



Avaya Solution & Interoperability Test Lab

Application Notes for Configuring the Telefonica USA SIP Trunk Service with Avaya Aura® Communication Manager Evolution Server 6.2, Avaya Aura® Session Manager 6.2 and Avaya Session Border Controller for Enterprise – Issue 1.0

Abstract

These Application Notes describe the steps to configure Session Initiation Protocol (SIP) Trunking between the Telefonica USA SIP Trunk Service and an Avaya SIP-enabled enterprise solution. The Avaya solution consists of Avaya Aura® Session Manager 6.2, Avaya Aura® Communication Manager Evolution Server 6.2, Avaya Session Border Controller for Enterprise and various Avaya endpoints. Telefonica USA is a member of the Avaya DevConnect Service Provider program.

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

1. Introduction

These Application Notes describe the steps to configure Session Initiation Protocol (SIP) Trunking between the Telefonica USA SIP Trunk Service and an Avaya SIP-enabled enterprise solution. The Avaya solution consists of Avaya Aura® Session Manager 6.2, Avaya Aura® Communication Manager Evolution Server 6.2, Avaya Session Border Controller for Enterprise and various Avaya endpoints.

Customers using this Avaya SIP-enabled enterprise solution with the Telefonica USA SIP Trunk Service are able to place and receive PSTN calls via a broadband WAN connection with SIP. This converged network solution is an alternative to traditional PSTN trunks such as ISDN-PRI.

Telefonica USA SIP Trunk Service is available in most US markets as well as globally in Latin America, Europe and APAC. Combined with Telefonica Global Inbound Services and premium international long distance calling it represents a compelling offer for companies looking to expand their global reach.

These Application Notes apply only to the US based service - Telefonica USA SIP Trunk Service.

2. General Test Approach and Test Results

The general test approach was to connect a simulated enterprise site to the Telefonica USA SIP Trunk Service via the public Internet and exercise the features and functionality listed in **Section 2.1**. The simulated enterprise site was comprised of Communication Manager, Session Manager and Avaya Session Border Controller for Enterprise. Communication Manager and Session Manager were part of the Avaya Aura® Solution for Midsize Enterprise platform. However, these compliance test results are applicable to other server and media gateway platforms running similar versions of Communication Manager and Session Manager.

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 trunking interoperability, the following features and functionality were covered during the interoperability compliance test.

- Response to SIP OPTIONS queries
- Incoming PSTN calls to various phone types including Avaya H.323 and SIP telephones at the enterprise. All inbound PSTN calls were routed to the enterprise across the SIP trunk from the service provider.

- Outgoing PSTN calls from various phone types including H.323 and SIP telephones at the enterprise. All outbound PSTN calls were routed from the enterprise across the SIP trunk to the service provider.
- Inbound and outbound PSTN calls to/from Avaya one-X® Communicator (soft client). Avaya one-X® Communicator can place calls from the local computer or control a remote phone. Both of these modes were tested. Avaya one-X® Communicator also supports two Voice Over IP (VoIP) protocols: H.323 and SIP. Each protocol version of Avaya one-X® Communicator was also tested.
- Various call types including: local, long distance, international, outbound toll-free, inbound toll-free and local directory assistance (411).
- Codec G.711MU and G.729B
- DTMF transmission using RFC 2833
- Caller ID presentation and Caller ID restriction
- Response to incomplete call attempts and trunk errors
- Voicemail navigation for inbound and outbound calls
- Voicemail Message Waiting Indicator (MWI)
- User features such as hold and resume, internal call forwarding, transfer, and conference
- Off-net call forwarding and mobility (extension to cellular – EC500)
- Network Call Redirection using the SIP REFER method
- Network Call Redirection using the 302 Moved Temporarily response

Emergency 911 calls are supported but were not tested as part of the compliance test.

Items not supported included the following:

- Operator (0) and operator assisted (0 + 10 digits) calls
- T.38 fax calls are supported in the service provider core network but are not supported with this solution. A decision was made to remove the T.38 parameters from the SIP signaling as a workaround to an interoperability issue discussed in **Section 2.2**. For more details see the bullet item titled **Removal of T.38 parameters in SIP SDP for audio calls**.

2.2. Test Results

Interoperability testing of the Telefonica USA SIP Trunk Service was completed with successful results for all test cases with the exception of the observations or limitations described below.

- **Carrier Diversity for Outbound:** Telefonica has multiple carriers available to complete outbound calls. During compliance testing, some carrier incidents were observed that impacted some calls or the passing of DTMF digits. These incidents were successfully worked around in the lab. If any issue arises at a customer site, contact Telefonica as described in **Section 2.3** to resolve them.
- **Carrier Diversity for Inbound:** Test numbers provided by Telefonica included 786 and 939 numbers to illustrate carrier/gateway diversity for inbound calls. Calls to/from these numbers can present different signaling to the service provider which was confirmed

during compliance testing. The 939 numbers were used for the majority of the testing for consistency. To support the solution described in these App Notes, Telefonica will ensure that the network configuration used during this compliance test will be applied for all customers using this solution, so the enterprise will always be presented with a standard signaling framework. If any issue arises at a customer site, contact Telefonica as described in **Section 2.3** to resolve them.

- **Support for Call Forward, Calling Party Block, and Blind transfer to the PSTN:** SIP header manipulation rules were implemented by Telefonica USA in the network to support these features.
- **Removal of T.38 parameters in SIP SDP for audio calls:** Both Communication Manager and Avaya 9600 Series SIP Deskphones do not support T.38 parameters in the signaling of audio calls. It causes call failures to Avaya 9600 Series SIP Deskphones as well as failures in various transfer, EC500, and Avaya one-X® Communicator (other phone mode) scenarios. As a workaround, Telefonica USA has implemented SIP header manipulation rules in the network to remove these parameters from all messaging. This also has the side effect of preventing the use of T.38 fax for this solution since the T.38 parameters will be removed for all calls.
- **Extra INVITE after REFER:** In call scenarios that utilize the REFER method, Communication Manager sends an INVITE immediately after the REFER as a result of media shuffling. Telefonica USA does not expect an INVITE at this point and returns an error to the INVITE. All scenarios where this occurred completed normally with no user noticeable impact. This is being investigated by Communication Manager development.
- **Extra INVITE before BYE:** When terminating either an inbound or outbound call to Avaya one-X® Communicator H.323, the Communication Manager sends an INVITE immediately prior to the BYE. Telefonica USA responds with 200 Race Condition to the BYE due to the unexpected INVITE. All scenarios where this occurred completed normally with no user noticeable impact. This is being investigated by Communication Manager development.
- **Intermittent failures of conferencing with Avaya one-X® Communicator:** Conference calls fail roughly 1 in 10 times. This has been observed with both the H.323 and SIP versions of Avaya one-X® Communicator but seems easier to reproduce with the SIP version. This is not a Telefonica USA interoperability issue and has been turned over to Communication Manager development for investigation.
- **No Matching Codec Offered:** If the Communication Manager SIP trunk is improperly configured to have no matching codec with the service provider and an outbound call is placed, the Telefonica USA returns a “480 Temporarily Unavailable” response instead of a “488 Not Acceptable Here” response. The user hears fast busy.
- **Calling Party Number (PSTN transfers):** The calling party number displayed on the PSTN phone is not updated to reflect the true connected party on calls that are transferred to the PSTN. After the call transfer is complete, the calling party number displays the number of the transferring party and not the actual connected party. Communication Manager provides the new connected party information by updating the Contact header in an UPDATE message but the far-end phone display is not updated. The PSTN phone display is ultimately controlled by the PSTN provider, thus this behavior is not

necessarily indicative of a limitation of the combined Avaya/Telefonica solution. It is listed here simply as an observation.

2.3. Support

For technical support and incident reporting on the Telefonica USA SIP Trunk Service, please contact the Telefonica USA Service Management Center via the following:

- Email: smc.ga.us@telefonica.com
- Phone: 1-866-993-6622

Avaya customers may obtain documentation and support for Avaya products by visiting <http://support.avaya.com>.

3. Reference Configuration

Figure 1 illustrates a sample Avaya SIP-enabled enterprise solution connected to the Telefonica USA SIP Trunk Service. This is the configuration used for compliance testing.

The components used to create the simulated customer site included:

- System Manager
- Session Manager
- Communication Manager
- Avaya G450 Media Gateway
- Avaya Session Border Controller for Enterprise
- Avaya 1600-Series IP telephones (H.323)
- Avaya 9600-Series IP telephones (H.323 and SIP)
- Avaya one-X® Communicator (H.323 and SIP)
- Avaya A175 Desktop Video Device

Located at the edge of the enterprise is the Avaya SBCE. It has a public side that connects to the external network and a private side that connects to the enterprise network. All SIP and RTP traffic entering or leaving the enterprise flows through the Avaya SBCE. In this way, the Avaya SBCE can protect the enterprise against any SIP-based attacks. The Avaya SBCE provides network address translation at both the IP and SIP layers. For security reasons, any actual public IP addresses used in the configuration have been replaced with private IP addresses. Similarly, any references to real routable PSTN numbers have also been changed to numbers that cannot be routed by the PSTN.

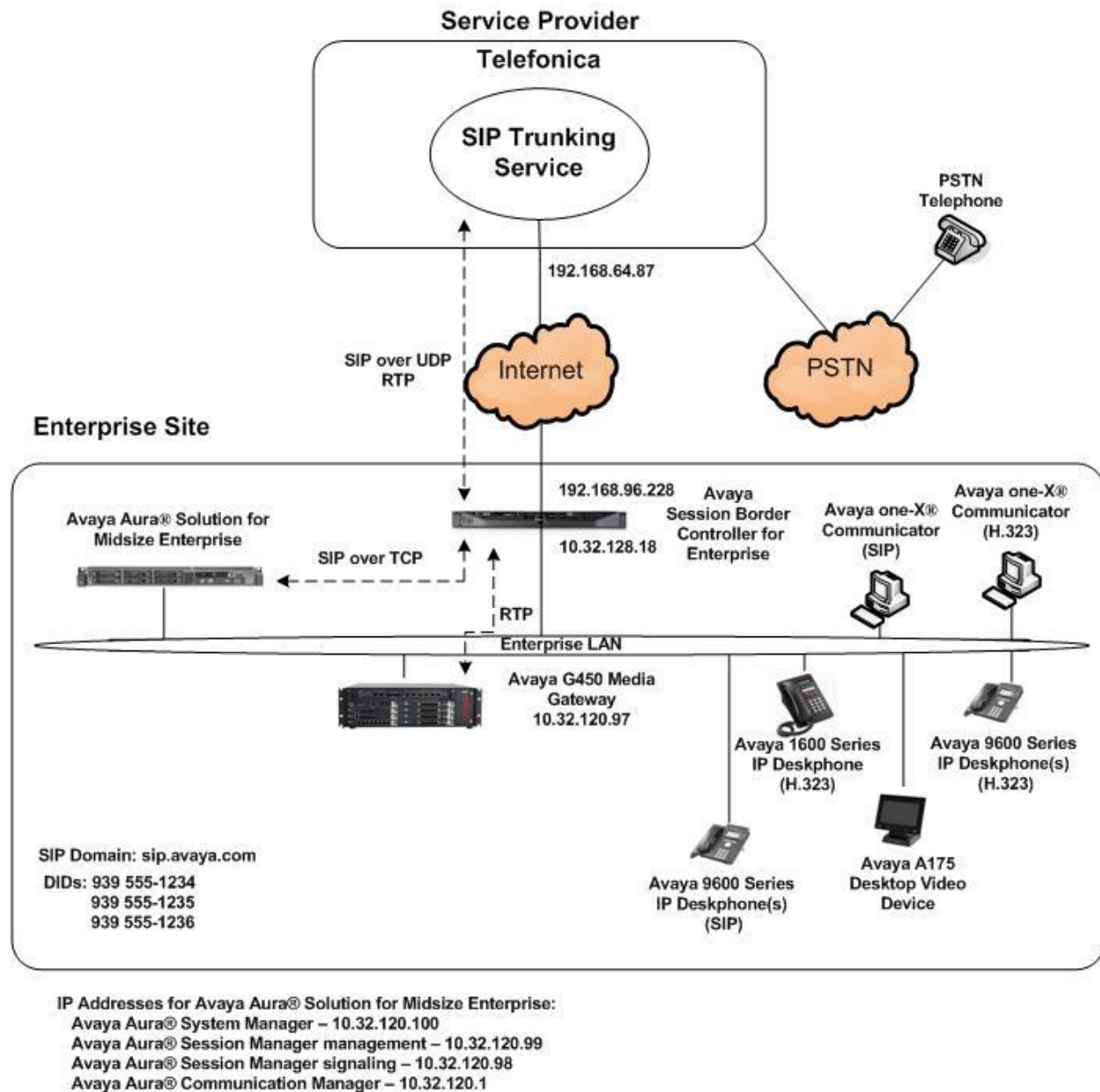


Figure 1: Avaya IP Telephony Network using the Telefonica USA SIP Trunk Service

A separate trunk was created between Communication Manager and Session Manager to carry the service provider traffic. This was done so that any trunk or codec setting required by the service provider could be applied only to this trunk and not affect other enterprise SIP traffic. In addition, this trunk carried both inbound and outbound traffic.

For inbound calls, the calls flow from the service provider to the Avaya SBCE then to Session Manager. Session Manager uses the configured dial patterns (or regular expressions) and routing policies to determine the recipient (in this case Communication Manager) and on which link to send the call. Once the call arrives at Communication Manager, further incoming call treatment, such as incoming digit translations and class of service restrictions may be performed.

Outbound calls to the PSTN are first processed by Communication Manager and may be subject to outbound features such as automatic route selection, digit manipulation and class of service restrictions. Once Communication Manager selects the proper SIP trunk, the call is routed to Session Manager. The Session Manager once again uses the configured dial patterns (or regular expressions) to determine the route to the Avaya SBCE. From the Avaya SBCE, the call is sent to the Telefonica USA SIP Trunk Service.

For outbound calls, the enterprise sent 10 digits in the SIP source headers (i.e., From, Contact, and P-Asserted-Identity). The enterprise was configured to send 11 digits in the SIP destination headers (Request URI and To). For inbound calls, Telefonica USA sent 10 digits in both the source headers and destination headers.

4. Equipment and Software Validated

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

Avaya IP Telephony Solution Components	
Equipment/Software	Release/Version
Avaya Aura® Solution For Midsize Enterprise running on an HP Proliant DL360 Server	6.2
- Avaya Aura® System Manager	6.2 SP4 (Build 6.2.0.0.15669-6.2.12.408)
- Avaya Aura® Session Manager	6.2 SP4 (Build 6.2.4.0.624005)
- Avaya Aura® Communication Manager	6.2 SP4 (Build R016x.02.0.823.0-20199)
- Avaya Aura® Communication Manager Messaging	6.2 SP1 (Build CMM-02.0.823.0-0104)
- System Platform	6.2.1.3.9
Avaya G450 Media Gateway	31.22.0
Avaya Session Border Controller for Enterprise running on a Dell R210 V2 server	4.0.5Q19
Avaya 1608 IP Deskphone (H.323) running Avaya one-X® Deskphone Value Edition	1.3 SP2
Avaya 9640G IP Deskphone (H.323) running Avaya one-X® Deskphone Edition	3.1 SP5 (3.1.05S)
Avaya 9641G IP Deskphone (H.323) running Avaya one-X® Deskphone Edition	6.2 SP2 (S6.2209)
Avaya 9611 IP Deskphone (SIP) running Avaya one-X® Deskphone SIP Edition	6.2 SP1 (6.2.1.26)
Avaya A175 Desktop Video Device with Avaya Flare® Experience	1.1.1
Avaya one-X® Communicator (H.323 or SIP)	6.1 SP7 (Build 6.1.7.04-SP7-39506)
Telefonica USA SIP Trunk Service Solution Components	
Equipment/Software	Release/Version
Acme Packet Net-Net 4250 Session Border Controller	SC6.1.0 MR-8 Patch 5 (Build 934)
Broadworks SIP Application Server	R17 SP3
Genband C20 Softswitch (Gateway for 939 Numbers)	CVM12
Cisco 2821 (Gateway for 786 numbers)	IOS 12.4 (25b), Software Release (fc1)

Table 1: Equipment and Software Tested

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

5. Configure Avaya Aura® Communication Manager

This section describes the procedure for configuring Communication Manager for the Telefonica USA SIP Trunk Service. A SIP trunk is established between Communication Manager and Session Manager for use by traffic to and from Telefonica USA. It is assumed the general installation of Communication Manager, Avaya Media Gateway and Session Manager has been previously completed and is not discussed here.

The Communication Manager configuration was performed using the System Access Terminal (SAT). Some screens in this section have been abridged and highlighted for brevity and clarity in presentation. Note that the IP addresses and phone numbers shown throughout these Application Notes have been edited so that the actual public IP addresses of the network elements and public PSTN numbers are not revealed.

5.1. Licensing and Capacity

Use the **display system-parameters customer-options** command to verify that the **Maximum Administered SIP Trunks** value on **Page 2** is sufficient to support the desired number of simultaneous SIP calls across all SIP trunks at the enterprise including any trunks to the service provider. The example shows that **12000** SIP trunks are available and **275** are in use. The license file installed on the system controls the maximum values for these attributes. If a required feature is not enabled or there is insufficient capacity, contact an authorized Avaya sales representative to add additional capacity.

display system-parameters customer-options		Page	2 of 11
OPTIONAL FEATURES			
IP PORT CAPACITIES		USED	
Maximum Administered H.323 Trunks:		12000	0
Maximum Concurrently Registered IP Stations:		18000	4
Maximum Administered Remote Office Trunks:		12000	0
Maximum Concurrently Registered Remote Office Stations:		18000	0
Maximum Concurrently Registered IP eCons:		128	0
Max Concur Registered Unauthenticated H.323 Stations:		100	0
Maximum Video Capable Stations:		36000	1
Maximum Video Capable IP Softphones:		18000	3
Maximum Administered SIP Trunks:		12000	275
Maximum Administered Ad-hoc Video Conferencing Ports:		12000	0

5.2. System Features

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

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

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

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

      CPN/ANI/ICLID PARAMETERS
      CPN/ANI/ICLID Replacement for Restricted Calls: anonymous
      CPN/ANI/ICLID Replacement for Unavailable Calls: anonymous

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

      INTERNATIONAL CALL ROUTING PARAMETERS
      Local Country Code: 1
      International Access Code: 011

      SSCAN DIALING PARAMETERS
      Enable Enbloc Dialing without ARS FAC? n

      CALLER ID ON CALL WAITING PARAMETERS
      Caller ID on Call Waiting Delay Timer (msec): 200
```

5.3. IP Node Names

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

change node-names ip		Page 1 of 2
		IP NODE NAMES
Name	IP Address	
SM	10.32.120.98	
default	0.0.0.0	
nwk-aes1	10.32.120.3	
procr	10.32.120.1	
procr6	::	

5.4. Codecs

Use the **change ip-codec-set** command to define a list of codecs to use for calls between the enterprise and the service provider. The list should include the codecs and preferred order defined by the service provider. For the compliance test, codecs G.729B and G.711MU were tested using ip-codec-set 4. To configure the codecs, enter the codecs in the **Audio Codec** column of the table in the order of preference. Default values can be used for all other fields.

change ip-codec-set 4		Page 1 of 2
		IP Codec Set
Codec Set: 4		
Audio Codec	Silence Suppression	Frames Per Pkt
1: G.729B	n	2
2: G.711MU	n	2
3:		

On **Page 2**, set the **Fax Mode** to **off** since T.38 fax calls are not supported with this solution.

change ip-codec-set 4		Page 2 of 2
		IP Codec Set
Allow Direct-IP Multimedia? n		
FAX	Mode	Redundancy
Modem	off	0
TDD/TTY	off	0
	US	3

5.5. IP Network Region

Create a separate IP network region for the service provider trunk. This allows for separate codec or quality of service settings to be used (if necessary) for calls between the enterprise and the service provider versus calls within the enterprise or elsewhere. For the compliance test, IP network region 4 was chosen for the service provider trunk. Use the **change ip-network-region 4** command to configure region 4 with the following parameters:

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

```
change ip-network-region 4                                     Page 1 of 20
                                                                IP NETWORK REGION
Region: 4
Location: Authoritative Domain: sip.avaya.com
Name: SP Region
MEDIA PARAMETERS                                             Intra-region IP-IP Direct Audio: yes
Codec Set: 4                                                 Inter-region IP-IP Direct Audio: yes
UDP Port Min: 2048                                           IP Audio Hairpinning? n
UDP Port Max: 3329
DIFFSERV/TOS PARAMETERS
Call Control PHB Value: 46
Audio PHB Value: 46
Video PHB Value: 26
802.1P/Q PARAMETERS
Call Control 802.1p Priority: 6
Audio 802.1p Priority: 6
Video 802.1p Priority: 5
H.323 IP ENDPOINTS
H.323 Link Bounce Recovery? y
Idle Traffic Interval (sec): 20
Keep-Alive Interval (sec): 5
Keep-Alive Count: 5
                                                                AUDIO RESOURCE RESERVATION PARAMETERS
                                                                RSVP Enabled? n
```

On **Page 4**, define the IP codec set to be used for traffic between region 4 and region 1. Enter the desired IP codec set in the **codec set** column of the row with destination region (**dst rgn**) **1**. Default values may be used for all other fields. The example below shows the settings used for the compliance test. It indicates that codec set 4 will be used for calls between region 4 (the service provider region) and region 1 (the rest of the enterprise). Creating this table entry for IP network region 4 will automatically create a complementary table entry on the IP network region 1 form for destination region 4. This complementary table entry can be viewed using the **display ip-network-region 1** command and navigating to **Page 4** (not shown).

change ip-network-region 4										Page	4	of	20
Source Region: 4 Inter Network Region Connection Management										I			M
										G	A		t
dst	codec	direct	WAN-BW-limits	Video	Intervening	Dyn	A	G					c
rgn	set	WAN	Units	Total Norm	Prio Shr Regions	CAC	R	L					e
1	4	y	NoLimit				n						t
2													
3													
4	4											all	

5.6. Signaling Group

Use the **add signaling-group** command to create a signaling group between Communication Manager and Session Manager for use by the service provider trunk. This signaling group is used for inbound and outbound calls between the service provider and the enterprise. For the compliance test, signaling group 4 was used for this purpose and was configured using the parameters highlighted below.

- Set the **Group Type** field to **sip**.
- Set the **Transport Method** to the recommended default value of **tls** (Transport Layer Security). For ease of troubleshooting during testing, part of the compliance test was conducted with the **Transport Method** set to **tcp**. The transport method specified here is used between Communication Manager and Session Manager.
- Set the **IMS Enabled** field to **n**. This specifies Communication Manager will serve as an Evolution Server for Session Manager.
- Set the **Peer Detection Enabled** field to **y**. The **Peer-Server** field will initially be set to **Others** and cannot be changed via administration. Later, the **Peer-Server** field will automatically change to **SM** once Communication Manager detects its peer as a Session Manager.
- Set the **Near-end Node Name** to **procr**. This node name maps to the IP address of the Communication Manager as defined in **Section 5.3**.
- Set the **Far-end Node Name** to **SM**. This node name maps to the IP address of Session Manager as defined in **Section 5.3**.
- Set the **Near-end Listen Port** and **Far-end Listen Port** to a valid unused port instead of the default well-known port value. (For TLS, the well-known port value is 5061 and for TCP the well-known port value is 5060). At the time of Session Manager installation, a SIP connection between Communication Manager and Session Manager would have been established for use by all Communication Manager SIP traffic using the well-known port

value for TLS or TCP. By creating a new signaling group with a separate port value, a separate SIP connection is created between Communication Manager and Session Manager for SIP traffic to the service provider. As a result, any signaling group or trunk group settings (**Section 5.7**) will only affect the service provider traffic and not other SIP traffic at the enterprise. The compliance test was conducted with the **Near-end Listen Port** and **Far-end Listen Port** set to **5260**.

- 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 **Direct IP-IP Audio Connections** to **y**. This field will enable media shuffling on the SIP trunk allowing Communication Manager to redirect media traffic directly between the SIP trunk and the enterprise endpoint.
- Set the **DTMF over IP** field to **rtp-payload**. This value enables Communication Manager to send DTMF transmissions using RFC 2833.
- Set the **Alternate Route Timer** to **15**. This defines the number of seconds that Communication Manager will wait for a response (other than 100 Trying) to an outbound INVITE before selecting another route. If an alternate route is not defined, then the call is cancelled after this interval.
- Default values may be used for all other fields.

add signaling-group 4		Page 1 of 2
SIGNALING GROUP		
Group Number: 4	Group Type: sip	
IMS Enabled? n	Transport Method: tls	
Q-SIP? n		
IP Video? n	Enforce SIPS URI for SRTP? y	
Peer Detection Enabled? y	Peer Server: SM	
Near-end Node Name: procr	Far-end Node Name: SM	
Near-end Listen Port: 5260	Far-end Listen Port: 5260	
	Far-end Network Region: 4	
	Far-end Secondary Node Name:	
Far-end Domain: sip.avaya.com		
Incoming Dialog Loopbacks: eliminate	Bypass If IP Threshold Exceeded? n	
DTMF over IP: rtp-payload	RFC 3389 Comfort Noise? n	
Session Establishment Timer(min): 3	Direct IP-IP Audio Connections? y	
Enable Layer 3 Test? y	IP Audio Hairpinning? n	
H.323 Station Outgoing Direct Media? n	Initial IP-IP Direct Media? n	
	Alternate Route Timer(sec): 15	

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 4 was configured using the parameters highlighted below.

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

```
add trunk-group 4                                     Page 1 of 21
                                                    TRUNK GROUP
Group Number: 4                                     Group Type: sip          CDR Reports: y
  Group Name: SP Trunk                             COR: 1                 TN: 1          TAC: *04
  Direction: two-way                               Outgoing Display? n
  Dial Access? n                                    Night Service:
  Queue Length: 0
  Service Type: public-ntwrk                       Auth Code? n
                                                    Member Assignment Method: auto
                                                    Signaling Group: 4
                                                    Number of Members: 10
```

On **Page 2**, the **Redirect On OPTIM Failure** value is the amount of time (in milliseconds) that Communication Manager will wait for a response (other than 100 Trying) to a pending INVITE sent to an EC500 remote endpoint before selecting another route. If another route is not defined, then the call is cancelled after this interval. This time interval should be set to a value equal to the **Alternate Route Timer** on the signaling group form described in **Section 5.6**.

Verify that the **Preferred Minimum Session Refresh Interval** is set to a value acceptable to the service provider. This value defines the interval that re-INVITEs must be sent to keep the active session alive. For the compliance test, the value of **900** seconds was used.

```

add trunk-group 4                                     Page 2 of 21
  Group Type: sip

TRUNK PARAMETERS

  Unicode Name: auto

                                     Redirect On OPTIM Failure: 15000

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

  Disconnect Supervision - In? y Out? y

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

```

On **Page 3**, set the **Numbering Format** field to **private**. This field specifies the format of the calling party number (CPN) sent to the far-end. Beginning with Communication Manager 6.0, public numbers are automatically preceded with a + sign (E.164 numbering format) when passed in the SIP From, Contact and P-Asserted Identity headers. To remove the + sign, the **Numbering Format** was set to **private** and the **Numbering Format** in the route pattern was set to **unk-unk** (see **Section 5.9**).

Set the **Replace Restricted Numbers** and **Replace Unavailable Numbers** fields to **y**. This will allow the CPN displayed on local endpoints to be replaced with the value set in **Section 5.2**, if the inbound call enabled CPN block. For outbound calls, these same settings request that CPN block be activated on the far-end destination if a local user requests CPN block on a particular call routed out this trunk. Default values were used for all other fields.

```

add trunk-group 4                                     Page 3 of 21
TRUNK FEATURES
  ACA Assignment? n           Measured: none           Maintenance Tests? y

                                     Numbering Format: private
                                     UUI Treatment: service-provider

                                     Replace Restricted Numbers? y
                                     Replace Unavailable Numbers? y

                                     Modify Tandem Calling Number: no

  Show ANSWERED BY on Display? y

```


On **Page 4**, the **Network Call Redirection** field was set to **y**. If set to **y**, Communication Manager will use the SIP REFER method to redirect calls back to the PSTN. Set the **Send Diversion Header** field to **y** and the **Support Request History** field to **n**. The **Send Diversion Header** field provides additional information to the network if the call has been redirected. These settings are needed to support call forwarding of inbound calls back to the PSTN and some Extension to Cellular (EC500) call scenarios.

Set the **Telephone Event Payload Type** to **101**, the value sent by Telefonica USA.

add trunk-group 4	Page 4 of 21
PROTOCOL VARIATIONS	
Mark Users as Phone?	n
Prepend '+' to Calling Number?	n
Send Transferring Party Information?	n
Network Call Redirection?	y
Send Diversion Header?	y
Support Request History?	n
Telephone Event Payload Type:	101
Convert 180 to 183 for Early Media?	n
Always Use re-INVITE for Display Updates?	n
Identity for Calling Party Display:	P-Asserted-Identity
Block Sending Calling Party Location in INVITE?	n
Enable Q-SIP?	n

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. The DID number will be assigned by the SIP service provider. It is used to authenticate the caller.

In the sample configuration, three DID numbers were assigned for testing. These three numbers were assigned to the three extensions 50003, 50006 and 50015. Thus, these same 10-digit numbers were used in the outbound calling party information on the service provider trunk when calls were originated from these three extensions.

change private-numbering 0					Page 1 of 2
NUMBERING - PRIVATE FORMAT					
Ext Len	Ext Code	Trk Grp (s)	Private Prefix	Total Len	
5	5			5	Total Administered: 4
5	50003	4	9395551234	10	Maximum Entries: 540
5	50006	4	9395551235	10	
5	50015	4	9395551236	10	

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

change private-numbering 0					Page 1 of 2
NUMBERING - PRIVATE FORMAT					
Ext Len	Ext Code	Trk Grp (s)	Private Prefix	Total Len	
5	5			5	Total Administered: 2
5	5	4	93955	10	Maximum Entries: 540

5.9. Outbound Routing

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

change dialplan analysis			DIAL PLAN ANALYSIS TABLE						Page 1 of 12
			Location: all			Percent Full: 2			
Dialed String	Total Length	Call Type	Dialed String	Total Length	Call Type	Dialed String	Total Length	Call Type	
0	1	attd							
1	5	ext							
5	5	ext							
9	1	fac							
*	3	dac							
#	3	dac							

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

change feature-access-codes			FEATURE ACCESS CODE (FAC)						Page 1 of 11
Abbreviated Dialing List1 Access Code: *10									
Abbreviated Dialing List2 Access Code: *12									
Abbreviated Dialing List3 Access Code: *13									
Abbreviated Dial - Prgm Group List Access Code: *14									
Announcement Access Code: *19									
Answer Back Access Code:									
Auto Alternate Routing (AAR) Access Code: *00									
Auto Route Selection (ARS) - Access Code 1: 9			Access Code 2:						
Automatic Callback Activation: *33			Deactivation: #33						
Call Forwarding Activation Busy/DA: *30 All: *31			Deactivation: #30						
Call Forwarding Enhanced Status: Act:			Deactivation:						

Use the **change ars analysis** command to configure the routing of dialed digits following the first digit 9. The example below shows a subset of the dialed strings tested as part of the compliance test. See **Section 2.1** for the complete list of call types tested. All dialed strings are mapped to route pattern **4** which contains the SIP trunk to the service provider (as defined next).

change ars analysis 0							Page 1 of 2	
ARS DIGIT ANALYSIS TABLE								
Location: all					Percent Full: 1			
Dialed	Total		Route	Call	Node	ANI		
String	Min	Max	Pattern	Type	Num	Reqd		
011	10	18	4	intl		n		
1732	11	11	4	fnpa		n		
1800	11	11	4	fnpa		n		
1877	11	11	4	fnpa		n		
1908	11	11	4	fnpa		n		
1939555	11	11	4	fnpa		n		
411	3	3	4	svcl		n		

The route pattern defines which trunk group will be used for the call and performs any necessary digit manipulation. Use the **change route-pattern** command to configure the parameters for the service provider route pattern in the following manner. The example below shows the values used for route pattern 4 during the compliance test.

- **Pattern Name:** Enter a descriptive name.
- **Grp No:** Enter the outbound trunk group for the SIP service provider. For the compliance test, trunk group **4** was used.
- **FRL:** Set the Facility Restriction Level (**FRL**) field to a level that allows access to this trunk for all users that require it. The value of **0** is the least restrictive level.
- **Pfx Mrk: 1** The prefix mark (**Pfx Mrk**) of one will prefix any FNPA 10-digit number with a 1 and leave numbers of any other length unchanged. This will ensure 1 + 10 digits are sent to the service provider for long distance North American Numbering Plan (NANP) numbers.
- **Numbering Format: unk-unk** All calls using this route pattern will use the private numbering table. See setting of the **Numbering Format** in the trunk group form for full details in **Section 5.7**.
- **LAR: next**

change route-pattern 4													Page 1 of 3		
Pattern Number: 4													Pattern Name: SP Route		
SCCAN? n													Secure SIP? n		
Grp	FRL	NPA	Pfx	Hop	Toll	No.	Inserted						DCS/	IXC	
No			Mrk	Lmt	List	Del	Digits						QSIG		
													Intw		
1:	4	0	1										n	user	
2:													n	user	
3:													n	user	
4:													n	user	
5:													n	user	
6:													n	user	
BCC		VALUE		TSC	CA-TSC		ITC		BCIE	Service/Feature		PARM	No.	Numbering	LAR
0	1	2	M	4	W	Request						Dgts		Format	
													Subaddress		
1:	y	y	y	y	y	n	n	rest				unk-unk		next	
2:	y	y	y	y	y	n	n	rest						none	
3:	y	y	y	y	y	n	n	rest						none	
4:	y	y	y	y	y	n	n	rest						none	
5:	y	y	y	y	y	n	n	rest						none	
6:	y	y	y	y	y	n	n	rest						none	

6. Configure Avaya Aura® Session Manager

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

- SIP domain
- Logical/physical Location that can be occupied by SIP Entities
- Adaptation module to perform dial plan manipulation
- SIP Entities corresponding to Communication Manager, the Avaya SBCE and Session Manager
- 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 governs which Routing Policy is used to service a call.
- Session Manager, corresponding to the Session Manager Server to be managed by System Manager.

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

6.1. Avaya Aura® System Manager Login and Navigation

Session Manager configuration is accomplished by accessing the browser-based GUI of System Manager, using the URL “https://<ip-address>/SMGR”, where “<ip-address>” is the IP address of System Manager. Log in with the appropriate credentials and click on **Login** (not shown). The **Home** page is displayed. The links displayed below will be referenced in subsequent sections to navigate to items requiring configuration. Most items will be located under the **Elements** → **Routing** link highlighted below.

AVAYA

Avaya Aura® System Manager 6.2

Last Logged on at June 25, 2012 11:58 AM
[Help](#) | [About](#) | [Change Password](#) | [Log off admin](#)

Users	Elements	Services
Administrators Manage Administrative Users	B5800 Branch Gateway Manage B5800 Branch Gateway 6.2 elements	Backup and Restore Backup and restore System Manager database
Directory Synchronization Synchronize users with the enterprise directory	Communication Manager Manage Communication Manager 5.2 and higher elements	Bulk Import and Export Manage Bulk Import and Export of Users, User Global Settings, Roles, Elements and others
Groups & Roles Manage groups, roles and assign roles to users	Conferencing Manage Conferencing Multimedia Server objects	Configurations Manage system wide configurations
User Management Manage users, shared user resources and provision users	Inventory Manage, discover, and navigate to elements, update element software	Events Manage alarms, view and harvest logs
	Meeting Exchange Manage Meeting Exchange and Avaya Aura Conferencing 6.0 elements	Licenses View and configure licenses
	Messaging Manage Avaya Aura Messaging, Communication Manager Messaging, and Modular Messaging	Replication Track data replication nodes, repair replication nodes
	Presence Presence	Scheduler Schedule, track, cancel, update and delete jobs
	Routing Network Routing Policy	Security Manage Security Certificates
	Session Manager Session Manager Element Manager	Templates Manage Templates for Communication Manager, Messaging System and B5800 Branch Gateway elements
	SIP AS 8.1 SIP AS 8.1	

Clicking the **Elements** → **Routing** link, displays the **Introduction to Network Routing Policy** page. In the left-hand pane is a navigation tree containing many of the items to be configured in the following sections.

The screenshot displays the Avaya Aura System Manager 6.2 web interface. At the top left is the Avaya logo. The header area includes the text 'Avaya Aura® System Manager 6.2' and a user status bar on the right indicating 'Last Logged on at June 25, 2012 11:58 AM' with links for 'Help', 'About', 'Change Password', and 'Log off admin'. Below the header, there are tabs for 'Routing' (active) and 'Home'. A left-hand navigation pane lists various configuration categories: Routing, Domains, Locations, Adaptations, SIP Entities, Entity Links, Time Ranges, Routing Policies, Dial Patterns, Regular Expressions, and Defaults. The main content area shows the 'Introduction to Network Routing Policy' page, which includes a breadcrumb trail 'Home /Elements / Routing', a 'Help ?' link, and a list of four steps for configuring the network routing policy.

AVAYA Avaya Aura® System Manager 6.2 Last Logged on at June 25, 2012 11:58 AM
[Help](#) | [About](#) | [Change Password](#) | [Log off admin](#)

Routing × **Home**

▼ **Routing** ◀ **Home /Elements / Routing**

Introduction to Network Routing Policy [Help ?](#)

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

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

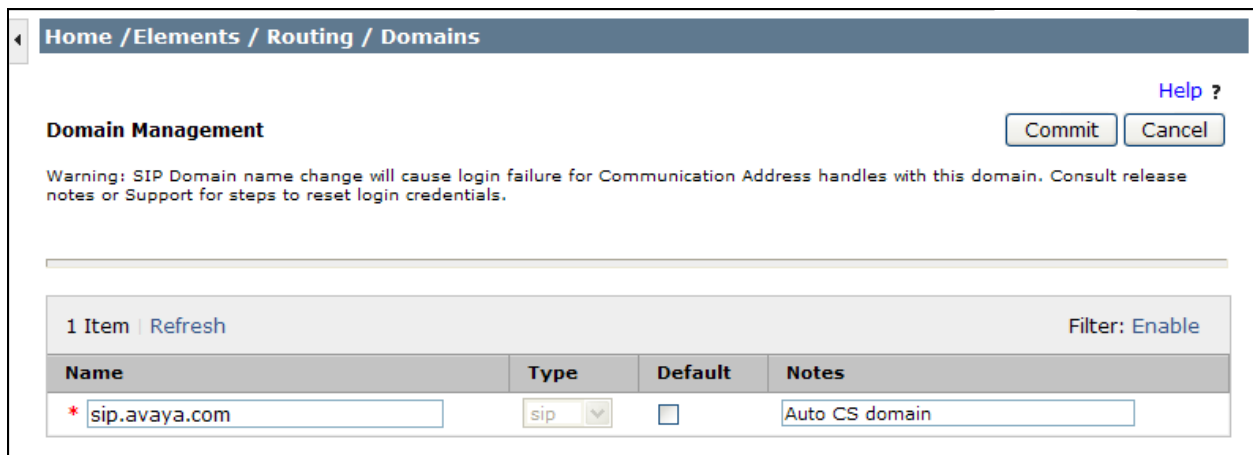
- Step 1: Create "Domains" of type SIP (other routing applications are referring domains of type SIP).
- Step 2: Create "Locations"
- Step 3: Create "Adaptations"
- Step 4: Create "SIP Entities"

6.2. Specify SIP Domain

Create a SIP domain for each domain for which Session Manager will need to be aware in order to route calls. For the compliance test, this includes the enterprise domain (**sip.avaya.com**). Navigate to **Routing → Domains** in the left-hand navigation pane (**Section 6.1**) and click the **New** button in the right pane (not shown). In the new right pane that appears (shown below), fill in the following:

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

Click **Commit**. The screen below shows the entry for the enterprise domain.



The screenshot shows the 'Domain Management' interface. At the top, there is a breadcrumb trail: 'Home / Elements / Routing / Domains'. Below this, the title 'Domain Management' is displayed. To the right of the title are two buttons: 'Commit' and 'Cancel', and a 'Help ?' link. A warning message states: 'Warning: SIP Domain name change will cause login failure for Communication Address handles with this domain. Consult release notes or Support for steps to reset login credentials.' Below the warning, there is a table with one item. The table has four columns: 'Name', 'Type', 'Default', and 'Notes'. The 'Name' column contains 'sip.avaya.com' with a red asterisk to its left. The 'Type' column contains a pull-down menu with 'sip' selected. The 'Default' column contains an unchecked checkbox. The 'Notes' column contains 'Auto CS domain'. Above the table, there is a '1 Item | Refresh' link and a 'Filter: Enable' link.

Name	Type	Default	Notes
* sip.avaya.com	sip	<input type="checkbox"/>	Auto CS domain

6.3. Add Location

Locations can be used to identify logical and/or physical locations where SIP Entities reside for purposes of bandwidth management and call admission control. A single location was defined for the enterprise even though multiple subnets were used. The screens below show the addition of the location named **Belleville**, which includes all equipment on the enterprise including Communication Manager, Session Manager and the Avaya SBCE.

To add a location, navigate to **Routing → Locations** in the left-hand navigation pane (**Section 6.1**) and click the **New** button in the right pane (not shown). In the new right pane that appears (shown below), fill in the following:

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

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

Home / Elements / Routing / Locations

Location Details

Help ?

Commit Cancel

General

* Name: Belleville

Notes: Enterprise Site for SP Testing

Scroll down to the **Location Pattern** section. Click **Add** and enter the following values. Use default values for all remaining fields.

- **IP Address Pattern:** Add all IP address patterns used to identify the location. The test environment included two subnets as shown below.
- **Notes:** Add a brief description (optional).

Click **Commit** to save.

Location Pattern

Add Remove

2 Items Refresh Filter: Enable

<input type="checkbox"/>	IP Address Pattern	Notes
<input type="checkbox"/>	* 10.32.120.*	CPE CM, SM and other devices
<input type="checkbox"/>	* 10.32.128.*	SBCs

Select : All, None

6.4. Add Adaptation Module

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

For the compliance test, an adaptation was applied to the Communication Manager SIP entity. This adaptation mapped inbound DID numbers from Telefonica USA to local Communication Manager extensions.

To create the adaptation that will be applied to the Communication Manager SIP entity, navigate to **Routing → Adaptations** in the left-hand navigation pane and click on the **New** button in the right pane (not shown). In the new right pane that appears (shown below), fill in the following:

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

- **Adaptation name:** Enter a descriptive name for the adaptation.
- **Module name:** Enter **DigitConversionAdapter**.
- **Notes:** Enter a description (optional).

Home / Elements / Routing / Adaptations

Help ?

Adaptation Details

General

* **Adaptation name:** NWK CM Adaptation

Module name: DigitConversionAdapter

Module parameter:

Egress URI Parameters:

Notes: Use with Avaya SBCE

Commit Cancel

To map inbound DID numbers from Telefonica USA to Communication Manager extensions, scroll down to the **Digit Conversion for Outgoing Calls from SM** section. Create an entry for each DID to be mapped. Click **Add** and enter the following values for each mapping. Use default values for all remaining fields.

- **Matching Pattern:** Enter a digit string used to match the inbound DID number.
- **Min:** Enter a minimum dialed number length used in the match criteria.
- **Max:** Enter a maximum dialed number length used in the match criteria.
- **Delete Digits** Enter the number of digits to delete from the beginning of the received number.
- **Insert Digits:** Enter the number of digits to insert at the beginning of the received number.
- **Address to modify:** Select **destination** since this digit conversion only applies to the destination number.

Click **Commit** to save.

Digit Conversion for Outgoing Calls from SM

3 Items Refresh Filter: Enable

<input type="checkbox"/>	Matching Pattern ▲	Min	Max	Phone Context	Delete Digits	Insert Digits	Address to modify	Adaptation C
<input type="checkbox"/>	* 9395551234	* 10	* 10		* 10	50003	destination ▼	
<input type="checkbox"/>	* 9395551235	* 10	* 10		* 10	50006	destination ▼	
<input type="checkbox"/>	* 9395551236	* 10	* 10		* 10	50015	destination ▼	

In a real customer environment, often the DID number is comprised of the local extension plus a prefix. If this is true, then a single digit conversion entry can be created for all extensions. In the example below, a 5 digit prefix is deleted from each incoming DID number leaving a 5 digit extension to be routed by Session Manager.

Digit Conversion for Outgoing Calls from SM

1 Items Refresh Filter: Enable

<input type="checkbox"/>	Matching Pattern ▲	Min	Max	Phone Context	Delete Digits	Insert Digits	Address to modify	Adaptation C
<input type="checkbox"/>	* 93955	* 10	* 10		* 5		destination ▼	

6.5. Add SIP Entities

A SIP Entity must be added for Session Manager and for each SIP telephony system connected to Session Manager which includes Communication Manager and the Avaya SBCE. Navigate to **Routing → SIP Entities** in the left-hand navigation pane (**Section 6.1**) and click on the **New** button in the right pane (not shown). In the new right pane that appears (shown below), fill in the following:

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

- **Name:** Enter a descriptive name.
- **FQDN or IP Address:** Enter the FQDN or IP address of the SIP Entity that is used for SIP signaling.
- **Type:** Enter **Session Manager** for Session Manager, **CM** for Communication Manager and **SIP Trunk** for the Avaya SBCE.
- **Adaptation:** This field is only present if **Type** is not set to **Session Manager**. If applicable, select the appropriate **Adaptation name** created in **Section 6.4** that will be applied to this entity.
- **Location:** Select the location that applies to the SIP entity being created. For the compliance test, all components were located in location **Belleville**.
- **Time Zone:** Select the time zone for the location above.

The following screen shows the addition of Session Manager. The IP address of the virtual SM-100 Security Module is entered for **FQDN or IP Address**.

The screenshot displays the 'SIP Entities' configuration page. The breadcrumb trail at the top reads 'Home / Elements / Routing / SIP Entities'. The page title is 'SIP Entity Details'. There are 'Commit' and 'Cancel' buttons in the top right corner, along with a 'Help ?' link. The 'General' section contains the following fields: 'Name' (required, value: nwk-sm), 'FQDN or IP Address' (required, value: 10.32.120.98), 'Type' (dropdown menu, value: Session Manager), 'Notes' (text area), 'Location' (dropdown menu, value: Belleville), 'Outbound Proxy' (dropdown menu), 'Time Zone' (dropdown menu, value: America/New_York), and 'Credential name' (text area). The 'SIP Link Monitoring' section at the bottom has a 'SIP Link Monitoring' dropdown menu with the value 'Use Session Manager Configuration'.

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

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

- **Port:** Port number on which the Session Manager can listen for SIP requests.
- **Protocol:** Transport protocol to be used with this port.
- **Default Domain:** The default domain associated with this port. For the compliance test, this was the enterprise SIP domain.

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

For the compliance test, four port entries were used. The first three are the standard ports used for SIP traffic: port 5060 for UDP/TCP and port 5061 for TLS. In addition, port 5260 defined in **Section 5.6** for use with service provider SIP traffic between Communication Manager and Session Manager was added to the list.

Port
TCP Failover port:
TLS Failover port:

4 Items | [Refresh](#) Filter: [Enable](#)

<input type="checkbox"/>	Port	Protocol	Default Domain	Notes
<input type="checkbox"/>	<input type="text" value="5060"/>	<input type="text" value="TCP"/>	<input type="text" value="sip.avaya.com"/>	<input type="text" value="for enterprise SBC's"/>
<input type="checkbox"/>	<input type="text" value="5060"/>	<input type="text" value="UDP"/>	<input type="text" value="sip.avaya.com"/>	<input type="text"/>
<input type="checkbox"/>	<input type="text" value="5061"/>	<input type="text" value="TLS"/>	<input type="text" value="sip.avaya.com"/>	<input type="text" value="for nwk-cm & nwk-aes1"/>
<input type="checkbox"/>	<input type="text" value="5260"/>	<input type="text" value="TLS"/>	<input type="text" value="sip.avaya.com"/>	<input type="text" value="for nwk-cm-trk4"/>

Select : All, None

The following screen shows the addition of Communication Manager. In order for Session Manager to send SIP service provider traffic on a separate entity link to Communication Manager, this requires the creation of a separate SIP entity for Communication Manager other than the one created at Session Manager installation for use with all other SIP traffic. The **FQDN or IP Address** field is set to the IP address of Communication Manager. For the **Adaptation** field, select the adaptation module previously defined for dial plan digit manipulation in **Section 6.4**. The **Location** field is set to **Belleville** which is the location defined for the subnet where Communication Manager resides.

[Home](#) / [Elements](#) / [Routing](#) / [SIP Entities](#)

[Help ?](#)

SIP Entity Details

CommitCancel

General

* Name: nwk-cm-trk4

* FQDN or IP Address: 10.32.120.1

Type: CM

Notes: TM SP Trunk

Adaptation: NWK CM Adaptation

Location: Belleville

Time Zone: America/New_York

Override Port & Transport with DNS SRV: ☐

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

Credential name:

Call Detail Recording: none

SIP Link Monitoring

SIP Link Monitoring: Use Session Manager Configuration

The following screen shows the addition of the Avaya SBCE. The **FQDN or IP Address** field is set to the IP address of its private network interface (see **Figure 1**). The **Location** field is set to **Belleville** which is the location defined for the subnet where the Avaya SBCE resides.

The screenshot shows a web-based configuration interface for SIP Entities. The breadcrumb navigation at the top reads "Home / Elements / Routing / SIP Entities". The page title is "SIP Entity Details", and there are "Commit" and "Cancel" buttons in the top right corner. A "Help ?" link is also present. The "General" section contains the following fields: "Name" (ASBCE), "FQDN or IP Address" (10.32.128.18), "Type" (SIP Trunk), "Notes" (Avaya SBC for Enterprise), "Adaptation" (empty), "Location" (Belleville), and "Time Zone" (America/New_York). There is an "Override Port & Transport with DNS SRV" checkbox which is unchecked. The "SIP Timer B/F (in seconds)" is set to 4. The "Credential name" field is empty. The "Call Detail Recording" is set to egress. The "SIP Link Monitoring" section at the bottom has a "SIP Link Monitoring" dropdown set to "Use Session Manager Configuration".

Home / Elements / Routing / SIP Entities

SIP Entity Details

Commit Cancel Help ?

General

* Name: ASBCE

* FQDN or IP Address: 10.32.128.18

Type: SIP Trunk

Notes: Avaya SBC for Enterprise

Adaptation:

Location: Belleville

Time Zone: America/New_York

Override Port & Transport with DNS SRV: ☐

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

Credential name:

Call Detail Recording: egress

SIP Link Monitoring

SIP Link Monitoring: Use Session Manager Configuration

6.6. Add Entity Links

A SIP trunk between Session Manager and a telephony system is described by an Entity Link. Two Entity Links were created: one to Communication Manager for use only by service provider traffic and one to the Avaya SBCE. To add an Entity Link, navigate to **Routing → Entity Links** in the left-hand navigation pane (**Section 6.1**) and click on the **New** button in the right pane (not shown). In the new right pane that appears (shown below), fill in the following:

- **Name:** Enter a descriptive name.
- **SIP Entity 1:** Select the Session Manager.
- **Protocol:** Select the transport protocol used for this link.
- **Port:** Port number on which Session Manager will receive SIP requests from the far-end. For the Communication Manager Entity Link, this must match the **Far-end Listen Port** defined on the Communication Manager signaling group in **Section 5.6**.
- **SIP Entity 2:** Select the name of the other system. For the Communication Manager Entity Link, select the Communication Manager SIP Entity defined in **Section 6.5**.
- **Port:** Port number on which the other system receives SIP requests from the Session Manager. For the Communication Manager Entity Link, this must match the **Near-end Listen Port** defined on the Communication Manager signaling group in **Section 5.6**.
- **Connection Policy:** Select **Trusted** from pull-down menu.

Click **Commit** to save. The following screen illustrates 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**.

Home / Elements / Routing / Entity Links

Entity Links Help ?

Commit Cancel

1 Item Refresh Filter: Enable

Name	SIP Entity 1	Protocol	Port	SIP Entity 2	Port	Connection Policy
* SM to CM TRK 4	* nwk-sm	TLS	* 5260	* nwk-cm-trk4	* 5260	Trusted

The following screen illustrates the Entity Link to the Avaya SBCE.

Home / Elements / Routing / Entity Links

Entity Links [Help ?](#)

1 Item | [Refresh](#) Filter: [Enable](#)

Name	SIP Entity 1	Protocol	Port	SIP Entity 2	Port	Connection Policy
* SM to ASBCE	* nwk-sm	TCP	* 5060	* ASBCE	* 5060	Trusted

6.7. Add Routing Policies

Routing policies describe the conditions under which calls will be routed to the SIP Entities specified in **Section 6.5**. Two routing policies must be added: one for Communication Manager and one for the Avaya SBCE. To add a routing policy, navigate to **Routing → Routing Policies** in the left-hand navigation pane (**Section 6.1**) and click on the **New** button in the right pane (not shown). In the new right pane that appears (shown below), fill in the following:

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

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

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

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

Home / Elements / Routing / Routing Policies

Help ?

Commit Cancel

Routing Policy Details

General

* Name:

CM TRK4 Policy

Disabled:

☐

* Retries:

0

Notes:

TM SP Testing

SIP Entity as Destination

Select

Name	FQDN or IP Address	Type	Notes
nwk-cm-trk4	10.32.120.1	CM	TM SP Trunk

Home / Elements / Routing / Routing Policies

Routing Policy Details

CommitCancel

Help ?

General

* Name:

ASBCE Policy

Disabled:

☐

* Retries:

0

Notes:

SIP Entity as Destination

Select

Name	FQDN or IP Address	Type	Notes
ASBCE	10.32.128.18	SIP Trunk	Avaya SBC for Enterprise

6.8. Add Dial Patterns

Dial Patterns are needed to route calls through Session Manager. For the compliance test, dial patterns were needed to route calls from Communication Manager to Telefonica USA and vice versa. Dial Patterns define which route policy will be selected for a particular call based on the dialed digits, destination domain and originating location. To add a dial pattern, navigate to **Routing → Dial Patterns** in the left-hand navigation pane (**Section 6.1**) and click on the **New** button in the right pane (not shown). In the new right pane that appears (shown below), fill in the following:

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

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

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

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

Two examples of the dial patterns used for the compliance test are shown below. The first example shows that numbers that begin with 1 and have a destination domain of **sip.avaya.com** from **ALL** locations use route policy **ASBCE Policy**.

Home / Elements / Routing / Dial Patterns

Dial Pattern Details
[Help ?](#)

General

* Pattern:

* Min:

* Max:

Emergency Call: ☐

Emergency Priority:

Emergency Type:

SIP Domain:

Notes:

Originating Locations and Routing Policies

1 Item Refresh Filter: [Enable](#)

<input type="checkbox"/>	Originating Location Name 1 ▲	Originating Location Notes	Routing Policy Name	Rank 2 ▲	Routing Policy Disabled	Routing Policy Destination	Routing Policy Notes
<input type="checkbox"/>	-ALL-	Any Locations	ASBCE Policy	0	<input type="checkbox"/>	ASBCE	

Select : All, None

The second example shows that 10 digit numbers that start with **939555** to domain **sip.avaya.com** and originating from **ALL** locations use route policy **CM TRK 4 Policy**. These are the DID numbers assigned to the enterprise from Telefonica USA.

Home / Elements / Routing / Dial Patterns

Dial Pattern Details
[Help ?](#)

General

* Pattern:

* Min:

* Max:

Emergency Call: ☐

Emergency Priority:

Emergency Type:

SIP Domain:

Notes:

Originating Locations and Routing Policies

1 Item | [Refresh](#)
[Filter: Enable](#)

<input type="checkbox"/>	Originating Location Name 1 ▲	Originating Location Notes	Routing Policy Name	Rank 2 ▲	Routing Policy Disabled	Routing Policy Destination	Routing Policy Notes
<input type="checkbox"/>	-ALL-	Any Locations	CM TRK4 Policy	0	<input type="checkbox"/>	nwk-cm-trk4	TM SP Testing

Select : All, None

The complete list of dial patterns defined for the compliance test is shown below.

Home / Elements / Routing / Dial Patterns

Help ?

Dial Patterns

Edit

New

Duplicate

Delete

More Actions ▾

11 Items

Refresh

Filter: Enable

<input type="checkbox"/>	Pattern	Min	Max	Emergency Call	Emergency Type	Emergency Priority	SIP Domain	Notes
<input type="checkbox"/>	011	10	18	<input type="checkbox"/>			sip.avaya.com	Outbound international call
<input type="checkbox"/>	1	11	11	<input type="checkbox"/>			sip.avaya.com	Outbound
<input type="checkbox"/>	4	5	5	<input type="checkbox"/>			sip.avaya.com	
<input type="checkbox"/>	411	3	3	<input type="checkbox"/>			sip.avaya.com	Outbound call for local directory assistance
<input type="checkbox"/>	5	5	5	<input type="checkbox"/>			sip.avaya.com	
<input type="checkbox"/>	939555	10	10	<input type="checkbox"/>			sip.avaya.com	DID Numbers

Select : All, None

6.9. Add/View Session Manager

The creation of a Session Manager element provides the linkage between System Manager and Session Manager. This was most likely done as part of the initial Session Manager installation. To add a Session Manager, from the **Home** page, navigate to **Elements → Session Manager → Session Manager Administration** in the left-hand navigation pane (**Section 6.1**) and click on the **New** button in the right pane (not shown). If the Session Manager already exists, select the appropriate Session Manager and click **View** (not shown) to view the configuration. Enter/verify the data as described below and shown in the following screen:

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

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

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

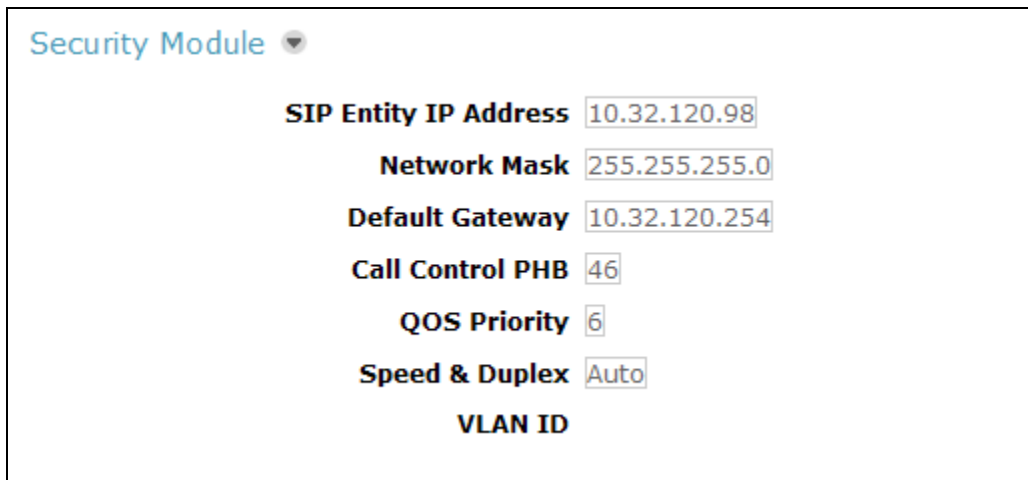
The screenshot shows the 'View Session Manager' configuration page. The breadcrumb navigation at the top reads 'Home / Elements / Session Manager / Session Manager Administration'. A 'Help ?' link is in the top right corner. The page title is 'View Session Manager' with a 'Return' button. Below the title is a horizontal menu with links: 'General | Security Module | NIC Bonding | Monitoring | CDR | Personal Profile Manager (PPM) - Connection Settings | Event Server |'. Below this menu are links for 'Expand All' and 'Collapse All'. The 'General' section is expanded, showing four configuration fields: 'SIP Entity Name' with the value 'nwk-sm', 'Description' (empty), 'Management Access Point Host Name/IP' with the value 'nwk-sm.avaya.com', and 'Direct Routing to Endpoints' with the value 'Disable'.

Field	Value
SIP Entity Name	nwk-sm
Description	
Management Access Point Host Name/IP	nwk-sm.avaya.com
Direct Routing to Endpoints	Disable

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

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

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



The screenshot displays the 'Security Module' configuration interface. It features a title bar with the text 'Security Module' and a dropdown arrow. Below the title, there are seven configuration fields, each with a label and a text input box. The fields are: 'SIP Entity IP Address' with the value '10.32.120.98', 'Network Mask' with '255.255.255.0', 'Default Gateway' with '10.32.120.254', 'Call Control PHB' with '46', 'QOS Priority' with '6', 'Speed & Duplex' with 'Auto', and 'VLAN ID' which is currently empty.

Field	Value
SIP Entity IP Address	10.32.120.98
Network Mask	255.255.255.0
Default Gateway	10.32.120.254
Call Control PHB	46
QOS Priority	6
Speed & Duplex	Auto
VLAN ID	


7. Configure Avaya Session Border Controller for Enterprise

This section describes the configuration of the Avaya SBCE. It is assumed that the initial installation of the Avaya SBCE has been completed including the assignment of a management IP address. The management interface **must** be provisioned on a different subnet than either the Avaya SBCE private or public network interfaces (e.g., A1 and B1). If the management interface has not been configured on a separate subnet, then contact your Avaya representative for guidance in correcting the configuration.

On all screens described in this section, it is to be assumed that parameters are left at their default values unless specified otherwise.

7.1. Access the Management Interface

Use a web browser to access the web interface by entering the URL **https://<ip-addr>**, where **<ip-addr>** is the management IP address assigned during installation. A screen will appear (not shown) requesting the user to **Choose a destination**. Select **UC-Sec Control Center** and the Avaya SBCE login page will appear as shown below. Log in with appropriate credentials.

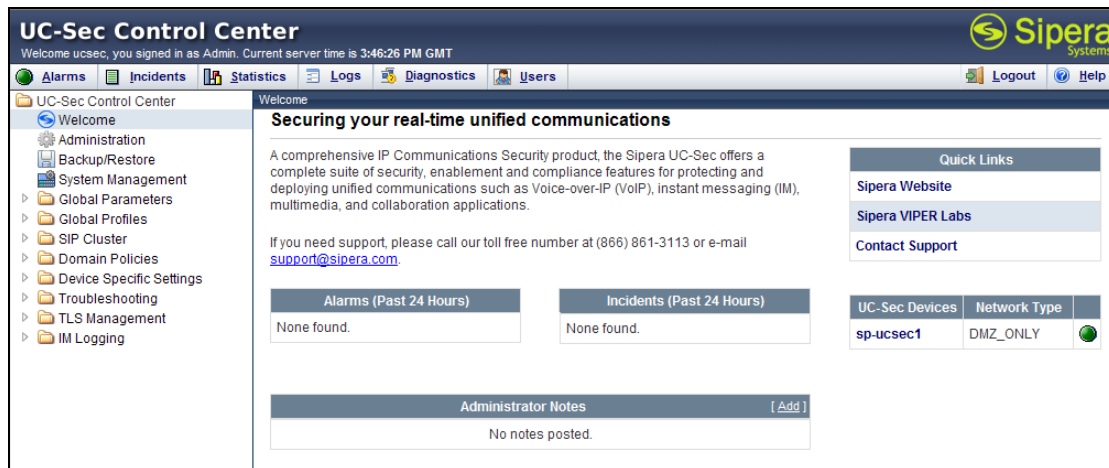


The UC-Sec™ family of products from Sipera Systems delivers comprehensive VoIP security by adapting the best practices of Internet security and by using unique, sophisticated techniques such as VoIP protocol misuse & anomaly detection, behavioral learning based anomaly detection and voice spam detection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

[Visit the Sipera Systems website to learn more.](#)

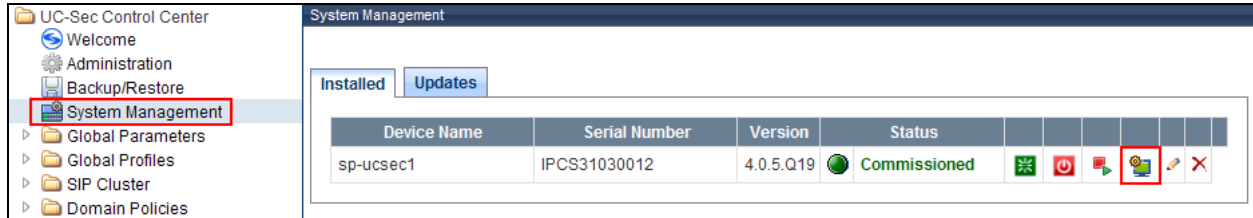
NOTICE TO USERS: This system is for authorized use only. Unauthorized use of this system is strictly prohibited. Unauthorized or improper use of this system may result in civil and/or criminal penalties. Use of this system constitutes consent to security monitoring. All activity is logged with login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

After logging in, the Welcome screen will appear as shown below. All configuration screens of the Avaya SBCE are accessed by navigating the menu tree in the left pane.



7.2. Verify Network Configuration and Enable Interfaces

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



A System Information page will appear showing the information provided during installation. In the **Appliance Name** field is the name of the device (**sp-ucsec1**). This name will be referenced in other configuration screens. Interfaces **A1** and **B1** represent the private and public interfaces of the Avaya SBCE. Each of these interfaces must be enabled after installation.

System Information: sp-ucsec1

Network Configuration

General Settings

Appliance Name	sp-ucsec1
Box Type	SIP
Deployment Mode	Proxy

Device Settings

HA Mode	No
Secure Channel Mode	None
Two Bypass Mode	No

Network Settings

IP	Public IP	Netmask	Gateway	Interface
10.32.128.18	10.32.128.18	255.255.255.0	10.32.128.254	A1
192.168.96.228	192.168.96.228	255.255.255.224	192.168.96.254	B1

DNS Configuration

Primary DNS	10.32.128.200
Secondary DNS	
DNS Location	DMZ
DNS Client IP	10.32.128.18

Management IP(s)

IP	10.32.101.10
----	--------------

To enable the interfaces, first navigate to **Device Specific Settings** → **Network Management** in the left pane and select the device being managed in the center pane. The right pane will show the same **A1** and **B1** interfaces displayed in the previous screen. Click on the **Interface Configuration** tab.

UC-Sec Control Center

Device Specific Settings > Network Management: sp-ucsec1

UC-Sec Devices

sp-ucsec1

Network Configuration Interface Configuration

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

A1 Netmask 255.255.255.0 A2 Netmask B1 Netmask 255.255.255.224 B2 Netmask

Add IP Save Changes Clear Changes

IP Address	Public IP	Gateway	Interface	
10.32.128.18		10.32.128.254	A1	✗
192.168.96.228		192.168.96.254	B1	✗

On the **Interface Configuration** tab, verify the **Administrative Status** is **Enabled** for both the **A1** and **B1** interfaces. If not, click the **Toggle State** button to enable the interface.

Network Configuration		Interface Configuration
Name	Administrative Status	
A1	Enabled	Toggle State
A2	Disabled	Toggle State
B1	Enabled	Toggle State
B2	Disabled	Toggle State

7.3. Signaling Interface

A signaling interface defines an IP address, protocols and listen ports that the Avaya SBCE can use for signaling. Create a signaling interface for both the internal and external sides of the Avaya SBCE.

To create a new interface, navigate to **Device Specific Settings → Signaling Interface** in the left pane. In the center pane, select the Avaya SBCE device (**sp-ucsec1**) to be managed. In the right pane, select **Add Signaling Interface**. A pop-up window (not shown) will appear requesting the name of the new interface, followed by series of pop-up windows in which the interface parameters can be configured. Once complete, the settings are shown in the far right pane.

For the compliance test, signaling interface **Int_Sig_Intf** was created for the Avaya SBCE internal interface. When configuring the interface, configure the parameters as follows:

- Set **Name** to a descriptive name.
- Set the **Signaling IP** to the IP address associated with the private interface (A1) defined in **Section 7.2**.
- Set **TCP port** to the port the Avaya SBCE will listen on for SIP requests on the internal interface.

Signaling interface **Ext_Sig_Intf** was created for the Avaya SBCE external interface. When configuring the interface, configure the parameters as follows:

- Set **Name** to a descriptive name.
- Set the **Signaling IP** to the IP address associated with the public interface (B1) defined in **Section 7.2**.
- Set **UDP port** to the port the Avaya SBCE will listen on for SIP requests on the external interface.

The screenshot displays the UC-Sec Control Center interface. On the left, the navigation pane shows the hierarchy: UC-Sec Control Center > Device Specific Settings > Signaling Interface. The 'Signaling Interface' option is highlighted. The main pane is titled 'Device Specific Settings > Signaling Interface: sp-ucsec1'. It shows a table of configured signaling interfaces. A red box highlights the 'sp-ucsec1' device in the left pane. Another red box highlights the 'Add Signaling Interface' button in the top right of the main pane. The table lists two interfaces: 'Int_Sig_Intf' and 'Ext_Sig_Intf'.

Name	Signaling IP	TCP Port	UDP Port	TLS Port	TLS Profile		
Int_Sig_Intf	10.32.128.18	5060	---	---	None		
Ext_Sig_Intf	192.168.96.228	---	5060	---	None		

7.4. Media Interface

A media interface defines an IP address and port range for transmitting media. Create a media interface for both the internal and external sides of the Avaya SBCE.

To create a new interface, navigate to **Device Specific Settings** → **Media Interface** in the left pane. In the center pane, select the Avaya SBCE device (**sp-ucsec1**) to be managed. In the right pane, select **Add Media Interface**. A pop-up window (not shown) will appear requesting the name of the new interface, followed by series of pop-up windows in which the interface parameters can be configured. Once complete, the settings are shown in the far right pane.

For the compliance test, signaling interface **Int_Media_Intf** was created for the Avaya SBCE internal interface. When configuring the interface, configure the parameters as follows:

- Set **Name** to a descriptive name.
- Set the **Media IP** to the IP address associated with the private interface (A1) defined in **Section 7.2**.
- Set **Port Range** to a range of ports allocated for transmitting media. For the compliance test, the default port range was used.

Signaling interface **Ext_Media_Intf** was created for the Avaya SBCE external interface. When configuring the interface, configure the parameters as follows:

- Set **Name** to a descriptive name.
- Set the **Media IP** to the IP address associated with the public interface (B1) defined in **Section 7.2**.
- Set **Port Range** to a range of ports allocated for transmitting media. For the compliance test, the default port range was used.

The screenshot displays the UC-Sec Control Center interface. On the left, the navigation pane shows the hierarchy: UC-Sec Control Center > Device Specific Settings > Media Interface. The center pane shows the 'Device Specific Settings > Media Interface: sp-ucsec1' view. A table lists the configured media interfaces:

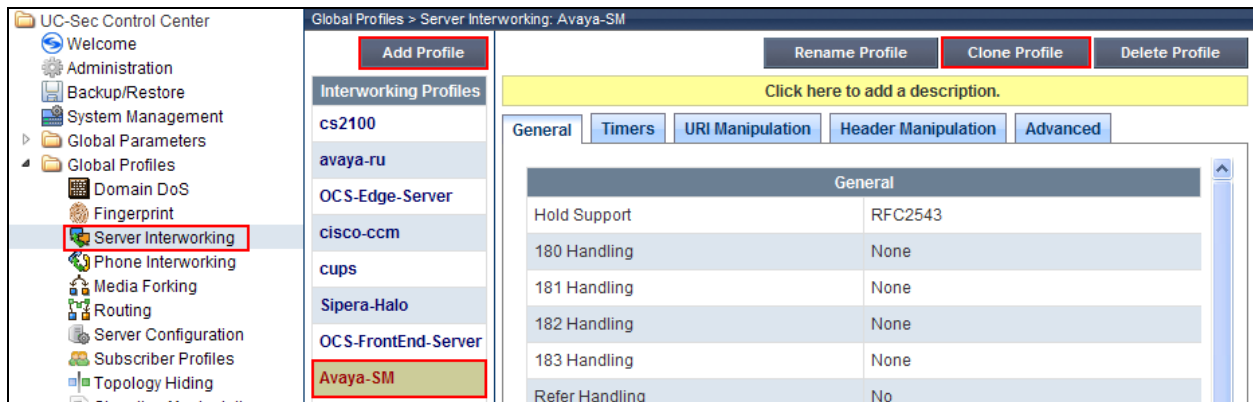
Name	Media IP	Port Range		
Int_Media_Intf	10.32.128.18	35000 - 40000		
Ext_Media_Intf	192.168.96.228	35000 - 40000		

An orange warning banner at the top of the table area states: 'Modifying or deleting an existing media interface will require an application restart before taking effect. Application restarts can be issued from System Management.' A red 'Add Media Interface' button is located above the table.

7.5. Server Interworking

A server interworking profile defines a set of parameters that aid in interworking between the Avaya SBCE and a connected server. Create a server interworking profile for the Session Manager and the service provider SIP server. These profiles will be applied to the appropriate server in **Section 7.7.1** and **7.7.2**.

To create a new profile, navigate to **Global Profiles → Server Interworking** in the left pane. In the center pane, select **Add Profile**. A pop-up window (not shown) will appear requesting the name of the new profile, followed by series of pop-up windows in which the profile parameters can be configured. Once complete, the settings are shown in the far right pane. Alternatively, a new profile may be created by selecting an existing profile in the center pane and clicking the **Clone Profile** button in the right pane. This will create a copy of the selected profile which can then be edited as needed. To view the settings of an existing profile, select the profile from the center pane. The settings will appear in the right pane.



7.5.1. Server Interworking – Session Manager

For the compliance test, server interworking profile **Avaya-SM** was created for Session Manager by cloning the existing profile **avaya-ru** then setting **T.38 Support** as needed. Since Telefonica USA is removing T.38 parameters in all messaging to the enterprise (see **Section 2.2**), the setting of the **T.38 Support** parameter (to **no** or **yes**) in the server interworking profile has no impact on signaling. Thus, it may be set to either value. During initial testing, the **T.38 Support** parameter was set to **yes** for both Session Manager and the Telefonica USA SIP server prior to determining that Telefonica would be removing the T.38 parameters. The screens below show the values used during testing. The **General** tab parameters of the interworking profile are shown with the non-default values highlighted as follows:

- **Hold Support** is set to **RFC2543**.
- **Enable T.38 Support**. (Not required for interoperability)

General	Timers	URI Manipulation	Header Manipulation	Advanced
General				
Hold Support	RFC2543			
180 Handling	None			
181 Handling	None			
182 Handling	None			
183 Handling	None			
Refer Handling	No			
3xx Handling	No			
Diversion Header Support	No			
Delayed SDP Handling	No			
T.38 Support	Yes			
URI Scheme	SIP			
Via Header Format	RFC3261			
Privacy				
Privacy Enabled	No			
User Name				
P-Asserted-Identity	No			
P-Preferred-Identity	No			
Privacy Header				
DTMF				
DTMF Support	None			
Edit				

On the **Advanced** tab, the **Topology Hiding: Change Call-ID** field is disabled and **AVAYA Extensions** are enabled.

GeneralTimersURI ManipulationHeader ManipulationAdvanced

Advanced Settings

Record Routes	BOTH
Topology Hiding: Change Call-ID	No
Call-Info NAT	No
Change Max Forwards	Yes
Include End Point IP for Context Lookup	No
OCS Extensions	No
AVAYA Extensions	Yes
NORTEL Extensions	No
SLIC Extensions	No
Diversion Manipulation	No
Metaswitch Extensions	No
Reset on Talk Spurt	No
Reset SRTP Context on Session Refresh	No
Has Remote SBC	Yes
Route Response on Via Port	No
Cisco Extensions	No

Edit

7.5.2. Server Interworking – Telefonica USA

For the compliance test, server interworking profile **SP-General** was created for the Telefonica USA SIP server. When creating the profile, the default values for all parameters were used except for **T.38 Support** which was enabled. For more information on **T.38 Support** see **Section 7.5.1**. The **General** tab parameters are as follows:

- Enable **T.38 Support**. (Not required for interoperability)

General	Timers	URI Manipulation	Header Manipulation	Advanced
General				
Hold Support	NONE			
180 Handling	None			
181 Handling	None			
182 Handling	None			
183 Handling	None			
Refer Handling	No			
3xx Handling	No			
Diversion Header Support	No			
Delayed SDP Handling	No			
T.38 Support	Yes			
URI Scheme	SIP			
Via Header Format	RFC3261			
Privacy				
Privacy Enabled	No			
User Name				
P-Asserted-Identity	No			
P-Preferred-Identity	No			
Privacy Header				
DTMF				
DTMF Support	None			
Edit				

The **Advanced** tab parameters are as follows:

General	Timers	URI Manipulation	Header Manipulation	Advanced
Advanced Settings				
Record Routes		BOTH		
Topology Hiding: Change Call-ID		Yes		
Call-Info NAT		No		
Change Max Forwards		Yes		
Include End Point IP for Context Lookup		No		
OCS Extensions		No		
AVAYA Extensions		No		
NORTEL Extensions		No		
SLiC Extensions		No		
Diversion Manipulation		No		
Metaswitch Extensions		No		
Reset on Talk Spurt		No		
Reset SRTP Context on Session Refresh		No		
Has Remote SBC		Yes		
Route Response on Via Port		No		
Cisco Extensions		No		
Edit				

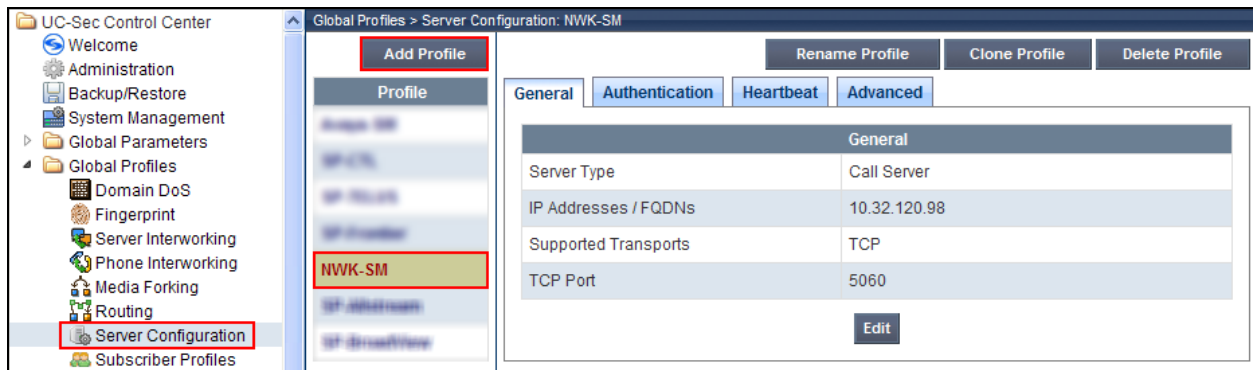
7.6. Signaling Manipulation

Signaling manipulation scripts provides for the manipulation of SIP messages which cannot be done by other configuration within the Avaya SBCE. It was not necessary to create any signaling manipulation scripts for interoperability with Telefonica USA.

7.7. Server Configuration

A server configuration profile defines the attributes of the physical server. Create a server configuration profile for the Session Manager and the service provider SIP server.

To create a new profile, navigate to **Global Profiles → Server Configuration** in the left pane. In the center pane, select **Add Profile**. A pop-up window (not shown) will appear requesting the name of the new profile, followed by series of pop-up windows in which the profile parameters can be configured. Once complete, the settings are shown in the far right pane. To view the settings of an existing profile, select the profile from the center pane. The settings will appear in the right pane.



7.7.1. Server Configuration – Session Manager

For the compliance test, server configuration profile **NWK-SM** was created for Session Manager. When creating the profile, configure the **General** tab parameters as follows:

- Set **Server Type** to **Call Server**.
- Set **IP Addresses / FQDNs** to the IP address of Session Manager signaling interface.
- Set **Supported Transports** to the transport protocol used for SIP signaling between the Session Manager and the Avaya SBCE.
- Set the **TCP Port** to the port the Session Manager will listen on for SIP requests from the Avaya SBCE.

The screenshot shows a configuration interface with three buttons at the top: "Rename Profile", "Clone Profile", and "Delete Profile". Below these are four tabs: "General", "Authentication", "Heartbeat", and "Advanced". The "General" tab is selected, displaying a table with the following configuration:

General	
Server Type	Call Server
IP Addresses / FQDNs	10.32.120.98
Supported Transports	TCP
TCP Port	5060

An "Edit" button is located at the bottom center of the configuration area.

On the **Advanced** tab, set the **Interworking Profile** field to the interworking profile for the Session Manager defined in **Section 7.5.1**. The **Signaling Manipulation Script** field retains the default value of **None**.

The screenshot shows the same configuration interface as above, but with the "Advanced" tab selected. The configuration table is as follows:

Advanced	
Enable DoS Protection	<input type="checkbox"/>
Enable Grooming	<input type="checkbox"/>
Interworking Profile	Avaya-SM
Signaling Manipulation Script	None
TCP Connection Type	SUBID

An "Edit" button is located at the bottom center of the configuration area.

7.7.2. Server Configuration – Telefonica USA

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

- Set **Server Type** to **Trunk Server**.
- Set **IP Addresses / FQDNs** to the IP address of the Telefonica USA SIP server.
- Set **Supported Transports** to the transport protocol used for SIP signaling between Telefonica USA and the Avaya SBCE.
- Set the **UDP Port** to the port Telefonica USA will listen on for SIP requests from the Avaya SBCE.

The screenshot shows the configuration interface for the 'SP-Telefonica' profile. At the top, there are three buttons: 'Rename Profile', 'Clone Profile', and 'Delete Profile'. Below these are four tabs: 'General', 'Authentication', 'Heartbeat', and 'Advanced'. The 'General' tab is selected. The configuration table below has the following data:

General	
Server Type	Trunk Server
IP Addresses / FQDNs	192.168.64.87
Supported Transports	UDP
UDP Port	5060

At the bottom of the table is an 'Edit' button.

On the **Advanced** tab, set the **Interworking Profile** field to the interworking profile for Telefonica USA defined in **Section 7.5.2**. The **Signaling Manipulation Script** field retains the default value of **None**.

The screenshot shows the configuration interface for the 'SP-Telefonica' profile, specifically the 'Advanced' tab. At the top, there are three buttons: 'Rename Profile', 'Clone Profile', and 'Delete Profile'. Below these are four tabs: 'General', 'Authentication', 'Heartbeat', and 'Advanced'. The 'Advanced' tab is selected. The configuration table below has the following data:

Advanced	
Enable DoS Protection	<input type="checkbox"/>
Enable Grooming	<input type="checkbox"/>
Interworking Profile	SP-General
Signaling Manipulation Script	None
UDP Connection Type	SUBID

At the bottom of the table is an 'Edit' button.

7.8. Signaling Rules

A signaling rule defines the processing to be applied to the selected signaling traffic. A signaling rule is one component of the larger endpoint policy group defined in **Section 7.10**. A specific signaling rule was created for Session Manager. The Telefonica USA SIP server used the **default** rule.

To create a new rule, navigate to **Domain Policies → Signaling Rules** in the left pane. In the center pane, select **Add Rule**. A pop-up window (not shown) will appear requesting the name of the new rule, followed by series of pop-up windows in which the rule parameters can be configured. Once complete, the settings are shown in the far right pane. To view the settings of an existing rule, select the rule from the center pane. The settings will appear in the right pane.

The screenshot displays the UC-Sec Control Center interface. On the left, the navigation pane shows the hierarchy: UC-Sec Control Center > Domain Policies > Signaling Rules. The 'Signaling Rules' item is selected and highlighted with a red box. The center pane, titled 'Domain Policies > Signaling Rules: SessMgr_SigRules', shows a list of signaling rules: 'default', 'No Content Type Checks', 'Frontier_SigRules', 'TELUS_SigRules', and 'SessMgr_SigRules'. The 'SessMgr_SigRules' rule is selected and highlighted with a red box. Above the list is an 'Add Rule' button, also highlighted with a red box. The right pane shows the configuration for the selected rule. It includes a 'Filter By Device...' dropdown, buttons for 'Rename Rule', 'Clone Rule', and 'Delete Rule', and a yellow bar with the text 'Click here to add a description.' Below this are tabs for 'General', 'Requests', 'Responses', 'Request Headers', 'Response Headers', and 'Signaling QoS'. The 'Requests' tab is active, showing a table for 'Inbound' traffic:





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

Below the 'Inbound' section is a section for 'Outbound' traffic, which is currently empty.

For the compliance test, signaling rule **SessMgr_SigRules** was created for Session Manager to prevent proprietary headers in the SIP messages sent from the Session Manager from being propagated to Telefonica USA. These headers may contain internal addresses or other information about the internal network. Select this rule in the center pane, then select the **Request Headers** tab to view the manipulations performed on request messages such as the initial INVITE or UPDATE message.

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

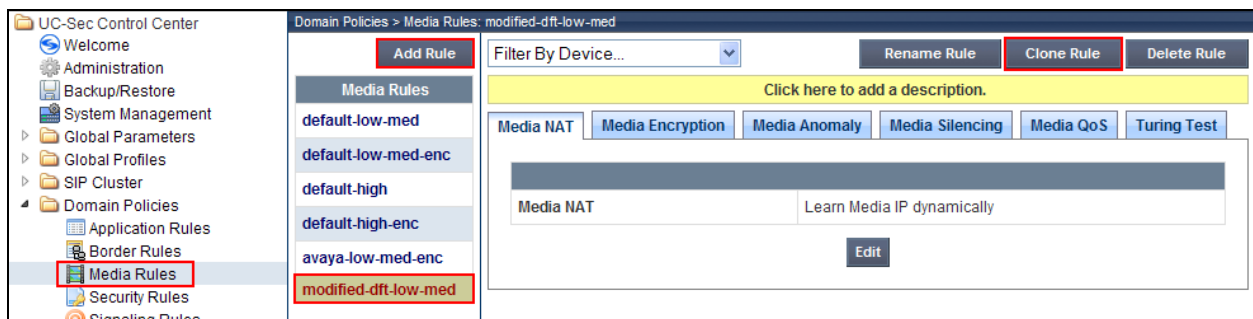
Similarly, manipulations can be performed on SIP response messages. These can be created by selecting the **Response Header** tab as shown below. Entries were created in the same manner as was done on the **Request Headers** tab. The entries shown perform the following actions:

- | General | | Requests | | Responses | | Request Headers | | Response Headers | | Signaling QoS | |
|---------|---------------|---------------|-------------|-----------------|---------------|-----------------|-----------|---|---|------------------------|--|
| | | | | | | | | Add In Header Control | | Add Out Header Control | |
| Row | Header Name | Response Code | Method Name | Header Criteria | Action | Proprietary | Direction | | | | |
| 1 | Endpoint-View | 2XX | ALL | Forbidden | Remove Header | Yes | IN |  |  | | |
| 2 | Endpoint-View | 1XX | INVITE | Forbidden | Remove Header | Yes | IN |  |  | | |

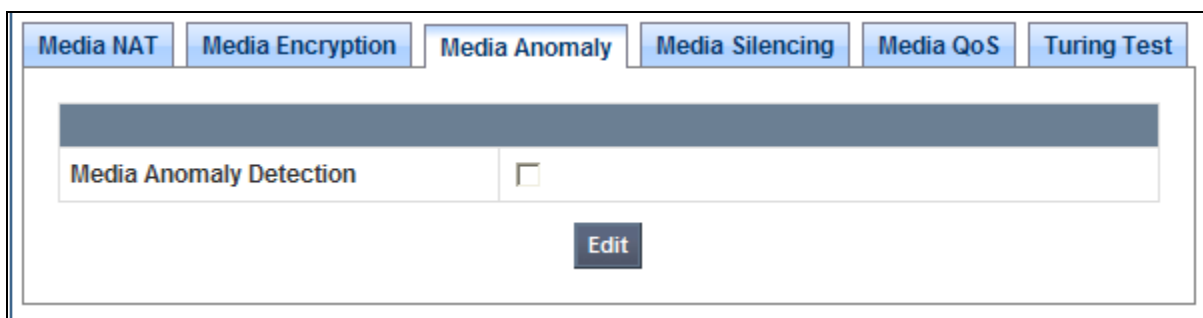
7.9. Media Rules

A media rule defines the processing to be applied to the selected media. A media rule is one component of the larger endpoint policy group defined in **Section 7.10**.

To create a new rule, navigate to **Domain Policies** → **Media Rules** in the left pane. In the center pane, select **Add Rule**. A pop-up window (not shown) will appear requesting the name of the new rule, followed by series of pop-up windows in which the rule parameters can be configured. Once complete, the settings are shown in the far right pane. Alternatively, a new rule may be created by selecting an existing rule in the center pane and clicking the **Clone Rule** button in the right pane. This will create a copy of the selected rule which can then be edited as needed. To view the settings of an existing rule, select the rule from the center pane. The settings will appear in the right pane.



For the compliance test, a single media rule **modified-dft-low-med** was created that was used for both the Session Manager and the Telefonica USA SIP server. It was created by cloning the existing rule **default-low-med** which uses unencrypted media and then disabling **Media Anomaly Detection** on the **Media Anomaly** tab. This was done to prevent some false media errors from impacting the RTP media stream.



7.10. Endpoint Policy Groups

An endpoint policy group is a set of policies that will be applied to traffic between the Avaya SBCE and a signaling endpoint (connected server). Thus, an endpoint policy group must be created for Session Manager and the service provider SIP server. The endpoint policy group is applied to the traffic as part of the endpoint flow defined in **Section 7.13**.

To create a new group, navigate to **Domain Policies → End Point Policy Groups** in the left pane. In the center pane, select **Add Group**. A pop-up window (not shown) will appear requesting the name of the new group, followed by series of pop-up windows in which the group parameters can be configured. Once complete, the settings are shown in the far right pane. To view the settings of an existing group, select the group from the center pane. The settings will appear in the right pane.

The screenshot shows the UC-Sec Control Center interface. On the left is a navigation tree with 'End Point Policy Groups' selected. The main area is titled 'Domain Policies > End Point Policy Groups: SM'. It features a list of policy groups on the left, including 'default-low', 'default-low-enc', 'default-med', 'default-med-enc', 'default-high', 'default-high-enc', 'OCS-default-high', 'avaya-def-low-enc', and 'SM' (which is highlighted). To the right of this list are buttons for 'Add Group', 'Filter By Device...', 'Rename Group', and 'Delete Group'. Below these are two yellow boxes with text: 'Click here to add a description.' and 'Click here to add a row description.'. Further right is a 'Policy Group' tab with 'View Summary' and 'Add Policy Set' buttons. Below this is a table with columns: Order, Application, Border, Media, Security, Signaling, Time of Day, and two empty columns. The first row contains the values: 1, default, default, modified-dft-low-med, default-low, SessMgr_SigRules, default, and two icons (a pencil and a plus sign).

Order	Application	Border	Media	Security	Signaling	Time of Day		
1	default	default	modified-dft-low-med	default-low	SessMgr_SigRules	default		

7.10.1. Endpoint Policy Group – Session Manager



For the compliance test, endpoint policy group **SM** was created for Session Manager. Default values were used for each of the rules which comprise the group with the exception of **Media** and **Signaling**. For **Media**, select the media rule created in **Section 7.9**. For **Signaling**, select the signaling rule created for the Session Manager in **Section 7.8.1**.

This is a close-up of the 'Policy Group' table from the previous screenshot. It shows the table structure with columns: Order, Application, Border, Media, Security, Signaling, Time of Day, and two empty columns. The first row contains the values: 1, default, default, modified-dft-low-med, default-low, SessMgr_SigRules, default, and two icons (a pencil and a plus sign).

Order	Application	Border	Media	Security	Signaling	Time of Day		
1	default	default	modified-dft-low-med	default-low	SessMgr_SigRules	default		

7.10.2. Endpoint Policy Group – Telefonica USA

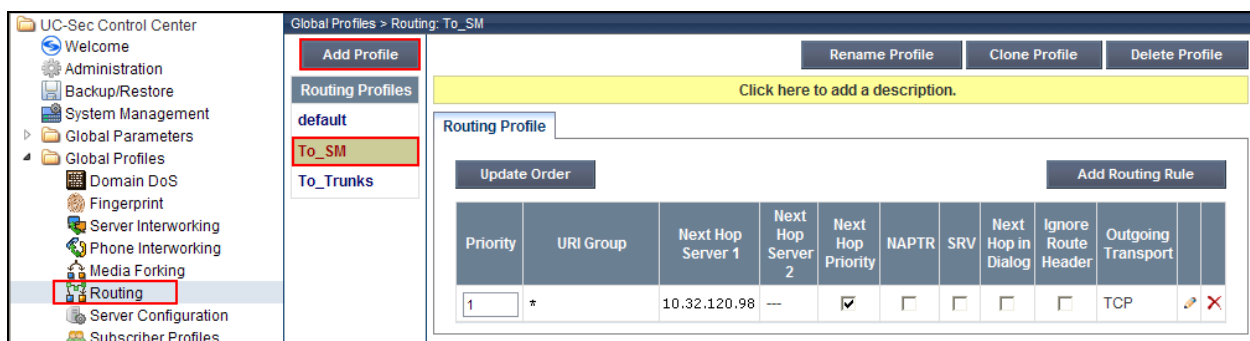
For the compliance test, endpoint policy group **General-SP** was created for the Telefonica USA SIP server. Default values were used for each of the rules which comprise the group with the exception of **Media**. For **Media**, select the media rule created in **Section 7.9**.

Policy Group							
				View Summary	Add Policy Set		
Order	Application	Border	Media	Security	Signaling	Time of Day	
1	default	default	modified-dft-low-med	default-low	default	default	 

7.11. Routing

A routing profile defines where traffic will be directed based on the contents of the URI. A routing profile is applied only after the traffic has matched an endpoint server flow defined in **Section 7.13**. Create a routing profile for the Session Manager and the service provider SIP server.

To create a new profile, navigate to **Global Profiles → Routing** in the left pane. In the center pane, select **Add Profile**. A pop-up window (not shown) will appear requesting the name of the new profile, followed by series of pop-up windows in which the profile parameters can be configured. Once complete, the settings are shown in the far right pane. To view the settings of an existing profile, select the profile from the center pane. The settings will appear in the right pane.



The screenshot displays the UC-Sec Control Center interface. The left sidebar shows the navigation tree with 'Routing' selected under 'Global Profiles'. The main area is titled 'Global Profiles > Routing: To_SM'. It features buttons for 'Add Profile', 'Rename Profile', 'Clone Profile', and 'Delete Profile'. Below these is a yellow bar with the text 'Click here to add a description.' The 'Routing Profile' section shows a table with one profile named 'To_SM'. The table has columns for Priority, URI Group, Next Hop Server 1, Next Hop Server 2, Next Hop Priority, NAPTR, SRV, Next Hop in Dialog, Ignore Route Header, and Outgoing Transport. The profile 'To_SM' has a priority of 1, a URI Group of *, Next Hop Server 1 of 10.32.120.98, Next Hop Server 2 of ---, Next Hop Priority of 1, and Outgoing Transport of TCP.

Priority	URI Group	Next Hop Server 1	Next Hop Server 2	Next Hop Priority	NAPTR	SRV	Next Hop in Dialog	Ignore Route Header	Outgoing Transport
1	*	10.32.120.98	---	1	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	TCP

7.11.1. Routing – Session Manager

For the compliance test, routing profile **To_NwkSM** was created for Session Manager. When creating the profile, configure the parameters as follows:

- Set the **URI Group** to the wild card * to match on any URI.
- Set the **Next Hop Server 1** field to the IP address of the Session Manager signaling interface.
- Enable **Next Hop Priority**.
- Set the **Outgoing Transport** field to **TCP**.

Priority	URI Group	Next Hop Server 1	Next Hop Server 2	Next Hop Priority	NAPTR	SRV	Next Hop in Dialog	Ignore Route Header	Outgoing Transport		
1	*	10.32.120.98	---	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	TCP		

7.11.2. Routing – Telefonica USA

For the compliance test, routing profile **To_Trunks** was created for Telefonica USA. When creating the profile, configure the parameters as follows:

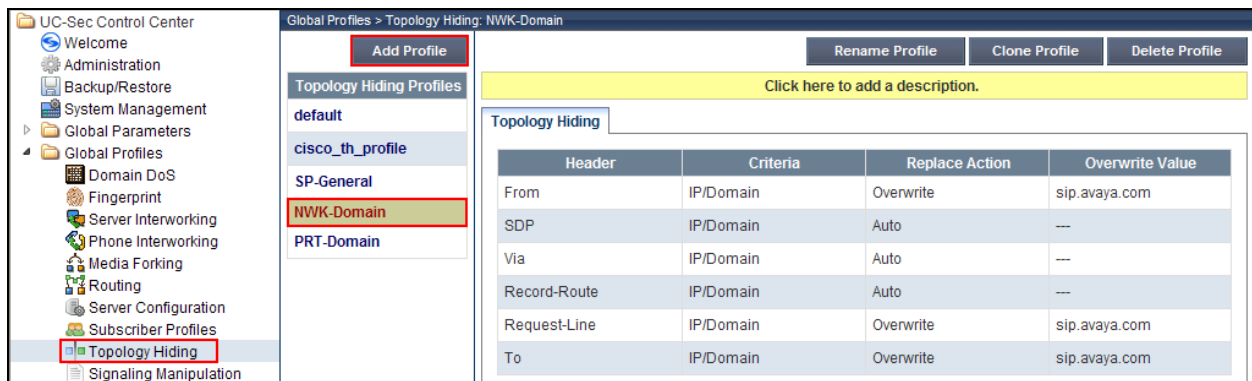
- Set the **URI Group** to the wild card * to match on any URI.
- Set the **Next Hop Server 1** field to the IP address of the Telefonica USA SIP server followed by the port number.
- Enable **Next Hop Priority**.
- Set the **Outgoing Transport** field to **UDP**.

Priority	URI Group	Next Hop Server 1	Next Hop Server 2	Next Hop Priority	NAPTR	SRV	Next Hop in Dialog	Ignore Route Header	Outgoing Transport		
1	*	192.168.64.87	---	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	UDP		

7.12. Topology Hiding

Topology hiding allows the host part of some SIP message headers to be modified in order to prevent private network information from being propagated to the untrusted public network. It can also be used as an interoperability tool to adapt the host portion of these same headers to meet the requirements of the connected servers. The topology hiding profile is applied as part of the endpoint flow in **Section 7.13**.

To create a new profile, navigate to **Global Profiles → Topology Hiding** in the left pane. In the center pane, select **Add Profile**. A pop-up window (not shown) will appear requesting the name of the new profile, followed by a pop-up window in which a header can be selected and configured. Additional headers can be added in this window. Once complete, the settings are shown in the far right pane. To view the settings of an existing profile, select the profile from the center pane. The settings will appear in the right pane.



7.12.1. Topology Hiding – Session Manager

For the compliance test, topology hiding profile **NWK-Domain** was created for Session Manager. This profile will be applied to traffic from the Avaya SBCE to Session Manager. When creating the profile, configure the parameters as follows:

- Set **Header** to the header whose host part of the URI is to be modified.
- Set **Criteria** to **IP/Domain** to indicate that the host part should be modified if it is an IP address or a domain.
- Set **Replace Action** to **Auto** for all headers except **Request-Line**, **From** and **To** which should be set to **Overwrite**.
- For those headers to be overwritten, the **Overwrite Value** is set to the enterprise domain (**sip.avaya.com**).

Topology Hiding

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

Edit

7.12.2. Topology Hiding – Telefonica USA

For the compliance test, topology hiding profile **SP-General** was created for Telefonica USA. This profile will be applied to traffic from the Avaya SBCE to Telefonica USA. When creating the profile, configure the parameters as follows:

- Set **Header** to the header whose host part of the URI is to be modified.
- Set **Criteria** to **IP/Domain** to indicate that the host part should be modified if it is an IP address or a domain.
- Set **Replace Action** to **Auto** for all headers.

Topology Hiding

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

Edit

7.13. End Point Flows

Endpoint flows are used to determine the signaling endpoints involved in a call in order to apply the appropriate policies. When a packet arrives at the Avaya SBCE, the content of the packet (IP addresses, URIs, etc) is used to determine which flow it matches. Once the flow is determined, the flow points to policies and profiles which control processing, privileges, authentication, routing, etc. Once routing is applied and the destination endpoint is determined, the policies for the destination endpoint are applied. Thus, two flows are involved in every call: the source endpoint flow and the destination endpoint flow. In the case of SIP trunking, the signaling endpoints are the Session Manager and the service provider SIP server.

To create a new flow for a server endpoint, navigate to **Device Specific Settings → End Point Flows** in the left pane. In the center pane, select the Avaya SBCE device (**sp-ucsec1**) to be managed. In the right pane, select the **Server Flows** tab and click the **Add Flow** button. A pop-up window (not shown) will appear requesting the name of the new flow and the flow parameters. Once complete, the settings are shown in the far right pane.





7.13.1. End Point Flow – Session Manager

For the compliance test, endpoint flow **SM** was created for the Session Manager. All traffic from the Session Manager will match this flow as the source flow and use the specified **Routing Profile To_Trunks** to determine the destination server and corresponding destination flow. The **End Point Policy** and **Topology Hiding Profile** will be applied as appropriate. When creating the flow, configure the parameters as follows:

- For the **Flow Name**, enter a descriptive name.
- For **Server Configuration**, select the Session Manager server created in **Section 7.7.1**.
- To match all traffic, set the **URI Group**, **Transport**, and **Remote Subnet** to *.
- Set the **Received Interface** to the external signaling interface.
- Set the **Signaling Interface** to the internal signaling interface.
- Set the **Media Interface** to the internal media interface.
- Set the **End Point Policy Group** to the endpoint policy group defined for Session Manager in **Section 7.10.1**.
- Set the **Routing Profile** to the routing profile defined in **Section 7.11.2** used to direct traffic to the Telefonica USA SIP server.




- Set the **Topology Hiding Profile** to the topology hiding profile defined for Session Manager in **Section 7.12.1**.

Server Configuration: NWK-SM													
Priority	Flow Name	URI Group	Transport	Remote Subnet	Received Interface	Signaling Interface	Media Interface	End Point Policy Group	Routing Profile	Topology Hiding Profile	File Transfer Profile		
<div>1</div>	NWK-SM	*	*	*	Ext_Sig_Intf	Int_Sig_Intf	Int_Media_Intf	SM	To_Trunks	NWK-Domain	None		

7.13.2. End Point Flow – Telefonica USA

For the compliance test, endpoint flow **Telefonica** was created for the Telefonica USA SIP server. All traffic from Telefonica USA will match this flow as the source flow and use the specified **Routing Profile To_SM** to determine the destination server and corresponding destination flow. The **End Point Policy** and **Topology Hiding Profile** will be applied as appropriate. When creating the flow, configure the parameters as follows:

- For the **Flow Name**, enter a descriptive name.
- For **Server Configuration**, select the Telefonica USA SIP server created in **Section 7.7.2**.
- To match all traffic, set the **URI Group**, **Transport**, and **Remote Subnet** to *.
- Set the **Received Interface** to the internal signaling interface.
- Set the **Signaling Interface** to the external signaling interface.
- Set the **Media Interface** to the external media interface.
- Set the **End Point Policy Group** to the endpoint policy group defined for Telefonica USA in **Section 7.10.2**.
- Set the **Routing Profile** to the routing profile defined in **Section 7.11.1** used to direct traffic to the Session Manager.
- Set the **Topology Hiding Profile** to the topology hiding profile defined for Telefonica USA in **Section 7.12.2**.

Server Configuration: SP-Telefonica														
Priority	Flow Name	URI Group	Transport	Remote Subnet	Received Interface	Signaling Interface	Media Interface	End Point Policy Group	Routing Profile	Topology Hiding Profile	File Transfer Profile			
<div>1</div>	SP-Telefonica	*	*	*	Int_Sig_Intf	Ext_Sig_Intf	Ext_Media_Intf	General-SP	To_NwkSM	SP-General	None			

8. Telefonica USA SIP Trunk Service Configuration

Telefonica USA is responsible for the network configuration and deployment of the Telefonica USA SIP Trunk Service. The service is offered through a MPLS transport network, and both public and private addressing is supported. The service is also configured following the guidelines of Acme Packet and Broadsoft for Avaya SIP trunking interoperability. The service also supports International Toll Free Service (ITFS) delivery through the same infrastructure.

Telefonica USA will require that the customer provide the IP address and port number used to reach the Avaya SBCE at the edge of the enterprise. Telefonica USA will provide the IP address and port number of the Telefonica USA SIP proxy/SBC, IP addresses/ports of media sources and Direct Inward Dialed (DID) numbers assigned to the enterprise. This information is used to complete the Communication Manager, Session Manager and the Avaya SBCE configuration discussed in the previous sections.

The configuration between Telefonica USA and the enterprise is a static configuration. There is no registration of the SIP trunk or enterprise users to the Telefonica USA network.

9. Verification Steps

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

Verification Steps:

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

Troubleshooting:

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

- **status trunk** <trunk access code number/channel number> - Displays signaling and media information for an active trunk channel.
2. Session Manager:
- **Call Routing Test** - The Call Routing Test verifies the routing for a particular source and destination. To run the routing test, navigate to **Elements → Session Manager → System Tools → Call Routing Test**. Enter the requested data to run the test.

10. Conclusion

These Application Notes describe the configuration necessary to connect Avaya Aura® Communication Manager, Avaya Aura® Session Manager and Avaya Session Border Controller for Enterprise to the Telefonica USA SIP Trunk Service. The Telefonica USA SIP Trunk Service is a SIP-based Voice over IP solution for customers ranging from small businesses to large enterprises. The Telefonica USA SIP Trunk Service provides businesses a flexible, cost-saving alternative to traditional hardwired telephony trunks. Please refer to **Section 2.2** for any exceptions or workarounds.

11. References

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

- [1] *Installing and Configuring Avaya Aura® System Platform*, Release 6.2.1, July 2012.
- [2] *Administering Avaya Aura® System Platform*, Release 6.2.1, July 2012.
- [3] *Administering Avaya Aura® Communication Manager*, Release 6.2, December 2012, Document Number 03-300509.
- [4] *Avaya Aura® Communication Manager Feature Description and Implementation*, Release 6.2, December 2012, Document Number 555-245-205.
- [5] *Upgrading Avaya Aura® System Manager*, Release 6.2, July 2012.
- [6] *Administering Avaya Aura® System Manager*, Release 6.2, July 2012.
- [7] *Installing and Configuring Avaya Aura® Session Manager*, Release 6.1, April 2011, Document Number 03-603473.
- [8] *Administering Avaya Aura® Session Manager*, Release 6.2, July 2012, Document Number 03-603324.
- [9] *Avaya 1600 Series IP Deskphones Administrator Guide Release 1.3.x*, May 2010, Document Number 16-601443.
- [10] *Avaya one-X® Deskphone Edition H.323 for 9600 Series IP Deskphones Administrator Guide*, Release 3.1.5, August 2012, Document Number 16-300698.
- [11] *Avaya one-X® Deskphone Edition H.323 9608,9611G,9621G and 9641G Administrator Guide*, Release 6.2, February 2012, Document Number 16-300698.
- [12] *Avaya one-X® Deskphone Edition SIP 9608/9611G/9621G/9641G Administrator Guide*, Release 6.2, August 2012, Document Number 16-601944.
- [13] *Administering Avaya one-X® Communicator*, July 2011.
- [14] RFC 3261 *SIP: Session Initiation Protocol*, <http://www.ietf.org/>

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

©2013 Avaya Inc. All Rights Reserved.

Avaya and the Avaya Logo are trademarks of Avaya Inc. All trademarks identified by ® and ™ are registered trademarks or trademarks, respectively, of Avaya Inc. All other trademarks are the property of their respective owners. The information provided in these Application Notes is subject to change without notice. The configurations, technical data, and recommendations provided in these Application Notes are believed to be accurate and dependable, but are presented without express or implied warranty. Users are responsible for their application of any products specified in these Application Notes.

Please e-mail any questions or comments pertaining to these Application Notes along with the full title name and filename, located in the lower right corner, directly to the Avaya DevConnect Program at devconnect@avaya.com.