Avaya Solution & Interoperability Test Lab

Application Notes for Configuring MTS Allstream SIP Trunking with Avaya Aura® Communication Manager and Avaya Session Border Controller for Enterprise – Issue 1.0

Abstract

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

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

1. Introduction

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

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

2. General Test Approach and Test Results

The general test approach was to connect a simulated enterprise site to the MTS Allstream SIP Trunking service via the public Internet and exercise the features and functionality listed in **Section 2.1**. The simulated enterprise site was comprised of Communication Manager and an Avaya SBCE. Communication Manager was a part of the Avaya Aura® Solution for Midsize Enterprise. However, these compliance test results are applicable to other server and media gateway platforms running similar versions of Communication Manager. Enterprise SIP endpoints are not supported since they require the use of Avaya Aura® Session Manager which is not part of this solution.

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

2.1. Interoperability Compliance Testing

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

- Response to SIP OPTIONS queries.
- Incoming PSTN calls to various phone types including H.323, digital, and analog telephones at the enterprise. All inbound PSTN calls were routed to the enterprise across the SIP trunk from the service provider.
- Outgoing PSTN calls from various phone types including H.323, digital, and analog telephones at the enterprise. All outbound PSTN calls were routed from the enterprise across the SIP trunk to the service provider.
- Inbound and outbound PSTN calls to/from Avaya one-X® Communicator (soft client). Avaya one-X® Communicator can place calls from the local computer or control a remote phone. Both of these modes were tested. Avaya one-X® Communicator was tested with the H.323 protocol.
- Various call types including: local, long distance, outbound toll-free, operator services and local directory assistance (411).

- Codecs G.711MU and G.729A.
- DTMF transmission using RFC 2833.
- Caller ID presentation and Caller ID restriction.
- Response to incomplete call attempts and trunk errors.
- Voicemail navigation for inbound and outbound calls.
- Voicemail Message Waiting Indicator (MWI).
- User features such as hold and resume, internal call forwarding, transfer, and conference.
- Off-net call forwarding and enterprise mobility (extension to cellular).

Items not supported or not tested included the following:

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

2.2. Test Results

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

- **Calling Party Number (PSTN transfers)**: The calling party number displayed on the PSTN phone is not updated to reflect the true connected party on calls that are transferred to the PSTN. After the call transfer is complete, the calling party number displays the number of the transferring party and not the actual connected party. Communication Manager provides the new connected party information by updating the Contact header in a re-INVITE message. MTS Allstream does not use the updated Contact header for displaying calling party information.
- **Local calls from the enterprise routed via the MTS Allstream network to another DID assigned to the enterprise results in no audio.** This problem is believed to have low user impact because all other local calls from the enterprise complete successfully with audio. Audio is only impacted when calling another DID associated with the enterprise and the call is routed via the service provider. At a typical customer site, these calls would not be routed to the service provider but would be routed within the enterprise which avoids the problem. It was also observed that this failure scenario was also related to shuffling because if shuffling was disabled on the service provider trunk then the no audio issue disappeared. However, it is recommended that shuffling remain enabled on the service provider trunk and the failing scenario is avoided by routing these types of calls within the enterprise.

- **Call connection issue with Avaya one-X® Communicator in "Other Phone" mode** – There is a known loss of connection issue during call transfer and conference scenarios with Avaya one-X® Communicator operating in "Other Phone" mode, in conjunction with Communication Manager 6.2. This issue is under investigation by Avaya. Therefore the use of Avaya one-X® Communicator operating in "Other Phone" mode with Communication Manager 6.2 is not recommended with this solution.

2.3. Support

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

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

3. Reference Configuration

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

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

- Communication Manager
- Avaya G450 Media Gateway
- Avaya 1600-Series IP Telephones (H.323)
- Avaya 9600-Series IP Telephones (H.323)
- Avaya one-X® Communicator (H.323)
- Avaya digital and analog telephones

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

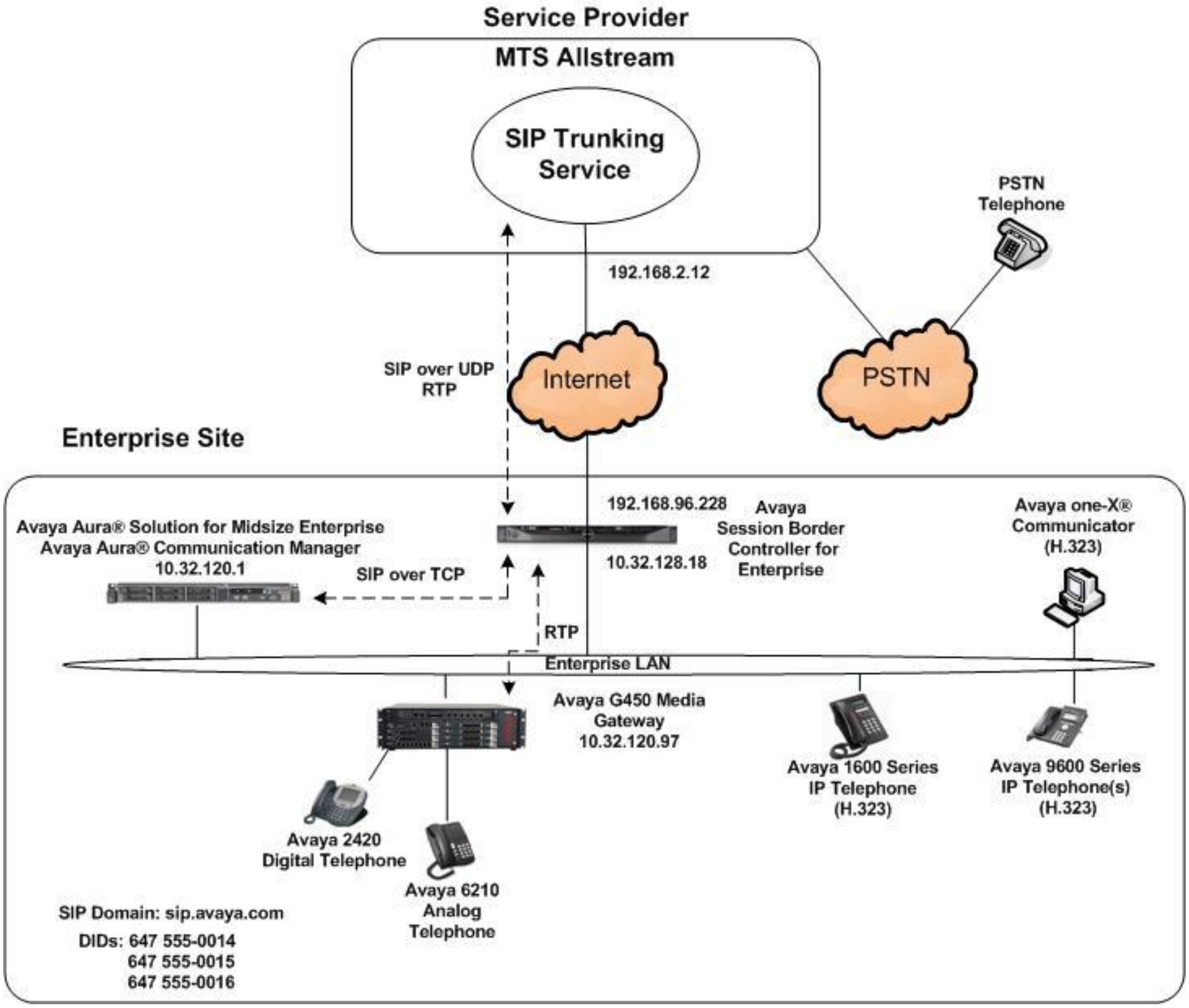

Service Provider
MTS Allstream
SIP Trunking Service
PSTN Telephone
192.168.2.12
SIP over UDP
RTP
Internet
PSTN
Enterprise Site
192.168.96.228
Avaya Session Border Controller for Enterprise
10.32.128.18
Avaya Aura® Solution for Midsize Enterprise
Avaya Aura® Communication Manager
10.32.120.1
SIP over TCP
RTP
Avaya one-X® Communicator (H.323)
Enterprise LAN
Avaya G450 Media Gateway
10.32.120.97
Avaya 1600 Series IP Telephone (H.323)
Avaya 9600 Series IP Telephone(s) (H.323)
Avaya 2420 Digital Telephone
Avaya 6210 Analog Telephone
SIP Domain: sip.avaya.com
DIDs: 647 555-0014
647 555-0015
647 555-0016

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

For inbound calls, the calls flow from the service provider to the Avaya SBCE then to Communication Manager. Once the call arrives at Communication Manager, incoming call treatment, such as incoming digit translations and class of service restrictions may be performed.

Outbound calls to the PSTN are first processed by Communication Manager and may be subject to outbound features such as automatic route selection, digit manipulation and class of service restrictions. Once Communication Manager selects the proper SIP trunk, the call is routed to Avaya SBCE. From the Avaya SBCE, the call is sent to MTS Allstream SIP Trunking.

On outbound calls, MTS Allstream requires a prefix of 11129 be added to the dialed number. For the compliance test, the enterprise sent 11129 + 11 digits in the destination headers (e.g., Request-URI and To) and sent 10 digits in the source headers (e.g., From, Contact, and P-Asserted-Identity (PAI)) of the SIP messaging. MTS Allstream sent 10 digits in both the source and destination headers.

4. Equipment and Software Validated

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

Avaya IP Telephony Solution Components	
Equipment/Software	Release/Version
Avaya Aura® Solution For Midsize Enterprise running on an HP Proliant DL360 Server - Avaya Aura® Communication Manager - Avaya Aura® Communication Manager Messaging - System Platform	6.2 6.2 SP1 (Build R016x.02.0.823.0-19721) 6.2 SP0 (Build CMM-02.0.823.0-0002) 6.0.3.6.3
Avaya G450 Media Gateway	31.22.0
Avaya Session Border Controller for Enterprise running on a Dell R210 V2 server	4.0.5Q09
Avaya 1608 IP Telephone (H.323) running Avaya one-X® Deskphone Value Edition	1.3 SP1
Avaya 9640G IP Telephone (H.323) running Avaya one-X® Deskphone Edition	3.1 SP4 (3.1.04S)
Avaya 9641G IP Telephone (H.323) running Avaya one-X® Deskphone SIP Edition	6.2 SP1 (6.2.1)
Avaya one-X® Communicator (H.323)	6.1 SP3 Patch 3 (Build 6.1.3.09-SP3-Patch3-35953)
Avaya 2420 Digital Telephone	n/a
Avaya 6210 Analog Telephone	n/a
MTS Allstream SIP Trunking Solution Components	
Equipment/Software	Release/Version
Genband S3 Session Border Controller	5.2.2.12
Nortel CS2K	CVM13

Table 1: Equipment and Software Tested

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

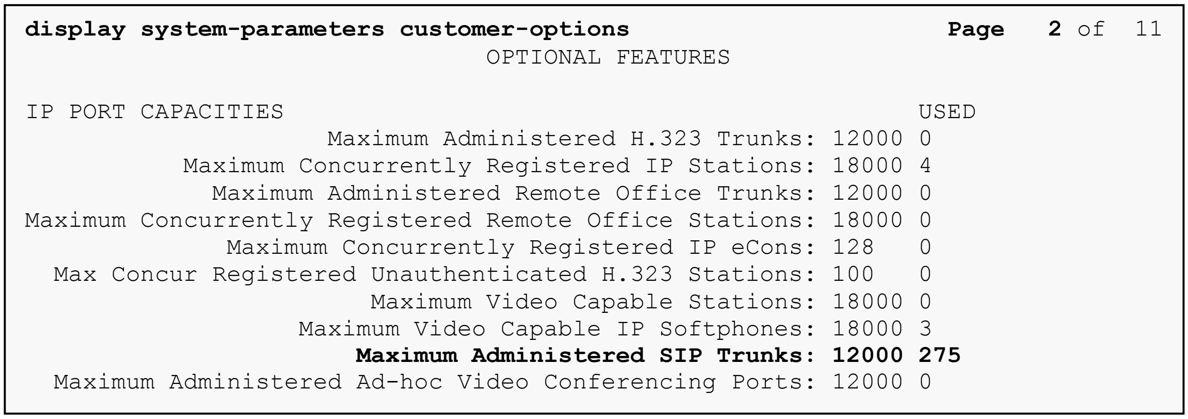
5. Configure Avaya Aura® Communication Manager

This section describes the procedure for configuring Communication Manager for MTS Allstream SIP Trunking. A SIP trunk is established between Communication Manager and Avaya SBCE for use by signaling traffic to and from MTS Allstream. It is assumed the general installation of Communication Manager and Avaya G450 Media Gateway has been previously completed and is not discussed here.

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

5.1. Licensing and Capacity

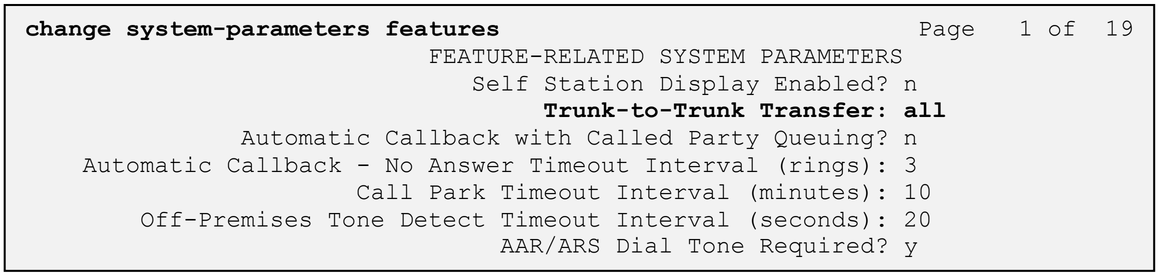
Use the **display system-parameters customer-options** command to verify that the **Maximum Administered SIP Trunks** value on **Page 2** is sufficient to support the desired number of simultaneous SIP calls across all SIP trunks at the enterprise including any trunks to the service provider. The example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



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

IP PORT CAPACITIES                                              USED
                     Maximum Administered H.323 Trunks: 12000 0
           Maximum Concurrently Registered IP Stations: 18000 4
             Maximum Administered Remote Office Trunks: 12000 0
Maximum Concurrently Registered Remote Office Stations: 18000 0
              Maximum Concurrently Registered IP eCons: 128   0
  Max Concur Registered Unauthenticated H.323 Stations: 100   0
                        Maximum Video Capable Stations: 18000 0
                   Maximum Video Capable IP Softphones: 18000 3
                       Maximum Administered SIP Trunks: 12000 275
  Maximum Administered Ad-hoc Video Conferencing Ports: 12000 0
```

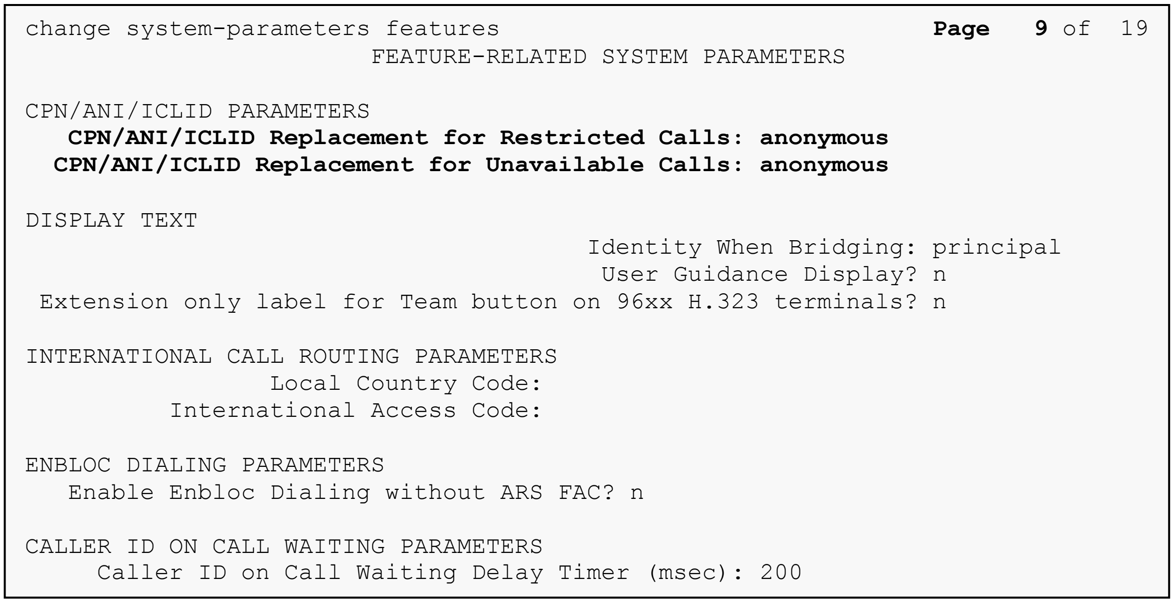
5.2. System Features

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



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

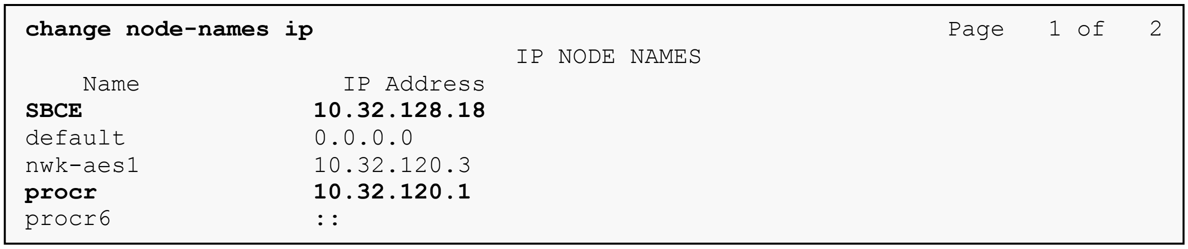
On **Page 9,** verify that a text string has been defined to replace the Calling Party Number (CPN) for restricted or unavailable calls. This text string is entered in the two fields highlighted below. The compliance test used the value of **anonymous** for both.



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

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

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

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

ENBLOC DIALING PARAMETERS
   Enable Enbloc Dialing without ARS FAC? n

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

5.3. IP Node Names

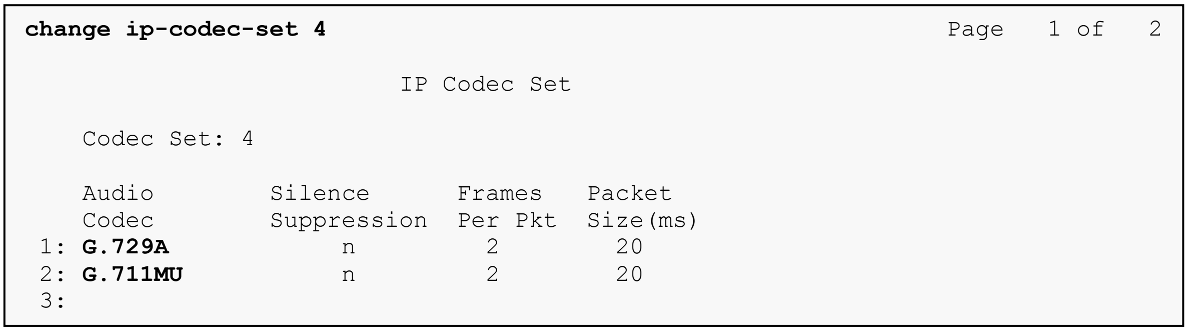
Use the **change node-names ip** command to verify that node names have been previously defined for the IP addresses of the server running Communication Manager **(procr**) and for Avaya SBCE (**SBCE**). These node names will be needed for defining the service provider signaling group in **Section 5.6**.



```
change node-names ip                                            Page   1 of   2
                                  IP NODE NAMES
    Name              IP Address
SBCE                 10.32.128.18
default              0.0.0.0
nwk-aes1             10.32.120.3
procr                10.32.120.1
procr6               ::
```

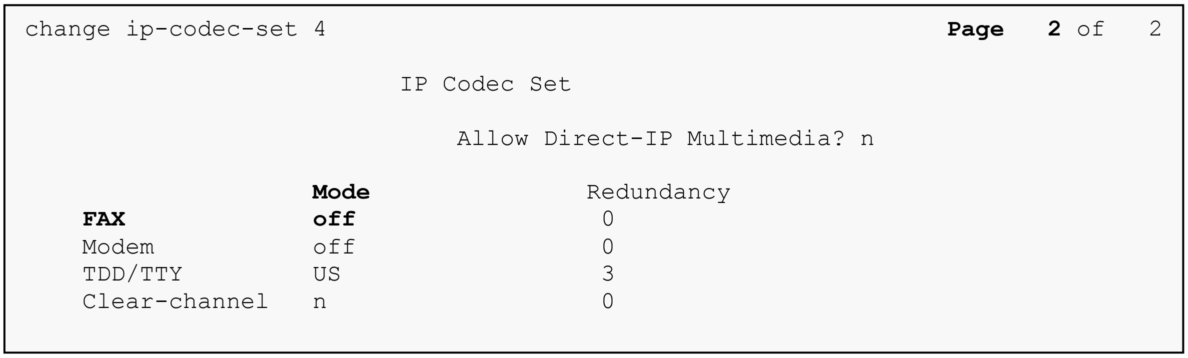
5.4. Codecs

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



```
change ip-codec-set 4                                           Page   1 of   2

                          IP Codec Set

    Codec Set: 4

    Audio        Silence      Frames   Packet
    Codec        Suppression  Per Pkt  Size(ms)
 1: G.729A           n          2        20
 2: G.711MU          n          2        20
 3:
```

On **Page 2**, set the **Fax Mode** to **off**. MTS Allstream does not support T.38 fax.

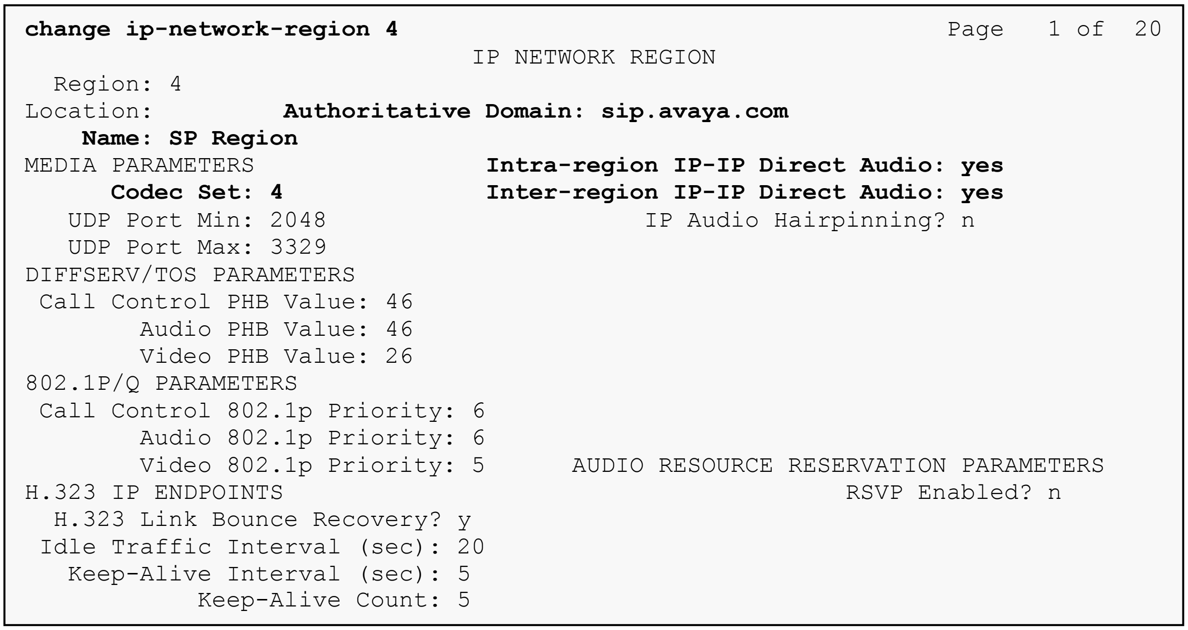


```
change ip-codec-set 4                                          Page   2 of   2

                          IP Codec Set

                              Allow Direct-IP Multimedia? n

                    Mode                Redundancy
    FAX             off                  0
    Modem           off                  0
    TDD/TTY         US                   3
    Clear-channel   n                    0
```

5.5. IP Network Region

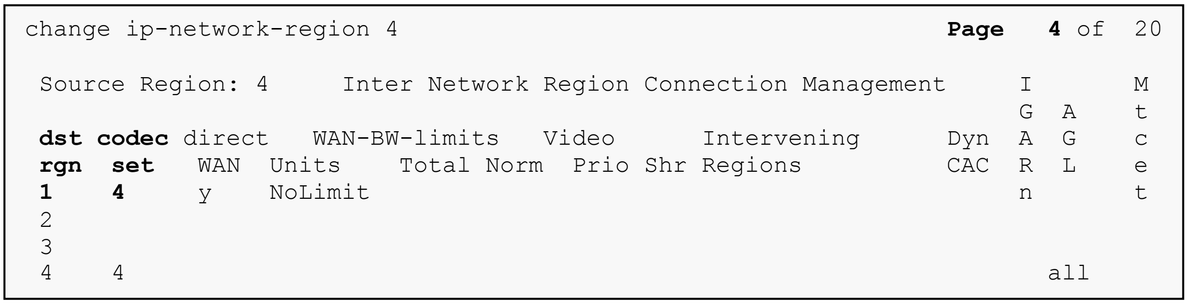
Create a separate IP network region for the service provider trunk. This allows for separate codec or quality of service settings to be used (if necessary) for calls between the enterprise and the service provider versus calls within the enterprise or elsewhere. For the compliance test, IP-network-region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

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



```
change ip-network-region 4                                      Page   1 of  20
                               IP NETWORK REGION
  Region: 4
Location:         Authoritative Domain: sip.avaya.com
    Name: SP Region
MEDIA PARAMETERS                Intra-region IP-IP Direct Audio: yes
      Codec Set: 4              Inter-region IP-IP Direct Audio: yes
   UDP Port Min: 2048                      IP Audio Hairpinning? n
   UDP Port Max: 3329
DIFFSERV/TOS PARAMETERS
 Call Control PHB Value: 46
        Audio PHB Value: 46
        Video PHB Value: 26
802.1P/Q PARAMETERS
 Call Control 802.1p Priority: 6
        Audio 802.1p Priority: 6
        Video 802.1p Priority: 5      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 4 and region 1. Enter the desired IP codec set in the **codec set** column of the row with destination region (**dst rgn**) 1. Default values may be used for all other fields. The example below shows the settings used for the compliance test. It indicates that codec set 4 will be used for calls between region 4 (the service provider region) and region 1 (the rest of the enterprise). Creating this table entry for IP network region 4 will automatically create a complementary table entry on the IP network region 1 form for destination region 4. This complementary table entry can be viewed using the **display ip-network-region 1** command and navigating to **Page 4** (not shown).



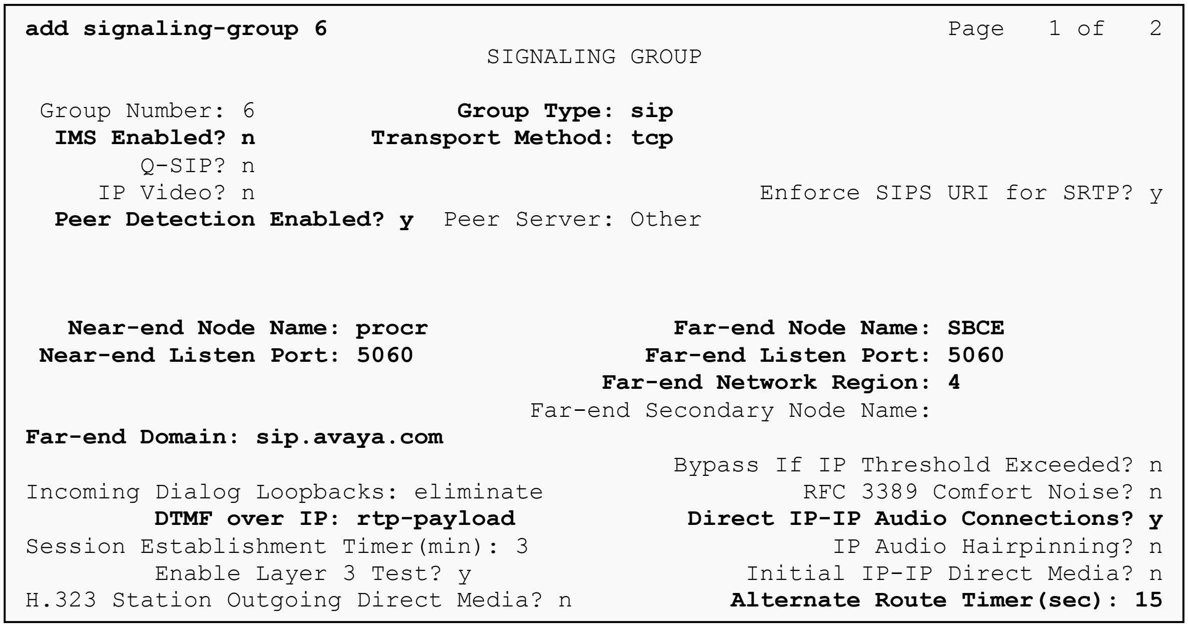
```
change ip-network-region 4                                      Page   4 of  20

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

5.6. Signaling Group

Use the **add signaling-group** command to create a signaling group between Communication Manager and Avaya SBCE for use by the service provider trunk. This signaling group is used for inbound and outbound calls between the service provider and the enterprise. For the compliance test, signaling group 6 was used for this purpose and was configured using the parameters highlighted below.

- Set the **Group Type** field to **sip**.
- Set the **Transport Method** to the value of **tcp**. The transport method specified here is used between Communication Manager and Avaya SBCE.
- Set the **IMS Enabled** field to **n**.
- Set the **Peer Detection Enabled** field to **y**. The **Peer-Server** field will initially be set to **Others** and can not be changed via administration.
- Set the **Near-end Node Name** to **procr**. This node name maps to the IP address of Communication Manager as defined in **Section 5.3**.
- Set the **Far-end Node Name** to **SBCE**. This node name maps to the IP address of Avaya SBCE as defined in **Section 5.3**.
- Set the **Near-end Listen Port** and **Far-end Listen Port** to **5060**. Port 5060 is the well-known port value for SIP over TCP.
- Set the **Far-end Network Region** to the IP network region defined for the service provider in **Section 5.5**.
- Set the **Far-end Domain** to the domain of the enterprise.
- Set **Direct IP-IP Audio Connections** to **y**. This field will enable media shuffling on the SIP trunk allowing Communication Manager to redirect media traffic directly between the SIP trunk and the enterprise endpoint.
- Set the **DTMF over IP** field to **rtp-payload**. This value enables Communication Manager to send DTMF transmissions using RFC 2833.

- Set the **Alternate Route Timer** to **15**. This defines the number of seconds that Communication Manager will wait for a response (other than 100 Trying) to an outbound INVITE before selecting another route. If an alternate route is not defined, then the call is cancelled after this interval.
- Default values may be used for all other fields.

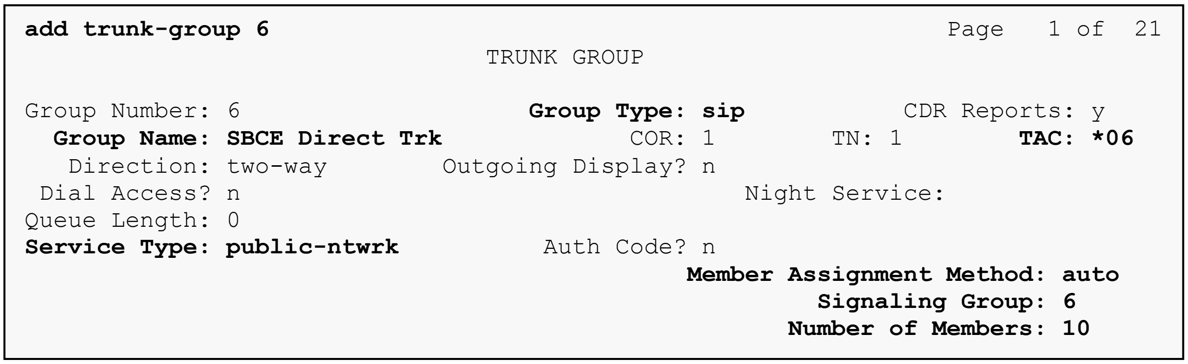


```
add signaling-group 6                                           Page   1 of   2
                                SIGNALING GROUP

 Group Number: 6              Group Type: sip
  IMS Enabled? n        Transport Method: tcp
        Q-SIP? n
     IP Video? n                                   Enforce SIPS URI for SRTP? y
  Peer Detection Enabled? y  Peer Server: Other



   Near-end Node Name: procr                 Far-end Node Name: SBCE
 Near-end Listen Port: 5060                Far-end Listen Port: 5060
                                        Far-end Network Region: 4
                                   Far-end Secondary Node Name:
Far-end Domain: sip.avaya.com
                                             Bypass If IP Threshold Exceeded? n
Incoming Dialog Loopbacks: eliminate                  RFC 3389 Comfort Noise? n
         DTMF over IP: rtp-payload            Direct IP-IP Audio Connections? y
Session Establishment Timer(min): 3                     IP Audio Hairpinning? n
         Enable Layer 3 Test? y                   Initial IP-IP Direct Media? n
H.323 Station Outgoing Direct Media? n           Alternate Route Timer(sec): 15
```

5.7. Trunk Group

Use the **add trunk-group** command to create a trunk group for the signaling group created in **Section 5.6**. For the compliance test, trunk group 6 was configured using the parameters highlighted below.

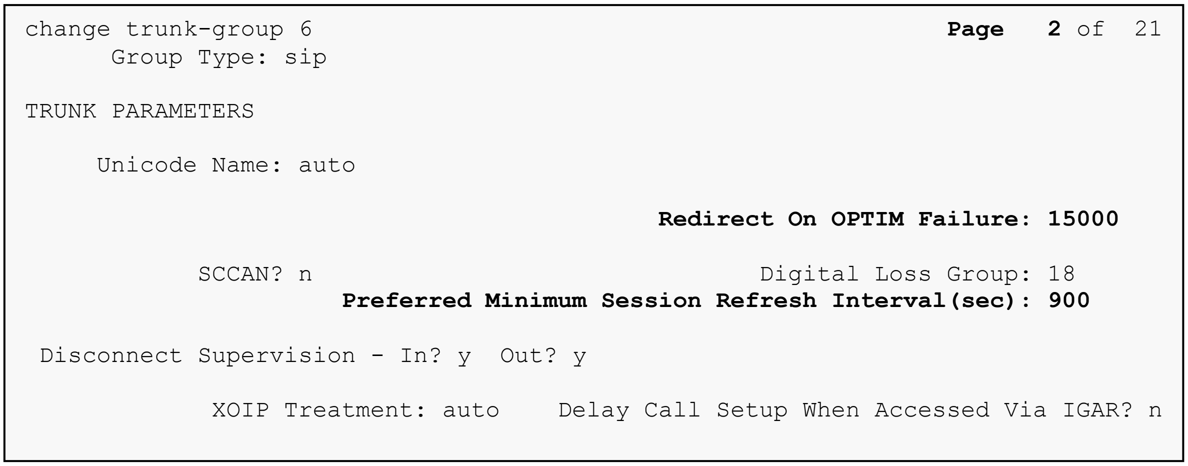
- Set the **Group Type** field to **sip**.
- Enter a descriptive name for the **Group Name**.
- Enter an available trunk access code (TAC) that is consistent with the existing dial plan in the **TAC** field.
- Set the **Service Type** field to **public-ntwrk**.
- Set **Member Assignment Method** to **auto**.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



```
add trunk-group 6                                               Page   1 of  21
                                TRUNK GROUP

Group Number: 6                    Group Type: sip           CDR Reports: y
  Group Name: SBCE Direct Trk             COR: 1        TN: 1        TAC: *06
   Direction: two-way        Outgoing Display? n
 Dial Access? n                                    Night Service:
Queue Length: 0
Service Type: public-ntwrk          Auth Code? n
                                              Member Assignment Method: auto
                                                       Signaling Group: 6
                                                     Number of Members: 10
```

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

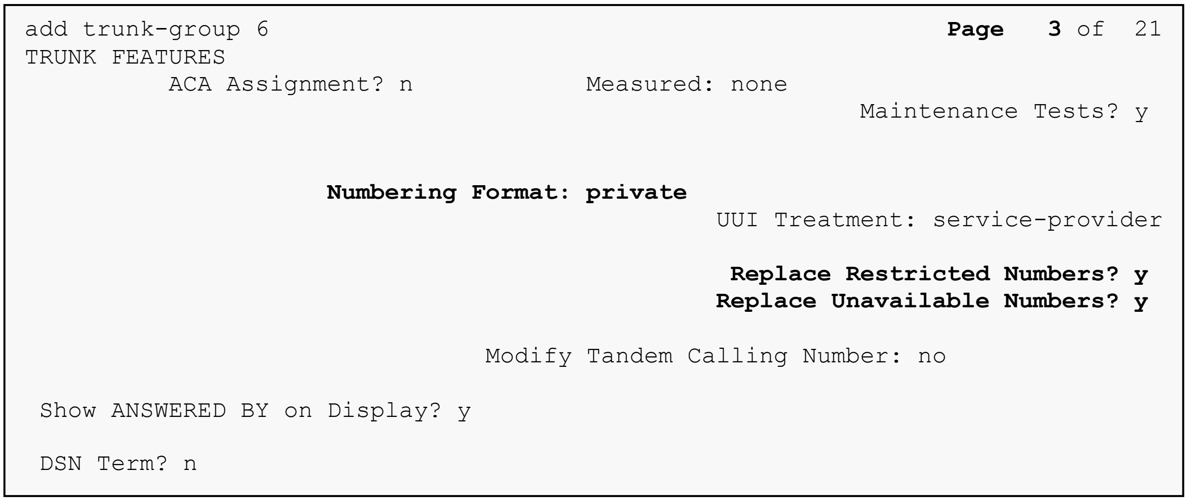
Verify that the **Preferred Minimum Session Refresh Interval** is set to a value acceptable to the service provider. This value defines the interval that re-INVITEs must be sent to keep the active session alive. For the compliance test, the value of **900** seconds was used.



```
change trunk-group 6                                            Page   2 of  21
      Group Type: sip

TRUNK PARAMETERS

     Unicode Name: auto

                                            Redirect On OPTIM Failure: 15000

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

 Disconnect Supervision - In? y  Out? y

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

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

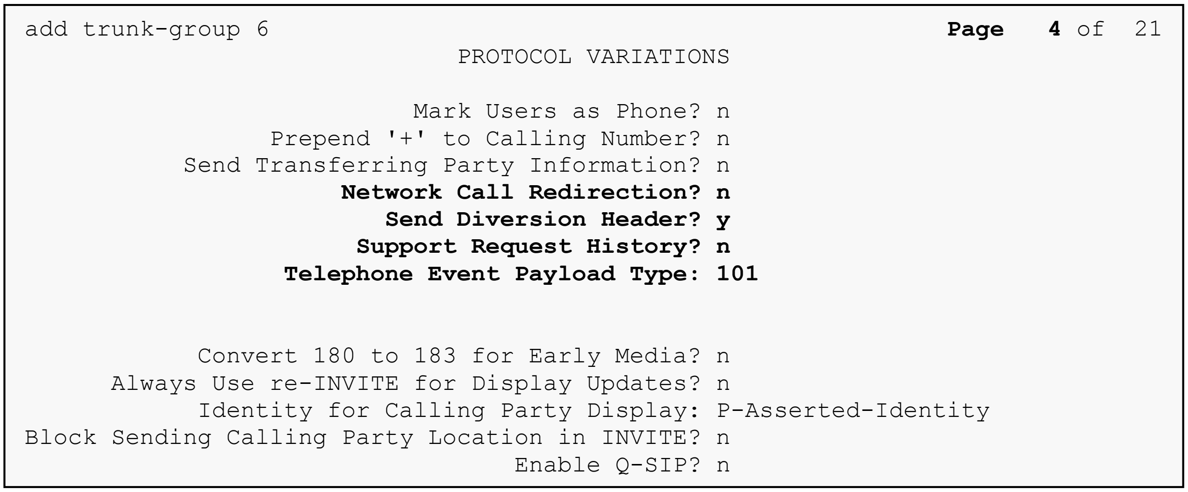
Set the **Replace Restricted Numbers** and **Replace Unavailable Numbers** fields to **y**. This will allow the CPN displayed on local endpoints to be replaced with the value set in **Section 5.2**, if the inbound call enabled CPN block. For outbound calls, these same settings request that CPN block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



```
add trunk-group 6                                               Page   3 of  21
TRUNK FEATURES
          ACA Assignment? n           Measured: none
                                                          Maintenance Tests? y


                     Numbering Format: private
                                                UUI Treatment: service-provider

                                                 Replace Restricted Numbers? y
                                                Replace Unavailable Numbers? y

                                Modify Tandem Calling Number: no

 Show ANSWERED BY on Display? y

 DSN Term? n
```

On **Page 4**, set the **Network Call Redirection** field to **n**. Set the **Send Diversion Header** field to **y** and the **Support Request History** field to **n**. The **Send Diversion Header** field provides additional information to the network if the call has been re-directed. These settings are needed by MTS Allstream to support call forwarding of inbound calls back to the PSTN and some Extension to Cellular (EC500) call scenarios.

Set the **Telephone Event Payload Type** to **101**, the value preferred by MTS Allstream.



```
add trunk-group 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? n
                         Send Diversion Header? y
                       Support Request History? n
                  Telephone Event Payload Type: 101


            Convert 180 to 183 for Early Media? n
      Always Use re-INVITE for Display Updates? n
            Identity for Calling Party Display: P-Asserted-Identity
Block Sending Calling Party Location in INVITE? n
                                  Enable Q-SIP? n
```

5.8. Calling Party Information

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

In the sample configuration, three DID numbers were assigned for testing. These three numbers were assigned to the three extensions **50003**, **50005** and **50006**. Thus, these same 10-digit numbers were used in the outbound calling party information on the service provider trunk when calls were originated from these three extensions.

```
change private-numbering 0                                        Page   1 of   2
                           NUMBERING - PRIVATE FORMAT

Ext Ext             Trk        Private      Total
Len Code            Grp(s)     Prefix        Len
                                                  Total Administered: 4
 5  5                                        5       Maximum Entries: 240
 5  50003          6         6475550014      10
 5  50005          6         6475550015      10
 5  50006          6         6475550016      10
```

In a real customer environment, normally the DID number is comprised of the local extension plus a prefix. If this is true, then a single private numbering entry can be applied for all extensions. In the example below, all stations with a 5-digit extension beginning with **5** and using trunk **6** 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 Ext             Trk        Private      Total
Len Code            Grp(s)     Prefix        Len
                                                  Total Administered: 2
 5  5                                        5      Maximum Entries: 240
 5  5              6         64755           10
```

In addition, each entry created in the Private Numbering table must be repeated in the Public Unknown Numbering table using the **change public-unknown-numbering 0** command. This is needed to ensure that the SIP Diversion header, which is used in call forwarding and EC500 scenarios, has the correct calling party information. This is not necessary if Communication Manager is connected to Session Manager.

```
change public-unknown-numbering 0                               Page   1 of   2
                      NUMBERING - PUBLIC/UNKNOWN FORMAT
                                           Total
Ext Ext           Trk       CPN             CPN
Len Code          Grp(s)    Prefix          Len
                                                  Total Administered: 3
 5  50003         6         6475550014      10       Maximum Entries: 9999
 5  50005         6         6475550015      10
 5  50006         6         6475550016      10    Note: If an entry applies to
                                                  a SIP connection to Avaya
                                                  Aura(R) Session Manager,
                                                  the resulting number must
                                                  be a complete E.164 number.
```

5.9. Outbound Routing

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

```
change dialplan analysis                                        Page   1 of  12
                             DIAL PLAN ANALYSIS TABLE
                                   Location: all           Percent Full: 2

    Dialed   Total  Call      Dialed   Total  Call      Dialed   Total  Call
    String   Length Type      String   Length Type      String   Length Type
   0            1   attd
   1            5   ext
   5            5   ext
   9            1   fac
   *            3   dac
   #            3   dac
```

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

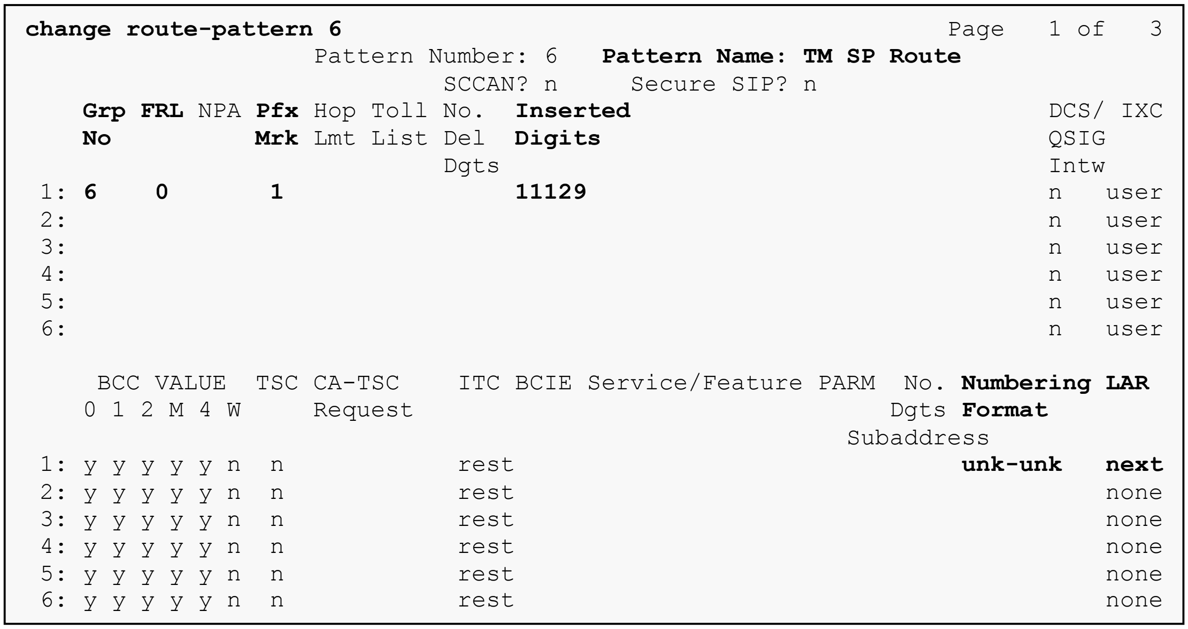
```
change feature-access-codes                                     Page   1 of  11
                               FEATURE ACCESS CODE (FAC)
         Abbreviated Dialing List1 Access Code: *10
         Abbreviated Dialing List2 Access Code: *12
         Abbreviated Dialing List3 Access Code: *13
Abbreviated Dial - Prgm Group List Access Code: *14
                      Announcement Access Code: *19
                       Answer Back Access Code:

      Auto Alternate Routing (AAR) Access Code: *00
    Auto Route Selection (ARS) - Access Code 1: 9     Access Code 2:
                 Automatic Callback Activation: *33    Deactivation: #33
Call Forwarding Activation Busy/DA: *30    All: *31    Deactivation: #30
   Call Forwarding Enhanced Status:        Act:        Deactivation:
```

Use the **change ars analysis** command to configure the routing of dialed digits following the first digit 9. The example below shows a subset of the dialed strings tested as part of the compliance test. See **Section 2.1** for the complete list of call types tested. All dialed strings are mapped to route pattern 6 which contains the SIP trunk to the service provider (as defined next).

```
change ars analysis 0                                           Page   1 of   2
                            ARS DIGIT ANALYSIS TABLE
                                  Location: all          Percent Full: 1

          Dialed           Total     Route    Call   Node  ANI
          String          Min  Max  Pattern   Type   Num   Reqd
    0                     1    1     6        op           n
    0                     11   11    6        op           n
    011                   10   18    6        intl         n
    1732                  11   11    6        fnpa         n
    1800                  11   11    6        fnpa         n
    1877                  11   11    6        fnpa         n
    1908                  11   11    6        fnpa         n
    411                   3    3     6        svcl         n
    647555                10   10    6        natl         n
```

The route pattern defines which trunk group will be used for the call and performs any necessary digit manipulation. Use the **change route-pattern** command to configure the parameters for the service provider route pattern in the following manner. The example below shows the values used for route pattern 6 during the compliance test.

- **Pattern Name**: Enter a descriptive name.
- **Grp No**: Enter the outbound trunk group for the SIP service provider. For the compliance test, trunk group 6 was used.
- **FRL**: Set the Facility Restriction Level (**FRL**) field to a level that allows access to this trunk for all users that require it. The value of **0** is the least restrictive level.
- **Pfx Mrk**: **1** The prefix mark (**Pfx Mrk**) of one will prefix any FNPA 10-digit number with a 1 and leave numbers of any other length unchanged. This will ensure 1 + 10 digits are sent to the service provider for long distance North American Numbering Plan (NANP) numbers.
- **Inserted Digits**: Set to **11129**. This is the prefix required on the dialed number for all outbound calls to MTS Allstream.
- **Numbering Format**: **unk-unk** All calls using this route pattern will use the private numbering table. See setting of the **Numbering Format** in the trunk group form for full details in **Section 5.7**.
- **LAR**: **next**



```
change route-pattern 6                                          Page   1 of   3
                    Pattern Number: 6   Pattern Name: TM SP Route
                             SCCAN? n     Secure SIP? n
    Grp FRL NPA Pfx Hop Toll No.  Inserted                             DCS/ IXC
    No          Mrk Lmt List Del  Digits                               QSIG
                             Dgts                                      Intw
 1: 6    0       1               11129                                 n   user
 2:                                                                    n   user
 3:                                                                    n   user
 4:                                                                    n   user
 5:                                                                    n   user
 6:                                                                    n   user

     BCC VALUE  TSC CA-TSC    ITC BCIE Service/Feature PARM  No. Numbering LAR
    0 1 2 M 4 W     Request                                 Dgts Format
                                                         Subaddress
 1: y y y y y n  n            rest                                 unk-unk   next
 2: y y y y y n  n            rest                                           none
 3: y y y y y n  n            rest                                           none
 4: y y y y y n  n            rest                                           none
 5: y y y y y n  n            rest                                           none
 6: y y y y y n  n            rest                                           none
```

5.10. Incoming Call Handling Treatment

Incoming call handling treatment is used to manipulate incoming numbers on a particular trunk to facilitate routing of the call to its destination. To map incoming DID numbers on the service provider trunk (trunk group 6) to an internal extension, use the **inc-call-handling-trmt trunk-group 6** command. Set the following:

- Set the **Service/Feature** field to **public-ntwrk**.
- Set the **Number Len** field to the number of digits to use when matching the incoming number.
- Set the **Number Digits** field to the incoming number to match on.
- Set the **Del** field to the number of digits to delete from the incoming number.
- Set the **Insert** field to the internal extension that will replace the deleted 10 digits.

```
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 6475550014       10  50003
 public-ntwrk    10 6475550015       10  50005
 public-ntwrk    10 6475550016       10  50006
 public-ntwrk
```

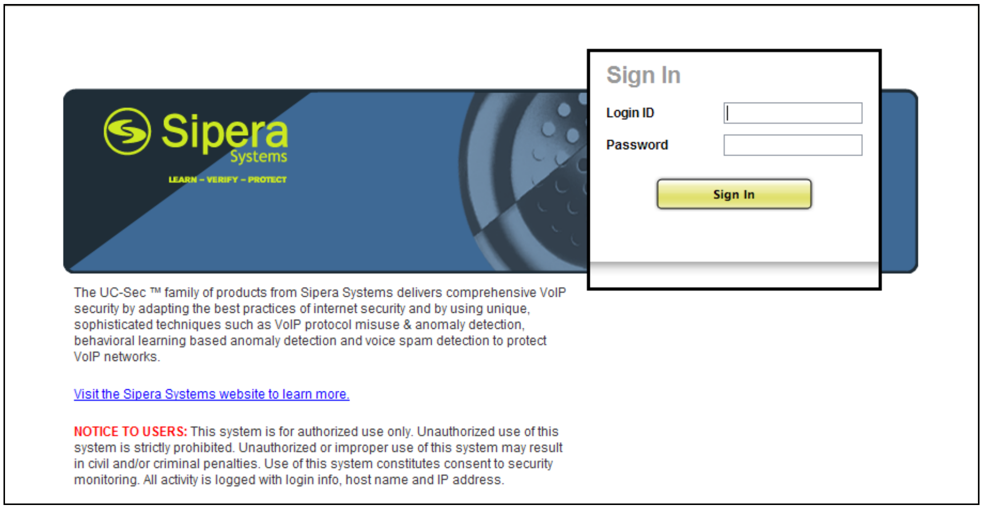
6. Configure Avaya Session Border Controller for Enterprise

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

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

6.1. Access the Management Interface

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

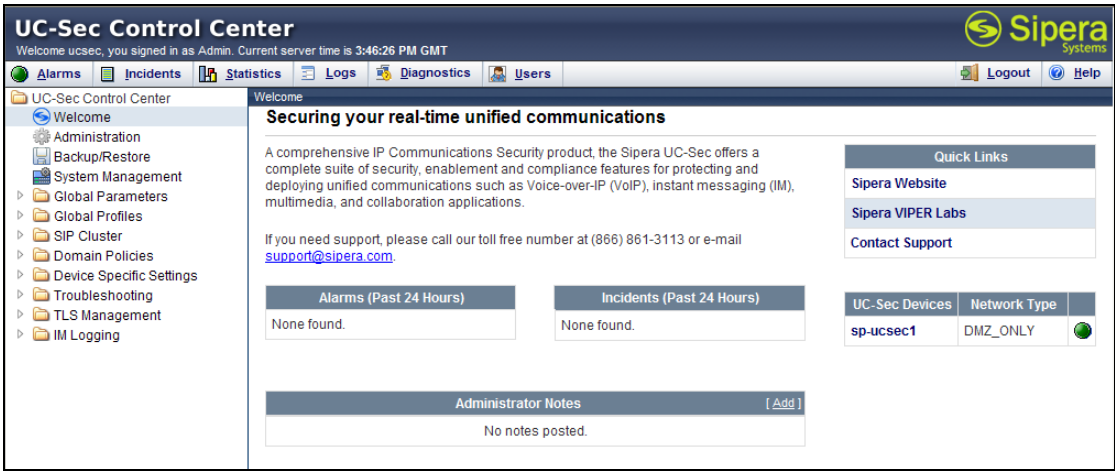


The UC-Sec ™ family of products from Sipera Systems delivers comprehensive VoIP security by adapting the best practices of internet security and by using unique, sophisticated techniques such as VoIP protocol misuse & anomaly detection, behavioral learning based anomaly detection and voice spam detection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

Visit the Sipera Systems website to learn more.

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

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



Welcome ucsec, you signed in as Admin. Current server time is 3:46:26 PM GMT

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)
None found.

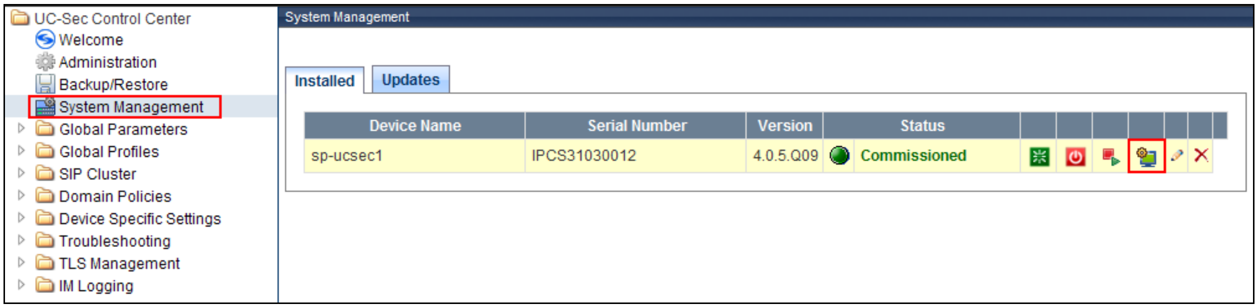
Incidents (Past 24 Hours)
None found.

UC-Sec Devices	Network Type	
sp-ucsec1	DMZ_ONLY	●

Administrator Notes
No notes posted.

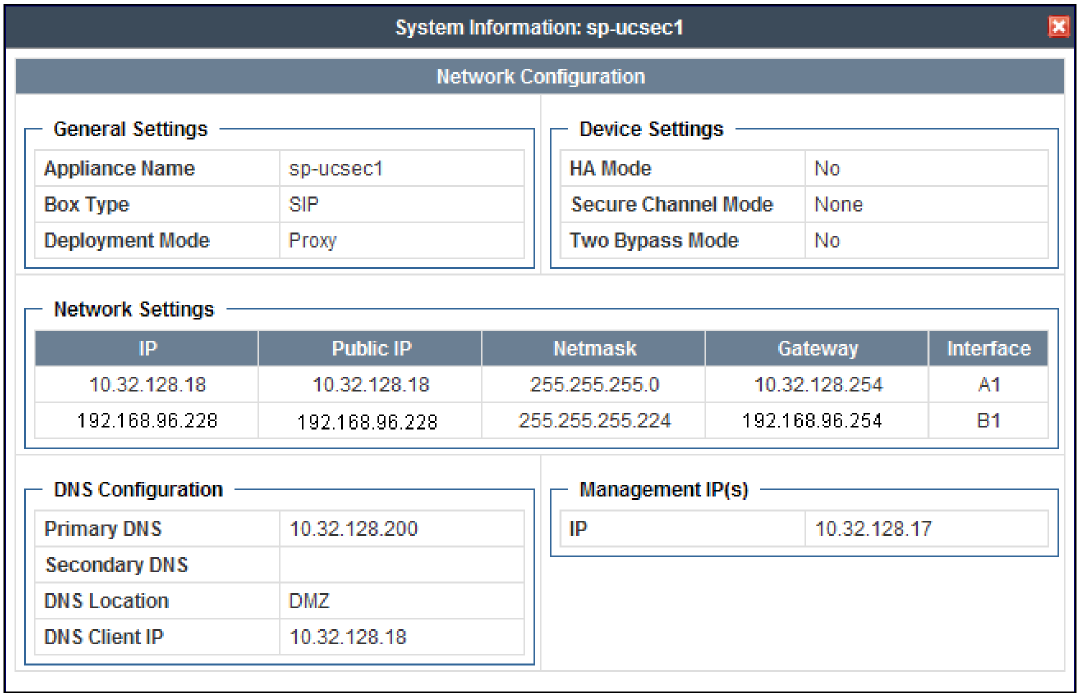
6.2. Verify Network Configuration and Enable Interfaces

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



Device Name	Serial Number	Version	Status
sp-ucsec1	IPCS31030012	4.0.5.Q09	● Commissioned

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



System Information: sp-ucsec1

Network Configuration

General Settings

Appliance Name	sp-ucsec1
Box Type	SIP
Deployment Mode	Proxy

Device Settings

HA Mode	No
Secure Channel Mode	None
Two Bypass Mode	No

Network Settings

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

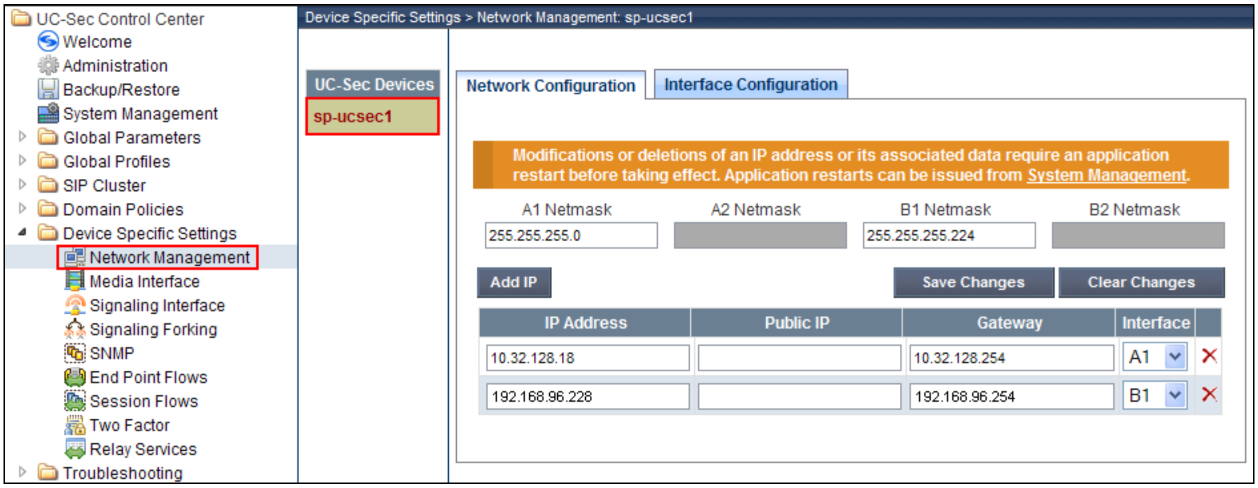
DNS Configuration

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

Management IP(s)

IP	10.32.128.17

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



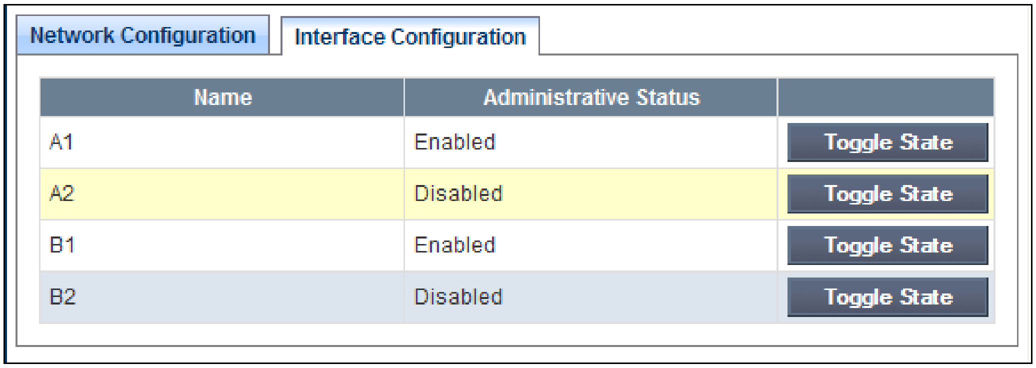
Device Specific Settings > Network Management: sp-ucsec1

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	A2 Netmask	B1 Netmask	B2 Netmask
255.255.255.0		255.255.255.224	

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

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



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

6.3. Signaling Interface

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

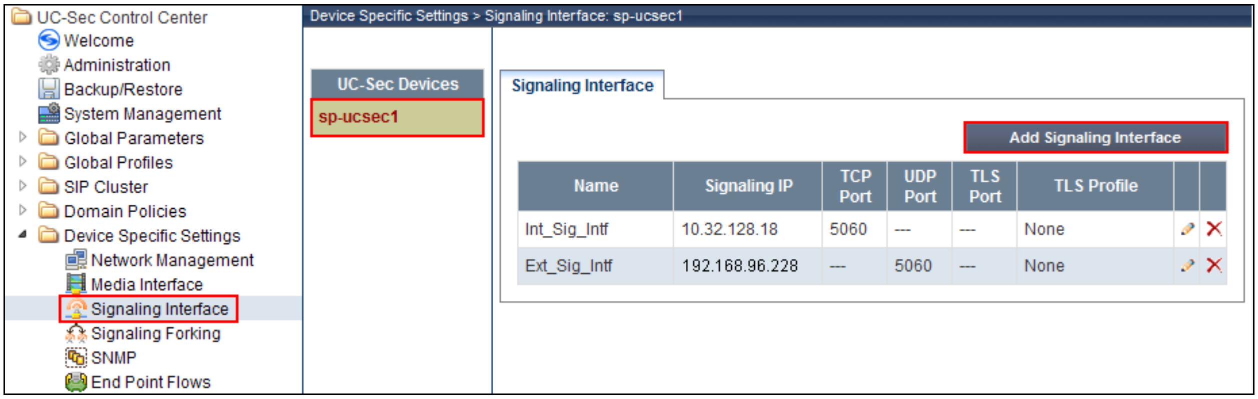
To create a new interface, navigate to **Device Specific Settings → Signaling Interface** in the left pane. In the center pane, select the Avaya SBCE device (**sp-ucsec1**) to be managed. In the right pane, select **Add Signaling Interface**. A pop-up window (not shown) will appear requesting the name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

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

- Set **Name** to a descriptive name.
- Set the **Signaling IP** to the IP address associated with the private interface (A1) defined in **Section 6.2**.
- Set **TCP port** to the port the Avaya SBCE will listen on for SIP requests from Communication Manager.

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

- Set **Name** to a descriptive name.
- Set the **Signaling IP** to the IP address associated with the public interface (B1) defined in **Section 6.2**.
- Set **UDP port** to the port the Avaya SBCE will listen on for SIP requests from the service provider.



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

6.4. Media Interface

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

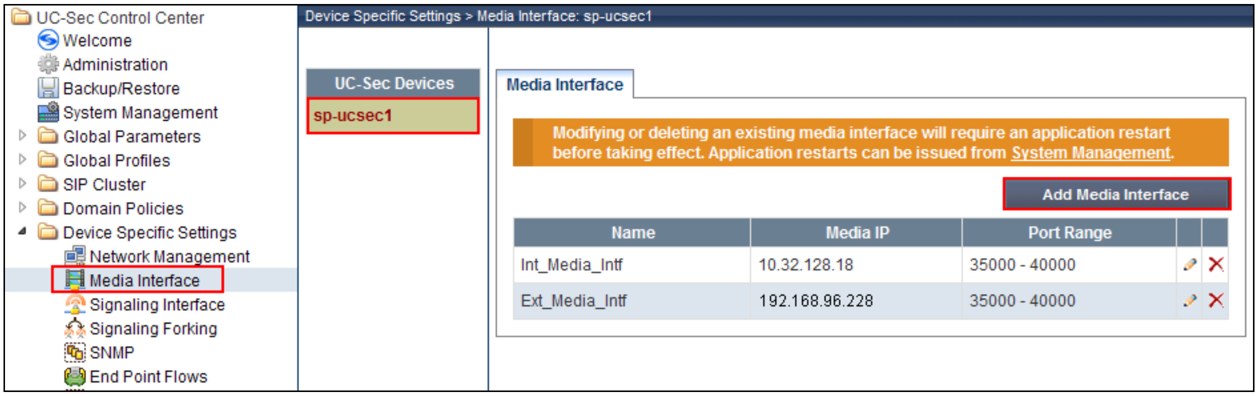
To create a new interface, navigate to **Device Specific Settings → Media Interface** in the left pane. In the center pane, select the Avaya SBCE device (**sp-ucsec1**) to be managed. In the right pane, select **Add Media Interface**. A pop-up window (not shown) will appear requesting the name of the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

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

- Set **Name** to a descriptive name.
- Set the **Media IP** to the IP address associated with the private interface (A1) defined in **Section 6.2**.
- Set **Port Range** to a range of ports acceptable to both the Avaya SBCE and Communication Manager. For the compliance test, the port range used was selected arbitrarily.

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

- Set **Name** to a descriptive name.
- Set the **Media IP** to the IP address associated with the public interface (B1) defined in **Section 6.2**.
- Set **Port Range** to a range of ports acceptable to both the Avaya SBCE and the service provider. For the compliance test, the port range used was selected arbitrarily.



Device Specific Settings > Media Interface: sp-ucsec1

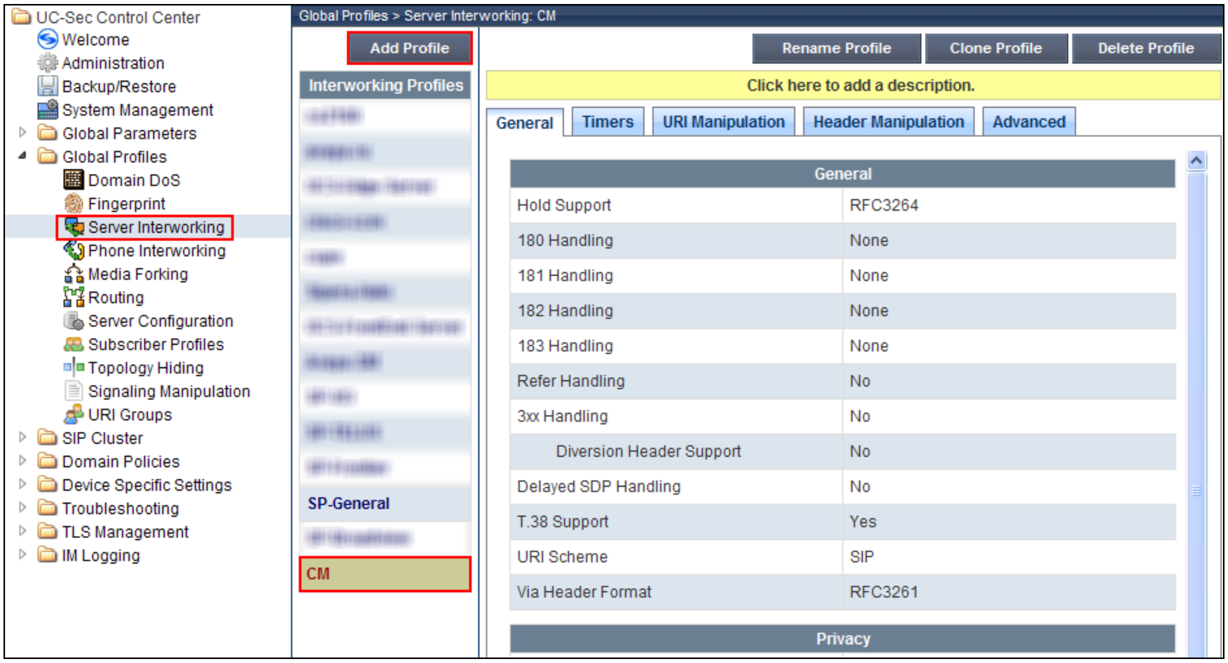
Modifying or deleting an existing media interface will require an application restart before taking effect. Application restarts can be issued from System Management.

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

6.5. Server Interworking

A server interworking profile defines a set of parameters that aid in interworking between the Avaya SBCE and a connected server. Create a server interworking profile for Communication Manager and the service provider SIP server. These profiles will be applied to the appropriate server in **Section 6.6.1** and **6.6.2**.

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

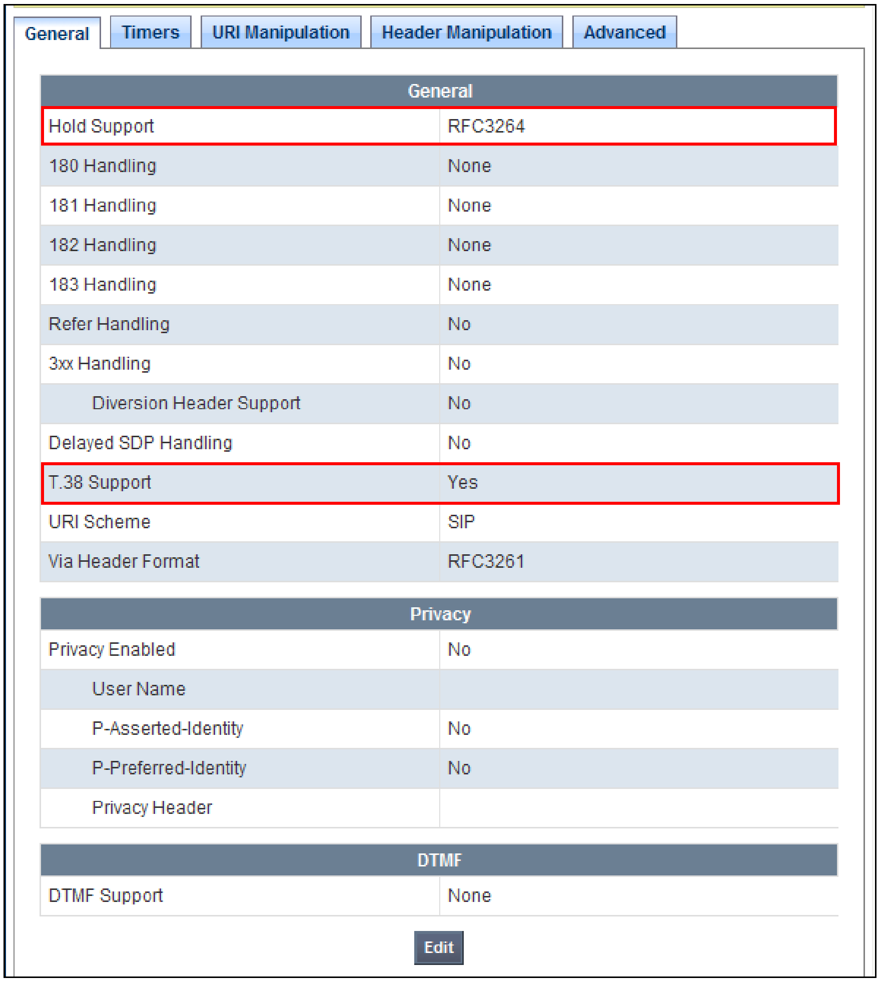


General	
Hold Support	RFC3264
180 Handling	None
181 Handling	None
182 Handling	None
183 Handling	None
Refer Handling	No
3xx Handling	No
Diversion Header Support	No
Delayed SDP Handling	No
T.38 Support	Yes
URI Scheme	SIP
Via Header Format	RFC3261

6.5.1. Server Interworking – Communication Manager

For the compliance test, server interworking profile **CM** was created for Communication Manager. When creating the profile, configure the General tab parameters as follows:

- Set **Hold Support** to **RFC3264.**
- Enable **T.38 Support**.

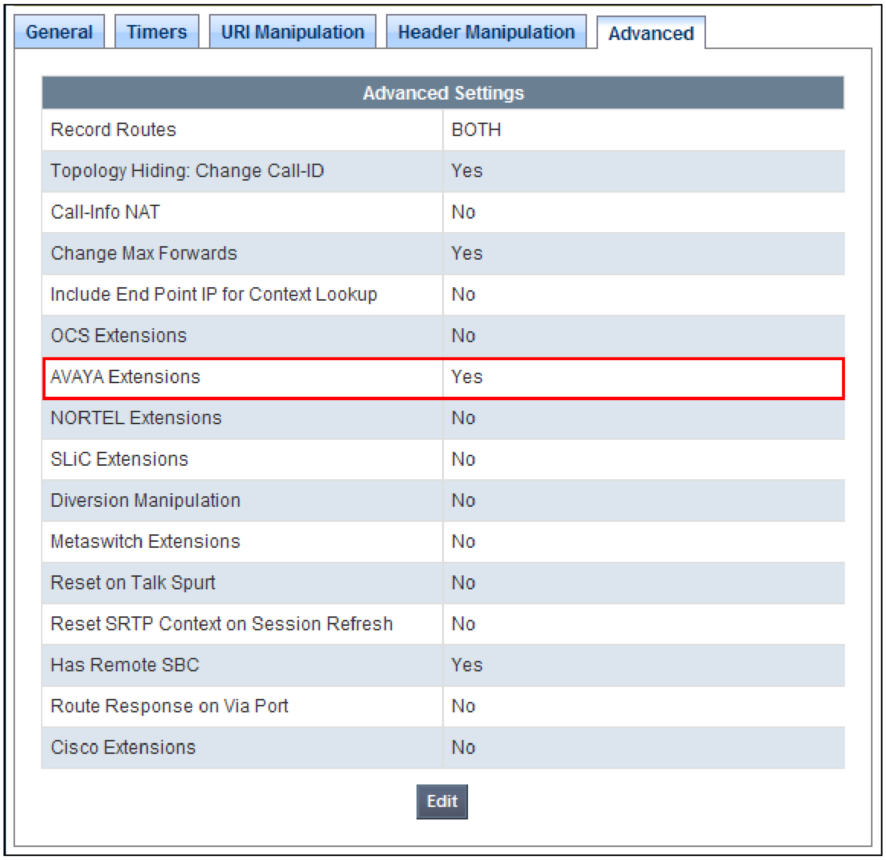


General	
Hold Support	RFC3264
180 Handling	None
181 Handling	None
182 Handling	None
183 Handling	None
Refer Handling	No
3xx Handling	No
Diversion Header Support	No
Delayed SDP Handling	No
T.38 Support	Yes
URI Scheme	SIP
Via Header Format	RFC3261

Privacy	
Privacy Enabled	No
User Name	
P-Asserted-Identity	No
P-Preferred-Identity	No
Privacy Header	

DTMF	
DTMF Support	None

On the Advanced tab, enable the **Avaya Extensions**.

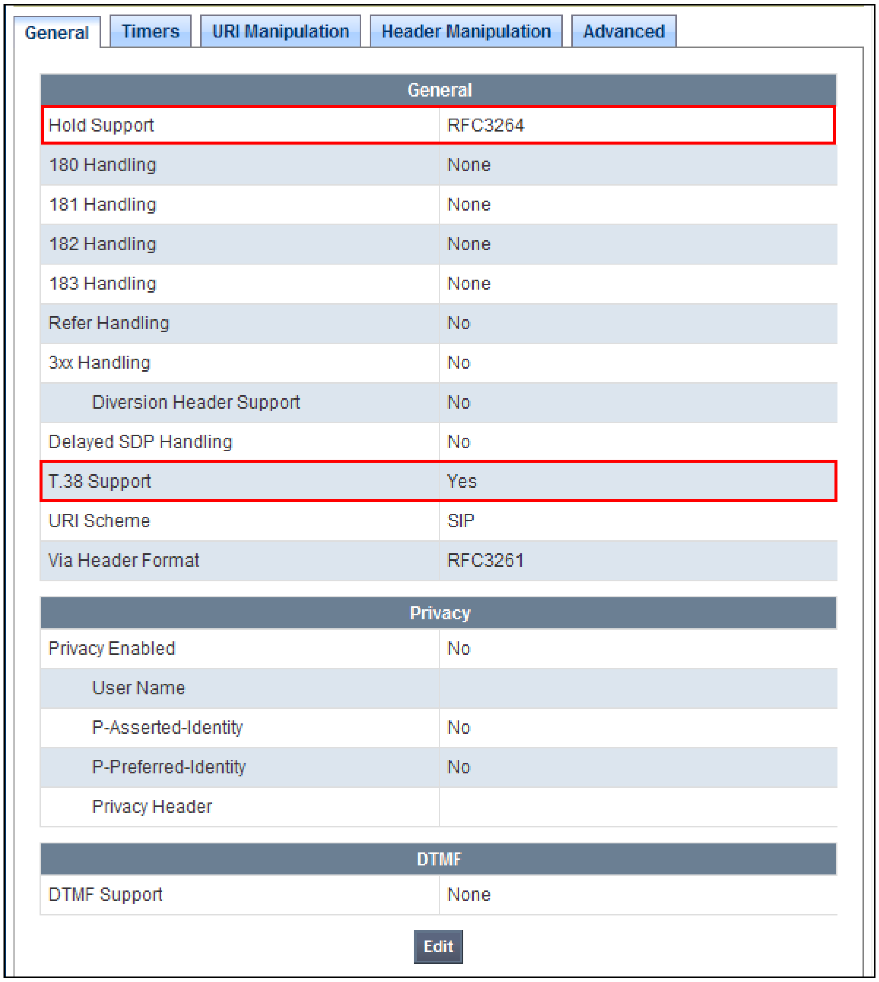


Advanced Settings	
Record Routes	BOTH
Topology Hiding: Change Call-ID	Yes
Call-Info NAT	No
Change Max Forwards	Yes
Include End Point IP for Context Lookup	No
OCS Extensions	No
AVAYA Extensions	Yes
NORTEL Extensions	No
SLiC Extensions	No
Diversion Manipulation	No
Metaswitch Extensions	No
Reset on Talk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

6.5.2. Server Interworking – MTS Allstream

For the compliance test, server interworking profile **SP-General** was created for the MTS Allstream SIP server. When creating the profile, configure the General tab parameters as follows:

- Set **Hold Support** to **RFC3264**.
- Enable **T.38 Support**.

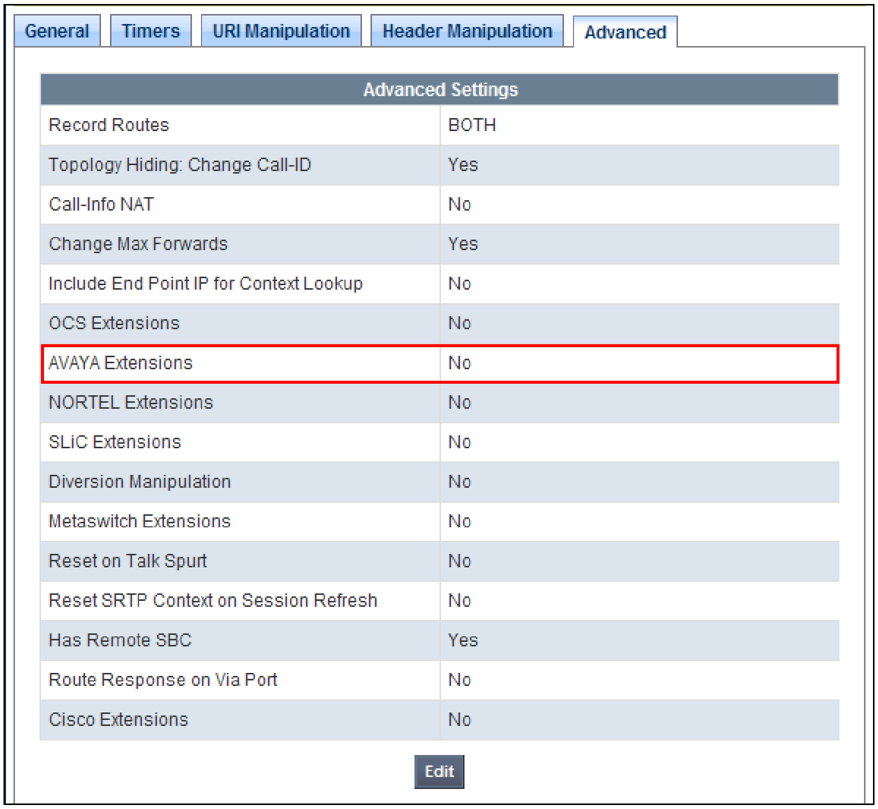


General	
Hold Support	RFC3264
180 Handling	None
181 Handling	None
182 Handling	None
183 Handling	None
Refer Handling	No
3xx Handling	No
Diversion Header Support	No
Delayed SDP Handling	No
T.38 Support	Yes
URI Scheme	SIP
Via Header Format	RFC3261

Privacy	
Privacy Enabled	No
User Name	
P-Asserted-Identity	No
P-Preferred-Identity	No
Privacy Header	

DTMF	
DTMF Support	None

On the Advanced tab, disable the **Avaya Extensions**.

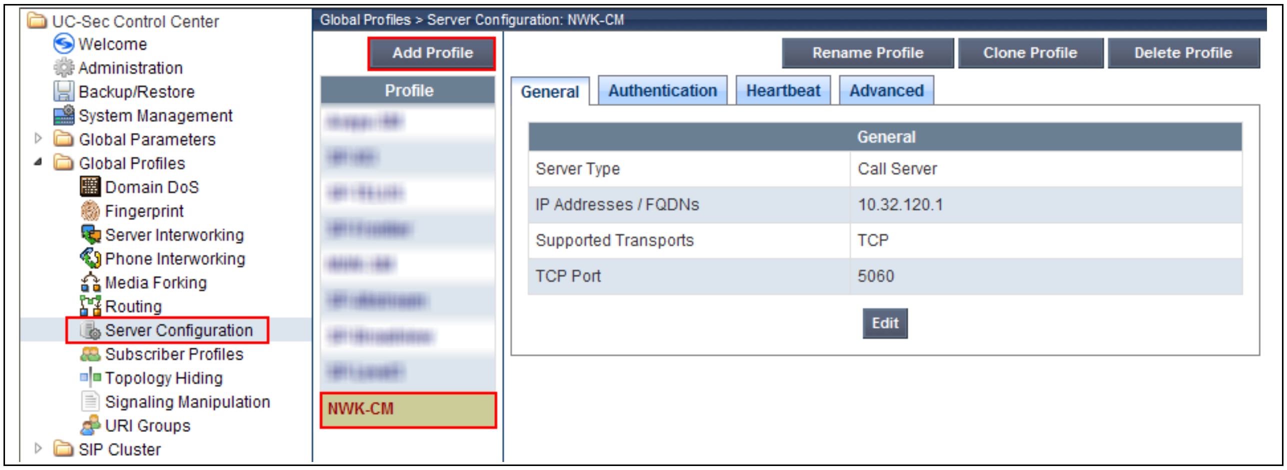


Advanced Settings	
Record Routes	BOTH
Topology Hiding: Change Call-ID	Yes
Call-Info NAT	No
Change Max Forwards	Yes
Include End Point IP for Context Lookup	No
OCS Extensions	No
AVAYA Extensions	No
NORTEL Extensions	No
SLiC Extensions	No
Diversion Manipulation	No
Metaswitch Extensions	No
Reset on Talk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

6.6. Server Configuration

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

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

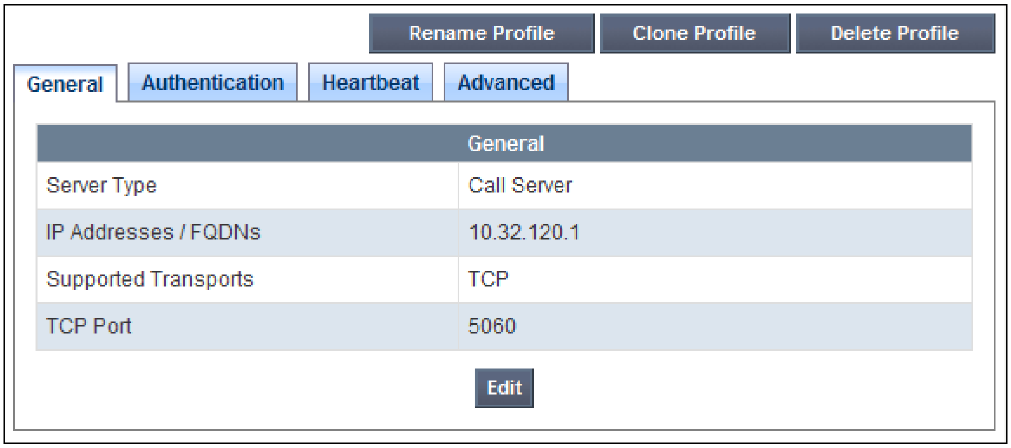


General	
Server Type	Call Server
IP Addresses / FQDNs	10.32.120.1
Supported Transports	TCP
TCP Port	5060

6.6.1. Server Configuration – Communication Manager

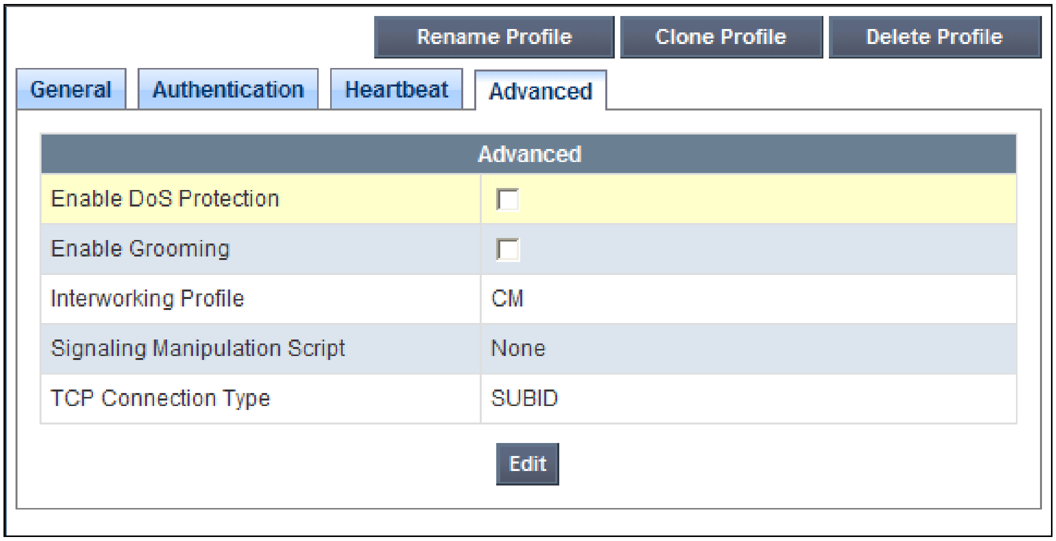
For the compliance test, server configuration profile **NWK-CM** was created for Communication Manager. When creating the profile, configure the General tab parameters as follows:

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



General	
Server Type	Call Server
IP Addresses / FQDNs	10.32.120.1
Supported Transports	TCP
TCP Port	5060

On the Advanced tab, set the **Interworking Profile** field to the interworking profile for the Communication Manager defined in **Section 6.5.1**.

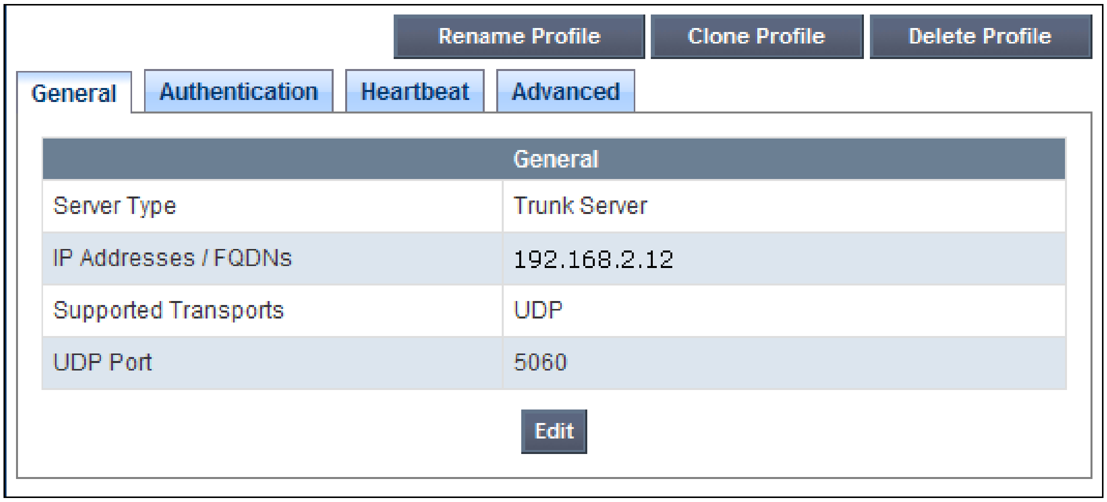


Advanced	
Enable DoS Protection	☐
Enable Grooming	☐
Interworking Profile	CM
Signaling Manipulation Script	None
TCP Connection Type	SUBID

6.6.2. Server Configuration – MTS Allstream

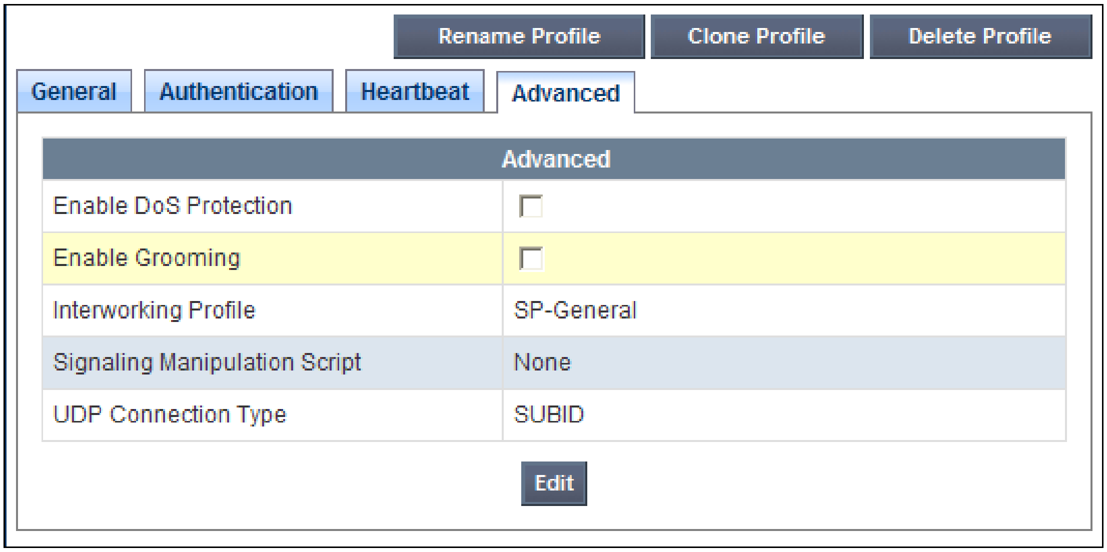
For the compliance test, server configuration profile **SP-Allstream** was created for MTS Allstream. When creating the profile, configure the General tab parameters as follows:

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



General	
Server Type	Trunk Server
IP Addresses / FQDNs	192.168.2.12
Supported Transports	UDP
UDP Port	5060

On the Advanced tab, set the **Interworking Profile** field to the interworking profile for MTS Allstream defined in **Section 6.5.2**.

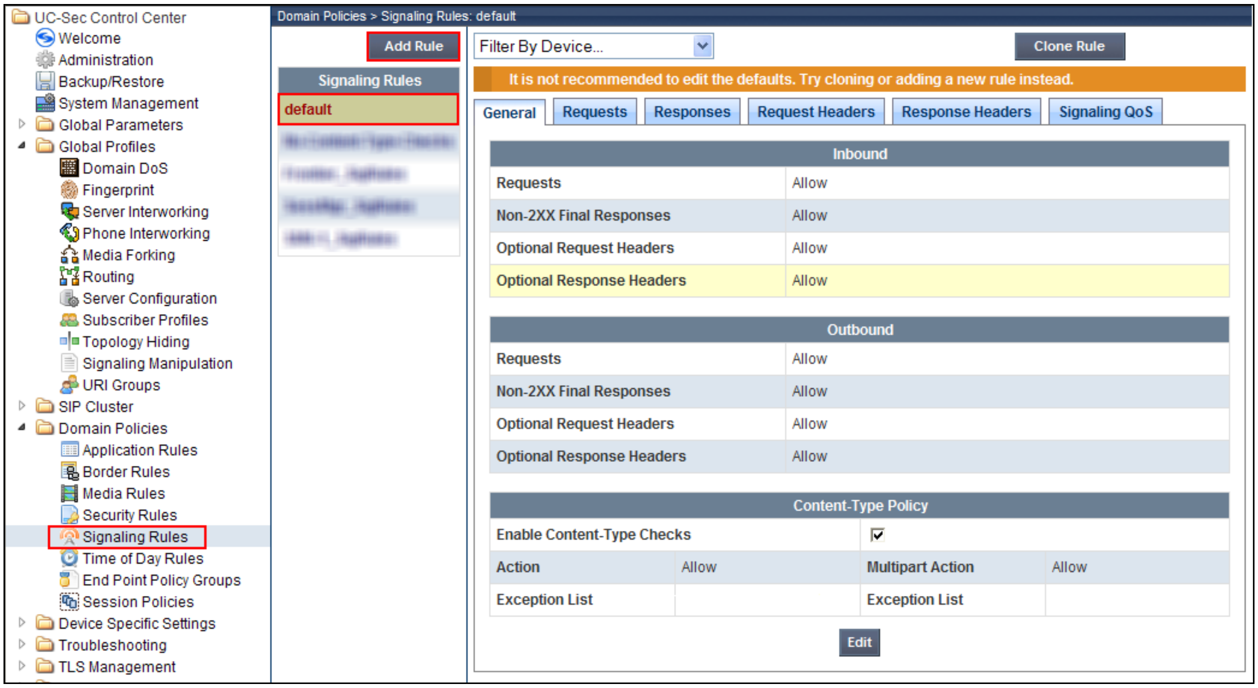


Advanced	
Enable DoS Protection	□
Enable Grooming	□
Interworking Profile	SP-General
Signaling Manipulation Script	None
UDP Connection Type	SUBID

6.7. Signaling Rules

A signaling rule defines the processing to be applied to the selected signaling traffic. A signaling rule is one component of the larger endpoint policy group defined in **Section 6.9**. Communication Manager and the MTS Allstream SIP server used the **default** rule. This test did not require the creation of a new rule. If a new rule had been needed, it could be created using the following steps.

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



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

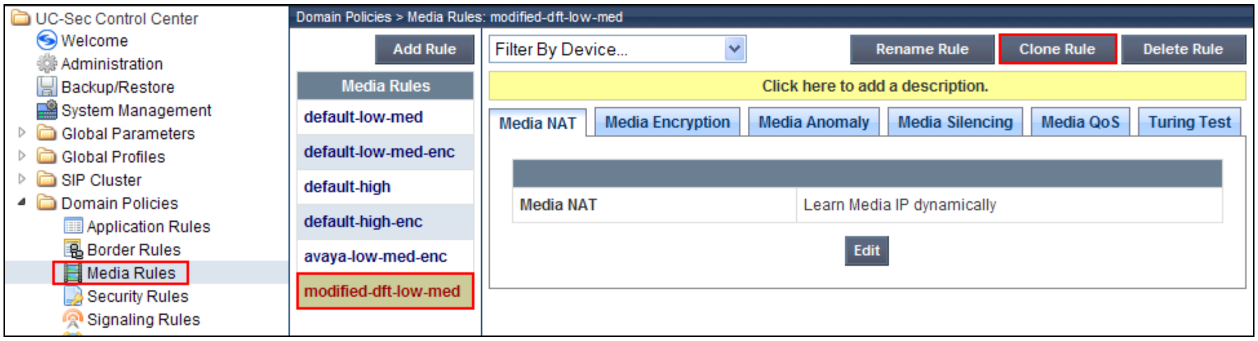
Outbound	
Requests	Allow
Non-2XX Final Responses	Allow
Optional Request Headers	Allow
Optional Response Headers	Allow

Content-Type Policy			
Enable Content-Type Checks	☑		
Action	Allow	Multipart Action	Allow
Exception List		Exception List	

6.8. Media Rules

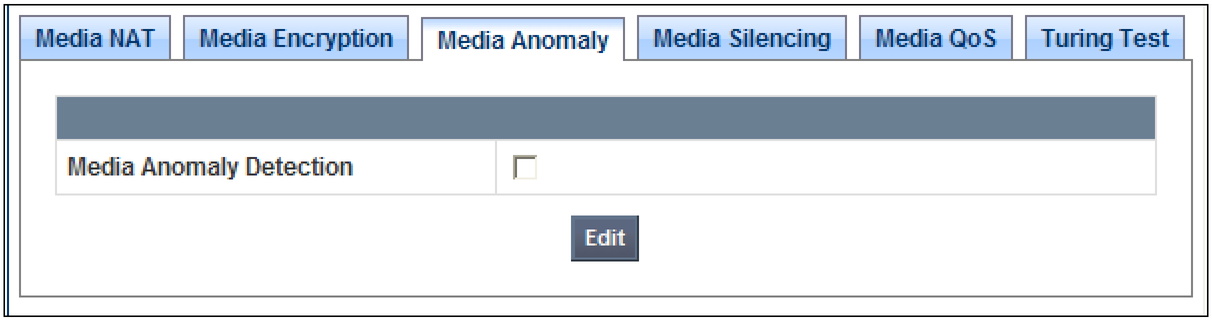
A media rule defines the processing to be applied to the selected media. A media rule is one component of the larger endpoint policy group defined in **Section 6.9**.

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



Media NAT	Learn Media IP dynamically

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

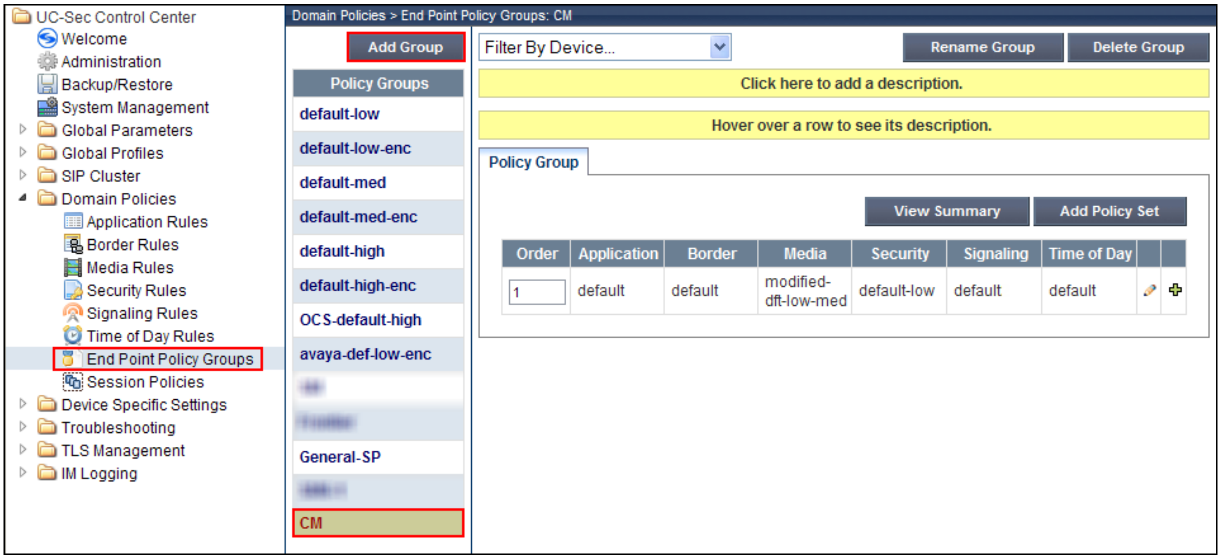


Media Anomaly Detection	□

6.9. Endpoint Policy Groups

An endpoint policy group is a set of policies that will be applied to traffic between the Avaya SBCE and a signaling endpoint (connected server). Thus, an endpoint policy group must be created for Communication Manager and the service provider SIP server. The endpoint policy group is applied to the traffic as part of the endpoint flow defined in **Section 6.12**.

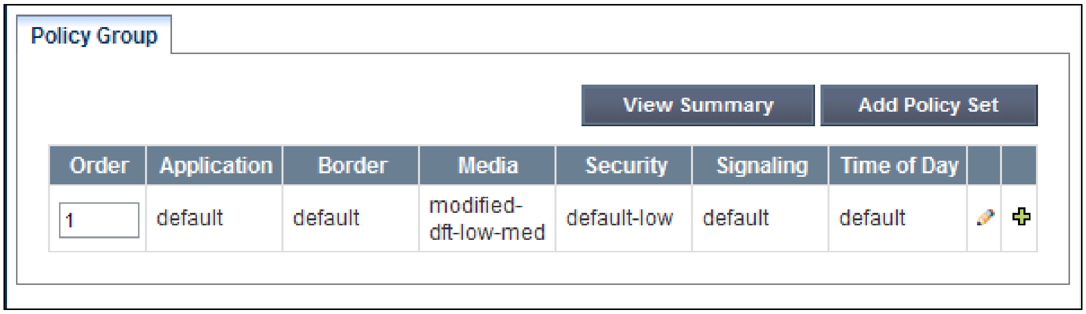
To create a new group, navigate to **Domain Policies → End Point Policy Groups** in the left pane. In the center pane, select **Add Group**. A pop-up window (not shown) will appear requesting the name of the new group, followed by series of pop-up windows in which the group parameters can be configured.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



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

6.9.1. Endpoint Policy Group – Communication Manager

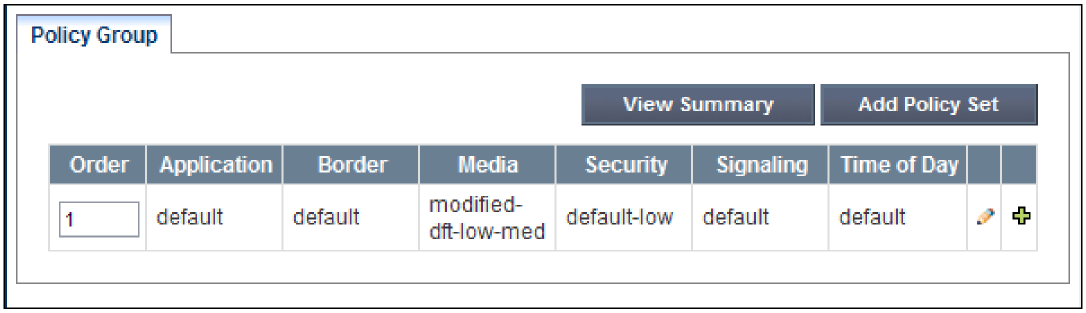
For the compliance test, endpoint policy group **CM** was created for Communication Manager. Default values were used for each of the rules which comprise the group with the exception of **Media**. For **Media**, select the media rule created in **Section 6.8**.



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

6.9.2. Endpoint Policy Group – MTS Allstream

For the compliance test, endpoint policy group **General-SP** was created for the MTS Allstream SIP server. Default values were used for each of the rules which comprise the group with the exception of **Media**. For **Media**, select the media rule created in **Section 6.8**.

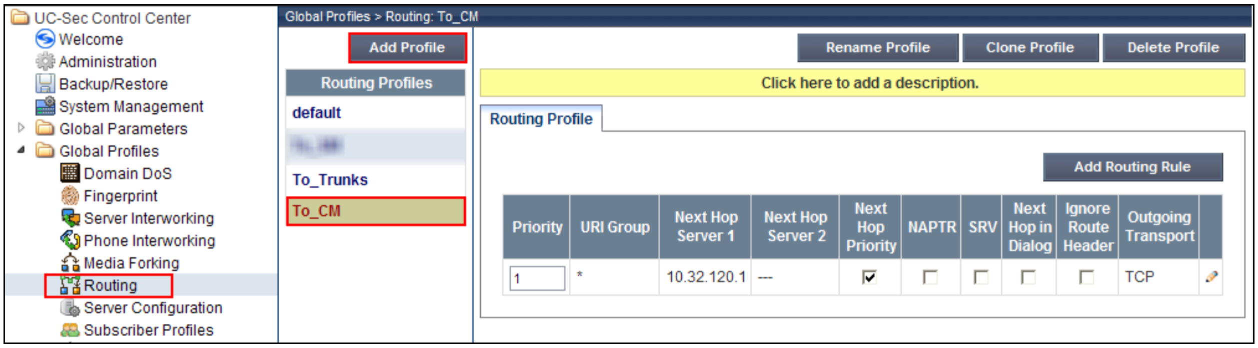


Order	Application	Border	Media	Security	Signaling	Time of Day		
1	default	default	modified-dft-low-med	default-low	default	default	✎	✚

6.10. Routing

A routing profile defines where traffic will be directed based on the contents of the URI. A routing profile is applied only after the traffic has matched an endpoint server flow defined in **Section 6.12**. Create a routing profile for the Communication Manager and the service provider SIP server.

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

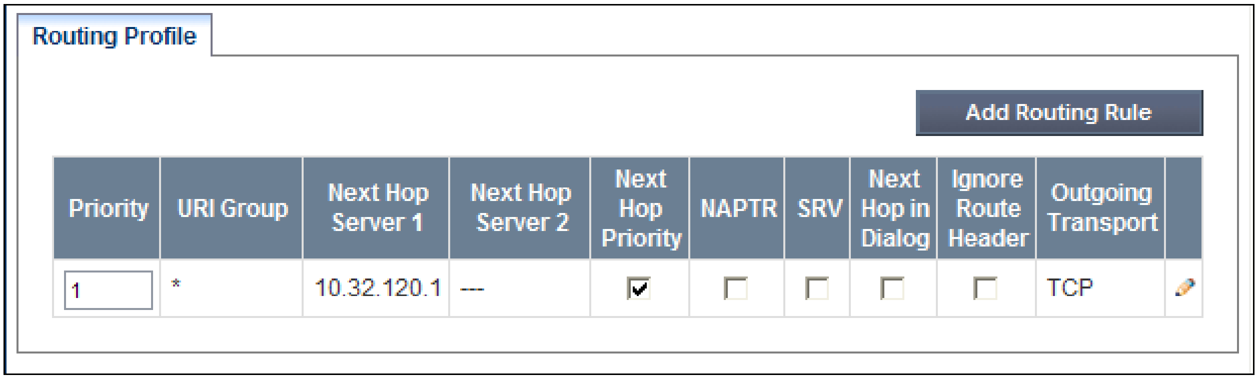


Priority	URI Group	Next Hop Server 1	Next Hop Server 2	Next Hop Priority	NAPTR	SRV	Next Hop in Dialog	Ignore Route Header	Outgoing Transport	
1	*	10.32.120.1	---	☑	□	□	□	□	TCP	✎

6.10.1. Routing – Communication Manager

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

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

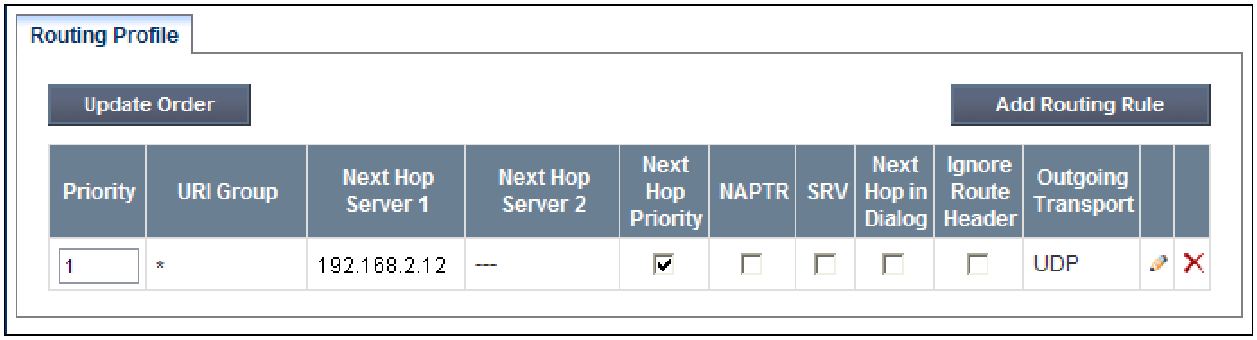


Priority	URI Group	Next Hop Server 1	Next Hop Server 2	Next Hop Priority	NAPTR	SRV	Next Hop in Dialog	Ignore Route Header	Outgoing Transport	
1	*	10.32.120.1	---	☑	□	□	□	□	TCP	✎

6.10.2. Routing – MTS Allstream

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

- Set the **URI Group** to the wild card ***** to match on any URI.
- Set the **Next Hop Server 1** field to the IP address of the MTS Allstream SIP server.
- Enable **Next Hop Priority**.
- Set the **Outgoing Transport** field to **UDP**.

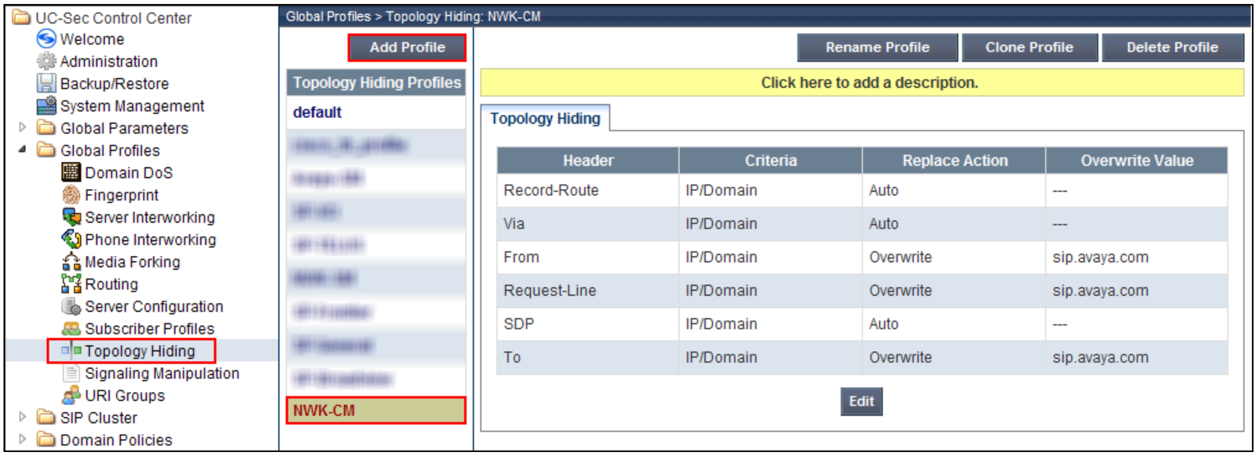


Priority	URI Group	Next Hop Server 1	Next Hop Server 2	Next Hop Priority	NAPTR	SRV	Next Hop in Dialog	Ignore Route Header	Outgoing Transport		
1	*	192.168.2.12	---	☑	□	□	□	□	UDP	✎	✕

6.11. Topology Hiding

Topology hiding allows the host part of some SIP message headers to be modified in order to prevent private network information from being propagated to the untrusted public network. It can also be used as an interoperability tool to adapt the host portion of these same headers to meet the requirements of the connected servers. The topology hiding profile is applied as part of the endpoint flow in **Section 6.12**.

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



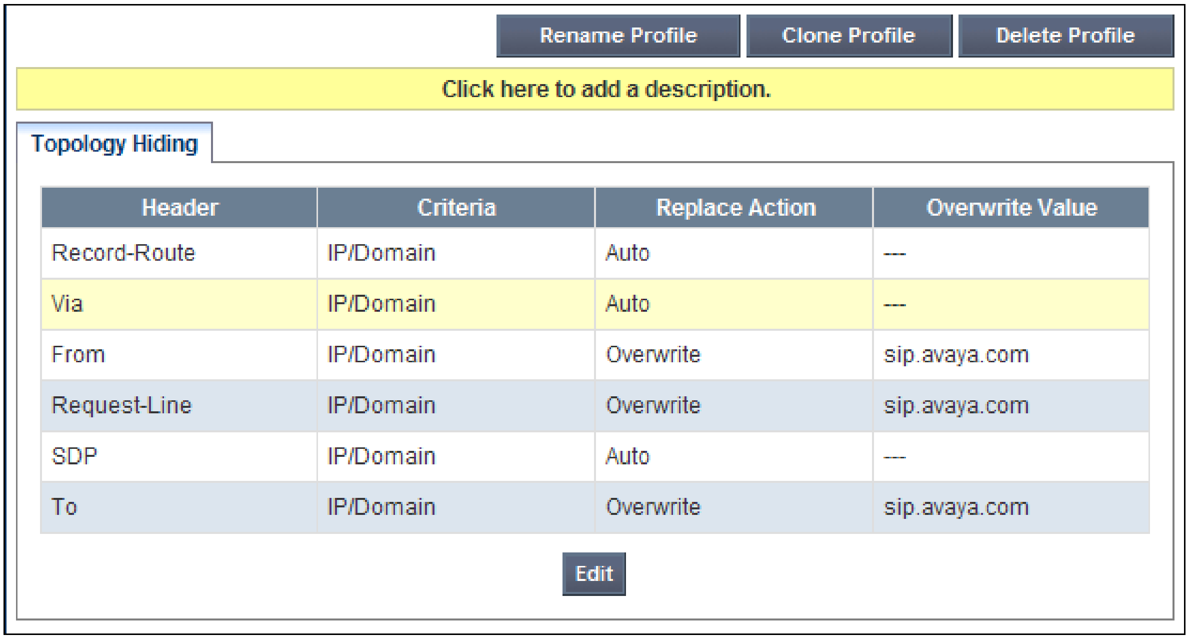
[redacted]

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

6.11.1. Topology Hiding – Communication Manager

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

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

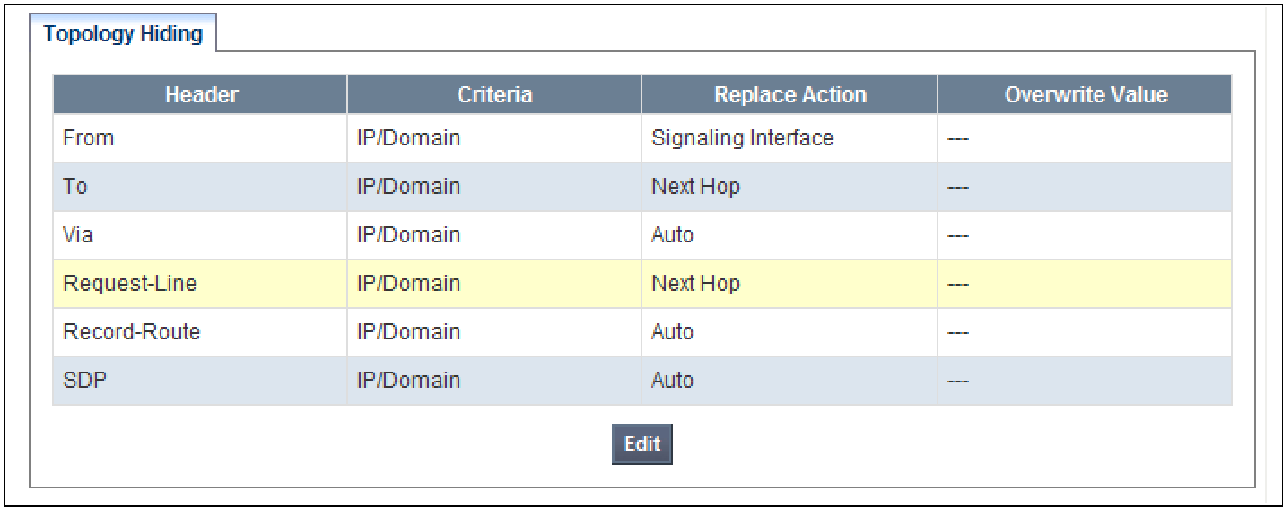


Header	Criteria	Replace Action	Overwrite Value
Record-Route	IP/Domain	Auto	---
Via	IP/Domain	Auto	---
From	IP/Domain	Overwrite	sip.avaya.com
Request-Line	IP/Domain	Overwrite	sip.avaya.com
SDP	IP/Domain	Auto	---
To	IP/Domain	Overwrite	sip.avaya.com

6.11.2. Topology Hiding – MTS Allstream

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

- Set **Header** to the header whose host part of the URI is to be modified.
- Set **Criteria** to **IP/Domain** to indicate that the host part should be modified if it is an IP address or a domain.
- Set **Replace Action** to **Auto** for all headers except **Request-Line**, **From** and **To**. Set the **Replace Action** for the **Request-Line** and **To** headers to **Next Hop** which is the IP address of the MTS Allstream SIP server. Set the **Replace Action** for the **From** header to **Signaling Interface** which is the IP address of the public interface of the Avaya SBCE.

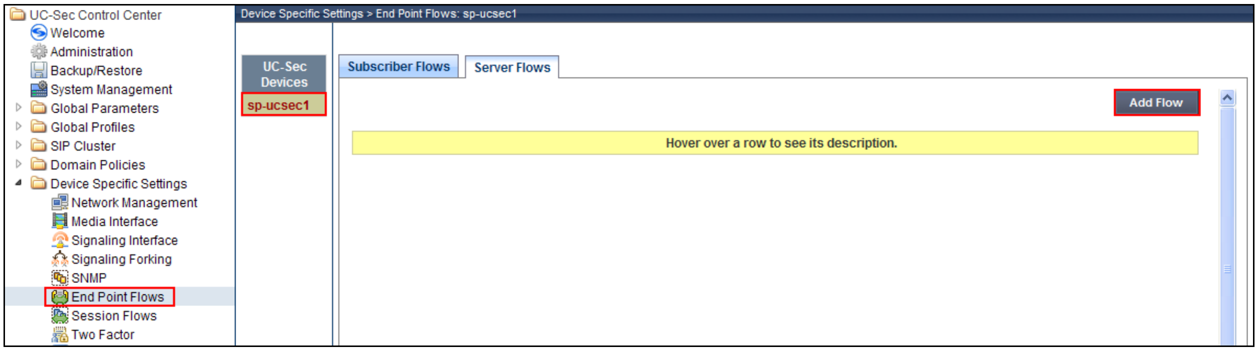


Header	Criteria	Replace Action	Overwrite Value
From	IP/Domain	Signaling Interface	---
To	IP/Domain	Next Hop	---
Via	IP/Domain	Auto	---
Request-Line	IP/Domain	Next Hop	---
Record-Route	IP/Domain	Auto	---
SDP	IP/Domain	Auto	---

6.12. End Point Flows

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

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

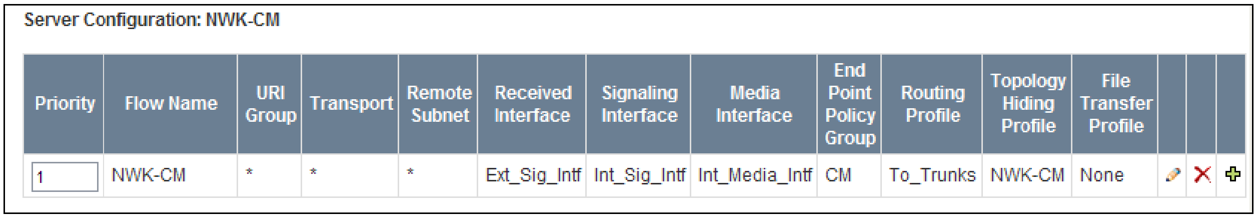


6.12.1. End Point Flow – Communication Manager

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

- For the **Flow Name**, enter a descriptive name.
- For **Server Configuration**, select the Communication Manager server created in **Section 6.6.1**.
- To match all traffic, set the **URI Group**, **Transport**, and **Remote Subnet** to *****.
- Set the **Received Interface** to the external signaling interface.
- Set the **Signaling Interface** to the internal signaling interface.
- Set the **Media Interface** to the internal media interface.
- Set the **End Point Policy Group** to the endpoint policy group defined for Communication Manager in **Section 6.9.1**.
- Set the **Routing Profile** to the routing profile defined in **Section 6.10.2** used to direct traffic to the MTS Allstream SIP server.

- Set the **Topology Hiding Profile** to the topology hiding profile defined for Communication Manager in **Section 6.11.1**.



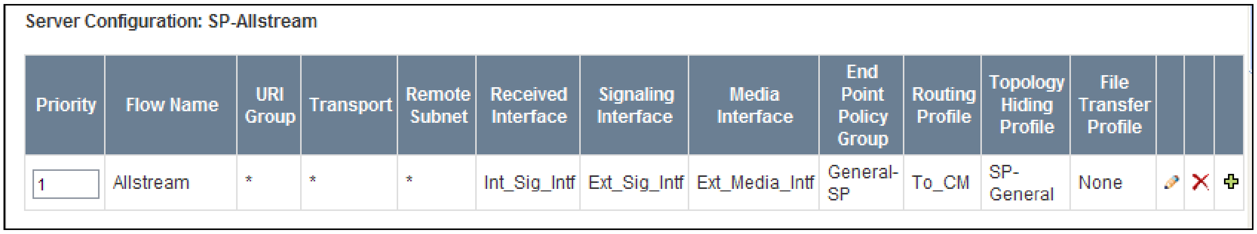
Server Configuration: NWK-CM

Priority	Flow Name	URI Group	Transport	Remote Subnet	Received Interface	Signaling Interface	Media Interface	End Point Policy Group	Routing Profile	Topology Hiding Profile	File Transfer Profile			
1	NWK-CM	*	*	*	Ext_Sig_Intf	Int_Sig_Intf	Int_Media_Intf	CM	To_Trunks	NWK-CM	None	✎	✗	✚

6.12.2. End Point Flow – MTS Allstream

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

- For the **Flow Name**, enter a descriptive name.
- For **Server Configuration**, select the MTS Allstream SIP server created in **Section 6.6.2**.
- To match all traffic, set the **URI Group**, **Transport**, and **Remote Subnet** to *****.
- Set the **Received Interface** to the internal signaling interface.
- Set the **Signaling Interface** to the external signaling interface.
- Set the **Media Interface** to the external media interface.
- Set the **End Point Policy Group** to the endpoint policy group defined for MTS Allstream in **Section 6.9.2**.
- Set the **Routing Profile** to the routing profile defined in **Section 6.10.1** used to direct traffic to Communication Manager.
- Set the **Topology Hiding Profile** to the topology hiding profile defined for MTS Allstream in **Section 6.11.2**.



Server Configuration: SP-Allstream

Priority	Flow Name	URI Group	Transport	Remote Subnet	Received Interface	Signaling Interface	Media Interface	End Point Policy Group	Routing Profile	Topology Hiding Profile	File Transfer Profile			
1	Allstream	*	*	*	Int_Sig_Intf	Ext_Sig_Intf	Ext_Media_Intf	General-SP	To_CM	SP-General	None	✎	✗	✚

7. MTS Allstream SIP Trunking Configuration

MTS Allstream is responsible for the network configuration of the MTS Allstream SIP Trunking service. MTS Allstream will require that the customer provide the public IP address used to reach the Avaya SBCE at the edge of the enterprise. MTS Allstream will provide the IP address of the MTS Allstream SIP proxy/SBC, IP addresses of media sources and Direct Inward Dialed (DID) numbers assigned to the enterprise. This information is used to complete the Communication Manager and the Avaya SBCE configuration discussed in the previous sections.

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

8. Verification Steps

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

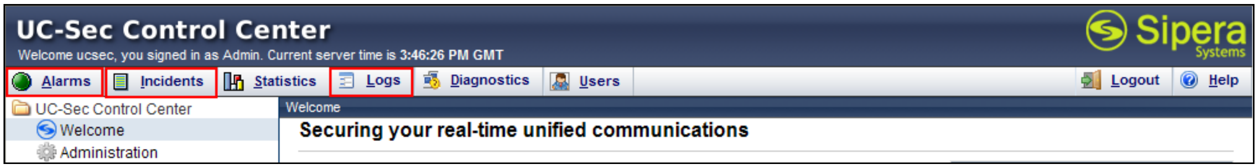
Verification Steps:

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

Troubleshooting:

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

2. Avaya SBC:
   Use the debugging links along the top of the UC-Sec Control Center window shown below to access the following.
   - Click on **Alarms** to display the alarm log.
   - Click on **Incidents** to display the incident report.
   - Navigate to **Logs** → **System Logs** to display the system log.


UC-Sec Control Center

Welcome ucsec, you signed in as Admin. Current server time is 3:46:26 PM GMT

Securing your real-time unified communications

9. Conclusion

These Application Notes describe the configuration necessary to connect Avaya Aura® Communication Manager and the Avaya Session Border Controller for Enterprise to MTS Allstream SIP Trunking. MTS Allstream SIP Trunking passed compliance testing. Please refer to **Section 2.2** for any exceptions or workarounds.

10. References

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

[1] *Installing and Configuring Avaya Aura® System Platform*, Release 6.0.3, March 2012.
[2] *Administering Avaya Aura® System Platform*, Release 6.0.3, February 2011.
[3] *Administering Avaya Aura® Communication Manager*, Issue 6.0, June 2010, Document Number 03-300509.
[4] *Avaya Aura® Communication Manager Feature Description and Implementation*, Issue 8.0, June 2010, Document Number 555-245-205.
[5] *Avaya 1600 Series IP Deskphones Administrator Guide Release 1.3.x*, April 2010, Document Number 16-601443.
[6] *Avaya one-X® Deskphone Edition for 9600 Series IP Telephones Administrator Guide*, Issue 8, March 2012, Document Number 16-300698.
[7] *Avaya one-X® Deskphone SIP 9608, 9611G, 9621G, 9641G Administrator Guide*, Release 6.0.1, May 2011, Document Number 16-603813.
[8] *Administering Avaya one-X® Communicator*, October 2011.
[9] RFC 3261 *SIP: Session Initiation Protocol*, http://www.ietf.org/
[10] RFC 2833 RTP Payload for DTMF Digits, Telephony Tones and Telephony Signals, http://www.ietf.org/

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.