Avaya Solution & Interoperability Test Lab

Application Notes for Configuring Star Telecom SIP Trunking with Avaya Aura® Communication Manager Release 6.2 and Avaya Session Border Controller for Enterprise Release 4.0.5 – Issue 1.0

Abstract

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

Customers using this Avaya SIP-enabled enterprise solution with Star Telecom 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 Star Telecom SIP Trunking service via the public Internet and exercise the features and functionality listed in **Section 2.1**. The simulated enterprise site comprised of a Communication Manager with an Avaya G450 Media Gateway and Avaya SBCE. 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) configured for H.323. Avaya one-X® Communicator can place calls from the local computer or control a separate physical phone. Both of these modes were tested.
- Various call types including: local, long distance, international, outbound toll-free, operator, operator assisted calls, and local directory assistance (411).
- G.711MU and G.729A codecs.
- DTMF transmission using RFC 2833.
- Caller ID presentation and Caller ID restriction.

- Inbound and outbound REFER messages.
- Response to incomplete call attempts and trunk errors.
- Voicemail access and navigation for inbound and outbound calls.
- Voicemail Message Waiting Indicator (MWI) on enterprise phones.
- User features such as hold and resume, internal call forwarding, transfer, and conference.
- Off-net call transfer, conference, forwarding and enterprise mobility (extension to cellular)

Items not supported or not tested included the following:

- Inbound toll-free and emergency 911 calls were not tested.
- T.38 faxing was not tested since fax application is not used/supported by Star Telecom SIP Trunking.

2.2. Test Results

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

- **G.729A Codec**: Star Telecom disables the G.729A codec on inbound calls to avoid transcoding in production platform for performance and scalability purposes. Outbound calls with G.729A succeeded. During compliance testing, G.729A was tested, but the finalized configuration used the G.711MU codec for both inbound and outbound calls.
- **No Matching Codec on Inbound Calls**: When Communication Manager was configured with a codec unsupported by Star Telecom, inbound call INVITE received the proper response "488 Not Acceptable Here" from the enterprise. However, the PSTN caller did not receive any audible indication (tones or recorded announcement) but dead audio for about a minute before hearing fast busy tones.
- **No Matching Codec on Outbound Calls**: When Communication Manager was configured with a codec unsupported by Star Telecom, outbound INVITE received the response "503 Service Unavailable -- no more gateways" from Star Telecom. A more appropriate status message like "488 Not Acceptable Here" could have been returned instead of 503.
- **All Trunks Busy**: When all trunks within the enterprise were used up by active calls, additional inbound call from the PSTN received “500 Service Unavailable (Signaling Resources Unavailable)” from the enterprise, the PSTN caller did not receive any audible indication (tones or recorded announcement) but dead audio.
- **Invalid Called Destination**: When an inbound call was routed to an invalid enterprise destination (e.g., an unadministered extension), the enterprise correctly returned "404 Not Found" to Star Telecom, but the PSTN caller did not receive any audible indication (tones or recorded announcement) but dead audio. When outbound call was to an invalid PSTN destination, the enterprise caller heard proper announcement about call not going through followed by call disconnect after about 40 seconds from call initiation. During this 40-second time span, the caller did not receive ringback tones or other audible signals, but dead audio.

- **Connected Party Display in PSTN Transfer**: After an existing call between a PSTN caller and an enterprise extension was transferred off-net to another PSTN party, the displayed connected party at both PSTN phones (the transferred party and the transfer-to party) showed the transferring party number (DID associated with the transferring extension) instead of the true connected-party number/ID. The true connected party information was conveyed by Communication Manager in SIP signaling messages (REFER, UPDATE) to the service provider, but this information was not used to update/display the true connected party numbers.
- **Avaya one-X® Communicator "Other Phone" Mode**: In the "Other Phone" mode, an outbound call is issued to the associated "Other Phone" when 1XC initiates/receives a call so that 1XC controls the call but voice media is to/from the physical "Other Phone". In this mode, an inbound call transferred to an internal extension (either consultative or blind transfer) would drop after about 30 seconds after the transfer was completed. The call termination was caused by Communication Manager failing to ACK the "200 OK" message from the service provider during the post-transfer media shuffling signaling exchange. The fix to this problem is included in the Communication Manager 6.2 Service Pack 4, therefore it is recommended that 1XC be used in normal mode but not in the "Other Phone" mode until the Communication Manager is upgraded to Release 6.2 Service Pack 4.

2.3. Support

For technical support by Star Telecom, please contact Star Telecom at:

- Toll Free: 1-855-STAR-TEL (1-855-782-7835)
- http://www.startelecom.ca

Avaya customers may obtain documentation and support for Avaya products by visiting http://support.avaya.com. Alternatively, in the United States, (866) GO-AVAYA (866-462-8292) provides access to sales and service support menus.

3. Reference Configuration

Figure 1 illustrates a sample Avaya SIP-enabled enterprise solution connected to Star Telecom SIP Trunking. This was the configuration used for compliance testing.

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

- Avaya Aura® Solution for Midsize Enterprise 6.2 that includes Communication Manager and Avaya Aura® Communication Manager Messaging
- Avaya G450 Media Gateway
- Avaya 96x1-Series IP Telephones (H.323)
- Avaya 9600-Series IP Telephones (H.323)
- Avaya 1600-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.

The compliance test used Communication Manager Messaging for testing voice mail access/navigation and MWI (Messaging Wait Indicator) on Avaya enterprise phones since it is included in Avaya Aura® Solution for Midsize Enterprise 6.2. Other voice messaging application such as Avaya Aura® Messaging could have been used to satisfy this test purpose.

For security purposes, any actual public IP addresses used in the compliance test were changed to 192.168.x.x throughout these Application Notes where the 3rd and 4th octets were retained from the real addresses.

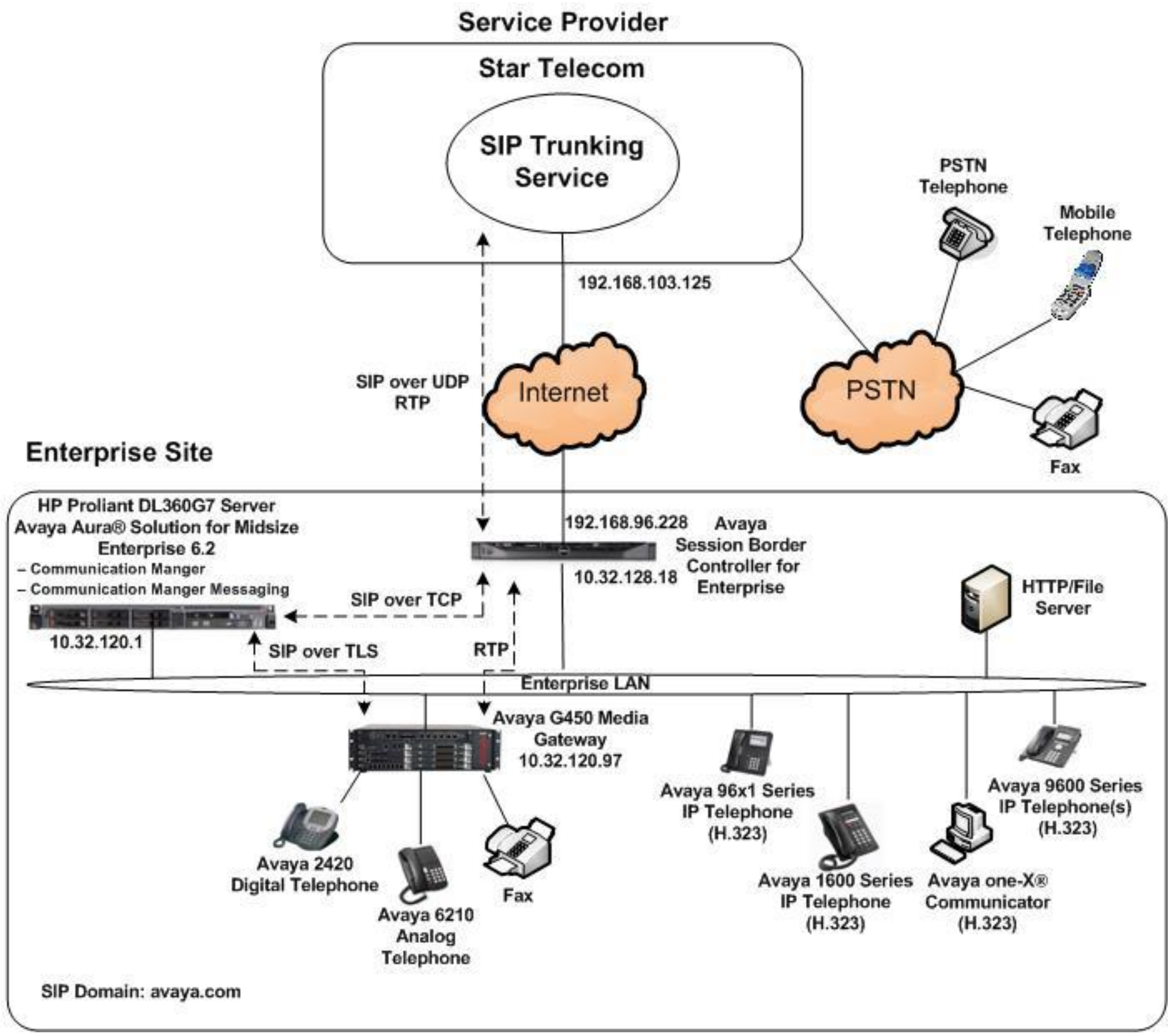


Figure 1: Avaya IP Telephony Network using Star Telecom SIP Trunking

Inbound 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. Communication Manager routes the call to the Avaya SBCE after selecting the proper SIP trunk connecting to the Avaya SBCE. From the Avaya SBCE, the call is sent to Star Telecom SIP Trunking.

The administration of Communication Manager Messaging and enterprise endpoints is standard. Since the configuration tasks for both are not directly related to the interoperability with the Star Telecom SIP Trunking service, they are not included in these Application Notes.

4. Equipment and Software Validated

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

Avaya IP Telephony Solution Components	
Equipment/Software	Release/Version
Avaya Aura® Solution for Midsize Enterprise 6.2 running on HP Proliant DL360G7 Server • Avaya Aura® Communication Manager • Avaya Aura® Communication Manager Messaging	6.2 (R016x.02.0.823.0-20001) 6.2 SP1 (CMM-02.0.823.0-0104)
Avaya G450 Media Gateway	31.22.0 /1
Avaya Session Border Controller For Enterprise running on Dell R210 V2 server	4.0.5Q19
Avaya 9630G IP Telephone (H.323) running Avaya one-X® Deskphone Edition	3.1 SP5 (3.1.05S)
Avaya 9611G IP Telephone (H.323) running Avaya one-X® Deskphone Edition	6.2 SP2 (6.2.2)
Avaya 1616 IP Telephone (H.323) running Avaya one-X® Deskphone Value Edition	1.3 SP2
Avaya one-X® Communicator (H.323)	6.1 SP7 (6.1.7.04-SP7-39506)
Avaya 2420 Digital Telephone	n/a
Avaya 6210 Analog Telephone	n/a
Star Telecom SIP Trunking Solution Components	
Component	Release
Star Telecom Free Switch	R3.2

Table 1: Equipment and Software Tested

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 Star Telecom SIP Trunking. A SIP trunk is established between Communication Manager and Avaya SBCE for use by signaling traffic to and from the service provider. 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.

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 2
             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 2
                       Maximum Administered SIP Trunks: 12000 275
  Maximum Administered Ad-hoc Video Conferencing Ports: 12000 0
   Maximum Number of DS1 Boards with Echo Cancellation: 522   0
                             Maximum TN2501 VAL Boards: 10    0
                     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*** for allowing inbound calls from the PSTN to be transferred to another PSTN endpoint. If for security reasons, incoming calls should not be allowed to be transferred off-net back to the PSTN then leave the field set to ***none***.

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

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

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

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

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

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

SCCAN 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
SM                    10.32.120.98
default               0.0.0.0
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. For the compliance test, ip-codec-set 5 was used for this purpose. Star Telecom SIP Trunking supports the G.711MU codec for both inbound and outbound calls, but G.729A works only for outbound calls (see the item **G.729A Codec** in the observation/limitation list in **Section 2.2**). Thus, only ***G.711MU*** was included in this codec set. Default values can be used for all other fields.

```
change ip-codec-set 5                                         Page   1 of   2

                          IP Codec Set

    Codec Set: 5

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

On **Page 2**, set the **Fax Mode** to **off** since Star Telecom SIP Trunkking service does not use/support fax application.

```
change ip-codec-set 5                                           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 5 was chosen for the service provider trunk. Use the **change ip-network-region 5** command to configure region 5 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 5                                      Page   1 of  20
                               IP NETWORK REGION
  Region: 5
Location:         Authoritative Domain: sip.avaya.com
    Name: SP Region
MEDIA PARAMETERS                Intra-region IP-IP Direct Audio: yes
      Codec Set: 5              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 5 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 5 will be used for calls between region 5 (the service provider region) and region 1 (the rest of the enterprise). Creating this table entry for IP network region 5 will automatically create a complementary table entry on the IP network region 1 form for destination region 5. This complementary table entry can be viewed using the **display ip-network-region 1** command and navigating to **Page 4**.

```
change ip-network-region 5                                      Page   4 of  20

 Source Region: 5     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    5     y    NoLimit                                             n       t
 2
 3
 4
 5    5                                                                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 7 was used for this purpose and was configured using the parameters highlighted below.

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

- Set **Alternate Route Timer** to **15**. This parameter 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 7                                               Page   1 of   2
                                SIGNALING GROUP

 Group Number: 5              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: Others



       Near-end Node Name: procr                  Far-end Node Name: SBCE
 Near-end Listen Port: 5060                 Far-end Listen Port: 5060
                                         Far-end Network Region: 5
                                   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 7 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 configured in **Section 5.6**.
- 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 may be retained for all other fields.

```
add trunk-group 7                                              Page   1 of  21
                                TRUNK GROUP

Group Number: 5                   Group Type: sip           CDR Reports: y
  Group Name: A SBCE Direct Trk          COR: 1        TN: 1        TAC: *07
   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: 7
                                                    Number of Members: 10
```

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

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

```
add trunk-group 7                                              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
```

On **Page 3**, set the **Numbering Format** field to ***public***. This field specifies the format of the calling party number (CPN) sent to the far-end.

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 an enterprise user exercises CPN block on a particular call routed out this trunk. Default values were used for all other fields.

```
add trunk-group 7                                               Page   3 of  21
TRUNK FEATURES
          ACA Assignment? n            Measured: none
                                                        Maintenance Tests? y



                     Numbering Format: public
                                                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 ***y***. Setting the **Network Call Redirection** flag to ***y*** enables use of the SIP REFER message for call transfer as verified in the compliance test; otherwise the SIP INVITE message will be used for call transfer

Set the **Send Diversion Header** field to ***y*** and the **Support Request History** field to ***n***. The **Send Diversion Header** and **Support Request History** fields provide additional information to the network if the call has been re-directed. These settings are needed to support call forwarding of inbound calls back to the PSTN and some Extension to Cellular (EC500) call scenarios.

Set **Telephone Event Payload Type** to ***101***, the value preferred by Star Telecom.

Set **Convert 180 to 183 for Early Media** to ***y*** so that Communication Manager will issue a SIP 183 message for ringing the called enterprise endpoint. This setting was configured to be consistent with Star Telecom SIP Trunking which uses SIP 183 message for ringing the called PSTN phone.

```
add trunk-group 5                                                 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
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", PAI and "Diversion" headers. Since public numbering was selected to define the format of this number (**Section 5.7**), use the **change public-unknown-numbering** command to create an entry for each extension which has a DID assigned. The DID number are assigned by the SIP service provider. It is used to authenticate the caller.

The screen below shows a subset of the DID numbers assigned for testing. These 3 numbers were mapped to the 3 enterprise extensions **41014**, **41016**, and **41018**. 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 3 extensions.

```
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: 20
 5  41014         7         6477252055      10       Maximum Entries: 9999
 5  41016         7         6477252056      10
 5  41018         7         6477252057      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
   2           5   ext
   3           5   ext
   4           5   ext
   5           5   ext
   6           5   ext
   7           5   ext
   8           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:
                         Call Park Access Code: *40
                       Call Pickup Access Code: *41
CAS Remote Hold/Answer Hold-Unhold Access Code: *42
                  CDR Account Code Access Code:
                        Change COR Access Code:
                   Change Coverage Access Code:
            Conditional Call Extend Activation:        Deactivation:
                   Contact Closure   Open Code: *80      Close Code: #80
```

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 *5*** 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     5        op           n
    0                     8    8     deny     op           n
    0                     11   11    5        op           n
    00                    2    2     deny     op           n
    01                    9    17    deny     iop          n
    011                   10   18    5        intl         n
    041                   4    4     5        op           n
    1732                  11   11    5        fnpa         n
    1800                  11   11    5        fnpa         n
    1877                  11   11    5        fnpa         n
    1908                  11   11    5        fnpa         n
```

The route pattern defines which trunk group will be used for the call and performs any necessary digit manipulation. Use the **change route-pattern** command to configure the parameters for the service provider trunk route pattern in the following manner. The example below shows the values used in route pattern 5 for 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 ***7*** (as configured in **Section 5.7)** 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**: 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.

```
change route-pattern 5                                          Page   1 of   3
                    Pattern Number: 5   Pattern Name: AC 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: 7    0       1                                                       n   user
 2:                                                                      n   user
 3:                                                                      n   user
 4:                                                                      n   user
 5:                                                                      n   user
 6:                                                                      n   user

     BCC VALUE  TSC CA-TSC    ITC BCIE Service/Feature PARM  No. Numbering LAR
    0 1 2 M 4 W     Request                                 Dgts Format
                                                         Subaddress
 1: y y y y y n  n            rest                                            none
 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 intended destination. To map incoming DID numbers on the service provider trunk (trunk group 7) to an internal extension, use the **change inc-call-handling-trmt trunk-group 7** command. Set the following:

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

```
change inc-call-handling-trmt trunk-group 7                     Page   1 of  30
                       INCOMING CALL HANDLING TREATMENT
 Service/      Number   Number      Del Insert
 Feature        Len      Digits
 public-ntwrk    10 6477252055       10  41014
 public-ntwrk    10 6477252056       10  41016
 public-ntwrk    10 6477252057       10  41018
 public-ntwrk
```

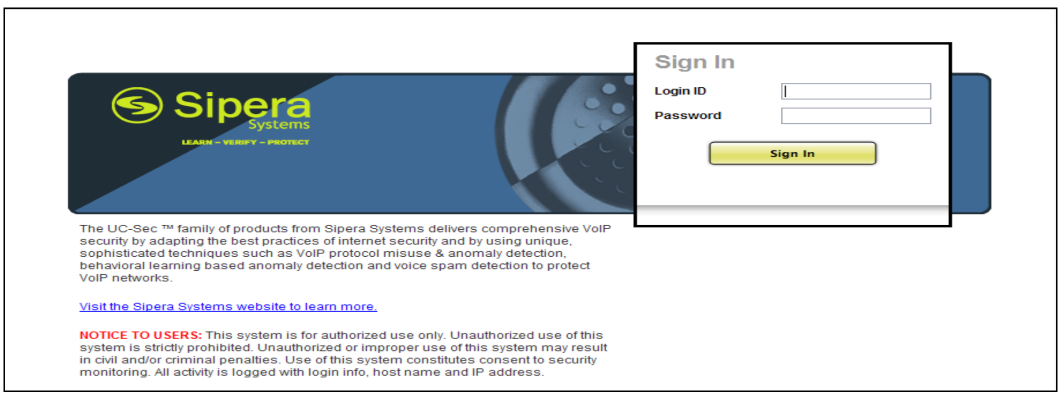
6. Configure Avaya Session Border Controller For Enterprise

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 which **must** be provisioned on a different subnet than either the Avaya SBCE private or public network interfaces (e.g., A1 and B1). If the management interface has not been configured on a separate subnet, then contact your Avaya representative for guidance in correcting the configuration.

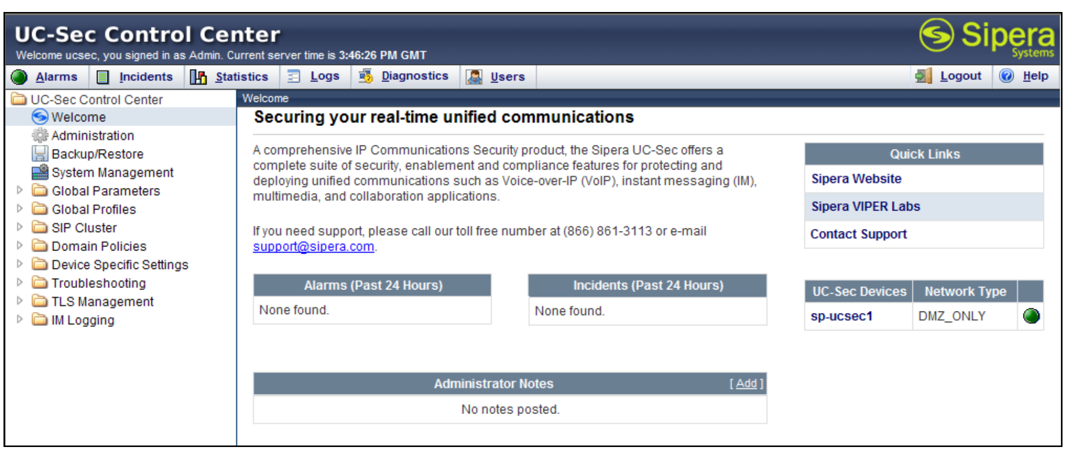
On all screens described in this section, it is to be assumed that parameters are left at their default values unless specified otherwise.

6.1. Access the Management Interface

Use a web browser to access the web management 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.

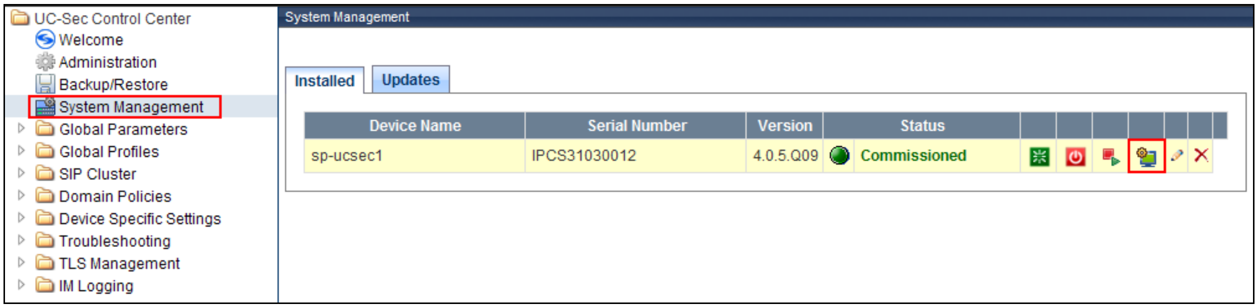


After logging in, the Welcome screen will appear as shown below. All configuration screens of the Avaya SBCE are accessed by navigating the menu tree in the left pane.

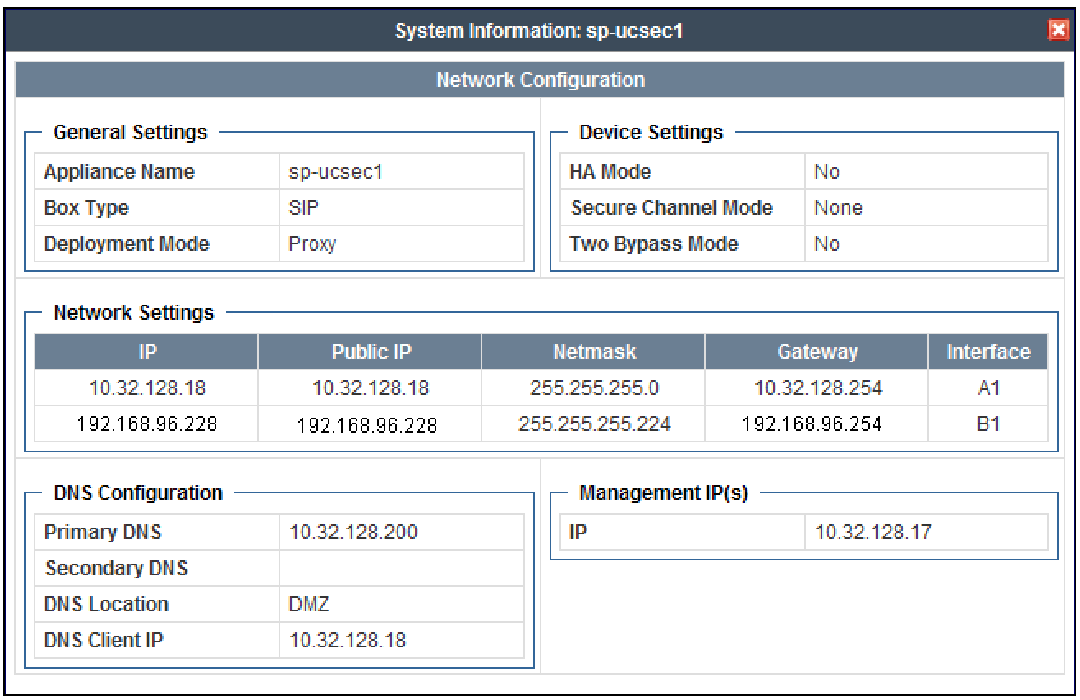


6.2. Verify Network Configuration and Enable Interfaces

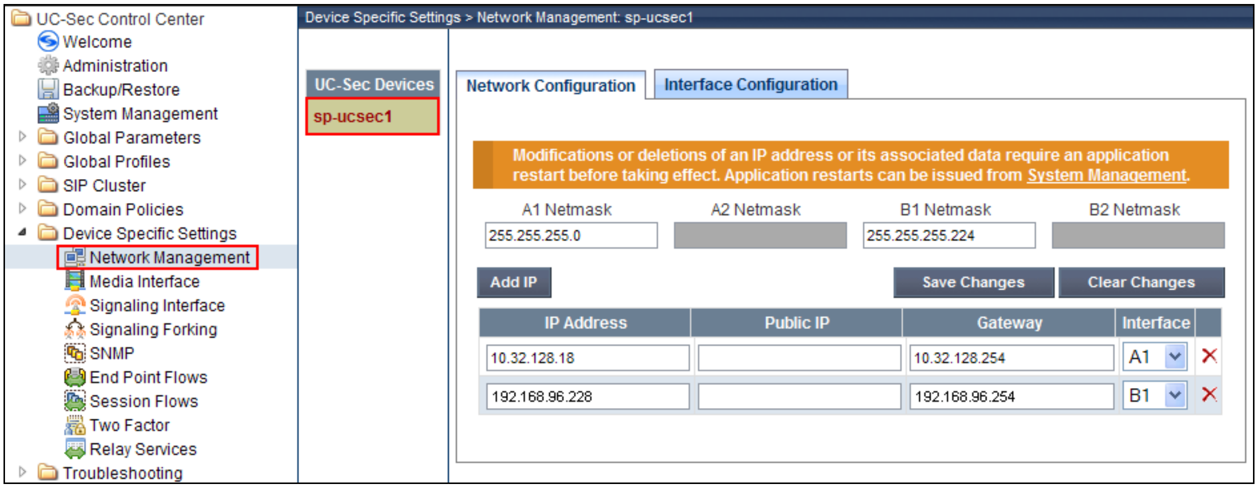
To view the network information provided during installation, navigate to **System Management**. In the right pane, click the **View Config** icon highlighted below.



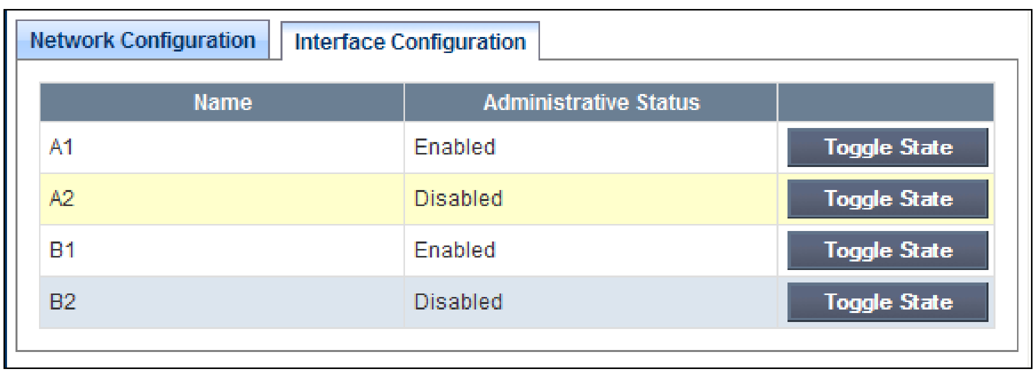
A System Information page will appear showing the information provided during installation. In the **Appliance Name** field is the name of the device (**sp-ucsec1**). This name will be referenced in other configuration screens. Interfaces **A1** and **B1** represent the private and public interfaces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



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.



In 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.



6.3. Signaling Interface

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

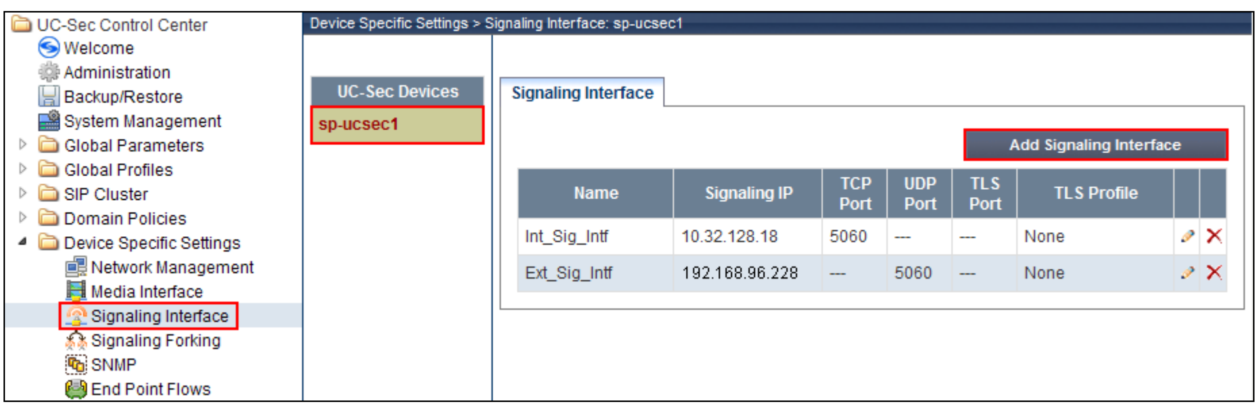
To create a new interface, navigate to **Device Specific Settings → Signaling Interface** in the left pane. In the center pane, select the Avaya SBCE device (**sp-ucsec1**) to be managed. In the right pane, select **Add Signaling Interface**. A pop-up window (not shown) will appear requesting the name of the new interface, followed by a 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) specified in **Section 6.2**.
- Set **TCP port** to the port the Avaya SBCE will listen on for SIP requests from Communication Manager.

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

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



6.4. Media Interface

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

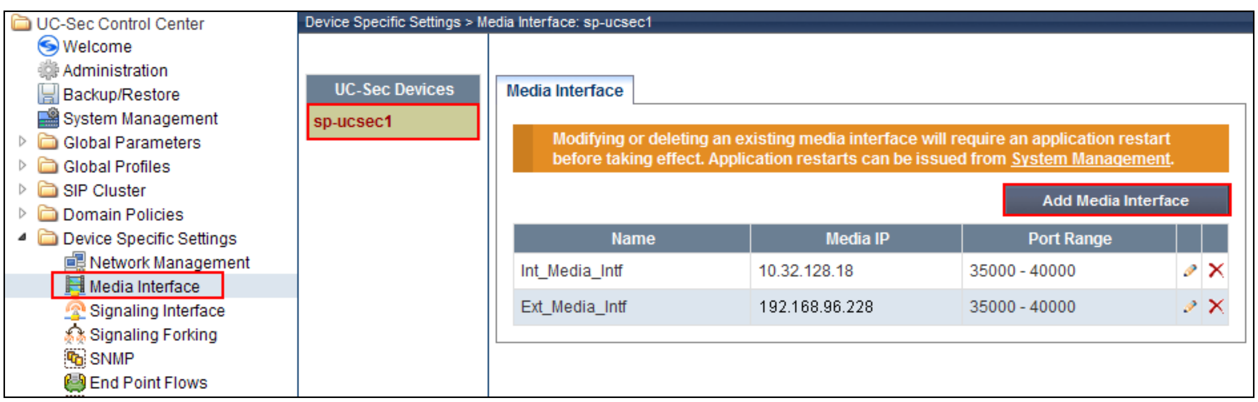
To create a new interface, navigate to **Device Specific Settings → Media Interface** in the left pane. In the center pane, select the Avaya SBCE device (**sp-ucsec1**) to be managed. In the right pane, select **Add Media Interface**. A pop-up window (not shown) will appear requesting the name of the new interface, followed by a 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, the media 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) specified 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.

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

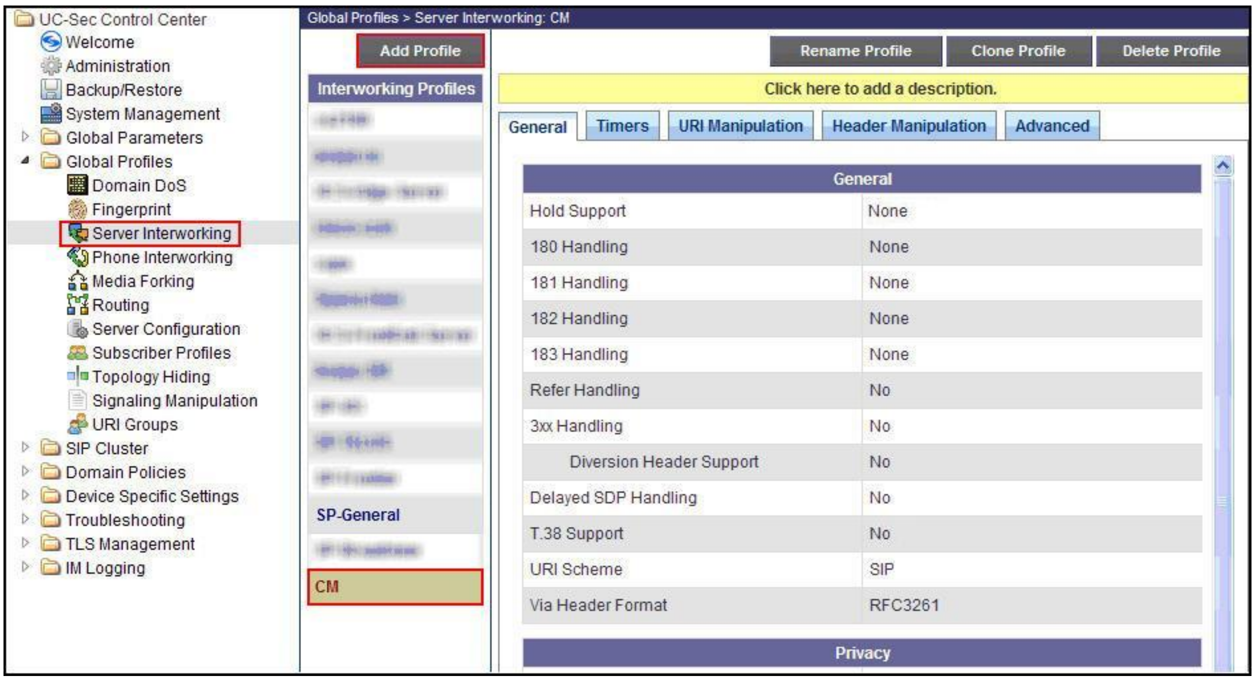
- Set **Name** to a descriptive name.
- Set the **Media IP** to the IP address associated with the public interface (B1) specified in **Section 6.2**.
- Set **Port Range** to a range of ports acceptable to both the Avaya SBCE and the service provider. For the compliance test, the port range used was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



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 the Communication Manager and a server interworking profile for 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 a 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.



 Solution & Interoperability Test Lab Application Notes

6.5.1. Server Interworking: Communication Manager

For the compliance test, a server interworking profile **CM** was created for Communication Manager. All default settings were adequate and retained for this server interworking profile. Shown below are the **General** and the **Advanced** tabs of the **CM** server interworking profile:

The **General** tab:

General | Timers | URI Manipulation | Header Manipulation | Advanced

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

Edit

Note that **T.38 Support** is disabled by default as shown in the preceding screenshot. This setting should be enabled if T.38 faxing is to be supported for the SIP Trunking service.

The **Advanced** tab:

6.5.2. Server Interworking: Star Telecom

For the compliance test, the server interworking profile **SP-General** was created for the Star Telecom SIP server. All default settings were adequate and retained for this server interworking profile. The parameter settings in the **General** and the **Advanced** tabs should be identical to those shown in **Section 6.5.1**.

See the same note in **Section 6.5.1** on the setting for **T.38 Support**.

6.6. Server Configuration

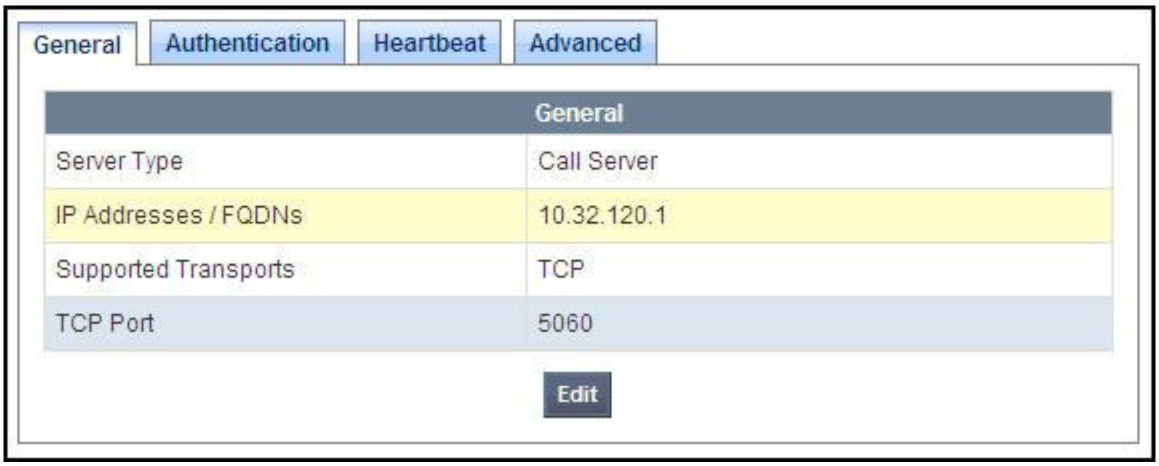
A server configuration profile defines the attributes of the physical server. Create a server configuration profile for the Communication Manager and another server configuration profile for the service provider SIP server.

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 a 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.

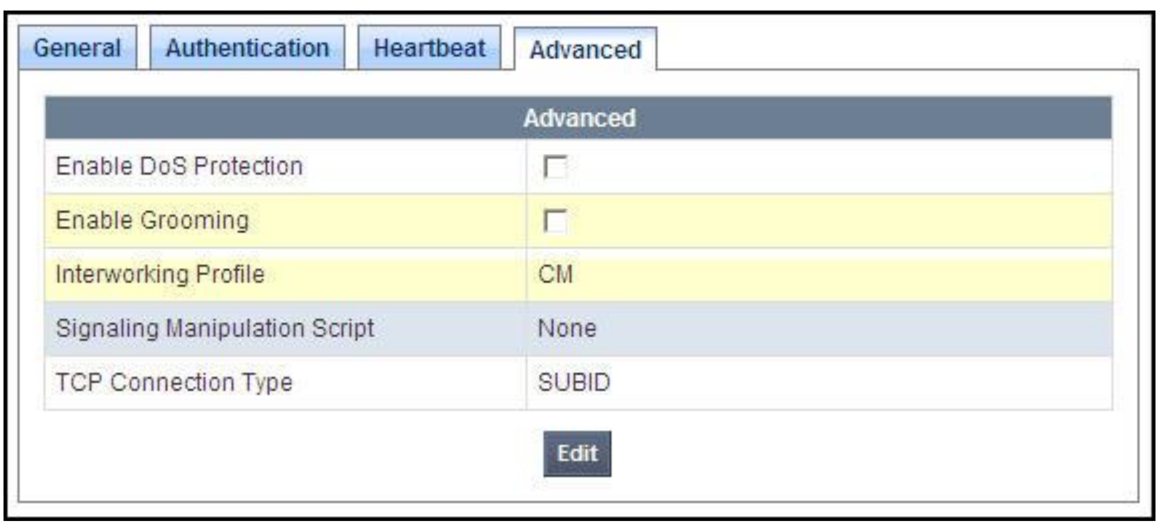
6.6.1. Server Configuration: Communication Manager

For the compliance test, the 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 the Communication Manager signaling interface.
- Set **Supported Transports** to the transport protocol used for SIP signaling between Communication Manager and the Avaya SBCE.
- Set **TCP Port** to the port Communication Manager will listen on for SIP requests from the Avaya SBCE.



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

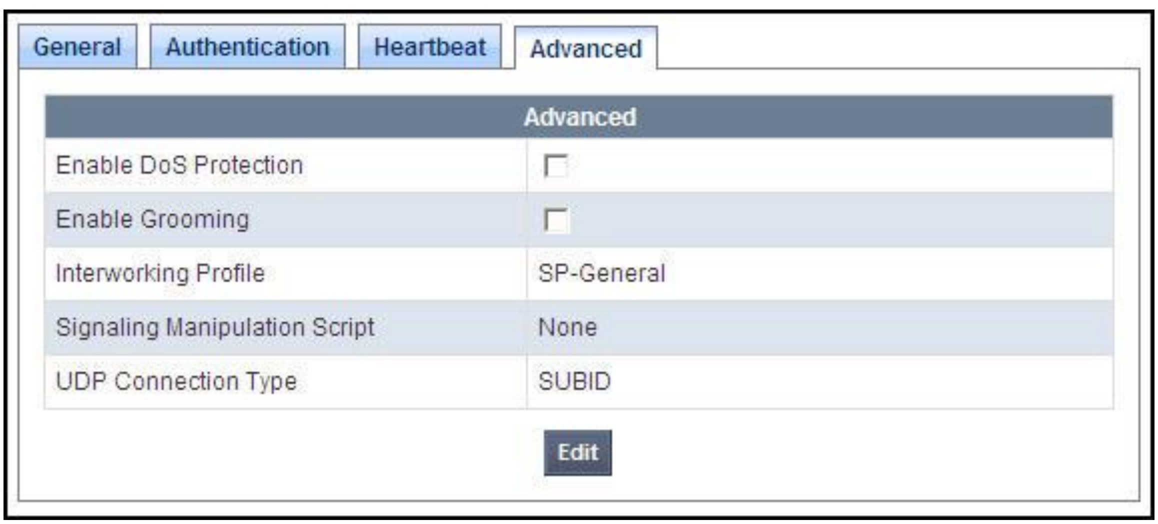


6.6.2. Server Configuration: Star Telecom

For the compliance test, the server configuration profile **SP-StarTelecom** was created for the service provider SIP server. 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 Star Telecom SIP server.
- Set **Supported Transports** to the transport protocol used for SIP signaling between Star Telecom and the Avaya SBCE.
- Set **UDP Port** to the port Star Telecom will listen on for SIP requests from the Avaya SBCE.

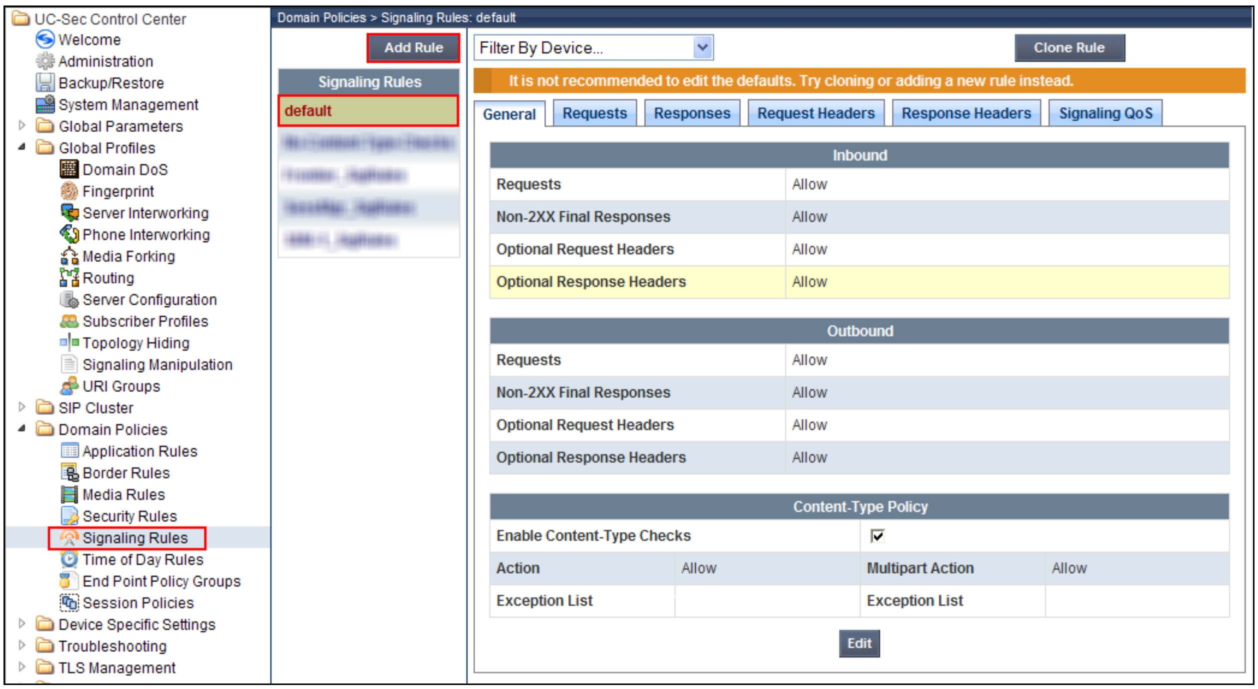
On the Advanced tab, set **Interworking Profile** to the interworking profile for Star Telecom defined in **Section 6.5.2**.



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 Star Telecom SIP server used the **default** rule. The compliance 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.

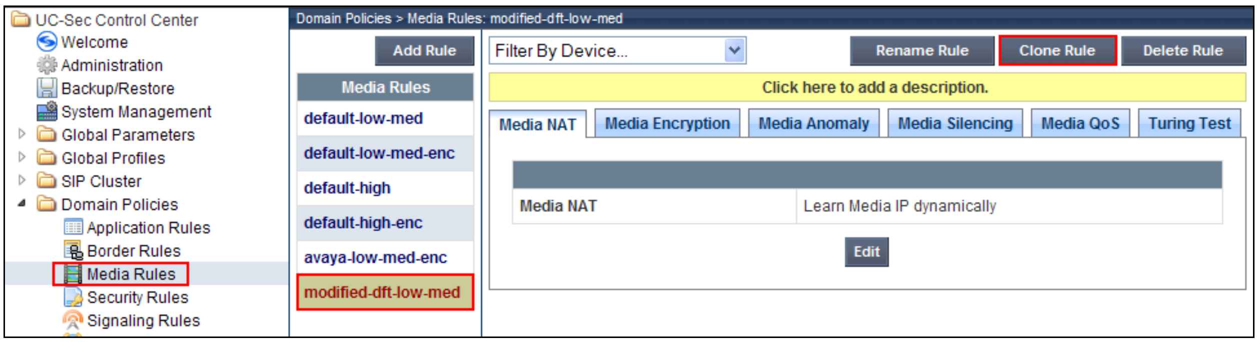
To create a new rule, navigate to **Domain Profiles → Signaling Rules** in the left pane. In the center pane, select **Add Rule**. A pop-up window (not shown) will appear requesting the name of the new rule, followed by a series of pop-up windows in which the rule parameters can be configured. Once complete,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



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 Profiles → 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 a series of pop-up windows in which the rule parameters can be configured. Once complete, the settings are shown in the far right pane. Alternatively, a new rule may be created by selecting an existing rule in the center pane and clicking the **Clone Rule** button in the right pane. This will create a copy of the selected rule which can then be edited as needed. To view the settings of an existing rule, select the rule from the center pane. The settings will appear in the right pane.

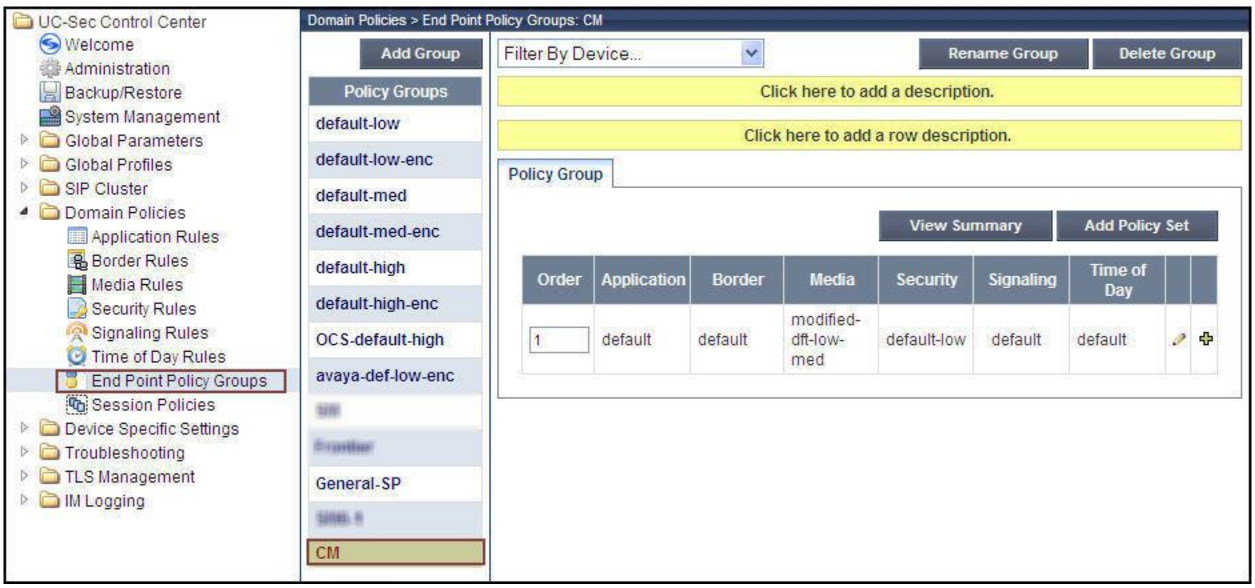


For the compliance test, a single media rule **modified-dft-low-med** was created that was used for both the Communication Manager and the Star Telecom SIP server. It was created by cloning the existing rule **default-low-med** which uses unencrypted media and then disabling **Media Anomaly Detection**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

6.9. Endpoint Policy Groups

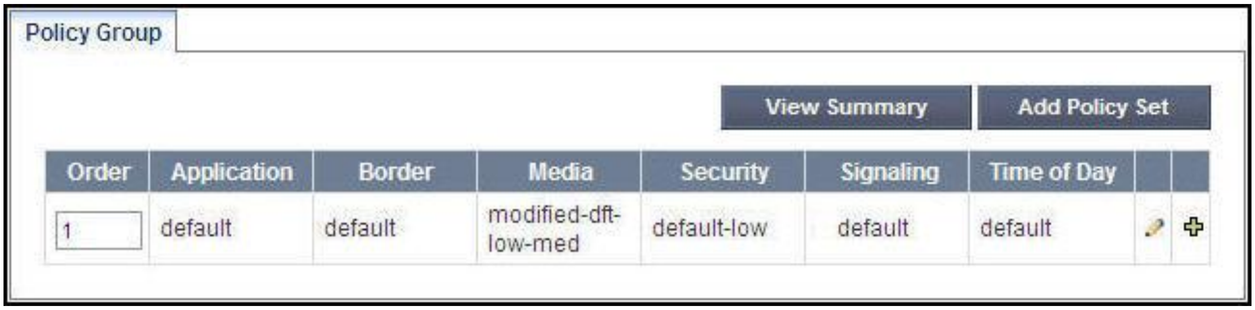
An endpoint policy group is a set of policies that will be applied to traffic between the Avaya SBCE and a signaling endpoint (connected server). Thus, separate endpoint policy groups must be created for Communication Manager and the service provider SIP server. The endpoint policy group is applied to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

To create a new group, navigate to **Domain Profiles → 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 a 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.



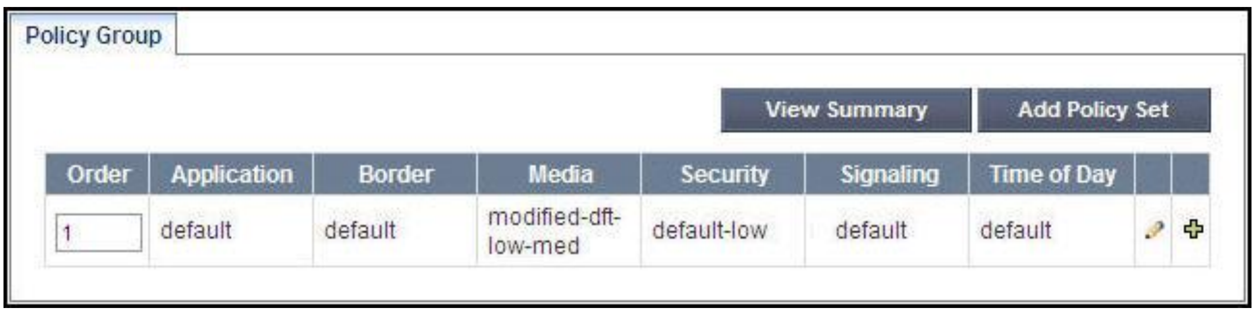
6.9.1. Endpoint Policy Group: Communication Manager

For the compliance test, the 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**.



6.9.2. Endpoint Policy Group: Star Telecom

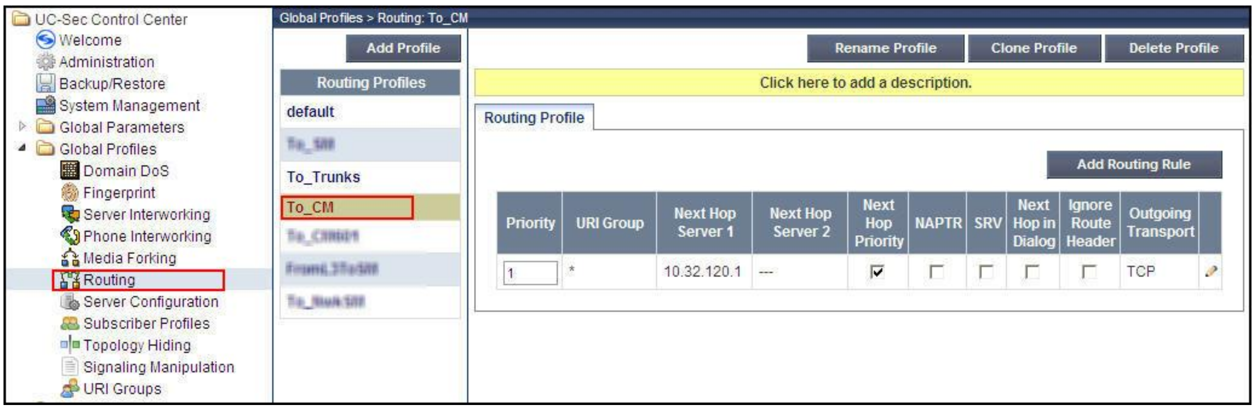
For the compliance test, the endpoint policy group **General-SP** was created for the Star Telecom SIP server. Default values were used for each of the rules which comprise the group with the exception of **Media**. For **Media**, select the media rule created in **Section 6.8**.



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 separate routing profiles for 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 a 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.



6.10.1. Routing: Communication Manager

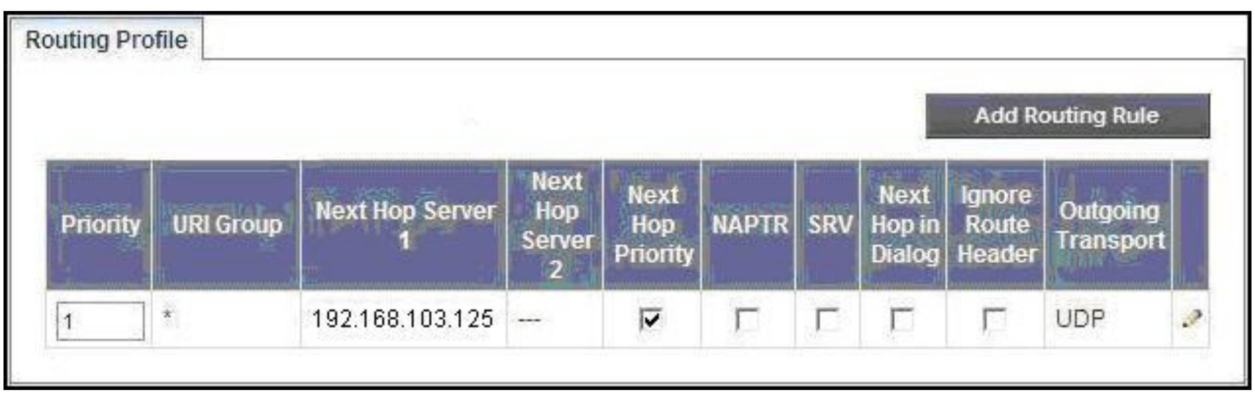
For the compliance test, the routing profile **To_CM** was created for Communication Manager. When creating the profile, configure the parameters as follows:

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

6.10.2. Routing: Star Telecom

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

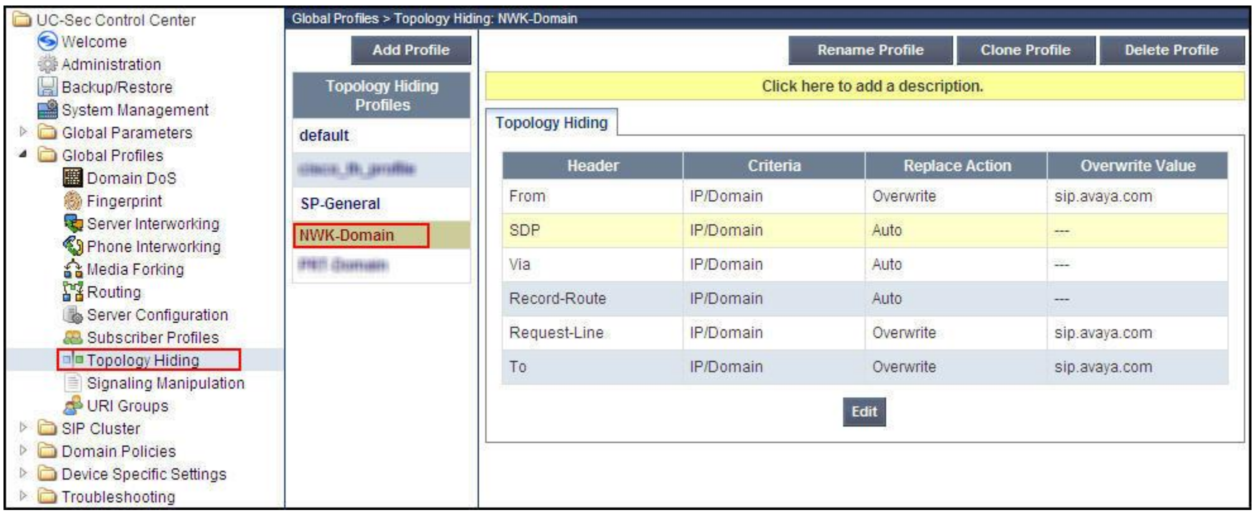
- Set **URI Group** to the wild card ***** to match on any URI.
- Set **Next Hop Server 1** field to the IP address of the Star Telecom SIP server.
- Enable **Next Hop Priority**.
- Set **Outgoing Transport** field to **UDP**.



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.



6.11.1. Topology Hiding: Communication Manager

For the compliance test, the topology hiding profile **NWK-Domain** 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**).

Topology Hiding

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

Edit

6.11.2. Topology Hiding: Star Telecom

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

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

Topology Hiding

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

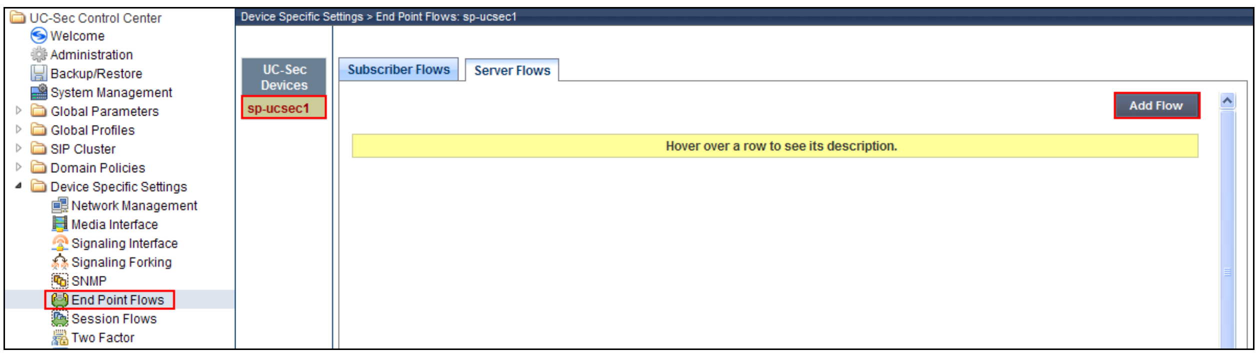
Edit

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 trunking, 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.

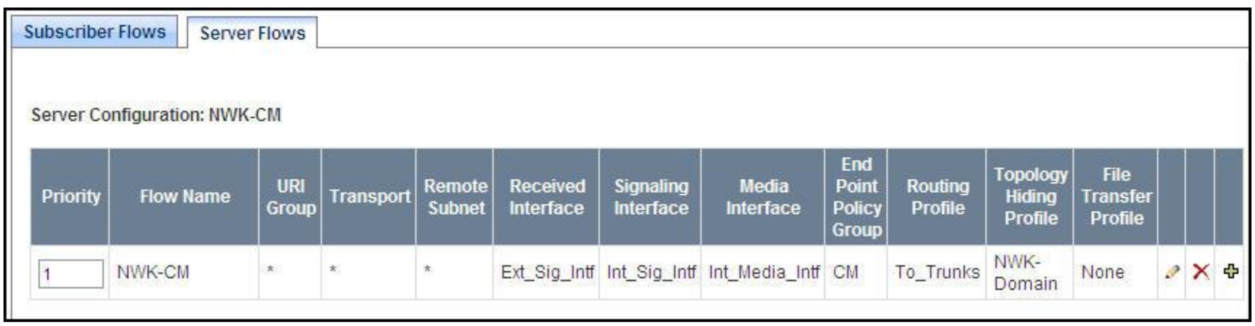


 Solution & Interoperability Test Lab Application Notes

6.12.1. End Point Flow: Communication Manager

For the compliance test, the endpoint flow **NWK-CM** was created for the Communication Manager. All traffic from the 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 **Flow Name**, enter a descriptive name.
- For **Server Configuration**, select the Communication Manager server created in **Section 6.6.1** (this setting is displayed as the flow heading in the screen shown below).
- To match all traffic, set **URI Group**, **Transport** and **Remote Subnet** to *.
- Set **Received Interface** to the external signaling interface.
- Set **Signaling Interface** to the internal signaling interface.
- Set **Media Interface** to the internal media interface.
- Set **End Point Policy Group** to the endpoint policy group defined for Communication Manager in **Section 6.9.1**.
- Set **Routing Profile** to the routing profile defined in **Section 6.10.1** used to direct traffic to the Star Telecom SIP server.
- Set **Topology Hiding Profile** to the topology hiding profile defined for Communication Manager in **Section 6.11.1**.



Subscriber Flows | Server Flows

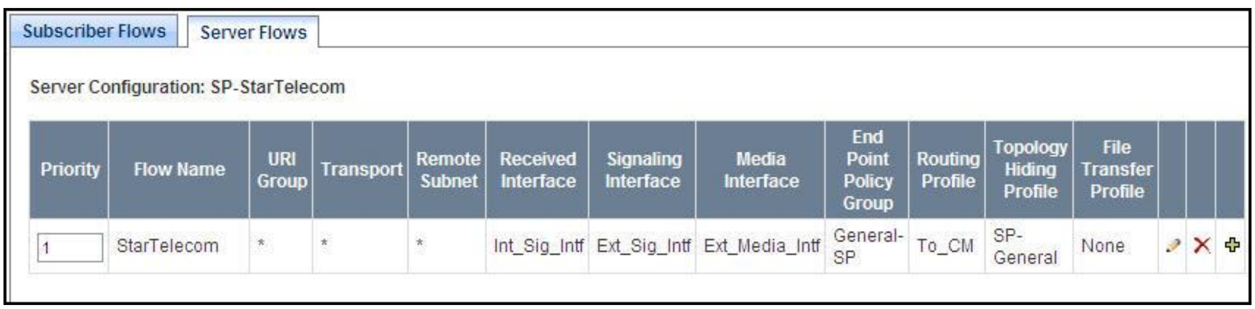
Server Configuration: NWK-CM

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-Domain	None

6.12.2. End Point Flow: Star Telecom

For the compliance test, the endpoint flow **StarTelecom** was created for the Star Telecom SIP server. All traffic from Star Telecom 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 Star Telecom SIP server created in **Section 6.6.2** (this setting is displayed as the flow heading in the screen shown below).
- To match all traffic, set **URI Group**, **Transport** and **Remote Subnet** to *****.
- Set **Received Interface** to the internal signaling interface.
- Set **Signaling Interface** to the external signaling interface.
- Set **Media Interface** to the external media interface.
- Set **End Point Policy Group** to the endpoint policy group defined for Star Telecom in **Section 6.9.2**.
- Set **Routing Profile** to the routing profile defined in **Section 6.10.2** used to direct traffic to Communication Manager.
- Set **Topology Hiding Profile** to the topology hiding profile defined for Star Telecom in **Section 6.11.2**.



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	StarTelecom	*	*	*	Int_Sig_Intf	Ext_Sig_Intf	Ext_Media_Intf	General-SP	To_CM	SP-General	None			

7. Star Telecom SIP Trunking Configuration

To use Star Telecom SIP Trunking, a customer must request the service from Star Telecom using the established sales and provisioning processes. The process can be started by contacting Star Telecom via the corporate web site at http://www.startelecom.ca and requesting information via the online sales links or telephone numbers.

During the signup process, Star Telecom will require that the customer provide the public IP address used to reach the Avaya SBCE at the edge of the enterprise network and information related to SIP configuration supported by the enterprise. Star Telecom will provide the customer the necessary information to configure the SIP-enabled Avaya enterprise solution. The provided information from Star Telecom includes:

- IP address of the Star Telecom SIP server / network edge SBC
- IP addresses and port numbers used for signaling and media through any security devices
- Transport and port number for the SIP connection from enterprise to Star Telecom
- Supported codecs
- DID numbers assigned to the enterprise

The above information is used to complete the configurations of Communication Manager and Avaya SBCE described in the previous sections.

The configuration between Star Telecom and the enterprise is a static configuration. There is no registration of the SIP trunk or enterprise users to the Star Telecom 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 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.

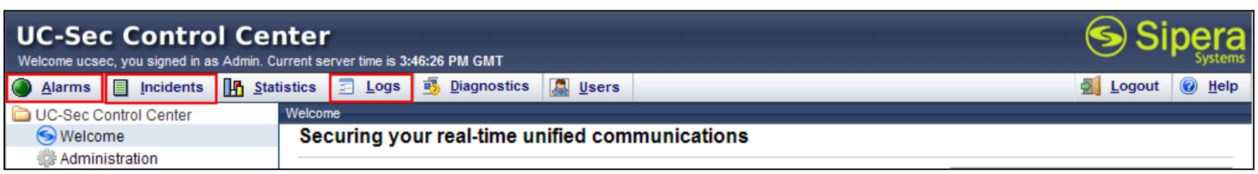
Troubleshooting:

1. Communication Manager:
   Use following Communication Manager SAT commands for troubleshooting.

   - **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 group number> - Displays trunk group information.
   - **status trunk** <trunk group number/channel number> - Displays signaling and media information for an active trunk channel.

2. Avaya SBCE:
   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.



9. Conclusion

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

10. References

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

Avaya Aura® Solution for Midsize Enterprise

[1] *Avaya Aura® Solution for the Midsize Enterprise (ME) 6.2 Intelligent Workbook*, Workbook Version 2.3, December 2012

[2] *Implementing Avaya Aura® Solution for Midsize Enterprise*, Release 6.2, Issue 4.2, July 2012

Avaya Aura® Communication Manager

[3] *Administering Avaya Aura® Communication Manager*, Document ID 03-300509, Release 6.2, Issue 7.0, December 2012

[4] *Programming Call Vectoring Features in Avaya Aura® Call Center Elite*, Release 6.2, Issue 1, December 2012

Avaya one-X®IP Phones

[5] *Avaya one-X® Deskphone H.323 9608 and 9611G User Guide*, Document ID 16-603593, Issue 3, February 2012

[6] *Avaya one-X® Deskphone H.323 for 9630 and 9630G IP Deskphone User Guide,* Document ID 16-300700, January 2013

[7] *Avaya one-X® Deskphone Value Edition 1616 IP Telephone User Guide,* Document ID 16-601448, June 2007

[8] *Administering Avaya one-X® Communicator,* October 2011

[9] *Using Avaya one-X® Communicator Release 6.1*, October 2011

Avaya Session Border Controller for Enterprise

Product documentation for UC-Sec can be obtained from Sipera using the link at http://www.sipera.com.

[9] *E-SBC 1U Installation Guide, Release 4.0.5,* Part Number: 101-5225-405v1.00, Release Date: November 2011

[10] *E-SBC Administration Guide, Release 4.0.5,* Part Number: 010-5424-405v1.00, Release Date: November 2011

RFC Documents

[11] RFC 3261 *SIP: Session Initiation Protocol*, http://www.ietf.org/

[12] 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.