



# **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 Acme Packet 3800 Net-Net 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, Acme Packet 3800 Net-Net 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, Acme Packet 3800 Net-Net 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 Acme Packet 3800 Net-Net 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 Acme Packet 3800 Net-Net SBC.
- 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.
- **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 than 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 one-X® Communicator 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. There is currently no workaround for this problem other than to use the H.323 version of Communicator. This same problem may also occur with the Avaya 9600 Series SIP Telephone unless using phone firmware 2.6.5 or later and the **DTMF\_PAYLOAD** value is set to the DTMF payload header used by MTS Allstream (**101**) in the phone configuration file (46xxsettings.txt).
- **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](mailto: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.

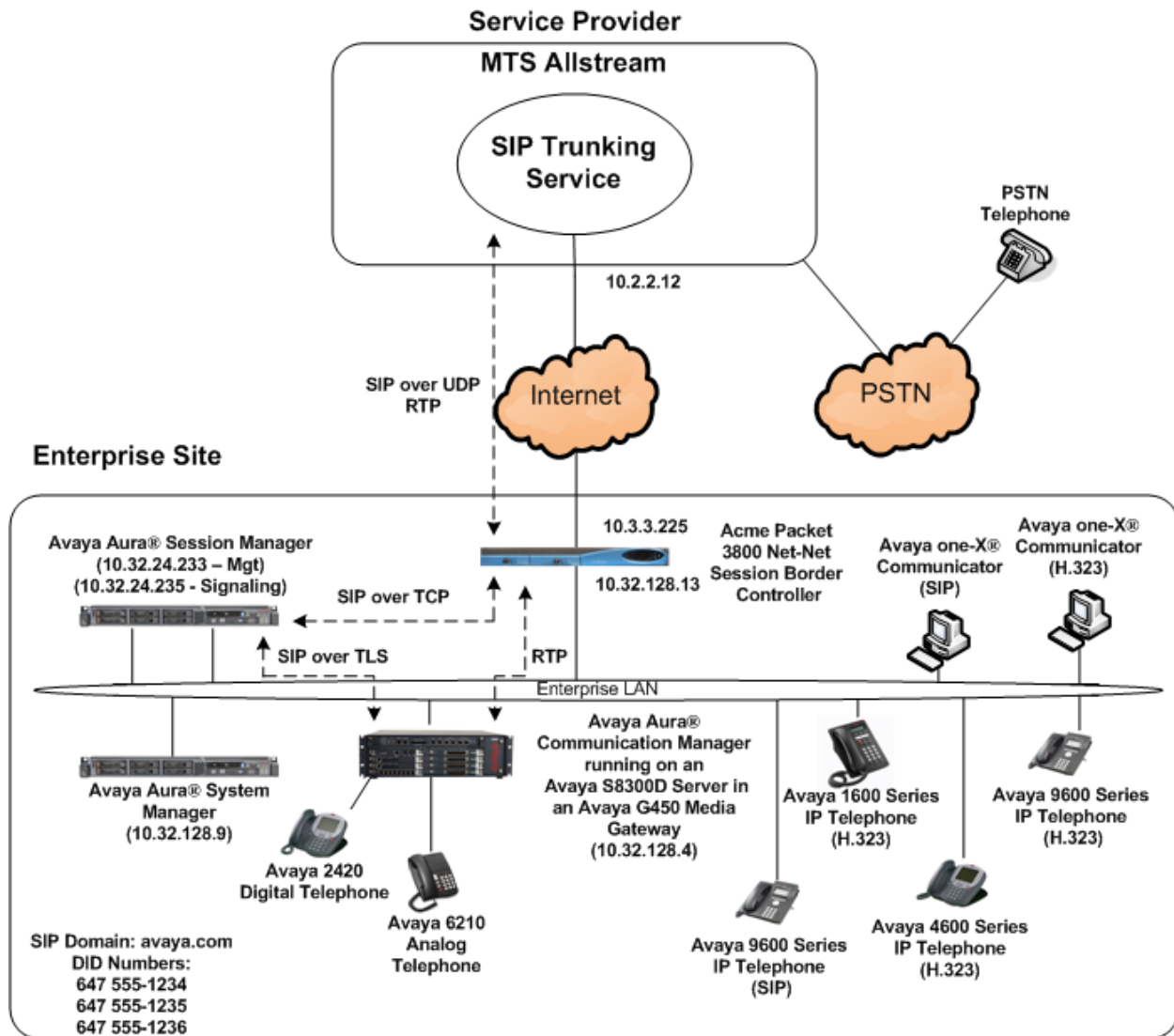
### 3. Reference Configuration

**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 Acme Packet 3800 Net-Net SBC (SBC). The SBC 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 SBC. In this way, the SBC can protect the enterprise against any SIP-based attacks. The SBC 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.



**Figure 1: Avaya IP Telephony Network using MTS Allstream SIP Trunking**

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 Acme Packet 3800 Net-Net SBC then to Session Manager. Session Manager uses the configured dial patterns (or regular expressions) and routing policies to determine the recipient (in this case the 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 Acme Packet 3800 Net-Net SBC. From the Acme Packet 3800 Net-Net SBC, 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 2.6.5
Avaya one-X® Communicator (H.323 or SIP)	6.1 SP1 (Build 6.1.1.02)
Avaya 2420 Digital Telephone	n/a
Avaya 6210 Analog Telephone	n/a
Acme Packet 3800 Net-Net Session Border Controller	SCX6.2.0 MR-3 GA (Build 619)
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.

<b>display system-parameters customer-options</b>		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
<b>Maximum Administered SIP Trunks:</b>	<b>4000</b>	<b>25</b>
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 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? 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		
<b>Name</b>	<b>IP Address</b>	
cmm	10.32.128.4	
default	0.0.0.0	
<b>procr</b>	<b>10.32.128.4</b>	
procr6	::	
<b>sessionMgr</b>	<b>10.32.24.235</b>	

### 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		
<b>Audio Codec</b>	<b>Silence Suppression</b>	<b>Frames Per Pkt</b>
1: <b>G.729A</b>	n	2
2: <b>G.711MU</b>	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		
<b>FAX</b>	<b>Mode</b>	<b>Redundancy</b>
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 3 was chosen for the service provider trunk. Use the **change ip-network-region 3** command to configure region 3 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 3                                     Page 1 of 20
                                                                IP NETWORK REGION
Region: 3
Location: 1           Authoritative Domain: avaya.com
Name: SP Region
MEDIA PARAMETERS                      Intra-region IP-IP Direct Audio: yes
Codec Set: 3                      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                      AUDIO RESOURCE RESERVATION PARAMETERS
H.323 Link Bounce Recovery? y                      RSVP Enabled? n
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 3 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 3 will be used for calls between region 3 (the service provider region) and region 1 (the rest of the enterprise). Creating this table entry for IP network region 3 will automatically create a complementary table entry on the IP network region 1 form for destination region 3. 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 3									
Source Region: 3      Inter Network Region Connection Management									
<b>dst</b>	<b>codec</b>	direct	WAN-BW-limits	Video	Intervening	Dyn	A	G	M
<b>rgn</b>	<b>set</b>	WAN	Units	Total Norm	Prio Shr Regions	CAC	R	L	t
1	3	y	NoLimit				n		c
2									e
3	3							all	t

## 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: 3

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                                     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): 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                                     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**, 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	
<b>Network Call Redirection? n</b>	
<b>Send Diversion Header? y</b>	
<b>Support Request History? n</b>	
<b>Telephone Event Payload Type: 101</b>	
Convert 180 to 183 for Early Media? n	
Always Use re-INVITE for Display Updates? n	
Identity for Calling Party Display: P-Asserted-Identity	
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 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	6475551234	10	Maximum Entries: 240
5	40005	3	6475551235	10	
5	40010	3	6475551236	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	64755	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		
<b>Dialed</b>	<b>Total</b>	<b>Call</b>	<b>Dialed</b>	<b>Total</b>	<b>Call</b>	<b>Dialed</b>	<b>Total</b>	<b>Call</b>
<b>String</b>	<b>Length</b>	<b>Type</b>	<b>String</b>	<b>Length</b>	<b>Type</b>	<b>String</b>	<b>Length</b>	<b>Type</b>
1	4	dac						
4	5	ext						
8	1	fac						
<b>9</b>	<b>1</b>	<b>fac</b>						
*	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							
Location: all						Percent Full: 2	
	Dialed	Total		Route	Call	Node	ANI
	String	Min	Max	Pattern	Type	Num	Reqd
0		1	1	2	op		n
0		11	11	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			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

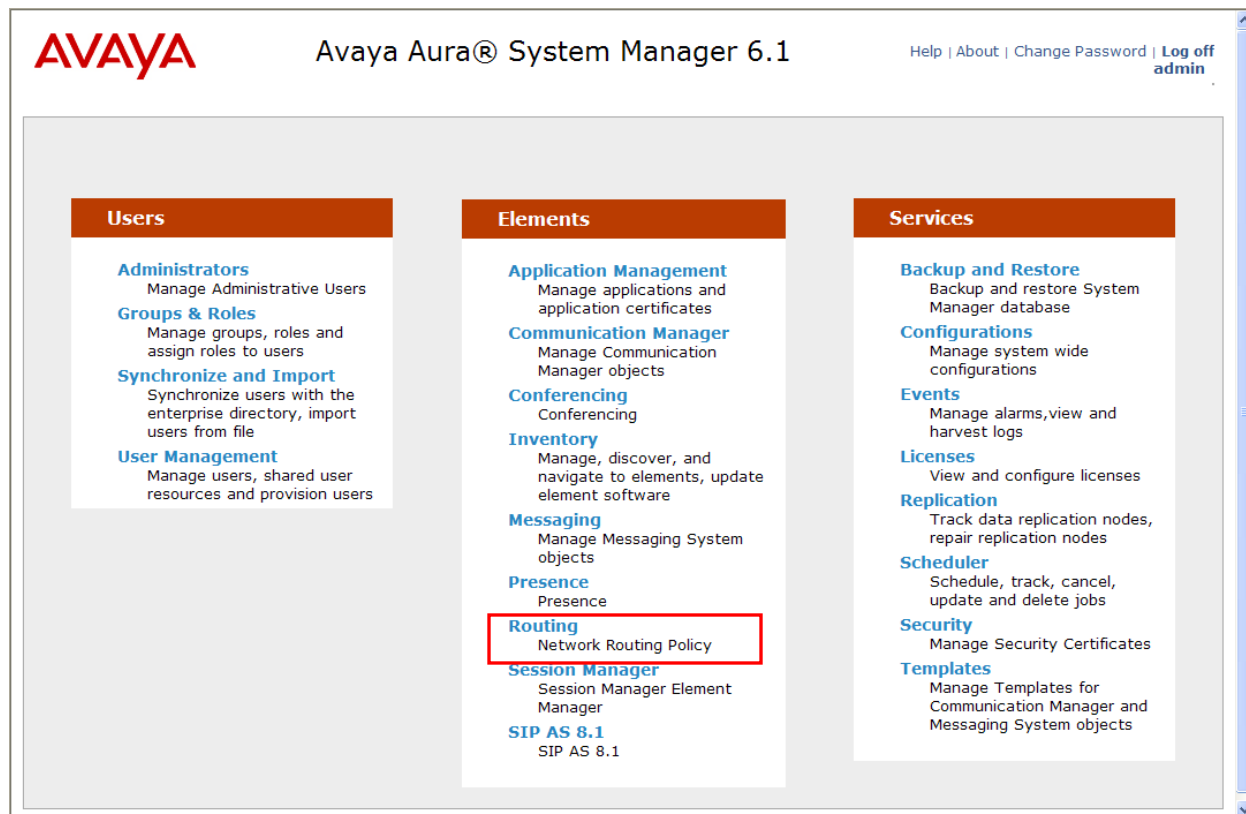
This section provides the procedures for configuring Session Manager. The procedures include configuring the following items:

- 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 SBC 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

Commit

Cancel

1 Item | [Refresh](#)

Filter: [Enable](#)

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

\* Input Required

Commit

Cancel



### 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 **Location 1**, which includes all equipment on the enterprise including Communication Manager, Session Manager and the Acme Packet 3800 Net-Net SBC.

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**

CommitCancel

**General**

\* Name: Location 1

Notes: SP Subnet(s)

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**

AddRemove

2 Items | RefreshFilter: Enable

<input type="checkbox"/>	IP Address Pattern	Notes
<input type="checkbox"/>	* 10.32.24.235	SM 6.1 (devcon-asm)
<input type="checkbox"/>	* 10.32.128.*	

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, two adaptations were needed. The first 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. The second adaptation is applied to the Acme Packet 3800 Net-Net SBC SIP entity and converts the domain part of the outbound Request URI header from Session Manager containing the enterprise domain to the MTS Allstream SIP proxy IP address.

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**.

The screenshot shows a web-based configuration interface for creating a new adaptation. The dialog is titled 'Adaptation Details' and has 'Commit' and 'Cancel' buttons in the top right. The 'General' section is active, showing several input fields: 'Adaptation name' with the value 'sp-cm3 Adaptation', 'Module name' with a dropdown menu showing 'DigitConversionAdapter', 'Module parameter' with the value 'osrcd=avaya.com', 'Egress URI Parameters' (empty), and 'Notes' (empty).

Adaptation Details	
<b>General</b>	
* 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"/>	* 6475551234	* 10	* 10		* 10	40003	destination ▼	
<input type="checkbox"/>	* 6475551235	* 10	* 10		* 10	40005	destination ▼	
<input type="checkbox"/>	* 6475551236	* 10	* 10		* 10	40010	destination ▼	

Select : All, None

\* Input Required
Commit
Cancel

To create the adaptation that will be applied to the Acme Packet 3800 Net-Net SBC SIP entity, navigate to **Routing → Adaptations** 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.

- **Adaptation name:** Enter a descriptive name for the adaptation.
- **Module name:** Enter **DigitConversionAdapter**.
- **Module parameter:** Enter **odstd=10.2.2.12**. This is the OverrideDestinationDomain parameter. This parameter replaces the domain in the Request URI header with the given value for outbound only.
- **Notes:** Add a brief description (optional).

Click **Commit** to save.

The screenshot shows a dialog box titled "Adaptation Details" with "Commit" and "Cancel" buttons in the top right. The "General" section is active, showing the following fields:

- \* Adaptation name:** A text field containing "Acme Adaptation".
- Module name:** A dropdown menu showing "DigitConversionAdapter".
- Module parameter:** A text field containing "odstd=10.2.2.12".
- Egress URI Parameters:** An empty text field.
- Notes:** A text field containing "Change RURI to Dest IP".

## 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 Acme Packet 3800 Net-Net SBC. 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 Acme Packet 3800 Net-Net SBC.
- **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 **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**.

The screenshot displays the 'SIP Entity Details' window. At the top right are 'Commit' and 'Cancel' buttons. The 'General' section contains the following fields:

- Name:** devcon-asm
- FQDN or IP Address:** 10.32.24.235
- Type:** Session Manager (dropdown menu)
- Notes:** (empty text box)
- Location:** Location 1 (dropdown menu)
- Outbound Proxy:** (empty dropdown menu)
- Time Zone:** America/New\_York (dropdown menu)
- Credential name:** (empty text box)

The 'SIP Link Monitoring' section at the bottom includes a dropdown menu set to '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**

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="avaya.com"/> ▼	<input type="text"/>
<input type="checkbox"/>	<input type="text" value="5060"/>	<input type="text" value="UDP"/> ▼	<input type="text" value="avaya.com"/> ▼	<input type="text"/>
<input type="checkbox"/>	<input type="text" value="5061"/>	<input type="text" value="TLS"/> ▼	<input type="text" value="avaya.com"/> ▼	<input type="text"/>
<input type="checkbox"/>	<input type="text" value="5062"/>	<input type="text" value="TLS"/> ▼	<input type="text" value="avaya.com"/> ▼	<input type="text"/>

Select : All, None

\* Input Required

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 Acme Packet 3800 Net-Net SBC. The **FQDN or IP Address** field is set to the IP address of its private network interface (see **Figure 1**). Set the **Adaptation** field to the **Acme Adaptation** created in **Section 6.4**. The **Location** field is set to **Location 1** which is the location defined for the subnet where the Acme Packet 3800 Net-Net SBC resides.

SIP Entity Details

CommitCancel

General

\* Name:sp-sbc2

\* FQDN or IP Address:10.32.128.13

Type:SIP Trunk

Notes:

Adaptation:Acme 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 Acme Packet 3800 Net-Net SBC. 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 Acme Packet 3800 Net-Net SBC.

**Entity Links**

CommitCancel

1 Item RefreshFilter: Enable

Name	SIP Entity 1	Protocol	Port	SIP Entity 2	Port	Connection Policy	Notes
* toAcmeSBC	* devcon-asm	TCP	* 5060	* sp-sbc2	* 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 Acme Packet 3800 Net-Net SBC. 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 Acme Packet 3800 Net-Net SBC.

Routing Policy Details

Commit

Cancel

General

\* Name:

sp3-cm Route 2

Disabled:

☐

Notes:

SIP Entity as Destination

Select

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

Routing Policy Details

Commit

Cancel

General

\* Name:

SP Acme SBC Route

Disabled:

☐

Notes:

SIP Entity as Destination

Select

Name	FQDN or IP Address	Type	Notes
sp-sbc2	10.32.128.13	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 **ALL** locations uses route policy **SP Acme SBC Route**.

Dial Pattern Details

Commit

Cancel

General

\* Pattern:

1

\* Min:

11

\* Max:

11

Emergency Call:

☐

SIP Domain:

avaya.com

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"/>	-ALL-	Any Locations	SP Acme SBC Route	0	<input type="checkbox"/>	sp-sbc2	

Select : All, None

The second example shows that 10 digit numbers that start with **64755512** to any domain 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 Acme Packet 3800 Net-Net SBC which resides in Location 1. The originating location could have also been set to **ALL**.

**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-sbc
<input type="checkbox"/>	<u>011</u>	10	18	<input type="checkbox"/>	avaya.com	Dest: sp-sbc
<input type="checkbox"/>	<u>1</u>	11	11	<input type="checkbox"/>	avaya.com	
<input type="checkbox"/>	<u>411</u>	3	3	<input type="checkbox"/>	avaya.com	Dest: sp-sbc
<input type="checkbox"/>	<u>6475512</u>	10	10	<input type="checkbox"/>	-ALL-	Allstream Inbound 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 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** ▼

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

## 7. Configure Acme Packet 3800 Net-Net Session Border Controller

The following sections describe the provisioning of the Acme Packet 3800 Net-Net SBC. Only the SBC provisioning required for the reference configuration is described in these Application Notes. The resulting SBC configuration file is shown in **Appendix A**.

The Acme Packet SBC was configured using the Acme Packet CLI via a serial console port connection. An IP remote connection to a management port is also supported. The following are the generic steps for configuring various elements.

1. Log in with the appropriate credentials.
2. Enable the Superuser mode by entering **enable** and the appropriate password (prompt will end with #).
3. In Superuser mode, type **configure terminal** and press <ENTER>. The prompt will change to *(configure)#*.
4. Type the name of the element that will be configured (e.g., **session-router**).
5. Type the name of the sub-element, if any (e.g., **session-agent**).
6. Type the name of the parameter followed by its value (e.g., **ip-address**).
7. Type **done**.
8. Type **exit** to return to the previous menu.
9. Repeat steps 4 - 8 to configure all the elements. When finished, exit from the configuration mode by typing **exit** until returned to the Superuser prompt.
10. Type **save-configuration** to save the configuration.
11. Type **activate-configuration** to activate the configuration.

Once the provisioning is complete, the configuration may be verified by entering the **show running-config** command.

### 7.1. Physical Interfaces

This section defines the physical interfaces for the private enterprise and public networks.

#### 7.1.1. Public Interface

Create a phy-interface for the public side of the Acme.

1. Enter **system → phy-interface**
2. Enter **name → s0p0**
3. Enter **operation-type → Media**
4. Enter **port → 0**
5. Enter **slot → 0**
6. Enter **duplex-mode → FULL**
7. Enter **speed → 100**
8. Enter **done**
9. Enter **exit**

### 7.1.2. Private Interface

Create a phy-interface for the private enterprise side of the Acme.

1. Enter **system** → **phy-interface**
2. Enter **name** → **s1p0**
3. Enter **operation-type** → **Media**
4. Enter **port** → **0**
5. Enter **slot** → **1**
6. **virtual-mac** → **00:08:25:a0:f4:8a**

Virtual MAC addresses are assigned based on the MAC address assigned to the Acme. This MAC address is found by entering the command **show prom-info mainboard** (e.g. **00 08 25 a0 fa 80**). To define a virtual MAC address, replace the last digit with **8** thru **f**.

7. Enter **duplex-mode** → **FULL**
8. Enter **speed** → **100**
9. Enter **done**
10. Enter **exit**

## 7.2. Network Interfaces

This section defines the network interfaces for the private enterprise and public IP networks.

### 7.2.1. Public Interface

Create a network-interface to the public side of the Acme.

1. Enter **system** → **network-interface**
2. Enter **name** → **s0p0**
3. Enter **ip-address** → **10.3.3.225**
4. Enter **netmask** → **255.255.255.224**
5. Enter **gateway** → **10.3.3.254**
6. Enter **dns-ip-primary** → **10.3.184.199**
7. Enter **hip-ip-list** → **10.3.3.225**
8. Enter **icmp-ip-list** → **10.3.3.225**
9. Enter **done**
10. Enter **exit**

### 7.2.2. Private Interface

Create a network-interface for the private enterprise side of the Acme.

1. Enter **system** → **network-interface**
2. Enter **name** → **s1p0**
3. Enter **ip-address** → **10.32.128.13**
4. Enter **netmask** → **255.255.255.0**
5. Enter **gateway** → **10.32.128.254**
6. Enter **hip-ip-list** → **10.32.128.13**
7. Enter **icmp-ip-list** → **10.32.128.13**
8. Enter **done**
9. Enter **exit**

## 7.3. Realms

Realms are used as a basis for determining egress and ingress associations between physical and network interfaces as well as applying header manipulation such as NAT.

### 7.3.1. Outside Realm

Create a realm for the external network.

1. Enter **media-manager → realm-config**
2. Enter **identifier → EXTERNAL**
3. Enter **network-interfaces → s0p0:0**
4. Enter **done**
5. Enter **exit**

### 7.3.2. Inside Realm

Create a realm for the internal network.

1. Enter **media-manager → realm-config**
2. Enter **identifier → INTERNAL2**
3. Enter **network-interfaces → s1p0:0**
4. Enter **done**
5. Enter **exit**

## 7.4. Steering-Pools

Steering pools define sets of ports that are used for steering media flows thru the Acme Packet 3800 Net-Net SBC.

### 7.4.1. Outside Steering-Pool

Create a steering-pool for the outside network. The start-port and end-port values should specify a range acceptable to MTS Allstream. For the compliance test, no specific range was specified by MTS Allstream, so the start and end ports shown below were chosen arbitrarily.

1. Enter **media-manager → steering-pool**
2. Enter **ip-address → 10.3.3.225**
3. Enter **start-port → 49152**
4. Enter **end-port → 65535**
5. Enter **realm-id → EXTERNAL**
6. Enter **done**
7. Enter **exit**

### 7.4.2. Inside Steering-Pool

Create a steering-pool for the inside network. The start-port and end-port values should specify a range acceptable to the internal enterprise network and include the port range used by Communication Manager. For the compliance test, a wide range was selected that included the default port range that Communication Manager uses and shown on the ip-network-region form in **Section 5.5**.

1. Enter **media-manager → steering-pool**
2. Enter **ip-address → 10.32.128.13**

3. Enter **start-port** → 2048
4. Enter **end-port** → 65535
5. Enter **realm-id** → INTERNAL2
6. Enter **done**
7. Enter **exit**

## 7.5. Media-Manager

Verify that the media-manager process is enabled.

1. Enter **media-manager** → **media-manager**
2. Enter **select** → **show** Verify that the media-manager state is enabled. If not, perform steps 3 – 5 as outlined in **Section 7**
3. Enter **state** → **enabled**
4. Enter **done**
5. Enter **exit**

## 7.6. SIP Configuration

This command sets the values for the Acme Packet 3800 Net-Net SBC SIP operating parameters. The home-realm is the internal default realm for the Acme Packet 3800 Net-Net SBC and the egress-realm is the realm that will be used to send a request if a realm is not specified elsewhere. If the egress-realm is blank, the home-realm is used instead.

1. Enter **session-router** → **sip-config**
2. Enter **state** → **enabled**
3. Enter **operation-mode** → **dialog**
4. Enter **home-realm-id** → INTERNAL2
5. Enter **egress-realm-id** →
6. Enter **nat-mode** → **Public**
7. Enter **done**
8. Enter **exit**

## 7.7. SIP Interfaces

The SIP interface defines the SIP signaling interface (IP address and port) on the Acme Packet 3800 Net-Net SBC.

### 7.7.1. Outside SIP Interface

Create a sip-interface for the outside network.

1. Enter **session-router** → **sip-interface**
2. Enter **state** → **enabled**
3. Enter **realm-id** → EXTERNAL
4. Enter **sip-port**
  - a. Enter **address** → 10.3.3.225
  - b. Enter **port** → 5060
  - c. Enter **transport-protocol** → UDP
  - d. Enter **allow-anonymous** → **agents-only**

- e. Enter **done**
- f. Enter **exit**
- 5. Enter **stop-recurse** → 401,407
- 6. Enter **done**
- 7. Enter **exit**

### 7.7.2. Inside SIP Interface

Create a sip-interface for the inside network.

- 1. Enter **session-router** → **sip-interface**
- 2. Enter **state** → **enabled**
- 3. Enter **realm-id** → **INTERNAL2**
- 4. Enter **sip-port**
  - a. Enter **address** → 10.32.128.13
  - b. Enter **port** → 5060
  - c. Enter **transport-protocol** → TCP
  - d. Enter **allow-anonymous** → all
  - e. Enter **done**
  - f. Enter **exit**
- 5. Enter **stop-recurse** → 401,407
- 6. Enter **done**
- 7. Enter **exit**

## 7.8. Session-Agents

A session-agent defines an internal “next hop” signaling entity for the SIP traffic. A realm is associated with a session-agent to identify sessions coming from or going to the session-agent. A session-agent is defined for the service provider (outside) and Session Manager (inside). SIP header manipulations can be applied to the session-agent level.

### 7.8.1. Outside Session-Agent

Create a session-agent for the outside network.

- 1. Enter **session-router** → **session-agent**
- 2. Enter **hostname** → 10.2.2.12
- 3. Enter **ip-address** → 10.2.2.12
- 4. Enter **port** → 5060
- 5. Enter **state** → **enabled**
- 6. Enter **app-protocol** → SIP
- 7. Enter **transport-method** → UDP
- 8. Enter **realm-id** → EXTERNAL
- 9. Enter **description** → Allstream
- 10. Enter **ping-method** → OPTIONS
- 11. Enter **ping-interval** → 60
- 12. Enter **ping-send-mode** → keep-alive
- 13. Enter **out-manipulationid** → outManToSP
- 14. Enter **done**
- 15. Enter **exit**

### 7.8.2. Inside Session-Agent

Create a session-agent for the inside network.

1. Enter **session-router** → **session-agent**
2. Enter **hostname** → **10.32.24.235**
3. Enter **ip-address** → **10.32.24.235**
4. Enter **port** → **5060**
5. Enter **state** → **enabled**
6. Enter **app-protocol** → **SIP**
7. Enter **transport-method** → **StaticTCP**
8. Enter **realm-id** → **INTERNAL2**
9. Enter **description** → **SM\_SPenv**
10. Enter **ping-method** →
11. Enter **ping-interval** → **60**
12. Enter **ping-send-mode** → **keep-alive**
13. Enter **in-manipulationid** → **inManFromSM**
14. Enter **done**
15. Enter **exit**

### 7.9. Local Policies

Local policies allow SIP requests from the **INTERNAL2** realm to be routed to the service provider session agent in the **EXTERNAL** realm (and vice-versa).

#### 7.9.1. INTERNAL2 to EXTERNAL

Create a local-policy for the **INTERNAL2** realm.

1. Enter **session-router** → **local-policy**
2. Enter **from-address** → **\***
3. Enter **to-address** → **\***
4. Enter **source-realm** → **INTERNAL2**
5. Enter **state** → **enabled**
6. Enter **policy-attributes**
  - a. Enter **next-hop** → **10.2.2.12**
  - b. Enter **realm** → **EXTERNAL**
  - c. Enter **terminate-recursion** → **enabled**
  - d. Enter **app-protocol** → **SIP**
  - e. Enter **state** → **enabled**
  - f. Enter **done**
  - g. Enter **exit**
7. Enter **done**
8. Enter **exit**

#### 7.9.2. EXTERNAL to INTERNAL2

Create a local-policy for the **EXTERNAL** realm.

1. Enter **session-router** → **local-policy**
2. Enter **from-address** → **\***
3. Enter **to-address** → **\***

4. Enter **source-realm** → **EXTERNAL**
5. Enter **state** → **enabled**
6. Enter **policy-attributes**
  - a. Enter **next-hop** → **10.32.24.235**
  - b. Enter **realm** → **INTERNAL2**
  - c. Enter **terminate-recursion** → **enabled**
  - d. Enter **app-protocol** → **SIP**
  - e. Enter **state** → **enabled**
  - f. Enter **done**
  - g. Enter **exit**
7. Enter **done**
8. Enter **exit**

## 7.10. SIP Manipulations

SIP manipulation specifies rules for manipulating the contents of specified SIP headers. Two separate sets of SIP manipulations were required for the compliance test listed below.

- **inManFromSM** – A set of SIP header manipulation rules (HMRs) on traffic from Session Manager to the SBC.
- **outManToSP** - A set of SIP header manipulation rules on traffic from the SBC to service provider (MTS Allstream).

### 7.10.1. Session Manager to SBC

The following set of SIP HMRs is applied to traffic from the Session Manager to the SBC. In some call flows the user part of the SIP Contact header received from the Session Manager was not passed unaltered to the public side of the SBC. To correct this, the user part of the Contact header is stored when received from the Session Manager and used to create a temporary header called X-Contact that will be deleted on the outbound (public) side of the SBC. The information contained in the X-Contact header will be used to recreate the proper Contact header on the public side of the SBC as shown in **Sections 7.10.2.8 and 7.10.2.9**.

To create this set of SIP HMRs:

1. Enter **session-router** → **sip-manipulation**
2. Enter **name** → **inManFromSM**
3. Enter **description** → **“Inbound SIP HMRs From SM”**
4. Proceed to the following sections. Once all sections are completed then proceed with **Steps 5 and 6** below.
5. Enter **done**
6. Enter **exit**

#### 7.10.1.1 Store Contact

This rule stores the user part of the incoming Contact header.

1. Enter **header-rule**
2. Enter **name** → **strcon**
3. Enter **header-name** → **Contact**



4. Enter **action** → **manipulate**
5. Enter **comparison-type** → **case-sensitive**
6. Enter **msg-type** → **request**
7. Enter **methods** → **INVITE,UPDATE**
8. Enter **element-rule**
  - a. Enter **name** → **strval**
  - b. Enter **type** → **uri-user**
  - c. Enter **action** → **store**
  - d. Enter **match-val-type** → **any**
  - e. Enter **comparison-type** → **case-sensitive**
  - f. Enter **match-value** → **(.\*)**
  - g. Enter **done**
  - h. Enter **exit**
9. Enter **done**
10. Enter **exit**

#### 7.10.1.2 Create X-Contact

This rule creates a temporary header called X-Contact containing only the user part of the incoming Contact header as stored by the rule defined in the previous section.

1. Enter **header-rule**
2. Enter **name** → **addXcontact**
3. Enter **header-name** → **X-Contact**
4. Enter **action** → **add**
5. Enter **comparison-type** → **pattern-rule**
6. Enter **msg-type** → **request**
7. Enter **methods** → **INVITE,UPDATE**
8. Enter **element-rule**
  - a. Enter **name** → **addX**
  - b. Enter **type** → **header-value**
  - c. Enter **action** → **replace**
  - d. Enter **match-val-type** → **any**
  - e. Enter **comparison-type** → **pattern-rule**
  - f. Enter **new-value** → **\$strcon.\$strval.\$0**
  - g. Enter **done**
  - h. Enter **exit**
9. Enter **done**
10. Enter **exit**

#### 7.10.2. SBC to MTS Allstream

The following set of SIP HMRs is applied to traffic from the SBC to MTS Allstream.

To create this set of SIP HMRs:

1. Enter **session-router** → **sip-manipulation**
2. Enter **name** → **outManFromSP**
3. Enter **description** → **“outbound SIP HMRs From SP”**

4. Proceed to the following sections. Once all sections are completed then proceed with **Steps 5 and 6** below.
5. Enter **done**
6. Enter **exit**

#### 7.10.2.1 Change Host of the To Header

This rule replaces the host part of the To header with the service provider's IP address. A similar manipulation is performed on the Request-URI by the Session Manager. The Request-URI could have also been manipulated by the SBC.

1. Enter **header-rule**
2. Enter **name** → **manipTo**
3. Enter **header-name** → **To**
4. Enter **action** → **manipulate**
5. Enter **comparison-type** → **case-sensitive**
6. Enter **msg-type** → **request**
7. Enter **element-rule** →
  - a. Enter **name** → **chgToHost**
  - b. Enter **type** → **uri-host**
  - c. Enter **action** → **replace**
  - d. Enter **match-val-type** → **any**
  - e. Enter **comparison-type** → **case-sensitive**
  - f. Enter **new-value** → **\$REMOTE\_IP**
  - g. Enter **done**
  - h. Enter **exit**
8. Enter **done**
9. Enter **exit**

#### 7.10.2.2 Change Host of the From Header

This rule replaces the host part of the From header with the public IP address of the SBC.

1. Enter **header-rule**
2. Enter **name** → **manipFrom**
3. Enter **header-name** → **From**
4. Enter **action** → **manipulate**
5. Enter **comparison-type** → **case-sensitive**
6. Enter **msg-type** → **request**
7. Enter **element-rule** →
  - a. Enter **name** → **From**
  - b. Enter **type** → **uri-host**
  - c. Enter **action** → **replace**
  - d. Enter **match-val-type** → **any**
  - e. Enter **comparison-type** → **case-sensitive**
  - f. Enter **new-value** → **\$LOCAL\_IP**
  - g. Enter **done**
  - h. Enter **exit**
8. Enter **done**

9. Enter **exit**

### 7.10.2.3 Change Host of the History Info Header

This rule replaces the host part of the History-Info header with the public IP address of the SBC.

1. Enter **header-rule**
2. Enter **name** → **manipHistInfo**
3. Enter **header-name** → **History-Info**
4. Enter **action** → **manipulate**
5. Enter **comparison-type** → **case-sensitive**
6. Enter **msg-type** → **request**
7. Enter **element-rule** →
  - a. Enter **name** → **HistoryInfo**
  - b. Enter **type** → **uri-host**
  - c. Enter **action** → **replace**
  - d. Enter **match-val-type** → **any**
  - e. Enter **comparison-type** → **case-sensitive**
  - f. Enter **new-value** → **\$LOCAL\_IP**
  - g. Enter **done**
  - h. Enter **exit**
8. Enter **done**
9. Enter **exit**

### 7.10.2.4 Change Host of the PAI Header

This rule replaces the host part of the P-Asserted-Identity header with the public IP address of the SBC.

1. Enter **header-rule**
2. Enter **name** → **manipPAI**
3. Enter **header-name** → **P-Asserted-Identity**
4. Enter **action** → **manipulate**
5. Enter **comparison-type** → **case-sensitive**
6. Enter **msg-type** → **request**
7. Enter **element-rule** →
  - a. Enter **name** → **Pai**
  - b. Enter **type** → **uri-host**
  - c. Enter **action** → **replace**
  - d. Enter **match-val-type** → **any**
  - e. Enter **comparison-type** → **case-sensitive**
  - f. Enter **new-value** → **\$LOCAL\_IP**
  - g. Enter **done**
  - h. Enter **exit**
8. Enter **done**
9. Enter **exit**

### 7.10.2.5 Change Host of the Diversion Header

This rule replaces the host part of the Diversion header with the public IP address of the SBC.

1. Enter **header-rule**
2. Enter **name** → **manipDiversion**
3. Enter **header-name** → **Diversion**
4. Enter **action** → **manipulate**
5. Enter **comparison-type** → **case-sensitive**
6. Enter **msg-type** → **request**
7. Enter **element-rule** →
  - a. Enter **name** → **Diversion**
  - b. Enter **type** → **uri-host**
  - c. Enter **action** → **replace**
  - d. Enter **match-val-type** → **any**
  - e. Enter **comparison-type** → **case-sensitive**
  - f. Enter **new-value** → **\$LOCAL\_IP**
  - g. Enter **done**
  - h. Enter **exit**
8. Enter **done**
9. Enter **exit**

#### 7.10.2.6 Change Host of the Refer-To Header

This rule replaces the host part of the Refer-To header with the service provider's IP address.

1. Enter **header-rule**
2. Enter **name** → **manipRefer**
3. Enter **header-name** → **Refer-To**
4. Enter **action** → **manipulate**
5. Enter **comparison-type** → **case-sensitive**
6. Enter **msg-type** → **request**
7. Enter **element-rule** →
  - a. Enter **name** → **chgHostRefer**
  - b. Enter **type** → **uri-host**
  - c. Enter **action** → **replace**
  - d. Enter **match-val-type** → **any**
  - e. Enter **comparison-type** → **case-sensitive**
  - f. Enter **new-value** → **\$REMOTE\_IP**
  - g. Enter **done**
  - h. Enter **exit**
8. Enter **done**
9. Enter **exit**

#### 7.10.2.7 Store X-Contact Header

This rule stores the contents of the X-Contact header so it can be used later. The X-Contact header contains only the user part of the Contact header as it was originally received from the Session Manager as described in **Section 7.10.1**.

1. Enter **header-rule**
2. Enter **name** → **storexcontact**
3. Enter **header-name** → **X-Contact**

4. Enter **action** → **manipulate**
5. Enter **comparison-type** → **case-sensitive**
6. Enter **msg-type** → **request**
7. Enter **methods** → **INVITE,UPDATE**
8. Enter **element-rule** →
  - a. Enter **name** → **storexcontact**
  - b. Enter **type** → **header-value**
  - c. Enter **action** → **store**
  - d. Enter **match-val-type** → **any**
  - e. Enter **comparison-type** → **case-sensitive**
  - f. Enter **match-value** → **(.\*)**
  - g. Enter **done**
  - h. Enter **exit**
9. Enter **done**
10. Enter **exit**

#### 7.10.2.8 Replace Contact Header

This rule uses the data stored from the X-Contact header to overwrite the user part of the outbound Contact header.

1. Enter **header-rule**
2. Enter **name** → **replacecontact**
3. Enter **header-name** → **Contact**
4. Enter **action** → **manipulate**
5. Enter **comparison-type** → **pattern-rule**
6. Enter **msg-type** → **request**
7. Enter **methods** → **INVITE,UPDATE**
8. Enter **element-rule**
  - a. Enter **name** → **replacecontact**
  - b. Enter **type** → **uri-user**
  - c. Enter **action** → **replace**
  - d. Enter **match-val-type** → **any**
  - e. Enter **comparison-type** → **pattern-rule**
  - f. Enter **match-value** → **(.\*)**
  - g. Enter **new-value** **\$storexcontact.\$storexcontact.\$0**
  - h. Enter **done**
  - i. Enter **exit**
9. Enter **done**
10. Enter **exit**

#### 7.10.2.9 Delete X-Contact Header

This rule deletes the temporary X-Contact header before sending the message to the service provider.

1. Enter **header-rule**
2. Enter **name** → **delxcontact**
3. Enter **header-name** → **X-Contact**

4. Enter **action** → **delete**
5. Enter **comparison-type** → **pattern-rule**
6. Enter **msg-type** → **request**
7. Enter **methods** → **INVITE,UPDATE**
8. Enter **done**
9. Enter **exit**

#### **7.10.2.10 Delete P-Location Header**

This rule deletes the P-Location header. This header is not used by the service provider and it may contain internal IP addresses which should not be shared outside of the enterprise. Thus, the header was removed.

1. Enter **header-rule**
2. Enter **name** → **delPloc**
3. Enter **header-name** → **P-Location**
4. Enter **action** → **delete**
5. Enter **comparison-type** → **case-sensitive**
6. Enter **msg-type** → **any**
7. Enter **methods** →
8. Enter **done**
9. Enter **exit**

#### **7.10.2.11 Delete Alert-Info Header**

This rule deletes the Alert-Info header. This header is not used by the service provider and it may contain internal IP addresses which should not be shared outside of the enterprise. Thus, the header was removed.

1. Enter **header-rule**
2. Enter **name** → **delAlert**
3. Enter **header-name** → **Alert-Info**
4. Enter **action** → **delete**
5. Enter **comparison-type** → **case-sensitive**
6. Enter **msg-type** → **any**
7. Enter **methods** →
8. Enter **done**
9. Enter **exit**

## 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](http://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 Acme Packet 3800 Net-Net SBC at the edge of the enterprise. MTS Allstream will provide the IP address of the MTS Allstream SIP proxy/SBC, 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 SBC 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 the Acme Packet 3800 Net-Net 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*, August 2010, Document Number 03-300509.
- [4] *Avaya Aura® Communication Manager Feature Description and Implementation*, August 2010, Document Number 555-245-205.
- [5] *Installing and Upgrading Avaya Aura® System Manager*, Release 6.1, November 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, October 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: Acme Packet 3800 Net-Net Session Border Controller Configuration File

```

host-routes
    dest-network      10.32.0.0
    netmask           255.255.0.0
    gateway           10.32.128.254
    description       DevConnectLAN
    last-modified-by  admin@135.11.141.118
    last-modified-date 2010-08-05 15:25:58
host-routes
    dest-network      192.168.0.0
    netmask           255.255.0.0
    gateway           10.32.128.254
    description       Route to testers
    last-modified-by  admin@192.168.168.37
    last-modified-date 2011-09-10 10:50:25
local-policy
    from-address
                                *
    to-address
                                *
    source-realm
                                INTERNAL2
    description
    activate-time           N/A
    deactivate-time         N/A
    state                   enabled
    policy-priority         none
    last-modified-by        admin@192.168.168.37
    last-modified-date      2011-10-11 17:12:38
    policy-attribute
        next-hop            10.2.2.12
        realm               EXTERNAL
        action              none
        terminate-recursion enabled
        carrier
        start-time          0000
        end-time            2400
        days-of-week        U-S
        cost                0
        app-protocol        SIP
        state               enabled
        methods
        media-profiles
        lookup              single
        next-key
        eloc-str-lkup       disabled
        eloc-str-match
local-policy
    from-address
                                *
    to-address
                                *
    source-realm
                                EXTERNAL
    description
    activate-time           N/A
    deactivate-time         N/A

```

state	enabled
policy-priority	none
last-modified-by	admin@192.168.168.37
last-modified-date	2011-10-10 15:24:09
policy-attribute	
next-hop	10.32.24.235
realm	INTERNAL2
action	none
terminate-recursion	enabled
carrier	
start-time	0000
end-time	2400
days-of-week	U-S
cost	0
app-protocol	SIP
state	enabled
methods	
media-profiles	
lookup	single
next-key	
eloc-str-lkup	disabled
eloc-str-match	
media-manager	
state	enabled
latching	enabled
flow-time-limit	86400
initial-guard-timer	300
subsq-guard-timer	300
tcp-flow-time-limit	86400
tcp-initial-guard-timer	300
tcp-subsq-guard-timer	300
tcp-number-of-ports-per-flow	2
hnt-rtcp	disabled
algd-log-level	NOTICE
mbcd-log-level	NOTICE
red-flow-port	1985
red-mgcp-port	1986
red-max-trans	10000
red-sync-start-time	5000
red-sync-comp-time	1000
media-policing	enabled
max-signaling-bandwidth	10000000
max-untrusted-signaling	100
min-untrusted-signaling	30
app-signaling-bandwidth	0
tolerance-window	30
rtcp-rate-limit	0
trap-on-demote-to-deny	enabled
min-media-allocation	2000
min-trusted-allocation	4000
deny-allocation	64000
anonymous-sdp	disabled
arp-msg-bandwidth	32000
fragment-msg-bandwidth	0
rfc2833-timestamp	disabled
default-2833-duration	100
rfc2833-end-pkts-only-for-non-sig	enabled
translate-non-rfc2833-event	disabled
media-supervision-traps	disabled
dnalg-server-failover	disabled
last-modified-by	admin@135.11.141.142
last-modified-date	2010-06-16 05:40:01

```

network-interface
  name          s0p0
  sub-port-id   0
  description
  hostname
  ip-address     10.3.3.225
  pri-utility-addr
  sec-utility-addr
  netmask        255.255.255.224
  gateway        10.3.3.254
  sec-gateway
  gw-heartbeat
    state        disabled
    heartbeat     0
    retry-count   0
    retry-timeout 1
    health-score  0
  dns-ip-primary 10.3.184.199
  dns-ip-backup1 10.3.184.7
  dns-ip-backup2
  dns-domain
  dns-timeout
    hip-ip-list   10.3.3.225
  ftp-address
    icmp-address  10.3.3.225
  snmp-address
  telnet-address
  ssh-address
  last-modified-by admin@192.168.168.37
  last-modified-date 2011-09-10 10:08:47
network-interface
  name          s1p0
  sub-port-id   0
  description
  hostname
  ip-address     10.32.128.13
  pri-utility-addr
  sec-utility-addr
  netmask        255.255.255.0
  gateway        10.32.128.254
  sec-gateway
  gw-heartbeat
    state        disabled
    heartbeat     0
    retry-count   0
    retry-timeout 1
    health-score  0
  dns-ip-primary
  dns-ip-backup1
  dns-ip-backup2
  dns-domain
  dns-timeout     11
    hip-ip-list   10.32.128.13
  ftp-address
    icmp-address  10.32.128.13
  snmp-address
  telnet-address  10.32.128.13
  ssh-address
  last-modified-by admin@console
  last-modified-date 2011-09-09 20:10:35
phy-interface
  name          s0p0

```

operation-type	Media
port	0
slot	0
virtual-mac	
admin-state	enabled
auto-negotiation	enabled
duplex-mode	
speed	
overload-protection	disabled
last-modified-by	admin@console
last-modified-date	2011-09-09 19:39:05
phy-interface	
name	slp0
operation-type	Media
port	0
slot	1
virtual-mac	00:08:25:a0:f4:8a
admin-state	enabled
auto-negotiation	enabled
duplex-mode	FULL
speed	100
overload-protection	disabled
last-modified-by	admin@console
last-modified-date	2011-09-09 19:38:24
realm-config	
identifier	EXTERNAL
description	
addr-prefix	0.0.0.0
network-interfaces	
s0p0:0	
mm-in-realm	disabled
mm-in-network	enabled
mm-same-ip	enabled
mm-in-system	enabled
bw-cac-non-mm	disabled
msm-release	disabled
generate-UDP-checksum	disabled
max-bandwidth	0
fallback-bandwidth	0
max-priority-bandwidth	0
max-latency	0
max-jitter	0
max-packet-loss	0
observ-window-size	0
parent-realm	
dns-realm	
media-policy	
media-sec-policy	
in-translationid	
out-translationid	
in-manipulationid	
out-manipulationid	
manipulation-string	
manipulation-pattern	
class-profile	
average-rate-limit	0
access-control-trust-level	none
invalid-signal-threshold	0
maximum-signal-threshold	0
untrusted-signal-threshold	0
nat-trust-threshold	0
deny-period	30

ext-policy-svr	
symmetric-latching	disabled
pai-strip	disabled
trunk-context	
early-media-allow	
enforcement-profile	
additional-prefixes	
restricted-latching	none
restriction-mask	32
accounting-enable	enabled
user-cac-mode	none
user-cac-bandwidth	0
user-cac-sessions	0
icmp-detect-multiplier	0
icmp-advertisement-interval	0
icmp-target-ip	
monthly-minutes	0
net-management-control	disabled
delay-media-update	disabled
refer-call-transfer	disabled
dyn-refer-term	disabled
codec-policy	
codec-manip-in-realm	disabled
constraint-name	
call-recording-server-id	
xnq-state	xnq-unknown
hairpin-id	0
stun-enable	disabled
stun-server-ip	0.0.0.0
stun-server-port	3478
stun-changed-ip	0.0.0.0
stun-changed-port	3479
match-media-profiles	
qos-constraint	
sip-profile	
sip-isup-profile	
block-rtcp	disabled
hide-egress-media-update	disabled
last-modified-by	admin@135.11.207.156
last-modified-date	2010-11-03 08:55:21
realm-config	
identifier	INTERNAL2
description	
addr-prefix	0.0.0.0
network-interfaces	
	slp0:0
mm-in-realm	disabled
mm-in-network	enabled
mm-same-ip	enabled
mm-in-system	enabled
bw-cac-non-mm	disabled
msm-release	disabled
generate-UDP-checksum	disabled
max-bandwidth	0
fallback-bandwidth	0
max-priority-bandwidth	0
max-latency	0
max-jitter	0
max-packet-loss	0
observ-window-size	0
parent-realm	
dns-realm	

media-policy	
media-sec-policy	
in-translationid	
out-translationid	
in-manipulationid	
out-manipulationid	
manipulation-string	
manipulation-pattern	
class-profile	
average-rate-limit	0
access-control-trust-level	none
invalid-signal-threshold	0
maximum-signal-threshold	0
untrusted-signal-threshold	0
nat-trust-threshold	0
deny-period	30
ext-policy-svr	
symmetric-latching	disabled
pai-strip	disabled
trunk-context	
early-media-allow	
enforcement-profile	
additional-prefixes	
restricted-latching	none
restriction-mask	32
accounting-enable	enabled
user-cac-mode	none
user-cac-bandwidth	0
user-cac-sessions	0
icmp-detect-multiplier	0
icmp-advertisement-interval	0
icmp-target-ip	
monthly-minutes	0
net-management-control	disabled
delay-media-update	disabled
refer-call-transfer	disabled
dyn-refer-term	disabled
codec-policy	
codec-manip-in-realm	disabled
constraint-name	
call-recording-server-id	
xnq-state	xnq-unknown
hairpin-id	0
stun-enable	disabled
stun-server-ip	0.0.0.0
stun-server-port	3478
stun-changed-ip	0.0.0.0
stun-changed-port	3479
match-media-profiles	
qos-constraint	
sip-profile	
sip-isup-profile	
block-rtcp	disabled
hide-egress-media-update	disabled
last-modified-by	admin@135.11.207.156
last-modified-date	2010-12-16 17:25:01
session-agent	
hostname	10.32.24.235
ip-address	10.32.24.235
port	5060
state	enabled
app-protocol	SIP

app-type	
transport-method	StaticTCP
realm-id	INTERNAL2
egress-realm-id	
description	SM_SPenv
carriers	
allow-next-hop-lp	enabled
constraints	disabled
max-sessions	0
max-inbound-sessions	0
max-outbound-sessions	0
max-burst-rate	0
max-inbound-burst-rate	0
max-outbound-burst-rate	0
max-sustain-rate	0
max-inbound-sustain-rate	0
max-outbound-sustain-rate	0
min-seizures	5
min-asr	0
time-to-resume	0
ttr-no-response	0
in-service-period	0
burst-rate-window	0
sustain-rate-window	0
req-uri-carrier-mode	None
proxy-mode	
redirect-action	
loose-routing	enabled
send-media-session	enabled
response-map	
ping-method	
ping-interval	0
ping-send-mode	keep-alive
ping-all-addresses	disabled
ping-in-service-response-codes	
out-service-response-codes	
media-profiles	
in-translationid	
out-translationid	
trust-me	disabled
request-uri-headers	
stop-recurse	
local-response-map	
ping-to-user-part	
ping-from-user-part	
li-trust-me	disabled
in-manipulationid	inManFromSM
out-manipulationid	
manipulation-string	
manipulation-pattern	
p-asserted-id	
trunk-group	
max-register-sustain-rate	0
early-media-allow	
invalidate-registrations	disabled
rfc2833-mode	none
rfc2833-payload	0
codec-policy	
enforcement-profile	
refer-call-transfer	disabled
reuse-connections	NONE
tcp-keepalive	none

tcp-reconn-interval	0
max-register-burst-rate	0
register-burst-window	0
sip-profile	
sip-isup-profile	
last-modified-by	admin@192.168.168.37
last-modified-date	2011-09-20 22:39:03
session-agent	
hostname	10.2.2.12
ip-address	10.2.2.12
port	5060
state	enabled
app-protocol	SIP
app-type	
transport-method	UDP
realm-id	EXTERNAL
egress-realm-id	
description	Allstream
carriers	
allow-next-hop-lp	enabled
constraints	disabled
max-sessions	0
max-inbound-sessions	0
max-outbound-sessions	0
max-burst-rate	0
max-inbound-burst-rate	0
max-outbound-burst-rate	0
max-sustain-rate	0
max-inbound-sustain-rate	0
max-outbound-sustain-rate	0
min-seizures	5
min-asr	0
time-to-resume	0
ttr-no-response	0
in-service-period	0
burst-rate-window	0
sustain-rate-window	0
req-uri-carrier-mode	None
proxy-mode	
redirect-action	
loose-routing	enabled
send-media-session	enabled
response-map	
ping-method	OPTIONS
ping-interval	60
ping-send-mode	keep-alive
ping-all-addresses	disabled
ping-in-service-response-codes	
out-service-response-codes	
media-profiles	
in-translationid	
out-translationid	
trust-me	disabled
request-uri-headers	
stop-recurse	
local-response-map	
ping-to-user-part	
ping-from-user-part	
li-trust-me	disabled
in-manipulationid	
out-manipulationid	outManToSP
manipulation-string	



manipulation-pattern	
p-asserted-id	
trunk-group	
max-register-sustain-rate	0
early-media-allow	
invalidate-registrations	disabled
rfc2833-mode	none
rfc2833-payload	0
codec-policy	
enforcement-profile	
refer-call-transfer	disabled
reuse-connections	NONE
tcp-keepalive	none
tcp-reconn-interval	0
max-register-burst-rate	0
register-burst-window	0
sip-profile	
sip-isup-profile	
last-modified-by	admin@192.168.168.37
last-modified-date	2011-10-10 14:40:17
sip-config	
state	enabled
operation-mode	dialog
dialog-transparency	enabled
home-realm-id	INTERNAL2
egress-realm-id	
nat-mode	Public
registrar-domain	*
registrar-host	*
registrar-port	5060
register-service-route	always
init-timer	500
max-timer	4000
trans-expire	32
invite-expire	180
inactive-dynamic-conn	32
enforcement-profile	
pac-method	
pac-interval	10
pac-strategy	PropDist
pac-load-weight	1
pac-session-weight	1
pac-route-weight	1
pac-callid-lifetime	600
pac-user-lifetime	3600
red-sip-port	1988
red-max-trans	10000
red-sync-start-time	5000
red-sync-comp-time	1000
add-reason-header	disabled
sip-message-len	4096
enum-sag-match	disabled
extra-method-stats	enabled
registration-cache-limit	0
register-use-to-for-lp	disabled
options	max-udp-length=0
refer-src-routing	disabled
add-ucid-header	disabled
proxy-sub-events	
pass-gruu-contact	disabled
sag-lookup-on-redirect	disabled
last-modified-by	admin@135.11.207.156

last-modified-date	2010-11-02 16:18:33
sip-interface	
state	enabled
realm-id	EXTERNAL
description	
sip-port	
address	10.3.3.225
port	5060
transport-protocol	UDP
tls-profile	
allow-anonymous	agents-only
ims-aka-profile	
carriers	
trans-expire	0
invite-expire	0
max-redirect-contacts	0
proxy-mode	
redirect-action	
contact-mode	none
nat-traversal	none
nat-interval	30
tcp-nat-interval	90
registration-caching	disabled
min-reg-expire	300
registration-interval	3600
route-to-registrar	disabled
secured-network	disabled
teluri-scheme	disabled
uri-fqdn-domain	
trust-mode	all
max-nat-interval	3600
nat-int-increment	10
nat-test-increment	30
sip-dynamic-hnt	disabled
stop-recurse	401,407
port-map-start	0
port-map-end	0
in-manipulationid	
out-manipulationid	
manipulation-string	
manipulation-pattern	
sip-ims-feature	disabled
operator-identifier	
anonymous-priority	none
max-incoming-conns	0
per-src-ip-max-incoming-conns	0
inactive-conn-timeout	0
untrusted-conn-timeout	0
network-id	
ext-policy-server	
default-location-string	
charging-vector-mode	pass
charging-function-address-mode	pass
ccf-address	
ecf-address	
term-tgrp-mode	none
implicit-service-route	disabled
rfc2833-payload	101
rfc2833-mode	transparent
constraint-name	
response-map	
local-response-map	

ims-aka-feature	disabled
enforcement-profile	
route-unauthorized-calls	
tcp-keepalive	none
add-sdp-invite	disabled
add-sdp-profiles	
sip-profile	
sip-isup-profile	
last-modified-by	admin@192.168.168.37
last-modified-date	2011-09-10 10:14:45
sip-interface	
state	enabled
realm-id	INTERNAL2
description	
sip-port	
address	10.32.128.13
port	5060
transport-protocol	TCP
tls-profile	
allow-anonymous	all
ims-aka-profile	
carriers	
trans-expire	0
invite-expire	0
max-redirect-contacts	0
proxy-mode	
redirect-action	
contact-mode	none
nat-traversal	none
nat-interval	30
tcp-nat-interval	90
registration-caching	disabled
min-reg-expire	300
registration-interval	3600
route-to-registrar	disabled
secured-network	disabled
teluri-scheme	disabled
uri-fqdn-domain	
trust-mode	all
max-nat-interval	3600
nat-int-increment	10
nat-test-increment	30
sip-dynamic-hnt	disabled
stop-recurse	401,407
port-map-start	0
port-map-end	0
in-manipulationid	
out-manipulationid	
manipulation-string	
manipulation-pattern	
sip-ims-feature	disabled
operator-identifier	
anonymous-priority	none
max-incoming-conns	0
per-src-ip-max-incoming-conns	0
inactive-conn-timeout	0
untrusted-conn-timeout	0
network-id	
ext-policy-server	
default-location-string	
charging-vector-mode	pass
charging-function-address-mode	pass

ccf-address	
ecf-address	
term-tgrp-mode	none
implicit-service-route	disabled
rfc2833-payload	101
rfc2833-mode	transparent
constraint-name	
response-map	
local-response-map	
ims-aka-feature	disabled
enforcement-profile	
route-unauthorized-calls	
tcp-keepalive	none
add-sdp-invite	disabled
add-sdp-profiles	
sip-profile	
sip-isup-profile	
last-modified-by	admin@135.105.224.163
last-modified-date	2011-08-03 16:00:53
sip-manipulation	
name	outManToSP
description	Outbound SIP HMRs To SP
split-headers	
join-headers	
header-rule	
name	manipTo
header-name	To
action	manipulate
comparison-type	case-sensitive
msg-type	request
methods	
match-value	
new-value	
element-rule	
name	chgToHost
parameter-name	
type	uri-host
action	replace
match-val-type	any
comparison-type	case-sensitive
match-value	
new-value	\$REMOTE_IP
header-rule	
name	manipFrom
header-name	From
action	manipulate
comparison-type	case-sensitive
msg-type	request
methods	
match-value	
new-value	
element-rule	
name	From
parameter-name	
type	uri-host
action	replace
match-val-type	any
comparison-type	case-sensitive
match-value	
new-value	\$LOCAL_IP
header-rule	
name	manipDiversion

header-name	Diversion
action	manipulate
comparison-type	case-sensitive
msg-type	request
methods	
match-value	
new-value	
element-rule	
name	Diversion
parameter-name	
type	uri-host
action	replace
match-val-type	any
comparison-type	case-sensitive
match-value	
new-value	\$LOCAL_IP
header-rule	
name	manipHistInfo
header-name	History-Info
action	manipulate
comparison-type	case-sensitive
msg-type	request
methods	
match-value	
new-value	
element-rule	
name	HistoryInfo
parameter-name	
type	uri-host
action	replace
match-val-type	any
comparison-type	case-sensitive
match-value	
new-value	\$LOCAL_IP
header-rule	
name	manipPAI
header-name	P-Asserted-Identity
action	manipulate
comparison-type	case-sensitive
msg-type	request
methods	
match-value	
new-value	
element-rule	
name	Pai
parameter-name	
type	uri-host
action	replace
match-val-type	any
comparison-type	case-sensitive
match-value	
new-value	\$LOCAL_IP
header-rule	
name	storeXcontact
header-name	X-Contact
action	manipulate
comparison-type	case-sensitive
msg-type	request
methods	INVITE, UPDATE
match-value	
new-value	
element-rule	

	name	storeXcontact
	parameter-name	
	type	header-value
	action	store
	match-val-type	any
	comparison-type	case-sensitive
	match-value	(.*)
	new-value	
header-rule	name	replacecontact
	header-name	Contact
	action	manipulate
	comparison-type	pattern-rule
	msg-type	request
	methods	INVITE, UPDATE
	match-value	
	new-value	
	element-rule	
	name	replacecontact
	parameter-name	
	type	uri-user
	action	replace
	match-val-type	any
	comparison-type	pattern-rule
	match-value	(.*)
	new-value	\$storeXcontact.\$storeXcontact.\$0
header-rule	name	delXcontact
	header-name	X-Contact
	action	delete
	comparison-type	pattern-rule
	msg-type	request
	methods	INVITE, UPDATE
	match-value	
	new-value	
header-rule	name	manipRefer
	header-name	Refer-To
	action	manipulate
	comparison-type	case-sensitive
	msg-type	request
	methods	
	match-value	
	new-value	
	element-rule	
	name	chgHostRefer
	parameter-name	
	type	uri-host
	action	replace
	match-val-type	any
	comparison-type	case-sensitive
	match-value	
	new-value	\$REMOTE_IP
header-rule	name	delPloc
	header-name	P-Location
	action	delete
	comparison-type	case-sensitive
	msg-type	any
	methods	
	match-value	
	new-value	

header-rule	
name	delAlert
header-name	Alert-Info
action	delete
comparison-type	case-sensitive
msg-type	any
methods	
match-value	
new-value	
last-modified-by	admin@135.105.233.139
last-modified-date	2011-08-08 16:04:15
sip-manipulation	
name	inManFromSM
description	storecontact
split-headers	
join-headers	
header-rule	
name	strcon
header-name	Contact
action	manipulate
comparison-type	case-sensitive
msg-type	request
methods	INVITE,UPDATE
match-value	
new-value	
element-rule	
name	strval
parameter-name	
type	uri-user
action	store
match-val-type	any
comparison-type	case-sensitive
match-value	(.*)
new-value	
header-rule	
name	addXcontact
header-name	X-Contact
action	add
comparison-type	pattern-rule
msg-type	request
methods	INVITE,UPDATE
match-value	
new-value	
element-rule	
name	addX
parameter-name	
type	header-value
action	replace
match-val-type	any
comparison-type	pattern-rule
match-value	
new-value	\$strcon.\$strval.\$0
last-modified-by	admin@135.11.207.156
last-modified-date	2011-01-03 17:14:28
steering-pool	
ip-address	135.10.96.225
start-port	49152
end-port	65535
realm-id	EXTERNAL
network-interface	
last-modified-by	admin@192.168.168.37

last-modified-date	2011-09-10 10:11:31
steering-pool	
ip-address	10.32.128.13
start-port	2048
end-port	65535
realm-id	INTERNAL2
network-interface	
last-modified-by	admin@135.11.141.118
last-modified-date	2010-10-06 11:28:26
system-config	
hostname	
description	
location	
mib-system-contact	
mib-system-name	
mib-system-location	
snmp-enabled	enabled
enable-snmp-auth-traps	disabled
enable-snmp-syslog-notify	disabled
enable-snmp-monitor-traps	disabled
enable-env-monitor-traps	disabled
snmp-syslog-his-table-length	1
snmp-syslog-level	WARNING
system-log-level	WARNING
process-log-level	NOTICE
process-log-ip-address	0.0.0.0
process-log-port	0
collect	
sample-interval	5
push-interval	15
boot-state	disabled
start-time	now
end-time	never
red-collect-state	disabled
red-max-trans	1000
red-sync-start-time	5000
red-sync-comp-time	1000
push-success-trap-state	disabled
call-trace	enabled
internal-trace	enabled
log-filter	all
default-gateway	10.3.3.254
restart	enabled
exceptions	
telnet-timeout	0
console-timeout	0
remote-control	enabled
cli-audit-trail	enabled
link-redundancy-state	disabled
source-routing	disabled
cli-more	disabled
terminal-height	24
debug-timeout	0
trap-event-lifetime	0
default-v6-gateway	::
ipv6-support	disabled
cleanup-time-of-day	00:00
last-modified-by	admin@192.168.168.37
last-modified-date	2011-09-10 11:04:14



---

**©2012 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](mailto:devconnect@avaya.com).