]**.

The compliance testing comprised the configuration for two major components, Trunk Server for service provider and Call Server for enterprise. Each component consists of a set of Global Profiles, Domain Policies and Device Specific Settings. The configuration is defined in the Avaya SBCE web user interface as described in the 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 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

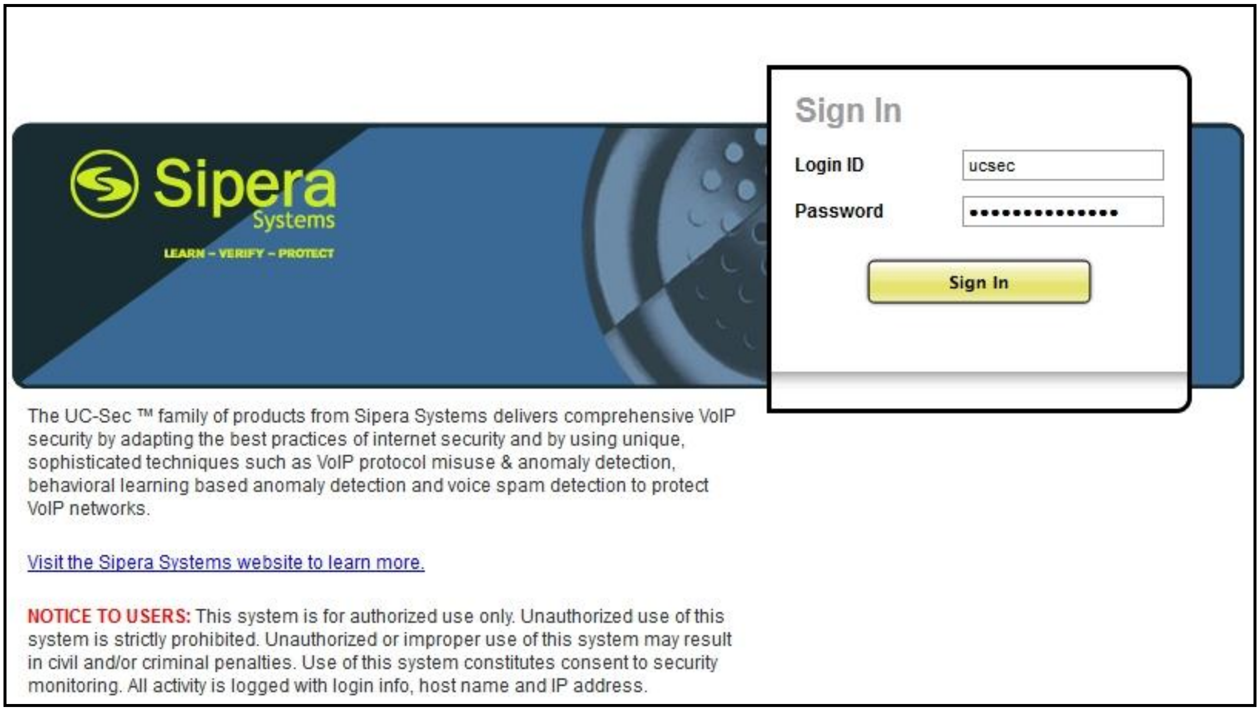
In the compliance testing, geographic redundancy was implemented on the Avaya SBCE. When the primary Avaya SBCE is out of service, the SIP Trunk will be established between Session Manager and the secondary Avaya SBCE. Therefore, the configuration for the primary Avaya SBCE needs to be replicated to the secondary Avaya SBCE.

Note: The primary and secondary Avaya SBCEs are two separate physical servers with different management IP addresses. The common procedure can be used for configuration using the Avaya SBCE web interface which is formerly the Sipera Unified Communication Security (UC-Sec) appliance. The screenshots in each section may be taken from both web interfaces to illustrate the detailed configuration of the primary and secondary Avaya SBCE.

7.1 Avaya Session Border Controller for Enterprise Login

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

Enter the appropriate credentials then click ***Sign In***.



Login ID: ucsec

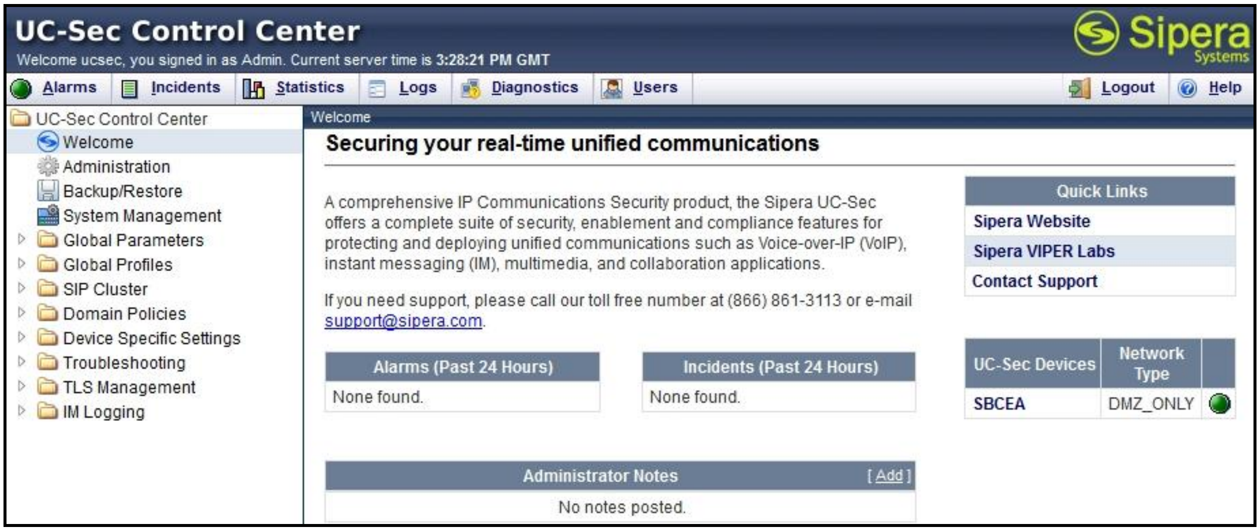
Password: •••••••••••••••

The UC-Sec ™ family of products from Sipera Systems delivers comprehensive VoIP security by adapting the best practices of internet security and by using unique, sophisticated techniques such as VoIP protocol misuse & anomaly detection, behavioral learning based anomaly detection and voice spam detection to protect VoIP networks.

Visit the Sipera Systems website to learn more.

NOTICE TO USERS: This system is for authorized use only. Unauthorized use of this system is strictly prohibited. Unauthorized or improper use of this system may result in civil and/or criminal penalties. Use of this system constitutes consent to security monitoring. All activity is logged with login info, host name and IP address.

The main page of the **UC-Sec Control Center** will appear.



Welcome ucsec, you signed in as Admin. Current server time is 3:28:21 PM GMT

Securing your real-time unified communications

A comprehensive IP Communications Security product, the Sipera UC-Sec offers a complete suite of security, enablement and compliance features for protecting and deploying unified communications such as Voice-over-IP (VoIP), instant messaging (IM), multimedia, and collaboration applications.

If you need support, please call our toll free number at (866) 861-3113 or e-mail support@sipera.com.

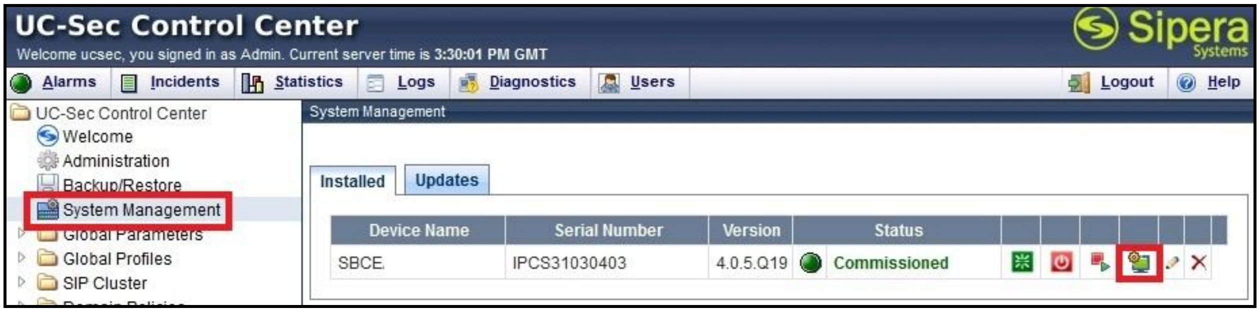
Alarms (Past 24 Hours)
None found.

Incidents (Past 24 Hours)
None found.

UC-Sec Devices	Network Type	
SBCEA	DMZ_ONLY	●

Administrator Notes
No notes posted.

To view system information that was configured during installation, navigate to **UC-Sec Control Center → System Management**. A list of installed devices is shown in the right pane. To view the configuration of this device, click the **View Config** icon (the third icon from the right).



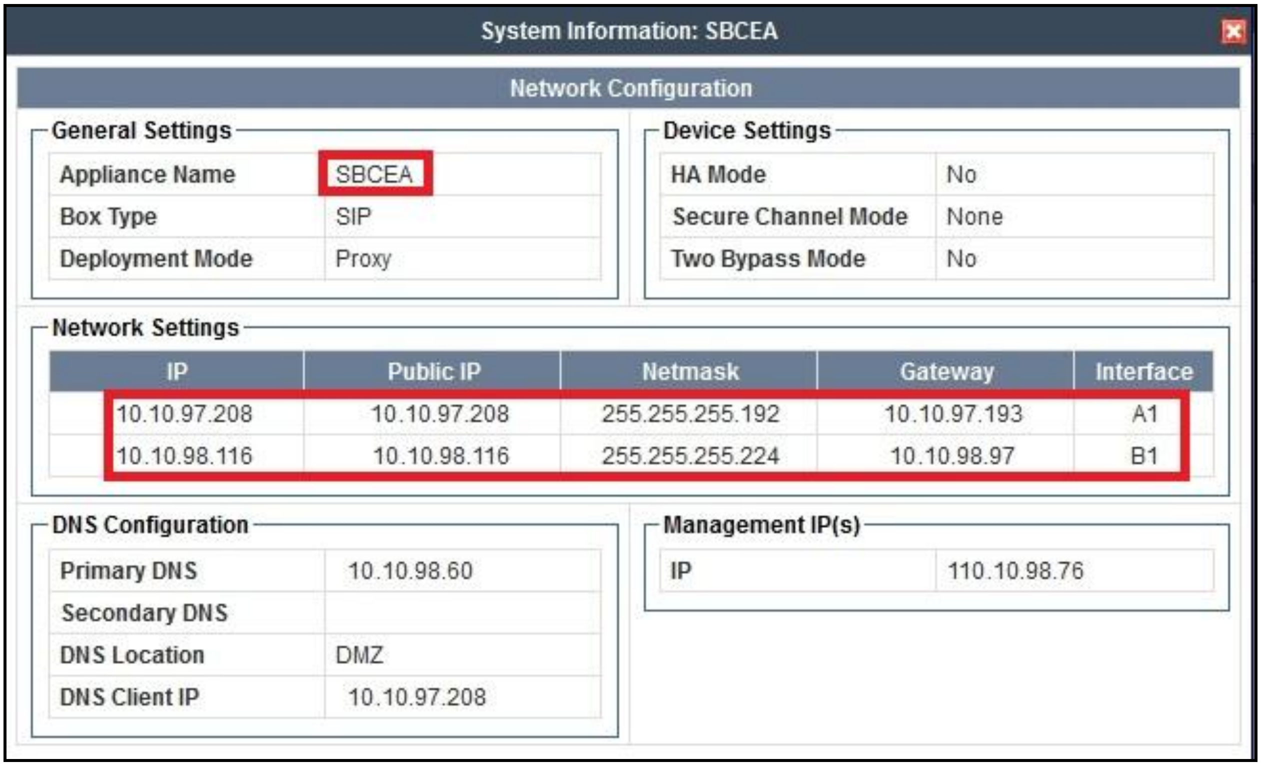
Welcome ucsec, you signed in as Admin. Current server time is 3:30:01 PM GMT

Device Name	Serial Number	Version	Status							
SBCE	IPCS31030403	4.0.5.Q19	● Commissioned							✕

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

Use the common procedure, login to the web interface of both primary and secondary Avaya SBCE to display the System Information as described below.

The following screenshot shows the System Information of the primary Avaya SBCE.



System Information: SBCEA

Network Configuration

General Settings

Appliance Name	SBCEA
Box Type	SIP
Deployment Mode	Proxy

Device Settings

HA Mode	No
Secure Channel Mode	None
Two Bypass Mode	No

Network Settings

IP	Public IP	Netmask	Gateway	Interface
10.10.97.208	10.10.97.208	255.255.255.192	10.10.97.193	A1
10.10.98.116	10.10.98.116	255.255.255.224	10.10.98.97	B1

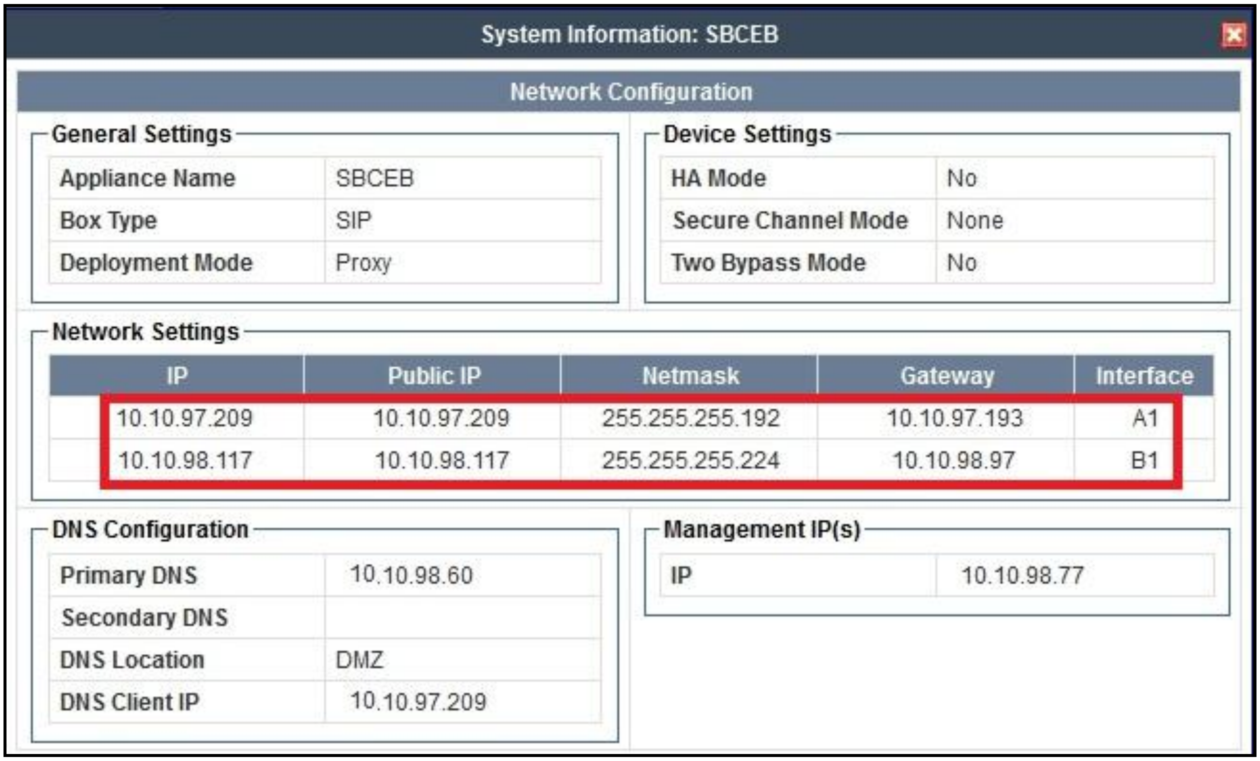
DNS Configuration

Primary DNS	10.10.98.60
Secondary DNS	
DNS Location	DMZ
DNS Client IP	10.10.97.208

Management IP(s)

IP	110.10.98.76

The following screenshot shows the System Information of the secondary Avaya SBCE.



System Information: SBCEB

Network Configuration

General Settings

Appliance Name	SBCEB
Box Type	SIP
Deployment Mode	Proxy

Device Settings

HA Mode	No
Secure Channel Mode	None
Two Bypass Mode	No

Network Settings

IP	Public IP	Netmask	Gateway	Interface
10.10.97.209	10.10.97.209	255.255.255.192	10.10.97.193	A1
10.10.98.117	10.10.98.117	255.255.255.224	10.10.98.97	B1

DNS Configuration

Primary DNS	10.10.98.60
Secondary DNS	
DNS Location	DMZ
DNS Client IP	10.10.97.209

Management IP(s)

IP	10.10.98.77

7.2 Global Profiles

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

Note: Each individual profile will need to be created for both the primary Avaya SBCE and secondary Avaya SBCE using separate web interfaces.

7.2.1 Uniform Resource Identifier (URI) Groups

The URI Group feature allows users to create any number of logical URI Groups that are comprised of individual SIP subscribers which are 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 taken for a given call flow.

To add an URI Group, select **UC-Sec Control Center → Global Profiles → URI Groups**. Click on **Add Group** (not shown).

After the URI Group has been added, click **Add URI** then select **Regular Expression** (not shown) to define URI values for each URI Group as described below.

In the compliance testing, multiple URI Groups were created on each Avaya SBCE. Typically, a single URI Group is defined to route OPTIONS heartbeat, another URI Group for incoming calls and multiple URI Groups for outgoing calls appropriately to multiple trunk groups provided by Bell Canada. These URI Groups are used to match the “From” and “To” headers in a SIP call dialog received from the enterprise or from Bell Canada. If there is a match, then the Avaya SBCE applies the appropriate Routing profile and Server Flow to route the incoming and outgoing calls to the right destinations. The Routing profile and Server Flow are discussed next in **Section 7.2.2** and **Section 7.4.4**.

Notes:

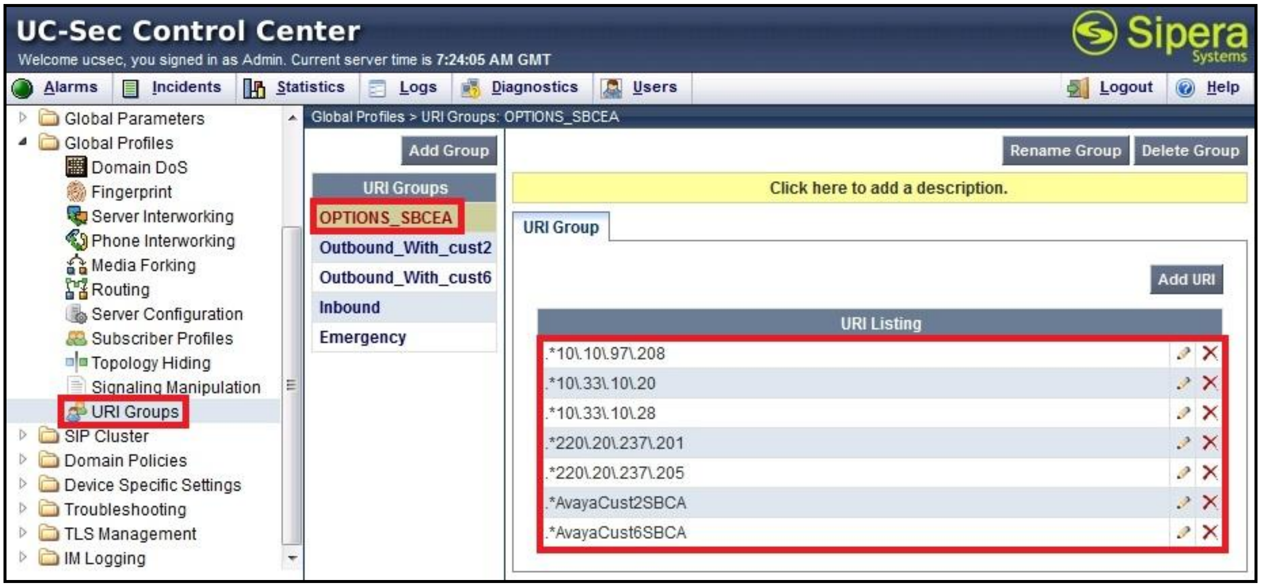
- Each URI Group will necessarily be created for both primary Avaya SBCE and secondary Avaya SBCE using separate web interfaces.
- The URI values were added using **Regular Expression** format.

The URI Group for OPTIONS heartbeat is to route the OPTIONS between Session Manager and Bell Canada networks to monitor for the status of SIP Trunk, it is to detect the failover that may happen at Session Manager or at Bell Canada CO level.

For incoming OPTIONS from the primary and secondary Bell Canada CO to Session Managers via the primary Avaya SBCE, if the OPTIONS is originated from the primary Bell Canada CO, it has the “Request-URI” and “To” headers with SIP domain **AvayaCust2SBCA** and the “From” header with IP address of the primary Bell Canada CO 220.20.237.201. Similarly, if the OPTIONS is originated from the secondary Bell Canada CO, it has the “Request-URI” and “To” headers with SIP domain **AvayaCust6SBCA** and the “From” header with IP address of the primary Bell Canada CO 220.20.237.205.

For outgoing OPTIONS from the primary Session Manager to Bell Canada via the primary Avaya SBC, if the OPTIONS is originated from the primary Session Manager, it has the "Request-URI" and "To" headers with the IP address of the primary Avaya SBCE 10.10.97.208 and the "From" header with the IP address of the primary Session Manager 10.33.10.20. Similarly, if the OPTIONS is originated from the secondary Session Manager, it has the "Request-URI" and "To" headers with the IP address of the primary Avaya SBCE 10.10.97.208 and the "From" header with the IP address of the secondary Session Manager 10.33.10.28.

Following screenshot shows the URI-Group **OPTIONS_SBCA** created on the primary Avaya SBCE.

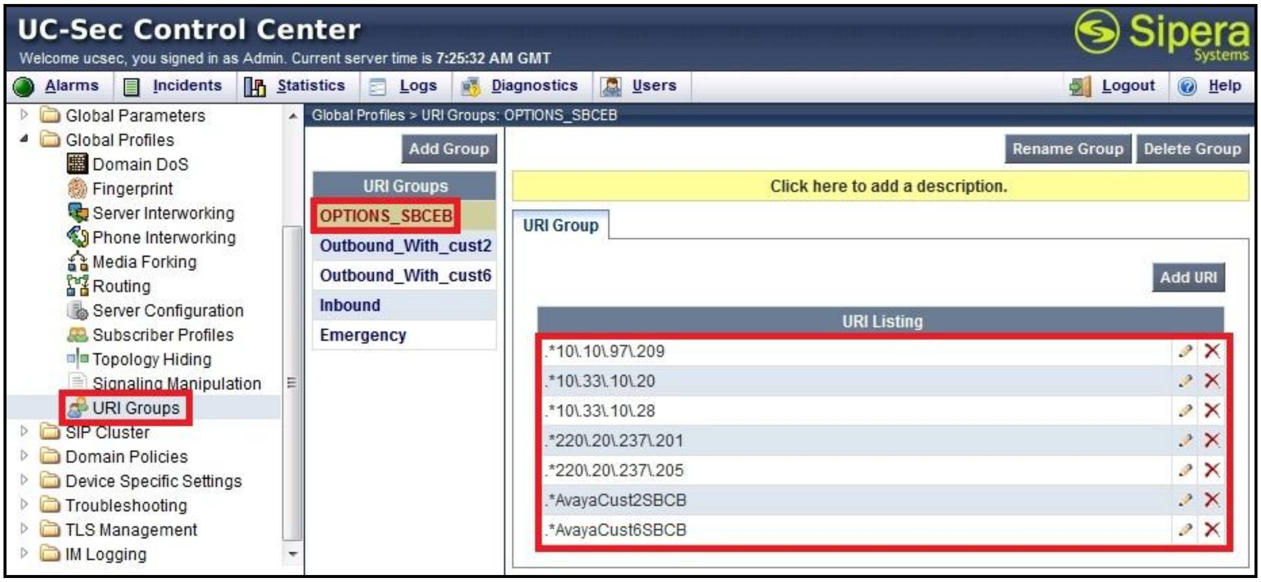


URI Listing
.*10\.10\.97\.208
.*10\.33\.10\.20
.*10\.33\.10\.28
.*220\.20\.237\.201
.*220\.20\.237\.205
.*AvayaCust2SBCA
.*AvayaCust6SBCA

For incoming OPTIONS from the primary and secondary Bell Canada CO at Bell Canada networks to Session Managers via the secondary Avaya SBCE, if the OPTIONS is originated from the primary Bell Canada CO, it has the "Request-URI" and "To" header with SIP domain **AvayaCust2SBCB** and the "From" header with IP address of the primary Bell Canada CO 220.20.237.201. Similarly, if the OPTIONS is originated from the secondary Bell Canada CO, it has the "Request-URI" and "To" header with SIP domain **AvayaCust6SBCB** and the "From" header with IP address of the primary Bell Canada CO 220.20.237.205.

For outgoing OPTIONS from the primary Session Manager to Bell Canada via the secondary Avaya SBC, if the OPTIONS is originated from the primary Session Manager, it has the "Request-URI" and "To" headers with the IP address of the secondary Avaya SBCE 10.10.97.209 and the "From" header with the IP address of the primary Session Manager 10.33.10.20. Similarly, if the OPTIONS is originated from the secondary Session Manager, it has the "Request-URI" and "To" headers with the IP address of the secondary Avaya SBCE 10.10.97.209 and the "From" header with the IP address of the secondary Session Manager 10.33.10.28.

Following screenshot shows the URI-Group **OPTIONS_SBCB** created on the secondary Avaya SBCE.



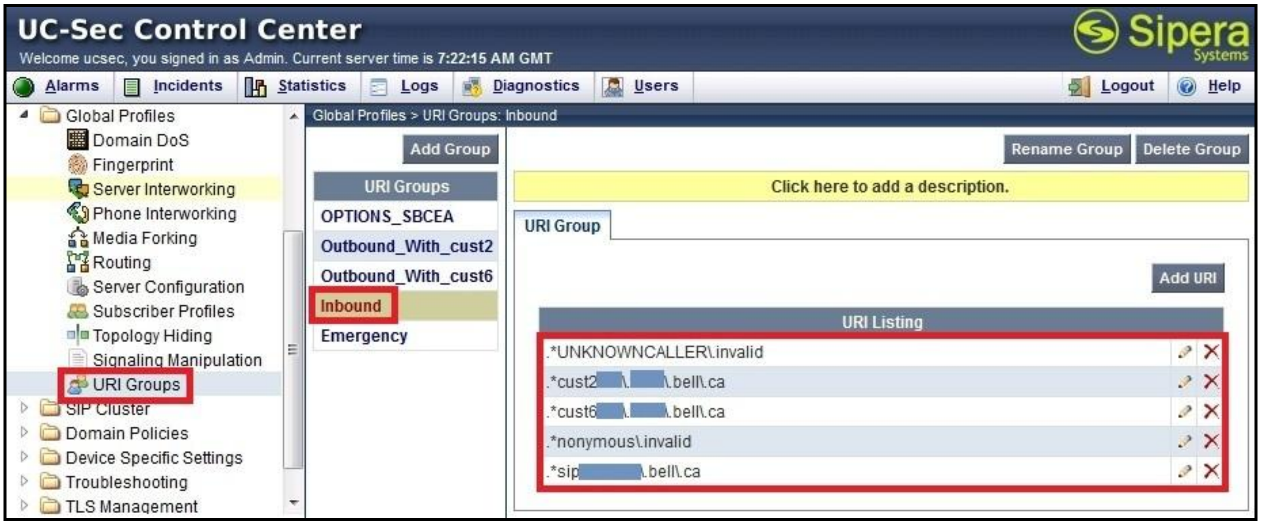
Global Profiles > URI Groups: OPTIONS_SBCEB

URI Groups:
- OPTIONS_SBCEB
- Outbound_With_cust2
- Outbound_With_cust6
- Inbound
- Emergency

URI Listing
.*10\.10\.97\.209
.*10\.33\.10\.20
.*10\.33\.10\.28
.*220\.20\.237\.201
.*220\.20\.237\.205
.*AvayaCust2SBCB
.*AvayaCust6SBCB

Another URI Group was added to route incoming calls from both primary and secondary Bell Canada CO to Communication Manager via Session Managers. If an incoming INVITE is originated by the primary Bell Canada CO, it has the "Request-URI" and "To" headers with SIP domain **cust2xxxx.xxxx.bell.ca** and the "From" header with SIP domain **sipxxxxxxxx.bell.ca**. Similarly, if an incoming INVITE is originated by the secondary Bell Canada CO, it has the "Request-URI" and "To" headers with SIP domain **cust6xxxx.xxxx.bell.ca** and the "From" header with SIP domain **sipxxxxxxxx.bell.ca**. In case of incoming private calls, Bell Canada sends the incoming INVITE with SIP domain **UNKNOWNCALLER.invalid** or **anonymous.invalid**. These values are also added to support receiving the private calls.

The following screenshot show URI Group **Inbound** created on the primary Avaya SBCE for incoming calls to include all possible SIP domains in the "From" and "To" headers.



.*UNKNOWNCALLER\.invalid
.*cust2[redacted]\.[redacted]\.bell\.ca
.*cust6[redacted]\.[redacted]\.bell\.ca
.*nonymous\.invalid
.*sip[redacted]\.bell\.ca

Use the procedure to replicate the same URI Group **Inbound** for incoming calls to the secondary Avaya SBCE (not shown).

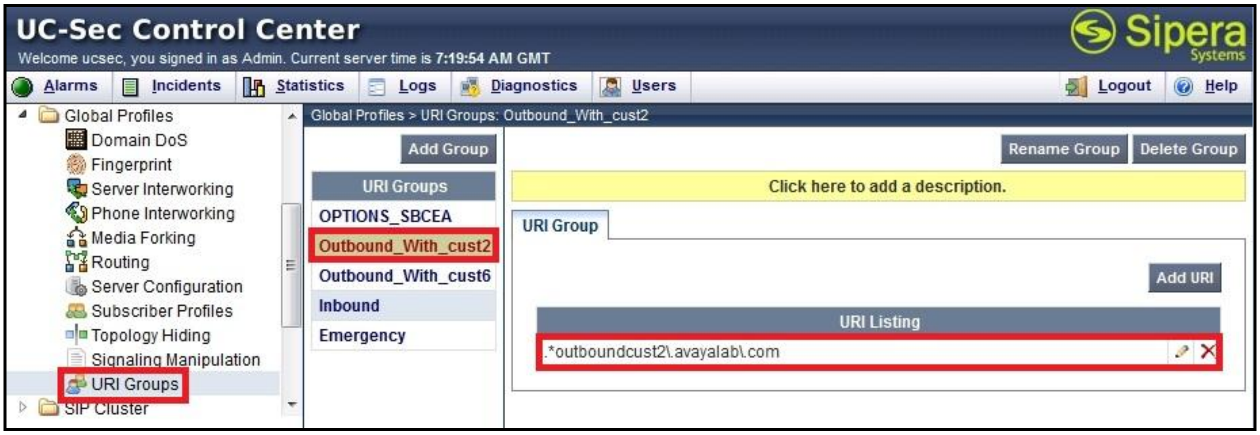
Two URI Groups **Outbound_With_cust2** and **Outbound_With_cust6** were added for outgoing calls from Communication Manager to Bell Canada via both primary and secondary Session Managers.

In the sample configuration, outgoing calls are manipulated by the SigMa script defined for Session Manager as described in **Section 7.2.5**. After the manipulation, if an outgoing INVITE is originated by DID numbers associated with service provider public SIP domain **cust2xxxx.xxxx.bell.ca**, it has the "Request-URI" and "To" headers with **outgoingcust2.avayalab.com** and the "From" header with **avayalab.com**. Similarly, if an outgoing INVITE is originated by DID numbers associated with service provider public SIP domain **cust6xxxx.xxxx.bell.ca**, it has the "Request-URI" and "To" headers with **outgoingcust6.avayalab.com** and the "From" header with **avayalab.com**.

The compliance testing was conducted with two DID ranges **416XXX13XX** and **416XXX18XX** which associated with two service provider public SIP domains **cust2xxxx.xxxx.bell.ca** and **cust6xxxx.xxxx.bell.ca**. Bell Canada assigned separate DID numbers under each service provider public SIP domain and require outgoing calls have the proper combination of the DID number with the service provider public SIP domain. For example, a DID number 416XXX1397 associates to service provider public SIP domain **cust2xxxx.xxxx.bell.ca**. If an outgoing call has the "Request-URI" with the right combination of 416XXX1397 and **cust2xxxx.xxxx.bell.ca**, it will be successful. However, if the same DID number makes an outgoing call and has the "Request-URI" with the incorrect combination of 416XXX1397 and **cust6xxxx.xxxx.bell.ca**, it will be examined and rejected by Bell Canada.

For the DID number and SIP domain constrained as described above, two separate URI Groups were created for SIP domains **outgoingcust2.avayalab.com** and **outgoingcust6.avayalab.com** to route the call into a certain Server Flow (see **Section 7.4.4**) so that the Topology Hiding profile (see **Section 7.2.2**) under that Server Flow can be applied to outgoing calls. For the SIP domain **outgoingcust2.avayalab.com**, the Topology Hiding profile masks the “From” header with **cust2xxxx.xxxx.bell.ca** and the “Request-URI” and “To” headers with **sipxxxxxxxx.bell.ca** before sending outgoing calls toward Bell Canada networks. Similarly, for the SIP domain **outgoingcust6.avayalab.com**, the Topology Hiding profile masks the “From” header with **cust6xxxx.xxxx.bell.ca** and the “Request-URI” and “To” headers with **sipxxxxxxxx.bell.ca**.

Following screenshots show the URI Groups **Outbound_With_cust2** and **Outbound_With_cust6** created on the primary Avaya SBCE for outgoing calls.

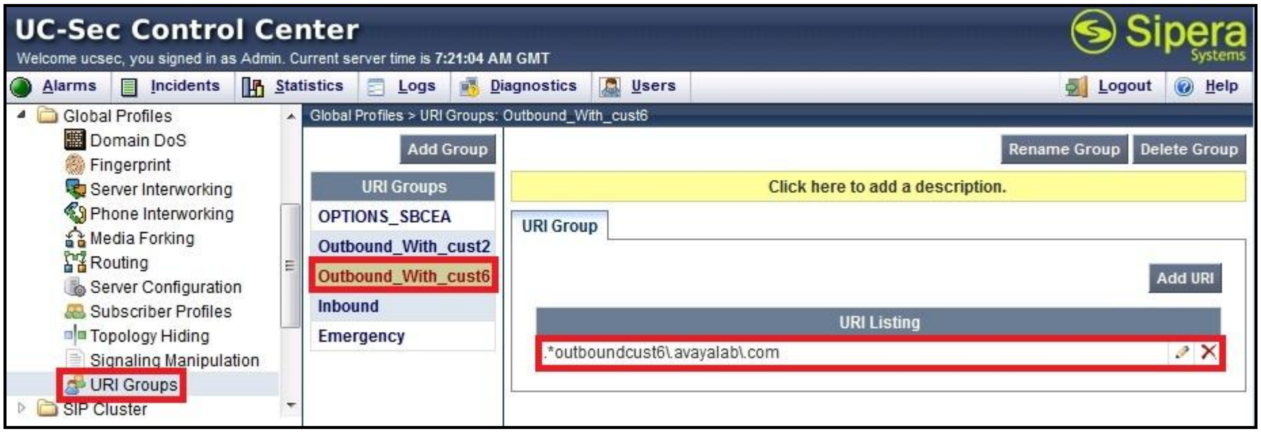


UC-Sec Control Center

Welcome ucsec, you signed in as Admin. Current server time is **7:19:54 AM GMT**

Global Profiles > URI Groups: Outbound_With_cust2

URI Listing: .*outboundcust2\.avayalab\.com



UC-Sec Control Center

Welcome ucsec, you signed in as Admin. Current server time is **7:21:04 AM GMT**

Global Profiles > URI Groups: Outbound_With_cust6

URI Listing: .*outboundcust6\.avayalab\.com

Use the procedure to replicate the same URI Groups **Outbound_With_cust2** and **Outbound_With_cust6** to the secondary Avaya SBCE (not shown).

7.2.2 Routing

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 a Routing profile, select **UC-Sec Control Center → Global Profiles → Routing**. Click on **Add Profile** (not shown).

In the compliance testing, two Routing profiles were created on each Avaya SBCE. Routing profile **To_BellCanada** was created to be used in conjunction with the Server Flows defined for Session Managers. This entry is to route the outgoing enterprise calls to Bell Canada. On the opposite direction, Routing profile **To_CM** was created to be used in conjunction with the Server Flows defined for Bell Canada. This entry is to route incoming calls from Bell Canada to the enterprise.

Note: Each Routing profile will need to be created for both the primary Avaya SBCE and secondary Avaya SBCE using separate web interfaces.

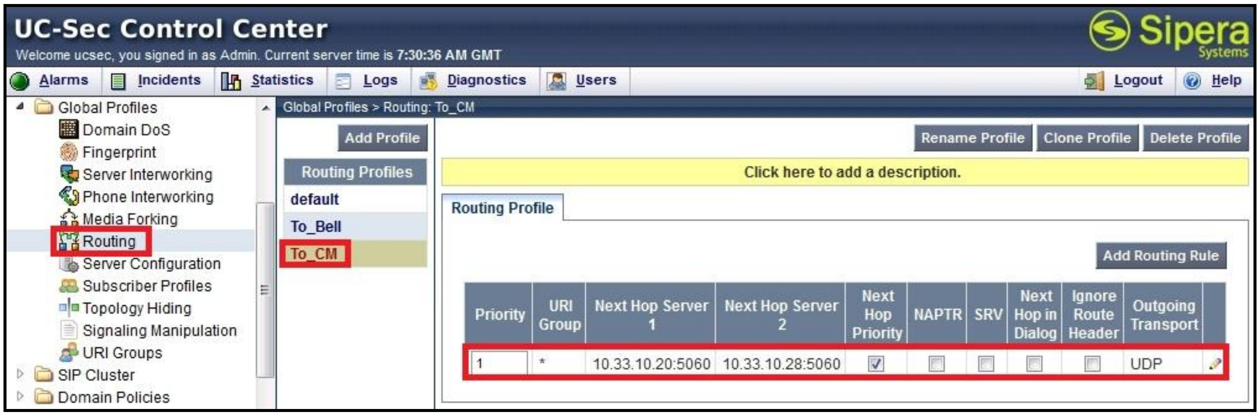
7.2.2.1 Routing Profile for Avaya Aura® Session Manager

The screenshot below illustrates the Routing profile **To_CM**. As shown in **Figure 1**, Session Managers are connected with transportation protocol **UDP** on port **5060**. Incoming calls will be routed firstly to the **Next Hop Server 1** which is the IP address of the primary Session Manager **10.10.13.20** and secondly to the **Next Hop Server 2** which is the IP address of the secondary Session Manager **10.10.13.28** if the primary Session Manager is out of service.

- Select **URI Group** as * to disable checking the "From" and "To" headers against predefine URI Groups in **Section 7.2.1**.
- Check on **Routing Priority based on Next Hop Server**.
- Enter the **Next Hop Server 1** and **Next Hop Server 2** as the IP address of the primary and secondary Session Manager with port **5060**.
- Select **Outgoing Transport** as **UDP**.

Click **Finish** to save.

Following screenshot shows the Routing profile **To_CM** created on the primary Avaya SBCE.



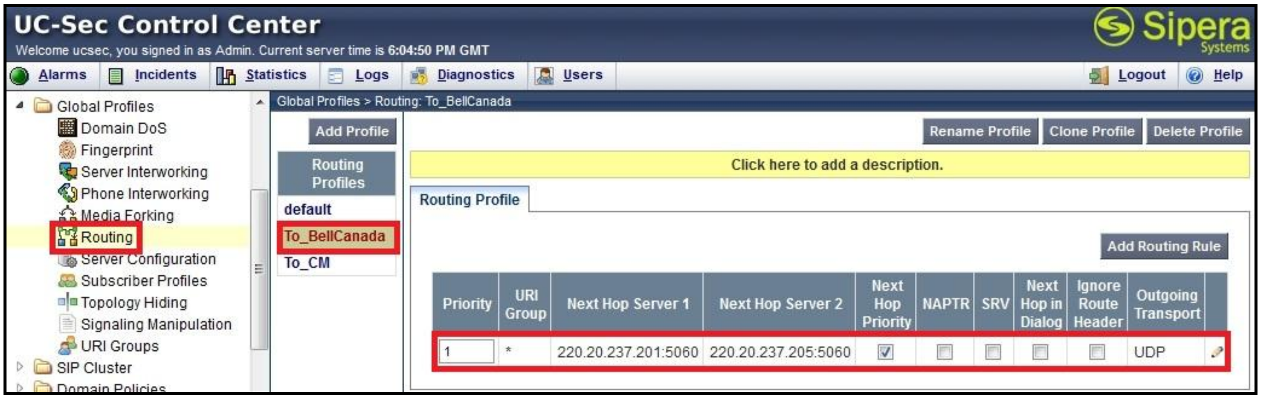
Priority	URI Group	Next Hop Server 1	Next Hop Server 2	Next Hop Priority	NAPTR	SRV	Next Hop in Dialog	Ignore Route Header	Outgoing Transport
1	*	10.33.10.20:5060	10.33.10.28:5060	☑	□	□	□	□	UDP

Use the procedure to replicate the same Routing profile **To_CM** to the secondary Avaya SBCE (not shown).

7.2.2.2 Routing Profile for Bell Canada

Routing profile **To_BellCanada** was similarly created to route outgoing calls to **Next Hop Server 1** and **Next Hop Server 2** which are the IP addresses of the primary Bell Canada CO 220.20.237.201 and the secondary Bell Canada CO 220.20.237.205. As shown in **Figure 1**, Bell Canada CO(s) are connected with transportation protocol **UDP** on port **5060**.

Following screenshot shows the Routing profile **To_BellCanada** created on the primary Avaya SBCE.



Welcome ucsec, you signed in as Admin. Current server time is 6:04:50 PM GMT

Priority	URI Group	Next Hop Server 1	Next Hop Server 2	Next Hop Priority	NAPTR	SRV	Next Hop in Dialog	Ignore Route Header	Outgoing Transport
1	*	220.20.237.201:5060	220.20.237.205:5060	☑	□	□	□	□	UDP

Use the procedure to replicate the same Routing profile **To_BellCanada** to the secondary Avaya SBCE (not shown).

7.2.3 Topology Hiding

Topology Hiding is an Avaya SBCE security feature 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 a Topology Hiding profile, select **UC-Sec Control Center → Global Profiles → Topology Hiding**. Click on **Add Profile** (not shown).

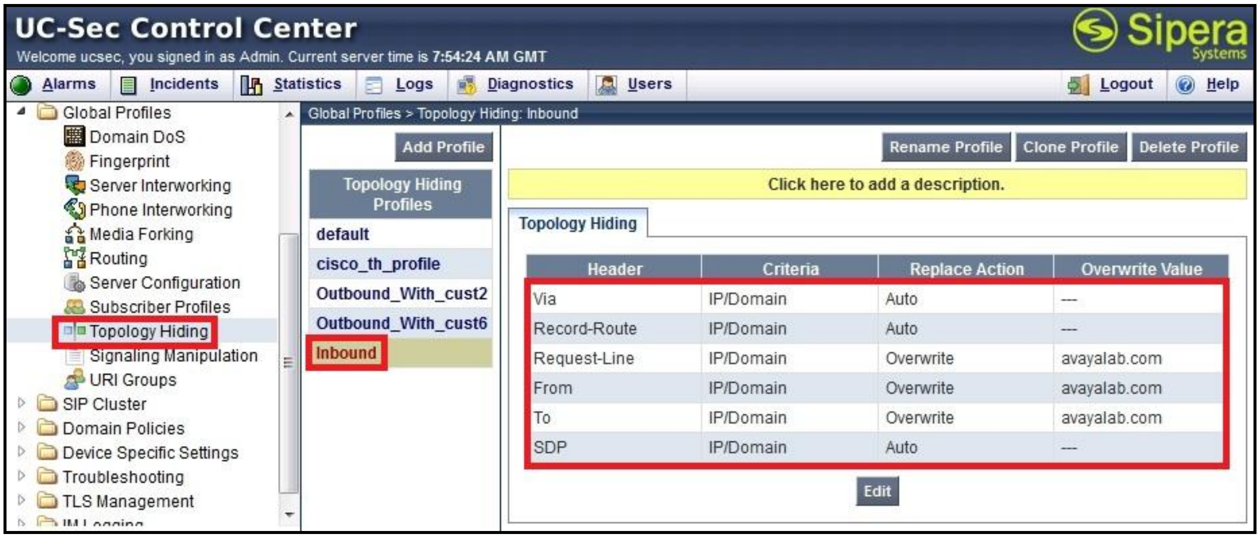
In the compliance testing, multiple Topology Hiding profiles were created on each Avaya SBCE. A single Topology Hiding profile was created for incoming calls and multiple Topology Hiding profiles for outgoing calls appropriately to multiple trunk groups provided by Bell Canada.

Note: Each Topology Hiding profile will need to be created for both the primary Avaya SBCE and secondary Avaya SBCE using separate web interfaces.

7.2.3.1 Topology Hiding Profiles for Incoming Calls

Topology Hiding profile **Inbound** was created to mask the service provider public SIP domains in the "Request-URI", "To" and "From" headers to **avayalab.com** which is the enterprise SIP domain configured on Session Manager and Communication Manager. It also normalizes the original "Record-Route" and "Via" headers from Bell Canada and replaces the external IP addresses in the SDP by internal IP address of the Avaya SBCE.

The screenshots below shows Topology Hiding profile **Inbound** created on the primary Avaya SBCE.



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

Use the procedure to replicate the same Topology Hiding profile **Inbound** to the secondary Avaya SBCE.

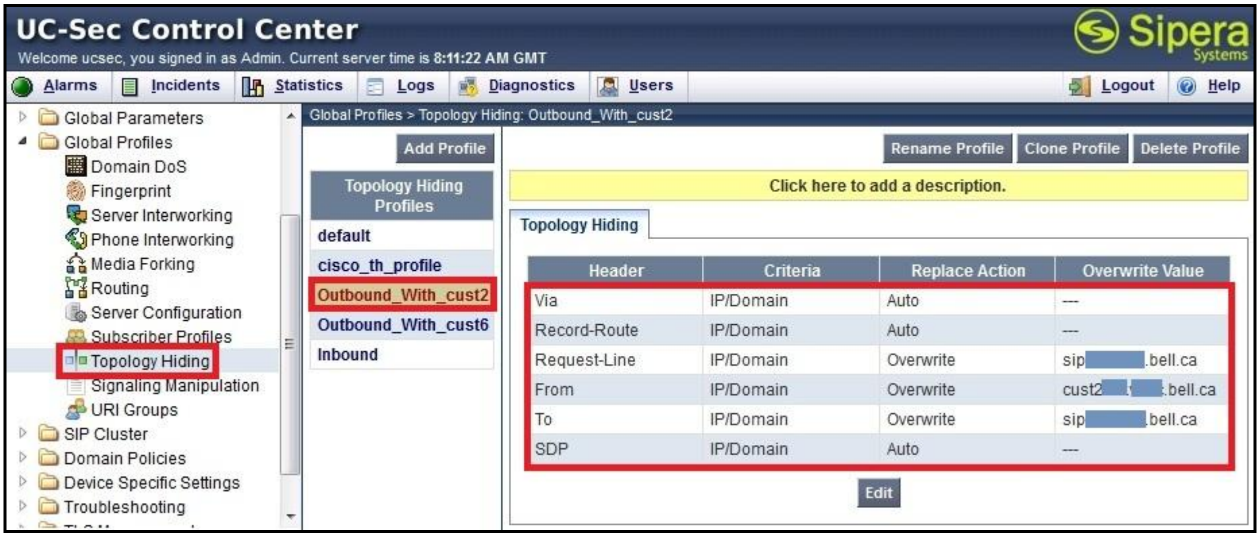
7.2.3.2 Topology Hiding Profile for Outgoing Calls

Two Topology Hiding profiles **Outbound_With_cust2** and **Outbound_With_cust6** were added for outgoing calls to Bell Canada.

As per described in **Section 7.2.1**, the compliance testing was conducted with two service provider public SIP domains **cust2xxxx.xxxx.bell.ca** and **cust6xxxx.xxxx.bell.ca**. The Topology Hiding profile **Outbound_With_cust2** masks the "From" header with **cust2xxxx.xxxx.bell.ca** and the "Request-URI" and "To" headers with **sipxxxxxxxx.bell.ca** before sending outgoing calls toward Bell Canada networks. Similarly, the Topology Hiding profile **Outbound_With_cust6** masks the "From" header with **cust6xxxx.xxxx.bell.ca** and the "Request-URI" and "To" headers with **sipxxxxxxxx.bell.ca**.

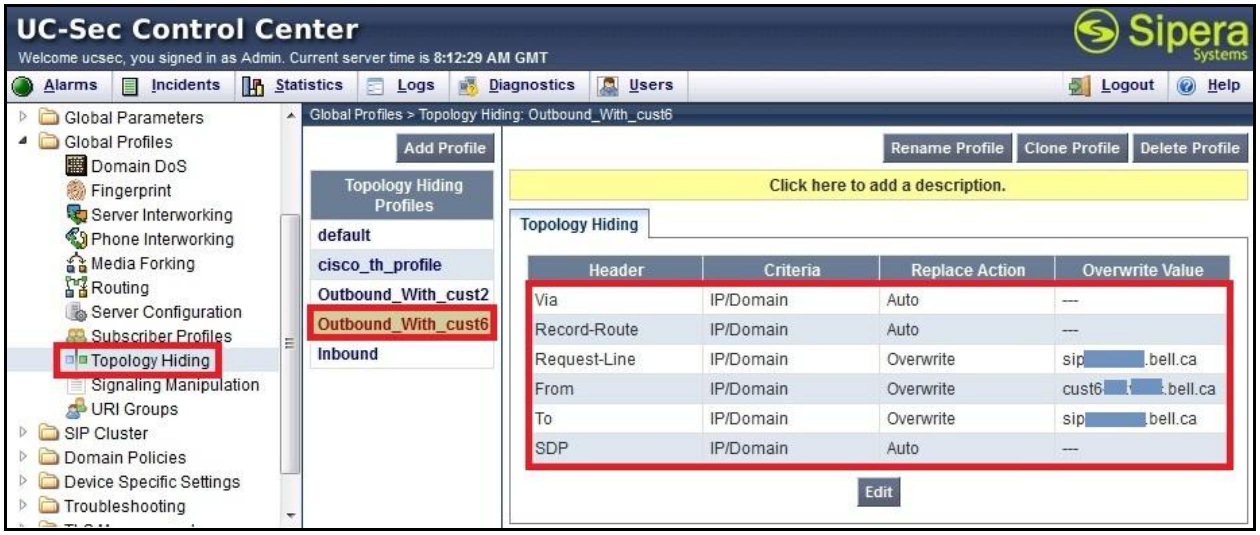
The Topology Hiding profiles also normalize the original "Record-Route" and "Via" headers from Communication Manager and replace the internal IP addresses in the SDP by external IP address of the Avaya SBCE.

Following screenshots show the Topology Hiding profiles **Outbound_With_cust2** and **Outbound_With_cust6** created on the primary Avaya SBCE.



Global Profiles > Topology Hiding: Outbound_With_cust2

Header	Criteria	Replace Action	Overwrite Value
Via	IP/Domain	Auto	---
Record-Route	IP/Domain	Auto	---
Request-Line	IP/Domain	Overwrite	sip[redacted].bell.ca
From	IP/Domain	Overwrite	cust2[redacted] [redacted].bell.ca
To	IP/Domain	Overwrite	sip[redacted].bell.ca
SDP	IP/Domain	Auto	---



Global Profiles > Topology Hiding: Outbound_With_cust6

Header	Criteria	Replace Action	Overwrite Value
Via	IP/Domain	Auto	---
Record-Route	IP/Domain	Auto	---
Request-Line	IP/Domain	Overwrite	sip[redacted].bell.ca
From	IP/Domain	Overwrite	cust6[redacted] [redacted].bell.ca
To	IP/Domain	Overwrite	sip[redacted].bell.ca
SDP	IP/Domain	Auto	---

Use the procedure to replicate the same Topology Hiding profiles **Outbound_With_cust2** and **Outbound_With_cust6** to the secondary Avaya SBCE (not shown).

Notes:

- The **Criteria** should be **IP/Domain** to give the Avaya SBCE the capability to mask both domain name and IP address present in the URI-Host.
- The masking applied to the "From" header also applies to the "Referred-By" and "P-Asserted-Identity" headers.
- The masking applied to the "To" header also applies to the "Refer-To header".

7.2.4 Server Interworking

Server Interworking profile features are configured based on the specification of Call Server and Trunk Server.

To create a Server Interworking profile, select **UC-Sec Control Center → Global Profiles → Server Interworking**. Click on **Add Profile** (not shown).

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

Note: Each Server Interworking profile will need to be created for both the primary Avaya SBCE and secondary Avaya SBCE using separate web interfaces.

7.2.4.1 Server Interworking profile for Avaya Aura® Communication Manager

Server Interworking profile **CM** was defined to match the specification of Communication Manager. The **General**, **Timers** and **Advanced** tabs were configured with the following parameters while the other tabs **URI Manipulation** and **Header Manipulation** were kept as default.

General settings:

- **Hold Support** = **None**. The Avaya SBCE will not handle Hold/ Resume signaling, it keeps the Hold/ Resume signaling unchanged to send to the destination server.
- **18X Handling** = **None**. The Avaya SBCE will not handle 18X, it keeps the incoming 18X responds unchanged to send to the destination server.
- **Refer Handling** = **unchecked**. The Avaya SBCE will not handle Refer, it keeps REFER unchanged to send to the destination server.
- **T.38 Support** = **unchecked**. Bell Canada did not support the T.38 codec for fax over IP in the compliance testing.
- **Privacy Enabled** = **unchecked**. The Avaya SBCE will not mask the “From” header with **anonymous** to the destination server. It depends on the far end to enable/ disable the “Privacy” on individual call basis.
- **DTMF Support** = **None**. The Avaya SBCE will not modify the DTMF transmission method. It keeps the DTMF unchanged to send to the destination server.

Timers settings:

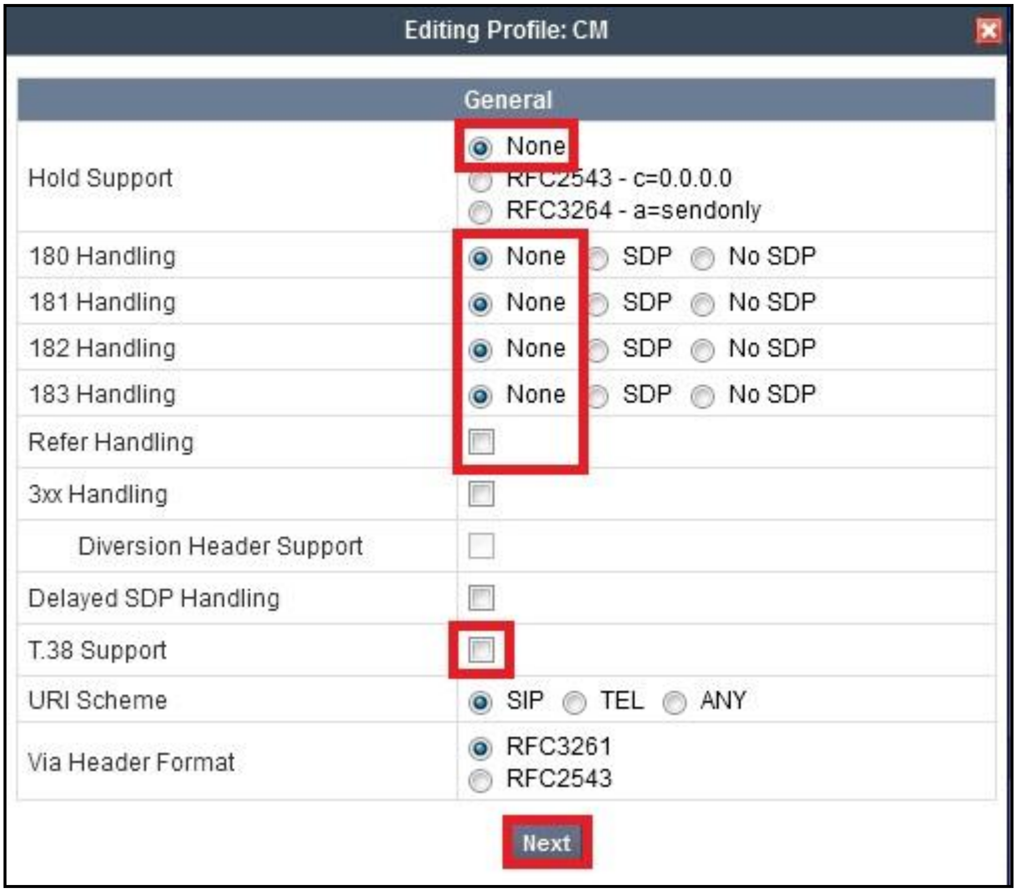
- **Init Timer = 1000 milliseconds**. The Avaya SBCE will re-transmit the INVITE if the initial INVITE has not received a response after 1 second.
- **Trans Expire** = **2 seconds**. The Avaya SBCE will try the **Next Hop Server** which was defined in the Routing profile (see **Section 7.2.2**) if the initial INVITE is not responded to after 2 seconds.

Advanced settings:

- **Record Routes** = **Both Sides**. The Avaya SBCE will send the “Record-Route” header to both Communication Manager and Bell Canada.
- **Topology-Hiding**: **Change Call-ID** = **checked**. The Avaya SBCE will mask the “Call-ID” header for the calls to the destination server.
- **Change Max-Forwards** = checked. The Avaya SBCE will reduce the counter of the “Max-Forwards” header by 1 for the calls to the destination server.

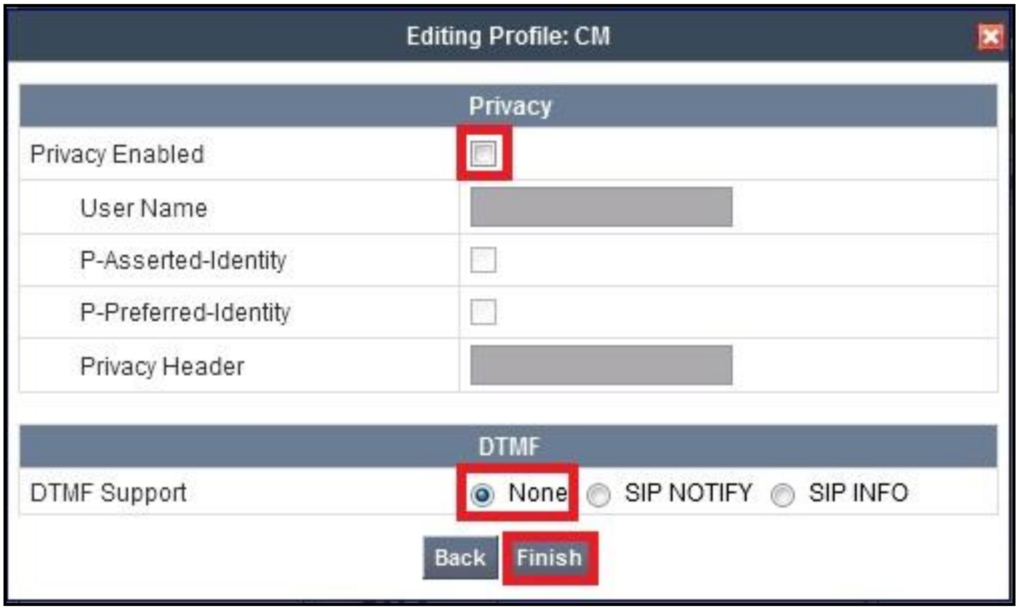
- **AVAYA Extensions** = **checked**. The Avaya SBCE will support interworking with Avaya Extensions.
- **Has Remote SBC** = **checked**. The Avaya SBCE will flexibly handle SDP from Communication Manager when Media Shuffling is active.

The screenshots below illustrate Server Interworking profile **CM** created on the primary Avaya SBCE for Communication Manager.



Editing Profile: CM

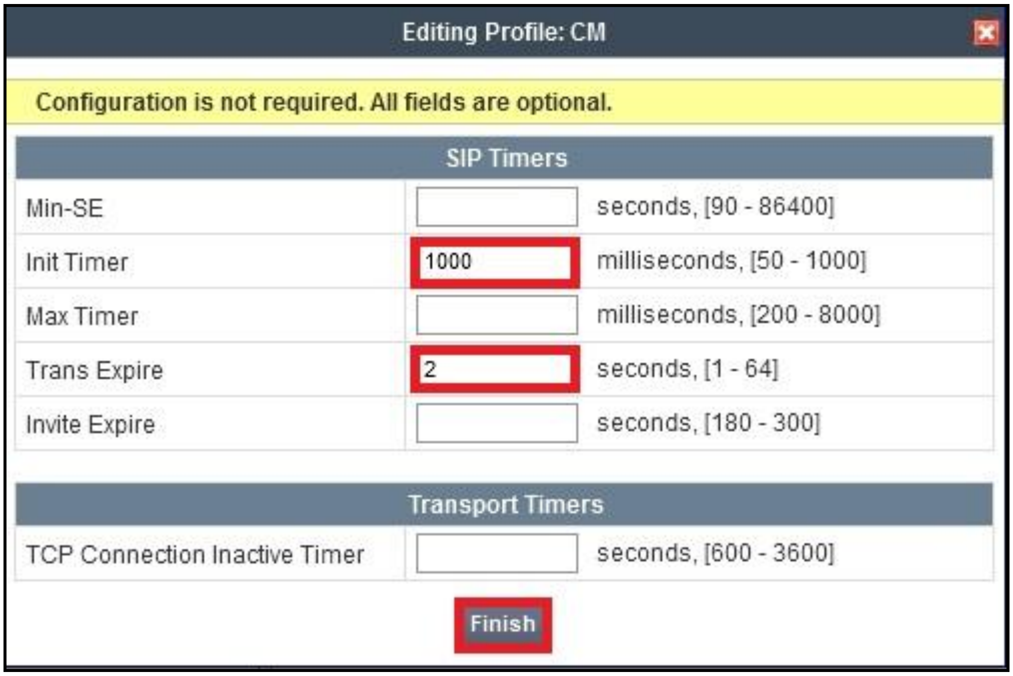
General	
Hold Support	● None ○ RFC2543 - c=0.0.0.0 ○ RFC3264 - a=sendonly
180 Handling	● None ○ SDP ○ No SDP
181 Handling	● None ○ SDP ○ No SDP
182 Handling	● None ○ SDP ○ No SDP
183 Handling	● None ○ SDP ○ No SDP
Refer Handling	□
3xx Handling	□
Diversion Header Support	□
Delayed SDP Handling	□
T.38 Support	□
URI Scheme	● SIP ○ TEL ○ ANY
Via Header Format	● RFC3261 ○ RFC2543



Editing Profile: CM

Privacy	
Privacy Enabled	□
User Name	
P-Asserted-Identity	□
P-Preferred-Identity	□
Privacy Header	

DTMF	
DTMF Support	● None ○ SIP NOTIFY ○ SIP INFO

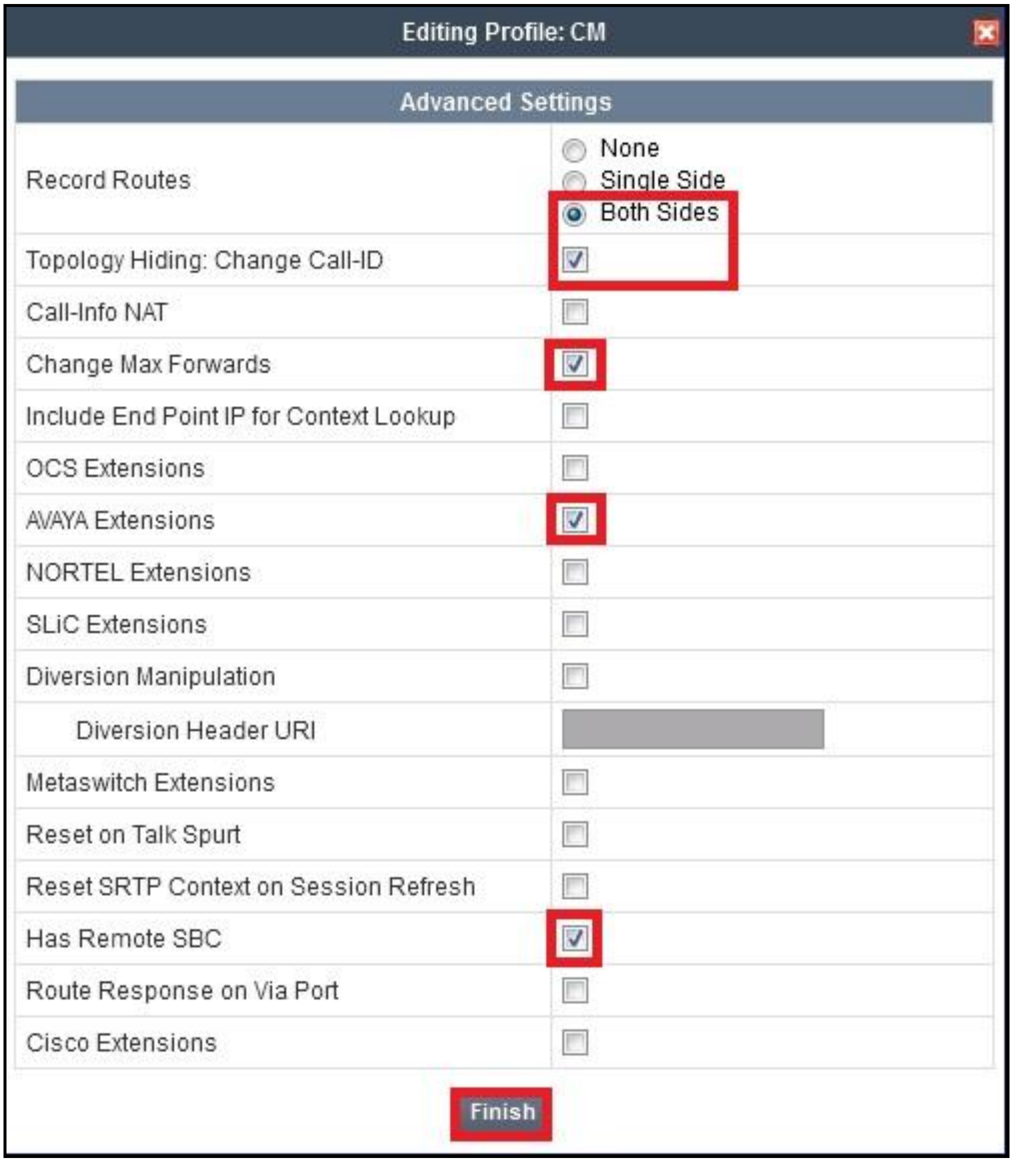


Editing Profile: CM

Configuration is not required. All fields are optional.

SIP Timers		
Min-SE		seconds, [90 - 86400]
Init Timer	1000	milliseconds, [50 - 1000]
Max Timer		milliseconds, [200 - 8000]
Trans Expire	2	seconds, [1 - 64]
Invite Expire		seconds, [180 - 300]

Transport Timers		
TCP Connection Inactive Timer		seconds, [600 - 3600]



Editing Profile: CM

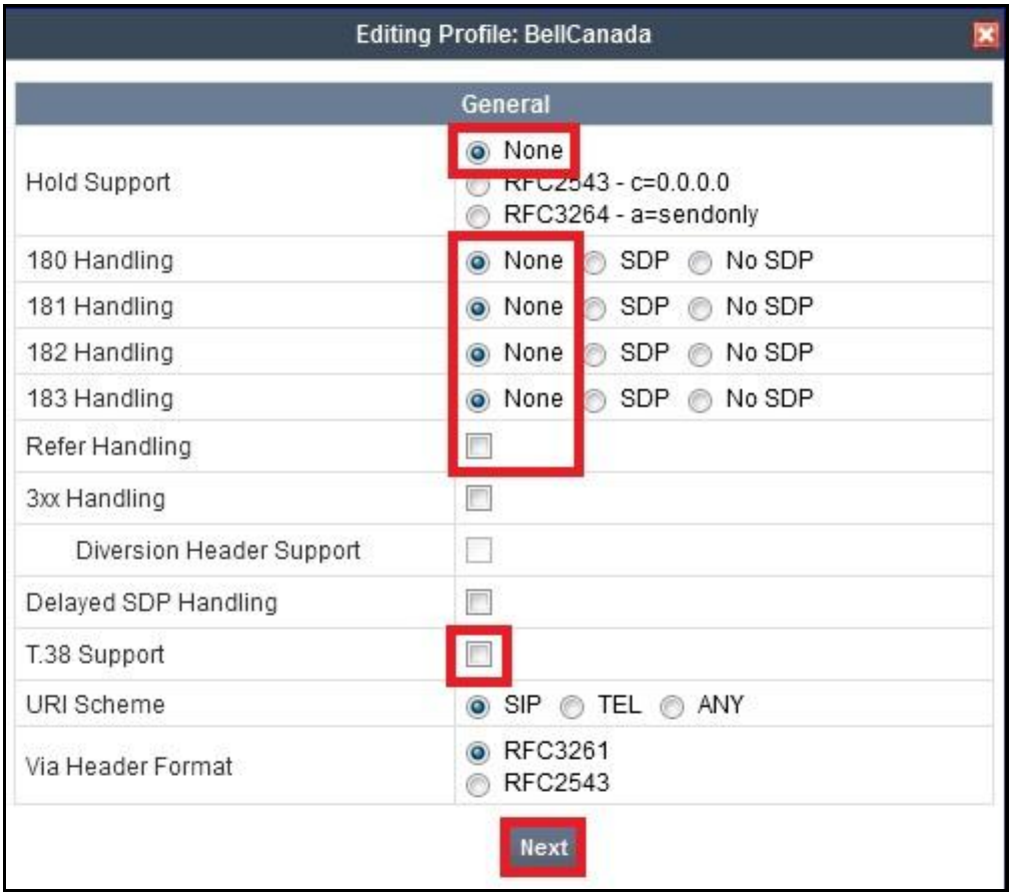
Advanced Settings	
Record Routes	○ None ○ Single Side ● Both Sides
Topology Hiding: Change Call-ID	☑
Call-Info NAT	□
Change Max Forwards	☑
Include End Point IP for Context Lookup	□
OCS Extensions	□
AVAYA Extensions	☑
NORTEL Extensions	□
SLiC Extensions	□
Diversion Manipulation	□
Diversion Header URI	
Metaswitch Extensions	□
Reset on Talk Spurt	□
Reset SRTP Context on Session Refresh	□
Has Remote SBC	☑
Route Response on Via Port	□
Cisco Extensions	□

Use the procedure to replicate the same Server Interworking profile **CM** to the secondary Avaya SBCE (not shown).

7.2.4.2 Server Interworking Profile for Bell Canada

Server Interworking profile **BellCanada** was similarly defined to match the specification of Bell Canada with the exception of the **Advanced** tab, it is set with **AVAYA Extension** unchecked because the terminals at Bell Canada networks may not be in the Avaya environment.

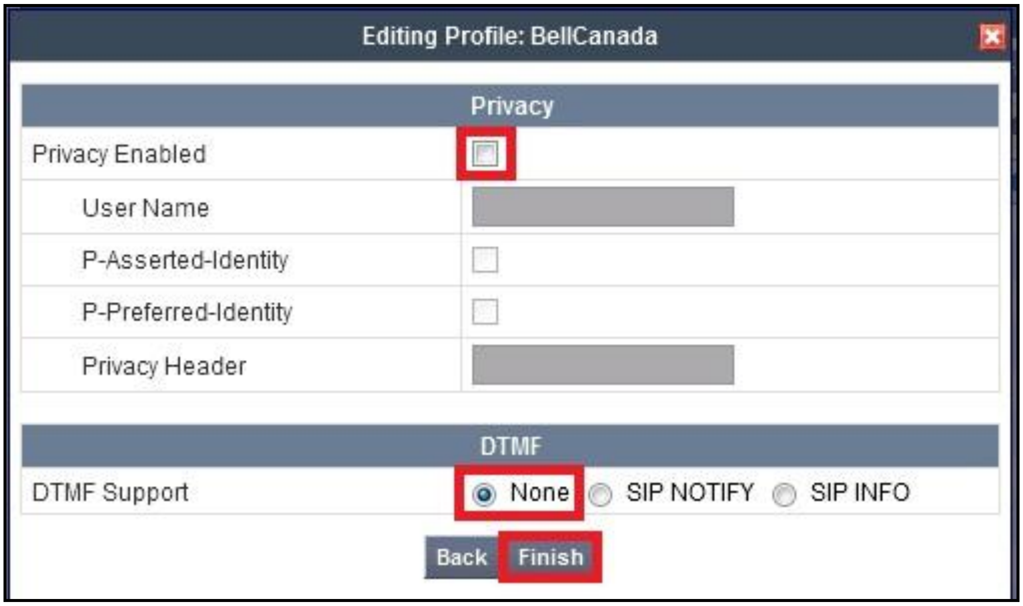
The screenshots below illustrate Server Interworking profile **Bell Canada** created on the primary Avaya SBCE for Bell Canada.



Editing Profile: BellCanada

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



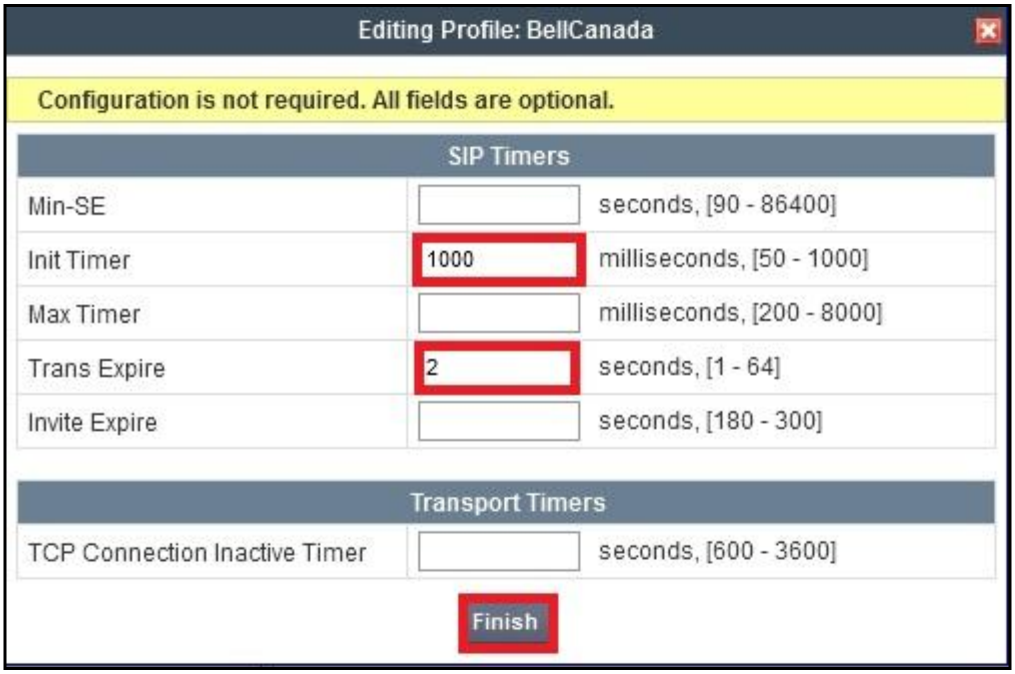
Editing Profile: BellCanada

Privacy

Privacy Enabled	□
User Name	
P-Asserted-Identity	□
P-Preferred-Identity	□
Privacy Header	

DTMF

DTMF Support	● None ○ SIP NOTIFY ○ SIP INFO

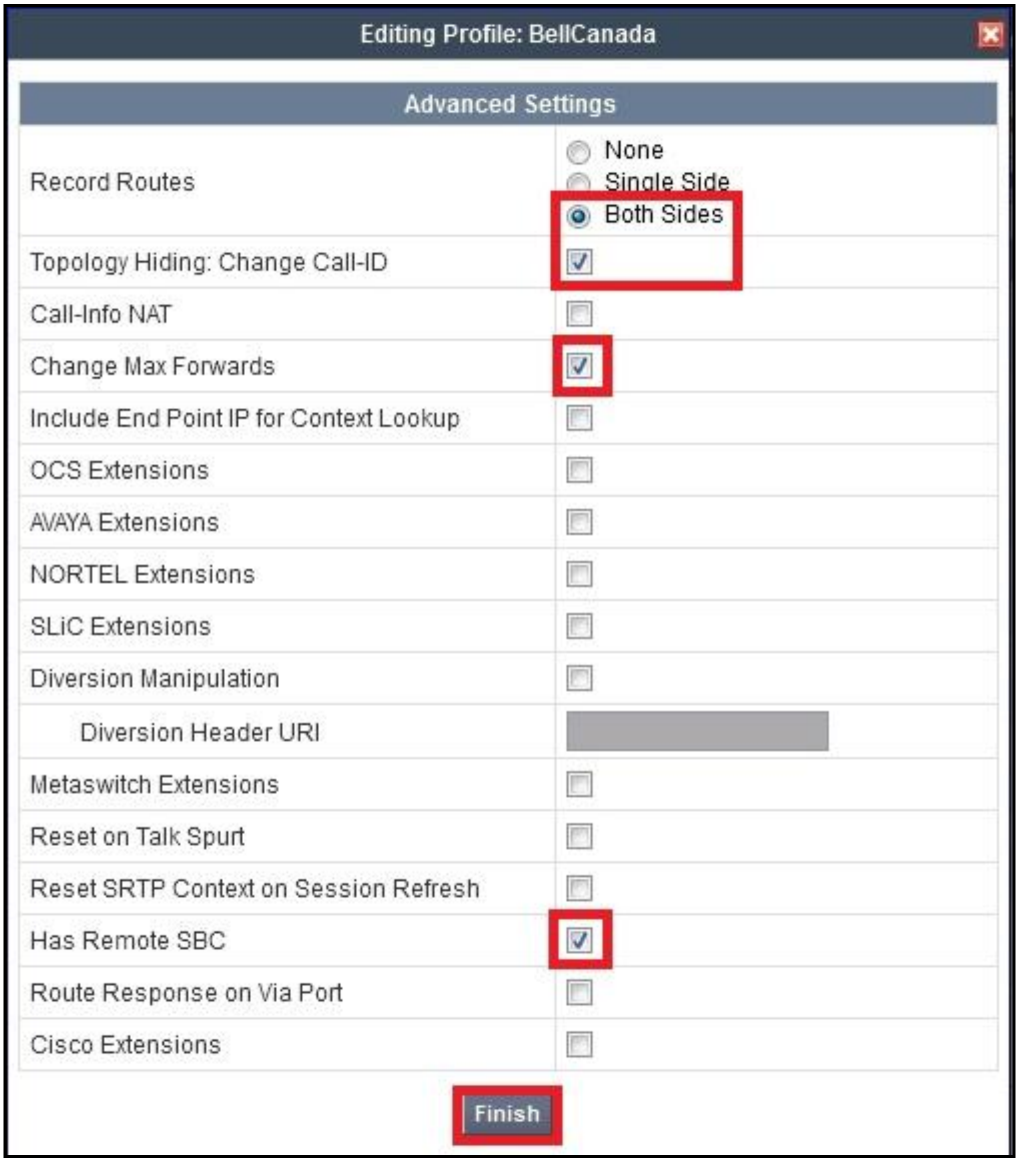


Editing Profile: BellCanada

Configuration is not required. All fields are optional.

SIP Timers		
Min-SE		seconds, [90 - 86400]
Init Timer	1000	milliseconds, [50 - 1000]
Max Timer		milliseconds, [200 - 8000]
Trans Expire	2	seconds, [1 - 64]
Invite Expire		seconds, [180 - 300]

Transport Timers		
TCP Connection Inactive Timer		seconds, [600 - 3600]



Editing Profile: BellCanada

Advanced Settings

Record Routes	○ None ○ Single Side ● Both Sides
Topology Hiding: Change Call-ID	☑
Call-Info NAT	□
Change Max Forwards	☑
Include End Point IP for Context Lookup	□
OCS Extensions	□
AVAYA Extensions	□
NORTEL Extensions	□
SLiC Extensions	□
Diversion Manipulation	□
Diversion Header URI	
Metaswitch Extensions	□
Reset on Talk Spurt	□
Reset SRTP Context on Session Refresh	□
Has Remote SBC	☑
Route Response on Via Port	□
Cisco Extensions	□

Use the procedure to replicate the same Server Interworking profile **Bell Canada** to the secondary Avaya SBCE (not shown).

7.2.5 Signaling Manipulation

The 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 a 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 manipulations done by the Avaya SBCE. Using this language, a script can be written and tied to a given Server Configuration (see **Section 7.2.6**) through the web interface. The 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 scripts but will show an example of a script created during compliance testing to aid in Topology Hiding.

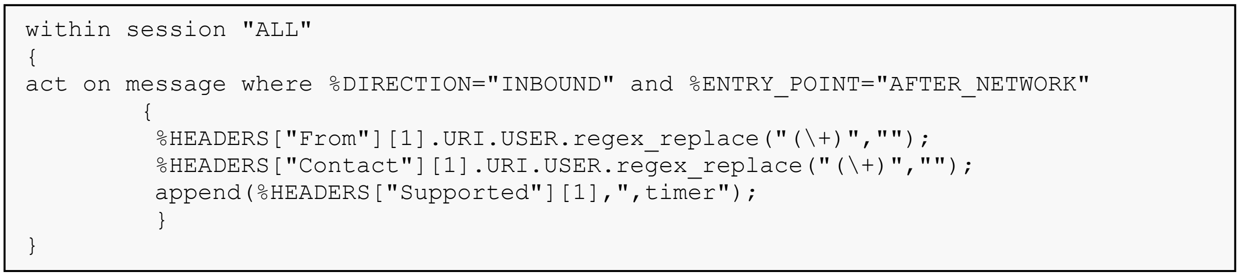
To create a Signaling Manipulation script, select **UC-Sec Control Center → Global Profiles → Signaling Manipulation**. Click on **Add Script** (not shown).

In the compliance testing, two SigMa scripts **Inbound** and **Outbound** were created on each Avaya SBCE.

Note: Each Signaling Manipulation script will need to be created for both the primary Avaya SBCE and secondary Avaya SBCE using separate web interfaces.

7.2.5.1 Signaling Manipulation Rules for Incoming Calls

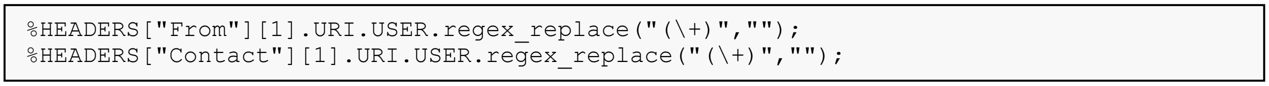
The following screenshot shows the SigMa script **Inbound** created on the primary Avaya SBCE to normalize incoming calls received from both primary and secondary Bell Canada CO located within Bell Canada networks, it applies to the Server Configuration for Bell Canada (see **Section 7.2.6**).



```
within session "ALL"
{
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("(\+)","");
         append(%HEADERS["Supported"][1],",timer");
         }
}
```

In the SigMa script 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 incoming SIP messages from Bell Canada and the manipulation will be done before routing. The manipulation will be according to the rules which were contained in this statement.

For incoming calls, it was observed that Bell Canada sends the "+" sign and 11 digits of the Calling Party Number in the "From" and "Contact" headers. The "+" sign should be removed to interwork with the dialing plan configuration on Communication Manager (see **Section 5.9**). This manipulation also supports the off-net call forward and EC500 features to work properly as per the description in **Section 2.2**, observation 1. The rules to remove the "+" sign are shown in the screenshot below.



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

Bell Canada does not implement Session Timer refresh as per RFC 4028, it does not send the "Supported: Timer" header for incoming calls. This prevents Communication Manager from sending the subsequent INVITE to refresh the Session Timer as described in **Section 5.7**. To support the Session Timer, a rule to add the "Support: Timer" header was created for incoming calls. It is shown in the screenshot below. With this rule, Communication Manager refreshes the Session Timer as expected.

```
append(%HEADERS["Supported"][1],",timer");
```

Note: Even Bell Canada does not implement Session Timer refresh as per RFC 4028, but it still sends subsequent INVITEs every 600 seconds. This implementation is done by Bell Canada CO without the knowledge of Communication Manager with regard to the Session Timer refresh.

Use the procedure to replicate the same SigMa script **Inbound** to the secondary Avaya SBCE (not shown).

7.2.5.2 Signaling Manipulation Rules for Outgoing Calls

The following screenshot shows the SigMa script **Outbound** created on the primary Avaya SBCE to normalize outgoing calls received from both primary and secondary Session Manager, it applies to the Server Configuration for Session Manager (see **Section 7.2.6**).

```
within session "ALL"
{
    act on message where %DIRECTION="INBOUND" and %ENTRY_POINT="AFTER_NETWORK"
{
        %HEADERS["Request_Line"][1].URI.HOST.regex_replace("-","_");
        %HEADERS["Request_Line"][1].URI.HOST.regex_replace(".avayalab.com","");
        %tgrp=%HEADERS["Request_Line"][1].URI.HOST;
        append(%HEADERS["Contact"][1].URI.USER,";tgrp=");
        append(%HEADERS["Contact"][1].URI.USER,%tgrp);
        append(%HEADERS["Contact"][1].URI.USER,";trunk-
context=sipxxxxxxxx.bell.ca");
        if(%HEADERS["Diversion"][1].URI.USER.regex_match("416XXX13"))then
               {
               %HEADERS["To"][1].URI.HOST="outgoingcust2.avayalab.com";
               %HEADERS["From"][1].URI.HOST="outgoingcust2.avayalab.com";
               }
         else
               {
               if (%HEADERS["P-Asserted-
Identity"][1].URI.USER.regex_match("416XXX13")) then
                    {
                    %HEADERS["To"][1].URI.HOST="outgoingcust2.avayalab.com";
                    %HEADERS["From"][1].URI.HOST="outgoingcust2.avayalab.com";
                    }
               }
        if(%HEADERS["Diversion"][1].URI.USER.regex_match("416XXX18"))then
               {
               %HEADERS["To"][1].URI.HOST="outgoingcust6.avayalab.com";
               %HEADERS["From"][1].URI.HOST="outgoingcust6.avayalab.com";
               }
         else
               {
               if (%HEADERS["P-Asserted-
Identity"][1].URI.USER.regex_match("416XXX18")) then
                    {
                    %HEADERS["To"][1].URI.HOST="outgoingcust6.avayalab.com";
                    %HEADERS["From"][1].URI.HOST="outgoingcust6.avayalab.com";
                    }
               }
    }
}
```

In the SigMa script 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 incoming SIP messages to the Avaya SBCE from Session Manager and the manipulation will be done before routing. The manipulation will be according to the rules which were contained in this statement.

As being described in **Section 5.6**, Bell Canada requires outgoing calls with a specific "tgrp" value in the "Contact" header to assist the Least Cost Routing feature at Bell Canada CO. To support this, the signaling group configuration on Communication Manager has the "tgrp" embedded in the SIP domains. The following SigMa rules which are shown in the screenshot below were created to extract the "tgrp" value by replacing the "-" (dash) character with a "_" (underscore) character, removing the suffix **.avaya.com** out of the SIP domain then storing the "tgrp" for constructing the "Contact" header purpose.

```
%HEADERS["Request_Line"][1].URI.HOST.regex_replace("-","_");
%HEADERS["Request_Line"][1].URI.HOST.regex_replace(".avayalab.com","");
%tgrp=%HEADERS["Request_Line"][1].URI.HOST;
```

Displayed above is the recovered “tgrp” value. The SigMa script constructs the “Contact” header to follow the format required by Bell Canada. The rules for the “Contact” headers are shown in the following screenshot.

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

The compliance testing was conducted with two DID ranges **416XXX13XX** and **416XXX18XX** which associate to two service provider public SIP domains **cust2xxxx.xxxx.bell.ca** and **cust6xxxx.xxxx.bell.ca**.

With the DID number and service provider public SIP domain constrained as described in **Section 7.2.1**, the SigMa script will examine the source number in the “Diversion” and “P-Asserted-Identity” headers to determine which DID range that outgoing calls are originated from.

If the DID number is detected to be in the **416XXX13XX** range, the following rules will change the SIP domains in the “From” and “To” headers to **outgoingcust2.avayalab.com**. This manipulation assists the URI Group (see **Section 7.2.1**) and Topology Hiding (see **Section 7.2.3**) to match and mask outgoing calls with the service provider public SIP domain **cust2xxxx.xxxx.bell.ca**.

```
if(%HEADERS["Diversion"][1].URI.USER.regex_match("416XXX13"))then
 {
 %HEADERS["To"][1].URI.HOST="outgoingcust2.avayalab.com";
 %HEADERS["From"][1].URI.HOST="outgoingcust2.avayalab.com";
 }
 else
  {
  if (%HEADERS["P-Asserted-Identity"][1].URI.USER.regex_match("416XXX13")) then
   {
   %HEADERS["To"][1].URI.HOST="outgoingcust2.avayalab.com";
   %HEADERS["From"][1].URI.HOST="outgoingcust2.avayalab.com";
   }
  }
```

Similarly, if the DID number is detected to be in the **416XXX18XX** range, the following rules will change the SIP domains in the “From” and “To” headers to **outgoingcust6.avayalab.com**. This manipulation assists the URI Group (see **Section 7.2.1**) and Topology Hiding (see **Section 7.2.3**) to match and mask outgoing calls with the service provider public SIP domain **cust6xxxx.xxxx.bell.ca**.

```
if(%HEADERS["Diversion"][1].URI.USER.regex_match("416XXX18"))then
 {
 %HEADERS["To"][1].URI.HOST="outgoingcust6.avayalab.com";
 %HEADERS["From"][1].URI.HOST="outgoingcust6.avayalab.com";
 }
 else
  {
  if (%HEADERS["P-Asserted-Identity"][1].URI.USER.regex_match("416XXX18")) then
   {
   %HEADERS["To"][1].URI.HOST="outgoingcust6.avayalab.com";
   %HEADERS["From"][1].URI.HOST="outgoingcust6.avayalab.com";
   }
  }
```

Use the procedure to replicate the same SigMa script **Outbound** to the secondary Avaya SBCE (not shown).

7.2.6 Server Configuration

Server Configuration screen contains four tabs **General**, **Authentication**, **Heartbeat**, and **Advanced**. Together, these tabs 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 a Server Configuration entry, select **UC-Sec Control Center → Global Profiles → Server Configuration**. Click on **Add Profile** (not shown).

In the compliance testing, on each Avaya SBCE there were two Server Configurations created for the primary and secondary Session Manager. Another two Server Configurations were also created for the primary and secondary Bell Canada CO.

Note: Each Server Configuration profile will need to be created for both the primary Avaya SBCE and secondary Avaya SBCE using separate web interfaces.

7.2.6.1 Server Configuration for the Primary and Secondary Avaya Aura® Session Manager

Server Configuration profiles **SM601A** and **SM601B** were defined to match the configuration of the primary and secondary Session Manager (see **Section 6**). The **General** and **Advanced** tabs were configured with the following parameters while the other tabs **Authentication** and **Heartbeat** were kept as default.

General settings:

- **Server Type**: select **Call Server**. Both Server Configurations are configured to route the traffic toward Session Manager which is the Call Server.
- **IP Address/ Supported FQDNs**: Enter the IP address of the primary Session Manager **10.33.10.20** or the IP address of the secondary Session Manager **10.33.10.28**.
- **Supported Transports**: Enable **UDP**.
- **UDP Port**: Enter 5060.

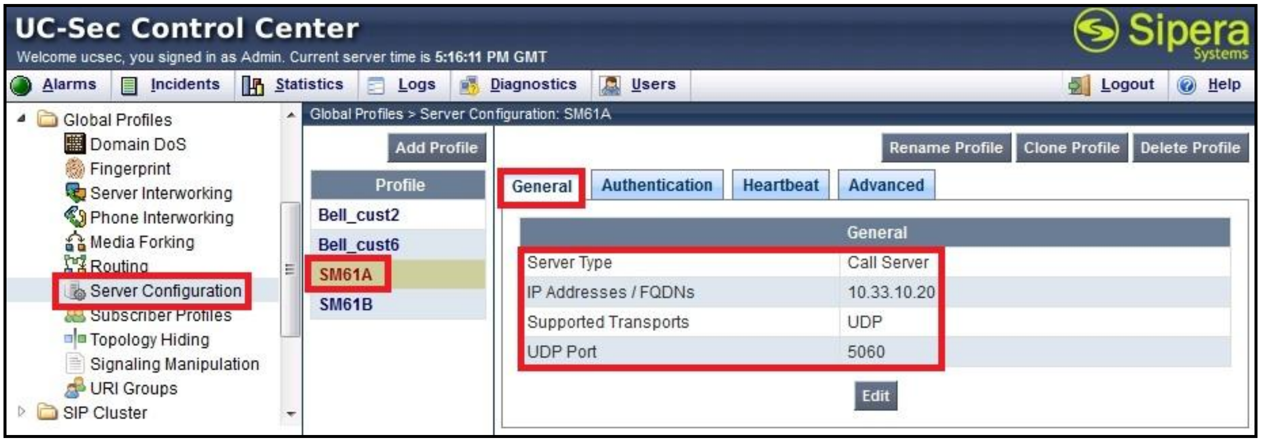
Note: The transport protocol is configured to match the SIP Entity Links defined for the primary and secondary Avaya SBCE in **Section 6.5**.

Advanced settings:

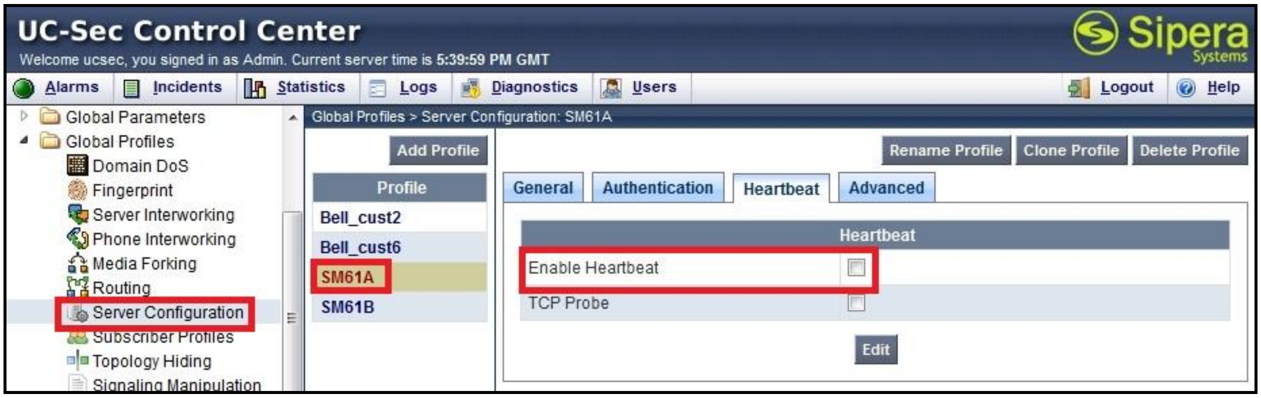
- **Interworking Profile**: select the Server Interworking **CM** which was created in **Section 7.2.4.1**.
- **Signaling Manipulation Script**: select the SigMa script **Outbound** which was created in **Section 7.2.5.2**.

Note: The Heartbeat settings were kept disabled as default to allow the Avaya SBCE to proxy the incoming OPTIONS from Bell Canada to Session Manager.

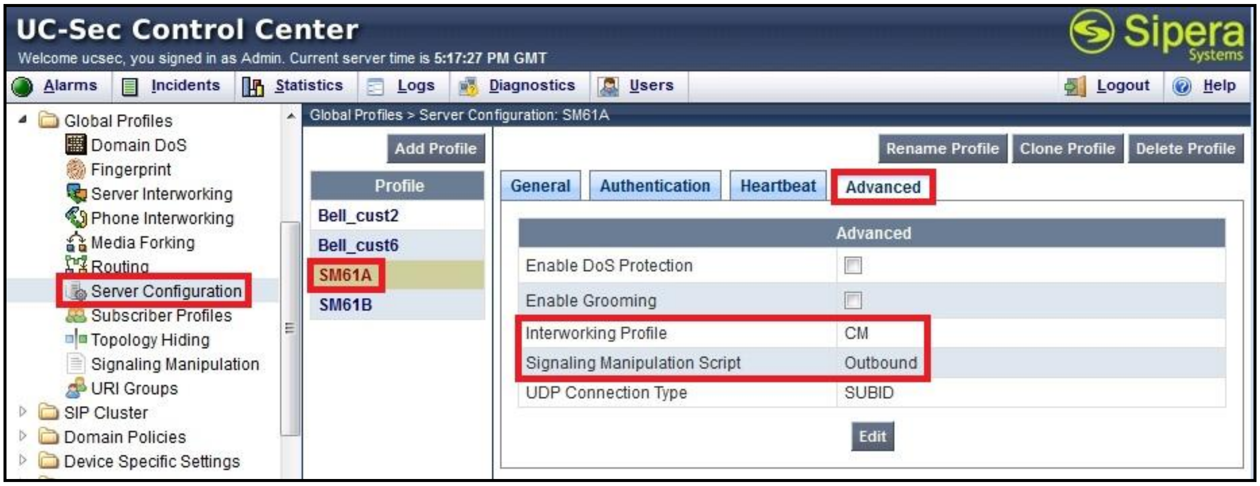
The screenshots below illustrate Server Configuration profile **SM601A** created on the primary Avaya SBCE for the primary Session Manager.



General	
Server Type	Call Server
IP Addresses / FQDNs	10.33.10.20
Supported Transports	UDP
UDP Port	5060

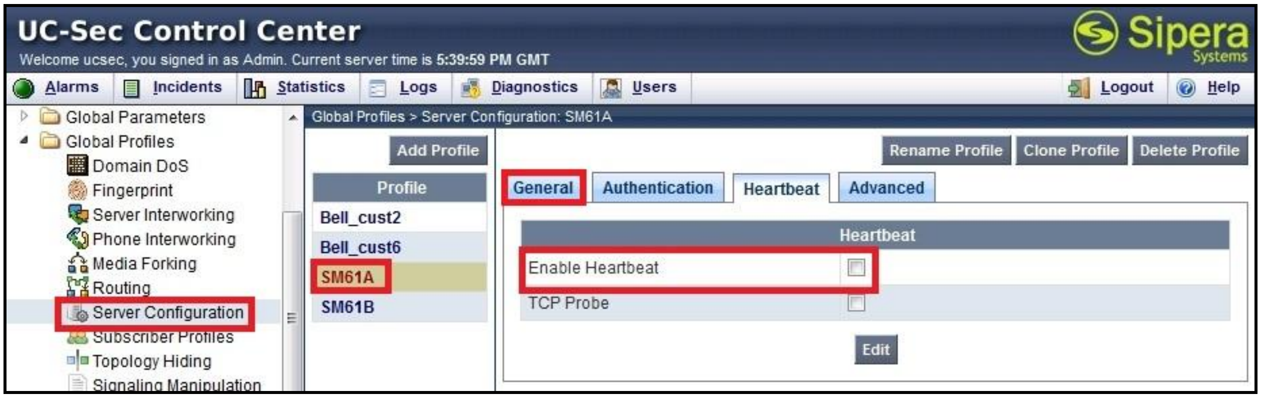


Heartbeat	
Enable Heartbeat	☐
TCP Probe	☐



Advanced	
Enable DoS Protection	☐
Enable Grooming	☐
Interworking Profile	CM
Signaling Manipulation Script	Outbound
UDP Connection Type	SUBID

The Server Configuration profile **SM601B** was similarly configured with the exception of the IP address is set to the secondary Session Manager. The screenshot below shows the **General** tab of the Server Configuration profile **SM601B** was created for the secondary Session Manager on the primary Avaya SBCE. The **Heartbeat** and **Advanced** tabs are kept as same as the **SM601A**.



Heartbeat	
Enable Heartbeat	☐
TCP Probe	☐

Use the procedure to replicate the same Server Configuration profile **SM601A** and **SM601B** to the secondary Avaya SBCE.

7.2.6.2 Server Configuration for the Primary and Secondary Bell Canada CO

Server Configuration profiles **Bell_cust2** and **Bell_cust6** were defined to match the configuration of the primary and secondary Bell Canada CO. The **General** and **Advanced** tabs were configured with the following parameters while the other tabs **Authentication** and **Heartbeat** were kept as default.

General settings:

- **Server Type**: select **Trunk Server**. Both Server Configurations are configured to route the traffic toward Bell Canada CO (s) which are the Trunk Servers.
- **IP Address/ Supported FQDNs**: Enter the IP address of the primary Bell Canada CO **220.20.237.201** or the IP address of the secondary Bell Canada CO **220.20.237.205**.
- **Supported Transports**: Enable **UDP**.

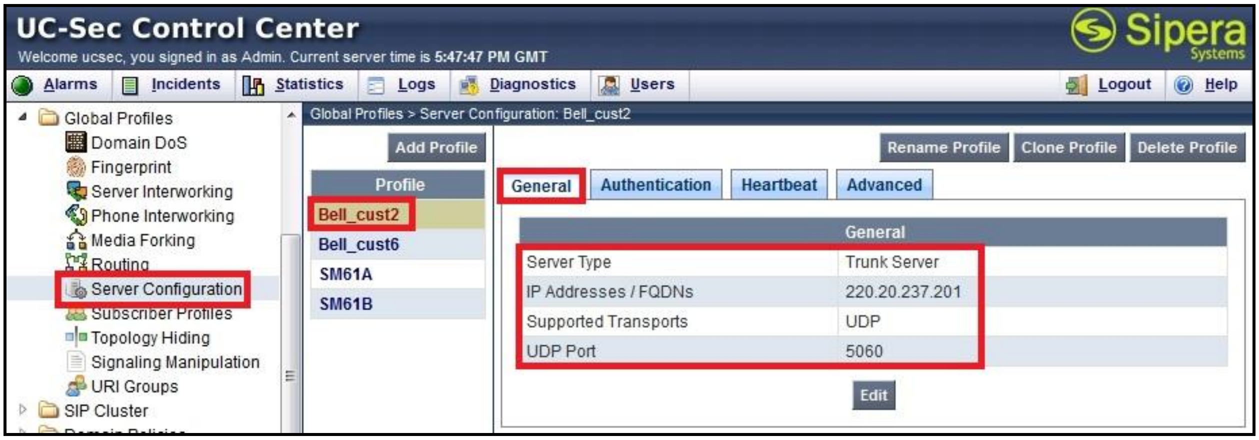
- **UDP Port**: Enter **5060**.

Advanced settings:

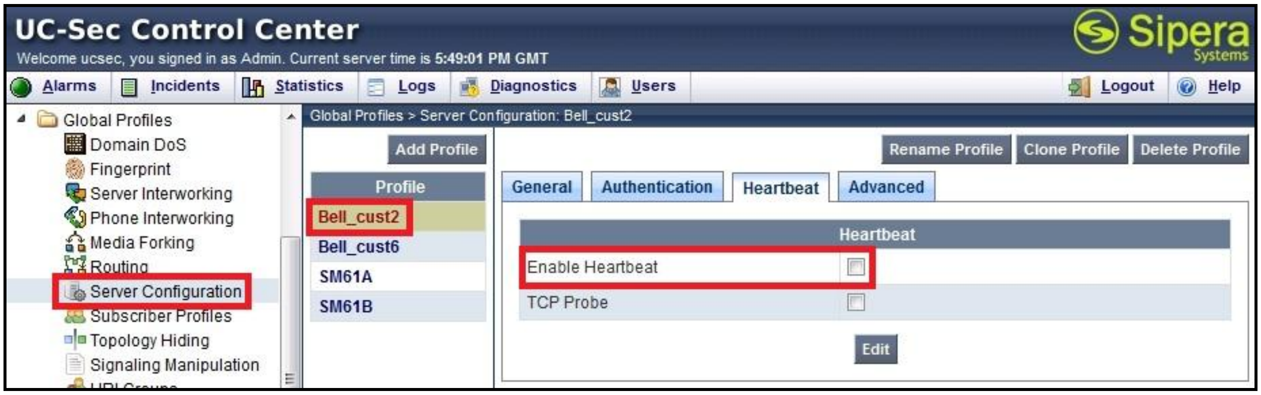
- **Interworking Profile**: select the Server Interworking **BellCanada** which was created in **Section 7.2.4.2**.
- **Signaling Manipulation Script**: select the SigMa script **Inbound** which was created in **Section 7.2.5.1**.

Note: The Heartbeat settings were kept disabled as default to allow the Avaya SBCE to proxy the incoming OPTIONS from Session Manager to Bell Canada.

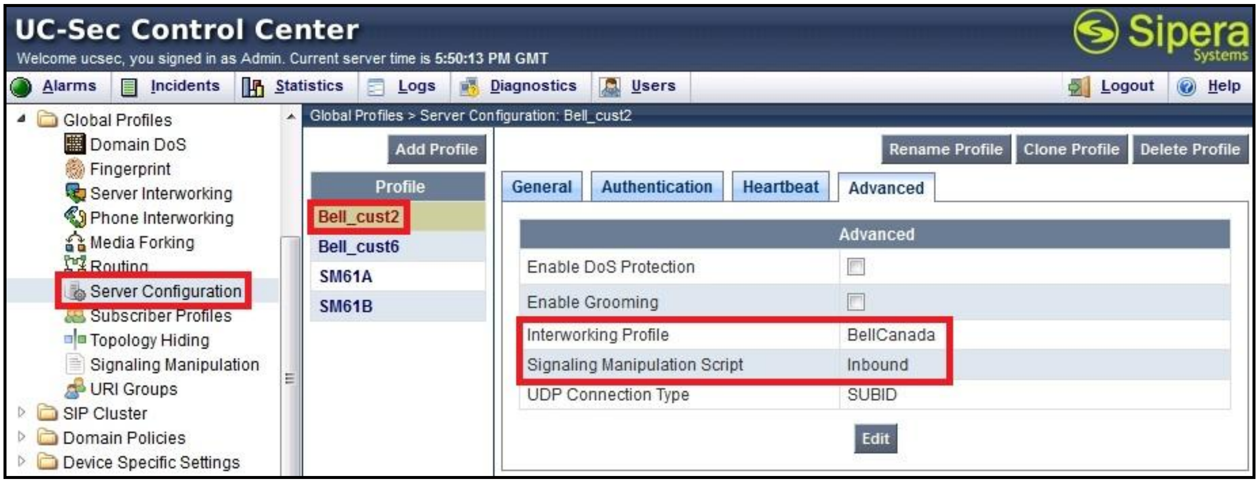
The screenshots below illustrate Server Configuration profile **Bell_cust2** created on the primary Avaya SBCE for the primary Bell Canada CO.



General	
Server Type	Trunk Server
IP Addresses / FQDNs	220.20.237.201
Supported Transports	UDP
UDP Port	5060

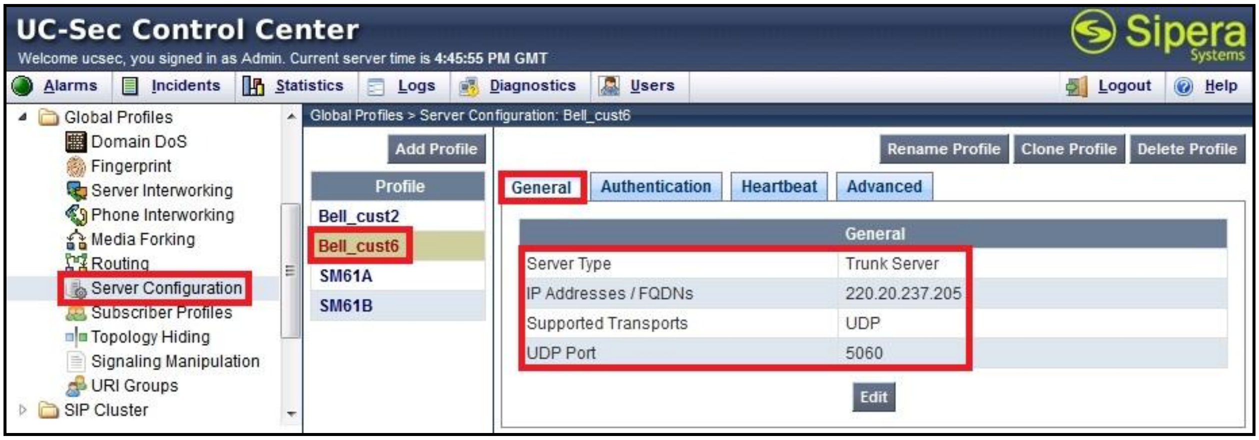


Heartbeat	
Enable Heartbeat	□
TCP Probe	□



Advanced	
Enable DoS Protection	☐
Enable Grooming	☐
Interworking Profile	BellCanada
Signaling Manipulation Script	Inbound
UDP Connection Type	SUBID

The Server Configuration profile **Bell_cust6** was similarly configured with the exception of the IP address is set to the secondary Bell Canada CO. The screenshot below shows the **General** tab of the Server Configuration profile **Bell_cust6** was created for the secondary Bell Canada CO on the primary Avaya SBCE. The **Heartbeat** and **Advanced** tabs are kept as same as the **Bell_cust2**.



General	
Server Type	Trunk Server
IP Addresses / FQDNs	220.20.237.205
Supported Transports	UDP
UDP Port	5060

Use the procedure to replicate the same Server Configuration profile **Bell_cust2** and **Bell_cust6** to the secondary Avaya SBCE.

7.3 Domain Policies

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

Note: Each individual policy will need to be created for both the primary Avaya SBCE and secondary Avaya SBCE using separate web interfaces.

7.3.1 Application Rules

Application Rules define which types of SIP-based Unified Communications (UC) applications the Avaya SBCE will protect: voice, video, and/or Instant Messaging (IM). In addition, it is possible to determine the maximum number of concurrent voice and video sessions the network will process in order to prevent resource exhaustion.

Create an Application Rule on the primary Avaya SBCE 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**.

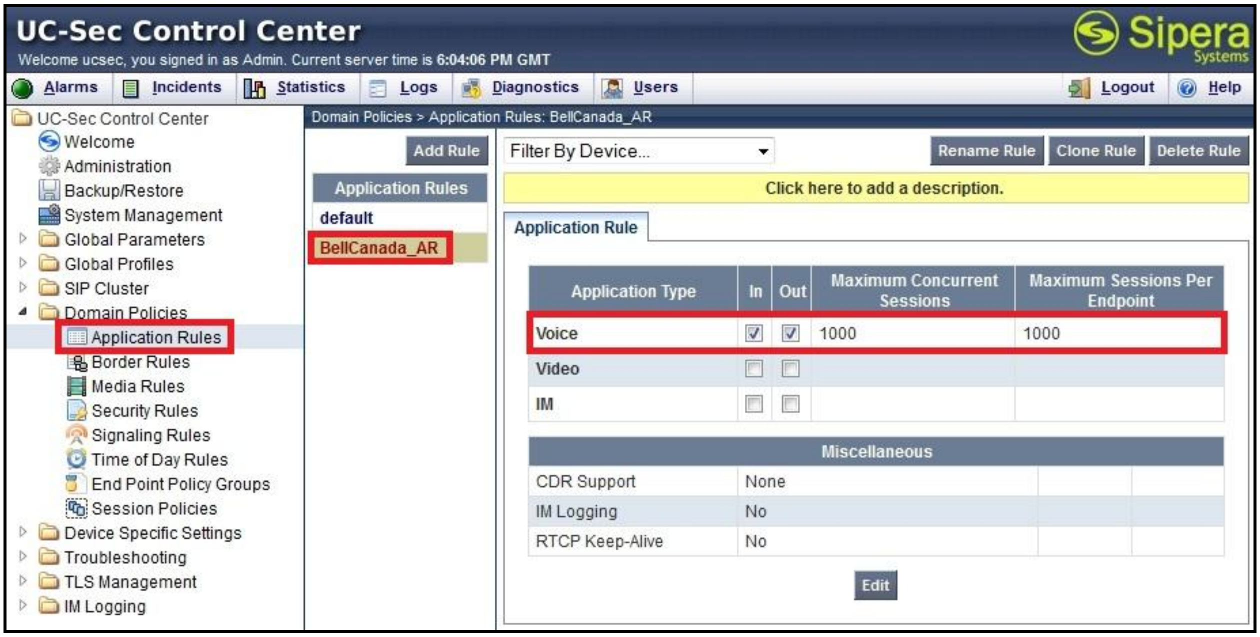
Note: The Application Rule will need to be created for both the primary Avaya SBCE and secondary Avaya SBCE using separate web interfaces.

To clone an Application Rule, navigate to **UC-Sec Control Center → Domain Policies → Application Rules**. With the default rule chosen, click on **Clone Rule** (not shown).

Enter a descriptive name .i.e. **BellCanada_AR** for the new rule and click **Finish** (not shown).

Modify the rule by clicking the **Edit** button. Set the **Maximum Concurrent Sessions** and **Maximum Session Per Endpoint** for the **Voice** application to a value high enough for the amount of traffic the network is able to process. The following screen shows the modified **Application Rule** with the **Maximum Concurrent Sessions** and **Maximum Session Per Endpoint** set to 1000. In the sample configuration, Communication Manager was programmed to control the concurrent sessions by setting the number of members in the trunk group (**Section 5.7**) to the allotted amount. Therefore, the values in the Application Rule **BellCanada_AR** were set high enough to be considered non-blocking.

The following screenshot shows the Application Rule **BellCanada_AR** created on the primary Avaya SBCE.



Welcome ucsec, you signed in as Admin. Current server time is 6:04:06 PM GMT

Application Type	In	Out	Maximum Concurrent Sessions	Maximum Sessions Per Endpoint
Voice	☑	☑	1000	1000
Video	□	□		
IM	□	□		

Miscellaneous	
CDR Support	None
IM Logging	No
RTCP Keep-Alive	No

Use the procedure to replicate the same Application Rule **BellCanada_AR** to the secondary Avaya SBCE (not shown).

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 packets matching these criteria will be handled by the Avaya SBCE
Create a Media Rule on the primary Avaya SBCE to set the **Media Anomaly Detection**, **Media Silencing** and **Quality of Service**. The sample configuration cloned and modified the default Media Rule to be used by both the enterprise and Bell Canada.

To clone a Media Rule, navigate to **UC-Sec Control Center → Domain Policies → Media Rules**. With **default-low-med** selected, click **Clone Rule** (not shown).

Enter a descriptive name .i.e. **BellCanada_MR** for the new rule and click **Finish** (not shown).

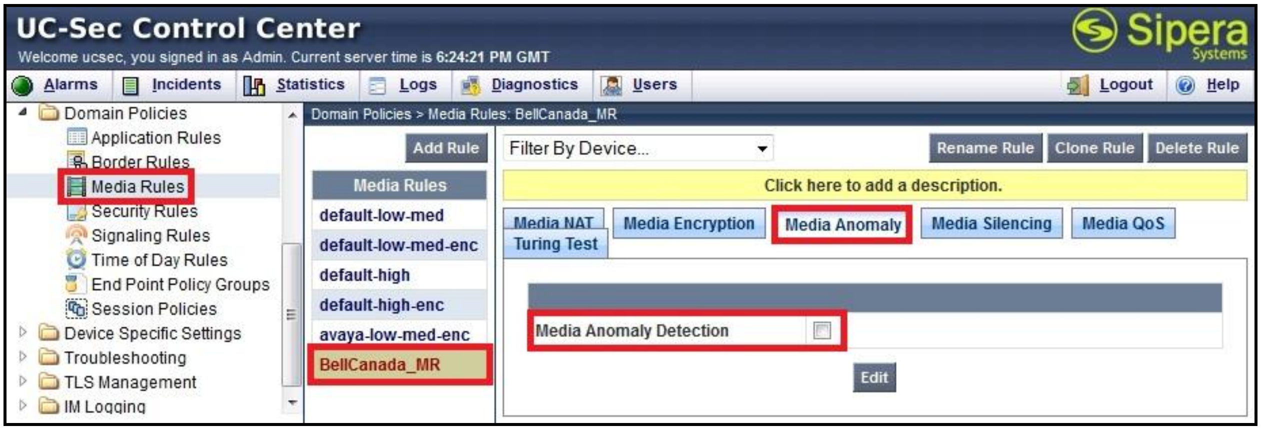
Note: The Media Rule will need to be created for both the primary Avaya SBCE and secondary Avaya SBCE using separate web interfaces.

When the RTP packets of a call are shuffled from Communication Manager to an IP terminal, the Avaya SBCE will interpret this as an anomaly and an alert will be created in the Incidents Log. Disabling **Media Anomaly Detection** prevents the **RTP Injection Attack** alerts from being created during an audio shuffle. To modify the rule, select the **Media Anomaly** tab and click **Edit**, uncheck **Media Anomaly Detection** and click **Finish** (not shown).

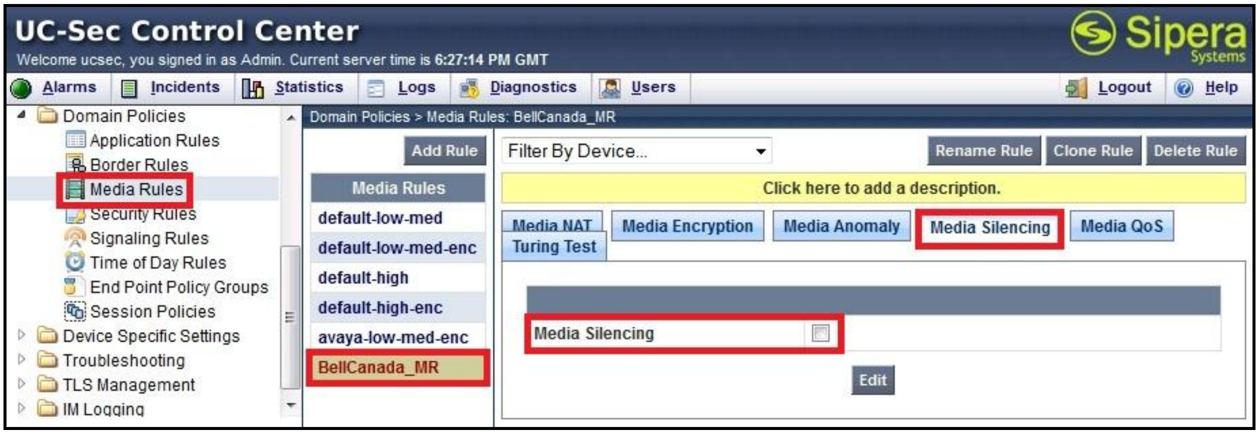
The Media Silencing feature detects the silence when the call is in progress. If the silence is detected and exceeds the allowed duration, the Avaya SBCE generates alert in the Incidents Log. In this sample configuration, the Media Silencing detection was disabled due to the RTP packets could be lost in part on public WAN. To modify the rule, select the **Media Silencing** tab and click **Edit**, uncheck **Media Silencing** and click **Finish** (not shown).

On **Media QoS** tab select the proper Quality of Service (QoS). The Avaya SBCE can be configured to mark the **Differentiated Services Code Point (DSCP)** in the IP packet header with specific values **EF** for **Audio**.

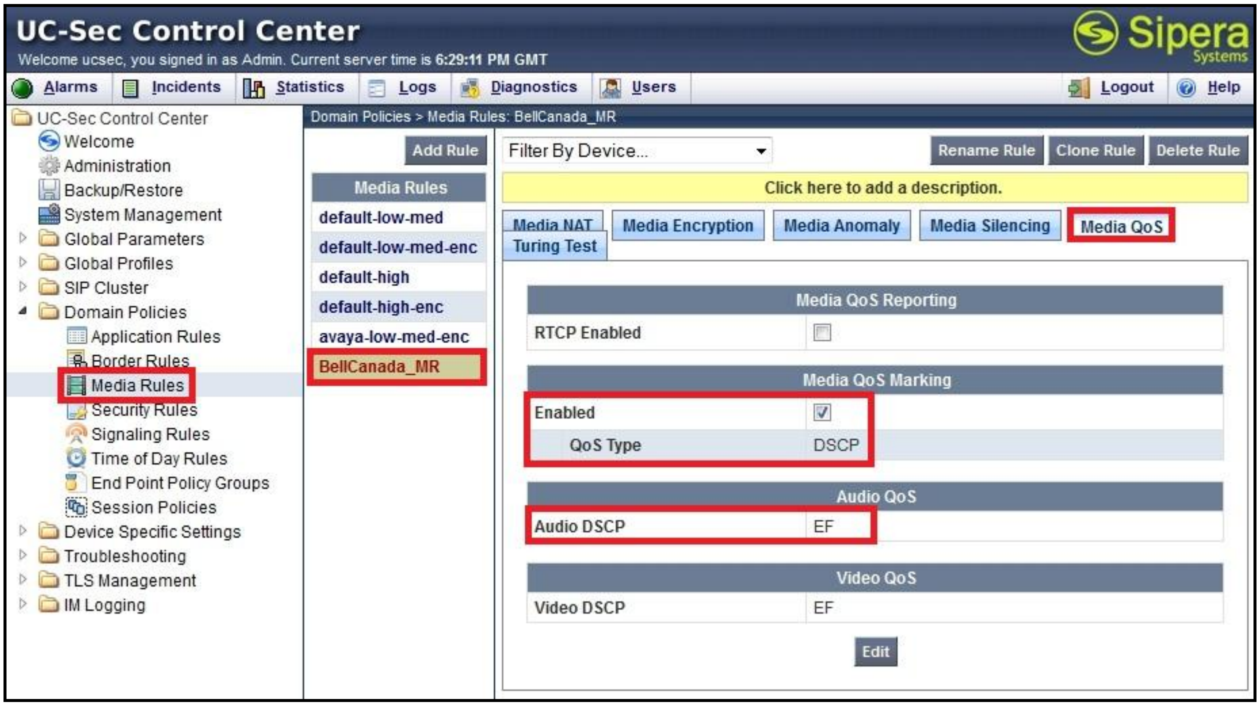
The following screenshots show the Media Rule **BellCanada_MR** created on the primary Avaya SBCE.



Media Anomaly Detection ☐



Media Silencing ☐



Media QoS Reporting	
RTCP Enabled	☐

Media QoS Marking	
Enabled	☑
QoS Type	DSCP

Audio QoS	
Audio DSCP	EF

Video QoS	
Video DSCP	EF

Use the procedure to replicate the same Media Rule **BellCanada_MR** to the secondary Avaya SBCE (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 the Avaya SBCE, they are parsed and "pattern-matched" against the particular signaling criteria defined by these rules. Packets matching the criteria defined by the Signaling Rules are tagged for further policy matching.

Create separate Signaling Rules **CM_SR** and **BellCanada_SR** on the primary Avaya SBCE for the enterprise and Bell Canada. The sample configuration cloned and modified the default Signaling Rule.

To clone a Signaling Rule, navigate to **UC-Sec Control Center → Domain Policies → Signaling Rules**. With **default** selected, click **Clone Rule** (not shown).

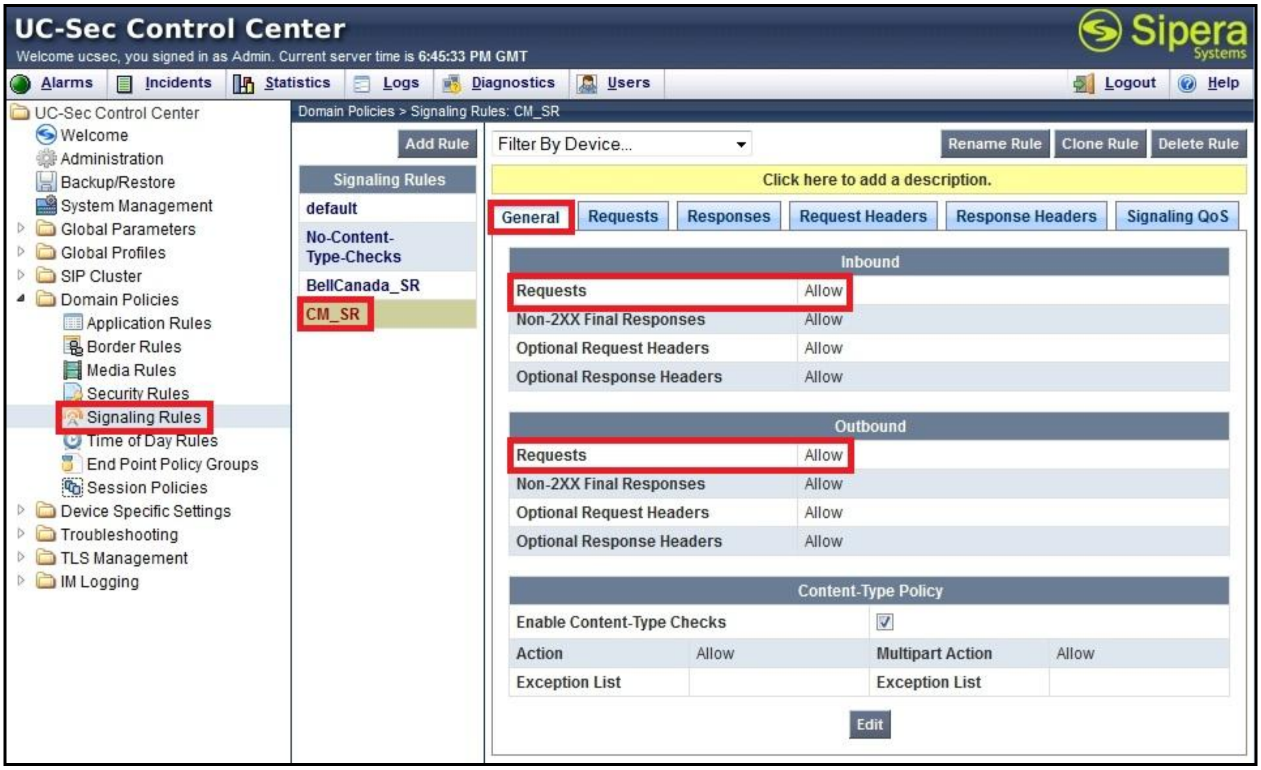
Enter a descriptive name .i.e. **CM_SR** or **BellCanada_SR** for the new rule and click **Finish** (not shown).

Note: The Signaling Rules will need to be created for both the primary Avaya SBCE and secondary Avaya SBCE using separate web interfaces.

The default Signaling Rule will block all requests with a **403 Forbidden**. To accept new call, go to **General** tab, click on **Edit** then change **Inbound** and **Outbound Request** to **Allow**.

On the **Signaling QoS** tab, check **Enabled** and DCSP value **EF** for the signaling to allow the Avaya SBCE to mark the DSCP in the IP packet header.

Following screenshots show the Signaling Rule **CM_SR** created on the primary Avaya SBCE for Communication Manager.

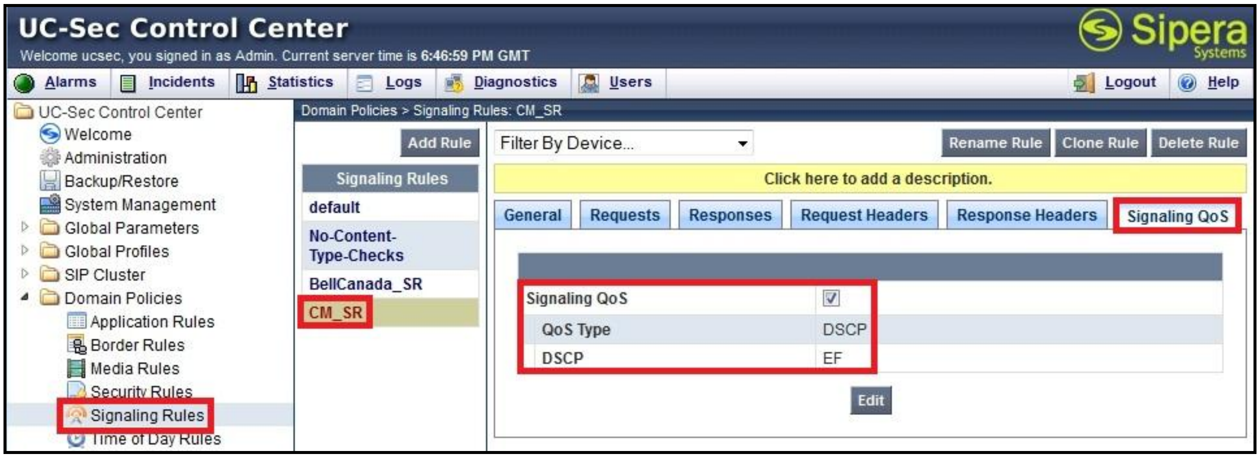


Domain Policies > Signaling Rules: CM_SR

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

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

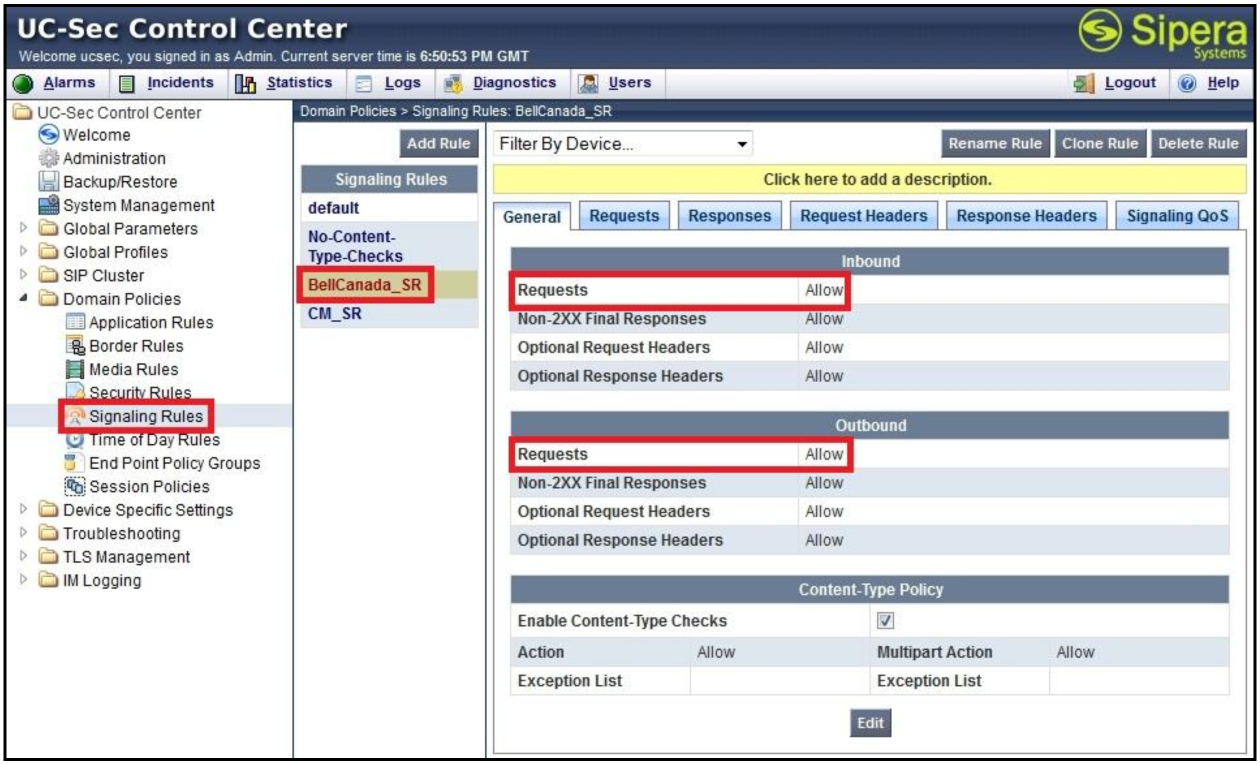
Content-Type Policy			
Enable Content-Type Checks		☑	
Action	Allow	Multipart Action	Allow
Exception List		Exception List	



Domain Policies > Signaling Rules: CM_SR

Signaling QoS	☑
QoS Type	DSCP
DSCP	EF

The Signaling Rule **BellCanada_SR** was similarly configured on the primary Avaya SBCE for Bell Canada. Its **General** settings are shown in the screenshot below. The **Signaling QoS** tab is kept as same as the Signaling Rule **CM_SR**.



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

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

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

Use the procedure to replicate the Signaling Rules **CM_SR** and **BellCanada_SR** to the secondary Avaya SBCE (not shown).

7.3.4 Endpoint Policy Groups

The rules created within the Domain Policies section are assigned to an Endpoint Policy Group. The Endpoint Policy Group is then applied to a Server Flow defined next in the **Section 7.4.4.**

This sample configuration, two Endpoint Policy Group **CM_PG** and **BellCanada_PG** were created on the primary Avaya SBCE for the enterprise and Bell Canada.

To create a new policy group, navigate to **UC-Sec Control Center → Domain Policies → Endpoint Policy Groups** and click on **Add Group** (not shown).

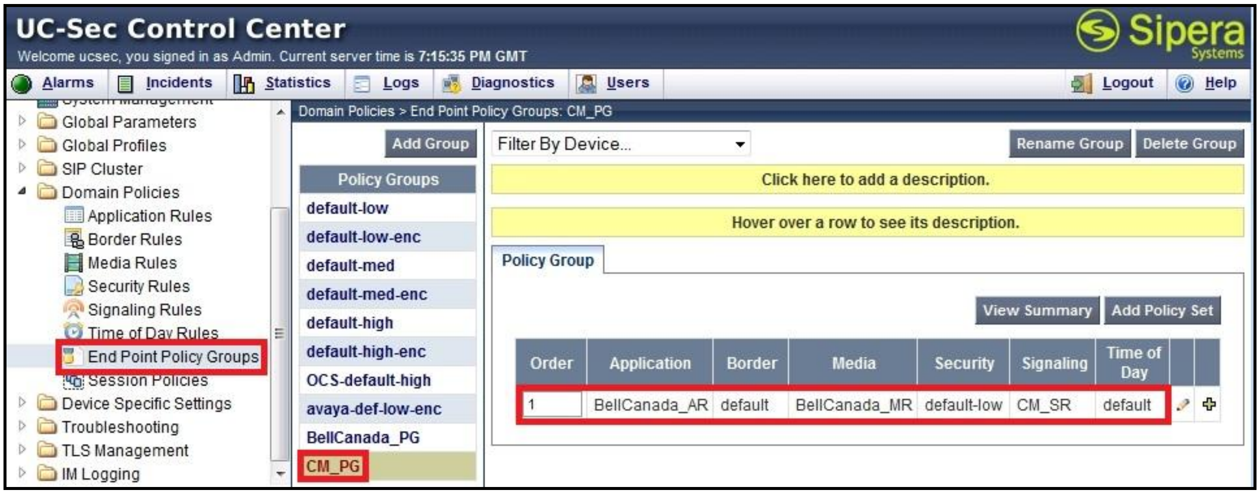
Note: The Policy Groups will need to be created for both the primary Avaya SBCE and secondary Avaya SBCE using separate web interfaces.

7.3.4.1 Endpoint Policy Group for Avaya Aura® Communication Manager

The following screen shows the Endpoint Policy Group **CM_PolicyG** created on the primary Avaya SBCE for Communication Manager.

- Set the Application Rule to the **BellCanada_AR** as created in **Section 7.3.1**.
- Set the Border Rule to **default**.
- Set the Media Rule to **BellCanada_MR** as created in **Section 7.3.2**.
- Set the Security Rule to **default-low**.

- Set the Signaling Rule to **CM_SR** as create in **Section 7.3.3**.
- Set the Time of Day to **default**.



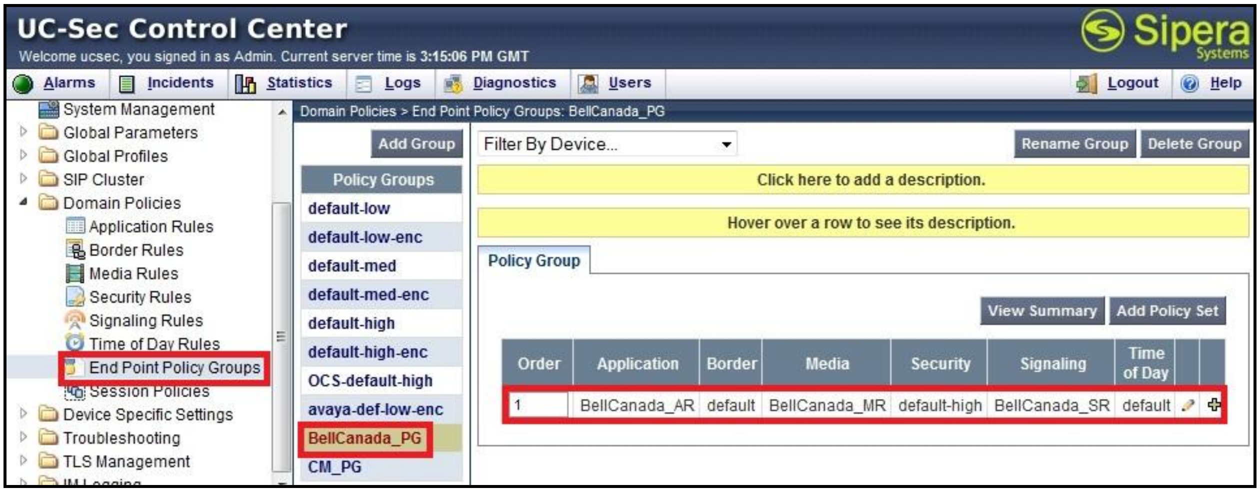
Order	Application	Border	Media	Security	Signaling	Time of Day
1	BellCanada_AR	default	BellCanada_MR	default-low	CM_SR	default

Use the procedure to replicate the same Endpoint Policy Group **CM_PG** to the secondary Avaya SBCE (not shown).

7.3.4.2 Endpoint Policy Group for Bell Canada

The following screen shows the Endpoint Policy Group **BellCanada_PG** created on the primary Avaya SBCE for Bell Canada.

- Set the Application Rule to the **BellCanada_AR** as created in **Section 7.3.1**.
- Set the Border Rule to **default**.
- Set the Media Rule to **BellCanada_MR** as created in **Section 7.3.2**.
- Set the Security Rule to **default-low**.
- Set the Signaling Rule to **BellCanada_SR** as create in **Section 7.3.4.2**.
- Set the Time of Day to **default**.



Order	Application	Border	Media	Security	Signaling	Time of Day
1	BellCanada_AR	default	BellCanada_MR	default-high	BellCanada_SR	default

Use the procedure to replicate the same Endpoint Policy Group **BellCanada_PG** to the secondary Avaya SBCE (not shown).

7.3.5 Session Policy

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

In this sample configuration, a common Session Policy **BellCanada_SP** was created on the primary Avaya SBCE to match to the codec configuration at the enterprise and Bell Canada networks. The policy also allows the Avaya SBCE to anchor media in off-net call forward or off-net call transfer scenarios.

Clone and modify the default Session Policy to apply for the enterprise and Bell Canada networks. To clone a Session Policy, navigate to **UC-Sec Control Center → Domain Policies → Session Policies**. With the **default** rule chosen, click on **Clone Rule** as shown below (not shown).

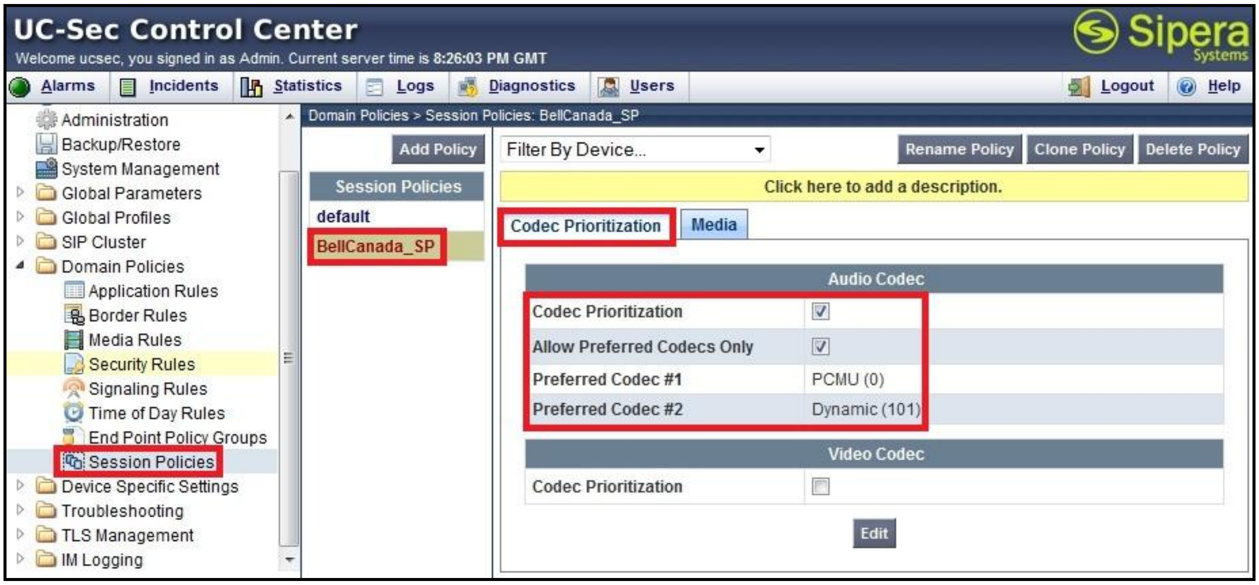
Enter a descriptive name **BellCanada_SP** for the new policy and click **Finish** (not shown).

Bell Canada supports only voice codec G.711MU with payload 101 for RFC2833/ DTMF. To define **Codec Prioritization** for Audio Codec, select the profile **BellCanada_SP**, click on **Edit** (not shown). Then check the **Codec Prioritization**, select **Preferred Codec #1** is **PCMU (0)**, **Preferred Codec #2** is **Dynamic (101)**. Check on the checkbox of **Allow Preferred Codecs Only** is to prevent the unsupported codec from being sent to both ends.

Note: The T.38 fax is not yet supported by Bell Canada SIP Trunk. In the compliance testing, the fax is successfully transmitted using G.711 codec.

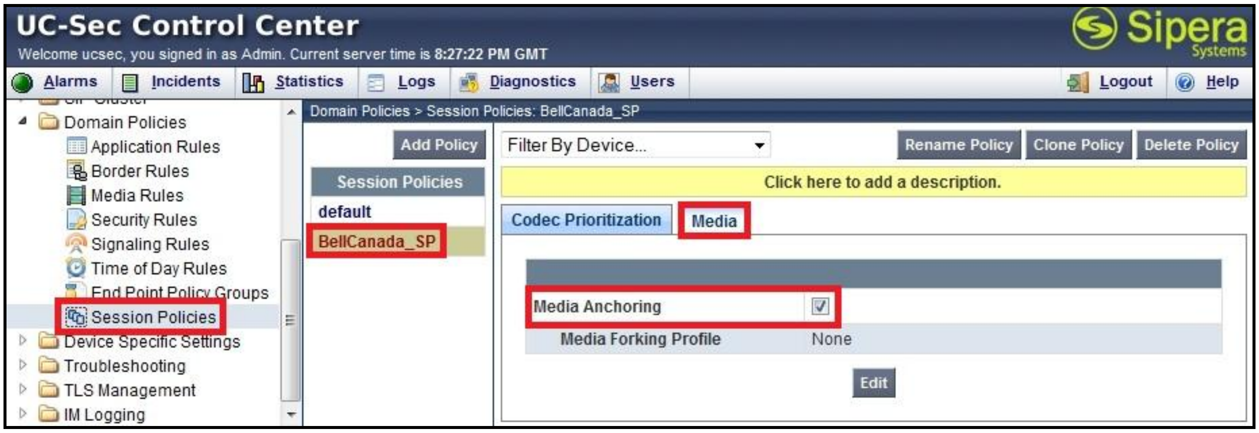
To enable **Media Anchoring** on the Avaya SBCE, select Session Policy **BellCanada_SP** then select **Media** tab. Click **Edit** (not shown) and check on **Media Anchoring**.

Following screenshots show the Session Policy **BellCanada_SP** was created on the primary Avaya SBCE.



Audio Codec	
Codec Prioritization	☑
Allow Preferred Codecs Only	☑
Preferred Codec #1	PCMU (0)
Preferred Codec #2	Dynamic (101)

Video Codec	
Codec Prioritization	☐



Media Anchoring	☑
Media Forking Profile	None

Use the procedure to replicate the same Session Policy **BellCanada_SP** to the secondary Avaya SBCE (not shown).

7.4 Device Specific Settings

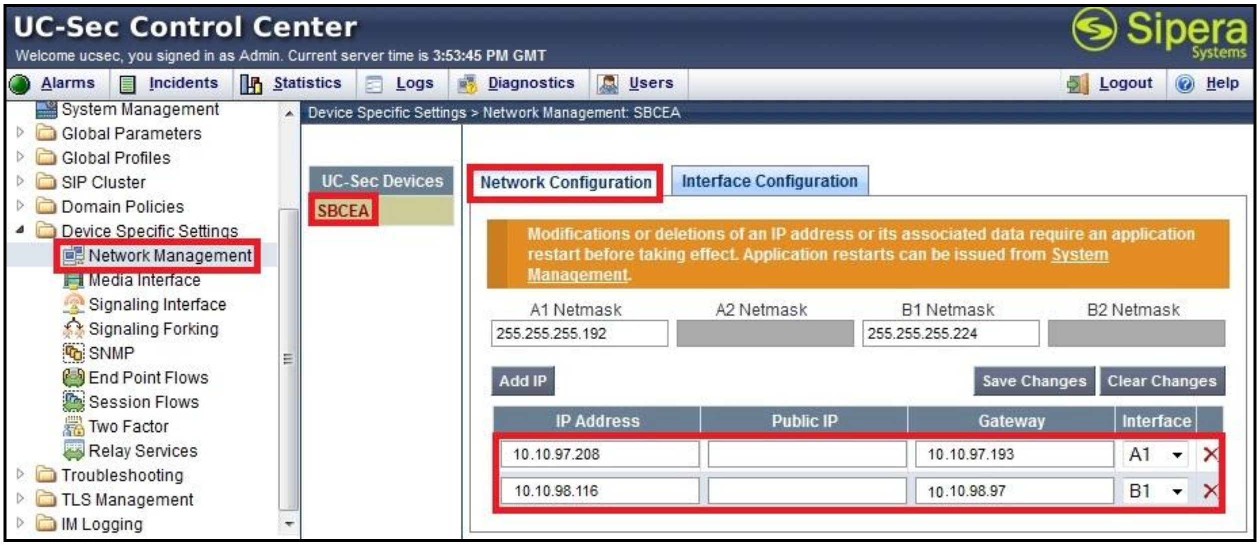
The Device Specific Settings feature allows aggregate system information to be viewed, and various device-specific parameters to be managed to determine how a particular device will function when deployed in the network. Specifically, it gives the ability to define and administer various device-specific 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 screen shows 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 addresses, public IP addresses, subnet mask, gateway, etc. to interfacing the device to the network. This information populates in the various tabs which can be edited as needed to optimize device performance and network efficiency.

Navigate to **UC-Sec Control Center → Device Specific Settings → Network Management** and verify the IP addresses assigned to the interfaces and that the interfaces are enabled.

The following screen shows the IP address **10.10.97.208** assigned to the private interface **A1** and the IP address **10.10.98.116** assigned to the public interface **B1** on the primary Avaya SBCE under **Network Configuration** tab.



Welcome ucsec, you signed in as Admin. Current server time is 3:53:45 PM GMT

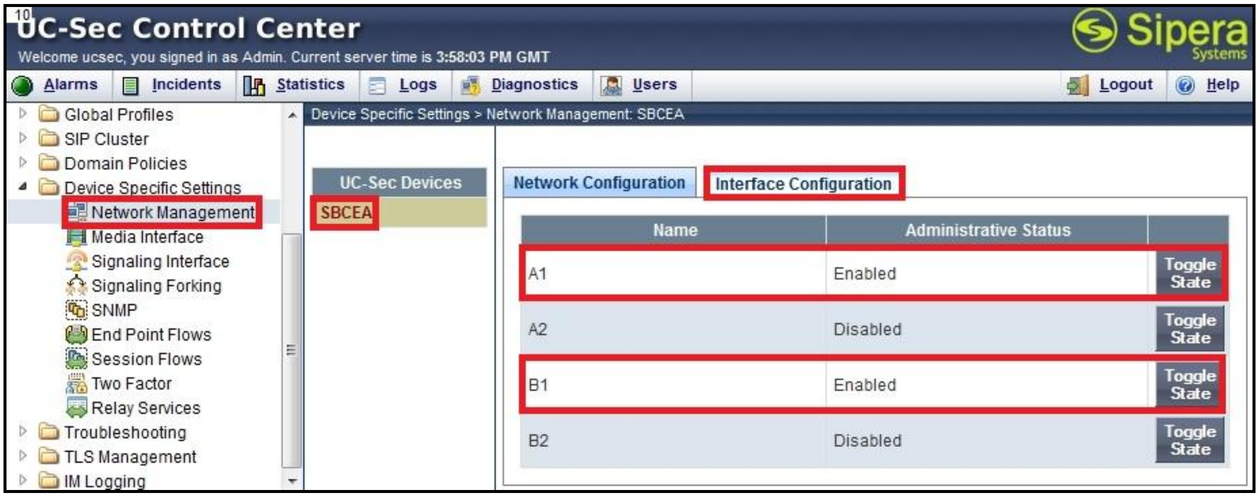
Device Specific Settings > Network Management: SBCEA

Modifications or deletions of an IP address or its associated data require an application restart before taking effect. Application restarts can be issued from System Management.

A1 Netmask	A2 Netmask	B1 Netmask	B2 Netmask
255.255.255.192		255.255.255.224	

IP Address	Public IP	Gateway	Interface
10.10.97.208		10.10.97.193	A1
10.10.98.116		10.10.98.97	B1

Enable the interfaces under the **Interface Configuration** tab. The following screen shows interface **A1** and **B1** are **Enabled** on the primary Avaya SBCE. To enable an interface, click its **Toggle State** button.

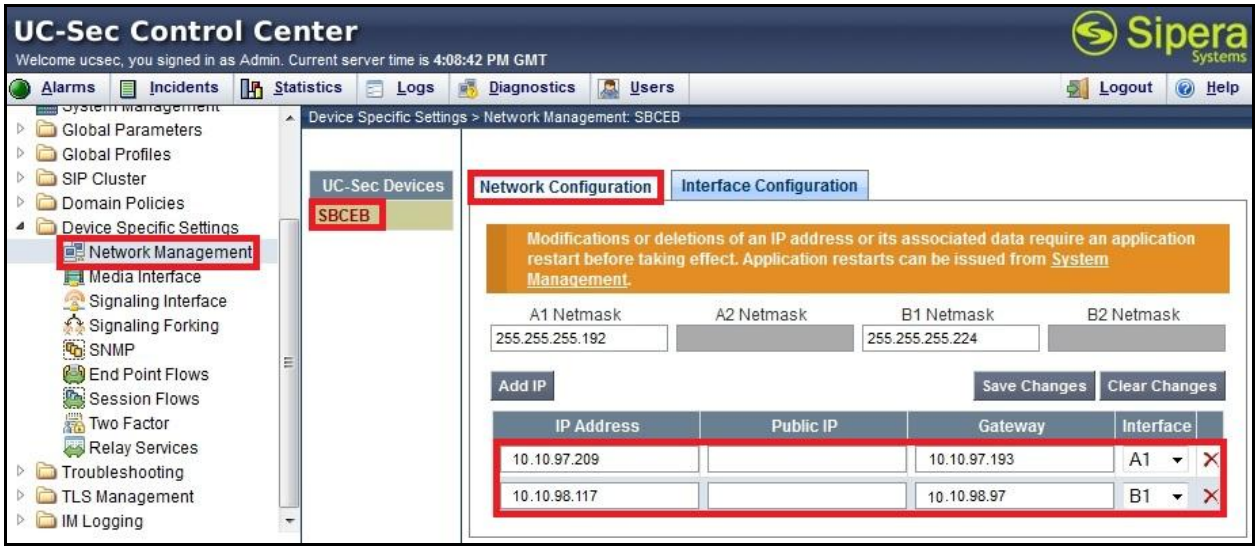


Welcome ucsec, you signed in as Admin. Current server time is 3:58:03 PM GMT

Device Specific Settings > Network Management: SBCEA

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

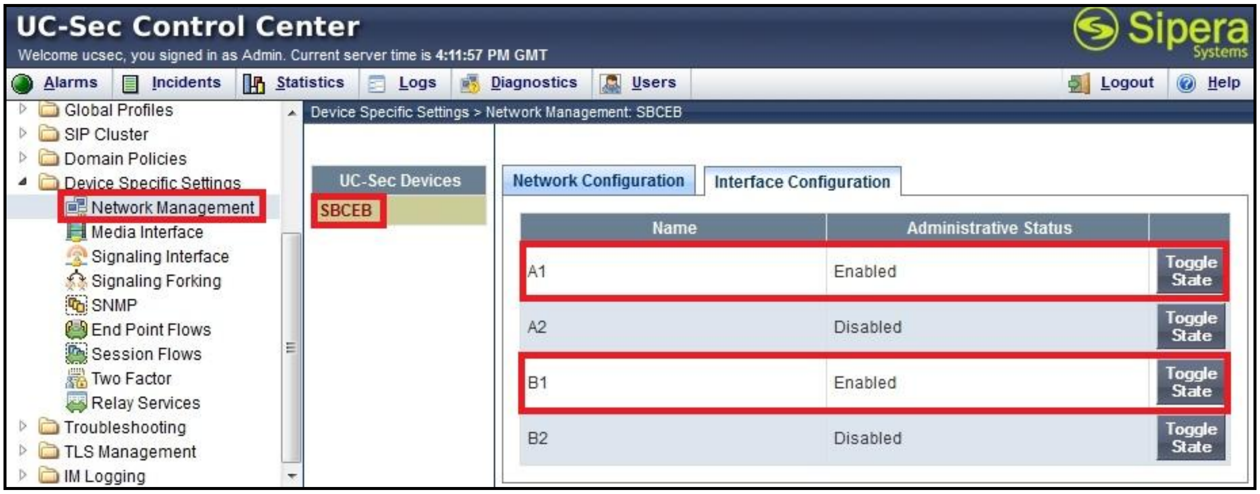
The following screenshots show the private interface **A1 10.10.97.209** and public interface **B1 10.10.98.117** that were similarly configured on the secondary Avaya SBCE.



Modifications or deletions of an IP address or its associated data require an application restart before taking effect. Application restarts can be issued from System Management.

A1 Netmask	A2 Netmask	B1 Netmask	B2 Netmask
255.255.255.192		255.255.255.224	

IP Address	Public IP	Gateway	Interface
10.10.97.209		10.10.97.193	A1
10.10.98.117		10.10.98.97	B1



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

7.4.2 Media Interface

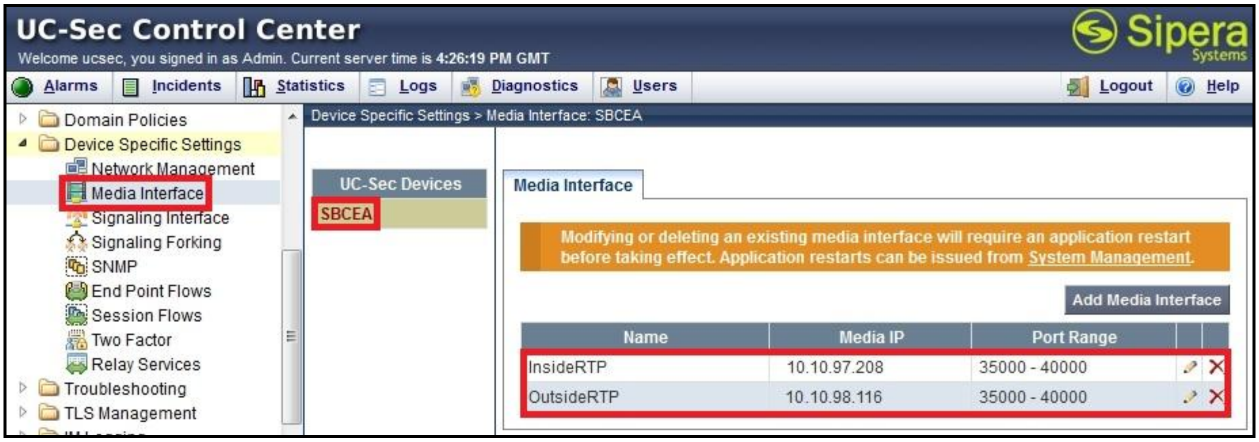
Media Interface screen shows the media ports that were defined. The Avaya SBCE will listen for RTP on the defined ports.

To create a new Media Interface, navigate to **UC-Sec Control Center → Device Specific Settings → Media Interface** and click **Add Media Interface** (not shown).

Create Media Interface **InsideRTP** and **OutsideRTP** on each Avaya SBCE for private interface **A1** and public interface **B1**.

Note**:** After the Media Interfaces are created, an application restart is necessary before the changes will take effect.

The following screen shows the Media Interfaces **InsideRTP** and **OutsideRTP** created on the primary Avaya SBCE for private interface **A1 10.10.97.208** and public interface **B1 10.10.98.116**.



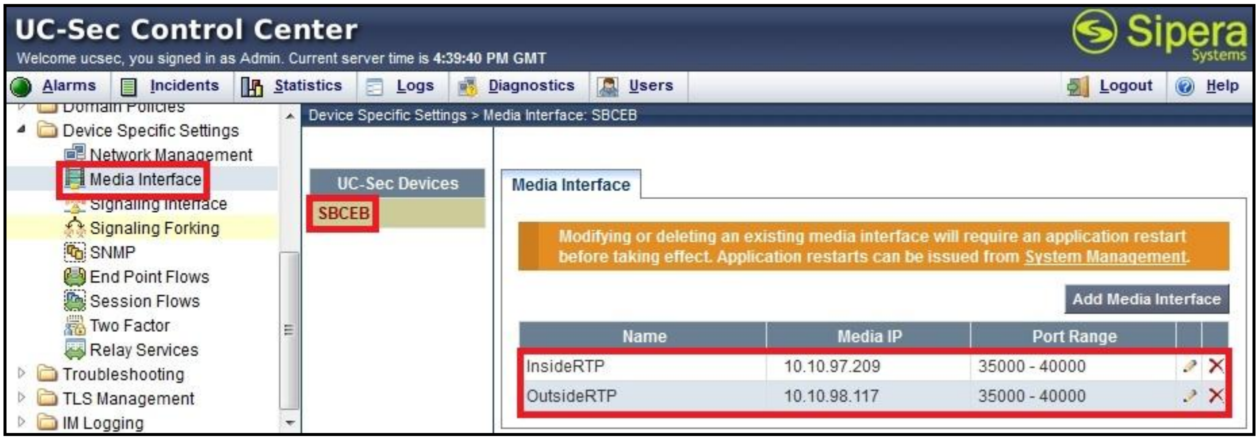
Welcome ucsec, you signed in as Admin. Current server time is **4:26:19 PM GMT**

Device Specific Settings > Media Interface: SBCEA

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

Name	Media IP	Port Range
InsideRTP	10.10.97.208	35000 - 40000
OutsideRTP	10.10.98.116	35000 - 40000

The screenshot below shows the Media Interfaces **InsideRTP** and **OutsideRTP** that were similarly created on the secondary Avaya SBCE for the private interface **A1 10.10.97.209** and public interface **B1 10.10.98.117**.



Welcome ucsec, you signed in as Admin. Current server time is **4:39:40 PM GMT**

Device Specific Settings > Media Interface: SBCEB

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

Name	Media IP	Port Range
InsideRTP	10.10.97.209	35000 - 40000
OutsideRTP	10.10.98.117	35000 - 40000

7.4.3 Signaling Interface

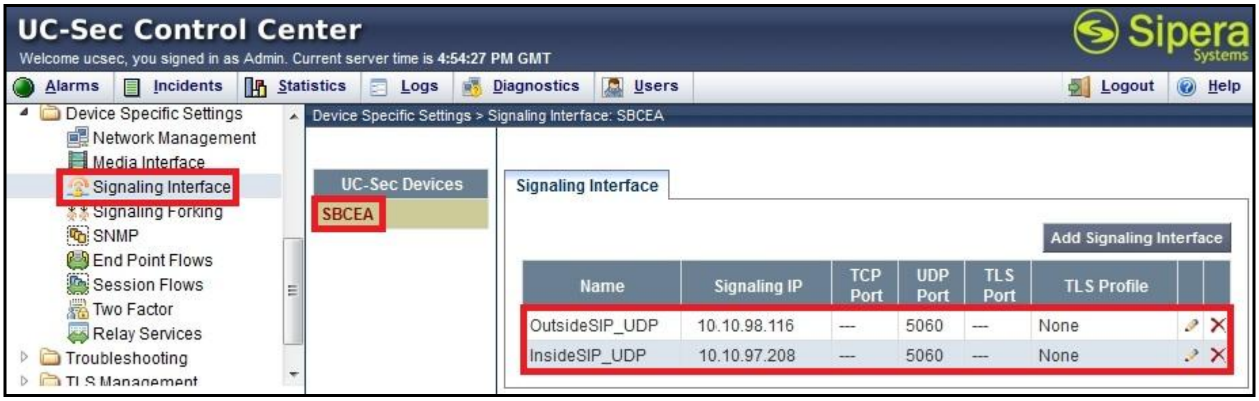
Signaling Interface screen shows the SIP signaling ports that were defined. The Avaya SBCE will listen for SIP requests on the defined ports.

To create a new Signaling Interface, navigate to **UC-Sec Control Center → Device Specific → Settings → Signaling Interface** and click **Add Signaling Interface** (not shown).

Create Signaling Interface **InsideSIP_UDP** and **OutsideSIP_UDP** on each Avaya SBCE for private interface **A1** and public interface **B1**.

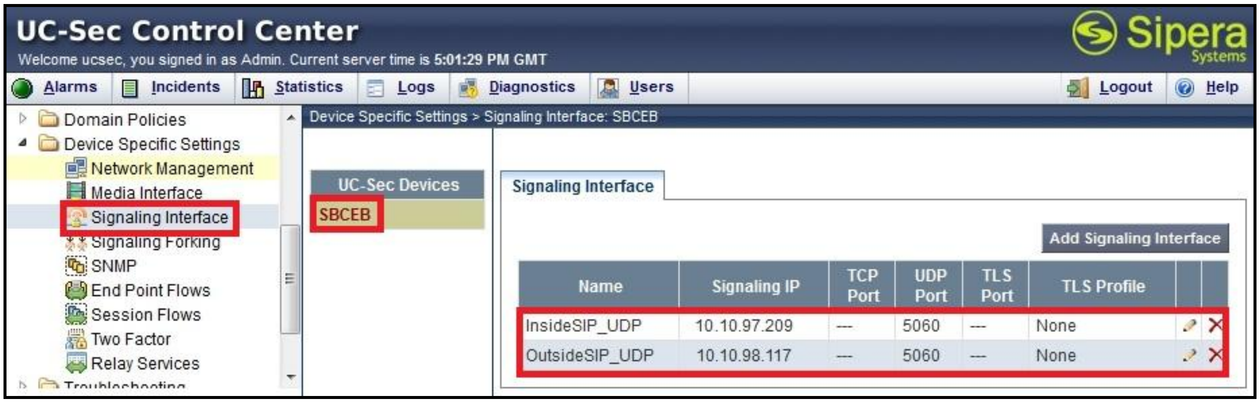
Note: After the Signaling Interfaces are created, an application restart is necessary before the changes will take effect.

The following screen shows the Signaling Interfaces **InsideSIP_UDP** and **OutsideSIP_UDP** created on the primary Avaya SBCE for private interface **A1 10.10.97.208** and public interface **B1 10.10.98.116**. Both Signaling Interfaces were defined with transport protocol UDP and port **5060**.



Name	Signaling IP	TCP Port	UDP Port	TLS Port	TLS Profile
OutsideSIP_UDP	10.10.98.116	---	5060	---	None
InsideSIP_UDP	10.10.97.208	---	5060	---	None

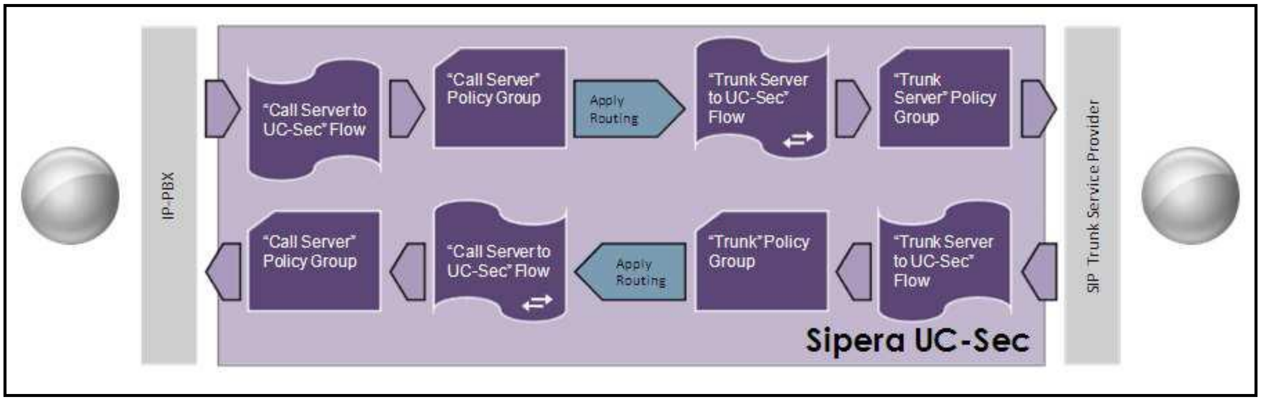
The screenshot below shows the Signaling Interfaces **InsideSIP_UDP** and **OutsideSIP_UDP** that were similarly created on the secondary Avaya SBCE for the private interface **A1 10.10.97.209** and public interface **B1 10.10.98.117**. Both Signaling Interfaces were also defined with transport protocol UDP and port **5060**.



Name	Signaling IP	TCP Port	UDP Port	TLS Port	TLS Profile
InsideSIP_UDP	10.10.97.209	---	5060	---	None
OutsideSIP_UDP	10.10.98.117	---	5060	---	None

7.4.4 End Point Flows - Server Flows

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


IP-PBX
"Call Server to UC-Sec" Flow
"Call Server" Policy Group
Apply Routing
"Trunk Server to UC-Sec" Flow
"Trunk Server" Policy Group
SIP Trunk Service Provider
"Call Server" Policy Group
"Call Server to UC-Sec" Flow
Apply Routing
"Trunk" Policy Group
"Trunk Server to UC-Sec" Flow
Sipera UC-Sec

To create a Server Flow, navigate to **UC-Sec Control Center → Device Specific Settings → End Point Flows**. Select the **Server Flows** tab and click **Add Flow** (not shown).

In the new window that appears, enter the following values:

- **Flow Name:** Enter a descriptive name.
- **Server Configuration:** Select a Server Configuration created in **Section 7.2.6**.
- **URI Group:** Select the URI Group created in **Section 7.2.1**.
- **Received Interface:** Select a Signaling Interface created in **Section 7.4.3** which the Server Configuration is designed to receive SIP signaling.
- **Signaling Interface:** Select a Signaling Interface created in **Section 7.4.3** which the Server Configuration is designed to send SIP signaling.
- **Media Interface:** Select the Media Interface created in **Section 7.4.2** which the Server Configuration is designed to send RTP.
- **End Point Policy Group:** Select an Endpoint Policy Group created in **Section 7.3.4**.
- **Routing Profile:** Select a Routing profile created in **Section 7.2.2** which the Server Configuration is designed to use to route the calls to the destination.
- **Topology Hiding Profile:** Select a Topology Hiding profile created in **Section 7.2.3** to apply toward the Server Configuration.

Use default values for all remaining fields. Click **Finish** to save and exit.

Note: Each Server Flow profile will need to be created for both the primary Avaya SBCE and secondary Avaya SBCE using separate web interfaces.

7.4.4.1 Server Flows for the Primary Avaya Aura® Session Manager

Multiple Sever Flows were created on the primary Avaya SBCE for the primary Session Manager including Server Flow **OPTIONS_SM61A** for routing the outgoing OPTIONS heartbeat, Server Flow **Inbound** for incoming calls and Server Flows **Outbound_With_cust2** and **Outbound_With_cust6** for outgoing calls.

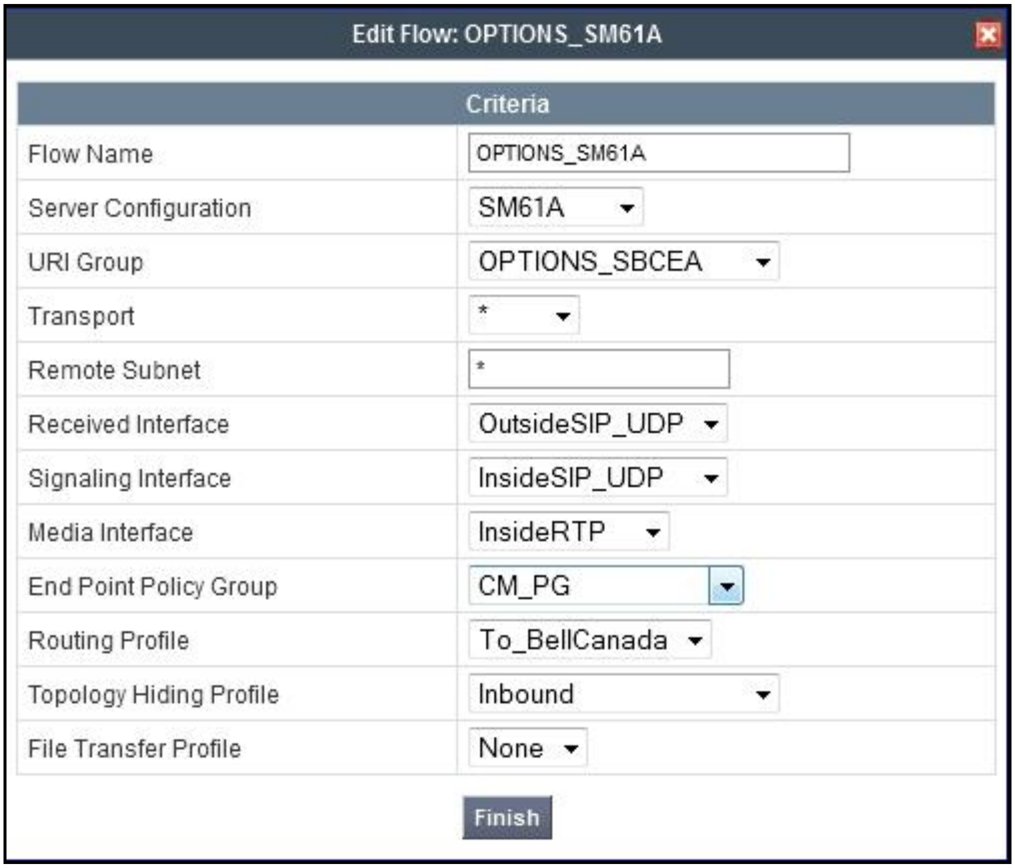
Note: In the compliance testing, two Server Flows for outgoing calls were defined for each of two combinations of DID range and service provider public SIP domain assigned by Bell Canada. If there are more than two combinations of DID range and service provider public SIP domain assigned by Bell Canada deployed in the field, then more Server Flows for outgoing calls will need to be created.

The Server Flows for the primary Session Manager were created with following values:

- **Flow Name:** Enter a descriptive name.
- **Server Configuration:** Select the Server Configuration **SM61A** created in **Section 7.2.6.1**.
- **URI Group:** Select the URI Group **OPTIONS_SBCA**, **Inbound**, **Outbound_With_cust2** and **Outbound_With_cust6** appropriately for each Server Flow. The URI Groups were created in **Section 7.2.1**.
- **Received Interface:** Select the Signaling Interface **OutsideSIP_UDP** created in **Section 7.4.3**.
- **Signaling Interface:** Select a Signaling Interface **InsideSIP_UDP** created in **Section 7.4.3**.
- **Media Interface:** Select the Media Interface **InsideRTP** created in **Section 7.4.2**.
- **End Point Policy Group:** Select an Endpoint Policy Group **CM_PG** created in **Section 7.3.4.1**.
- **Routing profile:** Select a Routing profile **To_BellCanada** created in **Section 7.2.2.2**.
- **Topology Hiding Profile:** Select a Topology Hiding profile **Inbound** created in **Section 7.2.3.1**.

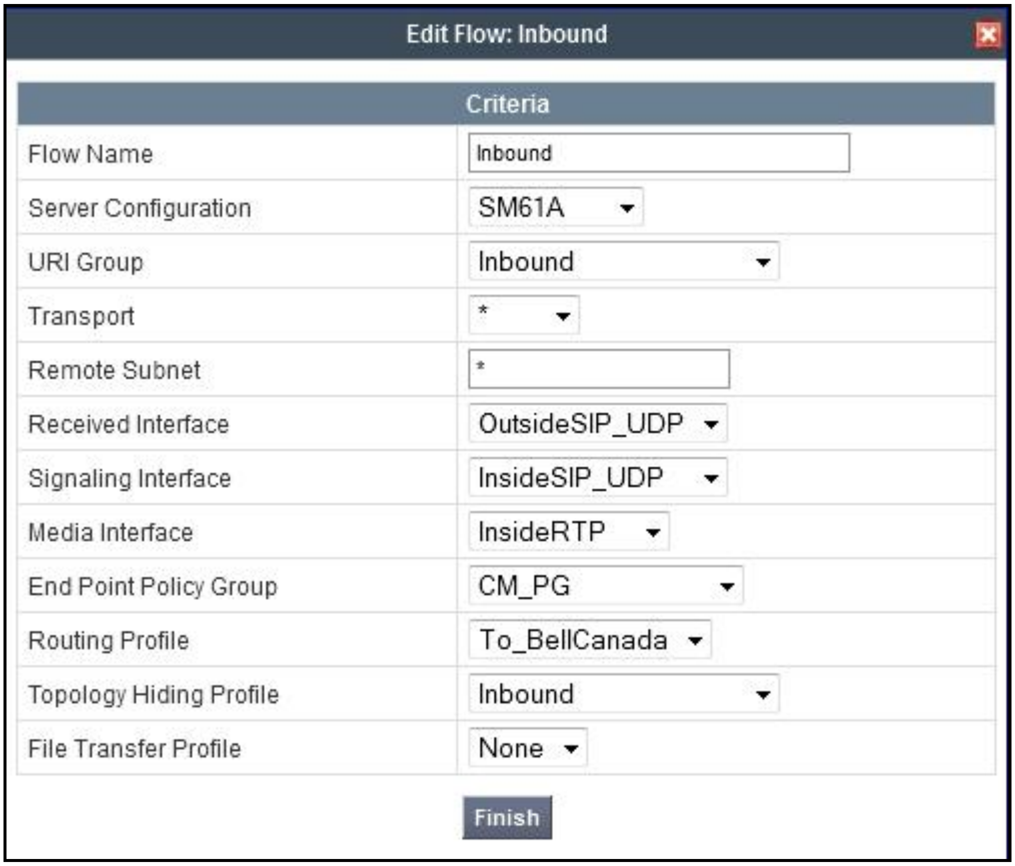
Use default values for all remaining fields. Click **Finish** to save and exit.

The following screenshots show the Sever Flows **OPTIONS_SM61A**, **Inbound**, **Outbound_With_cust2** and **Outbound_With_cust6** created on the primary Avaya SBCE for the primary Session Manager.



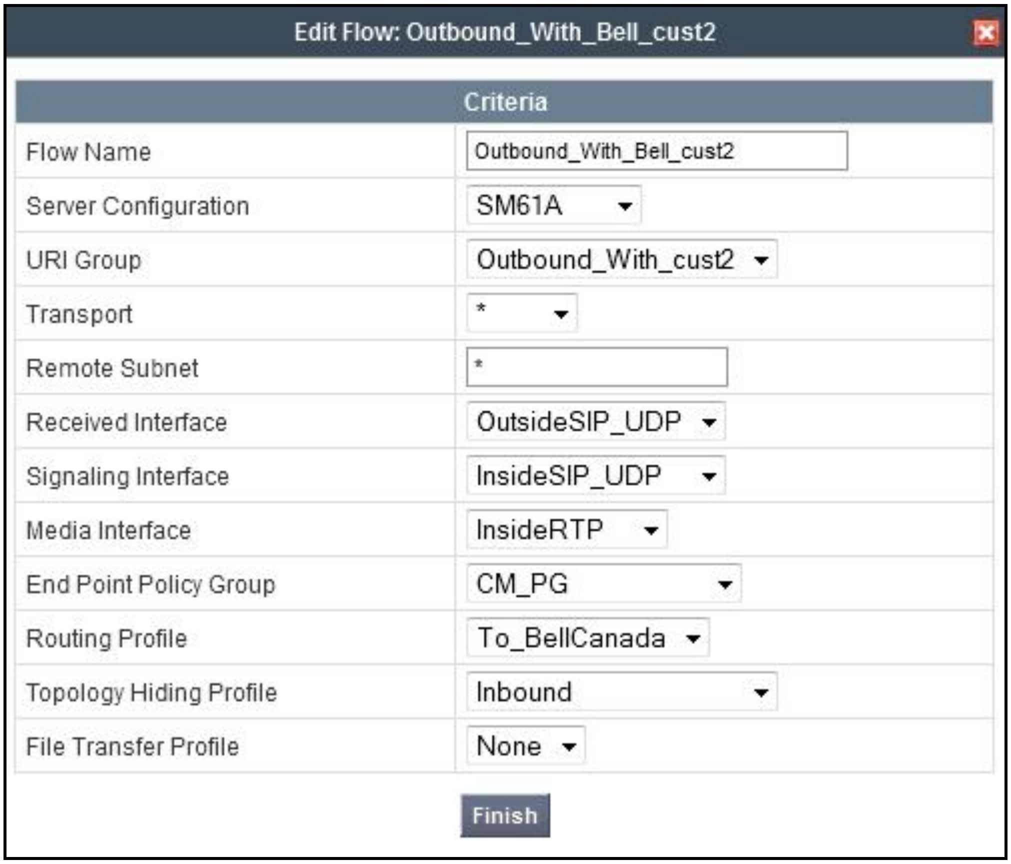
Edit Flow: OPTIONS_SM61A

Criteria	
Flow Name	OPTIONS_SM61A
Server Configuration	SM61A
URI Group	OPTIONS_SBCEA
Transport	*
Remote Subnet	*
Received Interface	OutsideSIP_UDP
Signaling Interface	InsideSIP_UDP
Media Interface	InsideRTP
End Point Policy Group	CM_PG
Routing Profile	To_BellCanada
Topology Hiding Profile	Inbound
File Transfer Profile	None



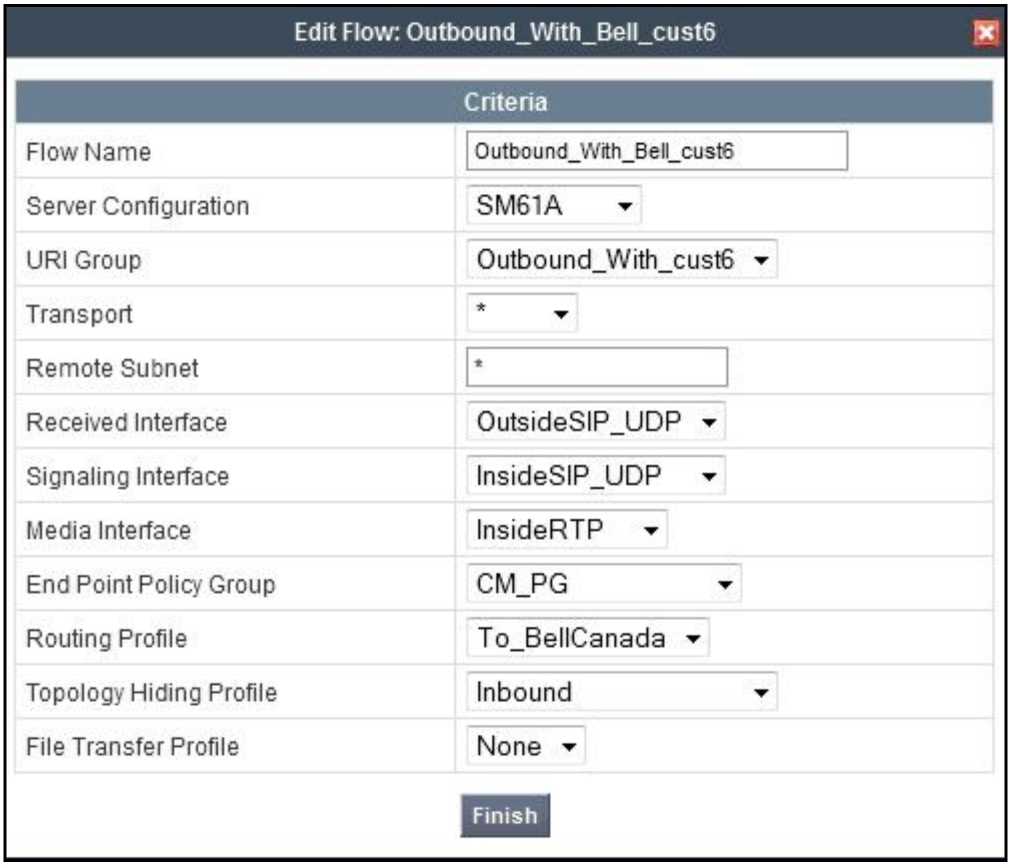
Edit Flow: Inbound

Criteria	
Flow Name	Inbound
Server Configuration	SM61A
URI Group	Inbound
Transport	*
Remote Subnet	*
Received Interface	OutsideSIP_UDP
Signaling Interface	InsideSIP_UDP
Media Interface	InsideRTP
End Point Policy Group	CM_PG
Routing Profile	To_BellCanada
Topology Hiding Profile	Inbound
File Transfer Profile	None



Edit Flow: Outbound_With_Bell_cust2

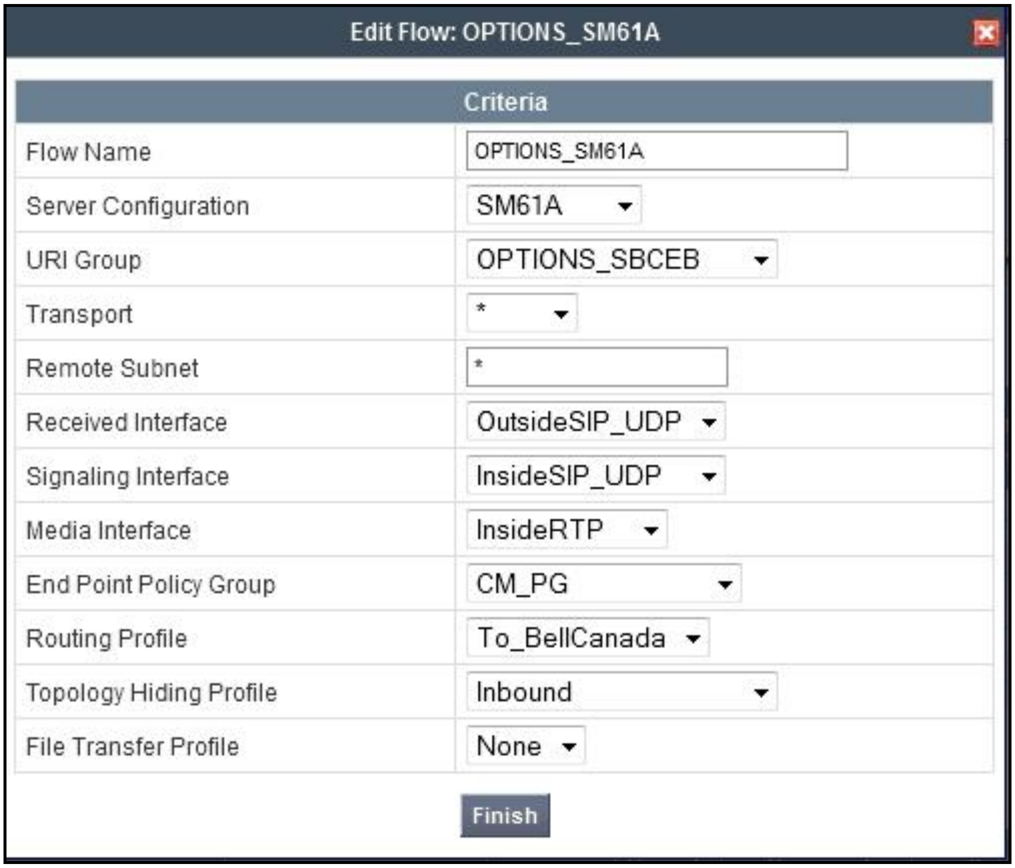
Criteria	
Flow Name	Outbound_With_Bell_cust2
Server Configuration	SM61A
URI Group	Outbound_With_cust2
Transport	*
Remote Subnet	*
Received Interface	OutsideSIP_UDP
Signaling Interface	InsideSIP_UDP
Media Interface	InsideRTP
End Point Policy Group	CM_PG
Routing Profile	To_BellCanada
Topology Hiding Profile	Inbound
File Transfer Profile	None



Edit Flow: Outbound_With_Bell_cust6

Criteria	
Flow Name	Outbound_With_Bell_cust6
Server Configuration	SM61A
URI Group	Outbound_With_cust6
Transport	*
Remote Subnet	*
Received Interface	OutsideSIP_UDP
Signaling Interface	InsideSIP_UDP
Media Interface	InsideRTP
End Point Policy Group	CM_PG
Routing Profile	To_BellCanada
Topology Hiding Profile	Inbound
File Transfer Profile	None

Use the procedure to replicate the same Server Flows **OPTIONS_SM61A**, **Inbound**, **Outbound_With_cust2** and **Outbound_With_cust6** to the secondary Avaya SBCE for the primary Session Manager (not shown). Note: There is one exception of the URI Group **OPTIONS_ SBCB** which was created in **Section 7.2.1** was set to the Server Flow **OPTIONS_SM61A** as shown below.



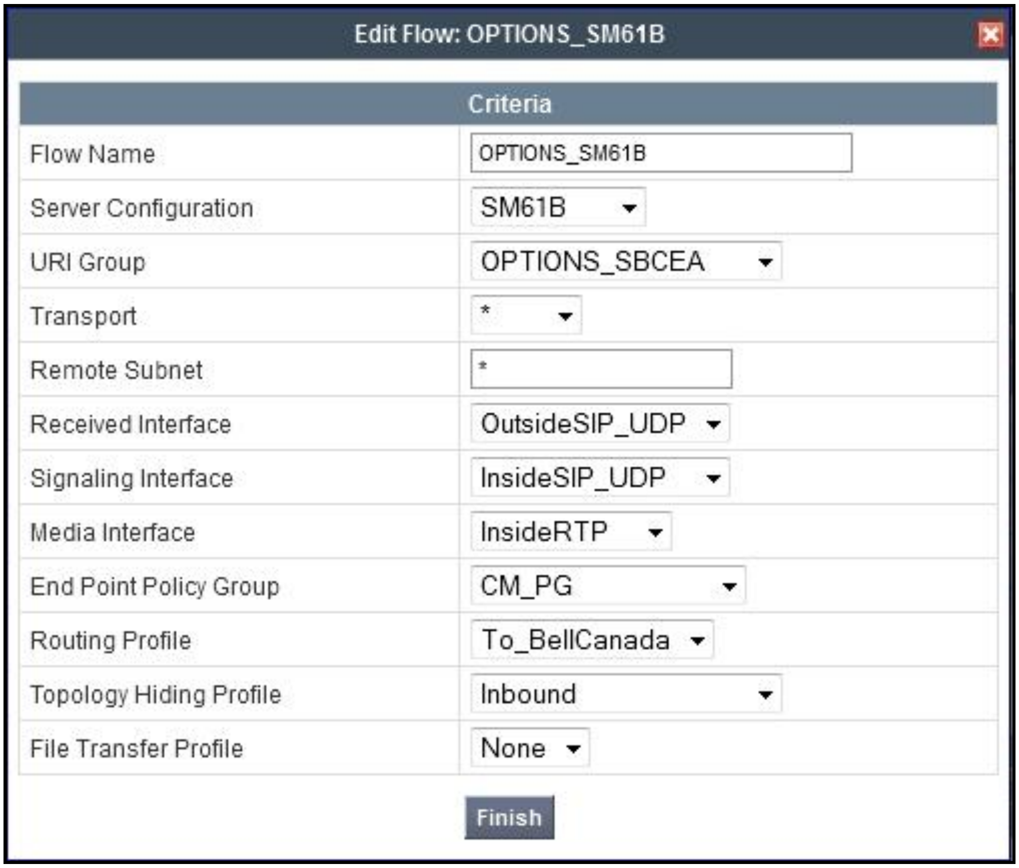
Edit Flow: OPTIONS_SM61A

Criteria	
Flow Name	OPTIONS_SM61A
Server Configuration	SM61A
URI Group	OPTIONS_SBCEB
Transport	*
Remote Subnet	*
Received Interface	OutsideSIP_UDP
Signaling Interface	InsideSIP_UDP
Media Interface	InsideRTP
End Point Policy Group	CM_PG
Routing Profile	To_BellCanada
Topology Hiding Profile	Inbound
File Transfer Profile	None

7.4.4.2 Server Flows for the Secondary Avaya Aura® Session Manager

The Server Flows for the secondary Session Manager were similarly created with the exemption of the Server Configuration was set to **SM61B** which was created in **Section 7.2.6.1**.

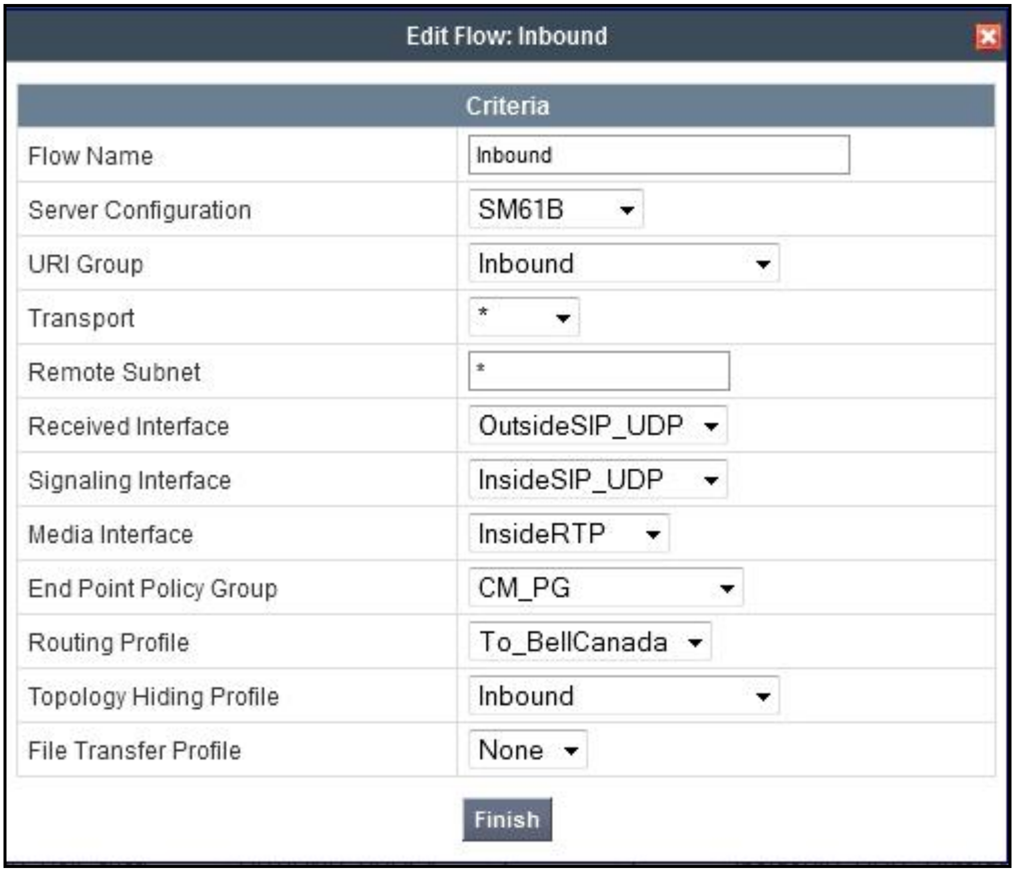
The following screenshots show the Sever Flows **OPTIONS_SM61B**, **Inbound**, **Outbound_With_cust2** and **Outbound_With_cust6** were created on the primary Avaya SBCE for the secondary Session Manager.



Edit Flow: OPTIONS_SM61B

Criteria

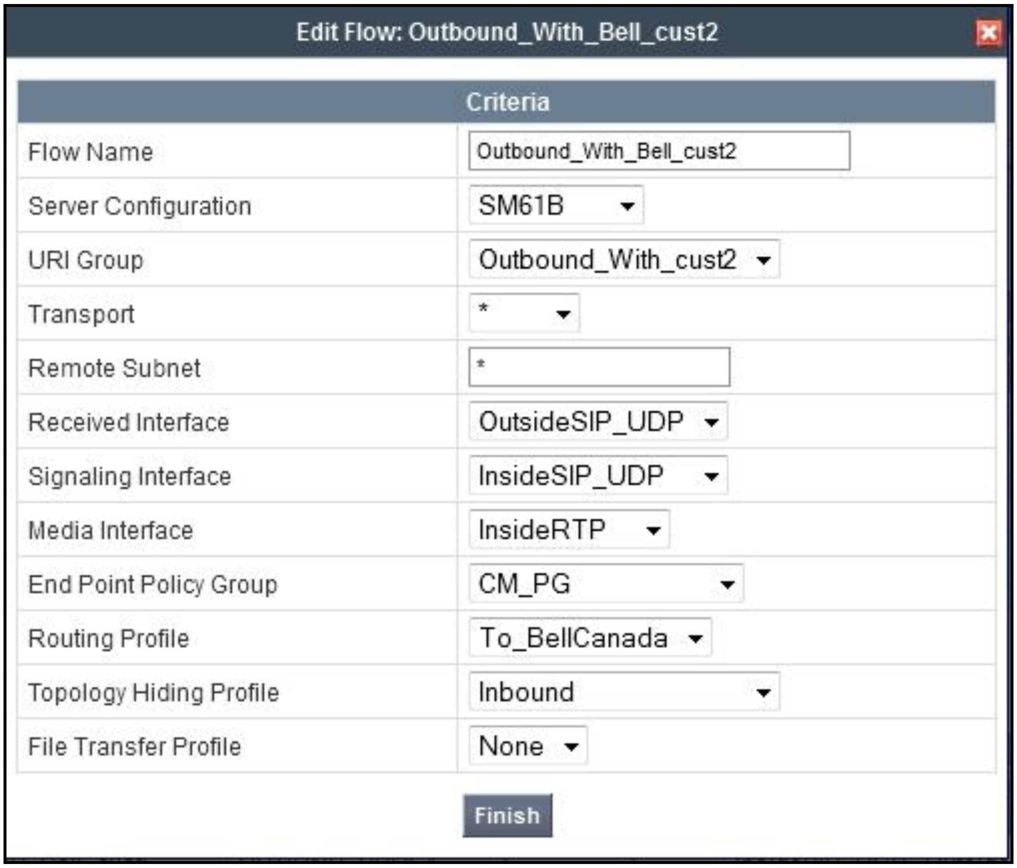
Flow Name	OPTIONS_SM61B
Server Configuration	SM61B
URI Group	OPTIONS_SBCEA
Transport	*
Remote Subnet	*
Received Interface	OutsideSIP_UDP
Signaling Interface	InsideSIP_UDP
Media Interface	InsideRTP
End Point Policy Group	CM_PG
Routing Profile	To_BellCanada
Topology Hiding Profile	Inbound
File Transfer Profile	None



Edit Flow: Inbound

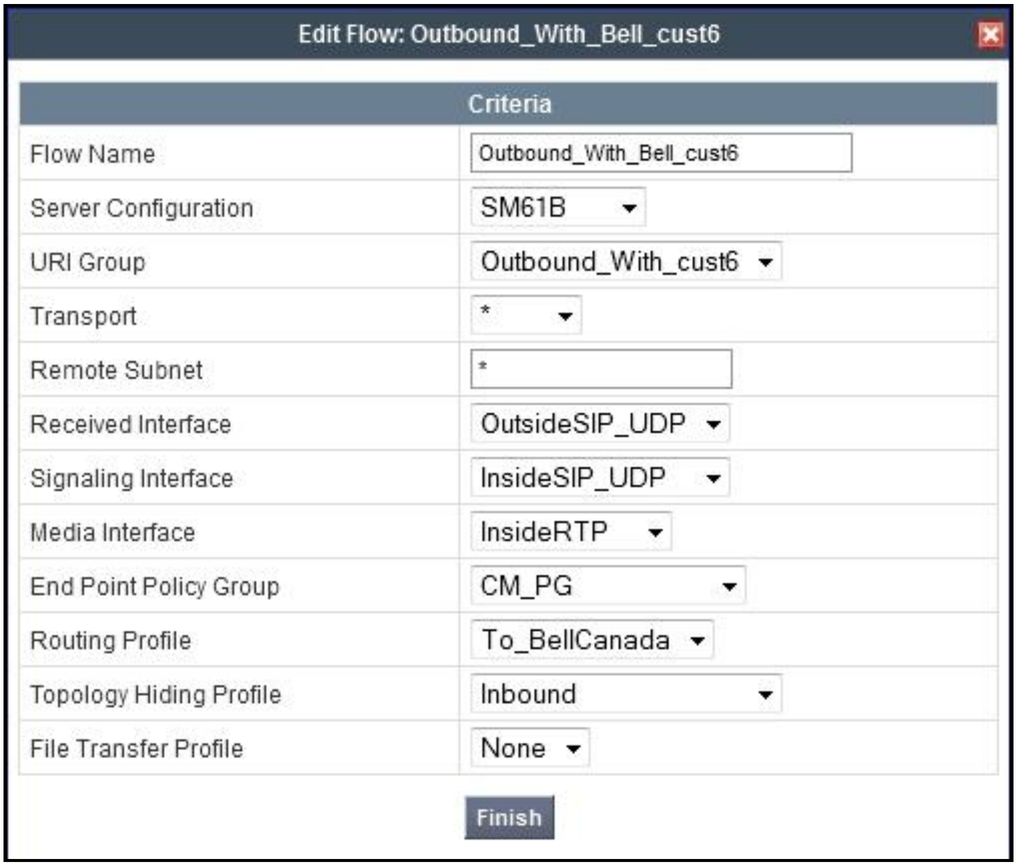
Criteria

Flow Name	Inbound
Server Configuration	SM61B
URI Group	Inbound
Transport	*
Remote Subnet	*
Received Interface	OutsideSIP_UDP
Signaling Interface	InsideSIP_UDP
Media Interface	InsideRTP
End Point Policy Group	CM_PG
Routing Profile	To_BellCanada
Topology Hiding Profile	Inbound
File Transfer Profile	None



Edit Flow: Outbound_With_Bell_cust2

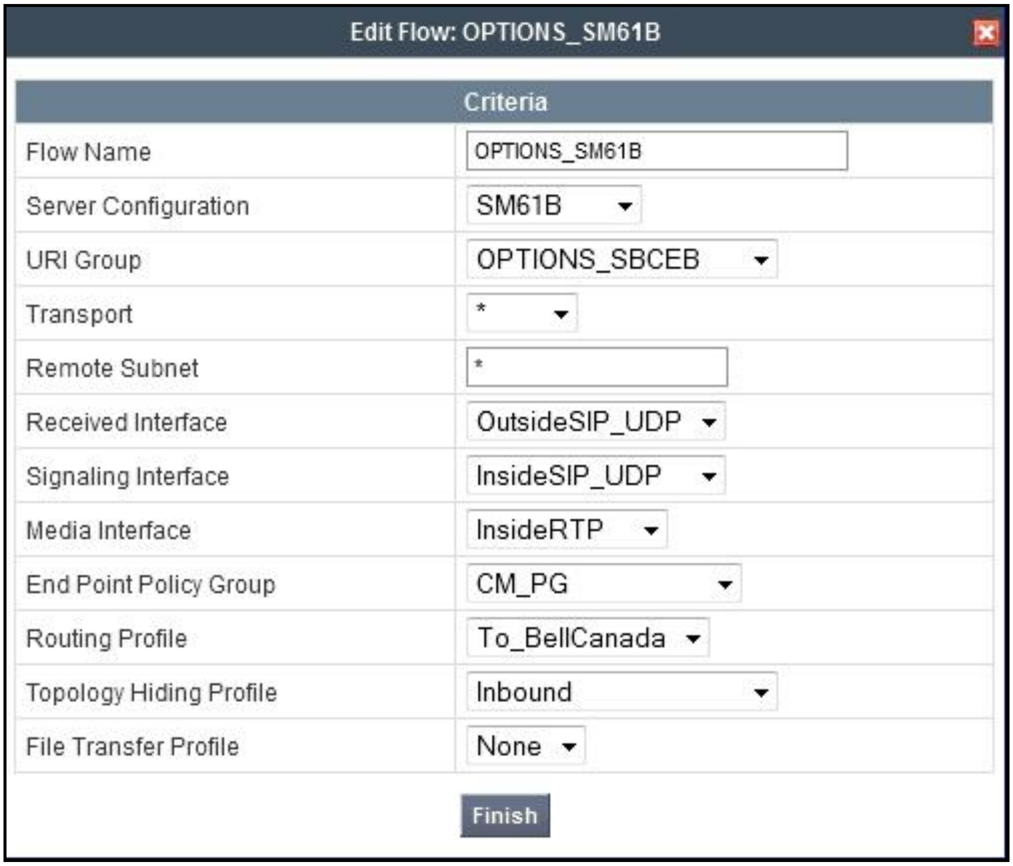
Criteria	
Flow Name	Outbound_With_Bell_cust2
Server Configuration	SM61B
URI Group	Outbound_With_cust2
Transport	*
Remote Subnet	*
Received Interface	OutsideSIP_UDP
Signaling Interface	InsideSIP_UDP
Media Interface	InsideRTP
End Point Policy Group	CM_PG
Routing Profile	To_BellCanada
Topology Hiding Profile	Inbound
File Transfer Profile	None



Edit Flow: Outbound_With_Bell_cust6

Criteria	
Flow Name	Outbound_With_Bell_cust6
Server Configuration	SM61B
URI Group	Outbound_With_cust6
Transport	*
Remote Subnet	*
Received Interface	OutsideSIP_UDP
Signaling Interface	InsideSIP_UDP
Media Interface	InsideRTP
End Point Policy Group	CM_PG
Routing Profile	To_BellCanada
Topology Hiding Profile	Inbound
File Transfer Profile	None

Use the procedure to replicate the same Server Flows **OPTIONS_SM61B**, **Inbound**, **Outbound_With_cust2** and **Outbound_With_cust6** to the secondary Avaya SBCE for the secondary Session Manager (not shown). Note: There is one exception of the URI Group **OPTIONS_ SBCB** which was created in **Section 7.2.1** was set to the Server Flow **OPTIONS_SM61B** as shown below.



Edit Flow: OPTIONS_SM61B

Criteria	
Flow Name	OPTIONS_SM61B
Server Configuration	SM61B
URI Group	OPTIONS_SBCEB
Transport	*
Remote Subnet	*
Received Interface	OutsideSIP_UDP
Signaling Interface	InsideSIP_UDP
Media Interface	InsideRTP
End Point Policy Group	CM_PG
Routing Profile	To_BellCanada
Topology Hiding Profile	Inbound
File Transfer Profile	None

7.4.4.3 Server Flows for the Primary Bell Canada CO

Multiple Sever Flows were created on the primary Avaya SBCE for the primary Bell Canada CO including Server Flow **OPTIONS_Bell_cust2** for routing the incoming OPTIONS heartbeat, Server Flow **Inbound** for incoming calls and Server Flows **Outbound_With_cust2** and **Outbound_With_cust6** for outgoing calls.

Note: In the compliance testing, two Server Flows for outgoing calls were defined in for each of two combinations of DID range and service provider public SIP domain assigned by Bell Canada. If there are more than two combinations of DID range and service provider public SIP domain assigned by Bell Canada deployed in the field, then more Server Flows for outgoing calls will need to be created.

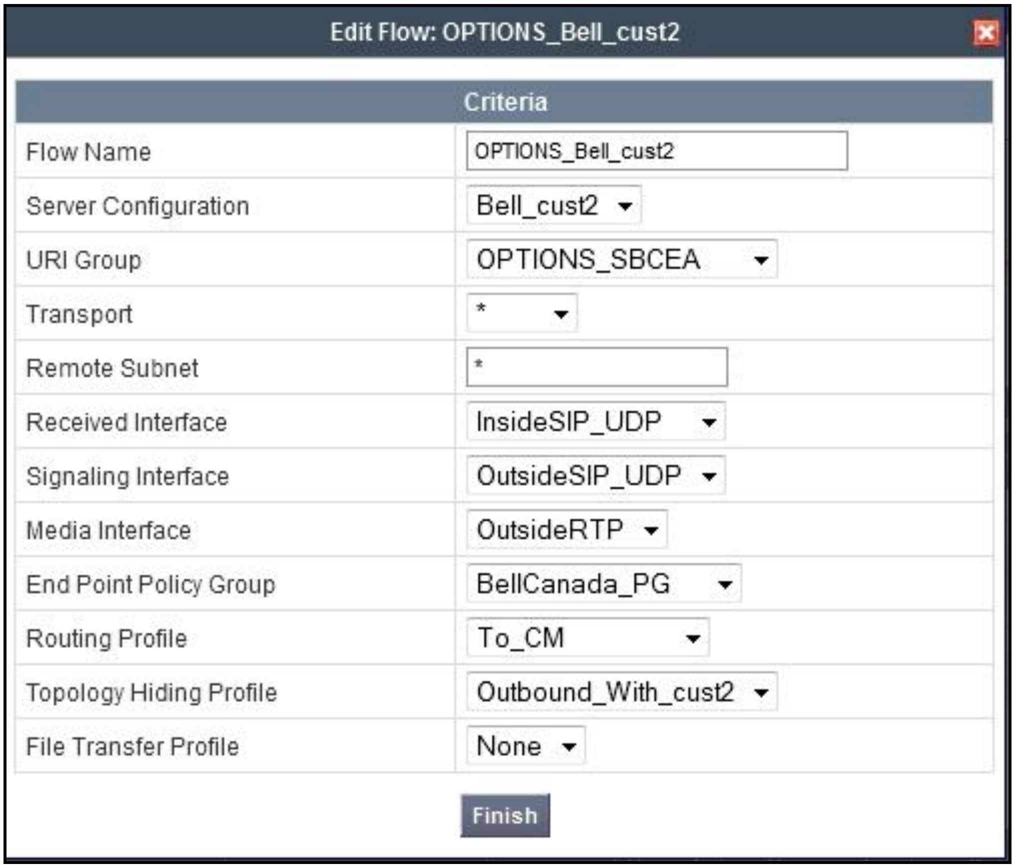
The Server Flows for the primary Bell Canada CO were created with following values:

- **Flow Name:** Enter a descriptive name.
- **Server Configuration:** Select the Server Configuration **Bell_cust2** created in **Section 7.2.6.2**.
- **URI Group:** Select the URI Group **OPTIONS_SBCA**, **Inbound**, **Outbound_With_cust2** and **Outbound_With_cust6** appropriately for each Server Flow. The URI Groups were created in **Section 7.2.1**.
- **Received Interface:** Select the Signaling Interface **InsideSIP_UDP** created in **Section 7.4.3**.

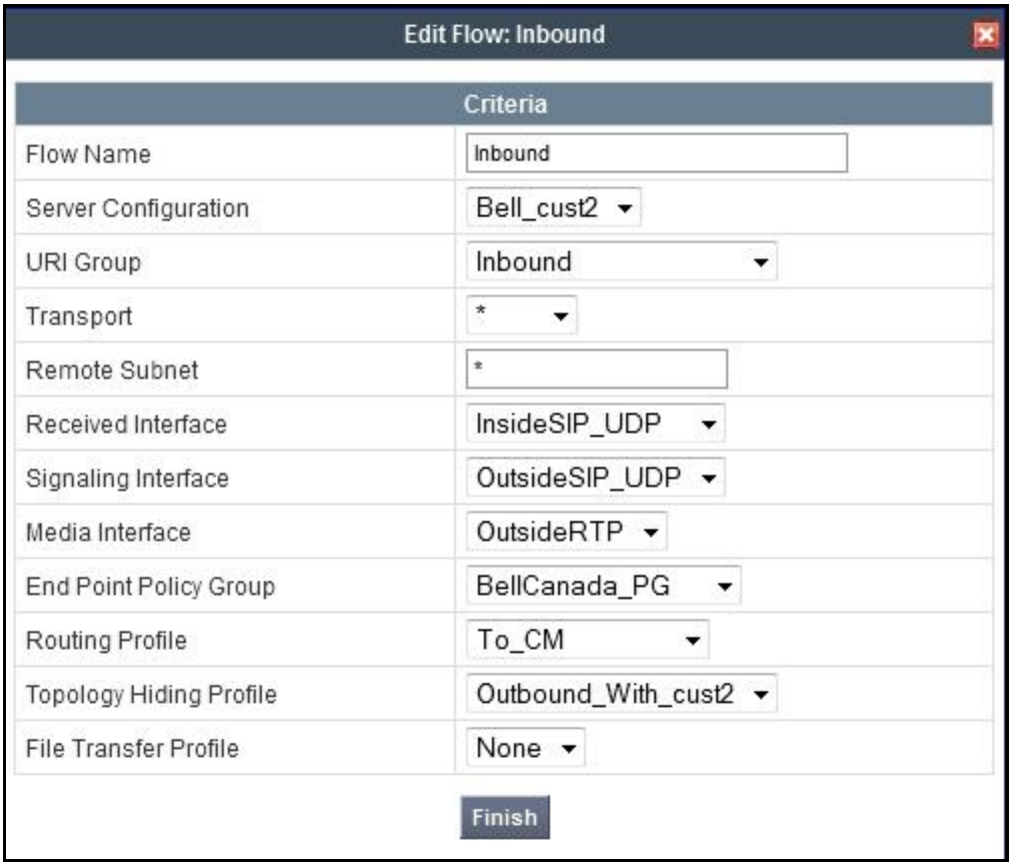
- **Signaling Interface:** Select the Signaling Interface **OutsideSIP_UDP** created in **Section 7.4.3**.
- **Media Interface:** Select the Media Interface **OutsideRTP** created in **Section 7.4.2**.
- **End Point Policy Group:** Select the Endpoint Policy Group **BellCanada_PG** created in **Section 7.3.4.2**.
- **Routing profile:** Select the Routing profile **To_CM** created in **Section 7.2.2.1**.
- **Topology Hiding Profile:** Select the Topology Hiding profile **Outbound_With_cust2** for the Server Flows with the URI Groups **OPTIONS_SBCA**, **Inbound**, **Outbound_With_cust2** and the Topology Hiding profile **Outbound_With_cust6** for the Server Flow with the URI Group **Outbound_With_cust6**. The Topology Hiding profiles were created in **Section 7.2.3.1**.

Use default values for all remaining fields. Click **Finish** to save and exit.

The following screenshots show the Sever Flows **OPTIONS_Bell_cust2**, **Inbound**, **Outbound_With_cust2** and **Outbound_With_cust6** were created on the primary Avaya SBCE for the primary Bell Canada CO.


Edit Flow: OPTIONS_Bell_cust2

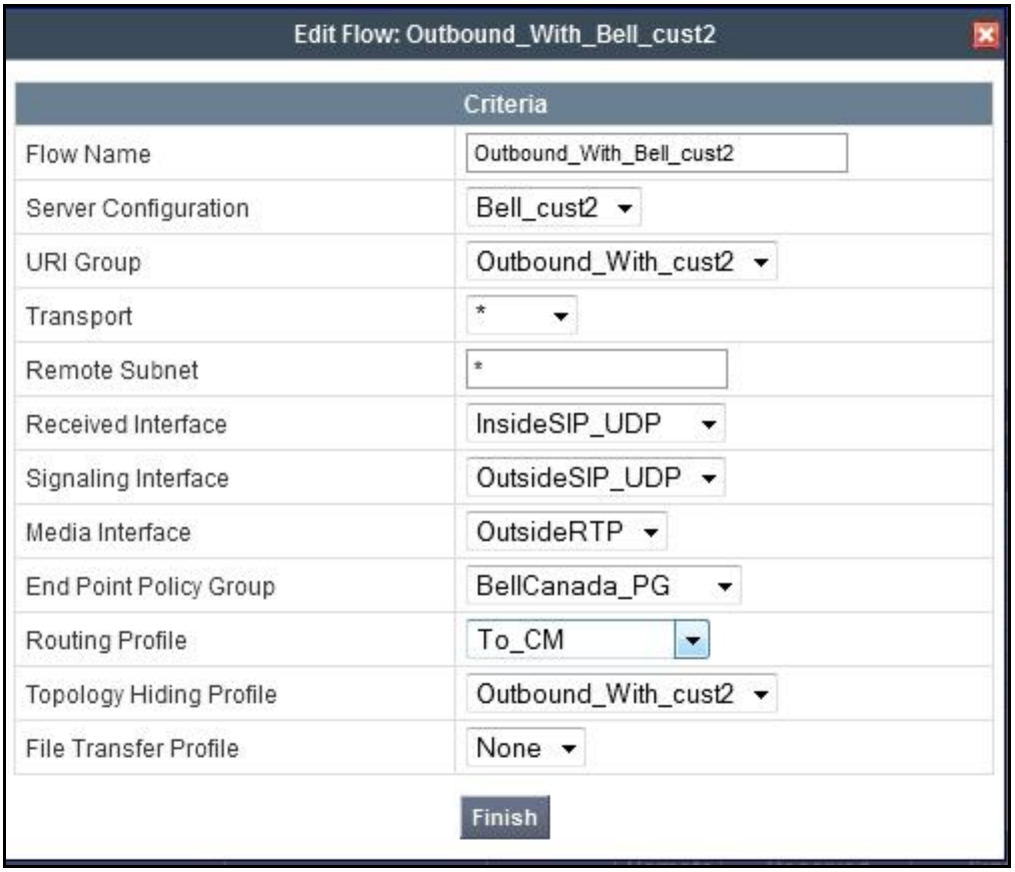
Criteria	
Flow Name	OPTIONS_Bell_cust2
Server Configuration	Bell_cust2
URI Group	OPTIONS_SBCEA
Transport	*
Remote Subnet	*
Received Interface	InsideSIP_UDP
Signaling Interface	OutsideSIP_UDP
Media Interface	OutsideRTP
End Point Policy Group	BellCanada_PG
Routing Profile	To_CM
Topology Hiding Profile	Outbound_With_cust2
File Transfer Profile	None



Edit Flow: Inbound

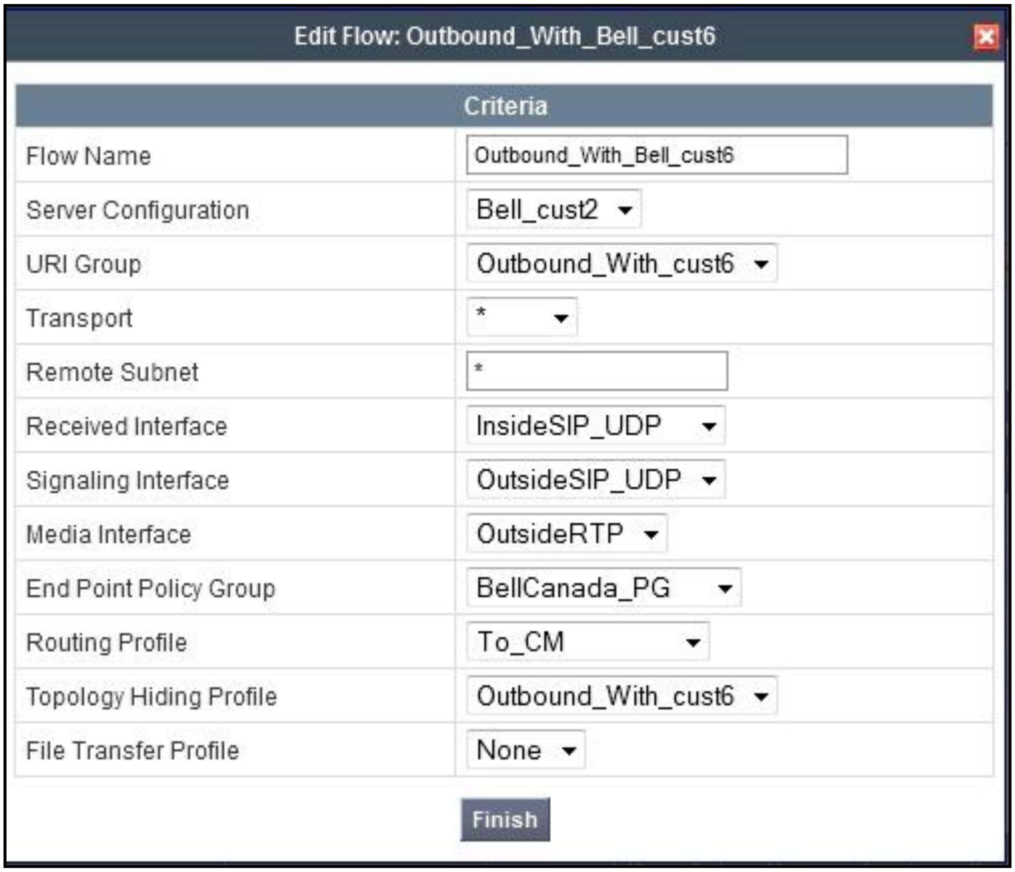
Criteria

Flow Name	Inbound
Server Configuration	Bell_cust2
URI Group	Inbound
Transport	*
Remote Subnet	*
Received Interface	InsideSIP_UDP
Signaling Interface	OutsideSIP_UDP
Media Interface	OutsideRTP
End Point Policy Group	BellCanada_PG
Routing Profile	To_CM
Topology Hiding Profile	Outbound_With_cust2
File Transfer Profile	None



Edit Flow: Outbound_With_Bell_cust2

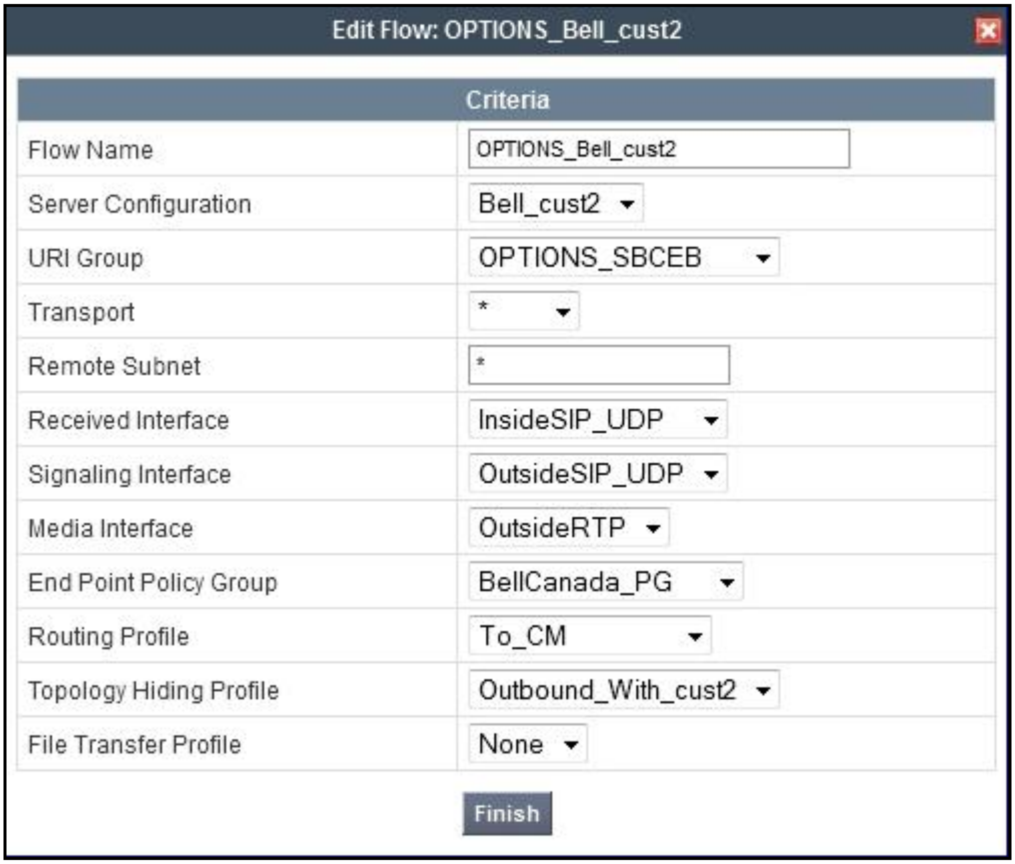
Criteria	
Flow Name	Outbound_With_Bell_cust2
Server Configuration	Bell_cust2
URI Group	Outbound_With_cust2
Transport	*
Remote Subnet	*
Received Interface	InsideSIP_UDP
Signaling Interface	OutsideSIP_UDP
Media Interface	OutsideRTP
End Point Policy Group	BellCanada_PG
Routing Profile	To_CM
Topology Hiding Profile	Outbound_With_cust2
File Transfer Profile	None



Edit Flow: Outbound_With_Bell_cust6

Criteria	
Flow Name	Outbound_With_Bell_cust6
Server Configuration	Bell_cust2
URI Group	Outbound_With_cust6
Transport	*
Remote Subnet	*
Received Interface	InsideSIP_UDP
Signaling Interface	OutsideSIP_UDP
Media Interface	OutsideRTP
End Point Policy Group	BellCanada_PG
Routing Profile	To_CM
Topology Hiding Profile	Outbound_With_cust6
File Transfer Profile	None

Use the procedure to replicate the same Server Flows **OPTIONS_Bell_cust2**, **Inbound**, **Outbound_With_cust2** and **Outbound_With_cust6** to the secondary Avaya SBCE for the primary Bell Canada CO (not shown). **Note**: There is one exception of the URI Group **OPTIONS_ SBCB** which was created in **Section 7.2.1** was set to the Server Flow **OPTIONS_Bell_cust2** as shown below.



Edit Flow: OPTIONS_Bell_cust2

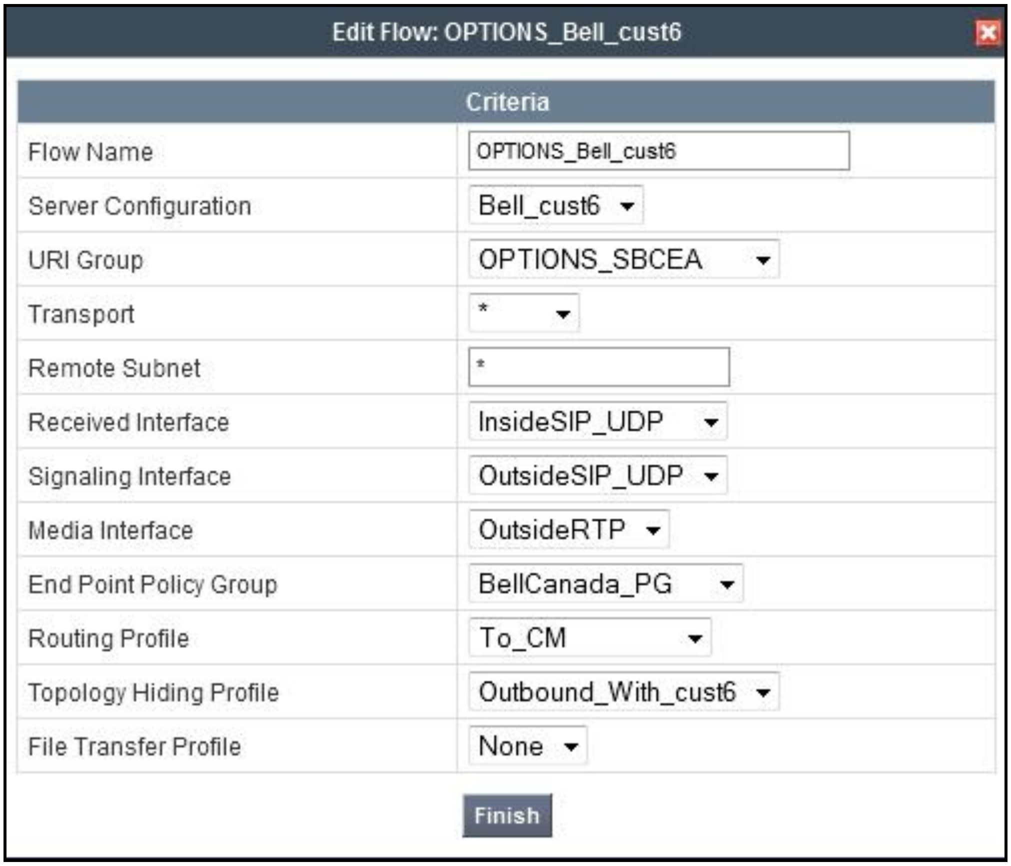
Criteria	
Flow Name	OPTIONS_Bell_cust2
Server Configuration	Bell_cust2
URI Group	OPTIONS_SBCEB
Transport	*
Remote Subnet	*
Received Interface	InsideSIP_UDP
Signaling Interface	OutsideSIP_UDP
Media Interface	OutsideRTP
End Point Policy Group	BellCanada_PG
Routing Profile	To_CM
Topology Hiding Profile	Outbound_With_cust2
File Transfer Profile	None

7.4.4.4 Server Flows for the Secondary Bell Canada CO

The Server Flows for the secondary Bell Canada CO were similarly created with the exception of the Server Configuration and Topology Hiding profile settings as following.

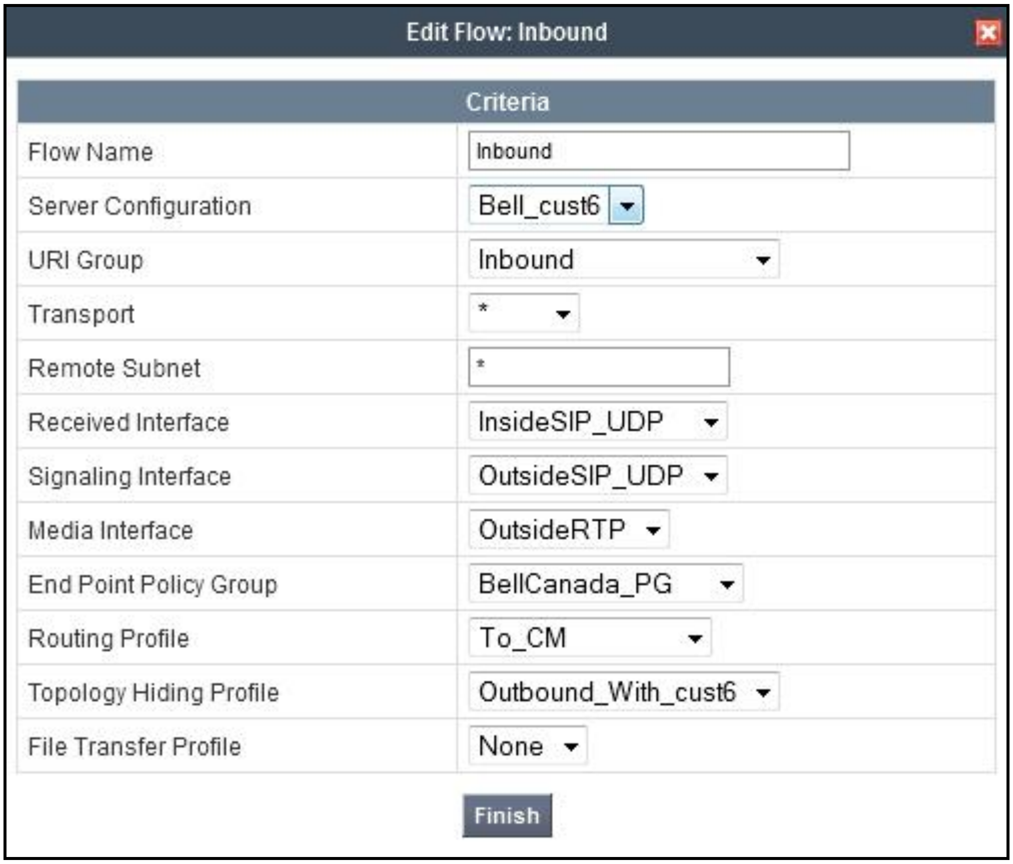
- **Server Configuration:** Select the Server Configuration **Bell_cust6** created in **Section 7.2.6.2**.
- **Topology Hiding Profile:** Select the Topology Hiding profile **Outbound_With_cust2** for the Server Flow with the URI Group **Outbound_With_cust2** and the Topology Hiding profile **Outbound_With_cust6** for the Server Flows with the URI Groups **OPTIONS_SBCA**, **Inbound**, **Outbound_With_cust6**. The Topology Hiding profiles were created in **Section 7.2.3.1**.

The following screen shows the Sever Flows **OPTIONS_Bell_cust6**, **Inbound**, **Outbound_With_cust2** and **Outbound_With_cust6** were created on the primary Avaya SBCE for the secondary Bell Canada CO.



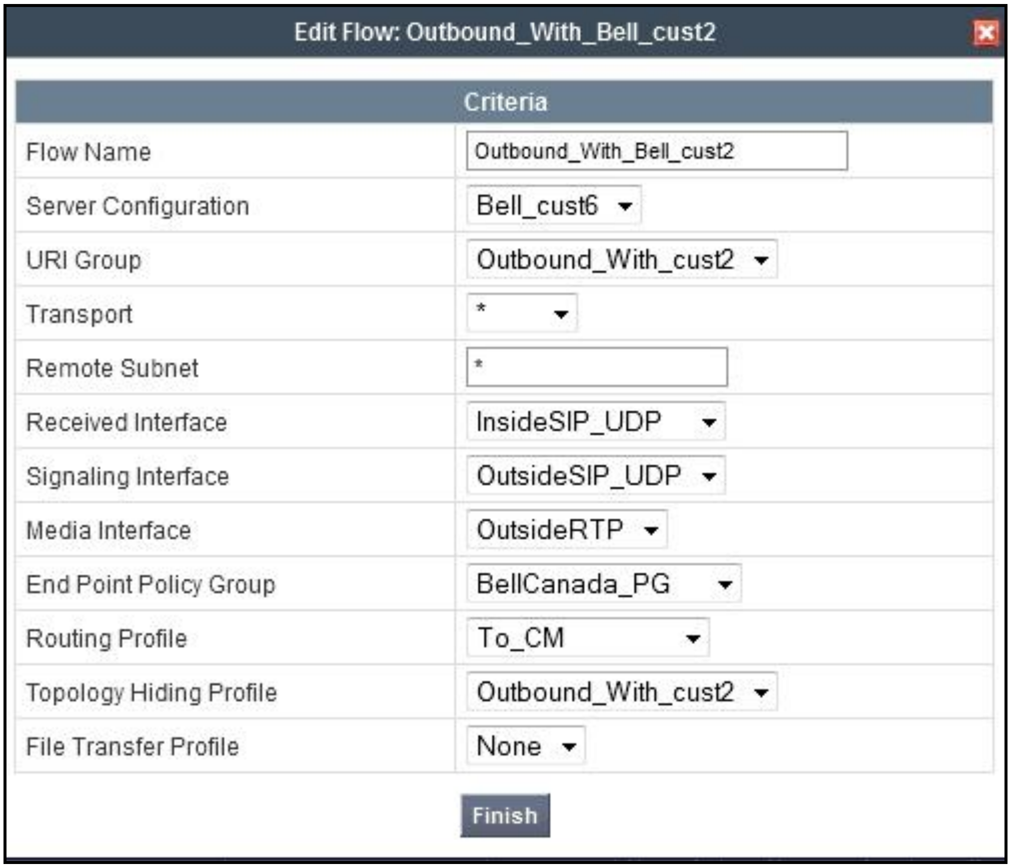
Edit Flow: OPTIONS_Bell_cust6

Criteria	
Flow Name	OPTIONS_Bell_cust6
Server Configuration	Bell_cust6
URI Group	OPTIONS_SBCEA
Transport	*
Remote Subnet	*
Received Interface	InsideSIP_UDP
Signaling Interface	OutsideSIP_UDP
Media Interface	OutsideRTP
End Point Policy Group	BellCanada_PG
Routing Profile	To_CM
Topology Hiding Profile	Outbound_With_cust6
File Transfer Profile	None



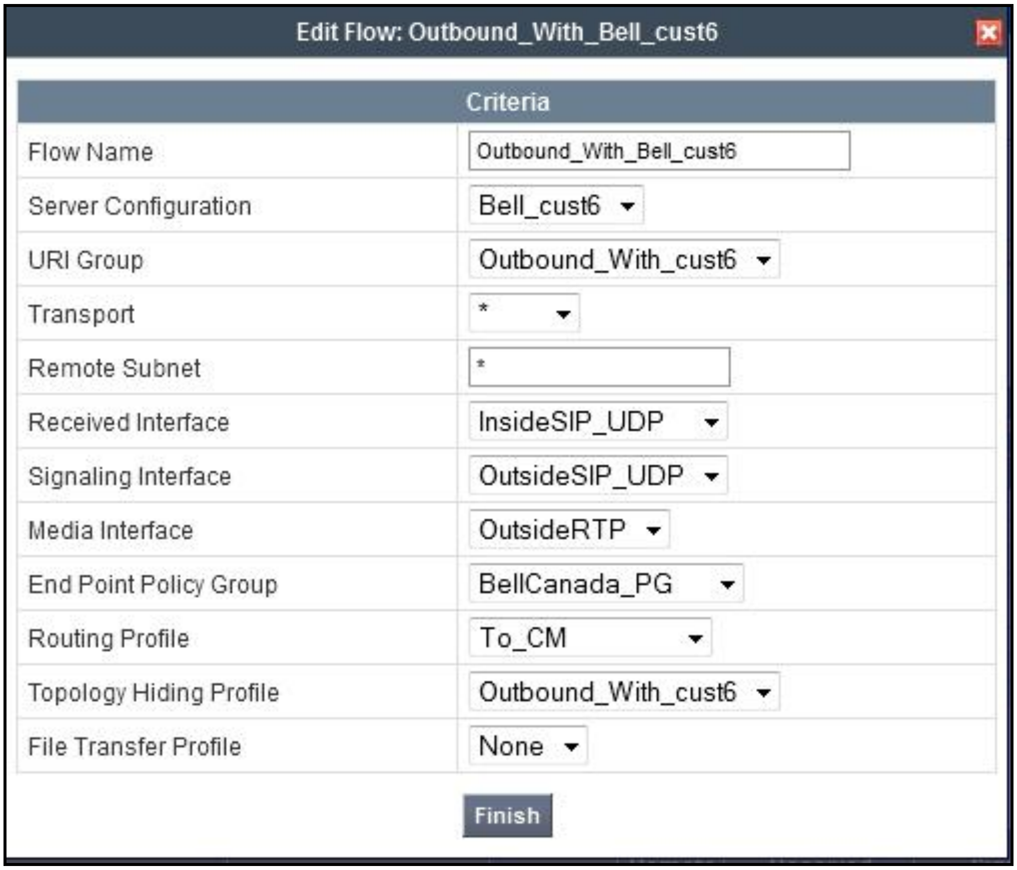
Edit Flow: Inbound

Criteria	
Flow Name	Inbound
Server Configuration	Bell_cust6
URI Group	Inbound
Transport	*
Remote Subnet	*
Received Interface	InsideSIP_UDP
Signaling Interface	OutsideSIP_UDP
Media Interface	OutsideRTP
End Point Policy Group	BellCanada_PG
Routing Profile	To_CM
Topology Hiding Profile	Outbound_With_cust6
File Transfer Profile	None



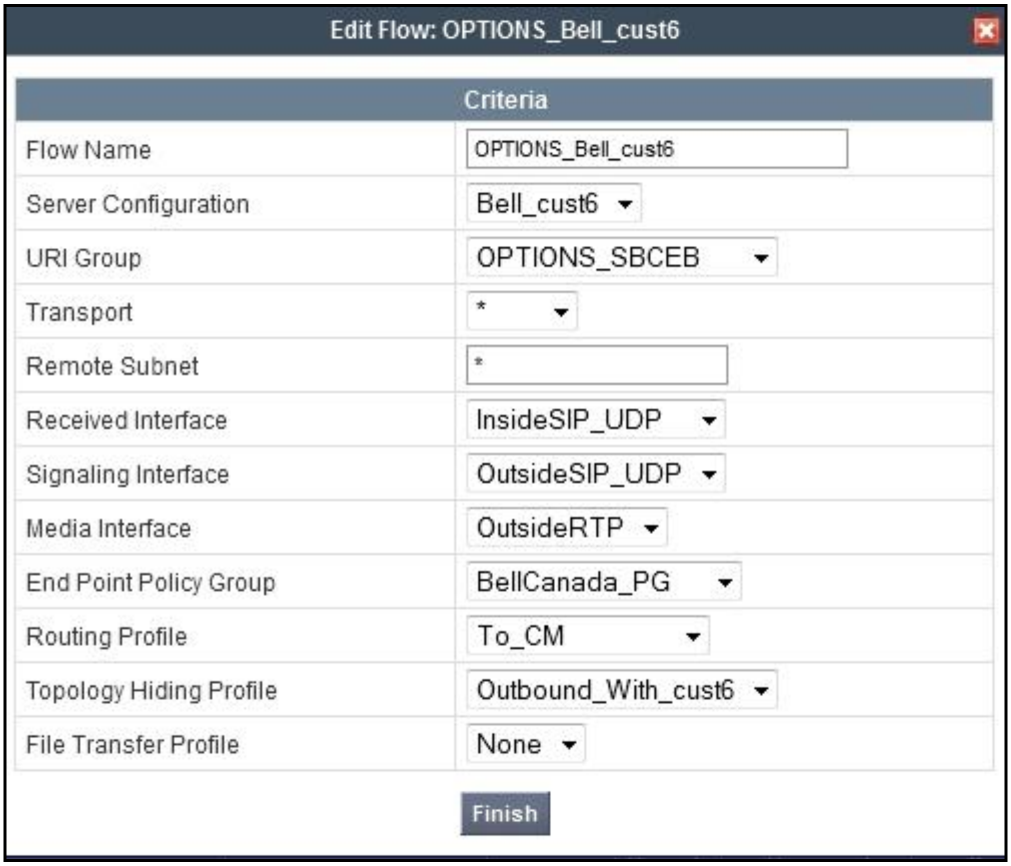
Edit Flow: Outbound_With_Bell_cust2

Criteria	
Flow Name	Outbound_With_Bell_cust2
Server Configuration	Bell_cust6
URI Group	Outbound_With_cust2
Transport	*
Remote Subnet	*
Received Interface	InsideSIP_UDP
Signaling Interface	OutsideSIP_UDP
Media Interface	OutsideRTP
End Point Policy Group	BellCanada_PG
Routing Profile	To_CM
Topology Hiding Profile	Outbound_With_cust2
File Transfer Profile	None



Criteria	
Flow Name	Outbound_With_Bell_cust6
Server Configuration	Bell_cust6
URI Group	Outbound_With_cust6
Transport	*
Remote Subnet	*
Received Interface	InsideSIP_UDP
Signaling Interface	OutsideSIP_UDP
Media Interface	OutsideRTP
End Point Policy Group	BellCanada_PG
Routing Profile	To_CM
Topology Hiding Profile	Outbound_With_cust6
File Transfer Profile	None

Use the procedure to replicate the same Server Flows **OPTIONS_Bell_cust6**, **Inbound**, **Outbound_With_cust2** and **Outbound_With_cust6** to the secondary Avaya SBCE for the secondary Session Manager (not shown). **Note**: There is one exception of the URI Group **OPTIONS_ SBCB** which was created in **Section 7.2.1** was set to the Server Flow **OPTIONS_Bell_cust6** as shown below.



Edit Flow: OPTIONS_Bell_cust6

Criteria	
Flow Name	OPTIONS_Bell_cust6
Server Configuration	Bell_cust6
URI Group	OPTIONS_SBCEB
Transport	*
Remote Subnet	*
Received Interface	InsideSIP_UDP
Signaling Interface	OutsideSIP_UDP
Media Interface	OutsideRTP
End Point Policy Group	BellCanada_PG
Routing Profile	To_CM
Topology Hiding Profile	Outbound_With_cust6
File Transfer Profile	None

7.4.5 Session Flow

The Session Flows feature allows the user to define certain parameters that pertain to the media portions of a call, whether it originates from within the enterprise or from without. Session Flow profiles SDP media parameters, to identify and characterize a call placed through the network.

Create a common Session Flow **BellCanada_SF** on the primary Avaya SBCE to be used for both enterprise and Bell Canada.

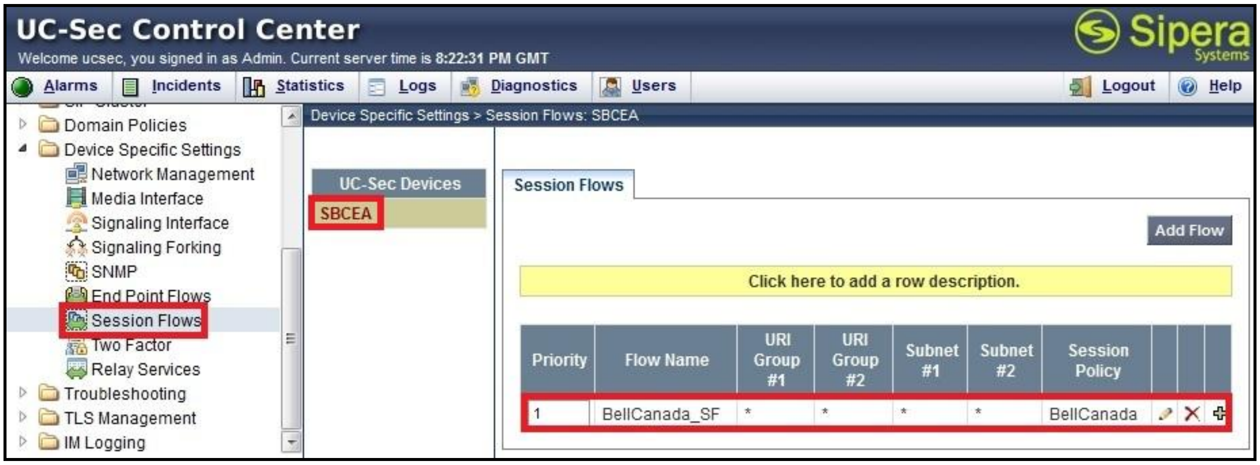
To create a Session Flow, navigate to **UC-Sec Control Center → Device Specific Settings → Session Flows**. Click **Add Flow** (not shown).

In the new window that appears, enter the following values:

- **Flow Name:** Enter a descriptive name.
- **Session Policy:** Select the Session Policy **BellCanada_SP** created in **Section 7.3.5**.

Use default values for all remaining fields and click **Finish** to save.

The following screen shows the Session Flow **BellCanada_SF** created on the primary Avaya SBCE.



Priority	Flow Name	URI Group #1	URI Group #2	Subnet #1	Subnet #2	Session Policy
1	BellCanada_SF	*	*	*	*	BellCanada

Use the procedure to replicate the same Session Flow **BellCanada_SF** to the secondary Avaya SBCE (not shown).

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 Bell Canada networks. The provided information from Bell Canada includes:

- IP address of Bell Canada SIP proxies for the primary and secondary CO.
- Trunk group identification parameters for Least Cost Routing feature.
- Service provider public SIP domains.
- CPE SIP domains.
- User and password for Digest Authentication.
- Supported codecs.
- DID numbers.
- IP addresses and port numbers used for signaling or media through any security devices.
- A customer specific SIP signaling reference.

The sample configuration between Bell Canada and the enterprise for the compliance testing is a static configuration. There is no registration of the SIP Trunk or enterprise users to Bell Canada networks.

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 commands that can be used to troubleshoot the solution.

9.1 Verification Steps

The following activities are made to each test scenario:

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

9.2 Protocol Traces

The following SIP message headers are inspected using sniffer traces:

- Request-URI: Verify the request number and SIP domain.
- From: Verify the display name and display number.
- To: Verify the display name and display number.
- P-Asserted-Identity: Verify the display name and display number.
- Privacy: Verify privacy masking with “user, id”.
- Diversion: Verify DID number.
- Authorization: Verify Digest Authentication implementation.

The following attributes in SIP message body are inspected using sniffer traces:

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

9.3 Troubleshooting

9.3.1 The Avaya SBCE

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

Following screenshots show an example of an 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 220.20.237.205:5060;branch=z9hG4bKenr6sr2010l1sjsrl0s0.1
From: "MTS x1226"<sip:+1647XXX1226@sipxxxxxxxx.bell.ca;user=phone>;tag=SDajfhb01-
1669741437-1355429209774-
To: "Bell Demo12345"<sip:416XXX1880@cust6xxxx.xxxx.bell.ca>
Call-ID: SDajfhb01-e838ddb48d0145a0c65d9c52640c0e31-a0n8330
CSeq: 183513944 INVITE
Contact: <sip:+1647XXX1226@220.20.237.205:5060;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: 188

v=0
o=BroadWorks 3454967 1 IN IP4 220.20.237.205
s=-
c=IN IP4 220.20.237.205
t=0 0
m=audio 21842 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: "MTS x1226" <sip:1647XXX1226@sipxxxxxxxx.bell.ca;user=phone>;tag=SDajfhb01-
1669741437-1355429209774-
To: "Bell Demo12345"
<sip:416XXX1880@cust6xxxx.xxxx.bell.ca>;tag=804e19b55b53e21bb2850e1848d00
CSeq: 183513944 INVITE
Call-ID: SDajfhb01-e838ddb48d0145a0c65d9c52640c0e31-a0n8330
Contact: "Bell x1880" <sip:416XXX1880;tgrp=;trunk-
context=sipxxxxxxxx.bell.ca@10.10.98.116:5060;transport=udp;user=phone>
Record-Route: <sip:10.10.98.116:5060;ipcs-line=58518;lr;transport=udp>
Allow: INVITE,ACK,OPTIONS,BYE,CANCEL,SUBSCRIBE,NOTIFY,REFER,INFO,PRACK,PUBLISH
Supported: 100rel, join, replaces, sdp-anat, timer
Via: SIP/2.0/UDP 220.20.237.205:5060;branch=z9hG4bKenr6sr2010l1sjsrl0s0.1
Accept-Language: en
Require: timer
Server:  Avaya CM/R016x.00.1.510.1 AVAYA-SM-6.1.7.0.617012
P-Asserted-Identity: "Bell x1880"
<sip:416XXX1880@cust6xxxx.xxxx.bell.ca;user=phone>
Session-Expires: 180;refresher=uas
Content-Type: application/sdp
P-Location: SM;origlocname="Belleville";termlocname="Belleville"
Content-Length: 175

v=0
o=- 1355429213 2 IN IP4 10.10.98.116
s=-
c=IN IP4 10.10.98.116
```

```
b=AS:64
t=0 0
m=audio 35482 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:16477761232@sipxxxxxxxx.bell.ca;user=phone SIP/2.0
From: "Bell x1881"
<sip:416XXX1881@cust6xxxx.xxxx.bell.ca;user=phone>;tag=056306e6553e21792950e1848d00
To: <sip:16477761232@sipxxxxxxxx.bell.ca;user=phone>
CSeq: 1 INVITE
Call-ID: 5efeac5ce759ae55ed0ae30028394c34
Contact: "Bell x1881" <sip:416XXX1881;tgrp=vsxx_416XXX1880_01a;trunk-
context=sipxxxxxxxx.bell.ca@10.10.98.116:5060;user=phone>
Record-Route: <sip:10.10.98.116:5060;ipcs-line=60039;lr;transport=udp>
Allow: INVITE,ACK,OPTIONS,BYE,CANCEL,SUBSCRIBE,NOTIFY,REFER,INFO,PRACK,PUBLISH
Supported: 100rel, join, replaces, sdp-anat, timer
User-Agent:  Avaya CM/R016x.00.1.510.1 AVAYA-SM-6.1.7.0.617012
Max-Forwards: 66
Via: SIP/2.0/UDP 10.10.98.116:5060;branch=z9hG4bK-s1632-000241999525-1--s1632-
Accept-Language: en
Alert-Info: <cid:internal@vsxx-416XXX1880-01a.avayalab.com>;avaya-cm-alert-
type=internal
P-Asserted-Identity: "Bell x1881"
<sip:416XXX1881@cust6xxxx.xxxx.bell.ca;user=phone>
Session-Expires: 180;refresher=uac
Min-SE: 180
Content-Type: application/sdp
P-Charging-Vector: icid-value="AAS:555-6e3056001e25365e15029788d84"
P-Location: SM;origlocname="Belleville";termlocname="Belleville"
Content-Length: 210

v=0
o=- 1355433390 1 IN IP4 10.10.98.116
s=-
c=IN IP4 10.10.98.116
b=AS:64
t=0 0
a=avf:avc=n prio=n
a=csup:avf-v0
m=audio 35494 RTP/AVP 0 101
a=rtpmap:0 PCMU/8000
a=rtpmap:101 telephone-event/8000
```

- Incoming 401 challenge to request the Digest Authentication.

```
SIP/2.0 401 Unauthorized
From: "Bell x1881"
<sip:416XXX1881@cust6xxxx.xxxx.bell.ca;user=phone>;tag=056306e6553e21792950e1848d0
0
```

```
To: <sip:16477761232@sipxxxxxxxx.bell.ca;user=phone>;tag=SDepmq999-1390711843-
1355433390679
CSeq: 1 INVITE
Call-ID: 5efeac5ce759ae55ed0ae30028394c34
Via: SIP/2.0/UDP 10.10.98.116:5060;branch=z9hG4bK-s1632-000241999525-1--s1632-
WWW-Authenticate: DIGEST
qop="auth",nonce="BroadWorksXhaoe1lqvT25rahnBW",realm="sipxxxxxxxx.bell.ca",algori
thm=MD5
Content-Length: 0
```

- Outgoing subsequent INVITE with Authorization header to respond to the Digest Authentication.

```
INVITE sip:16477761232@sipxxxxxxxx.bell.ca;user=phone SIP/2.0
From: "Bell x1881"
<sip:416XXX1881@cust6xxxx.xxxx.bell.ca;user=phone>;tag=056306e6553e21792950e1848d00
To: <sip:16477761232@sipxxxxxxxx.bell.ca;user=phone>
CSeq: 2 INVITE
Call-ID: 5efeac5ce759ae55ed0ae30028394c34
Contact: "Bell x1881" <sip:416XXX1881;tgrp=vsxx_416XXX1880_01a;trunk-
context=sipxxxxxxxx.bell.ca@10.10.98.116:5060;user=phone>
Record-Route: <sip:10.10.98.116:5060;ipcs-line=60039;lr;transport=udp>
Allow: INVITE,ACK,OPTIONS,BYE,CANCEL,SUBSCRIBE,NOTIFY,REFER,INFO,PRACK,PUBLISH
Supported: 100rel, join, replaces, sdp-anat, timer
User-Agent:  Avaya CM/R016x.00.1.510.1 AVAYA-SM-6.1.7.0.617012
Max-Forwards: 66
Via: SIP/2.0/UDP 10.10.98.116:5060;branch=z9hG4bK-s1632-002049921300-1--s1632-
Accept-Language: en
Alert-Info: <cid:internal@vsxx-416XXX1880-01a.avayalab.com>;avaya-cm-alert-
type=internal
Authorization: Digest username="avaya", realm="sipxxxxxxxx.bell.ca",
nonce="BroadWorksXhaoe1lqvT25rahnBW", uri="sip:vsxx_416XXX1880_01a",
response="2cb88978ada3c7a2ca3eaf082825e7b1", algorithm=MD5, cnonce="0a4f113b",
qop=auth, nc=00000001
P-Asserted-Identity: "Bell x1881"
<sip:416XXX1881@cust6xxxx.xxxx.bell.ca;user=phone>
Session-Expires: 180;refresher=uac
Min-SE: 180
Content-Type: application/sdp
P-Charging-Vector: icid-value="AAS:555-6e3056001e25365e15029788d84"
P-Location: SM;origlocname="Belleville";termlocname="Belleville"
Content-Length: 210

v=0
o=- 1355433390 1 IN IP4 10.10.98.116
s=-
c=IN IP4 10.10.98.116
b=AS:64
t=0 0
a=avf:avc=n prio=n
a=csup:avf-v0
m=audio 35494 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 x1881"
<sip:416XXX1881@cust6xxxx.xxxx.bell.ca;user=phone>;tag=056306e6553e21792950e1848d00
To: <sip:16477761232@sipxxxxxxxx.bell.ca;user=phone>;tag=SDepmq999-78691848-
1355433391612
CSeq: 2 INVITE
Call-ID: 5efeac5ce759ae55ed0ae30028394c34
Via: SIP/2.0/UDP 10.10.98.116:5060;branch=z9hG4bK-s1632-002049921300-1--s1632-
Record-Route: <sip:10.10.98.116:5060;ipcs-line=60039;lr;transport=udp>
Supported:
Contact: <sip:16477761232@220.20.237.201:5060;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: 188

v=0
o=BroadWorks 3479278 1 IN IP4 220.20.237.201
s=-
c=IN IP4 220.20.237.201
t=0 0
m=audio 20844 RTP/AVP 0 8 18 101
a=ptime:20
a=rtpmap:101 telephone-event/8000
a=fmtp:101 0-15
```

9.3.2 Avaya Aura® Communication Manager

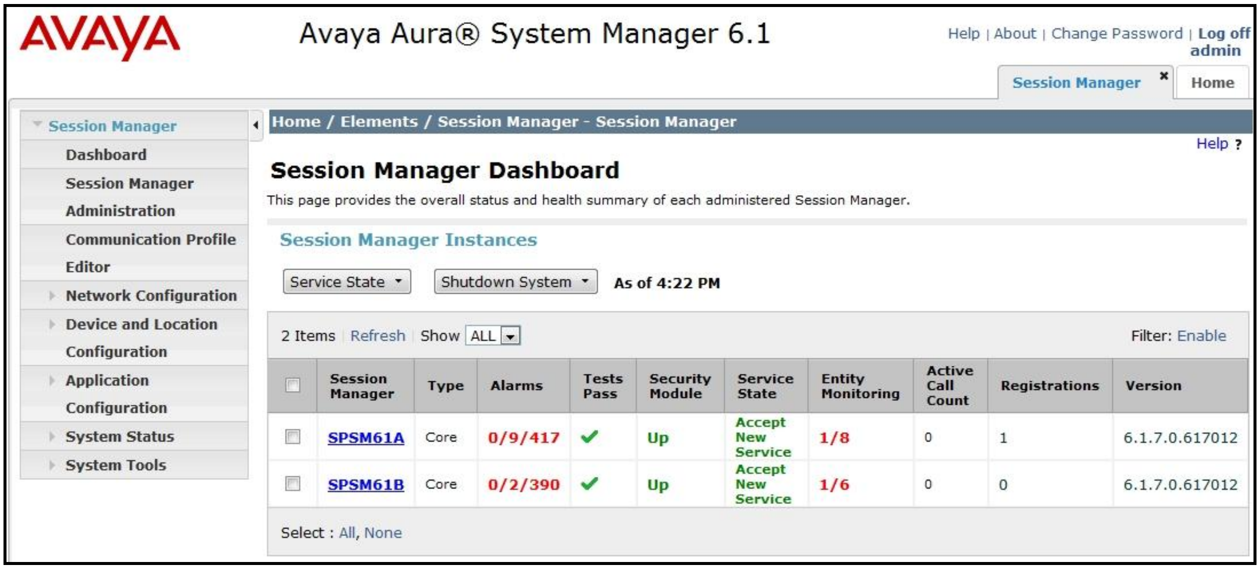
The followings are examples of the commands available on Communication Manager to trace the call when it is in progress.

- **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 Avaya Aura® Session Manager

The followings are examples of the troubleshooting procedure on 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**.


AVAYA
Avaya Aura® System Manager 6.1
Help | About | Change Password | Log off
admin
Session Manager
Home
Session Manager
Dashboard
Session Manager Administration
Communication Profile Editor
Network Configuration
Device and Location Configuration
Application Configuration
System Status
System Tools

Home / Elements / Session Manager - Session Manager

Help ?

Session Manager Dashboard

This page provides the overall status and health summary of each administered Session Manager.

Session Manager Instances

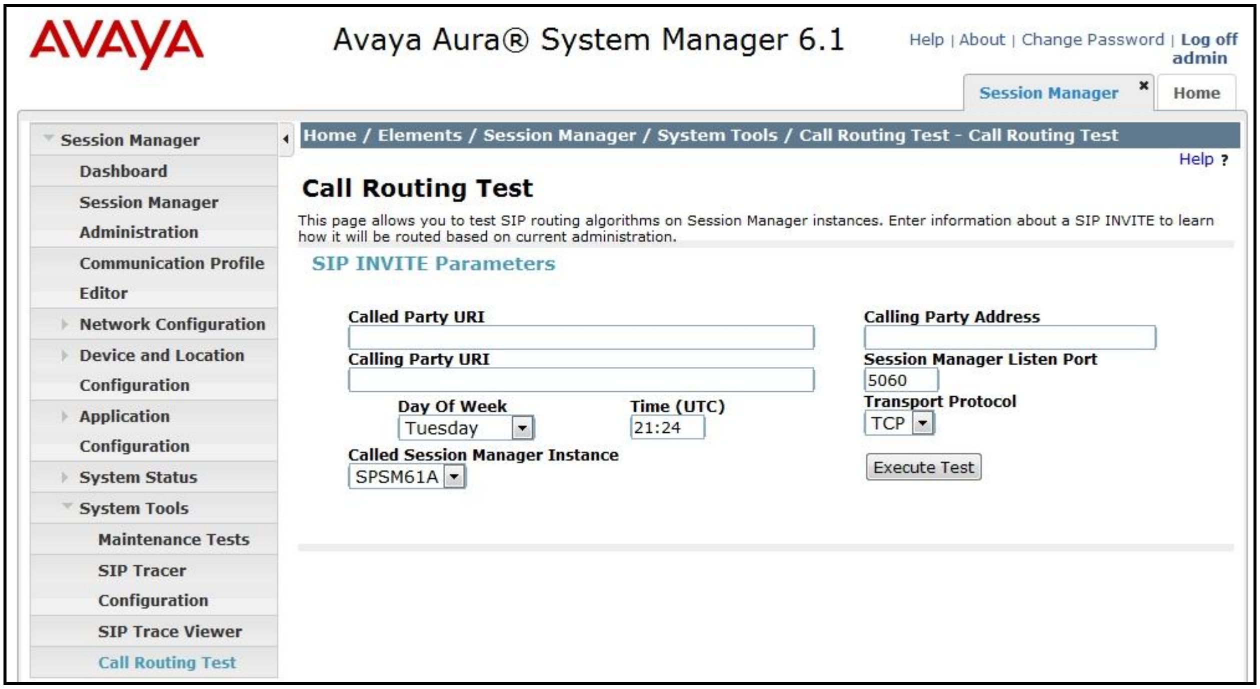
Service State ▾ Shutdown System ▾ As of 4:22 PM

2 Items | Refresh | Show ALL ▾ Filter: Enable

□	Session Manager	Type	Alarms	Tests Pass	Security Module	Service State	Entity Monitoring	Active Call Count	Registrations	Version
□	SPSM61A	Core	0/9/417	✓	Up	Accept New Service	1/8	0	1	6.1.7.0.617012
□	SPSM61B	Core	0/2/390	✓	Up	Accept New Service	1/6	0	0	6.1.7.0.617012

Select : All, None

- **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** as shown below. Enter the requested data to run the test.


AVAYA
Avaya Aura® System Manager 6.1
Help | About | Change Password | Log off
admin
Session Manager
Home
Session Manager
Dashboard
Session Manager Administration
Communication Profile Editor
Network Configuration
Device and Location Configuration
Application Configuration
System Status
System Tools
Maintenance Tests
SIP Tracer Configuration
SIP Trace Viewer
Call Routing Test
Execute Test

Home / Elements / Session Manager / System Tools / Call Routing Test - Call Routing Test

Help ?

Call Routing Test

This page allows you to test SIP routing algorithms on Session Manager instances. Enter information about a SIP INVITE to learn how it will be routed based on current administration.

SIP INVITE Parameters

Called Party URI:
Calling Party URI:
Day Of Week: Tuesday
Time (UTC): 21:24
Called Session Manager Instance: SPSM61A
Calling Party Address:
Session Manager Listen Port: 5060
Transport Protocol: TCP

10. Conclusion

These Application Notes describe the configuration necessary to connect Avaya Aura® Communication Manager 6.0.1, geographic redundant Avaya Aura® Session Managers 6.1 and geographic redundant Avaya Session Border Controllers for Enterprise 4.0.5 to Bell Canada SIP Trunking Service. Bell Canada SIP Trunking Service is a SIP-based Voice over IP solution for customers ranging from small businesses to large enterprises. Bell Canada SIP Trunking Service provides a flexible, cost-saving alternative to traditional hardwired telephony trunks.

All of the test cases have been executed. Despite the number of observations seen during testing as noted in **Section 2.2**, the test results met the objectives outlined in **Section 2.1**. Bell Canada SIP Trunking Service is considered **compliant** with Avaya Aura® Communication Manager 6.0.1, geographic redundant Avaya Aura® Session Managers 6.1 and geographic redundant Avaya Session Border Controllers for Enterprise 4.0.5.

11. References

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

[1] *Installing and Configuring Avaya Aura® System Platform*, Release 6.03, February 2011.

[2] *Administering Avaya Aura® System Platform*, Release 6, June 2010.

[3] *Administering Avaya Aura® Communication Manager*, Release 6.0, June 2010, Document Number 03-300509.

[4] *Avaya Aura® Communication Manager Feature Description and Implementation,* Release 6.0, June 2010, Document Number 555-245-205.

[5] *Installing and Upgrading Avaya Aura® System Manager*, Release 6.1, November 2010.

[6] *Installing and Configuring Avaya Aura® Session Manager*, Release 6.1, April 2011, Document Number 03-603473.

[7] *Administering Avaya Aura® Session Manager*, Release 6.1, May 2011, Document Number 03-603324.

[8] *Avaya one-X® Deskphone Edition for 9600 Series IP Telephones Administrator Guide*, Release 3.1, November 2009, Document Number 16-300698.

[9] *Avaya one-X® Deskphone SIP for 9600 Series IP Telephones Administrator Guide*, Release 2.6, June 2010, Document Number 16-601944.

[10] *Administering Avaya one-X® Communicator*, April 2011.

[11] *Using Avaya one-X® Communicator*, April 2011.

[12] *UC-Sec Install Guide (102-5224-400v1.01).*

[13] *UC-Sec Administration Guide (010-5423-400v106).*

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

[15] *RFC 3515, The Session Initiation Protocol (SIP) Refer Method, http://www.ietf.org/.*

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

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

The information provided in these Application Notes is subject to change without notice. The configurations, technical data, and recommendations provided in these Application Notes are believed to be accurate and dependable, but are presented without express or implied warranty. Users are responsible for their application of any products specified in these Application Notes.

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.