Avaya Solution & Interoperability Test Lab

Application Notes for Avaya Aura® Communication Manager 6.2, Avaya Aura® Session Manager 6.2, and Avaya Session Border Controller for Enterprise with Verizon Business IP Trunk SIP Trunk Service – Issue 1.0

Abstract

These Application Notes illustrate a sample configuration using Avaya Aura® Session Manager Release 6.2 and Avaya Aura® Communication Manager Release 6.2 with the Verizon Business Private IP (PIP) IP Trunk service. These Application Notes update previously published Application Notes with newer versions of Communication Manager and Session Manager. The Verizon Business SIP trunk redundant architecture (2-CPE) is supported by dual Avaya Session Border Controllers for Enterprise.

The Verizon Business IP Trunk service offer referenced within these Application Notes is designed for business customers with an Avaya SIP trunk solution. The service provides local and/or long distance PSTN calling via standards-based SIP trunks directly, without the need for additional TDM enterprise gateways or TDM cards and the associated maintenance costs.

The configuration and software versions described in these Application Notes have not yet been independently certified by Verizon labs. These Application Notes can be used to facilitate customer engagements via the Verizon field trial process, pending Verizon labs independent certification.

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., utilizing a Verizon Business Private IP (PIP) circuit connection to the production Verizon Business IP Trunking service.

NOTE: This Application Note is applicable with Avaya Aura® 6.2 which is currently in Controlled Introduction. Avaya Aura® 6.2 will be Generally Available in Summer 2012.

Table of Contents

1. Introduction

These Application Notes illustrate a sample configuration using Avaya Aura® Session Manager Release 6.2 and Avaya Aura® Communication Manager Release 6.2 with the Verizon Business Private IP (PIP) IP Trunk service. The Verizon Business IP Trunk service provides local and/or long-distance calls (with PSTN endpoints) via standards-based SIP trunks. These Application Notes update previously published Application Notes with newer versions of Communication Manager and Session Manager. The Verizon Business SIP trunk redundant architecture (2-CPE) is supported by dual Avaya Session Border Controllers for Enterprise (ASBCE). The Verizon Business SIP Trunk redundant (2-CPE) architecture provides for redundant SIP trunk access between the Verizon Business IP Trunk service offer and the customer premises equipment (CPE).

Dual ASBCEs are used as edge devices between the Avaya CPE and the Verizon Business network, and provide for Verizon Business 2-CPE redundancy. In addition, the ASBCEs provide Network Address Translation (NAT) functionality to convert the addresses used within the enterprise to the Verizon routable addresses.

Note - The Verizon Business SIP Trunk Redundant (2-CPE) architecture is a service option and its use is not a requirement of the Verizon Business IP Trunk service offer.

Verizon Business and Avaya developed the SIP Trunk Redundant (2-CPE) architecture to ensure that SIP trunk calls can be automatically re-routed to bypass SIP trunk failures due to network or component outages. The 2-CPE architecture described in these Application Notes is based on a customer location having two ASBCEs. One ASBCE is designated as Primary and one as Secondary.

Avaya Aura® Session Manager is provisioned for fail-over of outbound calls from one ASBCE to the other, if there is a failure (e.g., timeout, or error response) associated with the first choice. Similarly, the Verizon Business Private IP Trunk service node will send inbound calls to the Primary Avaya ASBCE if there is a failure (e.g., timeout, or error response), then the call will be sent to the Secondary ASBCE.

The configuration and software versions described in these Application Notes have not yet been independently certified by Verizon labs. These Application Notes can be used to facilitate customer engagements via the Verizon field trial process, pending Verizon labs independent certification.

2. General Test Approach and Test Results

2.1. Interoperability Compliance Testing

Compliance testing scenarios for the configuration described in these Application Notes included the following:

- Inbound and outbound voice calls between telephones controlled by Avaya Aura® Communication Manager and the PSTN can be made using G.711MU or G.729A codecs.
- Direct IP-to-IP Media (also known as “Shuffling”) when applicable.
- DTMF using RFC 2833
  - Outbound call to PSTN application requiring post-answer DTMF (e.g., an IVR or voice mail system)
  - Inbound call from PSTN to Avaya CPE application requiring post-answer DTMF (e.g., Avaya Modular Messaging, Avaya vector digit collection steps)
- Additional PSTN numbering plans (e.g., International, operator assist, 411)
- Hold / Retrieve with music on hold
- Call transfer using two approaches
  - REFER approach (Communication Manager Network Call Redirection flag on trunk group form set to “y”)
  - INVITE approach (Communication Manager Network Call Redirection flag on trunk group form set to “n”)
- Conference calls
- SIP Diversion Header for call redirection
  - Call Forwarding
  - EC500
- Long hold time calls
- Automatic fail-over testing associated with the 2-CPE redundancy (i.e., calls automatically re-routed around component outages).

2.2. Test Results

- When using an Avaya SIP phone with G.711 as the preferred codec and a call is established as G.711, when a re-invite is issued by Communication Manager for a shuffle, Verizon sends an ACK with just G.729 listed, so the SIP Phone will switch codecs to G.729. The user experience will not be affected and the calls stays connected.

- When a PSTN caller is transferred off-net (to another PSTN user) the 2nd PSTN phone will see the Caller-ID of the CPE phone.

- 2 – CPE testing. Although the Sipera will proxy OPTIONS messages from inside the network to outside, sourcing of OPTIONS must be turned on if a 2-CPE configuration is used or failover will not occur properly.

2.3. The SIP Trunk Redundant (2-CPE) Architecture Option

Verizon Business and Avaya developed the SIP Trunk Redundant (2-CPE) architecture to ensure that SIP trunk calls can be automatically rerouted to bypass SIP trunk failures due to network or component outages. The 2-CPE architecture described in these Application Notes is based on a customer location having two Avaya Session Border Controllers for Enterprise. One ASBCE is designated as Primary and one as Secondary. The ASBCEs reside at the edge of the customer network.

Avaya Aura® Session Manager is provisioned to attempt outbound calls to the Primary ASBCE first. If that attempt fails, the Secondary ASBCE is used. Similarly, the Verizon Business Private IP Trunk service node will send inbound calls to the Primary ASBCE. If there is no response then the call will be sent to the Secondary ASBCE.

2.4. Support

2.4.1 Avaya

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

2.4.2 Verizon

For technical support on Verizon Business IP Trunk service offer, visit online support at http://www.verizonbusiness.com/us/customer/

2.5. Known Limitations

The following limitations are noted for the sample configuration described in these Application Notes:

- Emergency 911/E911 Services Limitations and Restrictions - Although Verizon provides 911/E911 calling capabilities, 911 capabilities were not tested, therefore, it is Customer's responsibility to ensure proper operation with its equipment/software vendor.
- Verizon Business IP Trunking service does not support G.711a codec for domestic service (EMEA only).
- Verizon Business IP Trunking service does not support G.729B codec.

> **Note** – These Application Notes describe the provisioning used for the sample configuration shown in **Figure 1**. Other configurations may require modifications to the provisioning described in this document.

3. Reference Configuration

Figure 1 illustrates the sample configuration used for the testing. The Avaya CPE location simulates a customer site. The PIP service defines a secure MPLS connection between the Avaya CPE T1 connection and the Verizon service node.

The ASBCEs receive traffic from the Verizon Business IP Trunk service on port 5060 and send traffic to the Verizon Business IP trunk service on port 5071, using UDP protocol for network transport (required by the Verizon Business IP Trunk service). The Verizon Business IP Trunk service provided 10 digits Direct Inward Dial (DID) numbers. These DID numbers can be mapped by Avaya Aura® Session Manager or Avaya Aura® Communication Manager to Avaya telephone extensions.

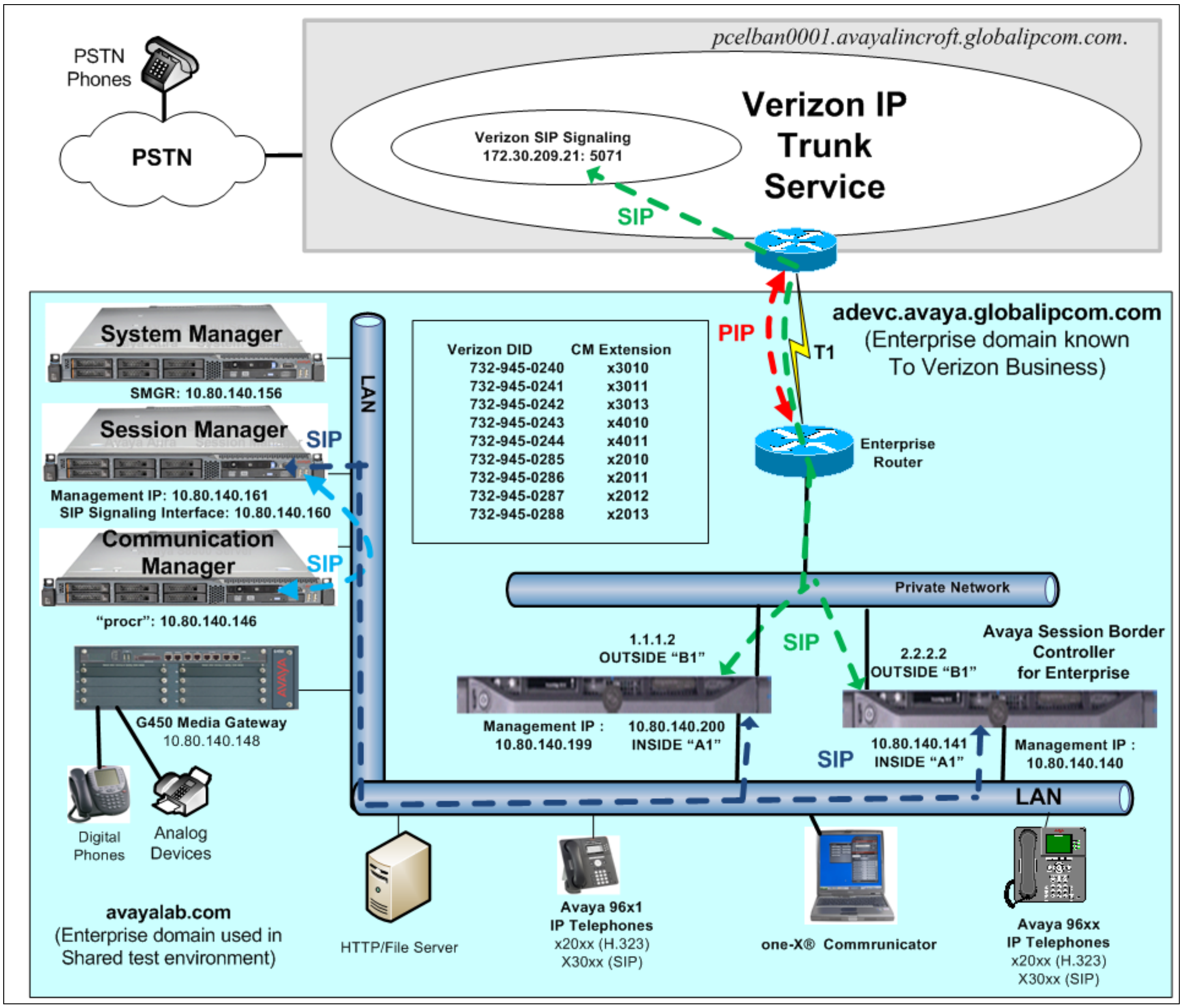


Figure 1: Avaya Interoperability Test Lab Configuration

The Verizon Business IP Trunk service used FQDN *pcelban0001.avayalincroft.globalipcom.com*. The Avaya CPE environment was known to Verizon Business IP Trunk service as FQDN *adevc.avaya.globalipcom.com*. Access to the Verizon Business IP Trunk service was added to a configuration that already used domain “avayalab.com” at the enterprise. As such, Session Manager or the ASBCE are used to adapt the “avayalab.com” domain to the domain known to Verizon. These Application Notes indicate a configuration that would not be required in cases where the CPE domain in Communication Manager and Session Manager match the CPE domain known to the Verizon Business IP Trunk service.

Note – The Fully Qualified Domain Names and IP addressing specified in these Application Notes apply only to the reference configuration shown in **Figure 1**. Verizon Business customers will use their own FQDNs and IP addressing as required.

In summary, the following components were used in the reference configuration.

- Verizon Business IP Trunk network Fully Qualified Domain Name (FQDN)
  - *pcelban0001.avayalincroft.globalipcom.com*
- Avaya CPE Fully Qualified Domain Name (FQDN) known to Verizon
  - *adevc.avaya.globalipcom.com*
- Primary and Secondary Avaya Session Border Controllers for Enterprise.
- Avaya Aura® Communication Manager Release 6.2
- Avaya Aura® Session Manager Release 6.2
- Avaya 96X1 Series IP telephones using the SIP and H.323 software bundle.
- Avaya 9600 Series IP telephones using the SIP and H.323 software bundle.
- Avaya Digital Phones
- Avaya Analog Phones

3.1. History Info and Diversion Headers

The Verizon Business IP Trunk service does not support SIP History Info Headers. Instead, the Verizon Business IP Trunk service requires that SIP Diversion Header be sent for redirected calls. The Avaya Aura® Communication Manager SIP trunk group form provides options for specifying whether History Info Headers or Diversion Headers are sent.

If Avaya Aura® Communication Manager sends the History Info Header, Avaya Aura® Session Manager can convert the History Info header into the Diversion Header. This is performed by specifying the “*VerizonAdapter*” adaptation in Avaya Aura® Session Manager.

The Avaya Aura® Communication Manager Call Forwarding or Extension to Cellular (EC500) features may be used for the call scenarios testing Diversion Header.

4. Equipment and Software Validated

The following equipment and software were used in the sample configuration.

Equipment:	Software:
HP ProLiant DL360 G7	Avaya Aura® Communication Manager Release 6.2 load 823.0
HP ProLiant DL360 G7	Avaya Aura® System Manager 6.2
HP ProLiant DL360 G7	Avaya Aura® Session Manager 6.2
G450 Gateway	3.1.20.1
DELL 210 RII	Avaya Session Border Controller for Enterprise Version 4.0.5Q02
Avaya 9600-Series Telephones (H.323)	96xx-IPT-H323-R3_1_3-112211
Avaya 9600-Series Telephones (SIP)	96xx-IPT-SIP-R2_6_6_0-102111
Avaya 96X1- Series Telephones (SIP)	96x1-IPT-SIP-R6_0_3-120511
Avaya 96X1- Series Telephones (H323)	96x1-IPT-H323-R6_0_5-091911
Avaya One-X Communicator (H.323)	6.1.3.08_SP3-Patch2-35791
Avaya 2400-Series and 6400-Series Digital Telephones	N/A
Okidata Analog Fax	N/A

Table 1: Equipment and Software Used in the Sample Configuration

5. Configure Avaya Aura® Communication Manager Release 6.2

This section illustrates an example configuration allowing SIP signaling via the "Processor Ethernet" of the Avaya HP Server to Session Manager. In configurations that use an Avaya G650 Media Gateway, it is also possible to use an Avaya C-LAN in the Avaya G650 Media Gateway for SIP signaling to Session Manager.

Note - The initial installation, configuration, and licensing of the Avaya servers and media gateways for Communication Manager are assumed to have been previously completed and are not discussed in these Application Notes.

5.1. Verify Licensed Features

Communication Manager license file controls customer capabilities. Contact an authorized Avaya representative for assistance if a required feature needs to be enabled.

On **Page 2** of the ***display system-parameters customer-options*** form, verify that the **Maximum Administered SIP Trunks** is sufficient for the combination of trunks to the Verizon Business IP Trunk service offer and any other SIP applications. Each call from a non-SIP endpoint to the Verizon Business IP Trunk service uses one SIP trunk for the duration of the call. Each call from a SIP endpoint to the Verizon Business IP Trunk service uses two SIP trunks for the duration of the call.

```
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 3
             Maximum Administered Remote Office Trunks: 12000 0
Maximum Concurrently Registered Remote Office Stations: 18000 0
              Maximum Concurrently Registered IP eCons: 414   0
  Max Concur Registered Unauthenticated H.323 Stations: 100   0
                        Maximum Video Capable Stations: 18000 0
                   Maximum Video Capable IP Softphones: 18000 0
                       Maximum Administered SIP Trunks: 24000 40
  Maximum Administered Ad-hoc Video Conferencing Ports: 24000 0
   Maximum Number of DS1 Boards with Echo Cancellation: 522   0
                             Maximum TN2501 VAL Boards: 128   0
                     Maximum Media Gateway VAL Sources: 250   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
```

On **Page 3** of the ***display system-parameters customer-options*** form, verify that **ARS** is enabled.

```
display system-parameters customer-options                      Page   3 of  11
                                OPTIONAL FEATURES

    Abbreviated Dialing Enhanced List? y          Audible Message Waiting? y
        Access Security Gateway (ASG)? n              Authorization Codes? y
        Analog Trunk Incoming Call ID? y                       CAS Branch? n
 A/D Grp/Sys List Dialing Start at 01? y                         CAS Main? n
Answer Supervision by Call Classifier? y                Change COR by FAC? n
                                 ARS? y  Computer Telephony Adjunct Links? y
                 ARS/AAR Partitioning? y   Cvg Of Calls Redirected Off-net? y
          ARS/AAR Dialing without FAC? n                      DCS (Basic)? y
          ASAI Link Core Capabilities? n                DCS Call Coverage? y
          ASAI Link Plus Capabilities? n               DCS with Rerouting? y
       Async. Transfer Mode (ATM) PNC? n
  Async. Transfer Mode (ATM) Trunking? n    Digital Loss Plan Modification? y
              ATM WAN Spare Processor? n                          DS1 MSP? y
                                ATMS? y           DS1 Echo Cancellation? y
                  Attendant Vectoring? y
```

On **Page 4** of the ***display system-parameters customer-options*** form, verify that the **Enhanced EC500**, **IP Trunks**, **IP Stations**, and **ISDN-PRI** features are enabled. If the use of SIP REFER messaging or send-only SDP attributes will be required verify that the **ISDN/SIP Network Call Redirection** feature is enabled.

```
display system-parameters customer-options                      Page   4 of  11
                                OPTIONAL FEATURES
   Emergency Access to Attendant? y                                IP Stations? y
           Enable 'dadmin' Login? y
           Enhanced Conferencing? y                          ISDN Feature Plus? n
                  Enhanced EC500? y        ISDN/SIP Network Call Redirection? y
    Enterprise Survivable Server? n                            ISDN-BRI Trunks? y
       Enterprise Wide Licensing? n                                   ISDN-PRI? y
              ESS Administration? y                 Local Survivable Processor? n
          Extended Cvg/Fwd Admin? y                       Malicious Call Trace? y
     External Device Alarm Admin? y                   Media Encryption Over IP? n
  Five Port Networks Max Per MCC? n     Mode Code for Centralized Voice Mail? n
                Flexible Billing? n
   Forced Entry of Account Codes? y                   Multifrequency Signaling? y
      Global Call Classification? y           Multimedia Call Handling (Basic)? y
             Hospitality (Basic)? y        Multimedia Call Handling (Enhanced)? y
 Hospitality (G3V3 Enhancements)? y                Multimedia IP SIP Trunking? y
                       IP Trunks? y

           IP Attendant Consoles? y
```

On **Page 5** of the ***display system-parameters customer-options*** form, verify that the **Private Networking** and **Processor Ethernet** features are enabled.

```
display system-parameters customer-options                 Page   5 of  11
                                OPTIONAL FEATURES

                Multinational Locations? n            Station and Trunk MSP? y
 Multiple Level Precedence & Preemption? n       Station as Virtual Extension? y
                     Multiple Locations? n
                                           System Management Data Transfer? n
           Personal Station Access (PSA)? y                Tenant Partitioning? y
                       PNC Duplication? n        Terminal Trans. Init. (TTI)? y
                  Port Network Support? y                Time of Day Routing? y
                       Posted Messages? y        TN2501 VAL Maximum Capacity? y
                                                          Uniform Dialing Plan? y
                     Private Networking? y     Usage Allocation Enhancements? y
                Processor and System MSP? y
                     Processor Ethernet? y               Wideband Switching? y
                                                                     Wireless? n
                          Remote Office? y
           Restrict Call Forward Off Net? y
                  Secondary Data Module? y
```

5.2. Dial Plan

In the reference configuration the Avaya CPE environment uses four digit local extensions, such as 2xxx, 3xxx or 4xxx. Trunk Access Codes (TAC) are 3 digits in length and begin with *. The Feature Access Code (FAC) to access ARS is the single digit 9. The Feature Access Code (FAC) to access AAR is the single digit 8. The dial plan illustrated here is not intended to be prescriptive; any valid dial plan may be used.

The dial plan is modified with the ***change dialplan analysis*** command as shown below.

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

    Dialed   Total  Call      Dialed   Total  Call      Dialed   Total  Call
    String   Length Type      String   Length Type      String   Length Type
   1           3   fac
   2           4   ext
   3           4   ext
   4           4   ext
   8           1   fac
   9           1   fac
   *           3   fac
   *1          4   dac
   #           3   fac
```

5.3. Node Names

Node names are mappings of names to IP addresses that can be used in various screens. The following ***change node-names ip*** output shows relevant node-names in the sample configuration. As shown in bold, the node name for Session Manager is "**ASM6-2**" with IP address **10.80.140.160**. The node name and IP address for the Processor Ethernet "**procr**" is **10.80.140.146**.

```
change node-names ip                                          Page   1 of   2
                                 IP NODE NAMES
    Name              IP Address
ASM6-2              10.80.140.160
Gateway1            10.80.140.1
default             0.0.0.0
procr               10.80.140.146
procr6              ::
```

5.4. Processor Ethernet Configuration on HP Common Server

The **add ip-interface procr** or **change ip-interface procr** command can be used to configure the Processor Ethernet (PE) parameters. The following screen shows the parameters used in the reference configuration.

- Verify that **Enable Interface?**, **Allow H.323 Endpoints?**, and **Allow H248 Gateways?** Fields are set to **y**.
- Assign a network region (e.g. **1**).
- Use default values for the remaining parameters.

```
change ip-interface procr                                   Page   1 of   2
                                  IP INTERFACES
                  Type: PROCR
Target socket load: 19660

      Enable Interface? y                            Allow H.323 Endpoints? y
                                                      Allow H.248 Gateways? y
        Network Region: 1                              Gatekeeper Priority: 5

                                 IPV4 PARAMETERS
             Node Name: procr                      IP Address: 10.80.140.146
```

5.5. Network Regions for Gateway, Telephones

Network regions provide a means to logically group resources. In the shared Communication Manager configuration used for the testing, the Avaya G450 Media Gateway is in region 1. To provide testing flexibility, network region 4 was associated with other components used specifically for the Verizon testing.

Non-IP telephones (e.g., analog, digital) derive network region and location configuration from the Avaya gateway to which the device is connected. The following display command shows that **Media Gateway 1** is an Avaya G450 Media Gateway configured for network region 1. It can also be observed that the **Controller IP Address** is the Avaya Processor Ethernet (10.80.140.146), and that the gateway IP address is 10.80,140.148. These fields are not configured in this screen, but just display the current information for the Media Gateway.

```
change media-gateway 1                                      Page   1 of   2
                            MEDIA GATEWAY 1

                   Type: g450
                   Name: G450
              Serial No: 08IS35173859
           Encrypt Link? y                  Enable CF? n
         Network Region: 1                   Location: 1
                                            Site Data:
          Recovery Rule: none

            Registered?  y
  FW Version/HW Vintage: 31 .20 .1  /1
      MGP IPV4 Address: 10.80.140.148
      MGP IPV6 Address:
  Controller IP Address: 10.80.140.146
            MAC Address: 00:1b:4f:03:42:d8
```

The following screen shows **Page 2** for **Media Gateway 1**. The gateway has an **S8300** in slot V1 (unused), a **MM712** media module supporting Avaya digital phones in slot V2, a **MM710** T1 board in V3(unused), a **MM711** supporting analog devices in slot V4, another **MM710** T1 board in V8 (unused), and the capability to provide announcements and music on hold via "gateway-announcements" in logical slot V9.

```
change media-gateway 1                                           Page   2 of   2
                             MEDIA GATEWAY 1

                                 Type: g450
Slot   Module Type             Name                    DSP Type  FW/HW version
 V1:   S8300                   ICC MM                  MP80      68   3
 V2:   MM712                   DCP MM
 V3:   MM710                   DS1 MM
 V4:   MM711                   ANA MM
 V5:
 V6:
 V7:
 V8:   MM710                   DS1 MM                Max Survivable IP Ext: 8
 V9:   gateway-announcements   ANN VMM
```

IP telephones can be assigned a network region based on an IP address mapping. The network region can also associate the IP telephone to a location for location-based routing decisions. The following screen illustrates a subset of the IP network map configuration used to verify these Application Notes. If the IP address of a registering IP Telephone does not appear in the ip-network-map, the phone is assigned the network region of the "gatekeeper" (e.g., CLAN or PE) to which it registers. When the IP address of a registering IP telephone is in the ip-network-map, the phone is assigned the network region assigned by the form shown below. For example, the IP address 10.80.140.29 would be mapped to network region 1, based on the configuration in bold below. In production environments, different sites will typically be on different networks, and ranges of IP addresses assigned by the DHCP scope serving the site can be entered as one entry in the network map, to assign all telephones in a range to a specific network region.

```
change ip-network-map                                            Page   1 of  63
                              IP ADDRESS MAPPING

                                                Subnet Network      Emergency
 IP Address                                     Bits   Region VLAN Location Ext
 ---------------------------------------------- ------ ------ ---- -------------
 FROM: 10.80.140.0                                /24    1      n
   TO: 10.80.140.255
```

The following screen shows IP Network Region 4 configuration. In the shared test environment, network region 4 is used to allow unique behaviors for the Verizon test environment. In this example, codec set 4 will be used for calls within region 4. The shared Avaya Interoperability Lab test environment uses the domain "avayalab.com" (i.e., for network region 1 including the region of the Processor Ethernet "procr"). However, to illustrate the more typical case where Communication Manager domain matches the enterprise CPE domain known to Verizon, the **Authoritative Domain** in the following screen is "adevc.avaya.globalipcom.com", the domain known to Verizon, as shown in **Figure 1**. Even with this configuration, note that the domain in the PAI header sent by Communication Manager to Session Manager will contain "avayalab.com", the domain of the Far-end of the Avaya signaling group. Session Manager will adapt "avayalab.com" to “adevc.avaya.globalipcom.com” in the PAI header, and the ASBCE will adapt the Diversion header.

```
change ip-network-region 4                                      Page   1 of  20
                               IP NETWORK REGION
  Region: 4
Location:          Authoritative Domain: adevc.avaya.globalipcom.com
    Name: Verizon testing
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? y
   UDP Port Max: 3029
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
```

The following screen shows the inter-network region connection configuration for region 4. The first bold row shows that network region 4 is directly connected to network region 1, and that codec set 4 will also be used for any connections between region 4 and region 1. For configurations where multiple remote gateways are used, each gateway will typically be configured for a different region, and this screen can be used to specify unique codec or call admission control parameters for the pairs of regions. If a different codec should be used for inter-region connectivity than for intra-region connectivity, a different codec set can be entered in the **codec set** column for the appropriate row in the screen shown below. Once submitted, the configuration becomes symmetric, meaning that network region 1, Page 4 will also show codec set 4 for region 4 to region 1 connectivity.

```
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
```

The following screen shows IP Network Region 1 configuration. In this example, codec set 1 will be used for calls within region 1 due to the Codec Set parameter on **Page 1**, but codec set 4 will be used for connections between region 1 and region 4 as noted previously. In the shared test environment, network region 1 was in place prior to adding the Verizon test environment and already used **Authoritative Domain** "avayalab.com". Where necessary, Session Manager or the ASBCE will adapt the domain from "avayalab.com" to "adevc.avaya.globalipcom.com".

```
change ip-network-region 1                                     Page   1 of  20
                               IP NETWORK REGION
  Region: 1
Location: 1       Authoritative Domain: avayalab.com
    Name: Enterprise
MEDIA PARAMETERS                Intra-region IP-IP Direct Audio: yes
      Codec Set: 1              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
```

The following screen shows the inter-network region connection configuration for region 1. The bold row shows that network region 1 is directly connected to network region 4, and that codec set 4 will be used for any connections between region 4 and region 1.

```
change ip-network-region 1                                     Page   4 of  20

 Source Region: 1     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    1                                                               all
 2    1     y    NoLimit                                             n       t
 3
 4    4     y    NoLimit                                             n       t
```

5.6. IP Codec Sets

The following screen shows the configuration for codec set 4, the codec set configured to be used for calls within region 4 and for calls between region 1 and region 4. In general, an IP codec set is a list of allowable codecs in priority order. Using the example configuration shown below, all calls to and from the PSTN via the SIP trunks would use G.729A, since G.729A is preferred by both Verizon and the Avaya ip-codec-set. Any calls using this same codec set that are between devices capable of the G.722-64K codec (e.g., Avaya 9600-Series IP Telephone) can use G.722. Note that if G.711MU is omitted from the list of allowed codecs in ip-codec-set 4, calls from Verizon that are answered by Avaya Modular Messaging will use G450 VoIP resources to convert from G.729a (facing Verizon) to G.711MU (facing Modular Messaging). If G.711MU is included in ip-codec-set 4, then calls from Verizon that are answered by Modular Messaging will not use G450 VoIP resources, but rather be "ip-direct" using G.711MU from Modular Messaging to the inside of the ASBCE. Include G.711MU in the ip-codec-set if fax will be used.

```
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.722-64K                   2        20
 2: G.729A           n          2        20
 3: G.711MU          n          2        20
 4:
```

On **Page 2** of the form:

- Configure the Fax **Mode** field to "t.38-standard", T.38 is newly supported by Verizon and was tested successfully in this test configuration.
- Configure the Fax **Redundancy** field to "**0".**

```
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
```

The following screen shows the configuration for codec set 1. This default configuration for codec set 1, using G.711MU, is used for Avaya Modular Messaging and other connections within region 1.

```
change ip-codec-set 1                                             Page   1 of   2
                          IP Codec Set
    Codec Set: 1

    Audio        Silence      Frames   Packet
    Codec        Suppression  Per Pkt  Size(ms)
 1: 1.722-64K                   2        20
 2: G.711MU          n          2        20
 3: G.729A           n          2        20
 4:
```

5.7. SIP Signaling Groups

This section illustrates the configuration of the SIP Signaling Groups. Each signaling group has a **Group Type** of "sip", a **Near-end Node Name** of "procr", and a **Far-end Node Name** of "SM6-2". In the example screens, the **Transport Method** for all signaling groups is "tcp". In production, TLS transport between Communication Manager and Session Manager can be used. The **Enable Layer 3 Test** field is enabled on each of the signaling groups to allow Communication Manager to maintain the signaling group using the SIP OPTIONS method. Fields that are not referenced in the text below can be left at default values, including **DTMF over IP** set to “rtp-payload”, which corresponds to RFC 2833.

The following screen shows signaling group 68. Signaling group 68 will be used for processing PSTN calls to / from Verizon via Session Manager. The **Far-end Network Region** is configured to region 4. Port 5062 has been configured as both the **Near-end Listen Port** and **Far-end Listen Port**. Session Manager will be configured to direct calls arriving from the PSTN with Verizon DID numbers to a route policy that uses a SIP entity link to Communication Manager specifying port 5062. The use of different ports is one means to allow Communication Manager to distinguish different types of calls arriving from the same Session Manager. In the sample configuration, the **Peer Detection Enabled** field was set to “n”. Other parameters may be left at default values. Note that the **Alternate Route Timer** that defaults to 6 seconds has been changed to 12 seconds, this timer impacts fail-over timing for outbound calls. If Communication Manager does not get an expected response, Look-Ahead Routing (LAR) can be triggered, after the expiration of the Alternate Route Timer.

```
change signaling-group 68                                       Page   1 of   2
                                SIGNALING GROUP

 Group Number: 68              Group Type: sip
  IMS Enabled? n         Transport Method: tcp
        Q-SIP? n
     IP Video? n                                   Enforce SIPS URI for SRTP? y
  Peer Detection Enabled? n  Peer Server: SM



   Near-end Node Name: procr                  Far-end Node Name: ASM6-2
 Near-end Listen Port: 5062                 Far-end Listen Port: 5062
                                         Far-end Network Region: 4

Far-end Domain: avayalab.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): 12
```

The following screen shows signaling group 3, the signaling group to Session Manager that was in place prior to adding the Verizon IP Trunk configuration to the shared Avaya Solutions and Interoperability Test Lab configuration. This signaling group reflects configuration not specifically related to Verizon IP Trunk but will be used to enable SIP phones to register to Session Manager and to use features from Communication Manager. Again, the **Near-end Node Name** is “procr” and the **Far-end Node Name** is “ASM6-2”, the node name of the Session Manager. Unlike the signaling group used for the Verizon IP Trunk signaling, the **Far-end Network Region** is **1**. The **Peer Detection Enabled** field is set to “y” and a peer Session Manager has been previously detected. The **Far-end Domain** is set to “avayalab.com” matching the configuration in place prior to adding the Verizon IP SIP Trunking configuration.

```
change signaling-group 3                                        Page   1 of   2
                                SIGNALING GROUP

 Group Number: 3              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: SM



   Near-end Node Name: procr                  Far-end Node Name: ASM6-2
 Near-end Listen Port: 5060                 Far-end Listen Port: 5060
                                         Far-end Network Region: 1

Far-end Domain: avayalab.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): 10
```

5.8. SIP Trunk Groups

This section illustrates the configuration of the SIP Trunks Groups corresponding to the SIP signaling groups from the previous section.

The following shows **Page 1** for trunk group 68, which will be used for incoming and outgoing PSTN calls from Verizon. The **Number of Members** field defines how many simultaneous calls are permitted for the trunk group. The **Service Type** field should be set to "public-ntwrk" for the trunks that will handle calls with Verizon. The **Direction** has been configured to "two-way" to allow incoming and outgoing calls only in the sample configuration.

```
change trunk-group 68                                           Page   1 of  21
                                TRUNK GROUP

Group Number: 68                   Group Type: sip           CDR Reports: y
  Group Name: To-ASM-Verizon              COR: 1        TN: 1        TAC: *168
   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: 68
                                                     Number of Members: 10
```

The following screen shows **Page 2** for trunk group 68. All parameters shown are default values, except for the **Preferred Minimum Session Refresh Interval**, which has been changed from the default 600 to 900. Although not strictly necessary, some SIP products prefer a higher session refresh interval than Communication Manager default value, which can result in unnecessary SIP messages to re-establish a higher refresh interval for each call.

```
change trunk-group 68                                           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): 900

                                     Delay Call Setup When Accessed Via IGAR? n
```

The following screen shows **Page 3** for trunk group 68. All parameters except those in bold are default values. The **Numbering Format** will use "private" numbering, meaning that the private numbering table would be consulted for any mappings of Communication Manager extensions to alternate numbers to be sent to Session Manager. Optionally, replacement text strings can be configured using the "system-parameters features" screen, such that incoming "private" (anonymous) or "restricted" calls can display an Avaya-configured text string on called party telephones.

```
change trunk-group 68                                           Page   3 of  21
TRUNK FEATURES
          ACA Assignment? n            Measured: none
                                                       Maintenance Tests? y

                     Numbering Format: private
                                                UUI Treatment: service-provider

                                                 Replace Restricted Numbers? y
                                                Replace Unavailable Numbers? y
 Show ANSWERED BY on Display? Y
```

The following screen shows **Page 4** for trunk group 68. The **PROTOCOL VARIATIONS** page is one reason why it can be advantageous to configure incoming calls from Verizon to arrive on specific signaling groups and trunk groups. The bold fields have non-default values. The **Convert 180 to 183 for Early Media** field was a new in Communication Manager Release 6. Verizon recommends that inbound calls to the enterprise result in a 183 with SDP rather than a 180 with SDP, and setting this field to "y" for the trunk group handling inbound calls from Verizon produces this result. Although not strictly necessary, the **Telephone Event Payload Type** has been set to 101 to match Verizon configuration. Setting the **Network Call Redirection** flag to "y" enables advanced services associated with the use of the REFER message, while also implicitly enabling Communication Manager to signal "send-only" media conditions for calls placed on hold at the enterprise site. If neither REFER signaling nor "send-only" media signaling is required, this field may be left at the default "n" value. In the testing associated with these Application Notes, transfer testing using REFER was successfully completed with the **Network Call Redirection** flag set to "y", and transfer testing using INVITE was successfully completed with the **Network Call Redirection** flag set to "n".

For redirected calls, Verizon supports the Diversion header, but not the History-Info header. Communication Manager can send the Diversion header by marking **Send Diversion Header** to "y". Alternatively, Communication can send the History-Info header by setting **Support Request History** to "y", and Session Manager can adapt the History-Info header to the Diversion header using the "VerizonAdapter". In the testing associated with these Application Notes, call redirection testing with Communication Manager sending Diversion Header was completed successfully. Communication Manager configuration was then changed, and call redirection testing with Communication Manager sending History-Info and Session Manager adapting to Diversion Header was completed successfully.

```
change trunk-group 68                                          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
                             Enable Q-SIP? N
```

The following screen shows **Page 1** for trunk group 3, the bi-directional "tie" trunk group to Session Manager that existed before adding the Verizon SIP Trunk configuration to the shared Avaya Interoperability Lab network. Recall that this trunk is used to enable SIP phones to use features from Communication Manager and to communicate with other Avaya applications, such as Avaya Modular Messaging, and does not reflect any unique Verizon configuration.

```
change trunk-group 3                                           Page   1 of  21
                                TRUNK GROUP

Group Number: 3                   Group Type: sip          CDR Reports: y
  Group Name: To_ASM6-2                  COR: 1        TN: 1        TAC: *103
   Direction: two-way       Outgoing Display? n
 Dial Access? n                                Night Service:
Queue Length: 0
Service Type: tie                  Auth Code? n
                                              Member Assignment Method: auto
                                                       Signaling Group: 3
                                                     Number of Members: 20
```

The following shows **Page 3** for trunk group 3. Note that this tie trunk group uses a "private" **Numbering Format**.

```
change trunk-group 3                                           Page   3 of  21
                                TRUNK FEATURES
          ACA Assignment? n            Measured: none
                                                        Maintenance Tests? y
                     Numbering Format: private
                                                UUI Treatment: service-provider

                                                 Replace Restricted Numbers? n
                                                Replace Unavailable Numbers? n

                                Modify Tandem Calling Number: no
```

The following screen shows **Page 4** for trunk group 3. Note that unlike the trunks associated with Verizon calls that have non-default "protocol variations", this trunk group maintains all default values. **Support Request History** must remain set to the default "y" to support proper subscriber mailbox identification by Modular Messaging.

```
change trunk-group 3                                            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? n
                  Support Request History? y
             Telephone Event Payload Type:

       Convert 180 to 183 for Early Media? n
 Always Use re-INVITE for Display Updates? n
                            Enable Q-SIP? N
```

5.9. Route Pattern Directing Outbound Calls to Verizon

Route pattern 68 will be used for calls destined for the PSTN via the Verizon IP Trunk service. Digit manipulation can be performed on the called number, if needed, using the **No. Del Dgts** and **Inserted Digits** parameters. Digit manipulation can also be performed by Session Manager.

If desired, one or more alternate Communication Manager trunks can be listed in the route pattern so that the Look-Ahead Routing (**LAR**) "next" setting can route-advance to attempt to complete the call using alternate trunks should there be no response or an error response from the far-end.

```
change route-pattern 68                                          Page   1 of   3
                    Pattern Number: 68  Pattern Name: To-VZ-IP-Trunk
                             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: 68   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                              unk-unk   next
 2: y y y y y n  n            rest                                        none
 3: y y y y y n  n            rest                                        none
 4: y y y y y n  n            rest                                        none
 5: y y y y y n  n            rest                                        none
 6: y y y y y n  n            rest                                        none
```

5.10. Route Pattern for Internal Calls via Session Manager

Route pattern 3 contains trunk group 3, the "private" tie trunk group to Session Manager. The **Numbering Format**: ***lev0-pvt*** means all calls using this route pattern will use the private numbering table.

```
change route-pattern 3                                                Page   1 of   3
                    Pattern Number: 3   Pattern Name: SIP_Phones
                             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: 3    0                                                                 n   user
 2:                                                                        n   user
 3:                                                                        n   user
 4:                                                                        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                                lev0-pvt  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
```

5.11. Private Numbering

The ***change private-unknown-numbering*** command may be used to define the format of numbers sent to Verizon in SIP headers such as the "From" and "PAI" headers. In general, the mappings of internal extensions to Verizon DID numbers may be done in Communication Manager (via public-unknown-numbering, and incoming call handling treatment for the inbound trunk group).

In the bolded row shown in the example abridged output below, a specific Communication Manager extension (x2010) is mapped to a DID number that is known to Verizon for this SIP Trunk connection (7329450285), when the call uses trunk group 68. Alternatively, Communication Manager can send the five digit extension to Session Manager, and Session Manager can adapt the number to the Verizon DID. Both methods were tested successfully.

```
change private-numbering 0                                            Page   1 of   2
                           NUMBERING - PRIVATE FORMAT
Ext Ext             Trk        Private           Total
Len Code            Grp(s)     Prefix            Len
 4  2               3                            4     Total Administered: 17
 4  3               3                            4        Maximum Entries: 540
 4  4               3                            4
 4  2010            68         7329450285        10
 4  2011            68         7329450286        10
 4  2012            68         7329450287        10
 4  2013            68         7329450288        10
 4  2014            68         7329450231        10
 4  3010            68         7329450240        10
 4  3011            68         7329450241        10
 4  3013            68         7329450242        10
 4  3688            68         7329450228        10
 4  4010            68         7329450243        10
```

5.12. ARS Routing For Outbound Calls

Although not illustrated in these Application Notes, location-based routing may be configured so that users at different locations that dial the same telephone number can have calls choose different route-patterns. Various example scenarios for a multi-location network with failover routing are provided in reference [PE]. In these Application Notes, the ARS "all locations" table directs ARS calls to specific SIP Trunks to Session Manager.

The following screen shows a specific ARS configuration as an example. If a user dials the ARS access code followed by 13035387024, the call will select route pattern 68. Of course, matching of the dialed string need not be this specific. The ARS configuration shown here is not intended to be prescriptive.

```
change ars analysis 13035387022                                 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
    13035387024           11   11    68       hnpa         n
```

The ***list ars route-chosen*** command can be used on a target dialed number to check whether routing will behave as intended. An example is shown below.

```
list ars route-chosen 13035387024
                           ARS ROUTE CHOSEN REPORT
     Location:  1                    Partitioned Group Number:  1

      Dialed            Total        Route    Call      Node
      String          Min    Max    Pattern   Type     Number    Location

 13035387024          11    11       68       hnpa                 all
   Actual Outpulsed Digits by Preference (leading 35 of maximum 42 digit)

 1: 13035387024
```

5.13. Incoming Call Handling Treatment for Incoming Calls

In general, the "incoming call handling treatment" for a trunk group can be used to manipulate the digits received for an incoming call if necessary. Since Session Manager is present, Session Manager can also be used to perform digit conversion, and digit manipulation and Communication Manager incoming call handling table may not be necessary. If the DID number sent by Verizon is unchanged by Session Manager, then the DID number can be mapped to an extension using the incoming call handling treatment of the receiving trunk group. As an example, the following screen illustrates a conversion of DID number 7329450240 to extension 3010. Both Session Manager digit conversion and Communication Manager incoming call handling treatment methods were tested successfully.

```
change inc-call-handling-trmt trunk-group 68                  Page   1 of  30
                           INCOMING CALL HANDLING TREATMENT
 Service/      Number   Number      Del Insert
 Feature         Len      Digits
 public-ntwrk    10 7329450240       10  3010
 public-ntwrk    10 7329450241       10  3011
 public-ntwrk    10 7329450242       10  3013
 public-ntwrk    10 7329450243       10  4010
 public-ntwrk    10 7329450244       10  4011
 public-ntwrk    10 7329450285       10  2010
 public-ntwrk    10 7329450286       10  2011
 public-ntwrk    10 7329450287       10  2012
 public-ntwrk    10 7329450288       10  2013
```

5.14. Avaya Aura® Communication Manager Stations

In the sample configuration, five digit station extensions were used with the format 2xxx, 3xxx, and 4xxx. The following abbreviated screen shows an example extension for an Avaya H.323 IP telephone.

```
change station 2010                                            Page   1 of   5
                                     STATION

Extension: 2010                         Lock Messages? n              BCC: 0
     Type: 9641                         Security Code: 1234            TN: 1
     Port: S00000                     Coverage Path 1: 1              COR: 1
     Name: 9641G H323                 Coverage Path 2:                COS: 1
                                      Hunt-to Station:
STATION OPTIONS
                                          Time of Day Lock Table:
              Loss Group: 19       Personalized Ringing Pattern: 1
                                                Message Lamp Ext: 2010
            Speakerphone: 2-way               Mute Button Enabled? y
        Display Language: english                 Button Modules: 0
 Survivable GK Node Name:
          Survivable COR: internal              Media Complex Ext:
   Survivable Trunk Dest? y                          IP SoftPhone? n

                                                         IP Video? n
```

5.15. EC500 Configuration for Diversion Header Testing

When EC500 is enabled for a Communication Manager station, a call to that station will generate a new outbound call from Communication Manager to the configured EC500 destination, typically a mobile phone. The following screen shows an example EC500 configuration for the user with station extension 2010. Use the command ***change off-pbx-telephone station mapping x*** where ***x*** is Communication Manager station (e.g. 2010).

- **Station Extension** – This field will automatically populate
- **Application** – Enter "EC500"
- **Dial Prefix** – Enter a prefix (e.g., 1) if required by the routing configuration
- **Phone Number** – Enter the phone that will also be called (e.g., 3035387024)
- **Trunk Selection** – Enter "ars". This means ARS will be used to determine how Communication Manager will route to the **Phone Number** destination.
- **Config Set** – Enter "1"
- Other parameters can retain default values

```
change off-pbx-telephone station-mapping 2010                     Page   1 of   3
                  STATIONS WITH OFF-PBX TELEPHONE INTEGRATION

 Station          Application Dial    CC   Phone Number      Trunk       Config   Dual
 Extension                    Prefix                         Selection   Set      Mode
 2010                EC500         -       3035387024         ars        1
```

5.16. Saving Communication Manager Configuration Changes

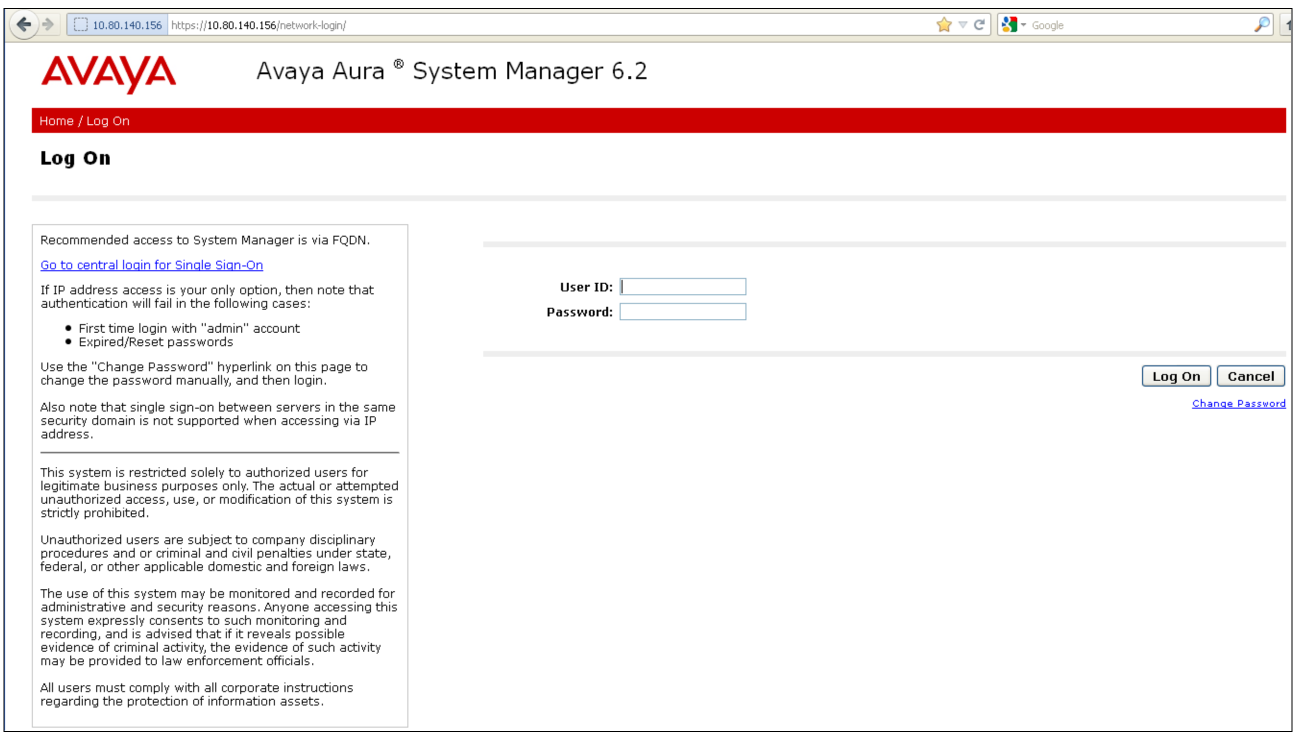
The command ***save translation all*** can be used to save the configuration.

6. Configure Avaya Aura® Session Manager Release 6.2

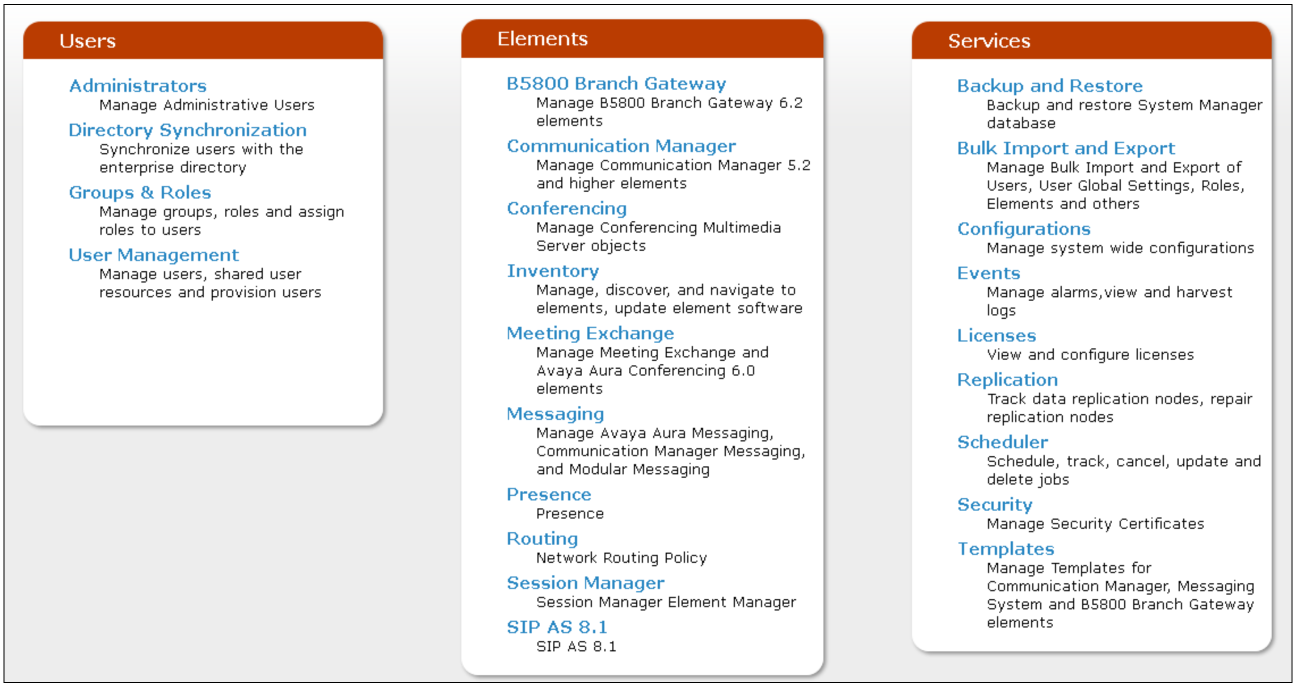
This section illustrates relevant aspects of the Session Manager configuration used in the verification of these Application Notes.

Note – The following sections assume that Session Manager and System Manager have been installed and that network connectivity exists between System Manager and Session Manager.

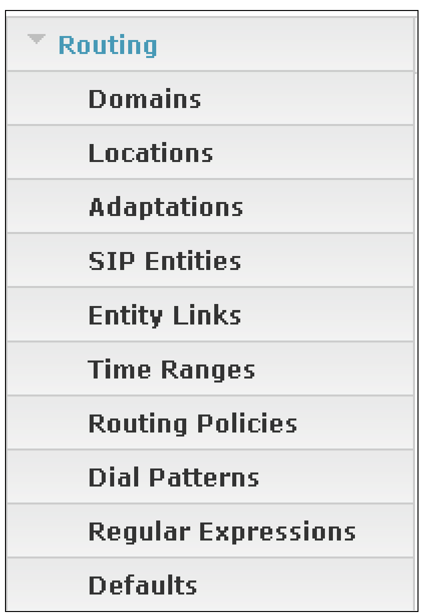
Session Manager is managed via System Manager. Using a web browser, access "https://<ip-addr of System Manager>/SMGR". In the **Log On** screen, enter appropriate **User ID** and **Password** and press the **Log On** button as shown in the example System Manager 6.2 **Log On** screen below.



Once logged in, a **Home Screen** is displayed. An abridged **Home Screen** is shown below.



Under the heading "Elements" in the center, select **Routing.** The screen shown below shows the various sub-headings available on the left hand side menu.



The right side of the screen, illustrated below, outlines a series of steps. The sub-sections that follow are in the same order as the steps outlined under **Introduction to Network Routing Policy** in the abridged screen shown below.

Introduction to Network Routing Policy

Network Routing Policy consists of several routing applications like "Domains", "Locations", "SIP Entities", etc.

The recommended order to use the routing applications (that means the overall routing workflow) to configure your network configuration is as follows:

Step 1: Create "Domains" of type SIP (other routing applications are referring domains of type SIP).

Step 2: Create "Locations"

Step 3: Create "Adaptations"

Step 4: Create "SIP Entities"

- SIP Entities that are used as "Outbound Proxies" e.g. a certain "Gateway" or "SIP Trunk"
- Create all "other SIP Entities" (Session Manager, CM, SIP/PSTN Gateways, SIP Trunks)
- Assign the appropriate "Locations", "Adaptations" and "Outbound Proxies"

Step 5: Create the "Entity Links"

- Between Session Managers
- Between Session Managers and "other SIP Entities"

Step 6: Create "Time Ranges"

- Align with the tariff information received from the Service Providers

Step 7: Create "Routing Policies"

- Assign the appropriate "Routing Destination" and "Time Of Day"

(Time Of Day = assign the appropriate "Time Range" and define the "Ranking")

Step 8: Create "Dial Patterns"

- Assign the appropriate "Locations" and "Routing Policies" to the "Dial Patterns"

Step 9: Create "Regular Expressions"

- Assign the appropriate "Routing Policies" to the "Regular Expressions"

Scroll down to review additional information as shown below. In these Application Notes, all steps are illustrated with the exception of Step 9, since "Regular Expressions" were not used.

Each "Routing Policy" defines the "Routing Destination" (which is a "SIP Entity") as well as the "Time of Day" and its associated "Ranking".

IMPORTANT: the appropriate dial patterns are defined and assigned afterwards with the help of the routing application "Dial patterns". That's why this overall routing workflow can be interpreted as

"Dial Pattern driven approach to define Routing Policies"

That means (with regard to steps listed above):

Step 7: "Routing Polices" are defined

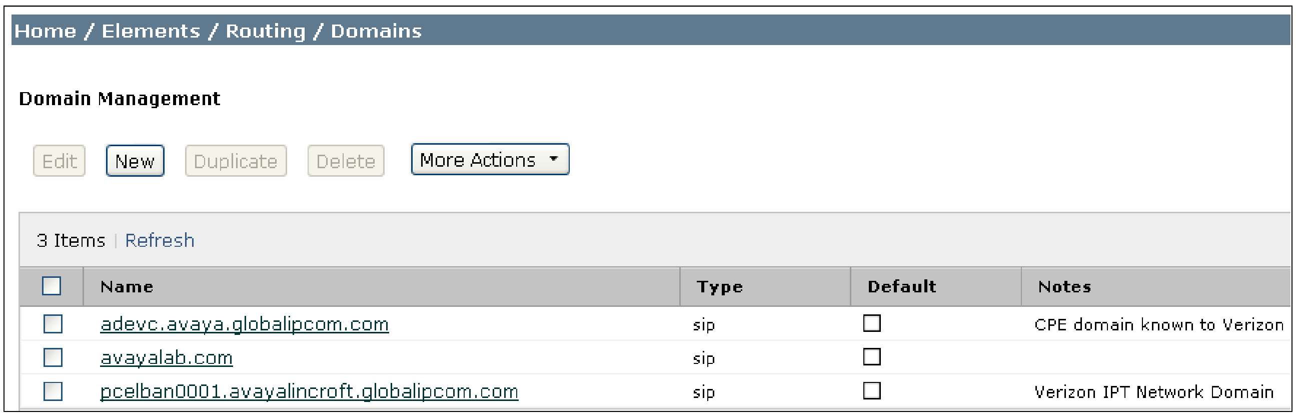
Step 8: "Dial Patterns" are defined and assigned to "Routing Policies" and "Locations" (one step)

Step 9: "Regular Expressions" are defined and assigned to "Routing Policies" (one step)

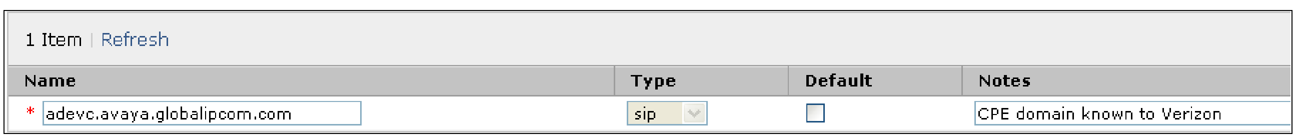
6.1. Domains

To view or change SIP domains, select **Routing → Domains**. Click on the checkbox next to the name of the SIP domain and **Edit** to edit an existing domain, or the **New** button to add a domain. Click the **Commit** button after changes are completed.

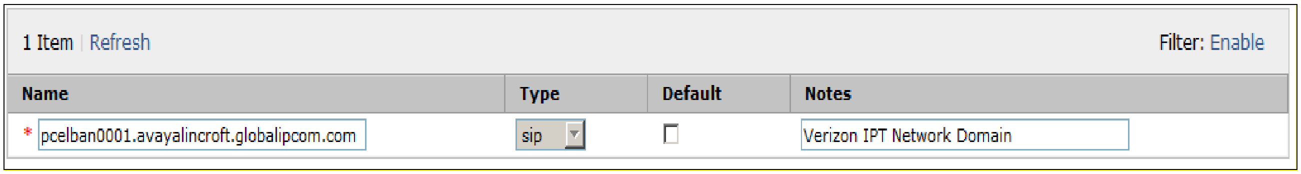
The following screen shows a list of configured SIP domains. The Session Manager used in the verification of these Application Notes was shared among other Avaya interoperability test efforts. The domain "avayalab.com" was used for communication with Avaya SIP Telephones and other Avaya systems and applications. The domain "avayalab.com" is not known to the Verizon production service.



The domain "adevc.avaya.globalipcom.com" is the domain known to Verizon as the enterprise SIP domain. In the sample configuration, Verizon included this domain as the host portion of the Request-URI for inbound DID calls.



The domain “pcelban0001.avayalincroft.globalipcom.com” is associated with the Verizon network in the sample configuration. For example, for calls from the enterprise site to Verizon, this domain can appear in the Request-URI in the INVITE message sent to Verizon. The following screen shows the relevant configuration.

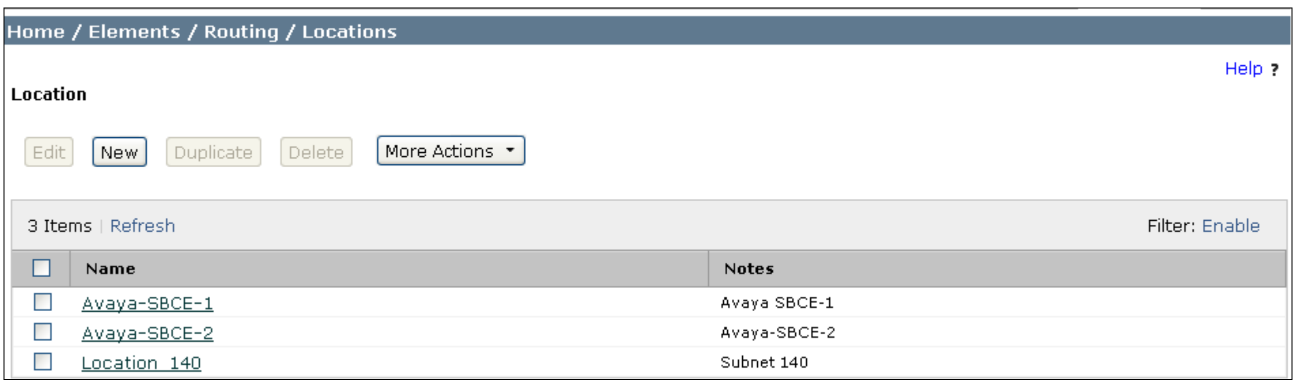


1 Item | Refresh Filter: Enable

Name	Type	Default	Notes
* pcelban0001.avayalincroft.globalipcom.com	sip	☐	Verizon IPT Network Domain

6.2. Locations

To view or change locations, select **Routing → Locations**. The following screen shows an abridged list of configured locations. Click on the checkbox corresponding to the name of a location and **Edit** to edit an existing location, or the **New** button to add a location. Click the **Commit** button after changes are completed. Assigning unique locations can allow Session Manager to perform location-based routing, bandwidth management, and call admission control.



Home / Elements / Routing / Locations

Help ?

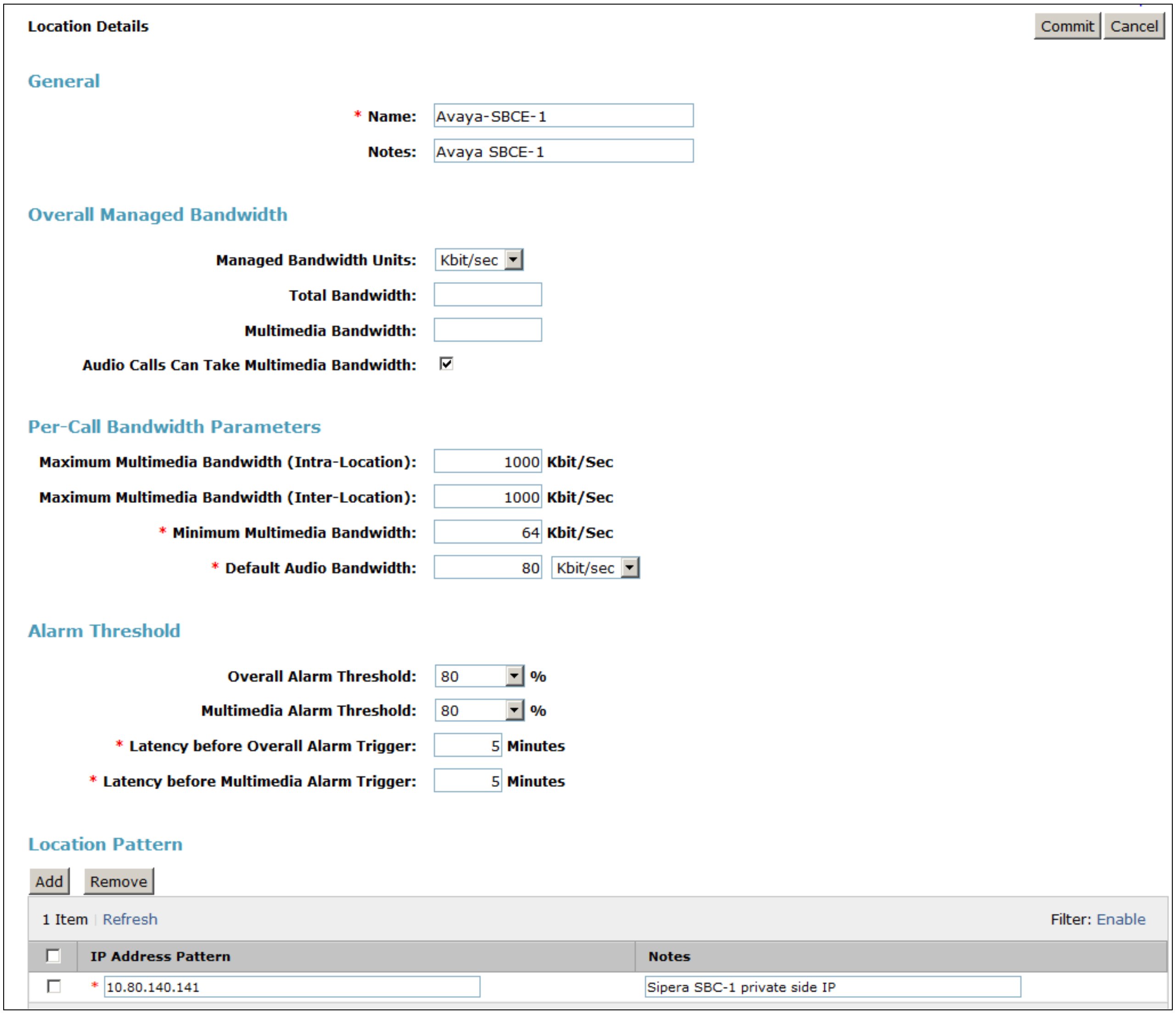
Location

Edit New Duplicate Delete More Actions

3 Items | Refresh Filter: Enable

☐	Name	Notes
☐	Avaya-SBCE-1	Avaya SBCE-1
☐	Avaya-SBCE-2	Avaya-SBCE-2
☐	Location_140	Subnet 140

The following image shows the top portion of the screen for the location details for the location named "Avaya-SBCE-1", corresponding to the ASBCE relevant to these Application Notes. Later, the location with name "Avaya-SBCE-1" will be assigned to the corresponding SIP Entity.



The following image shows the lower portion of the screen for the location details for the location named "Avaya-SBCE-2". The IP Address 10.80.140.200 of the inside (private) interface of the ASBCE is entered in the **IP Address Pattern** field. In the sample configuration, other location parameters (not shown) retained default values.

Location Pattern

Add | Remove

1 Item | Refresh

	IP Address Pattern	Notes
☐	* 10.80.140.200	Sipera SBC-2 private side IP

Select : All, None

If desired, additional locations can be configured with IP Address Patterns corresponding to other elements in the configuration.

6.3. Adaptations

To view or change adaptations, select **Routing → Adaptations**. Click on the checkbox corresponding to the name of an adaptation and **Edit** to edit an existing adaptation, or the **New** button to add an adaptation. Click the **Commit** button after changes are completed (not shown).

The following screen shows a portion of the list of adaptations that were available in the sample configuration, not all of which are applicable to these Application Notes.

Home / Elements / Routing / Adaptations

Adaptations

Edit | New | Duplicate | Delete | More Actions

5 Items | Refresh

	Name	Module name
☐	CM-ES-VZ	DigitConversionAdapter odstd=avayalab.com
☐	CM-ES-VZ-IPCC	DigitConversionAdapter odstd=avayalab.com fromto=true
☐	History_Diversion_IPT	VerizonAdapter osrcd=adevc.avaya.globalipcom.com odstd=pcelban0001.avayalincroft.globalipcom.com fromto=true
☐	SBC-VzB-IPCC	DigitConversionAdapter osrcd=adevc.avaya.globalipcom.com
☐	Verizon_Test	VerizonAdapter osrcd=adevc.avaya.globalipcom.com odstd=pcelban0001.avayalincroft.globalipcom.com

The following screen shows the adaptation details. The adapter named "History_Diversion_IPT" will later be assigned to the SIP Entity for the ASBCE, specifying that all communication from the Session Manager to the ASBCE will use this adapter. This adaptation uses the "VerizonAdapter" and specifies three parameters that are used to adapt the FQDN to the domains expected by the Verizon network in the sample configuration. Again, this may not be required in all networks, but is used here to adapt the avayalab.com domain that is used in the shared test environment among other Avaya interoperability test efforts.

The "**Module parameter:**" line contains the following line:

osrcd=adevc.avaya.globalipcom.com odstd=pcelban0001.avayalincroft.globalipcom.com fromto=true

- `overrideSourceDomain` : "**osrcd=adevc.avaya.globalipcom.com**". This configuration enables the source domain to be overwritten with "adevc.avaya.globalipcom.com". For example, for outbound PSTN calls from the Avaya CPE to Verizon, the PAI header will contain "adevc.avaya.globalipcom.com" as expected by Verizon.

- `overrideDestinationDomain` : "**odstd=pcelban0001.avayalincroft.globalipcom.com**" This configuration enables the destination domain to be overwritten with "pcelban0001.avayalincroft.globalipcom.com". For example, for outbound PSTN calls from the Avaya CPE to Verizon, the Request-URI header will contain "pcelban0001.avayalincroft.globalipcom.com" as expected by Verizon.

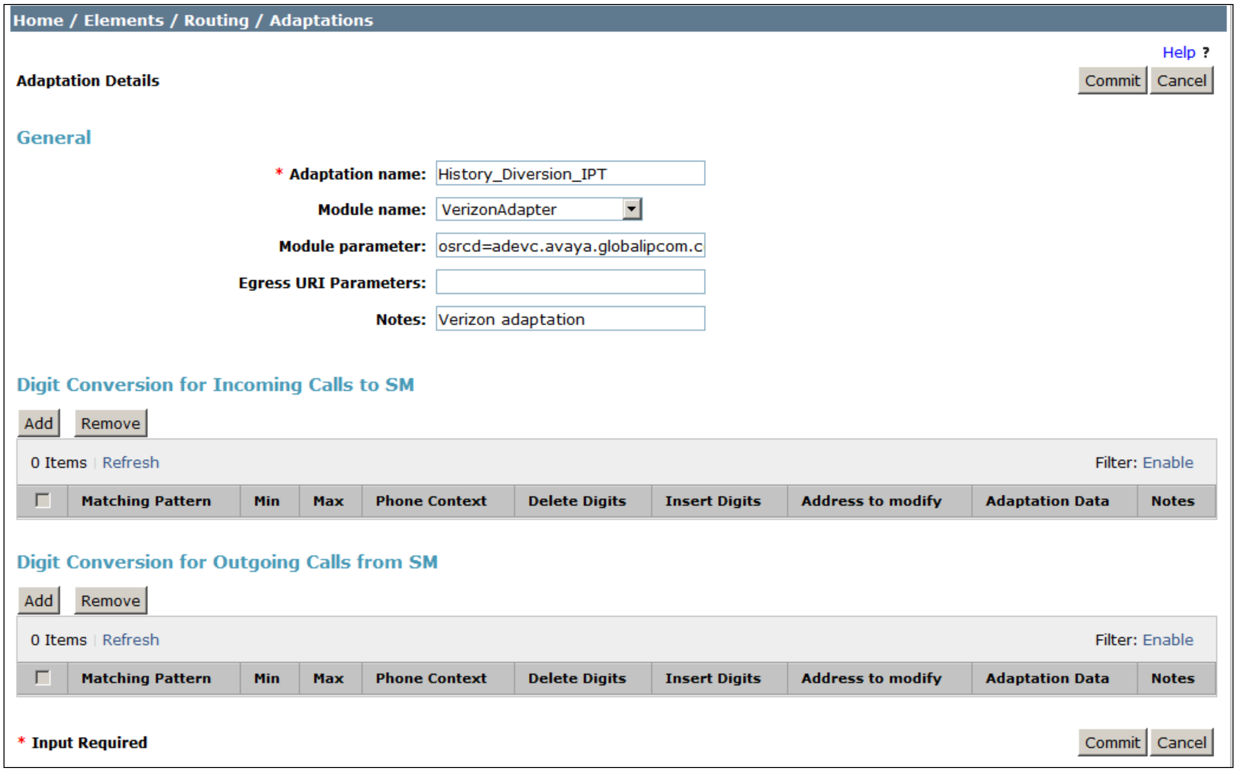
- `Fromto:` The parameter "**fromto=true**" enables Session to modify From and To headers of the message. If omitted or set to any other value, From and To headers will not be modified.

The "History_Diversion_IPT" Module Parameter statement above is overriding avayalab.com with the FQDNs know by Verizon towards the ASBCE. It is also necessary to override the FQDNs known to Verizon back to avayalab.com towards Communication Manager. This could be done on the next Adaptation "CM-ES-VZ" with the same parameters odstd and osrcd or here in the "History_Diversion_IPT" adapter with the statements:

- `ingressOverrideDestinationDomain: "`**`iodstd=avayalab.com`**`"`

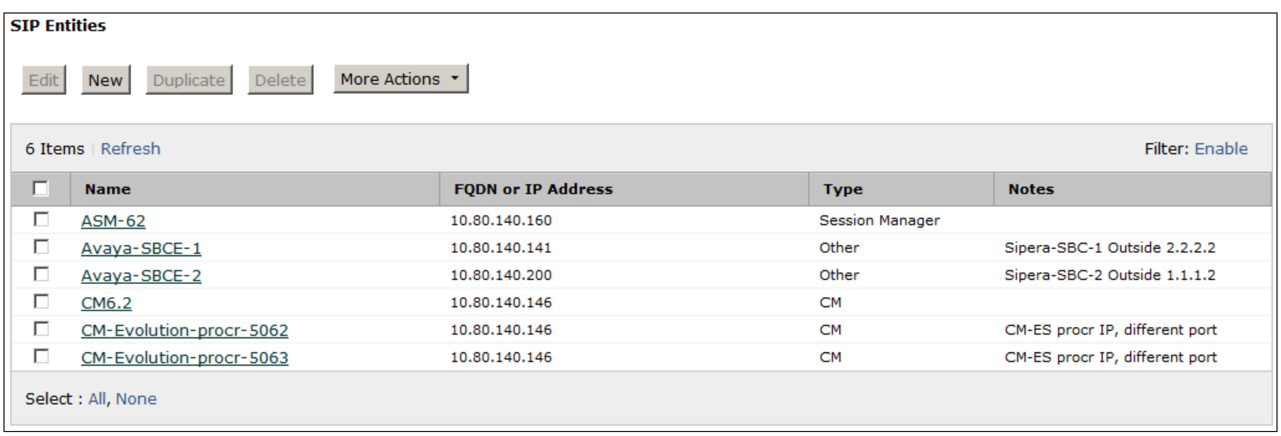
- `ingressOverrideDestinationDomain: "`**`iosrcd=avayalab.com`**`"`

However, in this configuration, that is being done in the ASBCE to show multiple locations to override the domain.

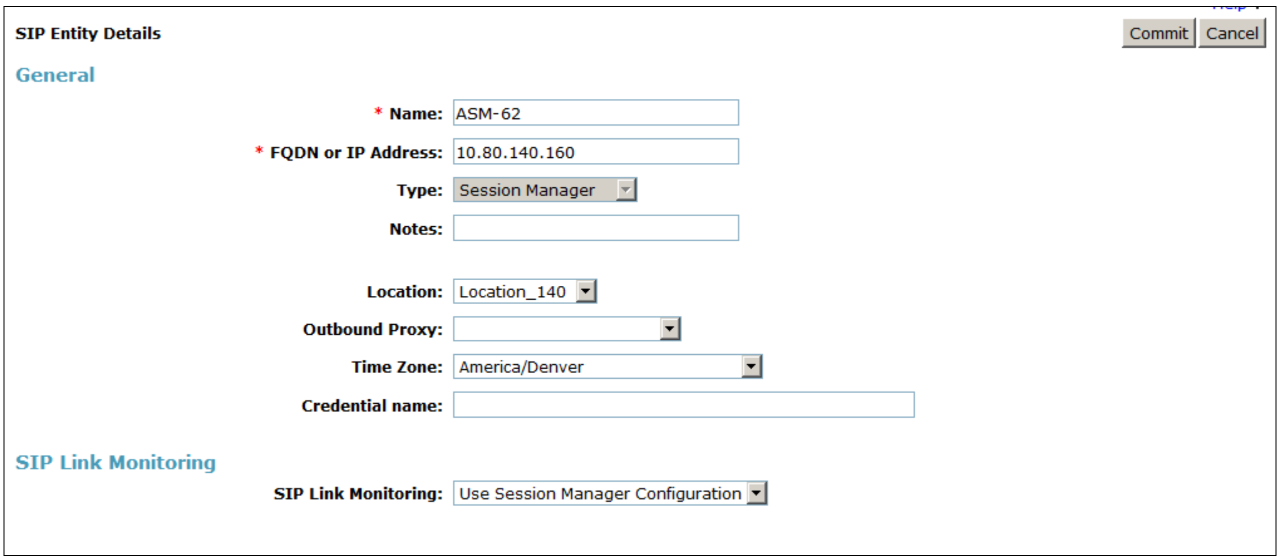


6.4. SIP Entities

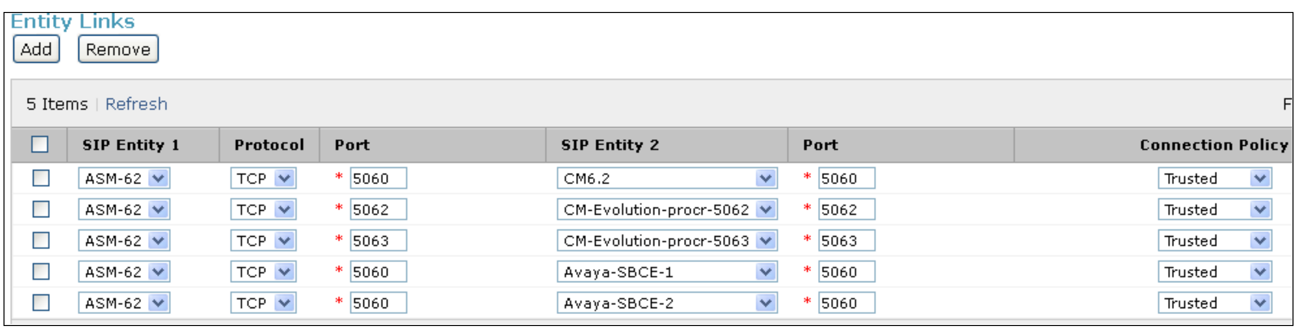
To view or change SIP entities, select **Routing → SIP Entities**. Click the checkbox corresponding to the name of an entity and **Edit** to edit an existing entity, or the **New** button to add an entity. Click the **Commit** button after changes are completed. The following screen shows a portion of the list of configured SIP entities. In this screen, the SIP Entities named "Avaya-SBCE-1", "Avaya-SBCE-2", "ASM-62", and "CM-Evolution-procr-5062" are relevant to these Application Notes.



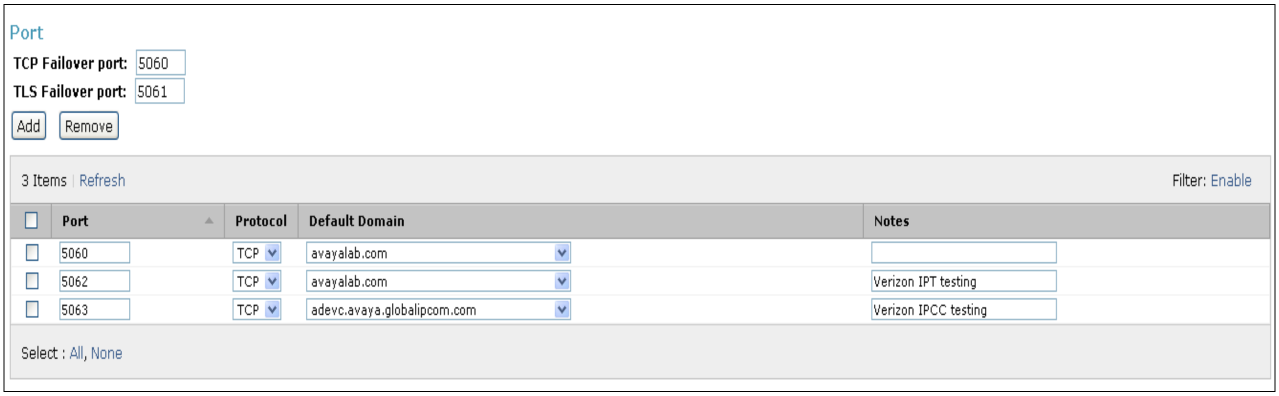
The following screen shows the upper portion of the **SIP Entity Details** corresponding to "ASM-62". The **FQDN or IP Address** field for "ASM-62" is the Session Manager Security Module IP Address (10.80.140.160), which is used for SIP signaling with other networked SIP entities. The **Type** for this SIP entity is "Session Manager". Select an appropriate location for the Session Manager from the **Location** drop-down menu. In the shared test environment, the Session Manager used location "Location_140". The default **SIP Link Monitoring** parameters may be used. Unless changed elsewhere, links from other SIP entities to this instance of Session Manager will use the default SIP Link Monitoring timers, configurable at the Session Manager level. If desired, these timers may be customized for each entity.



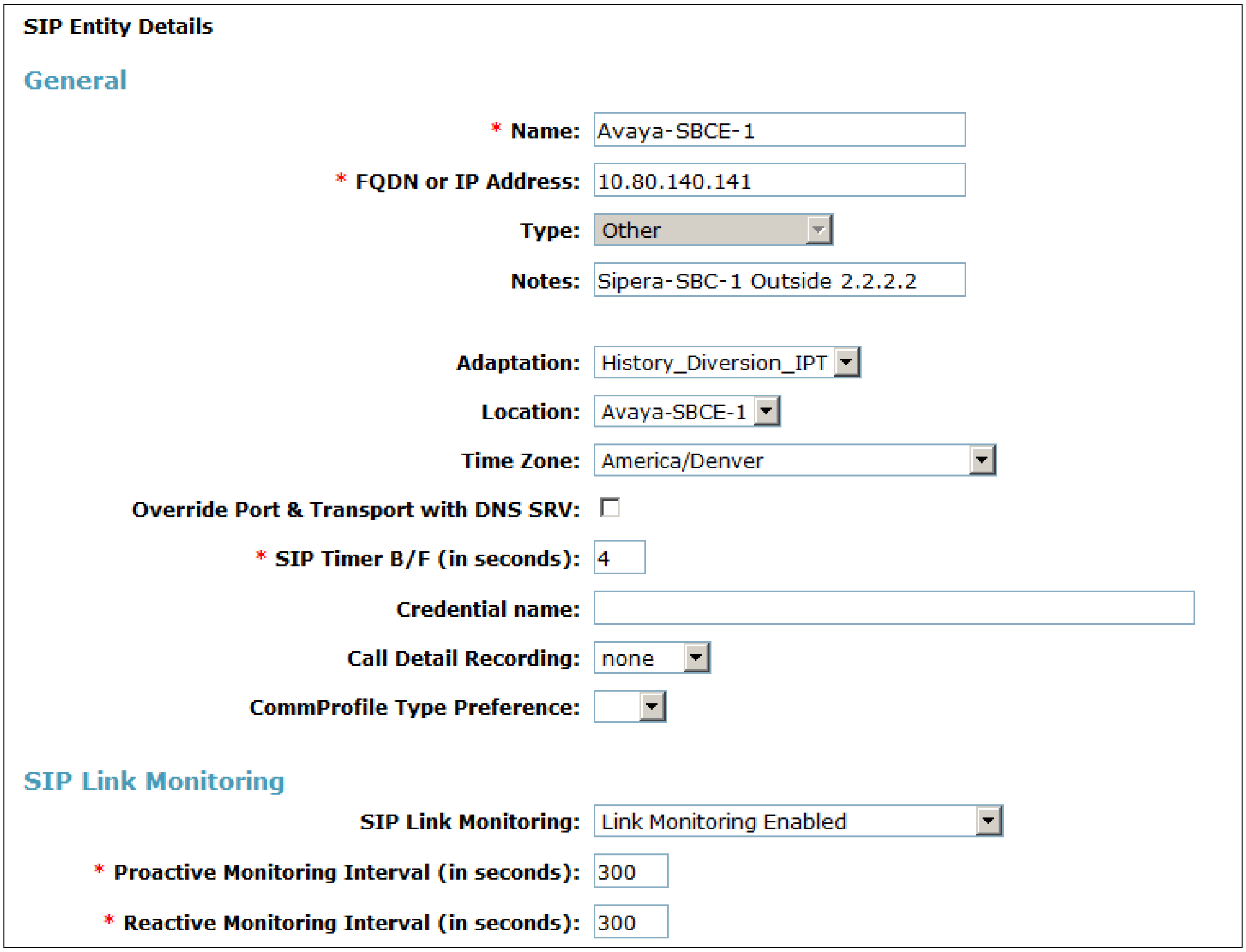
Scrolling down, the following screen shows the middle portion of the **SIP Entity Details**, a listing of the **Entity Links** previously configured for "ASM-62". The links relevant to these Application Notes are described in the subsequent section.



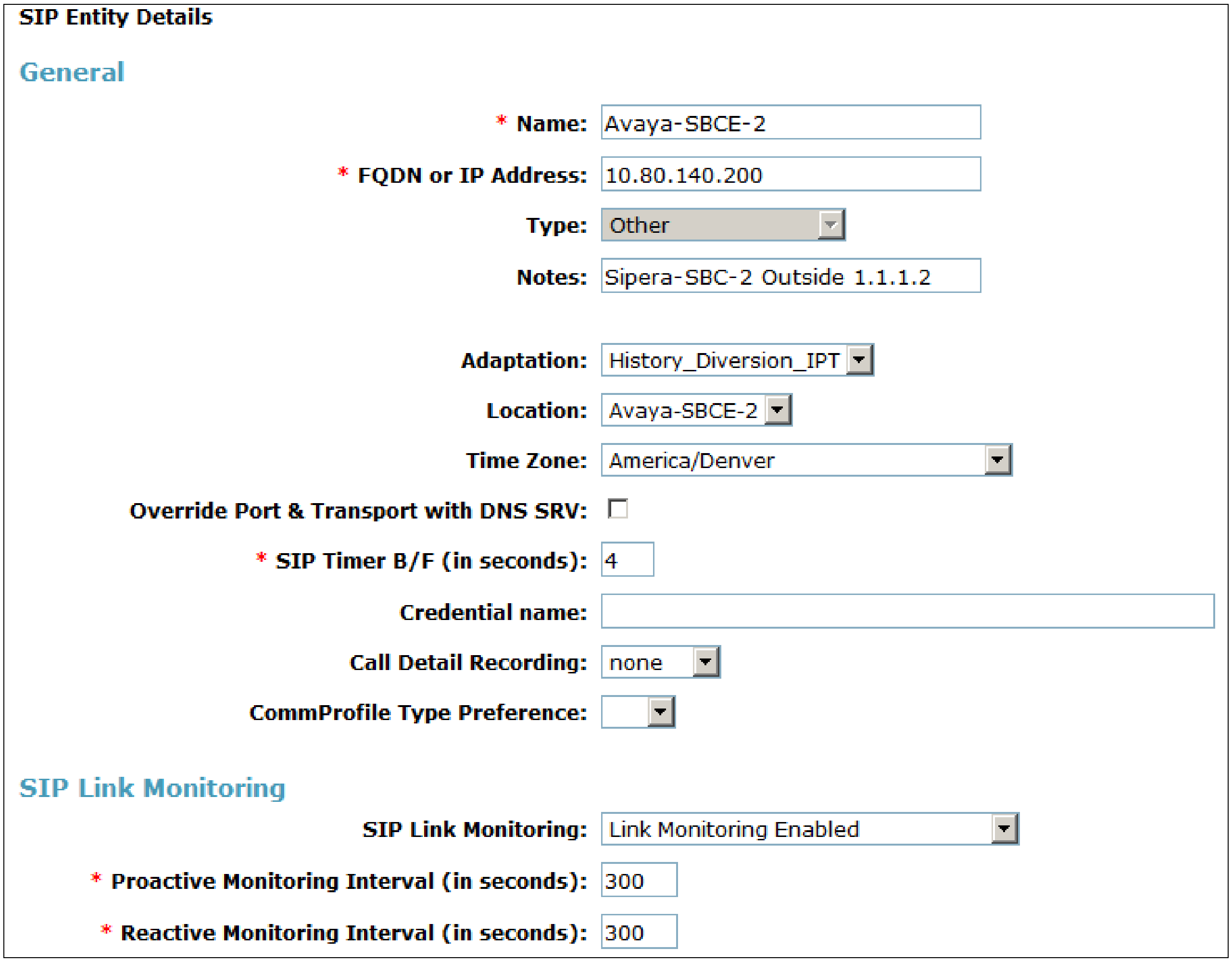
Scrolling down, the following screen shows the lower portion of the **SIP Entity Details**, illustrating the configured ports for "ASM-62". In the sample configuration, TCP port 5060 was already in place for the shared test environment, using **Default Domain** "avayalab.com". To enable calls with Verizon IP Trunk to be distinguished from other types of SIP calls using the same Session Manager, TCP port 5062 was added, with **Default Domain** "avayalab.com". Click the **Add** button to configure a new port. TCP was used in the sample configuration for improved visibility during testing.


Port
TCP Failover port: 5060
TLS Failover port: 5061
Add
Remove
3 Items | Refresh
Filter: Enable
Port
Protocol
Default Domain
Notes
5060
TCP
avayalab.com
5062
TCP
avayalab.com
Verizon IPT testing
5063
TCP
adevc.avaya.globalipcom.com
Verizon IPCC testing
Select : All, None

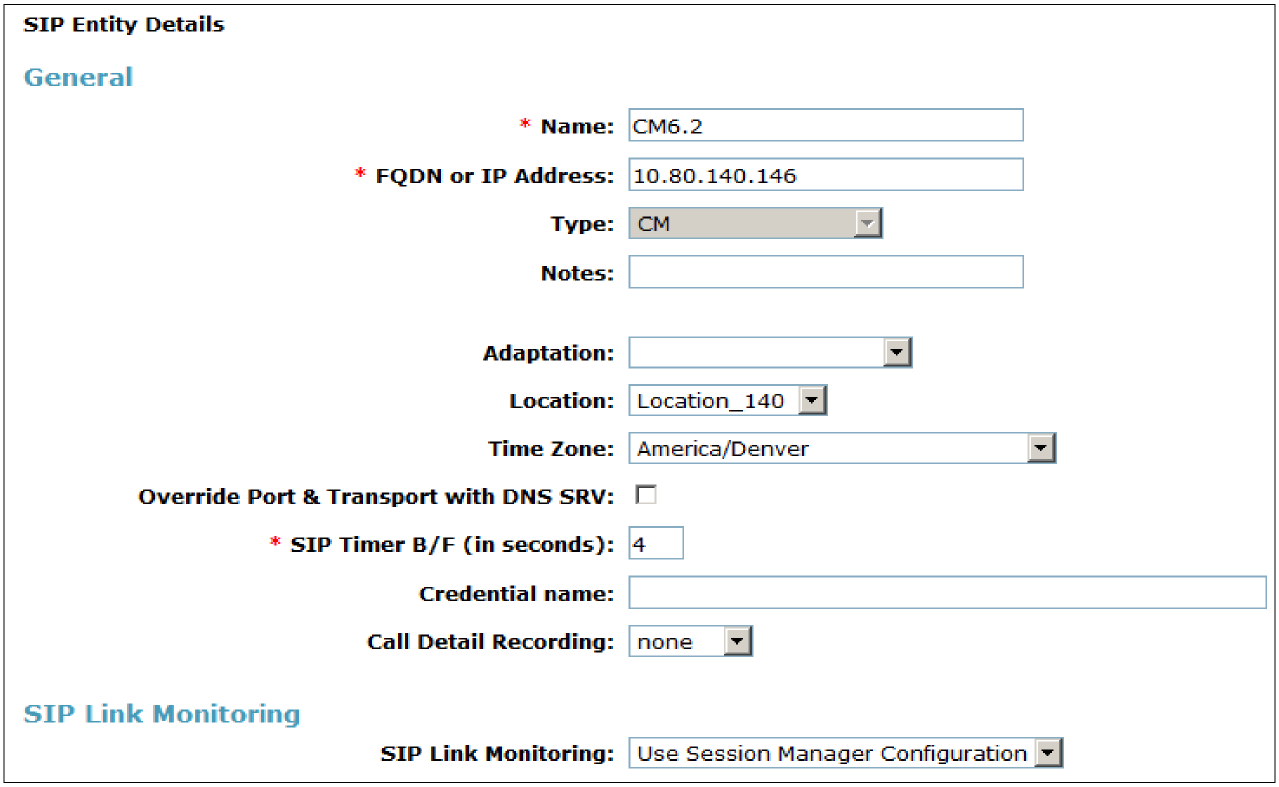
The following screen shows the upper portion of the **SIP Entity Details** corresponding to "Avaya-SBCE-1". The **FQDN or IP Address** field is configured with the ASBCE inside IP Address (10.80.140.141). "Other" is selected from the **Type** drop-down menu for ASBCE SIP Entities. This ASBCE has been assigned to **Location** "Avaya-SBCE-1", and the "History_Diversion_IPT" adapter is applied. Other parameters (not shown) retain default values.



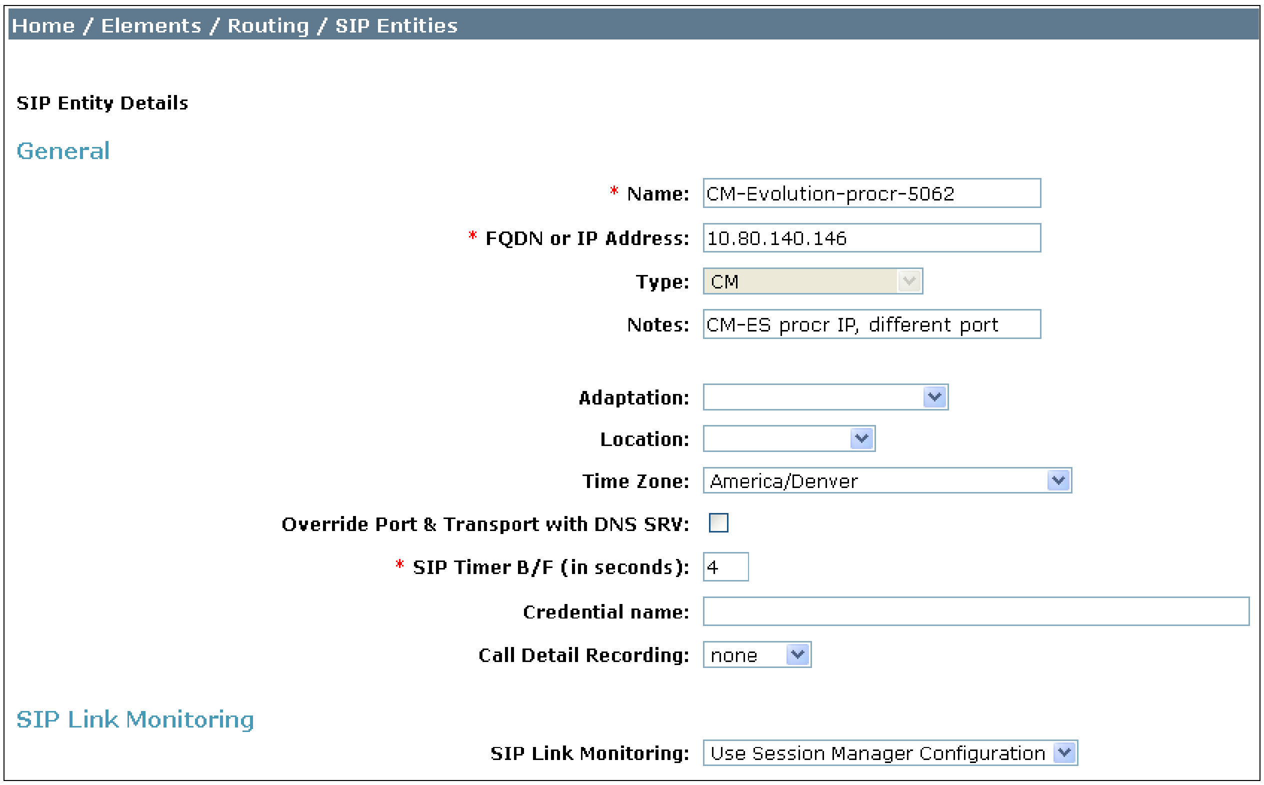
The following screen shows the upper portion of the **SIP Entity Details** corresponding to "Avaya-SBCE-2". The **FQDN or IP Address** field is configured with the ASBCE inside IP Address (10.80.140.200). "Other" is selected from the **Type** drop-down menu for ASBCE SIP Entities. This ASBCE has been assigned to **Location** "Avaya-SBCE-2", and the "History_Diversion_IPT" adapter is applied. Other parameters (not shown) retain default values.



The following screen shows a portion of the **SIP Entity Details** corresponding to a Communication Manager SIP Entity named “CM6.2” This is the SIP Entity that was already in place in the shared Avaya Interoperability Test Lab environment, prior to adding the Verizon IP Trunk configuration. The **FQDN or IP Address** field contains the IP Address of the “processor Ethernet” (10.80.140.146). In systems with Avaya G650 Media Gateways containing C-LAN cards, C-LAN cards may also be used as SIP entities, instead of, or in addition to, the “processor Ethernet”. “CM” is selected from the **Type** drop-down menu.



The following screen shows the **SIP Entity Details** for an entity named "CM-Evolution-procr-5062". This entity uses the same **FQDN or IP Address** (10.80.140.146) as the prior entity with name "CM6.2"; both correspond to Communication Manager Processor Ethernet IP Address. Later, a unique port, 5062, will be used for the Entity Link to "CM-Evolution-procr-5062". Using a different port is one approach that will allow Communication Manager to distinguish traffic originally from Verizon IP Trunk from other SIP traffic arriving from the same IP Address of the Session Manager, such as SIP traffic associated with SIP Telephones or other SIP-integrated applications. If desired, a location can be assigned if location-based routing criteria will be used.

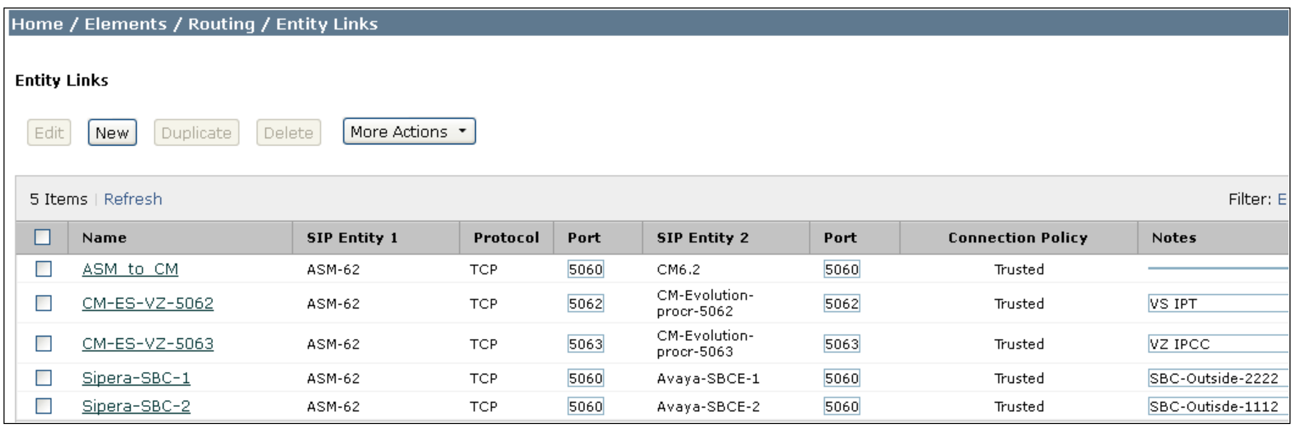


6.5. Entity Links

To view or change Entity Links, select **Routing → Entity Links**. Click on the checkbox corresponding to the name of a link and **Edit** to edit an existing link, or the **New** button to add a link. Click the **Commit** button after changes are completed.

Note – In the Entity Link configurations below (and in Communication Manager SIP trunk configuration), TCP was selected as the transport protocol for the CPE in the sample configuration. TCP was used to facilitate trace analysis during network verification. TLS may be used between Communication Manager and Session Manager in customer deployments.

The following screen shows a list of configured links. In the screen below, the links named "Sipera-SBC-1" , "Sipera-SBC-2" and "CM-ES-VZ-5062" are most relevant to these Application Notes. Each link uses the entity named "ASM-62" as **SIP Entity 1**, and the appropriate entity, such as "Avaya-SBCE-1", for **SIP Entity 2**. Note that there are multiple SIP Entity Links, using different TCP ports, linking the same "ASM-62" with the processor Ethernet of Communication Manager. For example, for one link, named "ASM_to_CM", both entities use TCP and port 5060. For the entity link used by Verizon IP Trunk named "CM-ES-VZ-5062", both entities use TCP and port 5062.



Home / Elements / Routing / Entity Links

Entity Links

Edit New Duplicate Delete More Actions

5 Items | Refresh Filter: E

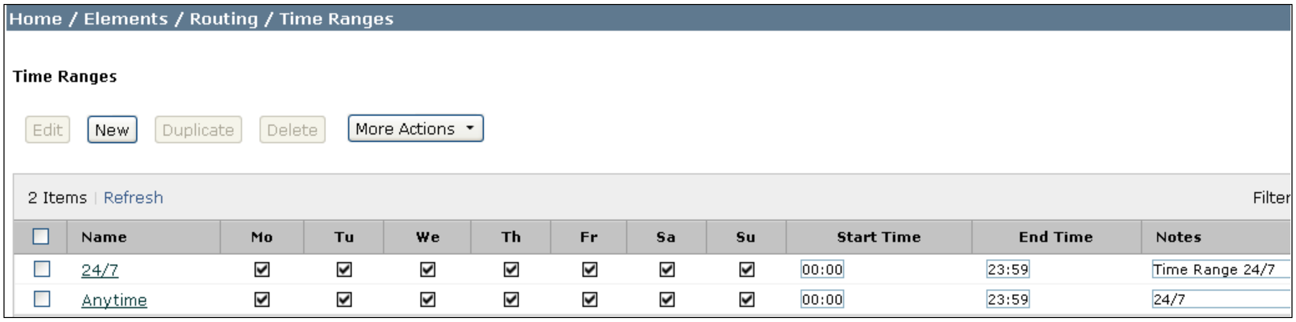
Name	SIP Entity 1	Protocol	Port	SIP Entity 2	Port	Connection Policy	Notes
ASM_to_CM	ASM-62	TCP	5060	CM6.2	5060	Trusted	
CM-ES-VZ-5062	ASM-62	TCP	5062	CM-Evolution-procr-5062	5062	Trusted	VS IPT
CM-ES-VZ-5063	ASM-62	TCP	5063	CM-Evolution-procr-5063	5063	Trusted	VZ IPCC
Sipera-SBC-1	ASM-62	TCP	5060	Avaya-SBCE-1	5060	Trusted	SBC-Outside-2222
Sipera-SBC-2	ASM-62	TCP	5060	Avaya-SBCE-2	5060	Trusted	SBC-Outisde-1112

The link named "ASM_to_CM" links Session Manager "ASM-62" with Communication Manager processor Ethernet. This link existed in the configuration prior to adding the Verizon IP Trunk related configuration. This link, using port 5060, can carry traffic between Session Manager and Communication Manager that is not necessarily related to calls with Verizon, such as traffic related to SIP Telephones registered to Session Manager.

The link named "CM-ES-VZ-5062" also links Session Manager "ASM-62" with Communication Manager processor Ethernet. However, this link uses port 5062 for both entities in the link. This link was created to allow Communication Manager to distinguish calls from Verizon IP Trunk from other calls that arrive from the same Session Manager. Other methods of distinguishing traffic could be used, if desired.

6.6. Time Ranges

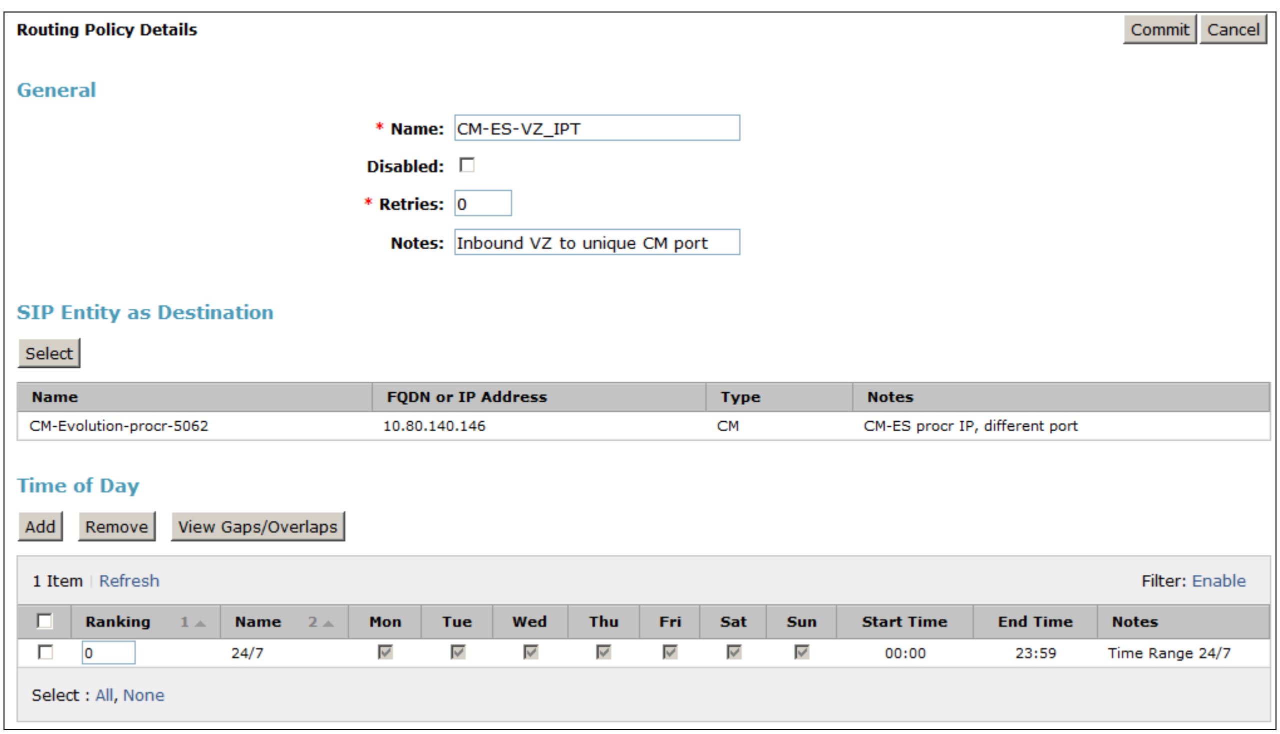
To view or change Time Ranges, select **Routing → Time Ranges**. The Routing Policies shown subsequently will use the "24/7" range since time-based routing was not the focus of these Application Notes. Click the **Commit** button (not shown) after changes are completed.



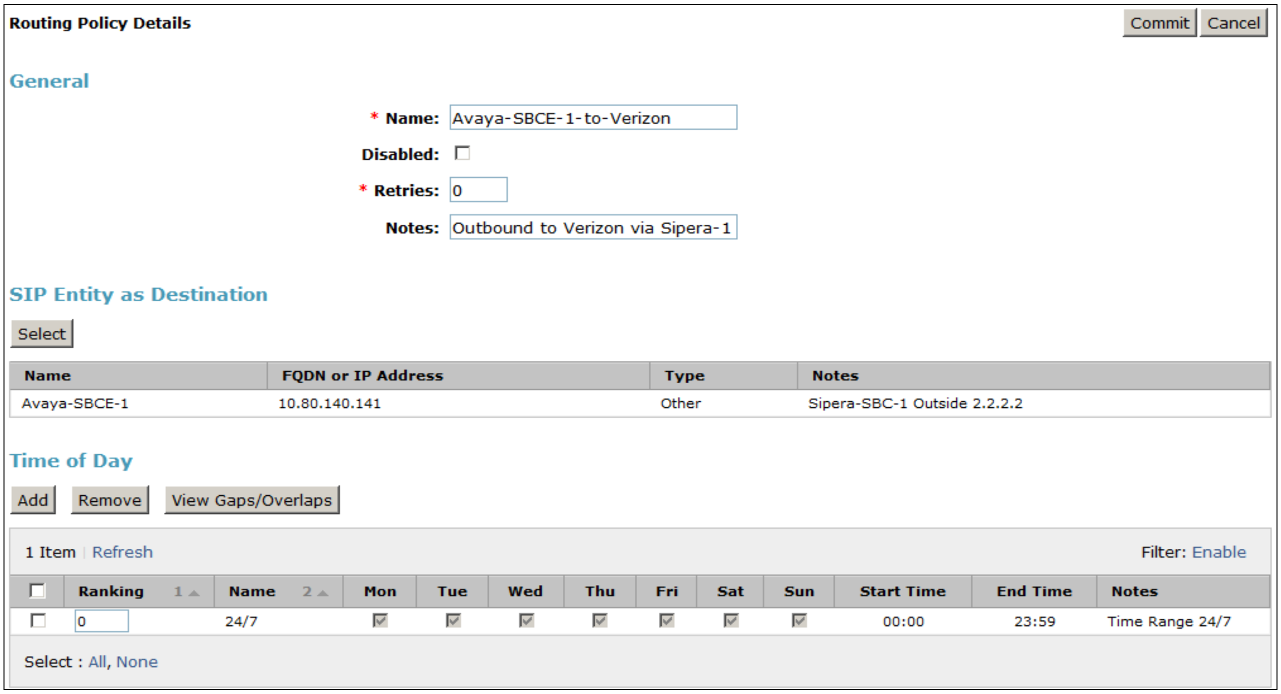
6.7. Routing Policies

To view or change routing policies, select **Routing → Policies**. Click on the checkbox corresponding to the name of a policy and **Edit** to edit an existing policy, or **New** to add a policy. Click the **Commit** button after changes are completed (not shown).

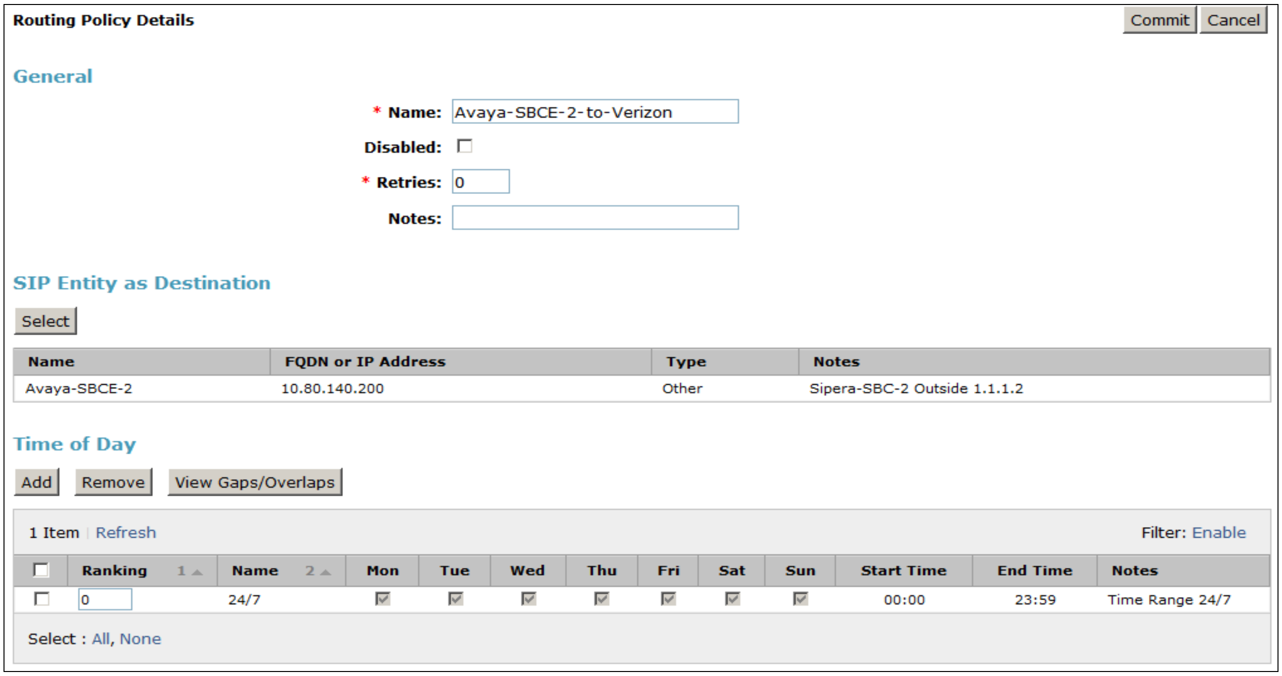
The following screen shows the **Routing Policy Details** for the policy named "CM-ES-VZ_IPT" associated with incoming toll-free calls from Verizon IP Trunk to Communication Manager. Observe the **SIP Entity as Destination** is the entity named "CM-Evolution-procr-5062" which uses Communication Manager processor Ethernet IP Address (10.80.140.146).



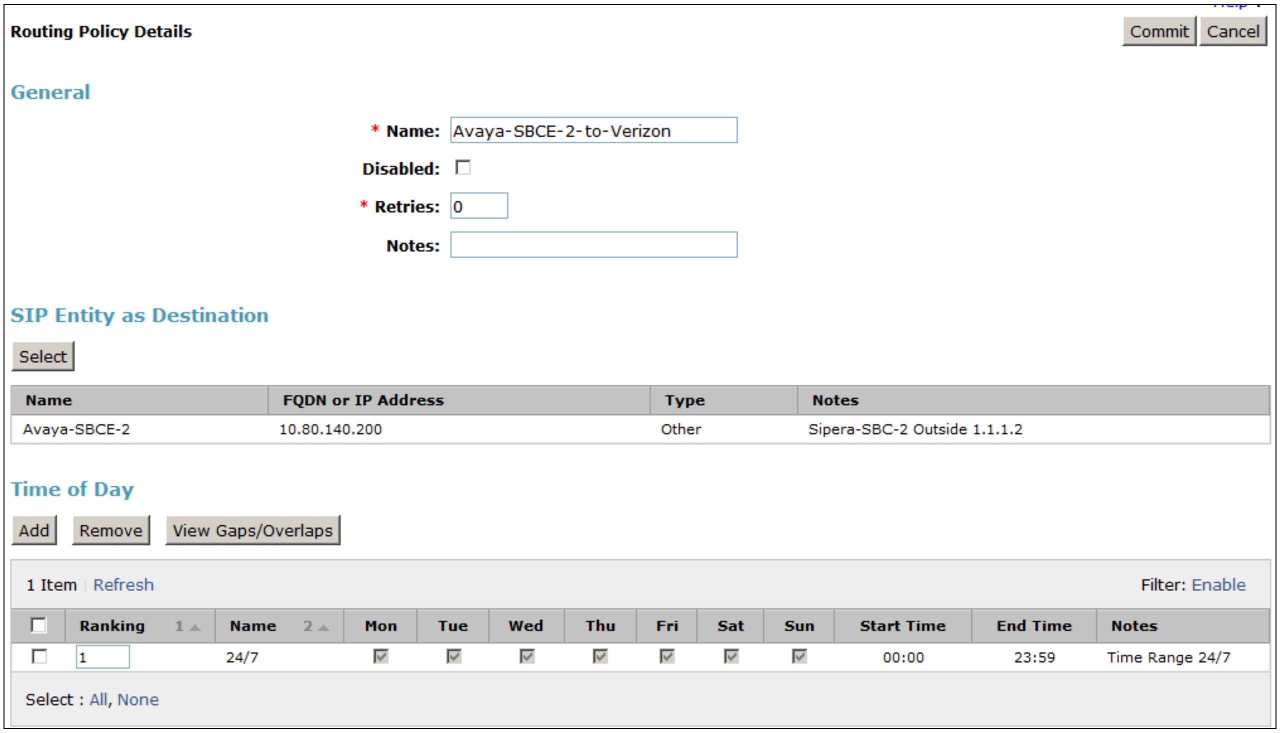
The following screen shows the **Routing Policy Details** for the policy named "Avaya-SBCE-1-to-Verizon" associated with outgoing calls from Communication Manager to the PSTN via Verizon through the ASBCE. Observe the **SIP Entity as Destination** as the entity named "Avaya-SBCE-1" that was created in Section 6.4.



The following screen shows the **Routing Policy Details** for the policy named "Avaya-SBCE-2-to-Verizon" associated with outgoing calls from Communication Manager to the PSTN via Verizon through the ASBCE. Observe the **SIP Entity as Destination** is the entity named "Avaya-SBCE-2". In the **Time of Day** area, note that a **Ranking** can be configured. To allow the "Avaya-SBCE-2" to receive calls from Session Manager even when the "Avaya-SBCE-1" is operational, the default rank of 0 (also assigned to "Avaya-SBCE-1") can be retained.



If it is intended that "Avaya-SBCE-1" should always be tried by Session Manager before "Avaya-SBCE-2", the rank of "Avaya-SBCE-2" can be changed to 1 as shown below. Both the "load sharing" approach where "Avaya-SBCE-1" and "Avaya-SBCE-2" use the same rank, and the strict rank order priority of "Avaya-SBCE-1" over "Avaya-SBCE-2" were successfully tested in the sample configuration.

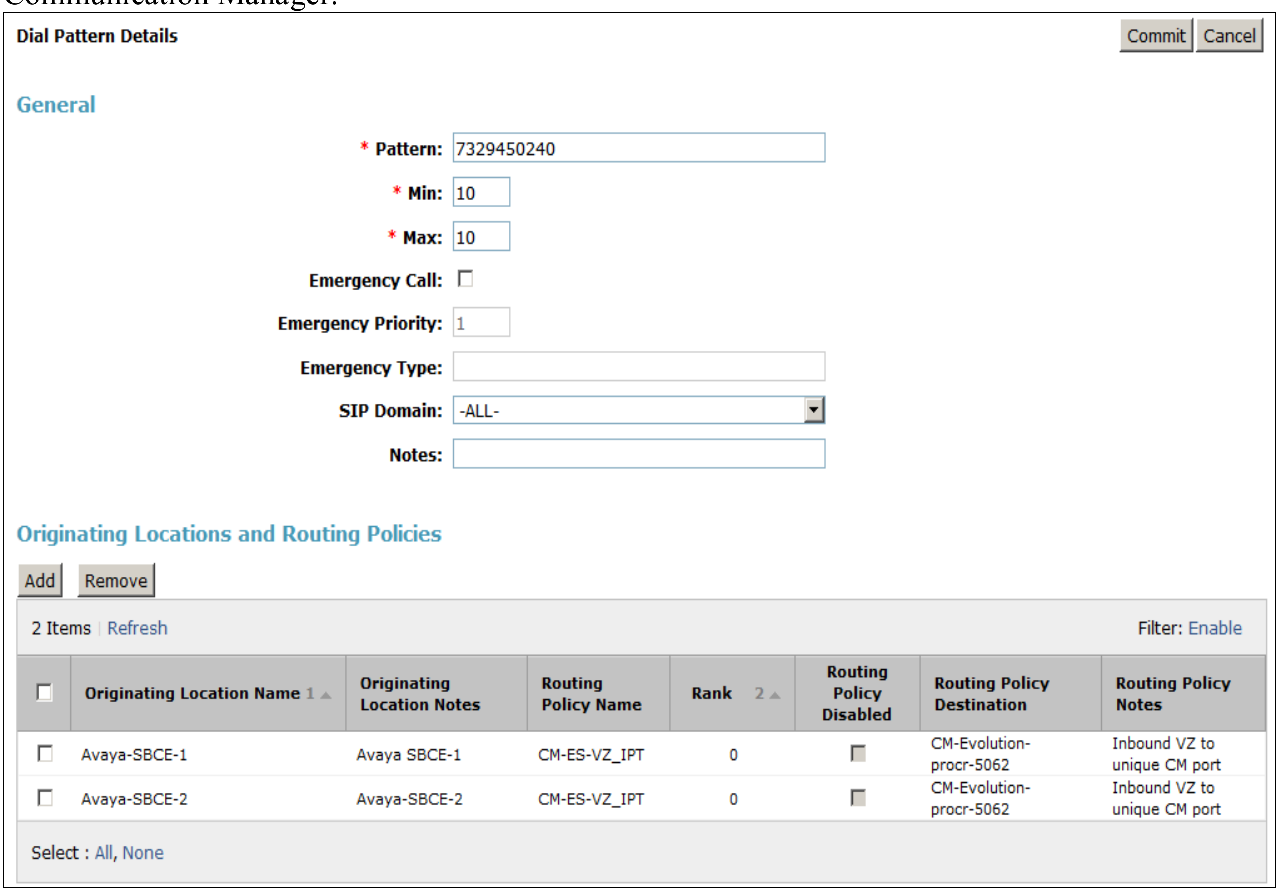


6.8. Dial Patterns

To view or change dial patterns, select **Routing → Dial Patterns**. Click on the checkbox corresponding to the name of a pattern and **Edit** to edit an existing pattern, or **New** to add a pattern. Click the **Commit** button after changes are completed.

6.8.1 Inbound Call Dial Pattern

The following screen illustrates an example dial pattern used to verify inbound PSTN calls to the enterprise. When a user on the PSTN dials a number assigned to the Verizon IP Trunk service, such as 732-945-0240, Verizon delivers the number to the enterprise, and the ASBCE sends the call to Session Manager. The pattern below matches on 732-945-0240 specifically. Dial patterns can alternatively match on ranges of numbers (e.g., a DID block). Under **Originating Locations and Routing Policies**, the routing policy named "CM-ES-VZ_IPT" is selected, which sends the call to Communication Manager using port 5062 as described previously. In the Avaya Interoperability Lab configuration, calls to this number from any of the two originating locations, including the one with **Originating Location Name** "Avaya-SBCE-1", are routed to Communication Manager.



6.8.2 Outbound Call Dial Pattern

The following screen illustrates an example dial pattern used to verify outbound calls from the enterprise to the PSTN. When a Communication Manager user dials a PSTN number such as 9-1-303-XXX-XXX, Communication Manager sends the call to Session Manager, via the HP Common Server Processor Ethernet. Session Manager will match the dial pattern shown below and send the call to the "Avaya-SBCE-1" or the "Avaya-SBCE-2" via the **Routing Policy Name** "Avaya-SBCE-1-to-Verizon"and "Avaya-SBCE-2-to-Verizon".

Dial Pattern Details Commit Cancel

General

* **Pattern:** 303

* **Min:** 10

* **Max:** 10

Emergency Call: ☐

Emergency Priority: 1

Emergency Type:

SIP Domain: -ALL-

Notes:

Originating Locations and Routing Policies

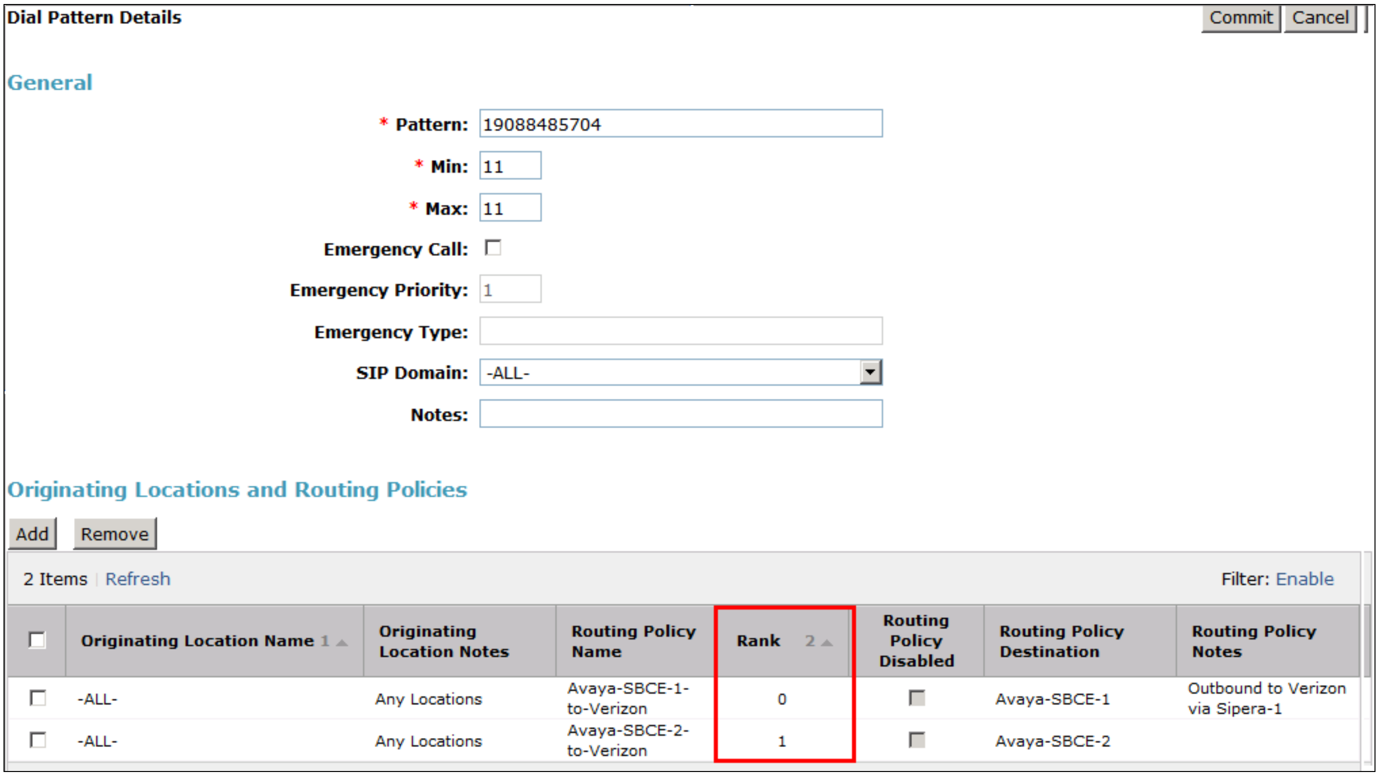
Add Remove

2 Items | Refresh Filter: Enable

☐	Originating Location Name 1	Originating Location Notes	Routing Policy Name	Rank 2	Routing Policy Disabled	Routing Policy Destination	Routing Policy Notes
☐	Location_140	Subnet 140	Avaya-SBCE-1-to-Verizon	0	☐	Avaya-SBCE-1	Outbound to Verizon via Sipera-1
☐	Location_140	Subnet 140	Avaya-SBCE-2-to-Verizon	0	☐	Avaya-SBCE-2	

Select : All, None

In the alternative screen shown below, the routing policy associated with the "Avaya-SBCE-2" for the number 19088485704, has a rank of 1. With this configuration, all calls will use "Avaya-SBCE-1" first, and only try "Avaya-SBCE-2" if the call attempt through "Avaya-SBCE-1" is unsuccessful. Session Manager can be configured to distribute the calls among the ASBCEs (same rank) or prefer one ASBCE over another (different ranks).



7. Avaya Session Border Controller for Enterprise

In the sample configuration, an ASBCE is used as the edge device between the CPE and Verizon Business.

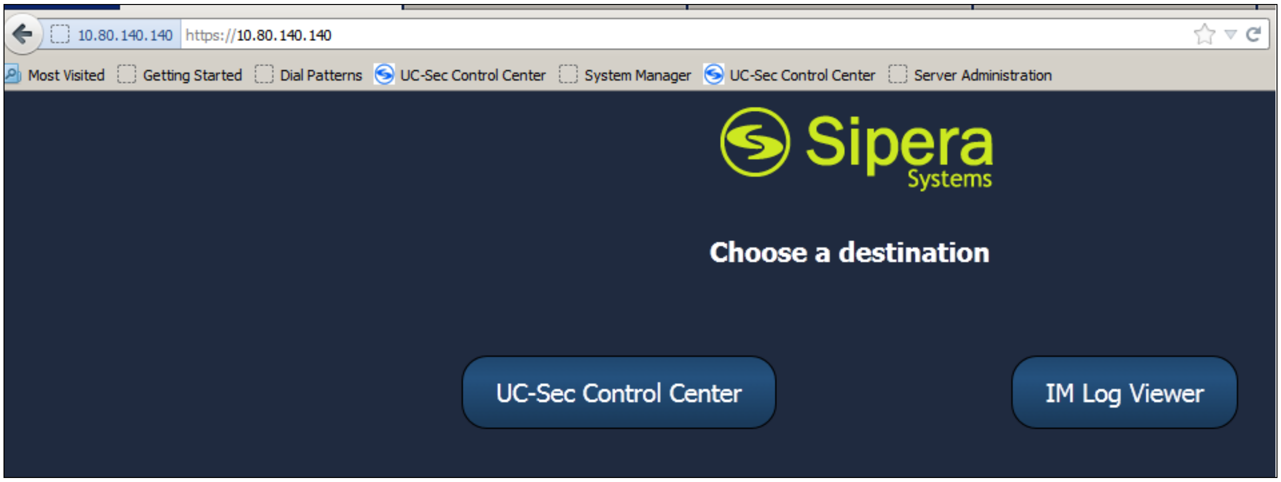
These Application Notes assume that the installation of the ASBCE and the assignment of a management IP Address have already been completed.

As described in **Section 1**, Verizon Business IP Trunking supports a redundant (2-CPE) architecture that provides for redundant SIP trunk access between the Verizon Business IP Trunk service offer and the SIP trunk architecture customer premises equipment (CPE). In the reference configuration two (ASBCEs) were used to provide the 2-CPE redundant access.

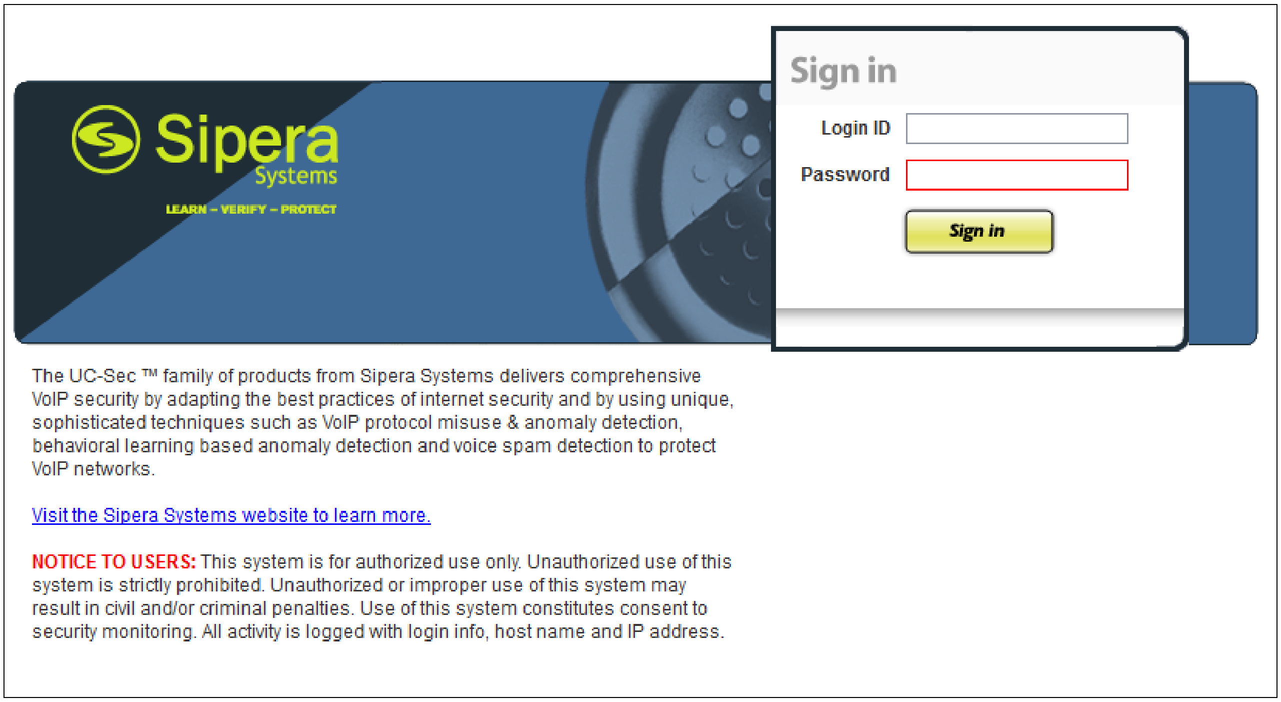
Note – The following Sections describe the provisioning of the Primary ASBCE. The configuration of the Secondary ASBCE is identical unless otherwise noted (e.g. IP addressing).

7.1. Access the Management Interface

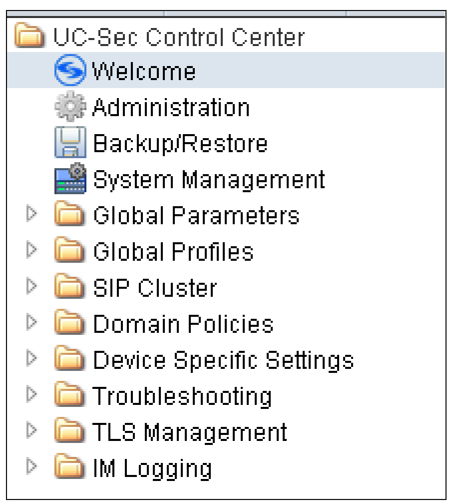
In the sample configuration, the management IP is 10.80.140.140. Access the web management interface by entering https://<ip-address> where <ip-address> is the management IP address assigned during installation. Select **UC-Sec Control Center**.


10.80.140.140
https://10.80.140.140
Most Visited
Getting Started
Dial Patterns
UC-Sec Control Center
System Manager
UC-Sec Control Center
Server Administration
Sipera
Systems
Choose a destination
UC-Sec Control Center
IM Log Viewer

A log in screen is presented. Enter an appropriate **Login ID** and **Password**.



Once logged in, a UC-Sec Control Center screen will be presented. The following image illustrates the menu items available on the left-side of the UC-Sec Control Center screen.

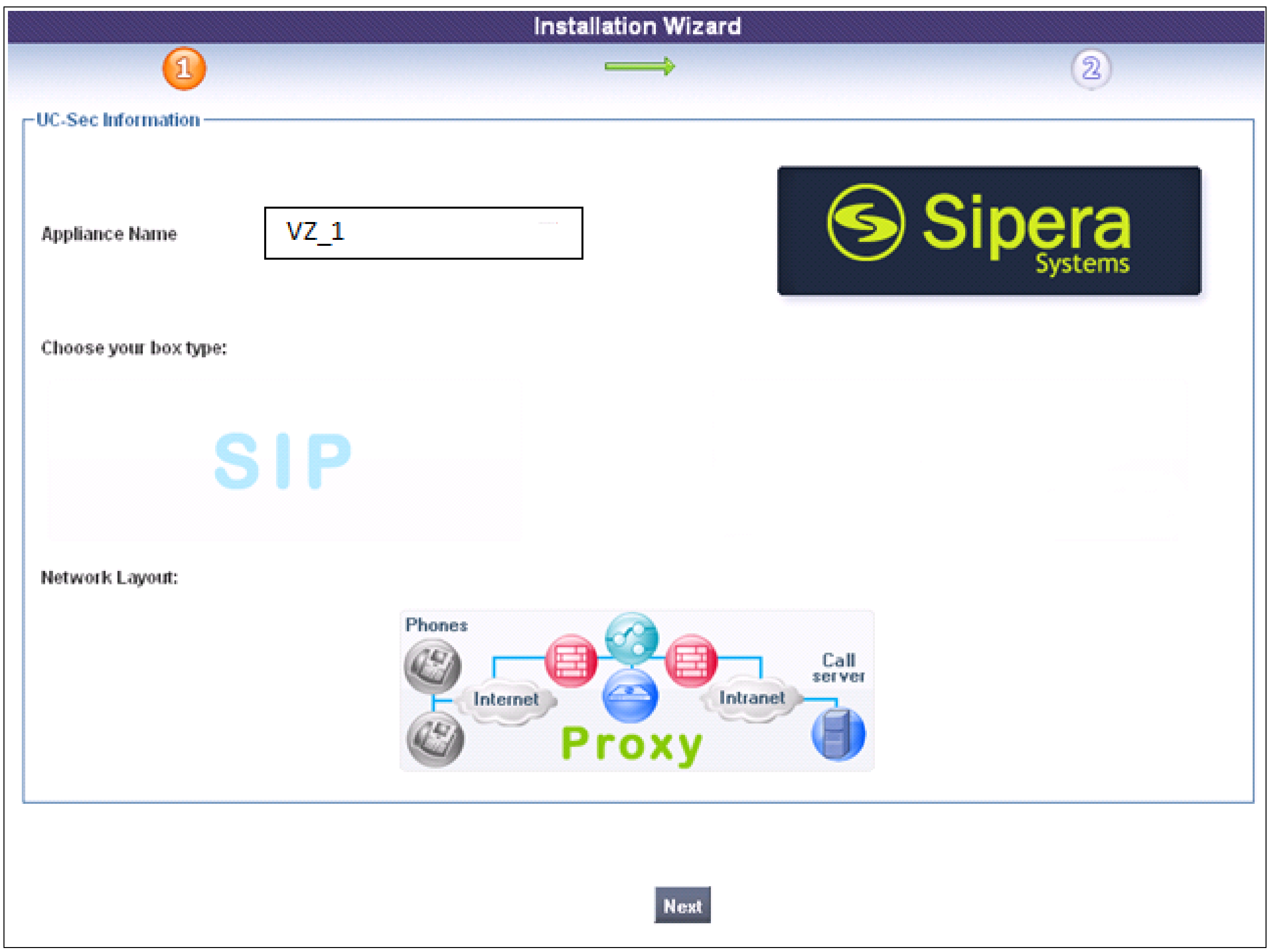


7.2. Commission the System

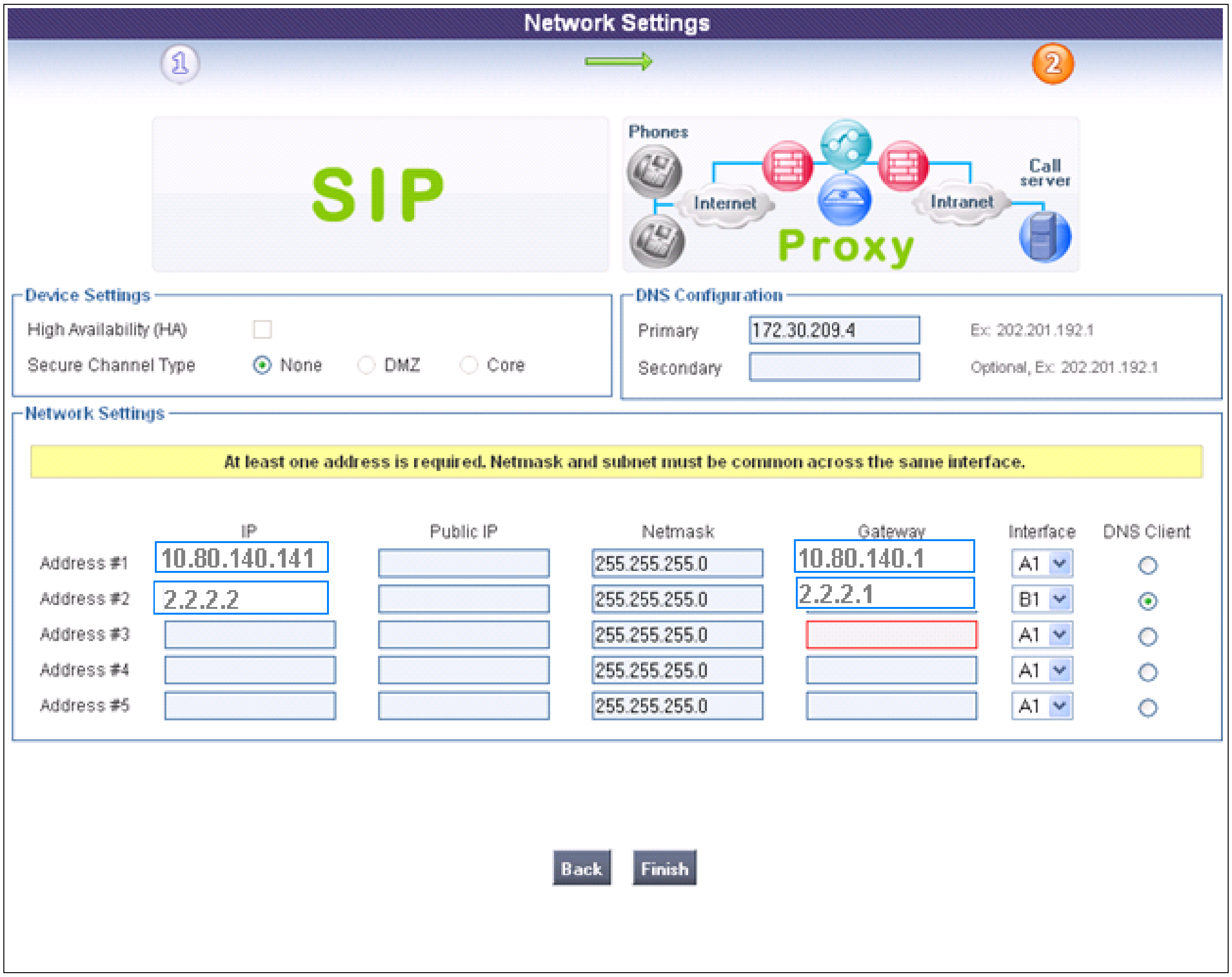
From the **UC-Sec Control Center** menu, select **System Management**.

If the system has not yet been "commissioned", a screen such as the following will appear. The **Status** will show "Registered". Run the installation wizard by clicking the icon.

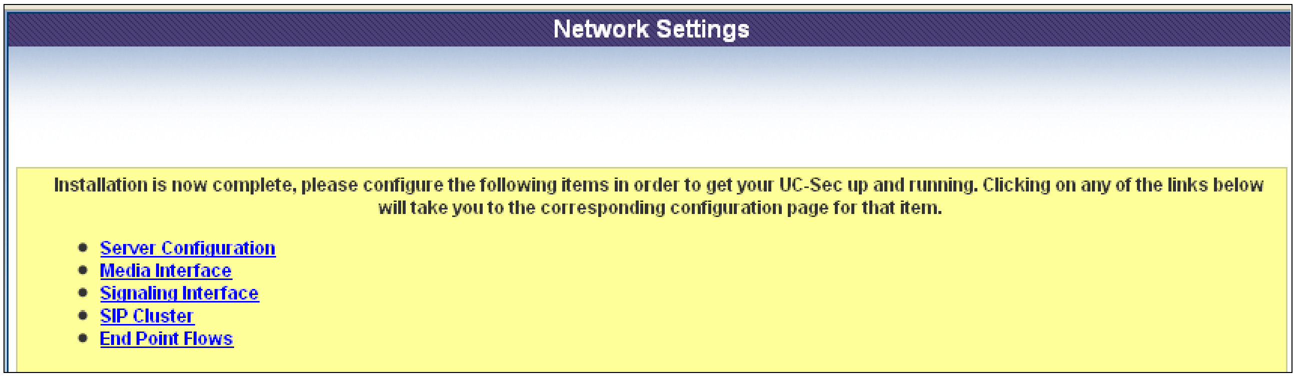
An installation wizard will appear. In the **Appliance Name** field, enter an appropriate name. In the sample configuration, "VZ_1" was entered. In the **Choose your box type** area, choose SIP. Click **Next**.



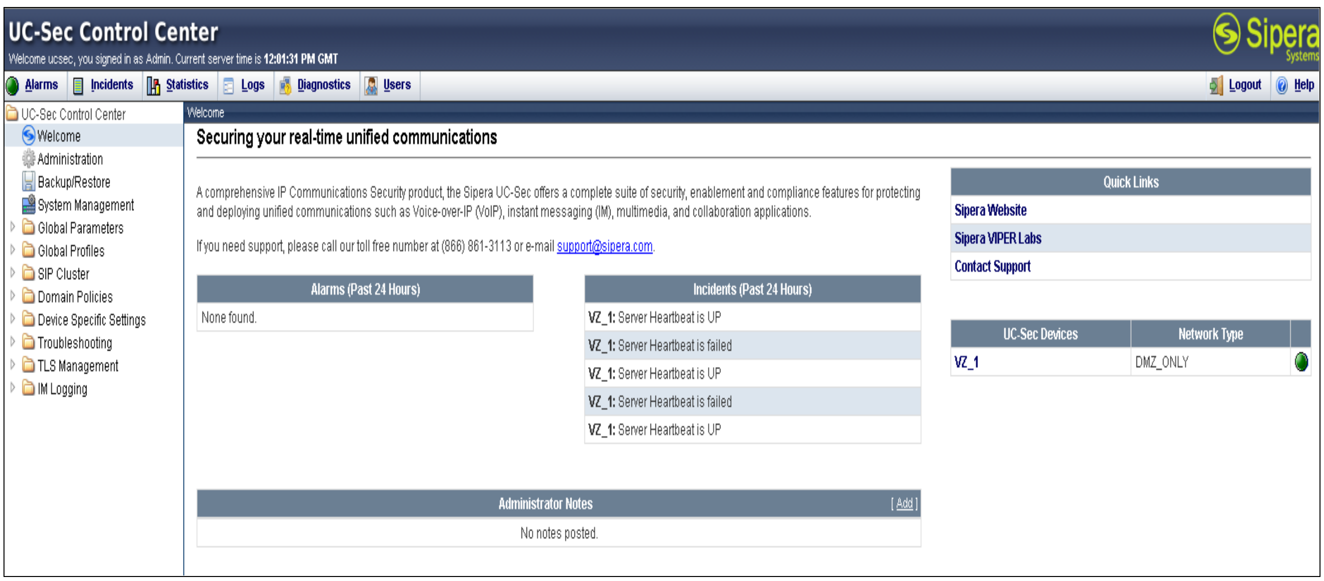
The following screen illustrates the **Network Settings** configured in the sample configuration. **Interface** A1 is the inside private interface, assigned IP Address 10.80.140.141, with **Gateway** 10.80.140.1. **Interface** B1 is the outside public interface, assigned IP Address 2.2.2.2, with **Gateway** 2.2.2.1. Note that 2.2.2.2 is the IP Address known to Verizon as the Avaya CPE IP Address. When appropriate network settings have been entered, click **Finish**.



After clicking **Finish (shown above)**, a screen such as the following will be displayed. The administrator may click the links such as **Server Configuration** to continue system configuration, or close the window to return to the UC-Sec Control Center Welcome Screen menu shown below.



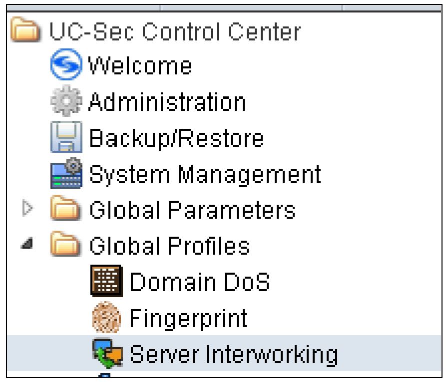
Welcome Screen:



Once the wizard has been completed, the **System Management** screen will show **Status** "Commissioned" as shown below.

7.3. Global Profiles – Server Interworking

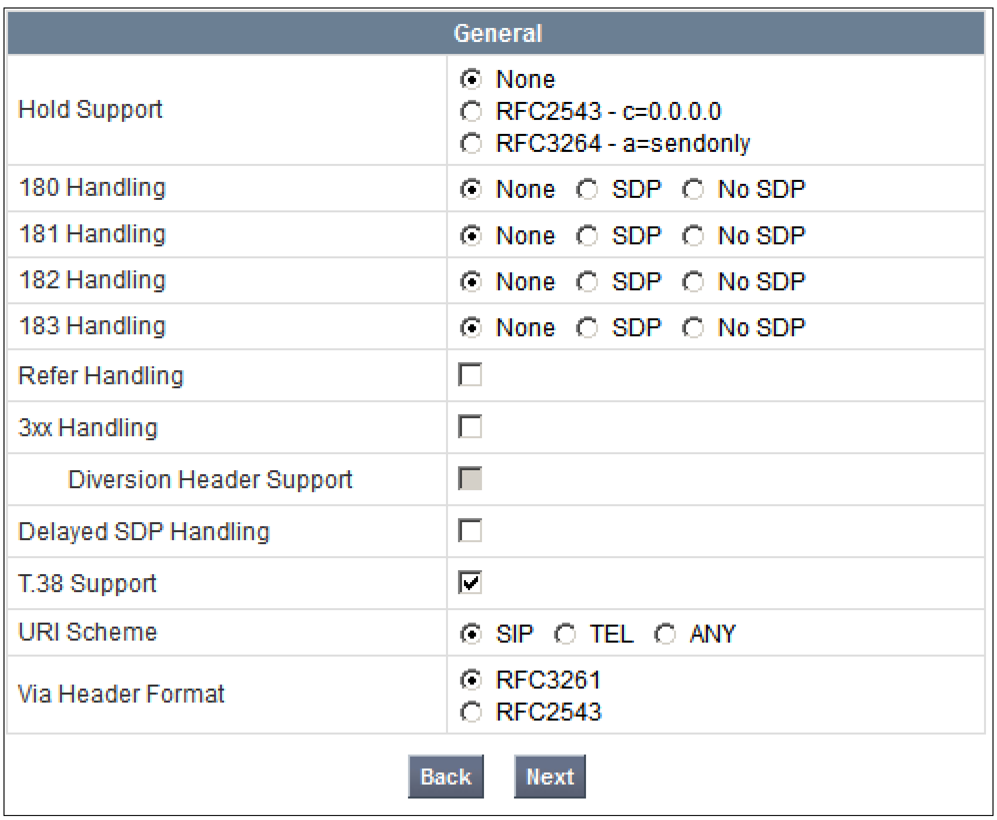
Select **Global Profiles → Server Interworking** from the left-side menu as shown below.


UC-Sec Control Center
Welcome
Administration
Backup/Restore
System Management
Global Parameters
Global Profiles
Domain DoS
Fingerprint
Server Interworking

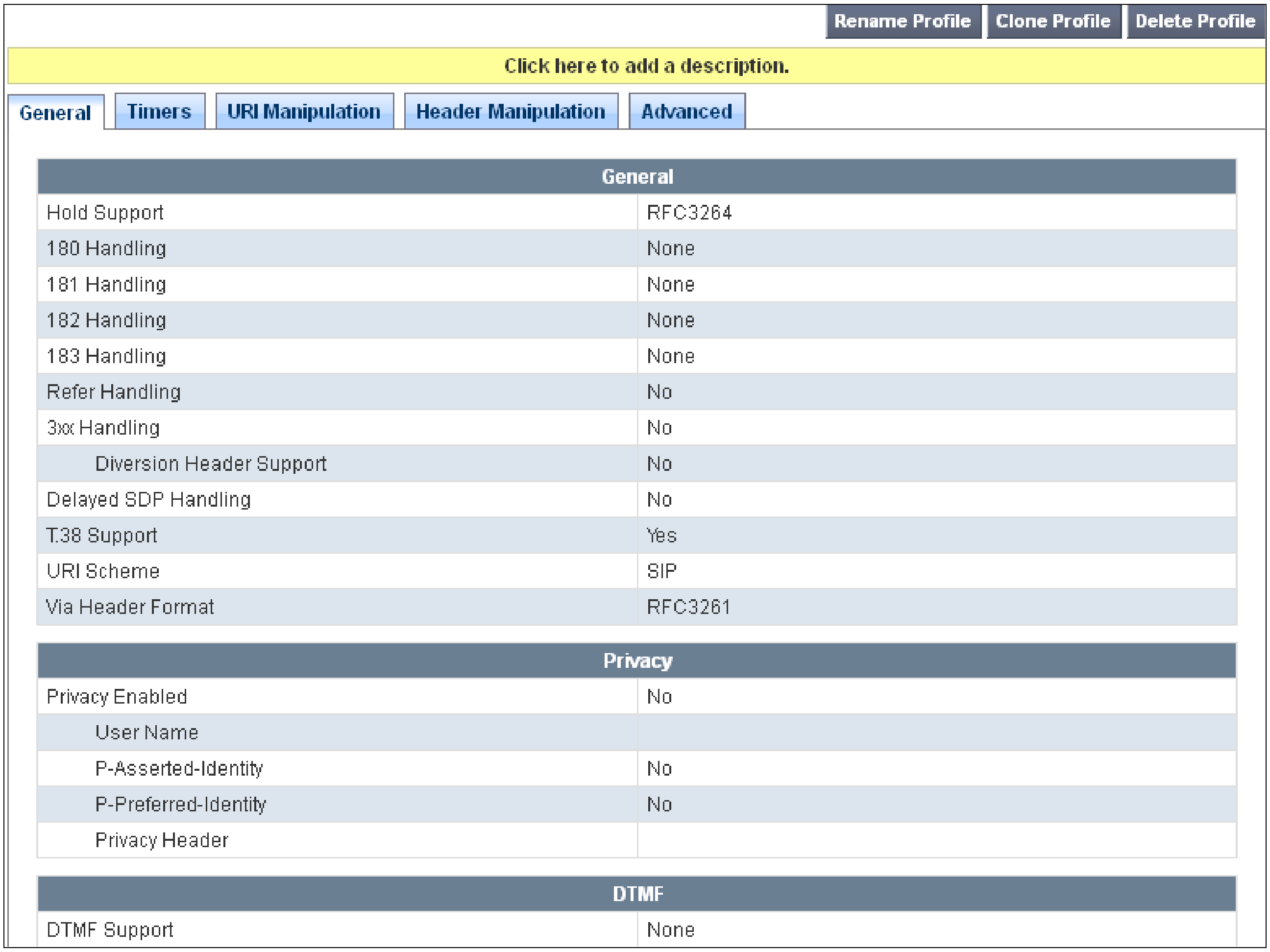
7.3.1 Server Interworking - Avaya

Click the **Add Profile** button (not shown) to add a new profile or select an existing interworking profile. If adding a profile, a screen such as the following is displayed. Enter an appropriate **Profile Name** such as "Avaya" shown below. Click **Next**.

The following screens illustrate the "General" parameters used in the sample configuration for the Interworking Profile named "Avaya". Most parameters retain default values. In the sample configuration, **T.38 support** was checked (optional), and **Hold Support** was set for RFC3261.

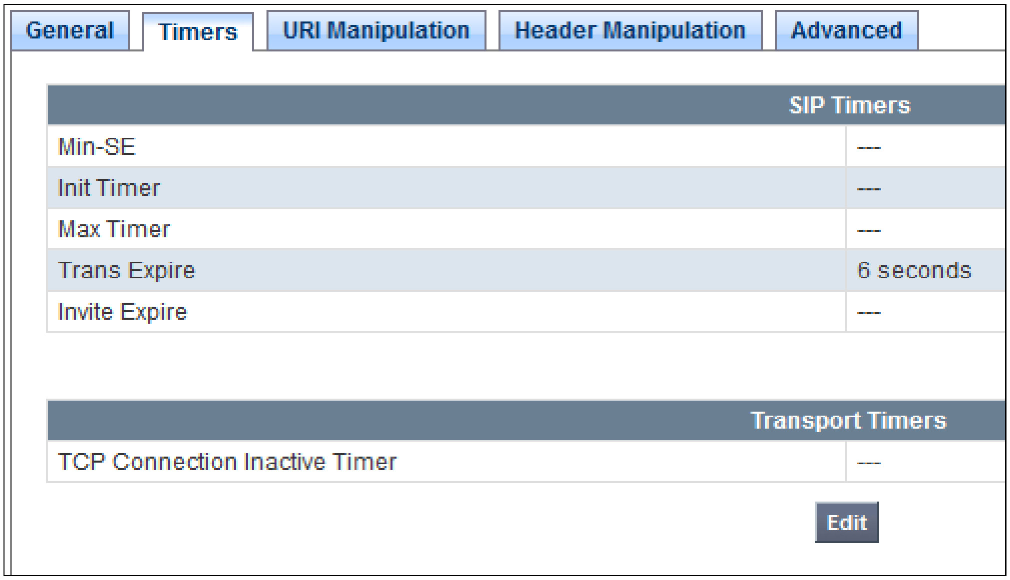


Click **Next** (not shown) to advance to configure Privacy and DTMF General parameters, which may retain default values. The following screen shows the complete **General** tab used in the sample configuration for interworking profile named “Avaya”.

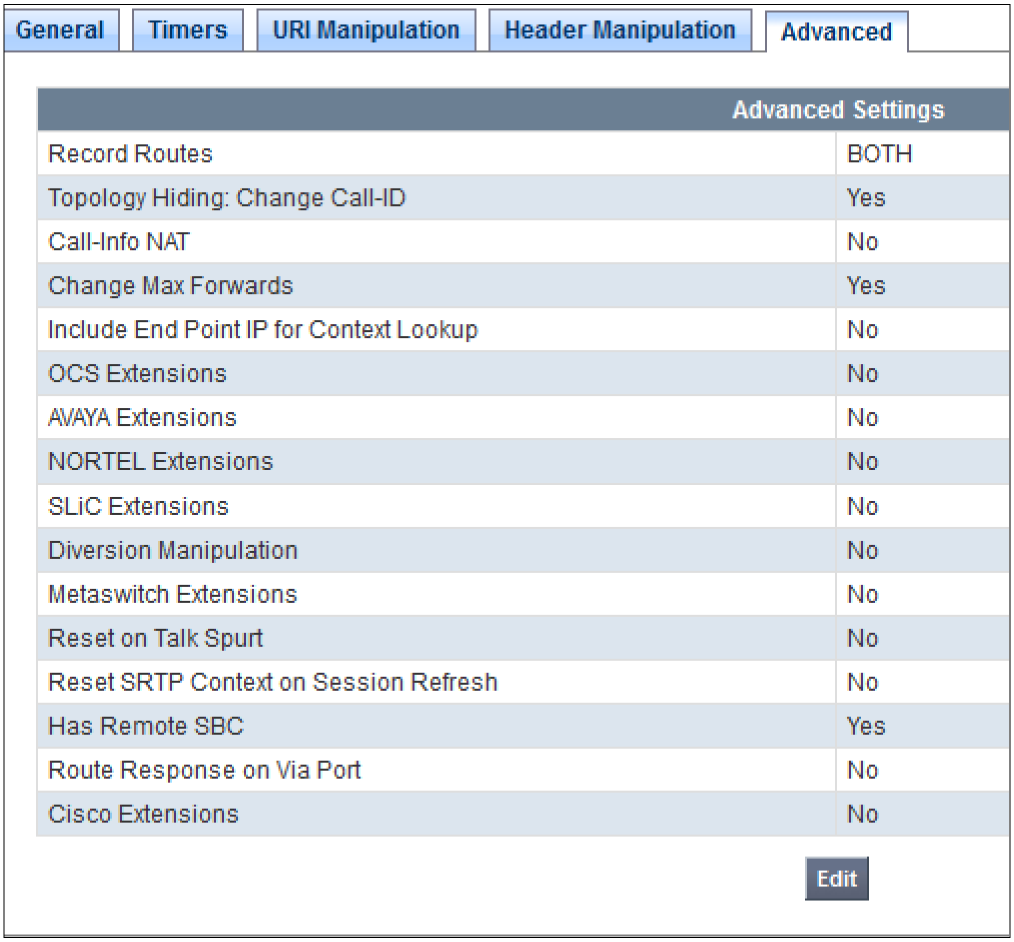


General	
Hold Support	RFC3264
180 Handling	None
181 Handling	None
182 Handling	None
183 Handling	None
Refer Handling	No
3xx Handling	No
Diversion Header Support	No
Delayed SDP Handling	No
T.38 Support	Yes
URI Scheme	SIP
Via Header Format	RFC3261
Privacy	
Privacy Enabled	No
User Name	
P-Asserted-Identity	No
P-Preferred-Identity	No
Privacy Header	
DTMF	
DTMF Support	None

The 2-CPE configuration requires the configuring of certain timers to assist in the failover process to happen smoothly. One of the timers is the **Trans Expire** timer. This timer is set to 6 seconds as shown below on the Avaya side only.



The following screen illustrates the **Advanced Settings** configuration. The "Topology Hiding: Change Call-ID" defaults to Yes, but was changed in the test configuration to allow for easier correlation of data. This value is set in the field at the discretion of the user. Both settings were tested. All other parameters shown are default values. Note that the default configuration will result in Record-Route headers in SIP messages.

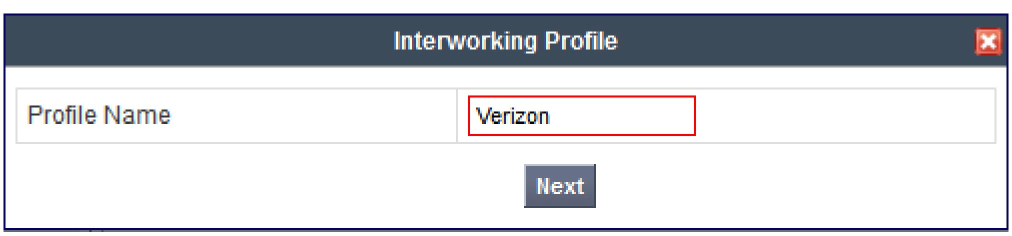


Advanced Settings	
Record Routes	BOTH
Topology Hiding: Change Call-ID	Yes
Call-Info NAT	No
Change Max Forwards	Yes
Include End Point IP for Context Lookup	No
OCS Extensions	No
AVAYA Extensions	No
NORTEL Extensions	No
SLiC Extensions	No
Diversion Manipulation	No
Metaswitch Extensions	No
Reset on Talk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

Edit

7.3.2 Server Interworking – Verizon IP Trunk

Click the **Add Profile** button (not shown) to add a new profile or select an existing interworking profile. If adding a profile, a screen such as the following is displayed. Enter an appropriate **Profile Name** such as "Verizon" shown below. Click **Next**.



The following screens illustrate the "General" parameters used in the sample configuration for the Interworking Profile named "Verizon". Most parameters retain default values. In the sample configuration, **T.38 support** was set to "Yes", **Hold Support** was set for RFC3261, and all other fields retained default values.

General | Timers | URI Manipulation | Header Manipulation | Advanced

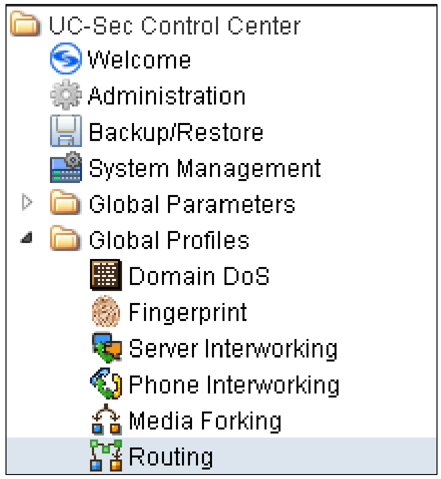
	General
Hold Support	RFC3264
180 Handling	None
181 Handling	None
182 Handling	None
183 Handling	None
Refer Handling	No
3xx Handling	No
Diversion Header Support	No
Delayed SDP Handling	No
T.38 Support	Yes
URI Scheme	SIP
Via Header Format	RFC3261
	Privacy
Privacy Enabled	No
User Name	
P-Asserted-Identity	No
P-Preferred-Identity	No
Privacy Header	
	DTMF
DTMF Support	None

Edit

The following screen illustrates the **Advanced Settings** configuration. All parameters shown are default values. Note that the default configuration will result in Record-Route headers in SIP messages.

7.4. Global Profiles – Routing

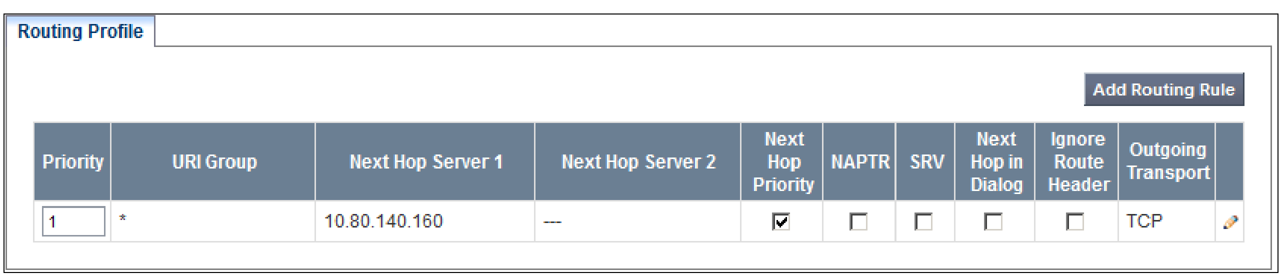
Select **Global Profiles → Routing** from the left-side menu as shown below.



7.4.1 Routing Configuration for Session Manager

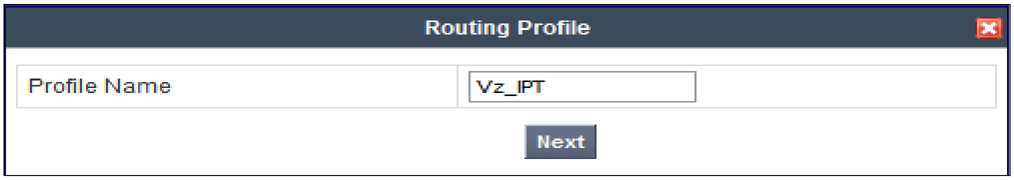
Click the **Add Profile** button (not shown) to add a new profile, or select an existing routing profile to edit. If adding a profile, a screen such as the following is displayed. Enter a **Profile Name** such as "To_Avaya" shown below. Click **Next**.

For the **Next Hop Routing**, enter the IP Address of the Session Manager SIP signaling interface as **Next Hop Server 1**, as shown below. Check **Next Hop Priority**. Choose **TCP** for **Outgoing Transport**. Then click **Finish**.

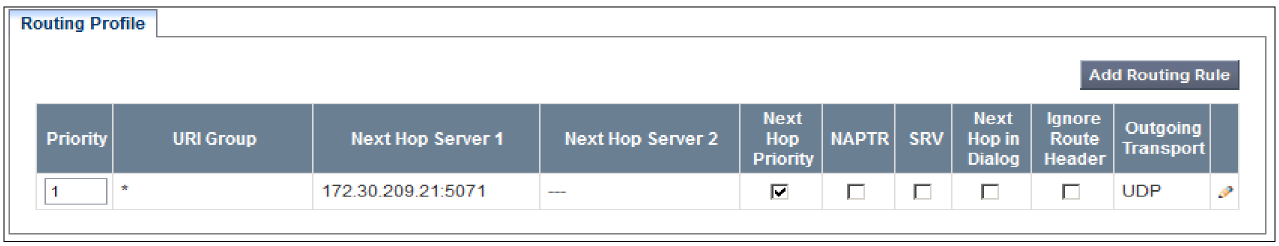


7.4.2 Routing Configuration for Verizon IP Trunk

Click the **Add Profile** button (not shown) to add a new profile, or select an existing routing profile to edit. If adding a profile, a screen such as the following is displayed. Enter a **Profile Name** such as "Vz_IPT" shown below. Click **Next**.



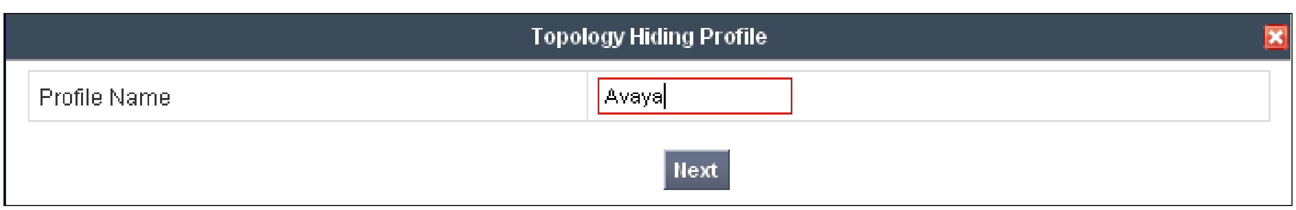
For the **Next Hop Routing**, enter the IP Address of the Verizon SIP signaling interface as **Next Hop Server 1**, as shown below. Check **Next Hop Priority**. Choose **UDP** for **Outgoing Transport**, then click **Finish (not shown)**.



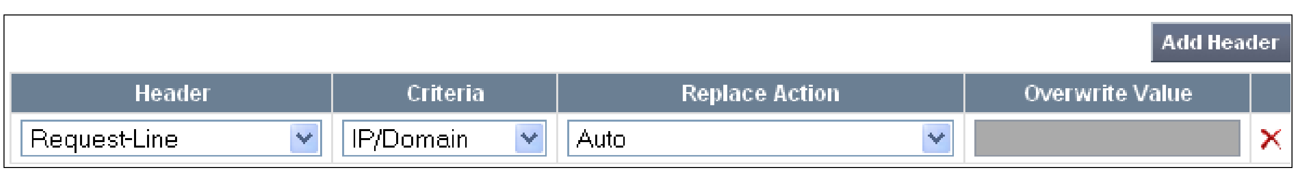
7.4.3 Topology Hiding for Session Manager

The Topology Hiding profile manages how various source, destination and routing information in SIP and SDP message headers are substituted or changed to maintain the integrity of the network. It hides the topology of the enterprise network from external networks.

Click the **Add Profile** button (not shown) to add a new profile, or select an existing topology hiding profile to edit. If adding a profile, a screen such as the following is displayed. Enter a **Profile Name** such as "Avaya" shown below. Click **Next**.



In the resultant screen, click the **Add Header** button in the upper right multiple times to reveal additional headers.



In the Replace Action column an action of "Auto" will replace the header field with the IP address of the Sipera interface and the Overwrite will use the value in the "Overwrite Value". In the example shown, this profile will later be applied in the direction of the Session Manager and "Overwrite" has been selected for the To/From and Request-Line headers and the shared interop lab domain of "avayalab.com" has been inserted. This action can also be done in the Session Manager in the Adaptations section. Click **Finish**.

Edit Topology Hiding Profile

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

Finish

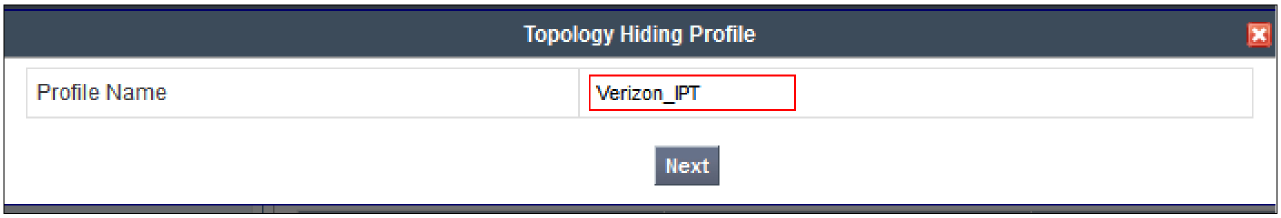
After configuration is completed, the Topology Hiding for profile "Avaya" will appear as follows.

Topology Hiding

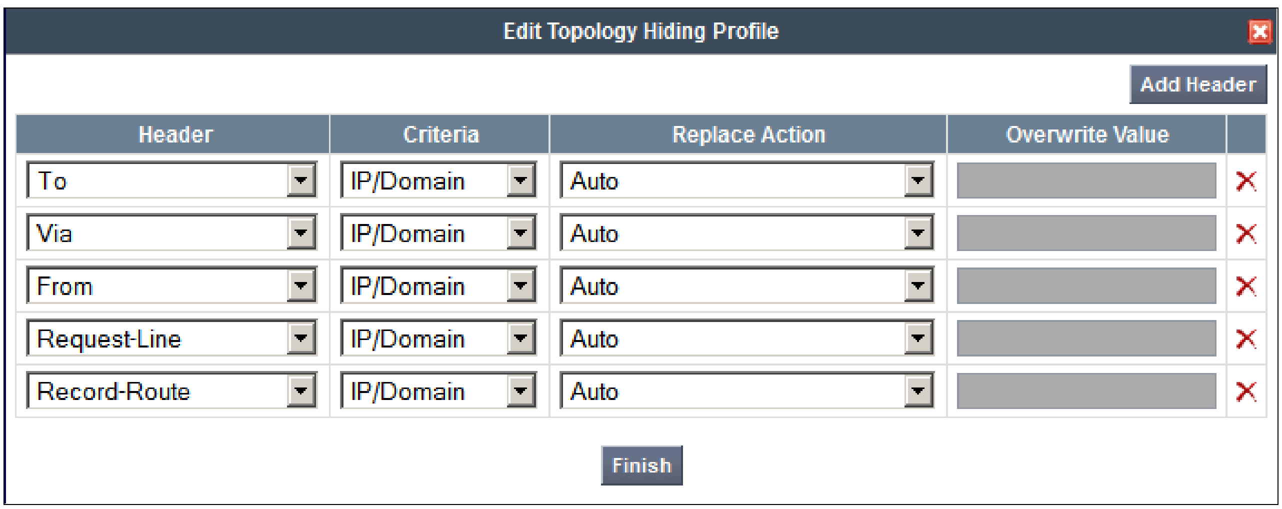
Header	Criteria	Replace Action	Overwrite Value
To	IP/Domain	Overwrite	avayalab.com
Via	IP/Domain	Auto	---
From	IP/Domain	Overwrite	avayalab.com
Request-Line	IP/Domain	Overwrite	avayalab.com
SDP	IP/Domain	Auto	---
Record-Route	IP/Domain	Auto	---

7.4.4 Topology Hiding for Verizon IP Trunk

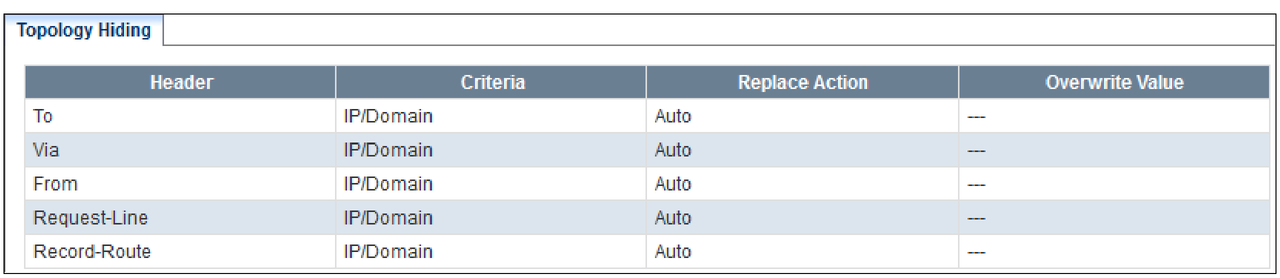
Click the **Add Profile** button (not shown) to add a new profile, or select an existing topology hiding profile to edit. If adding a profile, a screen such as the following is displayed. Enter a **Profile Name** such as "Verizon_IPT" shown below. Click **Next**.



Again, in the resultant screen, click the **Add Header** button in the upper right multiple times to reveal additional headers. The default "Auto" behaviors are sufficient. Click **Finish.**



After configuration is completed, the **Topology Hiding** for profile "Verizon_IPT" will appear as follows.

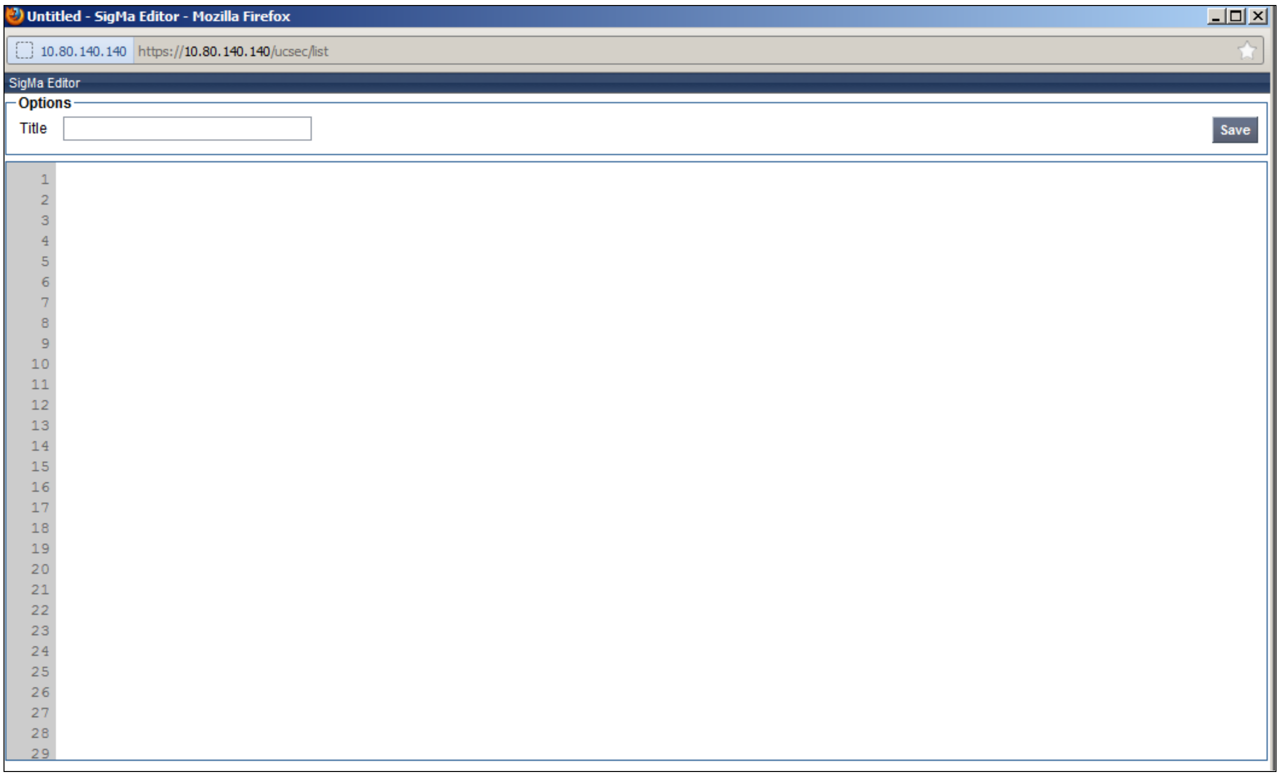

Topology Hiding

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

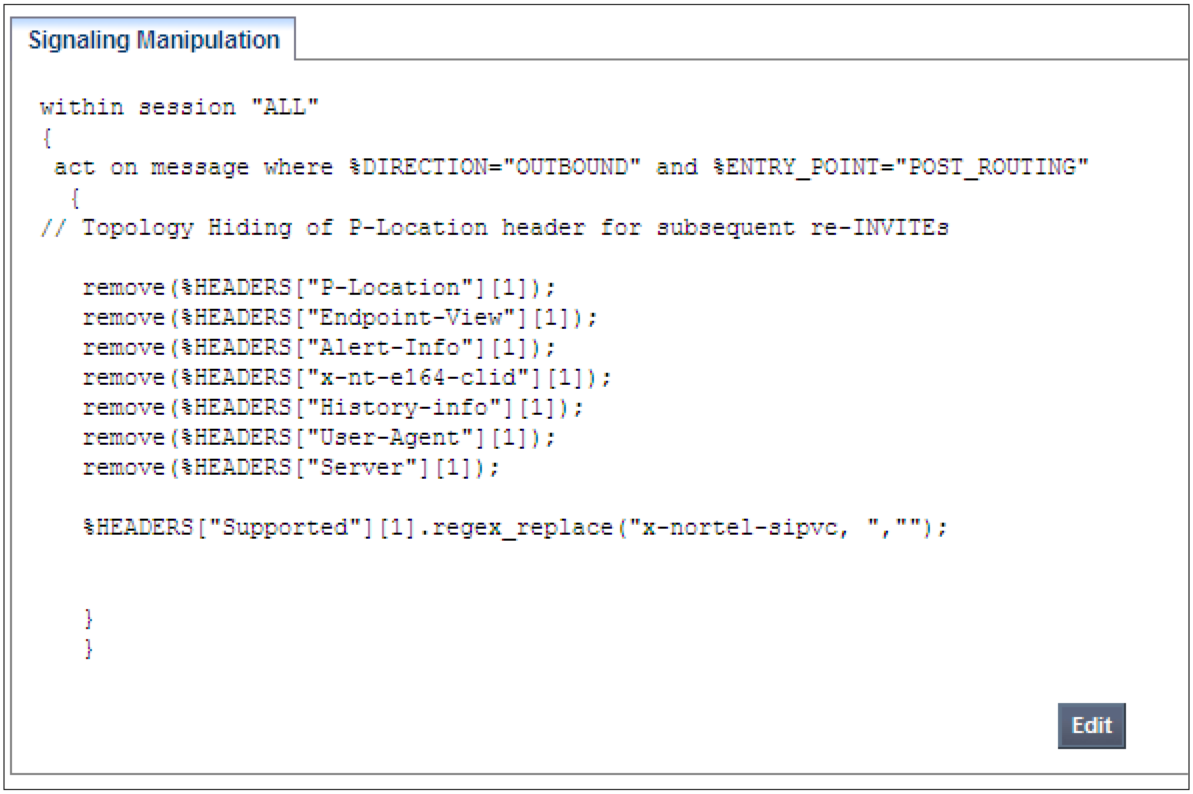
7.4.5 Signaling Manipulation

This feature adds the ability to add, change and delete any of the headers and other information in a SIP message on each flow in a highly flexible manner using a proprietary scripting language.

Click the **Add Script** button (not shown) to add a new script, or select an existing script to edit. If adding a script, a screen such as the following is displayed. Enter a title in the upper left and then enter the text to manipulate headers and click **Save**.



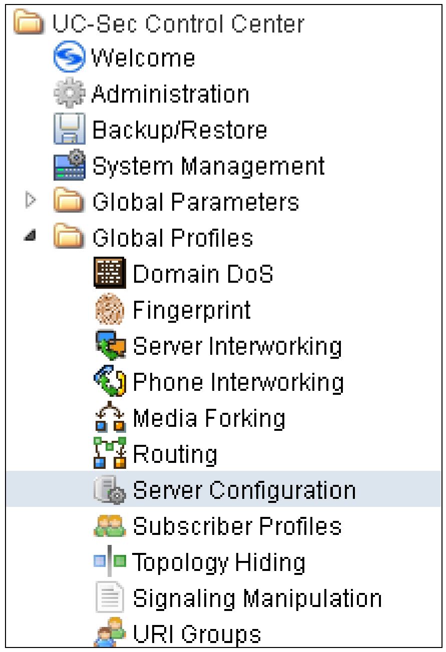
In Communication Manager and Session Manager 6.2, there are two proprietary headers (P-Location and Endpoint-View) and one standard header (Alert-Info) that contain internal information and that are not applicable to a service provider that need to be stripped. These headers were stripped with a Sigma script and applied in the server configuration section. The script “Example2”is shown here. This script will be applied in the next section, ‘Server Configuration’.




```
within session "ALL"
{
 act on message where %DIRECTION="OUTBOUND" and %ENTRY_POINT="POST_ROUTING"
  {
// Topology Hiding of P-Location header for subsequent re-INVITEs

   remove(%HEADERS["P-Location"][1]);
   remove(%HEADERS["Endpoint-View"][1]);
   remove(%HEADERS["Alert-Info"][1]);
   remove(%HEADERS["x-nt-e164-clid"][1]);
   remove(%HEADERS["History-info"][1]);
   remove(%HEADERS["User-Agent"][1]);
   remove(%HEADERS["Server"][1]);

   %HEADERS["Supported"][1].regex_replace("x-nortel-sipvc, ","");


   }
   }
```

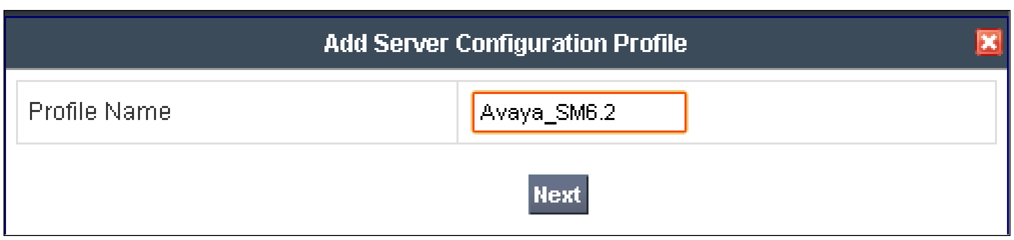
7.5. Global Profiles – Server Configuration

Select **Global Profiles → Server Configuration** from the left-side menu as shown below.

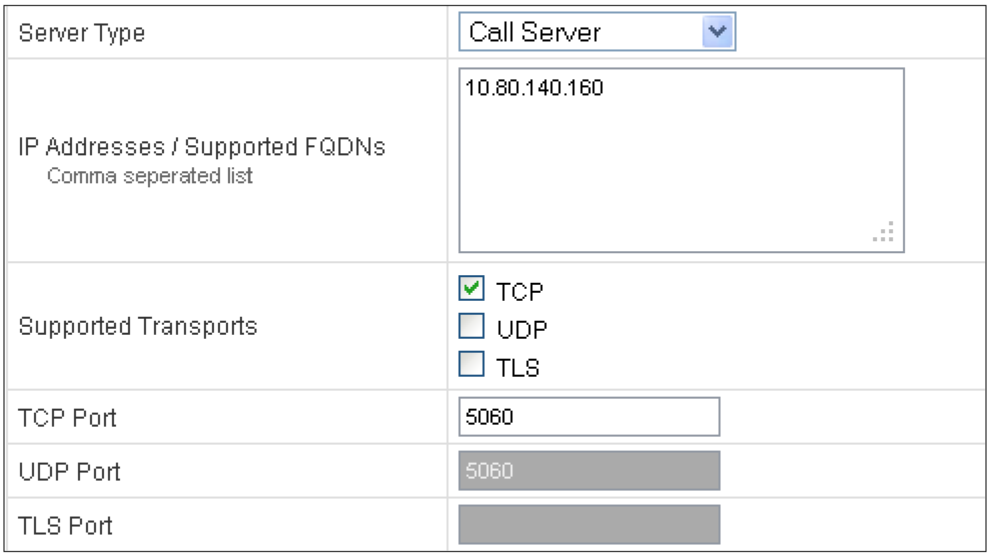


7.5.1 Server Configuration for Session Manager

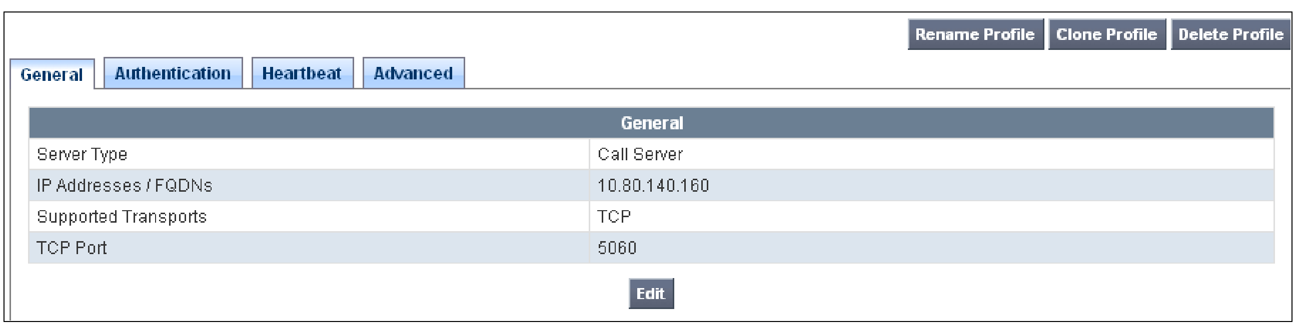
Click the **Add Profile** button (not shown) to add a new profile, or select an existing profile to edit. If adding a profile, a screen such as the following is displayed. Enter an appropriate Profile Name such as "Avaya_SM6.2" shown below. Click **Next**.



The following screens illustrate the Server Configuration for the Profile name “Avaya_SM6.2”. On the “General” tab, select “Call Server” from the **Server Type** drop-down menu. In the **IP Addresses / Supported FQDNs** area, the IP Address of the Session Manager SIP signaling interface in the sample configuration is entered. This IP Address is 10.80.140.160. In the **Supported Transports** area, TCP is selected, and the **TCP Port** is set to 5060. This configuration corresponds with the Session Manager entity link configuration for the entity link to the ASBCE created in Section 6.4. If adding a new profile, click **Next** (not shown). If editing an existing profile, click **Finish** (not shown).



Once configuration is completed, the **General** tab for “Avaya_SM6.2” will appear as shown below.



If adding the profile, click **Next** to accept default parameters for the Authentication tab (not shown), and advance to the Heartbeat area. If editing an existing profile, select the **Heartbeat** tab and click **Edit** (not shown).

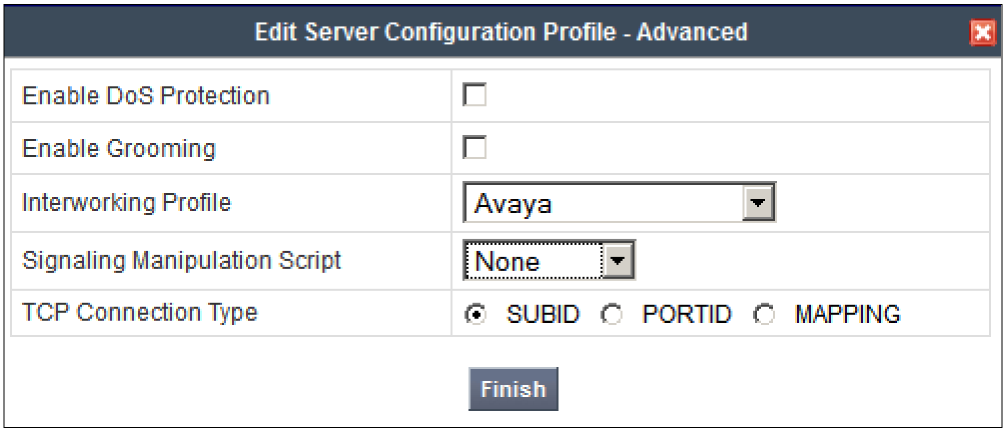
The ASBCE can be configured to source “heartbeats” in the form of SIP OPTIONS. In the sample configuration, with one Session Manager, this configuration is optional unless 2- CPE is used. If 2-CPE is used, the OPTIONS must be configured along with the **TCP Probe Frequency** at 10 seconds.

If ASBCE-sourced OPTIONS messages are desired, check the **Enable Heartbeat** box. Select "OPTIONS" from the **Method** drop-down menu. Select the desired frequency that the ASBCE will source OPTIONS to this server. The **From URI** and **To URI** may be filled in to configure easily identifiable URIs to appear in SIP OPTIONS sourced by the ASBCE towards Session Manager. If adding a new profile, click **Next** (not shown). If editing an existing profile, click **Finish** (not shown).

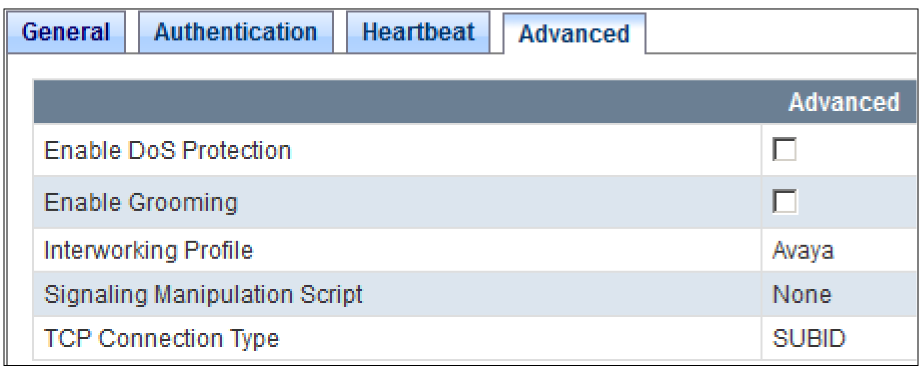
General | Authentication | Heartbeat | Advanced

		Heartbeat
Enable Heartbeat		☑
	Method	OPTIONS
	Frequency	60 seconds
	From URI	ping@10.80.140.141
	To URI	ping@10.80.140.160
TCP Probe		☑
	TCP Probe Frequency	10 seconds

If adding a profile, click **Next** to continue to the "Advanced" settings (not shown). If editing an existing profile, select the **Advanced** tab and **Edit** (not shown). In the resultant screen, select the **Interworking Profile** "Avaya" created previously. Click **Finish**.

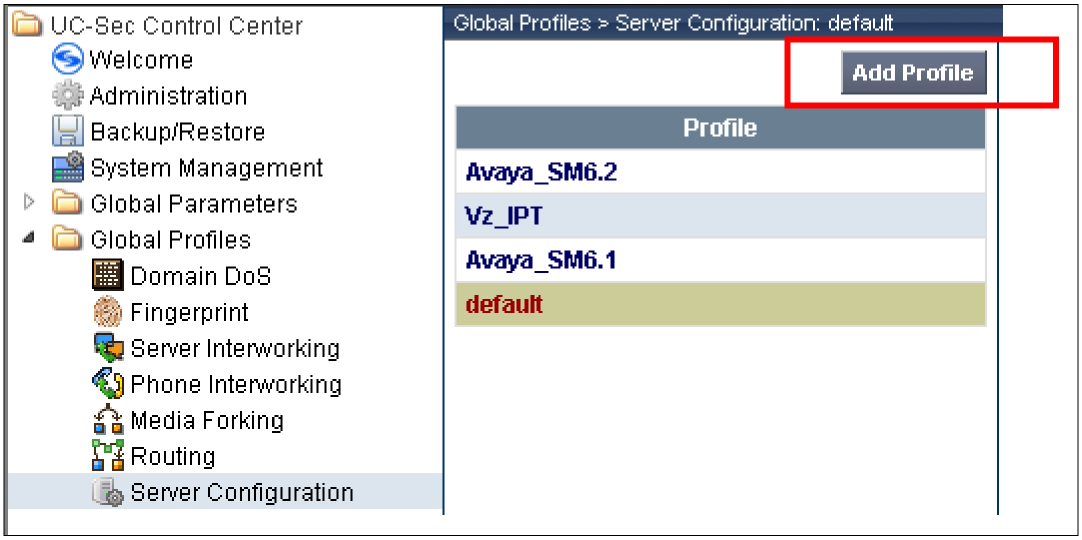


Once configuration is completed, the **Advanced** tab for the profile "Avaya_SM6.2" will appear as shown below.

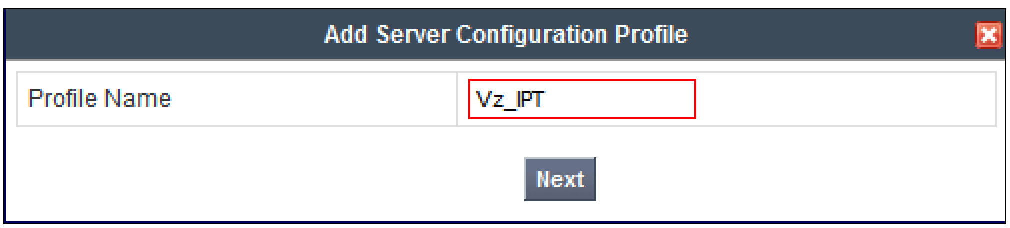


7.5.2 Server Configuration for Verizon IP Trunk

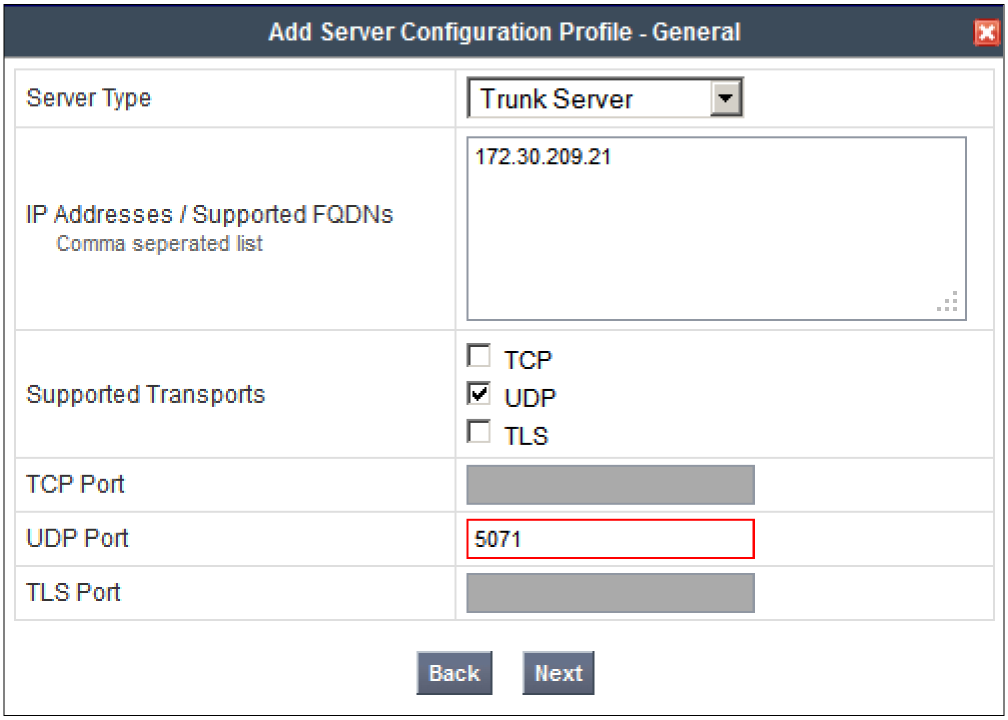
Click the **Add Profile** button to add a new profile, or select an existing profile to edit.



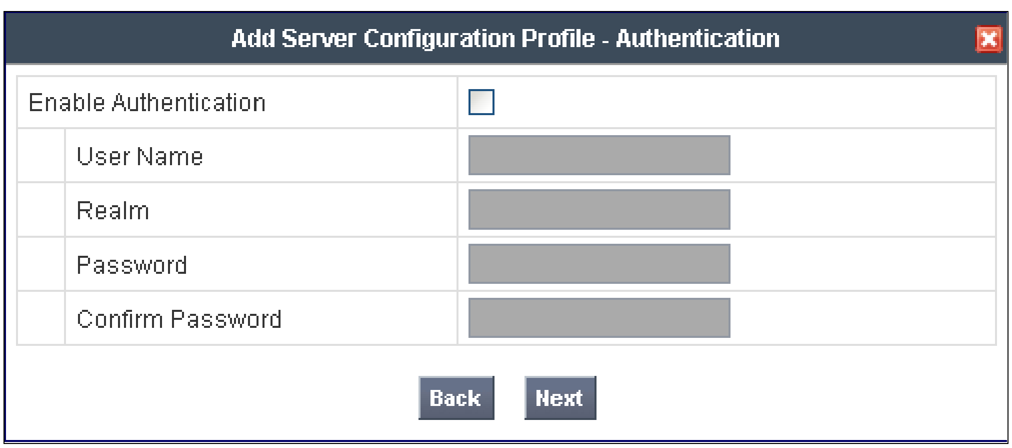
If adding a profile, a screen such as the following is displayed. Enter an appropriate Profile Name such as "Vz_IPT" shown below. Click **Next**.



The following screens illustrate the Server Configuration with Profile name "Vz_IPT". In the "General" parameters, select "Trunk Server" from the **Server Type** drop-down menu. In the **IP Addresses / Supported FQDNs** area, the Verizon-provided IP Trunk IP Address is entered. This IP Address is 172.30.209.21. In the **Supported Transports** area, UDP is selected, and the **UDP Port** is set to 5071. Click **Next** to proceed to the **Authentication** Tab.

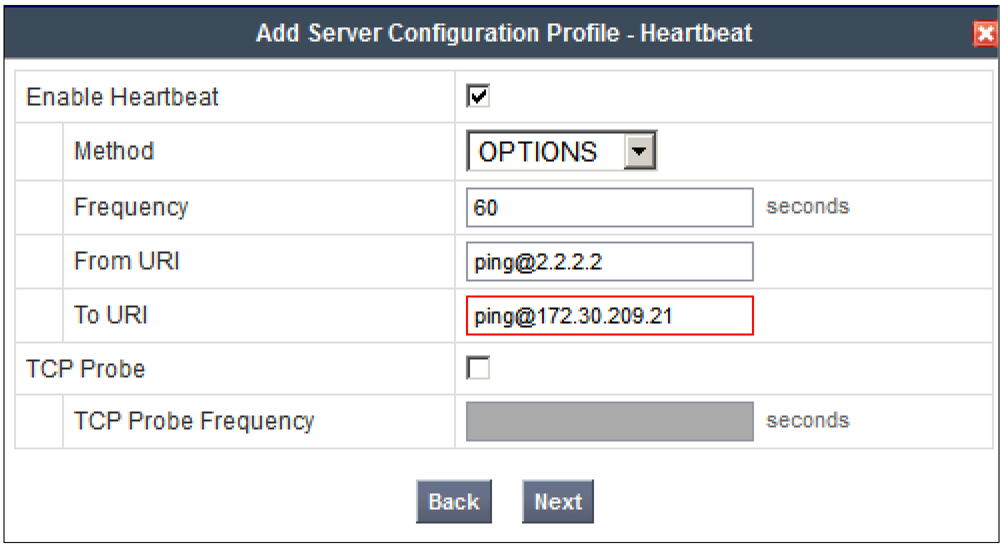


If adding the profile, click **Next** to accept default parameters for the **Authentication t**ab (below), and advance to the Heartbeat area. No authentication was used in the test configuration.

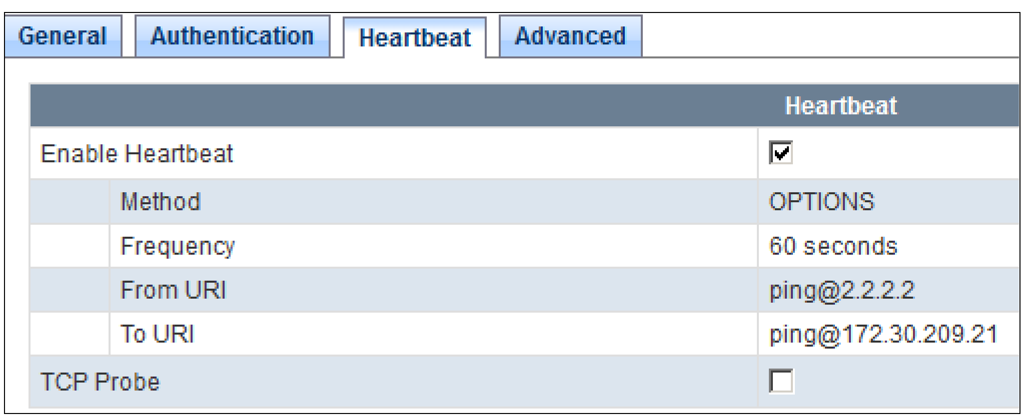


The ASBCE can be configured to source "heartbeats" in the form of SIP OPTIONS towards Verizon. This configuration is optional. Independent of whether the ASBCE is configured to source SIP OPTIONS towards Verizon, Verizon will receive OPTIONS from the enterprise site as a result of the SIP Entity Monitoring configured for Session Manager. When Session Manager sends SIP OPTIONS to the inside private IP Address of the ASBCE, the ASBCE will send SIP OPTIONS to Verizon. When Verizon responds, the ASBCE will pass the response to Session Manager.

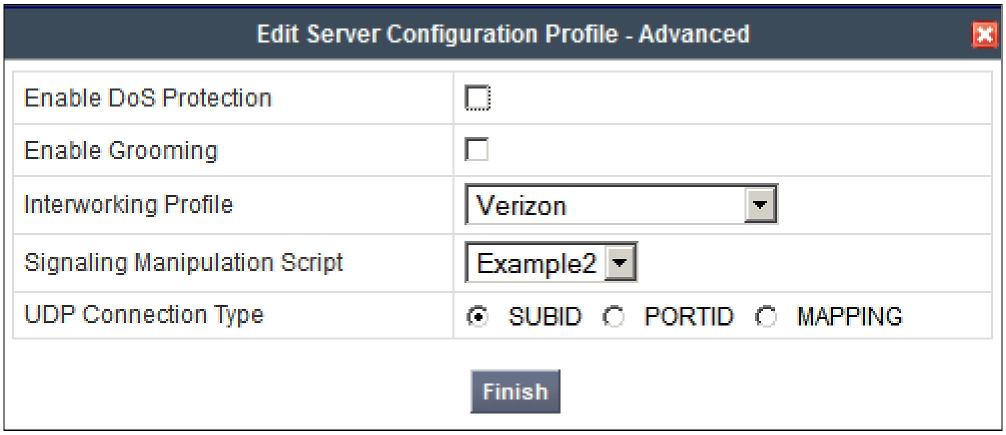
If ASBCE-sourced OPTIONS are desired, select "OPTIONS" from the **Method** drop-down menu. Select the desired frequency that the SBCE will source OPTIONS. The **From URI** and **To URI** may be filled in to configure easily identifiable URIs to appear in SIP OPTIONS sourced by the ASBCE. If adding a new profile, click **Next** to continuing to the "Advanced" settings. If editing an existing profile, click **Finish** (not shown).



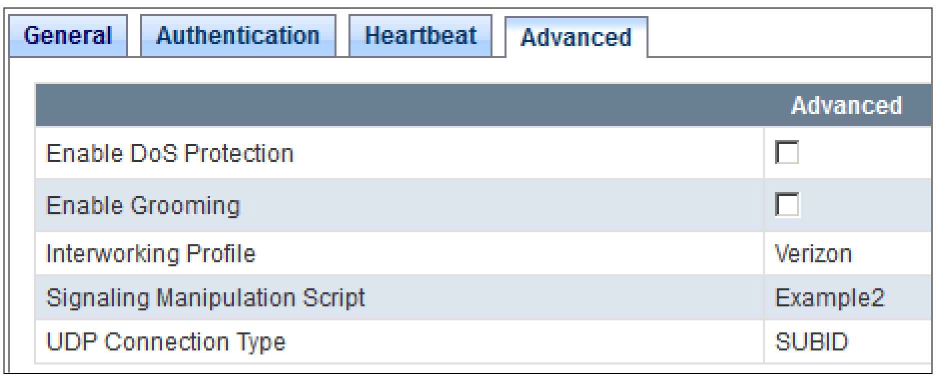
If the optional ASBCE sourced OPTIONS configuration is completed, the **Heartbeat** tab for "Vz_IPT" will appear as shown below.



If editing an existing profile, highlight the desired profile and select the **Advanced** tab and then click the **Edit button** (not shown). In the resultant screen, select the **Interworking Profile** "Verizon" created previously, and Signaling Manipulation Script will be the script shown in the previous section titled "Example2". Other ASBCE features, such as DoS Protection and Grooming, can be configured according to customer preference. Click **Finish**.

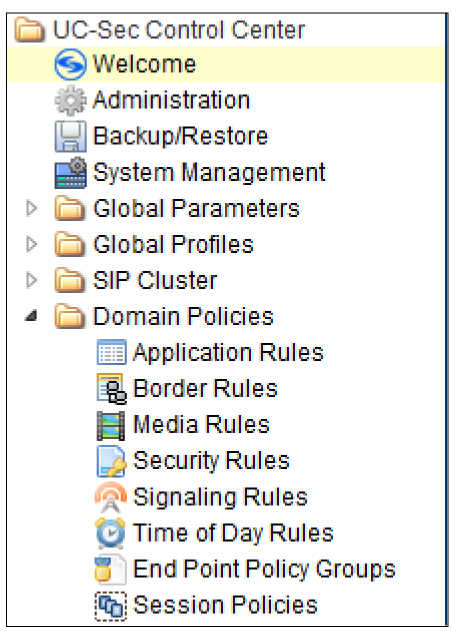


Once configuration is completed, the **Advanced** tab for "Vz_-IPT" will appear as shown below.

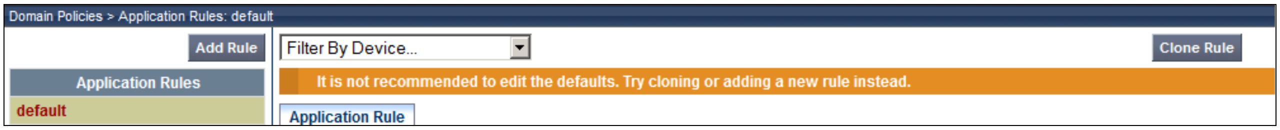


7.6. Domain Policies – Application Rule

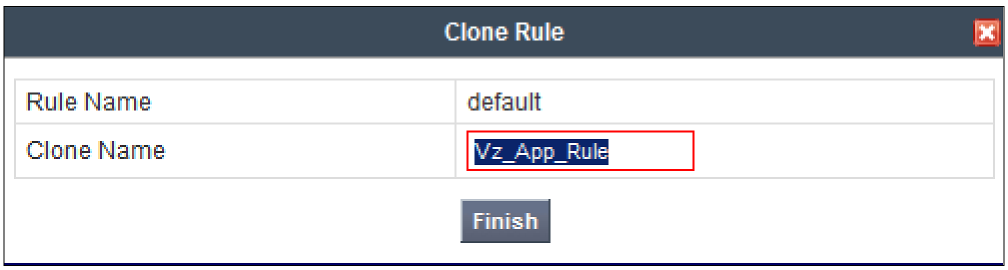
Select **Domain Policies → Application Rules** from the left-side menu as shown below.



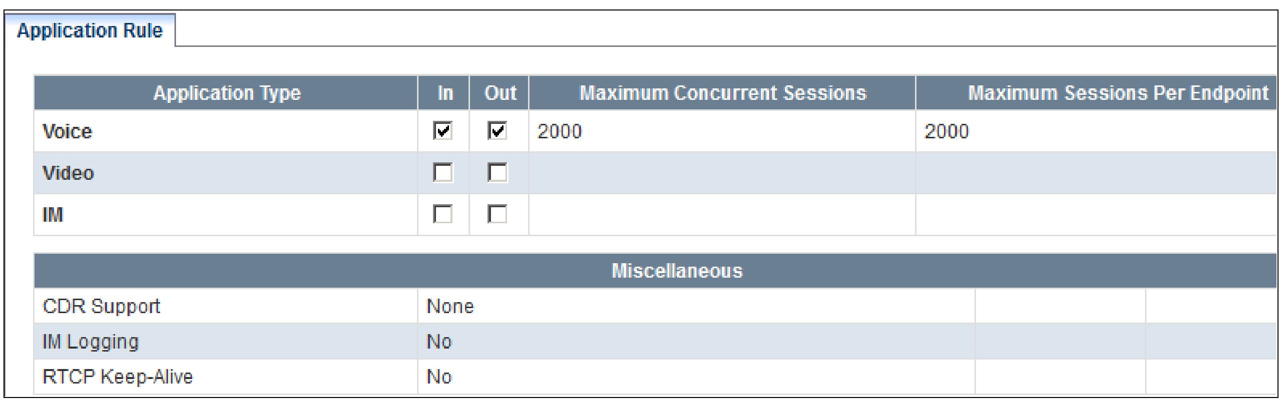
In the sample configuration, a single application rule was created by cloning the default rule called “default”. Select the default rule and click the **Clone Rule** button.



Enter a name in the **Clone Name** field, such as “Vz_App_Rule” as shown below. Click **Finish**.

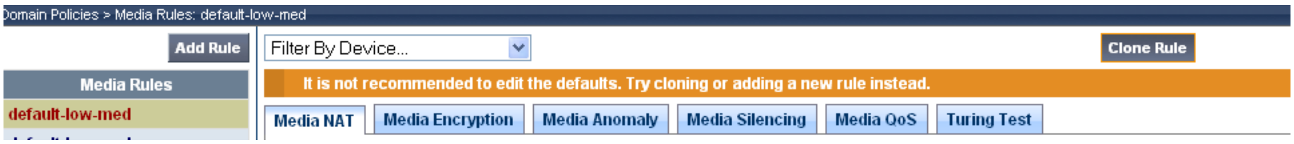


Select the newly created rule and click the **Edit** button (not shown). In the resulting screen, change the default **Maximum Concurrent Sessions** to 2000, the **Maximum Session per Endpoint** to 2000. Click **Finish**.

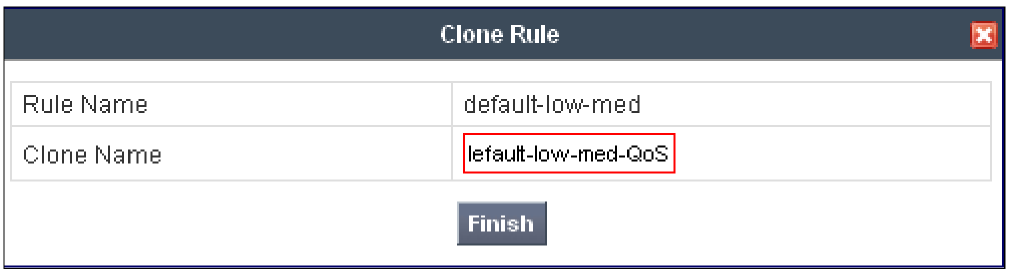


7.7. Domain Policy – Media Rules

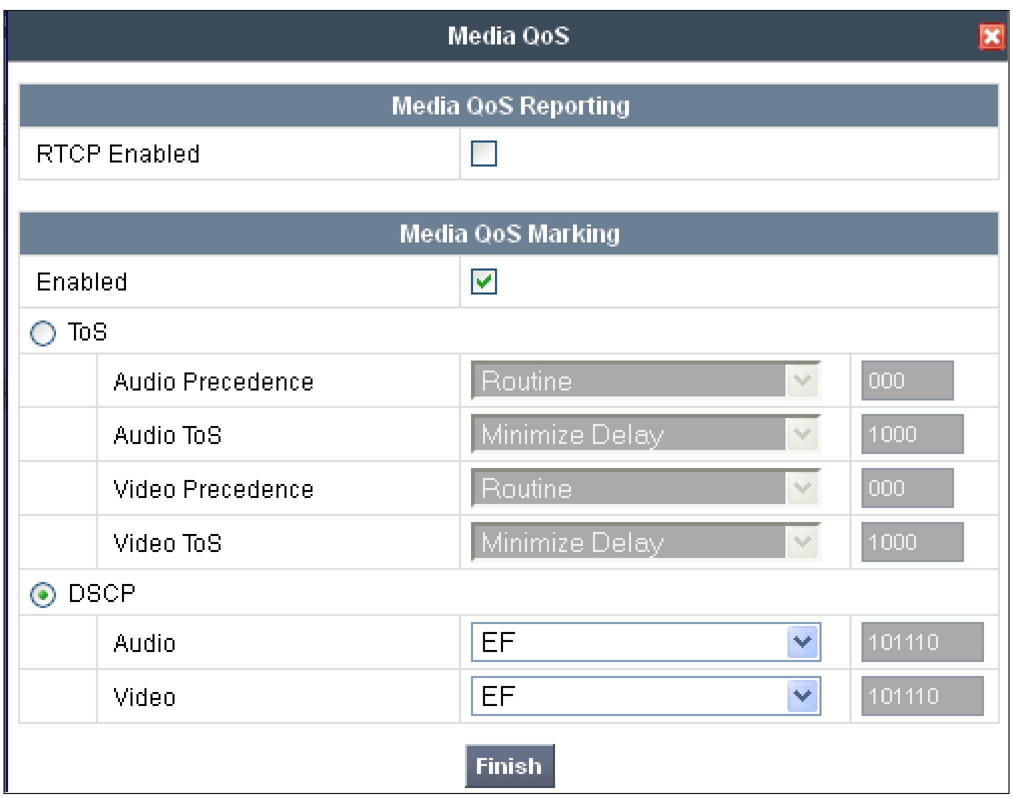
In the sample configuration, a single media rule was created by cloning the default rule called “default-low-med”. Select the default-low-med rule and click the **Clone Rule** button.



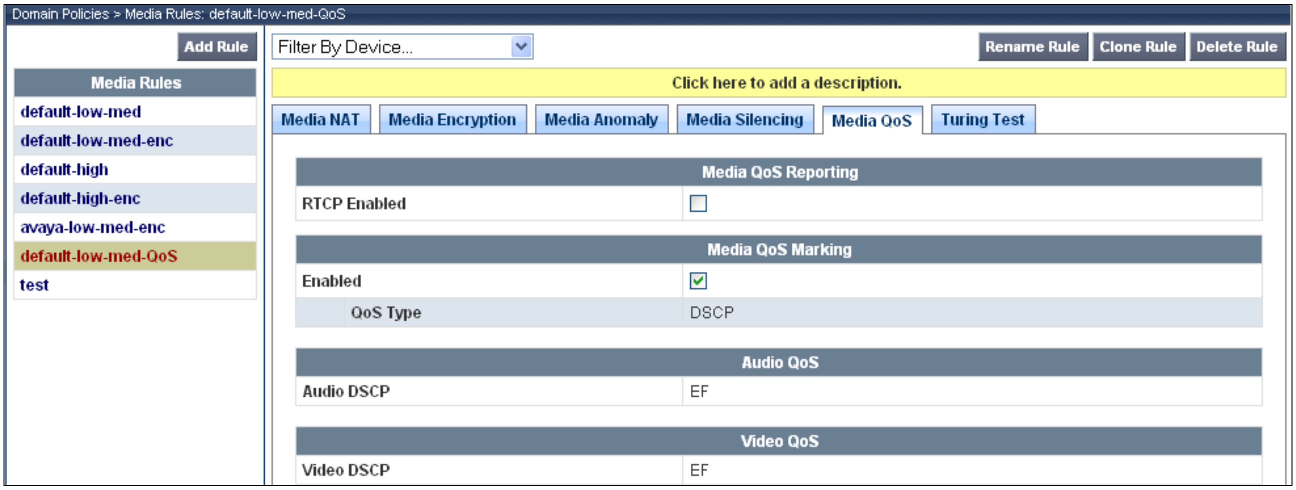
Enter a name in the **Clone Name** field, such as “default-low-med-QoS” as shown below. Click **Finish**.



Select the newly created rule, select the **Media QoS** tab (shown in previous screen), and click the **Edit** button (not shown). In the resulting screen below, check the **Media QoS Marking Enabled** checkbox. Select **DSCP** and select “EF” for expedited forwarding as shown below. Click **Finish**.

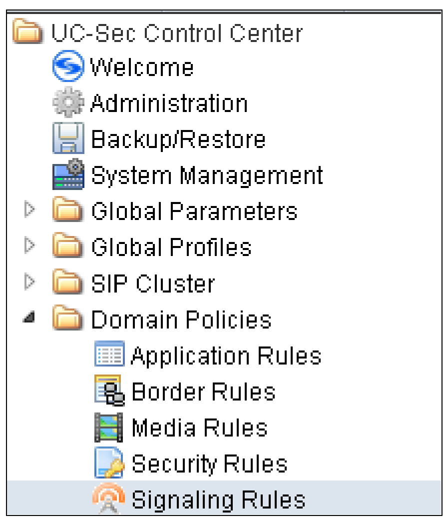


When configuration is complete, the “default-low-med-QoS” media rule **Media QoS** tab appears as follows.

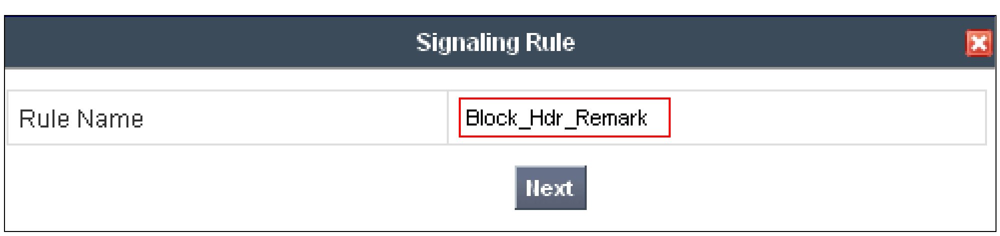


7.8. Domain Policies – Signaling Rules

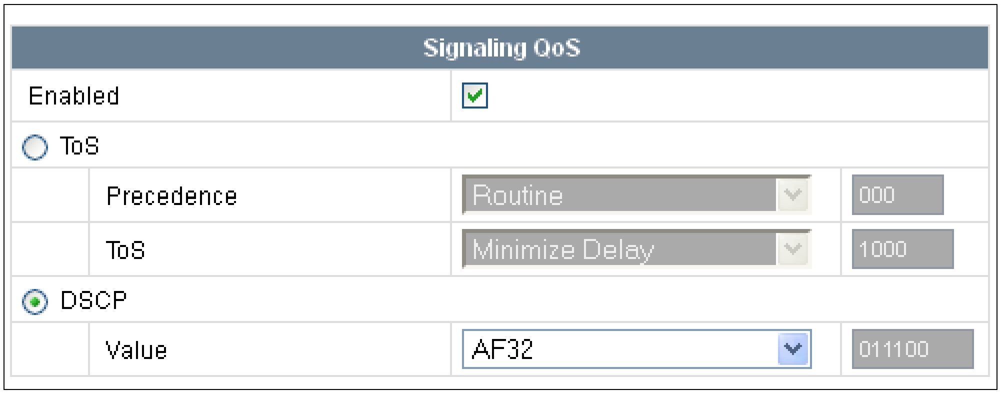
Select **Domain Policies → Signaling Rules** from the left-side menu as shown below.



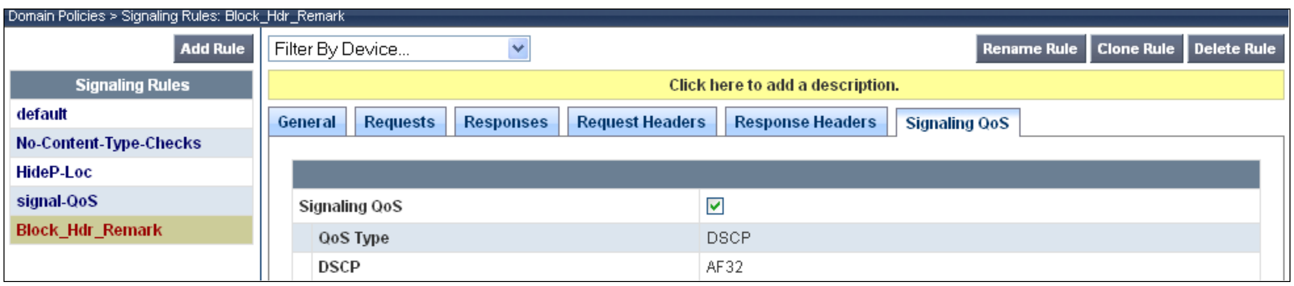
Click the **Add Rule** button (not shown) to add a new signaling rule. In the Rule Name field, enter an appropriate name, such as “Block_Hdr_Remark” and click **Next**.



In the subsequent screen (not shown), click **Next** to accept defaults. In the Signaling QoS screen below, select **DSCP** and select the desired **Value** for Signaling QoS from the drop-down box. In the sample configuration, "AF32" was selected for Assured Forwarding 32. Click **Finish** (not shown).

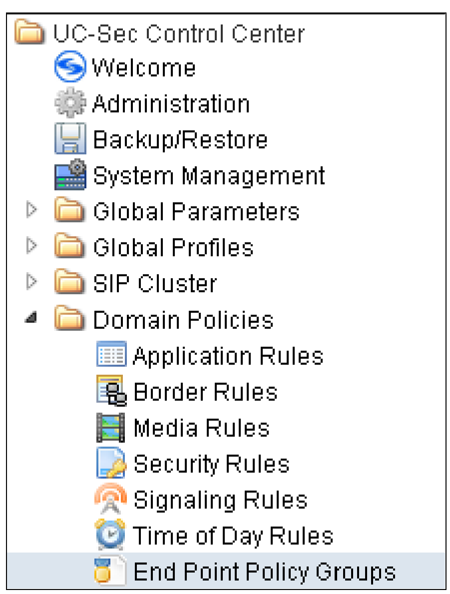


After this configuration, the new "Block_Hdr_Remark" will appear as follows.

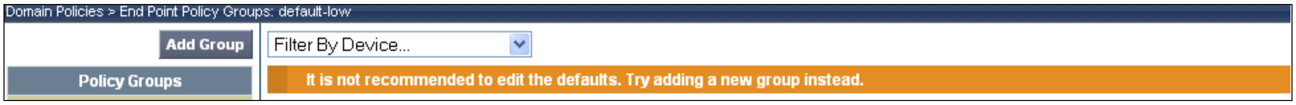


7.9. Domain Policies – End Point Policy Groups

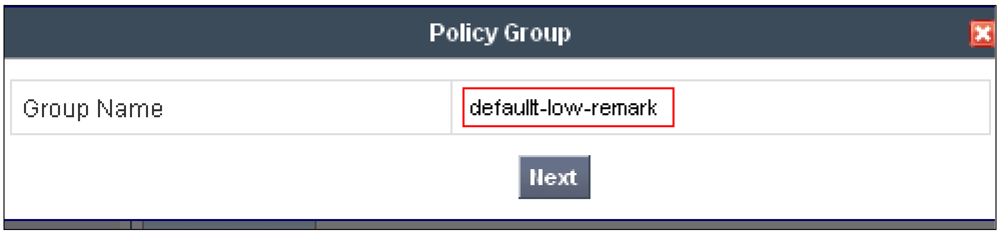
Select **Domain Policies → End Point Policy Groups** from the left-side menu as shown below.



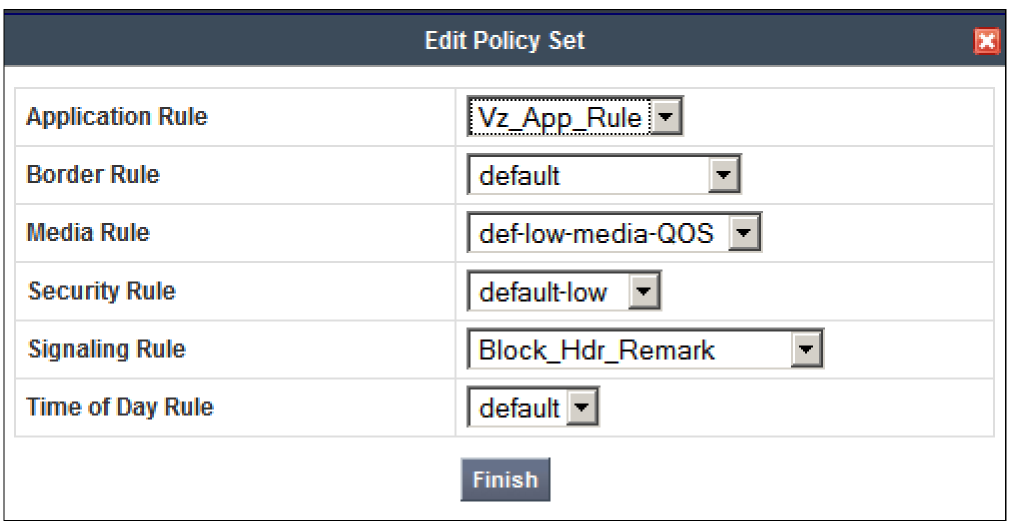
Select the **Add Group** button.



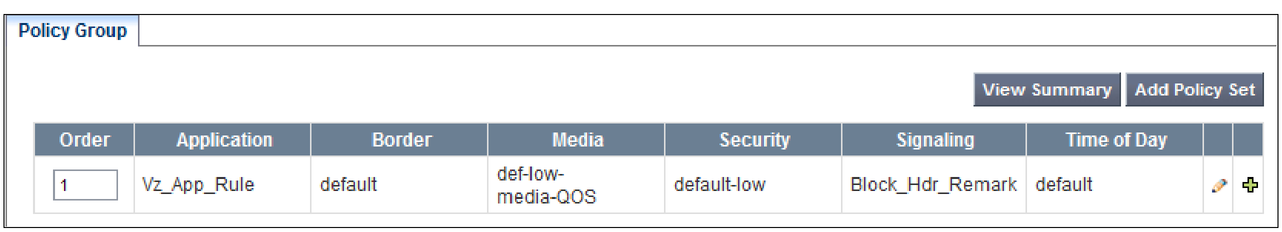
Enter a name in the **Group Name** field, such as "default-low-remark" as shown below. Click **Next**.



In the sample configuration, defaults were selected for all fields, with the exception of the **Application Rule** which was set to "Vz_App_Rule", **Media Rule** which was set to "default-low-med-QoS", and the **Signaling Rule**, which was set to "Block_Hdr_Remark" as shown below. The selected non-default media rule and signaling rule chosen were created in previous sections. Click **Finish**.

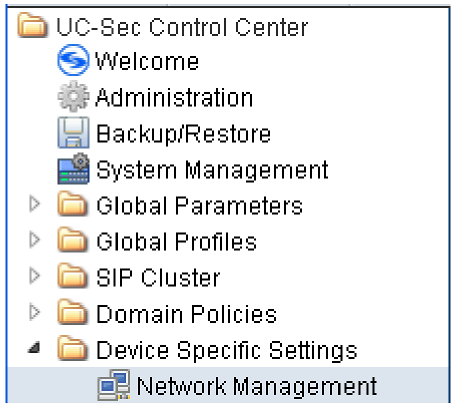


Once configuration is completed, the "default-low-remark" policy group will appear as follows.

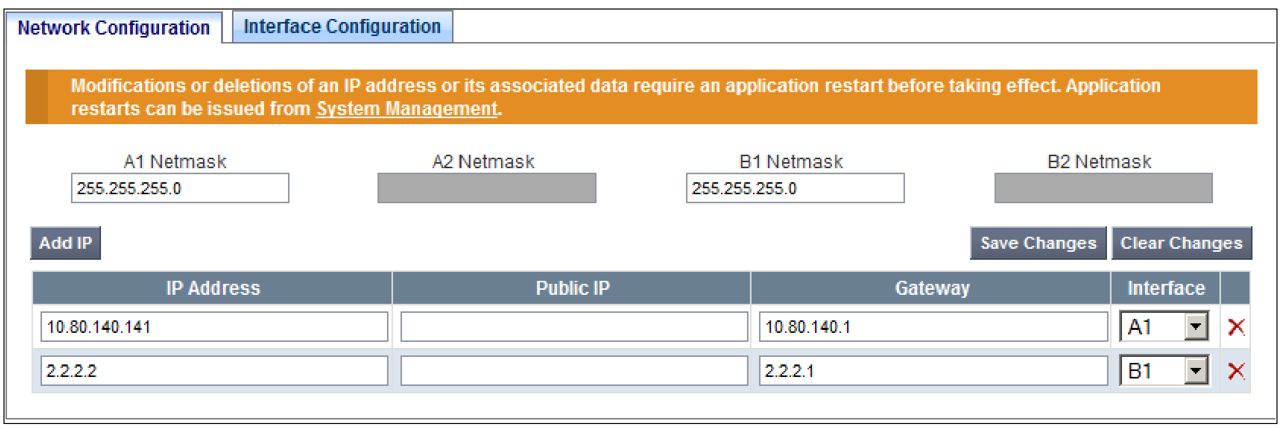


7.10. Device Specific Settings - Network Management

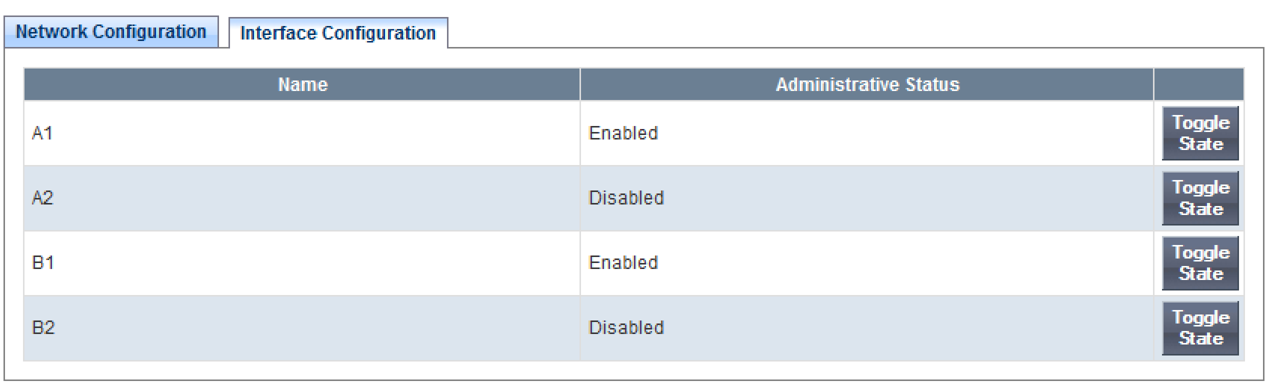
Select **Device Specific Setting → Network Management** from the left-side menu as shown below.



Under **UC-Sec Devices**, select the device being managed, which was named "VZ_1" in the sample configuration (not shown). The **Network Configuration** tab is shown below. Observe the **IP Address**, **Netmask (A1 and B1)**, **Gateway**, and **Interface** information previously assigned.

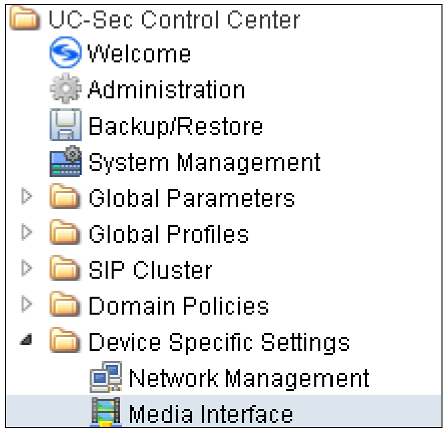


Select the **Interface Configuration** tab. The Administrative Status can be toggled between "Enabled" and "Disabled" in this screen. The following screen was captured after the interfaces had already been enabled. To enable the interface if it is disabled, click the **Toggle State** button.

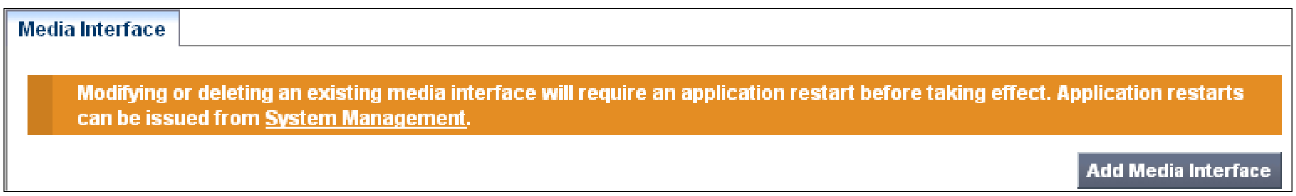


7.11. Device Specific Settings – Media Interface

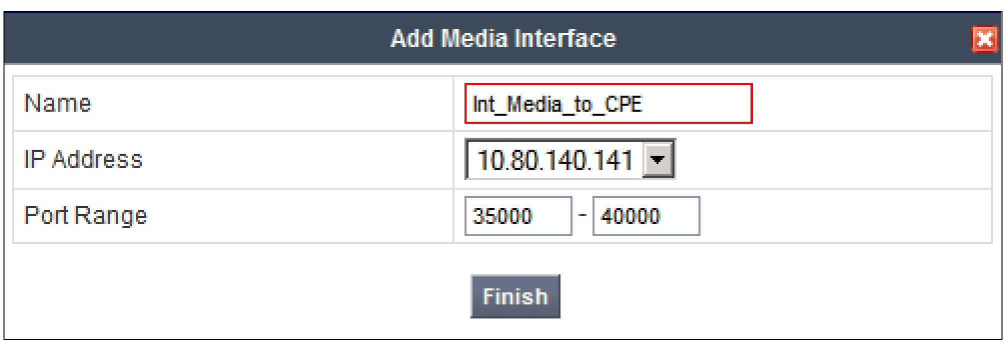
Select **Device Specific Setting → Media Interface** from the left-side menu as shown below.



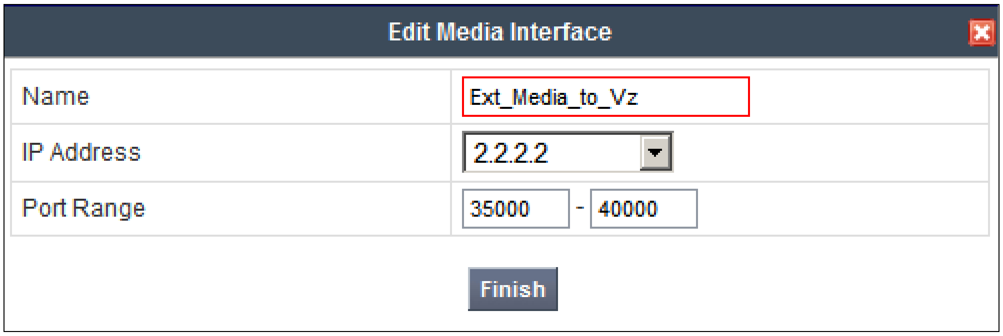
Under **UC-Sec Devices**, select the device being managed, which was named "VZ_1" in the sample configuration (not shown). Click **Add Media Interface**.



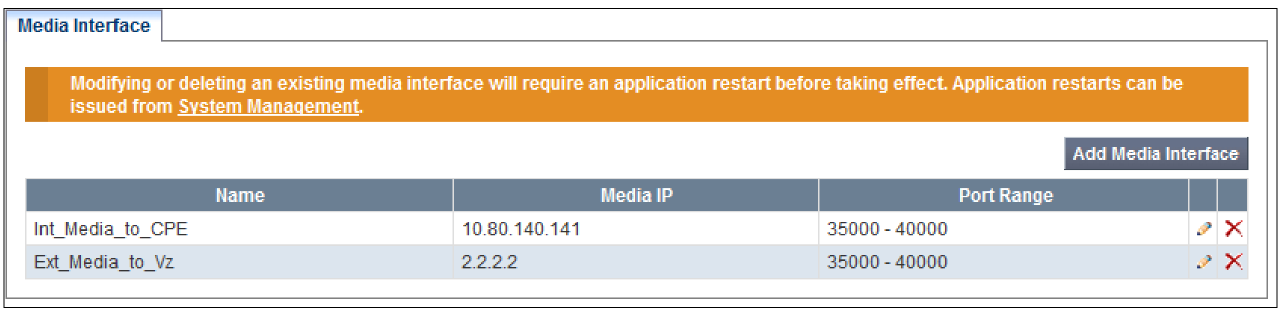
Enter an appropriate **Name** for the media interface for the Avaya CPE and select the inside private IP Address from the **IP Address** drop-down menu. In the sample configuration, "Int_Media_to_CPE" is chosen as the Name, and the "inside" IP Address of the ASBCE is "10.80.140.141". For the **Port Range**, default values are shown. Click **Finish**.



Once again, select **Add Media Interface**. Enter an appropriate **Name** for the media interface for the public "outside" of the ASBCE, and select the outside public IP Address from the **IP Address** drop-down menu. In the sample configuration, "Ext_Media_to_VZ" is chosen as the name, and the "outside" public IP Address of the ASBCE is "2.2.2.2". For the **Port Range**, default values are shown. Verizon IP Trunk does not require that the RTP ports be chosen within a specific range. Click **Finish**.

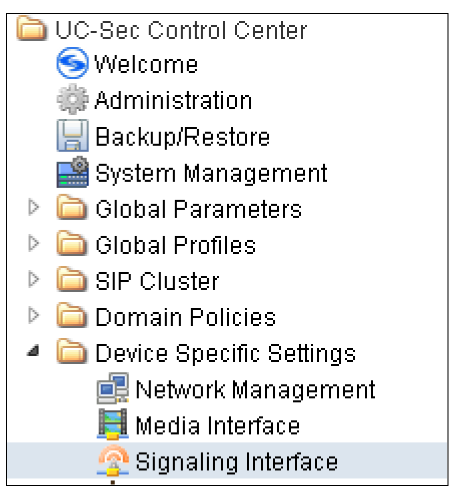


The resultant Media Interface configuration used in the sample configuration is shown below.

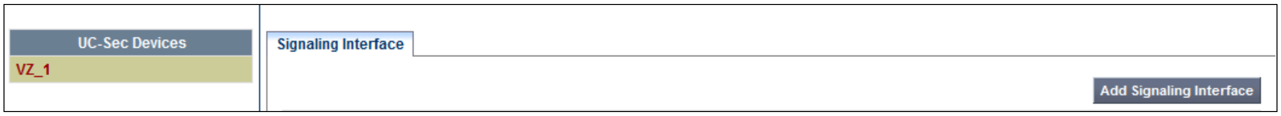


7.12. Device Specific Settings – Signaling Interface

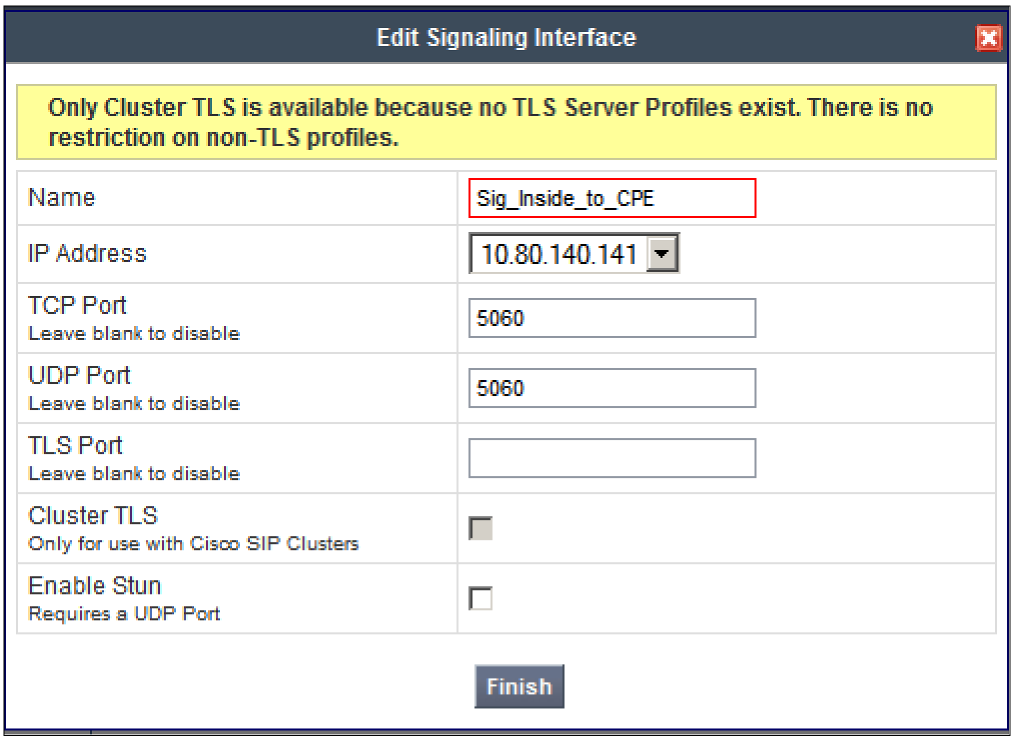
Select **Device Specific Setting → Signaling Interface** from the left-side menu as shown below.



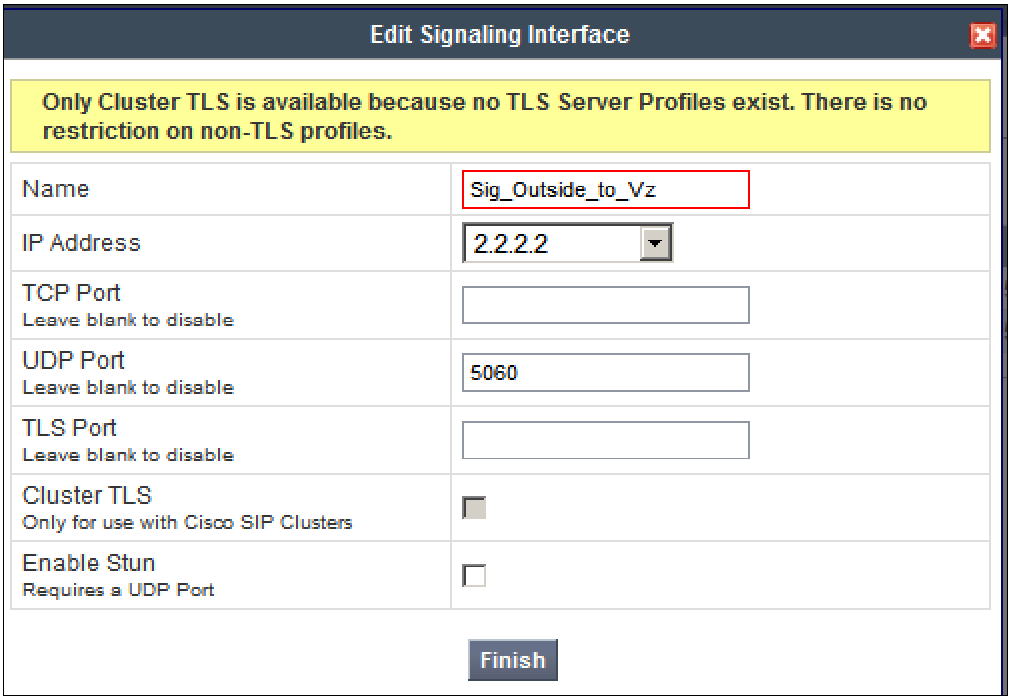
Under **UC-Sec Devices**, select the device being managed, which was named "VZ_1" in the sample configuration (not shown). Select **Add Signaling Interface**.



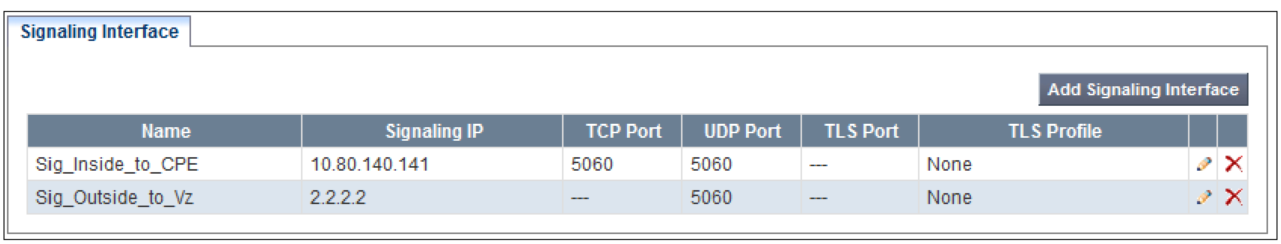
In the **Edit Signaling Interface** screen, enter an appropriate **Name** (e.g., "Sig_Inside_to_CPE") for the "inside" private interface, and choose the private inside IP Address (e.g., 10.80.140.141) from the **IP Address** drop-down menu. Choose **TCP Port** "5060" since TCP and port 5060 is used between Session Manager and the ASBCE in the sample configuration. Click **Finish**.



Once again, select **Add Signaling Interface**. In the Add Signaling Interface screen, enter an appropriate **Name** (e.g., "Sig_Outside_to_VZ") for the "outside" public interface, and choose the public IP Address (e.g., "2.2.2.2") from the **IP Address** drop-down box. Choose **UDP Port** "5060". In the sample configuration, Verizon will send SIP signaling using UDP to the CPE IP Address 2.2.2.2 and to UDP Port 5060. Click **Finish**.

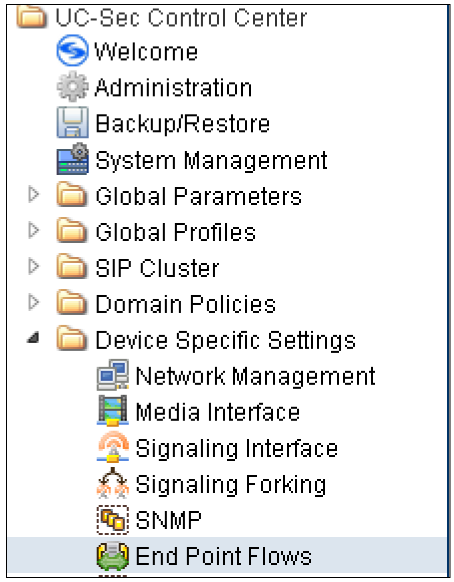


The following screen shows the signaling interfaces defined for the sample configuration.

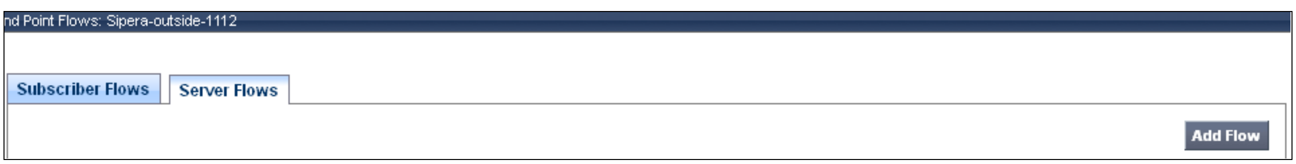


7.13. Device Specific Settings – End Point Flows

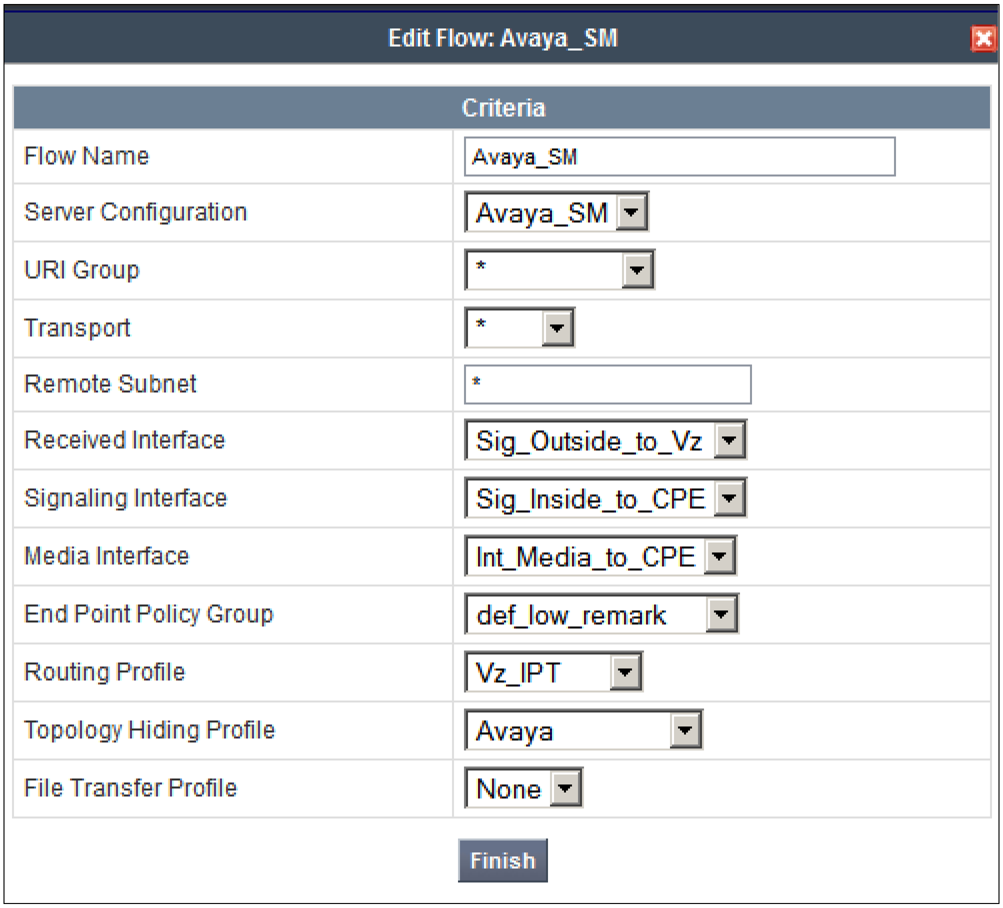
Select **Device Specific Setting → End Point Flows** from the left-side menu as shown below.



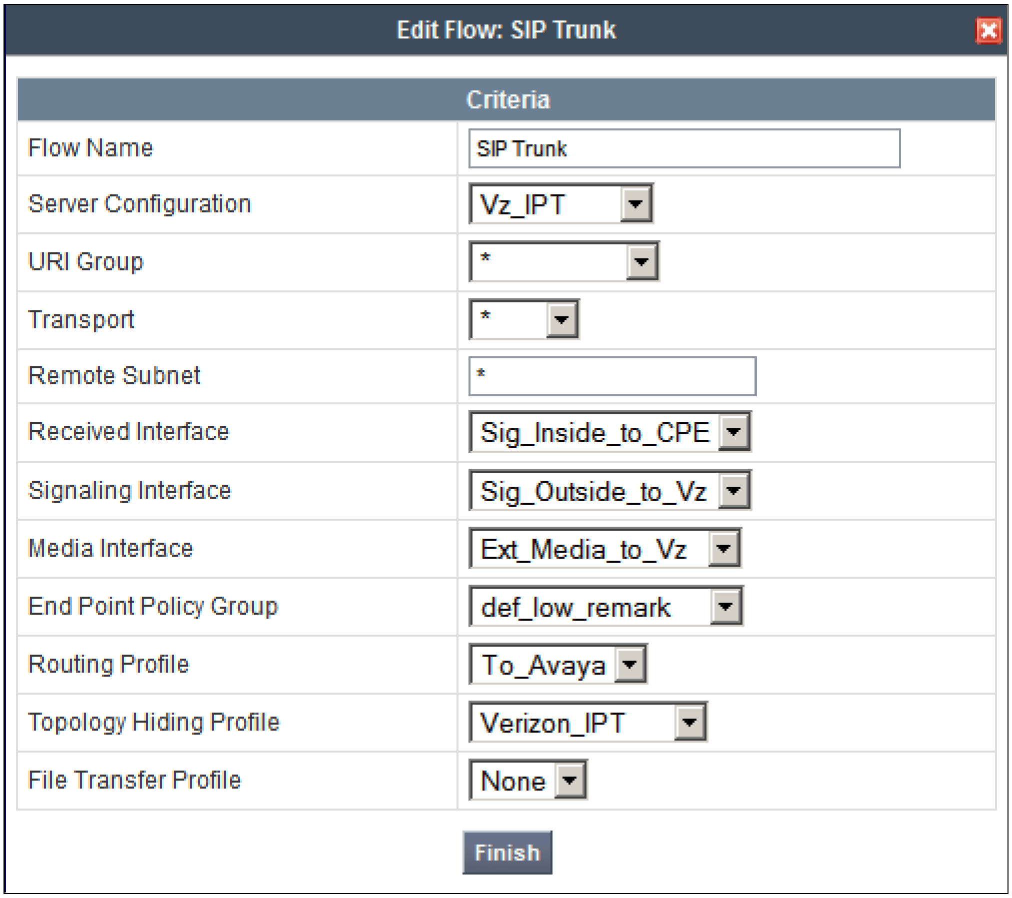
Under **UC-Sec Devices**, select the device being managed, which was named "VZ_1" in the sample configuration (not shown). Select the **Server Flows** tab. Select **Add Flow**.



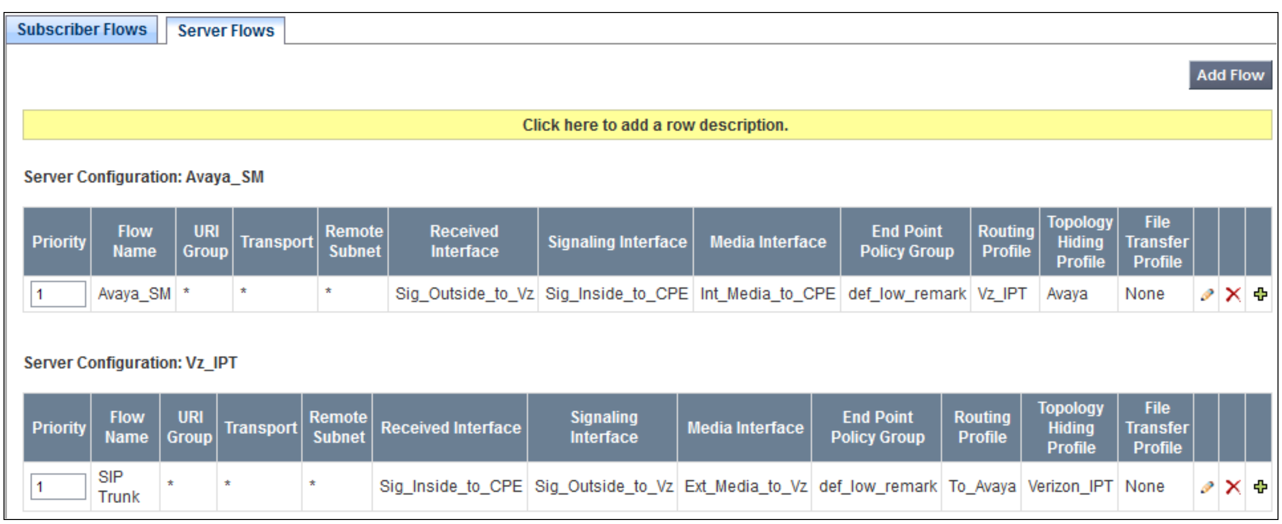
The following screen shows the flow named “Avaya_SM” being added to the sample configuration. This flow uses the interfaces, policies, and profiles defined in previous sections. Click **Finish**.



Once again, select the **Server Flows** tab. Select **Add Flow**. The following screen shows the flow named "Vz_IPT" being added to the sample configuration. This flow uses the interfaces, policies, and profiles defined in previous sections. Click **Finish**.



The following screen summarizes the Server Flows configured in the sample configuration.



Server Configuration: Avaya_SM

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	Avaya_SM	*	*	*	Sig_Outside_to_Vz	Sig_Inside_to_CPE	Int_Media_to_CPE	def_low_remark	Vz_IPT	Avaya	None

Server Configuration: Vz_IPT

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	SIP Trunk	*	*	*	Sig_Inside_to_CPE	Sig_Outside_to_Vz	Ext_Media_to_Vz	def_low_remark	To_Avaya	Verizon_IPT	None

8. Verizon Business IP Trunk Services Suite Configuration

Information regarding Verizon Business IP Trunk Services suite offer can be found at http://www.verizonbusiness.com/Products/communications/ip-telephony/ or by contacting a Verizon Business sales representative.

The reference configuration described in these Application Notes is located in the Avaya Solutions and Interoperability Test Lab. Access to the Verizon Business IP Trunk Services suite was via a Verizon Private IP (PIP) T1 connection. Verizon Business provided all of the necessary service provisioning.

8.1. Service Access Information

The following service access information (FQDN, IP addressing, ports, IP toll free numbers) was provided by Verizon for the sample configuration.

CPE (Avaya)	Verizon Network
adevc.avaya.globalipcom.com ***UDP port 5060***	***172.30.209.21*** ***UDP Port 5071***

IP DID Numbers
732-945-0240
732-945-0241
732-945-0242
732-945-0243
732-945-0244
732-945-0285
732-945-0286
732-945-0287
732-945-0288

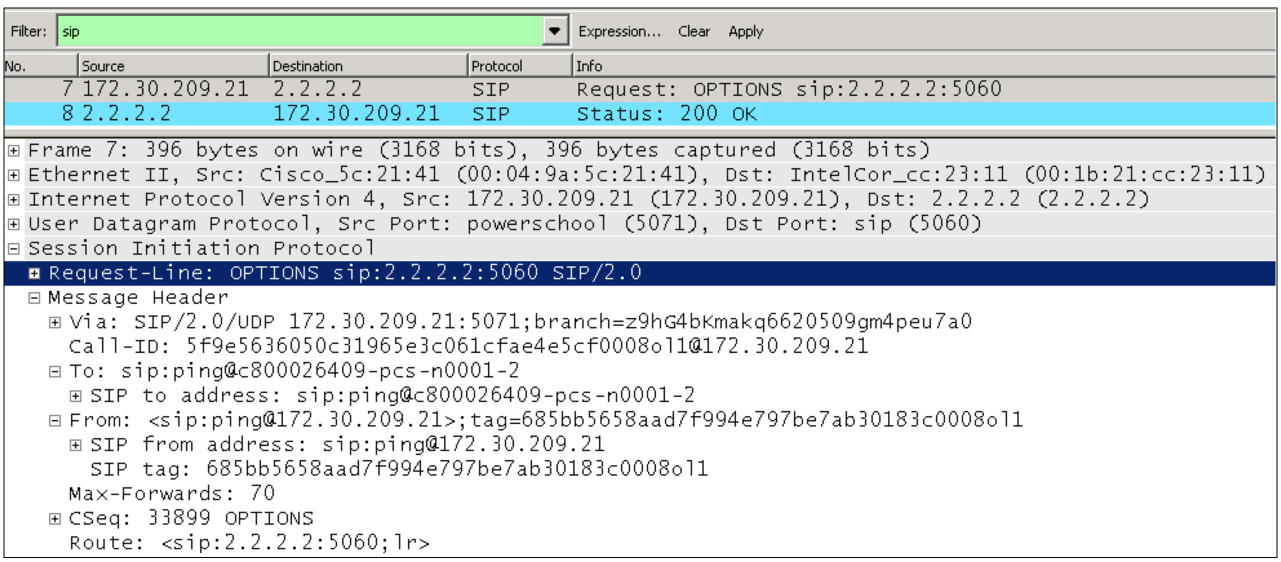
9. Verification Steps

This section provides example verifications of the Avaya configuration with Verizon Business Private IP (PIP) Trunk service.

9.1. Illustration of OPTIONS Handling

This section illustrates SIP OPTIONS monitoring of the SIP trunk from Verizon to the CPE and from the CPE to Verizon through the ASBCE.

The following screens from a filtered Wireshark trace illustrate OPTIONS sent by Verizon to the CPE. Verizon IP Trunk service uses OPTIONS to determine whether the CPE is available to receive inbound calls. Therefore, proper OPTIONS response is necessary. In the trace shown below, taken from the outside public side of the ASBCE, frame 7 is highlighted and expanded to show OPTIONS sent from Verizon IPC Trunk (172.30.209.21) to the ASBCE (2.2.2.2). Observe the use of UDP for transport, from source port 5071 (Verizon) to destination port 5060 (Avaya). Verizon sends the Avaya domain “2.2.2.2” in the Request-Line. Note that Max-Forwards is 70.



Before the ASBCE replies to Verizon, the ASBCE sends OPTIONS to Session Manager on the inside private interface. In the trace shown below, taken from the private side of the ASBCE, frame 34 is highlighted and expanded to show OPTIONS sent from the inside interface of the ASBCE (10.80.140.141) to Session Manager (10.80.140.160). Observe the use of TCP for transport, using port 5060. Observe that the ASBCE has changed the Request-URI, From and To headers per the previous configuration such that “avayalab.com” now appears. Note that Max-Forwards has been decremented by 1 and is now 69.

```
Filter: sip                                   Expression...  Clear  Apply
No.  Source         Destination    Protocol  Info
  34 10.80.140.141  10.80.140.160  SIP       Request: OPTIONS sip:avayalab.com
  35 10.80.140.160  10.80.140.141  SIP       Status: 200 OK

⊞ Frame 34: 447 bytes on wire (3576 bits), 447 bytes captured (3576 bits)
⊞ Ethernet II, Src: IntelCor_cc:23:15 (00:1b:21:cc:23:15), Dst: Hewlett-_2b:ad:40 (9c:8e:99:2b:ad:40)
⊞ Internet Protocol Version 4, Src: 10.80.140.141 (10.80.140.141), Dst: 10.80.140.160 (10.80.140.160)
⊞ Transmission Control Protocol, Src Port: entextnetwk (12001), Dst Port: sip (5060), Seq: 1, Ack: 2,
⊟ Session Initiation Protocol
  ⊞ Request-Line: OPTIONS sip:avayalab.com SIP/2.0
  ⊟ Message Header
    ⊞ From: <sip:ping@avayalab.com>;tag=685bb5658aad7f994e797be7ab30183c0008ol1
    ⊞ To: sip:ping@avayalab.com
    ⊞ CSeq: 33899 OPTIONS
      Call-ID: 4d399505a7da644e18107959c5f86535
      Record-Route: <sip:10.80.140.141:5060;ipcs-line=21309;lr;transport=tcp>
      Max-Forwards: 69
    ⊞ Via: SIP/2.0/TCP 10.80.140.141:5060;branch=z9hG4bK-s1632-000754112348-1--s1632-
      Content-Length: 0
```

9.2. Avaya Aura® Communication Manager Verifications

This section illustrates verifications from Communication Manager.

9.2.1 Example Incoming Call from PSTN via Verizon SIP Trunk

Incoming PSTN calls arrive from Verizon at ASBCE, which sends the call to Session Manager. In the sample configuration, when the ASBCE is in-service, Verizon sends all inbound calls to ASBCE-1 (i.e., not load balanced). Session Manager sends the call to Communication Manager via the entity link corresponding to the Avaya HP Common Server using port 5062. On Communication Manager, the incoming call arrives via signaling group 68 and trunk group 68.

The following edited Communication Manager ***list trace tac*** trace output shows a call incoming on trunk group 68. The PSTN telephone dialed 732-945-0286. Session Manager can map the number received from Verizon to the extension of a Communication Manager telephone (x2011), or the incoming call handling table for trunk group 68 can do the same. In the trace below, Communication Manager had already mapped the Verizon DID to Communication Manager extension. Extension 2011 is an IP Telephone with IP address 10.80.140.133 in Region 1. Initially, the G450 Media Gateway (10.80.140.148) is used, but as can be seen in the final trace output, once the call is answered, the final RTP media path is "ip-direct" from the IP Telephone (10.80.140.133) to the "inside" of the ASBCE (10.80.140.141).

```
list trace tac *168                                                  Page   1
                                LIST TRACE
time            data
13:50:35 TRACE STARTED 02/26/2012 CM Release String
13:50:42 SIP<INVITE sip:2011@avayalab.com SIP/2.0
13:50:42     Call-ID: BW15484315426021221418536510@65.211.120.226
13:50:42     active trunk-group 68 member 1    cid 0xcc2
13:50:42 SIP>SIP/2.0 180 Ringing
13:50:42     Call-ID: BW15484315426021221418536510@65.211.120.226
13:50:42     dial 2011
13:50:42     ring station      2011 cid 0xcc2
13:50:50 SIP>SIP/2.0 200 OK
13:50:50     Call-ID: BW15484315426021221418536510@65.211.120.226
13:50:50     active station      2011 cid 0xcc2
13:50:50     G729A ss:off ps:20
             rgn:1 [10.80.140.133]:2890
             rgn:4 [10.80.140.141]:35072
13:50:50     G729A ss:off ps:20
             rgn:4 [10.80.140.141]:35072
             rgn:1 [10.80.140.133]:2890
13:50:50 SIP<ACK sip:7329450286@10.80.140.146:5062;transport=tcp SIP
13:50:50 SIP</2.0
13:50:50     Call-ID: BW15484315426021221418536510@65.211.120.226
13:50:54 SIP<BYE sip:7329450286@10.80.140.146:5062;transport=tcp SIP
13:50:54 SIP</2.0
13:50:54     Call-ID: BW15484315426021221418536510@65.211.120.226
13:50:54 SIP>SIP/2.0 200 OK
13:50:54     Call-ID: BW15484315426021221418536510@65.211.120.226
13:50:54     idle trunk-group 68 member 1    cid 0xcc2
```

The following screen shows **Page 2** of the output of the ***status trunk*** command pertaining to this same call. Note the signaling using port 5062 between Communication Manager and Session Manager. Note the media is "ip-direct" from the IP Telephone (10.80.140.133) to the inside IP address of ASBCE (10.80.140.141) using G.729.

```
status trunk 68/1                                             Page   2 of   3
                                CALL CONTROL SIGNALING
Near-end Signaling Loc: PROCR
  Signaling   IP Address                              Port
   Near-end:  10.80.140.146                         : 5062
    Far-end:  10.80.140.160                         : 5062
 H.245 Near:
  H.245 Far:
   H.245 Signaling Loc:           H.245 Tunneled in Q.931? no

 Audio Connection Type: ip-direct     Authentication Type: None
    Near-end Audio Loc:                        Codec Type: G.729A
   Audio      IP Address                              Port
   Near-end:  10.80.140.133                         : 2890
    Far-end:  10.80.140.141                         : 35070

 Video Near:
  Video Far:
 Video Port:
  Video Near-end Codec:              Video Far-end Codec:
```

The following screen shows **Page 3** of the output of the ***status trunk*** command pertaining to this same call. Here it can be observed that G.729a codec is used.

```
status trunk 68/1                                                Page   3 of   3
                      SRC PORT TO DEST PORT TALKPATH
src port: T00031
T00031:TX:10.80.140.141:35070/g729a/20ms
S00001:RX:10.80.140.133:2890/g729a/20ms

dst port: S00001
```

9.2.2 Example Outgoing Calls to PSTN via Verizon IP Trunk

Depending on Session Manager configuration of the “rank” for the routing policies, outbound calls can either use ASBCE-1 preferentially or distribute calls across ASBCE-1 and ASBCE-2. At the time of the following trace, Session Manager was configured such that both ASBCE-1 and ASBCE-2 had the same “rank” and for this particular call, ASBCE-1 was used. Outbound calls using ASBCE-2 look similar and will not be repeated here.

The following edited trace shows an outbound ARS call from IP Telephone x2011 to the PSTN number 9-1-303-538-7023. The call is routed to route pattern 68 and trunk group 68. The call initially uses the gateway (10.80.140.148), but after the call is answered, the call is “shuffled” to become an “ip-direct” connection between the IP Telephone (10.80.140.133) and the “inside” of the ASBCE-1 (10.80.140.141).

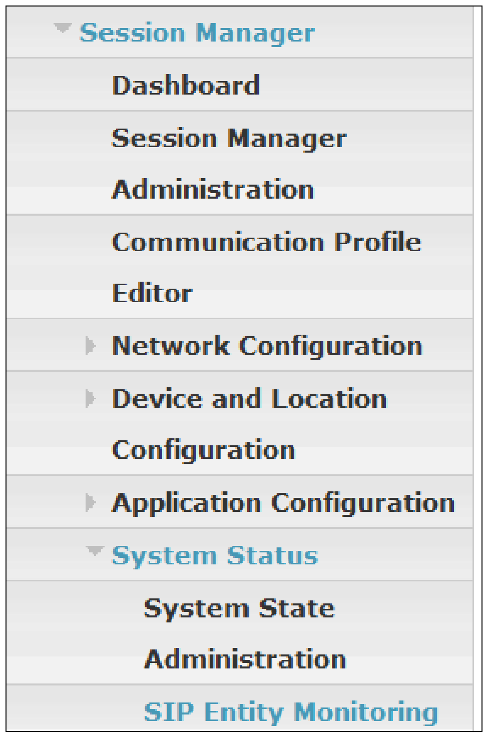
```
list trace tac *168                                                    Page   1
                                 LIST TRACE
time            data

12:18:17 TRACE STARTED 02/29/2012 CM Release String
12:18:20     Calling party station      2011 cid 0xd56
12:18:20     Calling Number & Name 2011 9608-H323
12:18:20     dial 913035387023 route:PREFIX|FNPA|ARS
12:18:20     term trunk-group 68      cid 0xd56
12:18:20     dial 913035387023 route:PREFIX|FNPA|ARS
12:18:20     route-pattern  68 preference 1 location 1/ALL  cid 0xd56
12:18:20     seize trunk-group 68 member 7    cid 0xd56
12:18:20     Calling Number & Name NO-CPNumber NO-CPName
12:18:20 SIP>INVITE sip:3035387023@avayalab.com SIP/2.0
12:18:20     Call-ID: 04e68a3e15ee1113f64f203b1f00
12:18:20     Setup digits 3035387023
12:18:20     Calling Number & Name 7329450286 9608-H323
12:18:20 SIP<SIP/2.0 100 Trying
12:18:20     Call-ID: 04e68a3e15ee1113f64f203b1f00
12:18:20     Proceed trunk-group 68 member 7    cid 0xd56
12:18:23 SIP<SIP/2.0 183 Session Progress
12:18:23     Call-ID: 04e68a3e15ee1113f64f203b1f00
12:18:23 SIP>UPDATE sip:3035387023@10.80.140.141:5060;transport=tcp
12:18:23 SIP>SIP/2.0
12:18:23     Call-ID: 04e68a3e15ee1113f64f203b1f00
12:18:23     G729 ss:off ps:20
             rgn:4 [10.80.140.141]:35200
             rgn:1 [10.80.140.148]:2072
12:18:23     xoip options: fax:T38 modem:off tty:US  uid:0x50025
             xoip ip: [10.80.140.148]:2072
12:18:23 SIP<SIP/2.0 200 OK
12:18:23     Call-ID: 04e68a3e15ee1113f64f203b1f00
12:18:24 SIP<SIP/2.0 200 OK
12:18:24     Call-ID: 04e68a3e15ee1113f64f203b1f00
12:18:24 SIP>ACK sip:3035387023@10.80.140.141:5060;transport=tcp SIP
12:18:24 SIP>/2.0
12:18:24     Call-ID: 04e68a3e15ee1113f64f203b1f00
12:18:24     active trunk-group 68 member 7    cid 0xd56
12:18:24 SIP>INVITE sip:3035387023@10.80.140.141:5060;transport=tcp
12:18:24 SIP>SIP/2.0
12:18:24     Call-ID: 04e68a3e15ee1113f64f203b1f00
12:18:24 SIP<SIP/2.0 100 Trying
12:18:24     Call-ID: 04e68a3e15ee1113f64f203b1f00
12:18:24 SIP<SIP/2.0 200 OK
12:18:24     Call-ID: 04e68a3e15ee1113f64f203b1f00
12:18:24     G729 ss:off ps:20
             rgn:1 [10.80.140.133]:2134
             rgn:4 [10.80.140.141]:35200
12:18:24 SIP>ACK sip:3035387023@10.80.140.141:5060;transport=tcp SIP
12:18:24 SIP>/2.0
12:18:24     Call-ID: 04e68a3e15ee1113f64f203b1f00
12:18:24     G729A ss:off ps:20
             rgn:4 [10.80.140.141]:35200
             rgn:1 [10.80.140.133]:2134
12:18:26 SIP>BYE sip:3035387023@10.80.140.141:5060;transport=tcp SIP
12:18:26 SIP>/2.0
12:18:26     Call-ID: 04e68a3e15ee1113f64f203b1f00
12:18:26     idle station      2011 cid 0xd56
```

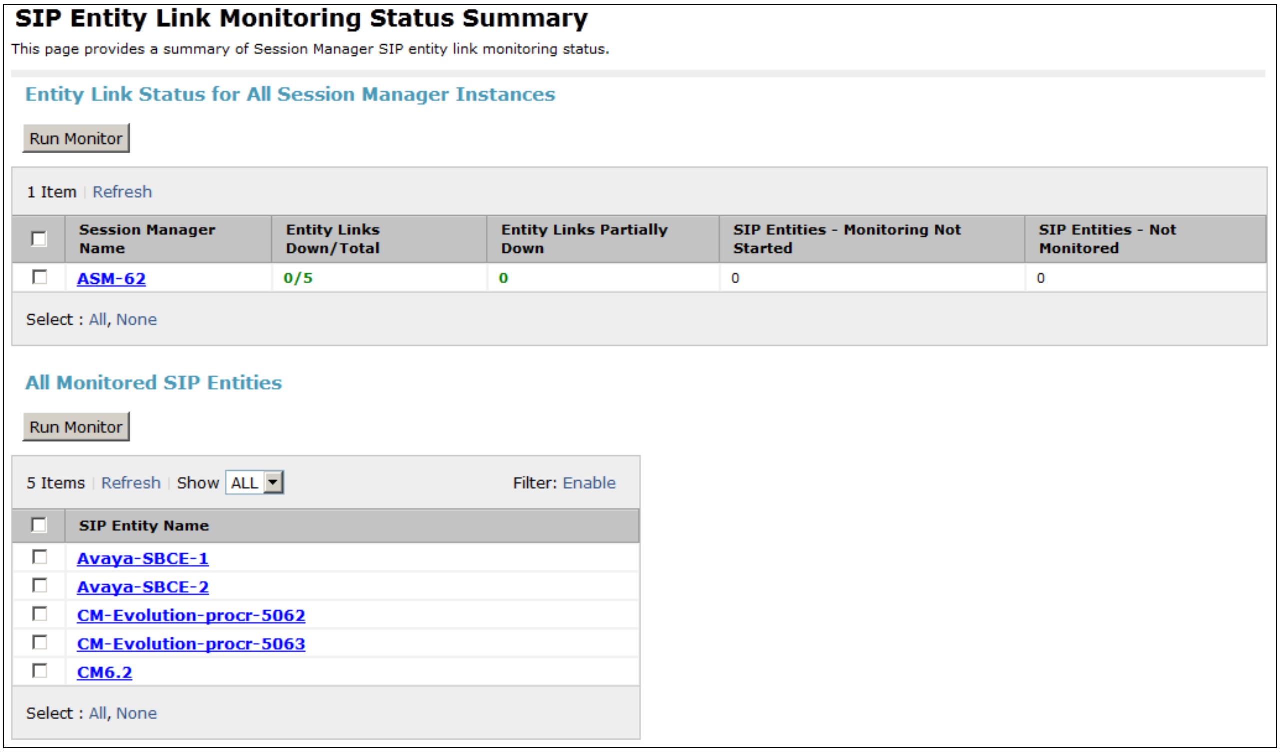
9.3. Avaya Aura® System Manager and Avaya Aura® Session Manager Verifications

This section contains verification steps that may be performed using System Manager for Session Manager.

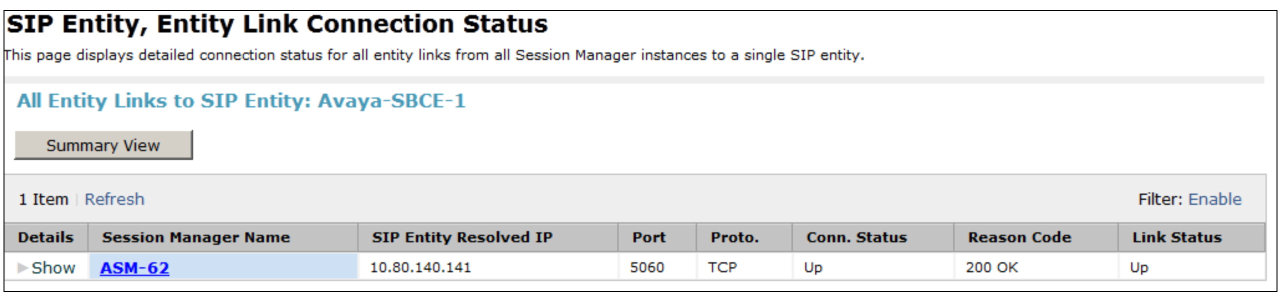
9.3.1 Verify SIP Entity Link Status

Log in to System Manager. Expand **Elements** → **Session Manager** → **System Status** → **SIP Entity Monitoring**, as shown below.

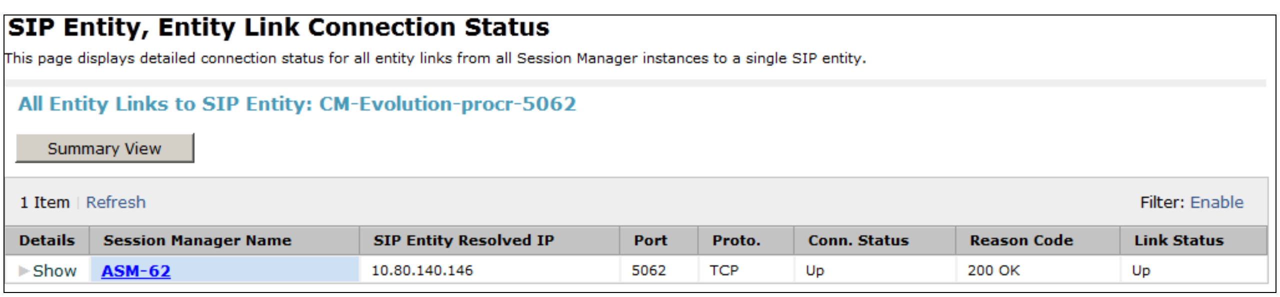




From the list of monitored entities, select an entity of interest, such as "Avaya-SBCE-1". Under normal operating conditions, the **Link Status** should be "Up" as shown in the example screen below.

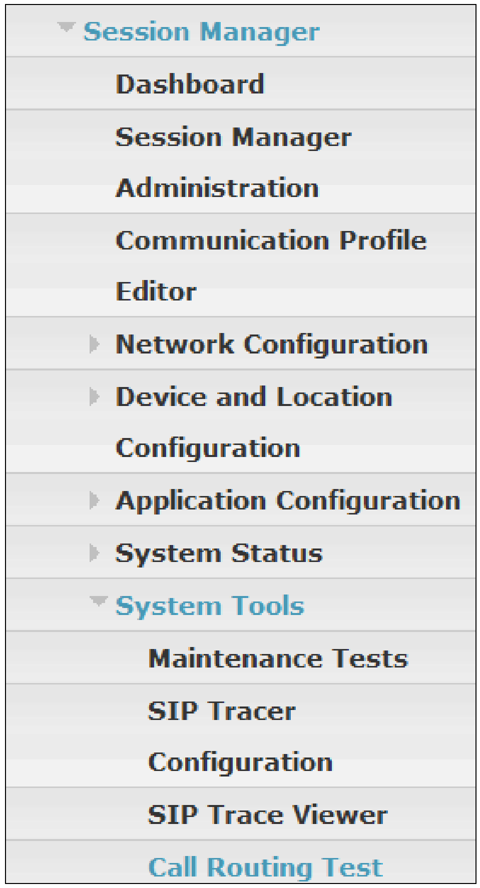


Return to the list of monitored entities, and select another entity of interest, such as "CM-Evolution-procr-5062". Under normal operating conditions, the **Link Status** should be "Up" as shown in the example screen below. Note the use of port 5062.

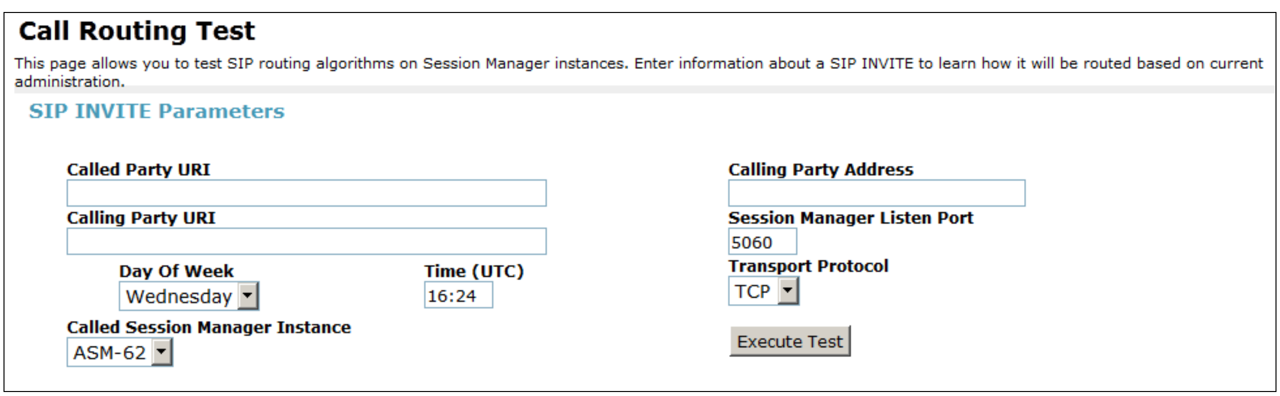


9.3.2 Call Routing Test

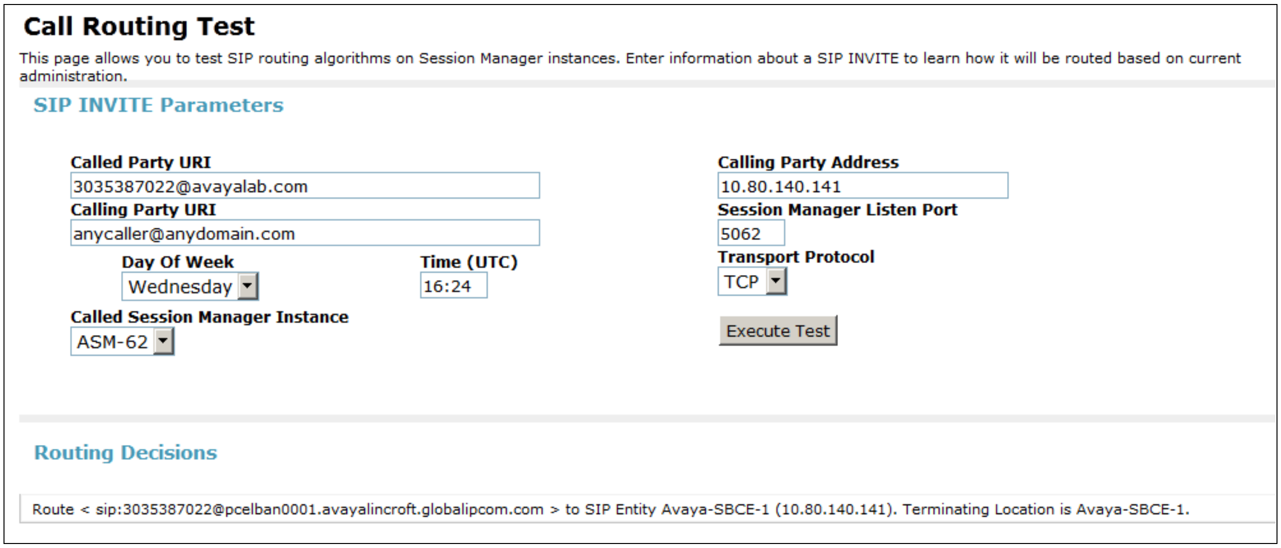
The **Call Routing Test** verifies the routing for a particular source and destination. To run the routing test, expand **Elements → Session Manager → System Tools → Call Routing Test**, as shown below.



A screen such as the following is displayed.



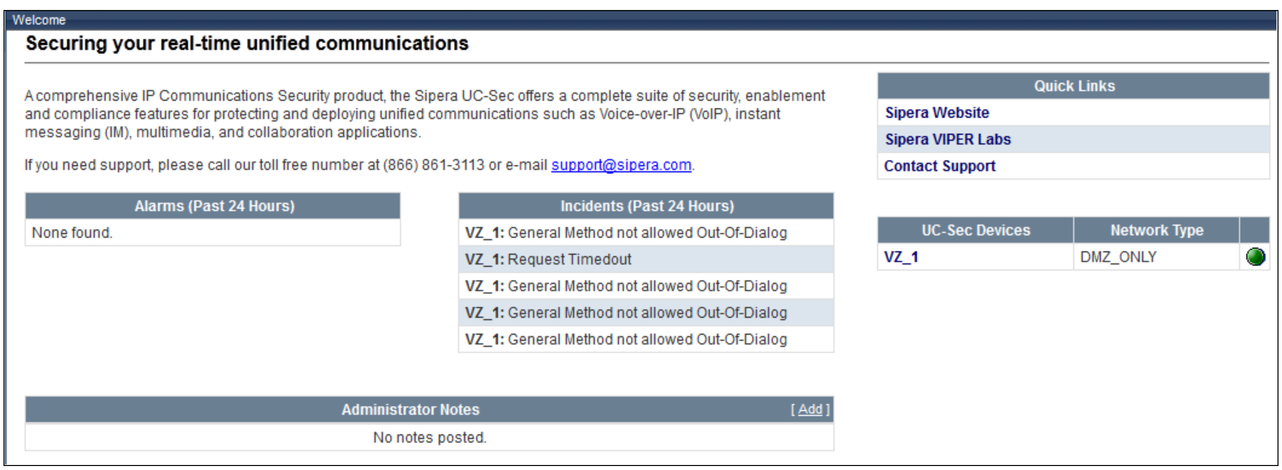
Populate the fields for the call parameters of interest. For example, the following screen shows an example call routing test for an outbound call to the PSTN via Verizon. Under **Routing Decisions**, observe that the call will route via an ASBCE on the path to Verizon. Scroll down to inspect the details of the **Routing Decision Process** if desired (not shown).



9.4. Avaya Session Border Controller for Enterprise Verification

9.4.1 Welcome Screen

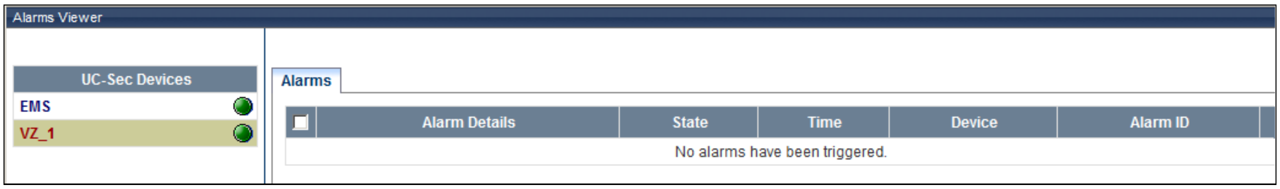
The welcome screen shows alarms, incidents, and the status of all managed ASBCEs at a glance.



9.4.2 Alarms

A lit of the most recent alarms can be found under the Alarm tab on the top left bar.

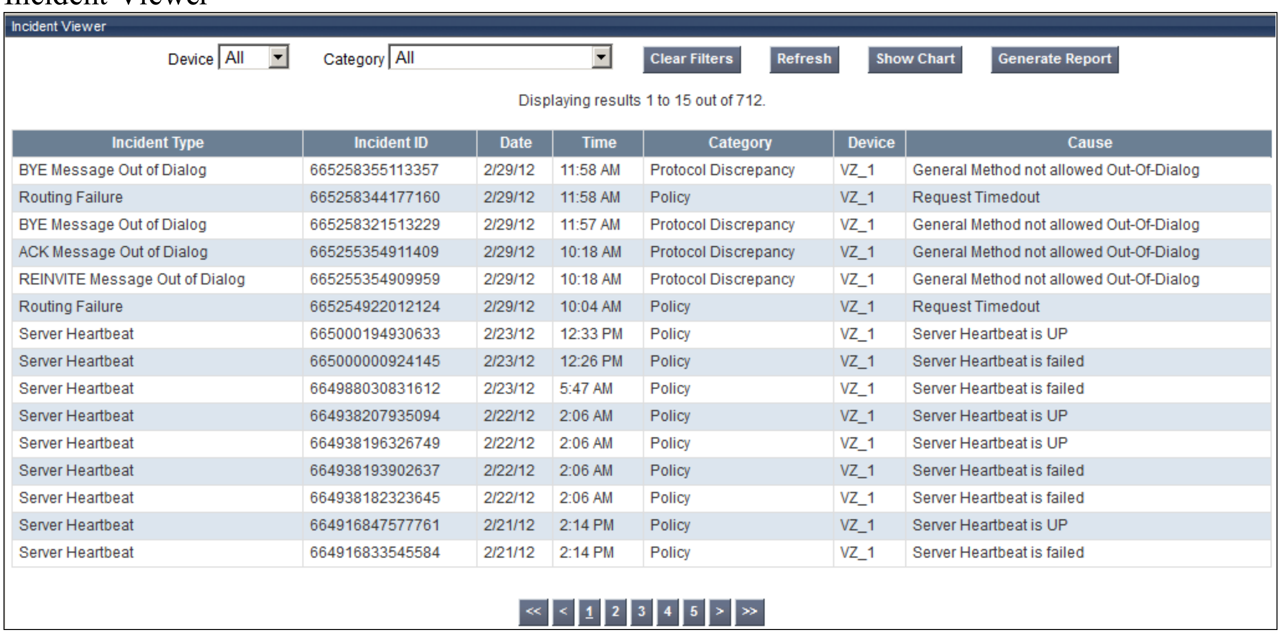
Alarms Viewer.



9.4.3 Incidents

A list of all recent incidents can be found under the incidents tab at the top left next to the Alarms.

Incident Viewer



Incident Viewer

Device All Category All Clear Filters Refresh Show Chart Generate Report

Displaying results 1 to 15 out of 712.

Incident Type	Incident ID	Date	Time	Category	Device	Cause
BYE Message Out of Dialog	665258355113357	2/29/12	11:58 AM	Protocol Discrepancy	VZ_1	General Method not allowed Out-Of-Dialog
Routing Failure	665258344177160	2/29/12	11:58 AM	Policy	VZ_1	Request Timedout
BYE Message Out of Dialog	665258321513229	2/29/12	11:57 AM	Protocol Discrepancy	VZ_1	General Method not allowed Out-Of-Dialog
ACK Message Out of Dialog	665255354911409	2/29/12	10:18 AM	Protocol Discrepancy	VZ_1	General Method not allowed Out-Of-Dialog
REINVITE Message Out of Dialog	665255354909959	2/29/12	10:18 AM	Protocol Discrepancy	VZ_1	General Method not allowed Out-Of-Dialog
Routing Failure	665254922012124	2/29/12	10:04 AM	Policy	VZ_1	Request Timedout
Server Heartbeat	665000194930633	2/23/12	12:33 PM	Policy	VZ_1	Server Heartbeat is UP
Server Heartbeat	665000000924145	2/23/12	12:26 PM	Policy	VZ_1	Server Heartbeat is failed
Server Heartbeat	664988030831612	2/23/12	5:47 AM	Policy	VZ_1	Server Heartbeat is failed
Server Heartbeat	664938207935094	2/22/12	2:06 AM	Policy	VZ_1	Server Heartbeat is UP
Server Heartbeat	664938196326749	2/22/12	2:06 AM	Policy	VZ_1	Server Heartbeat is UP
Server Heartbeat	664938193902637	2/22/12	2:06 AM	Policy	VZ_1	Server Heartbeat is failed
Server Heartbeat	664938182323645	2/22/12	2:06 AM	Policy	VZ_1	Server Heartbeat is failed
Server Heartbeat	664916847577761	2/21/12	2:14 PM	Policy	VZ_1	Server Heartbeat is UP
Server Heartbeat	664916833545584	2/21/12	2:14 PM	Policy	VZ_1	Server Heartbeat is failed

<< < 1 2 3 4 5 > >>

Further Information can be obtained by clicking on an incident in the incident viewer.

Incident Information			
General Information			
Incident Type	Server Heartbeat	**Category**	Policy
Timestamp	February 23, 2012 12:33:09 PM GMT	**Device**	VZ_1
Cause	Server Heartbeat is UP		
Message Data			
Response Code	200	**Transport**	TCP
Call ID	8d57142cb6a4bb2db3ab5301a040b218shiepaerrtab	**From**	sip:ping@avayalab.com
To	sip:ping@avayalab.com	**Source IP**	10.80.140.160
Destination IP	10.80.140.141		

9.4.4 Diagnostics

The full diagnostics check that can be run can run line checks in both directions.

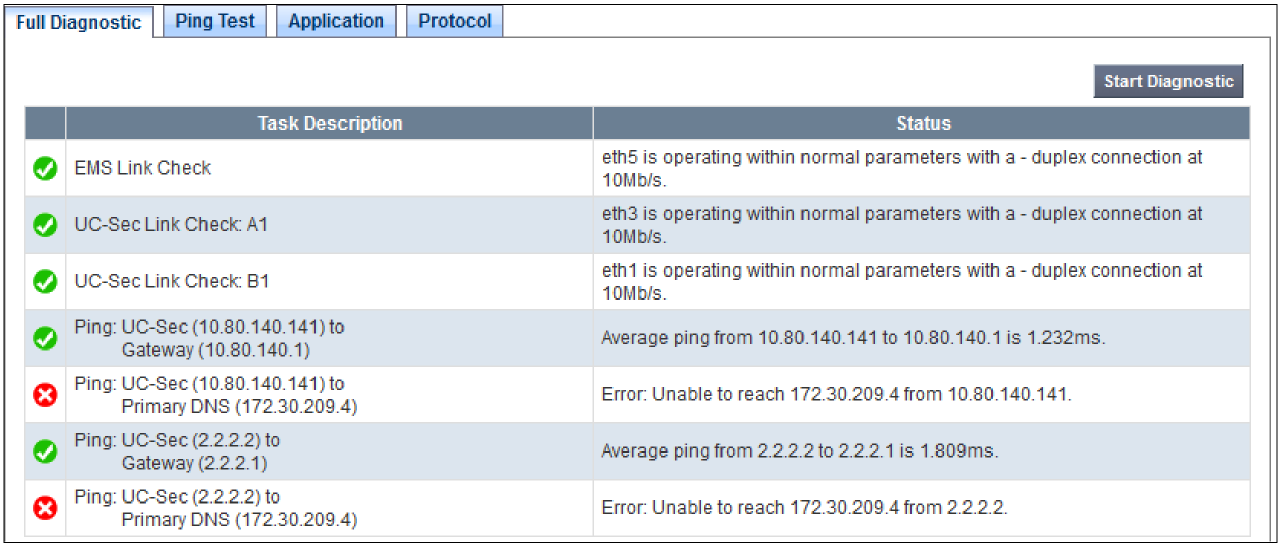
Click on Diagnostics on the top bar, select your ASBCE from the list of devices and then click "Start Diagnostics"

Full Diagnostic | Ping Test | Application | Protocol

Start Diagnostic

Task Description	Status
EMS Link Check	
UC-Sec Link Check: A1	
UC-Sec Link Check: B1	
Ping: UC-Sec (10.80.140.141) to Gateway (10.80.140.1)	
Ping: UC-Sec (10.80.140.141) to Primary DNS (172.30.209.4)	
Ping: UC-Sec (2.2.2.2) to Gateway (2.2.2.1)	
Ping: UC-Sec (2.2.2.2) to Primary DNS (172.30.209.4)	

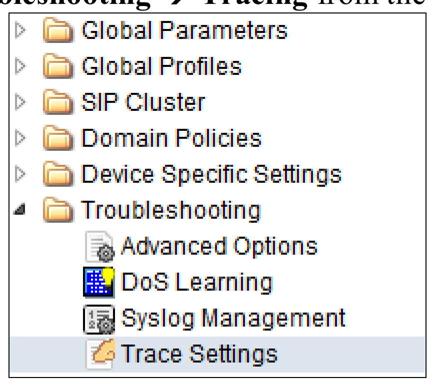
A green check mark or a red x will indicate success or failure.



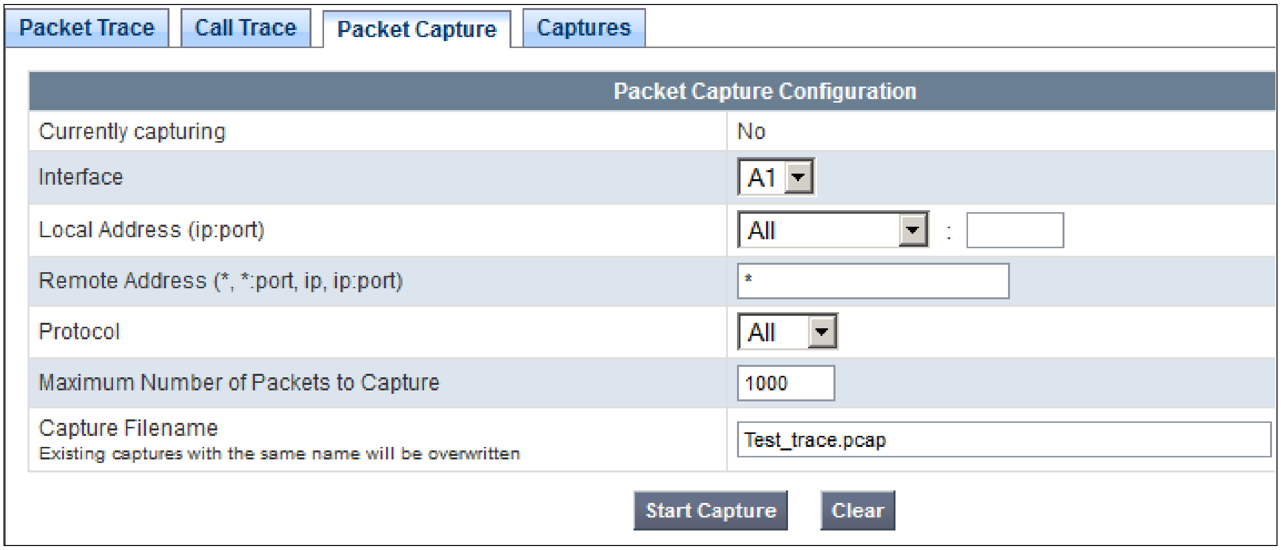
	Task Description	Status
✓	EMS Link Check	eth5 is operating within normal parameters with a - duplex connection at 10Mb/s.
✓	UC-Sec Link Check: A1	eth3 is operating within normal parameters with a - duplex connection at 10Mb/s.
✓	UC-Sec Link Check: B1	eth1 is operating within normal parameters with a - duplex connection at 10Mb/s.
✓	Ping: UC-Sec (10.80.140.141) to Gateway (10.80.140.1)	Average ping from 10.80.140.141 to 10.80.140.1 is 1.232ms.
✗	Ping: UC-Sec (10.80.140.141) to Primary DNS (172.30.209.4)	Error: Unable to reach 172.30.209.4 from 10.80.140.141.
✓	Ping: UC-Sec (2.2.2.2) to Gateway (2.2.2.1)	Average ping from 2.2.2.2 to 2.2.2.1 is 1.809ms.
✗	Ping: UC-Sec (2.2.2.2) to Primary DNS (172.30.209.4)	Error: Unable to reach 172.30.209.4 from 2.2.2.2.

9.4.5 Tracing

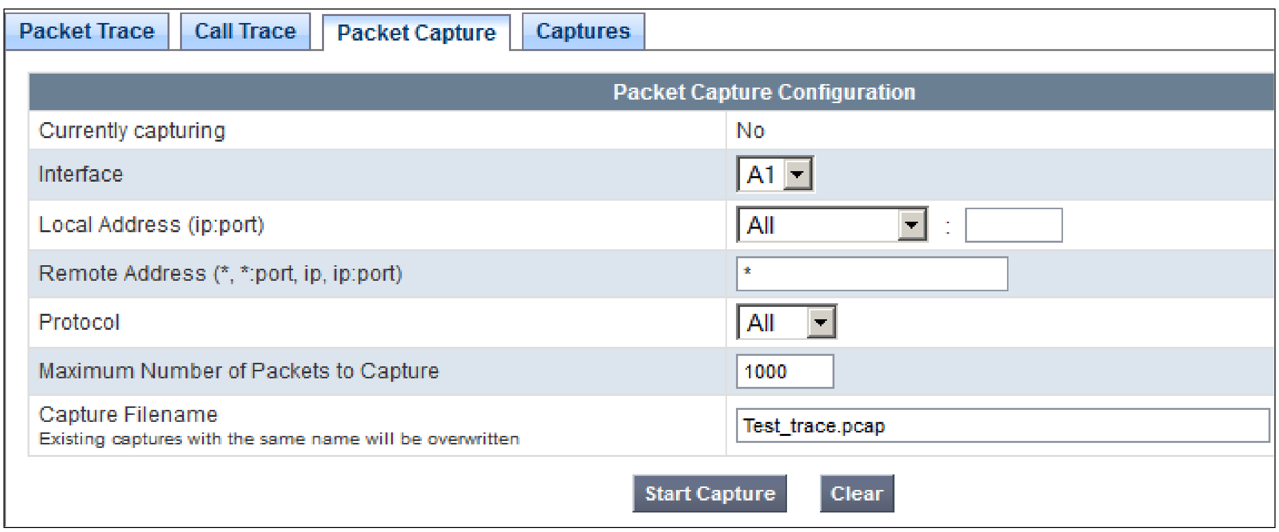
To take a call trace, Select **Troubleshooting → Tracing** from the left-side menu as shown below.



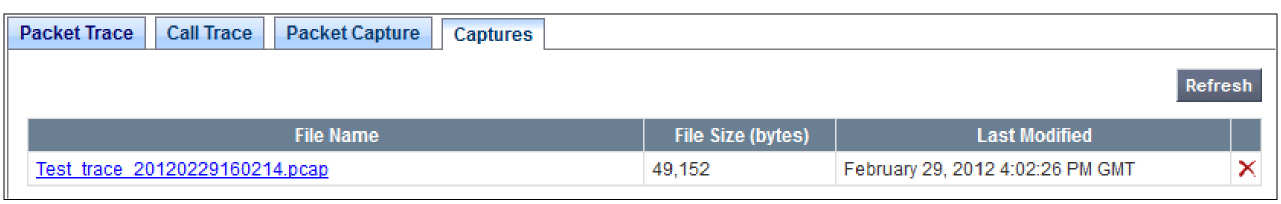
Select the Packet Capture tab and set the desired configuration for a call trace, hit **Start Capture**. Only one interface can be selected at once, so only an inside or only an outside trace is possible.



When tracing is has reached the desired number of packets the trace will stop automatically, or alternatively, hit the Stop Capture button at the bottom.



Select the Captures tab at the top and you capture will be listed, you can select the File Name and choose to open it with an application like Wireshark.



10. Conclusion

As illustrated in these Application Notes, Avaya Aura® Communication Manager 6.2, Avaya Aura® Session Manager 6.2, and Avaya Session Border Controller for Enterprise can be configured to interoperate successfully with Verizon Business IP Trunk service, inclusive of the "2-CPE" SIP trunk redundancy architecture. This solution allows Avaya Aura® Communication Manager and Avaya Aura® Session Manager users access to the PSTN using a Verizon Business IP Trunk public SIP trunk service connection.

11. Additional References

11.1. Avaya

Avaya product documentation, including the following, is available at http://support.avaya.com

[1] *Installing and Configuring Avaya Aura® Communication Manager*, Doc ID 03-603558, Release 6.2
[2] *Administering Avaya Aura® Communication Manager*, Doc ID 03-300509
[3] *Administering Avaya Aura® Session Manager*, Doc ID 03-603324
[4] *Installing and Configuring Avaya Aura® Session Manager,* Doc ID 03-603473
[5] *Maintaining and Troubleshooting Avaya Aura® Session Manager,* Doc ID 03-603325
[6] *Administering Avaya Aura® System Manager*, Document Number 03-603324

Avaya Application Notes are also available at http://support.avaya.com

11.2. Verizon Business

The following documents may be obtained by contacting a Verizon Business Account Representative.

[7] *Retail VoIP Interoperability Test Plan*
[8] *Network Interface Specification Retail VoIP Trunk Interface (for non-registering devices)*

Appendix A: Unscreened ANI Testing and Configuration

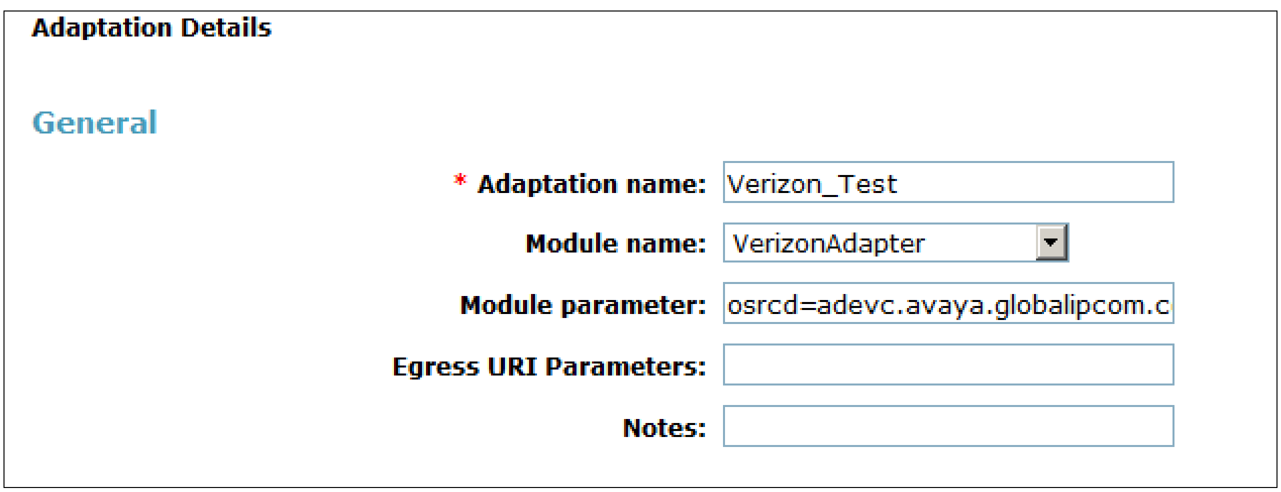
Unscreened ANI is a Verizon offered service (available with VoIP IP Integrated Access and VoIP IP Trunking) and is a new feature being offered with Session Manager 6.2. This service was tested successfully in this test configuration and can be implemented by following the steps here.

This feature allows Customer to send an "unscreened" ANI to the Company's network which is then displayed to the called party as Caller ID. An "unscreened" ANI can be any telephone number that Customer passes through the Company's network for Caller ID display purposes only. There is no charge for this feature. If Customer selects this feature, Verizon will designate one of Customer's assigned telephone numbers as a "Screened Telephone Number" for each Customer unique location. Verizon will use the Screened Telephone Number to determine call origination for billing, call routing and E911 support. The customer is responsible for configuring its IP-PBX, PBX or other devices to accommodate and properly process the Screened Telephone Number.

The Screened Telephone Number provided by Verizon for this test is 732-945-0821. Typically, customers would have one or more screened telephone number, one for every location and a central Session Manager could be used to pass multiple screened telephone numbers to Verizon based on a Matching Pattern (i.e. a user's Calling Line Identification).

Login to Session Manager as shown in **Section 6** above, navigate to Routing→Adaptations, and select "New".

Create a unique name for the Adaptation, here "Verizon_Test". Select the "VerizonAdapter" for the **Module Name**. In module parameter enter any domain adaptions that may be needed. Here the domains known to Verizon needed to overwrite the internal lab environment name of "avayalab.com" so a **Module Parameter** of "osrcd=adevc.avaya.globalipcom.com odstd=pcelban0001.avayalincroft.globalipcom.com fromto=true" was used.



Scroll down to the **Digit Conversion for Outgoing Calls from SM** section, enter a **Matching Pattern** (e.g. 732-945-0240), with the **Min** and **Max** number of digits to match on, in **Address to modify**, enter **origination**, and in the **Adaptation Data** enter the screened telephone number (e.g. 732-945-0821) provided by Verizon. Click **Commit**.

Digit Conversion for Outgoing Calls from SM

Add Remove

3 Items | Refresh Filter: Enable

	Matching Pattern	Min	Max	Phone Context	Delete Digits	Insert Digits	Address to modify	Adaptation Data	Notes
☐	* 7329450240	* 10	* 10		* 0		origination	7329450821	
☐	* 7329450285	* 10	* 10		* 0		origination	7329450821	
☐	* 7329450287	* 10	* 10		* 0		origination	7329450821	

Select : All, None

Once the Adaptation has been committed it needs to be applied to a SIP Entity. Back at the Routing screen, select SIP Entities as shown in the Session manager section above, and select the "Avaya-SBCE-1" entity. Under Adaptation, change to the newly created "Verizon_Test" adaptation.

SIP Entity Details

General

* **Name:** Avaya-SBCE-1

* **FQDN or IP Address:** 10.80.140.141

Type: Other

Notes: Sipera-SBC-1 Outside 2.2.2.2

Adaptation: Verizon_Test

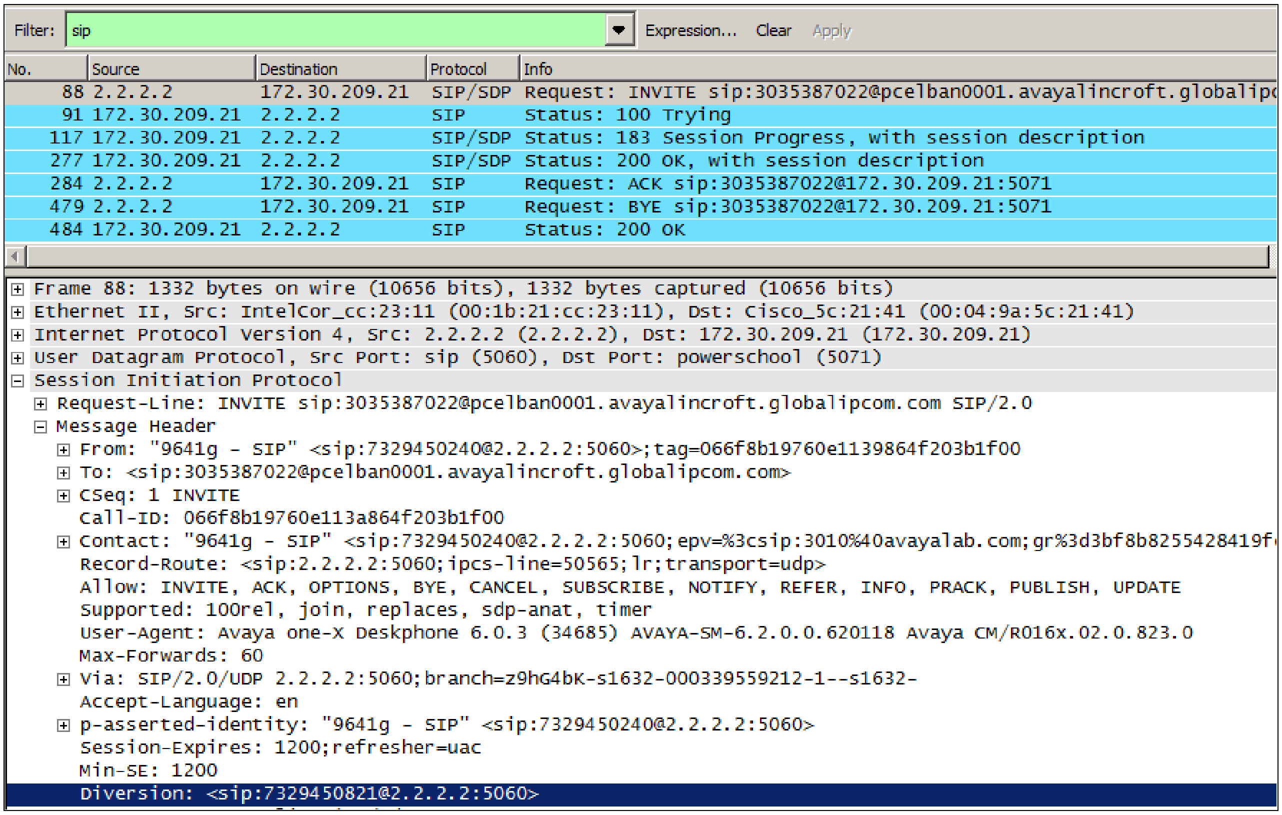
Location: Avaya-SBCE-1

Verification

In the following filter Wireshark trace, it is observed that the From line contains the DID number, 732-945-0240 and in the p-asserted identity section, a Diversion header has been added with the screened ANI (732-945-0821).

From: "9641g - SIP" <sip:**7329450240**@2.2.2.2:5060>;tag=066f8b19760e1139864f203b1f00

Diversion: sip:**7329450821**@2.2.2.2:5060>


Filter: sip
Expression... Clear Apply
No. Source Destination Protocol Info
88 2.2.2.2 172.30.209.21 SIP/SDP Request: INVITE sip:3035387022@pcelban0001.avayalincroft.globalipc
91 172.30.209.21 2.2.2.2 SIP Status: 100 Trying
117 172.30.209.21 2.2.2.2 SIP/SDP Status: 183 Session Progress, with session description
277 172.30.209.21 2.2.2.2 SIP/SDP Status: 200 OK, with session description
284 2.2.2.2 172.30.209.21 SIP Request: ACK sip:3035387022@172.30.209.21:5071
479 2.2.2.2 172.30.209.21 SIP Request: BYE sip:3035387022@172.30.209.21:5071
484 172.30.209.21 2.2.2.2 SIP Status: 200 OK
Frame 88: 1332 bytes on wire (10656 bits), 1332 bytes captured (10656 bits)
Ethernet II, Src: IntelCor_cc:23:11 (00:1b:21:cc:23:11), Dst: Cisco_5c:21:41 (00:04:9a:5c:21:41)
Internet Protocol Version 4, Src: 2.2.2.2 (2.2.2.2), Dst: 172.30.209.21 (172.30.209.21)
User Datagram Protocol, Src Port: sip (5060), Dst Port: powerschool (5071)
Session Initiation Protocol
Request-Line: INVITE sip:3035387022@pcelban0001.avayalincroft.globalipcom.com SIP/2.0
Message Header
From: "9641g - SIP" <sip:7329450240@2.2.2.2:5060>;tag=066f8b19760e1139864f203b1f00
To: <sip:3035387022@pcelban0001.avayalincroft.globalipcom.com>
CSeq: 1 INVITE
Call-ID: 066f8b19760e113a864f203b1f00
Contact: "9641g - SIP" <sip:7329450240@2.2.2.2:5060;epv=%3csip:3010%40avayalab.com;gr%3d3bf8b8255428419f
Record-Route: <sip:2.2.2.2:5060;ipcs-line=50565;lr;transport=udp>
Allow: INVITE, ACK, OPTIONS, BYE, CANCEL, SUBSCRIBE, NOTIFY, REFER, INFO, PRACK, PUBLISH, UPDATE
Supported: 100rel, join, replaces, sdp-anat, timer
User-Agent: Avaya one-X Deskphone 6.0.3 (34685) AVAYA-SM-6.2.0.0.620118 Avaya CM/R016x.02.0.823.0
Max-Forwards: 60
Via: SIP/2.0/UDP 2.2.2.2:5060;branch=z9hG4bK-s1632-000339559212-1--s1632-
Accept-Language: en
p-asserted-identity: "9641g - SIP" <sip:7329450240@2.2.2.2:5060>
Session-Expires: 1200;refresher=uac
Min-SE: 1200
Diversion: <sip:7329450821@2.2.2.2:5060>

Appendix B: Avaya Session Border Control for Enterprise – Sigma Script "EXAMPLE 2"

```
within session "ALL"
{
 act on request where %DIRECTION="OUTBOUND" and
%ENTRY_POINT="POST_ROUTING"
  {
// Topology Hiding of P-Location header for subsequent re-INVITEs

   remove(%HEADERS["P-Location"][1]);
   remove(%HEADERS["Endpoint-View"][1]);
   remove(%HEADERS["Alert-Info"][1]);

  }
 }

 within session "ALL"
{
 act on response where %DIRECTION="OUTBOUND" and
%ENTRY_POINT="POST_ROUTING"
  {
// Topology Hiding of P-Location header for subsequent re-INVITEs

   remove(%HEADERS["P-Location"][1]);
   remove(%HEADERS["Endpoint-View"][1]);
   remove(%HEADERS["Alert-Info"][1]);

  }
 }
```

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.