



Application Notes for Configuring MTS Allstream SIP Trunking Service with Avaya Aura® Communication Manager Evolution Server R6.0.1, Avaya Aura® Session Manager R6.1 and Avaya Session Border Controller for Enterprise R4.0.5 – Issue 1.0

Abstract

These Application Notes describe the steps to configure Session Initiation Protocol (SIP) Trunking between MTS Allstream SIP Trunking Service and an Avaya SIP-enabled enterprise solution. The Avaya solution consists of Avaya Aura® Communication Manager Evolution Server 6.0.1, Avaya Aura® Session Manager 6.1, Avaya Session Border Controller for Enterprise 4.0.5 and various Avaya endpoints. This documented solution does not extend to configurations without Avaya Aura® Session Manager and Avaya Session Border Controller for Enterprise.

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 is conducted via the DevConnect Program at the Avaya Solution and Interoperability Test Lab.

Table of Contents

1.	Introduction	4
2.	General Test Approach and Test Results	4
2.1.	Interoperability Compliance Testing	4
2.2.	Test Results	5
2.3.	Support	7
3.	Reference Configuration	8
4.	Equipment and Software Validated	10
5.	Configure Communication Manager	11
5.1.	Licensing and Capacity	11
5.2.	System Features	12
5.3.	IP Node Names	13
5.4.	Codecs	13
5.5.	IP Network Region	14
5.6.	Signaling Group	17
5.7.	Trunk Group	19
5.8.	Calling Party Information	22
5.9.	Outbound Routing	23
5.10.	Incoming Call Handling	25
5.11.	Saving Communication Manager Configuration Changes	25
6.	Configure Avaya Aura® Session Manager	25
6.1.	System Manager Login and Navigation	25
6.2.	Specify SIP Domain	27
6.3.	Add Location	27
6.4.	Add SIP Entities	28
6.5.	Add Entity Links	31
6.6.	Add Routing Policies	32
6.7.	Add Dial Patterns	33
6.8.	Add/View Session Manager	34
7.	Configure Avaya Session Border Controller for Enterprise	36
7.1.	Avaya Session Border Controller for Enterprise Login	37
7.2.	Global Profiles	39
7.2.1.	Uniform Resource Identifier (URI) Groups	39
7.2.2.	Routing Profiles	40
7.2.3.	Topology Hiding	42
7.2.4.	Server Interworking	43
7.2.5.	Signaling Manipulation	47
7.2.6.	Server Configuration	48
7.3.	Domain Policies	51
7.3.1.	Application Rules	52
7.3.2.	Media Rules	53
7.3.3.	Signaling Rules	55
7.3.4.	Endpoint Policy Groups	60
7.3.5.	Session Policy	62
7.4.	Device Specific Settings	64

7.4.1. Network Management	64
7.4.2. Media Interface	65
7.4.3. Signaling Interface	66
7.4.4. End Point Flows - Server Flow	66
7.4.5. Session Flows	69
8. MTS Allstream SIP Trunking Service Configuration	70
9. Verification and Troubleshooting	70
10. Conclusion	74
11. References	74

1. Introduction

These Application Notes describe the steps to configure Session Initiation Protocol (SIP) Trunking between MTS Allstream SIP Trunking Service (from this point it will be referred as MTS Allstream for brevity) and an Avaya SIP-enabled enterprise solution. The Avaya solution consists of Avaya Aura® Communication Manager 6.0.1 configured as an Evolution Server, Avaya Aura® Session Manager 6.1, Avaya SBC for Enterprise (Avaya SBCE) 4.0.5 and various Avaya endpoints.

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

2. General Test Approach and Test Results

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

MTS Allstream is a member of the Avaya DevConnect Service Provider program. The general test approach is to connect a simulated enterprise to MTS Allstream via the public internet and exercise the features and functionality listed in **Section 2.1**.

2.1. Interoperability Compliance Testing

To verify MTS Allstream SIP Trunking Service interoperability, the following features and functionalities are covered during the compliance test:

- Response to SIP OPTIONS queries.
- Incoming PSTN call to various phone types including SIP, H.323, digital and analog telephone at the enterprise. All inbound calls from PSTN are routed to the enterprise across the SIP trunk from the service provider.
- Outgoing PSTN call from various phone types including SIP, H.323, digital and analog telephone at the enterprise. All outbound calls to PSTN are routed from the enterprise across the SIP trunk to the service provider.
- Inbound and outbound PSTN calls to/from Avaya one-X® Communicator (1XC) soft phone. Both the 1XC Computer Mode (where 1XC is used for call control as well as audio path) and the 1XC Telecommuter Mode (where 1XC is used for call control and a separate telephone is used for audio path) are tested. Both SIP and H.323 protocols are tested.
- Dialing plans including local, long distance, international, outbound toll-free, operator assisted calls, local directory assistance (411)... etc.
- Proper codec negotiation with G.729 and G.711MU codecs.

- DTMF tone transmissions as out-of-band RTP events as per RFC 2833.
- Caller ID presentation and Caller ID restriction.
- Response to incomplete call attempts and trunk errors.
- Voicemail navigation for inbound and outbound calls.
- Incoming and outgoing fax over IP with G.711MU codec.
- User features such as hold and resume, transfer and conference.
- Off-net call forwarding with SIP Diversion method.
- EC500 mobility (extension to cellular).
- Routing inbound vector call to call center agent queues.
- Network Call Redirection using reINVITE for transferring off-net of inbound calls back to PSTN.
- Session Timers implementation from both ends of the enterprise and the service provider.

Items that are not supported or not tested including the following:

- Inbound toll-free and outbound emergency calls (911) are supported but are not tested as part of the compliance test because MTS Allstream does not provide the necessary configuration.
- T.38 fax is not supported.
- Off-net call forwarding using History-Info method is not supported.

2.2. Test Results

Interoperability testing of MTS Allstream SIP Trunking Service with the Avaya SIP-enabled enterprise solution is completed with successful results for all test cases with the exception of the observations/limitations described below.

1. **Off-net blind transfer is not successful with REFER method.** In an inbound call scenario, Communication Manager receives an initial INVITE with REFER method present in Allow header. Communication Manager transfers off-net an inbound call to PSTN with a REFER request. MTS Allstream does not properly support REFER as it accepts the REFER with a SIP/202 message but the call transfer is not successful. Both call legs are still unexpectedly maintained after transfer is complete. This issue is corrected by disabling the **Network Call Redirection** flag on outgoing trunk group to make Communication Manager transfer the call with **reINVITE** request. The detail configuration is described in **Section 5.7**.
2. **Network Call Redirection is not successful with “302 Moved Temporarily”.** A vector DN is programmed to use “302 Moved Temporarily” to redirect an inbound call to PSTN before answering. MTS Allstream does not properly support “302 Moved Temporarily” as it sends an ACK to the “302 Moved Temporarily” but does not redirect the call to PSTN party specified in the Contact header.
3. **The untrusted Calling Party Name (CPN) from Communication Manager is not examined.** In an outbound call scenario, PSTN displays the original untrusted CPN from Communication Manager. MTS Allstream does not examine the CPN before sending to

PSTN. This is a known issue on MTS Allstream SIP Trunking Service and there is no available resolution at this time.

4. **The CPN for outbound call is not being displayed by PSTN.** In an outbound call scenario, Communication Manager sends both calling party name and number to PSTN. But in some cases, PSTN phone displays the calling party number only and no calling party name. In other cases, PSTN phone displays both calling party name and number. The calling party name may be overridden by MTS Allstream or by intermediate service providers that route the call through PSTN. This issue has low user impact and is listed here simply as an observation.
5. **Communication Manager extension holds an inbound call but the incoming audio traffic is still being sent by MTS Allstream.** To hold an inbound call, Communication Manager sends a reINVITE with a=sendonly in SDP. MTS Allstream responds with 200OK and a=recvonly in SDP which means that the incoming audio traffic to Communication Manager will be deactivated. But MTS Allstream still sends audio when the call is in “recvonly” state. This issue has low user impact, it is listed here simply as an observation.
6. **In an inbound call scenario, MTS Allstream does not refresh the Session Timer.** MTS Allstream sends an initial INVITE with *Session-Expires: 3600; refresher: uac Min-SE: 600*. It means, as a user agent client, MTS Allstream should refresh the Session Timer every 300 seconds by a reINVITE or UPDATE method. In the compliance test, Communication Manager does not receive any Session Timer refresh signaling. This is a known issue on MTS Allstream SIP Trunking Service and there is no available resolution at this time.
7. **Mismatched Media Format setting on trunk group causes audio path being delayed.** Configure Direct IP-IP Early Media setting on Communication Manager SIP signaling group to MTS Allstream to "n" and a setting of "y" for the general SIP signaling group used for internal enterprise and make an outbound call to PSTN. The wireshark trace shows that the Media Format for audio from Communication Manager is different than the Media Format expected by MTS Allstream even though it is configured to be the same. PSTN phone hears a series of tones and delayed audio from Communication Manager to PSTN. To avoid this problem, the Direct IP-IP Early Media setting on Communication Manager must be set identically on signaling group dedicated to MTS Allstream and on the general signaling group used for the internal enterprise SIP endpoints.
8. **Fax over IP using G.711MU codec is successful.** Communication Manager does not officially support fax call using G.711MU codec. However, in the compliance test the incoming and outgoing fax calls appear to work with G.711MU codec by setting “fax=off” in codec profile. The fax document is transmitted successfully with acceptable quality. Communication Manager handles the fax call like a regular voice call using G.711MU codec and it only supports this fax call in best effort. Note: the codec set

should have G.711MU codec as a first choice otherwise the fax call would not be successfully established. The codec set is configured in **Section 5.4** and **Section 7.3.5**.

9. **Off-net call transfer, the calling party name and number is not updated to PSTN parties.** Communication Manager extension transfers an incoming call off-net to PSTN. Communication Manager sends UPDATE with true connected calling party name and number to both PTSN parties. The calling party information is in the URI-User of Contact header. However, the calling party name and number have not been updated; the calling and called PTSN parties still display calling party number of Communication Manager extension. This is a known issue on MTS Allstream SIP Trunking Service. It is recommended that MTS Allstream should support the calling party information update. This feature also needs to be supported by the service provider hosting the PSTN parties. This issue has low user impact, it is listed here simply as an observation.
10. **Blind transfer by a SIP phone to local extension is not successful if Network Call Redirection setting is different for private and public trunk groups.** Communication Manager SIP phone blind transfers an inbound call to a local H.323 phone. The transfer fails because Communication Manager does not respond ACK to MTS Allstream. This issue is corrected by turning off the **Network Call Redirection** flag on both private outgoing trunk group which connects to Session Manager for internal SIP phone configuration and public outgoing trunk group which connects to MTS Allstream for PSTN calls. Then Communication Manager successfully transfers the call.
11. **Local calls from a Communication Manager extension (Phone1) routed via MTS Allstream to another Communication Manager extension (Phone2) results in no audio.** This problem is believed to have low user impact because all other local outgoing calls from the enterprise to PSTN (i.e. calls within the same area code) complete successfully with audio. Audio is only impacted when calling another Communication Manager via MTS Allstream. In general, these calls would be routed within the enterprise which avoids the problem. This failure scenario is also related to shuffling because if shuffling is disabled on the service provider trunk then there is no audio issue. However, it is not recommended to disable shuffling and the failing scenario avoided by routing these types of calls within the enterprise.
12. **Performing an “Application Restart” or editing the SigMa script on Avaya SBCE causes the SigMa script not working.** There is no resolution currently. If the SigMa script does not work after an “Application Restart” or editing, please contact Avaya SBCE support by telephone number 1-866-861-3113 or 1-214-269-2424.

2.3. Support

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

For technical support on MTS Allstream SIP Trunking Service, please contact MTS Allstream technical support at:

- Phone: 204-941-8557 or 1-800-542-8703
- Website: <http://www.mts.ca/mts/personal/support>

3. Reference Configuration

Figure 1 illustrates the sample Avaya SIP-enabled enterprise solution connected to the MTS Allstream SIP Trunking Service (Vendor Validation circuit) through a public Internet WAN connection.

For security purposes, the real public IP addresses and PSTN routable phone numbers used in the compliance test are not shown in these Application Notes.

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

- Avaya S8800 Servers running Avaya Aura® System Manager
- Avaya S8800 Servers running Avaya Aura® Session Manager
- Avaya S8800 Servers running Avaya Aura® Communication Manager
- Avaya G650 Media Gateway
- Avaya S8800 Server running Avaya Aura® Messaging
- Avaya Session Border Controller for Enterprise
- Avaya 9600-Series IP Telephones (SIP and H.323)
- Avaya one-X® Communicator soft phones (SIP and H.323)
- Avaya digital and analog telephones

Located at the edge of the enterprise network is Avaya SBCE. It has a public side that connects to MTS Allstream via internet and a private side that connects to the enterprise network. All SIP and RTP traffic entering or leaving the enterprise network flows through the Avaya SBCE which can protect the enterprise against any outside SIP-based attacks. Avaya SBCE provides network address translation at both the IP and SIP layers. The transport protocol between the Avaya SBCE and MTS Allstream across the public network is UDP; the transport protocol between the Avaya SBCE and Session Manager across the enterprise network is TCP.

In the compliance testing, the Avaya Customer-Premises Equipment (CPE) environment is configured with SIP domain **avaya.com** for the enterprise. Avaya SBCE is used to adapt the enterprise SIP domain to the IP address based URI-Host known to MTS Allstream. **Figure 1** below illustrates the network diagram for the enterprise. All voice application elements are connected to internal trusted LAN.

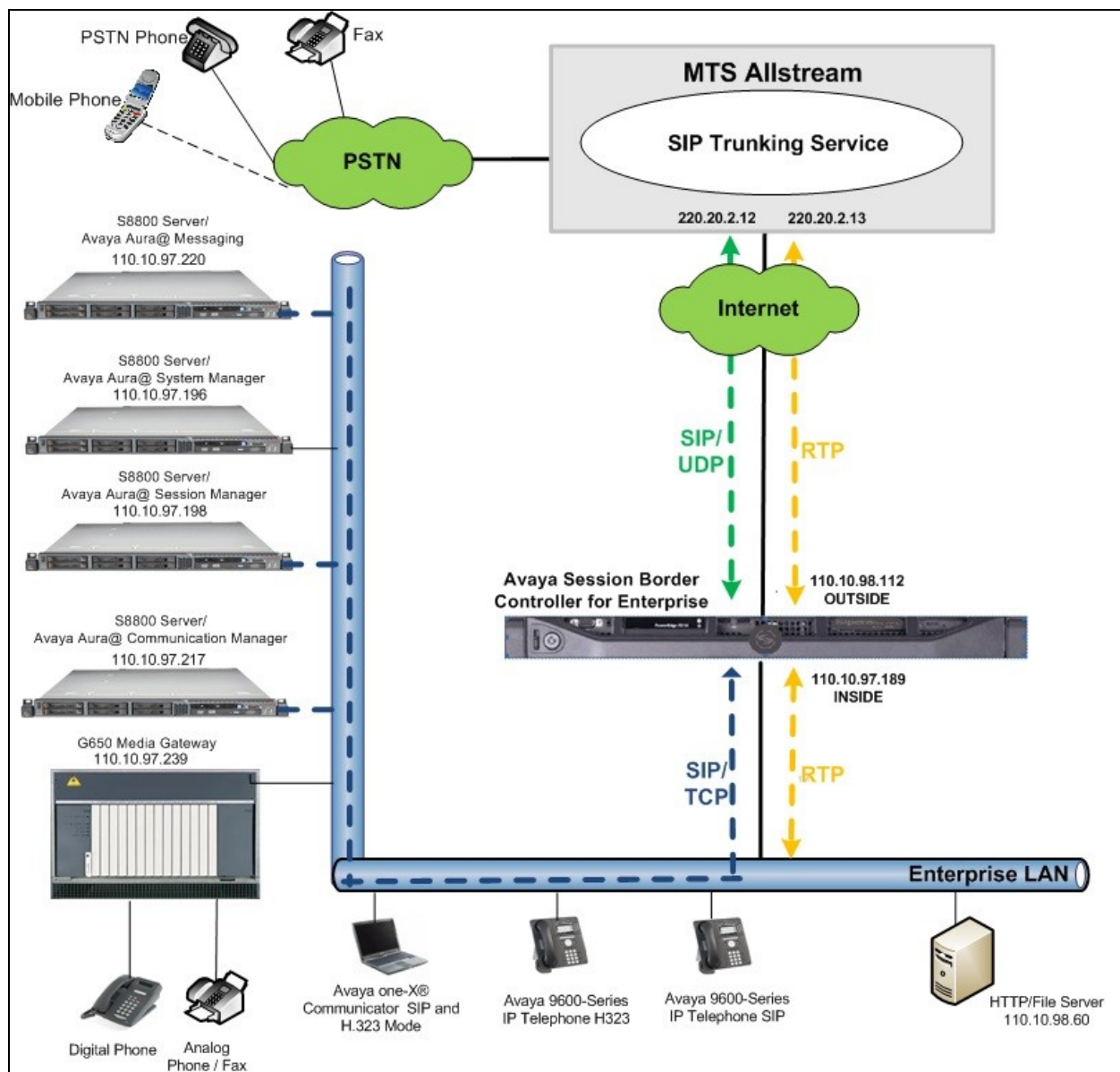


Figure 1: Avaya IP Telephony Network connecting to MTS Allstream SIP Trunking Service

4. Equipment and Software Validated

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

Avaya IP Telephony Solution Components	
Component	Release
Avaya Aura® Communication Manager running on an Avaya S8800 Server	6.0.1 (R016x.00.1.510.1-18621) (System Platform 6.0.3.0.3)
Avaya G650 Media Gateway	
IPSI TN2312BP	HW06 FW043
Control-LAN TN799DP	HW01 FW026
Medpro TN2302	HW20 FW117
Digital Line Card TN2224	000006
Analog Line Card TN746B	000019
Avaya Aura® System Manager running on an Avaya S8800 Server	6.1 (6.1.5.0) (System Platform 6.0.3.0.3)
Avaya Aura® Session Manager running on an Avaya S8800 Server	6.1 (6.1.1.0.611023)
Avaya Aura® Messaging running on an Avaya S8800 Server	6.1-11.0
Avaya Session Border Controller for Enterprise	4.0.5 Q09
Avaya 9640 IP Telephone (H.323)	Avaya one-X® Deskphone Edition 6.0.1
Avaya 9640 IP Telephone (SIP)	Avaya one-X® Deskphone SIP Edition R6_0_3-120511
Avaya one-X Communicator (SIP and H.323)	6.1.3.08-SP3-Patch2-35791
Avaya 1408 Digital Telephone	n/a
Avaya 6210 Analog Telephone	n/a
MTS Allstream SIP Trunking Service Components	
Component	Release
Genband S3	5.2.2.12
CS2K	CVM13

Table 1: Equipment and Software Tested

Note that this solution will be compatible with other Avaya Server and Media Gateway platforms running similar version of Communication Manager.

5. Configure Communication Manager

This section describes the procedure for configuring Communication Manager for inter-operating with the MTS Allstream.

Two separate SIP trunk groups are created between Communication Manager and Session Manager to carry traffic to and from service provider respectively. For inbound call, the call flows from the MTS Allstream to Avaya SBCE to Communication Manager via Session Manager. 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 call to PSTN is first processed by Communication Manager for outbound feature treatment such as automatic route selection and class of service restrictions. Once Communication Manager selected the proper SIP trunk, the call is routed to Session Manager toward Avaya SBCE for egress to the MTS Allstream.

For the compliance test, Communication Manager sends 11 digits in the destination headers (e.g., Request-URI and To) and sends 10 digit in the source headers (e.g., From, Contact, and P-Asserted-Identity (PAI)). MTS Allstream sends 10 digits in destination headers and 11 digits in source headers.

It is assumed the general installation of the Communication Manager and the Avaya G650 Media Gateway has been previously completed and is not discussed here.

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

5.1. Licensing and Capacity

Use the **display system-parameters customer-options** command to verify that the **Maximum Administered SIP Trunks** value on **Page 2** is sufficient to support the desired number of simultaneous SIP calls across all SIP trunks at the enterprise including any trunks to and from the service provider. The example shows that 24000 licenses are available and 222 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 sale representative to add the additional capacity or feature.

```

display system-parameters customer-options                               Page 2 of 11
                                OPTIONAL FEATURES

IP PORT CAPACITIES                                                    USED
    Maximum Administered H.323 Trunks: 12000 0
    Maximum Concurrently Registered IP Stations: 18000 5
    Maximum Administered Remote Office Trunks: 12000 0
    Maximum Concurrently Registered Remote Office Stations: 18000 0
    Maximum Concurrently Registered IP eCons: 414 0
    Max Concur Registered Unauthenticated H.323 Stations: 100 0
    Maximum Video Capable Stations: 18000 2
    Maximum Video Capable IP Softphones: 18000 3
    Maximum Administered SIP Trunks: 24000 222
    Maximum Administered Ad-hoc Video Conferencing Ports: 24000 0
    Maximum Number of DS1 Boards with Echo Cancellation: 522 0
    Maximum TN2501 VAL Boards: 128 1
    Maximum Media Gateway VAL Sources: 250 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

(NOTE: You must logoff & login to effect the permission changes.)

```

5.2. System Features

Use the **change system-parameters features** command to set the **Trunk-to-Trunk Transfer** field to **all** to allow incoming call from PSTN to be transferred to another PSTN endpoint. If for security reasons, incoming call should not be allowed to transfer back to 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. The compliance test used the value of **AV-Restricted** for restricted call and **AV-Unavailable** for unavailable call.

```

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

CPN/ANI/ICLID PARAMETERS
    CPN/ANI/ICLID Replacement for Restricted Calls: AV-Restricted
    CPN/ANI/ICLID Replacement for Unavailable Calls: AV-Unavailable

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

```

5.3. IP Node Names

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

change node-names ip		Page 1 of 2
IP NODE NAMES		
Name	IP Address	
AURAGateway	110.10.97.193	
DevASM	110.10.97.198	
IPMedia01A08	110.10.97.239	
default	0.0.0.0	
procr	110.10.97.217	
procr6	::	

5.4. Codecs

Use the **change ip-codec-set** command to define a list of codecs to be used for calls between the enterprise and the service provider. This compliance test used ip-codec-set 3. MTS Allstream supports G.729 and G.711MU. To use these codecs, enter G.711MU and G.729 in the **Audio Codec** column of the table in the order of preference. Default values can be used for all other fields.

The following screen shows the configuration for ip-codec-set 3. During testing, the codec set specifications are varied to test for individual codec support as well as codec negotiation between the enterprise and the network at call setup time.

change ip-codec-set 3				Page 1 of 2
IP Codec Set				
Codec Set: 3				
Audio Codec	Silence Suppression	Frames Per Pkt	Packet Size (ms)	
1: G.711MU	n	2	20	
2: G.729	n	2	20	
3:				

MTS Allstream only supports fax using G.711MU codec in the compliance test. The T.38 faxing is not currently supported. Communication Manager does not officially support fax call using G.711MU codec. However, incoming and outgoing fax call using G.711MU codec appeared to work during testing when configuring fax = off. Communication Manager handles the call like a regular voice call and only supports fax call using G.711MU codec in best effort. Note that the

codec profile should have G.711MU codec as a first choice otherwise the fax call would not be successfully established.

To use G.711MU codec for fax, set the **Fax Mode** to **off** on **Page 2**.

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

Note: To successfully send and receive fax using G.711MU codec, the voice call has to be established with G.711MU codec. The **Session Policy** configuration on Avaya SBCE in **Section 7.3.5** will ensure G.711MU is the first choice in the preference codec.

5.5. IP Network Region

A separate IP network region for the service provider trunk groups is created. This allows separate codec or quality of service setting to be used (if necessary) for call between the enterprise and the service provider versus call within the enterprise or elsewhere. For the compliance test, ip-network-region 3 is created by the **change ip-network-region 3** command with the following parameters:

- Set the **Authoritative Domain** field to match the SIP domain of the enterprise. In the compliance test, the domain name is **avaya.com** as assigned to the test environment in the Avaya test lab. This domain name appears in the “From” header of SIP message originating from this IP region. **Note:** In the compliance test, the Topology-Hiding configuration on Avaya SBCE in **Section 7.2.3** is used to convert this private domain name to the public IP Address of the Avaya SBCE for the URI-Host portion in From and PAI headers.
- 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 under 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 19

IP NETWORK REGION

Region: 3
 Location: 1 **Authoritative Domain: avaya.com**
 Name: MTS Allstream
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 RTCP Reporting Enabled? y
 Call Control PHB Value: 46 **RTCP MONITOR SERVER PARAMETERS**
 Audio PHB Value: 46 Use Default Server Parameters? y
 Video PHB Value: 26
802.1P/Q PARAMETERS
 Call Control 802.1p Priority: 6
 Audio 802.1p Priority: 6
 Video 802.1p Priority: 5 **AUDIO RESOURCE RESERVATION PARAMETERS**
H.323 IP ENDPOINTS RSVP Enabled? n
 H.323 Link Bounce Recovery? y
 Idle Traffic Interval (sec): 20
 Keep-Alive Interval (sec): 5
 Keep-Alive Count: 5

On **Page 4**, define the IP codec set to be used for traffic between region 3 and other regions. In the compliance test, Communication Manager, G650 Media Gateway, IP phones, Session Manager and Avaya SBCE are assigned to the same region 3. To configure IP codec set between regions, enter the desired IP codec set in the **codec set** column of the table with appropriate destination region (**dst rgn**). Default values may be used for all other fields. The example below shows codec set 3 will be used for call between region 3 and other regions.

change ip-network-region 1
Page 4 of 19

Source Region: 3		Inter Network Region Connection Management					I	M
dst rgn	codec set	direct	WAN Units	WAN-BW-limits	Video	Intervening	Dyn CAC	G A G L
1	3							all
2	3	y	NoLimit				n	t
3	3	y	NoLimit				n	t
4								

Non-IP telephones (e.g., analog, digital) derive network region from IP interface Medpro card of Avaya G650 Media Gateway to which the device is connected. IP telephones can be assigned a network region based on an IP address mapping.

For the compliance test, devices with IP addresses in the 110.10.97.0/24 subnet are assigned to network region 3. These include Communication Manager, Medpro card of Avaya G650 Media Gateway, Session Manager and Avaya SBCE that are set up for the test environment. IP telephones used for the compliance test, including both the Avaya 9600 IP Telephones and the Avaya one-X® Communicator soft phones are assigned to network region 3 with IP address in the 110.10.98.0/24 subnet.

The following screen illustrates a subset of the IP network map configuration used to verify in the compliance test.

change ip-network-map				Page 1 of 63	
IP ADDRESS MAPPING					
IP Address	Subnet Bits	Network Region	VLAN	Emergency Location	Ext
FROM: 110.10.97.0	/24	3	n		
TO: 110.10.97.255					
FROM: 110.10.98.0	/24	3	n		
TO: 110.10.98.255					
FROM:	/		n		
TO:					

Next step is to allocate the resource on Communication Manager for IP network region 3. For the SIP Trunk, the IP interface **procr** is used to process SIP signaling and Medpro card of Avaya G650 Media Gateway is used to process media. Both IP interfaces have to be assigned under the same region 3.

To define network region 3 for ip interface **procr**, use **change ip-interface procr** command as shown in the following screen.

change ip-interface procr		Page 1 of 2
IP INTERFACES		
Type: procr	Target socket load: 19660	
Enable Interface? y	Allow H.323 Endpoints? y	Allow H.248 Gateways? y
Network Region: 3	Gatekeeper Priority: 5	
IPV4 PARAMETERS		
Node Name: procr	IP Address: 110.10.97.217	
Subnet Mask: /26		

To define network region 3 for ip interface of Medpro card, use **change ip-interface 01A08** command as shown in the following table. **Note:** 01A08 is the physical position of the Medpro card on the Avaya G650 Media Gateway; it is at cabinet 1, carrier A and slot 8.

change ip-interface 01A08		Page 1 of 3
IP INTERFACES		
Type: MEDPRO Slot: 01A08 Code/Suffix: TN2302 Enable Interface? y VLAN: n Network Region: 3		
IPV4 PARAMETERS		
Node Name: IPMedia01A08	IP Address: 110.10.97.239	
Gateway Node Name: AURAGateway	IP Address: 110.10.97.193	
Subnet Mask: /26		

5.6. Signaling Group

Use the **add signaling-group** command to create two signaling groups between Communication Manager and Session Manager, one for inbound calls from the service provider network and other for outgoing calls from the enterprise.

For the compliance test, signaling group 6 is created for inbound calls from the service provider and is configured as follows:

- Set the **Group Type** field to **sip**.
- Set the **IMS Enabled** field to **n**.
- Set the **Transport Method** to **tcp**. The transport method specified here is used between the Communication Manager and Session Manager.
- Set the **Near-end Listen Port** and **Far-end Listen Port** to **5090** (the well-known port value for SIP/TCP is 5060).
- Set the **Peer Detection Enabled** field to **y**. The **Peer-Server** field will initially be set to **Others**. 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 interface of **procr** defined in **Section 5.3**.
- Set the **Far-end Node Name** to **DevASM**. 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 3 defined for the service provider in **Section 5.5**.
- Set the **Far-end Domain** to blank.
- Set the **DTMF over IP** field to **rtp-payload**. This setting enables Communication Manager to send DTMF transmissions using RFC 2833.
- Set **Enable Layer 3 Test?** to **y**. This setting allows Communication Manager to send OPTIONS heartbeat to Session Manager on the trunk group.
- 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. If this value is set to **n**, then Avaya Media Gateway will remain in the media path between the SIP trunk and the endpoint for the

duration of the call. Depending on the number of media resources available in the Avaya Media Gateway, these resources may be depleted during high call volume preventing additional calls from completing.

- Verify that the **Direct IP-IP Early Media** is set to the same value of the signaling group used for the enterprise site. The default setting for this field is **n**. See the **Media Format** bullet item in **Section 2.2** observation #7 for more information.
- Change default setting of **6** for **Alternate Route Timer (sec)** to **12**. This allows more time for inbound PSTN calls to complete through MTS Allstream.
- Default values may be used for all other fields.

add signaling-group 6		Page 1 of 1
SIGNALING GROUP		
Group Number: 6	Group Type: sip	
IMS Enabled? n	Transport Method: tcp	
Q-SIP? n	SIP Enabled LSP? n	
IP Video? n	Enforce SIPS URI for SRTP? y	
Peer Detection Enabled? n	Peer Server: Others	
Near-end Node Name: procr	Far-end Node Name: AvayaSBCE	
Near-end Listen Port: 5090	Far-end Listen Port: 5090	
	Far-end Network Region: 3	
Far-end Domain:		
Incoming Dialog Loopbacks: eliminate	Bypass If IP Threshold Exceeded? n	
DTMF over IP: rtp-payload	RFC 3389 Comfort Noise? n	
Session Establishment Timer(min): 3	Direct IP-IP Audio Connections? y	
Enable Layer 3 Test? y	IP Audio Hairpinning? n	
H.323 Station Outgoing Direct Media? n	Initial IP-IP Direct Media? n	
	Alternate Route Timer(sec): 12	

The signaling group for outbound calls from the enterprise to PSTN is similarly configured except that the Far-end Domain is set to **avaya.com**. This domain will be manipulated by Avaya SBCE to IP address in URI-Host that is known to MTS Allstream. For the compliance test, signaling group 7 is created and is shown below.

add signaling-group 7		Page 1 of 1
SIGNALING GROUP		
Group Number: 7	Group Type: sip	
IMS Enabled? n	Transport Method: tcp	
Q-SIP? n	SIP Enabled LSP? n	
IP Video? n	Enforce SIPS URI for SRTP? y	
Peer Detection Enabled? n Peer Server: Others		
Near-end Node Name: procr	Far-end Node Name: AvayaSBCE	
Near-end Listen Port: 5090	Far-end Listen Port: 5090	
	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? y	IP Audio Hairpinning? n	
H.323 Station Outgoing Direct Media? n	Initial IP-IP Direct Media? n	
	Alternate Route Timer(sec): 12	

5.7. Trunk Group

Use the **add trunk-group** command to create trunk group for the two signaling groups created in **Section 5.6**. For the compliance test, trunk group 6 is configured for incoming calls and trunk group 7 is configured for outgoing calls as follows:

- Set the **Group Type** field to **sip**.
- Enter a descriptive name for the **Group Name**.
- Enter an available trunk access code (TAC) that is consistent with the existing dial plan in the **TAC** field.
- Set the **Direction** field to **incoming** for trunk group 6 and **outgoing** for trunk group 7.
- Set the **Outgoing Display** to **y** to enable name display on the trunk.
- Set the **Service Type** field to **public-ntwrk**.
- Set the **Signaling Group** to the signaling group shown in **Section 5.6**. The incoming trunk group 6 is set to incoming signaling group 6 and the outgoing trunk group 7 is set to outgoing signaling group 7.
- Set the **Number of Members** field to 32. It is the number of trunk members in the SIP trunk group. This value determines how many simultaneous SIP calls can be supported by this trunk.
- Default values are used for all other fields.

add trunk-group 6		Page 1 of 21	
TRUNK GROUP			
Group Number: 6	Group Type: sip	CDR Reports: y	
Group Name: MTS_INBOUND_TRUNK	COR: 1	TN: 1	TAC: 8006
Direction: incoming	Outgoing Display? y	Night Service:	
Dial Access? n			
Service Type: public-ntwrk	Auth Code? n		
	Member Assignment Method: auto		
	Signaling Group: 6		
	Number of Members: 32		

On **Page 2**, verify that the **Preferred Minimum Session Refresh Interval (sec)** is set to a value acceptable to service provider. This value defines the interval a re-INVITEs must be sent to keep an active session alive. For the compliance test, a default value of **600** seconds is used.

add trunk-group 6		Page 2 of 21	
Group Type: sip			
TRUNK PARAMETERS			
Unicode Name: auto			
Redirect On OPTIM Failure: 5000			
SCCAN? n	Digital Loss Group: 18		
	Preferred Minimum Session Refresh Interval(sec): 600		
Disconnect Supervision - In? y			

On **Page 3**, set the **Numbering Format** field to **private**. This field specifies the format of the CPN sent to the far-end. Beginning with Communication Manager 6.0, public numbers are automatically preceded with a + sign when passed in the From, Contact and P-Asserted Identity headers. The addition of the + sign impacted interoperability with service provider. Thus, the **Numbering Format** is set to **private** and the **Numbering Format** in the route pattern is 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 endpoint to be replaced with the value set in **Section 5.2**, if inbound call enabled CPN block. Default values are used for all other fields.

add trunk-group 6		Page 3 of 21
TRUNK FEATURES		
ACA Assignment? n	Measured: none	Maintenance Tests? y
Numbering Format: private		
UI Treatment: service-provider		
Replace Restricted Numbers? y		
Replace Unavailable Numbers? y		
Show ANSWERED BY on Display? y		

On **Page 4**, the **Network Call Redirection** field can be set to **y**. The setting of **Network Call Redirection** flag to **y** enables use of the SIP REFER message to transfer an incoming call to a vector number back to PSTN.

- Set the **Send Diversion Header** field to **y**. This field provides additional information to the network if the call has been re-directed. This is needed to support call forwarding of inbound call back to PSTN and Extension to Cellular (EC500) call scenario.
- Set the **Support Request History** field to **n**. This parameter determines if History-Info header will be excluded in the call-redirection INVITE from the enterprise.
- Set the **Telephone Event Payload Type** to **101**, the value is preferred by MTS Allstream.
- Set the **Convert 180 to 183 for Early Media** field to **y**.

add trunk-group 6		Page 4 of 21
PROTOCOL VARIATIONS		
Mark Users as Phone? n		
Prepend '+' to Calling Number? n		
Send Transferring Party Information? n		
Network Call Redirection? y		
Send Diversion Header? y		
Support Request History? n		
Telephone Event Payload Type: 101		
Convert 180 to 183 for Early Media? y		
Always Use re-INVITE for Display Updates? n		
Identity for Calling Party Display: P-Asserted-Identity		
Enable Q-SIP? n		

For outgoing trunk group configuration, the screen below shows **Page 1** of trunk group 7 for outgoing calls from the enterprise to MTS Allstream.

add trunk-group 7		Page 1 of 21	
TRUNK GROUP			
Group Number: 7	Group Type: sip	CDR Reports: y	
Group Name: MTS_OUTBOUND_TRUNK	COR: 1	TN: 1	TAC: 8007
Direction: outgoing	Outgoing Display? y		
Dial Access? n			
Queue Length: 0			
Service Type: public-ntwrk			
		Member Assignment Method: auto	
		Signaling Group: 7	
		Number of Members: 32	

On Page 4 of trunk group 7, the **Network Call Redirection** is set to “n”.

add trunk-group 7		Page 4 of 21	
PROTOCOL VARIATIONS			
Mark Users as Phone? n			
Prepend '+' to Calling Number? n			
Send Transferring Party Information? n			
Network Call Redirection? n			
Send Diversion Header? y			
Support Request History? n			
Telephone Event Payload Type: 101			

Note: **Network Call Redirection** is set to “n”. This setting is used to reINVITE an off-net transfer for an incoming call back to PSTN. For more information, please refer to **Section 2.2**, observation #1.

The configuration on other pages of trunk group 7 is identical to trunk group 6.

5.8. Calling Party Information

The calling party number is sent in the SIP “From”, “Contact” and “PAI” headers. Since private numbering is selected to define the format of this number (**Section 5.7**), use the **change private-numbering** command to create an entry for each extension which has a DID assigned. The DID numbers are provided by service provider. They are used to authenticate the caller.

Normally DID number is comprised of the local extension plus a prefix. A single private numbering entry can be applied for all extensions. In the example below, all stations with a 7-digit extension beginning with **776** when receiving or calling call on trunk group 6 or 7 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		
7	776	6-7	647	10		
					Total Administered: 4	
					Maximum Entries: 540	

Even though private numbering is selected, currently the number used in the SIP Diversion header is derived from the public unknown numbering table and not the private numbering table. As a workaround for this, the entries in the private numbering table must be repeated in the public unknown numbering table.

change public-unknown-numbering 0					Page 1 of 2
NUMBERING - PUBLIC/UNKNOWN FORMAT					
Ext	Ext	Trk	CPN	Total	
Len	Code	Grp(s)	Prefix	CPN	
				Len	
7	776	6-7	647	10	Total Administered: 12
					Maximum Entries: 240

5.9. Outbound Routing

In these Application Notes, the **Automatic Route Selection (ARS)** feature is used to route outbound call via the SIP trunk to service provider. In the compliance test, a single digit 9 is used as the ARS access code. Enterprise caller will dial 9 to reach an outside line. To define feature access code (**fac**) 9, use the **change dialplan analysis** command as shown in the table below.

change dialplan analysis										Page 1 of 12
DIAL PLAN ANALYSIS TABLE										
Location: all										Percent Full: 0
	Dialed	Total	Call	Dialed	Total	Call	Dialed	Total	Call	
	String	Length	Type	String	Length	Type	String	Length	Type	
	6	1	fac							
	776	7	ext							
	9	1	fac							
	*	4	dac							
	#	4	fac							

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

change feature-access-codes			Page 1 of 8
FEATURE ACCESS CODE (FAC)			
Abbreviated Dialing List1 Access Code:			
Abbreviated Dialing List2 Access Code:			
Abbreviated Dialing List3 Access Code:			
Abbreviated Dial - Prgm Group List Access Code:			
Announcement Access Code: #007			
Answer Back Access Code:			
Attendant Access Code:			
Auto Alternate Routing (AAR) Access Code: 6			
Auto Route Selection (ARS) - Access Code 1: 9			Access Code 2:
Automatic Callback Activation:			Deactivation:
Call Forwarding Activation Busy/DA:			Deactivation:
Call Forwarding Enhanced Status:			Deactivation:

Use the **change ars analysis** command to configure the routing of dialed digits following the first digit 9. The example below shows a subset of the dialed strings tested as part of the

compliance test. See **Section 2.1** for the complete list of call types tested. All dialed strings are mapped to route pattern 7 for outbound call 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:	0	
	Dialed String	Total Min	Max	Route Pattern	Call Type	Node Num	ANI Req'd		
0		1	18	7	pubu		n		
011		13	24	7	intl		n		
1		11	11	7	fnpa		n		
411		3	3	7	svcl		n		
416		10	10	7	pubu		n		
647		10	10	7	pubu		n		

As being mentioned above, the route pattern defines which trunk group will be used for the outgoing calls and performs any necessary digit manipulation. Use the **change route-pattern** command to configure the parameters for route pattern 7 in the following manner.

- **Pattern Name:** Enter a descriptive name.
- **Grp No:** Enter the outbound trunk group for the SIP service provider. For the compliance test, trunk group 7 is 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:** The prefix mark (Pfx Mrk) of 1 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 the long distance North American Numbering Plan (NANP) numbers. All HNPA 10 digit numbers are left unchanged.
- **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 5.8**.

change route-pattern 7												Page	1 of	3						
Pattern Number: 7												Pattern Name: MTS Outgoing								
SCCAN? n												Secure SIP? n								
Grp	FRL	NPA	Pfx	Hop	Toll	No.	Inserted					DCS/	IXC							
No			Mrk	Lmt	List	Del	Digits					QSIG								
												Dgts								
1:	7	0	1									Intw								
2:												n	user							
3:												n	user							
4:												n	user							
5:												n	user							
6:												n	user							
BCC VALUE												TSC	CA-TSC	ITC	BCIE	Service/Feature	PARM	No.	Numbering	LAR
0 1 2 M 4 W													Request					Dgts	Format	
																		Subaddress		
1:	y	y	y	y	y	n	n	rest						unk-unk	none					
2:	y	y	y	y	y	n	n	rest							none					

5.10. Incoming Call Handling

When an incoming call arrives, Communication Manager applies incoming handling treatment on incoming trunk group 6 (created in **Section 5.7**). MTS Allstream sends 10 digits in Request-URI and To headers identical to the assigned DID number. The incoming call handling treatment will translate this DID number to an extension. In the compliance test, the DID numbers have prefix 647 which are deleted to normalize the incoming number to match 7 digits extension on Communication Manager.

Use the **inc-call-handling-trmt trunk-group 6** command to define an incoming handling for MTS Allstream. Following table shows the configuration in detail on incoming trunk group 6.

change inc-call-handling-trmt trunk-group 6				Page	1 of 30
INCOMING CALL HANDLING TREATMENT					
Service/	Number	Number	Del	Insert	
Feature	Len	Digits			
public-ntwrk	10	647776		3	

5.11. Saving Communication Manager Configuration Changes

The command “**save translation all**” can be used to save the configuration changes made on Communication Manager.

6. Configure Avaya Aura® Session Manager

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

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

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

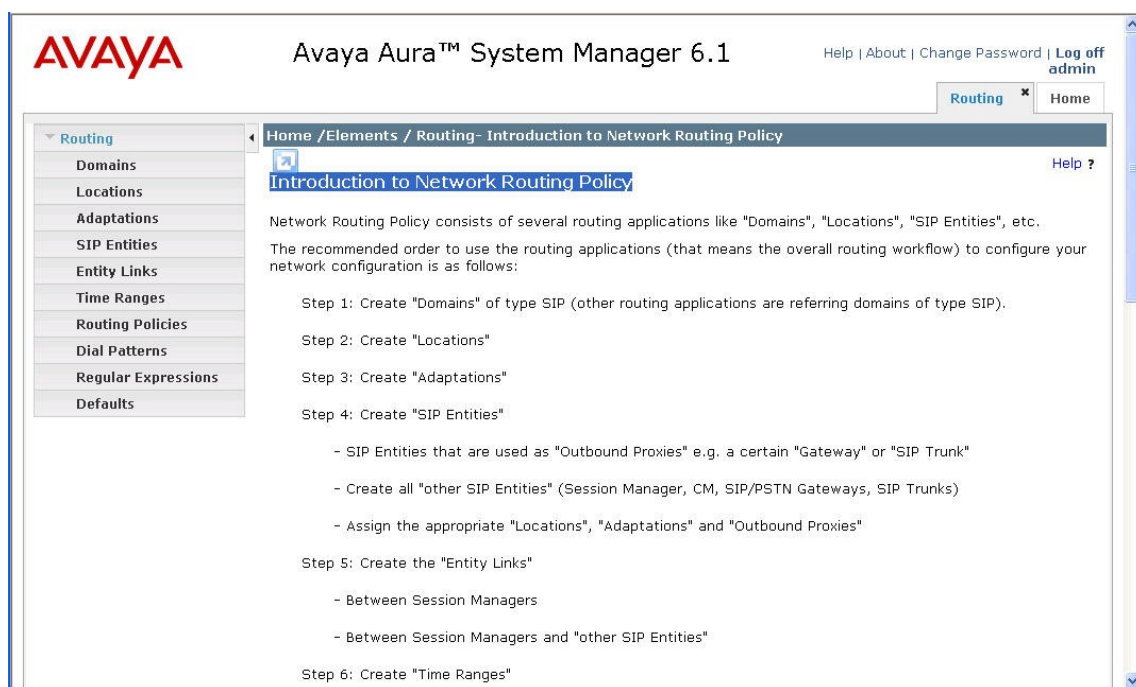
6.1. System Manager Login and Navigation

Session Manager configuration is accomplished by accessing the Web GUI of System Manager, using the URL “https://<ip-address>/SMGR”, where “<ip-address>” is the IP address of System Manager. At the **System Manager Log On** screen, provide the appropriate credentials and click on **Login** (not shown). The initial screen shown below is then displayed.



Most of the configuration items are performed in the Routing element. Click on **Routing** in the **Elements** column to bring up the **Introduction to Network Routing Policy** screen.

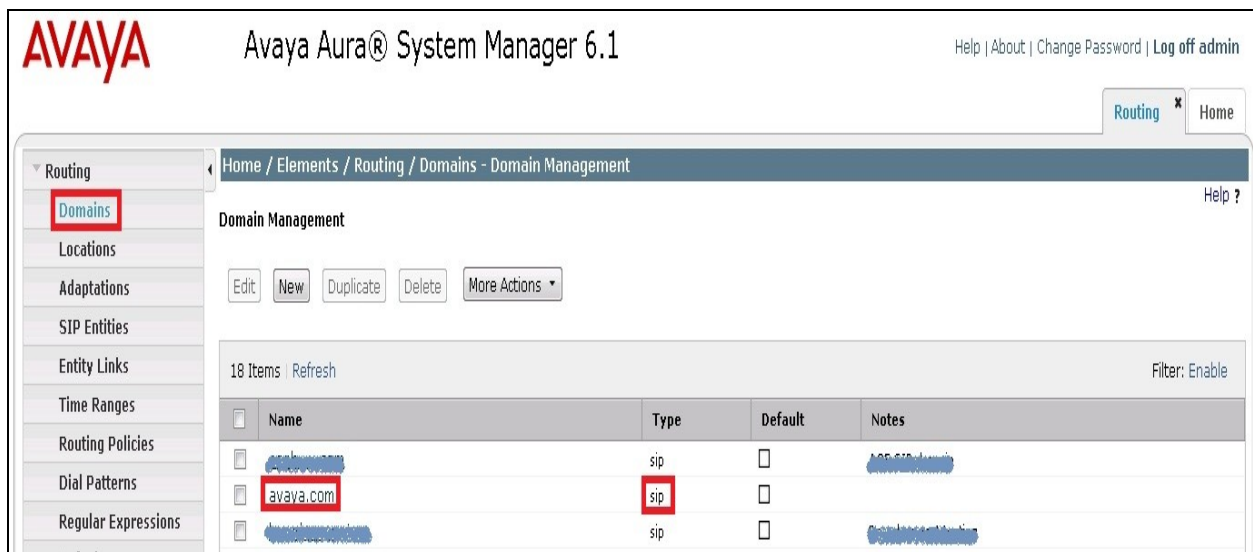
The navigation tree displayed in the left pane will be referenced in subsequent sections to navigate to items requiring configuration.



6.2. Specify SIP Domain

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

The following screen shows the list of configured SIP domains. The domain **avaya.com** is already being used for communication among a number of Avaya systems and applications, including an Avaya Aura® Messaging system with SIP integration to Session Manager. The domain **avaya.com** is not known to the MTS Allstream. Later on, it will be adapted by Avaya SBCE to IP address based URI-Host to meet the SIP specification of MTS Allstream.



6.3. Add Location

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

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

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

In the **Location Pattern** section (see the screen below), click **Add** and enter the following values:

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

Displayed below are the screenshot for **Belleville** location, which includes all equipment on the **110.10.x.x** subnet including Communication Manager, Session Manager and Avaya SBCE. Click **Commit** to save.

Avaya Aura® System Manager 6.1

Help | About | Change Password | Log off admin

Routing * Home

Home / Elements / Routing / Locations - Location Details

Location Details

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

General

* Name: Belleville

Notes: Belleville DevConnect lab

Overall Managed Bandwidth

Managed Bandwidth Units: Kbit/sec

Total Bandwidth: 1000000

Per-Call Bandwidth Parameters

* Default Audio Bandwidth: 80 Kbit/sec

Location Pattern

Add Remove

5 Items Refresh Filter: Enable

IP Address Pattern	Notes
110.10..*	

6.4. Add SIP Entities

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

To add a new SIP Entity, navigate to **Routing** → **SIP Entities** in the left navigation pane and click on the **New** button in the right pane (not shown).

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

- **Name:** Enter a descriptive name.
- **FQDN or IP Address:** Enter the FQDN or IP address of the SIP Entity that is used for SIP signaling.
- **Type:** Select **Session Manager** for Session Manager, **CM** for Communication Manager and **Other** for the Avaya SBCE.
- **Location:** Select one of the locations defined previously in **Section 6.3**.
- **Time Zone:** Select the time zone for the location above.

The following screen shows the addition of Session Manager SIP Entity. The IP address of the Session Manager signaling interface is entered for **FQDN or IP Address**.

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

Routing * Home

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

SIP Entity Details Commit Cancel Help ?

General

* Name: DevASM

* FQDN or IP Address: 110.10.97.198

Type: Session Manager

Notes: For Session Manager

Location: Belleville

Outbound Proxy:

Time Zone: America/Toronto

Credential name:

SIP Link Monitoring

SIP Link Monitoring: Use Session Manager Configuration

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

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

- **Port:** Port number on which the Session Manager can listen for SIP requests.
- **Protocol:** Transport protocol to be used to send SIP requests.
- **Default Domain:** The domain used for the enterprise.

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

The compliance test used **Port** entry **5090** with **TCP** for connecting to Communication Manager and Avaya SBCE.

Port

Add Remove

9 Items Refresh Filter: Enable

	Port	Protocol	Default Domain	Notes
<input type="checkbox"/>	15060	TLS		
<input type="checkbox"/>	5060	TCP		
<input type="checkbox"/>	5060	UDP		
<input type="checkbox"/>	5061	TLS		
<input type="checkbox"/>	5062	TCP		
<input type="checkbox"/>	5071	TLS		
<input type="checkbox"/>	5080	TCP		
<input type="checkbox"/>	5081	TCP		
<input type="checkbox"/>	5090	TCP	avaya.com	MTS_Allstream

Select : All, None

* Input Required Commit Cancel

The following screen shows the addition of Communication Manager SIP Entities. In order for Session Manager to send SIP traffic on an entity link to Communication Manager, it is necessary to create a SIP Entity for Communication Manager. The **FQDN or IP Address** field is set to the IP address of Communication Manager. Select **Type** is **CM**.

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

Routing Home

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

SIP Entity Details Commit Cancel Help ?

General

* Name: DevCM217_TCP_5090

* FQDN or IP Address: 110.10.97.217

Type: CM

Notes: MTS Allstream

Adaptation:

Location: Belleville

Time Zone: America/Toronto

Override Port & Transport with DNS SRV: ☐

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

Credential name:

Call Detail Recording: none

SIP Link Monitoring: Use Session Manager Configuration

The following screen shows the addition of the SIP Entity for Avaya SBCE. The **FQDN or IP Address** field is set to the IP address of its private network interface (see **Figure 1**). Select **Type** as **Other**.

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

Routing Home

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

SIP Entity Details Commit Cancel Help ?

General

* Name: AvayaSBCE_TCP_5090

* FQDN or IP Address: 110.10.97.189

Type: Other

Notes: MTS Allstream

Adaptation:

Location: Belleville

Time Zone: America/Toronto

Override Port & Transport with DNS SRV: ☐

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

Credential name:

Call Detail Recording: none

SIP Link Monitoring: Use Session Manager Configuration

6.5. Add Entity Links

A SIP trunk between Session Manager and a telephony system is described by an Entity Link. During compliance testing two Entity Links are created, one for Communication Manager and the other for Avaya SBCE. To add an Entity Link, navigate to **Routing → Entity Links** in the left navigation pane and click on the **New** button in the right pane (not shown). Fill in the following fields in the new row that is displayed:

- **Name:** Enter a descriptive name.
- **SIP Entity 1:** Select the Session Manager.
- **Protocol:** Select the transport protocol used for this link.
- **Port:** Port number on which Session Manager will receive SIP requests from the far-end. For Communication Manager, this must match the **Far-end Listen Port** defined on the Communication Manager signaling group in **Section 5.6**.
- **SIP Entity 2:** Select the name of the other system. For Communication Manager, select the Communication Manager SIP Entity defined in **Section 6.4**. For Avaya SBCE, select the Avaya SBCE SIP Entity defined in **Section 6.4**.
- **Port:** Port number on which the other system receives SIP requests from the Session Manager. For the Communication Manager, this must match the **Near-end Listen Port** defined on the Communication Manager signaling group in **Section 5.6**.
- **Connection Policy:** Select **Trusted**. Note: If this is not selected, calls from the associated SIP Entity specified in **Section 6.4** will be denied.
- Click **Commit** to save.

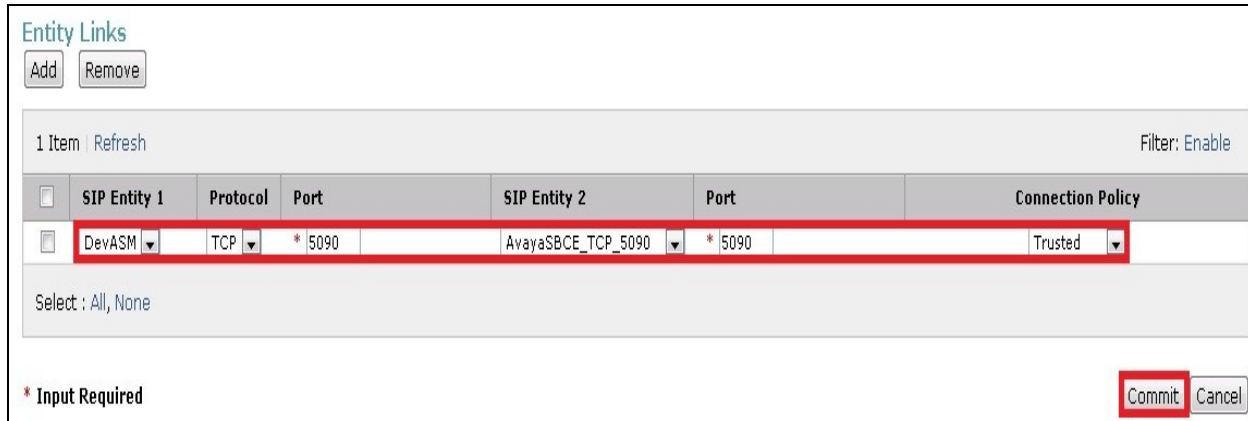
The following screens illustrate the Entity Links to Communication Manager and Avaya SBCE. For the compliance test, transport protocol TCP and port 5090 are used to match the values used on the Communication Manager signaling group form in **Section 5.6** and in **Figure 1**.

Entity Link to Communication Manager:

The screenshot shows the 'Entity Links' configuration page. At the top, there are 'Add' and 'Remove' buttons. Below them, a table lists the entity links. The table has columns for 'SIP Entity 1', 'Protocol', 'Port', 'SIP Entity 2', 'Port', and 'Connection Policy'. A single row is displayed, with the following values: 'DevASM' for SIP Entity 1, 'TCP' for Protocol, '* 5090' for Port, 'DevCM217_TCP_5090' for SIP Entity 2, '* 5090' for Port, and 'Trusted' for Connection Policy. The row is highlighted with a red border. Below the table, there is a 'Select : All, None' option. At the bottom right, there are 'Commit' and 'Cancel' buttons. A red box highlights the 'Commit' button. A note at the bottom left states '* Input Required'.

SIP Entity 1	Protocol	Port	SIP Entity 2	Port	Connection Policy
DevASM	TCP	* 5090	DevCM217_TCP_5090	* 5090	Trusted

Entity Link to Avaya SBCE:



The 'Entity Links' screen shows a table with one item. The table has columns for SIP Entity 1, Protocol, Port, SIP Entity 2, Port, and Connection Policy. The first row is highlighted with a red border. Below the table is a 'Select' dropdown menu. At the bottom right are 'Commit' and 'Cancel' buttons.

SIP Entity 1	Protocol	Port	SIP Entity 2	Port	Connection Policy
DevASM	TCP	* 5090	AvayaSBCE_TCP_5090	* 5090	Trusted

Select : All, None

* Input Required

Commit Cancel

6.6. Add Routing Policies

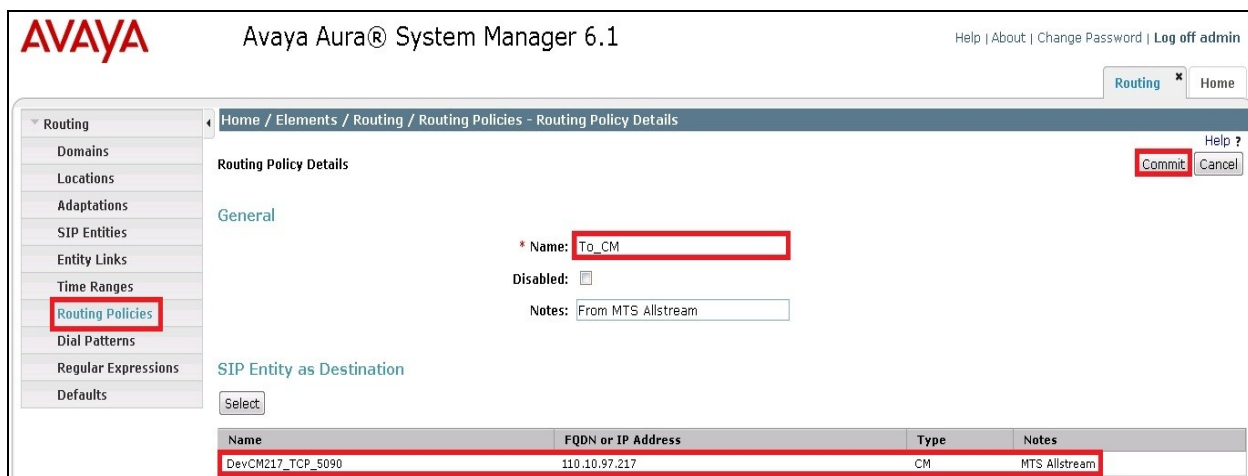
Routing policies describe the conditions under which calls will be routed to the SIP Entities specified in **Section 6.4**. Two routing policies must be added, one for Communication Manager and the other for Avaya SBCE. To add a routing policy, navigate to **Routing → Routing Policies** in the left navigation pane and click on the **New** button in the right pane (not shown). The following screen is displayed. Fill in the following:

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

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

In the **SIP Entity as Destination** section, click **Select**. The **SIP Entity List** page opens (not shown). Select the appropriate SIP entity to which this routing policy applies and click **Select**. The selected SIP Entity is displayed in 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 **To_CM** for Communication Manager.



The 'Routing Policy Details' screen shows the configuration for a routing policy. The left navigation pane has 'Routing Policies' highlighted. The main area has two sections: 'General' and 'SIP Entity as Destination'. The 'General' section has fields for Name, Disabled, and Notes. The 'SIP Entity as Destination' section has a 'Select' button. Below these sections is a table with columns for Name, FQDN or IP Address, Type, and Notes. The first row is highlighted with a red border. At the bottom right are 'Commit' and 'Cancel' buttons.

Avaya Aura® System Manager 6.1

Help | About | Change Password | Log off admin

Routing * Home

Home / Elements / Routing / Routing Policies - Routing Policy Details

Routing Policy Details

Commit Cancel

General

* Name: To_CM

Disabled: ☐

Notes: From MTS Allstream

SIP Entity as Destination

Select

Name	FQDN or IP Address	Type	Notes
DevCM217_TCP_5090	110.10.97.217	CM	MTS Allstream

The following screens show the Routing Policies **To_MTSAllstream** for the Avaya SBCE.

The screenshot shows the Avaya Aura System Manager 6.1 interface. The left navigation pane has 'Routing Policies' highlighted. The main content area is titled 'Routing Policy Details' and shows the 'General' tab. The 'Name' field is set to 'To_MTSAllstream'. The 'Disabled' checkbox is unchecked. The 'Notes' field contains 'From CM601'. Below this, there is a table for 'SIP Entity as Destination' with one entry: 'AvayaSBCE_TCP_5090' with FQDN '110.10.97.189', Type 'Other', and Notes 'MTS Allstream'. At the bottom right, there are 'Commit' and 'Cancel' buttons.

Name	FQDN or IP Address	Type	Notes
AvayaSBCE_TCP_5090	110.10.97.189	Other	MTS Allstream

6.7. Add Dial Patterns

Dial Patterns are needed to route specific calls through Session Manager. For the compliance test, dial patterns are 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 navigation pane and click on the **New** button in the right pane (not shown). Fill in the following, as shown in the screens below:

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

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

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

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

Two examples of the dial patterns used for the compliance test are shown below, one for outbound calls from the enterprise to the PSTN and one for inbound calls from the PSTN to the enterprise. Other dial patterns (e.g., 011 international calls, 411 directory assistance calls etc.) are similarly defined.

The first example shows that 11-digit dialed numbers that begin with **1** and has a destination domain of **avaya.com** uses route policy **To_MTSAllstream** as defined in **Section 6.6**.

The screenshot shows the 'Dial Pattern Details' page in Avaya Aura System Manager 6.1. The left sidebar has 'Dial Patterns' highlighted. The main form has the following fields:

- * Pattern: 1
- * Min: 11
- * Max: 11
- Emergency Call: ☐
- SIP Domain: avaya.com
- Notes:

Below the form is a table titled 'Originating Locations and Routing Policies' with 1 item. The table has the following columns: Originating Location Name, Originating Location Notes, Routing Policy Name, Rank, Routing Policy Disabled, Routing Policy Destination, and Routing Policy Notes.

Originating Location Name	Originating Location Notes	Routing Policy Name	Rank	Routing Policy Disabled	Routing Policy Destination	Routing Policy Notes
Belleville	Belleville DevConnect lab	To_MTSAllstream	0	<input type="checkbox"/>	AvayaSBCE_TCP_5090	From CM601

The second example shows that inbound 10-digit numbers that start with **647776** to domain **avaya.com** uses route policy **To_CM** as defined in **Section 6.6**. These are the DID numbers assigned to the enterprise by MTS Allstream.

The screenshot shows the 'Dial Pattern Details' page in Avaya Aura System Manager 6.1. The left sidebar has 'Dial Patterns' highlighted. The main form has the following fields:

- * Pattern: 647776
- * Min: 10
- * Max: 10
- Emergency Call: ☐
- SIP Domain: avaya.com
- Notes:

Below the form is a table titled 'Originating Locations and Routing Policies' with 1 item. The table has the following columns: Originating Location Name, Originating Location Notes, Routing Policy Name, Rank, Routing Policy Disabled, Routing Policy Destination, and Routing Policy Notes.

Originating Location Name	Originating Location Notes	Routing Policy Name	Rank	Routing Policy Disabled	Routing Policy Destination	Routing Policy Notes
Belleville	Belleville DevConnect lab	To_CM	0	<input type="checkbox"/>	DevCM217_TCP_5090	From MTS Allstream

6.8. Add/View Session Manager

The creation of a Session Manager element provides the linkage between System Manager and Session Manager. This is most likely done as part of the initial Session Manager installation. To add a Session Manager, navigate to **Home → Elements → Session Manager → Session**

Manager Administration in the left navigation pane and click on the **New** button in the right pane (not shown). If the Session Manager already exists, click **View** (not shown) to view the configuration. Enter/verify the data as described below and shown in the following screen:

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

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

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

AVAYA Avaya Aura® System Manager 6.1

Help | About | Change Password | Log off admin

Session Manager x Routing x Home

Home / Elements / Session Manager - Session Manager

Edit Session Manager Commit Cancel

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

General

SIP Entity Name

Description

*Management Access Point Host Name/IP

*Direct Routing to Endpoints

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

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

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

Security Module

SIP Entity IP Address

*Network Mask

*Default Gateway

*Call Control PHB

*QOS Priority

*Speed & Duplex

VLAN ID

7. Configure Avaya Session Border Controller for Enterprise

This section covers the configuration of Avaya Session Border Controller for Enterprise (Avaya SBCE). It is assumed that the software has already been installed. For additional information on these configuration tasks, see Reference [12] and [13].

The compliance test comprises of configuration for two major components, trunk server for service provider and call server for the enterprise. Each component consists of a set of Global Profiles, Domain Policies and Device Specific Settings. The configuration is performed using the Avaya SBCE web user interface as described in the following sections.

Trunk server configuration elements for service provider MTS Allstream:

- Global Profiles:
 - o URI Groups
 - o Routing
 - o Topology Hiding
 - o Server Interworking
 - o Signaling Manipulation
 - o Server Configuration
- Domain Policies:
 - o Application Rules
 - o Media Rules
 - o Signaling Rules
 - o Endpoint Policy Group
 - o Session Policy
- Device Specific Settings:
 - o Network Management
 - o Media Interface
 - o Signaling Interface
 - o End Point Flows → Server Flows
 - o Session Flows

Call server configuration elements at the enterprise for Session Manager:

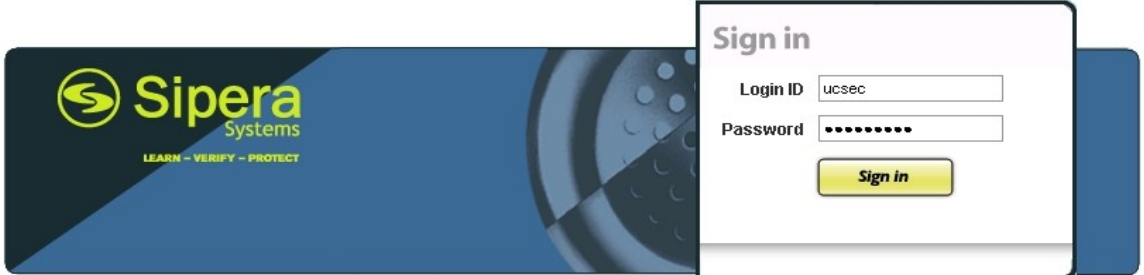
- Global Profiles:
 - o URI Groups
 - o Routing
 - o Topology Hiding
 - o Server Interworking
 - o Server Configuration
- Domain Policies:
 - o Application Rules
 - o Media Rules
 - o Signaling Rules
 - o Endpoint Policy Group
 - o Session Policy
- Device Specific Settings:

- Network Management
- Media Interface
- Signaling Interface
- End Point Flows → Server Flows
- Session Flows

7.1. Avaya Session Border Controller for Enterprise Login

Use a Web browser to access the Unify Communication Security (UC-Sec) web interface, enter `https://<ip-addr>/ucsec` in the address field of the web browser (not shown), where `<ip-addr>` is the management LAN IP address of UC-Sec.

Enter appropriate credentials and click **Sign In**.

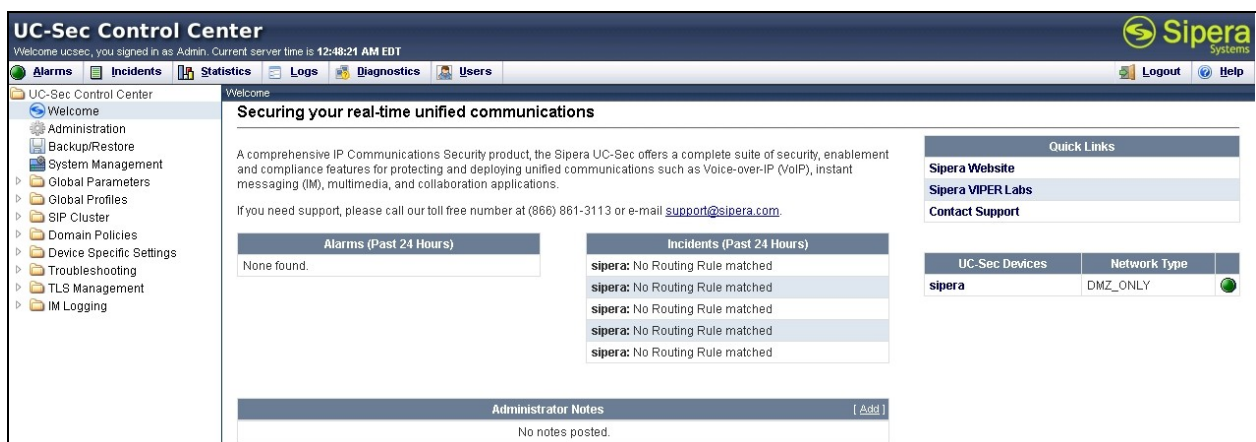


The UC-Sec™ family of products from Sipera Systems delivers comprehensive VoIP security by adapting the best practices of internet security and by using unique, sophisticated techniques such as VoIP protocol misuse & anomaly detection, behavioral learning based anomaly detection and voice spam detection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

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

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

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



UC-Sec Control Center
Welcome ucsec, you signed in as Admin. Current server time is 12:48:21 AM EDT

Securing your real-time unified communications

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

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

Alarms (Past 24 Hours)	Incidents (Past 24 Hours)
None found.	sipera: No Routing Rule matched
	sipera: No Routing Rule matched
	sipera: No Routing Rule matched
	sipera: No Routing Rule matched
	sipera: No Routing Rule matched

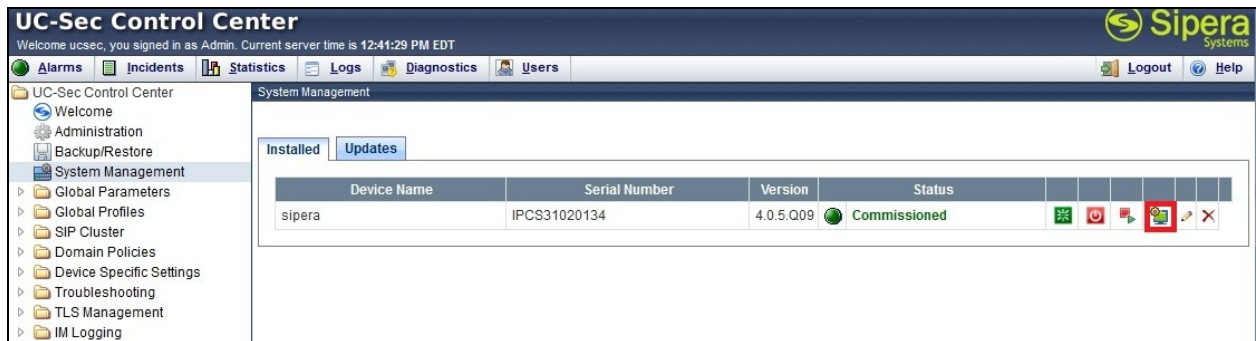
Administrator Notes [Add]
No notes posted.

Quick Links

- Sipera Website
- Sipera VIPER Labs
- Contact Support

UC-Sec Devices	Network Type
sipera	DMZ_ONLY

To view system information that has been configured during installation, navigate to **UC-Sec Control Center → System Management**. A list of installed devices is shown in the right pane. In the Compliance test, a single device named **sipera** is added. To view the configuration of this device, click the **View Config** icon (the third icon from the right) as shown below.



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

System Information: sipera

Network Configuration

General Settings

Appliance Name	sipera
Box Type	SIP
Deployment Mode	Proxy

Device Settings

HA Mode	No
Secure Channel Mode	None
Two Bypass Mode	No

Network Settings

IP	Public IP	Netmask	Gateway	Interface
110.10.97.189	110.10.97.189	255.255.255.192	110.10.97.129	A1
110.10.98.112	110.10.98.112	255.255.255.224	110.10.98.97	B1
110.10.98.108	110.10.98.108	255.255.255.224	110.10.98.97	B1
110.10.98.106	110.10.98.106	255.255.255.224	110.10.98.97	B1
110.10.98.98	110.10.98.98	255.255.255.224	110.10.98.97	B1
110.10.98.121	110.10.98.121	255.255.255.224	110.10.98.97	B1

DNS Configuration

Primary DNS	110.10.98.60
Secondary DNS	
DNS Location	DMZ
DNS Client IP	110.10.97.189

Management IP(s)

IP	110.10.98.85
----	--------------

7.2. Global Profiles

Global Profiles allows for configuration of parameters across all UC-Sec appliances.

7.2.1. Uniform Resource Identifier (URI) Groups

The **URI Group** feature allows user to create any number of logical URI groups that are comprised of individual SIP subscribers located in that particular domain or group. These groups are used by the various domain policies to determine which actions (Allow, Block, or Apply Policy) should be used for a given call flow.

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

In the compliance test, a URI Group named **CM_MTSAllstream** is added with URI type **Plain** (not shown) and consists of four domain [*@anonymous.invalid](#), [*@avaya.com](#), [*@110.10.98.112](#) and [*@220.20.2.12](#). Domain **anonymous.invalid** is defined for private calls received either from call server or trunk server and URI-Host masked by **anonymous.invalid**. The enterprise domain name **avaya.com** is for SIP Trunk domain defined in **Section 5.5** between Communication Manager and Avaya SBCE via Session Manager. For the public SIP Trunk between Avaya SBCE and MTS Allstream, the Avaya SBCE public IP address 110.10.98.112 is

TD; Reviewed:
SPOC 7/6/2012

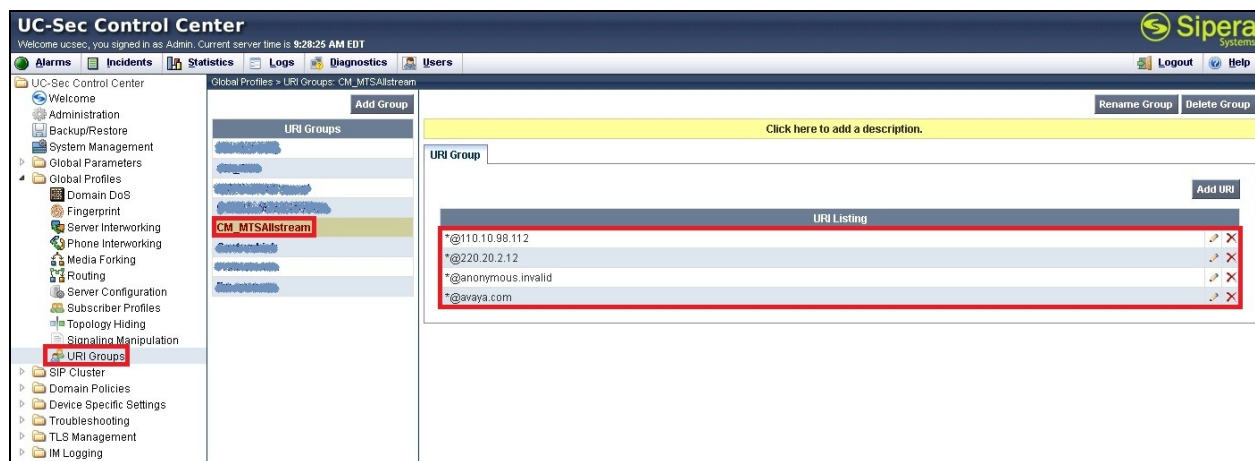
Solution & Interoperability Test Lab Application Notes
©2012 Avaya Inc. All Rights Reserved.

39 of 76
MTSCM6SM61SBCE

set as URI-Host of From, PAI and Diversion headers while the public IP address of MTS Allstream 220.20.2.12 is set as URI-Host of Request-URI and To headers.

This URI-Group is used to match the From and To headers in a SIP call dialog received from both Session Manager and MTS Allstream. If there is a match, the Avaya SBCE will apply the appropriate **Routing Profile** and **Server Flow** to route the inbound and outbound call to the right destination. The **Routing Profile** and **Server Flow** are configured in **Section 7.2.2** and **Section 7.4.4** appropriately.

The screenshot below illustrates the URI Listing for URI Group **CM_MTSAllstream**.



7.2.2. Routing Profiles

Routing Profiles define a specific set of packet routing criteria that are used in conjunction with other types of domain policies to identify a particular call flow and thereby ascertain which security features will be applied to those packets. Parameters defined by **Routing Profiles** include packet transport settings, name server addresses and resolution methods, next hop routing information and packet transport types.

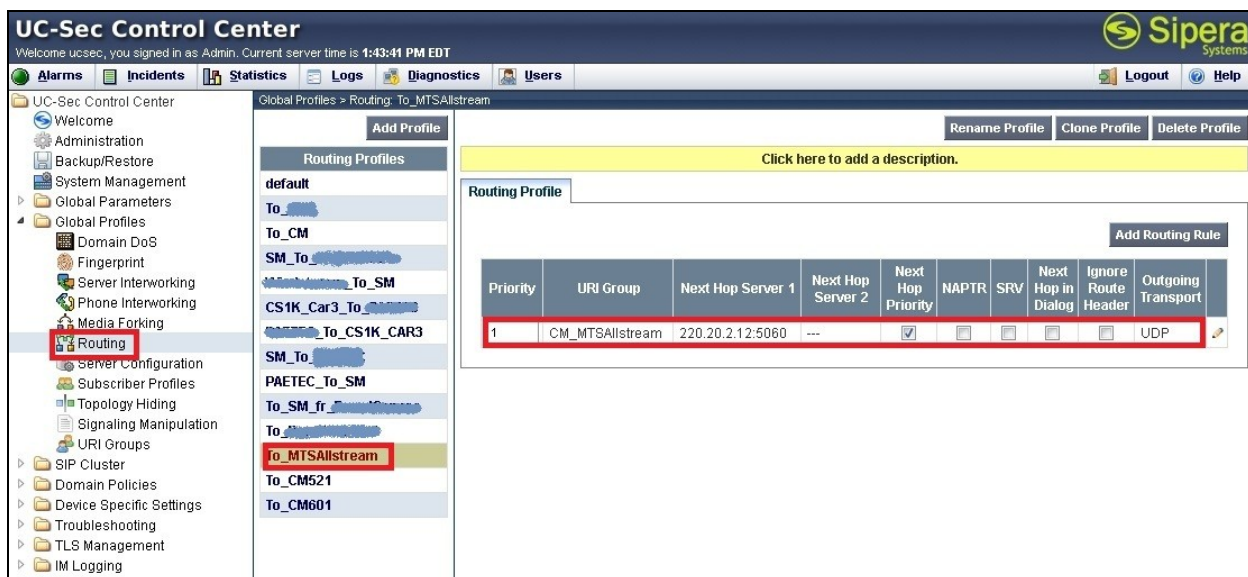
To create a **Routing Profile**, select **UC-Sec Control Center** → **Global Profiles** → **Routing**. Click on **Add Profile** (not shown).

In the compliance test, a **Routing Profile** named **To_MTSAllstream** is created to be used in conjunction with the server flow defined for Session Manager. This entry is to route the outgoing call from the enterprise to MTS Allstream.

In the opposite direction, a **Routing Profile** named **To_SM_TCP_5090** is created to be used in conjunction with the server flow defined for MTS Allstream. This entry is to route the incoming call from MTS Allstream to the enterprise.

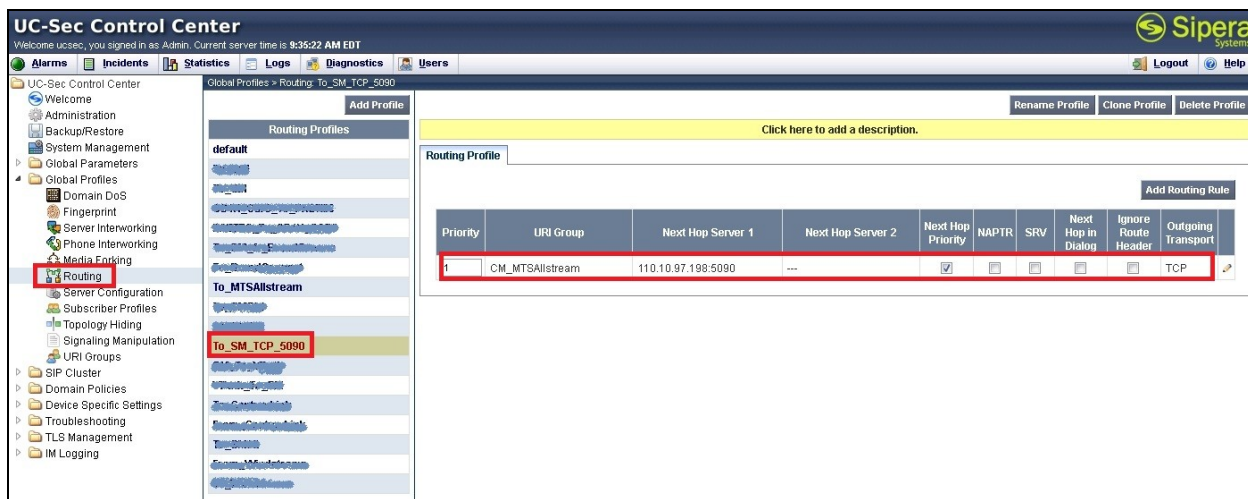
7.2.2.1 Routing Profile for MTS Allstream

The screenshot below illustrate the UC-Sec Control Center → Global Profiles → Routing: **To_MTSAllstream**. As shown in **Figure 1**, MTS Allstream SIP Trunk is connected with transportation protocol UDP. If there is a match in the **To** header of the **CM_MTSAllstream** URI Group defined in **Section 7.2.1**, the call will be routed to the **Next Hop Server 1** which is the IP address of MTS Allstream SIP Trunk on port 5060.



7.2.2.2 Routing Profile for Session Manager

The routing profile **To_SM_TCP_5090** is defined to route call where the **To** header matches the URI-Group **CM_MTSAllstream** defined in **Section 7.2.1** to **Next Hop Server 1** which is the IP address of Session Manager, on port 5090 as a destination. As shown in **Figure 1**, SIP Trunk between Session Manager and Avaya SBCE is connected with transportation protocol TCP.



7.2.3. Topology Hiding

Topology Hiding is an Avaya SBCE security feature which allows changing certain key SIP message parameters to 'hide' or 'mask' how the enterprise network may appear to an unauthorized or malicious user.

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

In the compliance test, two Topology Hiding profiles **To_MTSAllstream** and **To_CM** are created.

7.2.3.1 Topology Hiding Profile for MTS Allstream

Profile **To_MTSAllstream** is defined to mask the enterprise SIP domain **avaya.com** in Request-URI and To headers to IP **220.20.2.12** (the IP address MTS Allstream uses as URI-Host portion for Request-URI and To headers to meet the SIP specification requirement of MTS Allstream); mask the enterprise SIP domain **avaya.com** in From header to IP 110.10.98.112 (Avaya SBCE public IP address); and replace Record-Route, Via headers and SDP added by Communication Manager by external IP address known to MTS Allstream. It is to secure the enterprise network topology and also to meet the SIP requirement from service provider.

The screenshots below illustrate the **Topology Hiding** profile **To_MTSAllstream**.

The screenshot shows the UC-Sec Control Center web interface. On the left is a navigation tree with 'Topology Hiding' selected. The main panel shows the configuration for the 'To_MTSAllstream' profile. A table lists the headers to be modified:

Header	Criteria	Replace Action	Overwrite Value
Record-Route	IP/Domain	Auto	---
Request-Line	IP/Domain	Overwrite	220.20.2.12
SDP	IP/Domain	Auto	---
Via	IP/Domain	Auto	---
To	IP/Domain	Overwrite	220.20.2.12
From	IP/Domain	Overwrite	110.10.98.112

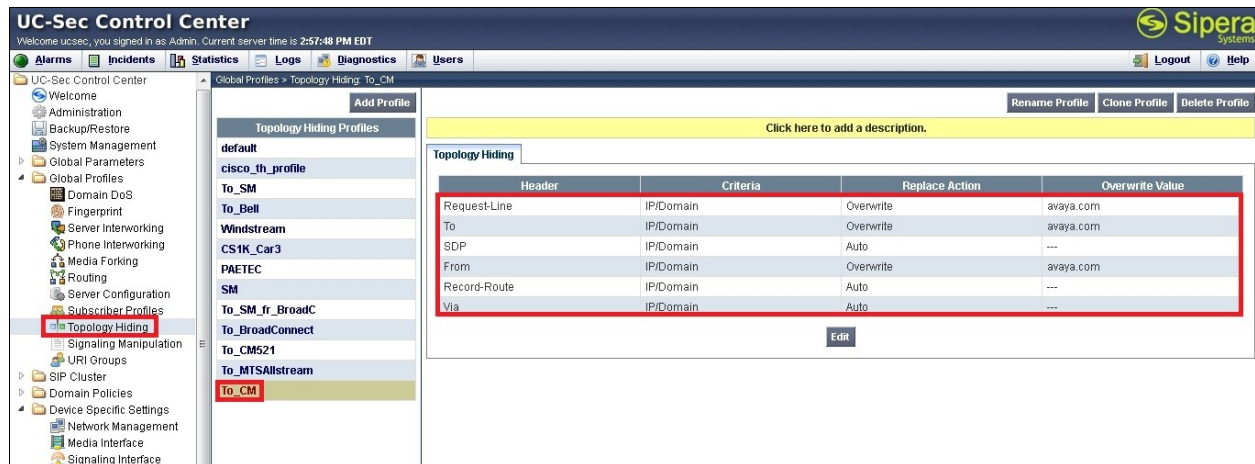
Notes:

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

7.2.3.2 Topology Hiding Profile for Communication Manager

Profile **To_CM** is also needed to mask MTS Allstream URI-Host in Request-URI, From, To headers to the enterprise SIP domain **avaya.com**; replace Record-Route, Via headers and SDP added by MTS Allstream by internal IP address known to Communication Manager.

The screenshots below illustrate the **Topology Hiding** profile **To_CM**.



Notes:

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

7.2.4. Server Interworking

Interworking Profile features are configured differently for Call and Trunk Servers.

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

In the compliance testing, two profiles **MTSAllstream** and **SM** are created for MTS Allstream and Session Manager respectively.

7.2.4.1 Server Interworking profile for MTS Allstream

Profile **MTS Allstream** is defined to match the specification of MTS Allstream. The **General** settings are configured with following parameters while the other settings for **Timers**, **URI Manipulation**, **Header Manipulation** and **Advanced** are kept as default.

General settings:

- Hold Support = **None**. Avaya SBCE will not modify the hold/ resume signaling from Communication Manager to MTS Allstream.

- 18X Handling = **None**. Avaya SBCE will not handle 180X, it will keep the 18X messages from Communication Manager unchanged to MTS Allstream.
- Refer Handling = **unchecked**. Avaya SBCE will not handle Refer. It will keep the Refer message from Communication Manager unchanged to MTS Allstream.
- T.38 Support = **unchecked**. MTS Allstream does not support T.38 fax in the compliance testing.
- Privacy Enabled = **unchecked**. Avaya SBCE will not mask the From header with anonymous for outbound call to MTS Allstream. It depends on the Communication Manager to enable/disable privacy on individual call basis.
- DTMF Support = **None**. Avaya SBCE will send original DTMF supported by Communication Manager to MTS Allstream.

The screenshots below illustrate the **Server Interworking** profile **MTSAllstream**.

Editing Profile: MTSAllstream	
General	
Hold Support	<input checked="" type="radio"/> None <input type="radio"/> RFC2543 - c=0.0.0.0 <input type="radio"/> RFC3264 - a=sendonly
180 Handling	<input checked="" type="radio"/> None <input type="radio"/> SDP <input type="radio"/> No SDP
181 Handling	<input checked="" type="radio"/> None <input type="radio"/> SDP <input type="radio"/> No SDP
182 Handling	<input checked="" type="radio"/> None <input type="radio"/> SDP <input type="radio"/> No SDP
183 Handling	<input checked="" type="radio"/> None <input type="radio"/> SDP <input type="radio"/> No SDP
Refer Handling	<input type="checkbox"/>
3xx Handling	<input type="checkbox"/>
Diversion Header Support	<input type="checkbox"/>
Delayed SDP Handling	<input type="checkbox"/>
T.38 Support	<input type="checkbox"/>
URI Scheme	<input checked="" type="radio"/> SIP <input type="radio"/> TEL <input type="radio"/> ANY
Via Header Format	<input checked="" type="radio"/> RFC3261 <input type="radio"/> RFC2543
<input type="button" value="Next"/>	

Privacy	
Privacy Enabled	<input type="checkbox"/>
User Name	<input type="text"/>
P-Asserted-Identity	<input type="checkbox"/>
P-Preferred-Identity	<input type="checkbox"/>
Privacy Header	<input type="text"/>

DTMF	
DTMF Support	<input checked="" type="radio"/> None <input type="radio"/> SIP NOTIFY <input type="radio"/> SIP INFO

Back Finish

7.2.4.2 Server Interworking profile for Session Manager

Profile **SM** is defined to match the specification of Communication Manager. The **General** settings are configured with the following parameters while the other settings for **Timers**, **URI Manipulation**, **Header Manipulation** and **Advanced** are kept as default.

General settings:

- Hold Support = **RFC3264**. Communication Manager supports hold/ resume as per RFC3264.
- 18X Handling = **None**. Avaya SBCE will not handle 180X, it will keep the 18X messages from MTS Allstream to Communication Manager unchanged.
- Refer Handling = **unchecked**. Avaya SBCE will not handle Refer, it will keep the Refer messages from MTS Allstream to Communication unchanged.
- T.38 Support = **unchecked**. MTS Allstream does not support T.38 fax in the compliance testing.
- Privacy Enabled = **unchecked**. Avaya SBCE will not mask the **From** header with anonymous for inbound call from MTS Allstream. It depends on the MTS Allstream to enable/ disable privacy on individual call basis.
- DTMF Support = **None**. Avaya SBCE will send original DTMF supported by MTS Allstream to Communication Manager.

The screenshots below illustrate the **Server Interworking** profile **SM**.

Editing Profile: SM

General

Hold Support	<input type="radio"/> None <input type="radio"/> RFC2543 - c=0.0.0.0 <input checked="" type="radio"/> RFC3264 a=sendonly
180 Handling	<input checked="" type="radio"/> None <input type="radio"/> SDP <input type="radio"/> No SDP
181 Handling	<input checked="" type="radio"/> None <input type="radio"/> SDP <input type="radio"/> No SDP
182 Handling	<input checked="" type="radio"/> None <input type="radio"/> SDP <input type="radio"/> No SDP
183 Handling	<input checked="" type="radio"/> None <input type="radio"/> SDP <input type="radio"/> No SDP
Refer Handling	<input type="checkbox"/>
3xx Handling	<input type="checkbox"/>
Diversion Header Support	<input type="checkbox"/>
Delayed SDP Handling	<input type="checkbox"/>
T.38 Support	<input type="checkbox"/>
URI Scheme	<input checked="" type="radio"/> SIP <input type="radio"/> TEL <input type="radio"/> ANY
Via Header Format	<input checked="" type="radio"/> RFC3261 <input type="radio"/> RFC2543

Next

Editing Profile: SM

Privacy

Privacy Enabled	<input type="checkbox"/>
User Name	
P-Asserted-Identity	<input type="checkbox"/>
P-Preferred-Identity	<input type="checkbox"/>
Privacy Header	

DTMF

DTMF Support	<input checked="" type="radio"/> None <input type="radio"/> SIP NOTIFY <input type="radio"/> SIP INFO
--------------	---

Back

Finish

7.2.5. Signaling Manipulation

The **Signaling Manipulation** feature allows the ability to add, change and delete any of the headers in a SIP message. This feature will add the ability to configure such manipulation in a highly flexible manner using a proprietary scripting language called SigMa.

The SigMa scripting language is designed to express any of the SIP header manipulation operations to be done by the Avaya SBCE. Using this language, a script can be written and tied to a given **Server Configuration** which is configured in the next steps through the UC-Sec GUI. The Avaya SBCE appliance then interprets this script at the given entry point or “hook point”.

These Application Notes will not discuss the full feature of the Signaling Manipulation but will show an example of a script created during compliance testing to aid in **Topology Hiding**.

To create a **Signaling Manipulation** script, select **UC-Sec Control Center → Global Profiles → Signaling Manipulation**. Click on **Add Script** (not shown). Separate SigMa script is created for call server and trunk server.

7.2.5.1 SigMa script for MTS Allstream

In the compliance testing, a SigMa script named **MTSAllstream** is created for Server Configuration MTS Allstream and described detail as following:

```
within session "ALL"
{
  act on message where %DIRECTION="OUTBOUND" and %ENTRY_POINT="POST_ROUTING"
  {
    %HEADERS["P-Asserted-Identity"][1].URI.HOST= "110.10.98.112";
  }
  act on message where %DIRECTION="INBOUND" and %ENTRY_POINT="AFTER_NETWORK"
  {
    %HEADERS["Request_Line"][1].regex_replace("sip:110.10.98.112","sip:avaya.com");
    %HEADERS["To"][1].regex_replace("sip:110.10.98.112","sip:ping@110.10.98.112");
    %HEADERS["From"][1].regex_replace("sip:220.20.2.12","sip:ping@220.20.2.12");
  }
}
```

The statement **act on message where %DIRECTION="OUTBOUND" and %ENTRY_POINT="POST_ROUTING"** is to specify the script will take effect on all type of SIP messages for outbound calls to MTS Allstream and the manipulation will be done after routing. The manipulation will be according to the rules contained in this statement. The **Topology-Hiding** profile **MTSAllstream** could mask the P-Asserted-Identity header properly. However, as a limitation, the P-Asserted-Identity header in “response” SIP message will still have the private enterprise SIP domain. Therefore, a SigMa rule is used to correct the URI-Host of P-Asserted-Identity header.

The statement **act on message where %DIRECTION="INBOUND" and %ENTRY_POINT="AFTER_NETWORK"** is to specify the script will take effect on all types of SIP messages for inbound calls from MTS Allstream and the manipulation will be done before routing. The manipulation will be according to the rules contained in this statement. The purpose of the SigMa script **MTAllstream** is to normalize the OPTIONS received from MTS Allstream.

The header **From** and **To** need to be modified to have URI-User@URI-Host format, otherwise the OPTIONS will fail to match the URI-Group defined in **Section 7.2.1**. If unmatching happens, the **Routing Profile** and **Server Flow** (discussed in **Section 7.4.4**) will not be applied to the call, and will result dropped packets. With the SigMa script in place, the OPTIONS heartbeat from MTS Allstream will be forwarded to Session Manager. The 200OK response from Session Manager will confirm the status of SIP Trunk as active. If there is no response, MTS Allstream will change the status of SIP Trunk to “out of service”.

7.2.5.2 SigMa script for Session Manager

In the compliance testing, a SigMa script named SM_For_MTSAllstream is created for Server Configuration Session Manager and described detail as following:

```
within session "ALL"
{
  act on message where %DIRECTION="INBOUND" and %ENTRY_POINT="AFTER_NETWORK"
  {
    %HEADERS["Request_Line"][1].regex_replace("sip:110.10.97.189","sip:220.20.2.12");
    %HEADERS["From"][1].regex_replace("sip:110.10.97.198","sip:ping@avaya.com");
    %HEADERS["To"][1].regex_replace("sip:110.10.97.189","sip:ping@avaya.com");
  }
}
```

The statement **act on message where %DIRECTION="INBOUND" and %ENTRY_POINT="AFTER_NETWORK"** is to specify the script will take effect on all types of SIP messages for outbound calls from Session Manager and the manipulation will be done before routing. The manipulation will be according to the rules contained in this statement. The purpose of the SigMa script SM_For_MTSAllstream is to normalize the OPTIONS received from Session Manager. The header **From** and **To** need to be modified to have URI-User@URI-Host format, otherwise the OPTIONS will fail to match the URI-Group defined in **Section 7.2.1**. If unmatching happens, the **Routing Profile** and **Server Flow** (discussed in **Section 7.4.4**) will not be applied to the call, and will result dropped packets. With the SigMa script in place, the OPTIONS heartbeat from Session Manager will be forwarded to MTS Allstream. The 200OK response from MTS Allstream will confirm the status of SIP Trunk as active. If there is no response, Session Manager will change the status of SIP Trunk to “out of service”.

7.2.6. Server Configuration

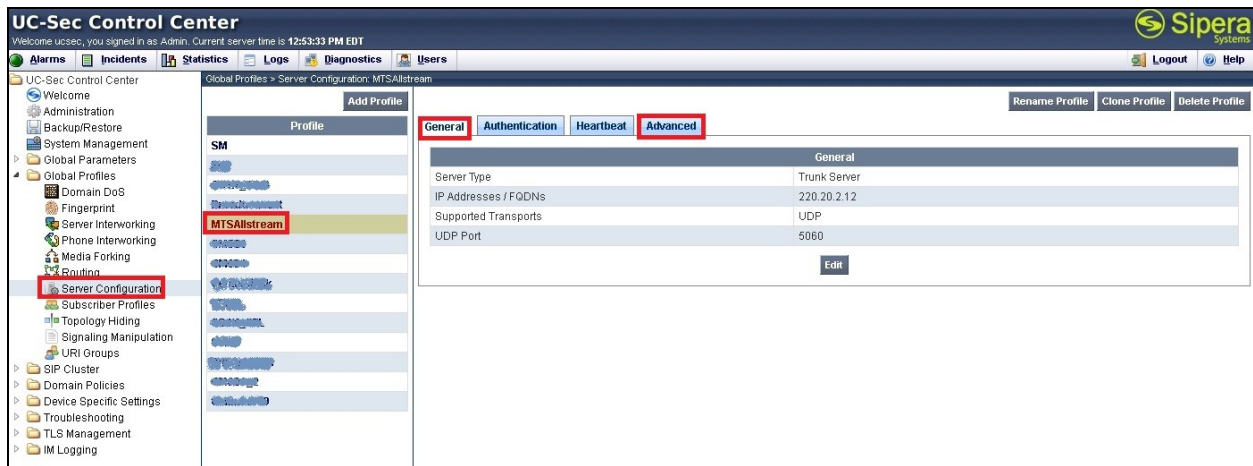
The **Server Configuration** screen contains four tabs: **General**, **Authentication**, **Heartbeat**, and **Advanced**. These tabs are used to configure and manage various SIP Call Server specific parameters such as TCP and UDP port assignments, heartbeat signaling parameters, DoS security statistics and trusted domains.

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

In the compliance testing, two separate Server Configurations are created, server entry **MTSAllsream** for MTS Allstream and server entry **SM** for Session Manager.

7.2.6.1 Server Configuration for MTS Allstream

The **Server Configuration** named **MTSAllstream** is added for MTS Allstream, it will be discussed in detail as below. **General** and **Advanced** tabs are provisioned but no configuration is done for **Authentication** tab as MTS Allstream does not implement Authentication on a SIP Trunk. The **Heartbeat** tab is kept as disabled as default to allow the Avaya SBCE to forward the OPTIONS heartbeat from Session Manager to MTS Allstream to query the status of the SIP Trunk.



In the **General** tab, set **Server Type** for MTS Allstream to **Trunk Server**. In the compliance testing, MTS Allstream supports UDP and listens on port 5060.

The screenshot shows a dialog box titled 'Edit Server Configuration Profile - General'. It contains the following fields and controls:

- Server Type:** A dropdown menu set to 'Trunk Server'.
- IP Addresses / Supported FQDNs:** A text area containing '220.20.2.12'.
- Supported Transports:** A group box containing three checkboxes: 'TCP' (unchecked), 'UDP' (checked), and 'TLS' (unchecked).
- TCP Port:** An empty text field.
- UDP Port:** A text field containing '5060'.
- TLS Port:** An empty text field.
- Finish:** A button at the bottom of the dialog.

Under **Advanced** tab, for **Interworking Profile** drop down list, select **MTSAllstream** as defined in **Section 7.2.4** and for **Signaling Manipulation Script** drop down list select **MTSAllsteram** as defined in **Section 7.2.5.1**. These configurations are applied to the specific SIP profile and SigMa rules for the traffic from MTS Allstream. The other settings are kept as default.

Enable DoS Protection	<input type="checkbox"/>
Enable Grooming	<input type="checkbox"/>
Interworking Profile	MTSAllstream
Signaling Manipulation Script	MTSAllstream
UDP Connection Type	<input checked="" type="radio"/> SUBID <input type="radio"/> PORTID <input type="radio"/> MAPPING

Finish

7.2.6.2 Server Configuration for Session Manager

The **Server Configuration** named **SM** added for Communication Manager is discussed in detail below. **General** and **Advanced** tabs are provisioned but no configuration is done for **Authentication** tab. The **Heartbeat** tab is kept as disabled as default to allow the Avaya SBCE to forward the OPTIONS heartbeat from MTS Allstream to Session Manager to query the status of the SIP Trunk.

General	
Server Type	Call Server
IP Addresses / FQDNs	110.10.97.198
Supported Transports	TCP
TCP Port	5090

Edit

In the **General** tab, specify **Server Type** as **Call Server**. In the compliance testing, the link between Avaya SBCE and Session Manager is TCP and Session Manager listens on port 5090.

Edit Server Configuration Profile - General	
Server Type	Call Server
IP Addresses / Supported FQDNs Comma separated list	110.10.97.198
Supported Transports	<input checked="" type="checkbox"/> TCP <input type="checkbox"/> UDP <input type="checkbox"/> TLS
TCP Port	5090
UDP Port	
TLS Port	
Finish	

Under **Advanced** tab, for **Interworking Profile** drop down list select **SM** as defined in **Section 7.2.4** and for **Signaling Manipulation Script** drop down list select **SM_For_MTSAllstream** as defined in **Section 7.2.5.2**. The other settings are kept as default.

Edit Server Configuration Profile - Advanced	
Enable DoS Protection	<input checked="" type="checkbox"/>
Enable Grooming	<input type="checkbox"/>
Interworking Profile	SM
Signaling Manipulation Script	SM_For_MTSAllstream
TCP Connection Type	<input checked="" type="radio"/> SUBID <input type="radio"/> PORTID <input type="radio"/> MAPPING
Finish	

7.3. Domain Policies

The **Domain Policies** feature configures various rule sets (policies) to control unified communications based upon criteria of communication sessions originating from or terminating at the enterprise. These criteria can be used to trigger policies which, in turn, activate various security features of the UC-Sec security device to aggregate, monitor, control and normalize call flow. There are default policies available for use, or a custom domain policy can be created.

7.3.1. Application Rules

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

An **Application Rule** is created to set the number of concurrent voice traffic. The sample configuration is cloned and modified to increase the number of **Maximum Concurrent Session** and **Maximum Sessions Per Endpoint**.

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

Enter a rule with a descriptive name **CM_MTSAllstream_AR** and click **Finish**.



Clone Rule	
Rule Name	default
Clone Name	CM_MTSAllstream_AR
Finish	

Click **Edit** button (not shown) to modify the rule. Set the **Maximum Concurrent Sessions** and **Maximum Session Per Endpoint** for the **Voice** application to a value high enough for the amount of traffic the network is able process. The following screen shows the modified **Application Rule** with the **Maximum Concurrent Sessions** and **Maximum Session Per Endpoint** set to 1000. In the compliance test, Communication Manager is programmed to control the concurrent sessions by setting the number of members in the trunk group (**Section 5.7**) to the allotted number. Therefore, the values in the **Application Rule** named **CM_MTSAllstream_AR** are set high enough to be considered non-blocking.

Application Type	In	Out	Maximum Concurrent Sessions	Maximum Sessions Per Endpoint
Voice	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	1000	1000
Video	<input type="checkbox"/>	<input type="checkbox"/>		
IM	<input type="checkbox"/>	<input type="checkbox"/>		

Miscellaneous

CDR Support
☒ None
☐ CDR w/ RTP
☐ CDR w/o RTP

IM Logging
☐

RTCP Keep-Alive
☐

Finish

7.3.2. Media Rules

Media Rules define RTP media packet parameters such as prioritizing encryption techniques and packet encryption techniques. Together these media-related parameters define a strict profile that is associated with other SIP-specific policies to determine how media packet matching the criteria will be handled by the UC-Sec security product.

A custom **Media Rule** is created to set the **Quality of Service** and **Media Anomaly Detection**. The sample configuration shows **Media Rule CM_MTSAllstream_MR** used for both the enterprise and MTS Allstream.

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

Enter a **Media Rule** with a descriptive name **CM_MTSAllstream_MR** and click **Finish**.

Clone Rule

Rule Name
default-low-med

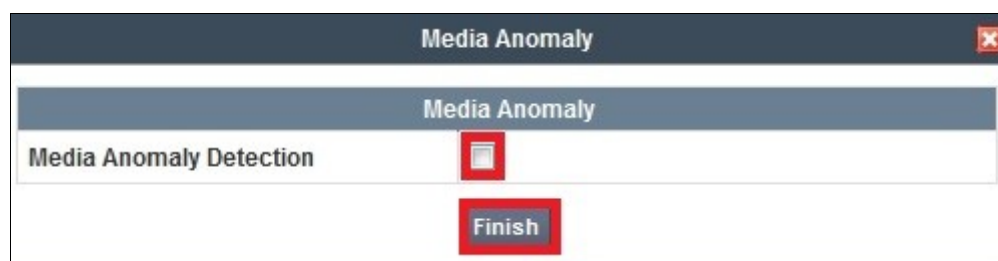
Clone Name
CM_MTSAllstream_M

Finish

When the RTP packets of a call are shuffled from Communication Manager to an IP Phone, Avaya SBCE will interpret this as an anomaly and an alert will be created in the **Incidents Log**.

Disabling **Media Anomaly Detection** prevents the **RTP Injection Attack** alerts from being created in the log during an audio shuffle.

To modify the rule, select the **Media Anomaly** tab (not shown) and click **Edit**, uncheck **Media Anomaly Detection** and click **Finish**.



The screenshot shows a window titled "Media Anomaly" with a close button in the top right corner. Inside the window, there is a sub-header "Media Anomaly". Below this, there is a table with two rows. The first row has the text "Media Anomaly Detection" and a checkbox that is currently unchecked. The second row is empty. Below the table, there is a button labeled "Finish". Red boxes highlight the checkbox and the "Finish" button.

The **Media Silencing** feature detects the silence when the call is in progress. If the silence is detected and exceeds the allowed duration, Avaya SBCE generates alert in the **Incidents Log**. In the compliance test, the **Media Silencing** detection is disabled to prevent the call from unexpectedly disconnected due to a RTP packet lost on public WAN.

To modify the rule, select the **Media Silencing** tab and click **Edit**, uncheck **Media Silencing** and click **Finish**.



The screenshot shows a window titled "Media Silencing" with a close button in the top right corner. Inside the window, there is a sub-header "Media Silencing". Below this, there is a table with two rows. The first row has the text "Media Silencing" and a checkbox that is currently unchecked. The second row has the text "Timeout (seconds)" and a text input field. Below the table, there is a button labeled "Finish". Red boxes highlight the checkbox and the "Finish" button.

Select the **Media QoS** tab and click **Edit** to configure the proper Quality of Service (QoS). Avaya SBCE can be configured to mark the Differentiated Services Code Point (DSCP) in the IP Header with specific values to support Quality of Services policies for the media. The following screen shows the QoS values used for the compliance test.

Media QoS Reporting			
RTCP Enabled	<input type="checkbox"/>		

Media QoS Marking			
Enabled	<input checked="" type="checkbox"/>		
<input checked="" type="radio"/> ToS			
Audio Precedence	Routine		000
Audio ToS	Minimize Delay		1000
Video Precedence	Routine		000
Video ToS	Minimize Delay		1000
<input type="radio"/> DSCP			
Audio	EF		101110
Video	EF		101110

Finish

7.3.3. Signaling Rules

Signaling Rules define the action to be taken (Allow, Block, Block with Response, etc.) for each type of SIP-specific signaling request and response message. When SIP signaling packets are received by the UC-Sec, they are parsed and “pattern-matched” against the particular signaling criteria defined by these rules. Packets matching the criteria defined by the Signaling Rules are tagged for further policy matching.

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

In the compliance testing, two **Signaling Rules** are created for MTS Allstream and Session Manager.

7.3.3.1 Signaling Rule for MTS Allstream

Clone a **Signaling Rule** with a descriptive name **MTSAllstream_SigR** and click **Finish**.

Clone Rule	
Rule Name	default
Clone Name	MTSAllstream_SigR
<input type="button" value="Finish"/>	

The **MTSAllstream_SigR** is configured to allow MTS Allstream to accept inbound and outbound call requests. It also blocks Accept-Language, Alert-Info and P-Charging-Vector headers from Communication Manager because these headers are not required by MTS Allstream.

Being cloned from the **Signaling Rule default**, the **MTSAllstream_SigR** will block all requests with 403 Forbidden. To start accepting calls, go to **General** tab, click on **Edit**. Then change **Inbound** and **Outbound Request** to **Allow** as shown in following screenshot.

General Control			
Inbound			
Requests	Allow	403	Forbidden
Non-2XX Final Responses	Allow	486	Busy Here
Optional Request Headers	Allow	403	Forbidden
Optional Response Headers	Allow	486	Busy Here
Outbound			
Requests	Allow	403	Forbidden
Non-2XX Final Responses	Allow	486	Busy Here
Optional Request Headers	Allow	403	Forbidden
Optional Response Headers	Allow	486	Busy Here
Content-Type Policy			
Enable Content-Type Checks		<input checked="" type="checkbox"/>	
Action	Allow	Multipart Action	Allow
Exception List (one per line)		Exception List (one per line)	
<input type="button" value="Finish"/>			

Request Headers setting is to allow or block a header in particular direction for request method. The buttons “**Add In Header Control**” and “**Add Out Header Control**” are used to define the

inbound and outbound Request header rules. The signaling rule **MTSAllstream_SigR** will be assigned to Server Configure for MTS Allstream as shown in **Section 7.2.6.1**.

The following screenshot shows three rules added to block the **Accept-Language**, **Alert-Info** and **P-Charging-Vector** headers.

- **Header Name**: Select the header to be manipulated.
- **Method Name**: Select **INVITE** in an outbound call request.
- **Header Criteria**: Click on **Forbidden** to block the header.
- **Action**: Select **Remove header** to delete the header.

The screenshot shows the UC-Sec Control Center interface. The left sidebar lists various configuration categories, with 'Signaling Rules' highlighted. The main panel displays the configuration for the 'MTSAllstream_SigR' rule. The 'Request Headers' tab is selected, showing a table of configured headers.

Row	Header Name	Method Name	Header Criteria	Action	Proprietary	Direction		
1	Accept-Language	INVITE	Forbidden	Remove Header	No	OUT		
2	Alert-Info	INVITE	Forbidden	Remove Header	No	OUT		
3	P-Charging-Vector	INVITE	Forbidden	Remove Header	Yes	OUT		

Note: Pre-defined list does not have P-Charging-Vector header, but the Avaya SBCE provides an option to define this proprietary header.

Response Headers setting is to allow or block a header in particular direction for response method. The buttons “**Add In Header Control**” and “**Add Out Header Control**” are used to define inbound and outbound Response Header rules. The **Signaling Rule MTSAllstream_SigR** will be assigned to Server Configure for MTS Allstream as shown in **Section 7.2.6.1**.

The following screenshots show three rules added to block the **Accept-Language**, **Alert-Info** and **P-Charging-Vector** headers:

- **Header Name**: Select the header to be manipulated.
- **Method Name**: Select **INVITE** for an inbound call request.
- **Header Criteria**: Click on **Forbidden** to block the header.
- **Action**: Select **Remove header** to delete the header.

UC-Sec Control Center
Welcome ucsec, you signed in as Admin. Current server time is 6:21:47 PM EDT

Alarms Incidents Statistics Logs Diagnostics Users Logout Help

Domain Policies > Signaling Rules: MTSAllstream_SigR

Filter By Device... [v] [Add Rule] [Rename Rule] [Clone Rule] [Delete Rule]

Click here to add a description.

General Requests Responses Request Headers **Response Headers** Signaling QoS

[Add In Header Control] [Add Out Header Control]

Row	Header Name	Response Code	Method Name	Header Criteria	Action	Proprietary	Direction		
1	Accept-Language	1XX	INVITE	Forbidden	Remove Header	No	OUT		
2	Alert-Info	1XX	INVITE	Forbidden	Remove Header	No	OUT		
3	P-Charging-Vector	1XX	INVITE	Forbidden	Remove Header	Yes	OUT		

Note: Pre-defined list does not have **P-Charging-Vector** header, but the Avaya SBCE provides an option to define this proprietary header.

On the **Signaling QoS** tab, select the proper Quality of Service (QoS). Avaya SBCE can be configured to mark the Differentiated Services Code Point (DSCP) in the IP Header with specific values to support Quality of Services policies for signaling. The following screen shows the QoS value used for the compliance test.

Signaling QoS

Signaling QoS

Enabled ☒

☐ ToS

Precedence

ToS

☒ **DSCP**

Value

Finish

7.3.3.2 Signaling Rule for Session Manager

Clone a **Signaling Rule** with a descriptive name **SM_SigR** and click **Finish**.

Clone Rule	
Rule Name	default
Clone Name	SM_SigR
<input type="button" value="Finish"/>	

This **SM_SigR** is configured to allow Communication Manager to accept inbound and outbound call requests.

Being cloned from the **Signaling Rule default**, the **SM_SigR** will block all requests with 403 Forbidden. To start accepting calls, select **CM_SigR** then go to **General** tab, click on **Edit** (not shown). Then change **Inbound-Requests** and **Outbound-Requests** to **Allow** as shown in following screenshot and click **Finish**.

General Control			
Inbound			
Requests	Allow	403	Forbidden
Non-2XX Final Responses	Allow	486	Busy Here
Optional Request Headers	Allow	403	Forbidden
Optional Response Headers	Allow	486	Busy Here
Outbound			
Requests	Allow	403	Forbidden
Non-2XX Final Responses	Allow	486	Busy Here
Optional Request Headers	Allow	403	Forbidden
Optional Response Headers	Allow	486	Busy Here
Content-Type Policy			
Enable Content-Type Checks		<input checked="" type="checkbox"/>	
Action	Allow	Multipart Action	Allow
Exception List (one per line)		Exception List (one per line)	
<input type="button" value="Finish"/>			

On the **Signaling QoS** tab, select the proper Quality of Service (QoS). Avaya SBCE can be configured to mark the Differentiated Services Code Point (DSCP) in the IP Header with specific

values to support Quality of Services policies for signaling. The following screen shows the QoS value used for the compliance test.

Signaling QoS			
Signaling QoS			
Enabled		<input checked="" type="checkbox"/>	
ToS			
	Precedence	Routine	000
	ToS	Minimize Delay	1000
DSCP			
	Value	EF	101110
Finish			

7.3.4. Endpoint Policy Groups

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

Endpoint Policy Groups are created for the Session Manager and the MTS Allstream.

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

7.3.4.1 Endpoint Policy Group for MTS Allstream

The following screen shows **MTSAllstream_PolicyG** created for MTS Allstream:

- Set **Application** and **Media** rules created in **Section 7.3.1** and **Section 7.3.2**.
- Set **Signaling** rule **MTSAllstream_SigR** created in **Section 7.3.3.3**.
- Set **Border** and **Time of Day** rules to **default**.
- Set **Security** rule to **default-high**.

The screenshot displays the UC-Sec Control Center web interface. The left sidebar shows a navigation tree with 'End Point Policy Groups' highlighted. The main content area shows the configuration for 'MTSAllstream_PolicyG'. A table lists the policy rules, with the first row highlighted in red:

Order	Application	Border	Media	Security	Signaling	Time of Day	
1	CM_MTSAllstream_AR	default	CM_MTSAllstream_MR	default-high	MTSAllstream_SigR	default	

7.3.4.2 Endpoint Policy Group for Session Manager

The following screen shows CMMTS_PolicyG created for Session Manager:

- Set **Application** and **Media** rules created in **Section 7.3.1** and **Section 7.3.2**.
- Set **Signaling** rule **SM_SigR** created in **Section 7.3.3.3**.
- Set the **Border** and **Time of Day** rules to **default**.
- Set the **Security** rule to **default-low**.

UC-Sec Control Center

Welcome ucsec, you signed in as Admin. Current server time is 12:56:33 PM EDT

Alarms Incidents Statistics Logs Diagnostics Users

Domain Policies > End Point Policy Groups: CMMTS_PolicyG

Showing page 1 of 2.

Policy Groups > >>

default-low
default-low-enc
default-med
default-med-enc
default-high
default-high-enc
OCS-default-high
avaya-def-low-enc
BellCanada_PolicyG
CMBell_PolicyG
CS1K_Car3_PolicyG
BroadConnect_PolicyG
SM_PolicyG
MTSAllstream_PolicyG
CM521_PolicyG
CMMTS_PolicyG
To_SM_PolicyG
CenturyLink_PolicyG
CS1K_For_MTS_PolicyG
Windstream_PolicyG
To_GenbandG9_PolicyG
Enterprise_DomPolicy
Bell_cust2_DomPolicy
CS1K_SigR
TELUS_PolicyG

Filter By Device...

Click here to add a description.

Click here to add a row description.

Policy Group

View Summary Add Policy Set

Order	Application	Border	Media	Security	Signaling	Time of Day
1	CM_MTSAllstream_AR	default	CM_MTSAllstream_MR	default-low	SM_SigR	default

7.3.5. Session Policy

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

In the compliance test, the **Session Policy** named **CM_MTSAllstream** is created to match the codec configuration on MTS Allstream. The policy also allows Avaya SBCE to anchor media in off-net call transfer scenarios.

To clone a **Session Policy**, navigate to **UC-Sec Control Center** → **Domain Policies** → **Session Policies**. With the **default** rule chosen, click on **Clone Rule** (not shown). It is applied to both Communication Manager and MTS Allstream.

Enter a descriptive name **CM_MTSAllstream** for the new policy and click **Finish**.

Clone Policy

Policy Name	default
Clone Name	CM_MTSAllstream

Finish

MTS Allstream supports voice codec G.729 and G.711MU in prioritized order with payload 101 for RFC2833/ DTMF. To define **Codec Prioritization** for Audio Codec, select the profile **CM_MTSAllstream** created above, click on **Edit** (not shown). Select **Preferred Codec #1** as G.711MU, **Preferred Codec #2** as G.729 and **Preferred Codec #3** as Dynamic (101) for RFC2833/ DTMF. Check **Allow Preferred Codecs Only** to prevent the unsupported codec from being sent to both ends.

Notes:

- The T.38 fax is not yet supported by MTS Allstream SIP Trunking Service.
- This **Session Policy** prioritizes voice codec G.711MU to establish the voice call. It is mandatory for a G.711MU fax call to be successful because both Communication Manager and MTS Allstream cannot switch the voice call using different codec to G.711MU for fax.

Codec Prioritization	
Audio Codec	
Codec Prioritization	<input checked="" type="checkbox"/>
Allow Preferred Codecs Only	<input checked="" type="checkbox"/>
Preferred Codec #1	PCMU (0)
Preferred Codec #2	G729 (18)
Preferred Codec #3	Dynamic (101)
Preferred Codec #4	None
Preferred Codec #5	None
Video Codec	
Codec Prioritization	<input type="checkbox"/>
Allow Preferred Codecs Only	<input type="checkbox"/>
Preferred Codec #1	CeIB (25)
Preferred Codec #2	None
Preferred Codec #3	None
Preferred Codec #4	None
Preferred Codec #5	None
Finish	

To enable **Media Anchoring** on Avaya SBCE, select Session Policy **CM_MTSAllstream** created above then select tab **Media**, click **Edit** (not shown). Check on **Media Anchoring**.

Media	
Media Anchoring	<input checked="" type="checkbox"/>
Media Forking Profile	None ▼
<input type="button" value="Finish"/>	

7.4. Device Specific Settings

The **Device Specific Settings** feature allows aggregate system information to be viewed and various device-specific parameters to be managed to determine how a particular device will function when deployed in the network. Specifically, it gives the ability to define and administer various device-specific protection features such as Message Sequence Analysis (MSA) functionality and protocol scrubber rules, end-point and session call flows, as well as the ability to manage system logs and control security features.

7.4.1. Network Management

The **Network Management** screen is where the network interface settings are configured and enabled. During the installation process of Avaya SBCE, certain network-specific information is defined such as device IP address(es), public IP address(es), netmask, gateway, etc. to interface the device to the network. This information populates the various **Network Management** tab displays, which can be edited as needed to optimize device performance and network efficiency.

Navigate to **UC-Sec Control Center** → **Device Specific Settings** → **Network Management** and under **Network Configuration** tab verify the IP addresses assigned to the interfaces and that the interfaces are enabled. The following screen shows the private interface is assigned to **A1** and the public interface is assigned to **B1**.

UC-Sec Control Center
Welcome ucsec, you signed in as Admin. Current server time is 12:45:53 AM EDT

Alarms Incidents Statistics Logs Diagnostics Users

UC-Sec Control Center

Device Specific Settings > Network Management: sipera

UC-Sec Devices

sipera

Network Configuration Interface Configuration

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

A1 Netmask 255.255.255.192 A2 Netmask B1 Netmask 255.255.255.224 B2 Netmask

Add IP

Changes will not take effect until the interface is updated. Save Changes Clear Changes

IP Address	Public IP	Gateway	Interface
110.10.97.169		110.10.97.129	A1
110.10.98.98		110.10.98.97	B1
110.10.98.112		110.10.98.97	B1

Enable the interfaces used to connect to the inside and outside networks on the **Interface Configuration** tab. The following screen shows interface **A1** and **B1** are **Enabled**. To enable an interface click it's **Toggle State** button.

The screenshot shows the UC-Sec Control Center interface. The left sidebar contains a tree view with 'Device Specific Settings' expanded, and 'Network Management' selected. The main panel is titled 'Device Specific Settings > Network Management: sipera'. It has two tabs: 'Network Configuration' and 'Interface Configuration'. The 'Interface Configuration' tab is active, displaying a table of network interfaces.

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

7.4.2. Media Interface

The **Media Interface** screen is where the media ports are defined. Avaya SBCE will open connection for RTP on the defined ports.

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

Media Interfaces are created for both the inside and outside interfaces. The following screen shows the **Media Interfaces** created in the compliance test.

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

The screenshot shows the UC-Sec Control Center interface. The left sidebar contains a tree view with 'Device Specific Settings' expanded, and 'Media Interface' selected. The main panel is titled 'Device Specific Settings > Media Interface: sipera'. It has a tab labeled 'Media Interface'. Below the tab is a message: 'Modifying or deleting an existing media interface will require an application restart before taking effect. Application restarts can be issued from System Management.' Below this is a table of media interfaces.

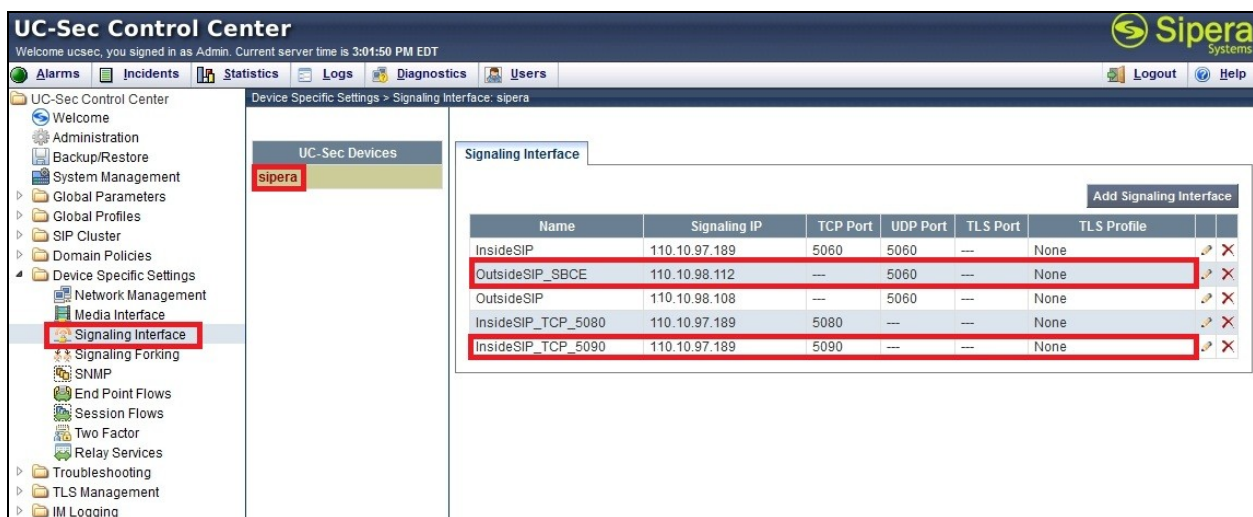
Name	Media IP	Port Range	
InsideMedia	110.10.97.189	35000 - 40000	✎ ✕
OutsideMedia_SBCE	110.10.98.112	35000 - 40000	✎ ✕
OutsideMedia	110.10.98.98	35000 - 40000	✎ ✕

7.4.3. Signaling Interface

The **Signaling Interface** screen is where the SIP signaling port is defined. Avaya SBCE will listen for SIP requests on the defined port.

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

Signaling Interface is created for both inside and outside interfaces. The following screen shows the **Signaling Interfaces** created in the compliance test with TCP/5090 and UDP/5060 used respectively for the inside and outside IP interface.

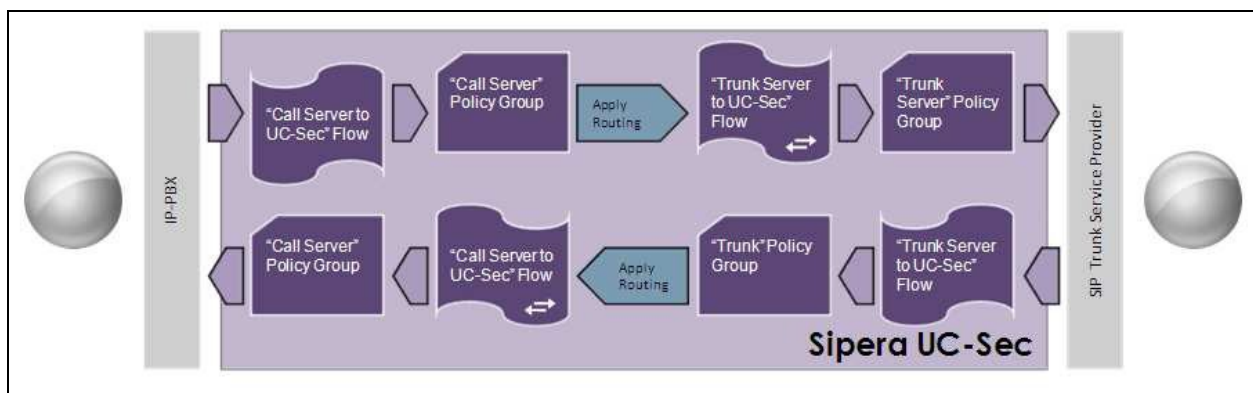


The screenshot shows the UC-Sec Control Center interface. The left sidebar contains a tree view with 'Signaling Interface' selected. The main content area shows a table of configured signaling interfaces for the device 'sipera'.

Name	Signaling IP	TCP Port	UDP Port	TLS Port	TLS Profile	
InsideSIP	110.10.97.189	5060	5060	---	None	
OutsideSIP_SBCE	110.10.98.112	---	5060	---	None	
OutsideSIP	110.10.98.108	---	5060	---	None	
InsideSIP_TCP_5080	110.10.97.189	5080	---	---	None	
InsideSIP_TCP_5090	110.10.97.189	5090	---	---	None	

7.4.4. End Point Flows - Server Flow

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



In the compliance test, separate **Server Flows** are created for MTS Allstream and Session Manager. To create a **Server Flow**, navigate to **UC-Sec Control Center → Device Specific Settings → End Point Flows**. Select the **Server Flows** tab and click **Add Flow** (not shown). In the new window that appears, enter the following values. The other fields are kept default.

- **Flow Name:** Enter a descriptive name.
- **Server Configuration:** Select a Server Configuration created in **Section 7.2.6** to assign to the Flow.
- **URI Group:** Select the URI Group created in **Section 7.2.1** to assign to the Flow.
- **Received Interface:** Select the Signaling Interface created in **Section 7.4.3** the Server Configuration is allowed to receive SIP messages from.
- **Signaling Interface:** Select the Signaling Interface created in **Section 7.4.3** used to communicate with the Server Configuration.
- **Media Interface:** Select the Media Interface created in **Section 7.4.2** used to communicate with the Server Configuration.
- **End Point Policy Group:** Select the End Point Policy Group created in **Section 7.3.4** assigned to the Server Configuration.
- **Routing Profile:** Select the Routing Profile created in **Section 7.2.2** the Server Configuration will use to route SIP messages to.
- **Topology Hiding Profile:** Select the Topology-Hiding profile created in **Section 7.2.3** to apply toward the Server Configuration.
- Click **Finish**.

The following screen shows the Server **Flow Name (MTS Allstream)** configured for MTS Allstream.

Edit Flow: MTSAllstream

Criteria	
Flow Name	MTSAllstream
Server Configuration	MTSAllstream
URI Group	MTSAllstream
Transport	*
Remote Subnet	*
Received Interface	InsideSIP
Signaling Interface	OutsideSIP_SBCE
Media Interface	OutsideMedia_SBCE
End Point Policy Group	MTSAllstream_PolicyG
Routing Profile	To_SM_TCP_5090
Topology Hiding Profile	To_MTSAllstream
File Transfer Profile	None

Finish

The following screen shows the Server **Flow Name (SM_For_MTSAllstream)** configured for Session Manager.

Criteria	
Flow Name	SM_For_MTSAllstream
Server Configuration	SM
URI Group	CM_MTSAllstream
Transport	*
Remote Subnet	*
Received Interface	OutsideSIP_SBCE
Signaling Interface	InsideSIP_TCP_5090
Media Interface	InsideMedia
End Point Policy Group	CMMTS_PolicyG
Routing Profile	To_MTSAllstream
Topology Hiding Profile	To_CM
File Transfer Profile	None

Finish

7.4.5. Session Flows

The **Session Flows** feature allows defining certain parameters that pertain to the media portions of a call, whether it originates from the enterprise or outside the enterprise. This feature provides the complete and unparalleled flexibility to monitor, identify and control very specific types of calls based upon these user-definable parameters. **Session Flows** profiles SDP media parameters, to completely identify and characterize a call placed through the network.

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

A common Session Flow is created for both Session Manager and the MTS Allstream. In the new window that appears, enter the following values. Use default values for the remaining fields:

- **Flow Name:** Enter a descriptive name.
- **URI Group #1:** Select the URI Group created in **Section 7.2.1** to assign to the Session Flow as the source URI Group.
- **URI Group #2:** Select the URI Group created in **Section 7.2.1** to assign to the Session Flow as the destination URI Group.
- **Session Policy:** Select the session policy created in **Section 7.3.5** to assign to the Session Flow.
- Click **Finish**.

Note: A unique **URI Group** is used for source and destination, since it contains multiple URIs defined for the source as well as for the destination.

The following screen shows the **Session Flow** named **CM_MTSAllstream** is created.

Criteria	
Flow Name	CM_MTSAllstream
URI Group #1	CM_MTSAllstream ▼
URI Group #2	CM_MTSAllstream ▼
Subnet #1	* Ex: 192.168.0.1/24
Subnet #2	* Ex: 192.168.0.1/24
Session Policy	CM_MTSAllstream ▼

Finish

8. MTS Allstream SIP Trunking Service Configuration

MTS Allstream is responsible for the configuration of its SIP Trunking Service. The customer will need to provide the IP address used to reach the Avaya SBCE at enterprise side. MTS Allstream will provide the customer with the necessary information to configure the SIP connection from enterprise to the MTS Allstream. The information provided by MTS Allstream includes:

- IP address of the MTS Allstream Session Border Controller.
- MTS Allstream SIP domain. In the compliance test, MTS Allstream preferred to use IP address as a URI-Host.
- CPE SIP domain. In the compliance test, MTS Allstream preferred to use IP address of Avaya SBCE as a URI-Host.
- Supported codecs.
- DID numbers.
- IP addresses and port numbers used for signaling or media through any security devices.

The sample configuration between MTS Allstream and the enterprise for the compliance test is a static configuration. There is no registration on the SIP trunk implemented on either MTS Allstream or enterprise side.

9. Verification and Troubleshooting

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

Verification Steps:

1. Verify that endpoints at the enterprise site can place call to PSTN and that the call remains active for more than 35 seconds. This time period is included to satisfy SIP protocol timers.
2. Verify that endpoints at the enterprise site can receive call from PSTN and that the call can remain active for more than 35 seconds. This time period is included satisfy SIP protocol timers.
3. Verify that the user on 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.

Protocol Traces:

The following SIP headers are inspected using Wireshark traces:

- Request-URI: verify the request number and SIP domain
- From: verify the display name and display number
- To: verify the display name and display number
- P-Assert-Identity: verify the display name and display number
- Privacy: verify the “user, id” masking

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

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

Troubleshooting:

Avaya SBCE

Using a network sniffing tool (e.g., Wireshark) to monitor the SIP signaling messages between MTS Allstream and Avaya SBCE

Following is an example inbound call from MTS Allstream to Communication Manager.

- Inbound INVITE request from MTS Allstream:

```
INVITE sip:6477763571@110.10.98.112;user=phone SIP/2.0
Max-Forwards: 69
Session-Expires: 3600;refresher=uac
Min-SE: 600
Supported: timer, 100rel
To: <sip:6477763571@110.10.98.112;user=phone>
From: <sip:16139675258@220.20.2.12;user=phone>;tag=3544979980-197490
P-Asserted-Identity: <sip:16139675258@220.20.2.12;user=phone>
Call-ID: 346201-3544979980-197481@nextone-msw-lab-3.mtsallstream.com
CSeq: 1 INVITE
Allow: CANCEL, INVITE, BYE, OPTIONS, REGISTER, NOTIFY, INFO, REFER, SUBSCRIBE,
PRACK, UPDATE, MESSAGE, PUBLISH
Via: SIP/2.0/UDP 220.20.2.12:5060;branch=z9hG4bK676db5bb3766d7e62389e2821aef275c
Contact: <sip:16139675258@220.20.2.12:5060;tgrp=TOROONSBSCIOT1>
Content-Type: application/sdp
Accept: application/sdp
```

Content-Length: 227

v=0
o=nextone-msw-lab-3 599717762 599717762 IN IP4 220.20.2.12
s=sip call
c=IN IP4 220.20.2.13
t=0 0
m=audio 24210 RTP/AVP 18 0 8 101
a=ptime:20
a=fmtp:18 annexb=no
a=rtpmap:101 telephone-event/8000
a=fmtp:101 0-15

- 200OK/SDP response by Communication Manager:

SIP/2.0 200 OK
From: <sip:16139675258@220.20.2.12;user=phone>;tag=3544979980-197490
To: <sip:6477763571@110.10.98.112;user=phone>;tag=80a5811ba8e1133214fc3f6900
CSeq: 1 INVITE
Call-ID: 346201-3544979980-197481@nextone-msw-lab-3.mtsallstream.com
Contact: "MTS H323 3571" <sip:6477763571@110.10.98.112:5060;transport=udp>
Record-Route: <sip:110.10.98.112:5060;ipcs-line=501999;lr;transport=udp>
Allow: INVITE,ACK,OPTIONS,BYE,CANCEL,SUBSCRIBE,NOTIFY,REFER,INFO,PRACK,PUBLISH
Supported: 100rel,join,replaces,sdp-anat,timer
Via: SIP/2.0/UDP 220.20.2.12:5060;branch=z9hG4bK676db5bb3766d7e62389e2821aef275c
Accept-Language: en
Require: timer
Server: Avaya CM/R016x.00.1.510.1 AVAYA-SM-6.1.1.0.611023
P-Asserted-Identity: "MTS H323 3571" <sip:6477763571@110.10.98.112>
Session-Expires: 3600;refresher=uac
Content-Type: application/sdp
P-Location: SM;origlocname="Belleville,Ont,Ca";termlocname="Belleville,Ont,Ca"
Content-Length: 175

v=0
o=- 1335991589 2 IN IP4 110.10.98.112
s=-
c=IN IP4 110.10.98.112
b=AS:64
t=0 0
m=audio 35248 RTP/AVP 0 101
a=rtpmap:0 PCMU/8000
a=rtpmap:101 telephone-event/8000

Following is an example outbound call from Communication Manager to MTS Allstream.

- Outbound INVITE request from Communication Manager:

INVITE sip:16132422192@220.20.2.12 SIP/2.0
From: "MTS H323 3571"
<sip:6477763571@110.10.98.112>;tag=803e8396c6a8e1147444fc3f6900
To: <sip:16132422192@220.20.2.12>
CSeq: 1 INVITE
Call-ID: 803e8396c6a8e1148444fc3f6900
Contact: "MTS H323 3571" <sip:6477763571@110.10.98.112:5060>
Record-Route: <sip:110.10.98.112:5060;ipcs-line=509453;lr;transport=udp>
Allow: INVITE,ACK,OPTIONS,BYE,CANCEL,SUBSCRIBE,NOTIFY,REFER,INFO,PRACK,PUBLISH
Supported: 100rel,join,replaces,sdp-anat,timer
User-Agent: Avaya CM/R016x.00.1.510.1 AVAYA-SM-6.1.1.0.611023
Max-Forwards: 66
Via: SIP/2.0/UDP 110.10.98.112:5060;branch=z9hG4bK-s1632-001368532687-1--s1632-
P-Asserted-Identity: "MTS H323 3571" <sip:6477763571@110.10.98.112>
Session-Expires: 600;refresher=uac

Min-SE: 600
Content-Type: application/sdp
Content-Length: 257

v=0
o=- 1336065069 1 IN IP4 110.10.98.112
s=-
c=IN IP4 110.10.98.112
b=AS:64
t=0 0
a=avf:avc=n prio=n
a=csup:avf-v0
m=audio 35334 RTP/AVP 18 0 101
a=rtpmap:0 PCMU/8000
a=rtpmap:18 G729/8000
a=fmtp:18 annexb=no
a=rtpmap:101 telephone-event/8000

- 200OK/SDP response by MTS Allstream:

SIP/2.0 200 OK
Session-Expires: 600;refresher=uac
Require: timer
Via: SIP/2.0/UDP 110.10.98.112:5060;received=110.10.98.112;branch=z9hG4bK-s1632-001368532687-1--s1632-
Record-Route: <sip:110.10.98.112:5060;ipcs-line=509453;lr;transport=udp>
To: <sip:16132422192@220.20.2.12>;tag=3545053461-939763
From: "MTS H323 3571"
<sip:6477763571@110.10.98.112>;tag=803e8396c6a8e1147444fc3f6900
Call-ID: 803e8396c6a8e1148444fc3f6900
CSeq: 1 INVITE
Allow: CANCEL, INVITE, BYE, OPTIONS, REGISTER, NOTIFY, INFO, REFER, SUBSCRIBE, PRACK, UPDATE, MESSAGE, PUBLISH
Contact: <sip:16132422192@220.20.2.12:5060>
Content-Type: application/sdp
Accept: application/sdp
Content-Length: 227

v=0
o=nextone-msw-lab-3 470534630 470534630 IN IP4 220.20.2.12
s=sip call
c=IN IP4 220.20.2.13
t=0 0
m=audio 24738 RTP/AVP 18 0 8 101
aptime:20
a=fmtp:18 annexb=no
a=rtpmap:101 telephone-event/8000
a=fmtp:101 0-15

Communication Manager Verification Steps

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

10. Conclusion

These Application Notes describe the configuration necessary to connect Avaya Aura® Communication Manager 6.0.1, Avaya Aura® Session Manager 6.1 and Avaya Session Border Controller for Enterprise 4.0.5 to MTS Allstream SIP Trunking Service. MTS Allstream SIP Trunking Service is a SIP-based Voice over IP solution for customers ranging from small businesses to large the enterprises. MTS Allstream SIP Trunking Service provides a flexible, cost-saving alternative to traditional analog and ISDN-PRI trunks.

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

11. References

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

- [1] *Installing and Configuring Avaya Aura® System Platform*, Release 6.03, February 2011.
- [2] *Administering Avaya Aura® System Platform*, Release 6, June 2010.
- [3] *Administering Avaya Aura® Communication Manager*, Release 6.0, June 2010, Document Number 03-300509.
- [4] *Avaya Aura® Communication Manager Feature Description and Implementation*, Release 6.0, June 2010, Document Number 555-245-205.
- [5] *Installing and Upgrading Avaya Aura® System Manager*, Release 6.1, November 2010.
- [6] *Installing and Configuring Avaya Aura® Session Manager*, Release 6.1, April 2011, Number 03-603473.
- [7] *Administering Avaya Aura® Session Manager*, Release 6.1, May 2011, Document Number 03-603324.
- [8] *Avaya one-X® Deskphone Edition for 9600 Series IP Telephones Administrator Guide*, Release 3.1, November 2009, Document Number 16-300698.
- [9] *Avaya one-X® Deskphone SIP for 9600 Series IP Telephones Administrator Guide*, Release 2.6, June 2010, Document Number 16-601944.
- [10] *Administering Avaya one-X® Communicator*, April 2011.
- [11] *Using Avaya one-X® Communicator*, April 2011.

- [12] *UC-Sec Install Guide (102-5224-400v1.01)*
- [13] *UC-Sec Administration Guide (010-5423-400v106)*
- [14] *RFC 3261 SIP: Session Initiation Protocol*, <http://www.ietf.org/>
- [15] *RFC 3515, The Session Initiation Protocol (SIP) Refer Method*, <http://www.ietf.org/>
- [16] *RFC 2833 RTP Payload for DTMF Digits, Telephony Tones and Telephony Signals*,
<http://www.ietf.org/>
- [17] *RFC 4244, An Extension to the Session Initiation Protocol (SIP) for Request History Information*, <http://www.ietf.org/>

Product documentation for MTS Allstream SIP Trunking Service is available from MTS Allstream.

©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.