Avaya Solution & Interoperability Test Lab

Application Notes for Configuring Avaya Aura® Communication Manager Rel. 7.0, Avaya Aura® Session Manager Rel. 7.0 and Avaya Session Border Controller for Enterprise Rel. 7.2 to support Telmex SIP Trunk Service using TLS – Issue 1.0

Abstract

These Application Notes describe the procedures for configuring Session Initiation Protocol (SIP) Trunk Service on an enterprise solution consisting of Avaya Aura® Communication Manager Rel. 7.0, Avaya Aura® Session Manager Rel. 7.0 and Avaya Session Border Controller for Enterprise Rel. 7.2, to interoperate with the Telmex SIP Trunk service using TLS.

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

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

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

Table of Contents

1. Introduction

These Application Notes describe the procedures for configuring Session Initiation Protocol (SIP) Trunk Service between the Telmex network and an Avaya SIP-enabled enterprise solution using Transport Layer Security (TLS). The Avaya solution consists of Avaya Aura® Communication Manager Rel. 7.0 (Communication Manager), Avaya Aura® Session Manager Rel. 7.0 (Session Manager), Avaya Session Border Controller for Enterprise Rel. 7.2 (Avaya SBCE) and various Avaya endpoints, listed in **Section 4**.

For privacy, TLS for Signaling and SRTP for media encryption were used inside of the enterprise (private network side) and outside of the enterprise (public network side).

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

The terms "Service Provider" and "Telmex" will be used interchangeably throughout these Application Notes.

2. General Test Approach and Test Results

The general test approach was to simulate an enterprise site at the Telmex facility in Mexico by connecting the Avaya SIP-enabled enterprise solution to Telmex's network, as depicted in **Figure 1**.

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

2.1. Interoperability Compliance Testing

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

- Static IP SIP Trunk authentication.
- Response to SIP OPTIONS queries.
- Incoming PSTN calls to various phone types. Phone types included H.323, SIP, digital, and analog telephones at the enterprise. All inbound calls from the PSTN were routed to the enterprise across the SIP trunk from the service provider.
- Outgoing PSTN calls from various phone types. Phone types included H.323, SIP, digital, and analog telephones at the enterprise. All outbound calls to the PSTN were routed from the enterprise across the SIP trunk via the service provider network.
- Inbound and outbound PSTN calls to/from Avaya one-X® Communicator softphones using "This Computer" and "Other Phone" modes. (H.323, SIP).
- Inbound and outbound PSTN calls to/from Avaya Equinox softphones (SIP).
- Codec G.729, currently the only codec supported by Telmex.
- DTMF tones passed as out-of-band RTP events as per RFC 2833.
- Caller ID presentation and Caller ID restriction.
- Voicemail redirection and navigation.
- User features such as hold and resume, transfer and conference.
- Off-net call transferring, call forwarding and mobility (extension to cellular).
- Routing inbound PSTN calls to call center agent queues.
- Proper response/error treatment to different failure conditions.

The following items were not tested:

- Remote Worker was not tested.
- Inbound toll-free calls, 911 calls (emergency), "0" calls (Operator), 0+10 digits calls (Operator Assisted), were not tested.
- G.711 pass-through fax was not tested.
- T.38 fax is not currently supported by Telmex; therefore T.38 fax was not tested.
- SIP REFER is not currently supported by Telmex; therefore SIP REFER was not tested.

2.2. Test Results

Interoperability testing of the Telmex SIP Trunk Service with the Avaya SIP-enabled enterprise solution was completed successfully with the observations/limitations noted below:

- **DTMF tones on H.323 end-points not recognized** – When attempting to login into PSTN voicemail systems from the enterprise using H.323 endpoints the DTMF tones were not recognized. This issue was solved by Telmex with the addition of "midcall-signaling block" to the Cisco CUBE configuration to allow DTMF pass-through. This issue was only seen on H.323 endpoints, this behavior was not seen on SIP endpoints.
- **Outbound Calling Party Number (CPN) Block**: To support outbound privacy calls (calling party number blocking), Communication Manager sends "anonymous" as the calling number in the SIP From header, uses the P-Asserted-Identity (PAI) header to pass the actual calling party number and includes "Privacy: id" in the INVITE. During testing this type of call resulted in call failure. For security reasons this feature may not be supported in Mexico.
- **SIP header optimization** – There are multiple SIP headers and parameters used by Communication Manager and Session Manager, some of them Avaya proprietary, that had no significance in the service provider's network. These headers were removed with the purposes of blocking enterprise information from being propagated outside of the enterprise boundaries, to reduce the size of the packets entering the service provider's network and to improve the solution interoperability in general. The following headers were removed from outbound messages using an Adaptation in Session Manager: AV-Global-Session-ID, AV-Correlation-ID, Alert-Info, Endpoint-View, P-AV-Message-Id, P-Charging-Vector and P-Location (**Section 6.4**).

2.3. Support

For support on Telmex SIP Trunk Service visit the corporate Web page at:
http://telmex.com/en/web/empresas

3. Reference Configuration

Figure 1 illustrates the sample Avaya SIP-enabled enterprise solution, connected to the Telmex SIP Trunk Service through a private connection.

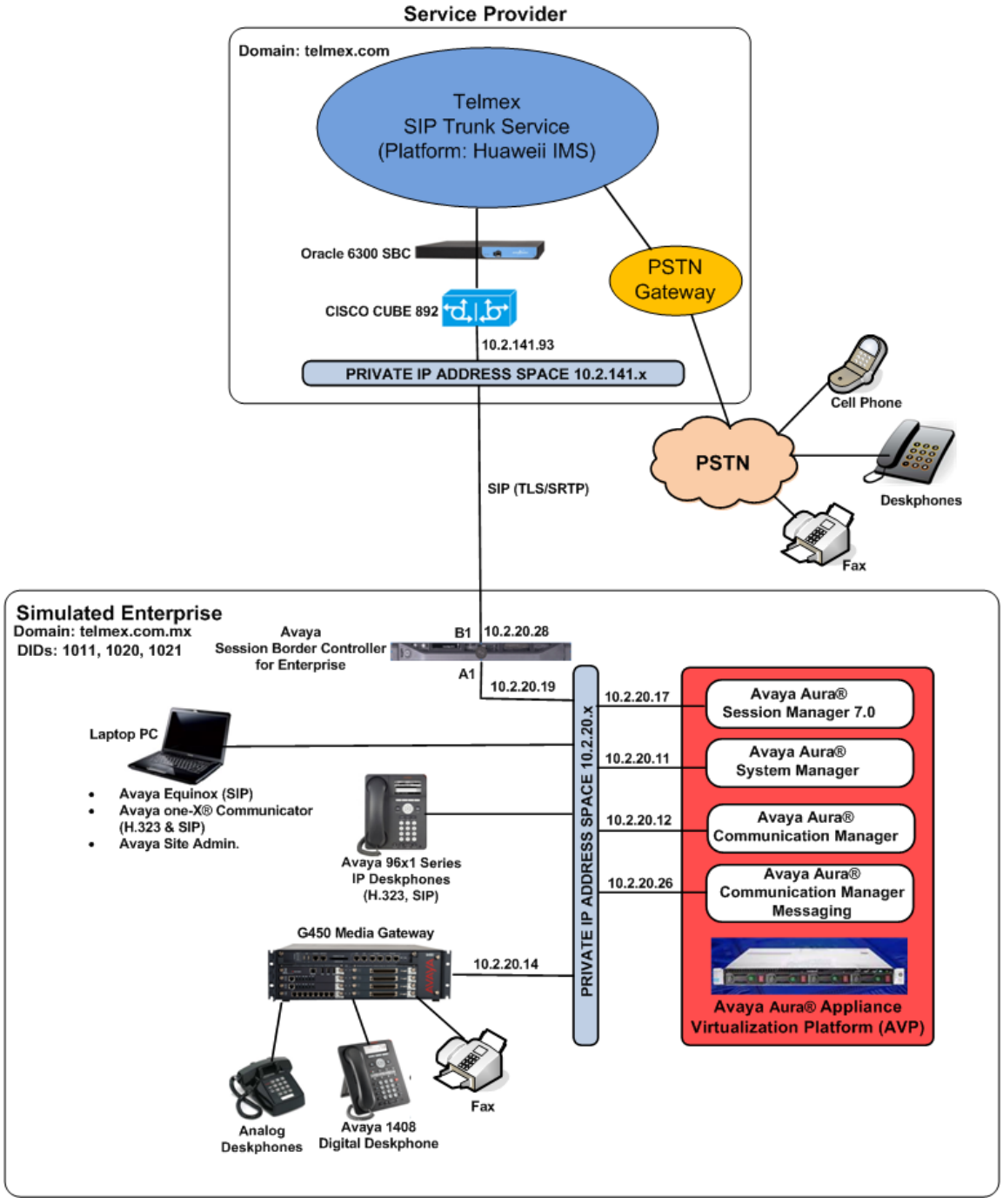


Figure 1: **Avaya SIP Enterprise Solution connected to Telmex SIP Trunk Service**

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

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

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

For inbound calls, the calls flowed from Telmex's network to the Avaya SBCE then to Session Manager. Session Manager used the configured dial patterns (or regular expressions) and routing policies to determine the recipient (in this case Communication Manager) and on which link to send the call. Once the call arrived at Communication Manager, further incoming call treatment, such as incoming digit translation was performed.

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

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

As part of the Avaya Aura® version 7.0 release, Communication Manager incorporates the ability to use the Avaya Aura® Media Sever (AAMS) as a media resource. The AAMS is a software-based, high density media server that provides DSP resources for IP-based sessions. Only Media resources from a G450 Media Gateway were utilized during the compliance test, the AAMS was not included as part of the compliance test, it's mentioned here simply as an option that could be used on customer deployments.

The Avaya Aura® Communication Manager Messaging (CMM) was used during the compliance test to verify voice mail redirection and navigation, as well as the delivery of Message Waiting

Indicator (MWI) messages to the enterprise telephones. Since the configuration tasks for Messaging are not directly related to the interoperability tests with the Telmex network SIP Trunk service, they are not included in these Application Notes.

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

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

For the compliance testing associated with this Application Note, TLS transport for signaling and SRTP for media was used inside of the enterprise (private network side) and outside of the enterprise (public network side).

Note – The configuration tasks required to support security and encryption capabilities, such as TLS certificate management and configuration of Avaya equipment components, are beyond the scope of these Application Notes; hence they are not discussed in this document.

4. Equipment and Software Validated

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

Equipment/Software	Release/Version
Avaya	
Avaya Aura® Appliance Virtualization Platform (AVP)	avaya-avp-7.0.1.0.0.5
Avaya Aura® Communication Manager	CM 7.0.1.2.0.441.23523
Avaya Aura® Session Manager	7.0.1.2.701230
Avaya Aura® System Manager	System Manager 7.0.1.2 Build No. - 7.0.0.0.16266 Software Update Revision No: 7.0.1.2.086007 Service Pack 2
Avaya Session Border Controller for Enterprise running on a DELL R210 V2 Server	ASBCE 7.2 7.2.0.0-18-13712
Avaya Aura® Communication Manager Messaging (CMM)	CMM 7.0.0.1.441.1
Avaya G450 Media Gateway	37.41.0
Avaya 96x1 Series IP Deskphones (SIP)	Version R7_1_0_1-061317
Avaya 96x1 Series IP Deskphones (H.323)	Version R6_6_4_01-102616
Avaya one-X® Communicator (H.323, SIP)	6.2.12.04-SP12
Avaya Equinox (SIP)	3.1.1.18
Avaya 1408 Series Digital Deskphones	46.0
Avaya 6210 Analog Deskphones	N/A
Telmex	
Cisco CUBE C892fsp	15.3(3)m7
Oracle SBC	Unknown
Huawei IMS	Unknown

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

Note – The Avaya Aura® servers used in the reference configuration, except for the Avaya Session Border Controller for Enterprise, as shown on the previous table, were deployed on an Avaya Aura® Appliance virtualization Platform (AVP). These Avaya components ran as virtual machines on an Avaya-supplied server, over a customized OEM version of VMware® (ESXi 5.5.). Consult the installation documentation on the **References** section for more information. The Avaya Session Border Controller for Enterprise was deployed on a DELL R210 V2 Server.

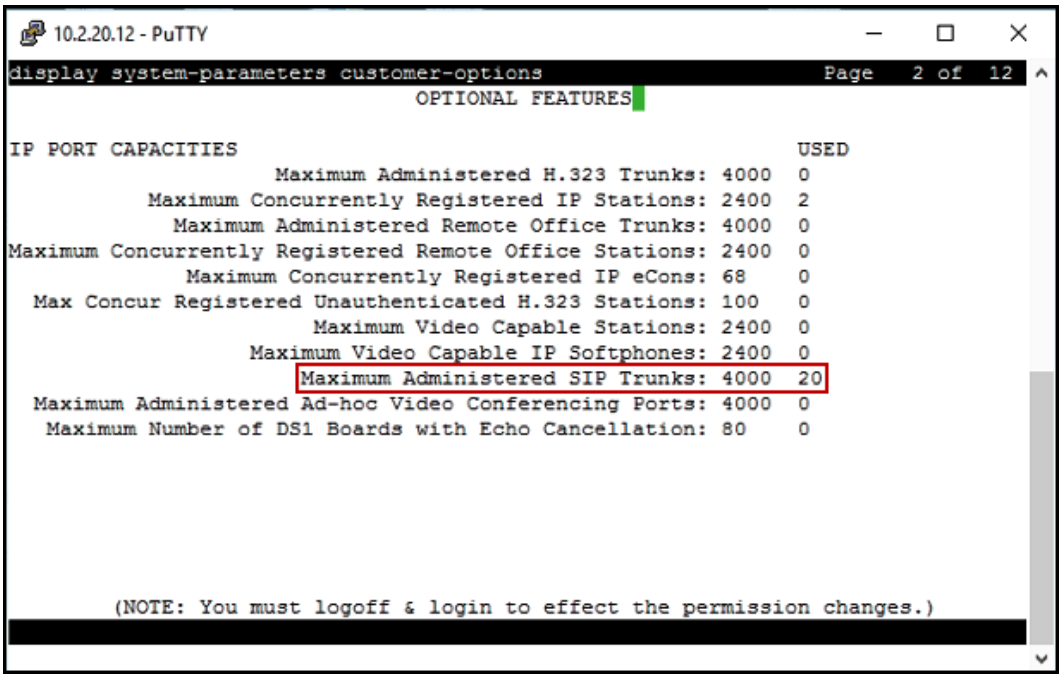
5. Configure Avaya Aura® Communication Manager

This section describes the procedure for configuring Communication Manager to work with the Telmex network SIP Trunk service. A SIP trunk is established between Communication Manager and Session Manager for use by signaling traffic to and from the service provider. It is assumed that the general installation of Communication Manager and the Avaya G450 Media Gateway has been previously completed and is not discussed here.

The Communication Manager configuration was performed using the System Access Terminal (SAT). Some screens in this section have been abridged and highlighted for brevity and clarity in presentation. Some screens captures will show the use of the **change** command instead of the **add** command, since the configuration used for the testing was previously added.

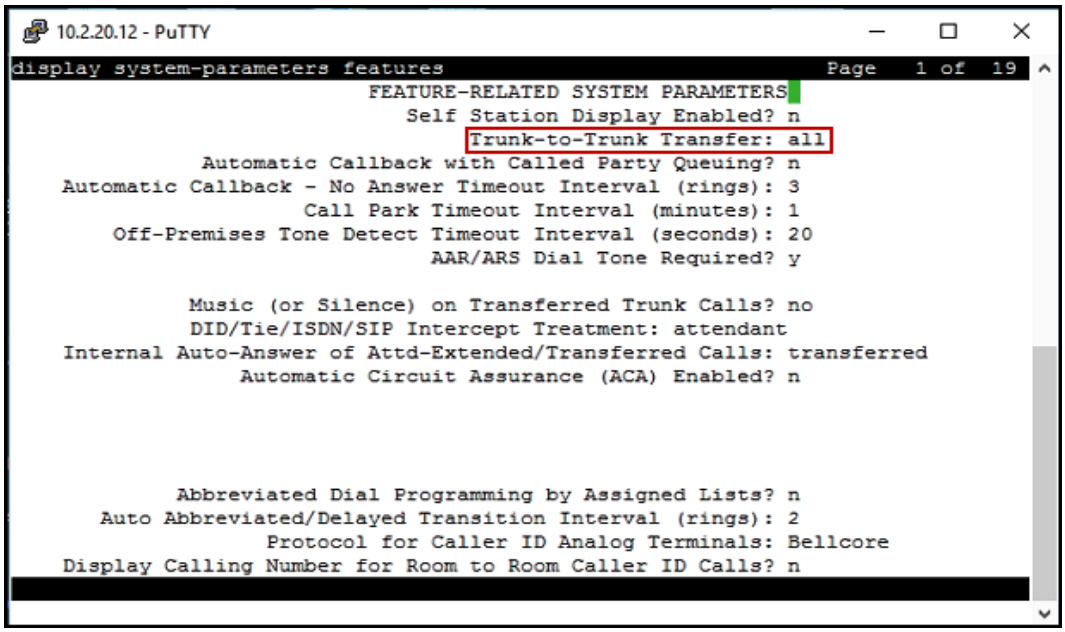
5.1. Licensing and Capacity

Use the **display system-parameters customer-options** command to verify that the **Maximum Administered SIP Trunks** value on **Page 2** is sufficient to support the desired number of simultaneous SIP calls across all SIP trunks at the enterprise including any trunks to and from the service provider. The example shows that **4000** licenses are available and **20** 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.

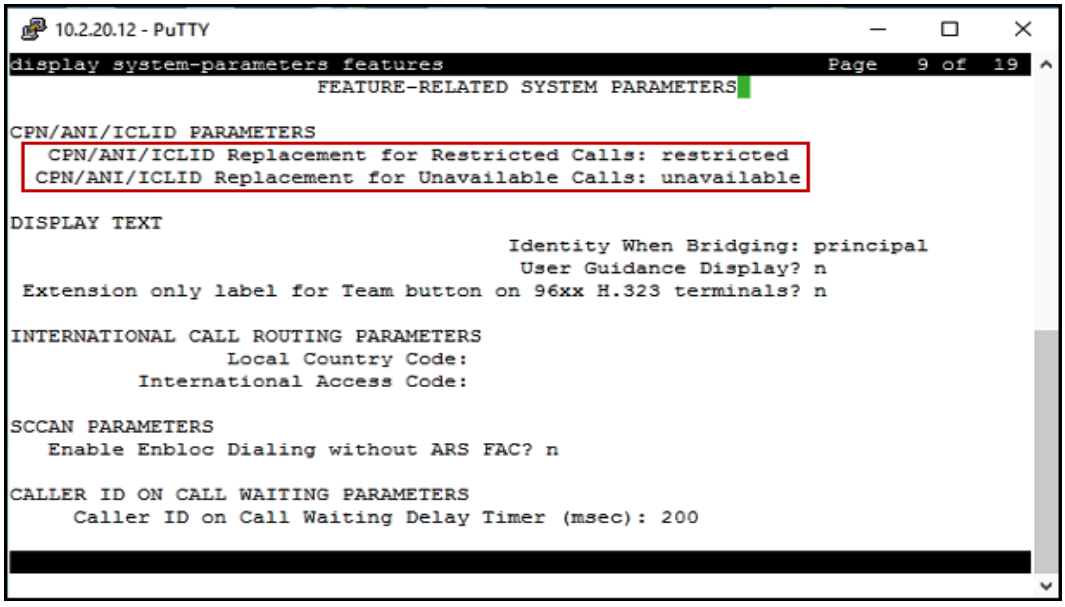


5.2. System Features

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***.

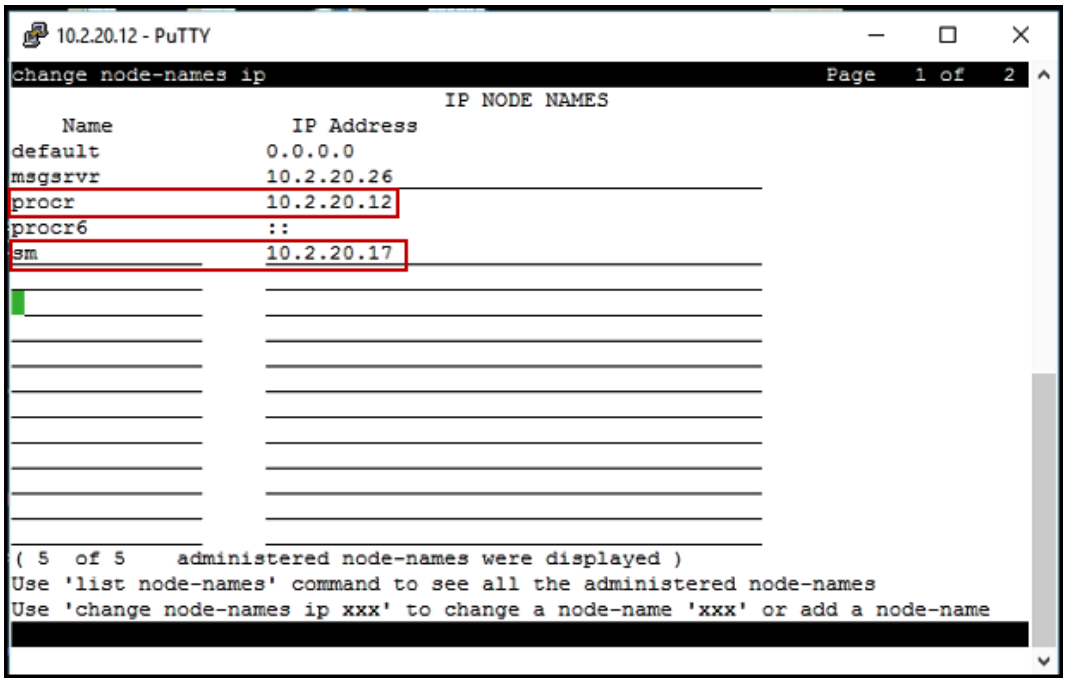


On **Page 9** verify that a text string has been defined to replace the Calling Party Number (CPN) for restricted or unavailable calls. This text string is entered in the two fields highlighted below. The compliance test used the value of ***restricted*** for restricted calls and ***unavailable*** for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



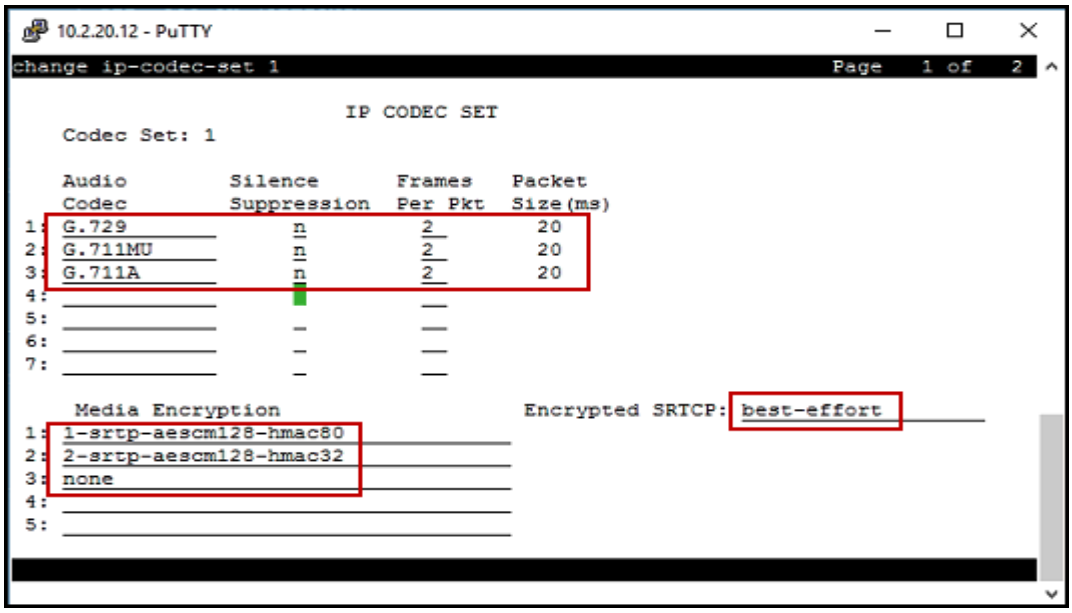
5.3. IP Node Names

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

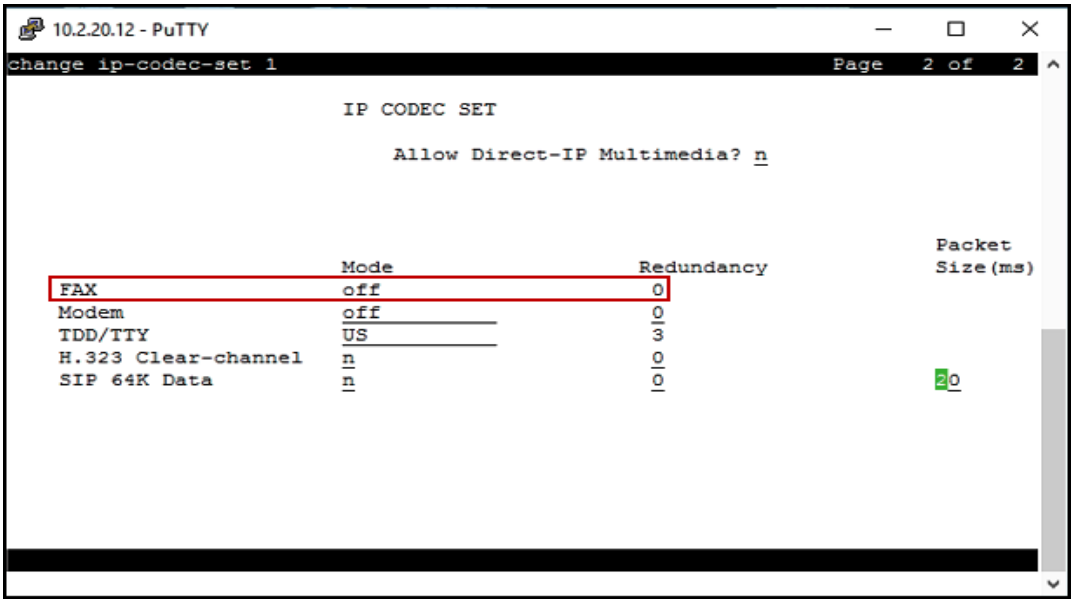


5.4. Codecs

Use the **change ip-codec-set** command to define a list of codecs to use for calls between the enterprise and the service provider. For the compliance test, ip-codec-set 1 was used for this purpose. Enter the corresponding codec in the **Audio Codec** column of the table. During the compliance test codecs ***G.729***, ***G.711MU*** *and* ***G.711A*** were used. Currently Telmex only supports codec G.729 for audio. Set **Media Encryption** to ***1-srtp-aescm128-hmac80***, ***2- srtp-aescm128-hmac32*** and ***none***, this value must match the Media Encryption value set under the Avaya SBCE **Media Rules**, **Section 7.11.2**. Set **Encrypted SRTCP** to ***best-effort***.



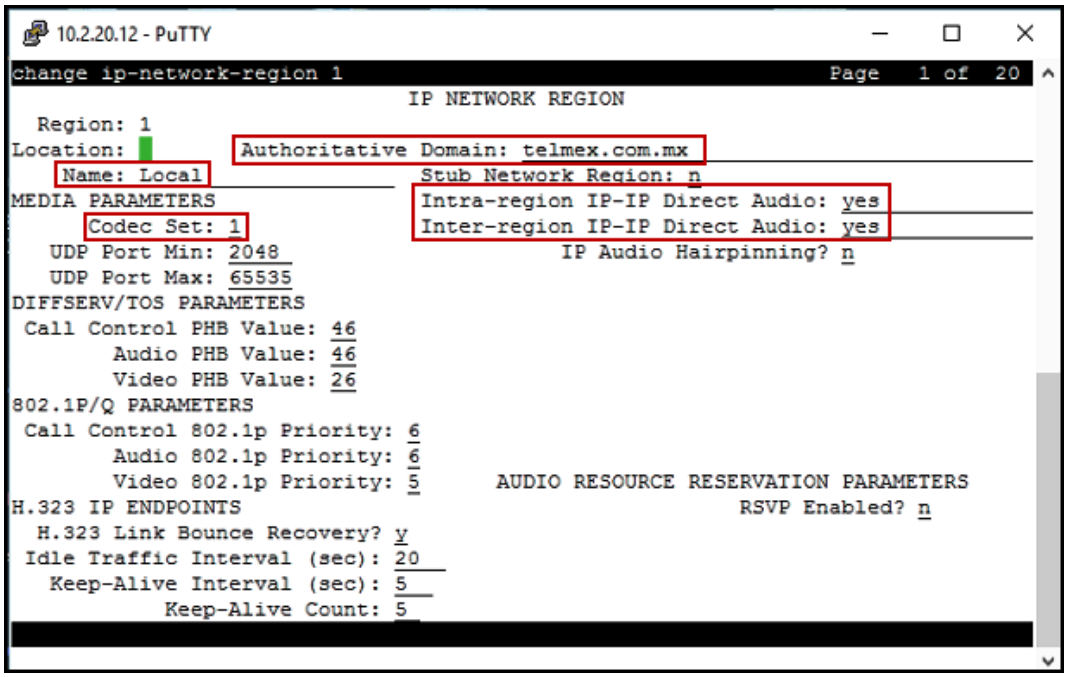
On **Page 2**, set the **Fax Mode** to ***off***.



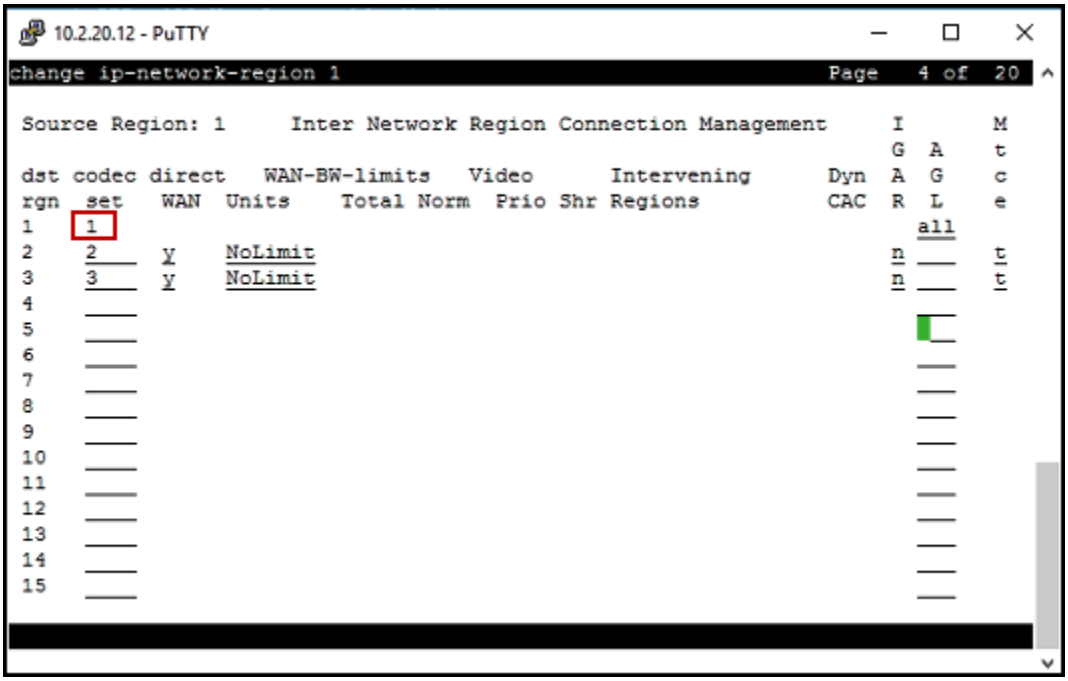
5.5. IP Network Regions

Avaya recommends creating a separate IP network region for the service provider trunk group. This allows for separate codec or quality of service settings to be used (if necessary) for calls between the enterprise and the service provider versus calls within the enterprise or elsewhere. For the compliance test IP Network Region 1 was used for the service provider trunk and for calls between the enterprise. 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 is ***telmex.com.mx*** as assigned to the test environment in the Avaya simulated enterprise. This domain name appears in the "From" header of SIP messages originating from this IP region.
- Enter a descriptive name in the **Name** field.
- Leave both **Intra-region** and **Inter-region IP-IP Direct Audio** set to ***yes*,** the default setting. This will enable **IP-IP Direct Audio** (shuffling), to allow audio traffic to be sent directly between IP endpoints without using media resources in the Avaya Media Gateway and Media Server. Shuffling can be further restricted at the trunk level on the Signaling Group form if needed.
- Set the **Codec Set** field to the IP codec set defined in **Section 5.4**.
- Default values may be used for all other fields.



On **Page 4**, define the IP codec set to be used for traffic within region 1. Enter the desired IP codec set in the **codec set** column of the row with destination region (**dst rgn**) 1. Default values may be used for all other fields. The following example shows the settings used for the compliance test.



5.6. Signaling Group

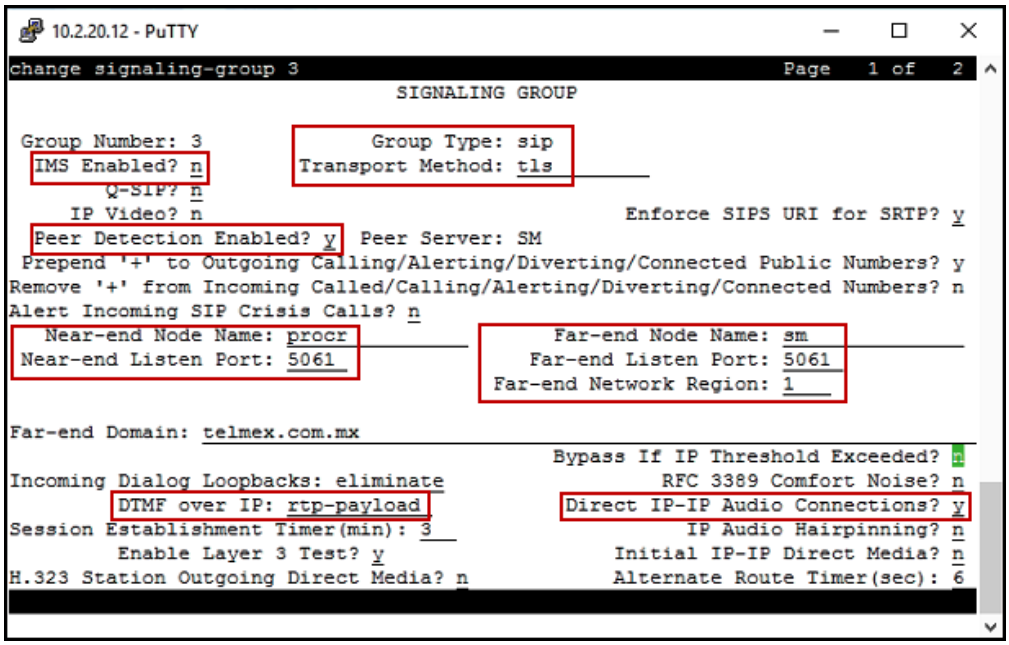
Use the **add signaling-group** command to create a signaling group between Communication Manager and Session Manager for use by the service provider trunk. This signaling group is used for inbound and outbound calls between the service provider and the enterprise. For the compliance test, signaling group 3 was used and was configured using the parameters highlighted below, shown on the screen on the next page:

- Set the **Group Type** field to ***sip***.
- Set the **IMS Enabled** field to ***n***. This specifies the Communication Manager will serve as an Evolution Server for Session Manager.
- Set the **Transport Method** to the transport protocol to be used between Communication Manager and Session Manager. For the compliance test, ***tls*** was used.
- Set the **Peer Detection Enabled** field to ***y***. The **Peer-Server** field will initially be set to ***Others*** and cannot be changed via administration. Later, the **Peer-Server** field will automatically change to ***SM*** once Communication Manager detects its peer is a Session Manager.

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

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

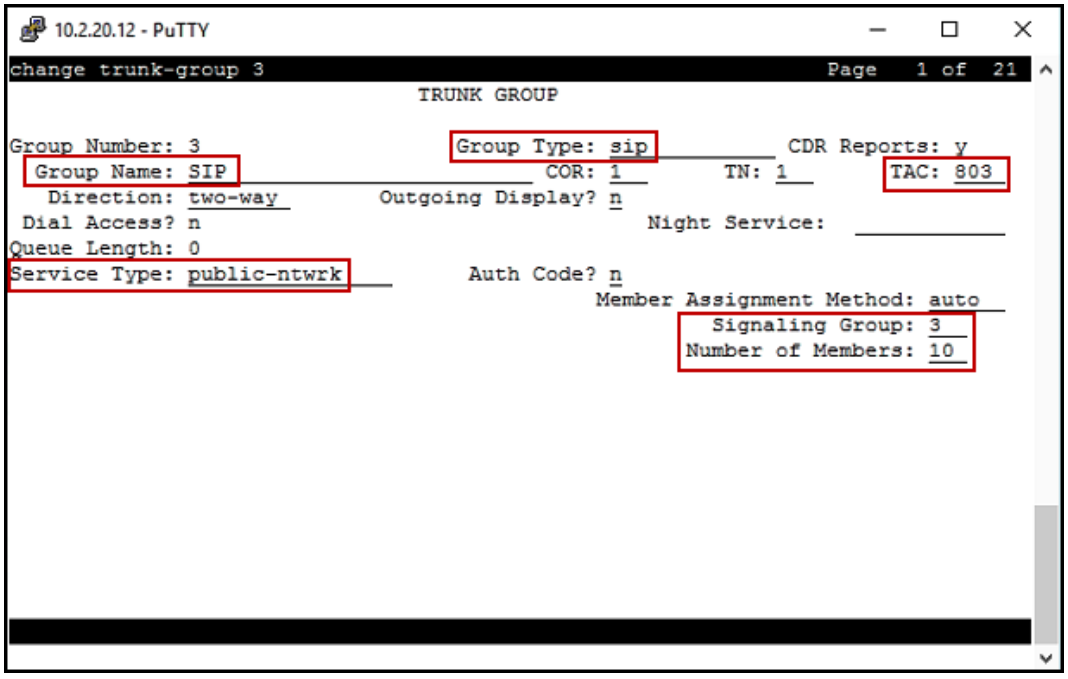
- **Remove '+' from Incoming Called/Calling/Alerting/Diverting/Connected Numbers?** is changed to ***n***.
- Set the **Near-end Node Name** to ***procr***. This node name maps to the IP address of the Communication Manager as defined in **Section 5.3**.
- Set the **Far-end Node Name** to ***sm***. This node name maps to the IP address of Session Manager, as defined in **Section 5.3**.
- Set the **Near-end Listen Port** and **Far-end Listen Port** to a valid port. The compliance test was conducted with the **Near-end Listen Port** and **Far-end Listen Port** set to ***5061***.
- Set the **Far-end Network Region** to the IP network region defined for the Service Provider in **Section 5.5**.
- Set the **Far-end Domain** to the domain of the enterprise.
- Set the **DTMF over IP** field to ***rtp-payload***. This value enables Communication Manager to send DTMF transmissions using RFC 2833.
- Set **Direct IP-IP Audio Connections** to ***y***. This field will enable media shuffling on the SIP trunk allowing Communication Manager to redirect media traffic directly between the Avaya SBCE and the enterprise endpoint. If this value is set to **n**, then the Avaya Media Gateway or Media Server (if used) will remain in the media path of all calls between the SIP trunk and the endpoint. Depending on the number of media resources available in the Media Gateway, these resources may be depleted during high call volume preventing additional calls from completing.
- Default values may be used for all other fields.



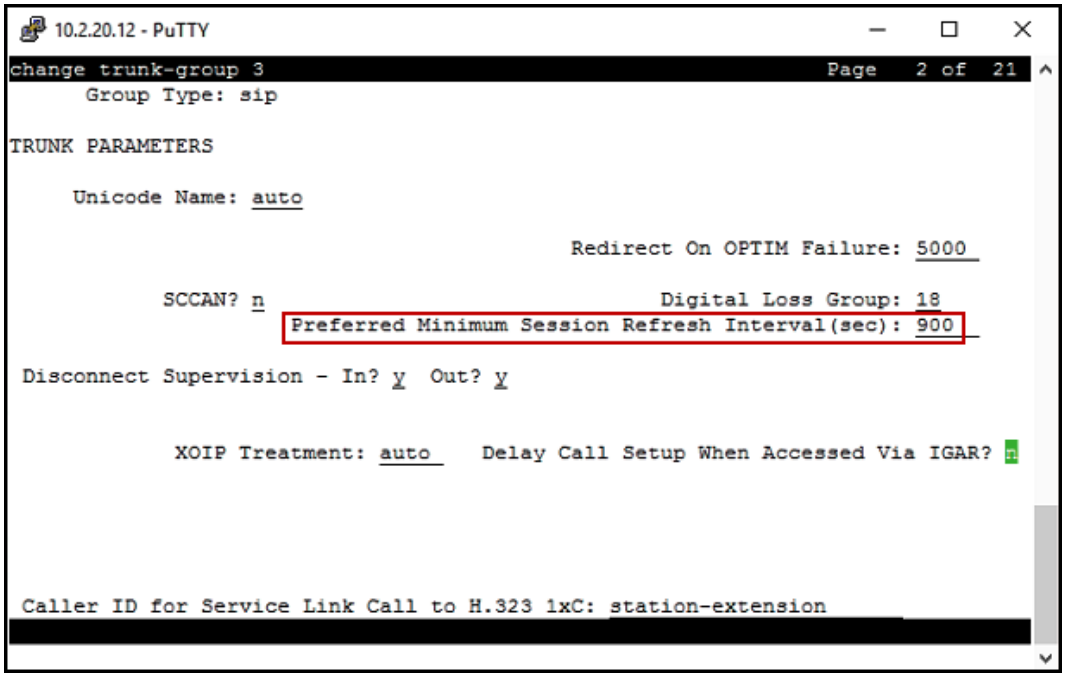
5.7. Trunk Group

Use the **add trunk-group** command to create a trunk group for the signaling group created in **Section 5.6**. For the compliance test, trunk group 3 was configured using the parameters highlighted below.

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

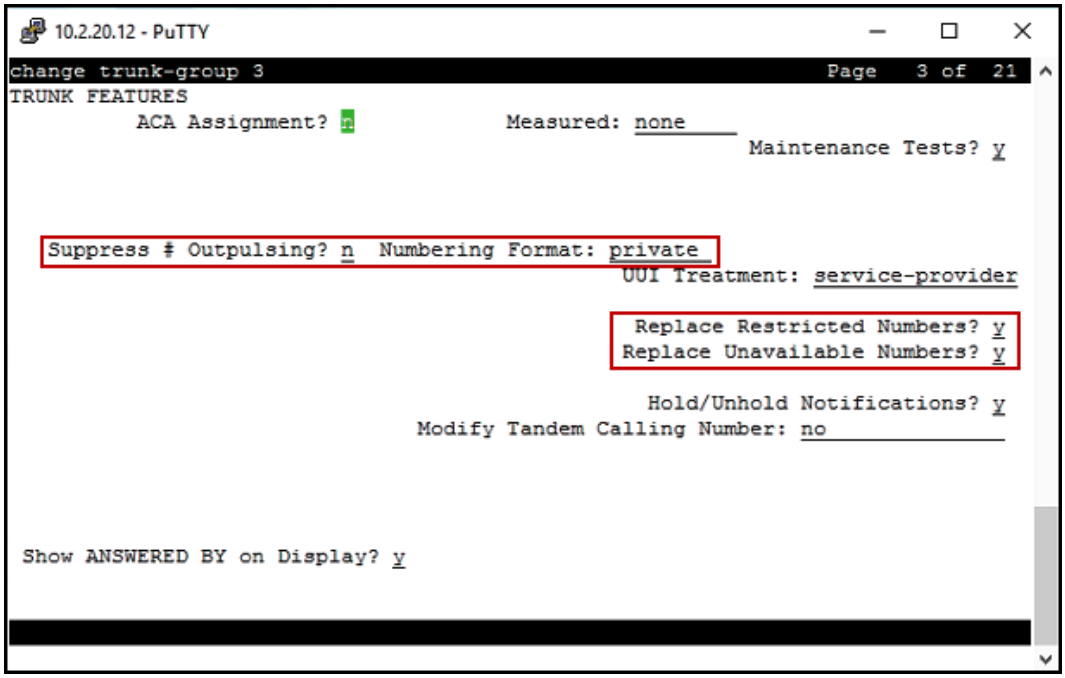


On **Page 2**, verify that the **Preferred Minimum Session Refresh Interval** is set to a value acceptable to the service provider. This value defines the interval that re-INVITEs must be sent to keep the active session alive, **900** seconds was used.



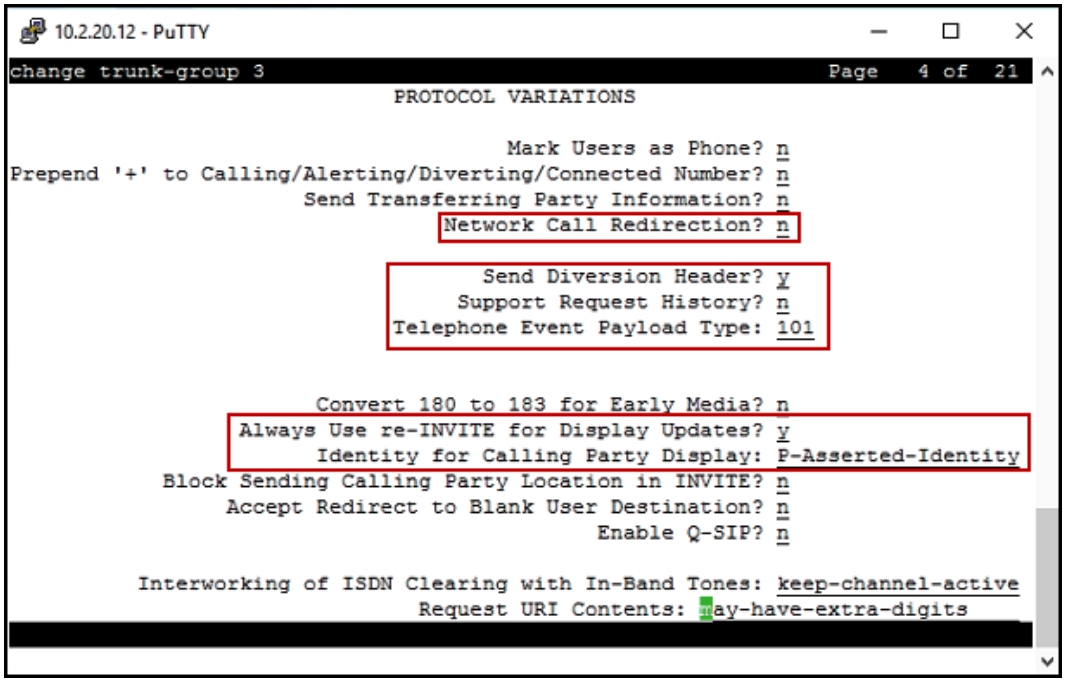
On **Page 3**:

- Set the **Numbering Format** field to ***private***. This field specifies the format of the calling party number (CPN) sent to the far-end. When ***public*** format is used, Communication Manager automatically inserts a "+" sign, preceding the numbers in the "From", "Contact" and "P-Asserted Identity" (PAI) headers. To keep uniformity with the format used by Telmex, the **Numbering Format** was set to ***private*** and the **Numbering Format** in the route pattern was set to ***unk-unk*** (see **Section 5.10**).
- Set the **Replace Restricted Numbers** and **Replace Unavailable Numbers** fields to ***y***. This will allow the CPN displayed on local endpoints to be replaced with the value set in **Section 5.2**, if the inbound call has enabled CPN block.



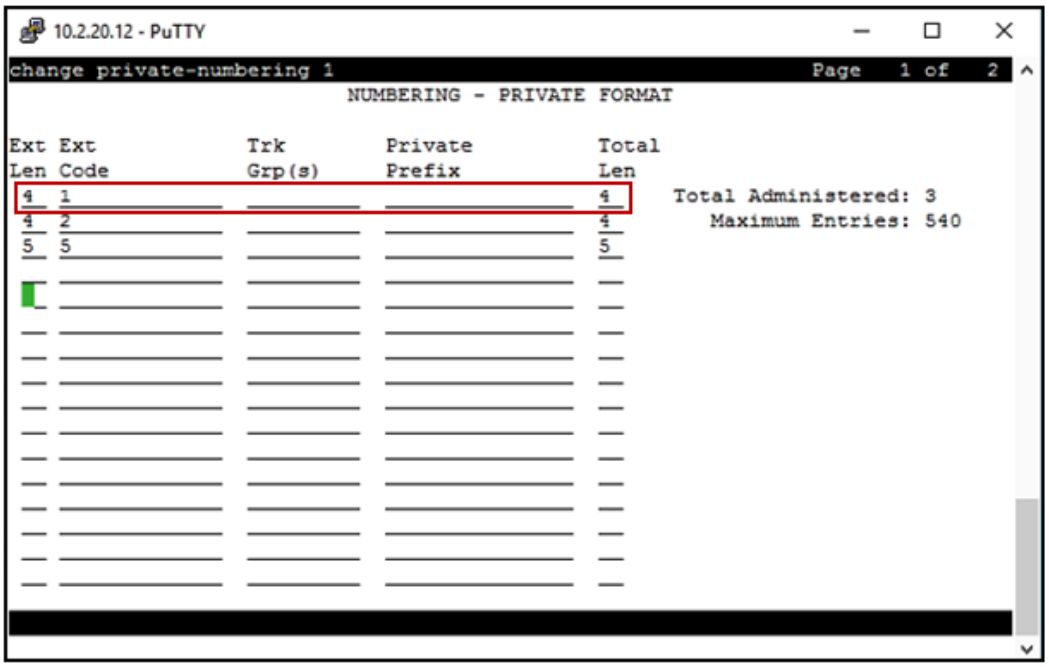
On **Page 4**:

- Set the **Network Call Redirection** field to ***n***. With this setting, Communication Manager will not use the REFER method for calls being redirected back to the PSTN across the SIP trunk. The REFER method is not supported by Telmex.
- Set the **Send Diversion Header** field to ***y*** and **Support Request History** to ***n***.
- Set the **Telephone Event Payload Type** to ***101***.
- Set **Always Use re-INVITE for Display Updates** to ***y***.
- Verify that **Identity for Calling Party Display** is set to ***P-Asserted-Identity***.
- Default values were used for all other fields.



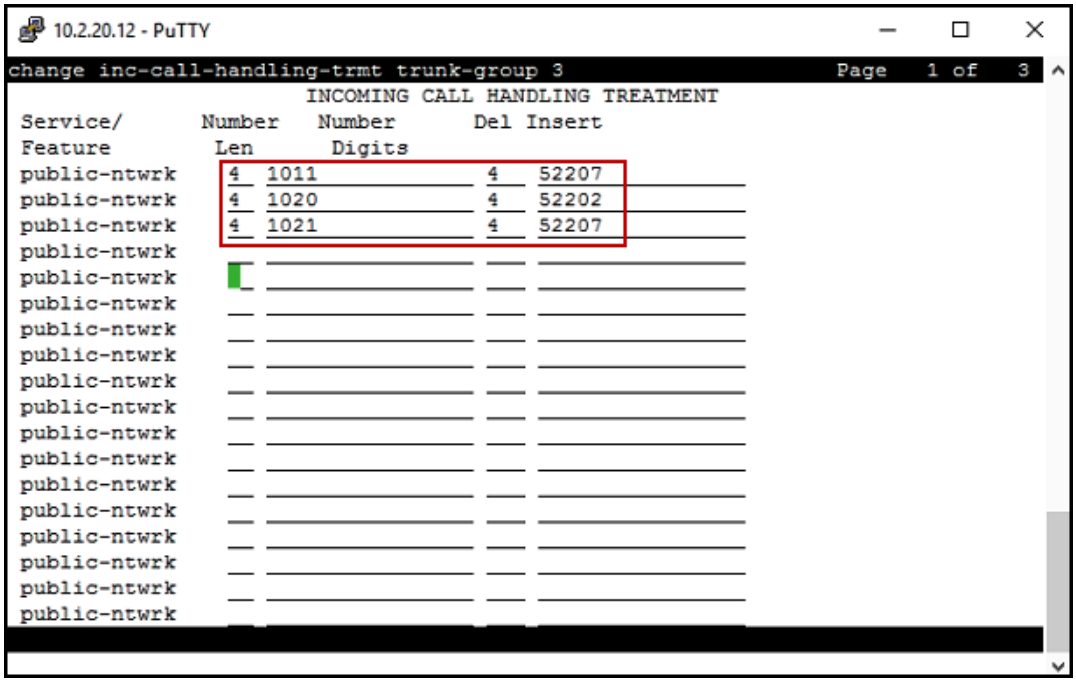
5.8. Calling Party Information

The calling party number is sent in the SIP "From", "Contact" and "PAI" headers. Since private numbering was selected to define the format of this number (**Section 5.7**), use the **change private-numbering** command to create an entry for each extension which has a DID assigned. DID numbers are provided by the SIP service provider. Each DID number is assigned in this table to one enterprise internal extension or Vector Directory Numbers (VDNs). In the example below, three DID numbers were assigned by the service provider for testing. The highlighted row shown below configures any four digit number beginning with 1 (i.e., 1xxx) that uses any trunk group to retain the original 4 digit number (i.e., no digit manipulation is specified), and the Total Len is 4. Thus, these same 4-digit numbers were used in the outbound calling party information on the service provider trunk when calls were originated from these 3 extensions.



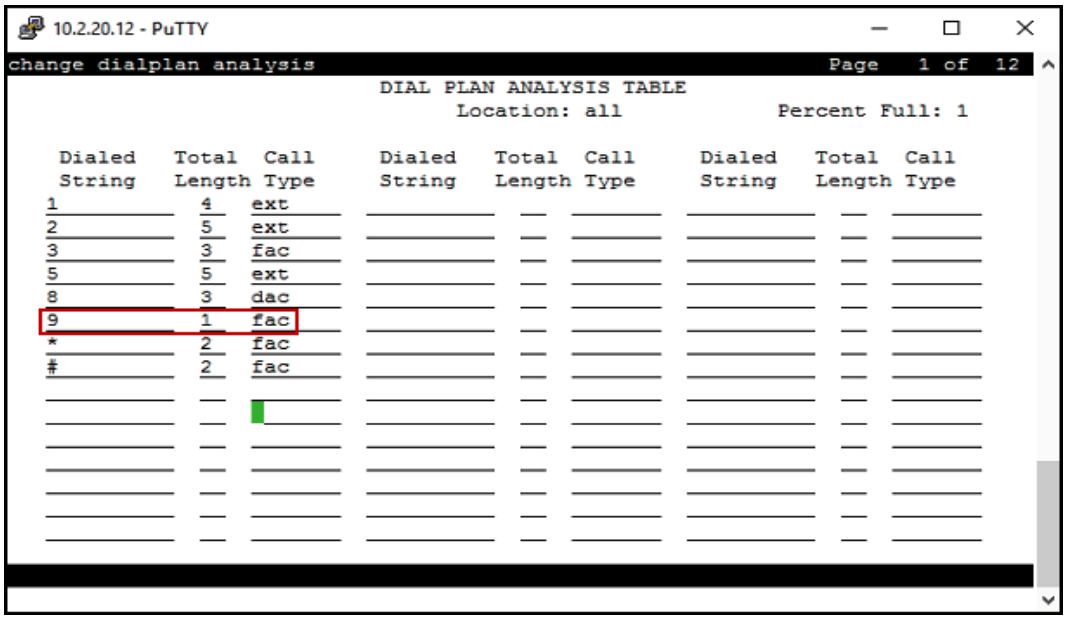
5.9. Inbound Routing

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

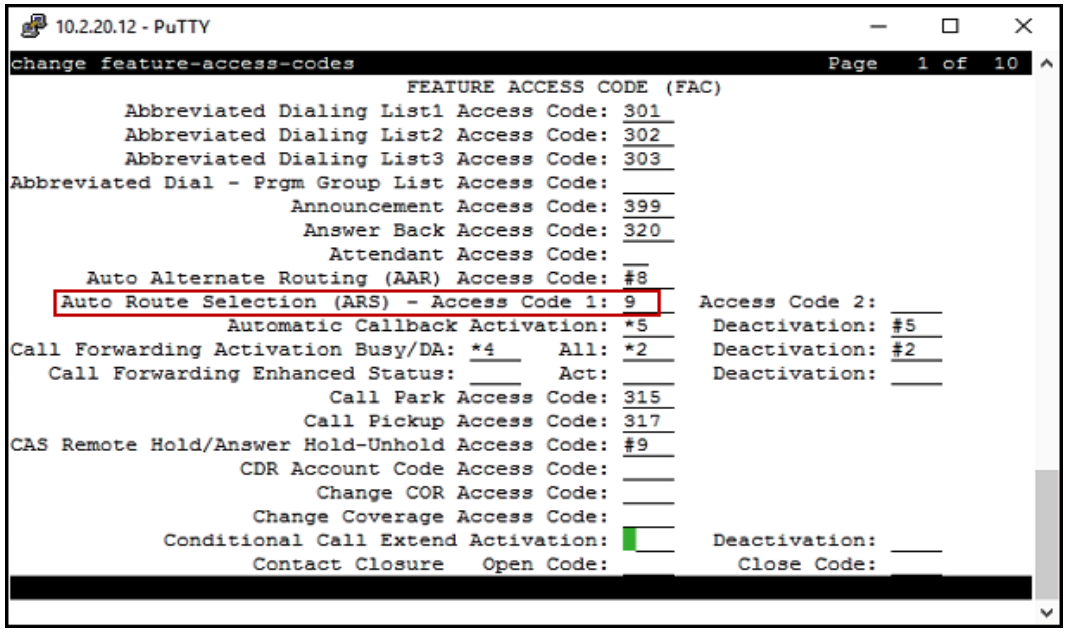


5.10. Outbound Routing

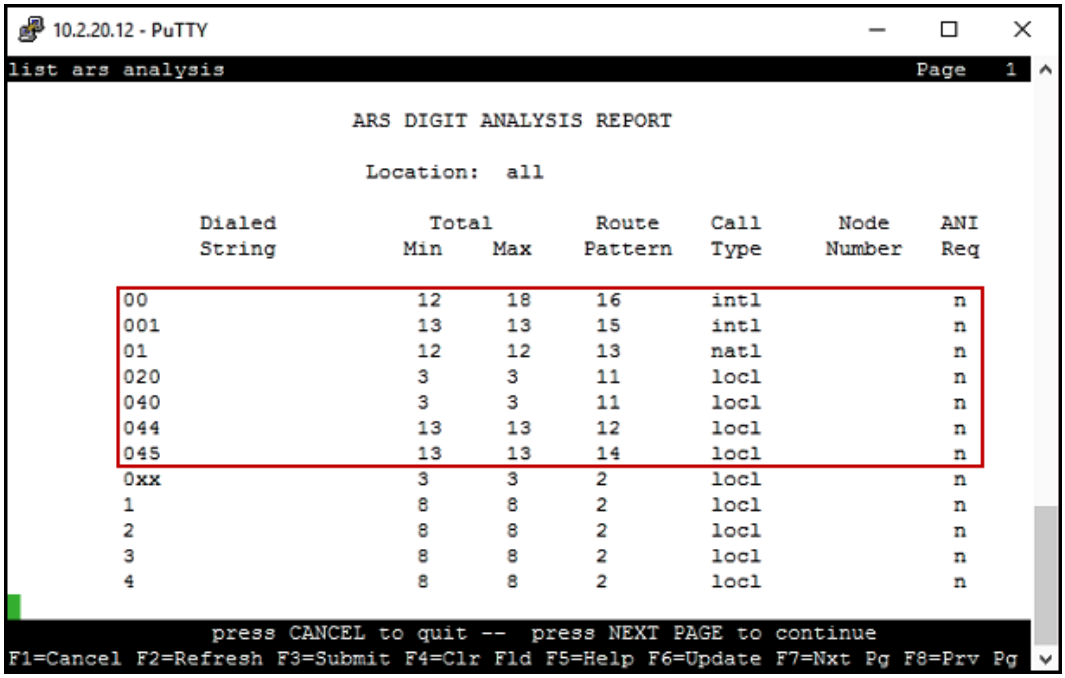
In these Application Notes, the Automatic Route Selection (ARS) feature is used to route outbound calls via the SIP trunk to the service provider. In the sample configuration, the single digit 9 is used as the ARS access code. Enterprise callers will dial 9 to reach an "outside line". This common configuration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



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

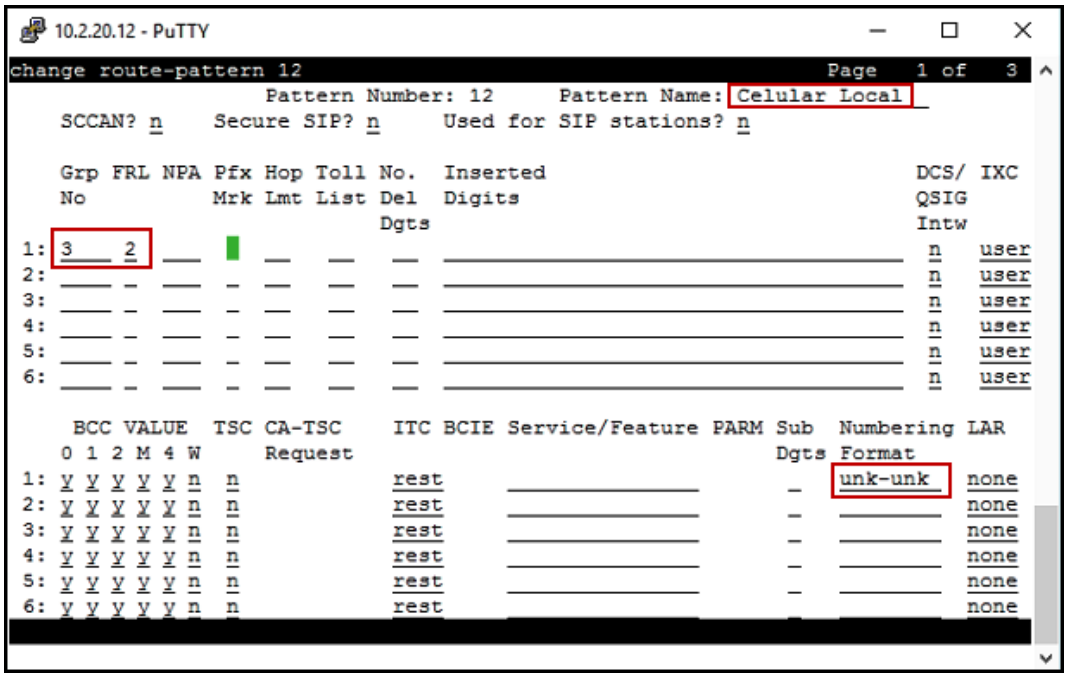


Use the **change ars analysis** command to configure the routing of dialed digits following the first digit 9. The example below shows a subset of the dialed strings tested as part of the compliance test. See **Section 2.1** for the complete list of call types tested. All dialed strings are mapped to route patterns 11-16, which contains the SIP trunk group to the service provider.



The route pattern defines which trunk group will be used for the call and performs any necessary digit manipulation. Use the **change route-pattern** command to configure the parameters for the service provider trunk route pattern in the following manner. The example below shows the values used for route pattern 12 in the compliance test.

- **Pattern Name**: Enter a descriptive name.
- **Grp No**: Enter the outbound trunk group for the SIP service provider.
- **FRL**: Set the Facility Restriction Level (**FRL**) field to a level that allows access to this trunk for all users that require it.
- **Numbering Format**: Set to ***unk-unk***. All calls using this route pattern will use the private numbering table. See setting of the **Numbering Format** in the trunk group form for full details in **Section 5.7**.



Repeat this procedure as needed to define additional route patterns. For the compliance test route patterns 11-16 were used. Calls to the PSTN, international, local/national, local/information and local/cellular are examples of call types that were assigned individual route patterns, only route pattern 12 (for cellular local calls) is shown on the screenshot shown above.

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

6. Configure Avaya Aura® Session Manager

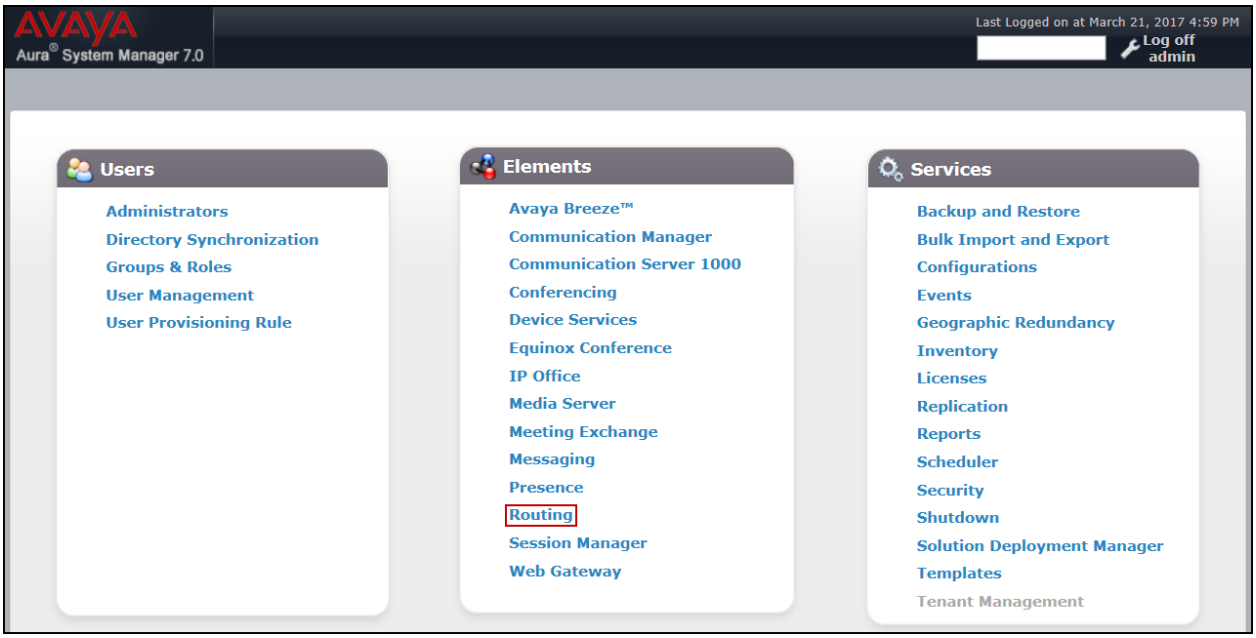
This section provides the procedures for configuring Session Manager. The procedures include adding the following items:

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

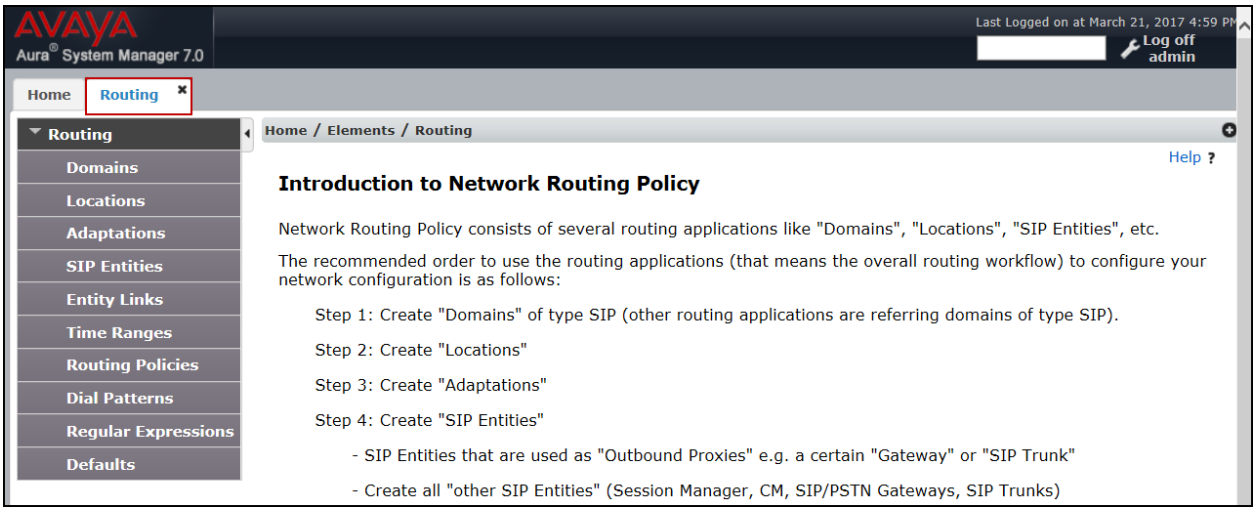
The following sections assume that the initial configuration of Session Manager and System Manager has already been completed, and that network connectivity exists between System Manager and Session Manager.

6.1. System Manager Login and Navigation

Session Manager configuration is accomplished by accessing the browser-based GUI of System Manager, using the URL "https://<ip-address>/SMGR", where "<ip-address>" is the IP address of System Manager. Log in with the appropriate credentials and click on **Log On** (not shown). The screen shown below is then displayed; click on **Routing**.



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

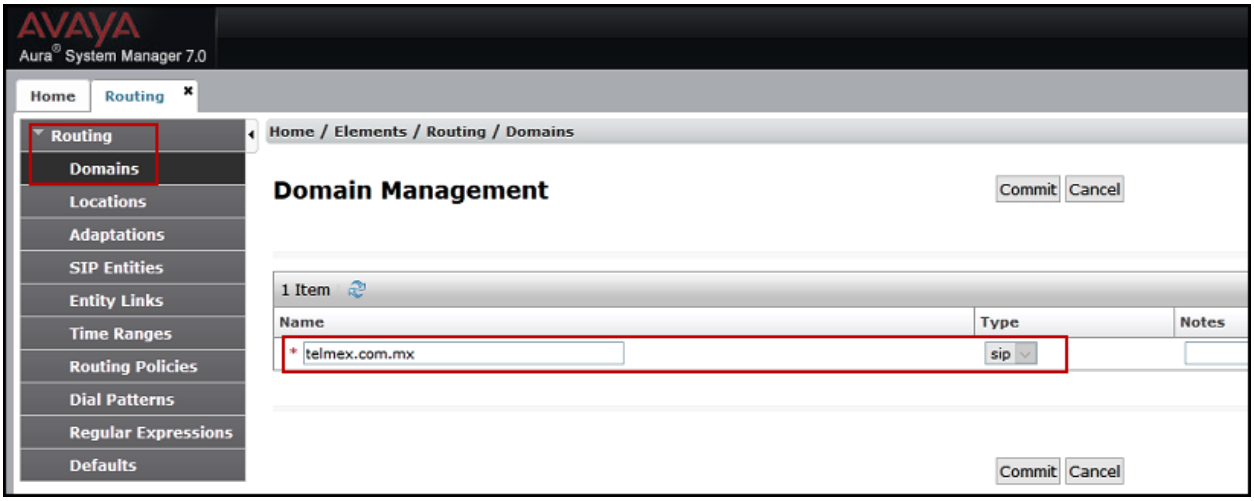


6.2. SIP Domain

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

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

The screen below shows the entry for the enterprise domain.



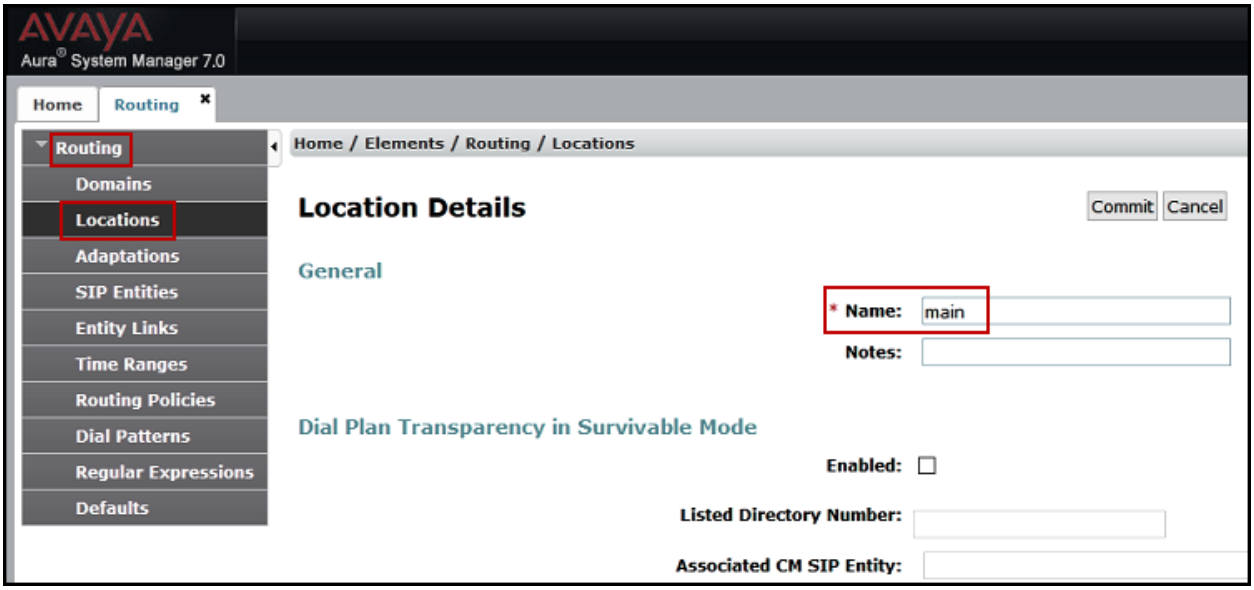
6.3. Locations

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

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

The following screen shows the location details for the location named ***main***.

Later, this location will be assigned to the SIP Entities. Other parameters for this location (not shown) retained the default values.



6.4. Adaptations

In order to improve interoperability with third party elements, Session Manager 7.0 incorporates the ability to use Adaptation modules to remove specific headers that are either Avaya proprietary or deemed excessive/unnecessary for non-Avaya elements.

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

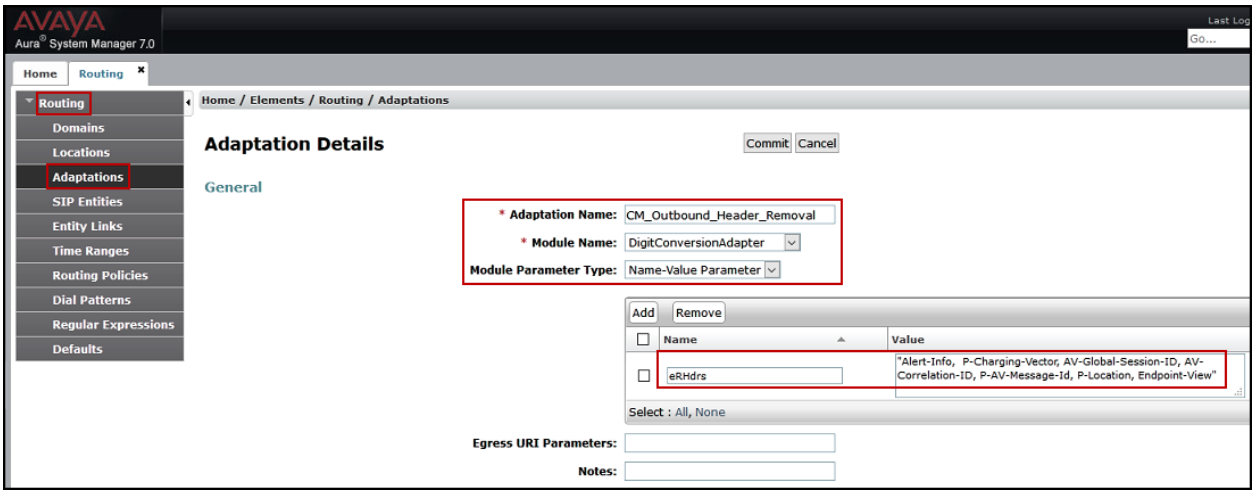
Navigate to **Routing → Adaptations** in the left-hand navigation pane and click the **New** button in the right pane (not shown). In the new right pane that appears (shown below), fill in the following:

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

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

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

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

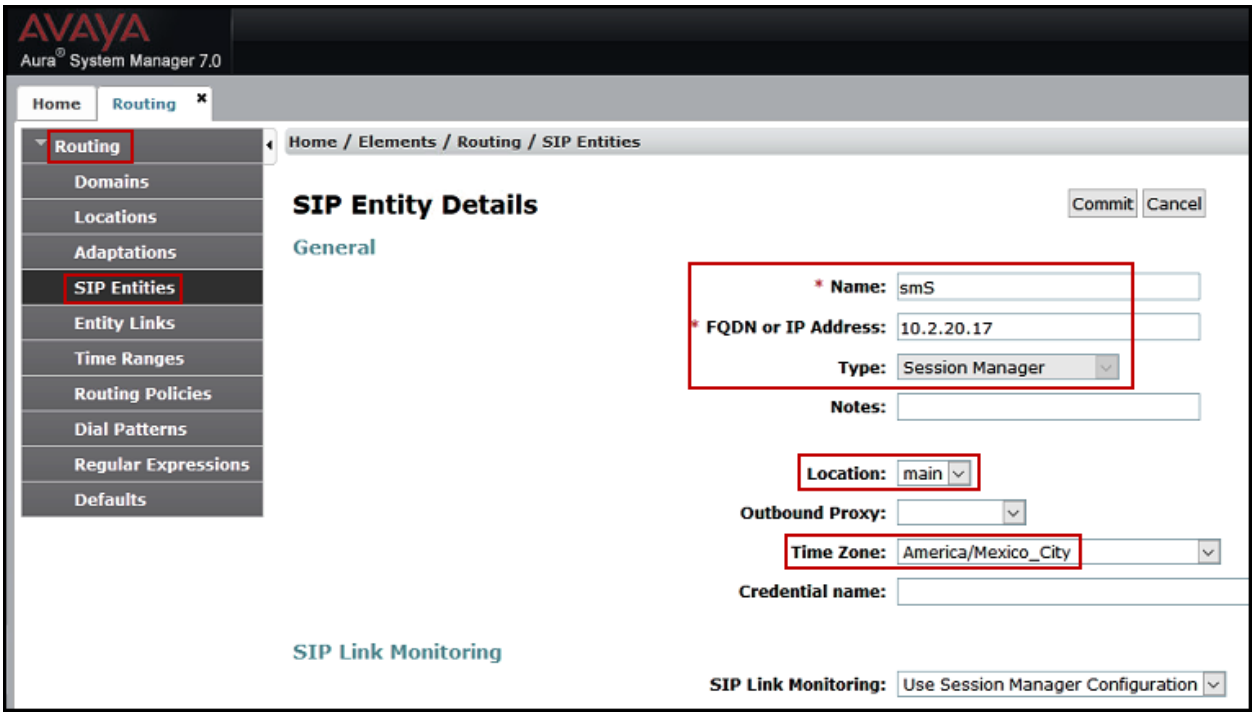


6.5. SIP Entities

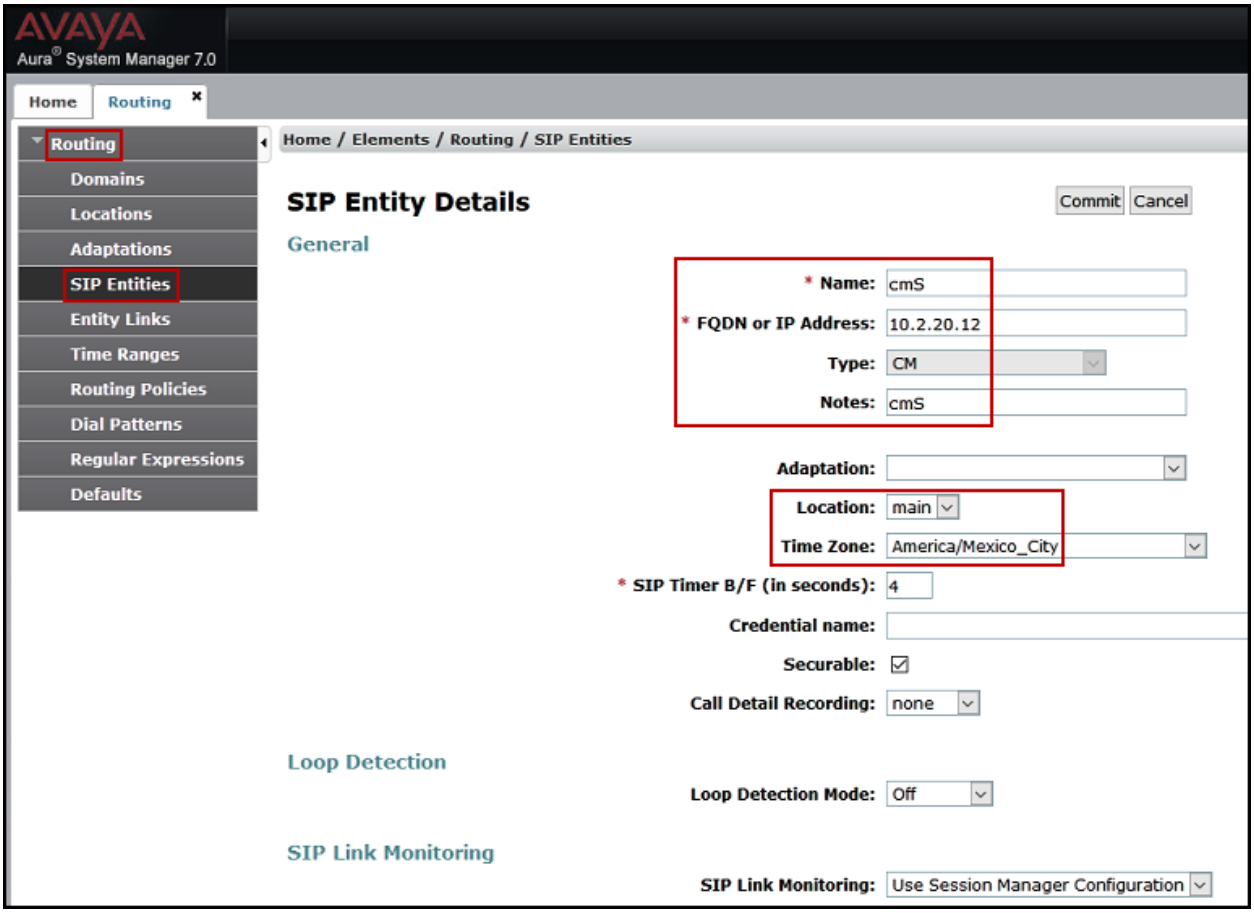
A SIP Entity must be added for Session Manager and for each SIP telephony system connected to it, which includes Communication Manager and the Avaya SBCE. Navigate to **Routing** → **SIP Entities** in the left navigation pane and click on the **New** button in the right pane (not shown). In the **General** section, enter the following values. Use default values for all remaining fields:

- **Name:** Enter a descriptive name.
- **FQDN or IP Address:** Enter the FQDN or IP address of the SIP Entity that is used for SIP signaling (see **Figure 1**).
- **Type:** Select ***Session Manager*** for Session Manager, ***CM*** for Communication Manager and ***SIP Trunk*** for the Avaya SBCE.
- **Adaptation:** This field is only present if **Type** is not set to **Session Manager**. If Adaptations were to be created, here is where they would be applied to the entity.
- **Location:** Select the location that applies to the SIP Entity being created, defined in **Section 6.3**.
- **Time Zone:** Select the time zone for the location above.
- Click **Commit** to save.

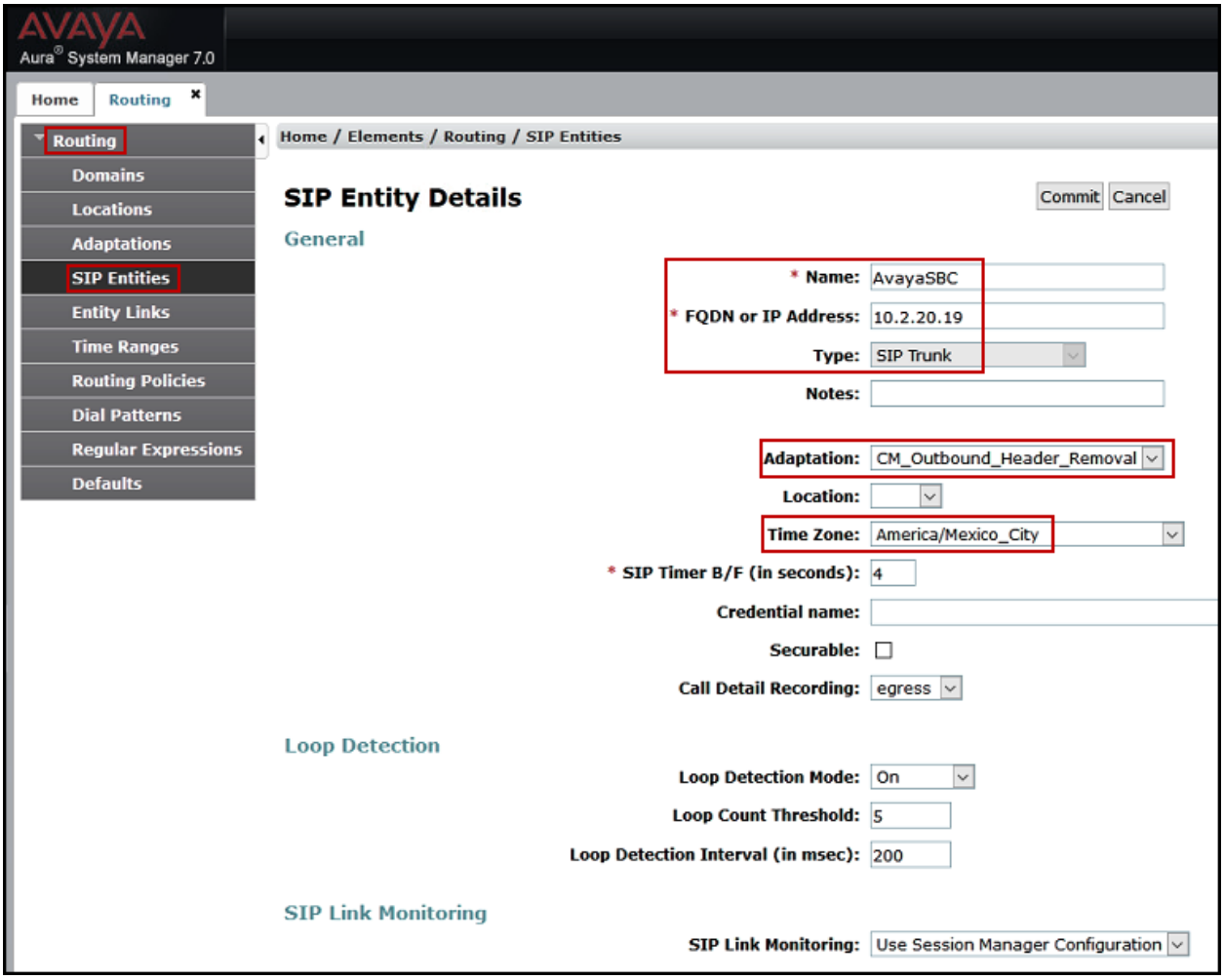
The following screen shows the addition of the ***smS*** SIP Entity for Session Manager. The IP address of the Session Manager Security Module is entered in the **FQDN or IP Address** field.



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



The following screen shows the addition of the ***AvayaSBC*** SIP Entity for the Avaya SBCE. The **FQDN or IP Address** field is set to the IP address of the SBC private network interface (see **Figure 1**). On the **Adaptation** field, the adaptation module ***CM_Outbound_Header_Removal*** previously defined in **Section 6.4** was selected. Select the **time zone** for the location above.

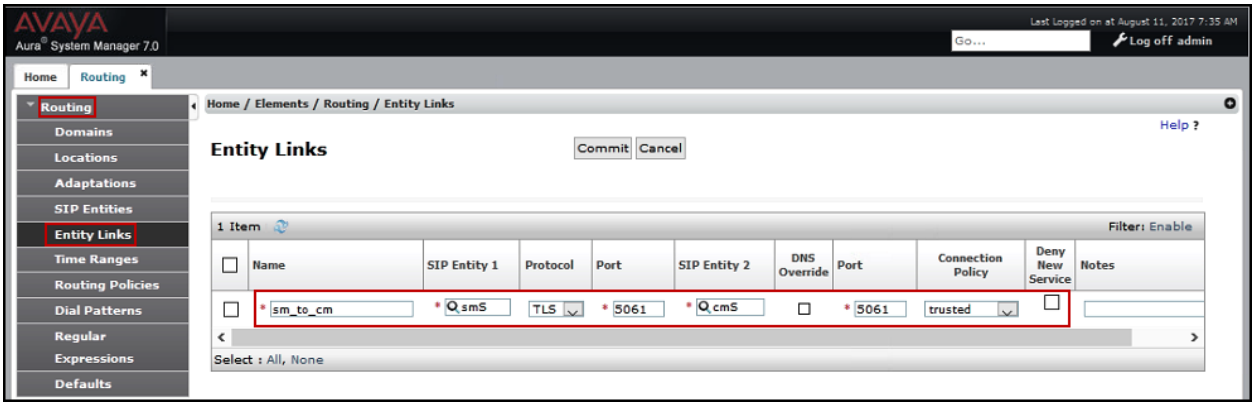


6.6. Entity Links

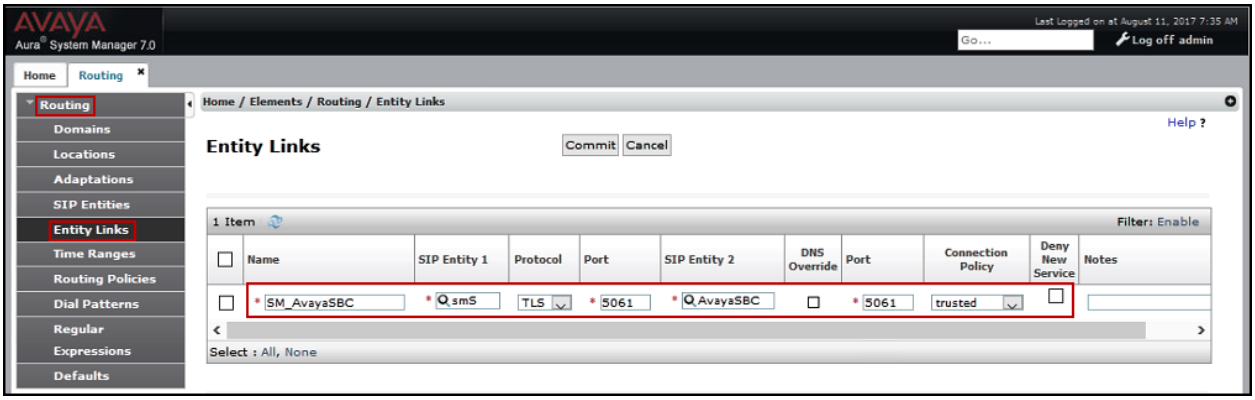
A SIP trunk between Session Manager and a telephony system is described by an Entity Link. Two Entity Links were created; one to the Communication Manager for use only by service provider traffic and one to the Avaya SBCE. To add an Entity Link, navigate to **Routing** → **Entity Links** in the left navigation pane and click on the **New** button in the right pane (not shown). Fill in the following fields in the new row that is displayed:

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

The screen below shows the Entity Link to Communication Manager. The protocol and ports defined here must match the values used on the Communication Manager signaling group form in **Section 5.6**. ***TLS*** transport and port ***5061*** were used.



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

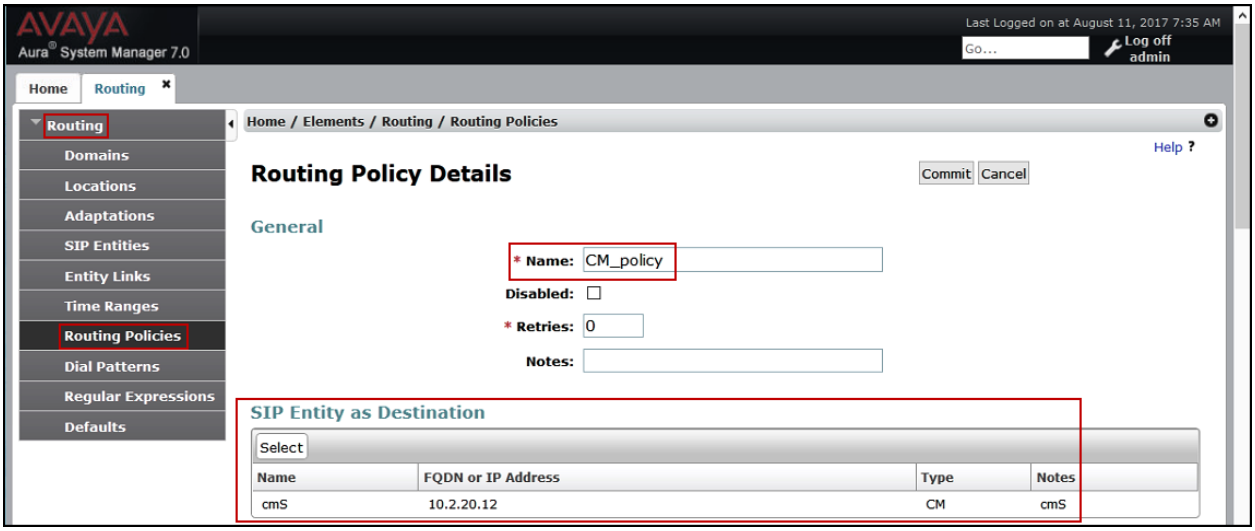


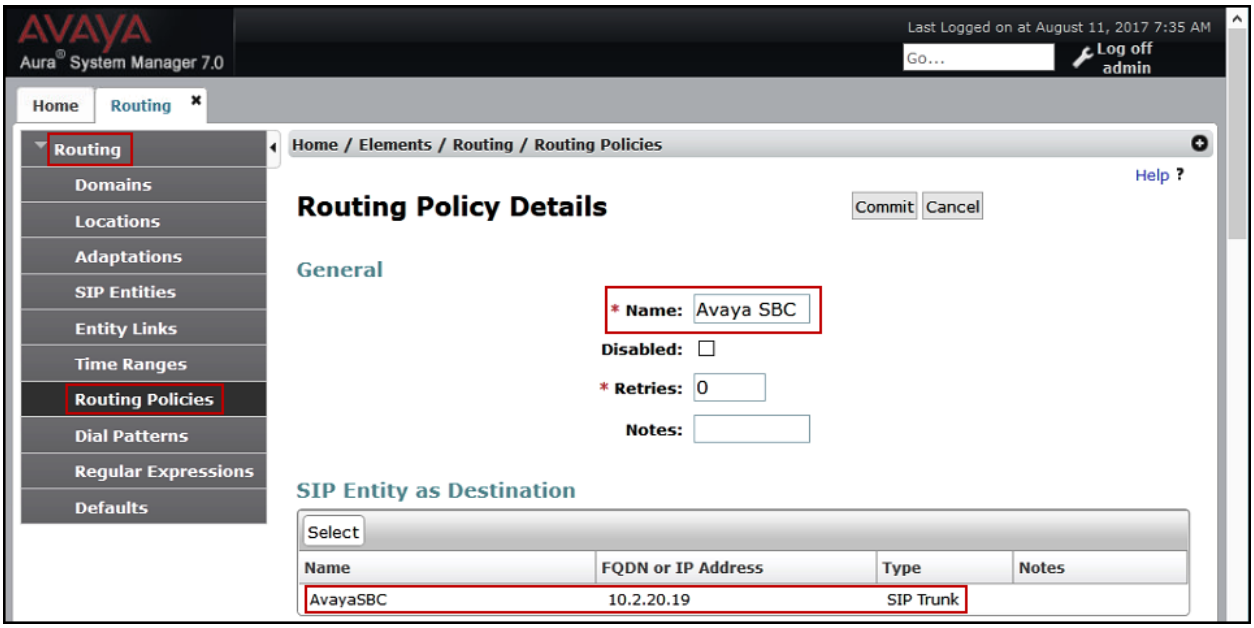
6.7. Routing Policies

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

- In the **General** section, enter a descriptive **Name** and add a brief description under **Notes** (optional).
- In the **SIP Entity as Destination** section, click **Select**. The **SIP Entity List** page opens (not shown). Choose the appropriate SIP entity to which this routing policy applies (**Section 6.5**) and click **Select**. The selected SIP Entity displays on the **Routing Policy Details** page as shown below.
- Use default values for remaining fields.
- Click **Commit** to save.

The following screens show the Routing Policies for Communication Manager and the Avaya SBCE.





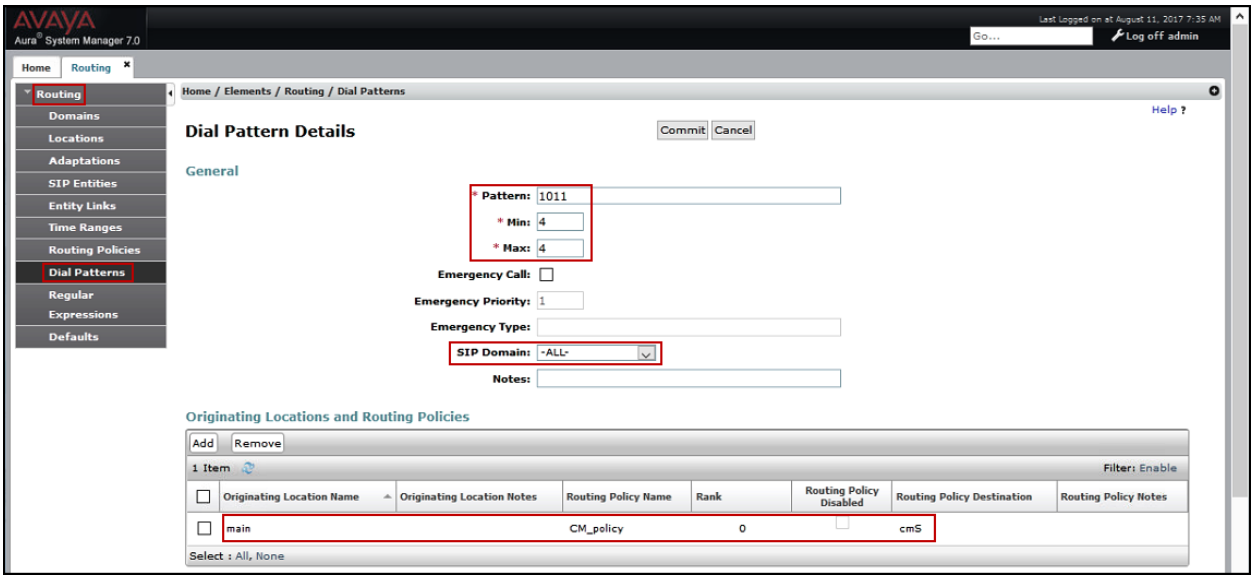
6.8. Dial Patterns

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

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

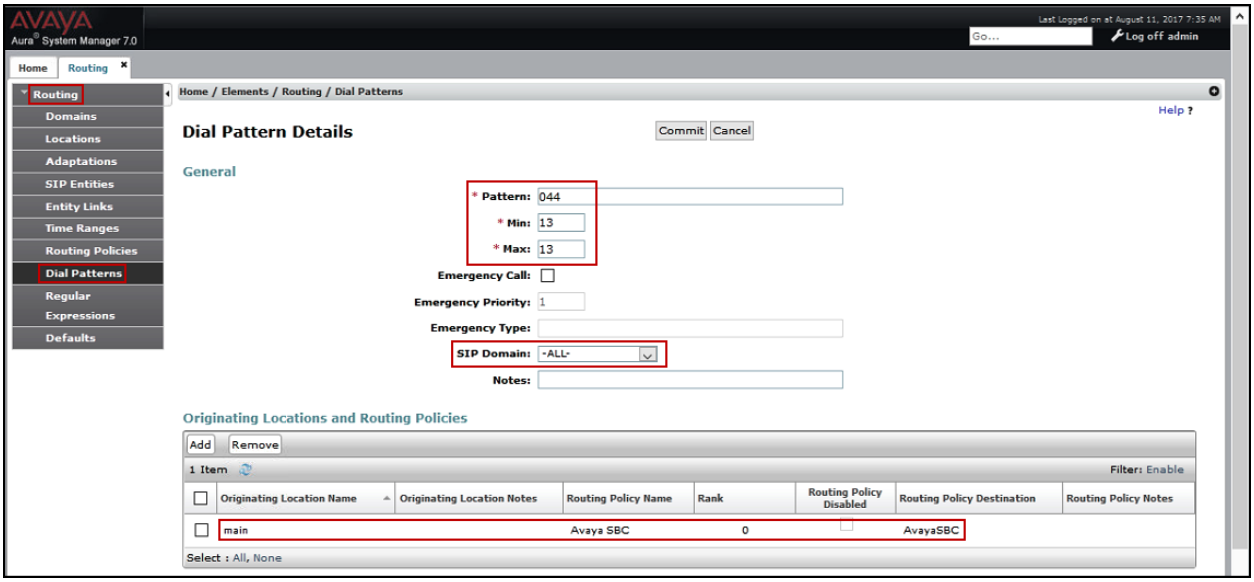
- **Pattern:** Enter a dial string that will be matched against the Request-URI of the call.
- **Min:** Enter a minimum length used in the match criteria.
- **Max:** Enter a maximum length used in the match criteria.
- **SIP Domain:** Enter the destination domain used in the match criteria (**Section 6.2**).
- **Notes:** Add a brief description (optional).
- In the **Originating Locations and Routing Policies** section, click **Add**. From the **Originating Locations and Routing Policy List** that appears (not shown), select the appropriate originating location for use in the match criteria (**Section 6.3**).
- Lastly, select the routing policy from the list that will be used to route all calls that match the specified criteria (**Section 6.7**). Click **Select** (not shown).
- Click **Commit** to save.

The following screen illustrates an example dial pattern used to verify inbound PSTN calls to the enterprise. In the example, calls to 4 digit number ***1011***, arriving from location ***main***, used route policy ***CM_policy*** to Communication Manager. The SIP Domain was set to ***all***.



Repeat this procedure as needed to define additional dial patterns for other range of DID numbers assigned by the service provider to the enterprise.

The example in this screen shows the 13 digit dialed numbers for outbound calls, beginning with ***044***, for calls to local cellular numbers, arriving from the ***main*** location, will use route policy ***AvayaSBC***, which sends the call out to the PSTN via Avaya SBCE and the service provider SIP Trunk. The SIP Domain was set to ***all***.



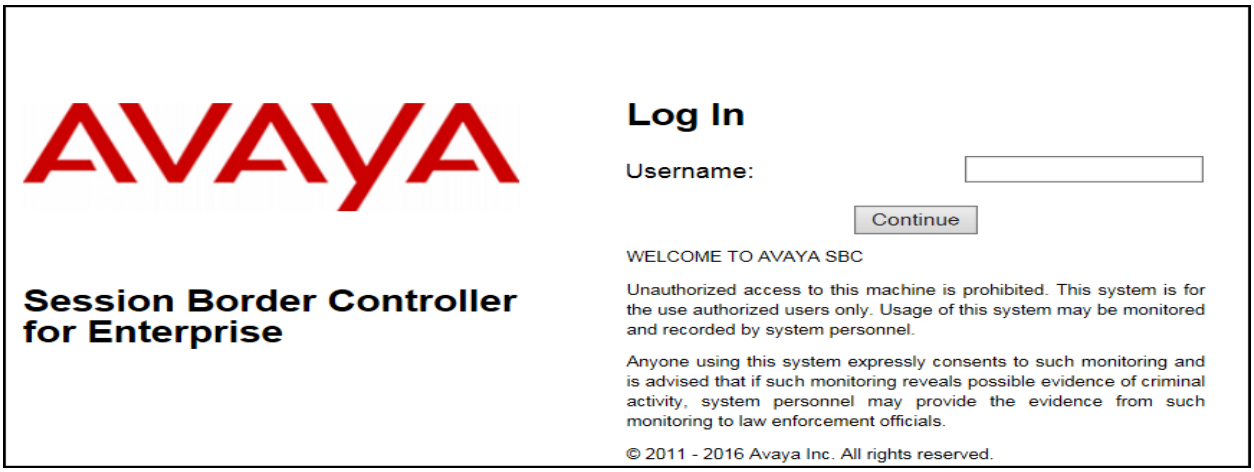
Repeat this procedure as needed, to define additional dial patterns for PSTN numbers to be routed to the service provider's network via the Avaya SBCE.

7. Configure Avaya Session Border Controller for Enterprise

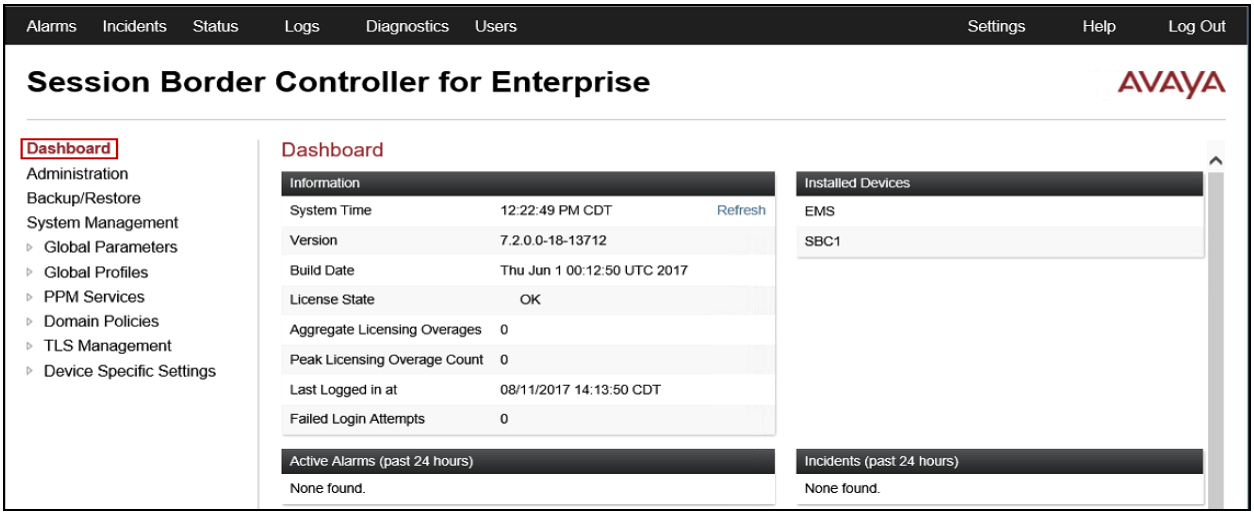
This section describes the configuration of the Avaya SBCE. It is assumed that the initial installation of the Avaya SBCE, the assignment of the management interface IP Address and license installation have already been completed; hence these tasks are not covered in these Application Notes. For more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

7.1. System Access

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

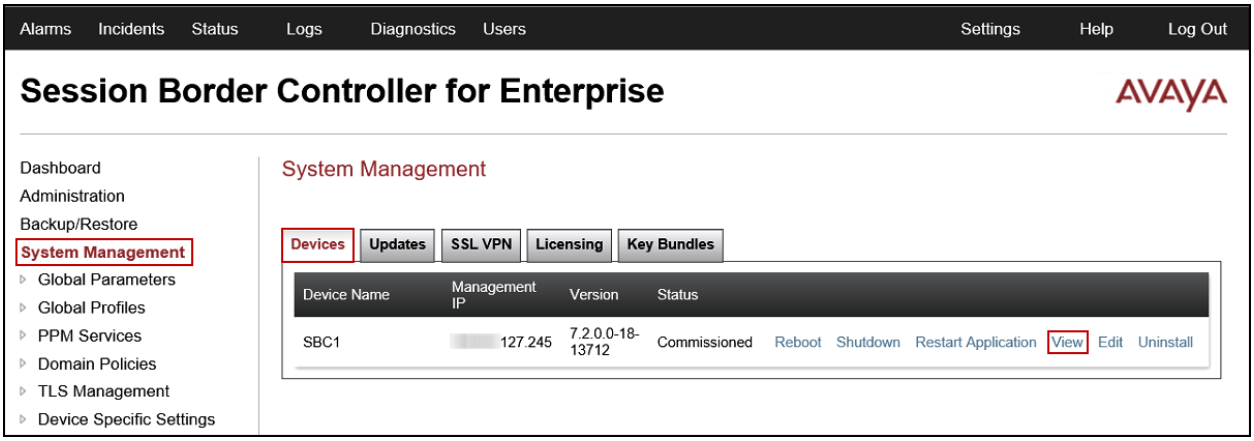


Once logged in, the Dashboard screen is presented. The left navigation pane contains the different available menu items used for the configuration of the Avaya SBCE. Verify that the status of the **License State** field is **OK**, indicating that a valid license is present. Contact an authorized Avaya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

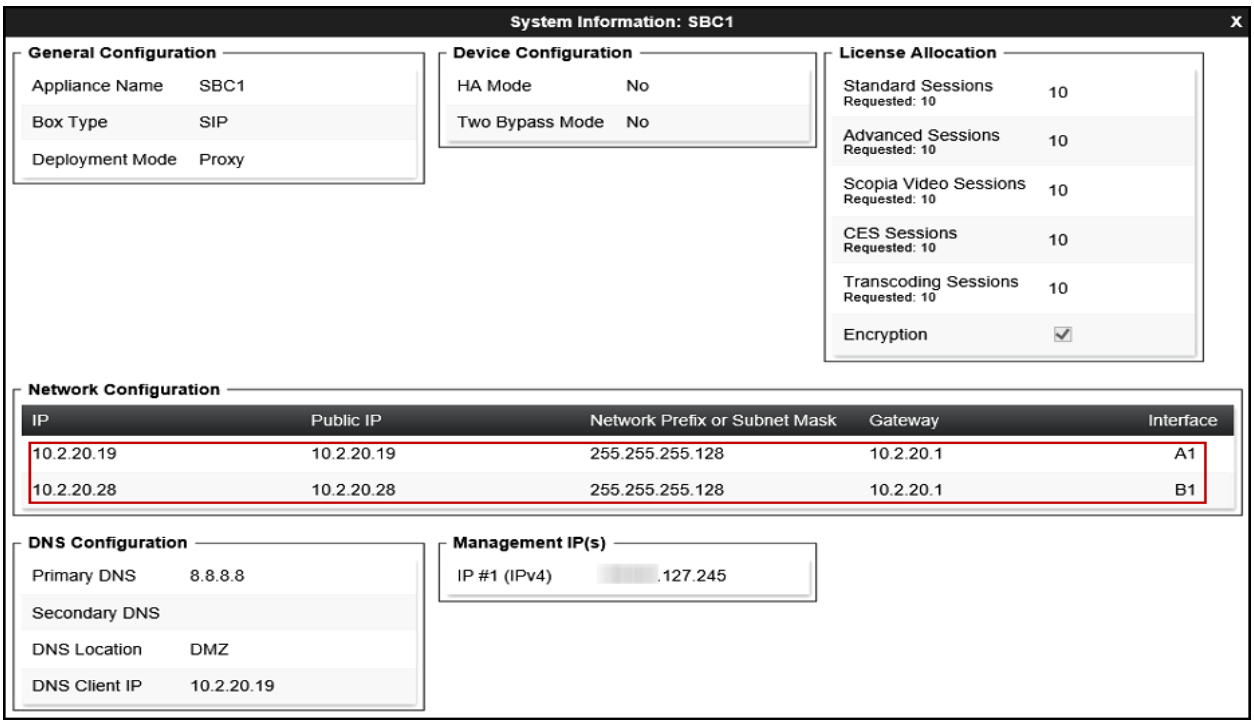


7.2. System Management

To view current system information, select **System Management** on the left navigation pane. A list of installed devices is shown in the **Devices** tab on the right pane. In the reference configuration, a single device named ***SBC1*** is shown. The management IP address that was configured during installation is blurred out for security reasons, the current software version is shown. The management IP address needs to be on a subnet separate from the ones used in all other interfaces of the Avaya SBCE, segmented from all VoIP traffic. Verify that the **Status** is ***Commissioned***, indicating that the initial installation process of the device has been previously completed, as shown on the screen below.



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



In the reference configuration, the private interface of the Avaya SBCE (10.2.20.19) was used to connect to the enterprise network, while its public interface (10.2.20.28) was used to connect to the Telmex private IP network for routing calls to and from the PSTN via Telmex's network. See **Figure 1**.

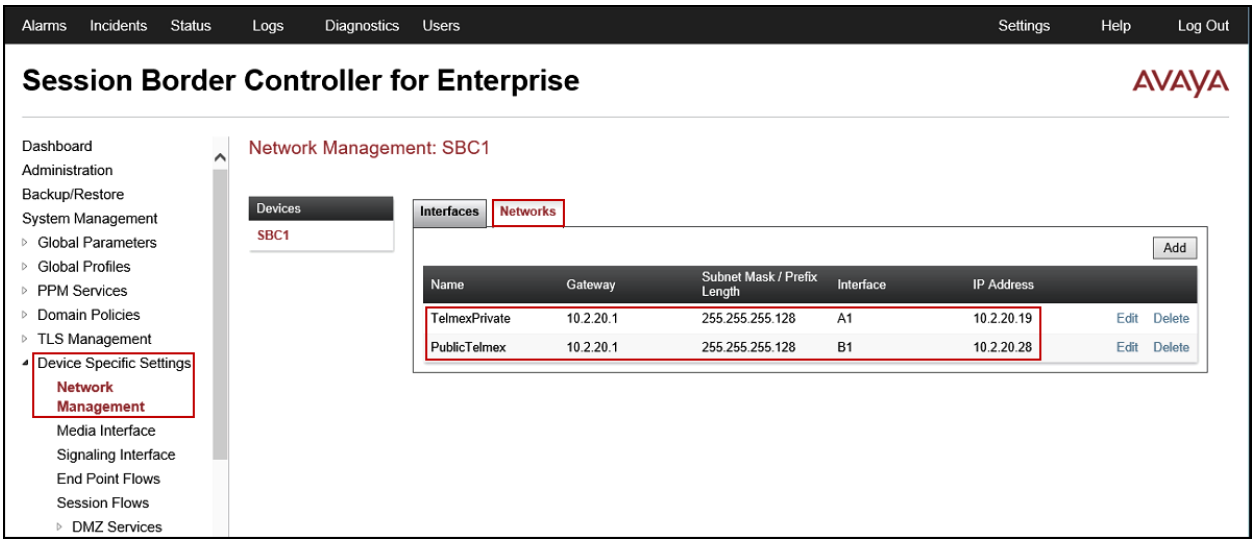
On the **License Allocation** area of the **System Information**, verify that the number of **Standard Sessions** is sufficient to support the desired number of simultaneous SIP calls across all SIP trunks at the enterprise. The number of sessions and encryption features are primarily controlled by the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

7.3. Network Management

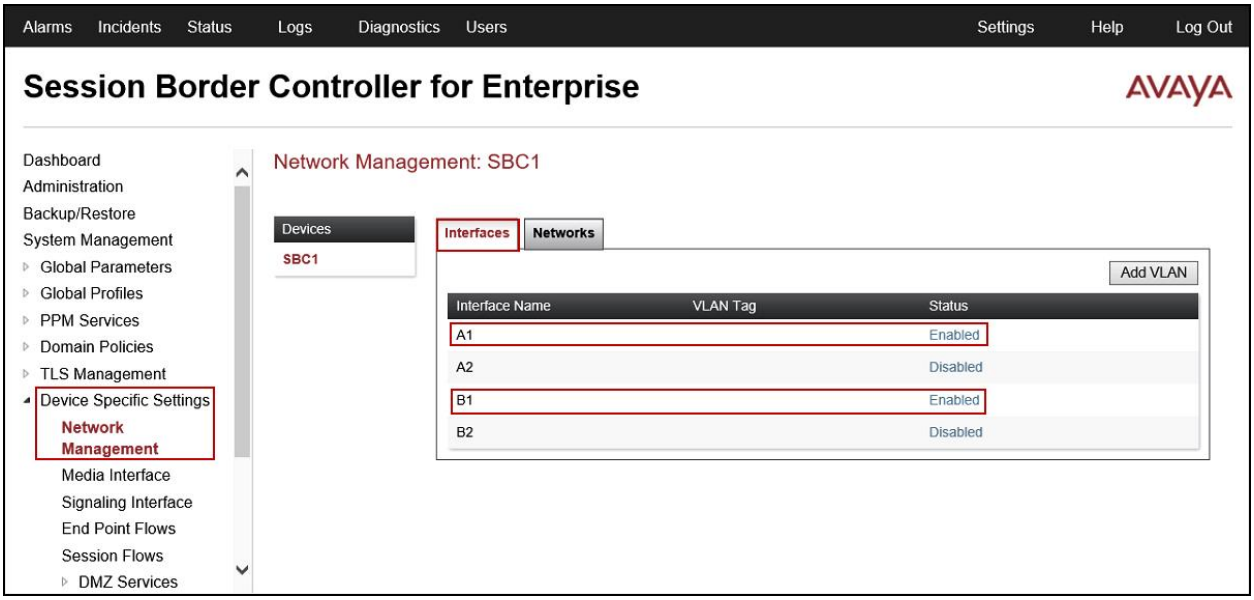
The network configuration parameters should have been previously specified during installation of the Avaya SBCE. In the event that changes need to be made to the network configuration, they can be entered here.

Select **Network Management** from **Device Specific Settings** on the left-side menu. Under **Devices** in the center pane, select the device being managed, ***SBC1*** in the sample configuration. On the **Networks** tab, verify or enter the network information as needed.

Note that in the configuration used during the compliance test, the IP addresses assigned to the private (***10.2.20.19***) and public (***10.2.20.28***) sides of the Avaya SBCE are the ones relevant to these Application Notes.



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

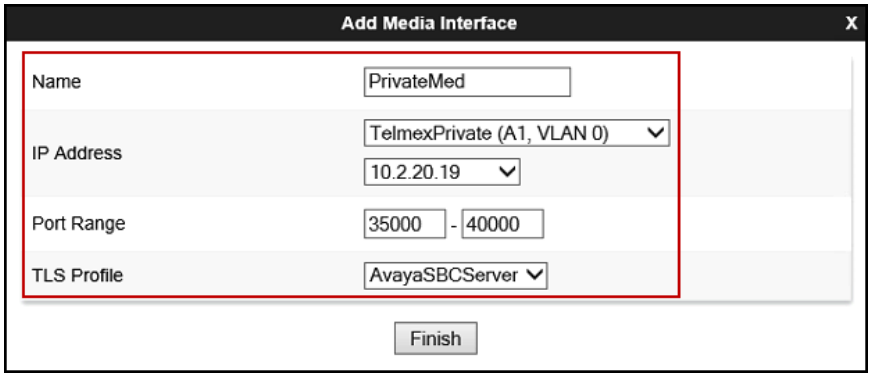


7.4. Media Interfaces

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

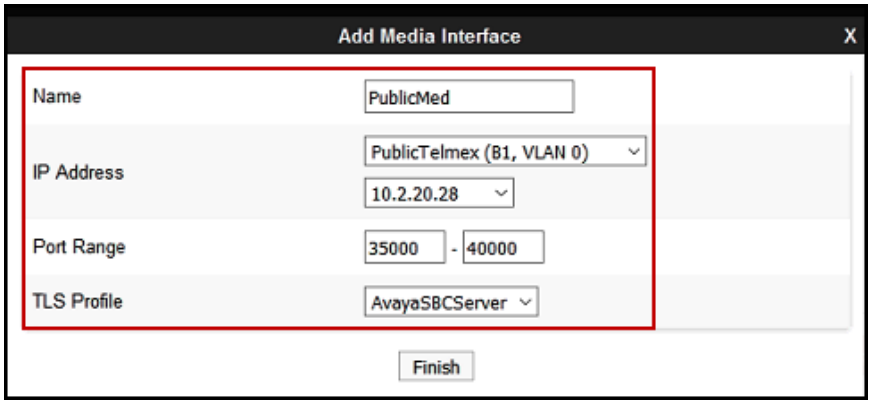
To add the Media Interface in the enterprise direction, select **Media Interface** from the **Device Specific Settings** menu on the left-hand side, select the device being managed and click the **Add** button (not shown).

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



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

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

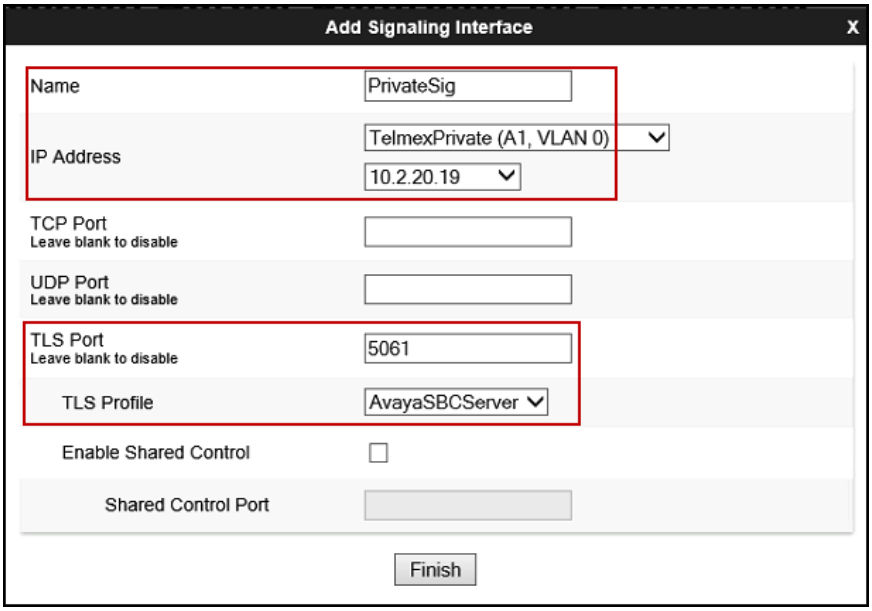


7.5. Signaling Interfaces

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

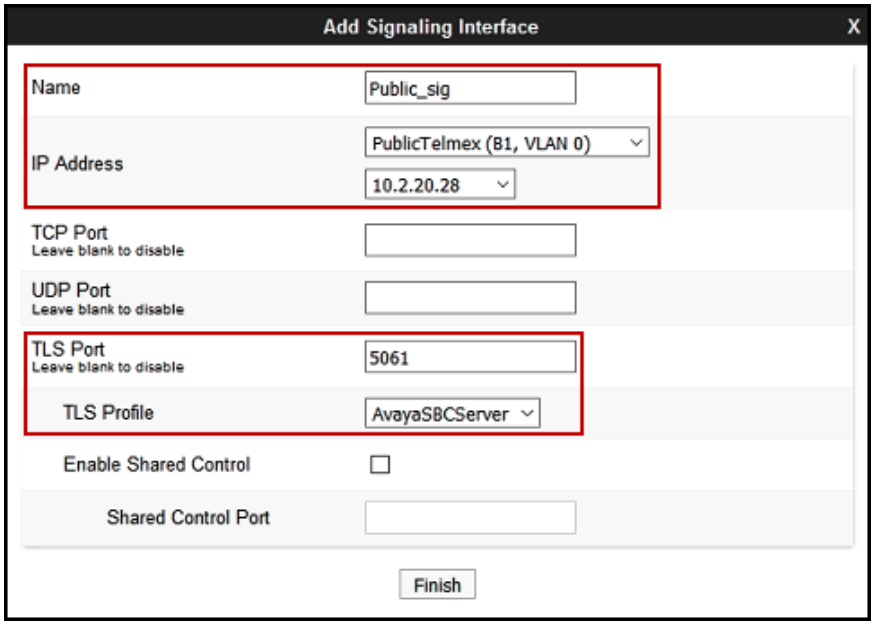
To add the Signaling Interface in the enterprise direction, select **Signaling Interface** from the **Device Specific Settings** menu on the left-hand side, select the device being managed and click the **Add** button (not shown).

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



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

- Under **IP Address**, select from the drop-down menus the network and IP address to be associated with this interface.
- Enter ***5061*** for **TLS Port**, since this is the protocol and port used by the Avaya SBCE to listen to the service provider's SIP traffic.
- Select a **TLS Profile**.
- Click **Finish**.

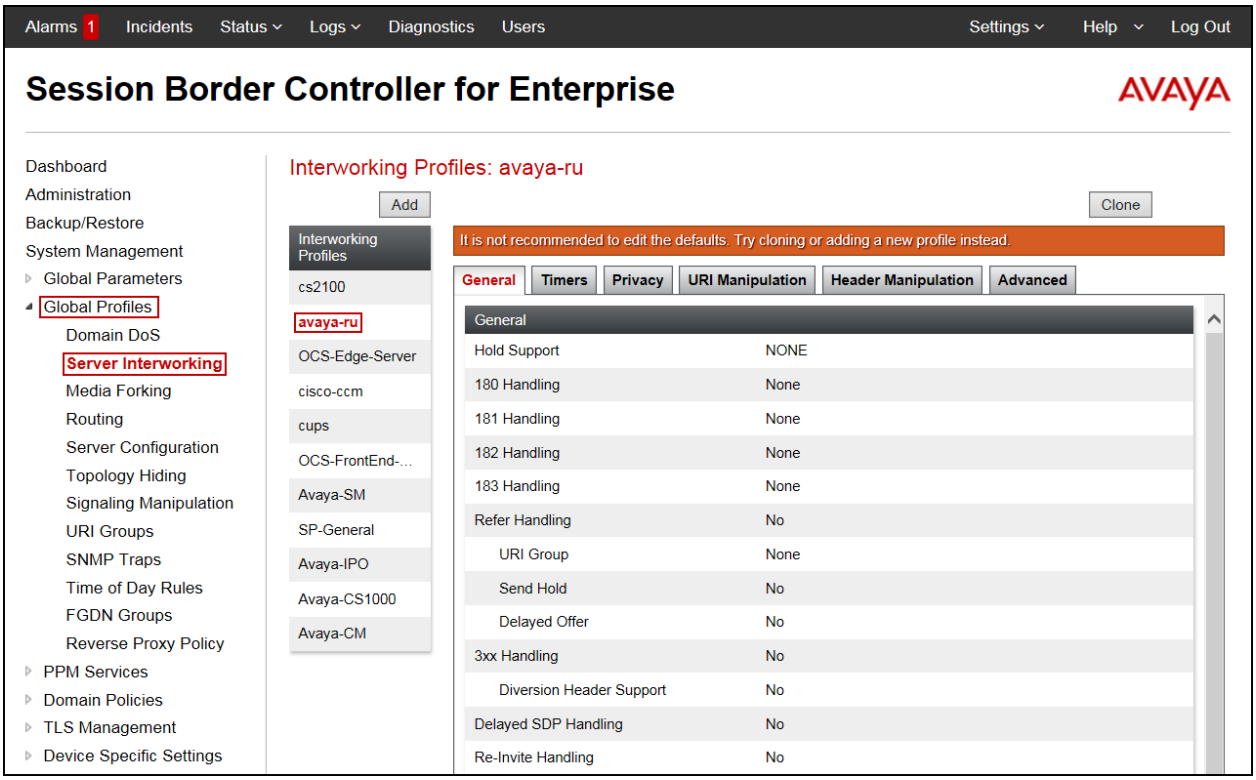


7.6. Server Interworking

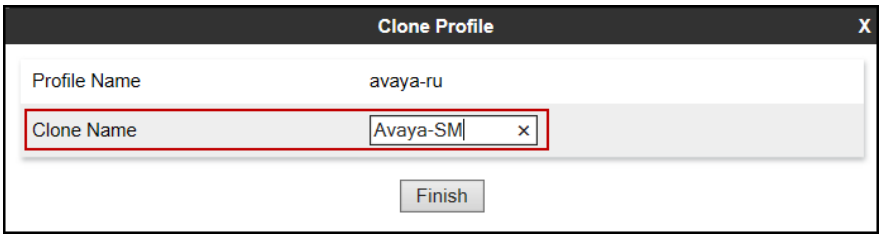
Interworking Profile features are configured to facilitate the interoperability between the enterprise SIP-enabled solution (Call Server) and the SIP trunk service provider (Trunk Server).

7.6.1. Server Interworking Profile – Enterprise

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

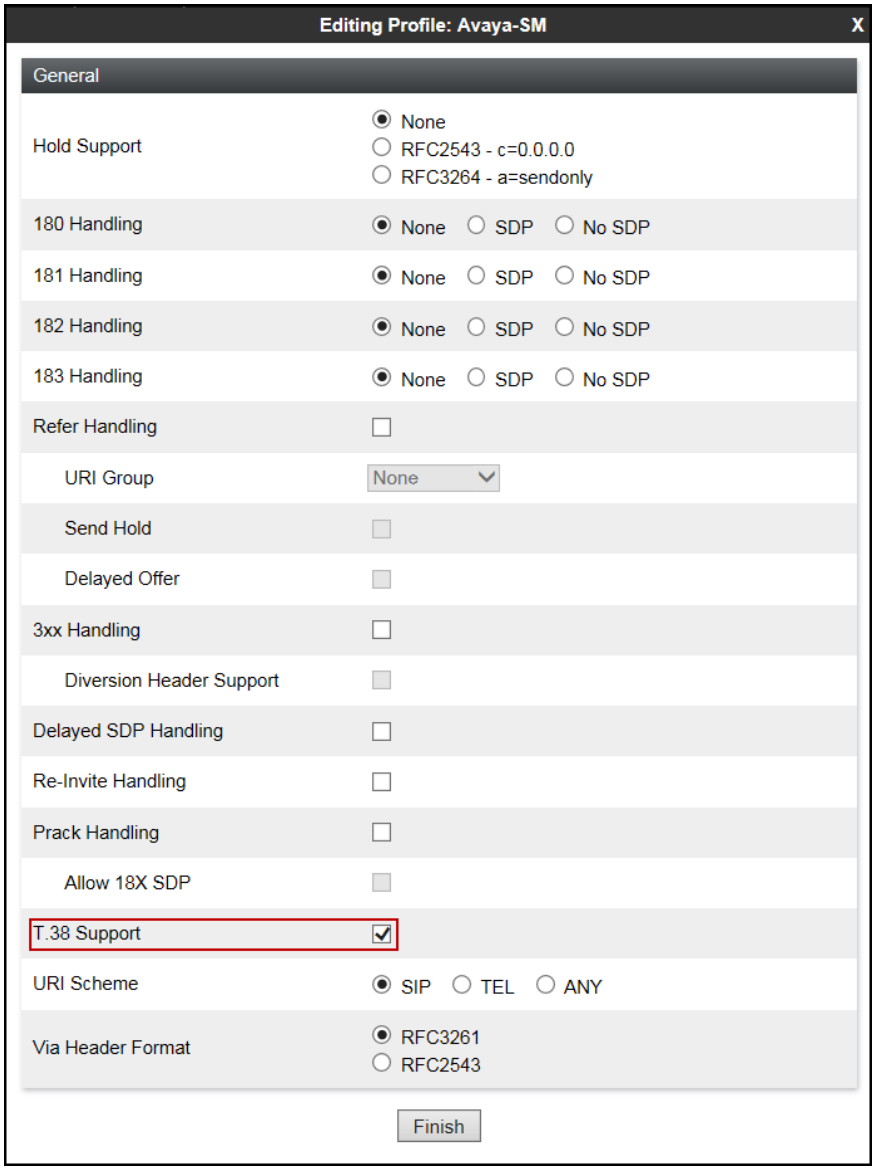


- Enter a descriptive name for the cloned profile.
- Click **Finish**.



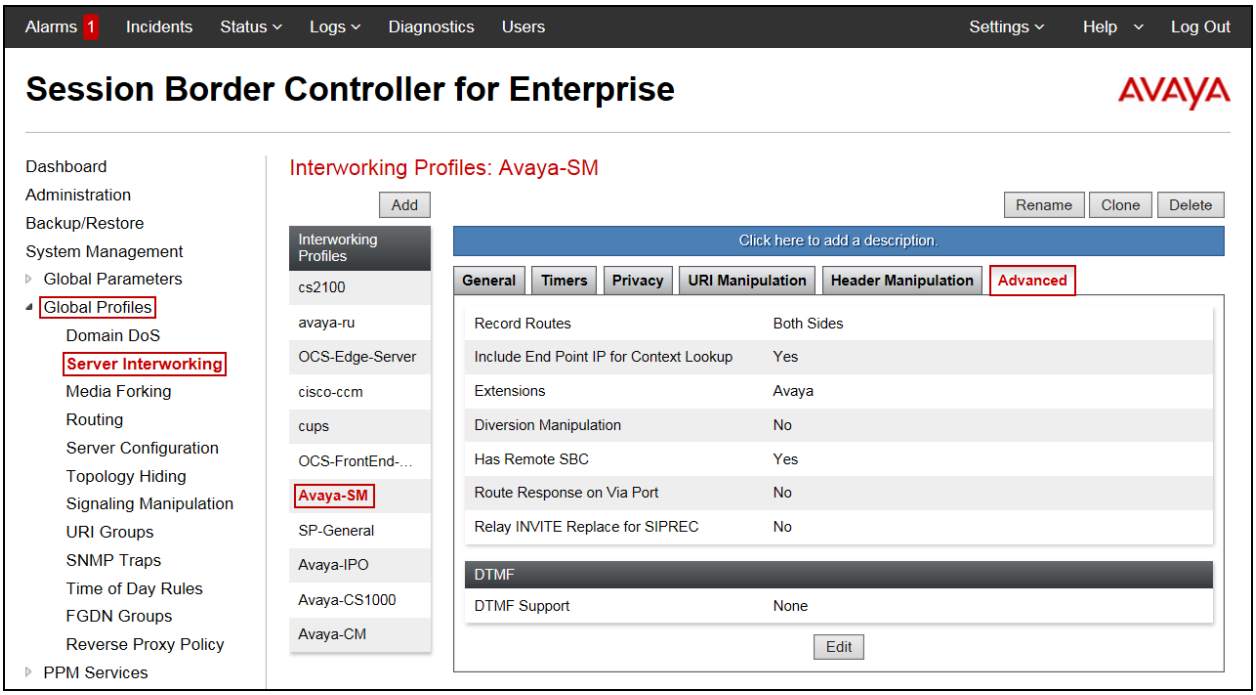
Click **Edit** on the newly cloned ***Avaya-SM*** interworking profile:

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



Note – Currently Telmex does not support T.38 fax in their SIP Trunk service offering, T.38 fax support was enabled for future use by Telmex.

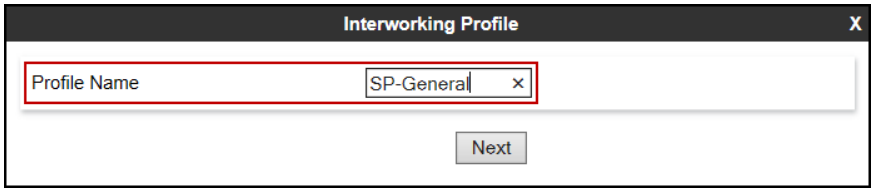
The **Timers**, **Privacy**, **URI Manipulation** and **Header Manipulation** tabs contain no entries. The **Advaced** tab settings are shown on the screen below:



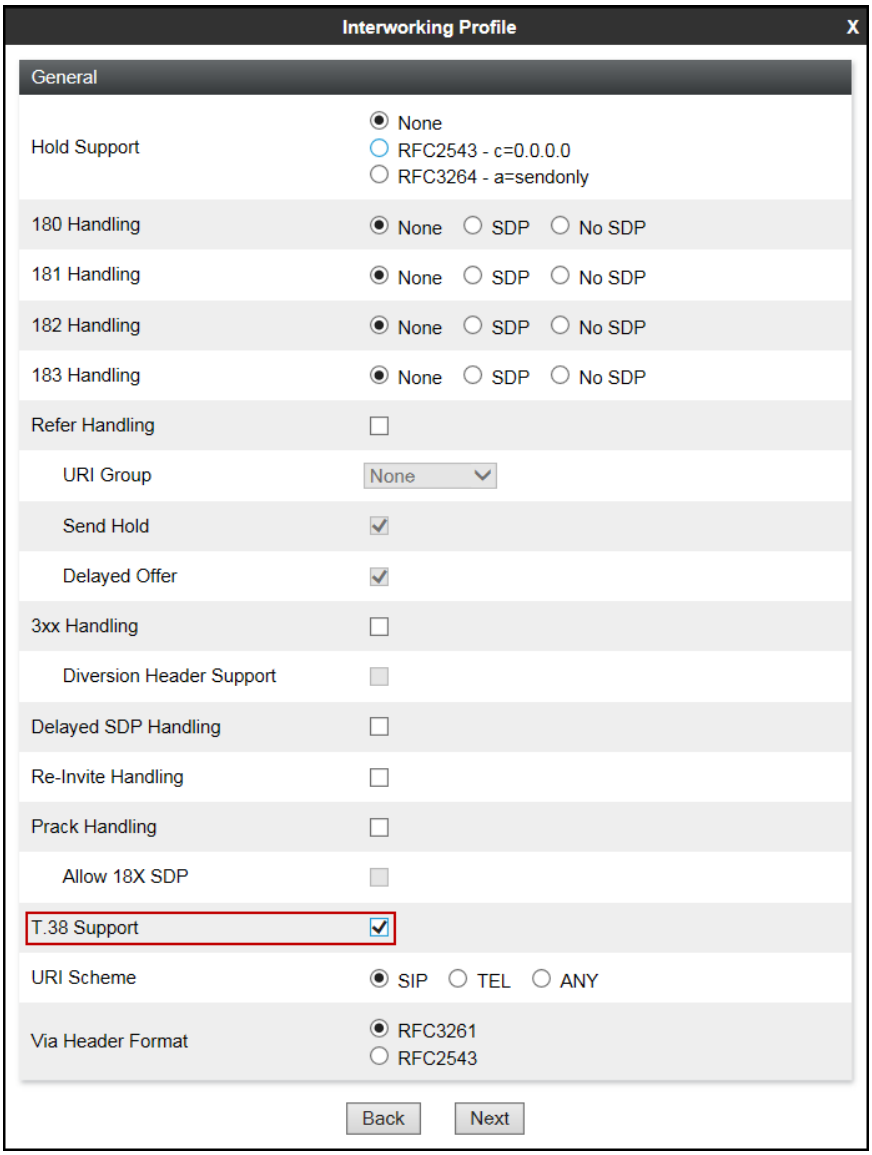
7.6.2. Server Interworking Profile – Service Provider

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

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

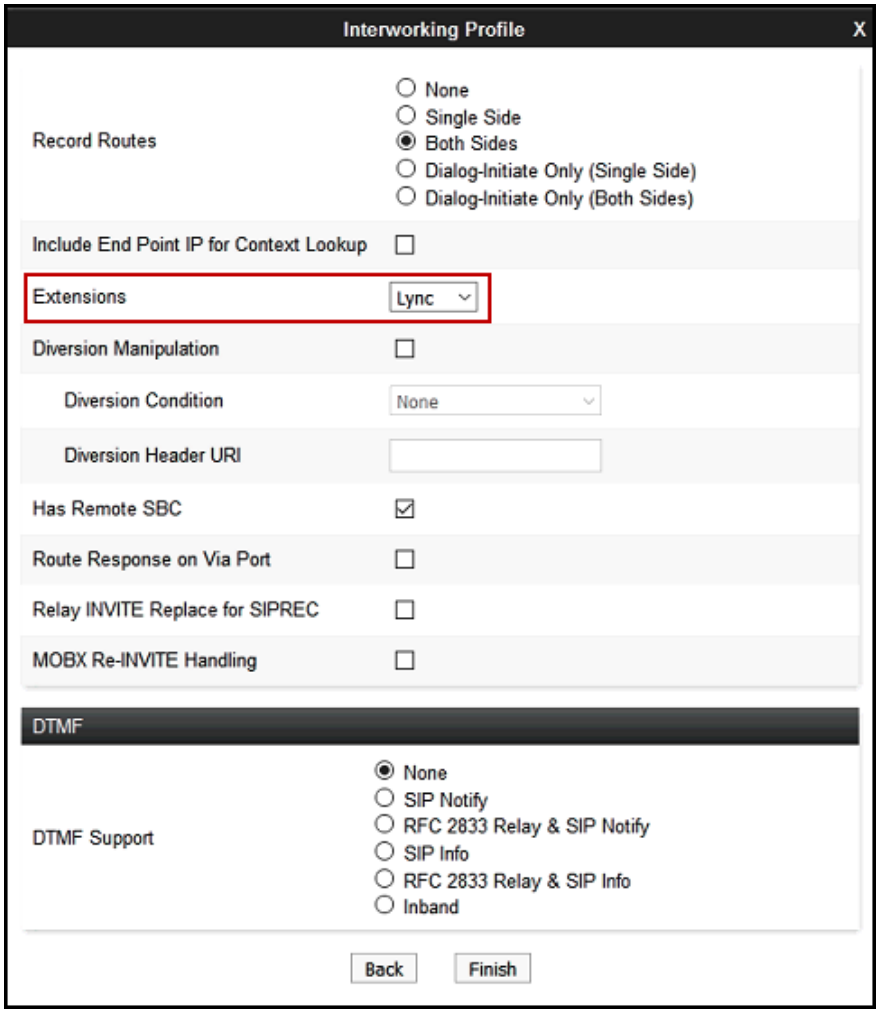


- On the **General** tab, check ***T.38 Support*** (See note below). Click **Next** until the last tab is reached.

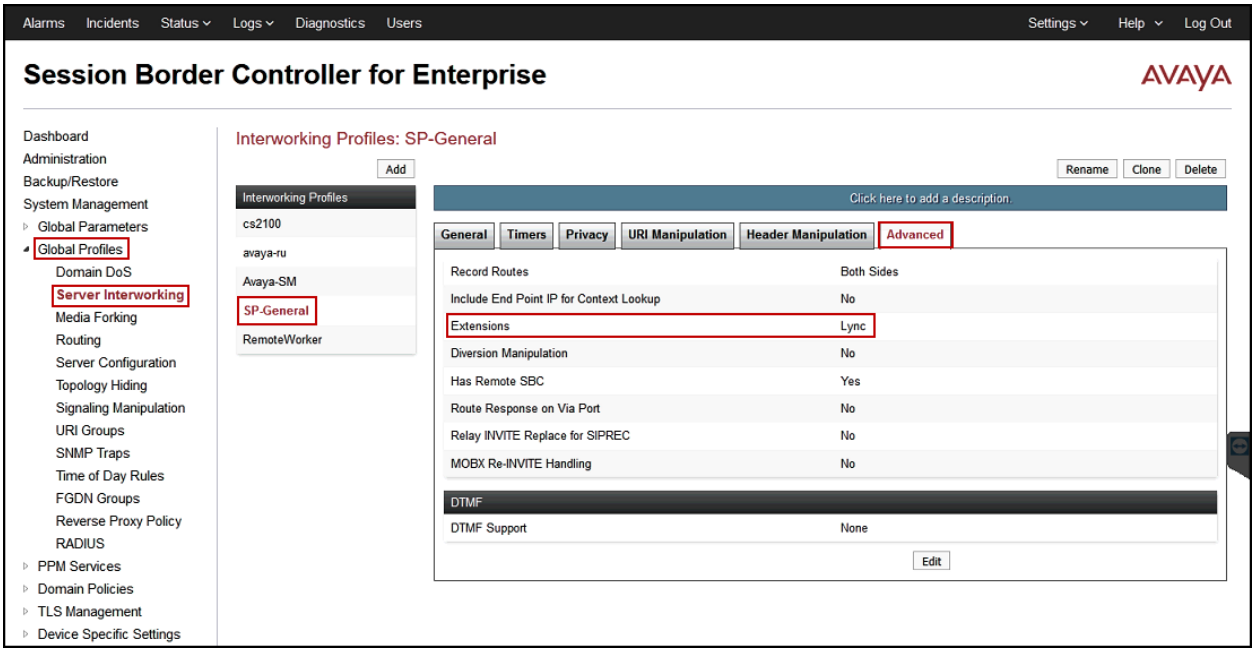


Note – Currently Telmex does not support T.38 fax in their SIP Trunk service offering, T.38 fax support was enabled for future use by Telmex.

On the lat tab select ***Lync*** under the **Extensions** pull down menu, then click **Finish**.



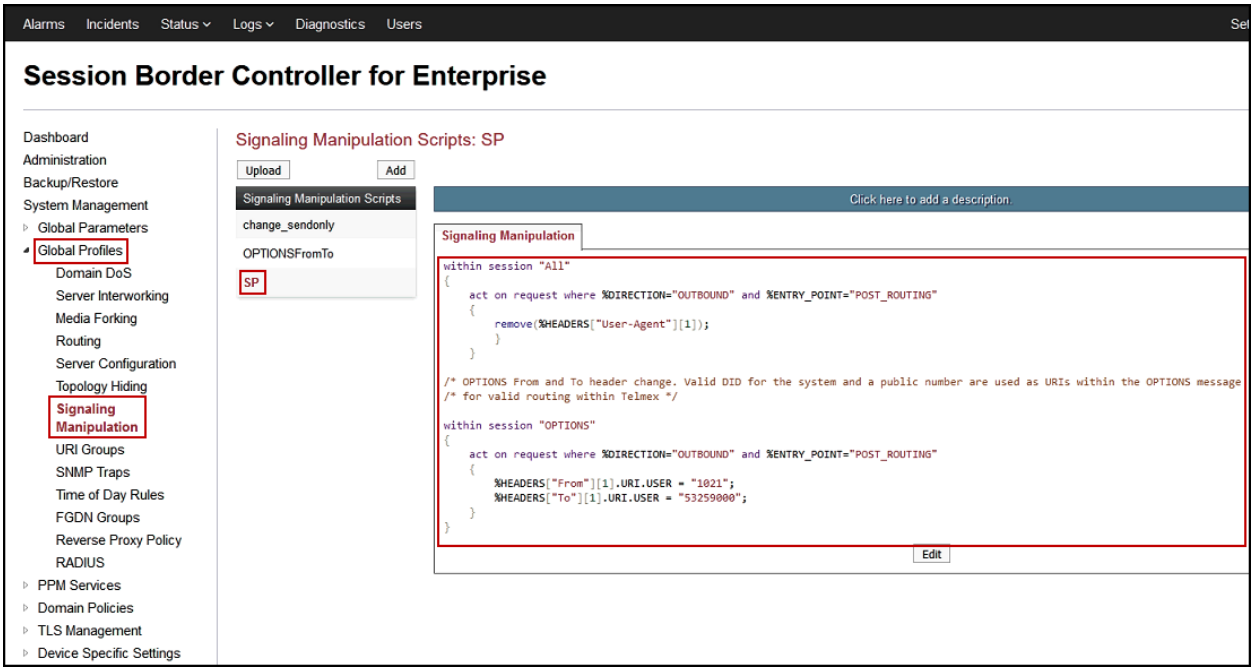
The **Advaced** tab settings are shown on the screen below:



7.7. Signaling Manipulation

A SigMa script was created to change the OPTION messages sent to Telmex, this was necessary in order for the OPTION messages to be accepted by Telmex.

To add a Signaling Manipulation script, from the **Global Profiles** menu on the left panel, select **Signaling Manipulation**. Click **Add** to open the SigMa Editor screen, where the text of the script can be entered or copied.



The details of the script used can also be found in **Appendix A** in this document.

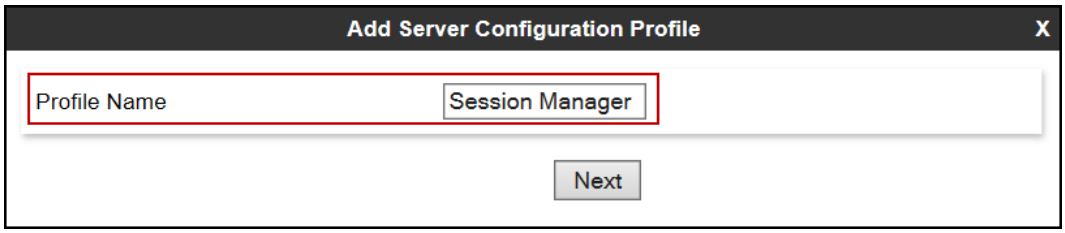
7.8. Server Configuration

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

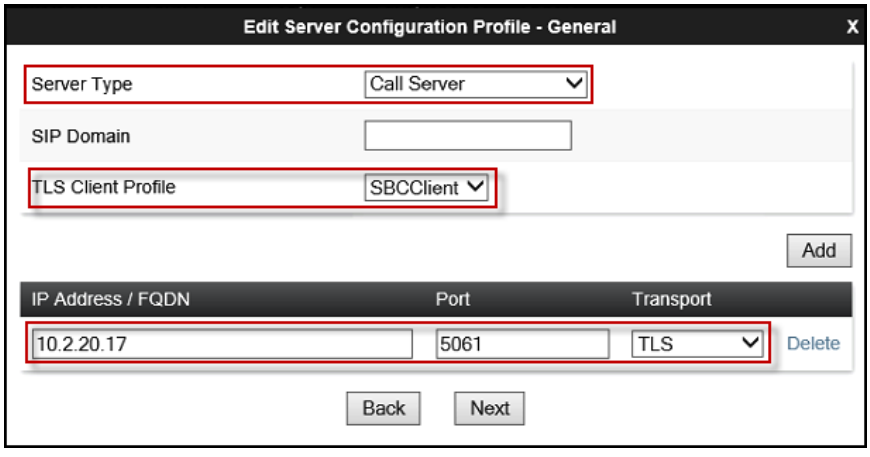
7.8.1. Server Configuration Profile – Enterprise

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

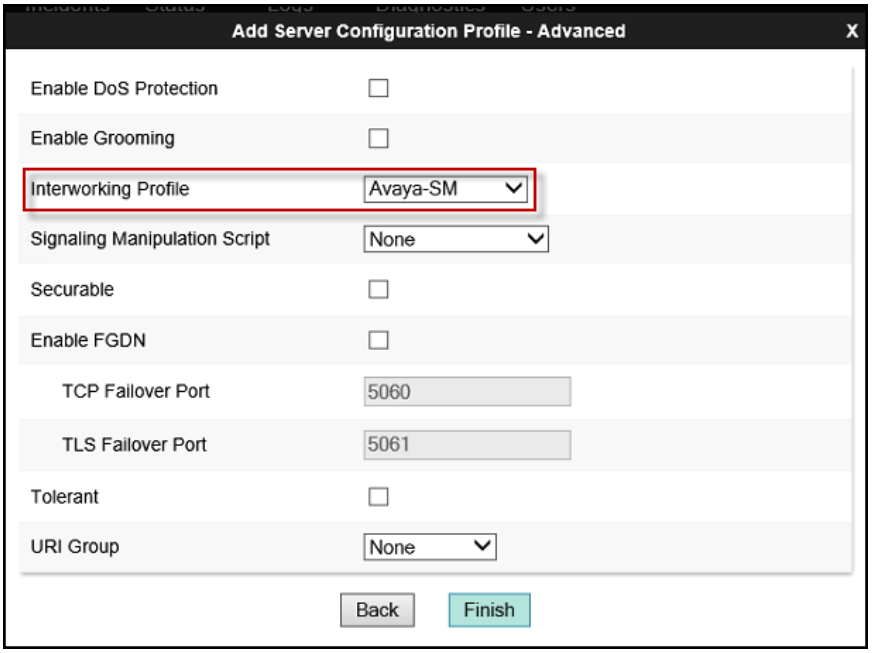
- Enter an appropriate **Profile Name** similar to the screen below.
- Click **Next**.



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



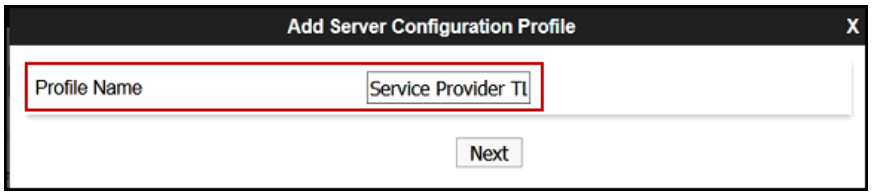
- Click **Next** on the **Authentication** and **Heartbeat** tabs (not shown).
- Select ***Avaya-SM*** from the **Interworking Profile** drop down menu.
- Click **Finish**.



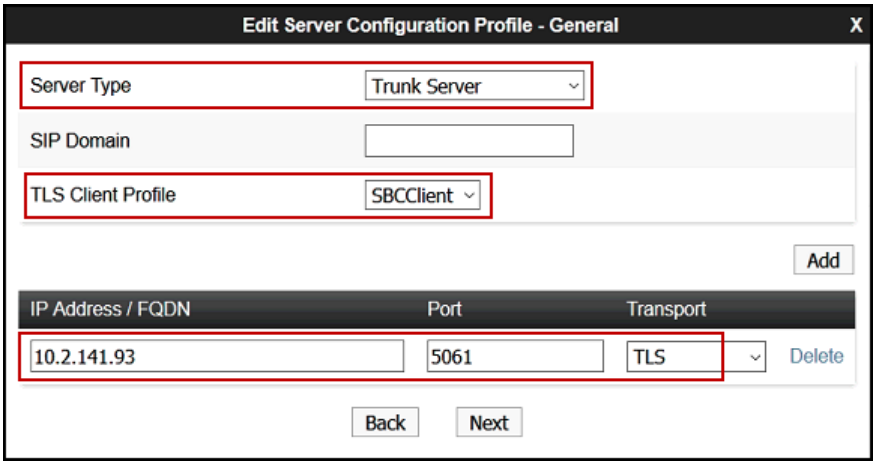
7.8.2. Server Configuration Profile – Service Provider

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

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



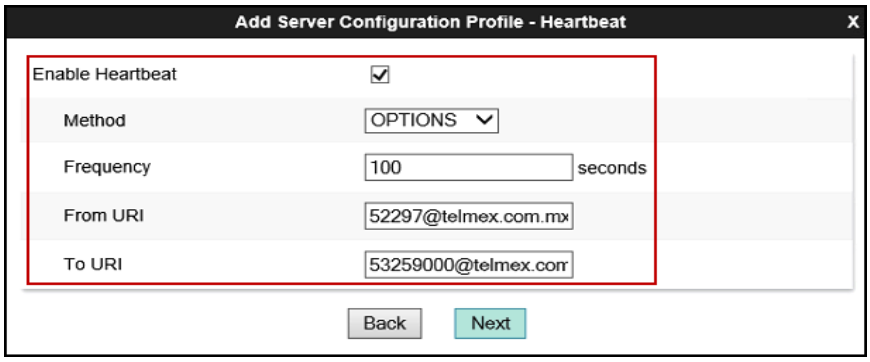
- On the **Edit Server Configuration Profile - General** Tab select ***Trunk Server*** from the drop down menu for the **Server Type**.
- On the **IP Addresses / FQDN** field, enter Telmex's proxy IP address (See figure 1).
- Enter ***5061*** under **Port**, and select **TLS** for **Transport** for both entries.
- Select a **TLS Client Profile**.
- Click **Next**.



Click next on the **Add Server Configuration Profile - Authentication** window.

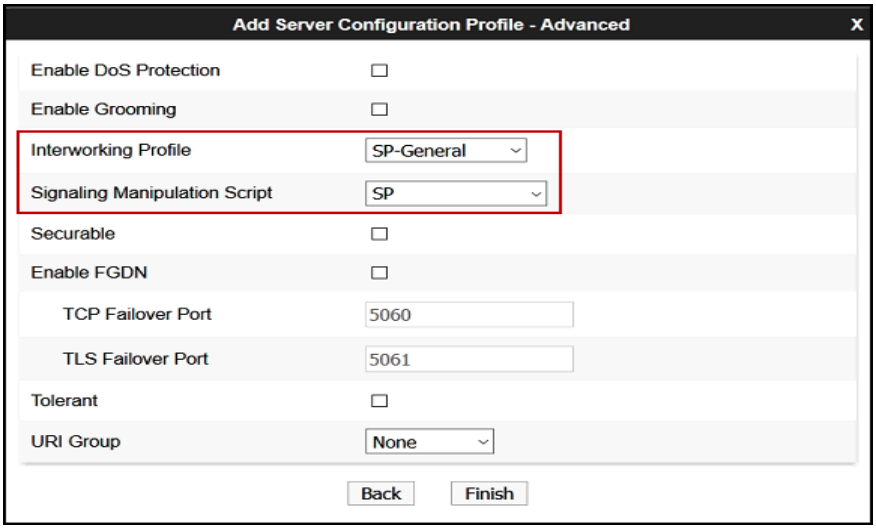
On the **Add Server Configuration Profile - Heartbeat** window:

- Check the **Enable Heartbeat** box.
- Under **Method**, select ***OPTIONS*** from the drop down menu.
- **Frequency:** Enter the amount of time (in seconds), ***100*** seconds was the value used during the compliance test.
- The **From URI** and **To URI** entries for the OPTION messages are built using the following:
  - **From URI**: An internal extension number was entered (52297) and the enterprise domain name (***telmex.com.mx***), as shown on the screen below.
  - **To URI**: An external extension number was entered (53259000) and the Service Provider's domain name (***telmex.com***), as shown on the screen below.
- Click **Next**.



Click next on the **Add Server Configuration Profile - Ping** window

- On the **Add Server Configuration Profile - Advanced** tab, select ***SP-General*** from the **Interworking Profile** and ***SP*** from the **Signaling Manipulation Script** windows created in **Section 7.7**.
- Click **Finish**.



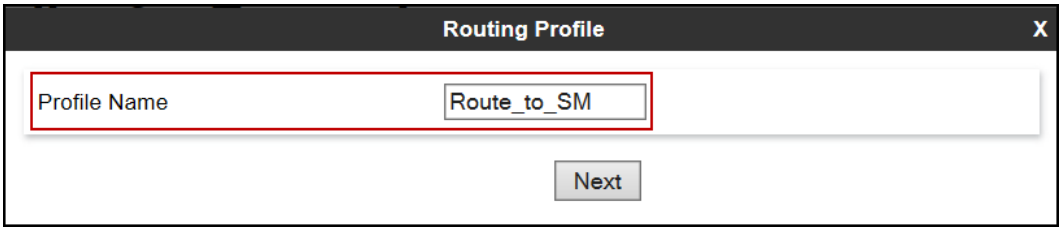
7.9. Routing

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

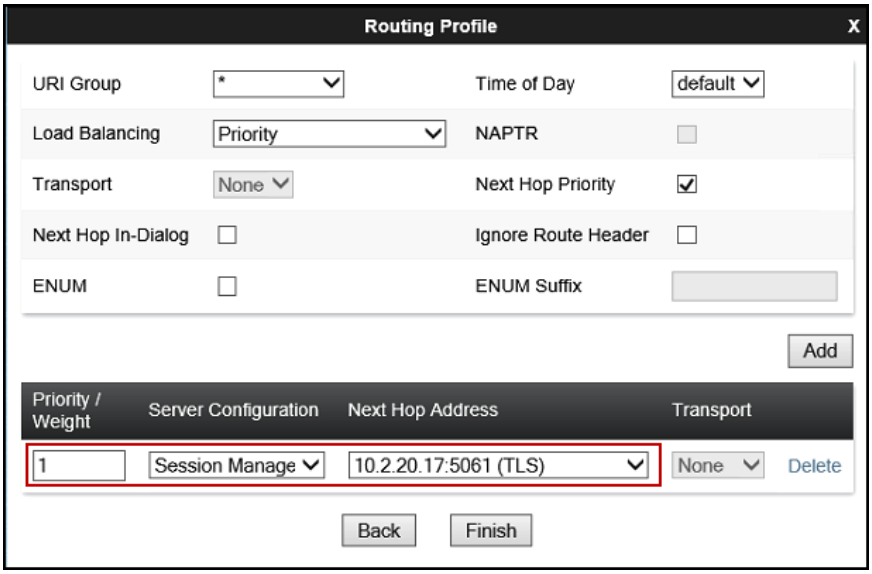
7.9.1. Routing Profile – Enterprise

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

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



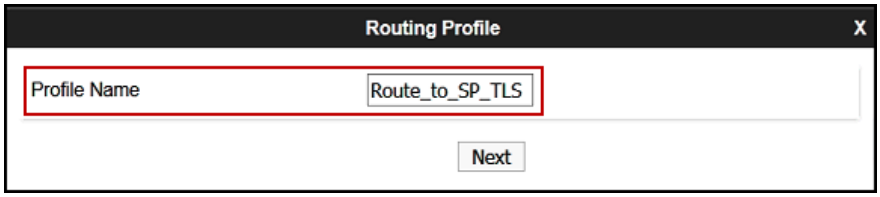
- On the **Routing Profile** tab, click the **Add** button to enter the next-hop address.
- Under **Server Configuration**, select ***Session Manager***. The **Next Hop Address** field will be populated with the IP address, port and protocol defined for the Session Manager Server Configuration Profile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



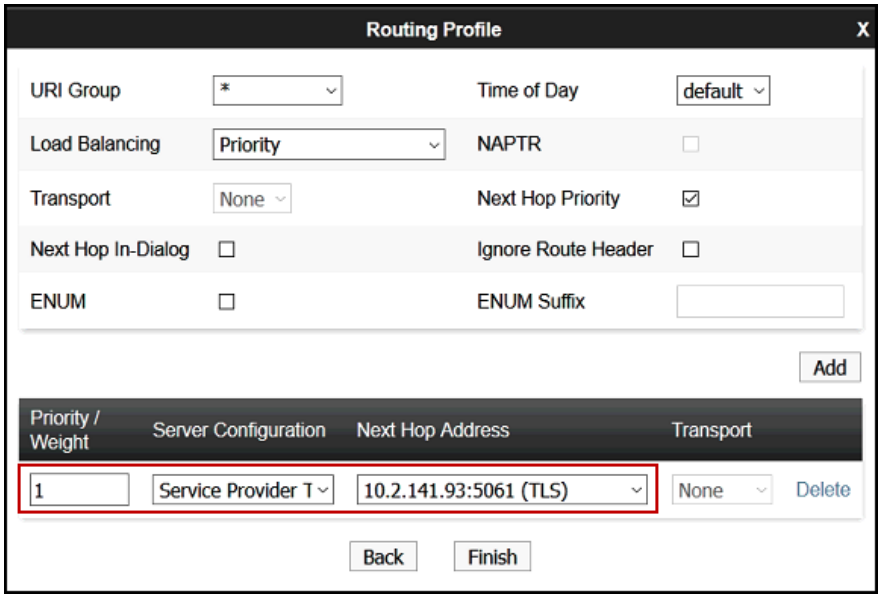
7.9.2. Routing Profile – Service Provider

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

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



- On the **Routing Profile** tab, click the **Add** button to enter the next-hop address. Under **Server Configuration**, select the Server Configuration for the Service Provider created in **Section 7.8.2**. The **Next Hop Address** field will be populated with the IP address, port and protocol defined for the Service Provider Server Configuration Profile in **Section 7.8.2**.
- Defaults were used for all other parameters.
- Click **Finish**.



7.10. Topology Hiding

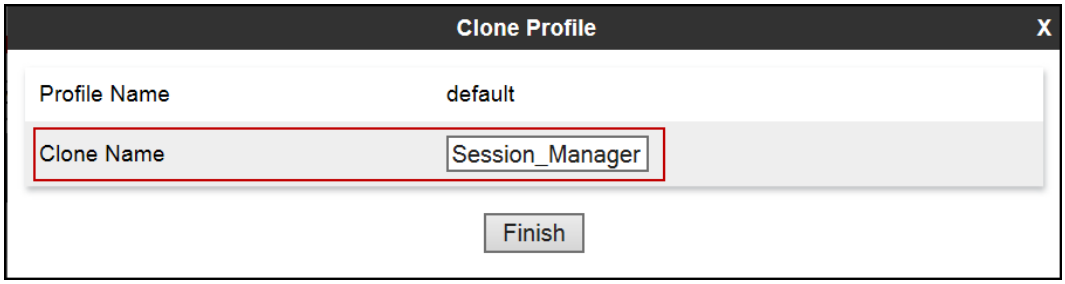
Topology Hiding is a security feature that allows the modification of several SIP headers, preventing private enterprise network information from being propagated to the untrusted public network.

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

7.10.1. Topology Hiding Profile – Enterprise

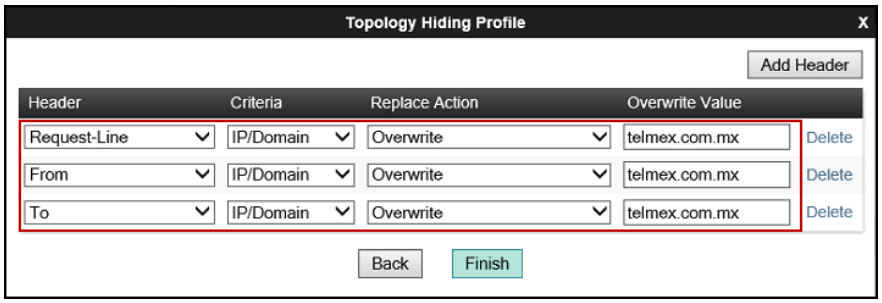
To add the Topology Hiding Profile in the enterprise direction, select **Topology Hiding** from the **Global Profiles** menu on the left-hand side, select ***default*** from the list of pre-defined profiles and click the **Clone** button (not shown).

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



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

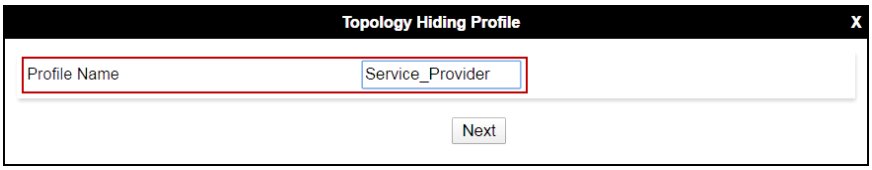
- For the, **From**, **To** and **Request-Line** headers, select ***Overwrite*** in the **Replace Action** column and enter the enterprise SIP domain ***telmex.com.mx***, in the **Overwrite Value** column of these headers, as shown below. This is the domain known by Session Manager, defined in **Section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



7.10.2. Topology Hiding Profile – Service Provider.

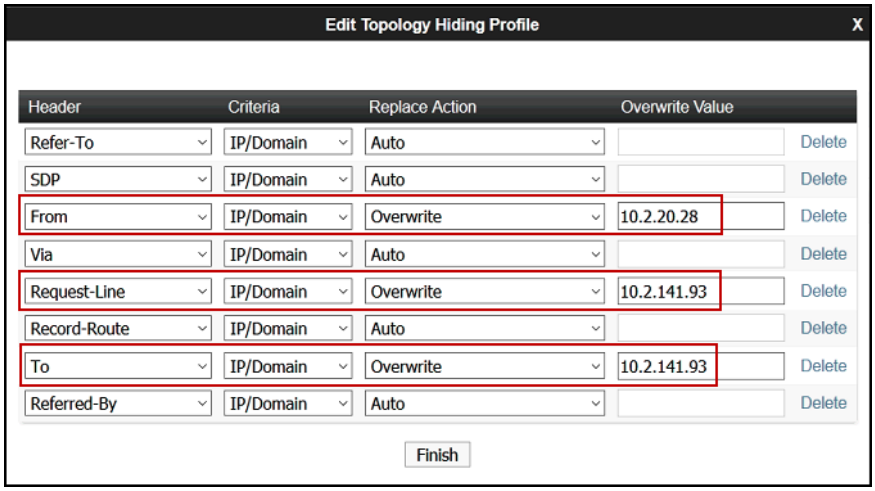
To add the Topology Hiding Profile in the Service Provider direction, select **Topology Hiding** from the **Global Profiles** menu on the left-hand side, select ***default*** from the list of pre-defined profiles and click the **Clone** button (not shown).

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



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

- For the, **From**, **To** and **Request-Line** headers, select ***Overwrite*** in the **Replace Action** column and enter IP addresses in the **Overwrite Value** column of these headers, as follows: **From**: Avaya SBCE public IP address (***10.2.20.28***), **Request-Line**: Telmex SIP Proxy IP address (***10.2.141.93***), **To**: Telmex SIP Proxy IP address (***10.2.141.93***).
- Default values were used for all other fields.
- Click **Finish**.



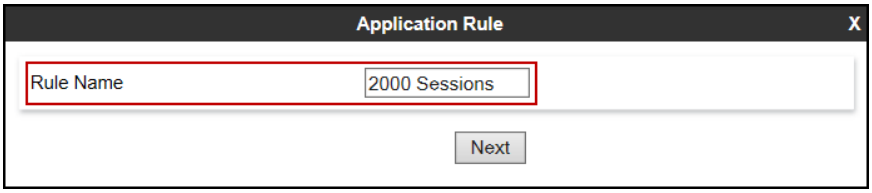
7.11. Domain Policies

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

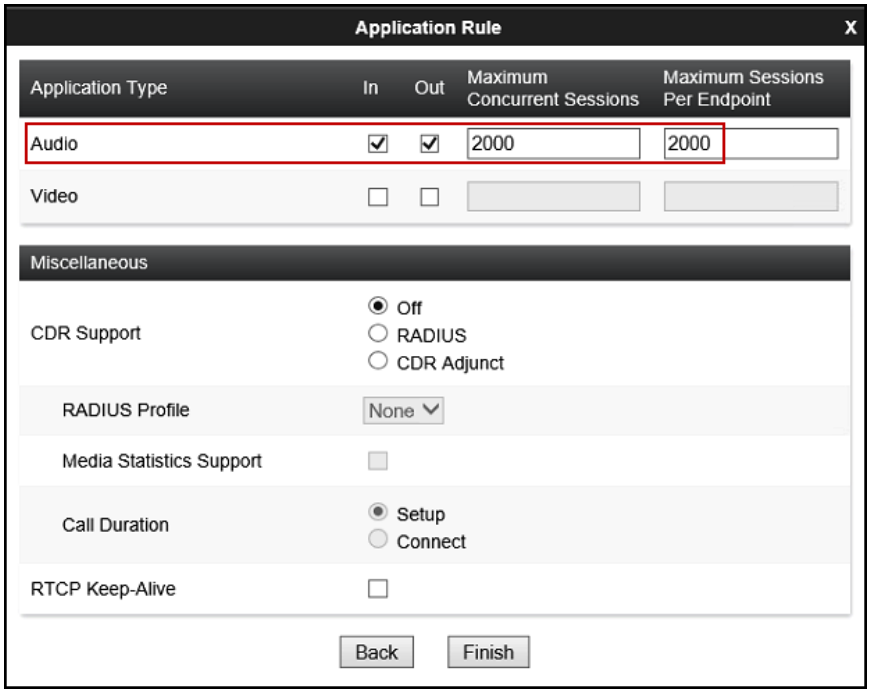
7.11.1. Application Rules

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

- Under **Rule Name** enter the name of the profile, e.g., ***2000 Sessions***.
- Click **Next**.



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

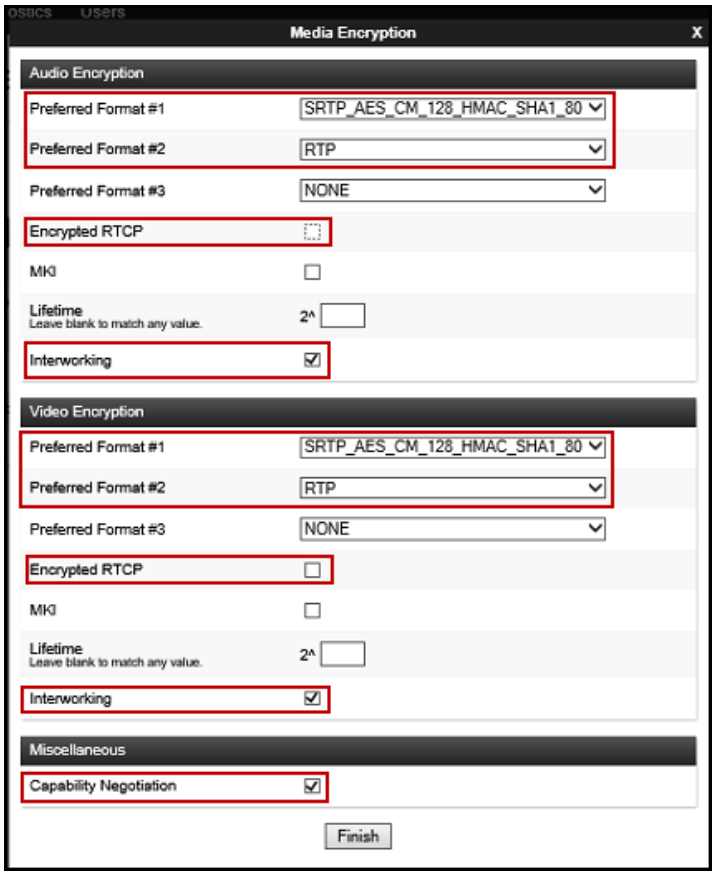


7.11.2. Media Rules

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

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

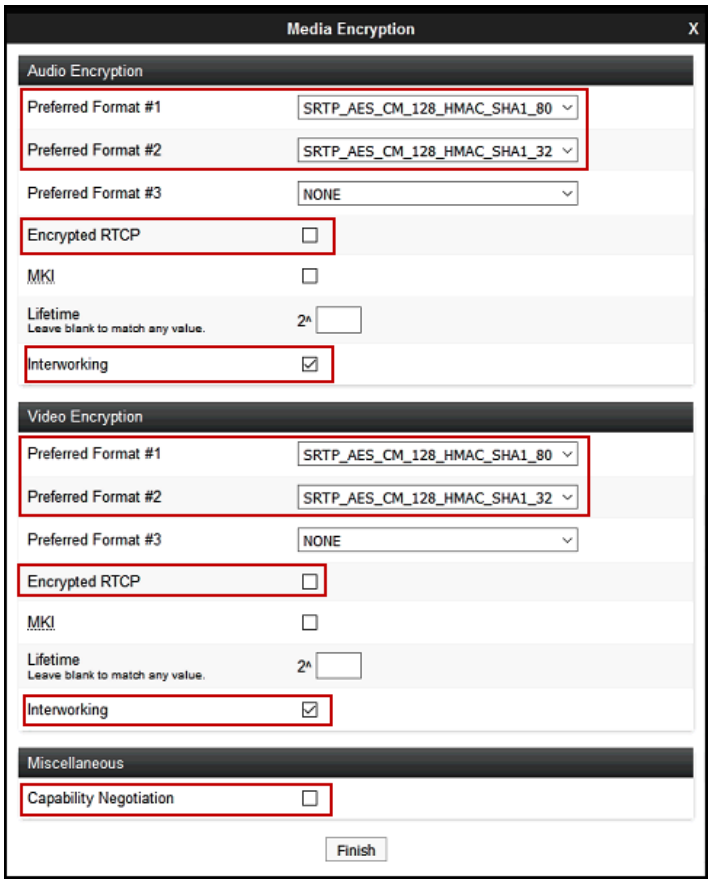
- Click on the **Add** button to add a new media rule (not shown).
- Under **Rule Name** enter ***SM_SRTP*** (not shown).
- Click **Next** (not shown).
- Under Audio Encryption, **Preferred Format #1**, select ***SRTP_AES_CM_128_HMAC_SHA1_80***.
- Under Audio Encryption, **Preferred Format #2**, select ***RTP***.
- Under Audio Encryption, uncheck ***Encrypted RTCP***.
- Under Audio Encryption, check ***Interworking***.
- Repeat the above steps under Video Encryption.
- Under Miscellaneous verify that ***Capability Negotiation*** is checked.
- Click **Next**.



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

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

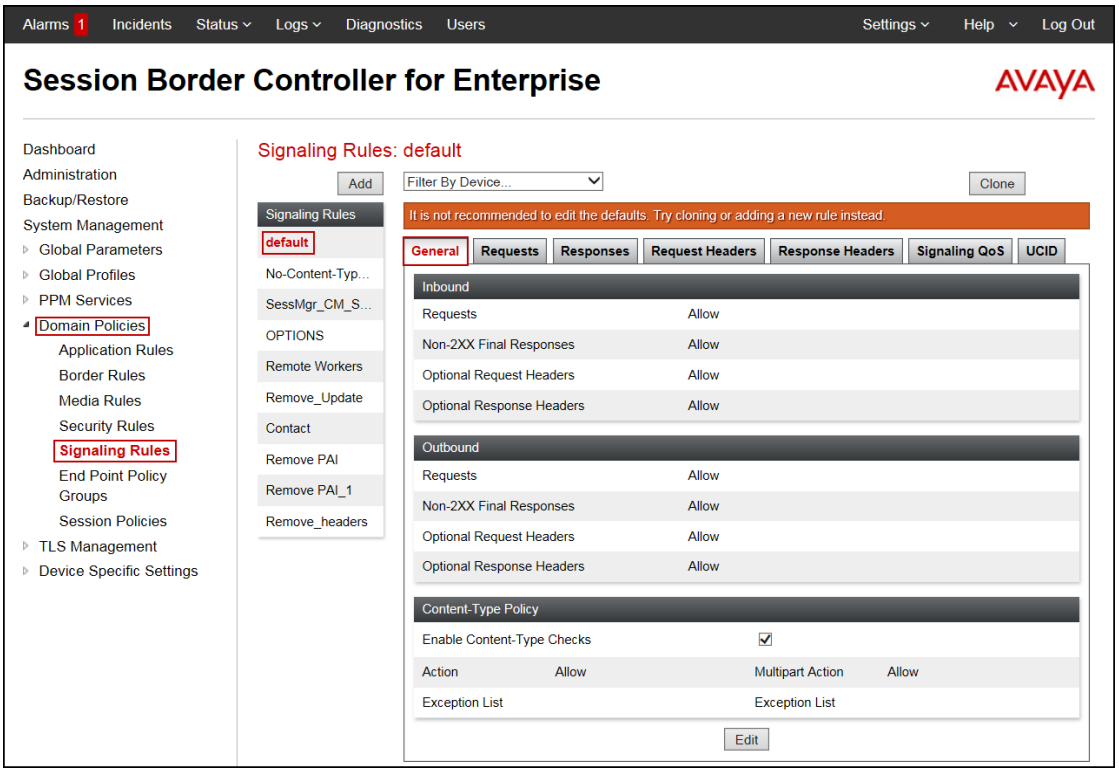
- Click on the **Add** button to add a new media rule (not shown).
- Under **Rule Name** enter ***SP_SRTP*** (not shown).
- Click **Next** (not shown).
- Under Audio Encryption, **Preferred Format #1**, select ***SRTP_AES_CM_128_HMAC_SHA1_80***.
- Under Audio Encryption, **Preferred Format #2**, select ***SRTP_AES_CM_128_HMAC_SHA1_32***.
- Under Audio Encryption, uncheck ***Encrypted RTCP***.
- Under Audio Encryption, check ***Interworking***.
- Repeat the above steps under Video Encryption.
- Under Miscellaneous verify that ***Capability Negotiation*** is unchecked.
- Click **Next**.



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

7.11.3. Signaling Rules

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



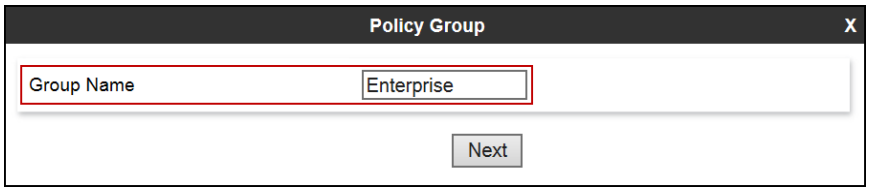
7.12. End Point Policy Groups

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

7.12.1. End Point Policy Group – Enterprise

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

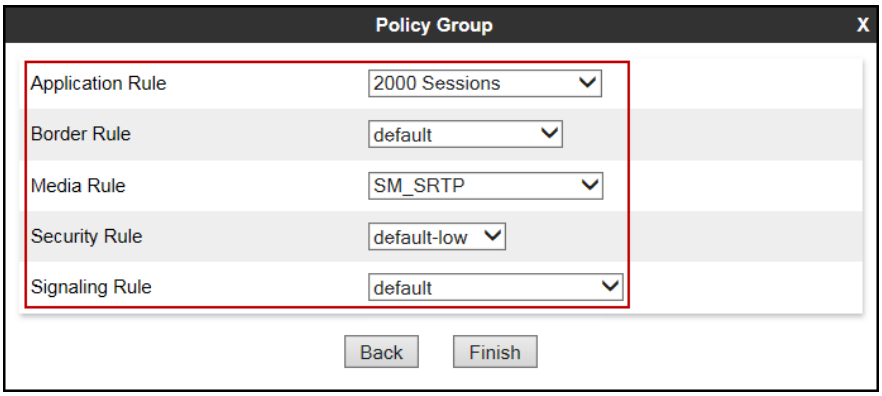
- Enter an appropriate name in the **Group Name** field.
- Click **Next**.



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

- **Application Rule:** ***2000 Sessions*** **(Section 7.11.1).**
- **Border Rule:** ***default.***

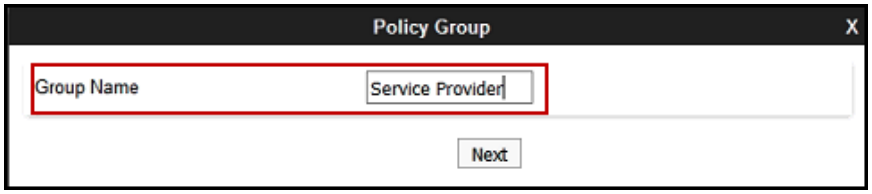
- **Media Rule: *SM_SRTP*** (**Section 7.11.2**).
- **Security Rule: *default-low***.
- **Signaling Rule: *default*** (**Section 7.11.3**).
- Click **Finish**.



7.12.2. End Point Policy Group – Service Provider

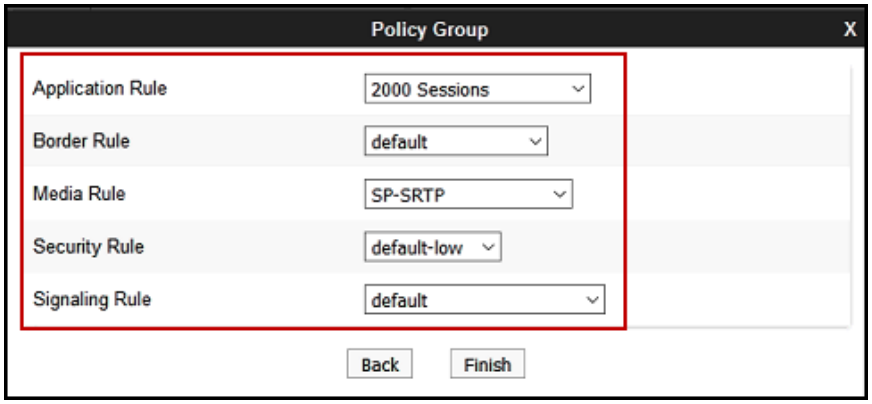
To create an End Point Policy Group for the Service Provider, select **End Point Policy Groups** under the **Domain Policies** menu and select **Add** (not shown).

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



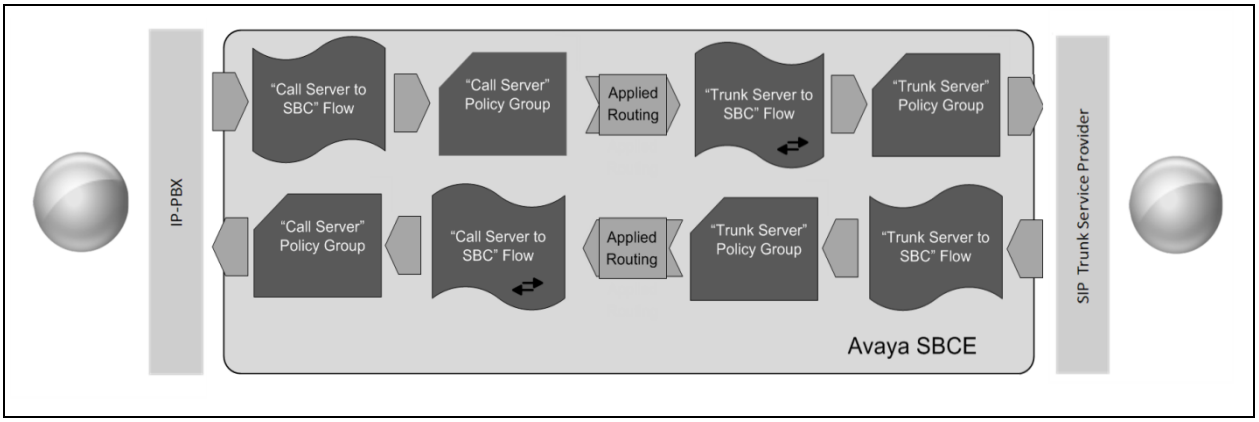
Under the **Policy Group** tab enter the following:

- **Application Rule:** ***2000 Sessions*** (**Section 7.11.1**).
- **Border Rule:** ***default.***
- **Media Rule:** ***SP_SRTP*** (**Section 7.11.2**).
- **Security Rule:** ***default-low***.
- **Signaling Rule:** ***default*** (**Section 7.11.3**).
- Click **Finish**.



7.13. End Point Flows

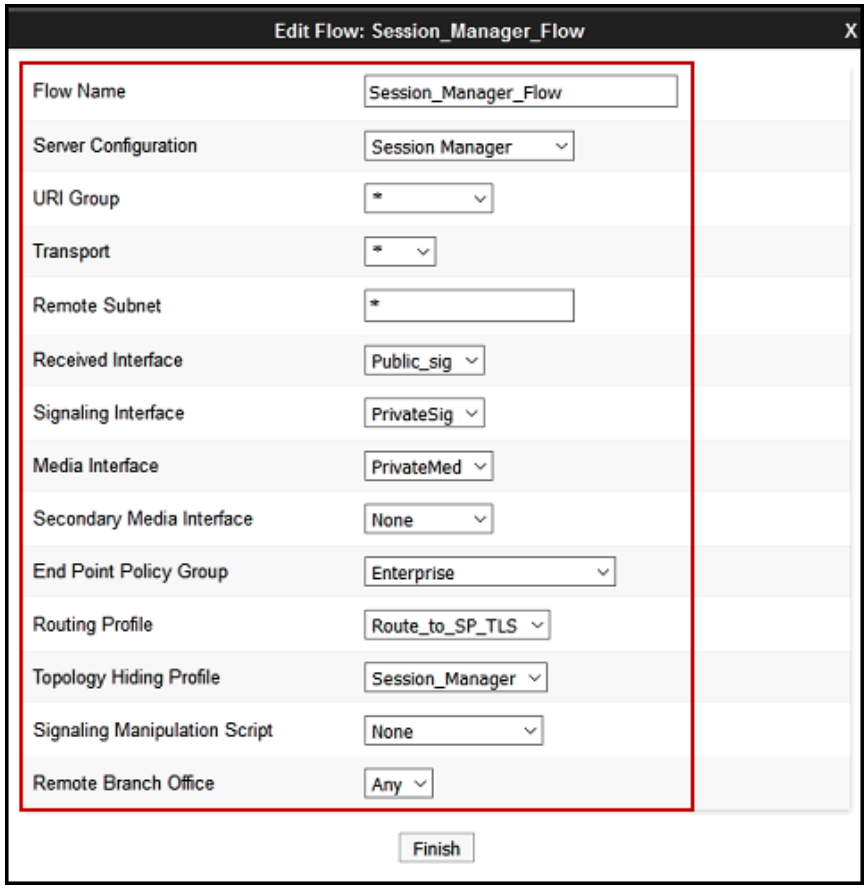
When a packet is received by Avaya SBCE, the content of the packet (IP addresses, URIs, etc.) is used to determine which flow it matches. Once the flow is determined, the flow points to a policy group which contains several rules concerning processing, privileges, authentication, routing, etc. Once routing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



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

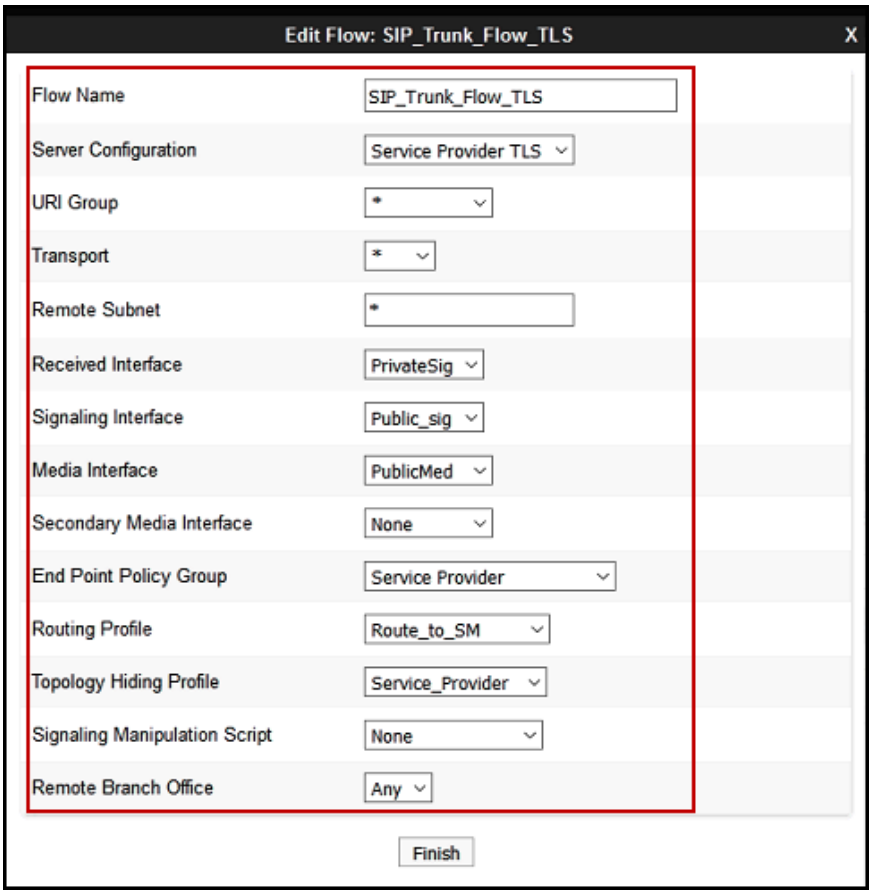
7.13.1. End Point Flow – Enterprise

To create the call flow toward the enterprise, from the **Device Specific** menu, select **End Point Flows**, then select the **Server Flows** tab. Click **Add** (not shown). The screen below shows the flow named ***Session_Manager_Flow*** created in the sample configuration. The flow uses the interfaces, policies, and profiles defined in previous sections. Note that the **Routing Profile** selection is the profile created for the Service Provider in **Section 7.9.2**, which is the reverse route of the flow. Click **Finish**.



7.13.2. End Point Flow – Service Provider

A second Server Flow with the name ***SIP_Trunk_Flow_TLS*** was similarly created in the Service Provider direction. The flow uses the interfaces, policies, and profiles defined in previous sections. Note that the **Routing Profile** selection is the profile created for Session Manager in **Section 7.9.1**, which is the reverse route of the flow. Also note that there is no selection under the **Signaling Manipulation Script** field. Click **Finish**.



8. Telmex SIP Trunk Service Configuration

To use Telmex SIP Trunk Service, a customer must request the service from Telmex using the established sales processes. The process can be started by contacting Telmex via the corporate web site at: http://telmex.com/en/web/empresas

During the signup process, Telmex and the customer will discuss details about the preferred method to be used to connect the customer's enterprise network to Telmex's network. Telmex will provide their SIP Proxy public IP address, Direct Inward Dialed (DID) numbers to be assigned to the enterprise, etc. This information is used to complete the Avaya Aura® Communication Manager, Avaya Aura® Session Manager and Avaya Session Border Controller for Enterprise configuration discussed in the previous sections.

9. Verification and Troubleshooting

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

9.1. General Verification Steps

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

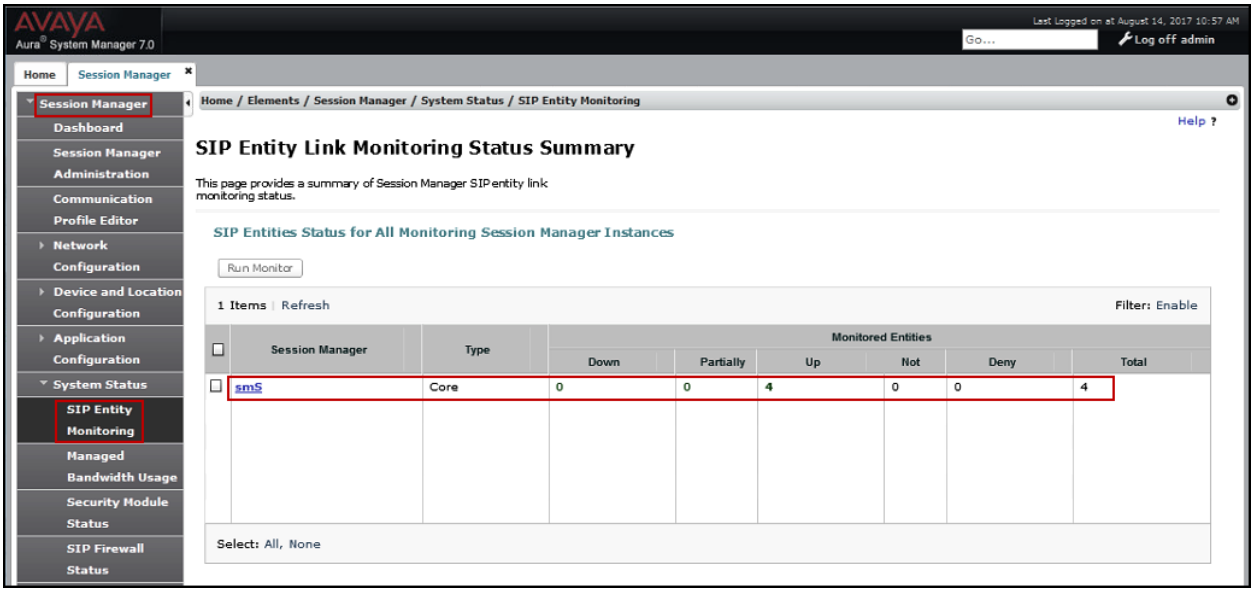
9.2. Communication Manager Verification

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

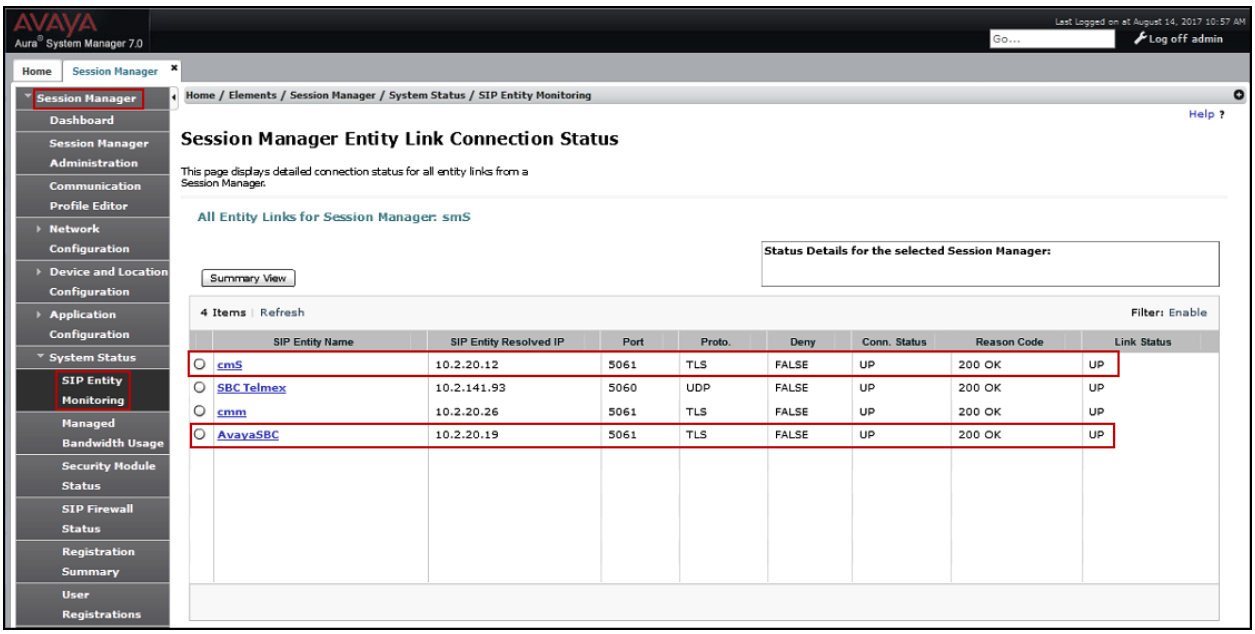
- **list trace station** <extension number>
  Traces calls to and from a specific station.
- **list trace tac** <trunk access code number>
  Trace calls over a specific trunk group.
- **status signaling-group** <signaling group number>
  Displays signaling group service state.
- **status trunk** <trunk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

9.3. Session Manager Verification

Log in to System Manager. Under the **Elements** section, navigate to **Session Manager → System Status → SIP Entity Monitoring**. Click the Session Manager instance (***smS*** in the example below).



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



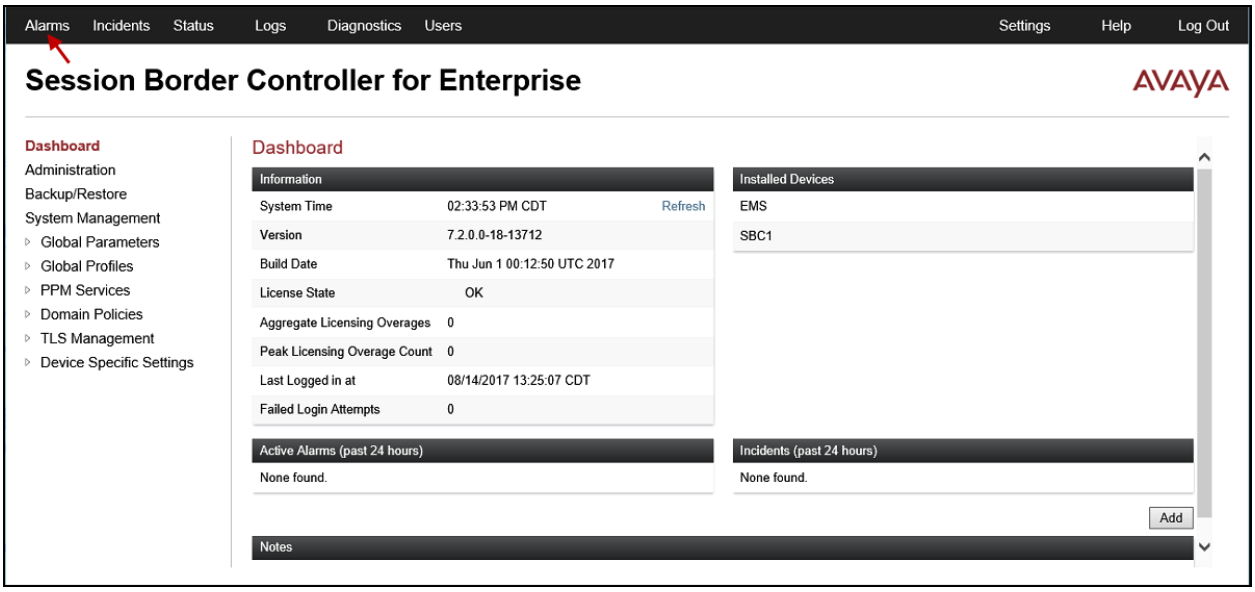
Other Session Manager useful verification and troubleshooting tools include:

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

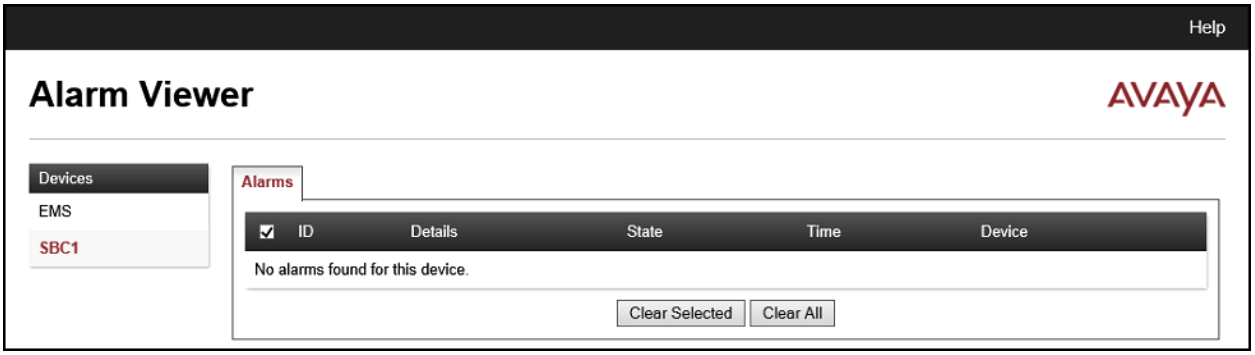
9.4. Avaya SBCE Verification

There are several links and menus located on the taskbar at the top of the screen of the web interface that can provide useful diagnostic or troubleshooting information.

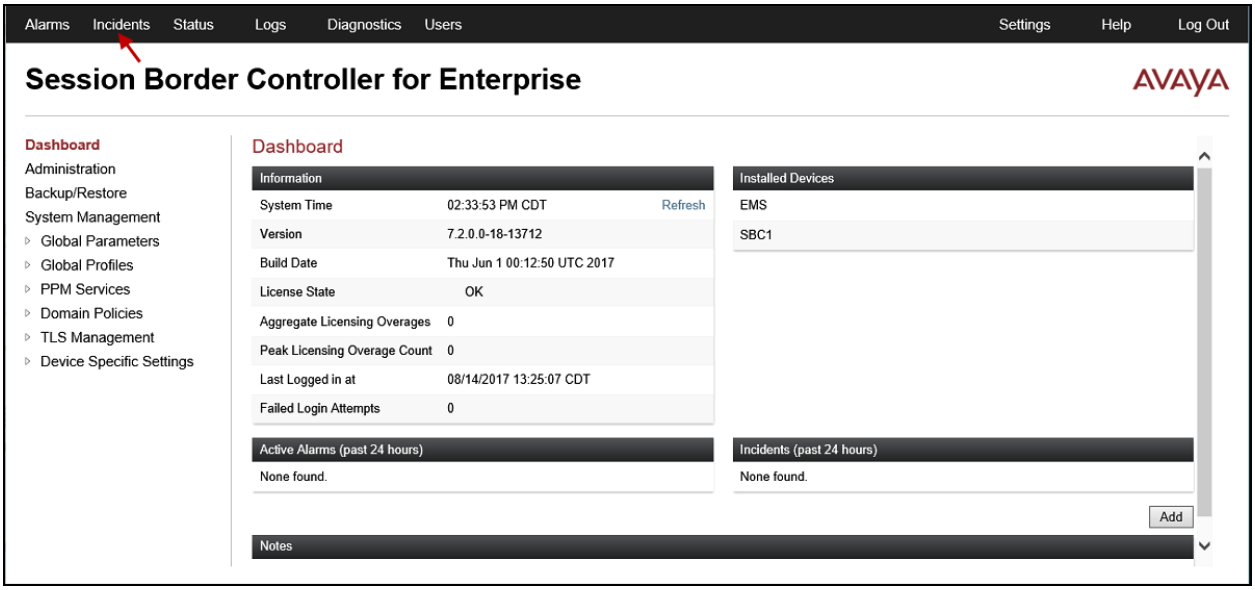
Alarms: This screen provides information about the health of the SBC.



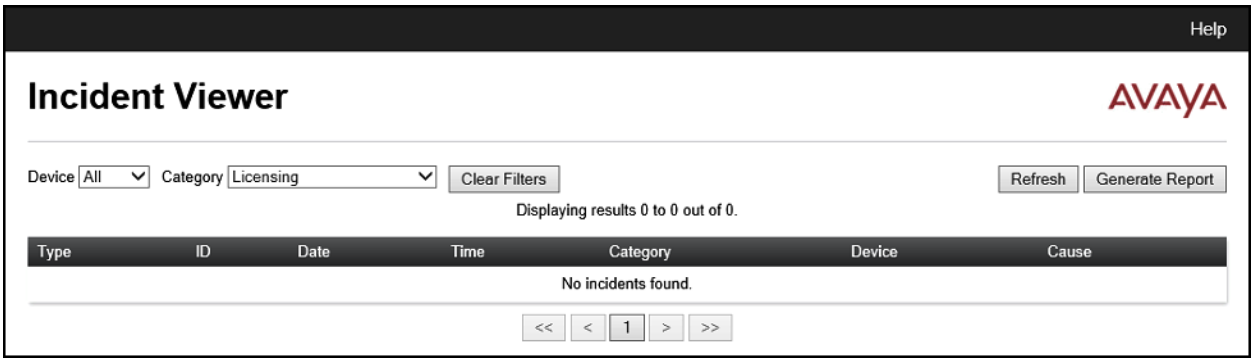
The following screen shows the **Alarm Viewer** page.



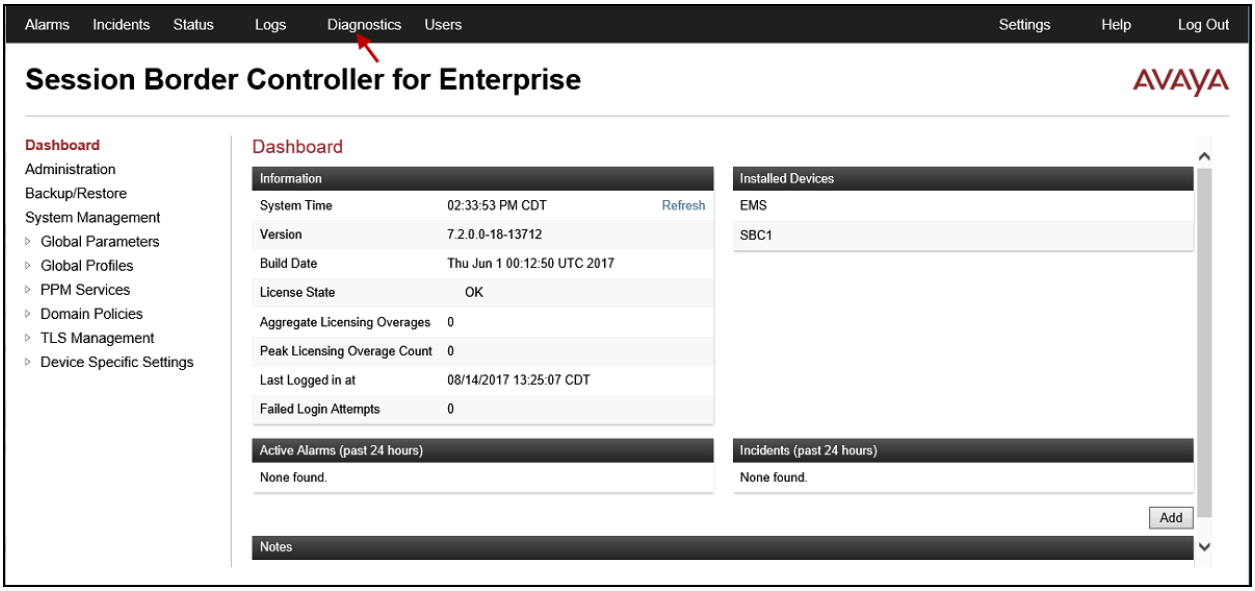
Incidents : Provides detailed reports of anomalies, errors, policies violations, etc.



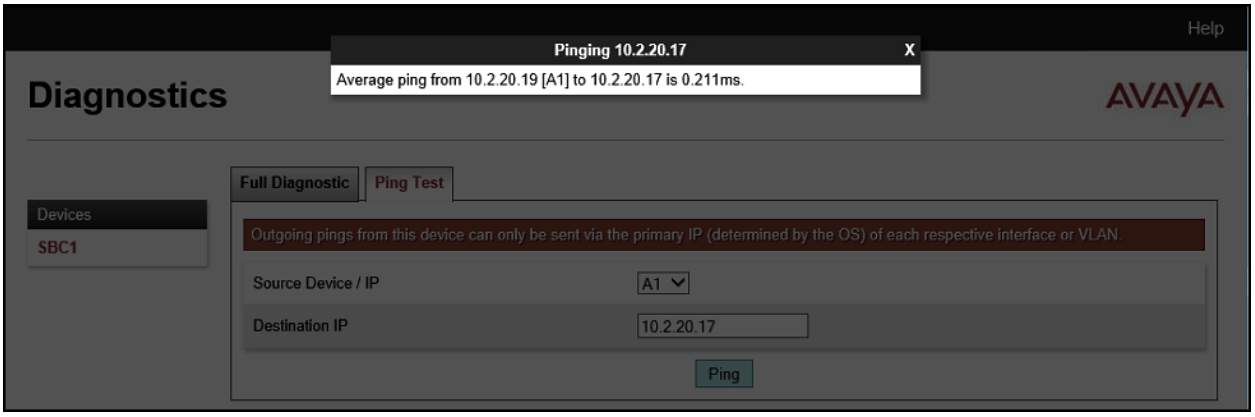
The following screen shows the Incident Viewer page.



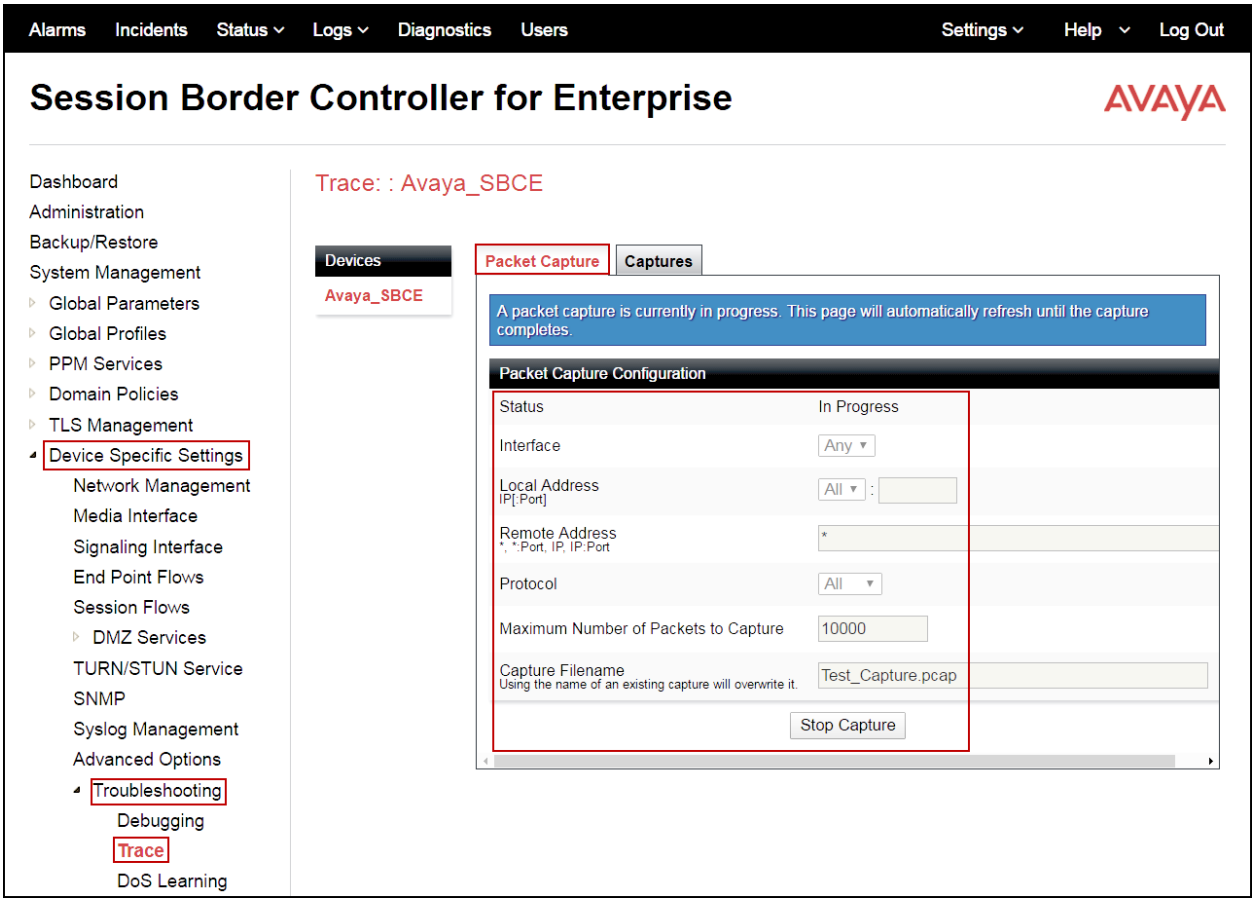
Diagnostics: This screen provides a variety of tools to test and troubleshoot the Avaya SBCE network connectivity.



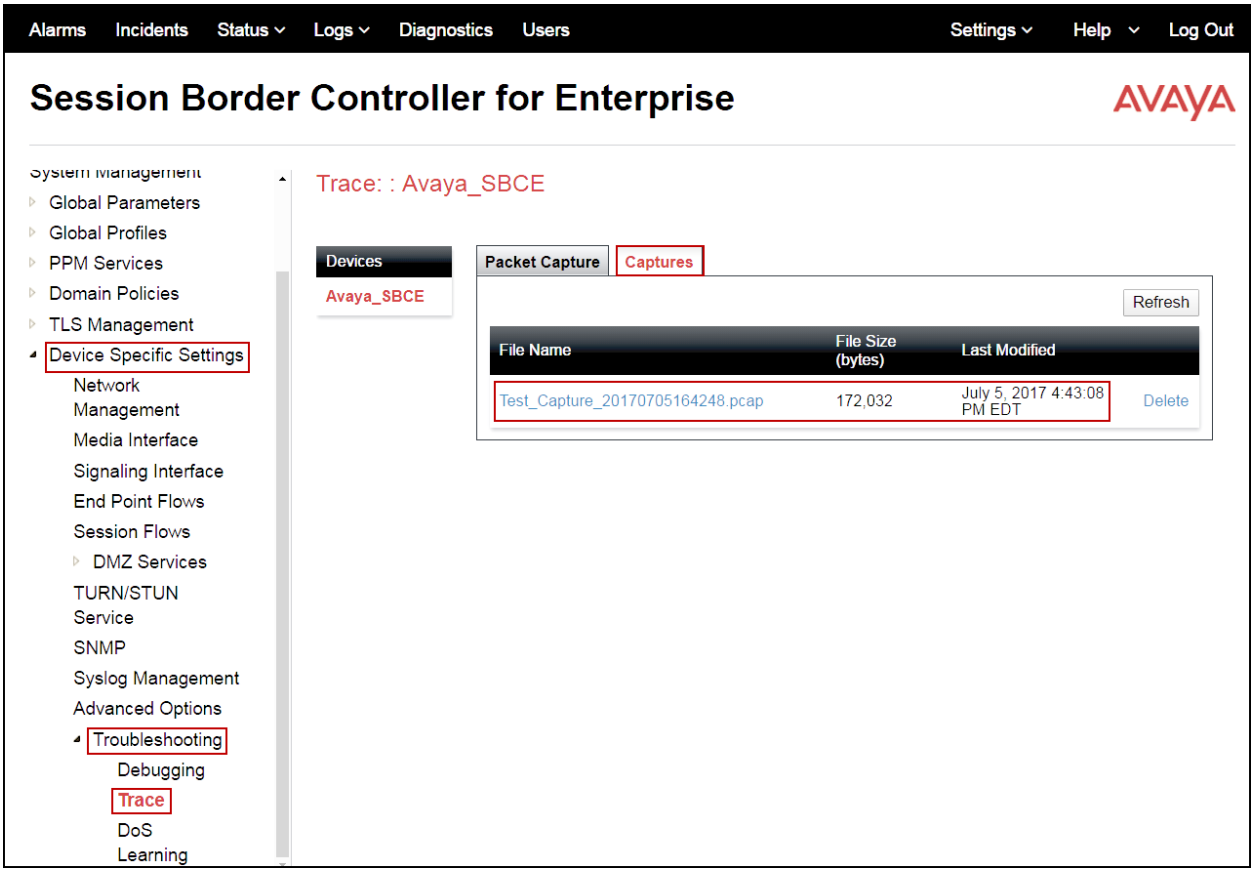
The following screen shows the Diagnostics page with the results of a successful ping test.



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



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



10. Conclusion

These Application Notes describe the procedures required to configure Avaya Aura® Communication Manager 7.0, Avaya Aura® Session Manager 7.0 and Avaya Session Border Controller for Enterprise 7.2, to connect to the Telmex SIP Trunk service using TLS transport for signaling and SRTP for media encryption, as shown in **Figure 1**.

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

11. References

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

[1] *Migrating and Installing Avaya Appliance Virtualization Platform*, Release 7.0.1, August 2016.
[2] *Deploying Avaya Aura® Communication Manager*, Release 7.0.1, Issue 2.1, October 2016.
[3] *Administering Avaya Aura® Communication Manager*, Release 7.0.1, August 2016, Document Number 03-300509.
[4] *Administering Avaya Aura® System Manager* for Release 7.0.1, Issue 3, January 2017.
[5] *Deploying Avaya Aura® System Manager*, Release 7.0.1, August 2016.
[6] *Deploying Avaya Aura® Session Manager*, Release 7.0.1, Issue 3, November 2016.
[7] *Administering Avaya Aura® Session Manager*, Release 7.0.1, Issue 2, May 2016.
[8] *Deploying Avaya Session Border Controller for Enterprise*, Release 7.2, Issue 3, August 2017.
[9] *Administering Avaya Session Border Controller for Enterprise*, Release 7.2, August 2017.
[10] *Configuring Remote Workers with Avaya Session Border Controller for Enterprise Rel. 7.0, Avaya Aura® Communication Manager Rel. 7.0 and Avaya Aura® Session Managers Rel. 7.0* - Issue 1.0.
[11] *RFC 3261 SIP: Session Initiation Protocol*, http://www.ietf.org/
[12] *RFC 2833 RTP Payload for DTMF Digits, Telephony Tones and Telephony Signals*, http://www.ietf.org/

12. Appendix A: SigMa Script

Following is the Signaling Manipulation scripts that was used in the configuration of the Avaya SBCE, **Section 7.8.2**. When adding these scripts as instructed in **Section 7.7** enter a name for the script in the Title (e.g., **SP**) and copy/paste the scripts as shown below.

```
within session "All"
{
    act on request where %DIRECTION="OUTBOUND" and %ENTRY_POINT="POST_ROUTING"
    {
        remove(%HEADERS["User-Agent"][1]);
        }
    }

/* OPTIONS From and To header change. Valid DID for the system and a public number are used
/* as URIs within the OPTIONS message for valid routing within Telmex

within session "OPTIONS"
{
    act on request where %DIRECTION="OUTBOUND" and %ENTRY_POINT="POST_ROUTING"
    {
        %HEADERS["From"][1].URI.USER = "1021";
        %HEADERS["To"][1].URI.USER = "53259000";
    }
}
```

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.