Avaya Solution & Interoperability Test Lab

Application Notes for Configuring Telefonica del Peru SIP Trunk Service 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 procedures for configuring Session Initiation Protocol (SIP) Trunk Service between the service provider Telefonica del Peru and an Avaya SIP-enabled enterprise solution. The Avaya solution consists of Avaya Aura® Communication Manager Release 6.2, Avaya Session Border Controller for Enterprise Release 4.0.5 and various Avaya endpoints. The solution does not include the Avaya Aura® Session Manager and consequently SIP endpoints are not supported.

The test was performed to verify SIP trunk features including basic call, call forward (all calls, busy, no answer), call transfer (blind and consult), conference, and voice mail. The calls were placed in both directions with various Avaya endpoints. T.38 fax was also tested.

Telefonica del Peru SIP Trunk Service provides PSTN access via a SIP trunk between the enterprise and Telefonica's network as an alternative to legacy analog or digital trunks. This approach generally results in lower cost for the enterprise.

Telefonica del Peru 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 one of Telefonica's customer sites in Lima, Peru.

Table of Contents

1. Introduction

These Application Notes describe the procedures for configuring Session Initiation Protocol (SIP) Trunk Service between Telefonica del Peru and an Avaya SIP-enabled enterprise solution. The Avaya solution consists of Avaya Aura® Communication Manager Release 6.2, Avaya Session Border Controller for Enterprise Release 4.0.5 and various Avaya endpoints. The solution does not include Avaya Aura® Session Manager and consequently SIP endpoints are not supported.

Telefonica del Peru SIP Trunk Service referenced within these Application Notes is designed for enterprise business customers. Customers using this service with the Avaya SIP-enabled enterprise solution 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 analog and/or ISDN-PRI.

For brevity in these Application Notes, hereafter, Telefonica del Peru will be referred to as "Telefonica" or "Service Provider". Avaya Session Border Controller for Enterprise will be abbreviated and referred to as "Avaya SBCE".

2. General Test Approach and Test Results

A simulated enterprise site containing all the equipment for the Avaya SIP-enabled solution was installed at one of Telefonica's customer sites in Lima, Peru. The enterprise site was configured to connect to Telefonica SIP Trunk service by means of a broadband connection to the Public Internet.

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:

- Incoming PSTN calls to various desk-phone types. Desk-phone types at the enterprise included H.323, digital, and analog. All inbound calls from the PSTN were routed to the enterprise across the SIP trunk from Telefonica's network.
- Outgoing PSTN calls from various desk-phone types. Desk-phone types at the enterprise included H.323, digital, and analog. All outbound calls to the PSTN were routed from the enterprise across the SIP trunk to Telefonica's network.
- Avaya Soft Client: Inbound and outbound PSTN calls to/from Avaya one-X® Communicator soft-phone using H.323 protocol, in both, Road Warrior and Telecommuter modes.

- Various call types, including: local, long distance, international, outbound toll-free and local directory assistance.
- Codec support and negotiation. Telefonica supports the following codec's and order of preference: G729A, G711A and G.711MU.
- DTMF tone transmissions passed as out-of-band RTP events, as per RFC 2833.
- Caller ID presentation and Caller ID restriction.
- Voicemail navigation for inbound and outbound calls.
- Supplementary features such as call hold and resume, calls transfers (within the enterprise and to the PSTN); call forward (within the enterprise and to the PSTN) and conference.
- Mobility (EC500: answering at host extension or cellular).
- Routing inbound PSTN calls to call center agent queues.
- Network Call Redirection, using the 302 Redirection method, for routing inbound calls from the PSTN back out to the PSTN.
- Inbound and outbound T.38 fax to and from the PSTN.
- Static IP Authentication with the Service Provider.
- Inbound and outbound incomplete call attempts.
- Simultaneous active calls.
- Long duration calls.
- Call treatment for inbound and outbound calls: All trunks busy, invalid or not supported codec, SIP trunk signaling failure, calls to busy and invalid numbers.

Items not supported or not tested included the following:

- **SIP REFER:** SIP REFER method was disabled in Telefonica's Network. To disable the REFER method in Avaya Aura® Communication Manager, set "Network Call Redirection" to "N" in the SIP Trunk Group dedicated to Telefonica. Refer to **Section 5.7**.
- **Codec's not supported:** Telefonica responds with "500 Server Internal Error" instead of "488 Not Acceptable Here" to calls attempts with codec's not supported by Telefonica. This issue should **not** be seen during normal operation since the list of supported codec's should be discussed with Telefonica and configured in Avaya Aura® Communication Manager during the initial installation. For a list of supported codec's and the order of preference refer to **Section 5.4**.
- **Calling Party Number Block:** Calls from the PSTN to the enterprise with "Calling Party Number Block" or privacy enabled at the PSTN telephone failed to block the display of the calling party's number. For security reason privacy is disabled.
- Operator services such as dialing 0 or 0 + 10 digits are not supported in this offer by Telefonica.
- Inbound toll-free calls were not tested as part of the compliance test.

2.2. Test Results

Interoperability testing of Telefonica SIP Trunk Service with the Avaya Aura® SIP-enabled enterprise solution was completed successfully with the observations and limitations described below:

- **T.38 Fax**: T.38 fax calls from the enterprise to the PSTN were failing due to attempts to re-negotiate T.38 parameters **after** the T.38 connection was established/active. Avaya Aura® Communication Manager was responding with "491 Request Pending – another fax request in progress" to a re-INVITE received **after** the T.38 connection was established with a 200 ok. The issue was solved by Telefonica with a parameter change in one of Telefonica's Media Gateways responsible for routing calls to the PSTN (Parameter changed: **SET FAXPARA: CUDP=DISABLE).**
- **302 SIP Redirect Method:** This applies to incoming calls from the PSTN being re-directed back out to the PSTN with the 302 SIP Redirect method. When static IP is used instead of domain name, Avaya Aura® Communication Manager inserts the IP address of the Service Provider's SIP proxy server in the "Contact Header" of the 302 message, instead of the IP address of Telefonica's Next-Hop server use by Telefonica to route calls to the PSTN. This causes an attempt by Telefonica's soft-switch to route the call right back to the same SIP proxy server, this results in the call failing to complete. The issue was solved by Telefonica with a Header Manipulation Rule (HMR) added to Telefonica's ACME SBC. The HMR changed the IP address in the Contact header of the 302 message received with a valid Next-Hop server IP address used by Telefonica to route calls to the PSTN.

2.3. Support

For support on Telefonica del Peru SIP Trunk Services offer, visit the online website at http://www.movistar.com.pe/negocios

3. Reference Configuration

Figure 1 illustrates the configuration used for the Compliance Testing, showing the Avaya SIP-enabled enterprise solution connected to Telefonica SIP Trunk Service through a public, high speed Internet connection.

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

- Avaya Aura® Communication Manager and Communication Manager Messaging, on the Avaya S8300D Server.
- Avaya G430 Media Gateway.
- Avaya Session Border Controller for Enterprise, on a Dell server.
- Avaya 4600 Series IP Deskphones (H.323).
- Avaya Digital Deskphone.
- Analog Deskphone.
- Avaya one-X® Communicator Softphone (H.323).

The Avaya SBCE constitutes the single point of connection between the public network and the Local Area Network in the enterprise. In addition to providing comprehensive security to all SIP and RTP traffic entering the private network, the Avaya SBCE enables the interoperability with dissimilar SIP trunk service providers, by allowing the manipulation and adjustment of the elements in the packets flowing through its interfaces.

For inbound calls, the calls flow from the service provider to the external firewall, then to the Avaya SBCE. After the Avaya SBCE performs the necessary security checks and manipulations, the call is sent to Avaya Aura® Communication Manager, where incoming call treatment, such as incoming digit translations and class of service restrictions may be performed.

Outbound calls to the PSTN were processed by Avaya Aura® Communication Manager for outbound feature treatment such as automatic route selection and class of service restrictions. Once Avaya Aura® Communication Manager selects the proper SIP trunk; the call is routed to the Avaya SBCE for additional call treatment and manipulations before sending the call to Telefonica's network.

The transport protocol between the Avaya SBCE and Telefonica across the public IP network is UDP. The transport protocol between the Avaya SBCE and the Avaya Aura® Communication Manager server across the enterprise IP network is TCP.

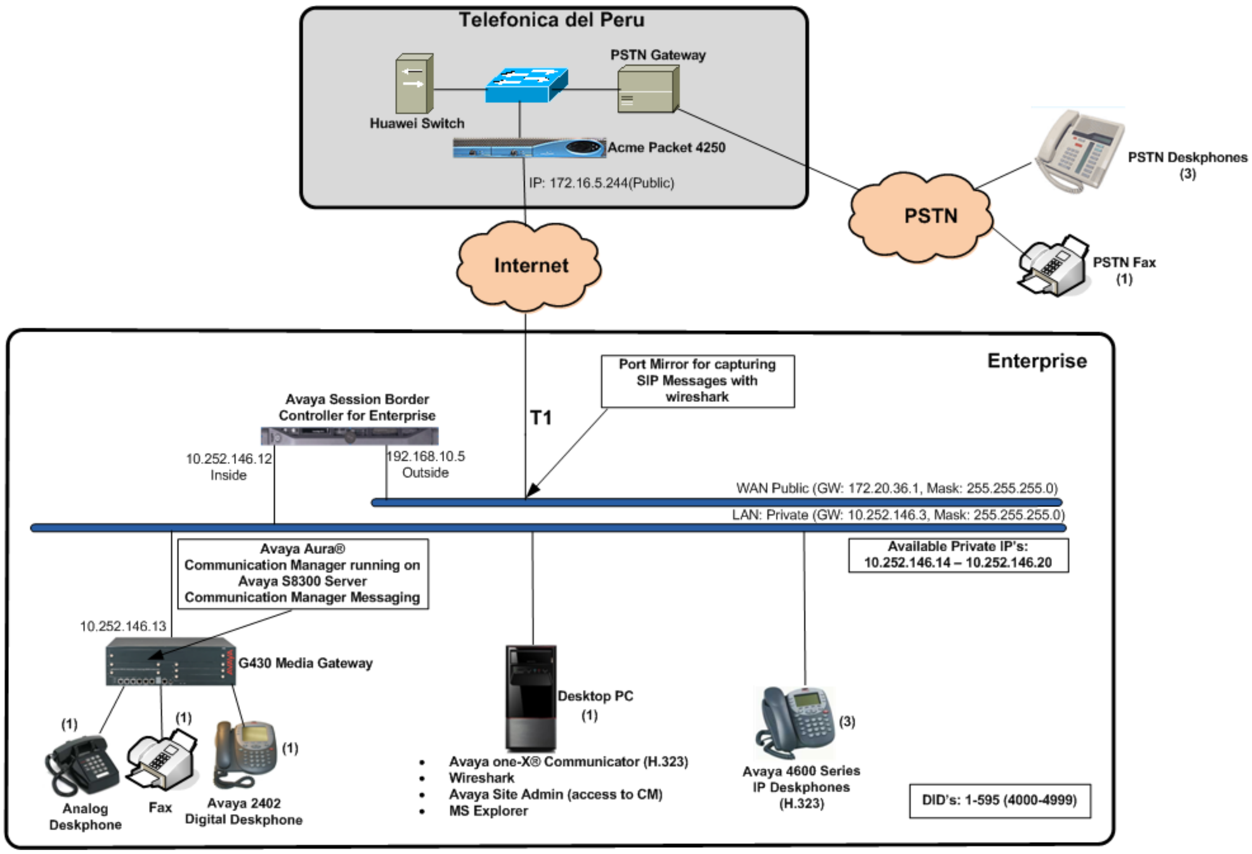


Figure 1: Telefonica del Peru SIP Trunk Service with Avaya SIP enabled enterprise solution.

For security purposes, private addresses are shown in these Application Notes for the Avaya SBCE and the service provider's network interfaces, instead of the real public IP addresses used during the compliance testing.

4. Equipment and Software Validated

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

Component	Version
Avaya	
Avaya Aura® Communication Manager, on Avaya S8300D Server	6.2 SP3 (02.0.823.0-20001)
Avaya Aura® Communication Manager Messaging	6.2 SP1 CMM-02.0.823.0-0104
Avaya Session Border Controller for Enterprise, on a Dell server.	4.0.5.Q19
Avaya G430 Media Gateway	31.20.1
Avaya 4600 Series IP Deskphones (H.323)	R2.9 SP2
Avaya one-X® Communicator Softphone (H.323)	6.1.5.07-SP5-37495
Avaya 2402 Digital Deskphone	n/a
Analog Deskphone	n/a
Telefonica	
Acme-Packet Net-Net 4250 SBC	Firmware SC6.2.0, MR-11 patch 2
Huawei Soft Switch	SoftX3000 V300R601

5. Configure Avaya Aura® Communication Manager

This section describes the procedure for configuring Avaya Aura® Communication Manager. A SIP trunk is established between Avaya Aura® Communication Manager and the Avaya SBCE for use by signaling traffic to and from Telefonica's network. It is assumed the general installation of Avaya Aura® Communication Manager, Messaging, Avaya G430 Media Gateway and endpoints has been previously completed.

The Avaya Aura® 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 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 and from the service provider. The example shows one license with a capacity of **4000** trunks are available and **6** are in use. The license file installed on the system controls the maximum values for these attributes. If a required feature is not enabled or there is insufficient capacity, contact an authorized Avaya sales representative to add additional capacity.

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

IP PORT CAPACITIES                                              USED
                     Maximum Administered H.323 Trunks: 4000  10
           Maximum Concurrently Registered IP Stations: 2400  3
             Maximum Administered Remote Office Trunks: 4000  0
Maximum Concurrently Registered Remote Office Stations: 2400  0
              Maximum Concurrently Registered IP eCons: 68    0
  Max Concur Registered Unauthenticated H.323 Stations: 100   0
                        Maximum Video Capable Stations: 2400  0
                   Maximum Video Capable IP Softphones: 2400  1
                       Maximum Administered SIP Trunks: 4000  6
  Maximum Administered Ad-hoc Video Conferencing Ports: 4000  0
   Maximum Number of DS1 Boards with Echo Cancellation: 80    0
                             Maximum TN2501 VAL Boards: 10    0
                     Maximum Media Gateway VAL Sources: 50    1
           Maximum TN2602 Boards with 80 VoIP Channels: 128   0
          Maximum TN2602 Boards with 320 VoIP Channels: 128   0
   Maximum Number of Expanded Meet-me Conference Ports: 300   0

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

5.2. System Features

Use the **change system-parameters features** command to set the **Trunk-to-Trunk Transfer** field to **all** to allow incoming 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

              Music (or Silence) on Transferred Trunk Calls? no
              DID/Tie/ISDN/SIP Intercept Treatment: attendant
    Internal Auto-Answer of Attd-Extended/Transferred Calls: transferred
                  Automatic Circuit Assurance (ACA) Enabled? n




             Abbreviated Dial Programming by Assigned Lists? n
       Auto Abbreviated/Delayed Transition Interval (rings): 2
                     Protocol for Caller ID Analog Terminals: Bellcore
    Display Calling Number for Room to Room Caller ID Calls? n
```

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: _____

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 Avaya Aura® Communication Manager *(***procr**) and the inside interface of the Avaya SBCE (**ASBCE_A1**). 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
ASBCE_A1               10.252.146.12
default                0.0.0.0
messaging              10.252.146.13
procr                  10.252.146.13
procr6                 ::















( 5  of 5    administered node-names were displayed )
Use 'list node-names' command to see all the administered node-names
Use 'change node-names ip xxx' to change a node-name 'xxx' or add a node-name
```

5.4. Audio Codec

Use the **change ip-codec-set** command to define a list of audio codec's to use for calls between the enterprise and the service provider. For the compliance test, ip-codec-set 4 was used for this purpose. The Telefonica SIP Trunk Service supports audio codec's G.729A, G.711A and G.711MU, in this order of preference. Enter **G.729A, G.711A** and **G.711MU** in the **Audio Codec** column of the table. 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.711A            n          2        20
 3: G.711MU           n          2        20
 4:
 5:
 6:
 7:
```

Set the **Fax Mode** field to **t.38-standard** on **Page 2**, Telefonica supports T.38 fax transport.

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

                          IP Codec Set

                              Allow Direct-IP Multimedia? n



                    Mode                    Redundancy
    FAX             t.38-standard              0
    Modem           off                        0
    TDD/TTY         US                         3
    Clear-channel   n                          0
```

5.5. IP Network Regions

Create a separate IP network region for the service provider trunk group. 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 ip-network region 4 with the following parameters:

- Leave the **Authoritative Domain** field blank. For the compliance test, IP addresses instead of domain names were used in the host portion of SIP URIs of packets flowing between Avaya Aura® Communication Manager and the Avaya SBCE.
- 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 could be further restricted at the trunk level on the Signaling Group form if necessary.
- 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: 1        Authoritative Domain: ________________________________________
    Name: ____________________
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 (the rest of the enterprise). Enter the desired IP codec set in the **codec set** column of the row with destination region (**dst rgn**) 1. Default values may be use 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).

```
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
 7
 8
 9
 10
 11
 12
 13
 14
 15
```

5.6. Signaling Group

Use the **add signaling-group** command to create a signaling group between Avaya Aura® Communication Manager and the 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 4 was used for this purpose. Configure signaling group 4 using the following parameters:

- Set the **Group Type** field to **sip**.
- Set the **IMS Enabled** field to **n**.
- Set the **Transport Method** to **tcp**.
- Set the **Peer Detection Enabled** field to **y**.
- Set the **Near-end Node Name** to **procr.** This node name maps to the IP address of Avaya Aura® Communication Manager as defined in **Section 5.3**.
- Set the **Far-end Node Name** to **ASBCE_A1.** This node name maps to the IP address of the inside interface of the Avaya SBCE, as defined in **Section 5.3**.
- Set the **Near-end Listen Port** and **Far-end Listen Port** set to **5060**.
- Set the **Far-end Network Region** to the IP network region defined for the service provider in **Section 5.5**.
- Leave the **Far-end Domain** field blank.
- Set the **DTMF over IP** field to **rtp-payload**. This value enables Avaya Aura® 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 Avaya Aura® Communication Manager to redirect media traffic directly between the SIP trunk and the enterprise endpoint. Note that media shuffling can also be enabled or restricted on each IP network regions forms.
- Default values may be used for all other fields.

```
change signaling-group 4                                        Page   1 of   2
                                SIGNALING GROUP

 Group Number: 4             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: ASBCE_A1
 Near-end Listen Port: 5060                   Far-end Listen Port: 5060
                                           Far-end Network Region: 4

Far-end Domain:
                                                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): 6
```

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 4 was used. Configure trunk group 4 using the following parameters.

- Set the **Group Type** field to **sip**.
- Enter a descriptive name for the **Group Name**.
- Leave the **Direction** field to **two-way** (default value)
- 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 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.

```
change trunk-group 4                                            Page   1 of  21
                                TRUNK GROUP

Group Number: 4                   Group Type: sip            CDR Reports: y
  Group Name: CM-Sipera                  COR: 1        TN: 1         TAC: 604
   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: 4
                                                 Number of Members: 6
```

On **Page 2**, 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 default value of **100** seconds was used.

```
change trunk-group 4                                            Page   2 of  21
      Group Type: sip

TRUNK PARAMETERS

     Unicode Name: auto

                                              Redirect On OPTIM Failure: 5000

            SCCAN? n                                 Digital Loss Group: 18
                      Preferred Minimum Session Refresh Interval(sec): 100

 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 **public.** 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.

```
change trunk-group 4                                            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
```

On **Page 4**, set the **Network Call Redirection** field to **n** (default value). This disables the use of the SIP REFER method for calls transferred back to the PSTN. This field needs to be disabled in Avaya Aura® Communication Manager since Network Call Redirection using the SIP REFER method was disabled in Telefonica's network. Set the **Send Diversion Header** field to **y**. This is needed to support call forwarding of inbound calls back to the PSTN and some Extension to Cellular (EC500) call scenarios. Set the **Support Request History** field to **n**.

Set the **Telephone Event Payload Type** to **97**, the value preferred by Telefonica. Default values were used for all other fields.

```
change trunk-group 4                                          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: 97


                    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 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. DID numbers are provided by the SIP service provider. Each DID number is assigned in this table to one enterprise internal extension or Vector Directory Numbers (VDNs), and they are used to authenticate the caller with the Service Provider. In the sample configuration, 9 DID numbers were assigned for testing. These 9 numbers were mapped to 9 extensions, 4001 to 4009. These 7-digit numbers, each with a prefix of "1"were used in the outbound calling party information on the trunk to the service provider when calls were originated from these 9 extensions. For routing Telefonica requires a prefix of "1" for each DID number, without the "1" some call types may not work, such as calls to international numbers.

```
change public-unknown-numbering 1                               Page   1 of   2
                      NUMBERING - PUBLIC/UNKNOWN FORMAT
                                          Total
Ext Ext             Trk       CPN          CPN
Len Code            Grp(s)    Prefix       Len
                                                  Total Administered: 10
 4  3                                       4        Maximum Entries: 240
 4  3001            4         15954001      8
 4  3002            4         15954002      8       Note: If an entry applies to
 4  3003            4         15954003      8       a SIP connection to Avaya
 4  3004            4         15954004      8       Aura(R) Session Manager,
 4  3005            4         15954005      8       the resulting number must
 4  3006            4         15954006      8       be a complete E.164 number.
 4  3007            4         15954007      8
 4  3008            4         15954008      8
 4  3009            4         15954009      8
```

In a real customer environment, DID numbers are usually comprised of the local extension plus a prefix. If this is true, then a single public unknown numbering entry can be applied for all extensions. In the example below, all stations with a 4-digit extension length, beginning with 3, will send the calling party number as the **CPN Prefix** plus the extension number.

```
change public-unknown-numbering 1                               Page   1 of   2
                      NUMBERING - PUBLIC/UNKNOWN FORMAT
                                          Total
Ext Ext             Trk       CPN          CPN
Len Code            Grp(s)    Prefix       Len
                                                  Total Administered: 10
 4  3               4         1595          8        Maximum Entries: 240
```

5.9. Inbound Routing

DID numbers received from Telefonica can be mapped to an extension using the incoming call handling treatment of the receiving trunk group. Use the **change inc-call-handling-trmt** command to create an entry for each DID.

```
change inc-call-handling-trmt trunk-group 4                   Page   1 of   3
                       INCOMING CALL HANDLING TREATMENT
 Service/      Number   Number       Del  Insert
 Feature        Len      Digits
 public-ntwrk   7   5954001          7    3001
 public-ntwrk   7   5954002          7    3002
 public-ntwrk   7   5954003          7    3003
 public-ntwrk   7   5954004          7    3004
 public-ntwrk   7   5954005          7    3005
 public-ntwrk   7   5954006          7    3006
 public-ntwrk   7   5954007          7    3007
 public-ntwrk   7   5954008          7    3011
 public-ntwrk   7   5954009          7    3009
 public-ntwrk
 public-ntwrk
 public-ntwrk
 public-ntwrk
 public-ntwrk
 public-ntwrk
 public-ntwrk
 public-ntwrk
 public-ntwrk
```

In a real customer environment, where the DID number is usually comprised of the local extension plus a prefix, a single entry can be applied for all extensions, like in the example below.

```
change inc-call-handling-trmt trunk-group 4                   Page   1 of   3
                       INCOMING CALL HANDLING TREATMENT
 Service/      Number   Number       Del  Insert
 Feature        Len      Digits
 public-ntwrk   7   595              3
```

5.10. Outbound Routing

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

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

Dialed String	Total Length	Call Type	Dialed String	Total Length	Call Type	Dialed String	Total Length	Call Type
1	4	ext						
2	4	ext						
3	4	ext						
4	4	ext						
5	5	ext						
6	3	dac						
7	5	ext						
8	1	fac						
9	1	fac						
*	3	dac						
#	2	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  10
                               FEATURE ACCESS CODE (FAC)
         Abbreviated Dialing List1 Access Code: ____
         Abbreviated Dialing List2 Access Code: ____
         Abbreviated Dialing List3 Access Code: ____
Abbreviated Dial - Prgm Group List Access Code: ____
                      Announcement Access Code: #1__
                       Answer Back Access Code: ____
                         Attendant Access Code: __
      Auto Alternate Routing (AAR) Access Code: 8___
    Auto Route Selection (ARS) - Access Code 1: 9___     Access Code 2: ____
                 Automatic Callback Activation: ____      Deactivation: ____
Call Forwarding Activation Busy/DA: ____    All: ____      Deactivation: ____
   Call Forwarding Enhanced Status: ____    Act: ____      Deactivation: ____
                         Call Park Access Code: ____
                       Call Pickup Access Code: ____
CAS Remote Hold/Answer Hold-Unhold Access Code: ____
                  CDR Account Code Access Code: ____
                        Change COR Access Code: ____
                   Change Coverage Access Code: ____
            Conditional Call Extend Activation: ____      Deactivation: ____
                   Contact Closure   Open Code: ____        Close Code: ____
```

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 4 which contains the SIP trunk group to the service provider.

```
change ars analysis 3                                           Page   1 of   2
                             ARS DIGIT ANALYSIS TABLE
                                 Location: all            Percent Full: 2
```

Dialed String	Total Min	Total Max	Route Pattern	Call Type	Node Num	ANI Reqd
3	7	7	4	hnpa		n
4	7	7	4	hnpa		n
411	3	3	deny	svcl		n
5	7	7	4	hnpa		n
555	7	7	deny	hnpa		n
595	7	7	4	hnpa		n
6	7	7	4	hnpa		n
611	3	3	1	svcl		n
7	7	7	2	hnpa		n
8	7	7	2	hnpa		n
811	3	3	1	svcl		n
9	9	9	4	hnpa		n
911	3	3	1	svcl		n
976	7	7	deny	hnpa		n
						n

The route pattern defines which trunk group will be used for the call and performs any necessary digit manipulation. Use the **change route-pattern** command to configure the parameters for the service provider trunk route pattern in the following manner. The example below shows the values used for route pattern 4 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 4 was used as described in **Section 5.7**.
- **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.
- Default values were used for all other fields.

```
change route-pattern 4                                          Page   1 of   3
                    Pattern Number: 4   Pattern Name: CM62-SIPERA
                             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: 4    0                                                               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
```

6. Configure Avaya Session Border Controller for Enterprise

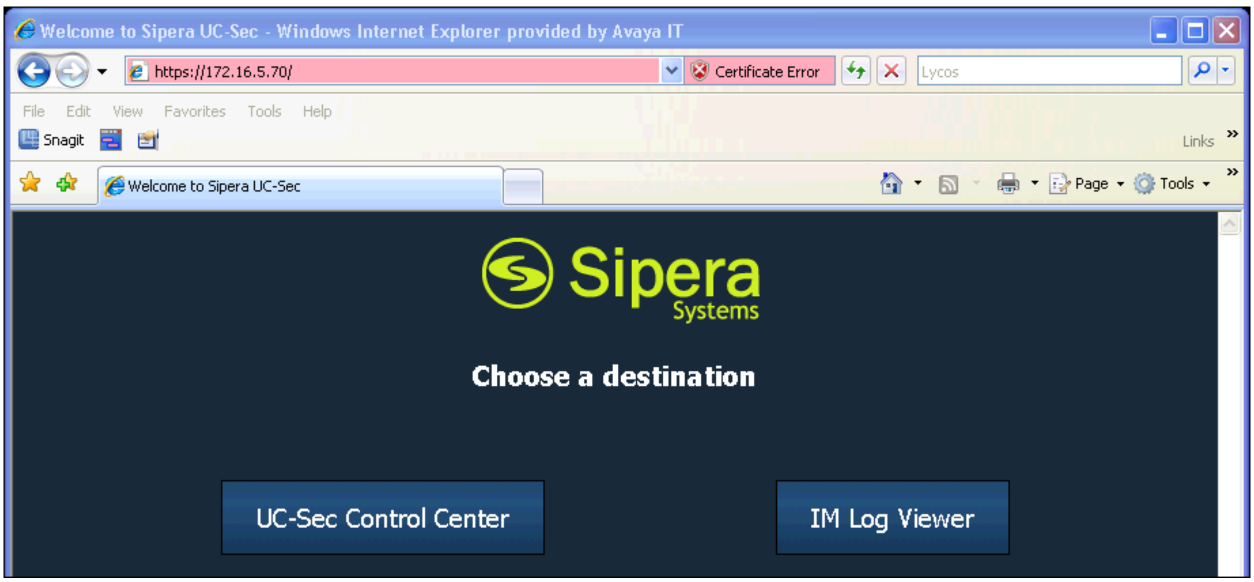
This section describes the required configuration of the Avaya SBCE to connect to Telefonica's SIP Trunk service. This configuration is done in two stages. The first part or initial configuration is done via the Provisioning Script (not shown), which requires a serial connection between a terminal device and the Console port of the Avaya SBCE.

Once the Avaya SBCE is provisioned and ready to be used on the IP network, the remainder of the configuration is accomplished using the server's web interface.

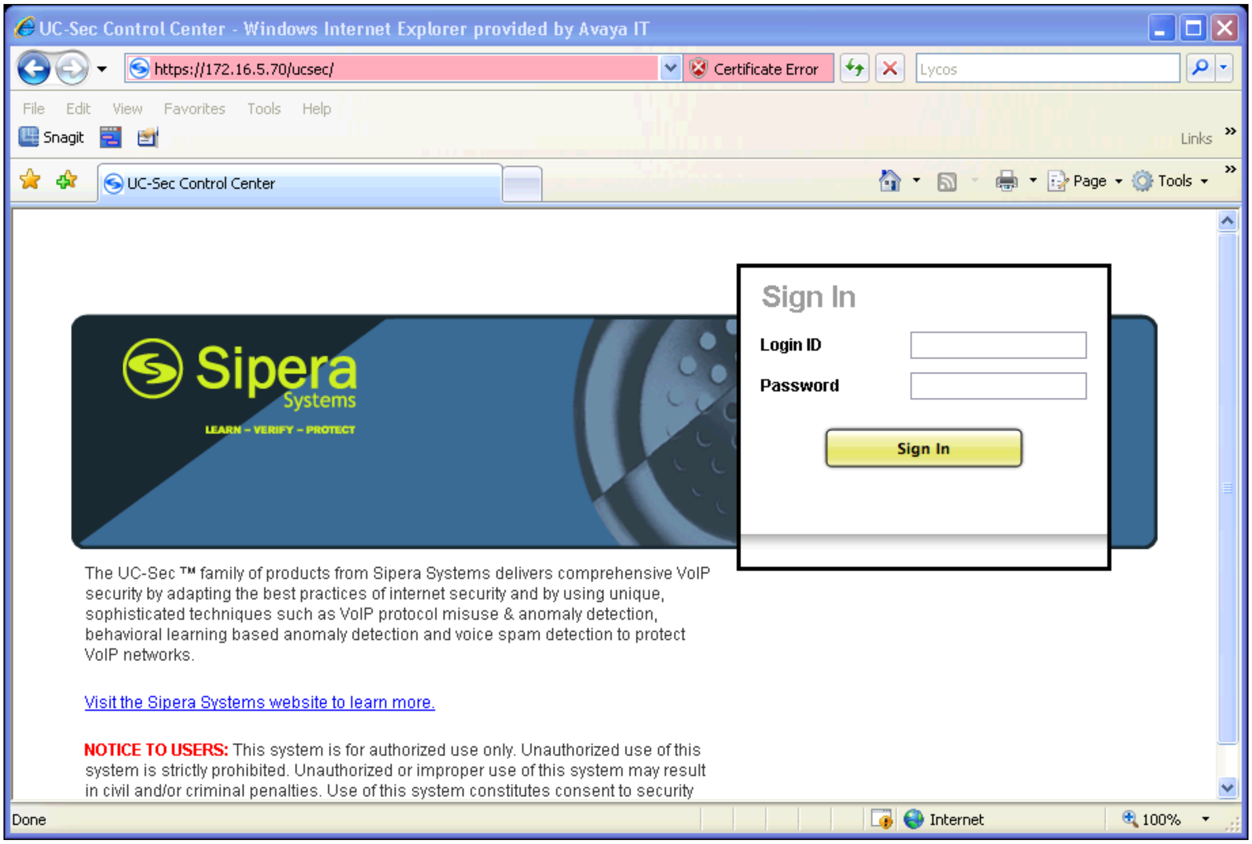
It is assumed in these Application Notes that the first stage of the configuration or the configuration that is accomplished via Provisioning script was already done; the configuration shown here is accomplished using the Avaya SBCE web interface.

6.1. Log in Avaya SBCE

Access the web interface by typing "https://x.x.x.x" (where x.x.x.x is the management IP of the Avaya SBCE)



Select **UC-Sec Control Center** and enter the **login ID** and **password.**



6.2. Global Profiles

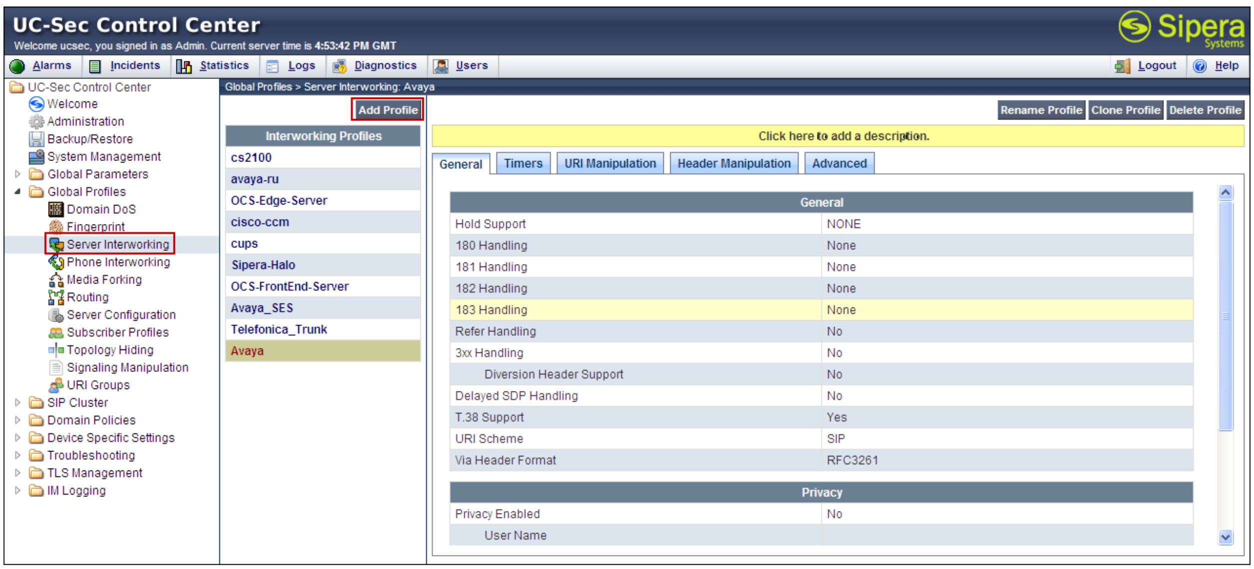
The Global Profiles Menu, on the left navigation pane, allows the configuration of parameters that affect all the devices under the UC-Sec control Center.

6.2.1. Server Interworking

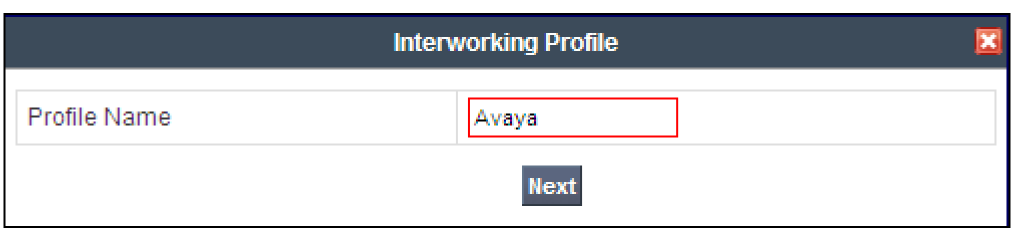
Interworking Profile features are configured to facilitate interoperability of implementations between enterprise SIP-enabled solutions and different SIP trunk service providers.

On the left navigation pane, select **Global Profiles → Server Interworking**. Several profiles have been already pre-defined and they populate the list under **Interworking Profiles**. If a different profile is needed, an existing default profile can be "cloned" and modified, or a new Interworking Profile can be created.

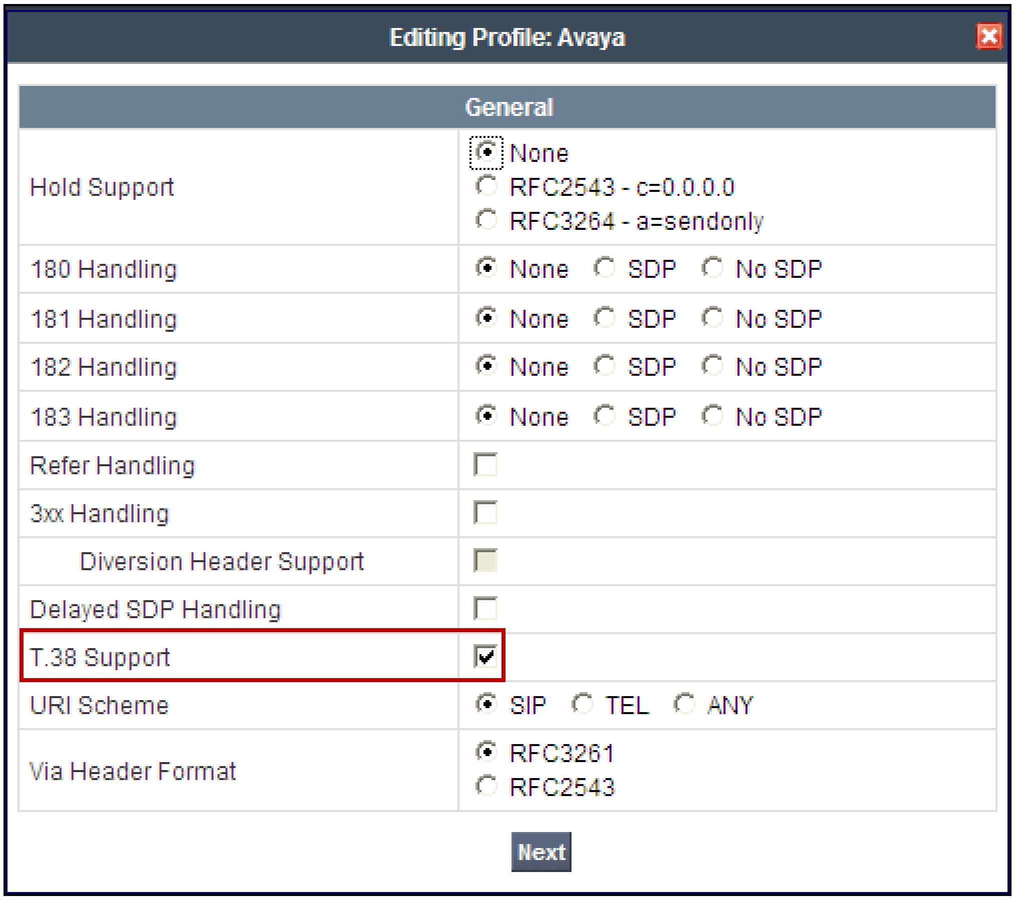
For the compliance test, a new profile was created. Click **Add Profile.**



Add a profile name and click **Next**.

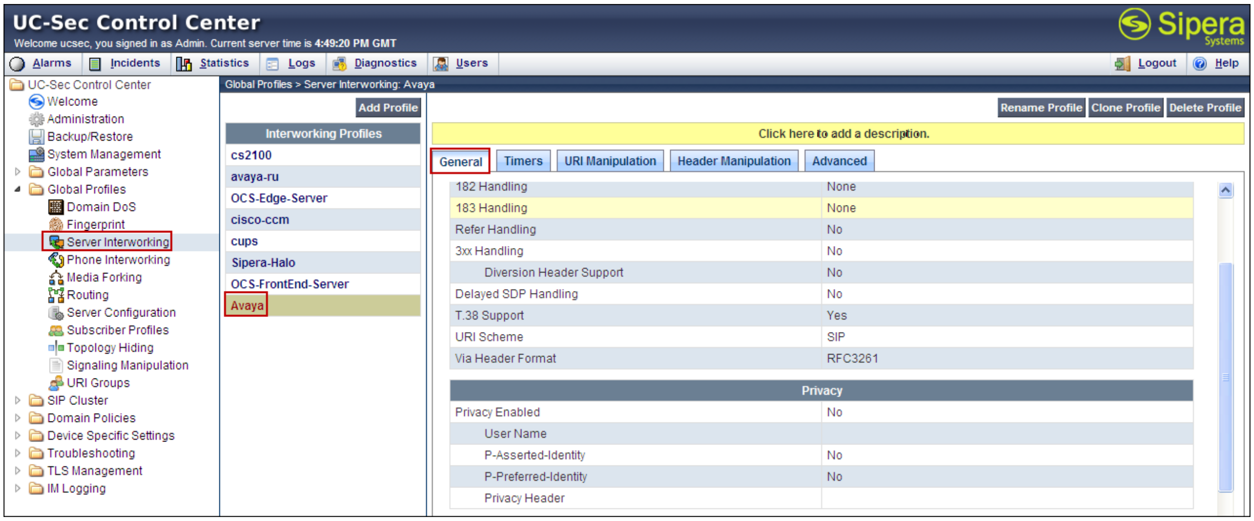


In the **General** screen, **T.38 Support** box is checked, since T.38 fax is supported by Telefonica. Leave other settings with their default values. Click **Next** to continue.



Click **Next** on the **Privacy** and **Timers** tabs and **Finish** on the **Advanced** tab (not shown) to save and exit.

The following screen capture shows the **General** tab of newly added **Avaya** Profile.

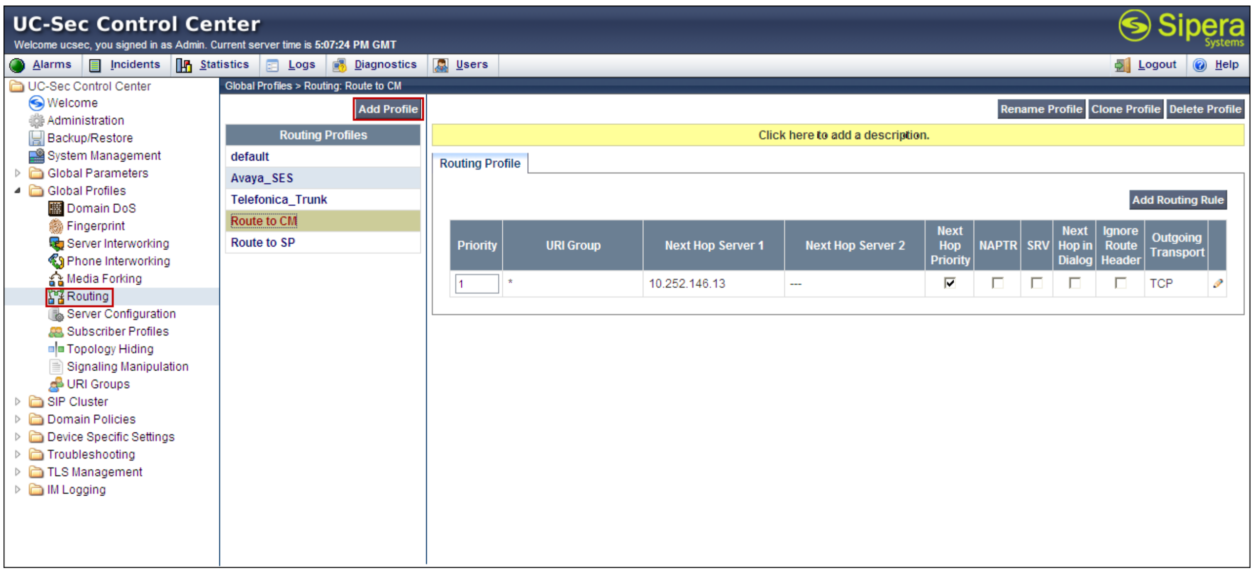


6.2.2. Routing Profiles

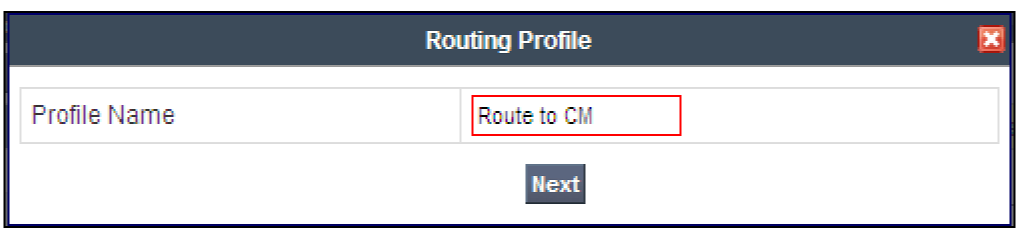
Routing profiles define a specific set of routing criteria to be used, in conjunction with other types of domain policies, to determine the route that SIP packets should follow to arrive at their intended destination. Two Routing Profiles were created in the test configuration, one for inbound calls, with Avaya Aura® Communication Manager as the destination, and the second one for outbound calls, which are routed to Telefonica's network as the destination.

To create the inbound route, from the **Global Profiles** menu on the left-hand side:

- Select the **Routing** tab.
- Select **Add Profile.**

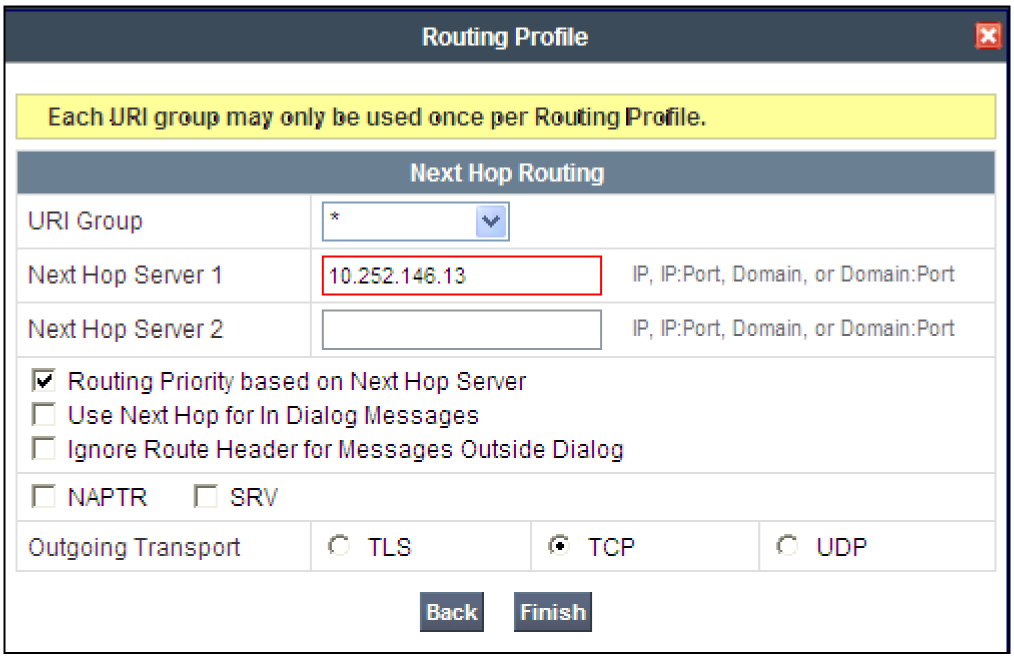


- Enter Profile Name: **Route to CM.** Click **Next.**

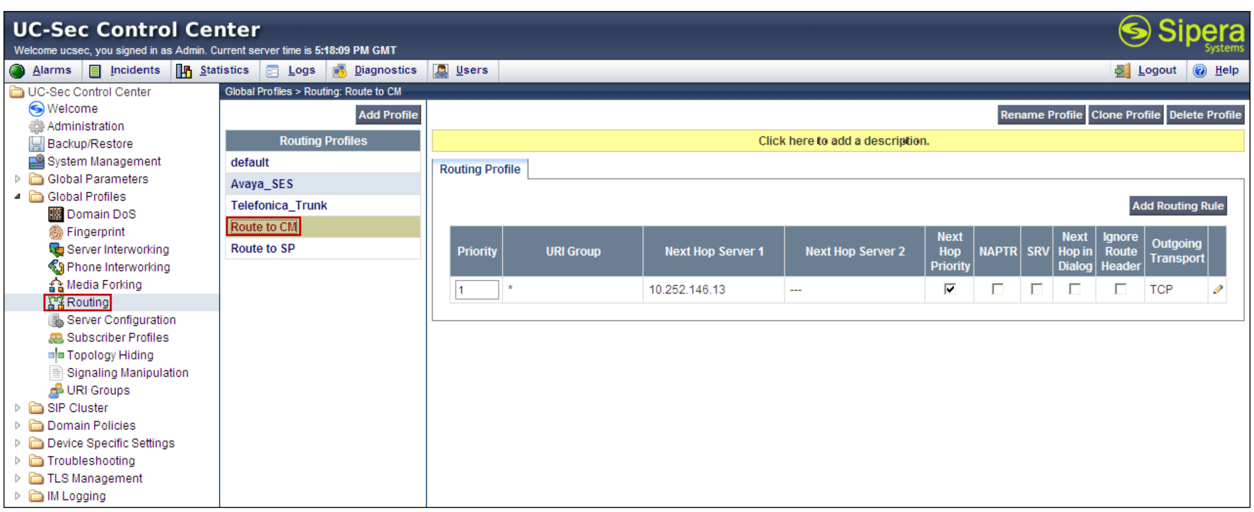


On the next screen, complete the following:

- **Next Hop Server 1: 10.252.146.13**. This is the IP address of the **procr** interface in Avaya Aura® Communication Manager configured in **Section 5.3**.
- Check **Routing Priority Based on Next Hop Server**.
- **Outgoing Transport: TCP**. This protocol must match the value used on the Avaya Aura® Communication Manager signaling group form in **Section 5.6**.
- Click **Finish**.

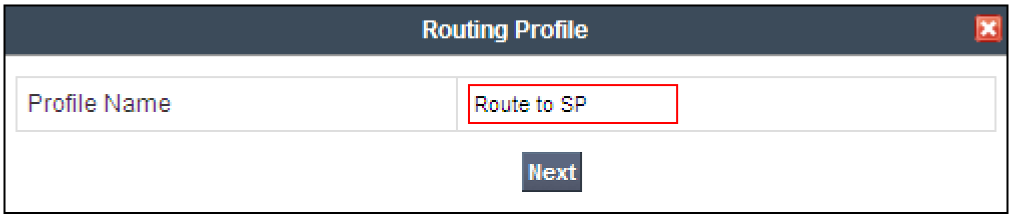


The following screen shows the added **Route to CM** Profile.

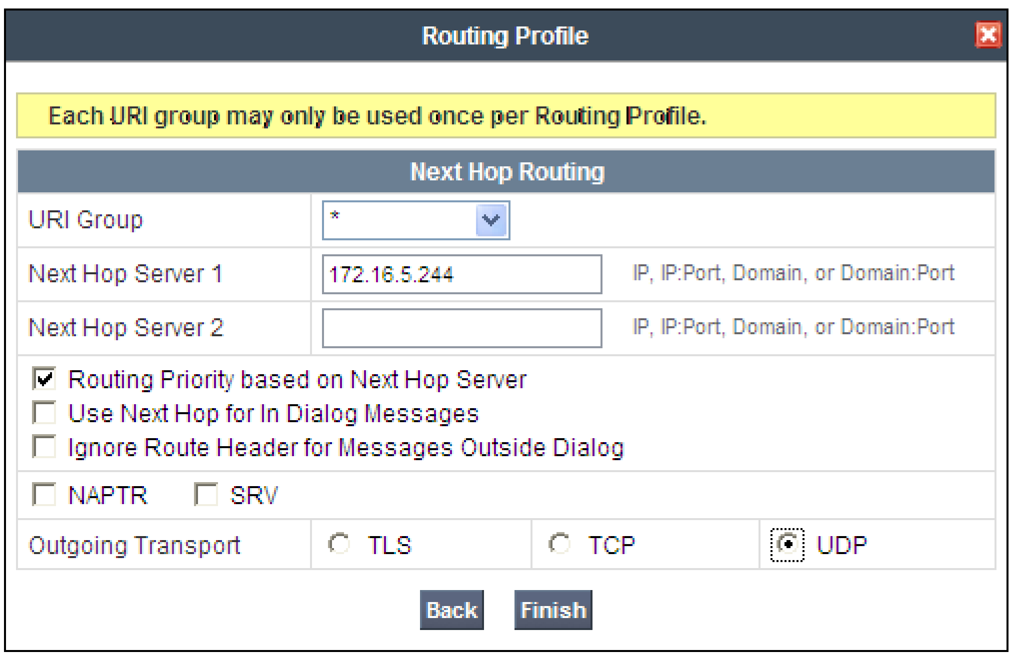


Similarly, for the outbound route:

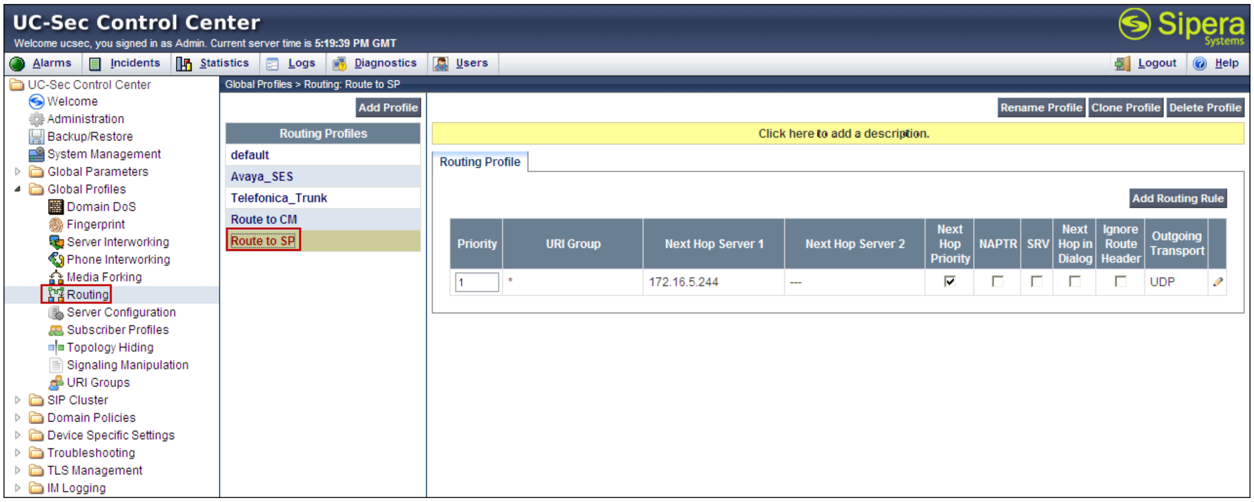
- Select **Add Profile** (not shown).
- Enter Profile Name: **Route to SP**
- Click **Next.**



- **Next Hop Server 1: 172.16.5.244** (service provider SIP Proxy IP address).
- Check **Routing Priority Based on Next Hop Server**.
- **Outgoing Transport: UDP**.
- Click **Finish**.



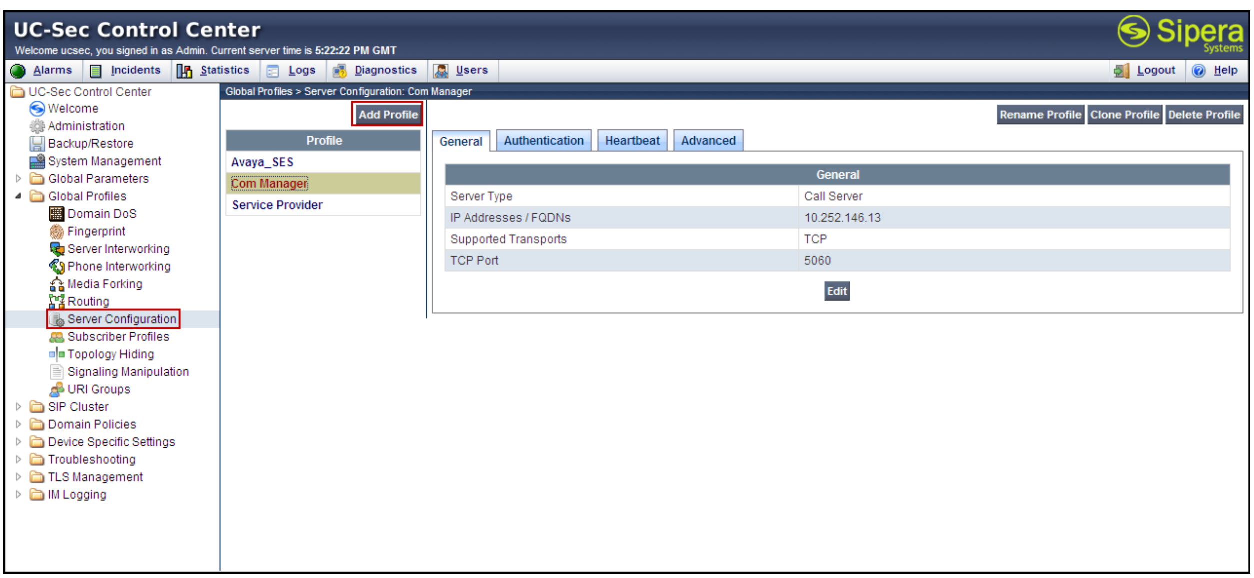
The following screen capture shows the added **Route to SP** Profile



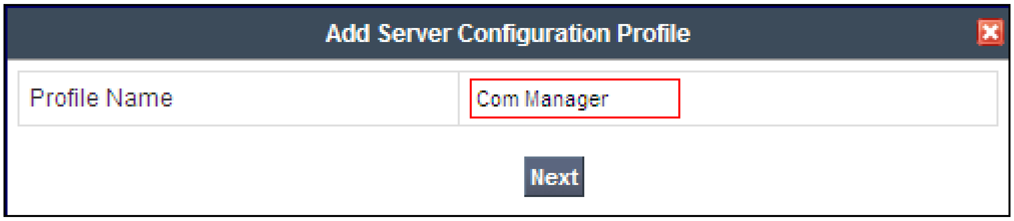
6.2.3. Server Configuration

Server Profiles should be created for the Avaya SBCE two peers, Avaya Aura® Communication Manager (Call Server) and the SIP Proxy at the service provider's network (Trunk Server).

To add the profile for the Call Server, from the **Global Profiles** menu, select **Server Configuration**. Click **Add Profile**.

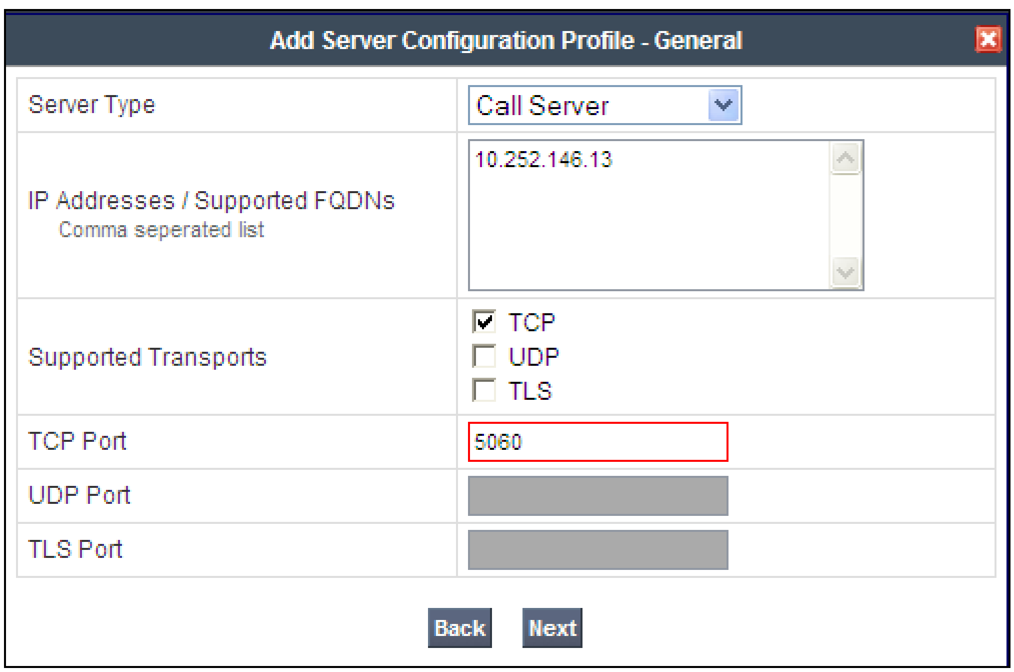


- Enter the profile name: **Com Manager**. Click **Next.**

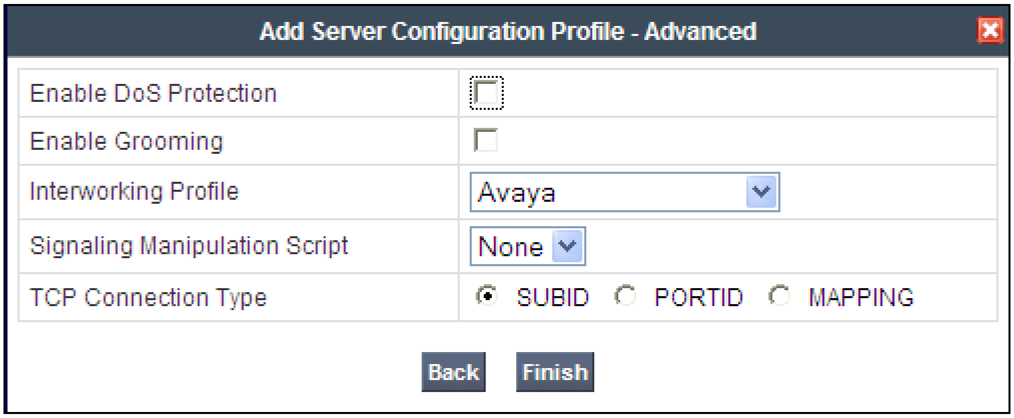


On the **Add Server Configuration Profile, General** Tab:

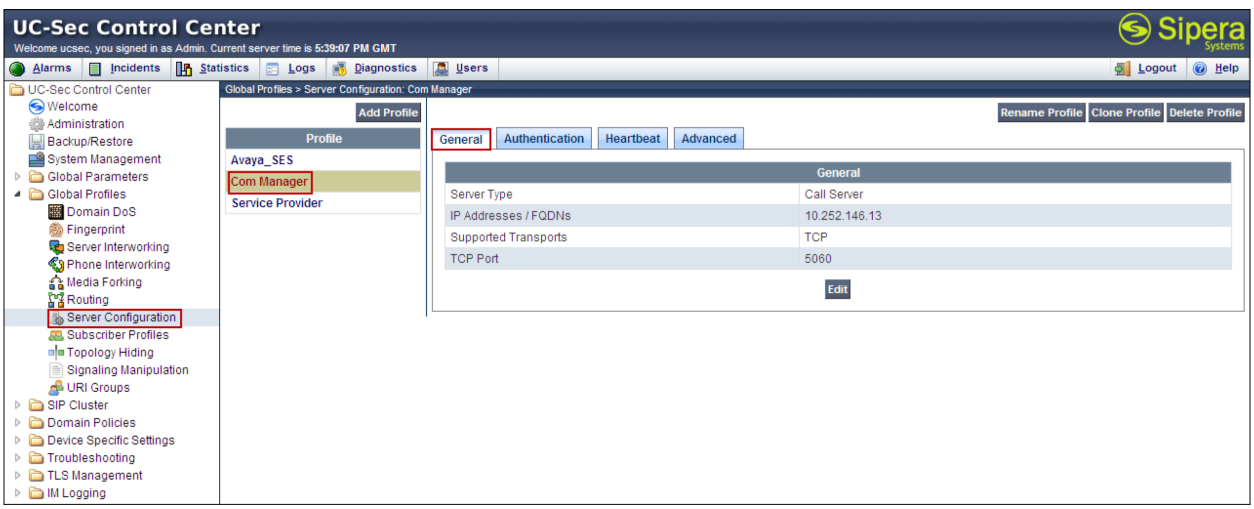
- Select **Server Type: Call Server**.
- **IP Address: 10.252.146.13** (IP Address of the **procr** interface in Avaya Aura® Communication Manager).
- **Supported Transports**: Check **TCP**. The protocol and port defined here must match the values used on the Avaya Aura® Communication Manager signaling group form in **Section 5.6**.
- **TCP Port: 5060**.
- Click **Next**.



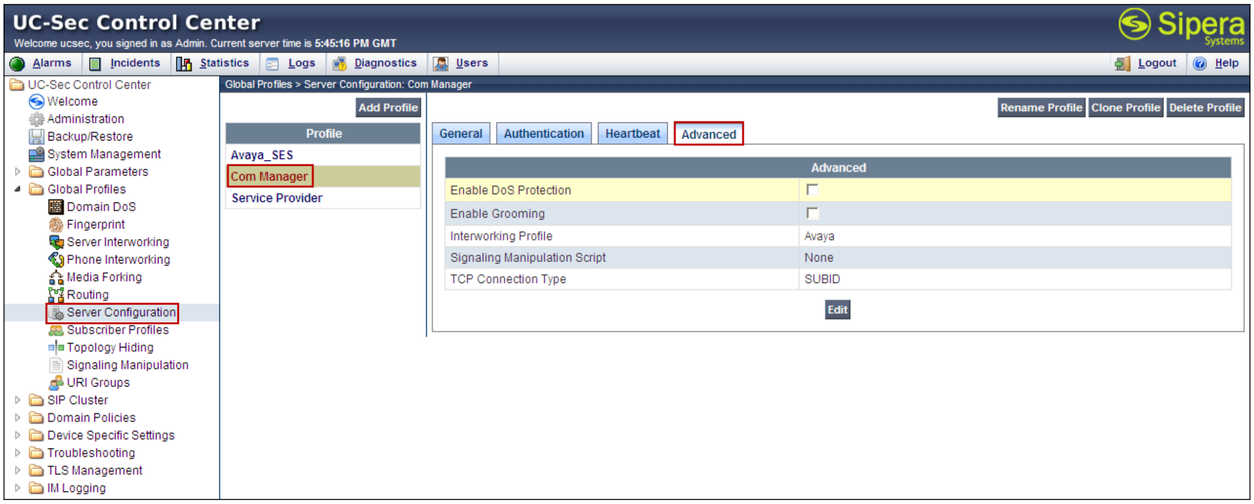
- Click **Next** on the **Authentication** tab (not shown).
- Click **Next** on the **Heartbeat** tab (not shown).
- On the **Advanced** tab, select **Avaya** from the **Interworking Profile** drop down menu.
- Click **Finish.**



The following screen capture shows the **General** tab of the added **Com Manager** Profile.

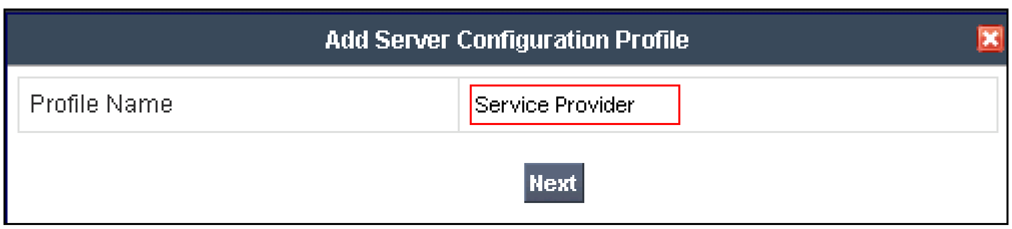


The following screen capture shows the **Advanced** tab of the added **Com Manager** Profile.



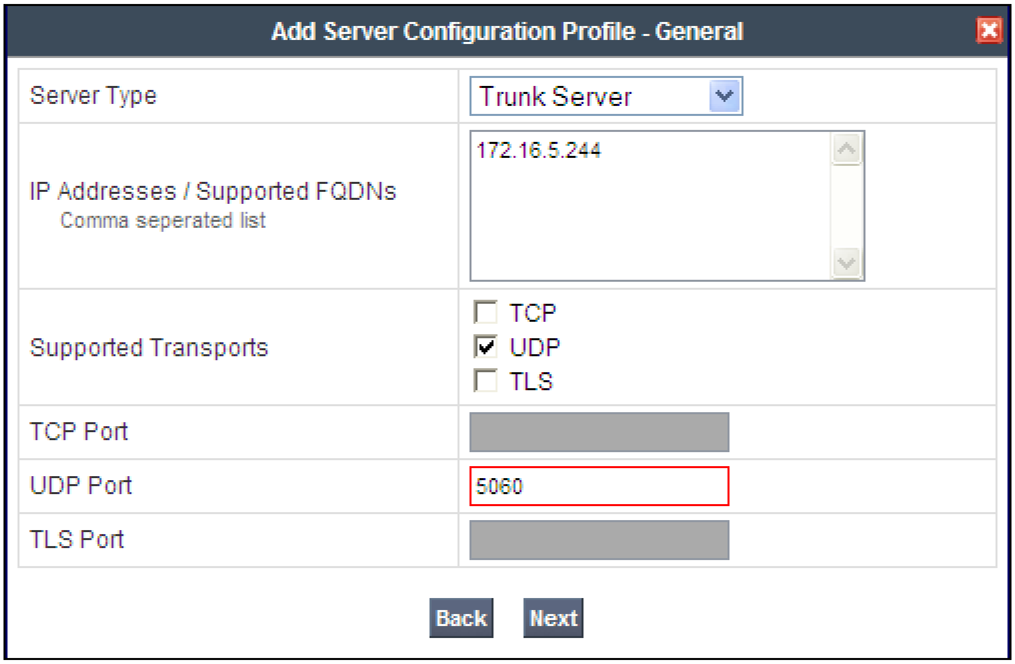
To add the profile for the Trunk Server, from the **Server Configuration** screen, click **Add Profile** (not shown).

- Enter the profile name: **Service Provider**. Click **Next.**

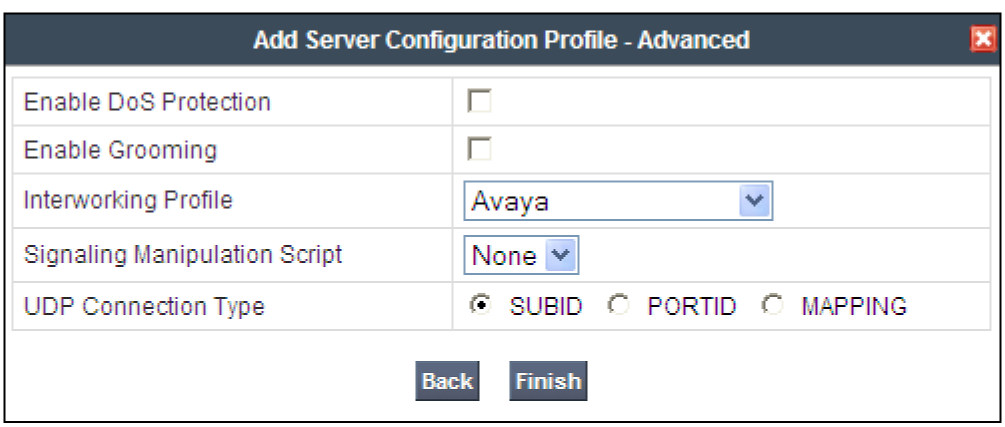


On the **Add Server Configuration Profile, General** Tab:

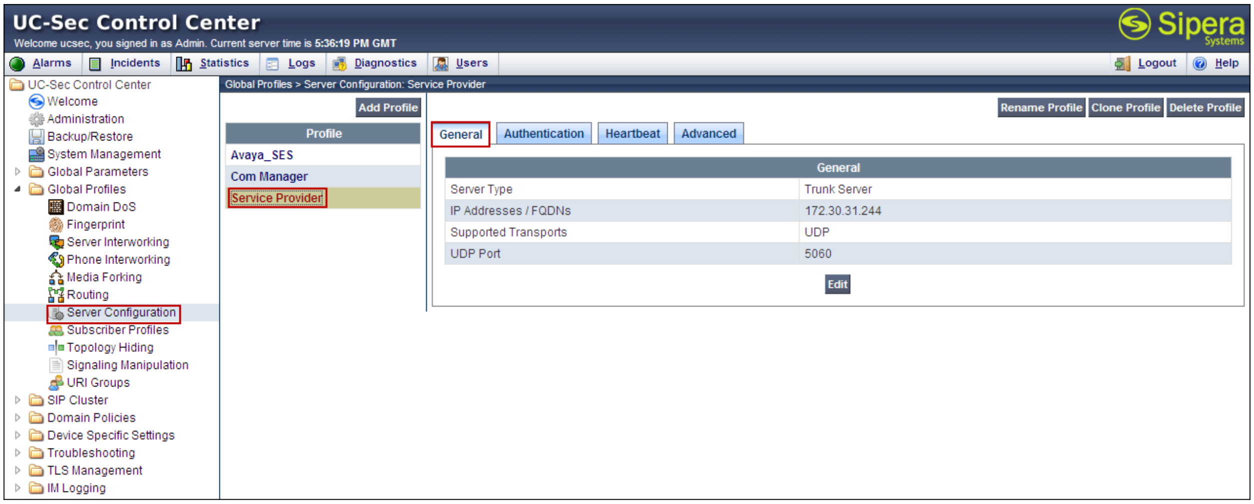
- Select **Server Type: Trunk Server**.
- **IP Address: 172.16.5.244** (service provider's SIP Proxy IP address).
- **Supported Transports**: Check **UDP**.
- **UDP Port: 5060**.
- Click **Next**.



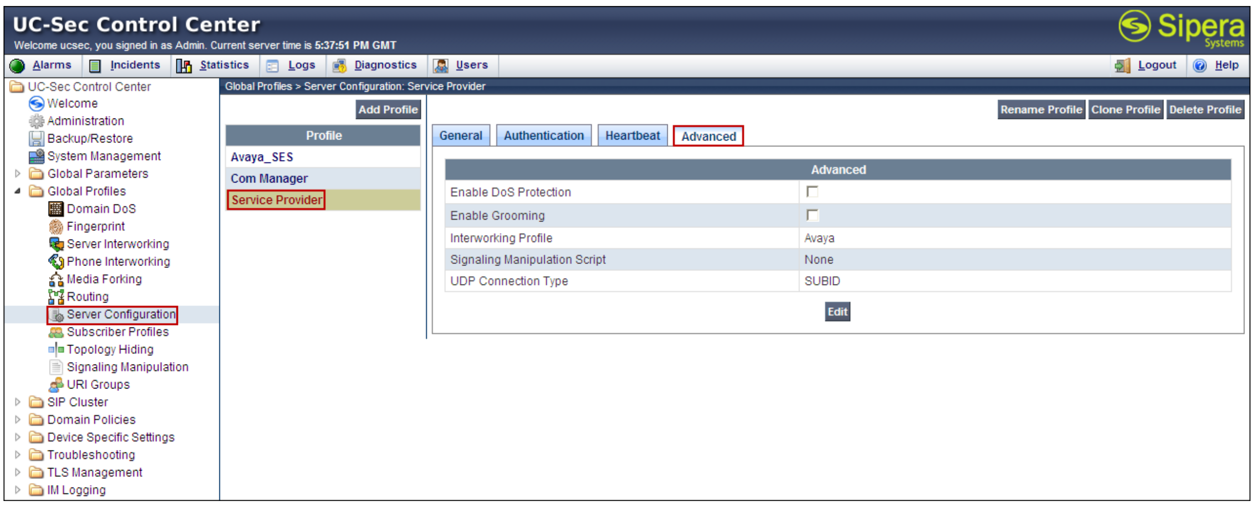
- Click **Next** on the **Authentication** tab (not shown).
- Click **Next** on the **Heartbeat** tab (not shown).
- On the **Advanced** tab, select **Avaya** from the **Interworking Profile** drop down menu. Leave other fields with their default values.
- Click **Finish.**



The following screen capture shows the **General** tab of the added **Service Provider** Profile.



The following screen capture shows the **Advanced** tab of the added **Service Provider** Profile.



6.2.4. Topology Hiding

Topology Hiding is a security feature which allows the manipulation of several parameters of the SIP packets, preventing private enterprise network information from being propagated to the untrusted public network.

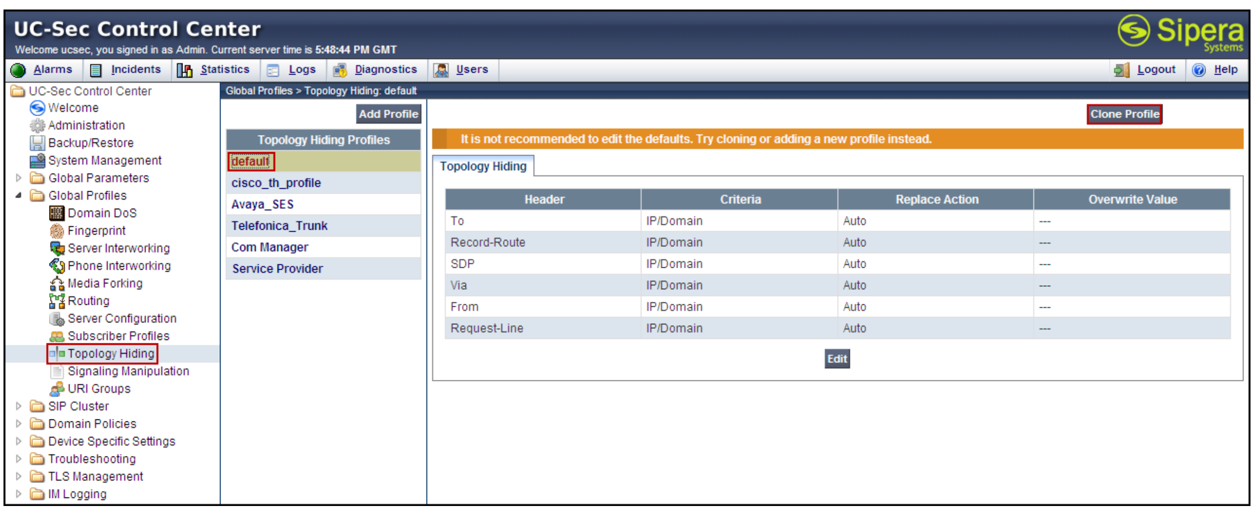
Topology Hiding can also be used as an interoperability tool to adapt the host portion in SIP headers such as To, From, Request-URI, Via, Record-Route and SDP to the IP addresses or domains expected by Avaya Aura® Communication Manager and the SIP trunk service provider, allowing the call to be accepted in each case.

For the compliance test, only the minimum configuration required to achieve interoperability on the SIP trunk was performed. Additional steps can be taken in this section to further mask the information that is sent from the enterprise to the public network.

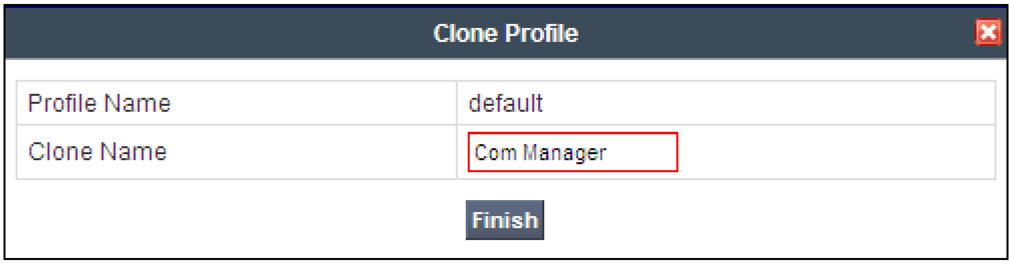
For the test configuration, default values of the Topology Hiding Profile were used in the enterprise and Service Provider directions. Since modifying a default profile is generally not recommended, the default was duplicated, or "cloned". That way if modifications are needed in the future, the default profile will not be affected by those changes.

To add the Topology Hiding Profile in the enterprise direction, select **Topology Hiding** from the **Global Profiles** menu on the left-hand side:

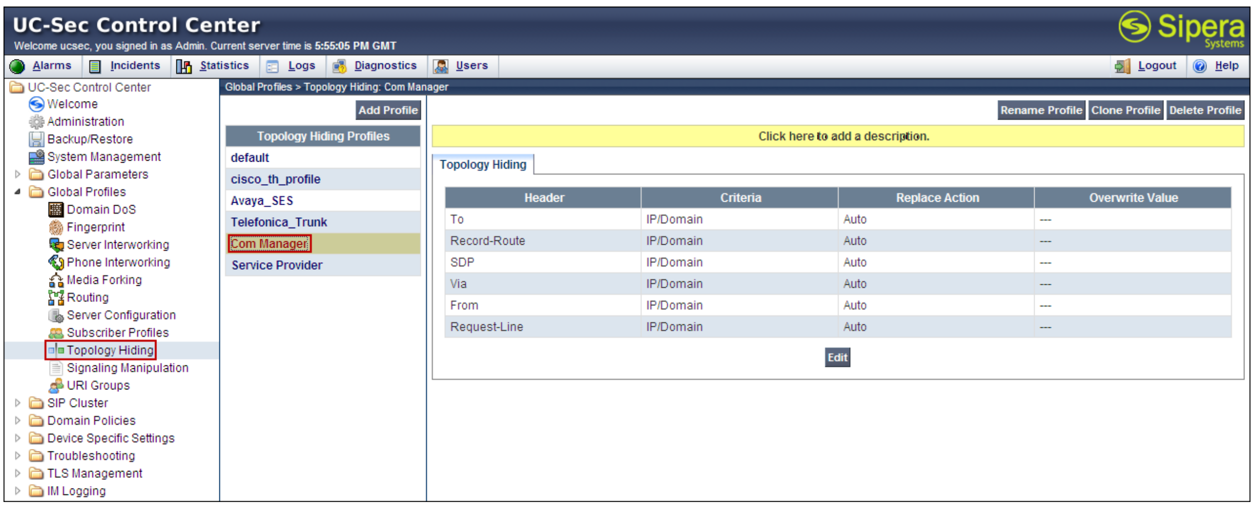
- Select **default** from the **Topology Hiding Profiles** list.
- Click **Clone Profile**.



- Enter the **Profile Name**: **Com Manager**.
- Click **Finish**.

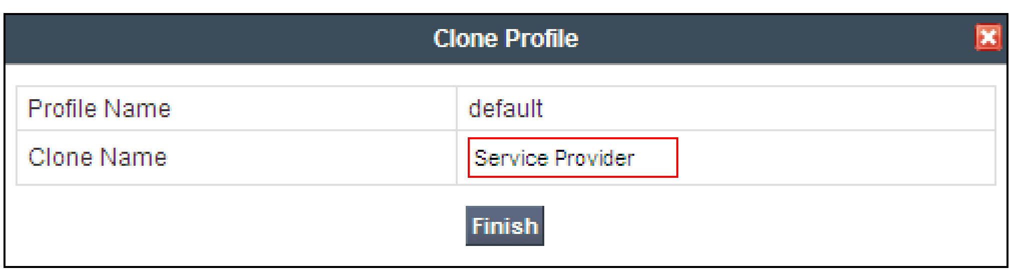


The following screen capture shows the added **Com Manager** Profile.

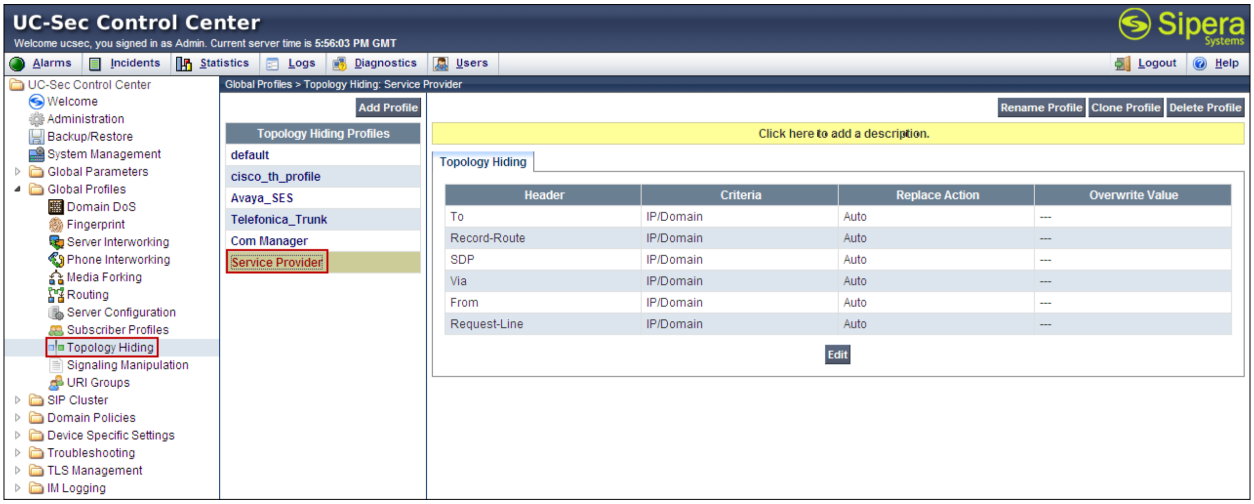


To add the Topology Hiding Profile in the Service Provider direction, select **Topology Hiding** from the **Global Profiles** menu on the left-hand side (not shown):

- Select **default** from the **Topology Hiding Profiles** list (not shown).
- Click **Clone Profile** (not shown).
- Enter the **Profile Name**: **Service Provider**. Click **Finish**.



The following screen capture shows the added **Service Provider** Profile.

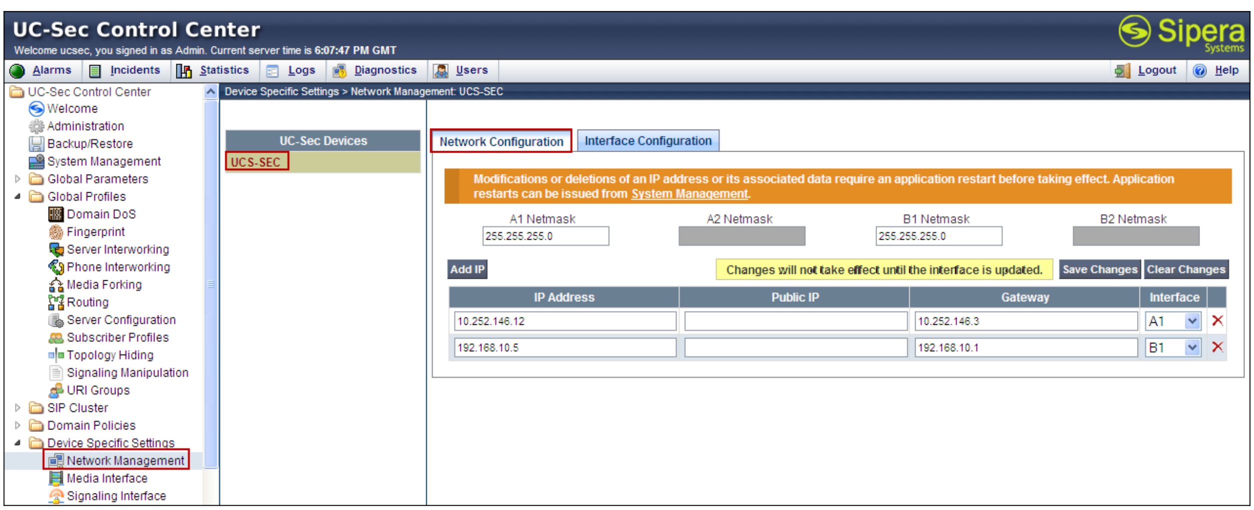


6.3. Device Specific Settings

The **Device Specific Settings** allow the management of various device-specific parameters, which determine how a particular device will function when deployed in the network. Specific server parameters, like network and interface settings, as well as call flows, etc. are defined here.

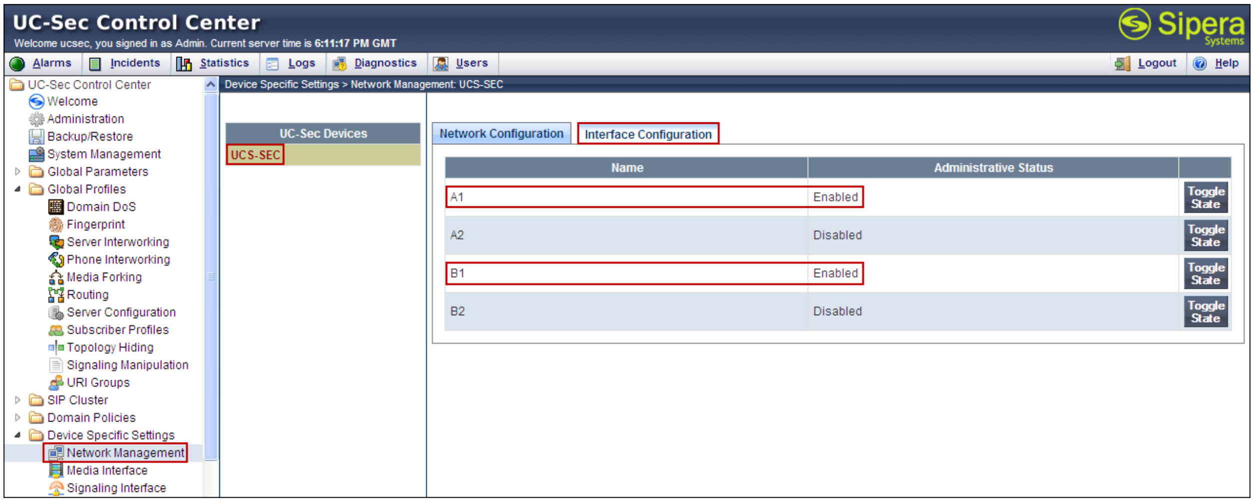
6.3.1. Network Management

The Network Management configuration should have been previously completed during the first part or when the initial configuration was done via the Provisioning Script, which requires a serial connection between a terminal device and the Console port of the Avaya SBCE. To verify the network configuration, from the **Device Specific Settings** menu on the left hand side, select **Network Management**. Select the **Network Configuration** tab.



In the event that changes need to be made to the network configuration information, they could be entered here.

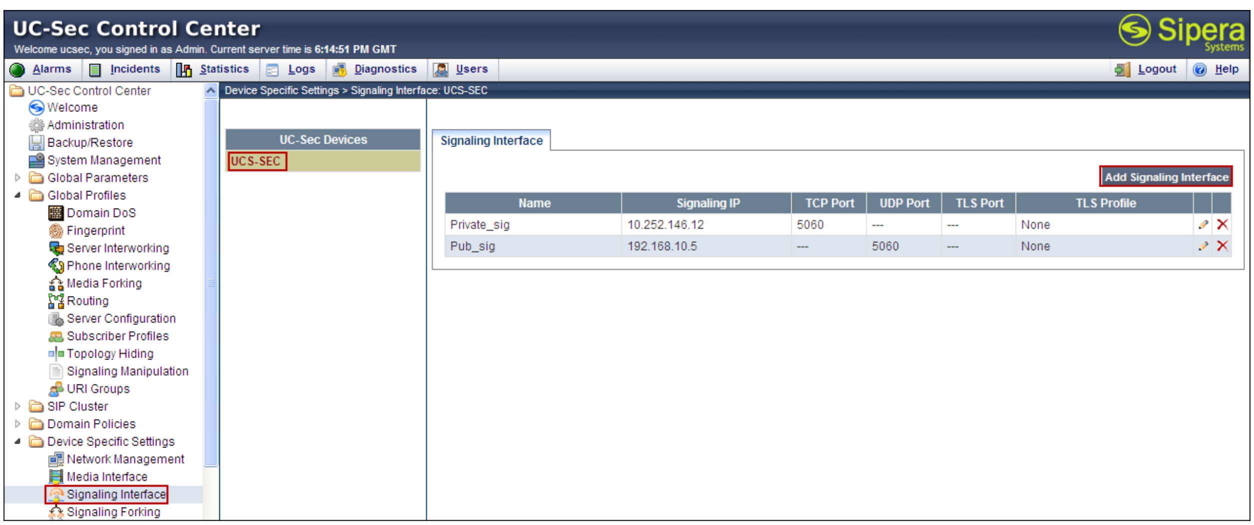
On the **Interface Configuration** tab, click the **Toggle State** control for interfaces **A1** and **B1** to change the status to **Enabled**. It should be noted that the default state for all interfaces is **Disabled**, so it is very important to perform this step, or the Avaya SBCE will not be able to communicate on any of its interfaces.



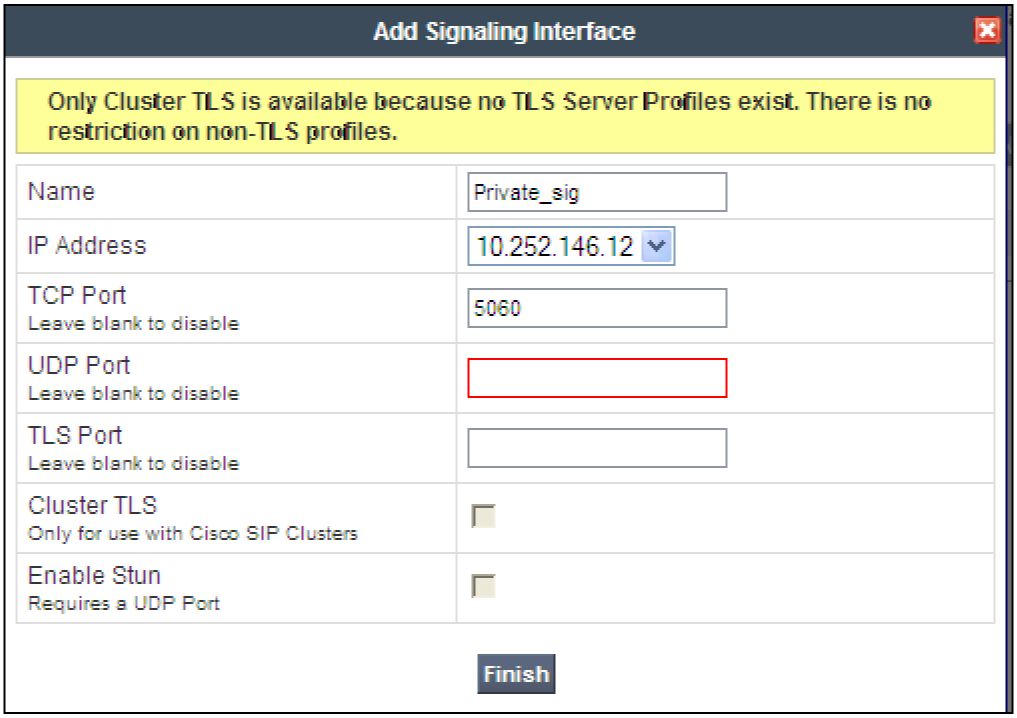
6.3.2. Signaling Interface

Signaling Interfaces need to be created for both the private and public network interfaces.

To create the Signaling Interface toward Avaya Aura® Communication Manager, from the **Device Specific Settings** menu on the left hand side, select **Signaling Interface**, then **Add Signaling Interface**:

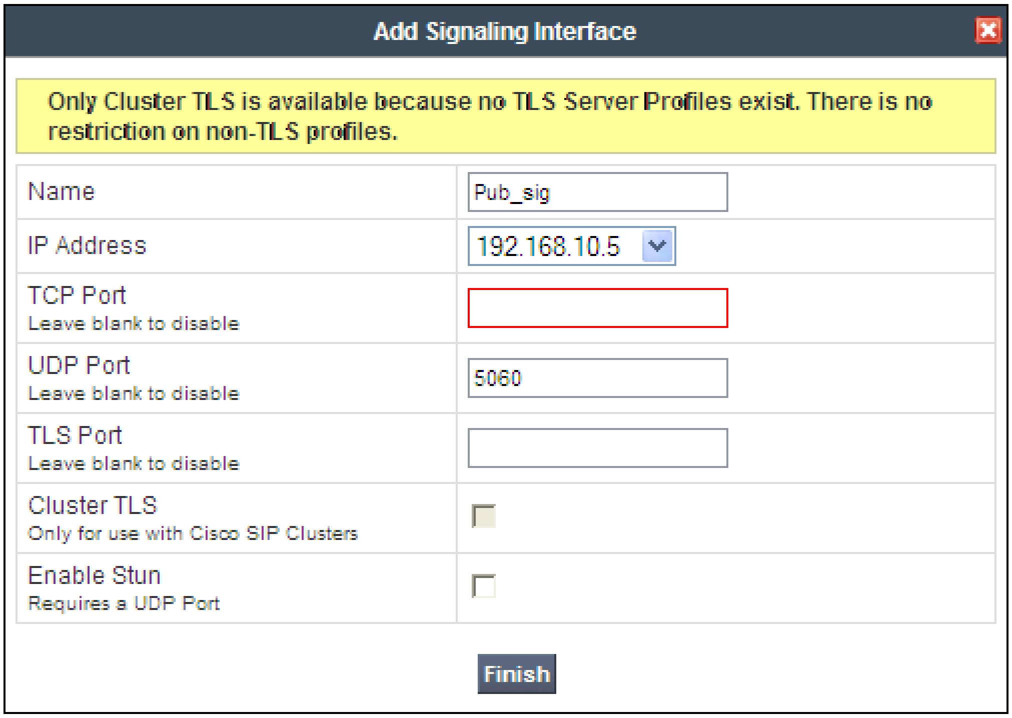


- **Name: Private_sig**.
- **IP Address: 10.252.146.12** (inside IP address of the Avaya SBCE).
- **TCP Port: 5060.** The Avaya SBCE will listen for SIP requests on the port specified here. The protocol and port defined in this screen must match the values used on the Avaya Aura® Communication Manager signaling group form in **Section 5.6**.
- Click **Finish**.

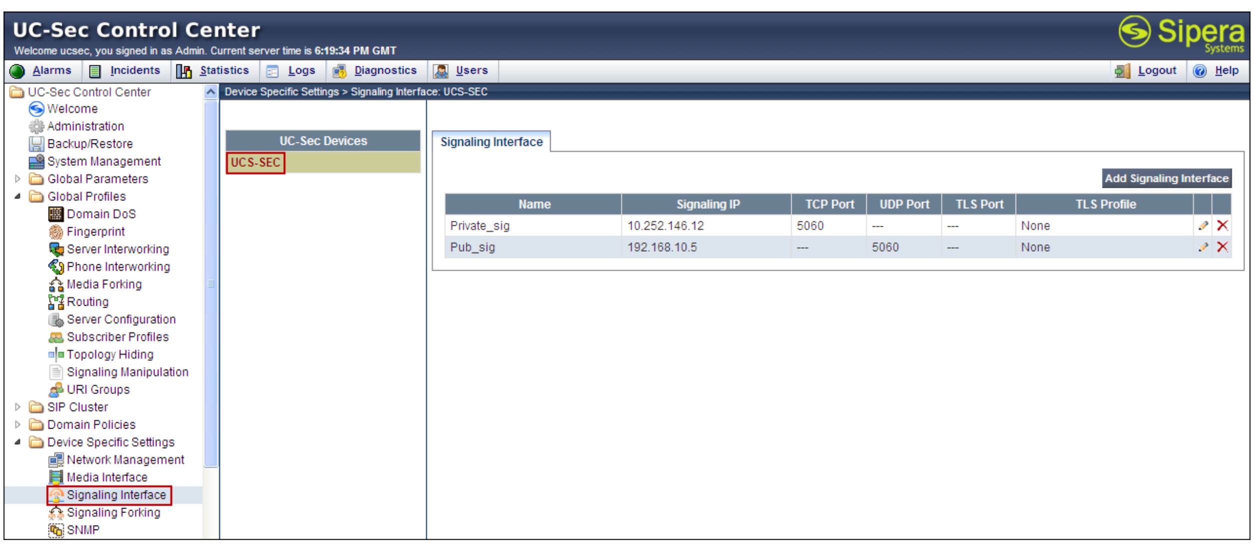


Similarly, to add the Signaling Interface toward Telefonica SIP Trunk:

- Click **Add Signaling Interface** (not shown):
- **Name: Pub_sig**.
- **IP Address: 192.168.10.5 (**Outside IP Address of the Avaya SBCE).
- **UDP Port: 5060**.
- Click **Finish**.



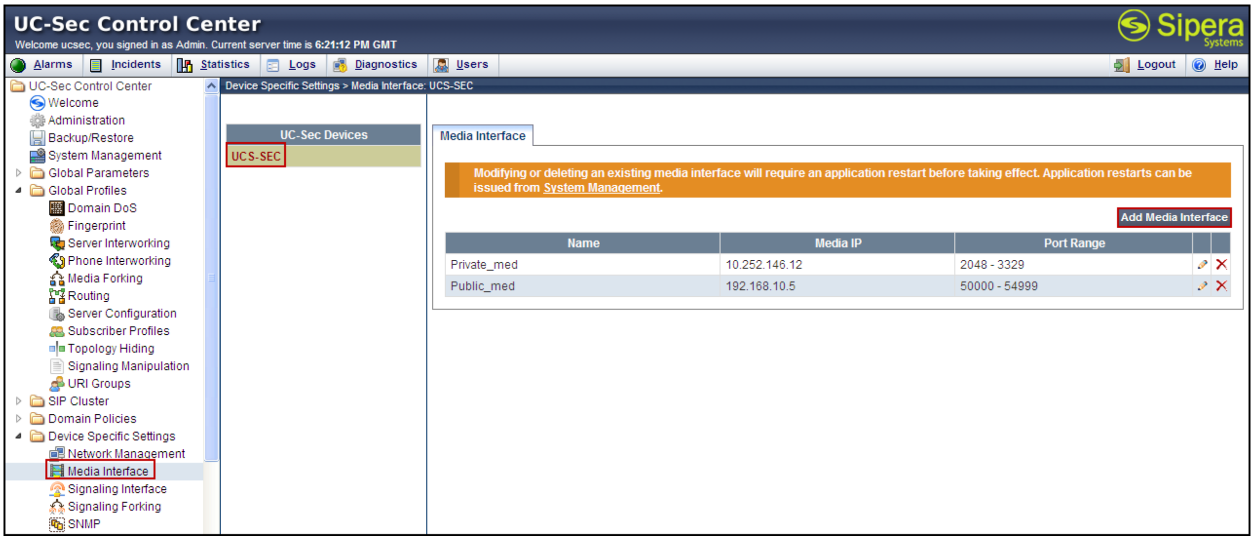
The following screen capture shows the added **Signaling Interface**s.



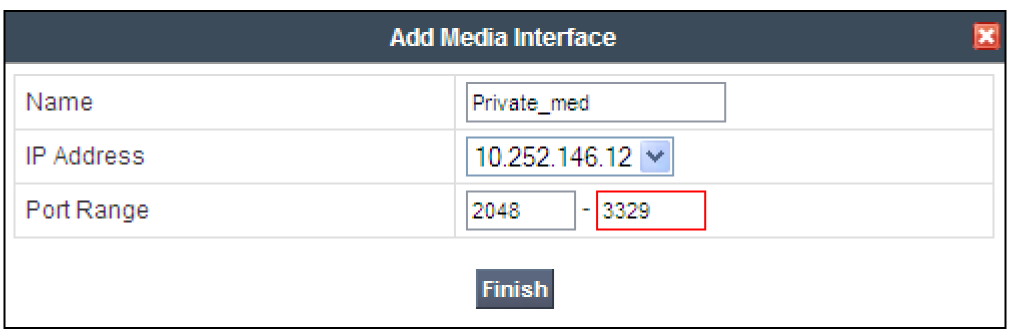
6.3.3. Media Interface

Media Interfaces were created to specify the port range in which the Avaya SBCE will accept media streams on each interface. Packets leaving the interfaces of the Avaya SBCE will advertise one of the ports in this range as the listening port in which it will accept media from the Call Server or Trunk Server. The Private interface was made to match the range specified in the IP-Network-Region in Avaya Aura® Communication Manager of 2048 to 3349, and the Public interface to match the range specified by Telefonica for the compliance test of 50000 to 54999.

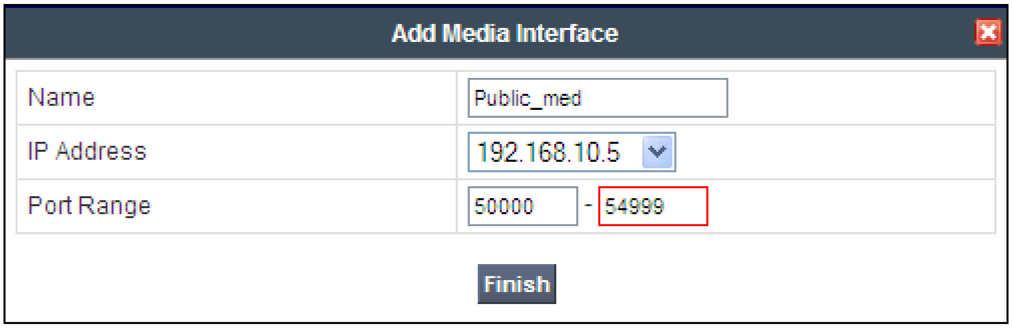
From the **Device Specific Settings** menu on the left-hand side, select **Media Interface,** then Select **Add Media Interface.**



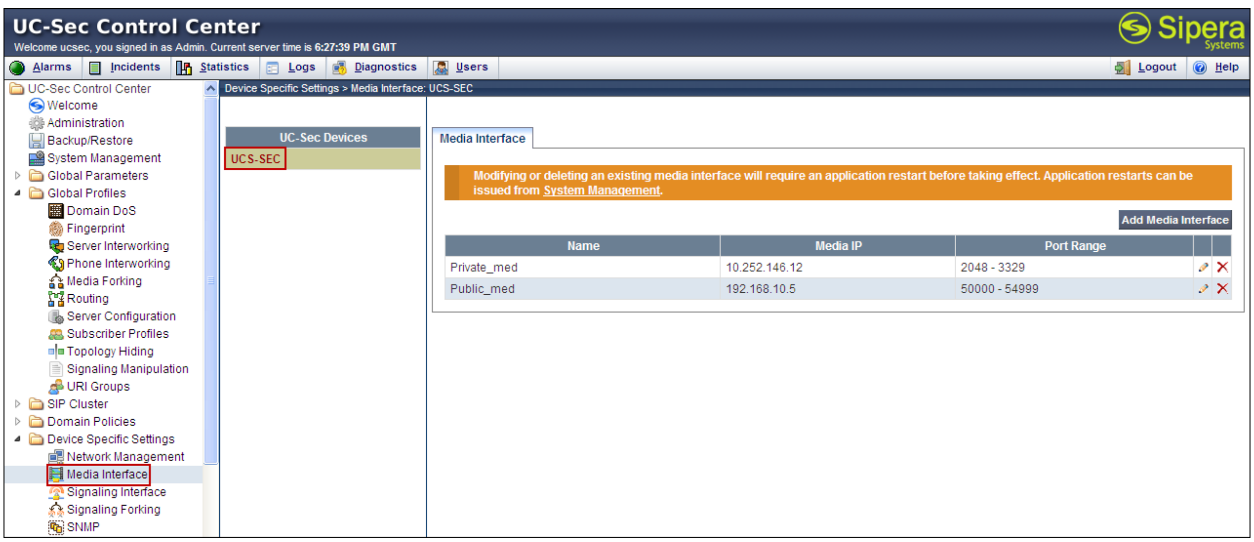
- **Name: Private_med**.
- **IP Address: 10.252.146.12** (Inside IP Address of the Avaya SBCE) .
- **Port Range: 2048-3329**.
- Click **Finish**.



- Select **Add Media Interface** (not shown).
- **Name: Public_med**.
- **IP Address: 192.168.10.5** (Outside IP Address of the SBC, toward Telefonica).
- **Port Range: 50000-54999**.
- Click **Finish.**



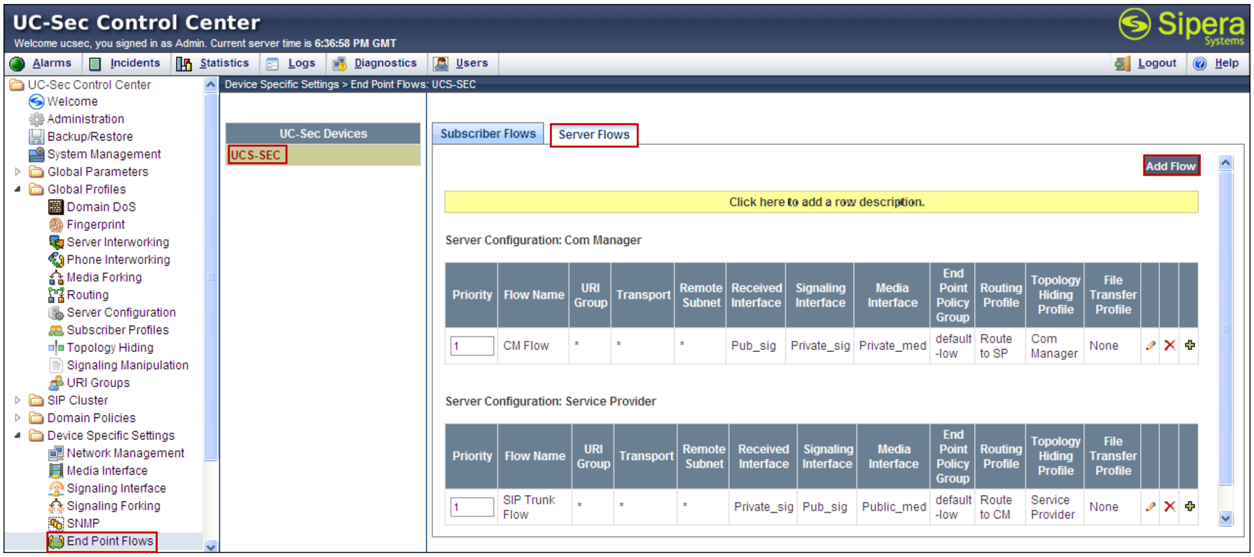
The following screen capture shows the added **Media Interfaces**.



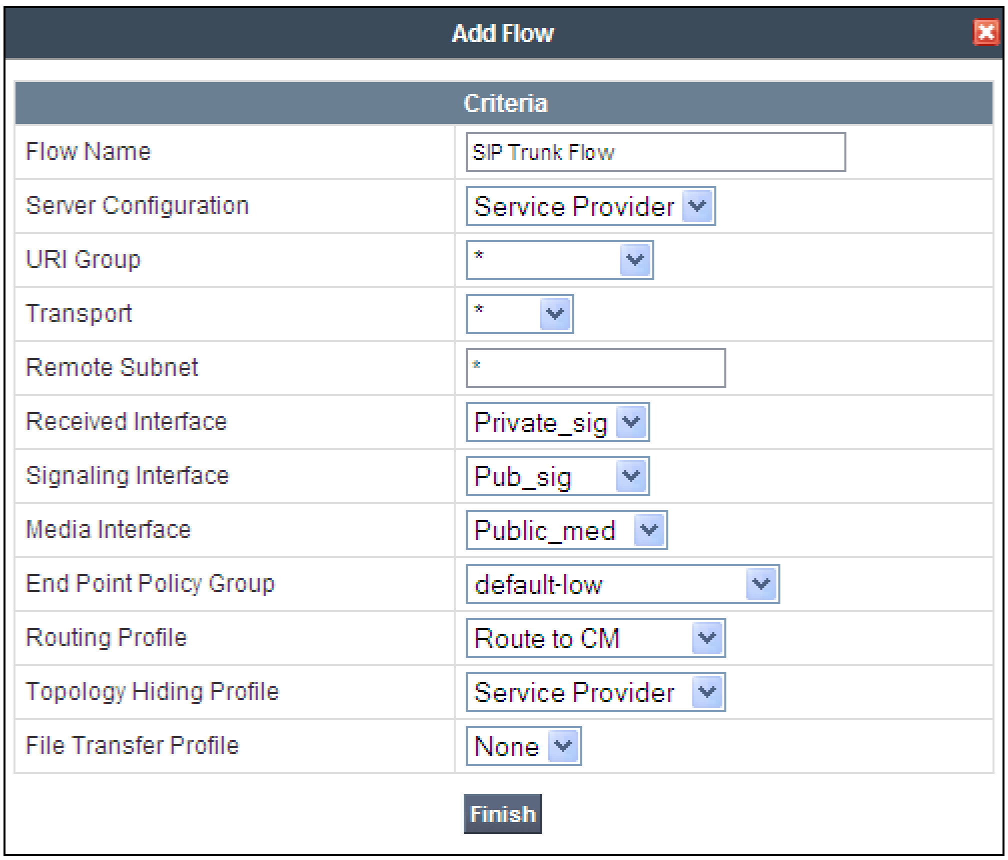
6.3.4. End Point Flows

End Point Flows determine the path to be followed by the packets traversing through the Avaya SBCE. They also combine the different sets of rules, profiles, etc. previously configured, to be applied to the packets traveling in each direction.

To create the call flow toward Telefonica SIP trunk, from the **Device Specific Settings** menu, select **End Point Flows**, then select the **Server Flows** tab. Click **Add Flow**.

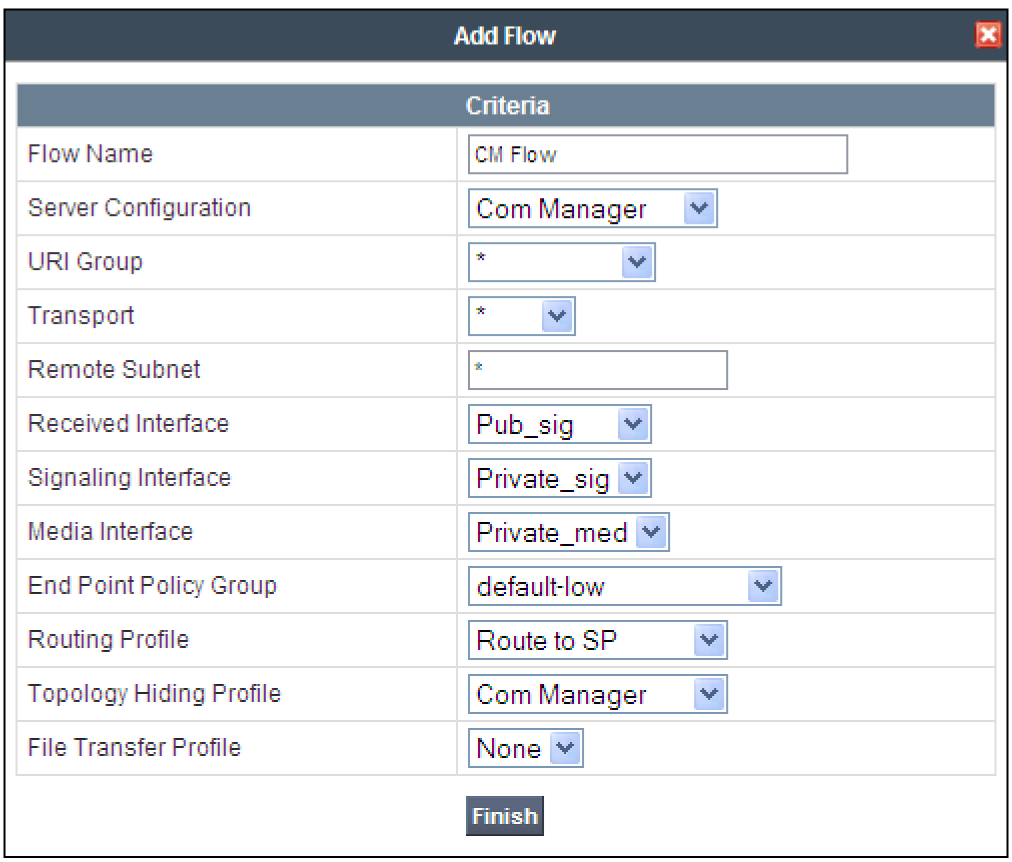


- **Name: SIP Trunk Flow**.
- **Server Configuration**: **Service Provider**.
- **URI Group: ***
- **Transport: ***
- **Remote Subnet: ***
- **Received Interface**: **Private_sig**.
- **Signaling Interface: Pub_sig**.
- **Media Interface**: **Public_med**.
- **End Point Policy: default-low**.
- **Routing Profile: Route to CM** (Note that this is the reverse route of the flow).
- **Topology Hiding Profile: Service Provider**.
- **File Transfer Profile: None**.
- Click **Finish.**

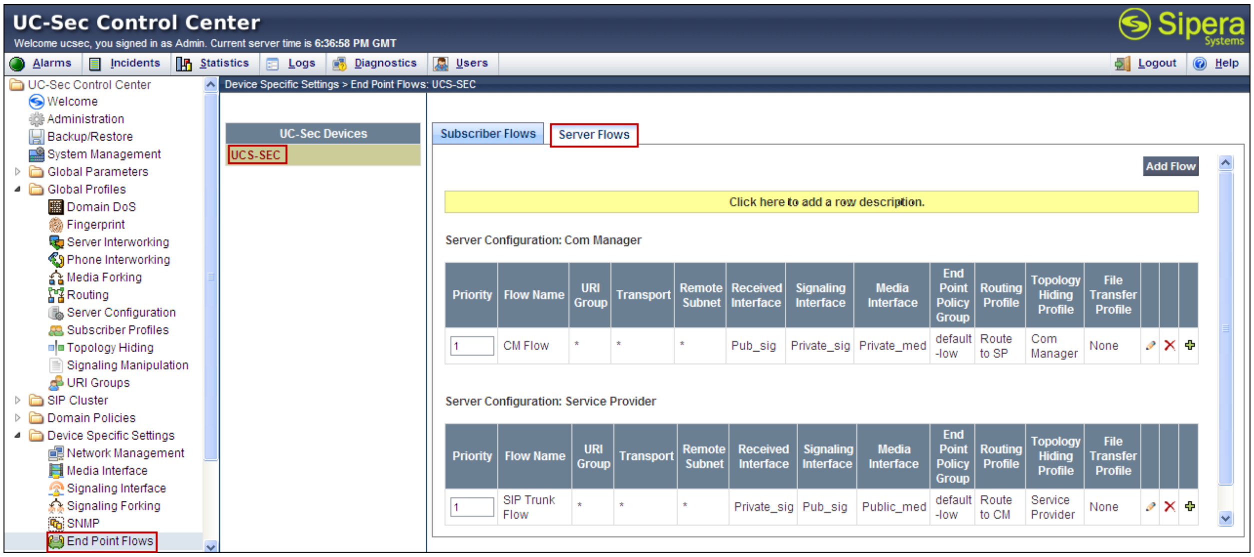


To create the call flow toward Avaya Aura® Communication Manager, click **Add Flow** (not shown).

- **Name: CM Flow**.
- **Server Configuration**: **Com Manager**.
- **URI Group: ***
- **Transport: ***
- **Remote Subnet: ***
- **Received Interface**: **Pub_sig**.
- **Signaling Interface: Private_sig**.
- **Media Interface**: **Private_med**.
- **End Point Policy Group: default-low**.
- **Routing Profile: Route to SP** (Note that this is the reverse route of the flow).
- **Topology Hiding Profile: Com Manager**.
- **File Transfer Profile: None**.
- Click **Finish**.



The following screen capture shows the added **End Point Flows.**



7. Telefonica SIP Trunk Service Configuration

To use Telefonica SIP Trunking, a customer must request the service from Telefonica using their sales processes. The process can be started by contacting Telefonica via the corporate web site at http://www.movistar.com.pe/negocios and requesting information via the online sales links or telephone numbers.

During the signup process, Telefonica will require that the customer provide the public IP address used to reach the Avaya SBCE at the edge of the enterprise. Telefonica will provide the IP address of the SIP proxy/SBC, Direct Inward Dialed (DID) numbers assigned to the enterprise, supported audio codec's, signaling port and media port range. This information is used to complete the Avaya Aura® Communication Manager, and the Avaya Session Border Controller for Enterprise configuration discussed in the previous sections.

The configuration between Telefonica and the enterprise is a static configuration. There is no registration of the SIP trunk to Telefonica network.

8. Verification and Troubleshooting

This section provides verification steps that may be performed in the field to verify that the solution is configured properly. This section also provides a list of useful troubleshooting commands 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. Avaya Aura® Communication Manager:
   - **list trace station** <extension number>
     Traces calls to and from a specific station.
   - **list trace tac** <trunk access code number>
     Trace calls over a specific trunk group.
   - **status signaling-group** <signaling group number>
     Displays signaling group service state.
   - **status trunk** <trunk group number>
     Display trunk group service state.
   - **status station** <extension number>
     Displays signaling and media information for an active call on a specific station.

2. Avaya SBCE:
   There are several links and menus located on the taskbar in the UC-Sec Control Center that can provide useful diagnostic or troubleshooting information:
   - **Alarms**. Provides information about the health of the SBC.
   - **Incidents.** Provides detailed reports of anomalies, errors, policies violations, etc.
   - **Diagnostics.** This screen provides a variety of tools to aid in troubleshooting the Avaya SBCE network connectivity and its operation.

   Other useful tools can also be found on the **Troubleshooting Menu,** on the left hand side of the **UC-Sec Control Center** page.
   - **Packet Capture**. Allows Avaya SBC to capture the packets in any of the Avaya SBCE interfaces, and save them as *pcap* files. From the menu on the left hand side, click **Troubleshooting → Trace Settings → Packet Capture** tab.

9. Conclusion

Telefonica del Peru SIP Trunk Service passed compliance testing. Interoperability testing was completed with successful results with the observations/limitations described in **Section 2.2.**

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 6.2.2, December 2012.
[2] *Administering Avaya Aura® Communication Manager*, Release 6.2, Issue 7.0, December 2012, Document Number 03-300509.
[3] *Avaya Aura® Communication Manager Feature Description and Implementation*, Release 6.2, Issue 9.0, December 2012, Document Number 555-245-205.
[4] *Sipera Systems E-SBC 1U Installation Guide*, Release 4.0.5.November 2011.
[5] *Sipera Systems E-SBC Administration Guide*, Release 4.0.5. November 2011.
[6] *Sipera Systems E-SBC Release Notes*, Release 4.0.5.Q02. November 2011.
[7] *Avaya one-X® Deskphone H.323 Administrator Guide*, Release 6.1, May 2011, Document Number 16-300698.
[8] *Administering Avaya one-X® Communicator*, October 2011.
[9] *Using Avaya one-X® Communicator*, Release 6.1, October 2011.
[10] *RFC 3261 SIP*: Session Initiation Protocol, http://www.ietf.org/.
[11] *RFC 2833 RTP Payload for DTMF Digits*, Telephony Tones and Telephony Signals, http://www.ietf.org/
[12] Recommendation ITU-T T-38. Procedures for real-time Group 3 facsimile communication over IP networks. September 2010.

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.