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 Contact Center IP-IVR – Issue 1.0

Abstract

These Application Notes describe a sample configuration of Avaya Aura® Communication Manager 6.2, Avaya Aura® Session Manager 6.2, and Avaya Session Border Controller for Enterprise with Verizon Business IP Contact Center (IPCC) IP-IVR service. The Verizon Business IPCC Services suite includes the IP Toll Free VoIP Inbound and IP-IVR SIP trunk service offers. These Application Notes illustrate IP-IVR service and are a companion to previously published Application Notes illustrating IP Toll Free VoIP Inbound.

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 in the Avaya Solution & Interoperability Test Lab, utilizing a Verizon Business Private IP (PIP) circuit connection to the production Verizon Business IPCC Services.

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 describe a sample configuration of Avaya Aura® Communication Manager 6.2, Avaya Aura® Session Manager 6.2, and Avaya Session Border Controller for Enterprise with Verizon Business IP Contact Center (IPCC) Services suite. The Verizon Business IPCC Services suite includes the IP Toll Free VoIP Inbound and IP-IVR SIP trunk service offers. Access to these Verizon features may use Internet Dedicated Access (IDA) or Private IP (PIP). These Application Notes illustrate IP-IVR service using PIP access, and are a companion to previously published Application Notes illustrating IP Toll Free VoIP Inbound with PIP access (reference [VZ-IPTF] in **Section 11**).

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.

In the sample configuration, an Avaya Session Border Controller for Enterprise (SBCE) is used as an edge device between the Avaya CPE and Verizon Business. The Avaya SBCE performs SIP header manipulation and provides topology hiding. Avaya Aura® Session Manager is used as the Avaya SIP trunking "hub" connecting to Avaya Aura® Communication Manager, the Avaya SBCE, and other applications.

Verizon Business IPCC is a portfolio of interaction services that include IP Toll Free and IP Interactive Voice Response (IP-IVR). IP Toll Free is the base service offering that includes call routing and termination features as well as basic and enhanced transfer capabilities. Consult reference [VZ-IPTF] for a sample configuration illustrating IP Toll Free. IP-IVR is an enhanced service offering that is built on top of IP Toll Free, and includes features such as menu-routing, customer transfer, and additional media capabilities. Customer use of IP-IVR is predicated upon having IP Toll Free service.

For more information on the Verizon Business IP Contact Center service, visit
http://www.verizonbusiness.com/Products/communications/contact-center/

2. General Test Approach and Test Results

The Avaya equipment depicted in **Figure 1** was connected to the commercially available Verizon Business IPCC IP Toll-Free and IP-IVR Services. This allowed PSTN users to dial toll-free telephone numbers assigned by Verizon. For IP-IVR, the PSTN user dials the IP-IVR "Published Number", and the IP-IVR Service sends the corresponding IP-IVR "Outdial Number" to the CPE in the Request-URI of the SIP INVITE. Calls were configured to be routed within the enterprise to Avaya Aura® Communication Manager extensions, including Vector Directory Numbers (VDNs). The VDNs were associated with vectors configured to exercise basic Communication Manager ACD functions.

The test approach was manual testing of inbound calls from the PSTN using the Verizon IPCC Services on a production Verizon PIP access circuit, as shown in **Figure 1**. The testing summarized in **Section 2.1** was successful. Test observations or limitations are described in **Section 2.2.** See **Section 9** for verifications and Wireshark traces illustrating representative call flows.

2.1. Interoperability Compliance Testing

The interoperability compliance testing included the execution of test cases from the Verizon-authored interoperability test plan [VZ-Test-Plan].

- SIP OPTIONS monitoring of the health of the SIP trunks was verified. Both the Avaya enterprise equipment and Verizon Business can monitor health using SIP OPTIONS.
- Incoming calls from the PSTN were routed to the IP-IVR numbers assigned by Verizon Business to the Avaya location. Configuration was varied such that these incoming calls were directed to Communication Manager telephone extensions and Communication Manager VDNs.
- Proper disconnect when either the PSTN caller or the Communication Manager party hangs up an active call.
- Proper disconnect when the PSTN caller abandons (i.e., hangs up) a call before the call has been answered.
- Proper SIP 486 response when a PSTN user calls an IP-IVR number directed to a busy user or resource when no redirection on busy conditions was configured (which would be unusual in a contact center).
- Proper termination of an inbound IP-IVR call left in a ringing state for a relatively long duration, which again would be unusual in a contact center. In the sample configuration, Verizon sent a SIP CANCEL to cancel the call after 36 seconds of ring no answer conditions.
- Privacy requests for inbound IP-IVR calls from the PSTN were verified. That is, when privacy is requested by a PSTN caller (e.g., dialing *67 from a mobile phone), the inbound IP-IVR call can be successfully completed while withholding presentation of the PSTN caller id from user displays. (When the caller requests privacy, Verizon IP-IVR sends the caller ID in the P-Asserted-Identity header and includes "Privacy: id" which is honored by Communication Manager).
- Inbound IP-IVR call long holding time call stability. Communication Manager sends a re-INVITE with SDP to refresh the session at the configured session refresh interval specified on the Communication Manager trunk group handling the call. In the sample configuration, the session refresh re-INVITE was sent after 900 seconds (15 minutes), the interval configured for the trunk group in **Section 5.8**. The call continued with proper talk path.
- Telephony features such as hold and resume. When a Communication Manager user holds a call in the sample configuration, Communication Manager will send a re-INVITE to Verizon with a media attribute "sendonly". The Verizon 200 OK to this re-INVITE will include media attribute "recvonly". While the call remains on hold, RTP will flow from the Avaya CPE to Verizon, but no RTP will flow from Verizon to the Avaya CPE (i.e., as intended). When the user resumes the call from hold, bi-directional media path resumes. A Wireshark illustration is presented in **Section 9**. Although it would be unexpected in a contact center, calls on hold for longer than the session refresh interval were also tested, and such calls could continue to hear music on hold and could be resumed by the user after the session refresh.
- Transfer of IP-IVR calls between Communication Manager users.

- Incoming voice calls using the G.711 ULAW codec and proper protocol procedures related to media. Note that G.729A was validated with Verizon IPCC IP Toll Free as outlined in reference [VZ-IPTF]. On the production circuit used for testing, Verizon IP-IVR offered only G.711MU in SDP and therefore only G.711MU was tested with IP-IVR. A Wireshark illustration of the IP-IVR SDP Offer is presented in **Section 9**.
- DTMF transmission using RFC2833. For inbound IP-IVR calls, PSTN users dialing post-answer DTMF digits are recognized properly by the Avaya CPE.
- Proper DiffServ markings for SIP signaling and RTP media flowing from the Avaya CPE to Verizon.

2.2. Test Results

The interoperability compliance testing of the sample configuration was completed with successful results as described in **Section 2.1**. The following observations may be noteworthy:

- Verizon Business IPCC Services suite does not support fax.
- Verizon Business IPCC Services suite does not support History Info or Diversion Headers. The Avaya CPE will not send History-Info or Diversion header to Verizon IPCC in the sample configuration.
- Verizon Business IPCC Services suite does not support G.729 Annex b. When using G729, the Avaya CPE will always include "annexb=no" in SDP in the sample configuration.
- Reference [JRR-VZIPCC] described potential problems with call hold and resume, and transfer when the Network Call Redirection flag was set to "y" on a Communication Manager Release 6.0 trunk group. In reference [JRR-VZIPCC], user perceivable problems were averted using SBC manipulation of the SIP signaling. In the verification of these Application Notes for Communication Manager Release 6.2, it is not necessary to implement an SBC workaround to the issue. As background, the "sendonly" media attribute in SDP is sent by Communication Manager when the Network Call Redirection (NCR) field on the SIP trunk is enabled and a call is on hold at the enterprise site. For example, when a call is placed on hold listening to music sourced from an Avaya G450 Media Gateway, Communication Manager signals a "sendonly" condition and Verizon replies with a "recvonly" condition. In this state, while music is being heard by the PSTN caller, RTP media is flowing from the CPE to Verizon only.
    - In the prior testing associated with reference [JRR-VZIPCC], if Communication Manager Network Call Redirection (NCR) is enabled for the SIP trunk group used for the call, and a Verizon IP-IVR call is on hold listening to music on hold from the Avaya CPE, the music on hold would cease to be heard by the caller if a refresh re-INVITE is sent to Verizon while the call is on hold. Using the set of products and releases covered by these Application Notes, this scenario was re-tested, and the problem no longer occurs. The music on hold continues to be heard, even after the session refresh re-INVITE. After the exchange of SIP messages stimulated by a session refresh re-INVITE while a call is on hold for longer than the refresh interval, in the prior testing associated with reference [JRR-VZIPCC], the audio path could not be re-established when the user tried to resume the call. In the set of products and releases covered by these Application Notes, this scenario was re-tested and the problem no longer occurs. That is, the user may resume the call with full media path even if the call had been on hold for longer than the session refresh interval.

- In the prior testing associated with reference [JRR-VZIPCC], if Communication Manager Network Call Redirection (NCR) is enabled for the SIP trunk group used for the call, traditional transfer of an inbound call to another CPE telephone could result in no talk path conditions with the Verizon network after the transfer operation was completed. In the set of products and releases covered by these Application Notes, this scenario was re-tested and the problem no longer occurs. Bi-directional talk path is present after a transfer of a Verizon IP-IVR call from one Communication Manager user to another, with NCR enabled on the SIP trunk group.

- The Session Manager Call Routing Test shown in **Section 9.3.2** of these Application Notes did not work properly when the Session Manager Listen Port was set to 5060, which is the port on which Session Manager receives the INVITE from the Avaya SBCE. The screen in **Section 9.3.2** shows the port set to a port other than 5060, which enabled the Call Routing test to show routing results. This observation affects the Call Routing test functionality only and has no bearing on the actual processing of calls, which were successful using TCP port 5060 between Session Manager and the SBC. This observation is under investigation (Session Manager WI00987473).
- The presence of Avaya generated SIP headers that Verizon need not receive, such as "P-Location", in a SIP message sent to Verizon does not cause any user-perceivable problems. Nevertheless, for consistency with previously published Application Notes, SBC procedures are shown in **Section 7.8** to illustrate how headers such as P-Location that are not required by Verizon may be removed by the Avaya SBC for Enterprise. The SBC procedures shown are effective in removing P-Location from INVITE, and 18x responses. However, ACKs sent from the CPE to Verizon may still contain a P-Location header in the sample configuration. This observation is under investigation (Avaya SBCE, Aurora-158).

2.3. Support

2.3.1 Avaya

For technical support, visit http://suppport.avaya.com

2.3.2 Verizon

For technical support, visit http://www.verizonbusiness.com/us/customer/

3. Reference Configuration

Figure 1 illustrates the sample configuration used for the DevConnect compliance testing. The configuration is comprised of the Avaya CPE location connected via a T1 Internet connection to the Verizon Business IPCC service node. The Avaya CPE location simulates a customer site. At the edge of the Avaya CPE location is an Avaya Session Border Controller for Enterprise. The enterprise SBC receives traffic from Verizon on port 5060 and sends traffic to Verizon using destination port 5072, using UDP for transport. The PIP service defines a secure MPLS connection between the Avaya CPE T1 connection and the Verizon IPCC service node. **Figure 1** includes both the IP Toll-Free VoIP Inbound numbers illustrated in reference [VZ-IPTF] as well as the IP-IVR numbers that are the focus of these Application Notes. The PSTN user dials the IP-IVR "Published" number, and Verizon sends the IP-IVR "Outdial" number to the enterprise.

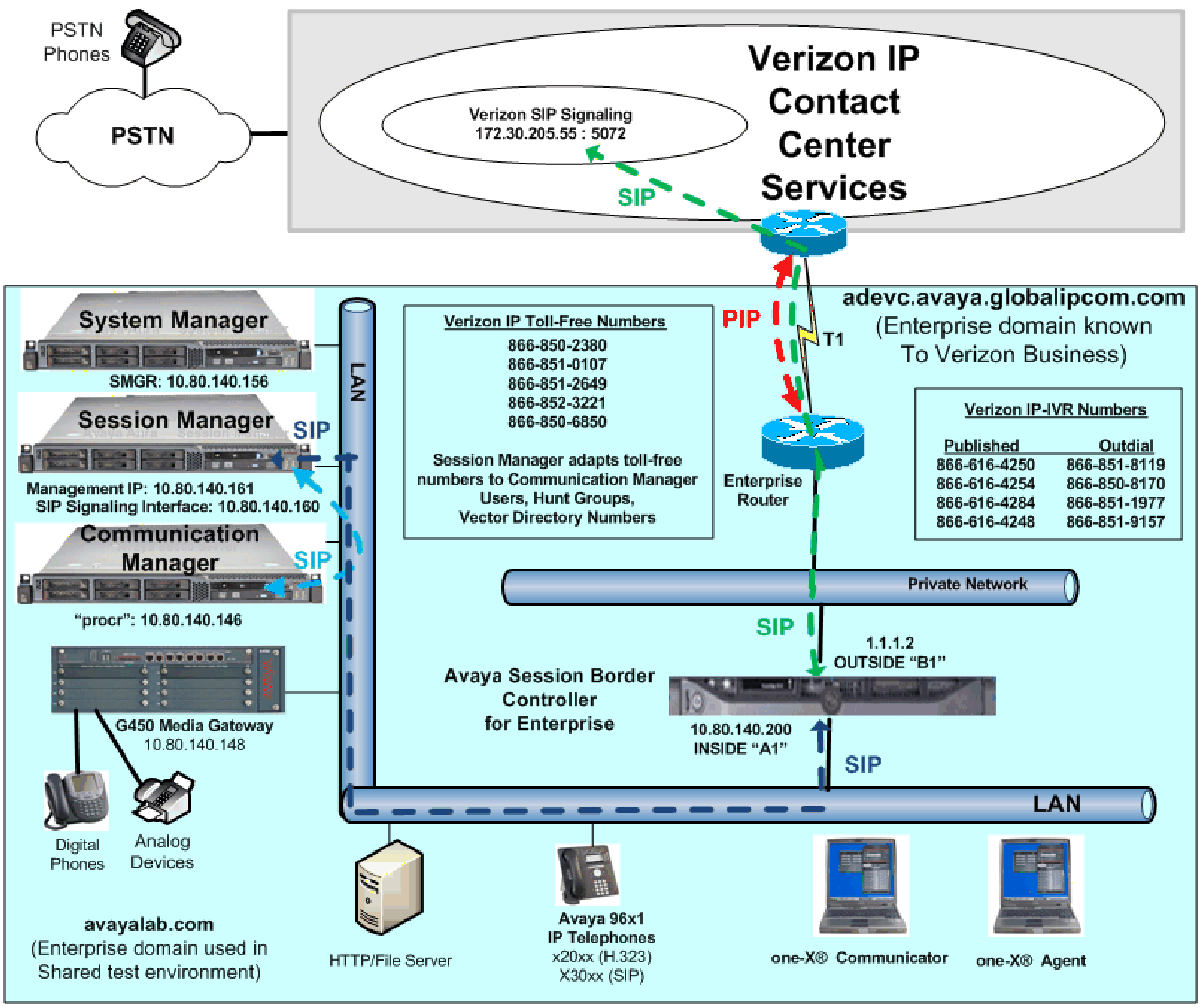


Figure 1: Avaya Interoperability Test Lab Configuration

The Verizon IP-IVR "Outdial" numbers shown in **Figure 1** were mapped by Session Manager to various Communication Manager extensions. The extension mappings were varied during the testing to allow inbound calls to terminate directly on user extensions or indirectly through hunt groups, vector directory numbers (VDNs) and vectors to user extensions and contact center agents.

The Avaya CPE environment was known to Verizon as domain *adevc.avaya.globalipcom.com*. For efficiency, the Avaya CPE environment utilizing Session Manager Release 6.2 and Communication Manager Release 6.2 was shared among other ongoing test efforts at the Avaya Solutions and Interoperability Test lab. Access to the Verizon Business IPCC services was added to a configuration that already used domain "avayalab.com" at the enterprise. As such, Session Manager or the SBC are used to adapt the domains as needed. These Application Notes indicate the configuration that would not be required in cases where the CPE domain in Communication Manager and Session Manager match the CPE domain known to Verizon.

The following summarizes various header contents and manipulations for IP-IVR calls in the sample configuration:

- Verizon sends the following in the initial INVITE to the CPE (see Wireshark in **Section 9**):
    - The IP-IVR Outdial number and the CPE FQDN of ***adevc.avaya.globalipcom.com*** in the Request URI and To header.
    - The PSTN Caller ID and the Verizon gateway IP address in the From header and P-Asserted-Identity header.
    - Sends the INVITE to Avaya CPE using destination port 5060 via UDP
- Avaya Session Border Controller for Enterprise sends Session Manager:
    - The Request URI contains ***avayalab.com***, to match the shared Avaya SIL test environment.
    - The host portion of the From header also contains ***avayalab.com***
    - The host portion of the To header also contains ***avayalab.com***
    - Sends the packet to Session Manager using destination port 5060 via TCP
- Session Manager to Communication Manager:
    - The Request URI contains ***avayalab.com***, to match the shared Avaya SIL test environment.
    - Session Manager sends to Communication Manager using destination port 5063 via TCP to allow Communication Manager to distinguish Verizon IPCC traffic from other traffic arriving from the same instance of Session Manager.

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 FQDNs and IP addressing appropriate for the unique customer environment.

4. Equipment and Software Validated

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

Equipment	Software
Avaya Aura® Communication Manager running on HP Common Server	Avaya Aura® Communication Manager Release 6.2 (823.0)
Avaya Aura® System Manager running on HP Common Server	Avaya Aura® System Manager Release 6.2
Avaya Aura® Session Manager running on HP Common Server	Avaya Aura® Session Manager Release 6.2
Avaya one-X® Communicator	Release 6.0.1.16 SP1
Avaya IP Agent	Release 2.5
Avaya 96x1-Series IP Telephones (H.323)	Release 6.0 SP5
Avaya 96x1-Series IP Telephones (SIP)	Release 6.0 SP3
Avaya 2400-Series Digital Telephones	N/A
Avaya Session Border Controller for Enterprise	Release 4.0.5 Q02

Table 1: Equipment and Software Used in the Sample Configuration

5. Configure Communication Manager Release 6.2

This section illustrates an example configuration allowing SIP signaling via the "Processor Ethernet" of Communication Manager 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 – For the Avaya servers and media gateways, the initial installation, configuration, and licensing are assumed to have been previously completed and are not discussed in these Application Notes. These Application Notes focus on describing the sample configuration as it relates to SIP Trunking to Verizon IPCC.

Configuration is illustrated via the Communication Manager SAT interface. Screens are abridged for brevity in presentation.

5.1. Verify Licensed Features

The 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 IPCC Services and any other SIP applications. Each call from the Verizon Business IPCC Services to a non-SIP endpoint uses one SIP trunk for the duration of the call. Each call from Verizon Business IPCC Services to a SIP endpoint 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 12
             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 50
  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 4** of the **System-Parameters Customer-Options** form, verify that **IP Trunks** and **IP Stations** are enabled. If the use of SIP REFER messaging 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
```

On **Page 5** of the **System-Parameters Customer-Options** form, verify that the **Private Networking** and **Processor Ethernet** features are enabled if these features will be used, as is the case in the sample configuration.

```
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
```

On **Page 6** of the **System-Parameters Customer-Options** form, verify that any required call center features are enabled.

```
display system-parameters customer-options                   Page   6 of  11
                          CALL CENTER OPTIONAL FEATURES

                           Call Center Release: 6.0

                                 ACD? y                           Reason Codes? y
                        BCMS (Basic)? y              Service Level Maximizer? n
          BCMS/VuStats Service Level? y             Service Observing (Basic)? y
  BSR Local Treatment for IP & ISDN? y     Service Observing (Remote/By FAC)? y
                   Business Advocate? n              Service Observing (VDNs)? y
                     Call Work Codes? y                            Timed ACW? y
        DTMF Feedback Signals For VRU? y                   Vectoring (Basic)? y
                    Dynamic Advocate? n                Vectoring (Prompting)? y
        Expert Agent Selection (EAS)? y             Vectoring (G3V4 Enhanced)? y
                             EAS-PHD? y              Vectoring (3.0 Enhanced)? y
                    Forced ACD Calls? n    Vectoring (ANI/II-Digits Routing)? y
                Least Occupied Agent? y    Vectoring (G3V4 Advanced Routing)? y
           Lookahead Interflow (LAI)? y                    Vectoring (CINFO)? y
Multiple Call Handling (On Request)? y      Vectoring (Best Service Routing)? y
    Multiple Call Handling (Forced)? y                  Vectoring (Holidays)? y
  PASTE (Display PBX Data on Phone)? y                 Vectoring (Variables)? y
```

On **Page 7** of the **System-Parameters Customer-Options** form, verify that the required call center capacities can be met. In the sample configuration, agents will log in (using agent-login IDs) to staff the ACD and handle inbound calls from Verizon IP-IVR.

```
display system-parameters customer-options                    Page   7 of  11
                         CALL CENTER OPTIONAL FEATURES

           VDN of Origin Announcement? y                          VuStats? y
               VDN Return Destination? y         VuStats (G3V4 Enhanced)? y

                                                 USED
                    Logged-In ACD Agents: 10000 0
               Logged-In Advocate Agents: 10000 0
           Logged-In IP Softphone Agents: 10000 0
               Logged-In SIP EAS Agents: 2500  0
```

5.2. Dial Plan

In the sample configuration, the Avaya CPE environment uses four digit local extensions, such as 2xxx, 3xxx, and 4xxx. Trunk Access Codes (TAC) are 4 digits in length and begin with *1. The Feature Access Code (FAC) to access ARS is the single digit 9. 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
   *           1   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 abridged "display 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 (**10.80.140.146**) for the Processor Ethernet "procr" appears automatically due to the initial installation and configuration of the system. The text at the bottom of the screen provides the command syntax for listing, changing, or adding node names.

```
display 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

Use 'list node-names' command to see all the administered node-names
Use 'change node-names ip xxx' to change a node-name 'xxx' or add a node-name
```

5.4. IP Interface for procr

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 sample configuration. While the focus here is the use of the PE for SIP Trunk Signaling, observe that the Processor Ethernet will also be used for registrations from H.323 IP Telephones and H.248 gateways in the sample configuration.

```
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
           Subnet Mask: /24
```

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 5 was associated with other logical components used specifically for the Verizon IPCC 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 processor Ethernet (10.80.140.146), and that the G450 "MGP IPV4 Address" is 10.80.140.148. These fields are not configured in this screen, but rather display the current information for the 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 **MM712** media module supporting Avaya digital phones in slot **v2**, an **MM711** supporting analog devices in slot **v4**, 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:                                                        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 following screen illustrates a subset of the IP network map configuration used to verify these Application Notes. If the IP address of a registering H.323 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 H.323 IP telephone is in the ip-network-map, the phone can be assigned the network region assigned by the form shown below. For example, the IP address 10.10.103.10 would be mapped to network region 5, based on the bold configuration 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: 10.10.103.0                            /24    5      n
   TO: 10.10.103.255
```

The following screen shows IP Network Region 5 configuration. In the shared test environment, network region 5 is used to allow unique behaviors for the Verizon IPCC test environment. In this example, codec set 5 will be used for calls within region 5. The shared Avaya Solutions and Interoperability Test Lab environment uses the domain “avayalab.com” (i.e., for network region 1 including the region of the processor Ethernet “procr”). However, to illustrate the case where the 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**. The domain in the PAI header sent by Communication Manager to Session Manager will contain “avayalab.com”, the domain of the near-end of the Avaya signaling group. Session Manager will adapt “avayalab.com” to “adevc.avaya.globalipcom.com” in the PAI header as needed.

```
change ip-network-region 5                                      Page   1 of  20
                               IP NETWORK REGION
  Region: 5
Location:         Authoritative Domain: adevc.avaya.globalipcom.com
    Name: Verizon IPCC Testing
MEDIA PARAMETERS                Intra-region IP-IP Direct Audio: yes
      Codec Set: 5              Inter-region IP-IP Direct Audio: yes
   UDP Port Min: 2048                      IP Audio Hairpinning? n
   UDP Port Max: 3329
DIFFSERV/TOS PARAMETERS
 Call Control PHB Value: 46
        Audio PHB Value: 46
        Video PHB Value: 26
802.1P/Q PARAMETERS
 Call Control 802.1p Priority: 6
        Audio 802.1p Priority: 6
        Video 802.1p Priority: 5      AUDIO RESOURCE RESERVATION PARAMETERS
H.323 IP ENDPOINTS                                       RSVP Enabled? n
  H.323 Link Bounce Recovery? y
 Idle Traffic Interval (sec): 20
   Keep-Alive Interval (sec): 5
            Keep-Alive Count: 5
```

The following screen shows the inter-network region connection configuration for region 5. The first bold row shows that network region 5 is directly connected to network region 1, and that codec set 5 will also be used for any connections between region 5 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 5 for region 5 to region 1 connectivity.

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

 Source Region: 5     Inter Network Region Connection Management     I       M
                                                                     G  A    t
 dst codec direct   WAN-BW-limits   Video      Intervening      Dyn  A  G    c
 rgn  set   WAN  Units    Total Norm  Prio Shr Regions          CAC  R  L    e
 1    5     y    NoLimit                                             n       t
 2
 3
 4
 5    5                                                               all
```

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 5 will be used for connections between region 1 and region 5 as noted previously. In the shared test environment, network region 1 was in place prior to adding the Verizon IPCC test environment and already used **Authoritative Domain** "avayalab.com". Where necessary, Session Manager or the SBC can adapt the domain.

```
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 5, and that codec set 5 will be used for any connections between region 5 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    5     y    NoLimit                                             n       t
```

5.6. IP Codec Sets

The following screen shows the configuration for codec set 5, the codec set configured to be used for calls within region 5 and for calls between region 1 and region 5. In general, an IP codec set is a list of allowable codecs in priority order. Using the example configuration shown below, all calls with Verizon IPCC via the SIP trunks would use **G.729A** or **G.711MU**. (The Verizon IPCC service will not include G.722 in SDP offers or SDP answers). On the production circuit, the Verizon IP Toll Free VoIP Inbound service includes both G.729A and G.711MU in SDP Offers while the IP-IVR service included only G.711MU in the SDP Offer. Any calls using this same codec set that are between devices capable of the **G.722-64K** codec can use G.722. The specification of G.722 as the first choice is not required. G.722 may be omitted from the codec set, but it is recommended that G.729A and G.711MU be included in the codec set for use with Verizon IPCC Services.

```
change ip-codec-set 5                                           Page   1 of   2
                          IP Codec Set
    Codec Set: 5

    Audio        Silence      Frames   Packet
    Codec        Suppression  Per Pkt  Size(ms)
 1: G.722-64K                   2        20
 2: G.729A           n          2        20
 3: G.711MU          n          2        20
 4:
 5:
 6:
 7:
```

On **Page 2** of the form, configure the **FAX Mode** field to **off.** Verizon IPCC does not support fax.

```
change ip-codec-set 5                                           Page   2 of   2
                          IP Codec Set

                              Allow Direct-IP Multimedia? n

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

Although codec set 1 is not used for connections with Verizon IPCC, the following screen shows the configuration for codec set 1. Codec set 1 is used for local Avaya CPE 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: G.722-64K                   2        20
 2: G.711MU           n         2        20
 3: G.729A            n         2        20
 4:
 5:
 6:
 7:
```

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 "ASM6-2". In the example screens, the **Transport Method** for all signaling groups is "tcp". In production, TLS transport between Communication Manager and Session Manager may 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 77. Signaling group 77 will be used for processing incoming calls from Verizon IPCC Services via Session Manager. The **Far-end Network Region** is configured to region 5. Port 5063 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 IP toll-free and IP-IVR numbers to a route policy that uses a unique SIP Entity and SIP Entity link to Communication Manager specifying port 5063. The use of different ports is one means to allow Communication Manager to distinguish different types of calls arriving from the same Session Manager. Other parameters may be left at default values.

```
change signaling-group 77                                     Page   1 of   2
                                SIGNALING GROUP

 Group Number: 77             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: 5063                 Far-end Listen Port: 5063
                                         Far-end Network Region: 5
Far-end Domain:
                                              Bypass If IP Threshold Exceeded? n
Incoming Dialog Loopbacks: eliminate                   RFC 3389 Comfort Noise? n
         DTMF over IP: rtp-payload             Direct IP-IP Audio Connections? y
Session Establishment Timer(min): 3                      IP Audio Hairpinning? n
         Enable Layer 3 Test? y                     Initial IP-IP Direct Media? n
H.323 Station Outgoing Direct Media? n              Alternate Route Timer(sec): 6
```

The following screen shows signaling group 3, the signaling group to Session Manager that was in place prior to adding the Verizon IPCC configuration to the shared Avaya Solutions and Interoperability Test Lab configuration. This signaling group reflects configuration not specifically related to Verizon IPCC. For example, calls using Avaya SIP Telephones and calls routed to other Avaya applications can use this signaling group. 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 IPCC 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 IPCC 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.

NOTE: If Network Call Redirection (i.e., use of REFER to redirect calls back to Verizon) will be needed, at least one **Elite Agent license is <u>required</u>**. This license is required to enable the **ISDN/SIP Network Call Redirection** feature. This licensed feature must be turned **ON** to support Network Call Redirection.

The following shows page 1 for trunk group 77, which will be used for incoming IPCC 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. Although not strictly necessary, the **Direction** has been configured to "incoming" to emphasize that trunk group 77 is used for incoming calls only in the sample configuration.

```
change trunk-group 77                                           Page   1 of  21
                                TRUNK GROUP

Group Number: 77                   Group Type: sip           CDR Reports: y
  Group Name: Verizon IPCC                COR: 1        TN: 1        TAC: *177
   Direction: incoming       Outgoing Display? n
 Dial Access? n                                 Night Service:

Service Type: public-ntwrk          Auth Code? n
                                              Member Assignment Method: auto
                                                       Signaling Group: 77
                                                     Number of Members: 10
```

The following shows **Page 2** for trunk group 77. All parameters shown are default values, except for the **Preferred Minimum Session Refresh Interval**, which has been changed from the default 600 to 900 (seconds). Although it is not strictly necessary to make this change, some SIP products prefer a higher session refresh interval than the Communication Manager default value, which can result in unnecessary SIP messages to re-establish a higher refresh interval for each call.

```
change trunk-group 77                                           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

 Disconnect Supervision - In? y
             XOIP Treatment: auto    Delay Call Setup When Accessed Via IGAR? n
```

The following shows **Page 3** for trunk group 77. 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.

```
change trunk-group 77                                           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 shows **Page 4** for trunk group 77. The **PROTOCOL VARIATIONS** page is one reason why it can be advantageous to configure incoming calls from Verizon IPCC 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 introduced in Communication Manager Release 6. Verizon expects inbound calls to the enterprise to result in either a SIP 180 without SDP, or a SIP 183 with SDP. (That is, Verizon prefers not to receive a 180 containing SDP.) Setting **Convert 180 to 183 for Early Media** field to "y" for the trunk group handling inbound calls from Verizon produces the 183 with SDP result. Although not strictly necessary, the **Telephone Event Payload Type** has been set to 101 to match Verizon expectation. 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 "sendonly" media conditions for calls placed on hold at the enterprise site. If neither REFER signaling for NCR nor "sendonly" signaling is required, the **Network Call Redirection** field may be left at the default "n" value. In the testing associated with these Application Notes, the **Network Call Redirection** flag was set to "y".

The Verizon IPCC Services do not support the Diversion header or the History-Info header, and therefore both **Support Request History** and **Send Diversion Header** are set to "n".

```
change trunk-group 77                                             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? n
                    Support Request History? n
               Telephone Event Payload Type: 101

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

The following 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 Solutions and Interoperability Test Lab network. Recall that this trunk is used for communication with other Avaya applications and Avaya SIP Telephones, 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. Trunk group 3 also was configured to use private numbering.

```
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
 Show ANSWERED BY on Display? y
```

The following shows **Page 4** for trunk group 3. Unlike the trunk associated with Verizon IPCC that uses non-default "protocol variations", this trunk group maintains all default values.

```
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
       Identity for Calling Party Display: P-Asserted-Identity
                             Enable Q-SIP? n
```

5.9. Contact Center Configuration

This section illustrates basic commands used to configure Vector Directory Numbers (VDNs) and corresponding vectors. In general, call centers will use vector functionality that is more complex and tailored to individual needs, and such configuration is beyond the scope of these Application Notes. For examples of vectors that contain steps that invoke the Communication Manager SIP Network Call Redirection (NCR) functionality (i.e., Communication Manager sending of REFER stimulated by a call vector step), consult **Section 5.9** of the companion Application Notes in reference [VZ-IPTF].

5.9.1 Announcements

Various announcements may be used within vectors. In the sample configuration, announcements were sourced by the Avaya G450 Media Gateway. The following abridged list command shows an announcement used in conjunction with the vector in this section. To add an announcement extension, use the command “add announcement <extension>”.

```
list announcement
                          ANNOUNCEMENTS/AUDIO SOURCES
Announcement                                                  Source      Num of
Extension             Type       Name                        Pt/Bd/Grp    Files
3760                  integ-rep  Recurring-in-Q-60-Annc       001V9       1
```

5.9.2 ACD Configuration for Call Queued for Handling by Agent

This section provides a simple example configuration for VDN, vector, hunt group, and agent logins used to queue inbound Verizon IPCC calls for handling by an agent. This section is not meant to be prescriptive.

The following screens show an example ACD hunt group. On page 1, note the bolded values.

```
display hunt-group 60                                           Page   1 of   4
                                  HUNT GROUP

            Group Number: 60                                ACD? y
              Group Name: ACD-Hunt-60                     Queue? y
         Group Extension: 3560                           Vector? y
              Group Type: ucd-mia
                      TN: 1
                     COR: 1                   MM Early Answer? n
           Security Code:              Local Agent Preference? n
```

The following screens show an example ACD hunt group. On the abbreviated page 2 shown below, note **Skill** is set to “y”.

```
display hunt-group 60                                           Page   2 of   4
                                  HUNT GROUP
                     Skill? y     Expected Call Handling Time (sec): 180
                       AAS? n
```

VDN 3660, shown below, is associated with vector 60.

```
display vdn 3660                                                Page   1 of   3
                            VECTOR DIRECTORY NUMBER

                             Extension: 3660
                                 Name*: Sales-60
                           Destination: Vector Number        60
                   Attendant Vectoring? n
                  Meet-me Conferencing? n
                    Allow VDN Override? n
                                   COR: 1
```

In this simple example, vector 60 briefly plays ring back, then queues the call to skill 60. Announcement 3760 is a simple recurring announcement. If an agent is immediately available to handle the call, the call will be delivered to the agent. If an agent is not immediately available, the call will be queued, and the caller will hear the announcement. Once an agent becomes available, the call will be delivered to the agent. In **Section 9**, example Wireshark traces are illustrated for the case where the agent is immediately available as well as the alternative case where the call is queued listening to the announcement before the agent becomes available.

```
display vector 60                                                 Page   1 of   6
                                  CALL VECTOR

    Number: 60               Name: Sales
Multimedia? n      Attendant Vectoring? n    Meet-me Conf? n           Lock? n
     Basic? y   EAS? y   G3V4 Enhanced? y   ANI/II-Digits? y   ASAI Routing? y
 Prompting? y   LAI? y  G3V4 Adv Route? y   CINFO? y   BSR? y   Holidays? y
 Variables? y   3.0 Enhanced? y
01 #    Wait hearing ringback
02 wait-time    2   secs hearing ringback
03 #    Simple queue to skill with recurring announcement until available
04 queue-to     skill 60   pri m
05 announcement 3760
06 stop
07
```

The following screen illustrates an example agent-loginID 4661. In the sample configuration, a one-X® Agent client logged in using agent-loginID 4661 and the configured Password to staff and take calls for skill 60.

```
change agent-loginID 4661                                          Page   1 of   3
                                 AGENT LOGINID

                Login ID: 4661                                        AAS? n
                    Name: EAS-Agent2                                AUDIX? n
                      TN: 1                                 LWC Reception: spe
                     COR: 1                        LWC Log External Calls? n
           Coverage Path:                        AUDIX Name for Messaging:
           Security Code:
                                        LoginID for ISDN/SIP Display? n
                                                                Password:
                                                   Password (enter again):
                                                             Auto Answer: station
                                                       MIA Across Skills: system
                                              ACW Agent Considered Idle: system
                                              Aux Work Reason Code Type: system
                                                Logout Reason Code Type: system
                       Maximum time agent in ACW before logout (sec): system
                                                Forced Agent Logout Time:   :
```

The following abridged screen shows Page 2 for agent-loginID 4661. Note that the Skill Number (**SN**) has been set to 60.

```
change agent-loginID 4661                                          Page   2 of   3
                                 AGENT LOGINID
      Direct Agent Skill:                                  Service Objective? n
Call Handling Preference: skill-level                  Local Call Preference? n

    SN   RL SL           SN   RL SL           SN   RL SL           SN   RL SL
 1: 60      1        16:                  31:                  46:
 2:                  17:                  32:                  47:
 3:                  18:                  33:                  48:
```

To enable a telephone or one-X® Agent client to log in with the agent-loginID shown above, ensure that **Expert Agent Selection (EAS) Enabled** is set to "y" as shown in the screen below.

```
change system-parameters features                                  Page  11 of  19
                        FEATURE-RELATED SYSTEM PARAMETERS
CALL CENTER SYSTEM PARAMETERS
  EAS
         Expert Agent Selection (EAS) Enabled? y
        Minimum Agent-LoginID Password Length: 4
```

5.10. Private Numbering

The "change private-numbering" command may be used to define the format of numbers sent to Verizon in SIP headers such as the "Contact" and "P-Asserted-Identity" headers.

In the bolded row shown in the example abridged output below, an entry is made for a specific Communication Manager Vector Directory Number (VDN) illustrated in the prior section. Without this configuration, calls to a VDN would result in a blank user portion of the Contact header in the 183 with SDP and 200 OK returned to Verizon. Although this did not present any user-perceivable problem in the sample configuration, the configuration in the bolded rows below illustrate how to cause Communication Manager to populate the Contact header with a user portion that corresponds with a Verizon IPCC number. In the course of the testing, multiple Verizon numbers were associated with different Communication Manager extensions and functions.

```
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: 16
 4  3               3                            4        Maximum Entries: 540
 4  4               3                            4
 4  3660            77         8668518119        10
```

5.11. 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. Since Session Manager is present, Session Manager can be used to perform digit conversion, and digit manipulation via the Communication Manager incoming call handling table is not necessary. In alternative configurations, if the number sent by Verizon was not changed before reaching Communication Manager, then the Verizon IPCC number could be mapped to a Communication Manager extension using the incoming call handling treatment of the receiving trunk group. As an example, the following screen illustrates a conversion of IP-IVR "outdial number" 8668518119 to extension 2013 when the call arrives on trunk group 77.

```
change inc-call-handling-trmt trunk-group 77                    Page   1 of  30
                       INCOMING CALL HANDLING TREATMENT
 Service/      Number   Number      Del Insert
 Feature        Len      Digits
 public-ntwrk    10 8668518119       10  2013
```

5.12. Communication Manager Stations

In the sample configuration, four digit station extensions were used with the format 2xxx and 3xxx. Since this configuration is not unique to Verizon, a minimum of information is presented simply to assist in understanding verification traces presented in subsequent sections.

The following abbreviated screen shows an example extension for an Avaya H.323 IP telephone also used by Avaya one-X® Communicator. Call appearances and desired features (e.g., call forwarding, EC500, etc.) can be assigned to the station on page 4 (not shown).

```
change station 2013                                             Page   1 of   5
                                     STATION
Extension: 2013                          Lock Messages? n               BCC: 0
     Type: 9630                          Security Code: *                TN: 1
     Port: S00007                      Coverage Path 1:                 COR: 1
     Name: One-X ComJR                 Coverage Path 2:                 COS: 1
                                       Hunt-to Station:
STATION OPTIONS
              Loss Group: 19       Personalized Ringing Pattern: 1
                                               Message Lamp Ext: 2013
            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? y
```

The following abbreviated screen shows an example extension used by an Avaya one-X® Agent client. Call appearances and appropriate features (e.g., aux-work, etc.) can be assigned on page 4 (not shown).

```
change station 2014                                              Page   1 of   5
                                     STATION

Extension: 2014                          Lock Messages? n               BCC: 0
     Type: 9630                          Security Code: *                TN: 1
     Port: S00013                      Coverage Path 1:                 COR: 1
     Name: One-x-Agent1                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: 2014
            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? y
```

5.13. Saving Communication Manager Configuration Changes

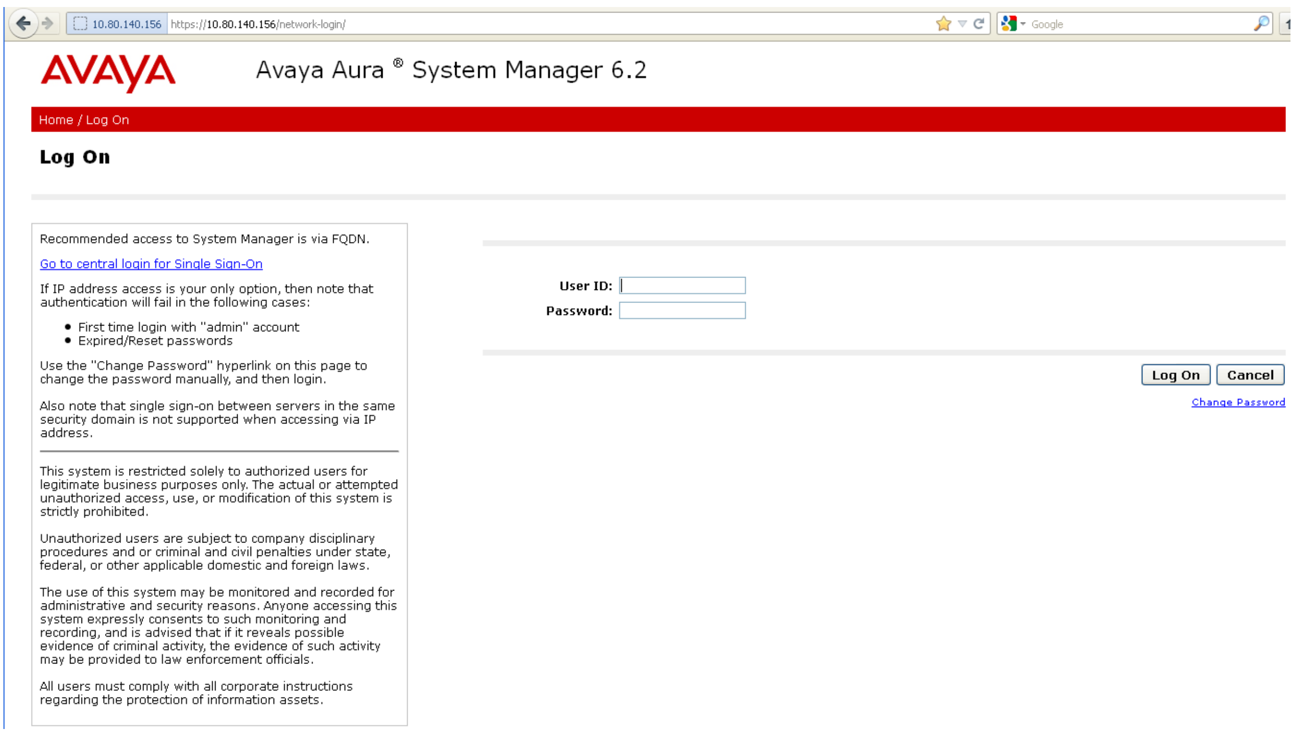
The command “save translation all” can be used to save the configuration.

6. Avaya Aura ® Session Manager Configuration for SIP Trunking

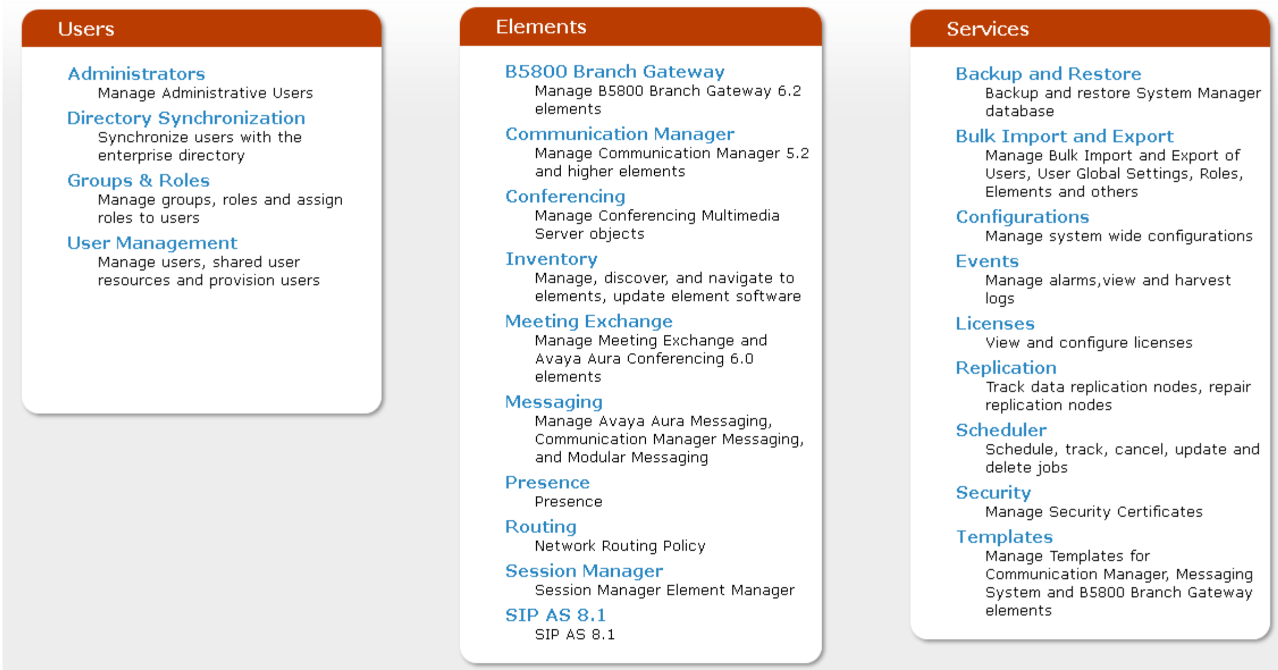
This section illustrates relevant aspects of the Session Manager configuration used in the verification of these Application Notes.

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.

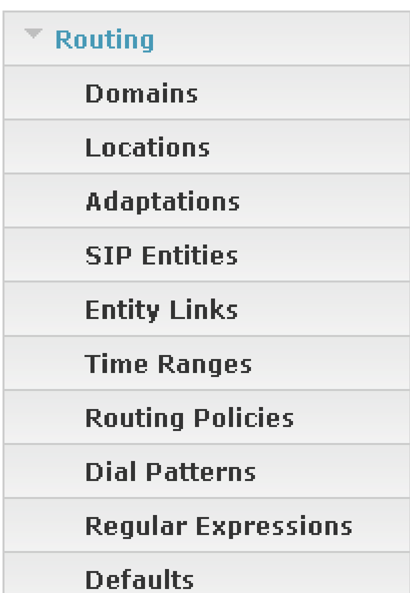
Session Manager is managed via System Manager. Using a web browser, access "https://<ip-addr of System Manager>/SMGR". In the **Log On** screen, enter appropriate **User ID** and **Password** and press the **Log On** button as shown in the example System Manager 6.2 **Log On** screen below.



Once logged in, a screen similar to the abridged screen shown below is displayed.



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

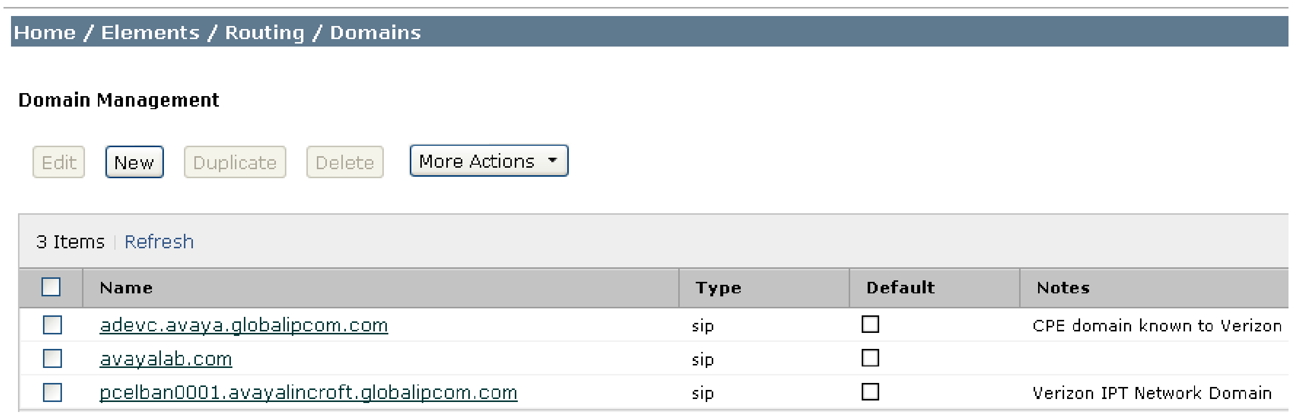
Step 8: "Dial Patterns" are defined and assigned to "Routing Policies" and "Locations" (one step)

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.


Home / Elements / Routing / Domains

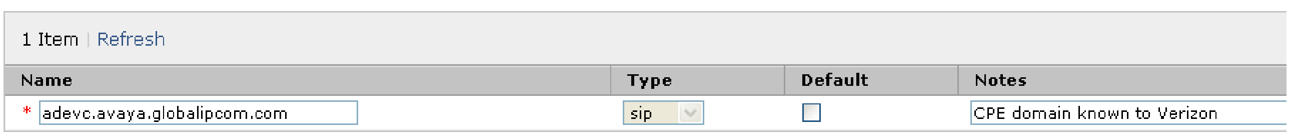
Domain Management

Edit New Duplicate Delete More Actions

3 Items | Refresh

	Name	Type	Default	Notes
☐	adevc.avaya.globalipcom.com	sip	☐	CPE domain known to Verizon
☐	avayalab.com	sip	☐	
☐	pcelban0001.avayalincroft.globalipcom.com	sip	☐	Verizon IPT Network Domain

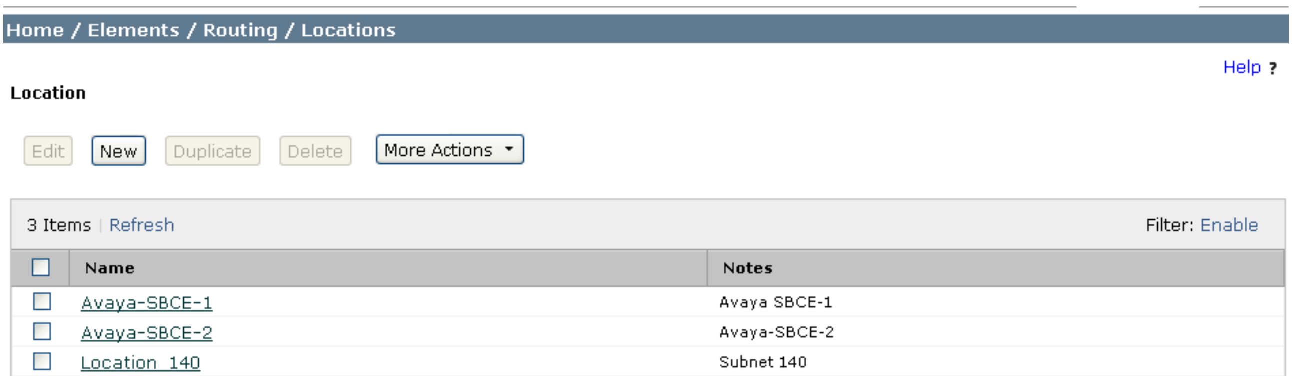
The domain "adevc.avaya.globalipcom.com" is the domain known to Verizon as the enterprise SIP domain. In the sample configuration, Verizon included this domain as the host portion of the Request-URI for inbound calls.


1 Item | Refresh

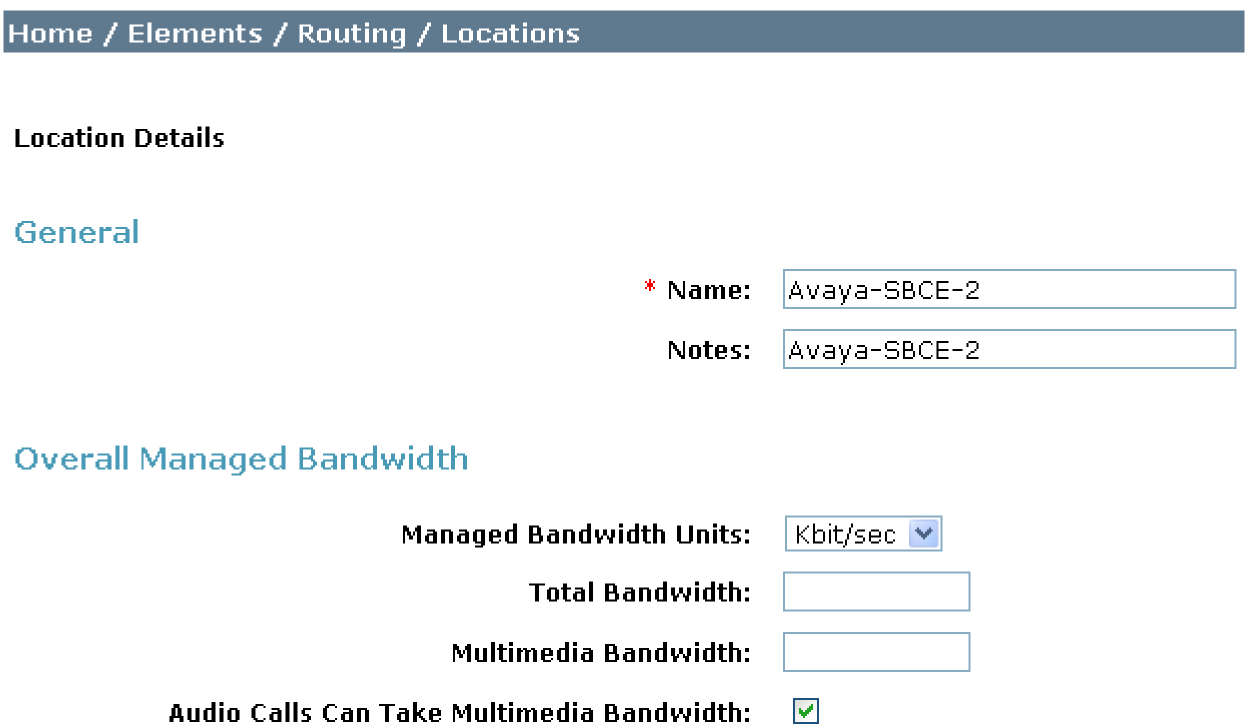
Name	Type	Default	Notes
* adevc.avaya.globalipcom.com	sip	☐	CPE domain known to Verizon

6.2. Locations

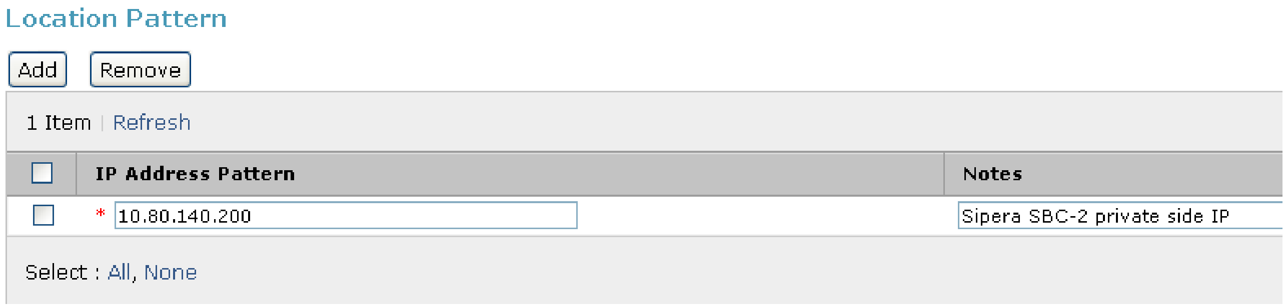
To view or change locations, select **Routing → Locations**. The following screen shows an abridged list of configured locations. Click on the checkbox corresponding to the name of a location and **Edit** to edit an existing location, or the **New** button to add a location. Click the **Commit** button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



The following image shows the top portion of the screen for the location details for the location named "Avaya-SBCE-2", corresponding to the Avaya SBC for Enterprise relevant to these Application Notes. Later, the location with name "Avaya-SBCE-2" 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 SBC is entered in the **IP Address Pattern** field. In the sample configuration, other location parameters (not shown) retained default values.

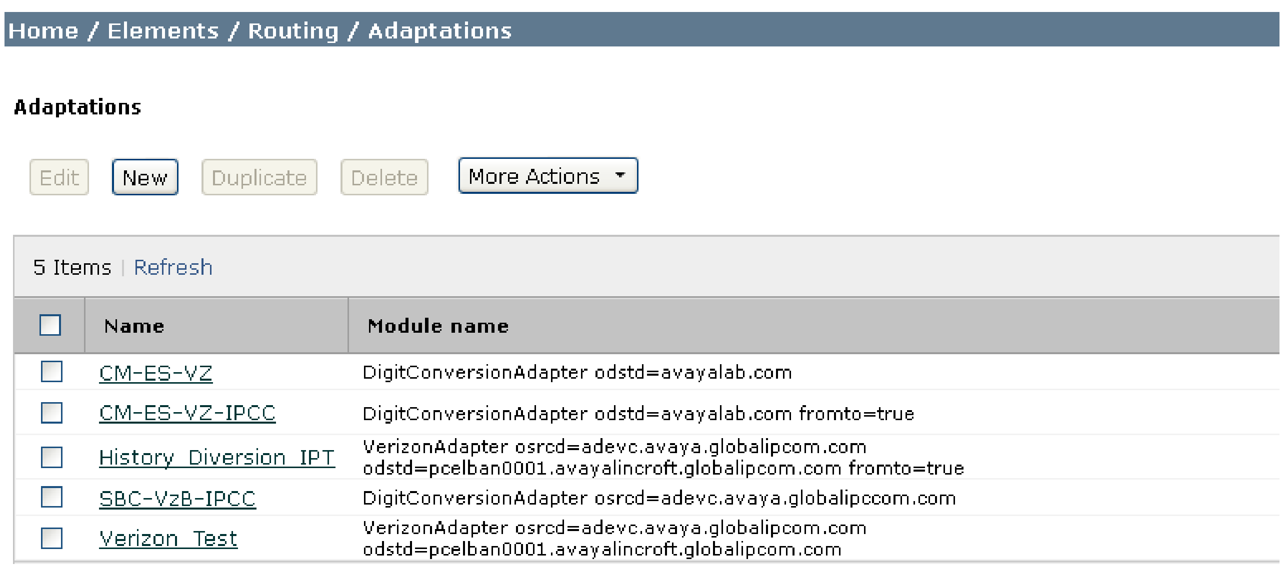


If desired, additional locations can be configured with IP Address Patterns corresponding to other elements in the configuration.

6.3. Adaptations

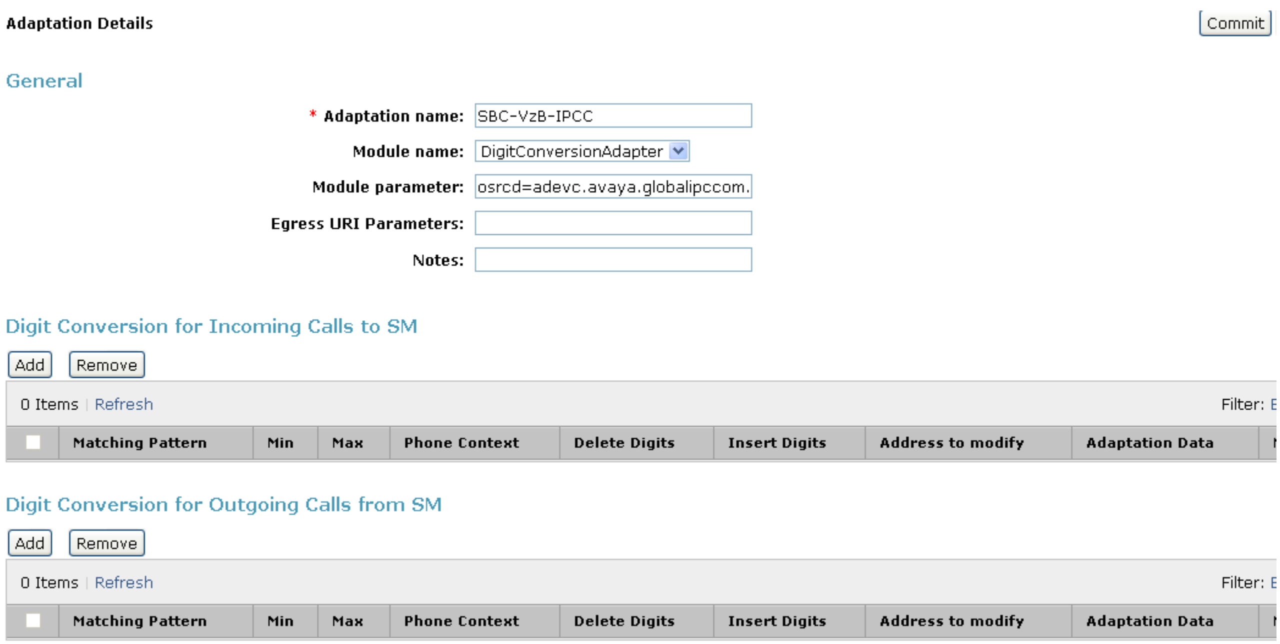
To view or change adaptations, select **Routing → Adaptations**. Click on the checkbox corresponding to the name of an adaptation and **Edit** to edit an existing adaptation, or the **New** button to add an adaptation. Click the **Commit** button after changes are completed.

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.



The adapter named “SBC-VzB-IPCC” will later be assigned to the SBC SIP Entity. The adapter is configured to apply the parameter “osrcd=adevc.avaya.globalipcom.com”. This configuration enables the source domain to be overwritten with “adevc.avaya.globalipcom.com”. For example, for inbound calls from Verizon, the PAI header sent to Verizon in the 200 OK will contain "adevc.avaya.globalipcom.com". Depending on the Communication Manager configuration, it may not be necessary for Session Manager to adapt the domain in this fashion. In the sample configuration, where "avayalab.com" was already in use in a shared Avaya environment, it was appropriate for Session Manager to adapt the domain from "avayalab.com" to "adevc.avaya.globalipcom.com" where the latter is the CPE domain known to Verizon.

The following screen shows the adaptation details. Although the "DigitConversionAdapter" is used, no conversion of digits is used. This adapter is used to apply the module parameters, and not for digit manipulation.



The adapter named "CM-ES-VZ-IPCC" shown in the following screen will later be assigned to the SIP Entity linking Session Manager to Communication Manager for calls involving Verizon IPCC. This adaptation uses the "DigitConversionAdapter" and specifies the "odstd=avayalab.com". More specifically, this configuration enables the destination domain to be overwritten with "avayalab.com" for calls that egress to a SIP entity using this adapter. For example, for inbound calls from Verizon IPCC to the Avaya CPE, the Request-URI header sent to Communication Manager will contain "avayalab.com", which was the domain used by Communication Manager in the shared Avaya Interoperability Test Lab configuration. Depending on the Communication Manager and Avaya SBCE configuration, it may not be necessary for Session Manager to adapt the domain in this fashion. The parameter "fromto=true" enables Session Manager to adapt the domain in the To header (to "avayalab.com") as well.

Home / Elements / Routing / Adaptations

Adaptation Details Commit

General

* Adaptation name:	CM-ES-VZ-IPCC
Module name:	DigitConversionAdapter
Module parameter:	odstd=avayalab.com fromto=true
Egress URI Parameters:	
Notes:	Verizon IPCC to CM Numbers

Scrolling down, the following screen shows a portion of the "CM-ES-VZ-IPCC" adapter that can be used to convert digits between the Communication Manager extension numbers (user extensions, VDNs) and the IP-IVR "outdial numbers" assigned by Verizon.

An example portion of the settings for "Digit Conversion for Outgoing Calls from SM" (i.e., inbound to Communication Manager) is shown below. During the testing, this digit conversion was varied to allow a small number of Verizon-provided IP-IVR "outdial numbers" to be used to test a variety of Communication Manager destinations.

Digit Conversion for Outgoing Calls from SM

Add Remove

6 Items | Refresh Filter: Enable

	Matching Pattern	Min	Max	Phone Context	Delete Digits	Insert Digits	Address to modify	Adaptation Data	Notes
☐	* 8668518119	* 10	* 10		* 10	2013	both		DTMF Test, or route to phone

Similarly, an abridged portion of the settings for "Digit Conversion for Incoming Calls to SM" is shown below. Although the direction of actual calls involving Verizon IPCC service are "inbound" to Communication Manager, SIP headers in responses from Communication Manager can be adapted using the "Digit Conversion for Incoming Calls to SM" area.

Digit Conversion for Incoming Calls to SM

Add Remove

3 Items | Refresh

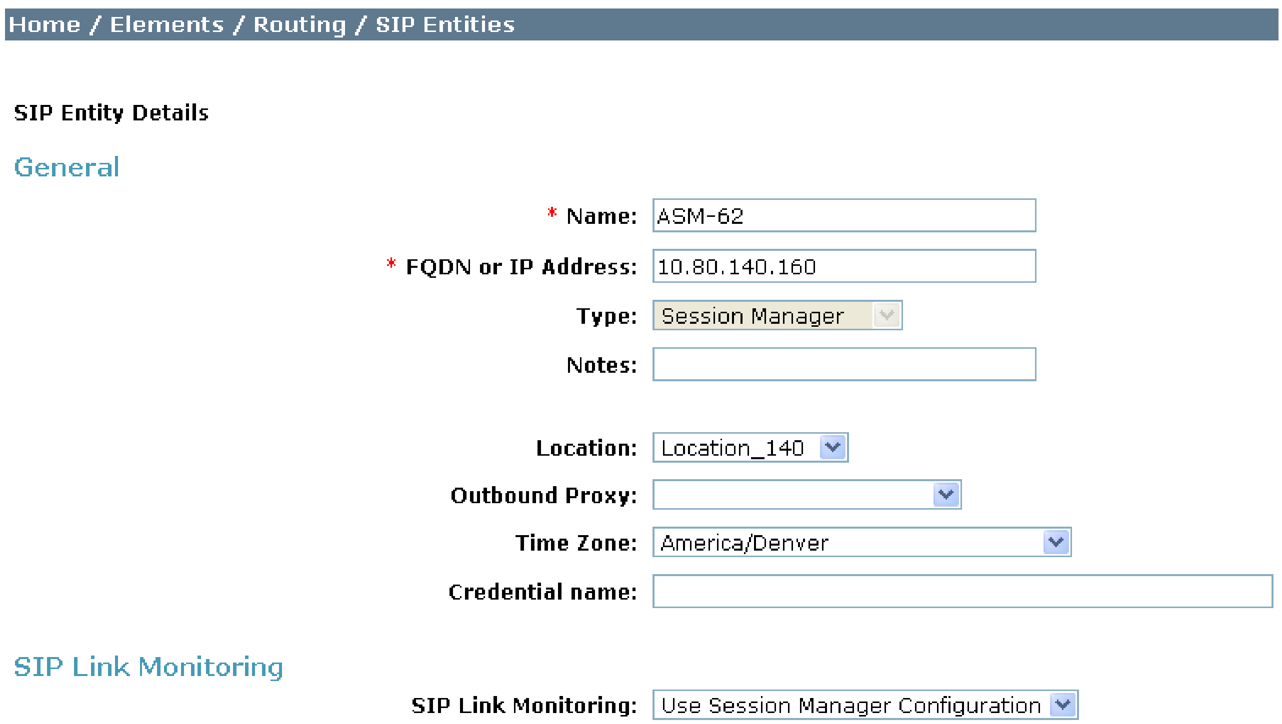
	Matching Pattern	Min	Max	Phone Context	Delete Digits	Insert Digits	Address to modify	Adaptation Data
☐	* 2013	* 4	* 4		* 4	8668518119	both	

In general, digit conversion that converts a Verizon IPCC number to a Communication Manager extension can be performed in Communication Manager or in Session Manager. In the example screens shown above, before sending the SIP INVITE to Communication Manager, Session Manager would adapt a received IP-IVR "outdial number" of 8668518119 to the extension 2013. As such, it would not be necessary to use the incoming call handling table of the receiving Communication Manager trunk group to convert the IP-IVR number to its corresponding extension. Similar mappings of IP-IVR "outdial numbers" to Communication Manager extensions may be defined for the remaining IP-IVR numbers.

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 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.

Entity Links

Add Remove

5 Items | Refresh F

	SIP Entity 1	Protocol	Port	SIP Entity 2	Port	Connection Policy
☐	ASM-62	TCP	* 5060	CM6.2	* 5060	Trusted
☐	ASM-62	TCP	* 5062	CM-Evolution-procr-5062	* 5062	Trusted
☐	ASM-62	TCP	* 5063	CM-Evolution-procr-5063	* 5063	Trusted
☐	ASM-62	TCP	* 5060	Avaya-SBCE-1	* 5060	Trusted
☐	ASM-62	TCP	* 5060	Avaya-SBCE-2	* 5060	Trusted

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 IPCC to be distinguished from other types of SIP calls using the same Session Manager, TCP port 5063 was added, with **Default Domain** "adevc.avaya.globalipcom.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	adevc.avaya.globalipcom.com	Verizon IPT testing
☐	5063	TCP	adevc.avaya.globalipcom.com	Verizon IPCC testing

Select : All, None

SIP Responses to an OPTIONS Request

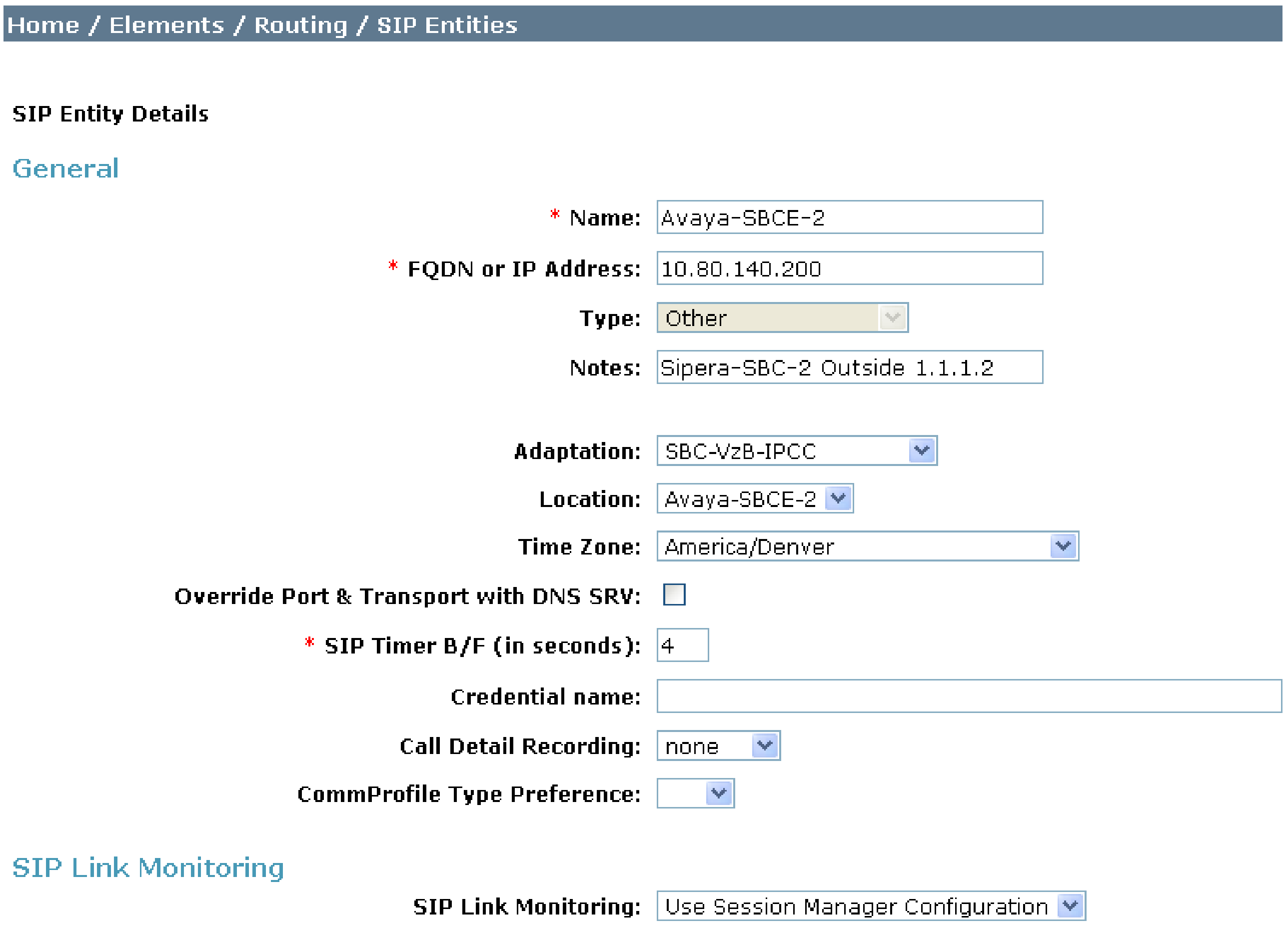
Add Remove

0 Items | Refresh Filter: Enable

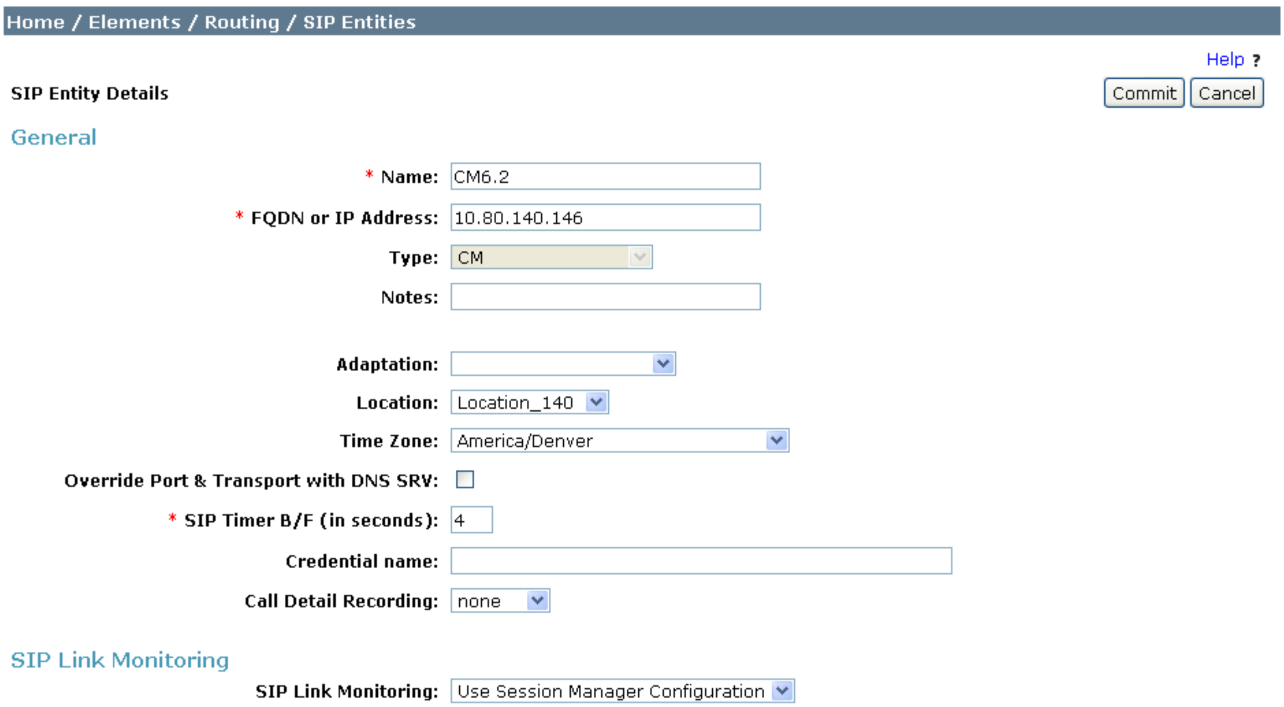
	Response Code & Reason Phrase	Mark Entity Up/Down	Notes

* **Input Required** Commit Cancel

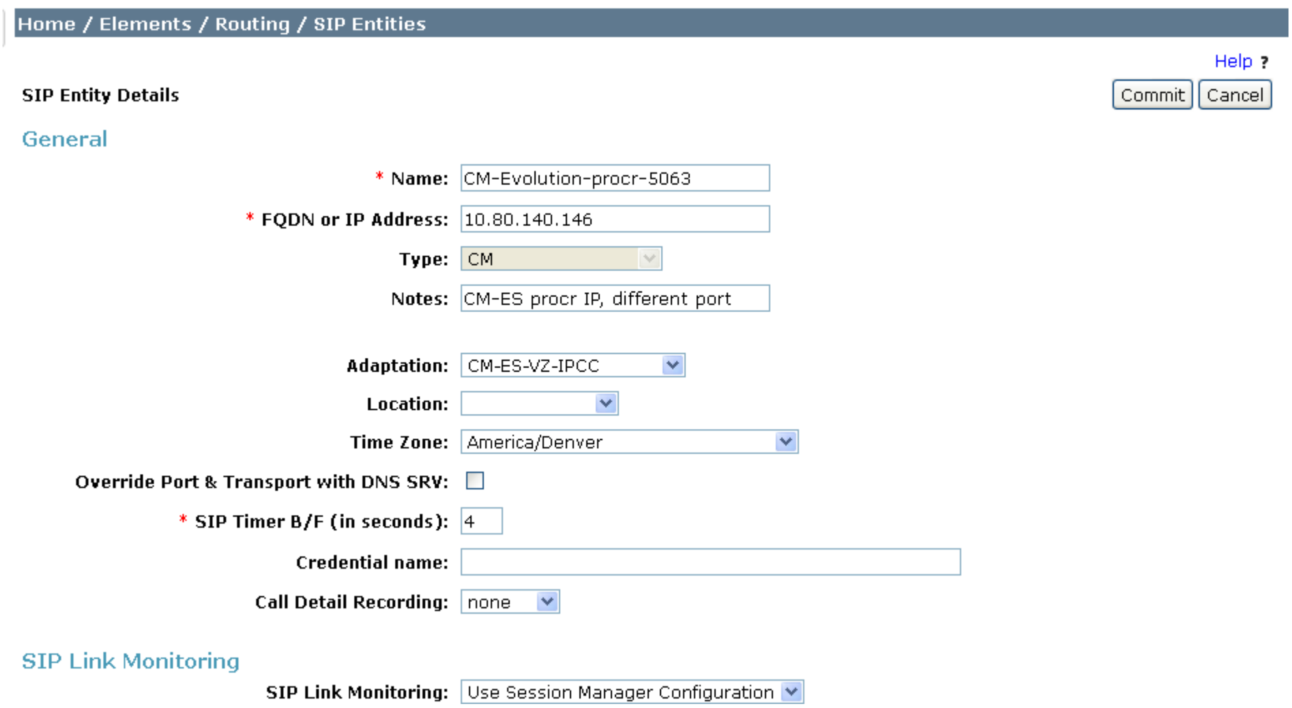
The following screen shows the upper portion of the **SIP Entity Details** corresponding to "Avaya-SBCE-2". The **FQDN or IP Address** field is configured with the Avaya SBCE inside IP Address (10.80.140.200). "Other" is selected from the **Type** drop-down menu for SBC SIP Entities. This SBC has been assigned to **Location** "Avaya-SBCE-2", and the "SBC-VzB-IPCC" 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 IPCC 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-5063". This entity uses the same **FQDN or IP Address** (10.80.140.146) as the prior entity with name "CM6.2"; both correspond to the Communication Manager Processor Ethernet IP Address. Later, a unique port, 5063, will be used for the Entity Link to "CM-Evolution-procr-5063". Using a different port is one approach that will allow Communication Manager to distinguish traffic originally from Verizon IPCC 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. The adapter "CM-ES-VZ-IPCC" is applied to this SIP entity. Recall that this adapter is used to adapt the domain as well as map the Verizon IPCC numbers to the corresponding Communication Manager extensions. 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 the Communication Manager SIP trunk configuration), TCP was selected as the transport protocol for the Avaya 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-2" and "CM-ES-VZ-5063" 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-2", 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 IPCC named "CM-ES-VZ-5063", both entities use TCP and port 5063.

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 the Communication Manager processor Ethernet. This link existed in the configuration prior to adding the Verizon IPCC-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-5063" also links Session Manager "ASM-62" with the Communication Manager processor Ethernet. However, this link uses port 5063 for both entities in the link. This link was created to allow Communication Manager to distinguish calls from Verizon IPCC 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 after changes are completed.

Home / Elements / Routing / Time Ranges

Time Ranges

Edit | New | Duplicate | Delete | More Actions

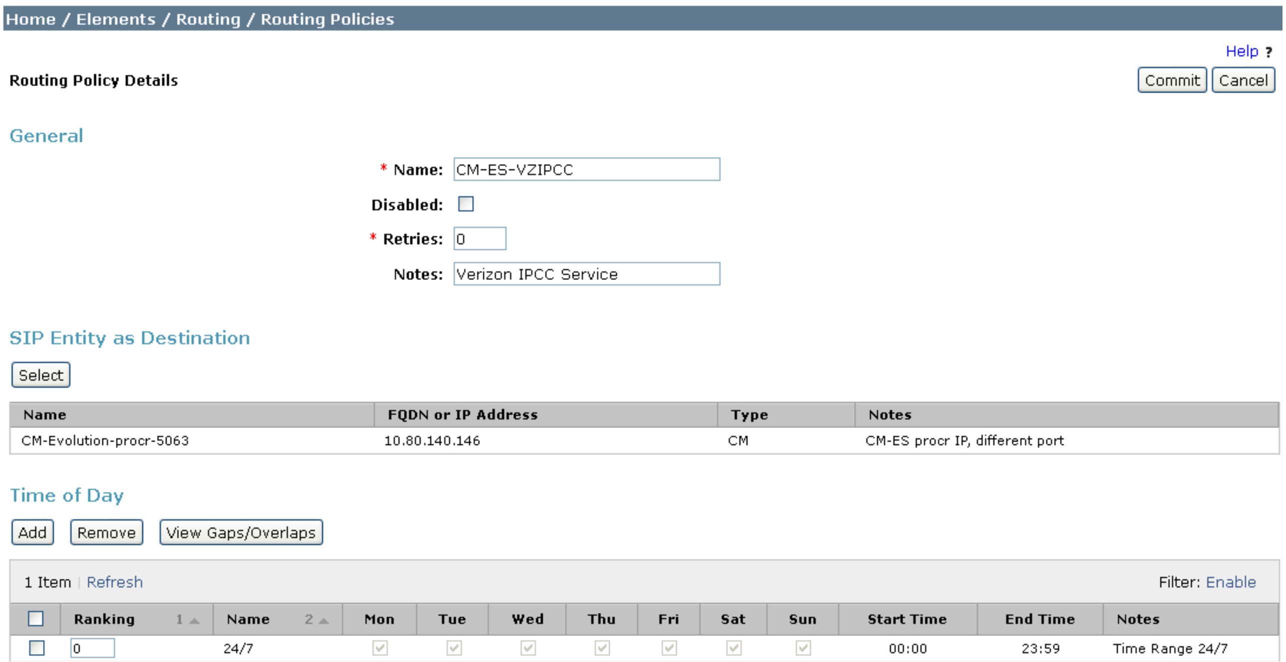
2 Items | Refresh Filter

Name	Mo	Tu	We	Th	Fr	Sa	Su	Start Time	End Time	Notes
24/7	☑	☑	☑	☑	☑	☑	☑	00:00	23:59	Time Range 24/7
Anytime	☑	☑	☑	☑	☑	☑	☑	00:00	23:59	24/7

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.

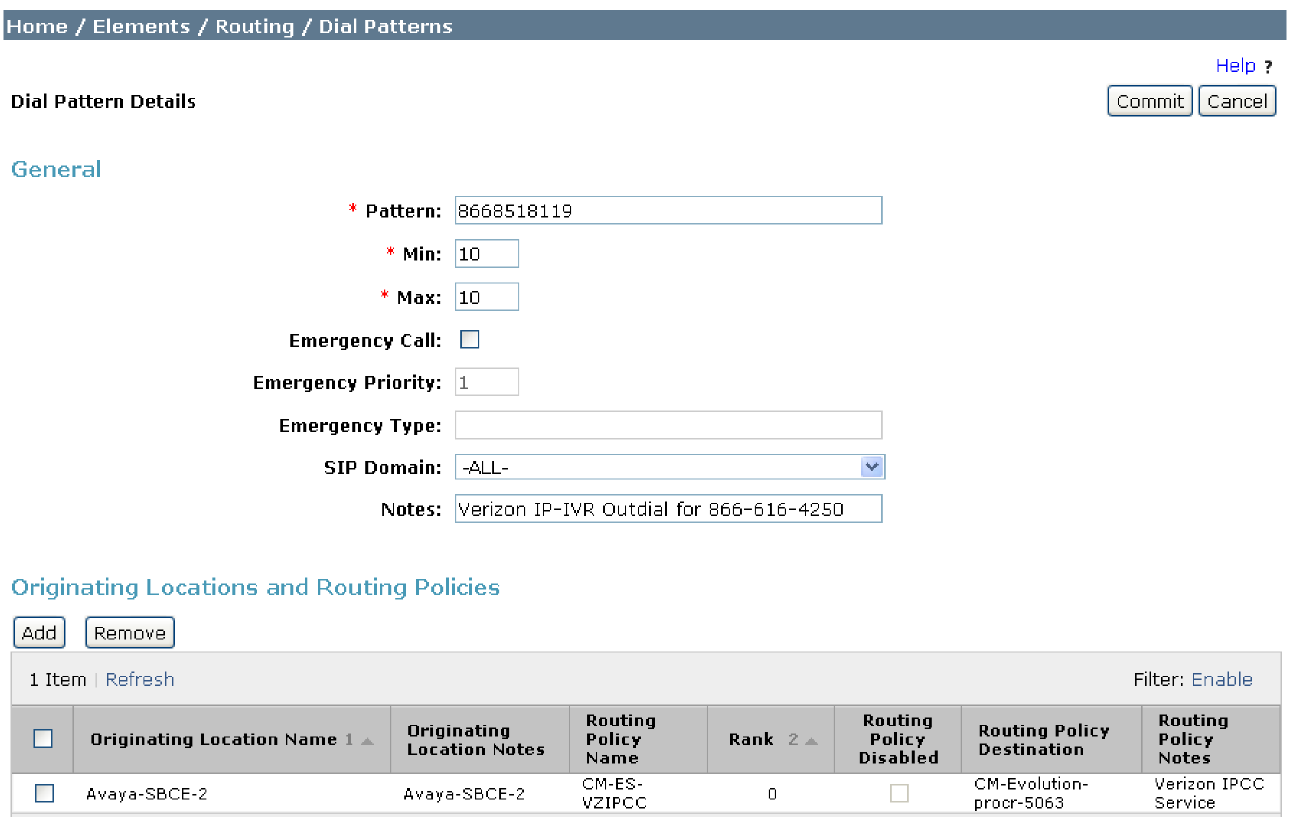
The following screen shows the **Routing Policy Details** for the policy named "CM-ES-VZIPCC" associated with incoming calls from Verizon IPCC to Communication Manager. Observe the **SIP Entity as Destination** is the entity named "CM-Evolution-procr-5063" which uses the Communication Manager processor Ethernet IP Address (10.80.140.146).



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.

The following screen illustrates an example dial pattern used to verify an inbound IP-IVR call to the enterprise. When a user on the PSTN dials an IP-IVR "published number" such as 866-616-4250, Verizon delivers the corresponding IP-IVR "outdial number" 866-851-8119 to the enterprise, and the SBC sends the call to Session Manager. The dial pattern below matches on the IP-IVR outdial number 8668518119 specifically. Dial patterns can alternatively match on ranges of numbers. Under **Originating Location and Routing Policies**, the routing policy named "CM-ES-VZIPCC" is selected, which sends the call to Communication Manager using the **Routing Policy Destination** "CM-Evolution-procr-5063" as described previously. The **Originating Location Name** is "Avaya-SBCE-2".



Once Dial Patterns are configured that associate dialed numbers with routing policies, a return to the routing policy screen will list the Dial Patterns associated with the policy. The screen shown below illustrates the lower portion of the routing policy "CM-ES-VZIPCC", after both Verizon IP Toll Free (shown in reference [VZ-IPTF]) and Verizon IP-IVR "outdial numbers" were added via the Dial Patterns.

Dial Patterns

Add Remove

9 Items | Refresh Filter: Enable

	Pattern	Min	Max	Emergency Call	SIP Domain	Originating Location	Notes
☐	8668502380	10	10	☐	-ALL-	Avaya-SBCE-2	Verizon IP Toll Free 866-850-2380
☐	8668506850	10	10	☐	-ALL-	Avaya-SBCE-2	Verizon IP Toll Free 866-850-6850
☐	8668508170	10	10	☐	-ALL-	Avaya-SBCE-2	Verizon IP-IVR Outdial for 866-616-4254
☐	8668510107	10	10	☐	-ALL-	Avaya-SBCE-2	Verizon IP Toll Free 866-851-0107
☐	8668511977	10	10	☐	-ALL-	Avaya-SBCE-2	Verizon IP-IVR Outdial for 866-616-4284
☐	8668512649	10	10	☐	-ALL-	Avaya-SBCE-2	Verizon IP Toll Free 866-851-2649
☐	8668518119	10	10	☐	-ALL-	Avaya-SBCE-2	Verizon IP-IVR Outdial for 866-616-4250
☐	8668519157	10	10	☐	-ALL-	Avaya-SBCE-2	Verizon IP-IVR Outdial for 866-616-4248
☐	8668523221	10	10	☐	-ALL-	Avaya-SBCE-2	Verizon IP Toll Free 866-852-3221

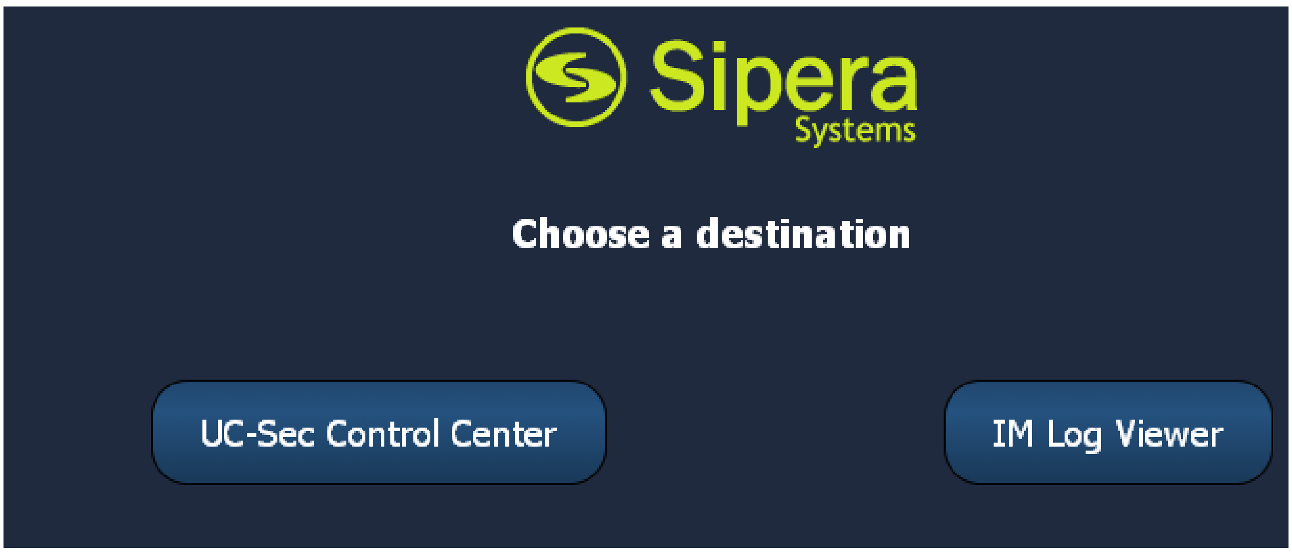
7. Avaya Session Border Controller for Enterprise

In the sample configuration, an Avaya Session Border Controller for Enterprise (SBCE) is used as the edge device between the Avaya CPE and Verizon Business.

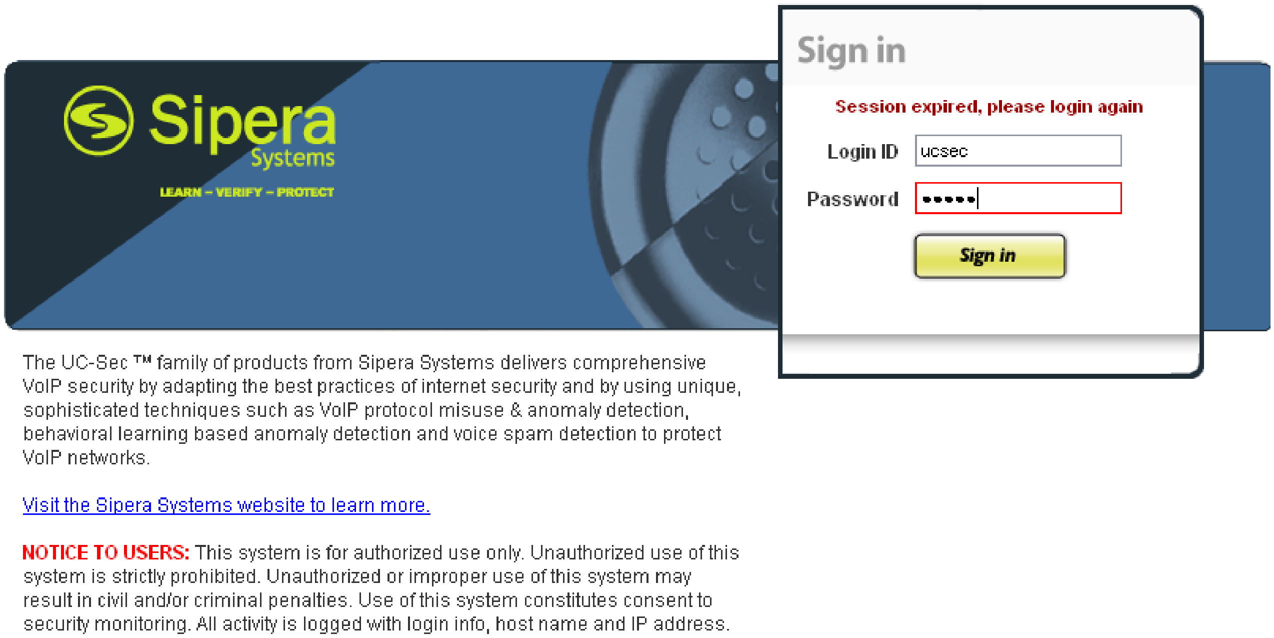
These Application Notes assume that the installation of the Avaya SBCE and the assignment of a management IP Address have already been completed.

7.1. Access the Management Interface

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**.



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

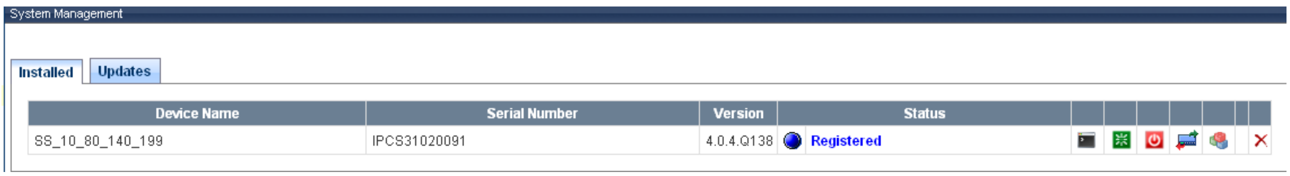


Once logged in, a UC-Sec Control Center screen will be presented. The following image illustrates the menu items available on the left-side of the UC-Sec Control Center screen.

7.2. Commission the System

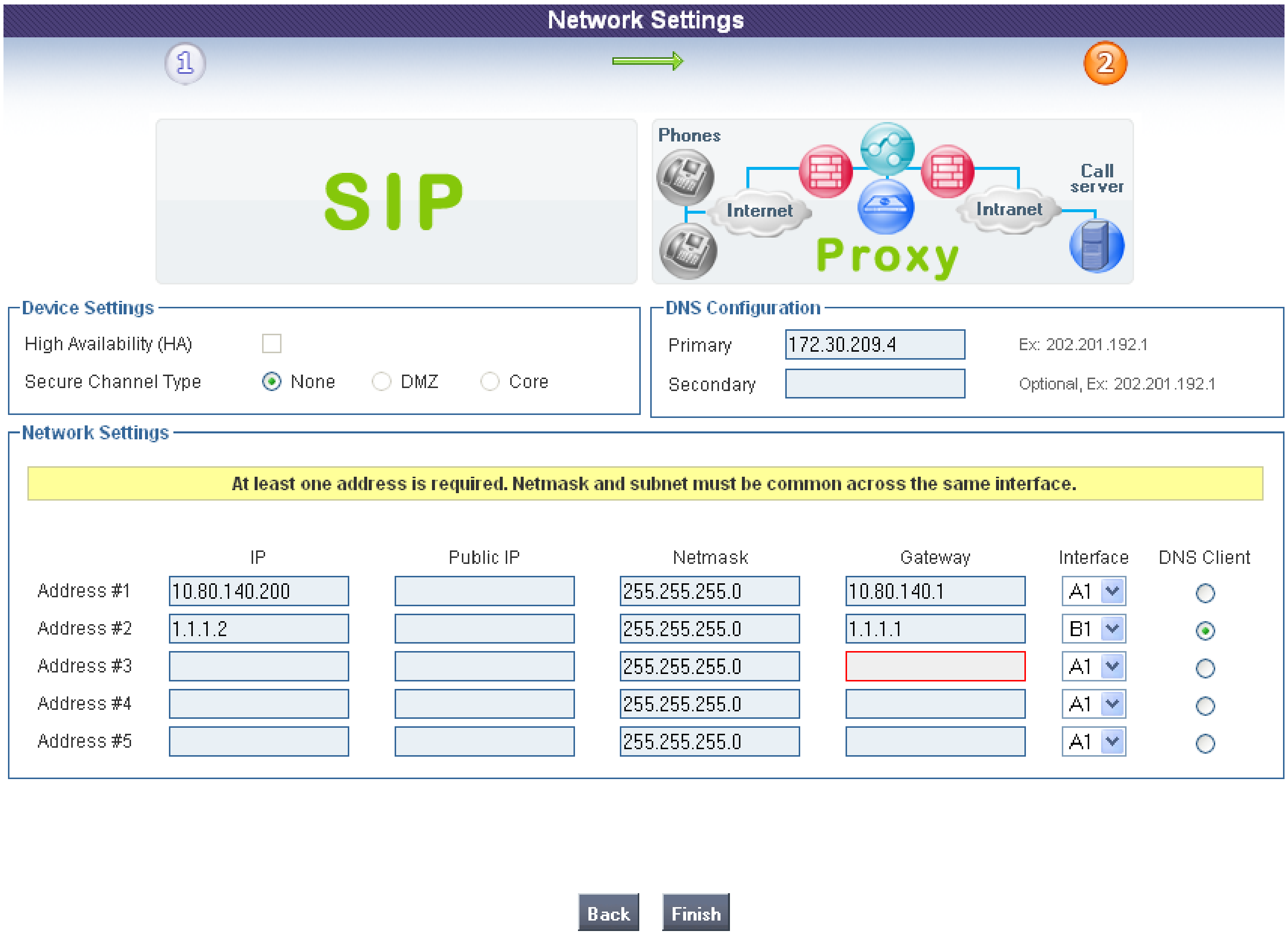
From the UC-Sec Control Center menu, select **System Management**.

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.

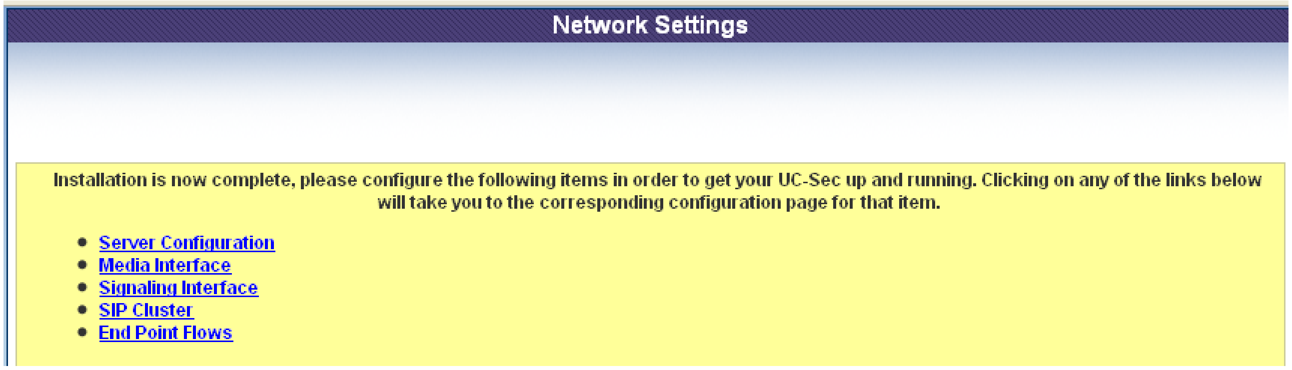


An installation wizard will appear. In the **Appliance Name** field, enter an appropriate name. In the sample configuration, "Sipera-outside-1112" was entered. In the **Choose your box type** area, choose SIP. Click **Next**.

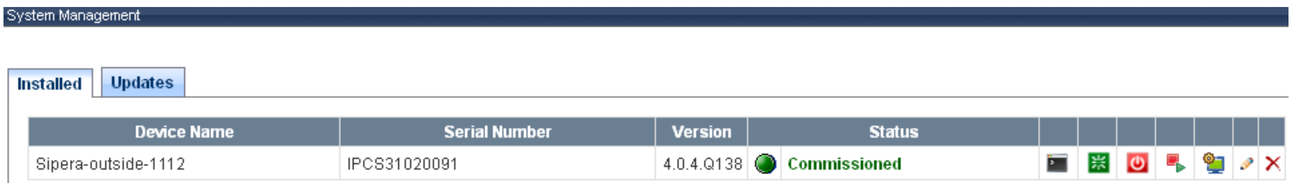
The following screen illustrates the **Network Settings** configured in the sample configuration. **Interface** A1 is the inside private interface, assigned IP Address 10.80.140.200, with **Gateway** 10.80.140.1. **Interface** B1 is the outside public interface, assigned IP Address 1.1.1.2, with **Gateway** 1.1.1.1. Note that 1.1.1.2 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**, 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 menu shown in Section 7.1.



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

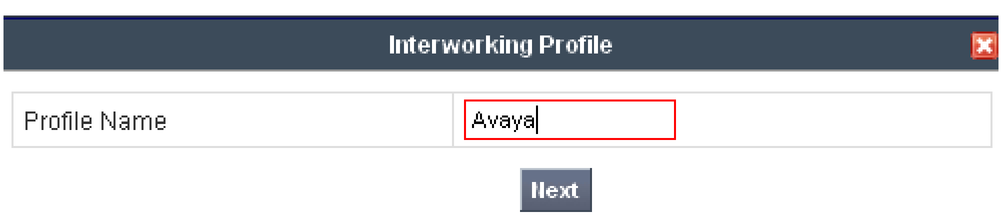


7.3. Global Profiles – Server Interworking

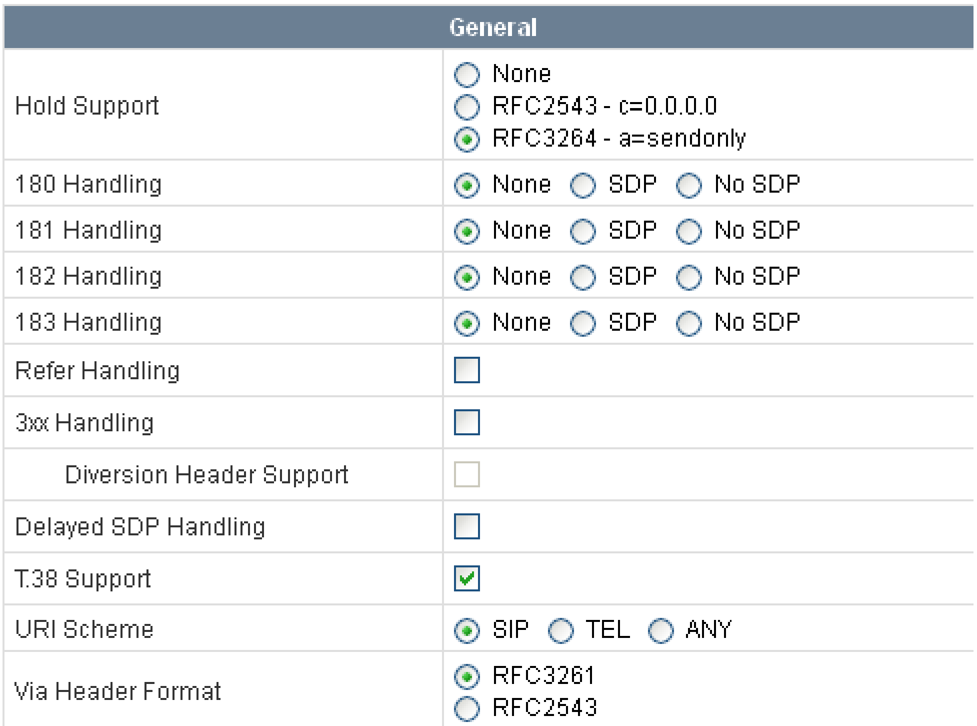
Select **Global Profiles → Server Interworking** from the left-side menu as shown below.

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 (although not necessary for Verizon IPCC), and **Hold Support** was set for RFC3264.



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

Rename Profile | Clone Profile | Delete Profile

Click here to add a description.

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

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.

General | Timers | URI Manipulation | Header Manipulation | Advanced

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

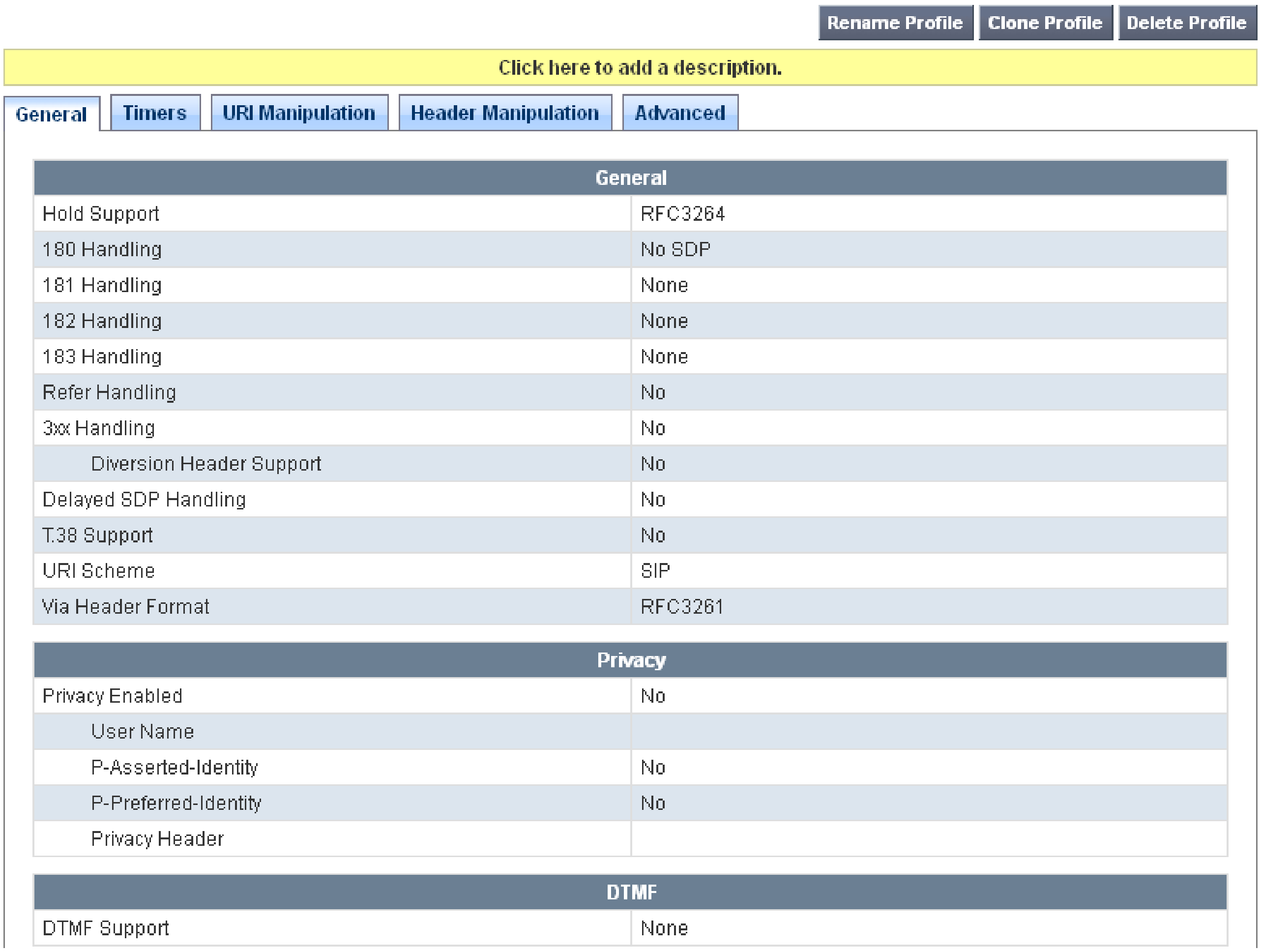
7.3.2 Server Interworking – Verizon IPCC

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-IPCC" shown below. Click **Next**.

Interworking Profile	
Profile Name	Verizon-IPCC

Next

The following screens illustrate the "General" parameters used in the sample configuration for the Interworking Profile named "Verizon-IPCC". Most parameters retain default values. In the sample configuration, **T.38 support** was set to "No", **Hold Support** was set for RFC3264, and **180 Handling** was set to "No SDP" (as noted earlier, this is optional. Communication Manager has been configured to send 183 with SDP in the sample configuration, so SDP will not be present in 180 anyway).



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

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

DTMF	
DTMF Support	None

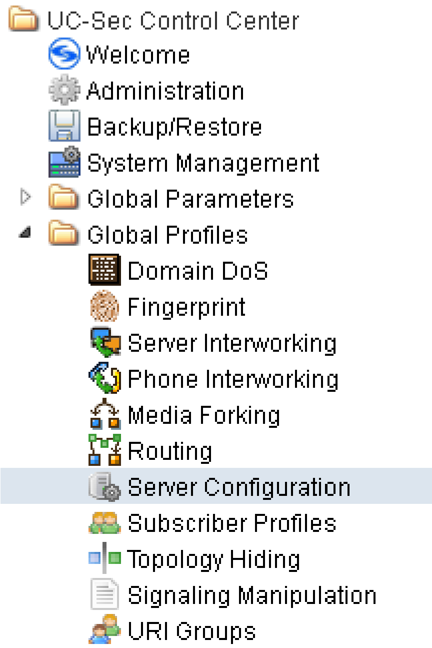
The following screen illustrates the **Advanced Settings** configuration. All parameters shown are default values. Note that the default configuration will result in Record-Route headers in SIP messages.

General | Timers | URI Manipulation | Header Manipulation | Advanced

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

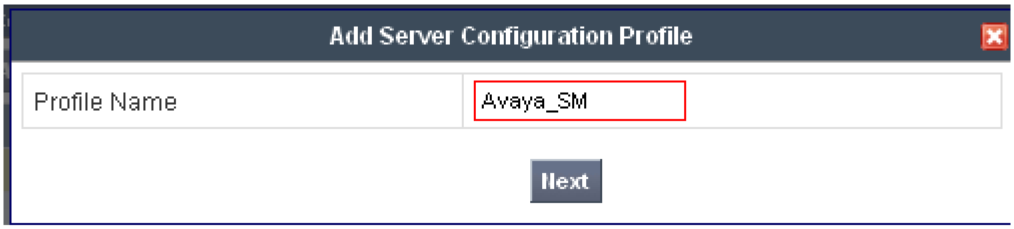
7.4. Global Profiles – Server Configuration

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

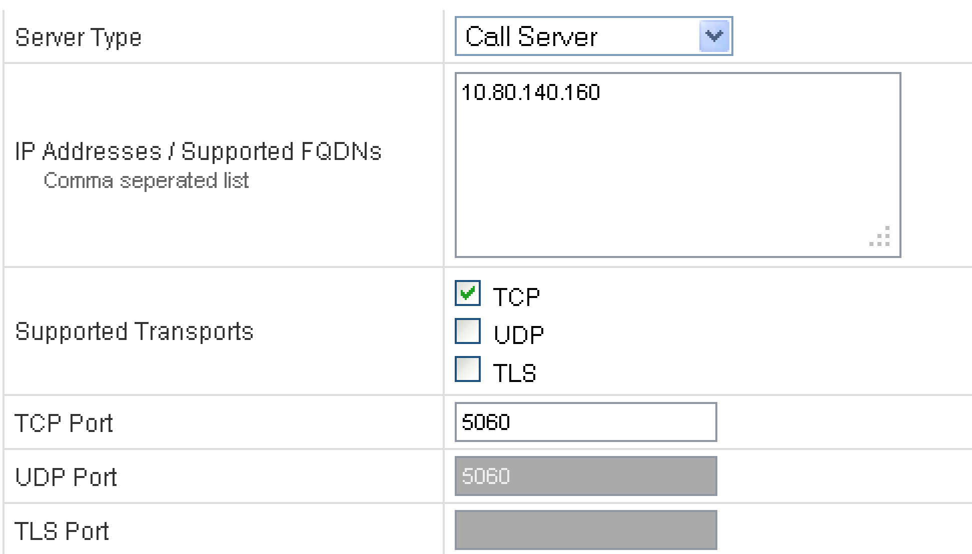


7.4.1 Server Configuration for Session Manager

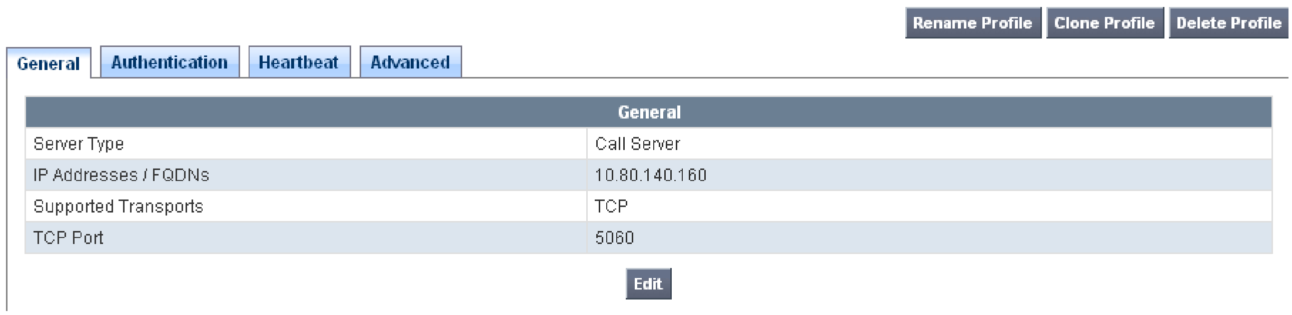
Click the **Add Profile** button (not shown) to add a new profile, or select an existing profile to edit. If adding a profile, a screen such as the following is displayed. Enter an appropriate Profile Name such as “Avaya_SM” shown below. Click **Next**.



The following screens illustrate the Server Configuration with Profile name “Avaya_SM”. In the “General” parameters, 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 SBC. If adding a new profile, click **Next**. If editing an existing profile, click **Finish**.



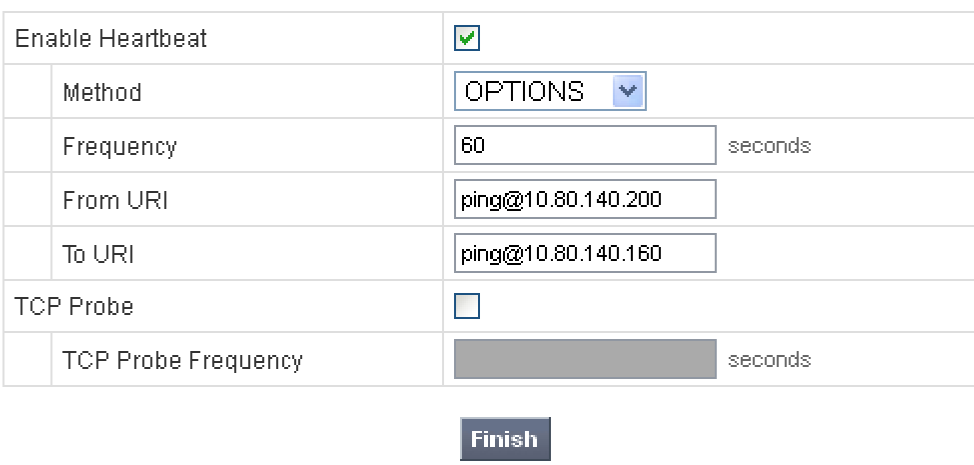
Once configuration is completed, the **General** tab for “Avaya_SM” will appear as shown below.



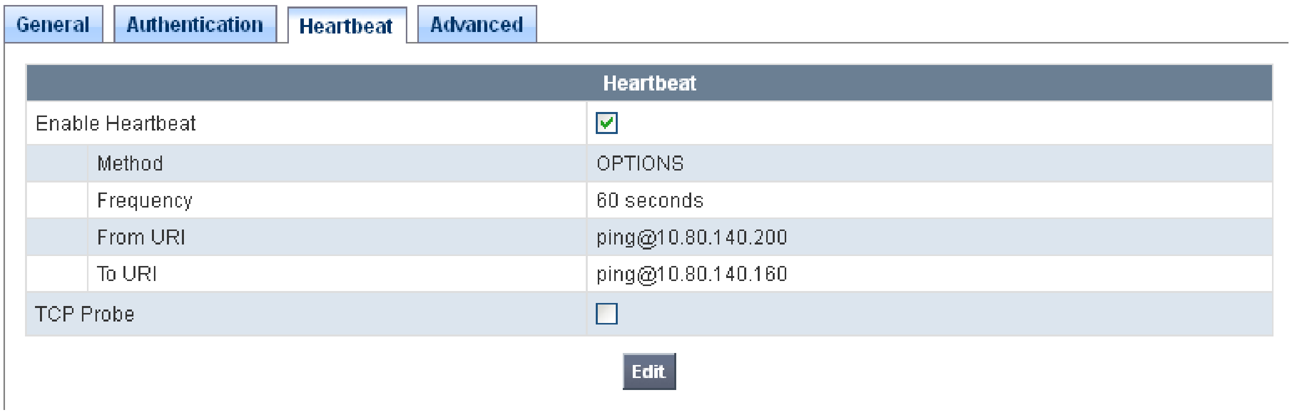
If adding the profile, click **Next** to accept default parameters for the **Authentication** tab, and advance to the **Heartbeat** area. If editing an existing profile, select the **Heartbeat** tab and click edit.

The SBC can be configured to source "heartbeats" in the form of SIP OPTIONS. In the sample configuration, with one Session Manager, this configuration is optional.

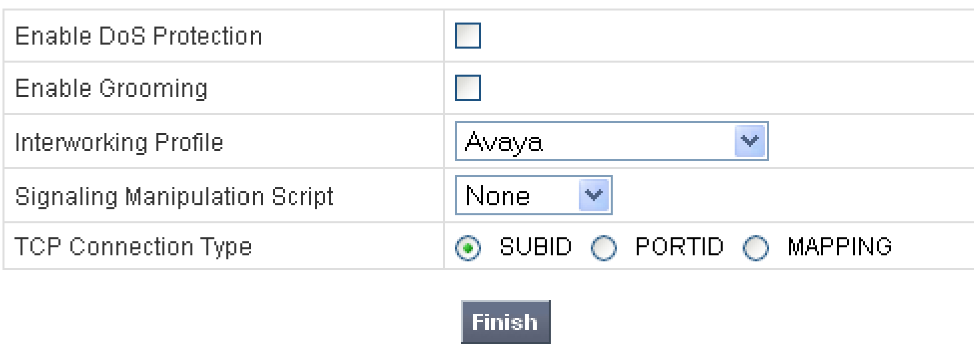
If SBC-sourced OPTIONS messages are desired, check the **Enable Heartbeat** box. Select "OPTIONS" from the **Method** drop-down menu. Select the desired frequency that the SBC will source OPTIONS to this server. The **From URI** and **To URI** may be filled in to configure easily identifiable URIs to appear in SIP OPTIONS sourced by the SBC toward Session Manager. If adding a new profile, click **Next**. If editing an existing profile, click **Finish**.



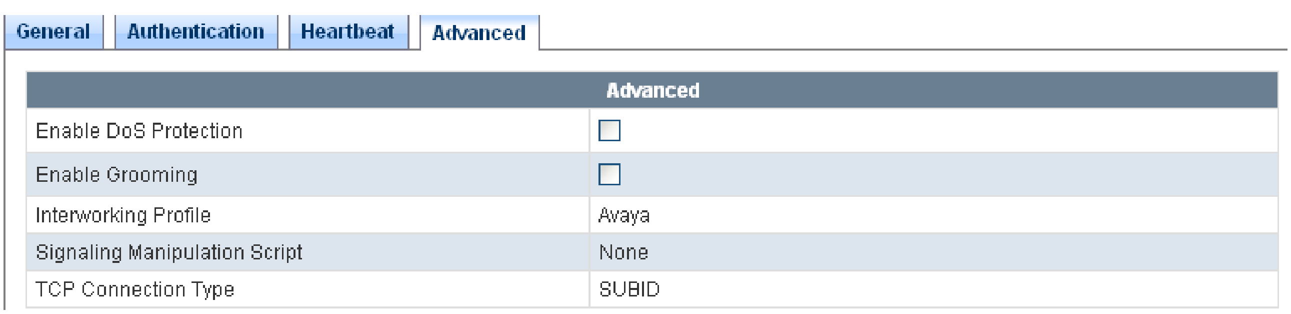
If SBC sourced OPTIONS are configured, the **Heartbeat** tab for "Avaya_SM" will appear as shown below.



If adding a profile, click **Next** to continue to the "Advanced" settings. If editing an existing profile, select the **Advanced** tab and **Edit**. In the resultant screen, select the **Interworking Profile** "Avaya" created previously. Click **Finish**.

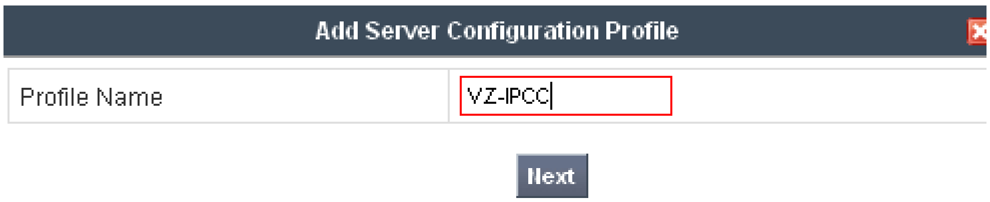


Once configuration is completed, the **Advanced** tab for "Avaya_SM" will appear as shown below.

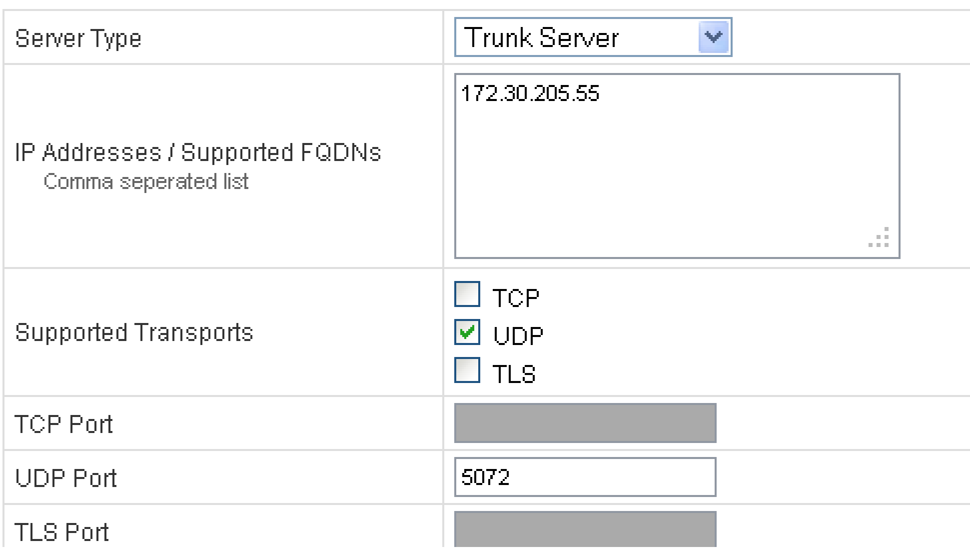


7.4.2 Server Configuration for Verizon IPCC

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 "VZ-IPCC" shown below. Click **Next**.



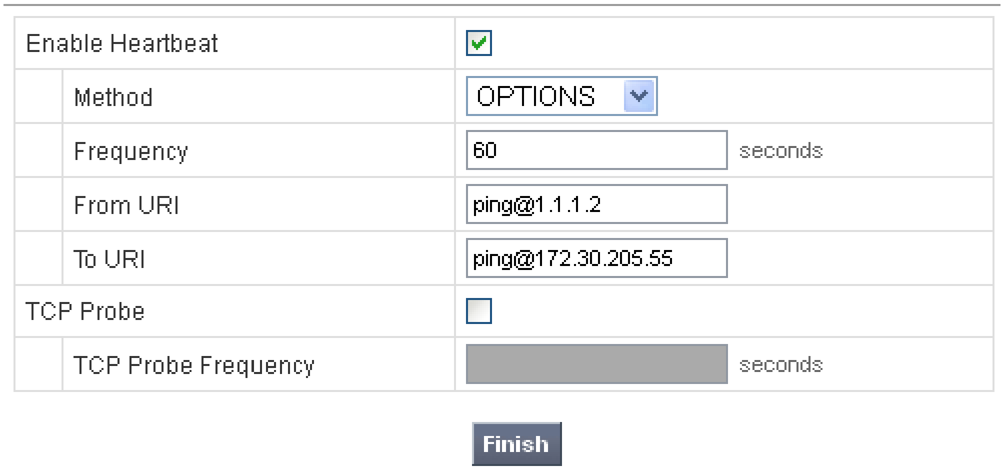
The following screens illustrate the Server Configuration with Profile name "VZ_IPCC". In the "General" parameters, select "Trunk Server" from the **Server Type** drop-down menu. In the **IP Addresses / Supported FQDNs** area, the Verizon-provided Verizon IPCC IP Address is entered. This IP Address is 172.30.205.55. In the **Supported Transports** area, UDP is selected, and the **UDP Port** is set to 5072.



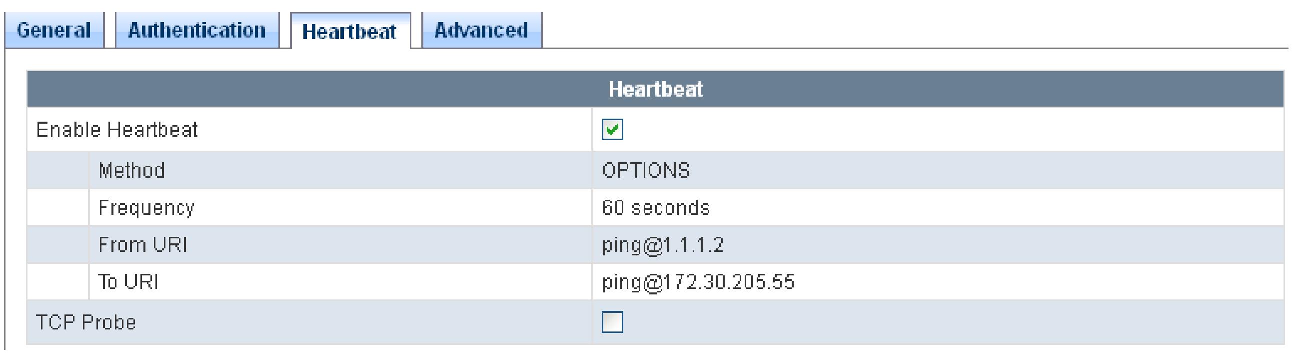
If adding the profile, click **Next** to accept default parameters for the **Authentication** tab, and advance to the **Heartbeat** area. If editing an existing profile, select the **Heartbeat** tab and click edit.

The SBC can be configured to source "heartbeats" in the form of SIP OPTIONS towards Verizon. This configuration is optional. Independent of whether the SBC 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 SBC, the SBC will send SIP OPTIONS to Verizon. When Verizon responds, the SBC will pass the response to Session Manager.

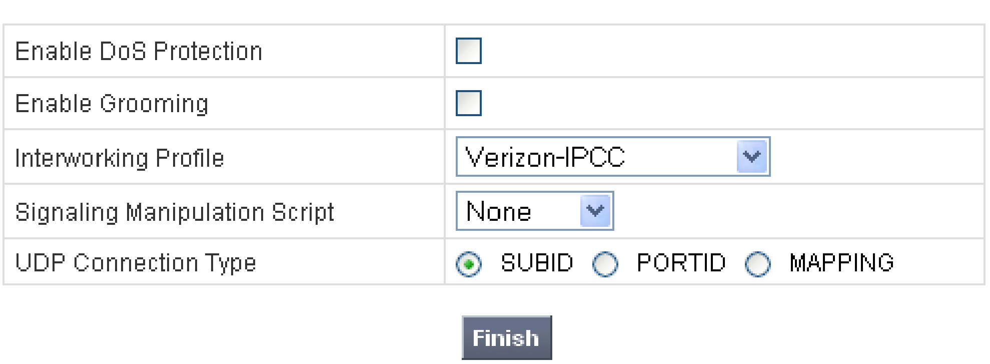
If SBC-sourced OPTIONS are desired, select "OPTIONS" from the **Method** drop-down menu. Select the desired frequency that the SBC will source OPTIONS. The **From URI** and **To URI** may be filled in to configure easily identifiable URIs to appear in SIP OPTIONS sourced by the SBC. If adding a new profile, click **Next**. If editing an existing profile, click **Finish**.



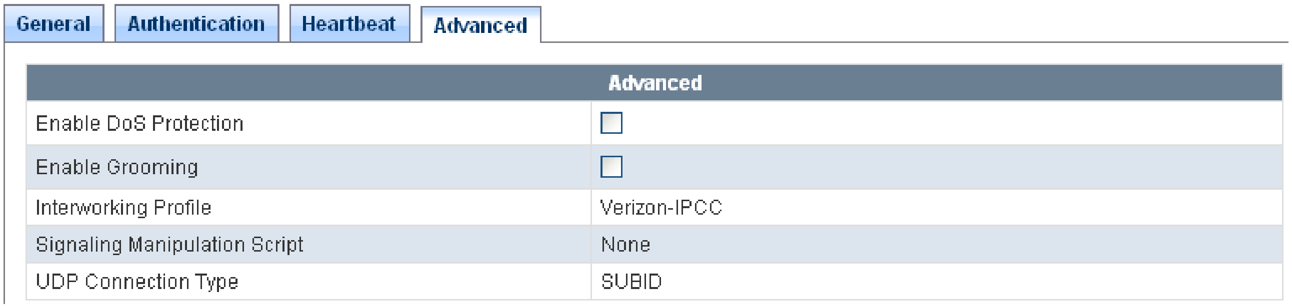
If the optional SBC sourced OPTIONS configuration is completed, the **Heartbeat** tab for "VZ-IPCC" will appear as shown below.



If adding a profile, click **Next** to continuing to the "Advanced" settings. If editing an existing profile, select the **Advanced** tab and **Edit**. In the resultant screen, select the **Interworking Profile** "Verizon-IPCC" created previously. Other SBC features, such as DoS Protection and Grooming, can be configured according to customer preference. Click **Finish**.

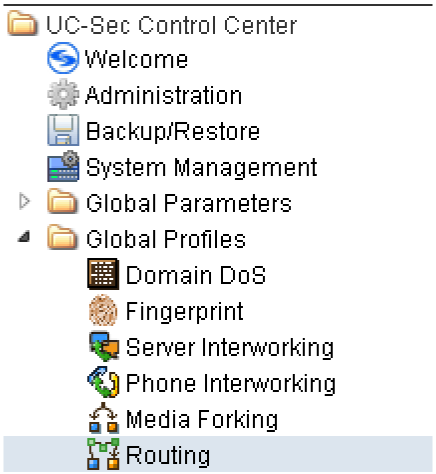


Once configuration is completed, the **Advanced** tab for "VZ-IPCC" will appear as shown below.



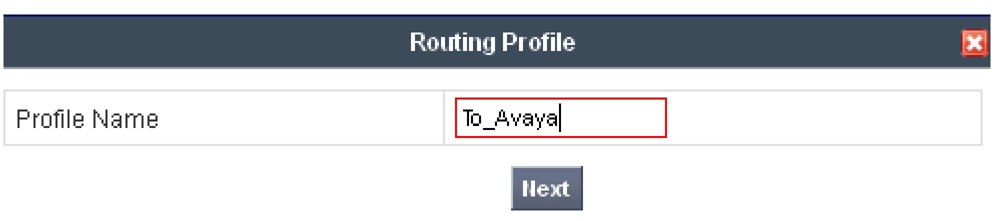
7.5. Global Profiles – Routing

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

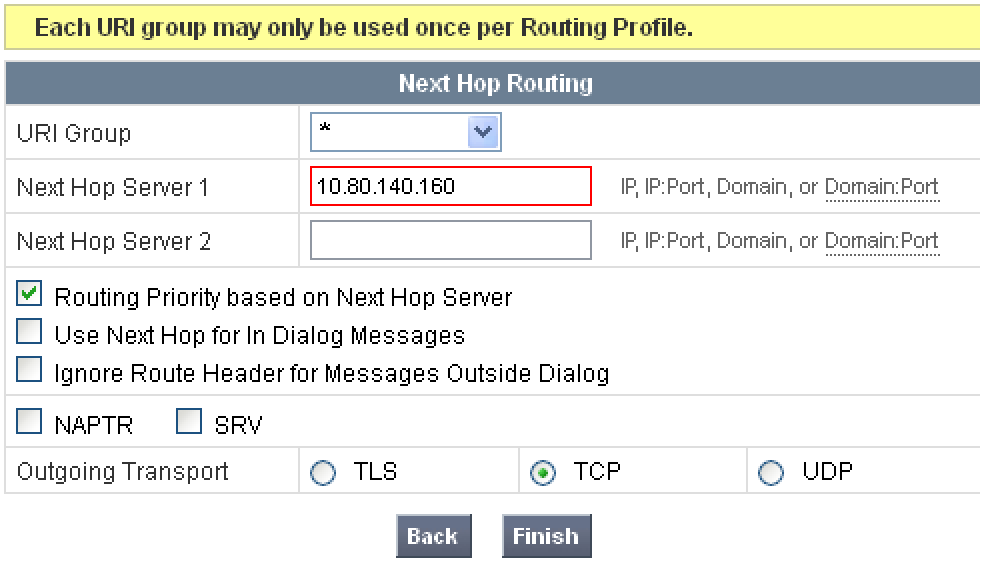


7.5.1 Routing Configuration for Session Manager

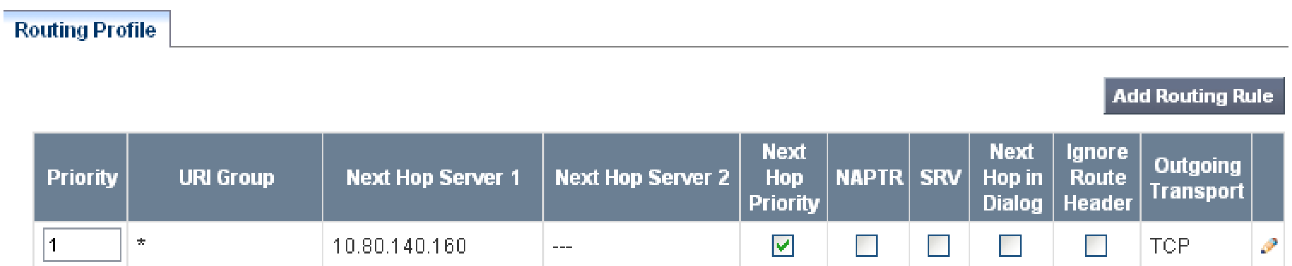
Click the **Add Profile** button (not shown) to add a new profile, or select an existing routing profile to edit. If adding a profile, a screen such as the following is displayed. Enter a **Profile Name** such as "To_Avaya" shown below. Click **Next**.



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 **Routing Priority based on Next Hop Server**. Choose **TCP** for **Outgoing Transport**.

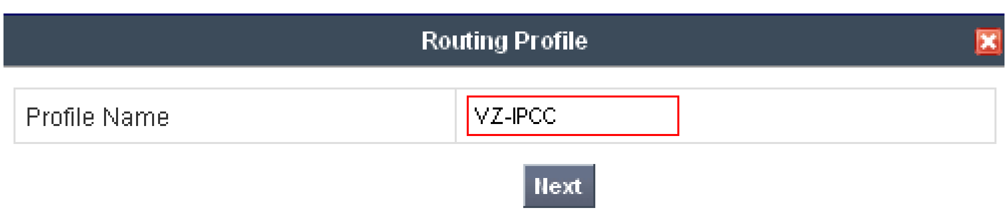


Once configuration is completed, the **Routing Profile** for "To_Avaya" will appear as follows.

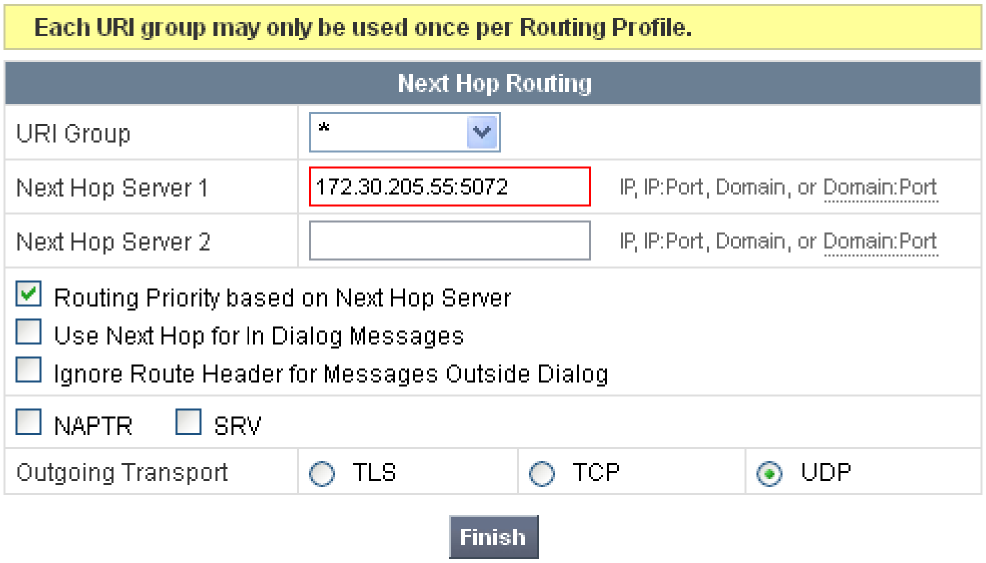


7.5.2 Routing Configuration for Verizon IPCC

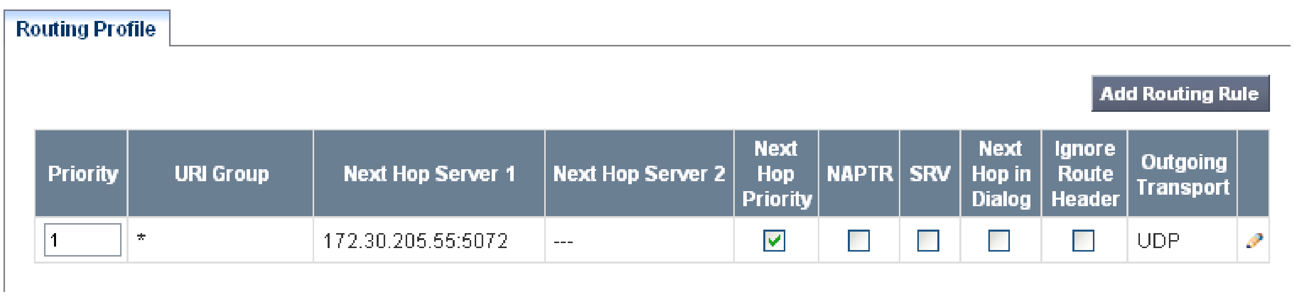
Click the **Add Profile** button (not shown) to add a new profile, or select an existing routing profile to edit. If adding a profile, a screen such as the following is displayed. Enter a **Profile Name** such as "VZ-IPCC" shown below. Click **Next**.



For the **Next Hop Server 1**, enter the IP Address of the Verizon IPCC service, a colon, and the port to be used (e.g., 172.30.205.55:5072) as shown in the screen below. Check **Routing Priority based on Next Hop Server**. Choose **UDP** for **Outgoing Transport**.

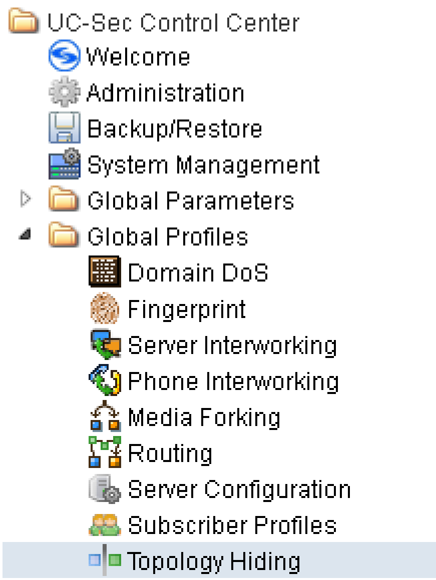


Once configuration is completed, the **Routing Profile** for "VZ-IPCC" will appear as follows.



7.6. Global Profiles – Topology Hiding

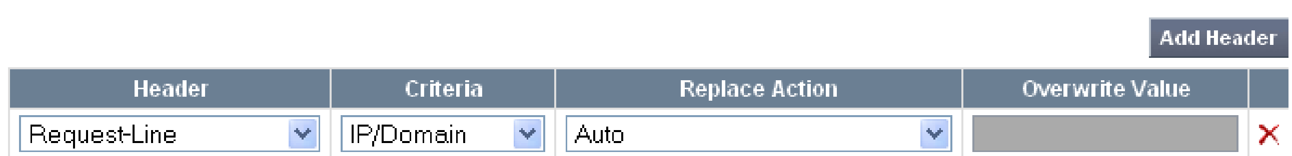
Select **Global Profiles → Topology Hiding** from the left-side menu as shown below.



7.6.1 Topology Hiding for Session Manager

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 to reveal additional headers.



If it is desired to ensure that the domain received by Session Manager from the SBC is the expected enterprise domain, select "Overwrite" as the **Replace Action** for the To, From, and Request-Line headers. Enter the enterprise domain in the **Overwrite Value** column as shown below. In the example below, the domain received by Session Manager is changed by the SBC to "avayalab.com". Click **Finish**.

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

7.6.2 Topology Hiding for Verizon IPCC

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 "VZ-IPCC" shown below. Click **Next**.

Topology Hiding Profile	
Profile Name	VZ-IPCC

Next

In the resultant screen, click the **Add Header** button in the upper right to reveal additional headers until the final screen appears as follows. The default "Auto" behaviors are sufficient. Click **Finish**.

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

Finish

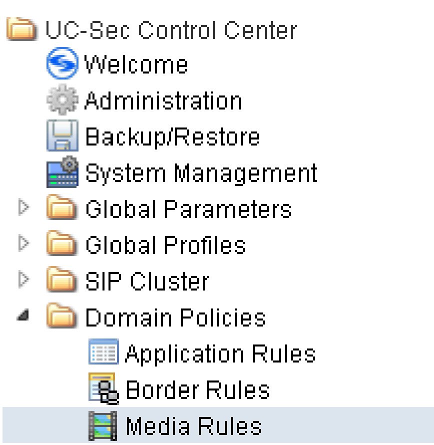
After configuration is completed, the **Topology Hiding** for profile “VZ-IPCC” will appear as follows.

Topology Hiding

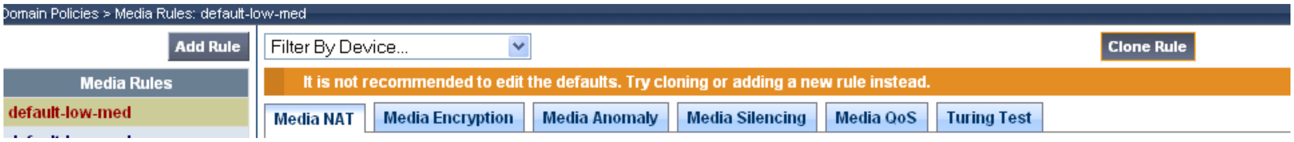
Header	Criteria	Replace Action	Overwrite Value
Record-Route	IP/Domain	Auto	---
Via	IP/Domain	Auto	---
To	IP/Domain	Auto	---
From	IP/Domain	Auto	---
Request-Line	IP/Domain	Auto	---
SDP	IP/Domain	Auto	---

7.7. Domain Policies – Media Rules

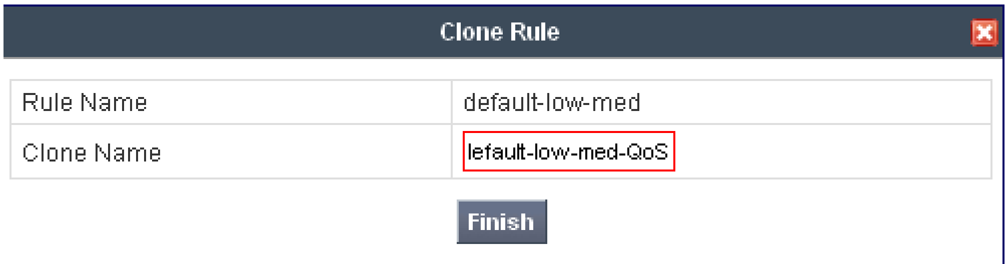
Select **Domain Policies → Media Rules** from the left-side menu as shown below.



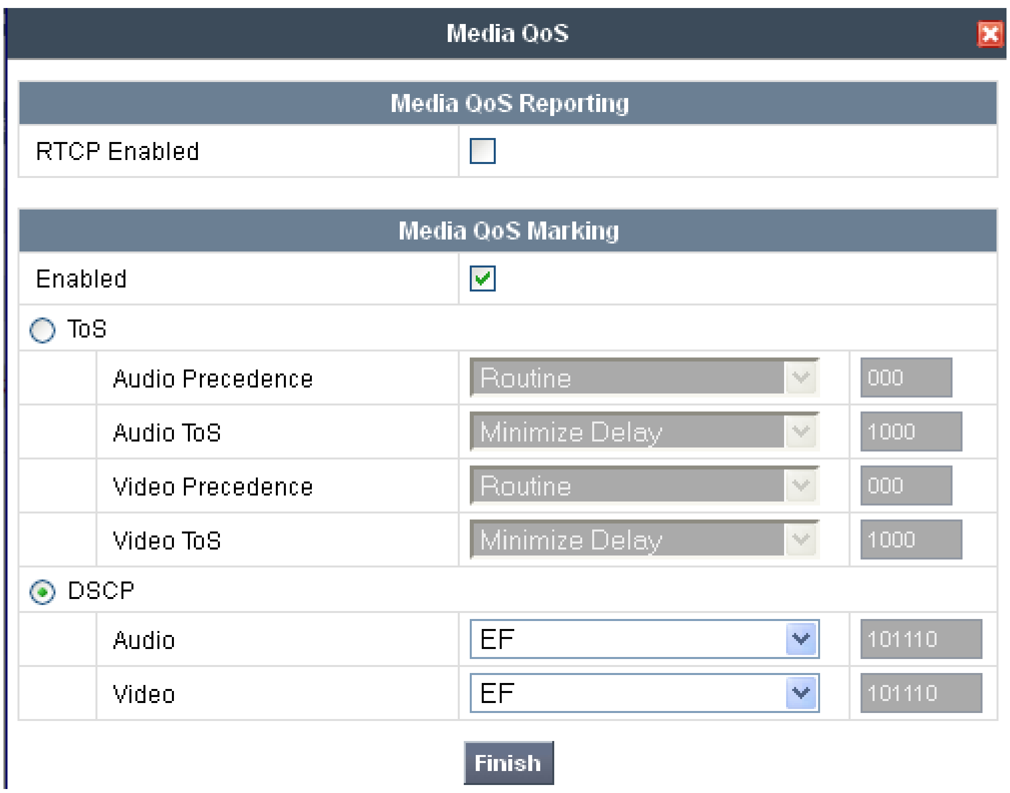
In the sample configuration, a single media rule was created by cloning the default rule called “default-low-med”. Select the default-low-med rule and click the **Clone Rule** button.



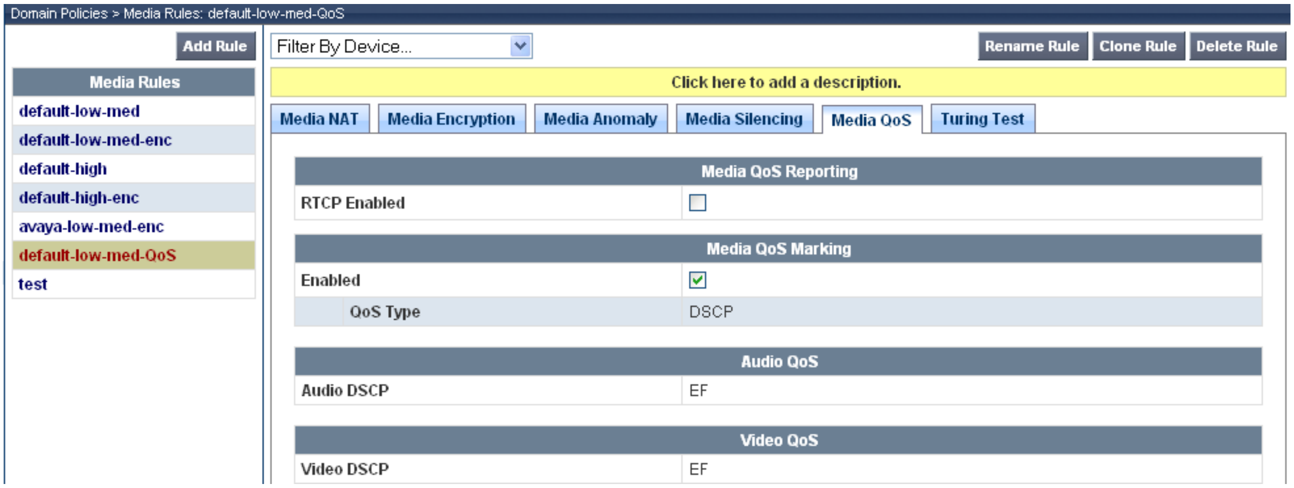
Enter a name in the **Clone Name** field, such as "default-low-med-QoS" as shown below. Click **Finish**.



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

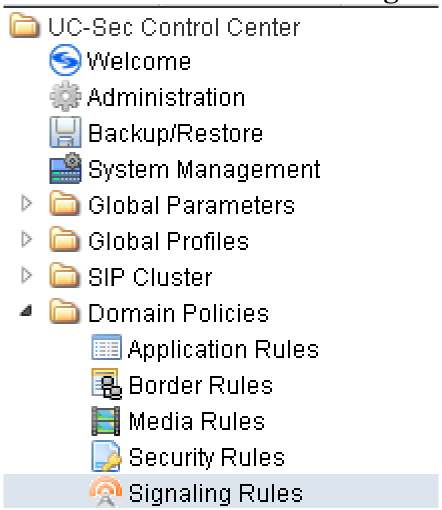


When configuration is complete, the “default-low-med-QoS” media rule **Media QoS** tab appears as follows.



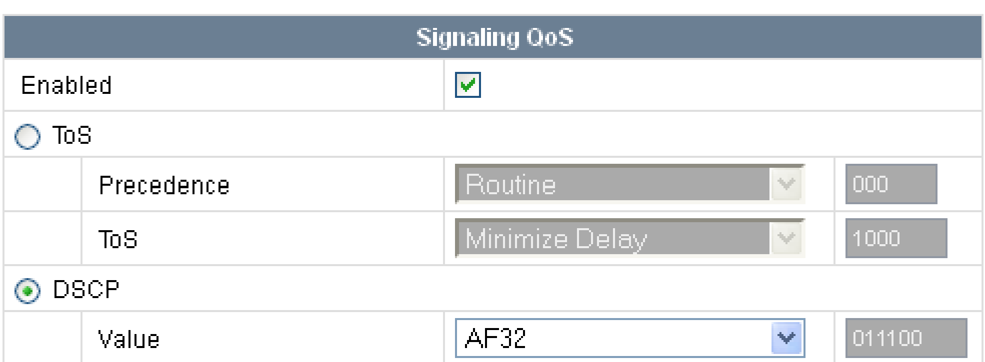
7.8. Domain Policies – Signaling Rules

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



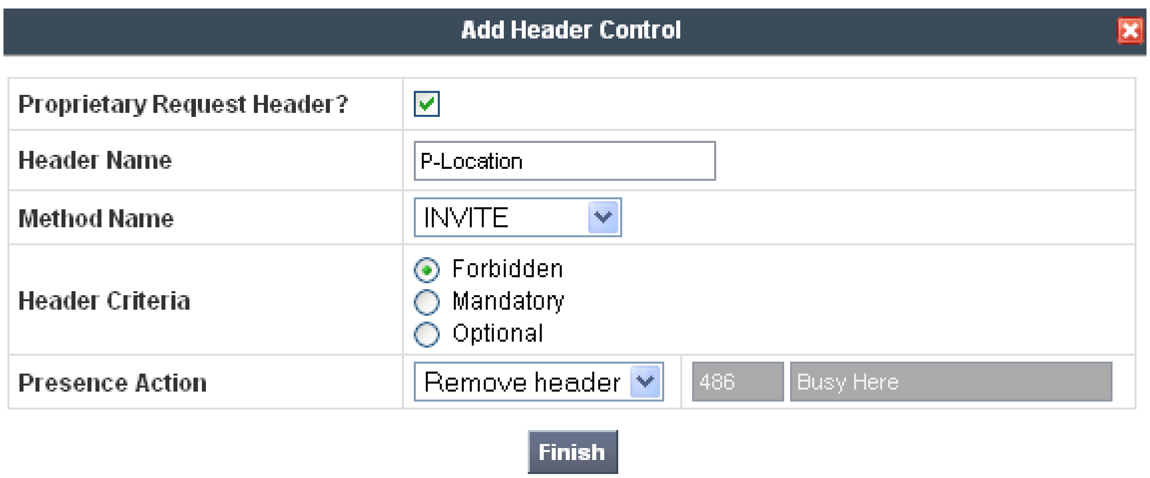
Click the **Add Rule** button to add a new signaling rule. In the **Rule Name** field, enter an appropriate name, such as "Block_Hdr_Remark".

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

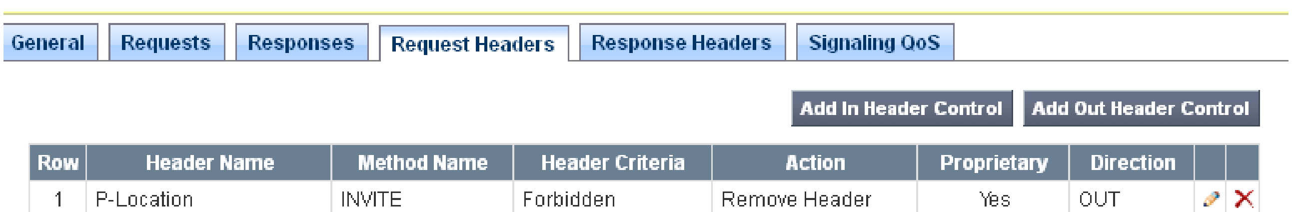


After this configuration, the new "Block_Hdr_Remark" will appear as follows.

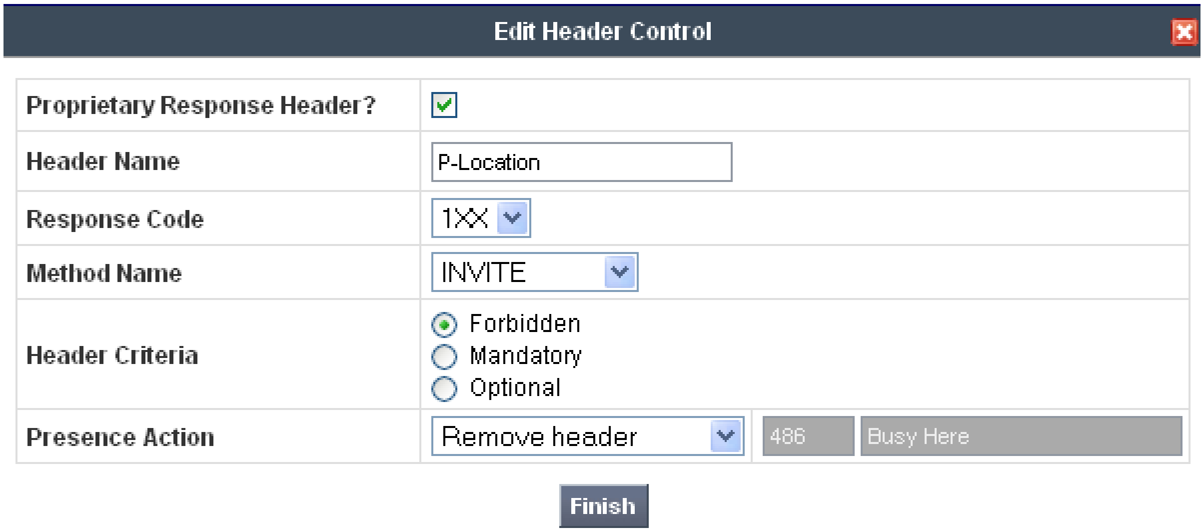
Select the **Request Headers** tab, and select the **Add Out Header Control** button (not shown). Check the **Proprietary Request Header?** Checkbox. In the **Header Name** field, type "P-Location". Select "INVITE" as the **Method Name**. In the Header Criteria, select **Forbidden**. Retain **Presence Action** "Remove header". The intent is to remove the P-Location header which is inserted by Session Manager, but not needed by Verizon. This configuration is optional in that the P-Location header does not cause any user-perceivable problem if presented to Verizon.



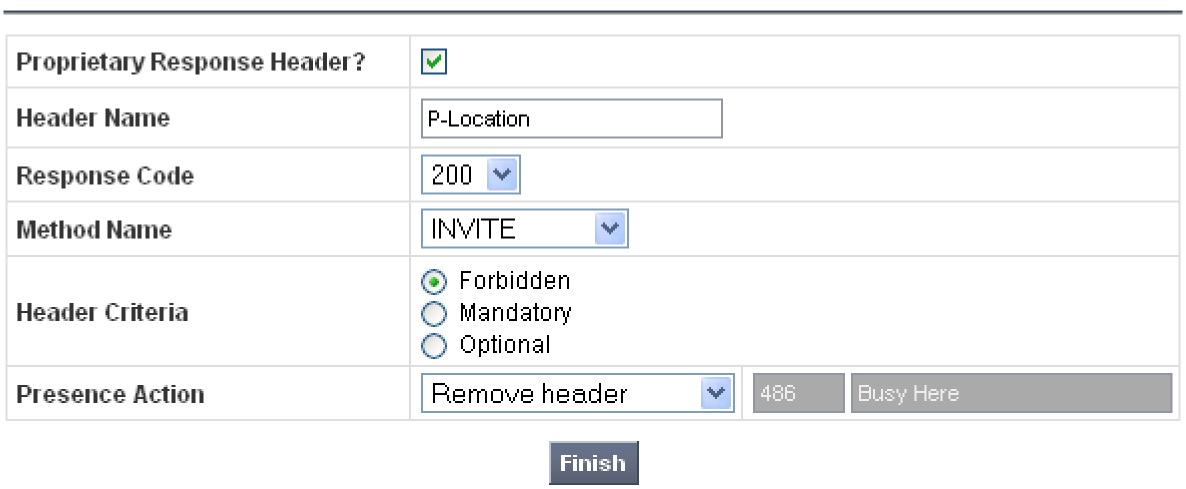
Once complete, the **Request Headers** tab appears as follows.



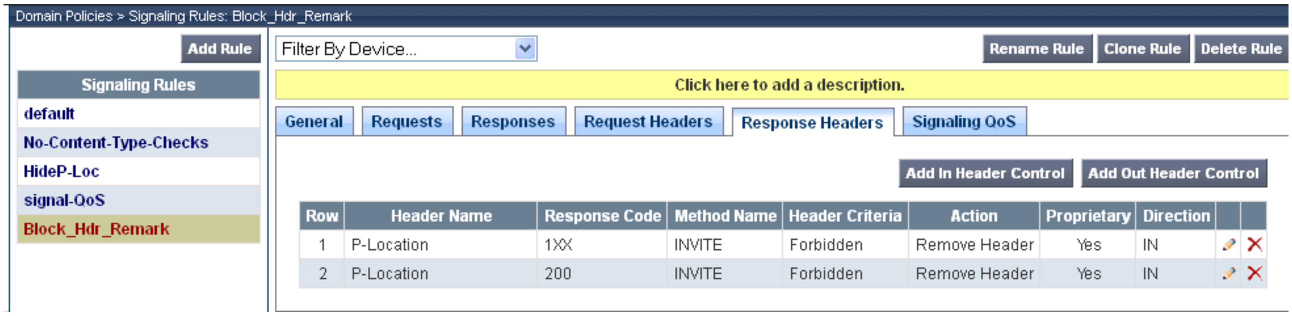
Select the **Response Headers** tab, and select the **Add In Header Control** button (not shown). Check **Proprietary Response Header?** In the **Header Name** field, type "P-Location". Select "INVITE" as the **Method Name,** and "1XX" from the **Response Code** drop-down. In the Header Criteria, select **Forbidden**. Retain **Presence Action** "Remove header". The intent is to remove the P-Location header from 1XX responses. This configuration is optional in that the P-Location header does not cause any user-perceivable problem if presented to Verizon. Click **Finish**.



Again, select or remain within the **Response Headers** tab, and select the **Add In Header Control** button. Check **Proprietary Response Header?** In the **Header Name** field, type "P-Location". Select "INVITE" as the **Method Name,** and "200" from the **Response Code** drop-down. In the **Header Criteria**, select **Forbidden**. Retain **Presence Action** "Remove header". The intent is to remove the P-Location header from 200 OK responses. This configuration is optional in that the P-Location header does not cause any user-perceivable problem if presented to Verizon. Click **Finish**.

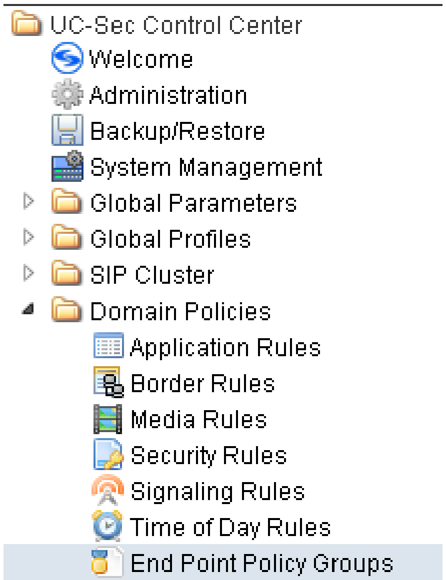


Once configuration is complete, the Response Headers tab for the "Block_Hdr_Remark" signaling rule will appear as follows.

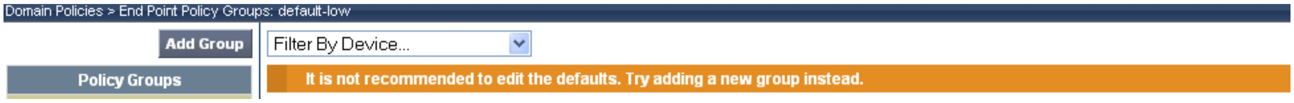


7.9. Domain Policies – End Point Policy Groups

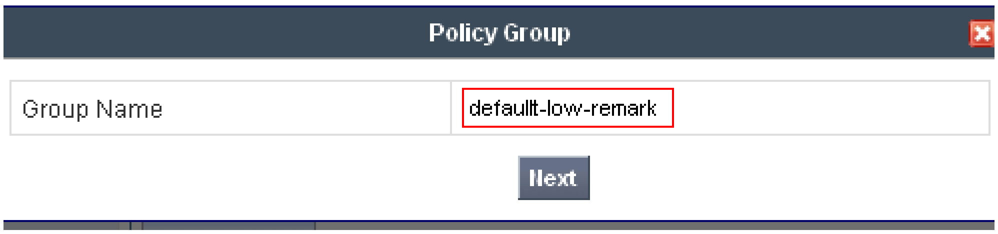
Select **Domain Policies → End Point Policy Groups** from the left-side menu as shown below.



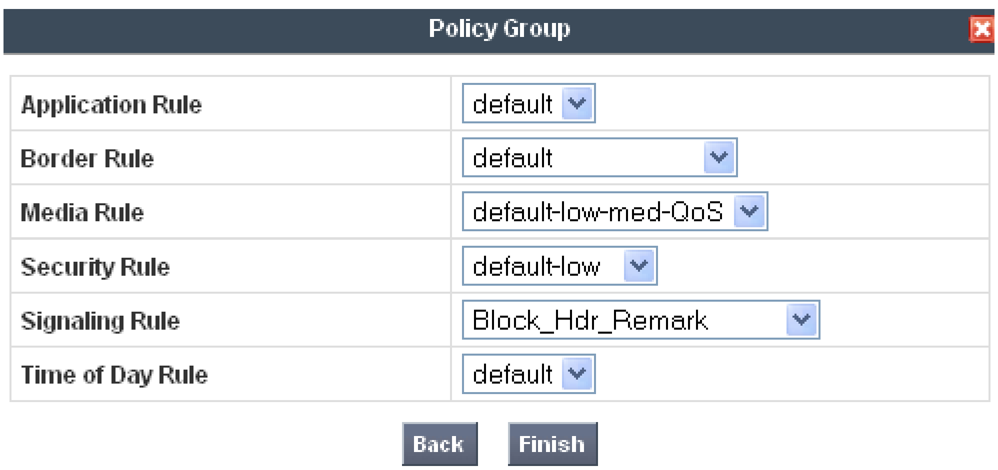
Select the **Add Group** button.



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



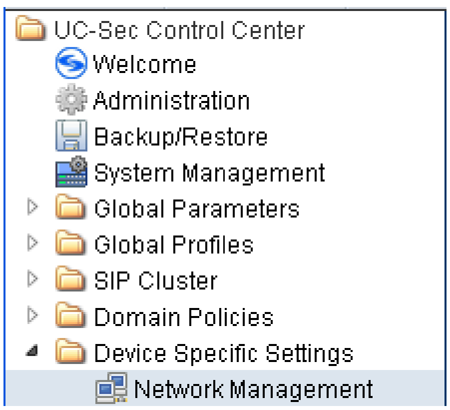
In the sample configuration, defaults were selected for all fields, with the exception of the **Media Rule** which was set to "default-low-med-QoS", and the **Signaling Rule**, which was set to "Block_Hdr_Remark" as shown below. The selected non-default media rule and signaling rule chosen were created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



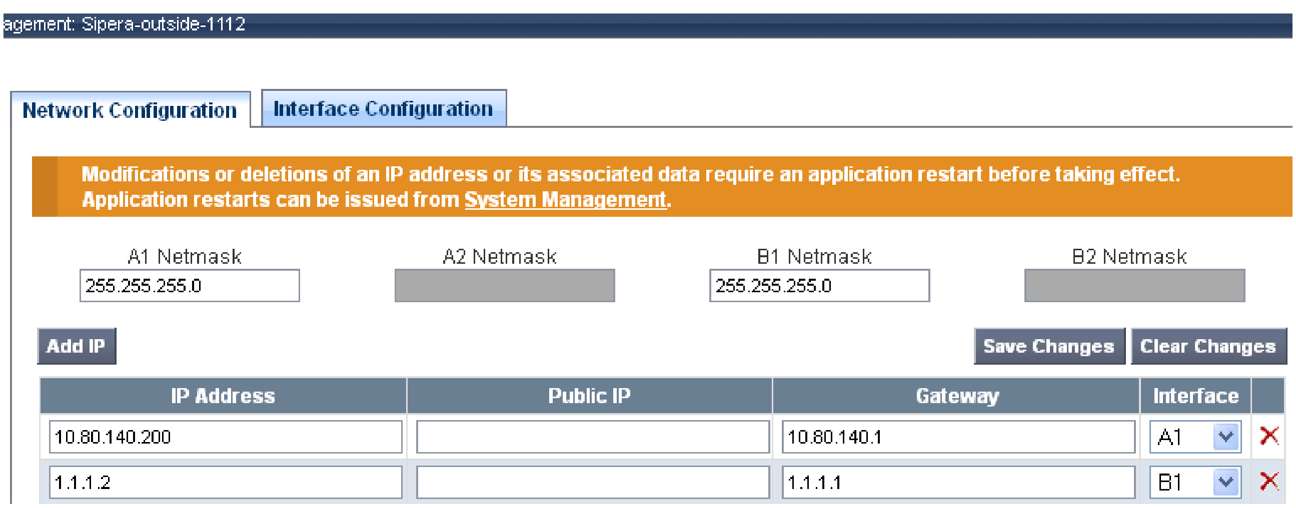
Once configuration is completed, the "default-low-remark" policy group will appear as follows.

7.10. Device Specific Settings - Network Management

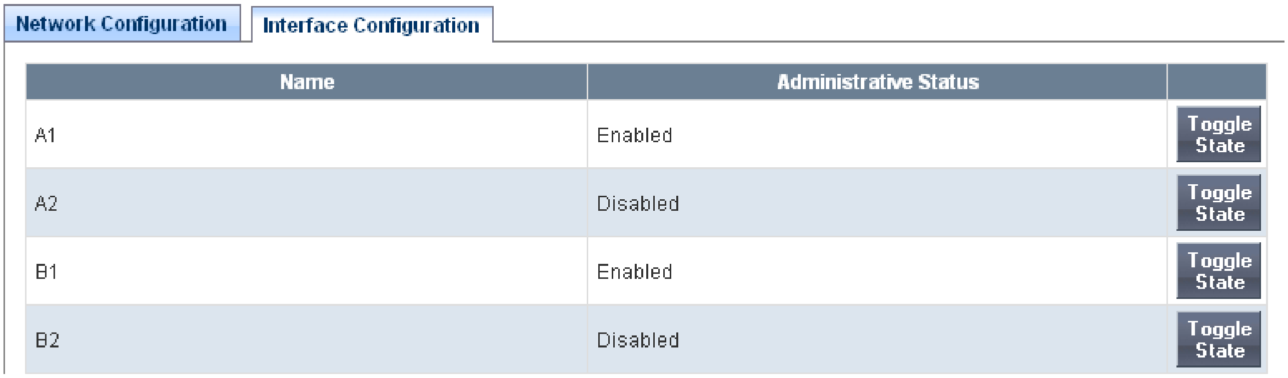
Select **Device Specific Setting → Network Management** from the left-side menu as shown below.



Under **UC-Sec Devices**, select the device being managed, which was named "Sipera-outside-1112" in the sample configuration (not shown). The **Network Configuration** tab is shown below. Observe the **IP Address**, **Netmask**, **Gateway**, and **Interface** information previously assigned.



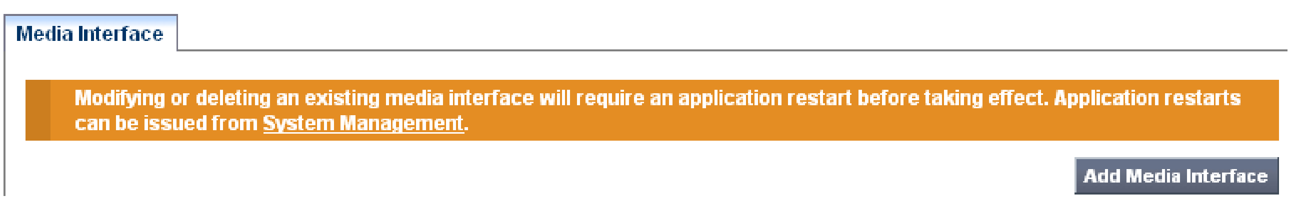
Select the **Interface Configuration** tab. The **Administrative Status** can be toggled between "Enabled" and "Disabled" in this screen. The following screen was captured after the interfaces had already been enabled. To enable the interface if it is disabled, click the **Toggle State** button.



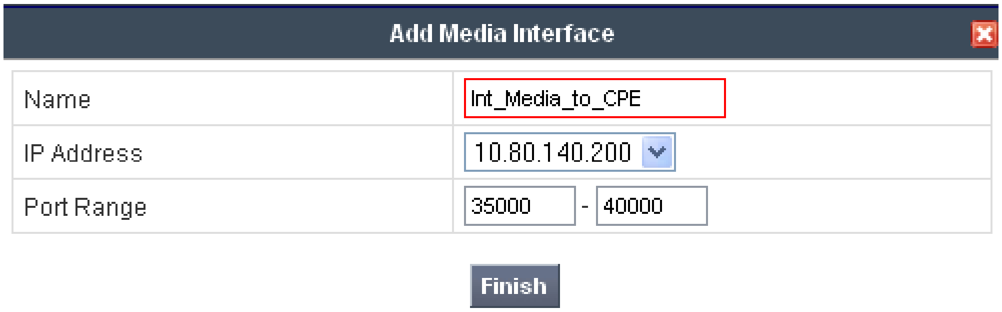
7.11. Device Specific Settings – Media Interface

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

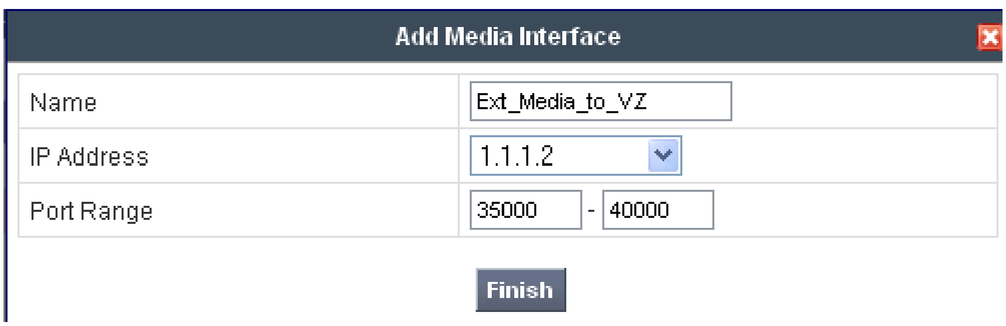
Under **UC-Sec Devices**, select the device being managed, which was named "Sipera-outside-1112" in the sample configuration (not shown). Select **Add Media Interface**.



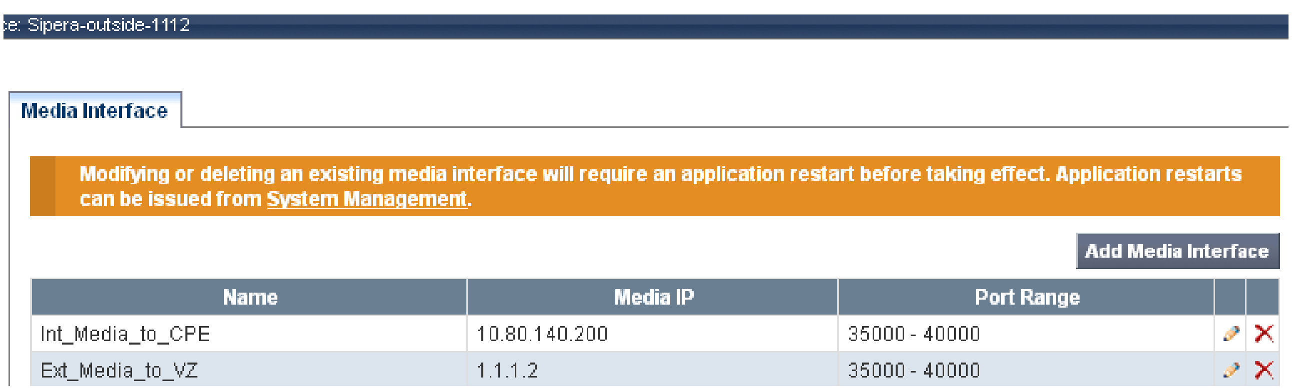
Enter an appropriate **Name** for the media interface for the Avaya CPE and select the inside private IP Address from the **IP Address** drop-down menu. In the sample configuration, "Int_Media_to_CPE" is chosen as the name, and the "inside" IP Address of the SBC is "10.80.140.200". For the **Port Range**, 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 SBC, 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 SBC is "1.1.1.2". For the **Port Range**, default values are shown. Verizon IPCC does not require that the RTP ports be chosen within a specific range. Click **Finish**.

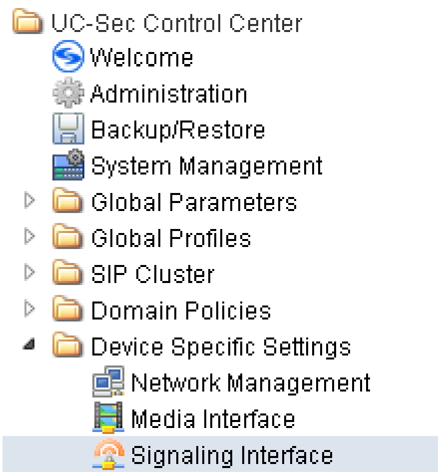


The resultant Media Interface configuration used in the sample configuration is shown below.



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 "Sipera-outside-1112" in the sample configuration (not shown). Select **Add Signaling Interface**.

In the Add 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., 10.80.140.200) from the **IP Address** drop-down menu. Choose **TCP Port** "5060" since TCP and port 5060 is used between Session Manager and the SBC in the sample configuration. Click **Finish**.

Name	Sig_Inside_to_CPE
IP Address	10.80.140.200
TCP Port Leave blank to disable	5060
UDP Port Leave blank to disable	
TLS Port Leave blank to disable	
Cluster TLS Only for use with Cisco SIP Clusters	☐
Enable Stun Requires a UDP Port	☐

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., 1.1.1.2) from the **IP Address** drop-down menu. Choose **UDP Port** "5060". In the sample configuration, Verizon will send SIP signaling using UDP to the CPE IP Address 1.1.1.2 and to UDP Port 5060. Click **Finish**.

Name	Sig_Outside_to_VZ
IP Address	1.1.1.2
TCP Port Leave blank to disable	
UDP Port Leave blank to disable	5060
TLS Port Leave blank to disable	
Cluster TLS Only for use with Cisco SIP Clusters	☐
Enable Stun Requires a UDP Port	☐

Finish

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

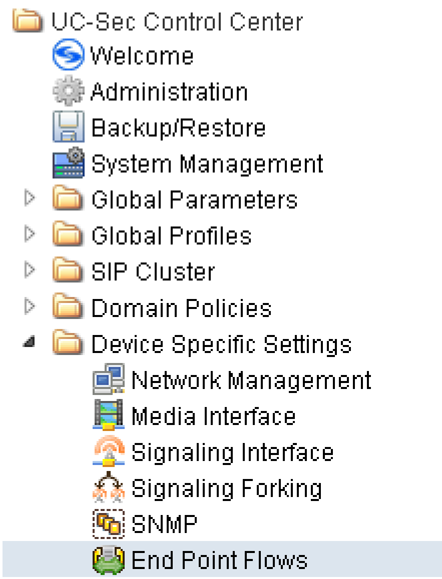
Signaling Interface

Add Signaling Interface

Name	Signaling IP	TCP Port	UDP Port	TLS Port	TLS Profile		
Sig_Inside_to_CPE	10.80.140.200	5060	---	---	None		
Sig_Outside_to_VZ	1.1.1.2	---	5060	---	None		

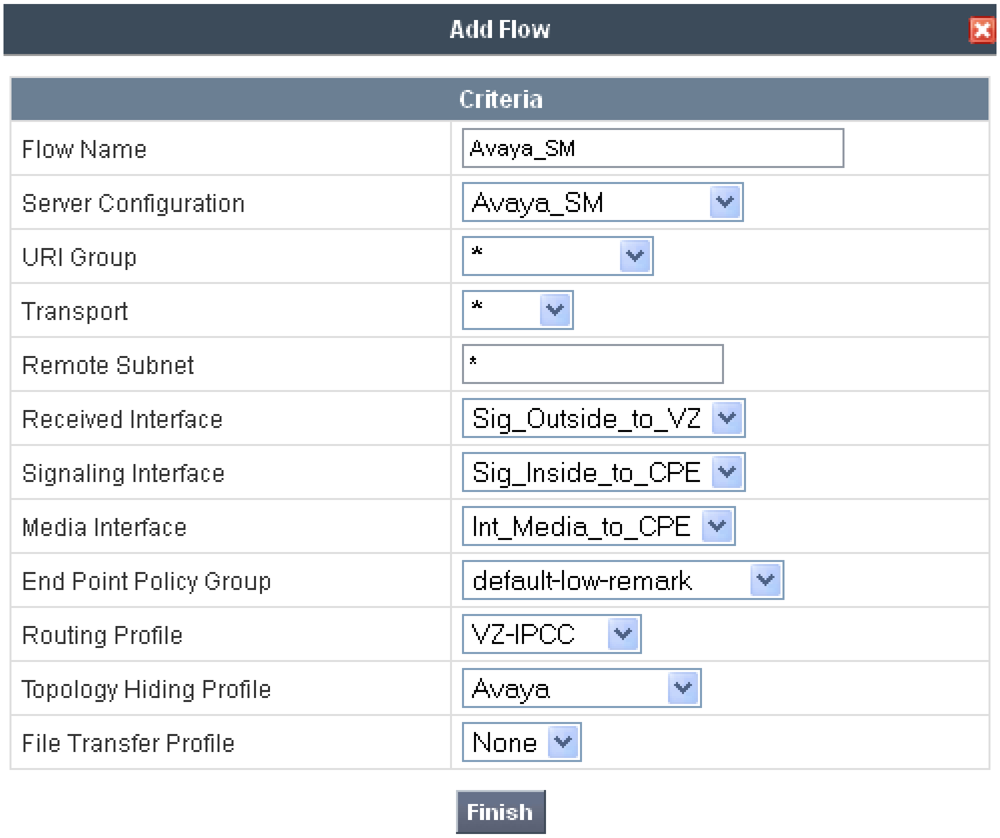
7.13. Device Specific Settings – End Point Flows

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



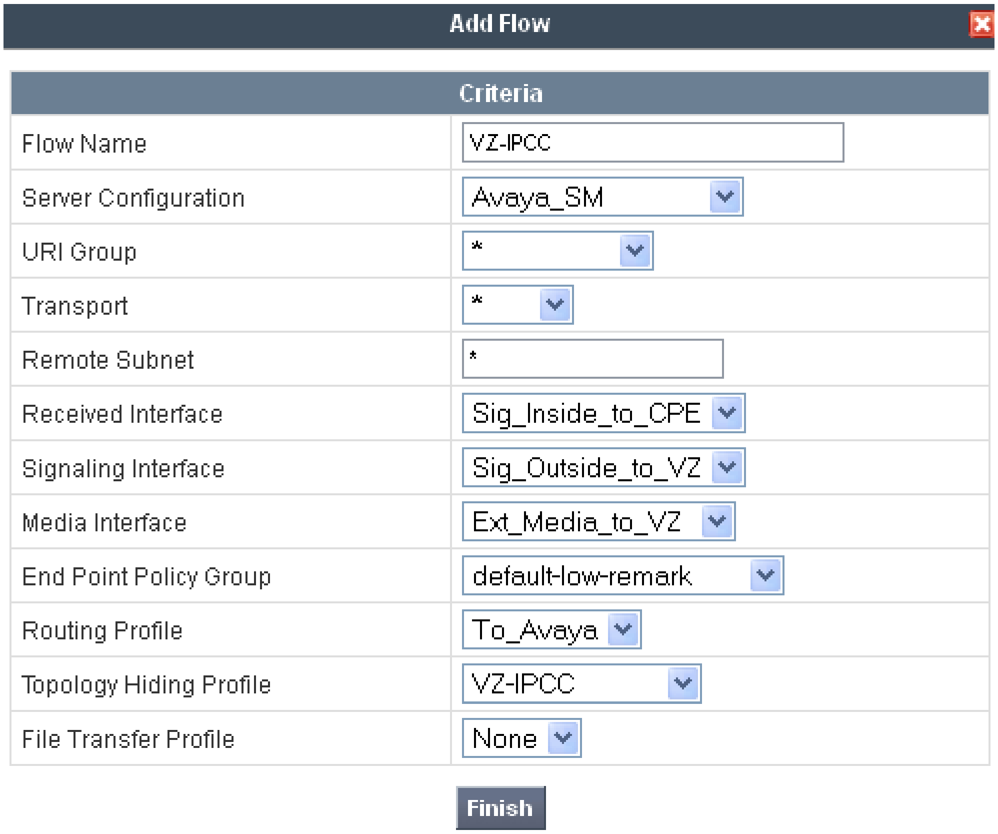
Under **UC-Sec Devices**, select the device being managed, which was named "Sipera-outside-1112" in the sample configuration (not shown). Select the **Server Flows** tab. Select **Add Flow**.

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-IPCC" being added to the sample configuration. This flow uses the interfaces, policies, and profiles defined in previous sections. Click **Finish**.

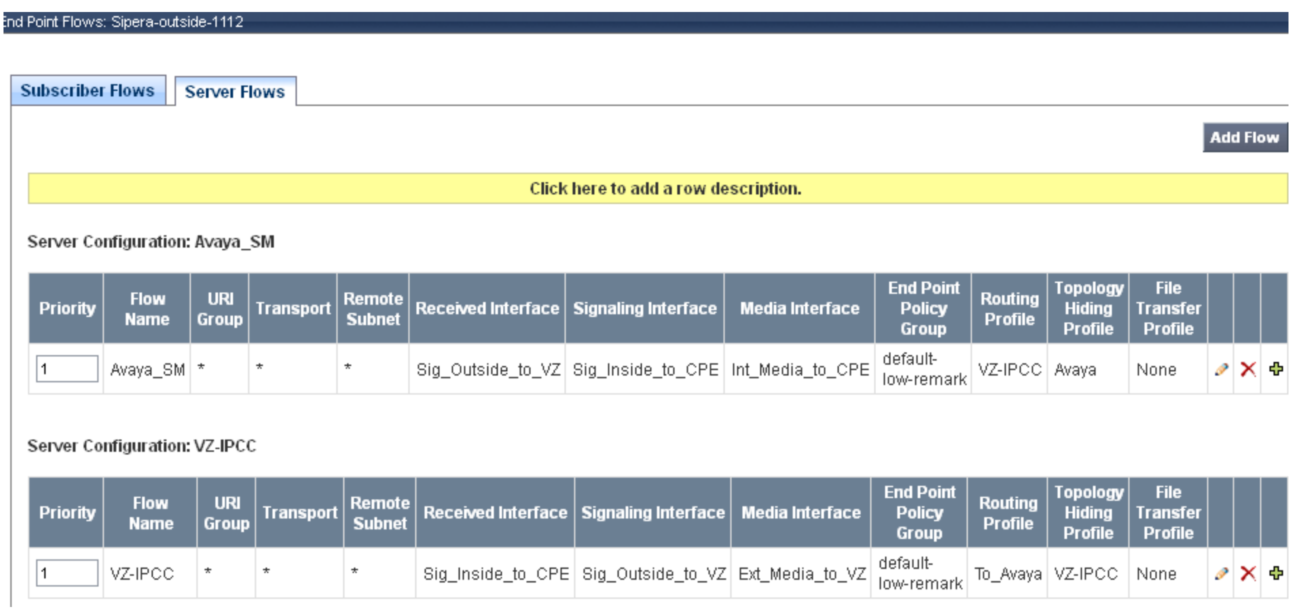


Add Flow

Criteria	
Flow Name	VZ-IPCC
Server Configuration	Avaya_SM
URI Group	*
Transport	*
Remote Subnet	*
Received Interface	Sig_Inside_to_CPE
Signaling Interface	Sig_Outside_to_VZ
Media Interface	Ext_Media_to_VZ
End Point Policy Group	default-low-remark
Routing Profile	To_Avaya
Topology Hiding Profile	VZ-IPCC
File Transfer Profile	None

Finish

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



End Point Flows: Sipera-outside-1112

Subscriber Flows | Server Flows

Add Flow

Click here to add a row description.

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	default-low-remark	VZ-IPCC	Avaya	None

Server Configuration: VZ-IPCC

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	VZ-IPCC	*	*	*	Sig_Inside_to_CPE	Sig_Outside_to_VZ	Ext_Media_to_VZ	default-low-remark	To_Avaya	VZ-IPCC	None

8. Verizon Business IPCC Services Suite Configuration

Information regarding Verizon Business IPCC Services suite offer can be found at http://www.verizonbusiness.com/products/contactcenter/ip/ or by contacting a Verizon Business sales representative.

The reference configuration described in these Application Notes was located in the Avaya Solutions and Interoperability Test Lab. Access to the Verizon Business IPCC 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) was provided by Verizon for the sample configuration.

CPE (Avaya)	Verizon Network
adevc.avaya.globalipcom.com ***UDP port 5060***	***172.30.205.55*** ***UDP Port 5072***

For IP-IVR, Verizon provided "Published Numbers" to be dialed by the PSTN callers, and the corresponding "Outdial Numbers" that Verizon sends in the Request-URI of INVITE messages sent to the enterprise site. These IP-IVR numbers are shown in **Figure 1** in **Section 3**.

9. Verification Steps

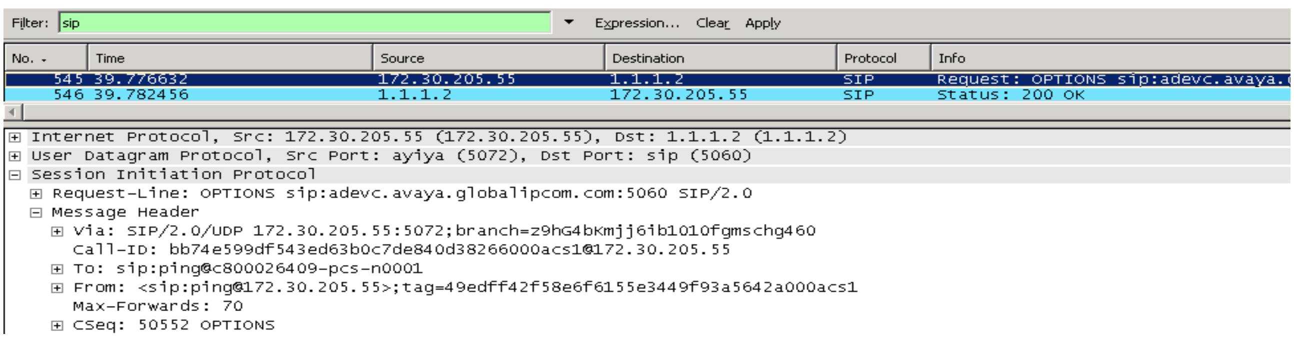
This section provides example verifications of the sample configuration illustrated in these Application Notes.

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 Avaya Session Border Controller for Enterprise.

9.1.1 Incoming OPTIONS from Verizon IPCC to Avaya CPE

The following screens from a filtered Wireshark trace illustrate OPTIONS sent by Verizon to the Avaya CPE. Verizon IPCC 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 SBC, frame 545 is highlighted and expanded to show OPTIONS sent from Verizon IPCC (172.30.205.55) to the SBC (1.1.1.2). Observe the use of UDP for transport, from source port 5072 (Verizon) to destination port 5060 (Avaya). Verizon sends the Avaya domain "adevc.avaya.globalipcom.com" in the Request-Line. Note that Max-Forwards is 70.



Before the SBC replies to Verizon, the SBC sends OPTIONS to Session Manager on the inside private interface. In the trace shown below, taken from the inside private side of the SBC, frame 997 is highlighted and expanded to show OPTIONS sent from the inside interface of the SBC (10.80.140.200) to Session Manager (10.80.140.160). Observe the use of TCP for transport, using port 5060. Observe that the SBC 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.  Time         Source          Destination     Protocol  Info
997  34.985891    10.80.140.200   10.80.140.160   SIP       Request: OPTIONS sip:avayalab.com
998  34.989622    10.80.140.160   10.80.140.200   SIP       Status: 200 OK

+ Internet Protocol, Src: 10.80.140.200 (10.80.140.200), Dst: 10.80.140.160 (10.80.140.160)
+ Transmission Control Protocol, Src Port: entextxid (12000), Dst Port: sip (5060), Seq: 1, Ack: 2, Len: 393
- Session Initiation Protocol
  + Request-Line: OPTIONS sip:avayalab.com SIP/2.0
  - Message Header
    + From: <sip:ping@avayalab.com>;tag=49edff42f58e6f6155e3449f93a5642a000acs1
    + To: sip:ping@avayalab.com
    + CSeq: 50552 OPTIONS
      Call-ID: 907adb2f2d9d6c6860e2c84a903e795e
      Record-Route: <sip:10.80.140.200:5060;ipcs-line=18755;lr;transport=tcp>
      Max-Forwards: 69
    + Via: SIP/2.0/TCP 10.80.140.200:5060;branch=z9hG4bK-s1632-001505359549-1--s1632-
      Content-Length: 0
```

In this same trace, highlighted frame 998 below shows Session Manager responding to the OPTIONS with 200 OK. Although not shown below, note that Session Manager includes a "Server" header in the 200 OK, where the "Server" headers will contain a string like "Avaya-SM-6.2<more>" where <more> further identifies the Session Manager release.

```
No.  Time         Source          Destination     Protocol  Info
997  34.985891    10.80.140.200   10.80.140.160   SIP       Request: OPTIONS sip:avayalab.com
998  34.989622    10.80.140.160   10.80.140.200   SIP       Status: 200 OK

+ Internet Protocol, Src: 10.80.140.160 (10.80.140.160), Dst: 10.80.140.200 (10.80.140.200)
+ Transmission Control Protocol, Src Port: sip (5060), Dst Port: entextxid (12000), Seq: 2, Ack: 394, Len: 536
- Session Initiation Protocol
  + Status-Line: SIP/2.0 200 OK
  - Message Header
    + Via: SIP/2.0/TCP 10.80.140.200:5060;branch=z9hG4bK-s1632-001505359549-1--s1632-
    + To: sip:ping@avayalab.com;tag=1012819428*1*016asm-callprocessing.sar-1601417206~1328646177948~-1272789723~1
    + From: <sip:ping@avayalab.com>;tag=49edff42f58e6f6155e3449f93a5642a000acs1
      Call-ID: 907adb2f2d9d6c6860e2c84a903e795e
    + CSeq: 50552 OPTIONS
```

Returning to the outside trace, and advancing to frame 546, the 200 OK sent back to the inbound OPTIONS from Verizon is illustrated below. The receipt of a valid OPTIONS response from the CPE is necessary for Verizon to route inbound calls to the CPE. Since the SBC proxies the OPTIONS received from Verizon to Session Manager, the end to end path from Verizon through to Session Manager must be in-service for OPTIONS (and ultimately calls) to be successful.

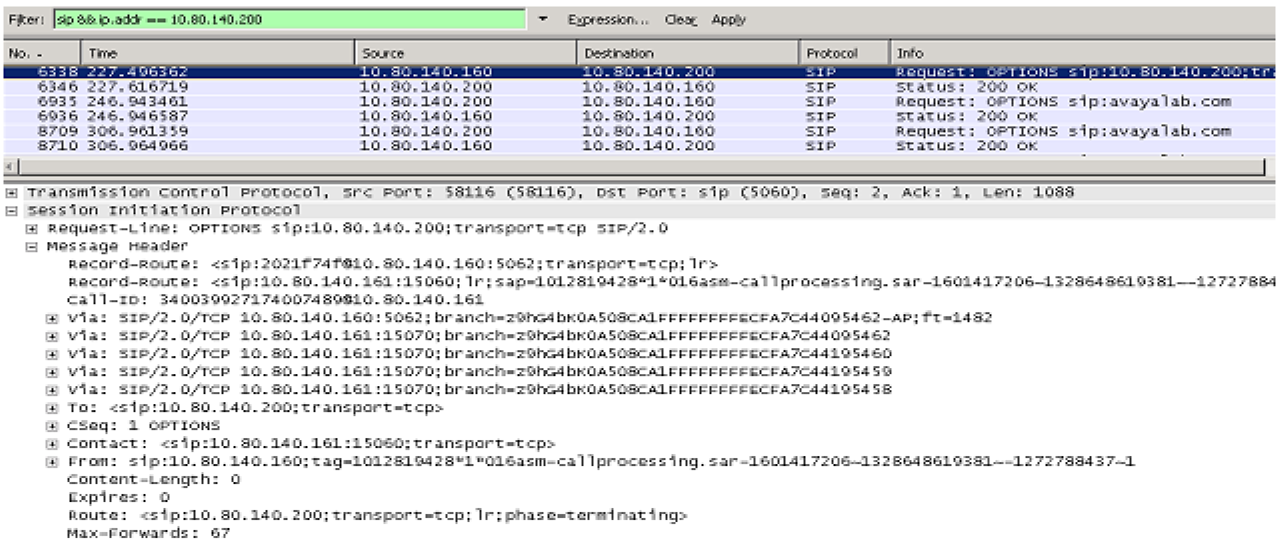
```
No.  Time         Source          Destination     Protocol  Info
545  39.776632    172.30.205.55   1.1.1.2         SIP       Request: OPTIONS sip:adevc.avaya.g
546  39.782456    1.1.1.2         172.30.205.55   SIP       Status: 200 OK

+ Internet Protocol, Src: 1.1.1.2 (1.1.1.2), Dst: 172.30.205.55 (172.30.205.55)
+ User Datagram Protocol, Src Port: sip (5060), Dst Port: ayiya (5072)
- Session Initiation Protocol
  + Status-Line: SIP/2.0 200 OK
  - Message Header
    + From: <sip:ping@172.30.205.55>;tag=49edff42f58e6f6155e3449f93a5642a000acs1
    + To: sip:ping@c800026409-pcs-n0001;tag=1012819428*1*016asm-callprocessing.sar-1601417206~1328646177948~-1272789723~1
    + CSeq: 50552 OPTIONS
      Call-ID: bb74e599df543ed63b0c7de840d38266000acs1@172.30.205.55
      Record-Route: <sip:1.1.1.2:5060;ipcs-line=18755;lr;transport=udp>
    + Via: SIP/2.0/UDP 172.30.205.55:5072;branch=z9hG4bKmjj6ib1010fgmschg460
```

The following filtered trace from the outside interface shows that Verizon IPCC service sends OPTIONS to the Verizon CPE every 60 seconds in the sample configuration.

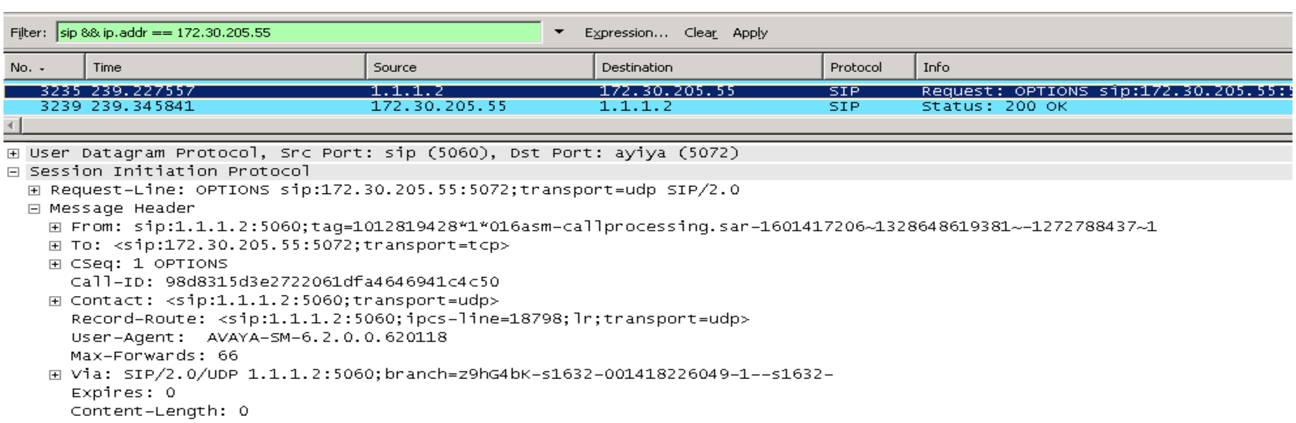
```
Filter: sip && ip.addr == 172.30.205.55      Expression...  Clear  Apply

No.   Time         Source          Destination     Protocol  Info
14    0.769599     172.30.205.55   1.1.1.2         SIP       Request: OPTIONS sip:adevc.avaya.glol
15    0.775465     1.1.1.2         172.30.205.55   SIP       Status: 200 OK
831   60.788340    172.30.205.55   1.1.1.2         SIP       Request: OPTIONS sip:adevc.avaya.glol
833   60.794280    1.1.1.2         172.30.205.55   SIP       Status: 200 OK
1693  120.807306   172.30.205.55   1.1.1.2         SIP       Request: OPTIONS sip:adevc.avaya.glol
1694  120.812854   1.1.1.2         172.30.205.55   SIP       Status: 200 OK
2514  180.823250   172.30.205.55   1.1.1.2         SIP       Request: OPTIONS sip:adevc.avaya.glol
2515  180.829282   1.1.1.2         172.30.205.55   SIP       Status: 200 OK
```

9.1.2 Outbound OPTIONS from Avaya CPE to Verizon IPCC

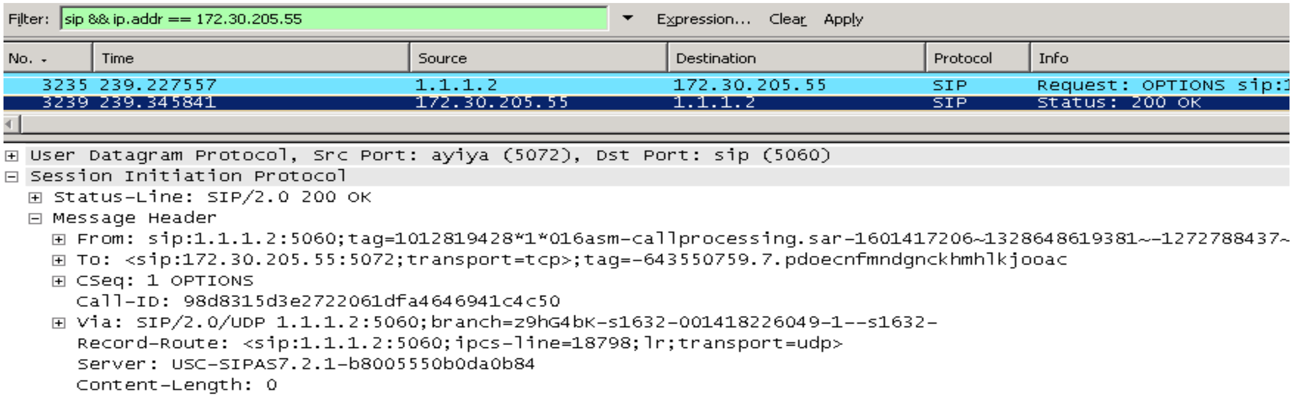
The following screens from filtered Wireshark traces illustrate OPTIONS sent by the Avaya CPE to Verizon IPCC. In the trace shown below, taken from the inside private interface of the SBC, frame 6338 is highlighted and expanded to show OPTIONS sent from the Session Manager SIP signaling interface (10.80.140.160) to the inside address of the SBC (10.80.140.200). Observe the use of TCP for transport using port 5060. Session Manager can send OPTIONS due to the SIP Entity Link Monitoring function. Note that Max-Forwards is 67 reflecting internal processing of the OPTIONS within Session Manager before it is sent to the destination SIP entity, in this case, the SBC.



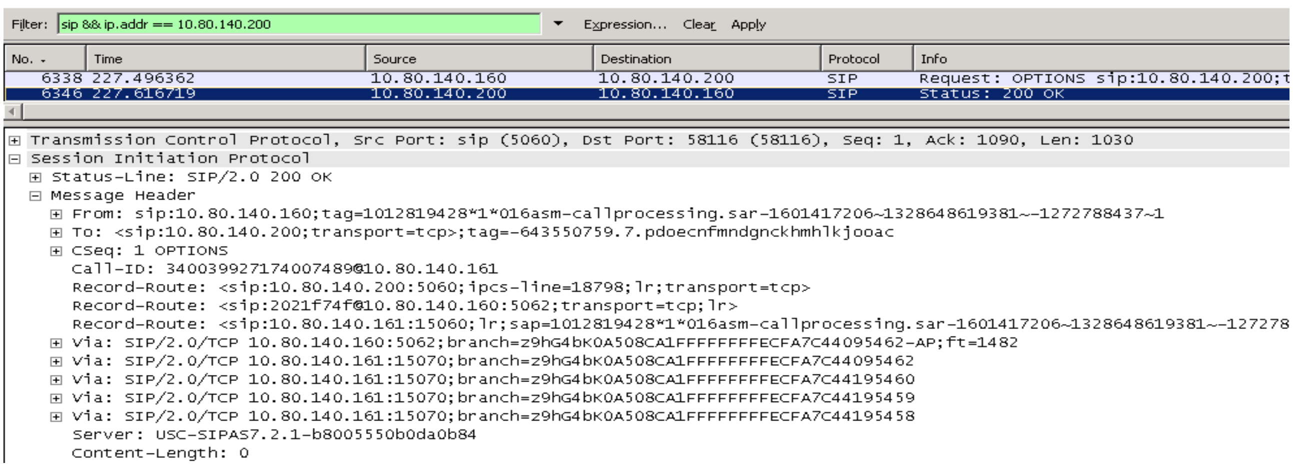
In the trace shown below, taken from the outside public side of the SBC, frame 3235 is highlighted and expanded to show OPTIONS sent from the SBC (1.1.1.2) to Verizon IPCC (172.30.205.55). Observe the use of UDP for transport, from source port 5060 (Avaya) to destination port 5072 (Verizon). Note that Max-Forwards has been decremented by one and is now 66.



Advancing to frame 3239 in the same outside trace, the following screen shows that the Verizon IPCC service responds with 200 OK. In this case, note that Verizon also added a "Server" header.



Returning to the inside private trace, the 200 OK from Verizon IPCC triggers the 200 OK back to Session Manager as shown in highlighted frame 6346 below. Note the "Server" header inserted by the Verizon IPCC server appears in this 200 OK sent back to Session Manager. Session Manager will consider the SIP Entity to the SBC "up".



As a result of the SBC relaying SIP OPTIONS from Verizon to Session Manager, and also relaying SIP OPTIONS from Session Manager to Verizon, SIP OPTIONS monitoring of the SIP trunk does not require the SBC to source its own SIP OPTIONS via the "heartbeat" capability, although that capability is also available if desired.

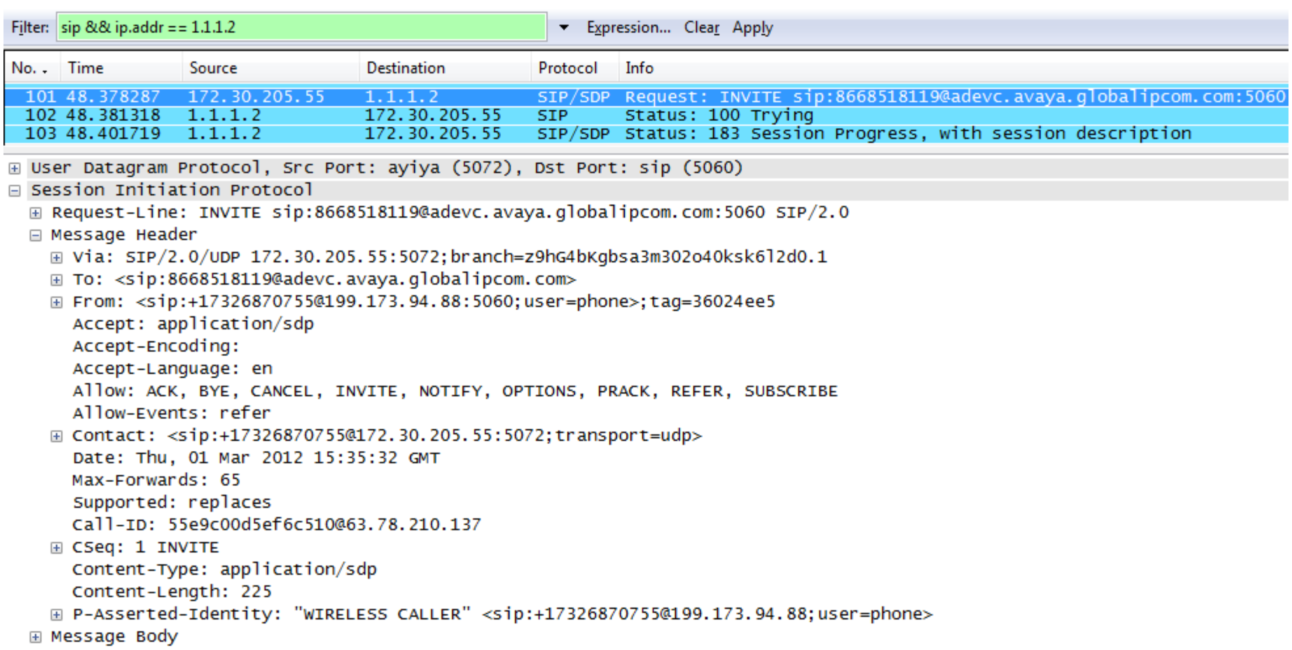
9.2. Sample Call Illustrations

This section uses Wireshark traces to illustrate basic IP-IVR SIP messaging and call flows. For Communication Manager "list trace" illustrations and for Wireshark traces showing more advanced call flows that use SIP REFER signaling, please refer to the corresponding **Section 9.2** of the companion Application Notes in reference [VZ-IPTF].

9.2.1 Example Incoming Call from PSTN via Verizon IP-IVR to Telephone

Incoming calls arrive from Verizon at the Avaya SBCE, which sends the call to Session Manager. Session Manager sends the call to Communication Manager via the entity link corresponding to Communication Manager processor Ethernet using port 5063. On Communication Manager, the incoming call arrives via signaling group 77 and trunk group 77.

The following portion of a filtered Wireshark trace (tracing only SIP messages on the public interface on the "outside" of the SBC) shows an incoming PSTN call. The PSTN user 732-687-0755 dialed the IP-IVR "published number" 866-616-4250. Verizon IPCC sends an INVITE to the CPE containing the corresponding IP-IVR "outdial number", in this case 866-851-8119. In frame 101, Verizon sends the INVITE to the Avaya SBCE (1.1.1.2). Frame 101 is selected and expanded so that the middle portion of the screen can illustrate the contents of the SIP headers sent by Verizon. The trace shows that the SIP message uses UDP with source port 5072 and destination port 5060. In frame 103, it can be observed that the Avaya CPE responds with 183 with SDP during the ringing phase.

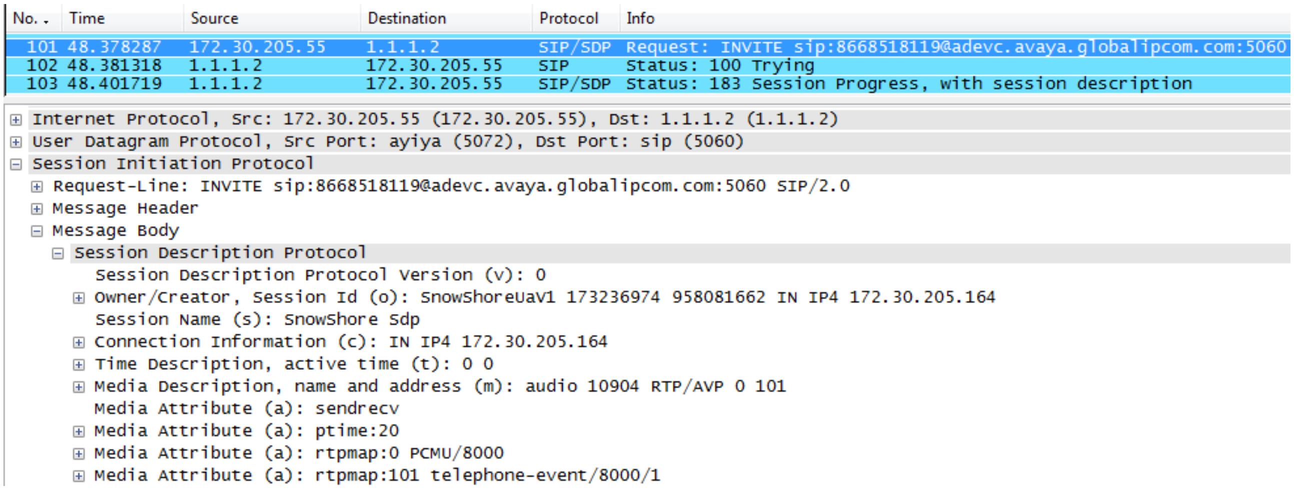


Filter: sip && ip.addr == 1.1.1.2 Expression... Clear Apply

No.	Time	Source	Destination	Protocol	Info
101	48.378287	172.30.205.55	1.1.1.2	SIP/SDP	Request: INVITE sip:8668518119@adevc.avaya.globalipcom.com:5060
102	48.381318	1.1.1.2	172.30.205.55	SIP	Status: 100 Trying
103	48.401719	1.1.1.2	172.30.205.55	SIP/SDP	Status: 183 Session Progress, with session description

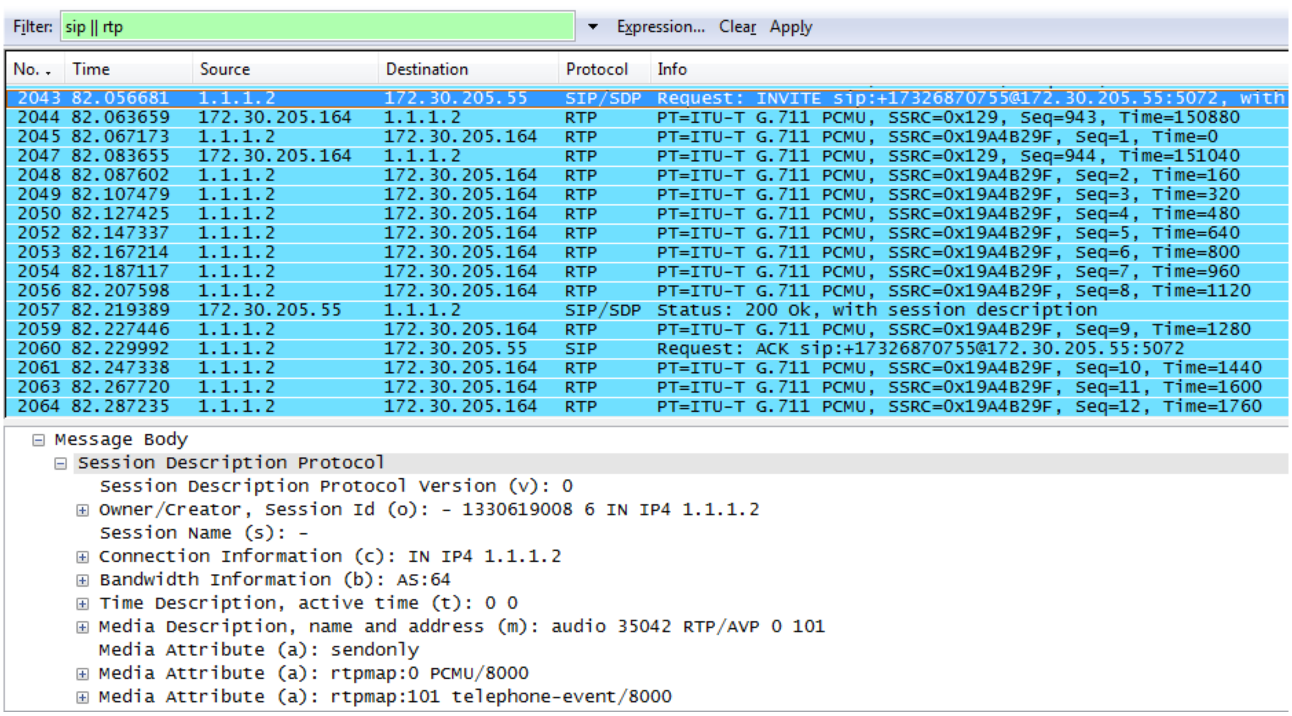
```
User Datagram Protocol, Src Port: ayiya (5072), Dst Port: sip (5060)
Session Initiation Protocol
  Request-Line: INVITE sip:8668518119@adevc.avaya.globalipcom.com:5060 SIP/2.0
  Message Header
    Via: SIP/2.0/UDP 172.30.205.55:5072;branch=z9hG4bKgbsa3m302o40ksk6l2d0.1
    To: <sip:8668518119@adevc.avaya.globalipcom.com>
    From: <sip:+17326870755@199.173.94.88:5060;user=phone>;tag=36024ee5
    Accept: application/sdp
    Accept-Encoding:
    Accept-Language: en
    Allow: ACK, BYE, CANCEL, INVITE, NOTIFY, OPTIONS, PRACK, REFER, SUBSCRIBE
    Allow-Events: refer
    Contact: <sip:+17326870755@172.30.205.55:5072;transport=udp>
    Date: Thu, 01 Mar 2012 15:35:32 GMT
    Max-Forwards: 65
    Supported: replaces
    Call-ID: 55e9c00d5ef6c510@63.78.210.137
    CSeq: 1 INVITE
    Content-Type: application/sdp
    Content-Length: 225
    P-Asserted-Identity: "WIRELESS CALLER" <sip:+17326870755@199.173.94.88;user=phone>
  Message Body
```

The following portion of the same trace highlights the same Verizon IP-IVR INVITE message, but expands the message body to illustrate the SDP Offer. Note that Verizon IP-IVR offers only G.711MU and uses "101" for RFC 2833 telephone events.



9.2.2 Example Call Hold / Resume

As noted earlier, when a call is put on hold at the enterprise site, and the Network Call Redirection parameter is set to yes on the Communication Manager trunk group handling the call, Communication Manager signals a "sendonly" media attribute in SDP. In the portion of the Wireshark trace illustrated below, frame 2043 is highlighted and expanded to show an INVITE sent to Verizon when the call is put on hold. Note the SDP media attribute "sendonly".



In the portion of the same Wireshark trace illustrated below, frame 2057 is highlighted and expanded to show the 200 OK back from Verizon. Note the SDP media attribute "recvonly". As can be observed, RTP (e.g., containing music on hold) flows only from the enterprise to Verizon while the call is on hold.

No.	Time	Source	Destination	Protocol	Info
2043	82.056681	1.1.1.2	172.30.205.55	SIP/SDP	Request: INVITE sip:+17326870755@172.30.205.55:5072, with s
2044	82.063659	172.30.205.164	1.1.1.2	RTP	PT=ITU-T G.711 PCMU, SSRC=0x129, Seq=943, Time=150880
2045	82.067173	1.1.1.2	172.30.205.164	RTP	PT=ITU-T G.711 PCMU, SSRC=0x19A4B29F, Seq=1, Time=0
2047	82.083655	172.30.205.164	1.1.1.2	RTP	PT=ITU-T G.711 PCMU, SSRC=0x129, Seq=944, Time=151040
2048	82.087602	1.1.1.2	172.30.205.164	RTP	PT=ITU-T G.711 PCMU, SSRC=0x19A4B29F, Seq=2, Time=160
2049	82.107479	1.1.1.2	172.30.205.164	RTP	PT=ITU-T G.711 PCMU, SSRC=0x19A4B29F, Seq=3, Time=320
2050	82.127425	1.1.1.2	172.30.205.164	RTP	PT=ITU-T G.711 PCMU, SSRC=0x19A4B29F, Seq=4, Time=480
2052	82.147337	1.1.1.2	172.30.205.164	RTP	PT=ITU-T G.711 PCMU, SSRC=0x19A4B29F, Seq=5, Time=640
2053	82.167214	1.1.1.2	172.30.205.164	RTP	PT=ITU-T G.711 PCMU, SSRC=0x19A4B29F, Seq=6, Time=800
2054	82.187117	1.1.1.2	172.30.205.164	RTP	PT=ITU-T G.711 PCMU, SSRC=0x19A4B29F, Seq=7, Time=960
2056	82.207598	1.1.1.2	172.30.205.164	RTP	PT=ITU-T G.711 PCMU, SSRC=0x19A4B29F, Seq=8, Time=1120
2057	82.219389	172.30.205.55	1.1.1.2	SIP/SDP	Status: 200 Ok, with session description
2059	82.227446	1.1.1.2	172.30.205.164	RTP	PT=ITU-T G.711 PCMU, SSRC=0x19A4B29F, Seq=9, Time=1280
2060	82.229992	1.1.1.2	172.30.205.55	SIP	Request: ACK sip:+17326870755@172.30.205.55:5072
2061	82.247338	1.1.1.2	172.30.205.164	RTP	PT=ITU-T G.711 PCMU, SSRC=0x19A4B29F, Seq=10, Time=1440
2063	82.267720	1.1.1.2	172.30.205.164	RTP	PT=ITU-T G.711 PCMU, SSRC=0x19A4B29F, Seq=11, Time=1600
2064	82.287235	1.1.1.2	172.30.205.164	RTP	PT=ITU-T G.711 PCMU, SSRC=0x19A4B29F, Seq=12, Time=1760

```
⊟ Message Body
  ⊟ Session Description Protocol
      Session Description Protocol Version (v): 0
    ⊞ Owner/Creator, Session Id (o): SnowShoreUav1 3539607676 3539607679 IN IP4 172.30.205.164
      Session Name (s): SnowShore Sdp
    ⊞ Connection Information (c): IN IP4 172.30.205.164
    ⊞ Time Description, active time (t): 0 0
    ⊞ Media Description, name and address (m): audio 10912 RTP/AVP 0 101
      Media Attribute (a): recvonly
    ⊞ Media Attribute (a): ptime:20
    ⊞ Media Attribute (a): rtpmap:0 PCMU/8000
    ⊞ Media Attribute (a): rtpmap:101 telephone-event/8000/1
```

In the portion of the same Wireshark trace illustrated below, frame 3729 is highlighted and expanded to show an INVITE sent to Verizon when the call is resumed (un-held) by the Communication Manager user. The absence of a "sendonly" attribute implies a "sendrecv" condition. Although not expanded, Verizon responds with a "sendrecv" media attribute in the 200 OK with SDP in frame 3739. As can be observed, RTP media resumes bi-directionally.

No.	Time	Source	Destination	Protocol	Info
3729	114.172764	1.1.1.2	172.30.205.55	SIP/SDP	Request: INVITE sip:+17326870755@172.30.205.55:5072, with se
3730	114.186683	1.1.1.2	172.30.205.164	RTP	PT=ITU-T G.711 PCMU, SSRC=0x19A4B29F, Seq=1607, Time=256960
3731	114.206608	1.1.1.2	172.30.205.164	RTP	PT=ITU-T G.711 PCMU, SSRC=0x19A4B29F, Seq=1608, Time=257120
3732	114.226456	1.1.1.2	172.30.205.164	RTP	PT=ITU-T G.711 PCMU, SSRC=0x19A4B29F, Seq=1609, Time=257280
3733	114.246436	1.1.1.2	172.30.205.164	RTP	PT=ITU-T G.711 PCMU, SSRC=0x19A4B29F, Seq=1610, Time=257440
3734	114.266360	1.1.1.2	172.30.205.164	RTP	PT=ITU-T G.711 PCMU, SSRC=0x19A4B29F, Seq=1611, Time=257600
3735	114.286764	1.1.1.2	172.30.205.164	RTP	PT=ITU-T G.711 PCMU, SSRC=0x19A4B29F, Seq=1612, Time=257760
3736	114.306693	1.1.1.2	172.30.205.164	RTP	PT=ITU-T G.711 PCMU, SSRC=0x19A4B29F, Seq=1613, Time=257920
3737	114.322118	172.30.205.164	1.1.1.2	RTP	PT=ITU-T G.711 PCMU, SSRC=0x129, Seq=950, Time=152000
3738	114.326504	1.1.1.2	172.30.205.164	RTP	PT=ITU-T G.711 PCMU, SSRC=0x19A4B29F, Seq=1614, Time=258080
3739	114.336382	172.30.205.55	1.1.1.2	SIP/SDP	Status: 200 Ok, with session description
3740	114.340959	172.30.205.164	1.1.1.2	RTP	PT=ITU-T G.711 PCMU, SSRC=0x129, Seq=951, Time=152160
3741	114.346409	1.1.1.2	172.30.205.164	RTP	PT=ITU-T G.711 PCMU, SSRC=0x19A4B29F, Seq=1615, Time=258240
3742	114.347483	1.1.1.2	172.30.205.55	SIP	Request: ACK sip:+17326870755@172.30.205.55:5072
3743	114.361052	172.30.205.164	1.1.1.2	RTP	PT=ITU-T G.711 PCMU, SSRC=0x129, Seq=952, Time=152320
3744	114.366431	1.1.1.2	172.30.205.164	RTP	PT=ITU-T G.711 PCMU, SSRC=0x19A4B29F, Seq=1616, Time=258400
3745	114.381028	172.30.205.164	1.1.1.2	RTP	PT=ITU-T G.711 PCMU, SSRC=0x129, Seq=953, Time=152480
3746	114.386290	1.1.1.2	172.30.205.164	RTP	PT=ITU-T G.711 PCMU, SSRC=0x19A4B29F, Seq=1617, Time=258560

```
⊟ Message Body
  ⊟ Session Description Protocol
      Session Description Protocol Version (v): 0
    ⊞ Owner/Creator, Session Id (o): - 1330619008 7 IN IP4 1.1.1.2
      Session Name (s): -
    ⊞ Connection Information (c): IN IP4 1.1.1.2
    ⊞ Bandwidth Information (b): AS:64
    ⊞ Time Description, active time (t): 0 0
    ⊞ Media Description, name and address (m): audio 35042 RTP/AVP 0 101
    ⊞ Media Attribute (a): rtpmap:0 PCMU/8000
    ⊞ Media Attribute (a): rtpmap:101 telephone-event/8000
```

9.2.3 Example Incoming Calls Answered by Agents

In the Wireshark example below, the PSTN caller 732-290-9267 dialed the IP-IVR "published number" 866-616-4284, and Verizon sends the CPE the corresponding IP-IVR "outdial number"

866-850-8170 in the INVITE, as shown in frame 64. This outdial number was associated with VDN 3660 associated with vector 60 which queues the call to split 60. In this case, a one-X® Agent in auto-answer mode is available to take the call immediately. After two seconds of ringback programmed in vector 60, the call is delivered to the agent. The call is answered (frame 373), and Communication Manager begins the process of "shuffling to ip-direct" from the one-X® Agent to the inside interface of the SBC. The SIP messaging corresponding to the "shuffling" occurring on the inside interface can be observed on the outside trace below in frames 395, 412, and 414.

Filter: sip && ip.addr == 172.30.205.55 Expression... Clear Apply

No.	Time	Source	Destination	Protocol	Info
64	28.755361	172.30.205.55	1.1.1.2	SIP/SDP	Request: INVITE sip:8668508170@adevc.avaya.globalipcom.com:5060, with sessi
65	28.759613	1.1.1.2	172.30.205.55	SIP	Status: 100 Trying
66	28.815990	1.1.1.2	172.30.205.55	SIP/SDP	Status: 183 Session Progress, with session description
275	30.827326	1.1.1.2	172.30.205.55	SIP/SDP	Status: 183 Session Progress, with session description
373	31.782527	1.1.1.2	172.30.205.55	SIP/SDP	Status: 200 OK, with session description
389	31.933912	172.30.205.55	1.1.1.2	SIP	Request: ACK sip:8666164254@1.1.1.2:5060;transport=udp
395	31.984708	1.1.1.2	172.30.205.55	SIP	Request: INVITE sip:+17322909267@172.30.205.55:5072
412	32.135367	172.30.205.55	1.1.1.2	SIP/SDP	Status: 200 Ok, with session description
414	32.149313	1.1.1.2	172.30.205.55	SIP/SDP	Request: ACK sip:+17322909267@172.30.205.55:5072, with session description

The following Wireshark illustrates an alternative scenario where no agent is immediately available to take the call. In frame 281, observe the 182 Queued message. In the sample configuration, the caller would hear a recurring announcement after the 200 OK (frame 283) is sent to Verizon when the announcement step in vector 60 answers the call. When an agent ultimately becomes available, Communication Manager delivers the call to the agent, and the "shuffling to ip-direct" would occur if appropriate for the answering agent. In the trace shown below, the answering agent was a one-X® Agent, and the SIP messaging corresponding to the "shuffling to ip-direct" occurring on the inside interface can be observed in the INVITE (frame 2506), 200 OK (frame 2520), and ACK (frame 2523) shown below. From the Time stamps, it can be ob served that the caller was listening to the enterprise announcement for a little more than 20 seconds before the agent became available and answered the call.

Filter: sip && ip.addr == 172.30.205.55 Expression... Clear Apply

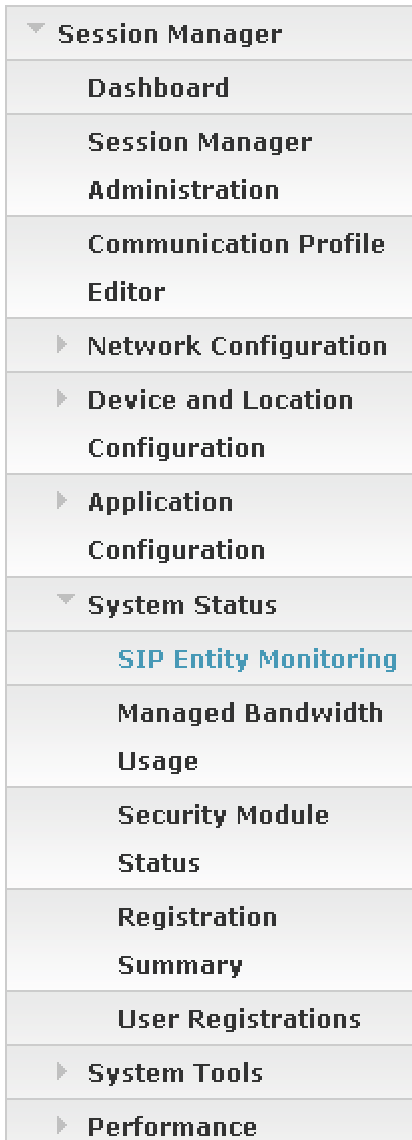
No.	Time	Source	Destination	Protocol	Info
70	34.991978	172.30.205.55	1.1.1.2	SIP/SDP	Request: INVITE sip:8668508170@adevc.avaya.globalipcom.com:5060, with session
71	34.995210	1.1.1.2	172.30.205.55	SIP	Status: 100 Trying
72	35.052280	1.1.1.2	172.30.205.55	SIP/SDP	Status: 183 Session Progress, with session description
281	37.070974	1.1.1.2	172.30.205.55	SIP/SDP	Status: 182 Queued, avaya-cm-data=000100AB015600AB, with session description
282	37.073641	1.1.1.2	172.30.205.55	SIP/SDP	Status: 183 Session Progress, with session description
283	37.076290	1.1.1.2	172.30.205.55	SIP/SDP	Status: 200 OK, with session description
298	37.214400	172.30.205.55	1.1.1.2	SIP	Request: ACK sip:8666164254@1.1.1.2:5060;transport=udp
2506	58.969953	1.1.1.2	172.30.205.55	SIP	Request: INVITE sip:+17326870755@172.30.205.55:5072
2520	59.101722	172.30.205.55	1.1.1.2	SIP/SDP	Status: 200 Ok, with session description
2523	59.113930	1.1.1.2	172.30.205.55	SIP/SDP	Request: ACK sip:+17326870755@172.30.205.55:5072, with session description

9.3. System Manager and 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-2", corresponding to the entity link to the inside or private interface of the Avaya SBC. Under normal operating conditions, the **Link Status** should be "Up" as shown in the example screen below.

Home / Elements / Session Manager / System Status / SIP Entity Monitoring

Help ?

SIP Entity, Entity Link Connection Status

This page displays detailed connection status for all entity links from all Session Manager instances to a single SIP entity.

All Entity Links to SIP Entity: Avaya-SBCE-2

Summary View

1 Item | Refresh — Filter: Enable

Details	Session Manager Name	SIP Entity Resolved IP	Port	Proto.	Conn. Status	Reason Code	Link Status
▶ Show	ASM-62	10.80.140.200	5060	TCP	Up	200 OK	Up

If "Show" in the Details column is selected, additional information can be observed. In the screen below, note that the "Last Response Latency" was 130 msec for the last OPTIONS 200 OK response. Recall that the Avaya SBCE sends the OPTIONS received from Session Manager to Verizon. Verizon sends the 200 OK to the SBC, and the SBC sends the 200 OK to Session Manager, accounting for the greater latency compared with OPTIONS sent to other local entities.

SIP Entity, Entity Link Connection Status

This page displays detailed connection status for all entity links from all Session Manager instances to a single SIP entity.

All Entity Links to SIP Entity: Avaya-SBCE-2

Summary View

1 Item | Refresh — Filter: Enable

Details	Session Manager Name	SIP Entity Resolved IP	Port	Proto.	Conn. Status	Reason Code	Link Status
▼ Hide	ASM-62	10.80.140.200	5060	TCP	Up	200 OK	Up

Time Last Down	Time Last Up	Last Message Sent	Last Message Response	Last Response Latency (ms)
Jan 26, 2012 8:24:52 AM MST	Jan 26, 2012 9:39:59 AM MST	Jan 30, 2012 3:27:48 PM MST		130

Return to the list of monitored entities, and select another entity of interest, such as "CM-Evolution-procr-5063". Under normal operating conditions, the **Link Status** should be "Up" as shown in the example screen below. Note the use of port 5063.

SIP Entity, Entity Link Connection Status

This page displays detailed connection status for all entity links from all Session Manager instances to a single SIP entity.

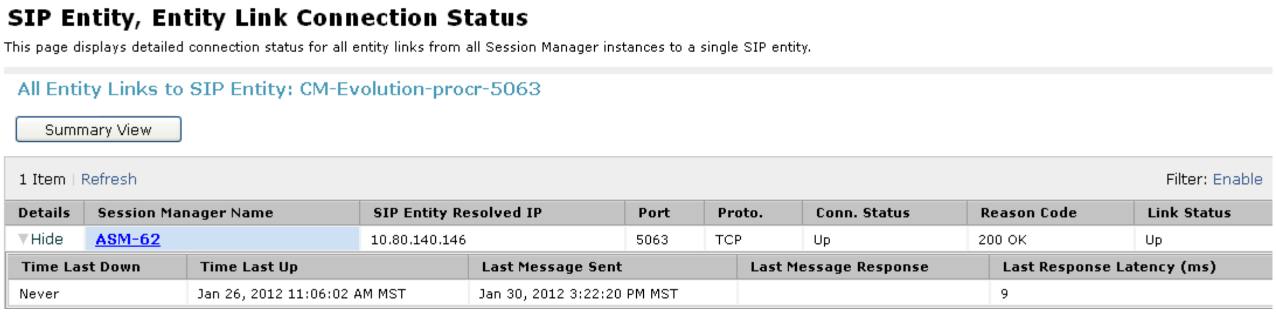
All Entity Links to SIP Entity: CM-Evolution-procr-5063

Summary View

1 Item | Refresh — Filter: Enable

Details	Session Manager Name	SIP Entity Resolved IP	Port	Proto.	Conn. Status	Reason Code	Link Status
▶ Show	ASM-62	10.80.140.146	5063	TCP	Up	200 OK	Up

In the following screen, "Show" under Details was selected to view additional information. Note the Last Response Latency is only 9 msec in this case, owing to the fact that Communication Manager responds to the OPTIONS without proxying the OPTIONS to a next hop, as did the Avaya SBCE to Verizon.



SIP Entity, Entity Link Connection Status

This page displays detailed connection status for all entity links from all Session Manager instances to a single SIP entity.

All Entity Links to SIP Entity: CM-Evolution-procr-5063

Summary View

1 Item | Refresh   Filter: Enable

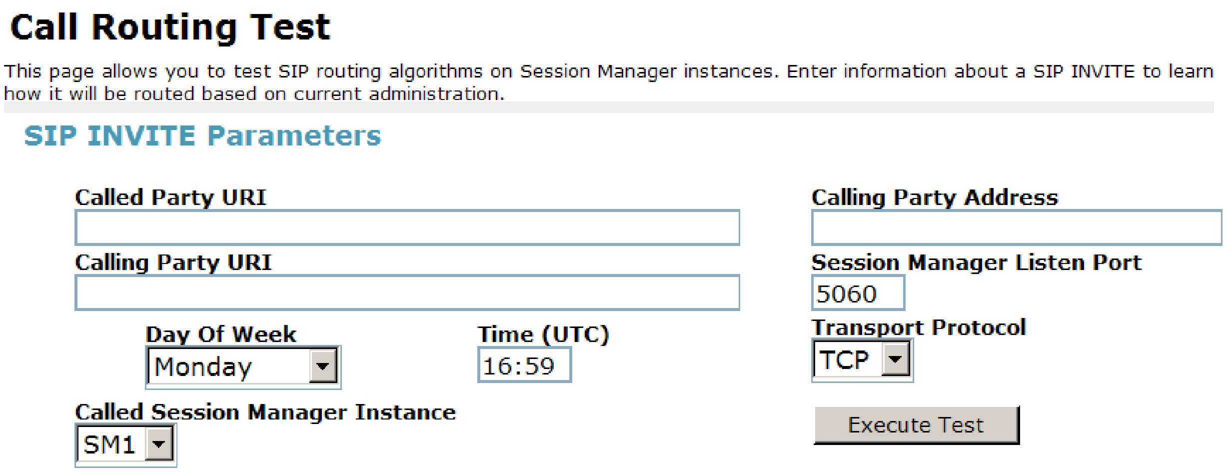
Details	Session Manager Name	SIP Entity Resolved IP	Port	Proto.	Conn. Status	Reason Code	Link Status
Hide	ASM-62	10.80.140.146	5063	TCP	Up	200 OK	Up

Time Last Down	Time Last Up	Last Message Sent	Last Message Response	Last Response Latency (ms)
Never	Jan 26, 2012 11:06:02 AM MST	Jan 30, 2012 3:22:20 PM MST		9

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.

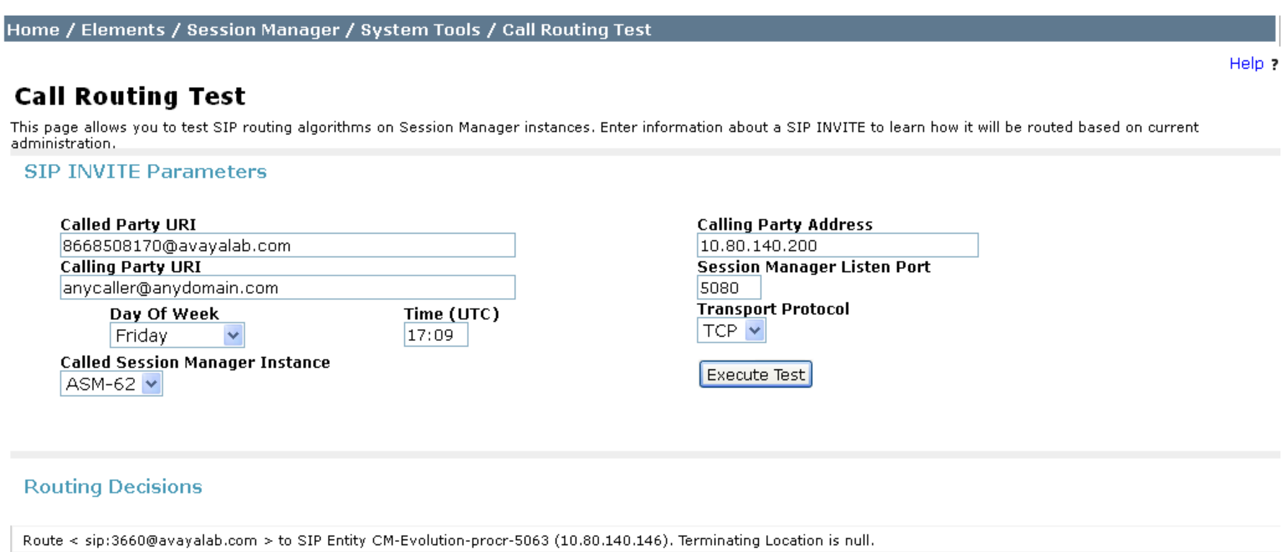
A screen such as the following is displayed.



Populate the fields for the call parameters of interest and click **Execute Test**.

For example, the following shows a call routing test for an inbound IP-IVR call from the PSTN to the enterprise via the Avaya SBCE (10.80.140.200). Under **Routing Decisions**, observe that the call will route to Communication Manager using the SIP entity named "CM-Evolution-procr-5063". The digits are manipulated such that the Verizon IP-IVR "outdial number" (i.e., 866-850-8170) is converted to a Communication Manager extension (i.e., VDN 3660) by the adapter assigned to the Communication Manager entity. Scroll down to inspect the details of the **Routing Decision Process** if desired (not shown).

The **Session Manager Listen Port** needed to be set to a port other than 5060 for this call routing test to produce the result shown below, but in fact the SBC and Session Manager communicate using port 5060. In Session Manager 6.0, this field could be set to 5060, the port from which the INVITE arrives. See **Section 2.2**.



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 Contact Center IP-IVR service.

Please note that the sample configurations shown in these Application Notes are intended to provide configuration guidance to supplement other Avaya product documentation.

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.

11. Additional References

11.1. Avaya

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

[1] *Implementing Avaya Aura® Communication Manager*, Doc ID 03-603558, Release 6.2
[2] *Administering Avaya Aura® Communication Manager*, Doc ID 03-300509, Release 6.2
[3] *Administering Avaya Aura® Session Manager*, Doc ID 03-603324, Release 6.2
[4] *Implementing 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*, March 2012

Avaya Application Notes, including the following, are also available at http://support.avaya.com

The following reference is a companion to these Application Notes illustrating interoperability with the Verizon IPCC IP Toll Free VoIP Inbound Service.

[VZ-IPTF] – 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 Toll Free VoIP Inbound – Issue 1.0.

The following Application Notes cover Communication Manager 6.0 with Verizon IP Contact Center using the Avaya Aura® SBC.

[JRR-VZIPCC] Application Notes for Avaya Aura™ Communication Manager 6.0, Avaya Aura™ Session Manager 6.0, and Avaya Aura SBC with Verizon Business IP Contact Centers Services Suite – Issue 1.1
http://support.avaya.com/css/P8/documents/100113361

The following Application Notes cover Communication Manager 6.0 with Verizon IP Contact Center using the Acme Packet SBC.

[JRR-VZIPCCAcme] Application Notes for Avaya Aura™ Communication Manager 6.0, Avaya Aura™ Session Manager 6.0, and Acme Packet Net-Net SBC with Verizon Business IP Contact Centers Services Suite – Issue 1.2
http://support.avaya.com/css/P8/documents/100113497

The following Application Notes cover Communication Manager 5.2 with Verizon IP Contact Center.

[JF-VZIPCC] Application Notes for Avaya Aura™ Communication Manager 5.2, Avaya Aura™ Session Manager 1.1, and Acme Packet 3800 Net-Net Session Director with Verizon Business IP Contact Centers Services Suite – Issue 1.2
https://devconnect.avaya.com/public/download/dyn/AvayaSM_VzBIPCC.pdf

11.2. Verizon Business

Information in the following documents was also used for these Application Notes:

- *Verizon Business IPCC Interoperability Test Plan, Revision 1.7, Aug 27, 2009*
- *Verizon Business IP Contact Center Trunk Interface Network Interface Specification, Document Version 2.2.1.9, Aug 25, 2009*
- *Test Suite for CPE IP Trunking Interoperability, VIT.2011.91202.TPL.001, V1.1, 2/1/2012 (this revised test document includes both Verizon IP Trunking and Verizon IPCC Services).*
- *Additional information regarding Verizon Business IPCC Services suite offer can be found at http://www.verizonbusiness.com/products/contactcenter/ip/*