



Avaya Solution & Interoperability Test Lab

Application Notes for Configuring MTS Allstream SIP Trunking with Avaya Aura® Communication Manager Evolution Server 6.0.1, Avaya Aura® Session Manager 6.1, and Avaya Aura® Session Border Controller – Issue 1.0

Abstract

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

MTS Allstream 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 MTS Allstream SIP Trunking and an Avaya SIP-enabled enterprise solution. The Avaya solution consists of Avaya Aura® Session Manager, Avaya Aura® Communication Manager Evolution Server, Avaya Aura® Session Border Controller and various Avaya endpoints.

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

2. General Test Approach and Test Results

The general test approach was to connect a simulated enterprise site to the MTS Allstream SIP Trunking service via the public Internet and exercise the features and functionality listed in **Section 2.1**. The simulated enterprise site was comprised of Avaya Aura® Communication Manager, Avaya Aura® Session Manager and the Avaya Aura® Session Border Controller.

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 H.323, SIP, digital, and analog 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, SIP, digital, and analog 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). Communicator supports two modes (Road Warrior and Telecommuter). Each of these modes was tested. Communicator also supports two Voice Over IP (VoIP) protocols: H.323 and SIP. Both protocol versions of Communicator were tested.
- Various call types including: local, long distance, international, outbound toll-free, operator services and directory assistance.
- Codecs G.711MU and G.729A
- 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
- User features such as hold and resume, internal call forwarding, transfer, and conference
- Off-net call forwarding and mobility (extension to cellular)

Items not supported or not tested included the following:

- MTS Allstream SIP Trunking was not configured to send SIP OPTIONS messages during the compliance test but will respond to the OPTIONS messages sent by the Session Border Controller.
- Inbound toll-free and emergency calls (911) are supported but were not tested as part of the compliance test.
- Local outbound calling using 7 digit dialing is not supported. These calls require dialing 10 digits. Inbound local calls can be configured for 7 digits but this was not tested.
- T.38 fax is not supported.
- The SIP REFER method is not supported for network redirection.
- A “302 Moved Temporarily” response with new Contact header is not supported for network redirection.

2.2. Test Results

Interoperability testing of MTS Allstream SIP Trunking was completed with successful results for all test cases with the exception of the observations/limitations described below.

- **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. Not all PSTN destinations have the ability to update their call display after the call is answered. It is listed here simply as an observation. (See related item below.)
- **Incorrect Contact header sent by Avaya Aura® Session Border Controller:** After the transfer of an inbound PSTN call to a 2nd PSTN phone is completed, Communication Manager sends an UPDATE message to the Session Border Controller with updated Contact header information to reflect the actual connected party. It was observed that the UPDATE message sent to the Session Border Controller correctly contained the originating PSTN phone number (the actual connected party) in the Contact header. However, in the UPDATE message sent from the Session Border Controller to MTS Allstream, the Contact header was altered to contain the number of the transferring party. This problem was addressed via configuration in a previous release of the Session Border Controller. However, this same configuration failed to work in the release used for this compliance test. This issue was reported to development and will be addressed in a later release of the Session Border Controller software.
- **Asymmetric DTMF payload header values are not supported:** MTS Allstream does not support the use of a different DTMF payload header value in each direction of a single call. This may occur if the media is re-directed from the Communication Manager to an endpoint and the endpoint wishes to use a different DTMF payload header value then was negotiated when the call was initially established. MTS Allstream accepts the SIP signaling that establishes the use of asymmetric DTMF payload headers but does not honor it. The result is that DTMF tones are not properly recognized. During the compliance testing, this was observed when an Avaya 9600 Series SIP Telephone called a PSTN based IVR application such as a user’s cell phone voicemail. The DTMF tones

needed to navigate the voicemail menus were not recognized by the application. Normally, this particular situation could be worked around by setting the default DTMF payload value used by the Avaya 9600 Series SIP Telephone to the value used by MTS Allstream (101). This is done by adding the line **DTMF_PAYLOAD 101** to the phone configuration file (46xxsettings.txt). However, this exposed a problem in the phone firmware as described in the next bullet item.

- **Avaya 9600 Series SIP Telephones do not always use the correct DTMF payload header value:** In some call scenarios, the Avaya 9600 Series SIP Telephones will use the DTMF payload header value set in the configuration file (46xxsettings.txt) in signaling messages during call-setup but continues to use its default payload header value of 120 when transmitting the actual DTMF tone. One such scenario is dialing a feature name extension (FNE) from the phone to set-up call forwarding. When the FNE call is established, digits are entered by the user to specify the call forwarding destination. In this case, the phone is sending the digits using a DTMF payload header value of 120 but Communication Manager is expecting the DTMF payload header value provisioned in the phone configuration file. As a result, the DTMF tones are not recognized by Communication Manager and call forwarding can not be established. The only workaround is to leave the DTMF payload header value in the phone configuration file as 120. However, it causes DTMF problems in other call scenarios like the one described in the previous bullet item regarding calling an external IVR application from the Avaya 9600 Series SIP Telephones.
- **Local calls from the enterprise routed via the MTS Allstream network to another DID assigned to the enterprise results in no audio.** This problem is believed to have low user impact because all other local calls from the enterprise (calls within the same area code) complete successfully with audio. Audio is only impacted when calling another DID associated with the enterprise and the call is routed via the service provider. In general, these calls would not be routed to the service provider but would be routed within the enterprise which avoids the problem. It was also observed that this failure scenario was also related to shuffling because if shuffling was disabled on the service provider trunk then the no audio issue disappeared. However, it is recommended that shuffling remain enabled on the service provider trunk and the failing scenario is avoided by routing these types of calls within the enterprise.

2.3. Support

For technical support on the MTS Allstream SIP Trunking Service, contact MTS Allstream Customer Care by calling 866-282-0111 or by sending email to ABC3@mtsallstream.com.

Avaya customers may obtain documentation and support for Avaya products by visiting <http://support.avaya.com>. Selecting the **Support Contact Options** link followed by **Maintenance Support** provides the worldwide support directory for Avaya Global Services. Specific numbers are provided for both customers and partners based on the specific type of support or consultation services needed. Some services may require specific Avaya service support agreements. Alternatively, in the United States, (866) GO-AVAYA (866-462-8292) provides access to overall sales and service support menus.

3. Reference Configuration

Figure 1 illustrates a sample Avaya SIP-enabled enterprise solution connected to MTS Allstream SIP Trunking. This is the configuration used for compliance testing.

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

- Avaya S8300D Server running Avaya Aura® Communication Manager
- Avaya G450 Media Gateway
- Avaya S8800 Server running Avaya Aura® Session Manager
- Avaya S8800 Server running Avaya Aura® System Manager
- Avaya 9600-Series IP telephones (H.323 and SIP)
- Avaya 4600-Series IP telephones (H.323)
- Avaya 1600-Series IP telephones (H.323)
- Avaya one-X® Communicator (H.323 and SIP)
- Avaya digital and analog telephones

Located at the edge of the enterprise is the Avaya Aura® Session Border Controller. 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 Session Border Controller. In this way, the Session Border Controller can protect the enterprise against any SIP-based attacks. The Session Border Controller 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 can not be routed by the PSTN.

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 Session Border Controller. From the Session Border Controller, the call is sent to MTS Allstream SIP Trunking.

For the compliance test, the enterprise sent 11 digits in the destination headers (e.g., Request-URI and To) and sent 10 digits in the source headers (e.g., From, Contact, and P-Asserted-Identity (PAI)). MTS Allstream sent 10 digits in both the source 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	
Component	Release
Avaya Aura® Communication Manager running on an Avaya S8300D Server	6.0.1 SP2 (R016x.00.1.510.1-18860) (System Platform 6.0.3.0.3)
Avaya G450 Media Gateway	30.14.0
Avaya Aura® Session Manager running on an Avaya S8800 Server	6.1 SP2 (Build 6.1.2.0.612004)
Avaya Aura® System Manager running on an Avaya S8800 Server	6.1 SP2 (Build 6.1.0.0.7345-6.1.5.106; SW Update Revision 6.1.6.1.1087) (System Platform 6.0.3.0.3)
Avaya 1608 IP Telephone (H.323)	Avaya one-X® Deskphone Value Edition 1.3.00B
Avaya 4621SW IP Telephone (H.323)	2.9.2
Avaya 9640 IP Telephone (H.323)	Avaya one-X® Deskphone Edition 3.1.2
Avaya 9630 IP Telephone (SIP)	Avaya one-X® Deskphone SIP Edition 2.6.4
Avaya one-X® Communicator (H.323 or SIP)	6.1 (Build 6.1.0.12-GA-30334)
Avaya 2420 Digital Telephone	n/a
Avaya 6210 Analog Telephone	n/a
Avaya Aura® Session Border Controller running on an Avaya S8800 Server	6.0.2 (Build SBCT_6.0.2.0.3) (System Platform 6.0.3.0.3)
MTS Allstream SIP Trunking Solution Components	
Component	Release
Genband S3 Session Border Controller	5.2.2.12
Nortel CS2K	CVM13

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 MTS Allstream SIP Trunking. A SIP trunk is established between Communication Manager and Session Manager for use by signaling traffic to and from MTS Allstream. It is assumed the general installation of Communication Manager, Avaya G450 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 4000 SIP trunks are available and 25 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: 4000	36		
	Maximum Concurrently Registered IP Stations: 2400	3		
	Maximum Administered Remote Office Trunks: 4000	0		
	Maximum Concurrently Registered Remote Office Stations: 2400	0		
	Maximum Concurrently Registered IP eCons: 68	0		
	Max Concur Registered Unauthenticated H.323 Stations: 100	0		
	Maximum Video Capable Stations: 2400	0		
	Maximum Video Capable IP Softphones: 2400	0		
	Maximum Administered SIP Trunks: 4000	25		
	Maximum Administered Ad-hoc Video Conferencing Ports: 4000	0		
	Maximum Number of DS1 Boards with Echo Cancellation: 80	0		
	Maximum TN2501 VAL Boards: 10	0		
	Maximum Media Gateway VAL Sources: 50	0		
	Maximum TN2602 Boards with 80 VoIP Channels: 128	0		
	Maximum TN2602 Boards with 320 VoIP Channels: 128	0		
	Maximum Number of Expanded Meet-me Conference Ports: 300	0		

5.2. System Features

Use the **change system-parameters feature** 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? n
      Trunk-to-Trunk Transfer: all
      Automatic Callback with Called Party Queuing? n
      Automatic Callback - No Answer Timeout Interval (rings): 3
      Call Park Timeout Interval (minutes): 10
      Off-Premises Tone Detect Timeout Interval (seconds): 20
      AAR/ARS Dial Tone Required? y
```

On **Page 9**, verify that a text string has been defined to replace the Calling Party Number (CPN) for restricted or unavailable calls. 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:
      International Access Code:

      ENBLOC 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 Avaya S8300D Server running Communication Manager (*procr*) and for Session Manager (*sessionMgr*). 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	
cmm	10.32.128.4	
default	0.0.0.0	
procr	10.32.128.4	
procr6	::	
sessionMgr	10.32.24.235	

5.4. Codecs

Use the **change ip-codec-set** command to define a list of codecs to use for calls between the enterprise and the service provider. For the compliance test, codecs G.729A and G.711mu were tested using ip-codec-set 2. To use these codecs, enter **G.729A** and **G.711MU** 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 2		Page 1 of 2
IP Codec Set		
Codec Set: 2		
Audio Codec	Silence Suppression	Frames Per Pkt
1: G.729A	n	2
2: G.711MU	n	2
3:		

On **Page 2**, set the **Fax Mode** to *off* since T.38 fax is not supported.

change ip-codec-set 2		Page 2 of 2
IP Codec Set		
Allow Direct-IP Multimedia? n		
FAX	Mode	Redundancy
	off	0
Modem	off	0
TDD/TTY	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 2 was chosen for the service provider trunk. Use the **change ip-network-region 2** command to configure region 2 with the following parameters:

- Set the **Authoritative Domain** field to match the SIP domain of the enterprise. In this configuration, the domain name is **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 2                                     Page 1 of 20
                                                                IP NETWORK REGION
Region: 2
Location: 1           Authoritative Domain: avaya.com
Name: SP Region
MEDIA PARAMETERS      Intra-region IP-IP Direct Audio: yes
Codec Set: 2          Inter-region IP-IP Direct Audio: yes
UDP Port Min: 2048    IP Audio Hairpinning? n
UDP Port Max: 3329
DIFFSERV/TOS PARAMETERS
Call Control PHB Value: 46
Audio PHB Value: 46
Video PHB Value: 26
802.1P/Q PARAMETERS
Call Control 802.1p Priority: 6
Audio 802.1p Priority: 6
Video 802.1p Priority: 5      AUDIO RESOURCE RESERVATION PARAMETERS
H.323 IP ENDPOINTS      RSVP Enabled? n
H.323 Link Bounce Recovery? y
Idle Traffic Interval (sec): 20
Keep-Alive Interval (sec): 5
Keep-Alive Count: 5
```

On **Page 4**, define the IP codec set to be used for traffic between region 2 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 2 will be used for calls between region 2 (the service provider region) and region 1 (the rest of the enterprise). Creating this table entry for IP network region 2 will automatically create a complementary table entry on the IP network region 1 form for destination region 2. 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 2										Page	4 of	20
Source Region: 2										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	2	y	NoLimit				n		t			
2	2									all		
3												

5.6. Signaling Group

Use the **add signaling-group** command to create a signaling group between Communication Manager and Session Manager for use by the service provider trunk. This signaling group is used for inbound and outbound calls between the service provider and the enterprise. For the compliance test, signaling group 3 was used 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 the Communication Manager and Session Manager.
- Set the **IMS Enabled** field to *n*. This specifies the Communication Manager will serve as an Evolution Server for Session Manager.
- 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 **5062**.

- Set the **Peer Detection Enabled** field to *y*. The **Peer-Server** field will initially be set to *Others* and can not 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 Avaya S8300D Server running Communication Manager as defined in **Section 5.3**.
- Set the **Far-end Node Name** to *sessionMgr*. This node name maps to the IP address of Session Manager as defined in **Section 5.3**.
- Set the **Far-end Network Region** to the IP network region defined for the service provider in **Section 5.5**.
- Set the **Far-end Domain** to 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 3                                     Page 1 of 1

                                SIGNALING GROUP

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

Near-end Node Name: procr              Far-end Node Name: sessionMgr
Near-end Listen Port: 5062             Far-end Listen Port: 5062
                                      Far-end Network Region: 2

Far-end Domain: 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? n                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 3 was configured using the parameters highlighted below.

- Set the **Group Type** field to *sip*.
- Enter a descriptive name for the **Group Name**.
- Enter an available trunk access code (TAC) that is consistent with the existing dial plan in the **TAC** field.
- Set the **Service Type** field to *public-ntwrk*.
- Set **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 3                                     Page 1 of 21
                                                    TRUNK GROUP

Group Number: 3                Group Type: sip        CDR Reports: y
  Group Name: SP Trunk          COR: 1                TN: 1        TAC: 1003
  Direction: two-way           Outgoing Display? n
  Dial Access? n                Night Service:
  Queue Length: 0
  Service Type: public-ntwrk    Auth Code? n
                                Member Assignment Method: auto
                                Signaling Group: 3
                                Number of Members: 5
```

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 **600** seconds was used.

```

add trunk-group 3
    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): 600
    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. The addition of the + sign impacted interoperability with MTS Allstream. Thus, 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 3
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**, set the **Network Call Redirection** field to *n*. Set the **Send Diversion Header** field to *y* and the **Support Request History** field to *n*. The **Send Diversion Header** and **Support Request History** fields provide additional information to the network if the call has been re-directed. 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 preferred by MTS Allstream.

```
add trunk-group 3                                     Page 4 of 21
                                                    PROTOCOL VARIATIONS
                Mark Users as Phone? n
        Prepend '+' to Calling Number? n
    Send Transferring Party Information? n
            Network Call Redirection? n
            Send Diversion Header? y
            Support Request History? n
            Telephone Event Payload Type: 101

                Convert 180 to 183 for Early Media? n
        Always Use re-INVITE for Display Updates? n
                Enable Q-SIP? n
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 one 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 40003, 40005 and 40010. 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	4			5	Total Administered: 4
5	40003	3	7325551234	10	Maximum Entries: 240
5	40005	3	7325551235	10	
5	40010	3	7325551236	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 4 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	4	3	73255	10	Total Administered: 1
					Maximum Entries: 240

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						Page 1 of 12		
DIAL PLAN ANALYSIS TABLE								
Location: all						Percent Full: 2		
Dialed String	Total Length	Call Type	Dialed String	Total Length	Call Type	Dialed String	Total Length	Call Type
1	4	dac						
4	5	ext						
8	1	fac						
9	1	fac						
*	3	fac						
#	3	fac						

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

change feature-access-codes		Page 1 of 10	
FEATURE ACCESS CODE (FAC)			
Abbreviated Dialing List1 Access Code:			
Abbreviated Dialing List2 Access Code:			
Abbreviated Dialing List3 Access Code:			
Abbreviated Dial - Prgm Group List Access Code:			
Announcement Access Code:			
Answer Back Access Code:			
Attendant Access Code:			
Auto Alternate Routing (AAR) Access Code: 8			
Auto Route Selection (ARS) - Access Code 1: 9		Access Code 2:	
Automatic Callback Activation:		Deactivation:	
Call Forwarding Activation Busy/DA: *01 All: *02		Deactivation: *03	

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 2 which contains the SIP trunk to the service provider (as defined next).

change ars analysis 0						Page	1 of	2
ARS DIGIT ANALYSIS TABLE						Percent Full: 2		
Location: all								
Dialed String	Total Min	Total Max	Route Pattern	Call Type	Node Num	ANI	Reqd	
0	1	1	2	op		n		
0	11	11	2	op		n		
00	2	2	2	op		n		
011	10	18	2	intl		n		
1800	11	11	2	fpna		n		
1877	11	11	2	fpna		n		
1908	11	11	2	fpna		n		
411	3	3	2	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 trunk route pattern in the following manner. The example below shows the values used for route pattern 2 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 3 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 2 Page 1 of 3

Pattern Number: 2 **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:	3	0	1					n	user
2:								n	user
3:								n	user
4:								n	user
5:								n	user
6:								n	user

	BCC	VALUE	TSC	CA-TSC	ITC	BCIE	Service/Feature	PARM	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

6. Configure Avaya Aura® Session Manager

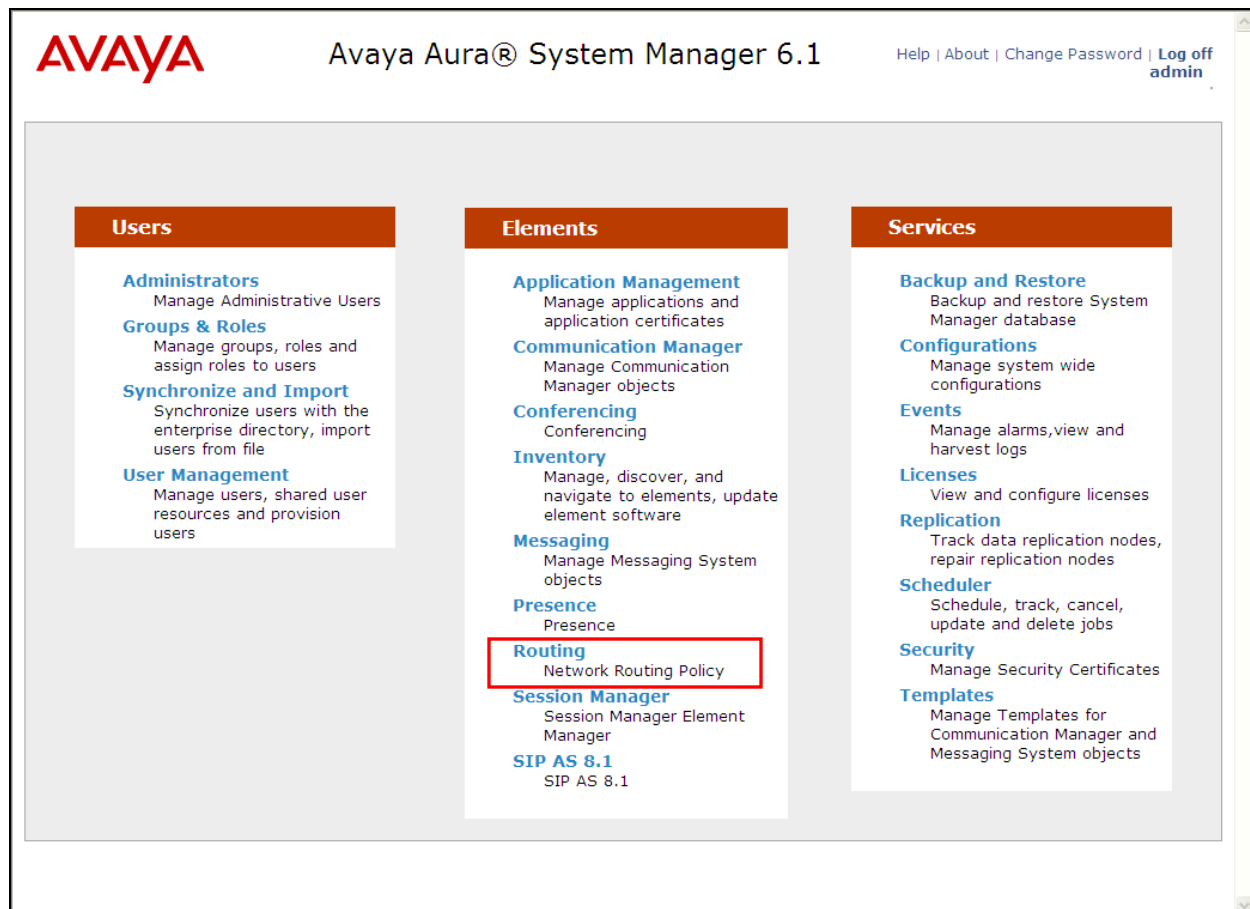
This section provides the procedures for configuring Session Manager. The procedures include configuring the following items:

- 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 Session Border Controller 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.



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 6.1 web interface. At the top left is the Avaya logo. The title bar reads 'Avaya Aura® System Manager 6.1'. On the top right, there are links for 'Help | About | Change Password | Log off admin'. Below the title bar, there are two tabs: 'Routing' (active) and 'Home'. The left-hand navigation pane shows a tree structure with 'Routing' expanded, listing sub-items: Domains, Locations, Adaptations, SIP Entities, Entity Links, Time Ranges, Routing Policies, Dial Patterns, Regular Expressions, and Defaults. The main content area has a breadcrumb trail: 'Home / Elements / Routing- Introduction to Network Routing Policy'. The page title is 'Introduction to Network Routing Policy' with a 'Help ?' link. The text explains that Network Routing Policy consists of several routing applications like 'Domains', 'Locations', 'SIP Entities', etc., and provides a recommended order for configuration:

- 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 (*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.

Domain Management

CommitCancel

1 Item | RefreshFilter: Enable

Name	Type	Default	Notes
* avaya.com	sip	<input type="checkbox"/>	Enterprise Domain

* Input Required

CommitCancel

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. For the compliance test, two locations were defined based on the two enterprise subnets shown in **Figure 1**. However, this was not required for interoperability. A single location could have been defined for the enterprise even though multiple subnets were used. The screens below show the addition of the location named **Location 1**, which includes all equipment on the **10.32.128.x** subnet including Communication Manager, and the Session Border Controller.

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).

Location Details [Commit] [Cancel]

Call Admission Control has been set to ignore SDP. All calls will be counted using the Default Audio Bandwidth.
See Session Manager -> Session Manager Administration -> Global Setting

General

* **Name:** Location 1

Notes:

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

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

Click **Commit** to save.

Location Pattern [Add] [Remove]

1 Item | Refresh Filter: Enable

<input type="checkbox"/>	IP Address Pattern	Notes
<input type="checkbox"/>	* 10.32.128.*	

Select : All, None

* Input Required [Commit] [Cancel]

Repeat the preceding procedure to create location **BR-DevConnect** which includes all equipment on the **10.32.24.x** subnet which includes the Session Manager.

Location Details

CommitCancel

Call Admission Control has been set to ignore SDP. All calls will be counted using the Default Audio Bandwidth.
See Session Manager -> Session Manager Administration -> Global Setting

General

*** Name:**

Notes:

Scrolling down to the **Location Pattern** section:

Location Pattern

AddRemove

1 Item | RefreshFilter: Enable

<input type="checkbox"/>	IP Address Pattern	Notes
<input type="checkbox"/>	* <input type="text" value="10.32.24.*"/>	<input type="text"/>

Select : All, None

*** Input Required**CommitCancel

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, one adaptation was needed. The adaptation was applied to the Communication Manager SIP entity and converts the domain part of the inbound PAI header to the enterprise domain (*avaya.com*). In addition, this adaptation maps inbound DID numbers from MTS Allstream 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*.
- **Module parameter:** Enter *osrcd=avaya.com*. This is the OverrideSourceDomain parameter. This parameter replaces the domain in the inbound PAI header with the given value. This parameter must match the value used for the **Far-end Domain** setting on the Communication Manager signaling group form in **Section 5.6**.

Adaptation Details

CommitCancel

General

* Adaptation name:sp-cm3 Adaptation

Module name:DigitConversionAdapter

Module parameter:osrcd=avaya.com

Egress URI Parameters:

Notes:

To map inbound DID numbers from MTS Allstream 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 Incoming Calls to SM

Add
Remove

0 Items | Refresh
Filter: Enable

	Matching Pattern	Min	Max	Phone Context	Delete Digits	Insert Digits	Address to modify	Notes
--	------------------	-----	-----	---------------	---------------	---------------	-------------------	-------

Digit Conversion for Outgoing Calls from SM

Add
Remove

3 Items | Refresh
Filter: Enable

	Matching Pattern ▲	Min	Max	Phone Context	Delete Digits	Insert Digits	Address to modify	Notes
<input type="checkbox"/>	* 7325551234	* 10	* 10		* 10	40003	destination ▼	
<input type="checkbox"/>	* 7325551235	* 10	* 10		* 10	40005	destination ▼	
<input type="checkbox"/>	* 7325551236	* 10	* 10		* 10	40010	destination ▼	

Select : All, None

* Input Required
Commit
Cancel

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 Session Border Controller. 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 Session Border Controller.
- **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, the Session Manager was located in location *BR-DevConnect* and the Communication Manager and Session Border Controller were located in location *Location 1*.
- **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**.

SIP Entity Details

CommitCancel

General

* Name:

devcon-asm

* FQDN or IP Address:

10.32.24.235

Type:

Session Manager

Notes:

Location:

BR-DevConnect

Outbound Proxy:

Time Zone:

America/New_York

Credential name:

SIP Link Monitoring

SIP Link Monitoring:

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 5062 defined in **Section 5.6** for use with service provider SIP traffic between Communication Manager and Session Manager was added to the list.

Port

Add

Remove

4 Items | Refresh Filter: Enable

<input type="checkbox"/>	Port	Protocol	Default Domain	Notes
<input type="checkbox"/>	5060	TCP	avaya.com	
<input type="checkbox"/>	5060	UDP	avaya.com	
<input type="checkbox"/>	5061	TLS	avaya.com	
<input type="checkbox"/>	5062	TLS	avaya.com	

Select : All, None

* Input Required

Commit

Cancel

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 the Avaya Server running 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 **Location 1** which is the location defined for the subnet where Communication Manager resides.

SIP Entity Details

CommitCancel

General

* Name:sp3-cm-2

* FQDN or IP Address:10.32.128.4

Type:CM

Notes:

Adaptation:sp-cm3 Adaptation

Location:Location 1

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 Session Border Controller. The **FQDN or IP Address** field is set to the IP address of its private network interface (see **Figure 1**). Leave the **Adaptation** field blank. The **Location** field is set to **Location 1** which is the location defined for the subnet where the Session Border Controller resides.

SIP Entity Details

CommitCancel

General

* Name:sp-sbc1

* FQDN or IP Address:10.32.128.12

Type:SIP Trunk

Notes:

Adaptation:

Location:Location 1

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 Session Border Controller. 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**.
- **Trusted:** Check this box. *Note: If this box is not checked, calls from the associated SIP Entity specified in **Section 6.5** will be denied.*

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**.

Name	SIP Entity 1	Protocol	Port	SIP Entity 2	Port	Trusted	Notes
* sp3-cm-link2	* devcon-asm	TLS	* 5062	* sp3-cm-2	* 5062	<input checked="" type="checkbox"/>	

The following screen illustrates the Entity Link to the Session Border Controller.

Entity Links

CommitCancel

1 Item | RefreshFilter: Enable

Name	SIP Entity 1	Protocol	Port	SIP Entity 2	Port	Trusted	Notes
* toAuraSBC	* devcon-asm	TCP	* 5060	* sp-sbc1	* 5060	<input checked="" type="checkbox"/>	

6.7. Add Routing Policies

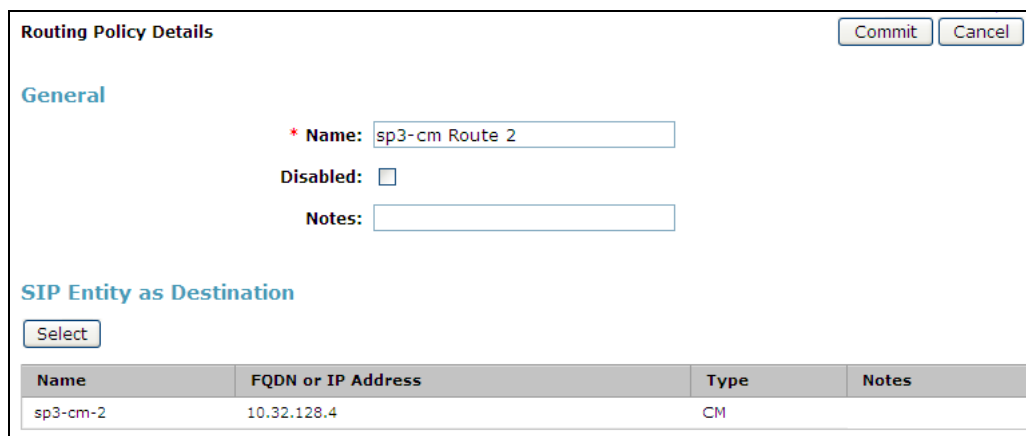
Routing policies describe the conditions under which calls will be routed to the SIP Entities specified in **Section 6.5**. Two routing policies must be added: one for Communication Manager and one for the Session Border Controller. To add a routing policy, navigate to **Routing → Routing Policies** 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).

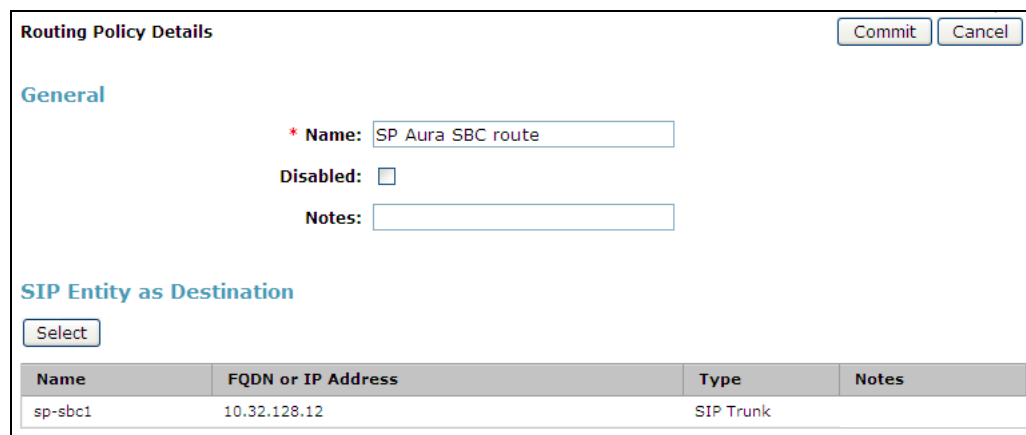
In the **SIP Entity as Destination** section, click **Select**. The **SIP Entity List** page opens (not shown). Select the appropriate SIP entity to which this routing policy applies and click **Select**. The selected SIP Entity displays on the Routing Policy Details page as shown below. Use default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

The following screens show the Routing Policies for Communication Manager and the Session Border Controller.



The screenshot shows the 'Routing Policy Details' form for a Communication Manager (CM) routing policy. The 'General' section has 'Name' set to 'sp3-cm Route 2', 'Disabled' is unchecked, and 'Notes' is empty. The 'SIP Entity as Destination' section has a 'Select' button. Below is a table with one row showing the selected entity 'sp3-cm-2' with FQDN '10.32.128.4' and Type 'CM'.

Name	FQDN or IP Address	Type	Notes
sp3-cm-2	10.32.128.4	CM	



The screenshot shows the 'Routing Policy Details' form for a Session Border Controller (SBC) routing policy. The 'General' section has 'Name' set to 'SP Aura SBC route', 'Disabled' is unchecked, and 'Notes' is empty. The 'SIP Entity as Destination' section has a 'Select' button. Below is a table with one row showing the selected entity 'sp-sbc1' with FQDN '10.32.128.12' and Type 'SIP Trunk'.

Name	FQDN or IP Address	Type	Notes
sp-sbc1	10.32.128.12	SIP Trunk	

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 MTS Allstream 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 11 digit numbers that begin with a 1 and have a destination domain of *avaya.com* from **Location 1** uses route policy *SP Aura SBC route*.

Dial Pattern Details
Commit
Cancel

General

* Pattern: 1

* Min: 11

* Max: 11

Emergency Call: ☐

SIP Domain: avaya.com

Notes: Dest: sp-sbc

Originating Locations and Routing Policies

Add Remove

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"/>	Location 1	SP Subnet(s)	SP Aura SBC route	0	<input type="checkbox"/>	sp-sbc1	

Select : All, None

The second example shows that 11 digit numbers that start with **732555** to domain **avaya.com** and originating from **Location 1** uses route policy **sp3-cm Route 2**. These are the DID numbers assigned to the enterprise from MTS Allstream. Location 1 is selected because these calls come from the Session Border Controller which resides in Location 1.

Dial Pattern Details
Commit Cancel

General

* **Pattern:**

* **Min:**

* **Max:**

Emergency Call: ☐

SIP Domain:

Notes:

Originating Locations and Routing Policies

Add Remove

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"/>	Location 1	SP Subnet(s)	sp3-cm Route 2	0	<input type="checkbox"/>	sp3-cm-2	

Select : All, None

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

Dial Patterns

Edit New Duplicate Delete More Actions ▼ Commit

8 Items | Refresh
Filter: Enable

<input type="checkbox"/>	Pattern	Min	Max	Emergency Call	SIP Domain	Notes
<input type="checkbox"/>	<u>0</u>	1	11	<input type="checkbox"/>	avaya.com	Dest: sp-sbc1
<input type="checkbox"/>	<u>011</u>	10	18	<input type="checkbox"/>	avaya.com	Dest: sp-sbc1
<input type="checkbox"/>	<u>1</u>	11	11	<input type="checkbox"/>	avaya.com	Dest: sp-sbc1
<input type="checkbox"/>	<u>411</u>	3	3	<input type="checkbox"/>	avaya.com	Dest: sp-sbc1
<input type="checkbox"/>	<u>732555</u>	10	10	<input type="checkbox"/>	avaya.com	Dest: sp3-cm-2

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 IP address of the Session Manager management interface.

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

View Session Manager

Return

General | Security Module | NIC Bonding | Monitoring | CDR | Personal Profile Manager (PPM) - Connection Settings | Event Server |
Expand All | Collapse All

General ▾

SIP Entity Name

devcon-asm

Description

Management Access Point Host Name/IP

10.32.24.233

Direct Routing to Endpoints

Enable

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.

Security Module ▼

SIP Entity IP Address	10.32.24.235
Network Mask	255.255.255.0
Default Gateway	10.32.24.1
Call Control PHB	46
QOS Priority	6
Speed & Duplex	Auto
VLAN ID	

7. Configure Avaya Aura® Session Border Controller

This section describes the configuration of the Avaya Aura® Session Border Controller. This configuration is done in two parts. The first part is done during the Session Border Controller installation via the installation wizard. These Application Notes will not cover the Session Border Controller installation in its entirety but will include the use of the installation wizard. For information on installing the Avaya Aura® System Platform and the loading of the Session Border Controller template see [1] and [5].

The second part of the configuration is done after the installation is complete using the Session Border Controller web interface. The resulting Session Border Controller configuration file is shown in **Appendix A**.

7.1. Installation Wizard

During the installation of the Session Border Controller template, the installation wizard will prompt the installer for information that will be used to create the initial configuration of the Session Border Controller.

7.1.1. Network Settings

The first screen of the installation wizard is the **Network Settings** screen. Fill in the fields as described below and shown in the following screen:

- **IP Address:** Enter the IP address of the private side of the Session Border Controller.
- **Hostname:** Enter the host name of the Session Border Controller.
- **Domain:** Enter the domain of the host name provided.
- **Default Domain:** Enter the domain of the host name provided.

Click the **Apply to all VMs** button. Click **Next Step** to continue.

The screenshot shows the Avaya Network Settings installation wizard. The left sidebar contains a navigation menu with 'Configuration' expanded and 'Installation' selected. Under 'Installation', 'Network Settings' is marked with a red 'X', indicating it is the current step. Other steps include 'Logins', 'VPN Access', 'SBC', 'Summary', and 'Finish'. The main content area is titled 'Network Settings' and 'Enter network settings'. It contains several input fields for network configuration: Domain-0 IP Address (10.32.128.10), CDom IP Address (10.32.128.11), Gateway IP Address (10.32.128.254), Network Mask (255.255.255.0), Primary DNS (10.32.24.150), Secondary DNS (Optional), Default Search List (Optional), and HTTPS Proxy (Optional) [IP Address:Port Number]. Below these fields is a table for Virtual Machine settings:

Virtual Machine	IP Address	Hostname	Domain	
SBC	10.32.128.12	sp-sbc1	avaya.com	(Optional)

Below the table, there is a 'Default Domain' field set to 'avaya.com' (Optional) and an 'Apply to all VMs' button. At the bottom right, there is a 'Next Step' link with a red arrow.

7.1.2. Service Logins

Optionally, logins can be created for the following login names *craft*, *init*, and *dadmin*. To create the login, simply enter and re-enter a password for the login to be created in the screen below. The creation of a service login was not required for the compliance test. Click **Next Step** to continue.

Logins

Services logins for SBC (optional)

Login name	Password	Re-type password
craft	<input type="text"/>	<input type="text"/>
init	<input type="text"/>	<input type="text"/>
dadmin	<input type="text"/>	<input type="text"/>

[◀ Previous Step](#)[Next Step ▶](#)

7.1.3. VPN Access

VPN remote access to the Session Border Controller was not part of the compliance test. Thus, on the VPN Access screen, select **No** to the question, **Would you like to configure the VPN remote access parameters for System Platform?** Click **Next Step** to continue.

VPN Access

Configure VPN Access

Would you like to configure the VPN remote access parameters for System Platform?

☐ Yes ☒ No

VPN Access Configuration

VPN Router IP Address	<input type="text"/>	(Optional)
Remote Access Network	<input type="text"/>	
Remote Access Network Subnet Mask	<input type="text"/>	

The data on this page is used to configure static routes on System Platform to enable remote VPN access to the component applications and the Avaya Aura™ System Platform Web Console.

Once the template has been installed, the user must access the Avaya Aura™ System Platform Web Console and check the "Server Management -> Static Route Configuration" page to verify that the static routes configured by the Wizard are suitable for the intended remote access application.

If in doubt, please refer to the documentation.

[◀ Previous Step](#)[Next Step ▶](#)

7.1.4. SBC

On the **SBC** screen, fill in the fields as described below and shown in the following screen:

In the **SIP Service Provider Data** section:

- **Service Provider:** From the pull-down menu, select the name of the service provider to which the Session Border Controller will connect. This will allow the wizard to create a configuration file customized for this service provider. At the time of the compliance test, a customized configuration file did not exist for MTS Allstream. Thus, **Generic** was chosen instead. Further customization can be done manually after the wizard is complete.
- **Port:** Enter the port number that the service provider uses to listen for SIP traffic.
- **IP Address1:** Enter the IP address of the SIP proxy of the service provider.
- **Signalling/Media Network1:** Enter the network address of the network where signaling and media traffic will originate from the service provider.
- **Signalling/Media Netmask1:** Enter the netmask corresponding to the **Signalling/Media Network** defined above.

Default values may be used for all other fields. Scroll down to continue.

SBC
Session Border Controller Data

SIP Service Provider Data			
Service Provider	Port		
Generic	5060		
IP Address1	Signalling/Media Network1	Signalling/Media Netmask1	
10.2.2.12	10.2.2.0	255.255.255.0	
IP Address2 (Optional)	Signalling/Media Network2 (Optional)	Signalling/Media Netmask2 (Optional)	Hunting (Optional)

Further down on the same **SBC** screen, fill in the fields as described below:

In the **SBC Network Data** section:

- **Public IP Address:** Enter the IP address of the public side of the Session Border Controller.
- **Public Net Mask:** Enter the netmask associated with the public network to which the Session Border Controller connects.
- **Public Gateway:** Enter the default gateway of the public network.

SBC Network Data			
Interface	IP Address	Net Mask	Gateway
Private (Management)	10.32.128.12	255.255.255.0	10.32.128.254
Public	<input type="text" value="10.3.9.191"/>	<input type="text" value="255.255.255.128"/>	<input type="text" value="10.3.9.129"/>

In the **Enterprise SIP Server** section:

- **SIP Domain** Enter the enterprise SIP domain.
- **IP Address1:** Enter the IP address of the Enterprise SIP Server to which the Session Border Controller will connect. In the case of the compliance test, this is the IP address of Session Manager.
- **Transport1:** From the pull-down menu, select the transport protocol to be used for SIP traffic between the Session Border Controller and Session Manager.

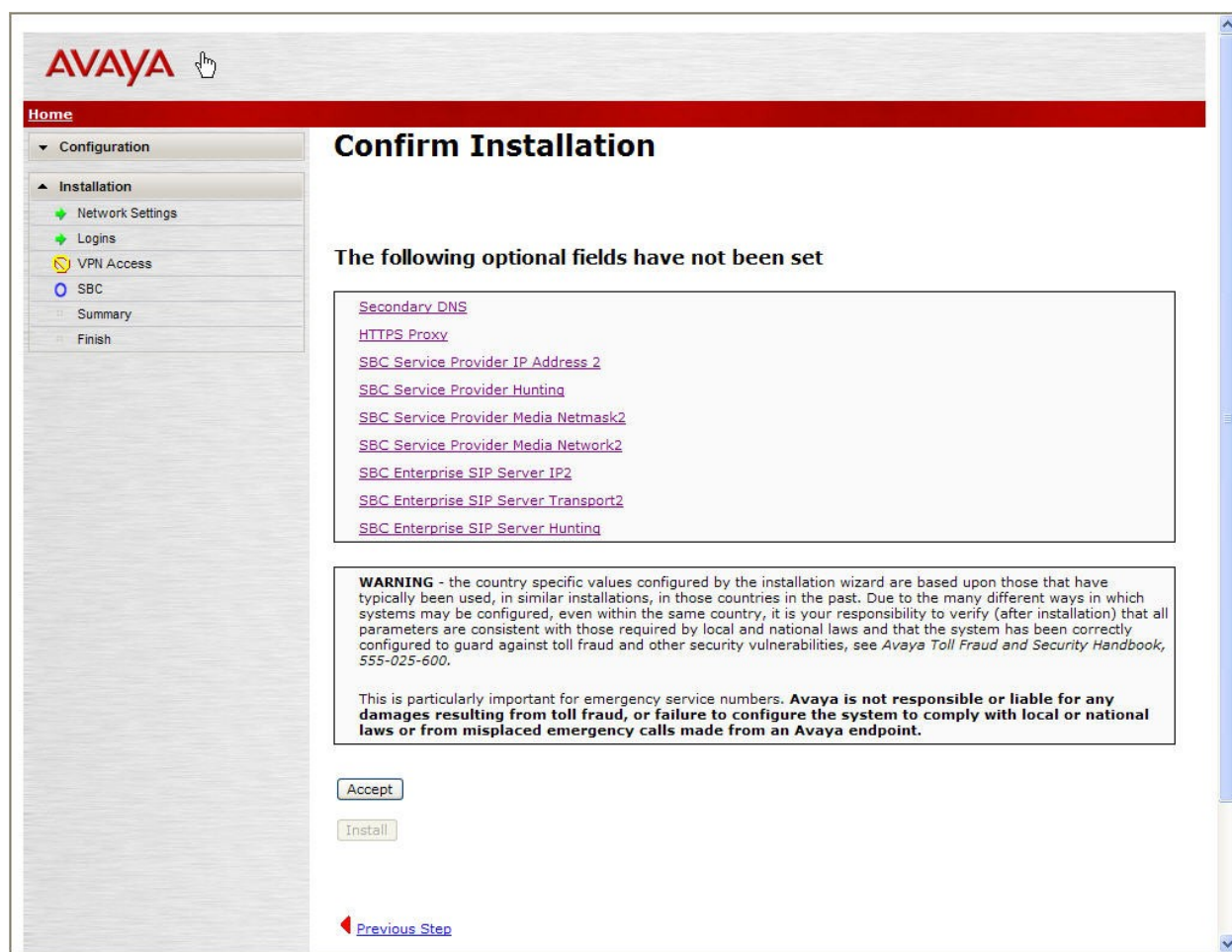
Default values may be used for all other fields. Click **Next Step** to continue. A summary screen will be displayed (not shown). Check the displayed values and click **Next Step** again to continue to the final step.

Enterprise SIP Server			
SIP Domain <input type="text" value="avaya.com"/>			
IP Address1 <input type="text" value="10.32.24.235"/>		Transport1 <input type="text" value="TCP"/>	
IP Address2 (Optional) <input type="text"/>	Transport2 (Optional) <input type="text"/>	Hunting (Optional) <input type="text"/>	

[Previous Step](#) [Next Step](#)

7.1.5. Confirm Installation

The **Confirm Installation** screen will indicate if any required or optional fields have not been set. All required fields should be set. If not, click **Previous Step** to navigate to the necessary screen to set the required field. Otherwise, click **Accept**. This will change the state of the **Install** button on this same page so that it is no longer grayed-out. Click **Install** to finish the wizard.



7.2. Post Installation Configuration

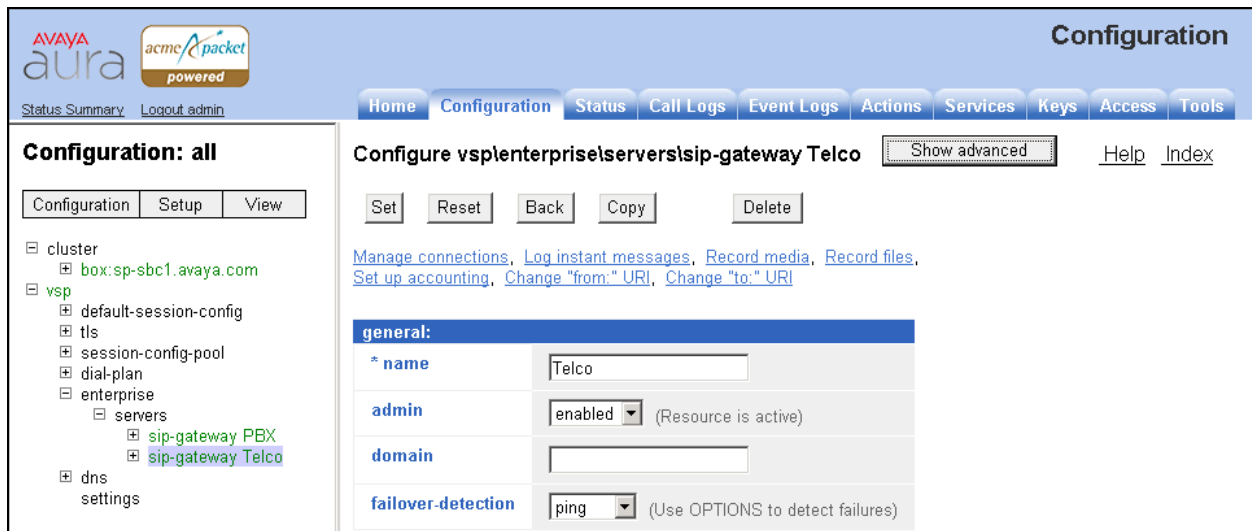
Once the installation wizard is complete, additional changes may be performed by accessing the browser-based GUI of the Session Border Controller, using the URL **https://<ip-address>**, where **<ip-address>** is the private IP address configured in **Section 6.1**. Log in with the appropriate credentials.



The image shows a login screen for the Acme Packet Net-Net OS-E. The title is "Acme Packet Net-Net OS-E". Below the title, a message states: "To access the NNOS-E management interface, you must first log in. Please provide your user name and password." There are two input fields: "Username:" and "Password:". Below these fields is a "Login" button.

7.2.1. Options Frequency

To set the frequency of the OPTIONS messages sent from the Session Border Controller to the service provider, first navigate to **vsp → enterprise → servers → sip-gateway Telco**. Click **Show Advanced**.



The image shows the Avaya Aura Configuration page. The top navigation bar includes "Home", "Configuration", "Status", "Call Logs", "Event Logs", "Actions", "Services", "Keys", "Access", and "Tools". The left sidebar shows a tree view of the configuration hierarchy: "cluster" (box: sp-sbc1.avaya.com), "vsp" (default-session-config, tls, session-config-pool, dial-plan), "enterprise" (servers: sip-gateway PBX, sip-gateway Telco), "dns", and "settings". The main content area is titled "Configure vspenterprise\servers\sip-gateway Telco". It includes a "Show advanced" button and links for "Manage connections", "Log instant messages", "Record media", "Record files", "Set up accounting", "Change 'from:' URI", and "Change 'to:' URI". Below this is a "general:" section with the following fields: "name" (Telco), "admin" (enabled), "domain" (empty), and "failover-detection" (ping). The "admin" field has a note "(Resource is active)". The "failover-detection" field has a note "(Use OPTIONS to detect failures)".

Scroll down to the **routing** section of the form. Enter the desired interval in the **ping-interval** field. Click **Set** at the top of the form (shown in previous figure).

The screenshot shows the AVAYA aura Configuration page. The top navigation bar includes links for Home, Configuration, Status, Call Logs, Event Logs, Actions, Services, Keys, Access, and Tools. The left sidebar shows a tree view of configuration options under 'Configuration: all', including cluster, vsp, default-session-config, tls, session-config-pool, dial-plan, enterprise, servers, sip-gateway PBX, sip-gateway Telco, dns, and settings. The main content area displays the 'routing' configuration form. The 'routing-setting' dropdown is set to 'normalization'. Below it are 'Select All' and 'Unselect All' buttons. The 'domain-alias' and 'domain-subnet' fields have links to 'Edit domain-alias' and 'Edit domain-subnet' respectively. The 'loop-detection' dropdown is set to 'tight' with a tooltip that reads '(Compare source and destination address/port/transport)'. The 'service-type' dropdown is set to 'provider' with a tooltip that reads '(Provider peer)'. The 'ping-interval' field is set to '60' seconds.

7.2.2. Save the Configuration

To save the configuration, begin by clicking on **Configuration** in the left pane to display the configuration menu. Next, select **Update and save configuration**.

The screenshot shows the AVAYA aura Configuration page with the 'Configuration' menu open. The menu options are: 'Update and save configuration' (highlighted), 'Reload configuration', 'Validate configuration', 'Analyze configuration', 'Search configuration', 'Save as XML', and 'Load from XML'. A tooltip for 'Update and save configuration' reads 'Update and save the current configuration.'. The left sidebar shows the same tree view of configuration options as in the previous screenshot.

8. MTS Allstream SIP Trunking Configuration

To use MTS Allstream SIP Trunking, a customer must request the service from MTS Allstream using their sales processes. The process can be started by contacting MTS Allstream via the corporate web site at www.allstream.com and requesting information via the online sales links or telephone numbers.

During the signup process, MTS Allstream will require that the customer provide the public IP address used to reach the Session Border Controller at the edge of the enterprise. MTS Allstream will provide the IP address of the MTS Allstream SIP proxy/Session Border Controller, IP addresses 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 Session Border Controller configuration discussed in the previous sections.

The configuration between MTS Allstream and the enterprise is a static configuration. There is no registration of the SIP trunk or enterprise users to the MTS Allstream 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> - Traces 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 Aura® Session Border Controller to MTS Allstream SIP Trunking. MTS Allstream SIP Trunking is a SIP-based Voice over IP solution for customers ranging from small businesses to large enterprises. MTS Allstream SIP Trunking provides businesses a flexible, cost-saving alternative to traditional hardwired telephony trunks. MTS Allstream SIP Trunking passed compliance testing. 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 6.0.3, February 2011.
- [2] *Administering Avaya Aura® System Platform*, Release 6.0.3, February 2011.
- [3] *Administering Avaya Aura® Communication Manager*, June 2010, Document Number 03-300509.
- [4] *Avaya Aura® Communication Manager Feature Description and Implementation*, June 2010, Document Number 555-245-205.
- [5] *Installing and Upgrading Avaya Aura® System Manager*, Release 6.0, June 2010.
- [6] *Administering Avaya Aura® System Manager*, Release 6.1, November 2010.
- [7] *Installing and Configuring Avaya Aura® Session Manager*, Release 6.1, April 2011, Document Number 03-603473.
- [8] *Administering Avaya Aura® Session Manager*, Release 6.1, May 2011, Document Number 03-603324.
- [9] *Avaya 1600 Series IP Deskphones Administrator Guide Release 1.3.x*, May 2010, Document Number 16-601443.
- [10] *4600 Series IP Telephone LAN Administrator Guide*, October 2007, Document Number 555-233-507.
- [11] *Avaya one-X® Deskphone Edition for 9600 Series IP Telephones Administrator Guide*, November 2009, Document Number 16-300698.
- [12] *Avaya one-X® Deskphone Edition SIP for 9600 Series IP Telephones Administrator Guide*, Release 2.6, June 2010, 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/>

12. Appendix A: Avaya Aura® Session Border Controller Configuration File

```
#
# Copyright (c) 2004-2011 Acme Packet Inc.
# All Rights Reserved.
#
# File: /cxc/cxc.cfg
# Date: 12:31:20 Tue 2011-08-09
#
config cluster
config box 1
  set hostname sp-sbcl.avaya.com
  set timezone America/New_York
  set name sp-sbcl.avaya.com
  set identifier 00:ca:fe:23:00:00
config interface eth0
  config ip inside
    set ip-address static 10.32.128.12/24
  config ssh
  return
  config snmp
    set trap-target 10.32.128.11 162
    set trap-filter generic
    set trap-filter dos
    set trap-filter sip
    set trap-filter system
  return
  config web
  return
  config web-service
    set protocol https 8443
    set authentication certificate "vsp\tls\certificate ws-cert"
  return
  config sip
    set udp-port 5060 "" "" any 0
    set tcp-port 5060 "" "" any 0
    set tls-port 5061 "" "" TLS 0 "vsp\tls\certificate aasbc.p12"
  return
  config icmp
  return
  config media-ports
  return
  config routing
    config route Default
      set gateway 10.32.128.254
    return
    config route Static0
      set destination network 192.11.13.4/30
      set gateway 10.32.128.10
    return
    config route Static1
      set admin disabled
    return
```

```

    config route Static2
        set admin disabled
    return
    config route Static3
        set admin disabled
    return
    config route Static4
        set admin disabled
    return
    config route Static5
        set admin disabled
    return
    config route Static6
        set admin disabled
    return
    config route Static7
        set admin disabled
    return
    return
    return
return
config interface eth2
    config ip outside
        set ip-address static 10.3.9.191/25
    config sip
        set udp-port 5060 "" "" any 0
    return
    config media-ports
    return
    config routing
        config route Default
            set admin disabled
        return
        config route external-sip-media-1
            set destination network 10.2.2.0/24
            set gateway 10.3.9.129
        return
    return
    config kernel-filter
        config allow-rule allow-sip-udp-from-peer-1
            set destination-port 5060
            set source-address/mask 10.2.2.0/24
            set protocol udp
        return
        config deny-rule deny-all-sip
            set destination-port 5060
        return
    return
    return
return
config cli
    set prompt sp-sbc1.avaya.com
    return
return
return

```

```

config services
  config event-log
    config file access
      set filter access info
      set count 3
    return
  config file system
    set filter system info
    set count 3
  return
  config file errorlog
    set filter all error
    set count 3
  return
  config file db
    set filter db debug
    set filter dosDatabase info
    set count 3
  return
  config file management
    set filter management info
    set count 3
  return
  config file peer
    set filter sipSvr info
    set count 3
  return
  config file dos
    set filter dos alert
    set filter dosSip alert
    set filter dosTransport alert
    set filter dosUrl alert
    set count 3
  return
  config file krnlsys
    set filter krnlsys debug
    set count 3
  return
return

config master-services
  config database
    set media enabled
  return
return

config vsp
  set admin enabled
  config default-session-config
    config media
      set anchor enabled
      set rtp-stats enabled
    return
  config sip-directive
    set directive allow

```

```

return
config log-alert
    set apply-to-methods-for-filtered-logs
return
config third-party-call-control
    set handle-refer-locally disabled
return
return
config tls
    config default-ca
        set ca-file /cxc/certs/sipca.pem
    return
    config certificate ws-cert
        set certificate-file /cxc/certs/ws.cert
    return
    config certificate aasbc.p12
        set certificate-file /cxc/certs/aasbc.p12
        set passphrase-tag aasbc-cert-tag
    return
return
config session-config-pool
    config entry ToTelco
        config to-uri-specification
            set host next-hop
        return
        config from-uri-specification
            set host local-ip
        return
        config request-uri-specification
            set host next-hop
        return
        config p-asserted-identity-uri-specification
            set host local-ip
        return
    return
    config entry ToPBX
        config to-uri-specification
            set host next-hop-domain
        return
        config request-uri-specification
            set host next-hop-domain
        return
    return
    config entry Discard
        config sip-directive
        return
    return
return
config dial-plan
    config route Default
        set priority 500
        set location-match-preferred exclusive
        set session-config vsp\session-config-pool\entry Discard
    return
    config source-route FromTelco
        set peer server "vsp\enterprise\servers\sip-gateway PBX"

```

```

    set source-match server "vsp\enterprise\servers\sip-gateway Telco"
    return
    config source-route FromPBX
    set peer server "vsp\enterprise\servers\sip-gateway Telco"
    set source-match server "vsp\enterprise\servers\sip-gateway PBX"
    return
    return
    config enterprise
    config servers
    config sip-gateway PBX
    set domain avaya.com
    set failover-detection ping
    set outbound-session-config-pool-entry vsp\session-config-pool\entry
ToPBX
    config server-pool
    config server PBX1
    set host 10.32.24.235
    set transport TCP
    return
    return
    return
    config sip-gateway Telco
    set peer-identity ""
    set failover-detection ping
    set ping-interval 60
    set outbound-session-config-pool-entry vsp\session-config-pool\entry
ToTelco
    config server-pool
    config server Telco1
    set host 10.2.2.12
    return
    return
    return
    return
    return
    config dns
    config resolver
    config server 10.32.24.150
    return
    return
    return
    config settings
    set read-header-max 8191
    return
    return
    config external-services
    return

    config preferences
    config gui-preferences
    return
    return

    config access
    config permissions superuser

```



```
    set cli advanced
return
config permissions read-only
    set config view
    set actions disabled
return
config users
    config user admin
        set password 0x001b5a94dfdalc0e001018107e3517d4b24b514cb7e0a2a0f11f3dd23e
        set permissions access\permissions superuser
    return
    config user cust
        set password 0x006374a67de611279d7900d9d973cbe5c5466a3049615a0a250063e4d7
        set permissions access\permissions read-only
    return
return
return

config features
return
```

©2011 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.