Avaya Solution & Interoperability Test Lab

Application Notes for Avaya Aura® Communication Manager 6.0.1, Avaya Aura® Session Manager 6.1, and Avaya Session Border Controller for Enterprise with Verizon Business IP Contact Center VoIP Inbound – Issue 1.1

Abstract

These Application Notes describe a sample configuration of Avaya Aura® Communication Manager 6.0.1, Avaya Aura® Session Manager 6.1, and Avaya Session Border Controller for Enterprise with Verizon Business IP Contact Center (IPCC) IP Toll Free VoIP Inbound 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 Toll Free VoIP Inbound. This service provides toll free inbound calling via standards-based SIP trunks as well as re-routing of inbound toll free calls to alternate destinations based upon SIP messages (i.e., REFER) generated by Avaya Aura® Communication Manager. The Network Call Redirection (NCR) and SIP User-to-User Information (UUI) features can be utilized together to transmit UUI within SIP signaling messages to alternate destinations via the Verizon network. These Application Notes update previously published Application Notes with newer versions of Avaya Aura® Communication Manager and Avaya Aura® Session Manager, and present an example configuration for the Avaya Session Border Controller for Enterprise.

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 Dedicated Internet Access (IDA) circuit connection to the production Verizon Business IPCC Services.

Table of Contents

1. Introduction

These Application Notes describe a sample configuration of Avaya Aura® Communication Manager 6.0.1, Avaya Aura® Session Manager 6.1, 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 cover IP Toll Free VoIP Inbound using IDA access. Verizon IP Toll Free VoIP Inbound service provides toll free inbound calling via standards-based SIP trunks as well as re-routing of inbound toll free calls to alternate destinations based upon SIP messages (i.e., REFER) generated by Avaya Aura® Communication Manager. The Network Call Redirection (NCR) and SIP User-to-User Information (UUI) features can be utilized together to transmit UUI within SIP signaling messages to alternate destinations via the Verizon network.

In the sample configuration, an Avaya Session Border Controller for Enterprise (ASBCE) is used as the 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.

The Verizon Business IP Toll Free VoIP Inbound service provides inbound toll-free service via standards-based SIP trunks. Using SIP Network Call Redirection (NCR), trunk-to-trunk connections of certain inbound calls at Avaya Aura® Communication Manager can be avoided by requesting that the Verizon network transfer the inbound caller to an alternate destination. In addition, the SIP User-to-User Information (UUI) feature can be utilized with the SIP NCR feature to transmit UUI within SIP signaling messages to alternate destinations. This capability allows the service to transmit a limited amount of call-related data between call centers to enhance customer service and increase call center efficiency. Examples of UUI data might include a customer account number obtained during a database query or the best service routing data exchanged between sites.

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 VoIP Inbound Service. This allowed PSTN users to dial toll-free numbers assigned by Verizon. The toll-free numbers 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 Communication Manager ACD functions as well as Verizon IPCC Services such as network call redirection to PSTN destinations, and network call redirection with UUI.

The test approach was manual testing of inbound and referred calls using the Verizon IPCC Services on a production Verizon IDA access circuit, as shown in **Figure 1**.

The main objectives were to verify the following features and functionality:

- Inbound Verizon toll-free calls to Communication Manager telephones and VDNs/Vectors
- Inbound private toll-free calls (e.g., PSTN caller uses *67 followed by the toll-free number)
- Inbound Verizon toll-free calls redirected using Communication Manager SIP NCR (via SIP REFER/Refer-To) to PSTN alternate destinations
- Inbound Verizon IP toll-free calls redirected using Communication Manager SIP NCR with UUI (via SIP REFER/Refer-To with UUI) to a SIP-connected destination
- Inbound toll-free voice calls can use G.711MU or G.729A codecs.
- Inbound toll-free voice calls can use DTMF transmission using RFC 2833
- Inbound toll-free voice calls via the Verizon IP-IVR
- Inbound toll-free voice calls received via the Verizon IP-IVR and redirected using a vector

Testing was successful. Test observations or limitations are described in **Section 2.2.**

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].

- Incoming calls from the PSTN were routed to the toll-free numbers assigned by Verizon Business to the Avaya location. Configuration was varied such that these incoming toll-free calls were directed to Communication Manager telephone extensions and Communication Manager VDNs containing call routing logic to exercise SIP Network Call Redirection.
- Proper disconnect when either party hangs up an active call.
- Proper disconnect when the PSTN caller abandons (i.e., hangs up) a toll free call before the call has been answered.
- Proper SIP 486 response and busy tone heard by the caller when a PSTN user calls a toll-free 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 Toll Free 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 three minutes of ring no answer conditions, returning busy tone to the PSTN caller.

- Privacy requests for inbound toll-free 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 toll-free call can be successfully completed while withholding presentation of the PSTN caller id to user displays. (When the caller requests privacy, Verizon IP Toll Free sends the caller ID in the P-Asserted-Identity header and includes “Privacy: id” which is honored by Communication Manager).
- Inbound toll-free 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 of “sendonly”. The Verizon 200 OK to this re-INVITE will include the 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, the bi-directional media path resumes. Although it would be unexpected in a contact center, calls on hold for longer than the session refresh interval were tested, and such calls could be resumed after the session refresh.
- Transfer of toll-free calls between Communication Manager users.
- Incoming voice calls using the G.729a and G.711 ULAW codecs and proper protocol procedures related to media.
- DTMF transmission using RFC2833. For inbound toll-free 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.
- Inbound toll-free calls from the Verizon IP-IVR answered at a station or a vector.
- Inbound toll-free calls from the Verizon IP-IVR answered at a station or a vector and then transferred using a SIP REFER message.

2.2. Test Results

The interoperability compliance testing of the sample configuration was completed with successful results. 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 headers 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.
- 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 7.3.4** to illustrate how headers such as P-Location that are not required by Verizon may be removed by the Avaya SBC for Enterprise.

- **SIP REFER/TRANSFER OFF-NET:** If on Communication Manager the public-unkonwn numbering table is being used to map local extensions to DIDs and a transfer to the PSTN is attempted using a SIP REFER, the Contact header will incorrectly contain the local extension instead of the DID. This may cause the service provider to send a 603 DECLINE instead of a 202 ACCEPT on the REFER. This will allow the call to be transferred but will not release media resources for the transfer and the call will stay resident on the system. The recommended work-around is to use a Sigma Script as detailed in **Section 7.3.4**. Internal tracking issue defsw121215 has been created for this issue.

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 with a secure VPN used for SIP signaling and the internet T1 used for RTP. 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 Avaya SBC-E receives traffic from Verizon on port 5060 and sends traffic to Verizon using destination port 5060. UDP is the transport protocol.

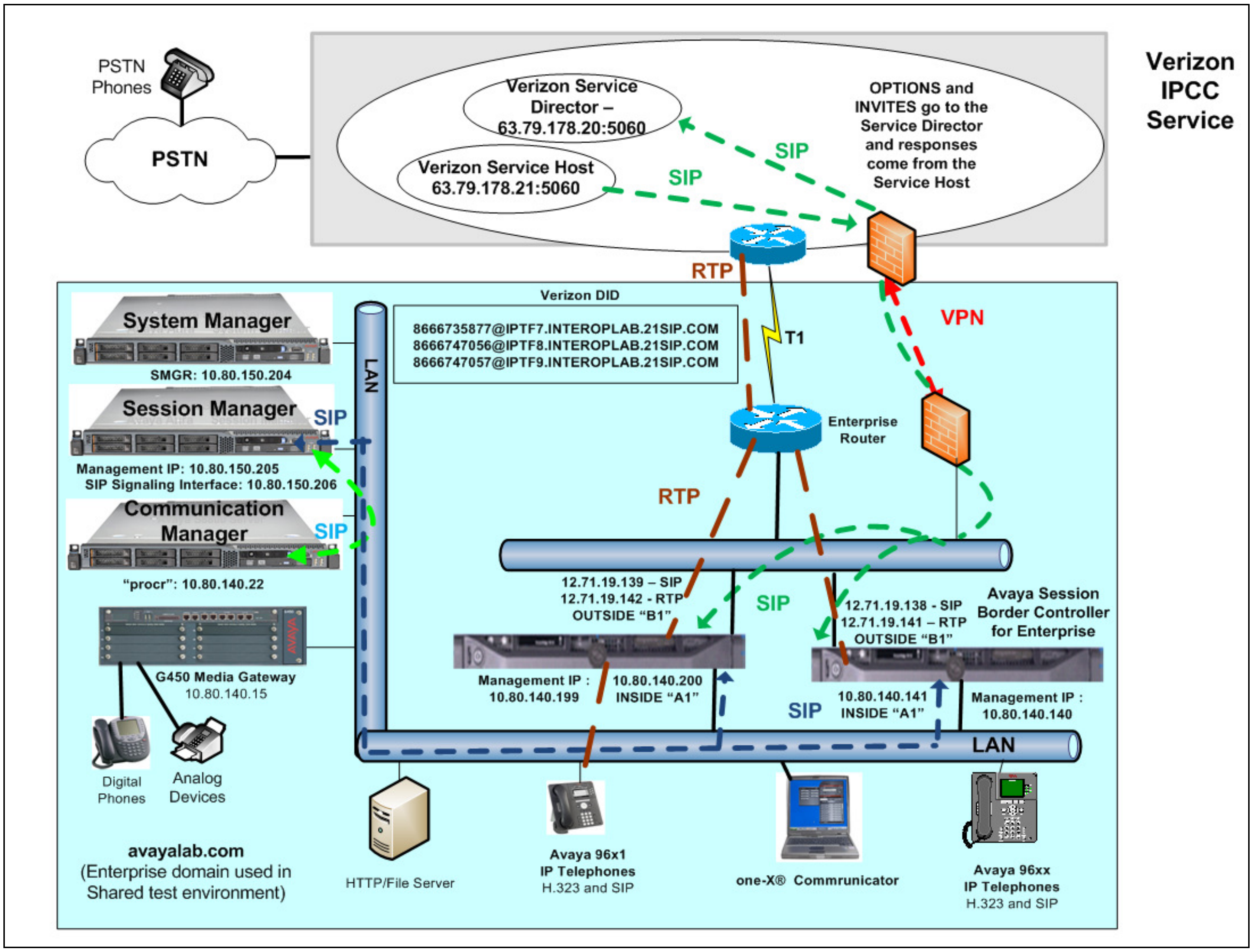


Figure 1: Avaya Interoperability Test Lab Configuration

The Verizon IP toll-free numbers were mapped by Session Manager or Communication Manager to various Communication Manager extensions. The extension mappings were varied during the testing to allow inbound toll-free 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.

For efficiency, the Avaya CPE environment utilizing Session Manager Release 6.1 and Communication Manager Release 6.0.1 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 the domain "avayalab.com" at the enterprise. As such, Session Manager or the ASBCE were 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 content and manipulations for IP toll-free calls in the sample configuration:

- Verizon sends the following in the initial INVITE to the CPE:
    - The CPE domain depending on the DID in the Request URI.
        - *8666735877@IPTF7.INTEROPLAB.21SIP.COM*
        - *8666747056@IPTF8.INTEROPLAB.21SIP.COM*
        - *8666747057@IPTF9.INTEROPLAB.21SIP.COM*
    - The Verizon gateway IP address in the From header.
    - The assigned DID and CPE domain in the To 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 containing ***avayalab.com***, to match the shared Avaya SIL test environment.
    - The host portion of the From header also containing ***avayalab.com***
    - The host portion of the To header also containing ***avayalab.com***
    - Sends the packet to Session Manager using destination port 5060 via TCP
- Session Manager to Communication Manager:
    - The Request URI containing ***avayalab.com***, to match the shared Avaya SIL test environment.
    - Session Manager sends to Communication Manager using destination port 5060 via TCP to allow Communication Manager to distinguish Verizon IP Toll Free traffic from other traffic arriving from the same instance of Session Manager.
    - Communication Manager uses the ***incoming call handling treatment trunk group x*** form to translate the inbound toll-free number to a Communication Manager extension or vector and then adapts the number as configured.

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.

3.1. History Info and Diversion Headers

The Verizon Business IPCC Services suite does not support SIP History Info headers or Diversion headers. Therefore, Communication Manager was provisioned not to send History Info headers or Diversion headers.

4. Equipment and Software Validated

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

Equipment	Software
Avaya Aura® Communication Manager running on an HP Common Server	Avaya Aura® Communication Manager Release 6.0.1
Avaya Aura® System Manager running on an HP Common Server	Avaya Aura® System Manager 6.1
Avaya Aura® Session Manager running on an HP Common Server	Avaya Aura® Session Manager 6.1
Avaya G650 Gateway	3.1.20.1
Avaya one-X® Communicator (H.323)	6.1.2.06_SP2-35739
Avaya 96x1-Series IP Telephones (H.323)	96x1-IPT-H323-R6_0-090610
Avaya 96x1-Series IP Telephones (SIP)	96x1-IPT-SIP-R6_0_3-120511
Avaya 2400-Series Digital Telephones	N/A
Avaya Session Border Controller for Enterprise	Release 4.0.5 Q09

Table 1: Equipment and Software Used in the Sample Configuration

5. Configure Communication Manager Release 6.0.1

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 with 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 the SIP REFER method 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. In the sample configuration, vectoring is used to refer calls to alternate destinations using SIP NCR. Vector Variables are used to include User-User Information (UUI) with the referred calls.

```
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 Toll Free.

```
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. System Features

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

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

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

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

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

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

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

SCCAN PARAMETERS
   Enable Enbloc Dialing without ARS FAC? n

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

5.3. Node Names

Node names are mappings of names to IP Addresses that can be used in various screens. The following abridged **change node-names ip** output shows relevant node-names in the sample configuration. As shown in bold, the node name for Session Manager is ***ASM*** with IP Address ***10.80.150.206***. The node name (***procr***) and IP Address (***10.80.140.22***) for the Communication Manger Processor Ethernet 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.

```
change node-names ip                                              Page   1 of   2
                                  IP NODE NAMES
    Name              IP Address
ASM                 10.80.150.206
Gateway1            10.80.140.1
default             0.0.0.0
procr               10.80.140.22
procr6              ::

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: 10.80.140.22
           Subnet Mask: /24
```

5.5. IP Codec Sets

Use the **change ip-codec-set** command to define a list of codecs to use for calls between the enterprise and the service provider. For the compliance test **ip-codec-set *1*** was used for this purpose. In the example below, ***G.729***, ***G.711MU* and *G.711A*** were entered in the **Audio Codec** column of the table. Default values can be used for all other fields.

```
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.729             n         2        20
 2: G.711MU           n         2        20
 3: G.711A            n         2        20
 4:
```

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

```
change ip-codec-set 1                                          Page   2 of   2
                          IP Codec Set
                              Allow Direct-IP Multimedia? n

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

5.6. IP Network Region

Create a separate IP network region for the service provider trunk. This allows for separate codecs or quality of service settings to be used (if necessary) for calls between the enterprise and the service provider versus calls within the enterprise or elsewhere. For the compliance test, **IP-network-region *5*** was chosen for the service provider trunk. IP network region 1 is the default IP network region and encompasses the rest of the enterprise. Use the **change ip-network-region *5*** command to configure region 5 with the following parameters:

- Set the **Location** field (optional) to match the enterprise location for this SIP trunk.

- Set the **Authoritative Domain** field to match the SIP domain of the enterprise. In this configuration, the domain name is ***avayalab.com***. This name appears in the “From” header of SIP messages originating from this IP region.
- Enter a descriptive name in the **Name** field.
- Enable **IP-IP Direct Audio** (shuffling) to allow audio traffic to be sent directly between IP endpoints without using media resources in the Avaya Media Gateway. To enable shuffling, set both **Intra-region** and **Inter-region IP-IP Direct Audio** fields to ***yes*.** This is the default setting. Shuffling can be further restricted at the trunk level on the Signaling Group form.
- Set the **Codec Set** field to the IP codec set defined in **Section 5.5**.
- Default values can be used for all other fields.

```
change ip-network-region 5                                      Page   1 of  20
                               IP NETWORK REGION
  Region: 5
Location:  to Verizon       Authoritative Domain: avayalab.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
```

On **Page 4**, define the IP codec set to be used for traffic between region 5 and region 1 (the rest of the enterprise). Enter the desired IP codec set in the **codec set** column of the row with destination region (**dst rgn**) 1. Default values may be used for all other fields. The example below shows the settings used for the compliance test. It indicates that codec set 1 will be used for calls between region 5 (the service provider region) and region 1 (the rest of the enterprise).

```
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    1      y    NoLimit                                            n       t
 2
 3
 4
```

5.7. Signaling Group

Use the **add signaling-group** command to create a signaling group between Communication Manager and Session Manager for use by the service provider trunk. This signaling group is used for inbound and outbound calls between the service provider and the enterprise. For the compliance test, signaling group 5 was used for this purpose and was configured using the parameters highlighted below.

- Set the **Group Type** field to ***sip***.
- Set the **IMS Enabled** field to ***n***. This specifies Communication Manager will serve as an Evolution Server for Session Manager.
- Set the **Transport Method** to the recommended default value of ***tls*** (Transport Layer Security). Set the **Near-end Listen Port** and **Far-end Listen Port** to a valid unused port. For compliance testing the **Near-end Listen Port** and **Far-end Listen Port** were set to ***5060*** and ***tcp*** was used so traces could be taken.
- Set the **Peer Detection Enabled** field to ***y***. The **Peer Server** field will initially be set to ***Others*** and cannot be changed via administration. The Peer Server field will automatically change to ***SM*** once Communication Manager has detected a Session Manager peer.
- Set the **Near-end Node Name** to ***procr***. This node name maps to the IP address of Communication Manager as defined in **Section 5.3**.
- Set the **Far-end Node Name** to *ASM*. This node name maps to the IP address of Session Manager as defined in **Section 5.3**.
- Set the **Far-end Network Region** to the IP network region defined for the service provider in **Section 5.6**
- Set the **Far-end Domain** to the domain of the enterprise.
  Set **Direct IP-IP Audio Connections** to ***y***. This field will enable media shuffling on the SIP trunk.
- Set the **DTMF over IP** field to ***rtp-payload***. This value sends the DTMF digits in the RTP event packets.
- Default values may be used for all other fields.

```
change signaling-group 5                                        Page   1 of   1
                                SIGNALING GROUP

 Group Number: 5              Group Type: sip
  IMS Enabled? n        Transport Method: tcp
       Q-SIP? n                                                 SIP Enabled LSP? 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: ASM
 Near-end Listen Port: 5060                Far-end Listen Port: 5060
                                        Far-end Network Region: 5

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? y
H.323 Station Outgoing Direct Media? n              Alternate Route Timer(sec): 12
```

5.8. SIP Trunk Groups

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

NOTE: For Verizon Business customers utilizing either Verizon **IP Contact Center** or **IP-IVR** service offers, at least one **Elite Agent license** is **required** to support the ability to utilize the Network Call Redirection capabilities of those services with Communication Manager. 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. Additional details on how to configure Network Call Redirection in Communication Manager can be found within the supporting text and figures contained within this section.

Use the **add trunk-group** command to create a trunk group for the signaling group created in **Section 5.7**. For the compliance test**, trunk group 5** was configured using the parameters highlighted below.

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

```
change trunk-group 5                                              Page   1 of  21
                                TRUNK GROUP

Group Number: 5                  Group Type: sip           CDR Reports: y
  Group Name: OUTSIDE CALL              COR: 1        TN: 1        TAC: *105
   Direction: two-way       Outgoing Display? n
 Dial Access? n                                 Night Service:
Queue Length: 0
Service Type: public-ntwrk          Auth Code? n
                                             Member Assignment Method: auto
                                                      Signaling Group: 5
                                                    Number of Members: 255
```

On **Page 2**, verify that the **Preferred Minimum Session Refresh Interval** is set to a value acceptable to the service provider. This value defines the interval that re-INVITEs must be sent to keep the active session alive. For the compliance test, the value of ***900*** seconds was used.

```
change trunk-group 5                                             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
```

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

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

```
change trunk-group 5                                             Page   3 of  21
TRUNK FEATURES
          ACA Assignment? n            Measured: none
                                                         Maintenance Tests? y
                     Numbering Format: public
                                                UUI Treatment: service-provider

                                                 Replace Restricted Numbers? y
                                                Replace Unavailable Numbers? y

 Show ANSWERED BY on Display? y
```

The following shows **Page 4** for **trunk-group** ***5***. 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's expectation. Setting the **Network Call Redirection** flag to ***y*** enables advanced services associated with the use of the SIP REFER method, 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 for calls held at the enterprise, 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*** to allow REFER to be exercised with the Verizon IP Toll Free Service.

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 5                                            Page   4 of  21
                              PROTOCOL VARIATIONS

                      Mark Users as Phone? n
            Prepend '+' to Calling Number? n
      Send Transferring Party Information? n
                 Network Call Redirection? y
                    Send Diversion Header? 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
```

5.9. Contact Center Configuration

This section describes the basic commands used to configure Vector Directory Numbers (VDNs) and corresponding vectors. These vectors contain steps that invoke the Communication Manager SIP Network Call Redirection (NCR) functionality. These Application Notes provide rudimentary vector definitions to demonstrate and test the SIP NCR and UUI functionalities. In general, call centers will use vector functionality that is more complex and tailored to individual needs. Call centers may also use customer hosts running applications used in conjunction with Application Enablement Services (AES) to define call routing and provide associated UUI. The definition and documentation of those complex applications and associated vectors are beyond the scope of these Application Notes.

5.9.1 Announcements

Various announcements will be used within the vectors. In the sample configuration, these announcements were sourced by the Avaya G450 Media Gateway. The following abridged **list** command summarizes the announcements used in conjunction with the vectors 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
7696                  integrated Refer-Fail-Announcement      001V9       1
7697                  integrated Pre-REFER-Announcement       001V9       1
```

5.9.2 Post-Answer Redirection to a PSTN Destination

This section provides an example configuration of a vector that will use post-answer redirection to a PSTN destination. In this example, the inbound toll-free call is routed to **VDN *7698*** shown in the following screen. The originally dialed Verizon IP Toll Free number may be mapped to VDN 7698 by Session Manager digit conversion, or via the incoming call handling treatment for the Communication Manager trunk group handling the call.

```
display vdn 7698                                                   Page   1 of   3
                            VECTOR DIRECTORY NUMBER

                             Extension: 7698
                                 Name*: Refer-to-PSTN
                           Destination: Vector Number        3
                   Attendant Vectoring? n
                  Meet-me Conferencing? n
                    Allow VDN Override? n
                                   COR: 1
                                   TN*: 1
                              Measured: none
```

VDN 7698 is associated with **vector *3***, which is shown below. Vector 3 plays an announcement (step 03) to answer the call. After the announcement, the **route-to number** (step 05) includes ***~r+13035387023*** where the number 303-538-7023 is a PSTN destination. This step causes a REFER message to be sent where the Refer-To header includes "+13035387023" as the user portion. Note that Verizon IP Contact Center services require the "+" in the Refer-To header for this type of call redirection.

```
display vector 3                                            Page   1 of   6
                                  CALL VECTOR

    Number: 3                Name: Refer-to_PSTN
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-time    2   secs hearing ringback
02 #    Play Announcement to caller in step 3.  This answers the call.
03 announcement 7697
04 #    Refer the call to PSTN destination in Step 5 below.
05 route-to     number ~r+13035387023   with cov n if unconditionally
06 #    If Refer fails play announcement and disconnect
07 disconnect   after announcement 3696
```

5.9.3 Post-Answer Redirection With UUI to a SIP Destination

This section provides an example of post-answer redirection with UUI passed to a SIP destination. In this example, the inbound call is routed to **VDN *7690*** shown in the following screen. The originally dialed Verizon toll-free number may be mapped to VDN 7690 by Session Manager digit conversion, or via the incoming call handling treatment for the Communication Manager trunk group handling the call.

```
display vdn 7690                                               Page   1 of   3
                            VECTOR DIRECTORY NUMBER

                             Extension: 7690
                                 Name*: Refer-with-UUI
                           Destination: Vector Number        5
                   Attendant Vectoring? n
                  Meet-me Conferencing? n
                    Allow VDN Override? n
                                   COR: 1
```

To facilitate testing of NCR with UUI, the following vector variables were defined.

```
change variables                                                Page   1 of  39
                              VARIABLES FOR VECTORS

Var Description                     Type    Scope Length Start Assignment       VAC
A   Test1                           asaiuui L     16     1
B   Test2                           asaiuui L     16     17
C
```

VDN 7690 is associated with vector 5, which is shown below. Vector 5 sets data in the vector variables A and B (steps 01 and 02) and plays an announcement to answer the call (step 05). After the announcement, the **route-to** number step includes ***~r+18666747056***. This step causes a REFER message to be sent where the Refer-To header includes "+18666747056" as the user portion. The Refer-To header will also contain the UUI set in variables A and B. Verizon will include this UUI in the INVITE ultimately sent to the SIP-connected target of the REFER, which is toll-free number "18666747056". In the sample configuration, where only one location was used, 866-674-7056 is another toll-free number assigned to the same circuit as the original call. In practice, NCR with UUI would allow Communication Manager to send call or customer-related data along with the call to another contact center.

```
display vector 5                                           Page   1 of   6
                                  CALL VECTOR

    Number: 5                Name: Refer-with-UUI
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 set          A      = none   CATR  1234567890123456
02 set          B      = none   CATR  7890123456789012
03 wait-time    2   secs hearing ringback
04 #    Play announcement to answer call and route to ~r to cause REFER
05 announcement 7697
06 route-to     number ~r+18666747056   with cov n if unconditionally
07 #    If REFER fails play announcement and disconnect
08 disconnect   after announcement 7696
09
```

5.10. Inbound Routing

In general, the **incoming call handling treatment** for a trunk group can be used to manipulate the digits received for an incoming call if necessary. Since Session Manager is present, Session Manager can 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 toll-free 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 form of the receiving trunk group. As an example, the following screen illustrates a conversion of toll-free number 8666735877 to extension 7684 when the call arrives on trunk group 5.

```
change inc-call-handling-trmt trunk-group 5                  Page   1 of  30
                     INCOMING CALL HANDLING TREATMENT
 Service/      Number   Number      Del Insert
 Feature        Len      Digits
 public-ntwrk    10 8666735877       10  7684
 public-ntwrk    10 8666747056       10  7689
 public-ntwrk    10 8666747057       10  7690
```

5.11. Calling Party Information

The calling party number is sent in the SIP "From", "Contact" and "PAI" headers. Since public numbering was selected to define the format of this number (**Section 5.8**), use the **change public-**

unknown-numbering command to create an entry for each extension which has a DID assigned. The DID number will be one assigned by the SIP service provider. It is used to authenticate the caller.

In the bolded rows shown in the example abridged output below, Communication Manager extensions are mapped to DID numbers that are known to Verizon for this SIP Trunk connection when the call uses trunk group 5.

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

Ext Ext            Trk       CPN             CPN
Len Code           Grp(s)    Prefix          Len
                                                    Total Administered: 10
  4  7690           5         8666747057      10     Maximum Entries: 9999
  4  7689           5         8666747056      10     Note: If an entry applies to
  4  7684           5         8666735877      10     a SIP connection to Avaya
                                                     Aura(tm) Session Manager,
                                                     the resulting number must
                                                     be a complete E.164 number.
```

5.12. Outbound Routing

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

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

    Dialed   Total  Call      Dialed   Total  Call      Dialed   Total  Call
    String   Length Type      String   Length Type      String   Length Type
   0           1   attd
   1           5   ext
   2           5   ext
   3           5   ext
   4           5   ext
   5           5   ext
   6           5   ext
   7           5   ext
   8           5   ext
   9           1   fac
   *           3   dac
   #           3   dac
```

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

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

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

Use the **change ars analysis** command to configure the routing of dialed digits following the first digit 9.

- **Dialed String:** enter the leading digits (e.g., ***1303***) necessary to uniquely select the desired route pattern.
- **Total Min:** enter the minimum number of digits (e.g., ***11***) expected for this PSTN number.
- **Total Max:** enter the maximum number of digits (e.g., ***11***) expected for this PSTN number.
- **Route Pattern:** enter the route pattern number (e.g., ***1***) to be used. The route pattern (to be defined next) will specify the trunk group(s) to be used for calls matching the dialed number.
- **Call Type:** enter ***fnpa***, the call type for North American 1+10 digit calls. For local 7 or 10 digit calls enter ***hnpa***. For 411 and 911 calls use ***svcl*** and ***emer*** respectively. The call type tells Communication Manager what kind of call is made to help decide how to handle the dialed string and whether or not to include a preceding 1.

The example below shows a subset of the dialed strings tested as part of the compliance test. All dialed strings are mapped to route pattern 1 which contains the SIP trunk to the service provider (as defined next).

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

          Dialed           Total     Route    Call   Node   ANI
          String          Min  Max  Pattern   Type   Num    Reqd
    1303                  11   11     1       fnpa          n
    1502                  11   11     1       fnpa          n
    17                    11   11     1       fnpa          n
    1720                  11   11     1       fnpa          n
    18                    11   11     1       fnpa          n
    1866                  11   11     1       fnpa          n
    1877                  11   11     1       fnpa          n
    1888                  11   11     1       fnpa          n
    1908                  11   11     1       fnpa          n
```

The route pattern defines which trunk group will be used for the call and performs any necessary digit manipulation. Use the **change route-pattern** command to configure the parameters for the service provider trunk route pattern in the following manner. The example below shows the values used for **route-pattern *1*** during the compliance test.

- **Pattern Name**: Enter a descriptive name.
- **Grp No**: Enter the outbound trunk group for the SIP service provider. For the compliance test, trunk group ***5*** was used.
- **FRL**: Set the Facility Restriction Level (**FRL**) field to a level that allows access to this trunk for all users that require it. The value of ***0*** is the least restrictive level.
- **Pfx Mrk**: A prefix mark (**Pfx Mrk**) of ***1*** will prefix any FNPA 10-digit number with a 1 and leave numbers of any other length unchanged. This will ensure 1 + 10 digits are sent to the service provider for long distance North American Numbering Plan (NANP) numbers. All HNPA 10 digit numbers are left unchanged.

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

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

5.13. Saving Communication Manager Configuration Changes

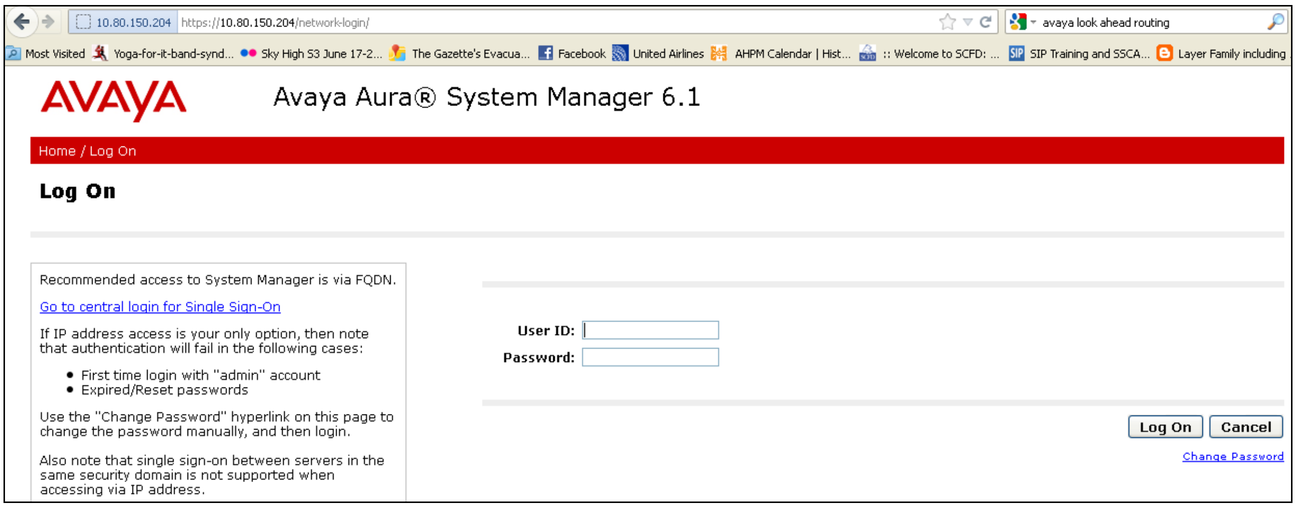
The command "save translation all" can be used to save the configuration.

6. Avaya Aura ® Session Manager Configuration for SIP Trunking

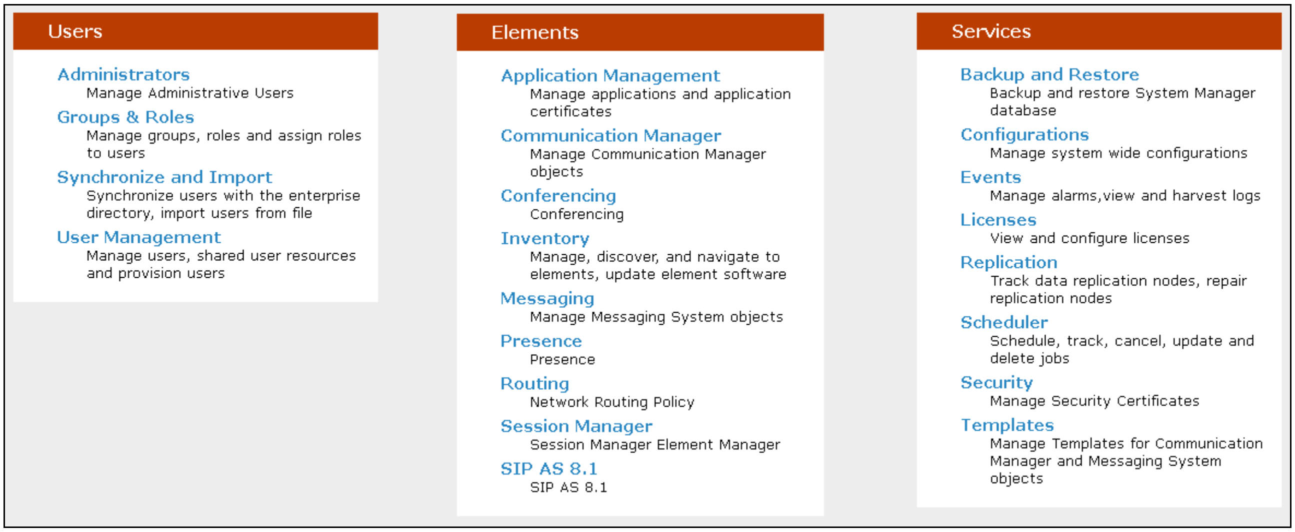
This section illustrates relevant aspects of the Session Manager configuration used in the verification of these Application Notes.

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.

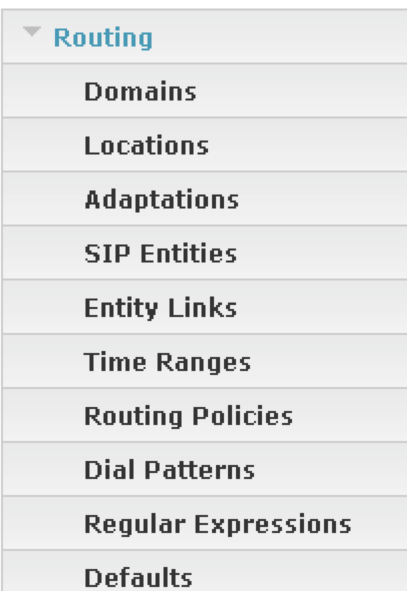
Session Manager is managed via System Manager. Using a web browser, access "https://<ip-addr of System Manager>/SMGR". In the **Log On** screen, enter appropriate **User ID** and **Password** and press the **Log On** button as shown in the example System Manager 6.1 **Log On** screen below.



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)

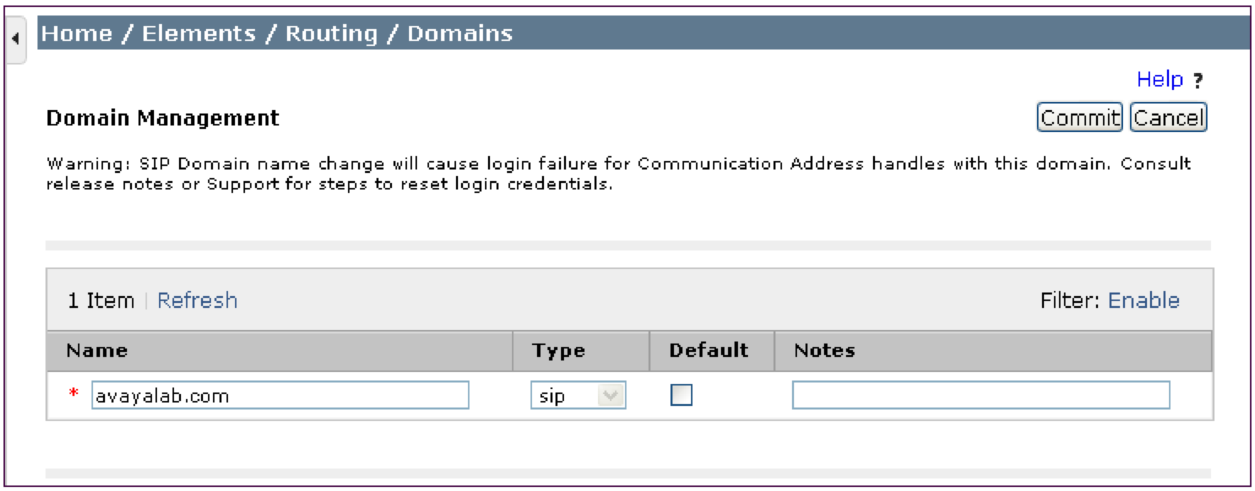
Step 9: "Regular Expressions" are defined and assigned to "Routing Policies" (one step)

6.1. Specify SIP Domain

Create a **SIP Domain** for each domain for which Session Manager will need to be aware in order to route calls. For the compliance test, this includes the enterprise domain (***avayalab.com***). Navigate to **Routing → Domains** and click the **New** button in the right pane (not shown). In the new right pane that appears, fill in the following:

- **Name:** Enter the domain name.
- **Type:** Select **sip** from the pull-down menu.
- **Notes:** Add a brief description (optional).

Click **Commit**. The screen below shows the entry for the ***avayalab.com*** domain.



6.2. Add Location

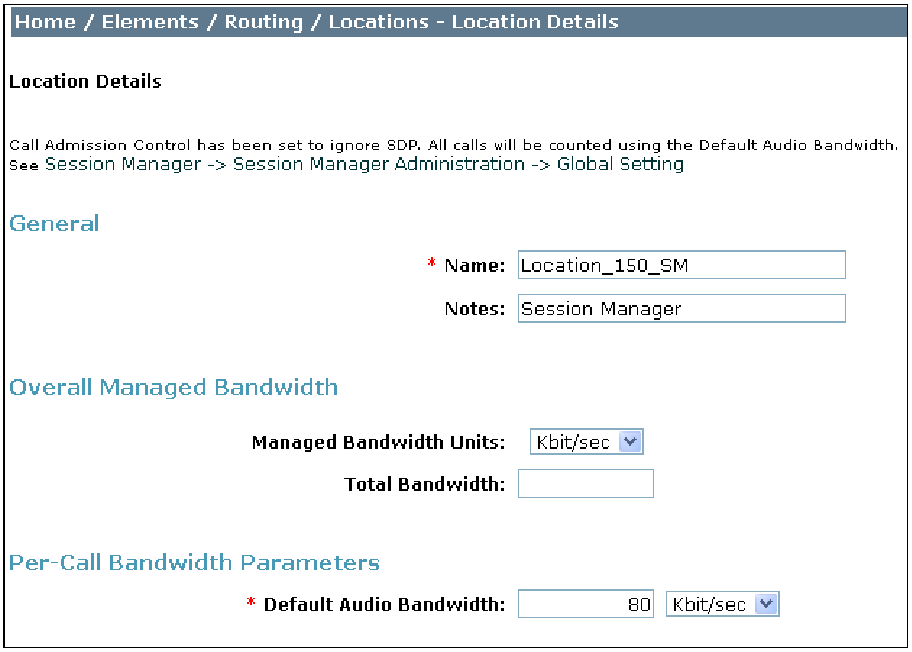
Locations can be used to identify logical and/or physical locations where SIP Entities reside for purposes of bandwidth management and call admission control. To add a location, navigate to **Routing →Locations** in the left-hand navigation pane and click the **New** button in the right pane (not shown).

In the **General** section, enter the following values. Use default values for all remaining fields:

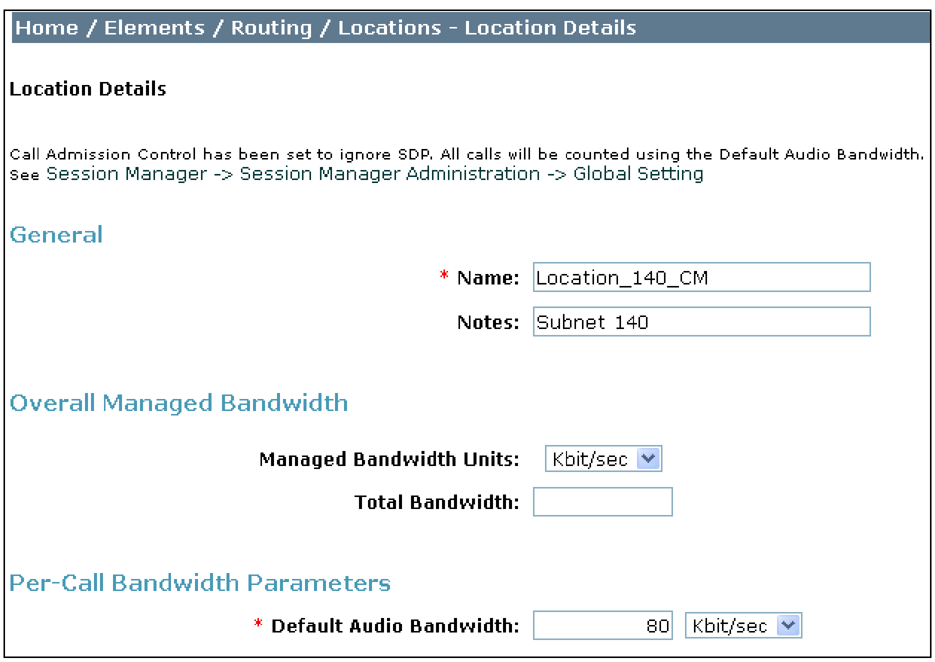
- **Name:** Enter a descriptive name for the location.
- **Notes:** Add a brief description (optional).

The **Location Pattern** was not populated. The Location Pattern is used to identify call routing based on IP address. Session Manager matches the IP address against the patterns defined in this section. If a call is from a SIP Entity that does not match the IP address pattern, then Session Manager uses the location administered for the SIP Entity. In this sample configuration Locations are added to SIP Entities (**Section 6.4**), so it was not necessary to add a pattern.

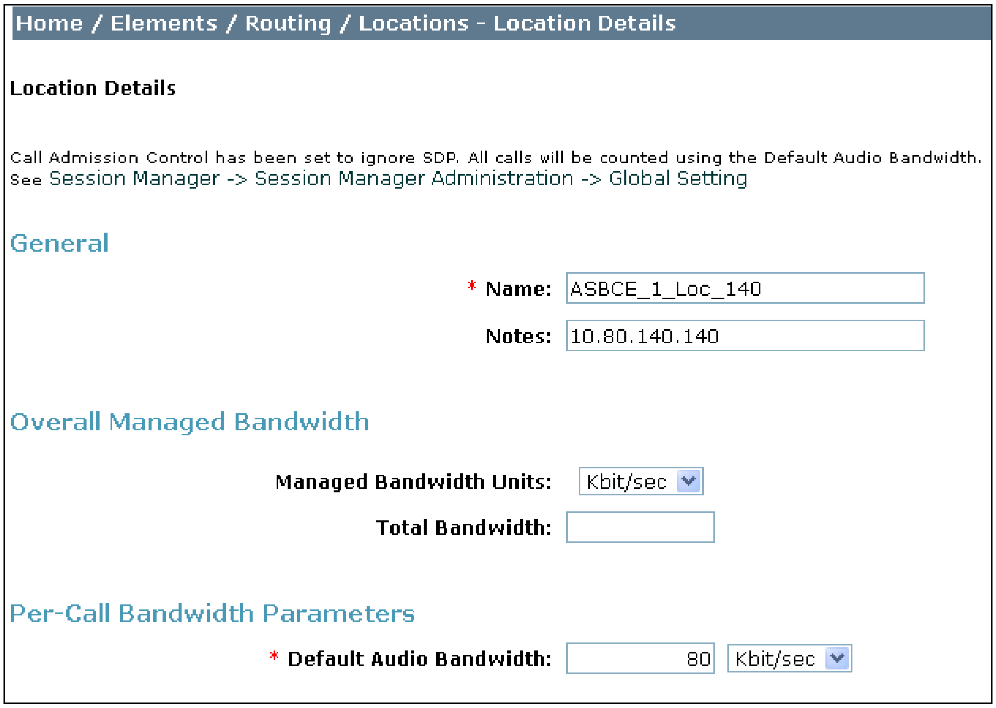
The following screen shows the addition of ***Location_150_SM***, this location will be used for Session Manager. Click **Commit** to save.



Repeat the preceding procedure to create a separate Location for Communication Manager and the Avaya SBCE. Displayed below is the screen for ***Location_140_CM*** used for Communication Manager.



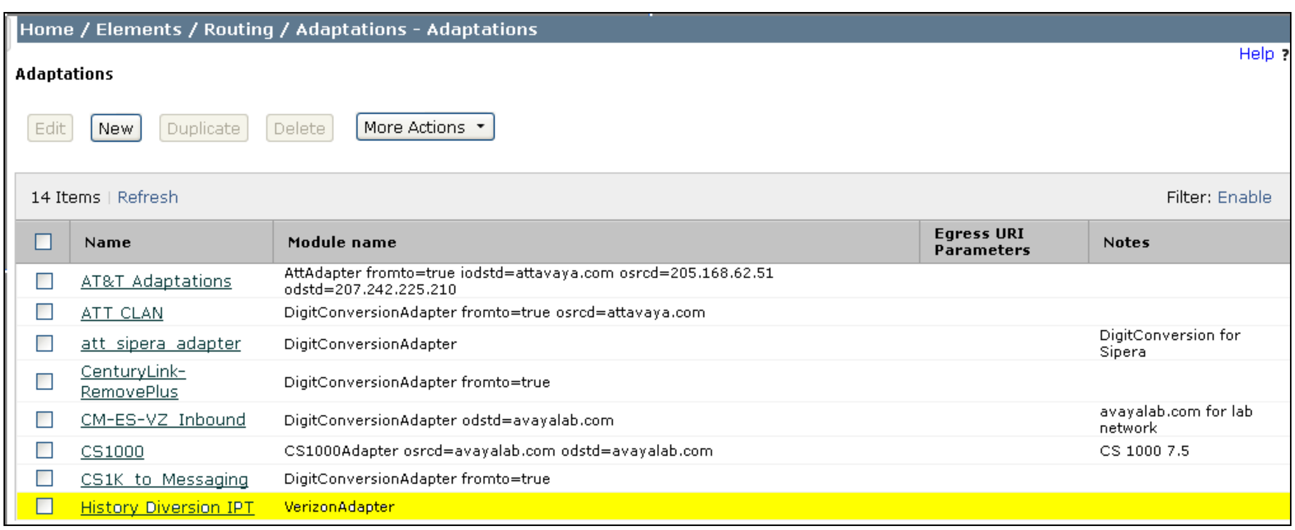
Below is the screen for ***ASBCE_1_Loc_140*** used for Avaya SBCE.



6.3. Adaptations

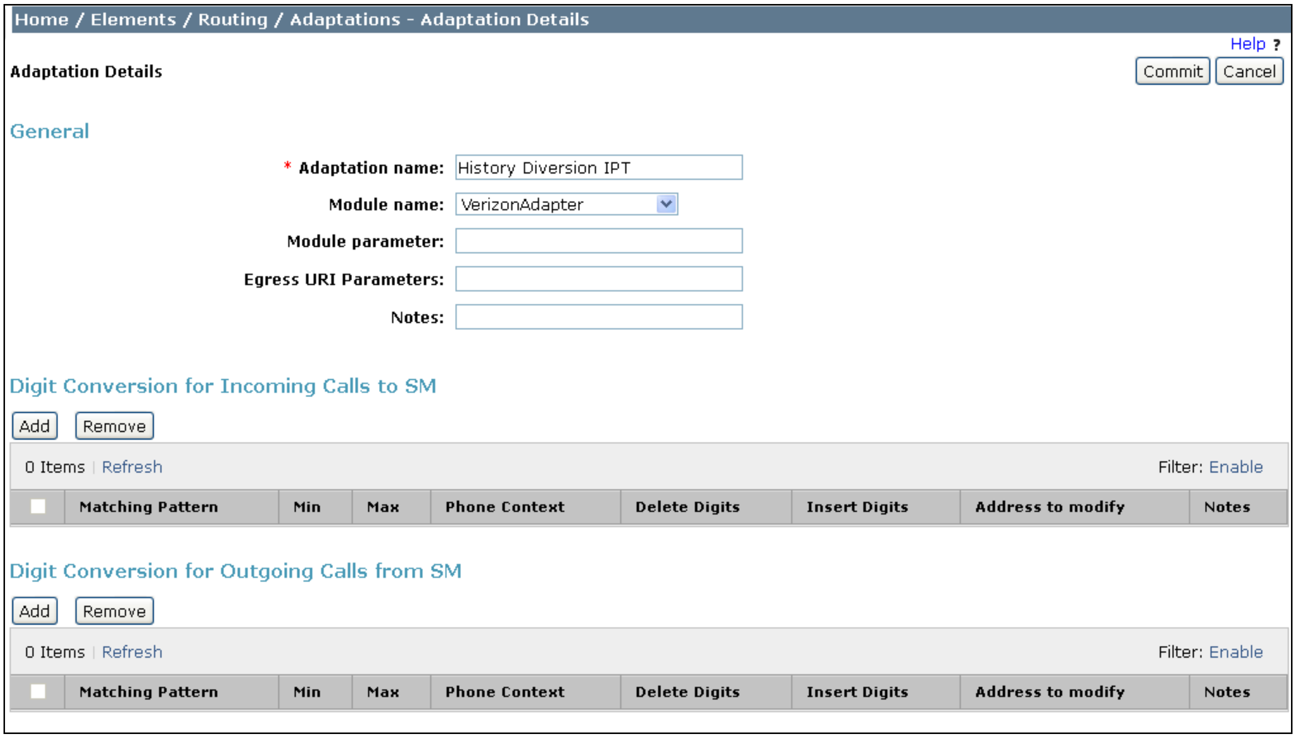
To view or change adaptations, select **Routing → Adaptations**. Click on the checkbox corresponding to the name of an adaptation and then **Edit** to edit an existing adaptation, or the **New** button to add an adaptation. Click the **Commit** button after changes are completed.

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 ***History Diversion IPT*** will later be assigned to the ASBCE SIP Entity. The History Diversion IPT Adapter uses the Verizon Adapter and performs the History-Info to

Diversion adaptation. The Verizon Adapter also performs all the conversions available by the Digit Conversion Adapter.



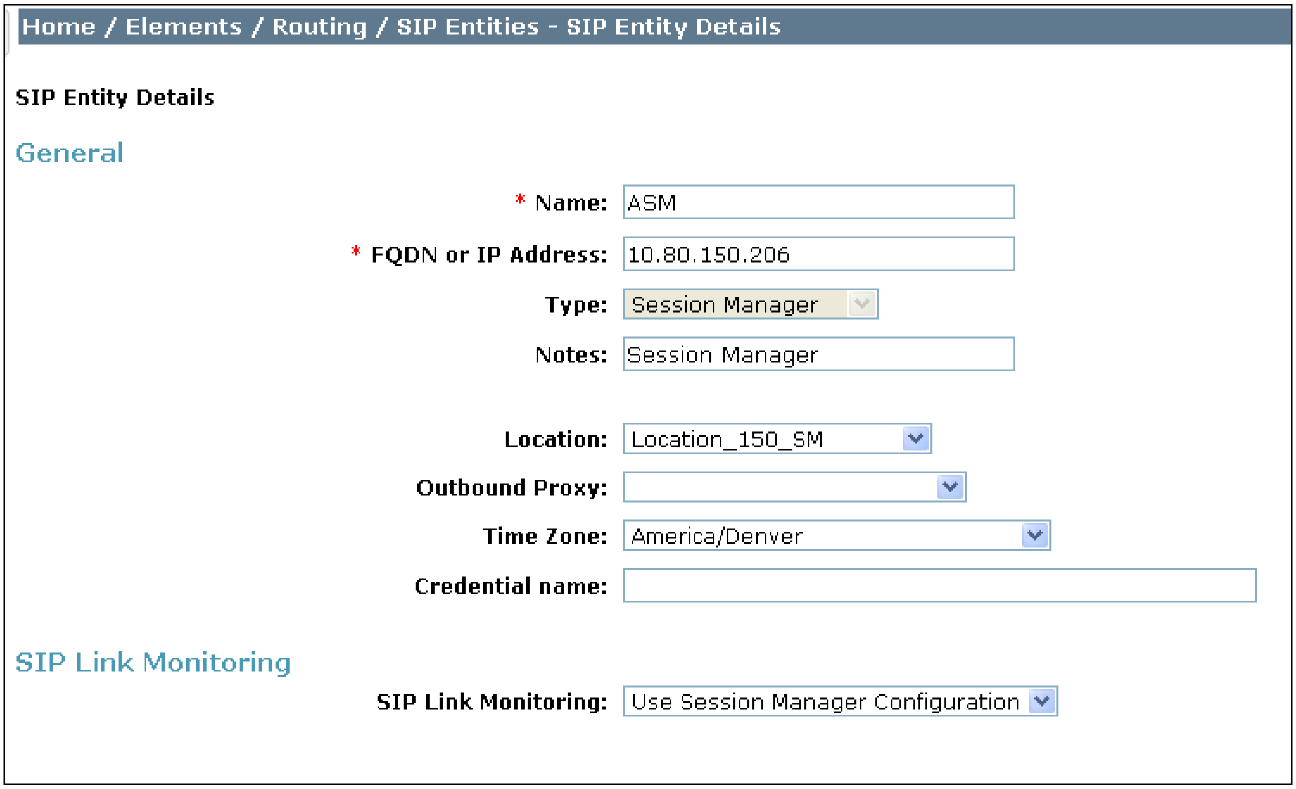
6.4. SIP Entities

A **SIP Entity** must be added for Session Manager and for each SIP telephony system connected to it which includes Communication Manager and the Avaya SBCE. Navigate to **Routing → SIP Entities** in the left-hand navigation pane and click on the **New** button in the right pane (not shown).

In the **General** section, enter the following values. Use default values for all remaining fields:

- **Name:** Enter a descriptive name.
- **FQDN or IP Address:** Enter the FQDN or IP address of the SIP Entity that is used for SIP signaling.
- **Type:** Enter ***Session Manager*** for Session Manager, ***CM*** for Communication Manager and ***SIP Trunk*** for the Avaya SBCE.
- **Adaptation:** This field is only present if **Type** is not set to ***Session Manager***. If applicable, select the **Adaptation Name** that will be applied to this entity.
- **Location:** Select one of the locations defined previously.
- **Time Zone:** Select the time zone for the location above.

The following screen shows the addition of Session Manager. The IP address of the Session Manager signaling interface is entered for **FQDN or IP Address**.

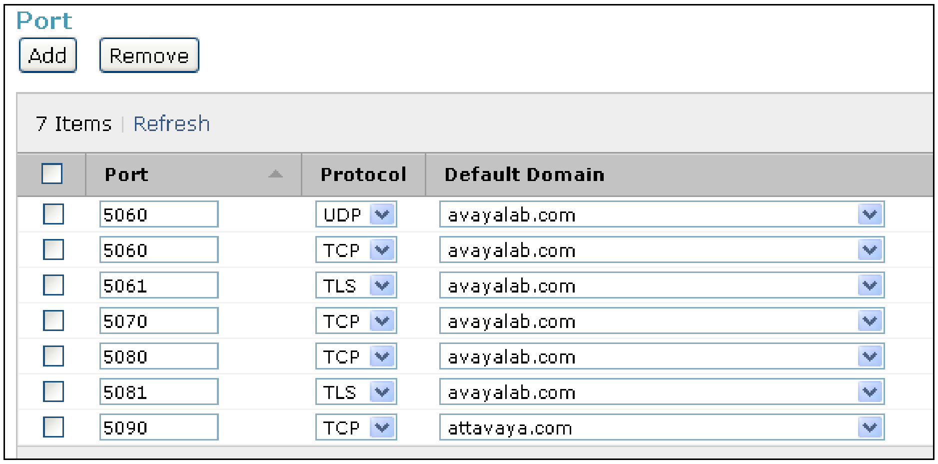


To define the ports used by Session Manager, scroll down to the **Port** section of the **SIP Entity Details** screen. This section is only present for **Session Manager** SIP entities. This section defines a default set of ports that Session Manager will use to listen for SIP requests, typically from registered SIP endpoints. Session Manager can also listen on additional ports defined elsewhere such as the ports specified in the SIP Entity Link definition in **Section 6.5**.

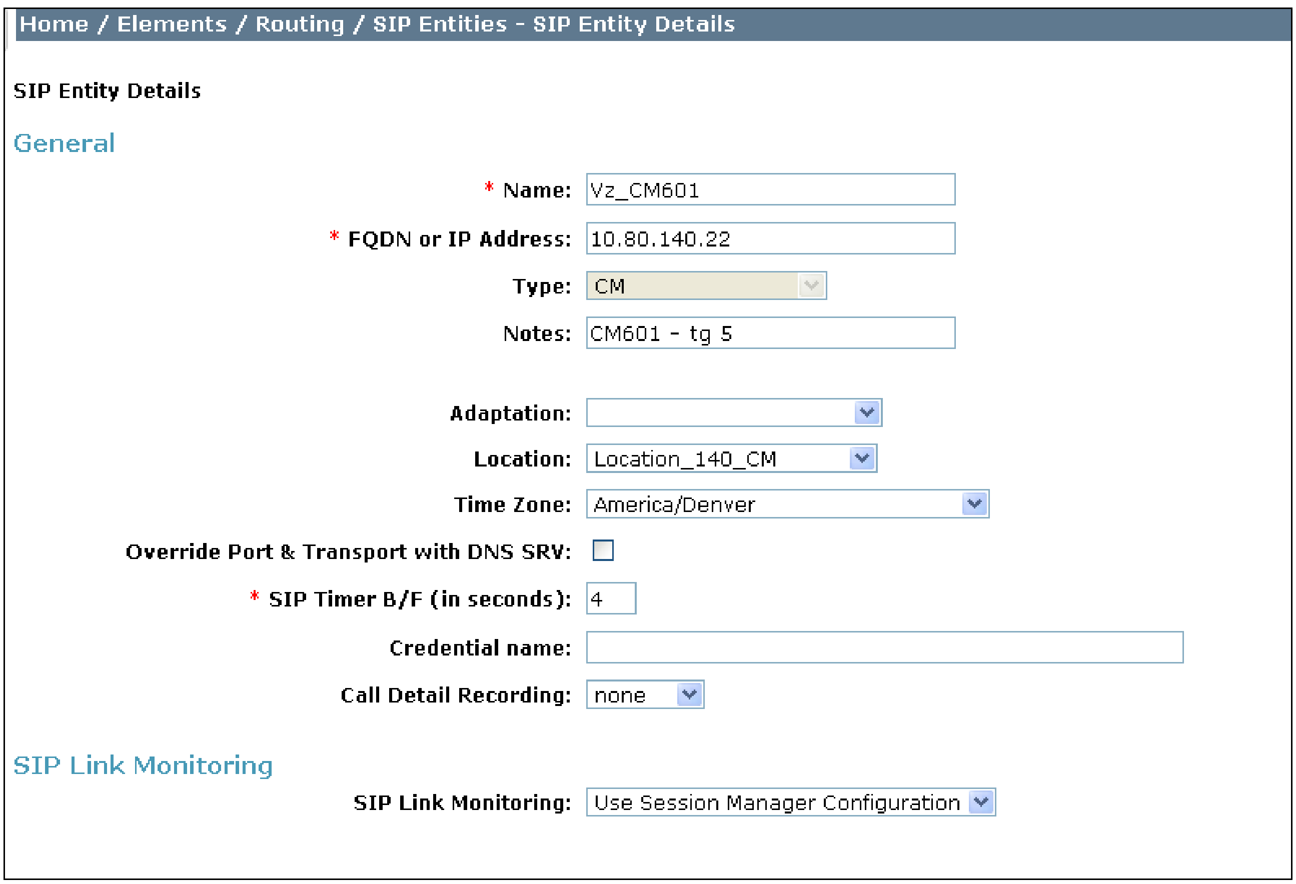
In the **Port** section, click **Add** and enter the following values. Use default values for all remaining fields:

- **Port:** Port number on which Session Manager can listen for SIP requests.
- **Protocol:** Transport protocol to be used to send SIP requests.
- **Default Domain:** The domain used for the enterprise.

Defaults can be used for the remaining fields. Click **Commit** to save.

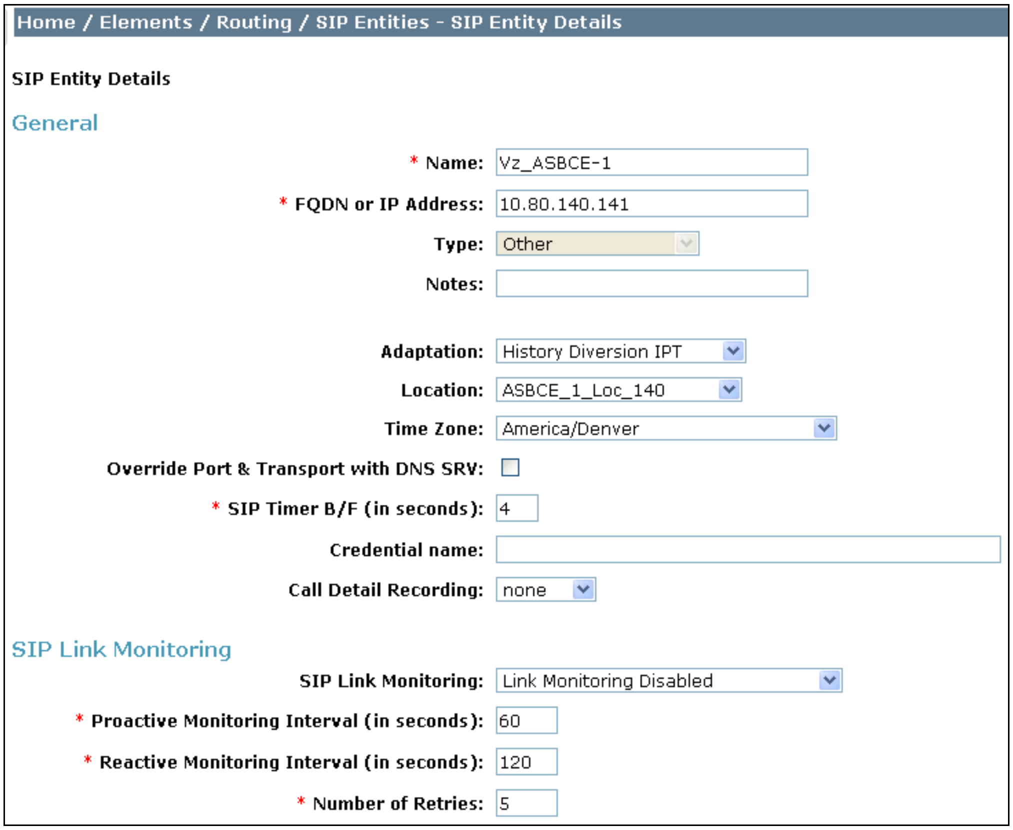


The following screen shows the addition of Communication Manager. The **FQDN or IP Address** field is set to the IP address defined in **Section 5.3** for the procr interface on Communication Manager. The Location is set to the one defined for Communication Manager in **Section 6.2**.



The following screen shows the upper portion of the **SIP Entity Details** corresponding to ***Vz_ASBCE-1***. The **FQDN or IP Address** field is configured with the Avaya SBCE inside IP Address (***10.80.140.141***). ***Other*** is selected from the **Type** drop-down menu for SBC SIP Entities. This SBC has been assigned to **Location** ***ASBCE_1_Loc_140***. Link Monitoring was Disabled as

SIP OPTIONS were not exchanged between Verizon and Avaya for the test. Other parameters (not shown) retain default values.



6.5. Entity Links

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.

A SIP trunk between Session Manager and a telephony system is described as an **Entity Link**. Two Entity Links were created; one to Communication Manager for use only by service provider traffic, and one to the Avaya SBCE. To add an Entity Link, navigate to **Routing → Entity Links** in the left-hand navigation pane and click on the **New** button in the right pane (not shown). Fill in the following fields in the new row that is displayed:

- **Name:** Enter a descriptive name.
- **SIP Entity 1:** Select the SIP Entity for Session Manager.
- **Protocol:** Select the transport protocol used for this link.
- **Port:** Port number on which Session Manager will receive SIP requests from the far-end. For Communication Manager, this must match the

Far-end Listen Port defined on the Communication Manager signaling group in **Section 5.7**.

- **SIP Entity 2:** Select the name of the other system. For Communication Manager, select the Communication Manager SIP Entity defined in **Section 6.4**.
- **Port:** Port number on which the other system receives SIP requests from the Session Manager. For Communication Manager, this must match the **Near-end Listen Port** defined on the Communication Manager signaling group in **Section 5.7**.
- **Trusted:** Check this box. **Note**: If this box is not checked, calls from the associated SIP Entity specified in **Section 6.4** will be denied.

Click **Commit** to save. The following screens illustrate the Entity Links to Communication Manager and Avaya SBCE.

Entity Link to Communication Manager:

Entity Links

1 Item | Refresh

Name	SIP Entity 1	Protocol	Port	SIP Entity 2	Port	Connection Policy
* Vz_ASM_CM601_tg5	* ASM	TCP	* 5060	* Vz_CM601	* 5060	Trusted

Entity Link to Avaya SBCE:

Entity Links

1 Item | Refresh

Name	SIP Entity 1	Protocol	Port	SIP Entity 2	Port	Connection Policy
* Vz_ASM_ASBCE-1	* ASM	TCP	* 5060	* Vz_ASBCE-1	* 5060	Trusted

6.6. Routing Policies

Routing Policies describe the conditions under which calls will be routed to the SIP Entities specified in **Section 6.4**. Two routing policies must be added; one for Communication Manager and one for the Avaya SBCE. To add a routing policy, navigate to **Routing → Routing Policies** in the left-hand navigation pane and click on the **New** button in the right pane (not shown). The screen below is displayed. Fill in the following:

In the **General** section, enter the following values. Use default values for all remaining fields:

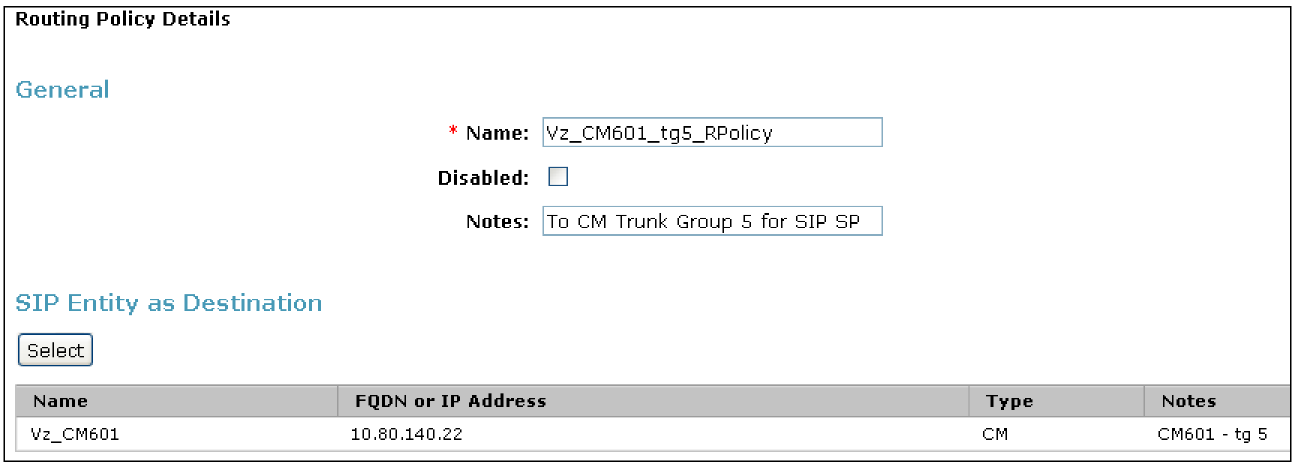
- **Name:** Enter a descriptive name.

- **Notes:** Add a brief description (optional).

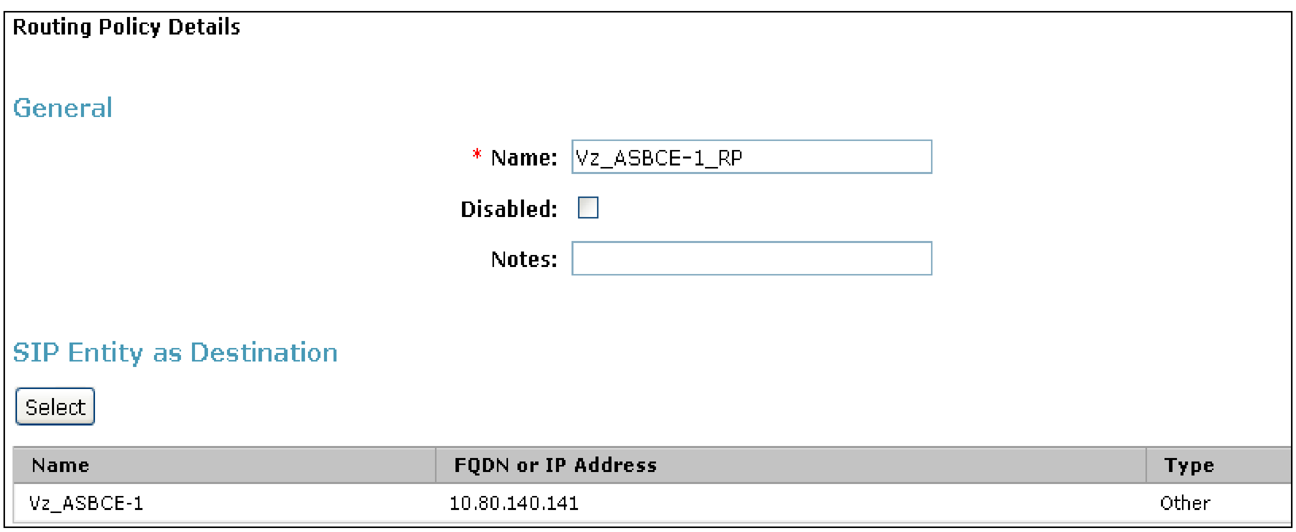
In the **SIP Entity as Destination** section, click **Select.** The **SIP Entity List** page opens (not shown). Select the appropriate SIP entity to which this routing policy applies and click **Select** (not shown)**.** The selected SIP Entity displays on the **Routing Policy Details** page as shown below. Use default values for remaining fields. Click **Commit** to save.

The following screens show the Routing Policies for Communication Manager and the Avaya SBCE.

Routing Policy for Communication Manger:



Routing Policy for Avaya SBCE:



6.7. Dial Patterns

Dial Patterns are needed to route calls through Session Manager. For the compliance test, dial patterns were needed to route calls from Communication Manager to Verizon and vice versa. Dial Patterns define which route policy will be selected for a particular call based on the dialed digits, destination domain and originating location. To add a dial pattern, navigate to **Routing → Dial Patterns** in the left-hand navigation pane and click on the **New** button in the right pane (not shown). Fill in the following, as shown in the screens below:

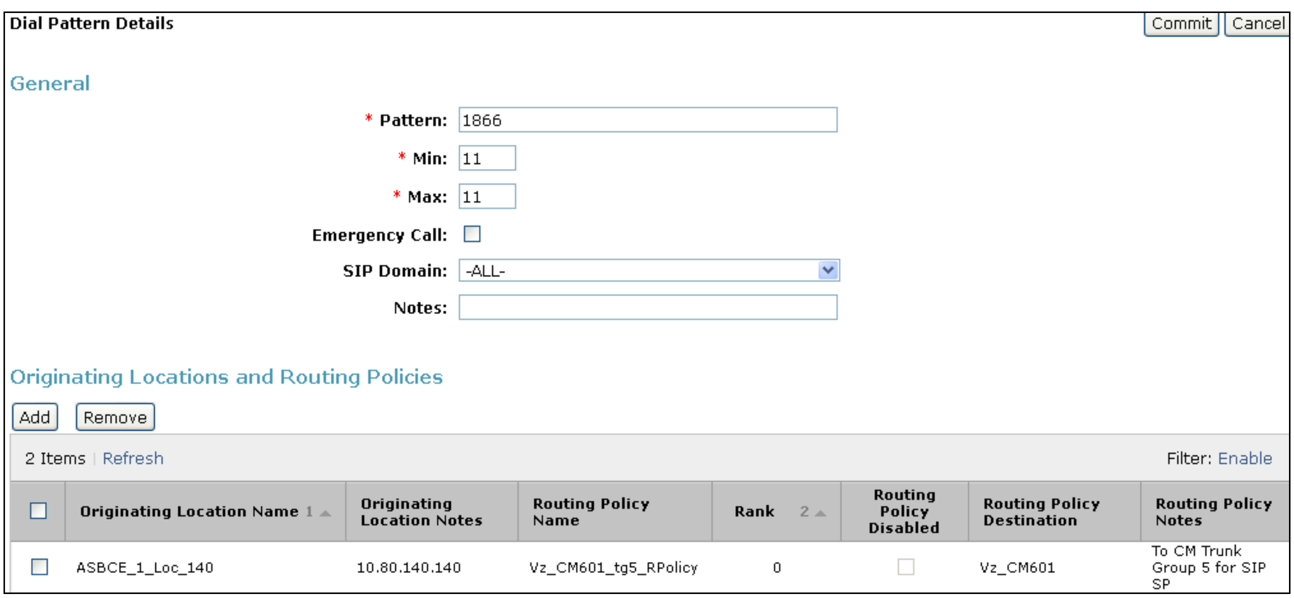
In the **General** section, enter the following values. Use default values for all remaining fields:

- **Pattern:** Enter a dial string that will be matched against the Request-URI of the call.
- **Min:** Enter a minimum length used in the match criteria.
- **Max:** Enter a maximum length used in the match criteria.
- **SIP Domain:** Enter the destination domain used in the match criteria.
- **Notes:** Add a brief description (optional).

In the **Originating Locations and Routing Policies** section, click **Add**. From the **Originating Locations and Routing Policy** list that appears (not shown), select the appropriate originating location for use in the match criteria. Lastly, select the routing policy from the list that will be used to route all calls that match the specified criteria. Click **Select**.

Default values can be used for the remaining fields. Click **Commit** to save.

An example of an inbound dial pattern used for the compliance test is shown below. The example shows that 11 digit dialed numbers that begin with ***1866*** originating from ***ASBCE_1_Loc_140*** uses route policy ***Vz_CM601_tg5_RPolicy***.


Dial Pattern Details

Commit | Cancel

General

* Pattern: 1866

* Min: 11

* Max: 11

Emergency Call:

SIP Domain: -ALL-

Notes:

Originating Locations and Routing Policies

Add | Remove

2 Items | Refresh

Filter: Enable

	Originating Location Name	Originating Location Notes	Routing Policy Name	Rank	Routing Policy Disabled	Routing Policy Destination	Routing Policy Notes
	ASBCE_1_Loc_140	10.80.140.140	Vz_CM601_tg5_RPolicy	0		Vz_CM601	To CM Trunk Group 5 for SIP SP

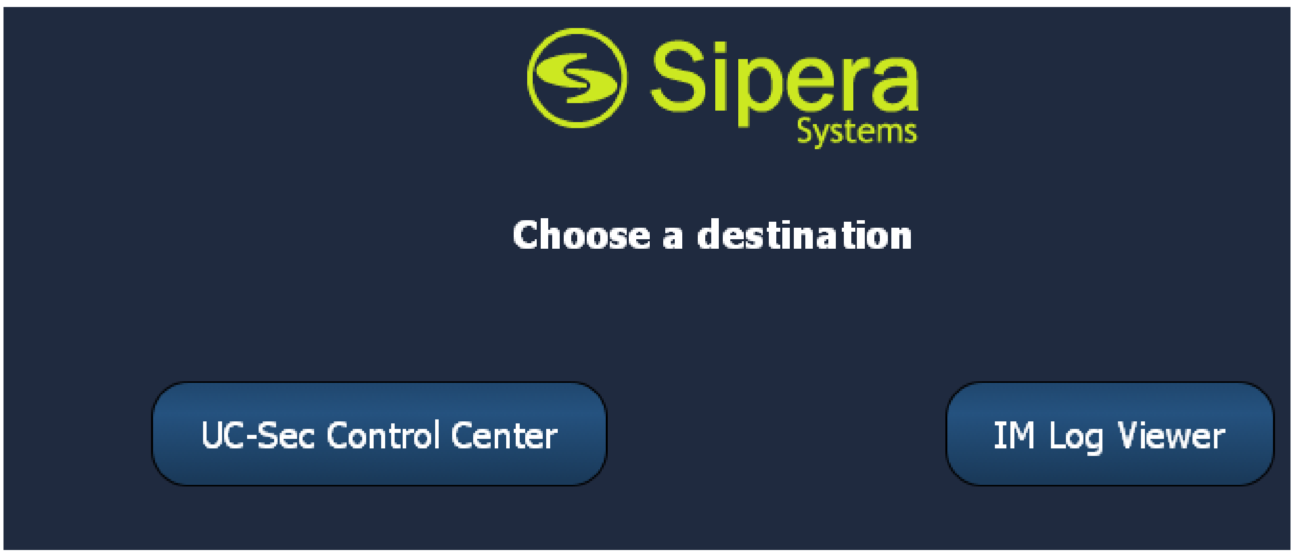
7. Avaya Session Border Controller for Enterprise

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

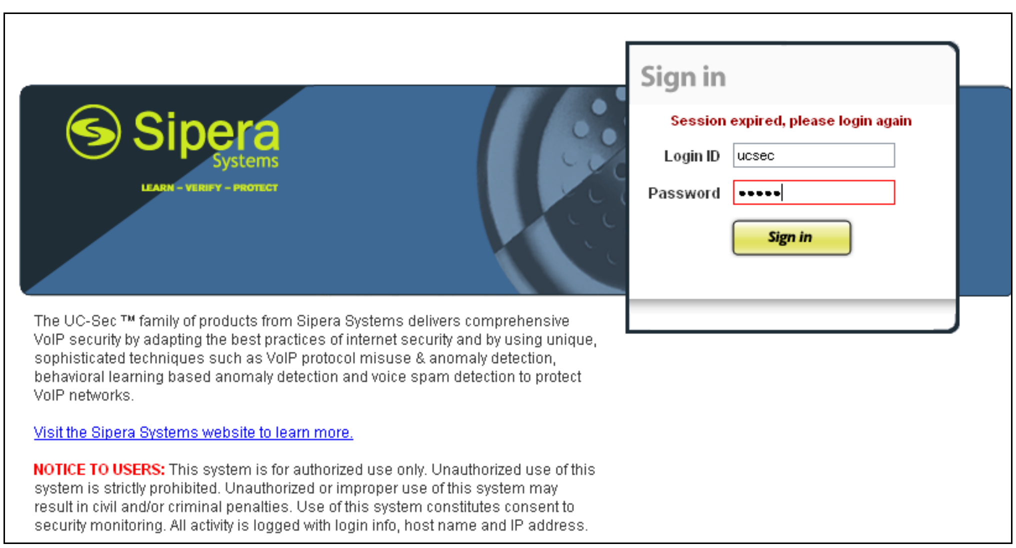
These Application Notes assume that the installation of the Avaya SBCE, and the assignment of a management IP Address, have already been completed.

7.1. Access the Management Interface

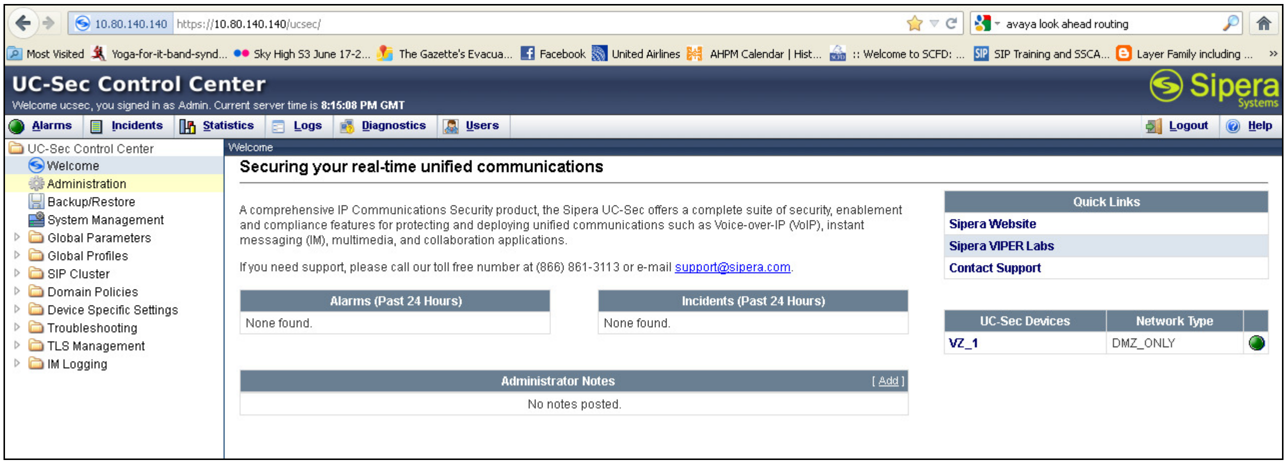
Access the web management interface by entering https://<ip-address> where <ip-address> is the management IP address assigned during installation. Select **UC-Sec Control Center**.



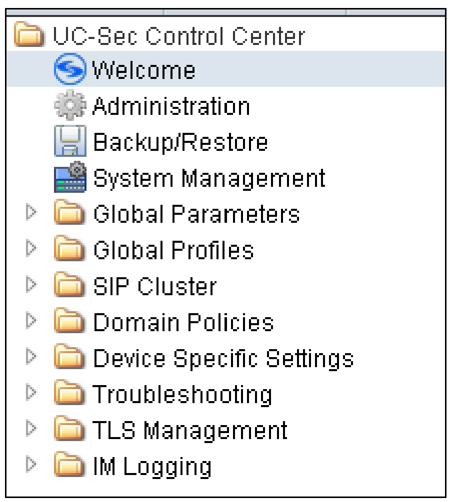
A login screen is presented. Enter an appropriate **Login ID** and **Password**.



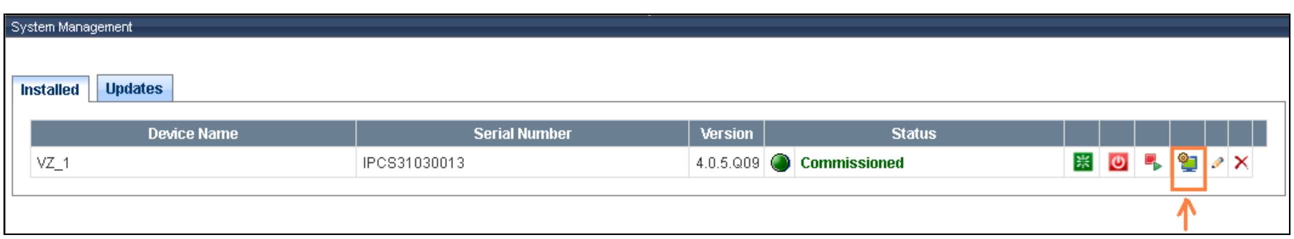
The main page of the UC-Sec Control Center will appear.



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.

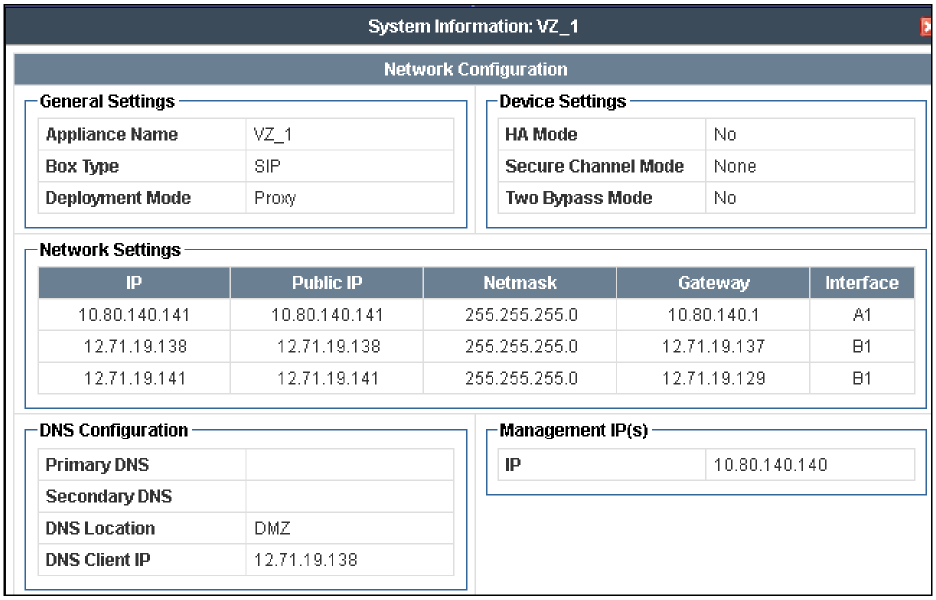


To view system information that was configured during installation, navigate to **UC-Sec Control Center → System Management**. A list of installed devices is shown in the right pane. In the case of the sample configuration, a single device named VZ_1 is shown. To view the configuration of this device, click the monitor icon (the third icon from the right).



The **System Information** screen shows the **Network Settings, DNS Configuration** and

Management IP(s) information provided during installation and corresponds to **Figure 1**. The **Box Type** was set to ***SIP*** and the **Deployment Mode** was set to ***Proxy***. Default values were used for all other fields.


System Information: VZ_1

Network Configuration

General Settings

Appliance Name	VZ_1
Box Type	SIP
Deployment Mode	Proxy

Device Settings

HA Mode	No
Secure Channel Mode	None
Two Bypass Mode	No

Network Settings

IP	Public IP	Netmask	Gateway	Interface
10.80.140.141	10.80.140.141	255.255.255.0	10.80.140.1	A1
12.71.19.138	12.71.19.138	255.255.255.0	12.71.19.137	B1
12.71.19.141	12.71.19.141	255.255.255.0	12.71.19.129	B1

DNS Configuration

Primary DNS	
Secondary DNS	
DNS Location	DMZ
DNS Client IP	12.71.19.138

Management IP(s)

IP	10.80.140.140

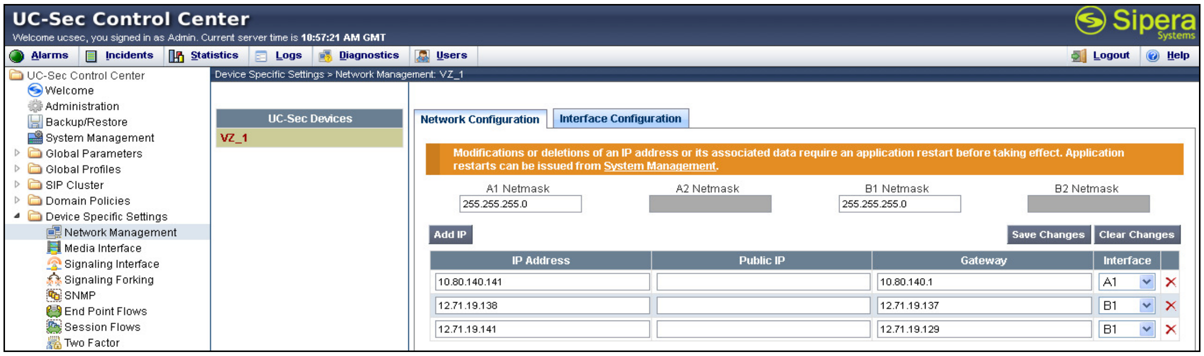
7.2. Device Specific Settings

7.2.1 Define Network Information

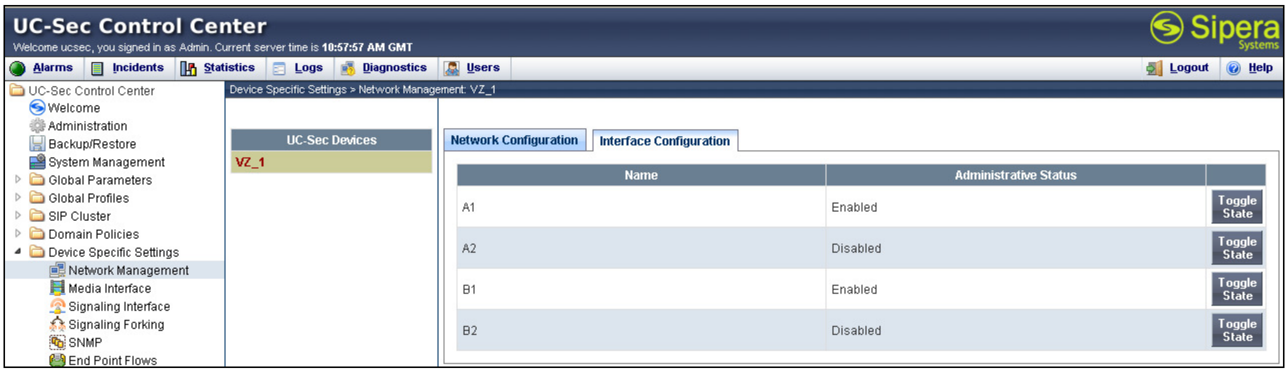
Network information is required on the Avaya SBCE to allocate IP addresses and masks to the interfaces. Note that only the **A1** and **B1** physical interfaces are used. Typically the **A1** interface is used for the internal side and **B1** is used for external. Each side of the Avaya SBCE can have only one physical interface assigned. One internal interface address and two external interface addresses (both configured on physical interface B1) were required for the Verizon testing. To define the network information, navigate to **Device Specific Settings → Network Management** in the **UC-Sec Control Center** menu on the left hand side and click **Add IP**. A new line appears that can be configured.

- **IP Address:** Enter the IP Address for the internal interface
- **Gateway:** Enter the appropriate gateway IP Address
- **Interface:** Select the desired hardware interface **(A1)**

Click **Save Changes**.
Repeat the process for external interface addresses using **B1.**
Note: Multiple IP addresses defined on a single interface must be in the same subnet.



Select the **Interface Configuration** tab and click on **Toggle State** to enable the interfaces.



7.2.2 Signaling Interfaces

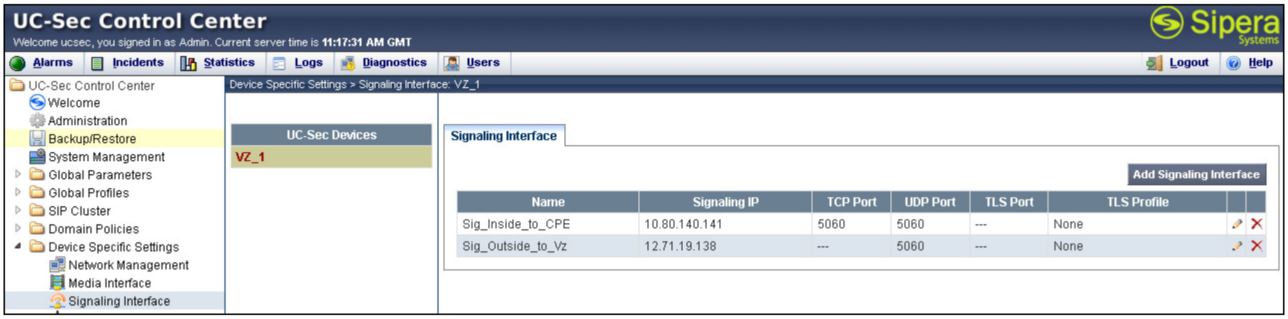
To define the **Signaling Interfaces** on the Avaya SBCE, navigate to **Device Specific Settings → Signaling Interface** in the **UC-Sec Control Center** menu on the left hand side and Select **Add Signaling Interface**.

Define a signaling interface for Verizon:

- **Name** — Enter a descriptive name for the external signaling interface to the Verizon network
- **IP Address:** — Choose the external address for the signaling
- **TCP/UDP/TLS Port:** — Enter the port for the desired transport protocol

Click **Finish** (not shown).

Repeat the process for the internal Avaya network.



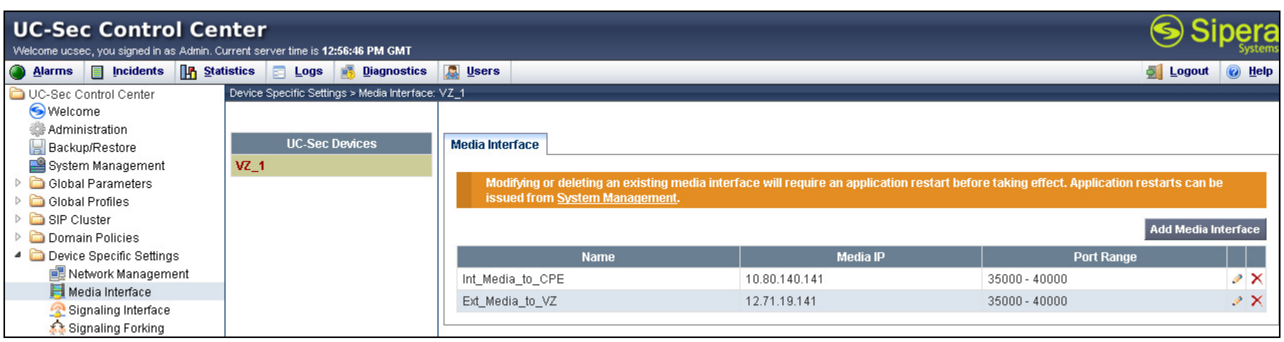
7.2.3 Media Interfaces

To define the **Media Interfaces** on the Avaya SBCE, navigate to **Device Specific Settings → Media Interface** in the **UC-Sec Control Center** menu on the left hand side, and select **Add Media Interface**. Details of the RTP and SRTP port ranges for the internal and external media streams are entered here. The IP addresses for media can be the same as those used for signaling or can be different.

Define a media interface for Verizon:

- **Name** — Enter a descriptive name for the external media interface for the Verizon network
- **IP Address:** — Choose the external address for the media
- **Port Range:** — Enter port ranges for the media path

Repeat the process for the internal Avaya network.



7.3. Global Profiles

Global Profiles allows for configuration of parameters across all UC-Sec appliances.

7.3.1 Routing Profile

Routing Profiles define a specific set of packet routing criteria that are used in conjunction with other types of domain policies to identify a particular call flow and thereby ascertain which security features will be applied to those packets. Parameters defined by Routing Profiles include packet transport settings, name server addresses and resolution methods, next hop routing information, and packet transport types.

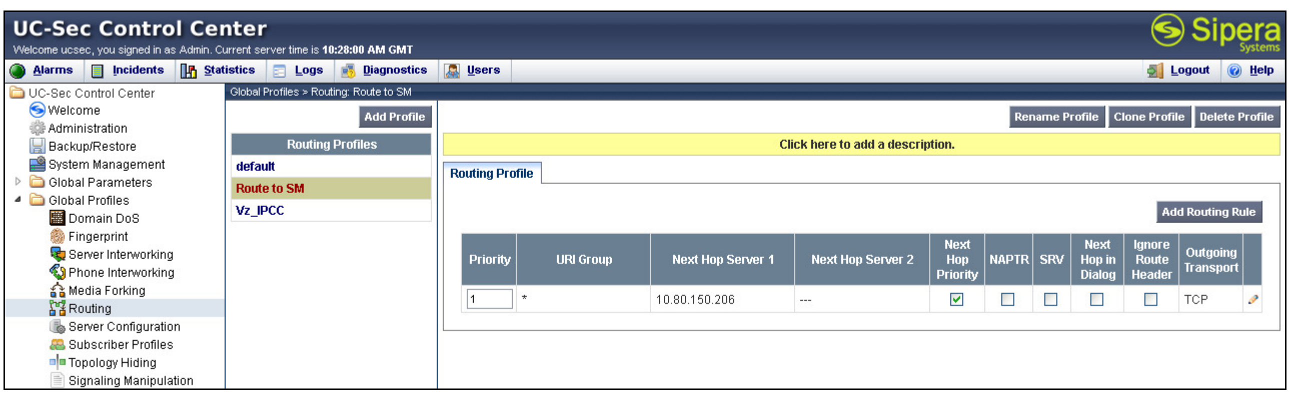
Create a Routing Profile for Session Manager and Verizon SIP Trunk. To add a routing profile, navigate to **UC-Sec Control Center →Global Profiles → Routing** and select **Add Profile**. Enter a **Profile Name** and click **Next** to continue (not shown).

In the new window that appears, enter the following values. Use default values for all remaining fields:

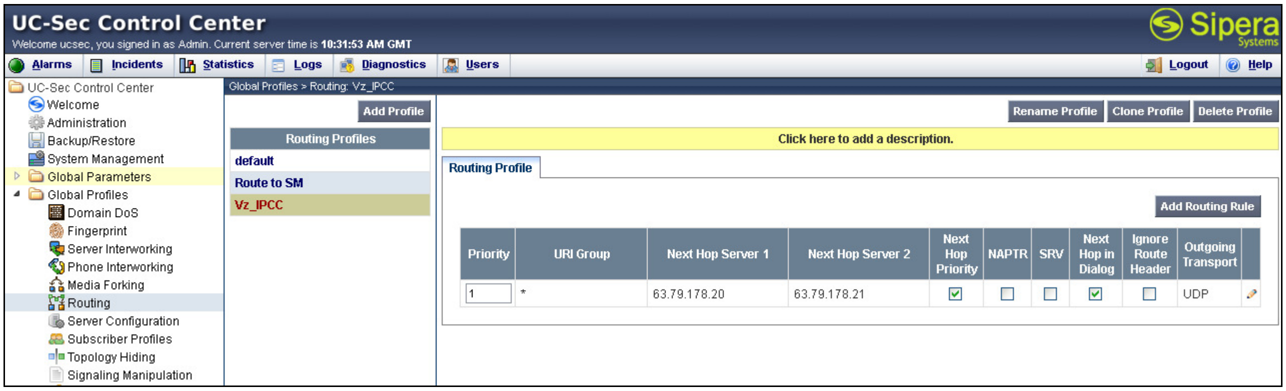
- **URI Group:** Select "*" from the drop down box.
- **Next Hop Server 1:** Enter the Domain Name or IP address of the Primary Next Hop server.
- **Next Hop Server 2:** (Optional) Enter the Domain Name or IP address of the secondary Next Hop server.
- **Routing Priority Based on Next Hop Server**: Checked.
- **Next Hop in Dialog:** (Optional) Checked only information in the Via Header is to be used instead of received port and IP.
- **Outgoing Transport:** Choose the protocol used for transporting outgoing signaling packets.

Click **Finish** (not shown).

The following screen shows the Routing Profile to Session Manager. The **Next Hop Server 1** IP address must match the IP address of the Session Manager Security Module. The **Outgoing Transport** must match the Avaya SBCE Entity Link created on Session Manager in **Section 6.5**.



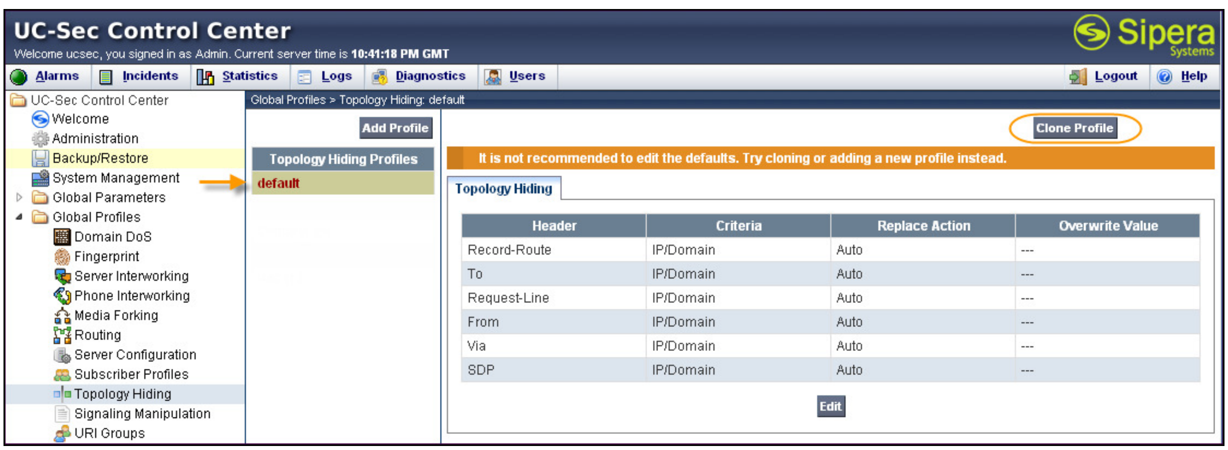
The following screen shows the Routing Profile to Verizon. In the **Next Hop Server 1** field enter the IP address that Verizon uses for the IPCC Service Director. In the **Next Hop Server 2** field enter the IP address that Verizon uses for the IPCC Service Host. Check the **Next Hop Priority** and the **Next Hop in Dialog** (This is only used if the information in the Via header is to be used and not the IP and port that the request was received on. See Verification **Section 9** for a detailed description). Enter **UDP** for the **Outgoing Transport** field.



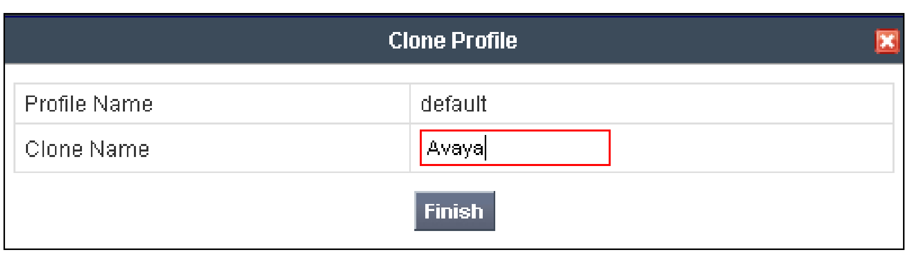
7.3.2 Topology Hiding Profile

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

Create a Topology Hiding Profile for both the enterprise and the SIP Trunk. In the sample configuration, the **Enterprise** and **SIP Trunk** profiles were cloned from the default profile. To clone a default profile, navigate to **UC-Sec Control Center →Global Profiles → Topology Hiding**. Select the **default** profile and click on **Clone Profile** as shown below.

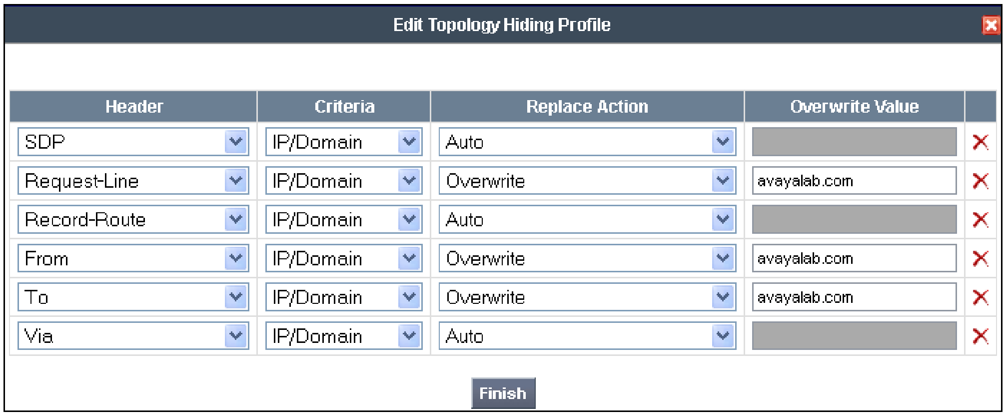


Enter a descriptive name for the new profile and click **Finish**.



Edit the ***Avaya*** profile to overwrite the **To**, **Request-Line** and **From** headers shown below to the enterprise domain. The **Overwrite Value** should match the Domain set in Session Manager

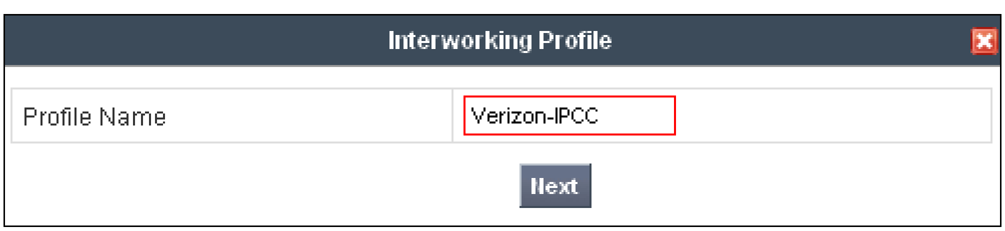
(**Section 6.1**) and the Communication Manager signaling group Far-end Domain (**Section 5.7**). Click **Finish** to save the changes.



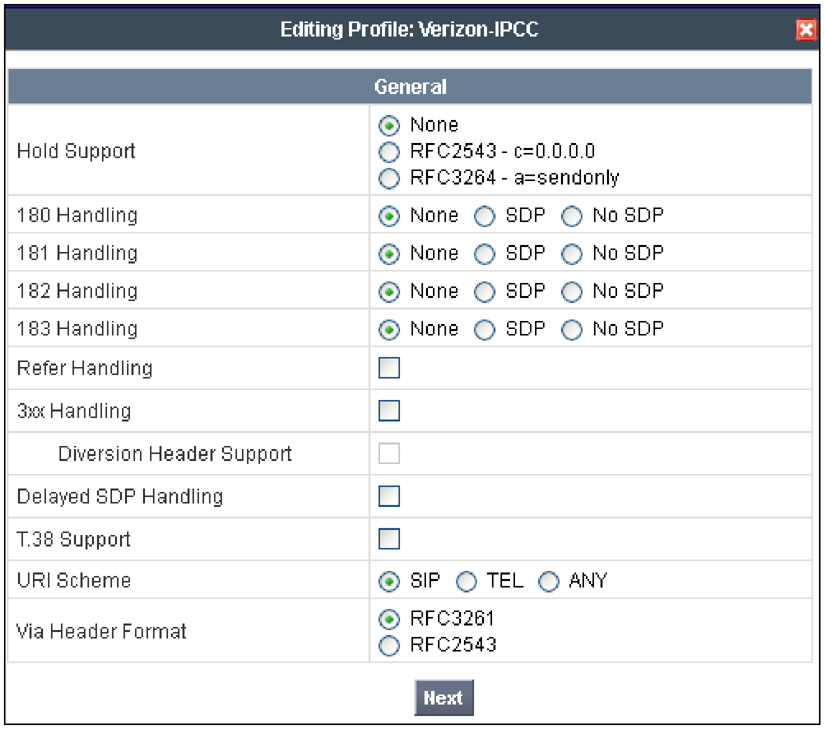
It is not necessary to modify the ***Verizon*** profile from the default values. The following screen shows the Topology Hiding Profile ***Verizon_IPT*** created for Verizon

7.3.3 Server Interworking

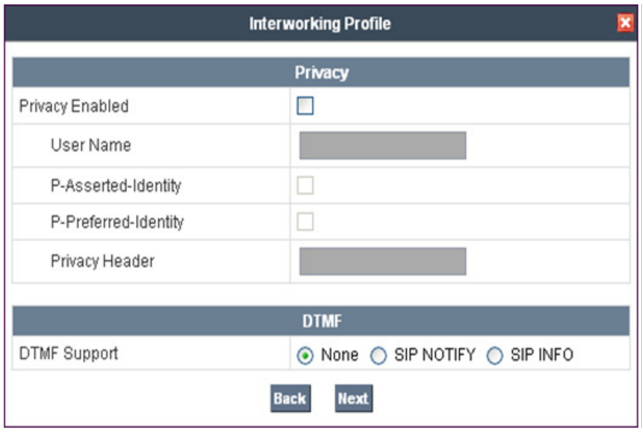
Click the **Add Profile** button (not shown) to add a new profile or select an existing interworking profile. If adding a profile, a screen such as the following is displayed. Enter an appropriate **Profile Name** such as ***Verizon-IPCC*** shown below. Click **Next**.

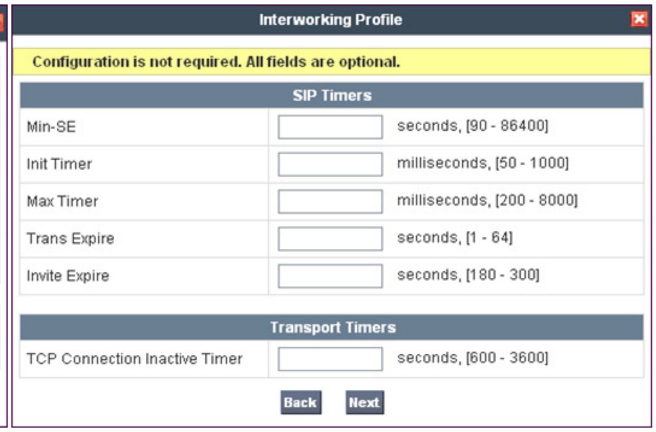


In the new window that appears, default values can be used. Click **Next** to continue**.**


Editing Profile: Verizon-IPCC
General
Hold Support
None
RFC2543 - c=0.0.0.0
RFC3264 - a=sendonly
180 Handling
None SDP No SDP
181 Handling
None SDP No SDP
182 Handling
None SDP No SDP
183 Handling
None SDP No SDP
Refer Handling
3xx Handling
Diversion Header Support
Delayed SDP Handling
T.38 Support
URI Scheme
SIP TEL ANY
Via Header Format
RFC3261
RFC2543
Next

Default values can also be used for the next two windows that appear. Click **Next** to continue.

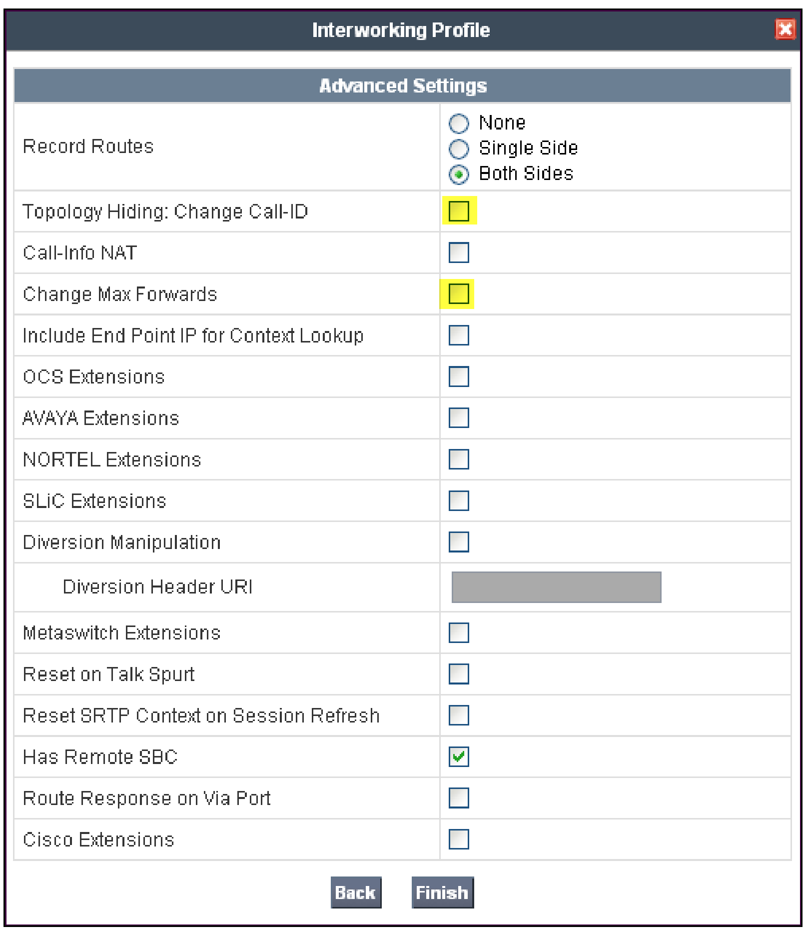




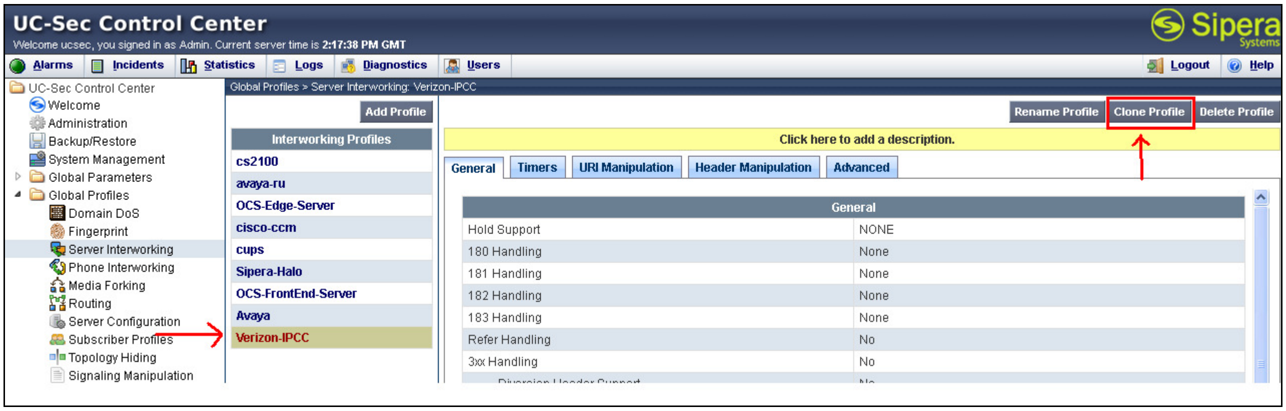
On the **Advanced Settings** window uncheck the following default settings:

- **Topology Hiding: Change Call-ID**
- **Change Max Forwards**

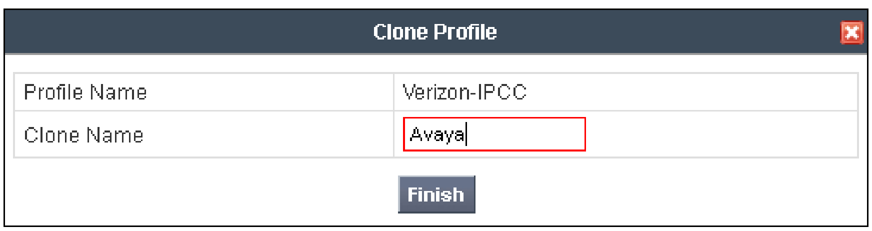
Click **Finish** to save changes.



The ***Avaya*** profile will be created by cloning the ***Verizon*** profile created in the previous section. To clone a Server Interworking Profile, navigate to **UC-Sec Control Center →Global Profiles → Server Interworking** and click on the previously created profile (e.g., ***Verizon-IPCC***), then click on **Clone Profile** as shown below.



Enter a descriptive name for the new profile and click **Finish** to save the profile.



7.3.4 Signaling Manipulation

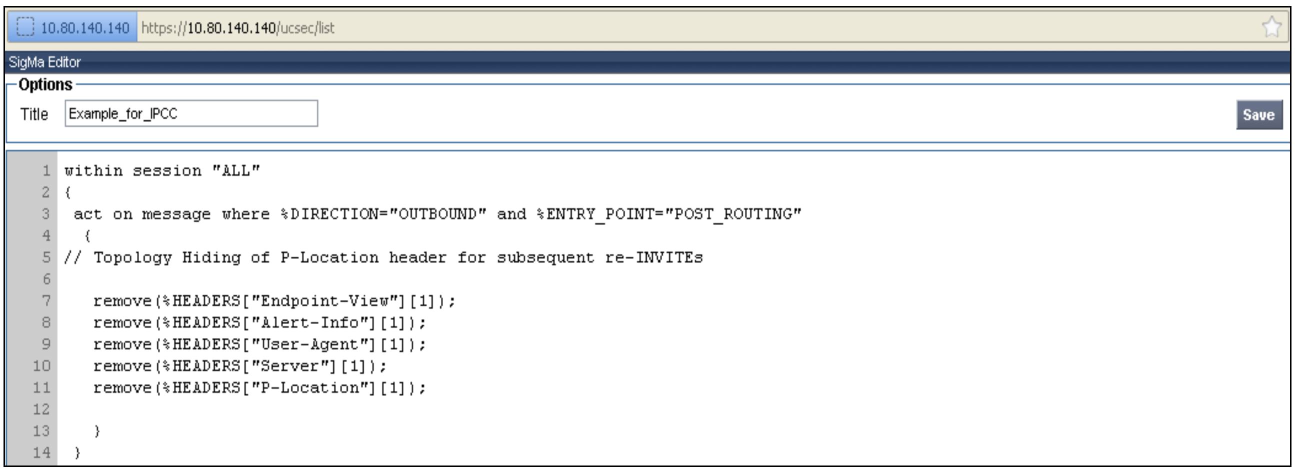
The **Signaling Manipulation** feature allows the ability to add, change or delete any of the headers in a SIP message. This feature will add the ability to configure such manipulation in a highly flexible manner using a proprietary scripting language called SigMa.

The SigMa scripting language is designed to express any of the SIP header manipulation operations to be done by the Avaya SBCE. Using this language, a script can be written and tied to a given flow through the EMS GUI. The Avaya SBCE appliance then interprets this script at the given entry point or "hook point".

These Application Notes will not discuss the full feature of the Signaling Manipulation but will show an example of a script created during compliance testing to aid in topology hiding and to remove unwanted headers in the SIP messages to and from Verizon. To create a new Signaling Manipulation, navigate to **UC-Sec Control Center →Global Profiles → Signaling Manipulation** and click on **Add Script** (not shown). A new blank SigMa Editor window will pop up. The script will act on all outbound traffic to Verizon after the SIP message has been routed through the Avaya SBCE. The script is further broken down as follows:

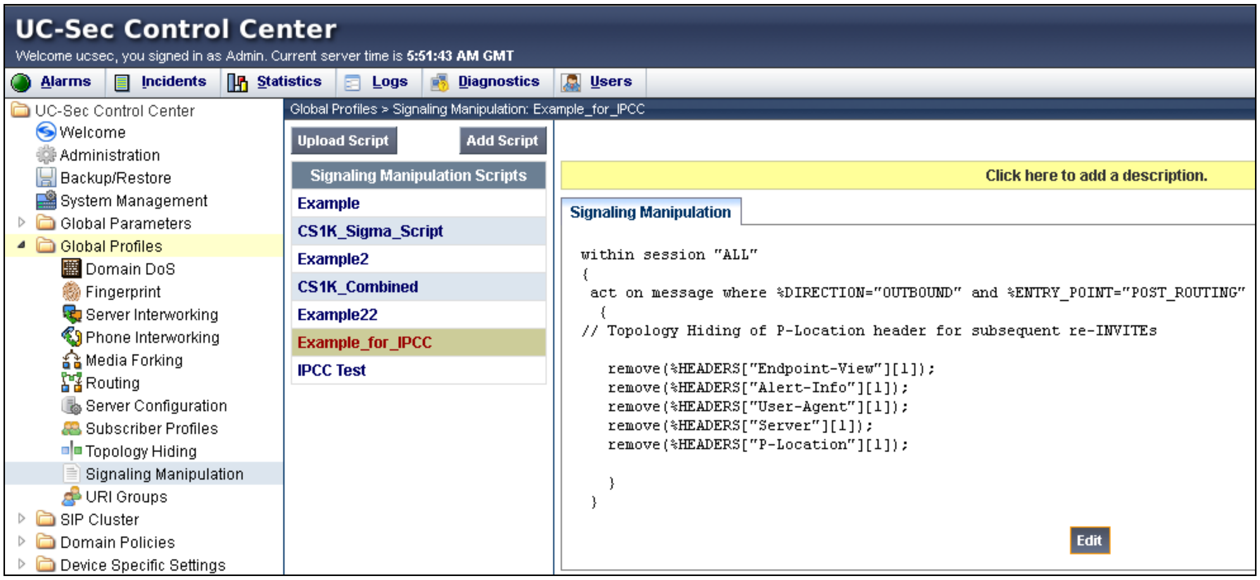
- **within session “All”** Transformations applied to all SIP sessions.
- **act on message** Actions to be taken to any SIP message.
- ***%*DIRECTION=“OUTBOUND”** Applied to a message leaving the Avaya SBCE.
- ***%*ENTRY_POINT=“POST_ROUTING”** The “hook point” to apply the script after the SIP message has routed through the Avaya SBCE.
- **Remove(%HEADERS[“Alert-Info”][1]);** Used to remove an entire header. The first dimension denotes which header while the second dimension denotes the 1st instance of the header in a message**.**

With this script, the Endpoint-View, Alert-Info, User-Agent, Server, and P-Location headers will be removed.



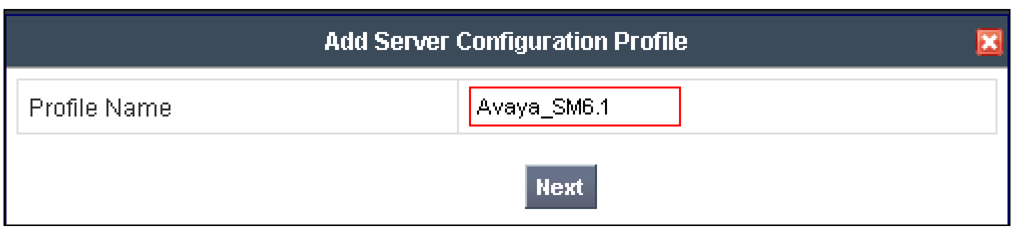
Click **Save**.

The following screen shows the finished Signaling Manipulation Script ***Example_for_IPCC***. This script will later be applied to the Verizon Service Director and Service Host in the **Server Configuration** in **Section 7.3.5**. The details of these script elements can be found in **Appendix A**.



7.3.5 Server Configuration

Servers are defined for each server connected to the Avaya SBCE. In this case, Verizon is connected as the Trunk Server and Session Manager is connected as the Call Server. To define the Session Manager, navigate to **Global Profiles → Server Configuration** in the **UC-Sec Control Center** menu on the left hand side. Click on **Add Profile** and enter details in the pop-up menu.

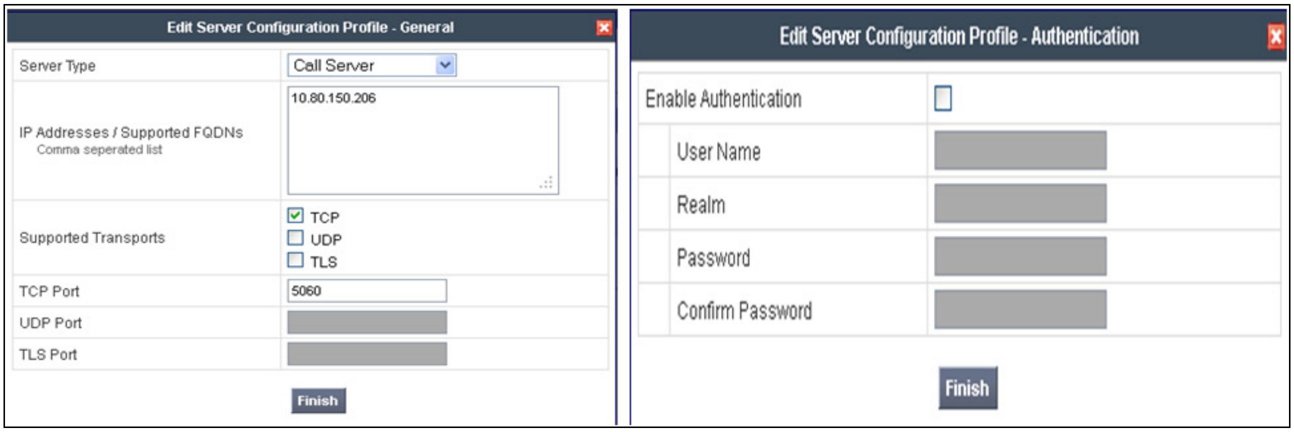


In the new window that appears, enter the following values. Use default values for all remaining fields:

- **Server Type:** Select ***Call Server*** from the drop-down box.
- **IP Addresses / Supported FQDNs:** Enter the IP address of the Session Manager signaling interface. This should match the IP address of the Session Manager Security Module
- **Supported Transports:** Select ***TCP***. This is the transport protocol used in the Avaya SBCE Entity Link on Session Manager **Section 6.5**
- **TCP Port:** Port number on which to send SIP requests to Session Manager. This should match the port number used in the Avaya SBCE Entity Link on Session Manager in **Section 6.5.**

Click **Next** to continue.

Verify **Enable Authentication** is unchecked as Session Manager does not require authentication. Click **Next** to continue.



In the new window that appears, enter the following values. Use default values for all remaining fields:

- **Enabled Heartbeat:** Checked.
- **Method:** Select ***OPTIONS*** from the drop-down box.
- **Frequency:** Choose the desired frequency in seconds the Avaya SBCE will send SIP OPTIONS. For compliance testing ***60*** seconds was chosen.
- **From URI:** Enter an URI to be sent in the FROM header for SIP OPTIONS.
- **TO URI:** Enter an URI to be sent in the TO header for SIP OPTIONS.

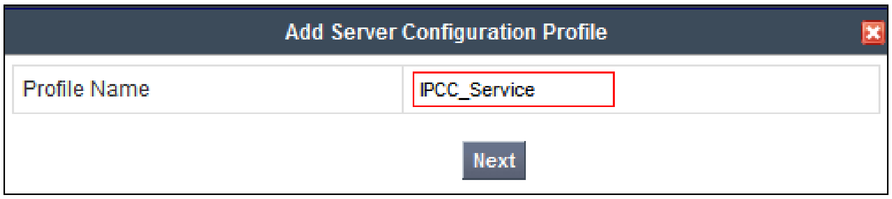
Click **Next** to continue.

In the new window that appears, select the **Interworking Profile** created for the enterprise in **Section 7.3.3**. For **Signaling Manipulation Script**, select a script if desired. Use default values for all remaining fields. Click **Finish** to save the configuration.

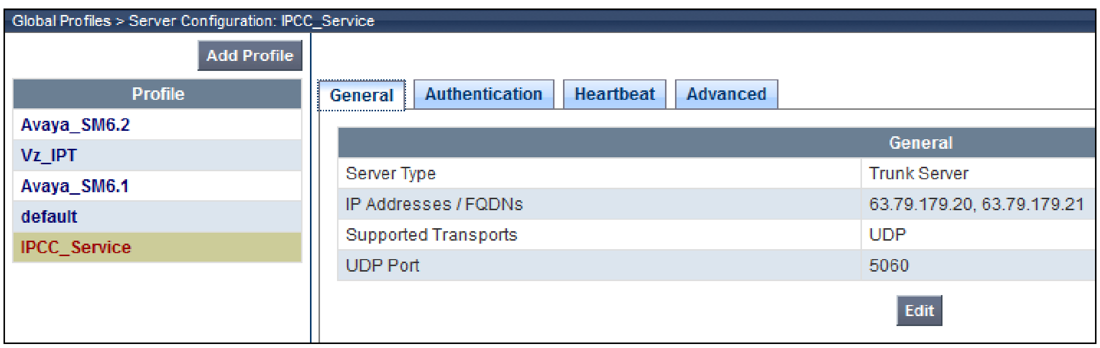
7.3.6 Server Configuration for Verizon IPCC

In the Routing Profile created in **Section 7.3.1**, there were two IP addresses configured for one routing profile. In the **Server Configuration** section both of these addresses will be configured.

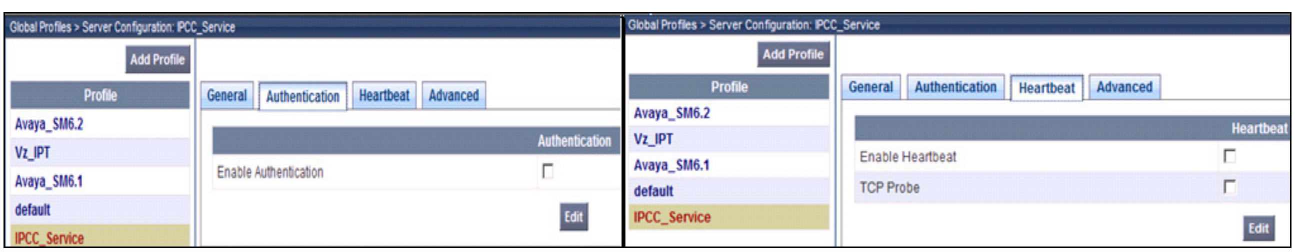
To define the Verizon Service Director and Service Host, navigate to **Global Profiles → Server Configuration** in the **UC-Sec Control Center** menu on the left hand side. Click on **Add Profile** and repeat the instructions above with the displayed values.



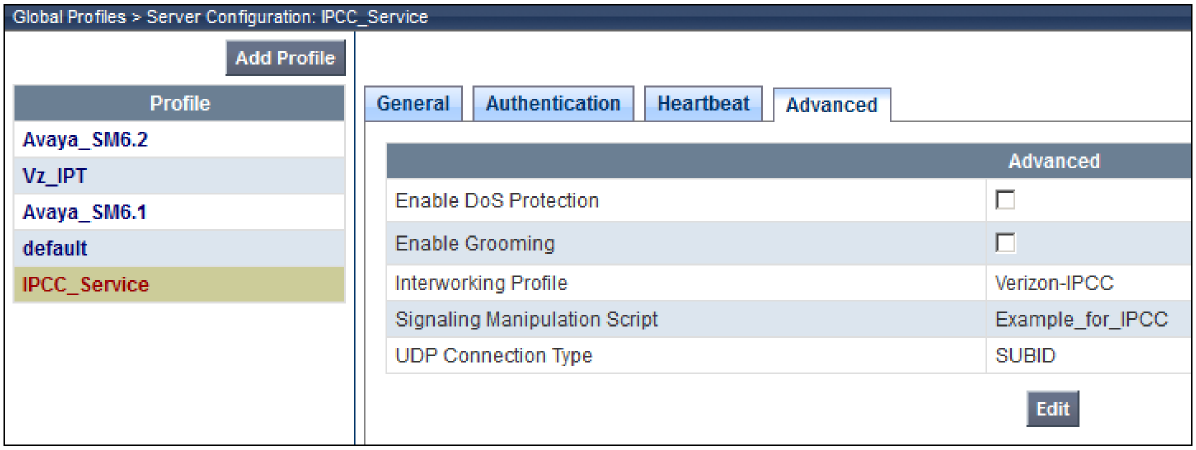
General Properties, using ***Trunk Server*** with both IP Addresses listed (Service Host and Service Director):



Authentication and **Heartbeat** tabs were left at defaults (notice that external OPTIONS are not enabled since they are not used in this configuration):



Configure the **Advanced Tab** by selecting ***Verizon -IPCC*** for **Internetworking Profile** and ***Example_for_IPCC*** as the **Signaling Manipulation Script**:

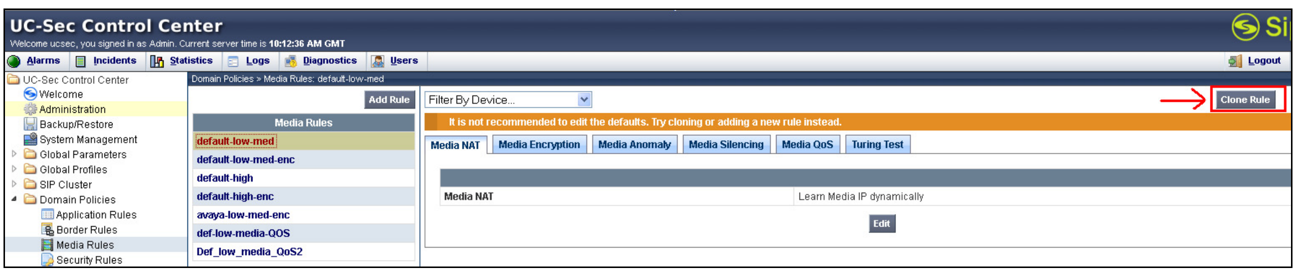


Click **Finish** to save changes (not shown).

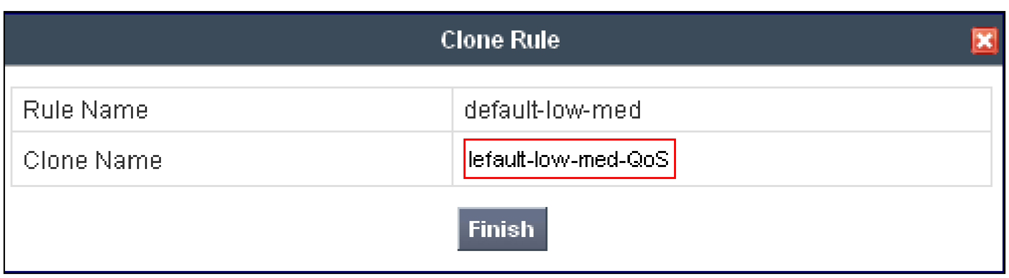
7.4. Domain Policies – Media Rules

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

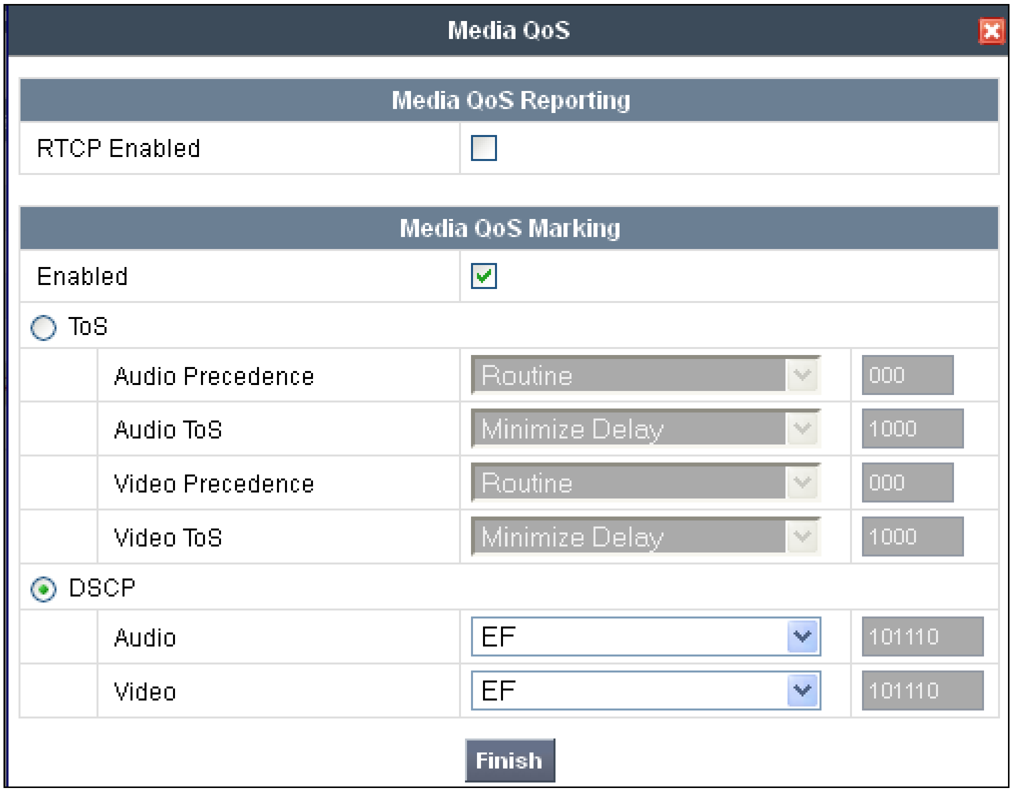
In the sample configuration, a single media rule was created by cloning the default rule called **default-low-med**. Select the **default-low-med** rule and click the **Clone Rule** button.



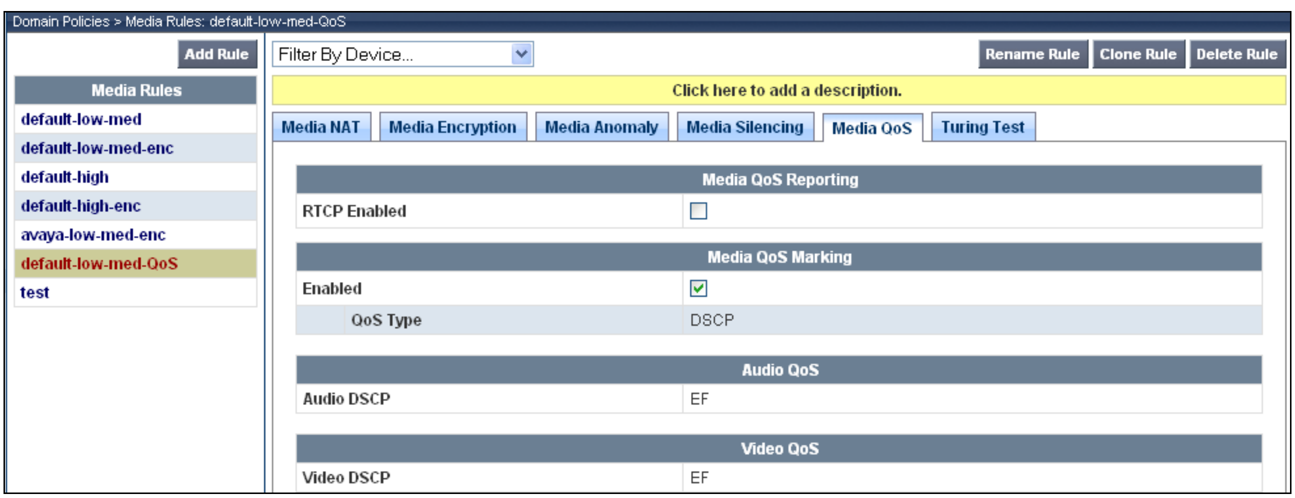
Enter a name in the **Clone Name** field, such as ***default-low-med-QoS*** as shown below. Click **Finish**.



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**.

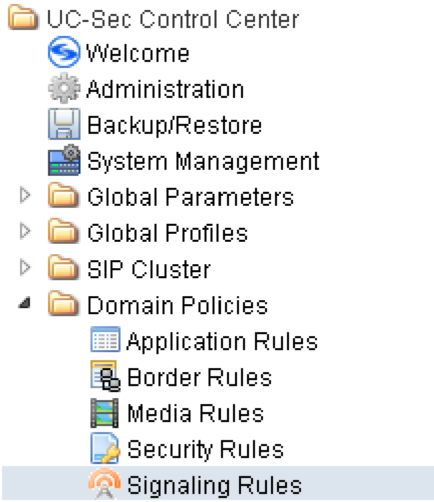


When configuration is complete, the ***default-low-med-QoS*** media rule's **Media QoS** tab appears as follows.

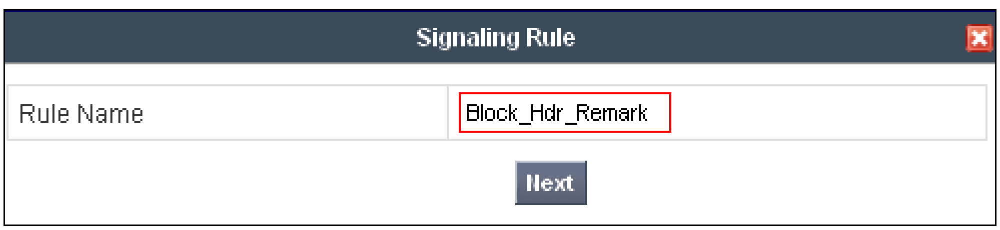


7.5. Domain Policies – Signaling Rules

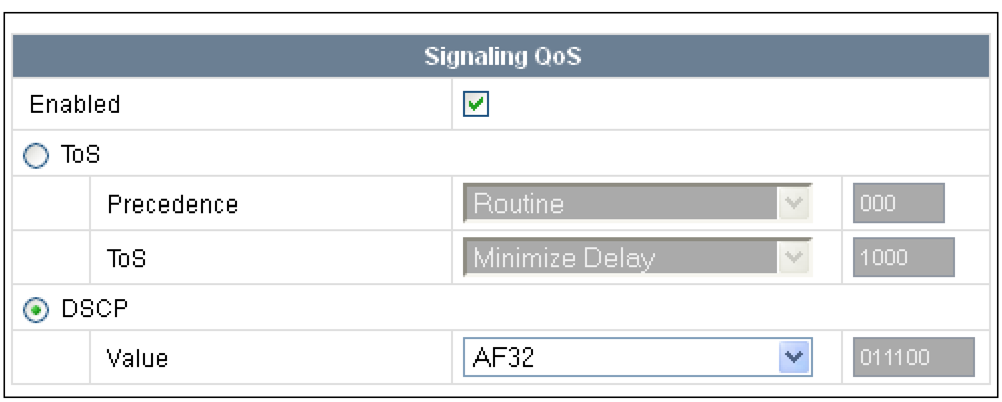
Select **Domain Policies → Signaling Rules** from the left-side menu as shown below.



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).

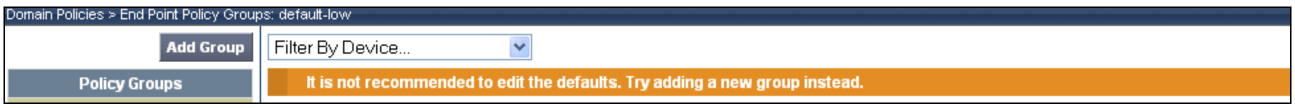


After this configuration, the new ***Block_Hdr_Remark*** will appear as follows.

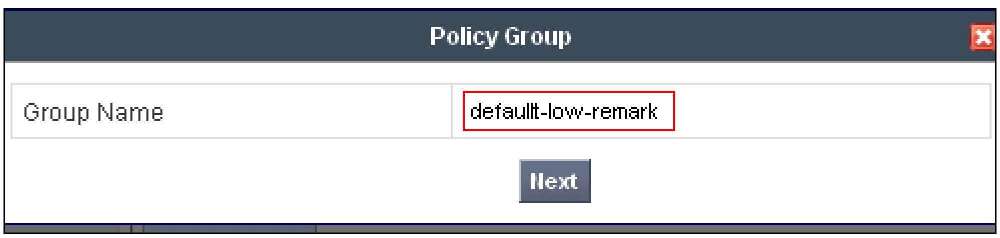
7.6. Domain Policies – End Point Policy Groups

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

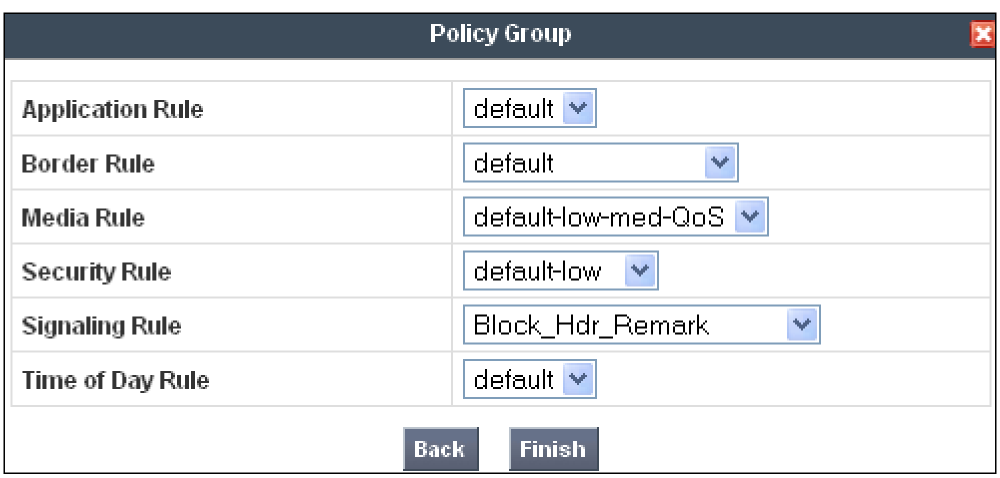
Select the **Add Group** button.



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



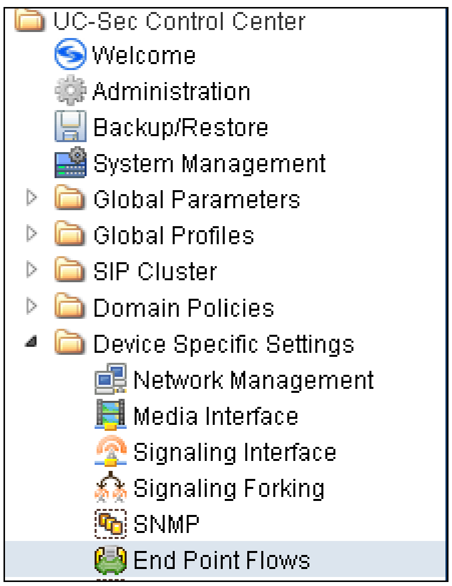
In the sample configuration, defaults were selected for all fields, with the exception of the **Media Rule** which was set to ***default-low-med-QoS***, and the **Signaling Rule**, which was set to ***Block_Hdr_Remark*** as shown below. The selected non-default media rule and signaling rule were created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



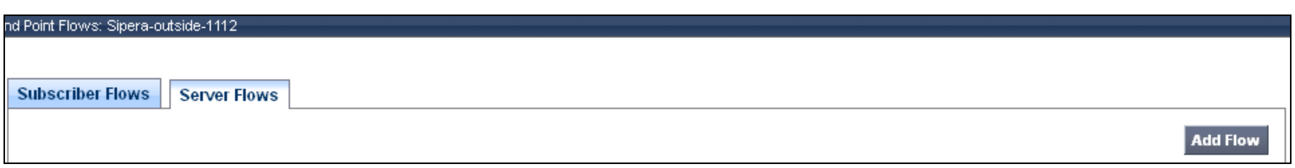
Once configuration is completed, the ***default-low-remark*** policy group will appear as follows.

7.7. Device Specific Settings – End Point Flows

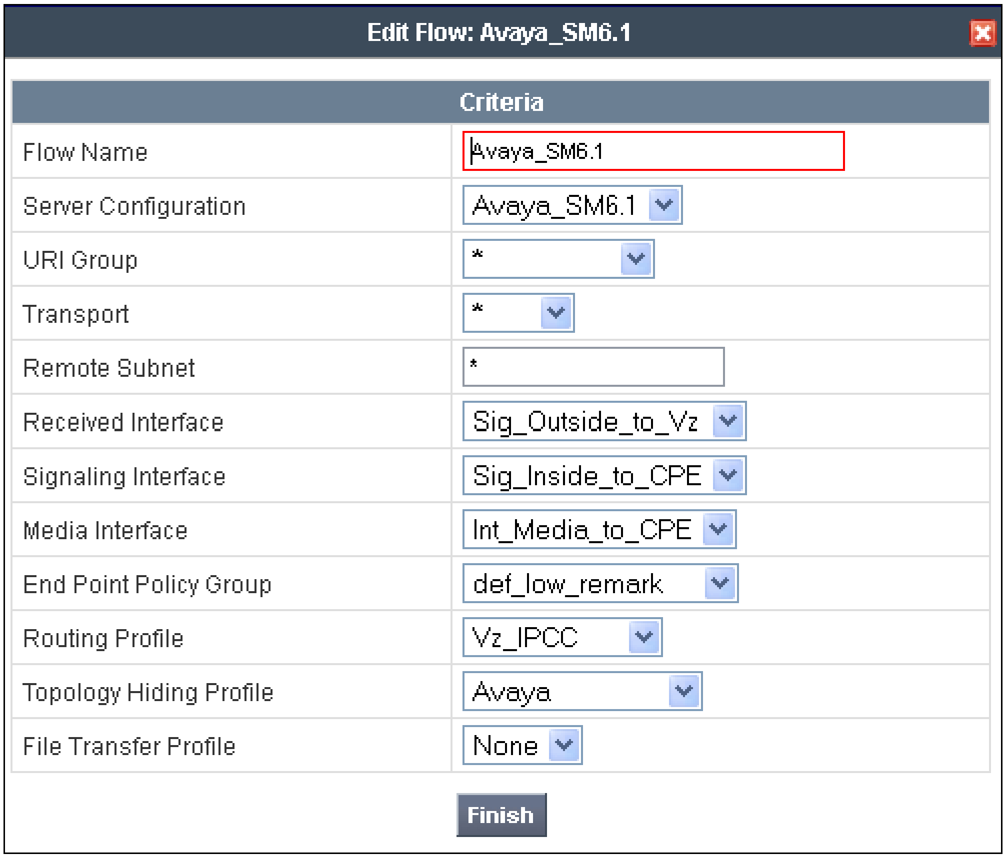
Select **Device Specific Settings → End Point Flows** from the left-side menu as shown below.



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

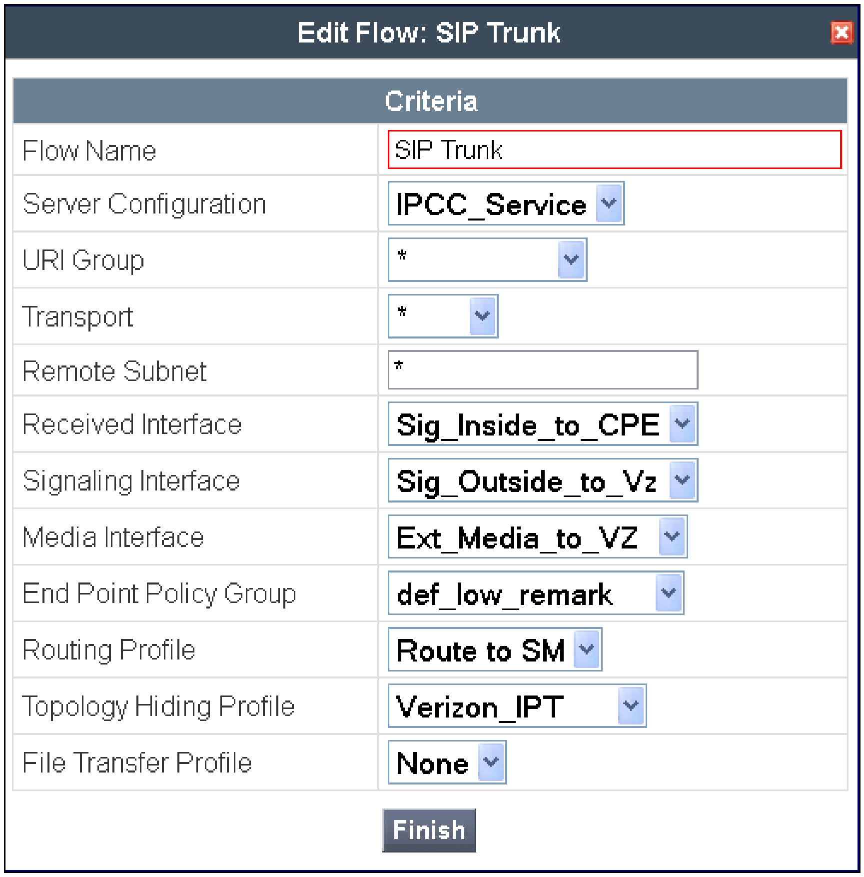


The following screen shows the flow named ***Avaya_SM6.1*** being added to the sample configuration. This flow uses the interfaces, policies, and profiles defined in previous sections. Click **Finish**.

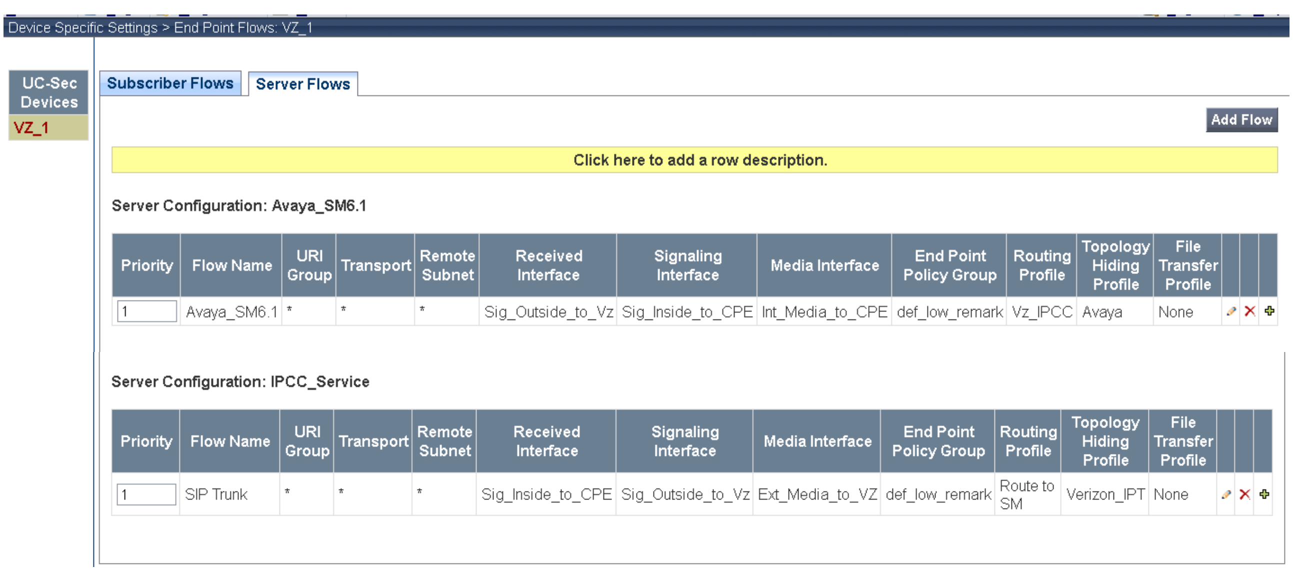


Once again, select the **Server Flows** tab. Select **Add Flow**.

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



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



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_SM6.1	*	*	*	Sig_Outside_to_Vz	Sig_Inside_to_CPE	Int_Media_to_CPE	def_low_remark	Vz_IPCC	Avaya	None

Priority	Flow Name	URI Group	Transport	Remote Subnet	Received Interface	Signaling Interface	Media Interface	End Point Policy Group	Routing Profile	Topology Hiding Profile	File Transfer Profile
1	SIP Trunk	*	*	*	Sig_Inside_to_CPE	Sig_Outside_to_Vz	Ext_Media_to_VZ	def_low_remark	Route to SM	Verizon_IPT	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 Dedicated Internet Access (IDA) T1 connection. Verizon Business provided all of the necessary service provisioning.

9. Verification Steps

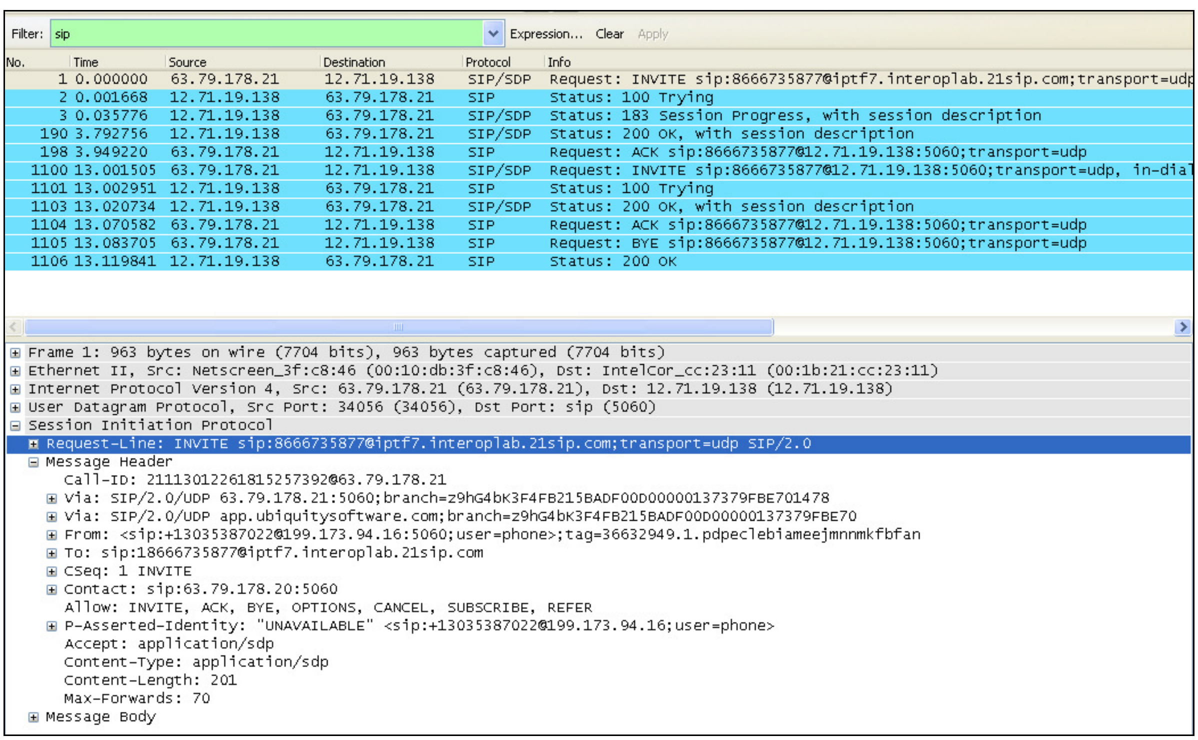
This section provides example verifications of the sample configuration illustrated in these Application Notes.

9.1. Communication Manager and Wireshark Trace Call Verifications

This section illustrates verifications using Communication Manager and Wireshark to illustrate key SIP messaging and call flows.

9.1.1 Wireshark Example of Incoming Call from PSTN via Verizon IPCC

Incoming toll-free 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 5060. On Communication Manager, the incoming call arrives via signaling group 5 and trunk group 5.



The following abridged and annotated Communication Manager **list trace** trace output shows a call incoming on trunk group 5. The PSTN telephone 3035387022 dialed 866-674-7056. Session Manager can map the number received from Verizon to the extension of a Communication Manager telephone (x7689), or the incoming call handling table for trunk group 5 can do the same. In the trace below, Communication Manager receives the DID of 866-674-7056 and translates that to local extension 7689.

```
list trace tac *105                                                    Page   1
                                LIST TRACE
time            data

17:39:29 TRACE STARTED 06/20/2012 CM Release String cold-00.1.510.1-19528
/* Incoming call arrives to Communication Manager for DID 8666747056 */
17:39:37 SIP<INVITE sip: 8666747056@avayalab.com;transport=tcp SIP/2.
17:39:37 SIP<0
17:39:37     Call-ID: 1137110669543718452@63.79.178.21
17:39:37     active trunk-group 5 member 249    cid 0x1aa
/* Communication Manager sends 183 with SDP as a result of TG 5 configuration */
17:39:37 SIP>SIP/2.0 183 Session Progress
17:39:37     Call-ID: 1137110669543718452@63.79.178.21
/* Communication Manager translates the DID to extension 7689   */
17:39:37     dial 7689
17:39:37     ring station      7689 cid 0x1aa
/* G450 Gateway at 10.80.140.15, ringback tone heard by caller */
17:39:37     G729A ss:off ps:20
             rgn:1 [10.80.140.40]:32670
             rgn:1 [10.80.140.15]:16394
17:39:37     G729 ss:off ps:20
             rgn:1 [10.80.140.141]:35020
             rgn:1 [10.80.140.15]:16386
17:39:37     xoip options: fax:off modem:off tty:US  uid:0x50107
             xoip ip: [10.80.140.15]:16386
/* User Answers call, Communication Manager sends 200 OK */
17:39:42 SIP>SIP/2.0 200 OK
17:39:42     Call-ID: 1137110669543718452@63.79.178.21
17:39:42     active station      7689 cid 0x1aa
/* Communication Manager receives ACK to 200 OK */
17:39:42 SIP<ACK sip: 8666747056@10.80.140.22;transport=tcp SIP/2.0
17:39:42     Call-ID: 1137110669543718452@63.79.178.21
/* Communiction Manager Extension terminates the call      */
17:39:44 SIP>BYE sip:10.80.140.141:5060;transport=tcp SIP/2.0
17:39:44     Call-ID: 1137110669543718452@63.79.178.21
17:39:44     idle station      7689 cid 0x1aa
```

9.1.2 Example Incoming Call Referred with UUI to Alternate SIP Destination

The following Communication Manager **list trace vector** trace output shows a different example of an incoming Verizon toll-free call. The call was routed to a Communication Manager vector directory number (VDN 3690) associated with a call vector (call vector 5). As in previous illustrations, this vector will answer the call, play an announcement to the caller, and then use a "route-to" step to cause a REFER message to be sent to Verizon. In this case, the Refer-To number will cause Verizon to route the call to another SIP-connected destination. In the sample configuration, where only one site is available, this was tested by including a different IP Toll Free number (1866-674-7056) assigned to the same site in the Route-To step in the vector. The vector also sets UUI data that will be included in the Refer-To header. When Verizon originates a new call to the "alternate" destination, the INVITE message sent by Verizon will contain a User-To-User header containing the UUI data originally sent by the referring site in the Refer-To header. In practice, this would allow Communication Manager at one site to pass call or customer-related data to another site via the Verizon network.

```
list trace tac *105                                                 Page   1
                                    LIST TRACE
time            data
17:27:13 TRACE STARTED 06/20/2012 CM Release String cold-00.1.510.1-19528
/* Inbound call arrives to DID 8666747057 -- VDN 7690 associated with vector 5 */
17:27:40 SIP<INVITE sip:8666747057@avayalab.com;transport=tcp SIP/2.
17:27:40 SIP<0  Call-ID: -2087842424-449653436@63.79.178.21
17:27:40     active trunk-group 5 member 249    cid 0x1a5
17:27:40    0  0 ENTERING TRACE cid 421
17:27:40    5  1 vdn e7690 bsr appl   0 strategy 1st-found override n
/* Steps in vector 5 add UUI */
17:27:40    5  1 set A = none CATR 1234567890123456
17:27:40    5  1      operand    = []
17:27:40    5  1      operand    = [1234567890123456]
17:27:40    5  1      ========= CATR =========
17:27:40    5  1      variable A = [1234567890123456] asaiuui local
17:27:40    5  1      asaiuui chg from [] to [1234567890123456]
17:27:40    5  2 set B = none CATR 7890123456789012
17:27:40    5  2      operand    = []
17:27:40    5  2      operand    = [7890123456789012]
17:27:40    5  2      ========= CATR =========
17:27:40    5  2      variable B = [7890123456789012] asaiuui local
17:27:40    5  2      asaiuui chg from [] to [7890123456789012]
17:27:40    5  3 wait 2 secs hearing ringback
17:27:40 SIP>SIP/2.0 183 Session Progress
17:27:40     Call-ID: -2087842424-449653436@63.79.178.21
17:27:40     dial 7690
17:27:40     ring vector 5      cid 0x1a5
17:27:40     G729 ss:off ps:20
             rgn:1 [10.80.140.141]:35012
             rgn:1 [10.80.140.15]:16390
17:27:42    5  4 # Play announcement to answer c...
17:27:42    5  5 announcement 7697
17:27:42 SIP>SIP/2.0 183 Session Progress
17:27:42     Call-ID: -2087842424-449653436@63.79.178.21
17:27:42    5  5      announcement: board 001V9 ann ext: 7697
/* Pre-refer announcement answers call,200 OK sent to Verizon */
17:27:42 SIP>SIP/2.0 200 OK
17:27:42     Call-ID: -2087842424-449653436@63.79.178.21
17:27:42     hear annc board 001V9 ext 7697 cid 0x1a5
17:27:42 SIP<ACK sip:10.80.140.22;transport=tcp SIP/2.0
17:27:42     Call-ID: -2087842424-449653436@63.79.178.21
17:27:49     idle announcement       cid 0x1a5
/* Announcement completes, route-to step executes and REFER (with UUI) is sent */
17:27:49    5  6 route-to number ~r+18666747056 cov n if unconditionally
17:27:49 SIP>REFER sip:10.80.140.141:5060;transport=tcp SIP/2.0
17:27:49     Call-ID: -2087842424-449653436@63.79.178.21
/* Communication Manager receives 202 Accepted for the REFER */
17:27:49 SIP<SIP/2.0 202 Accepted
17:27:49     Call-ID: -2087842424-449653436@63.79.178.21
/* Verizon sends re-INVITE with c=0.0.0.0 SDP */
17:27:49 SIP<INVITE sip:10.80.140.22;transport=tcp SIP/2.0
17:27:49     Call-ID: -2087842424-449653436@63.79.178.21
17:27:49 SIP>SIP/2.0 100 Trying
17:27:49     Call-ID: -2087842424-449653436@63.79.178.21
17:27:49 SIP>SIP/2.0 200 OK
17:27:49     Call-ID: -2087842424-449653436@63.79.178.21
17:27:50 SIP<ACK sip:8776735877@10.80.140.22;transport=tcp SIP/2.0
/* Communication Manager receives SIP NOTIFY with sipfrag 200 OK,agent answered */
17:27:50 SIP<NOTIFY sip:8776735877@10.80.140.22;transport=tcp SIP/2.
17:27:50 SIP<0  Call-ID: -2087842424-449653436@63.79.178.21
17:27:50 SIP>SIP/2.0 200 OK
17:27:50     Call-ID: -2087842424-449653436@63.79.178.21
17:27:56 SIP<NOTIFY sip:10.80.140.22;transport=tcp SIP/2.0
17:27:56     Call-ID: -2087842424-449653436@63.79.178.21
17:27:56 SIP>SIP/2.0 200 OK
17:27:56     Call-ID: -2087842424-449653436@63.79.178.21
17:27:56    5  6 LEAVING VECTOR PROCESSING cid 421
17:27:56 SIP>BYE sip:10.80.140.141:5060;transport=tcp SIP/2.0
17:27:56     idle vector 0      cid 0x1a5
```

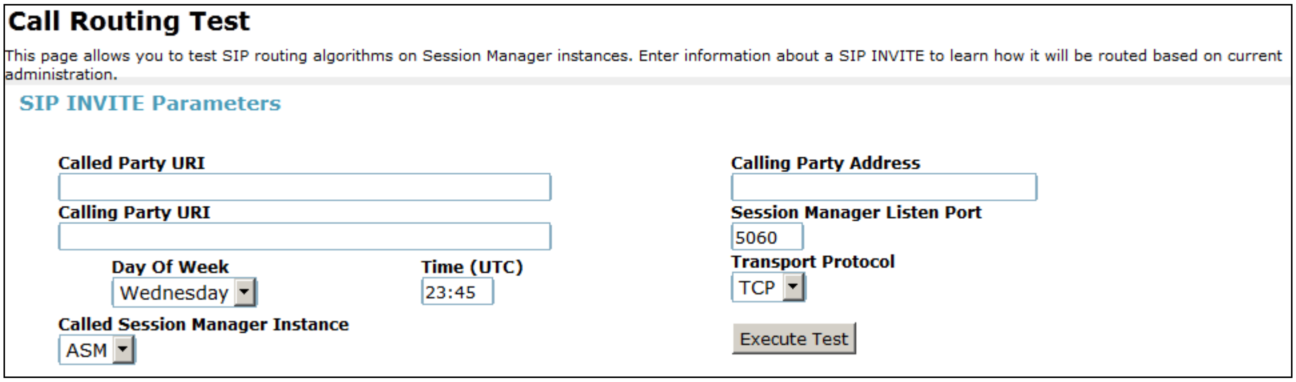
9.2. System Manager and Session Manager Verifications

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

9.2.1 Call Routing Test

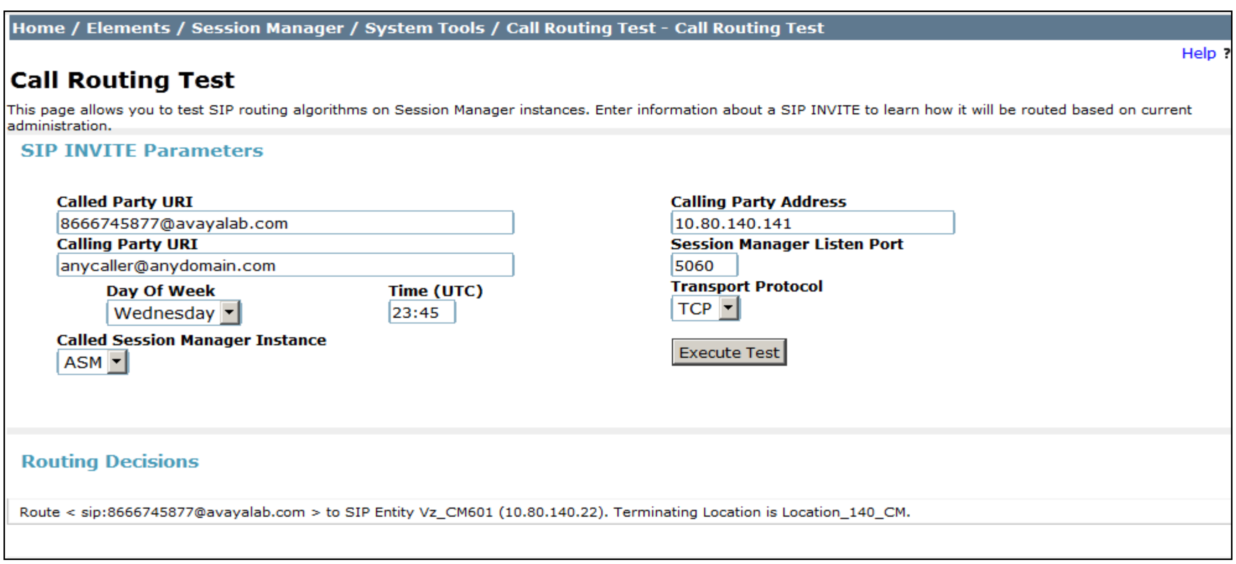
The Call Routing Test verifies the routing for a particular source and destination. To run the call routing test, expand **Elements → Session Manager → System Tools → Call Routing Test**, as shown below.

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 toll-free call from the PSTN to the enterprise via the Avaya SBCE (***10.80.140.141***). Under **Routing Decisions**, observe that the call will route to Communication Manager using the SIP entity named ***Vz_CM601***. The digits are manipulated such that the Verizon toll-free number (i.e., 866-674-5877) is converted to a Communication Manager extension by the Communication Manager **incoming-call-handling-treatment-trunk-group** form. Scroll down to inspect the details of the **Routing Decision Process** if desired (not shown).



Below is an example of an active call.

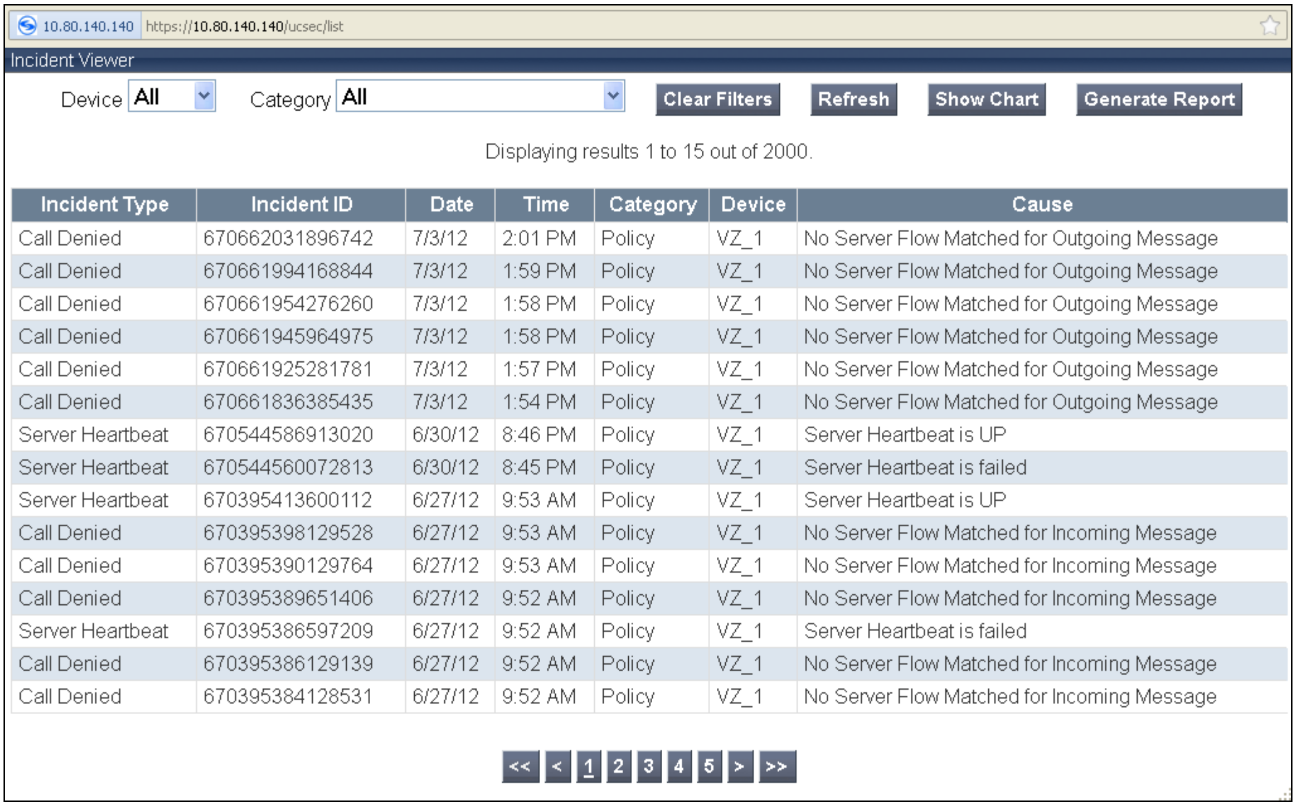
```
status trunk 5

                              TRUNK GROUP STATUS

Member   Port     Service State      Mtce Connected Ports
                                     Busy

0001/001 T00001   in-service/active  no   S00000
0001/002 T00002   in-service/idle    no
0001/003 T00003   in-service/idle    no
0001/004 T00004   in-service/idle    no
```

Verify the port returns to **in-service/idle** after the call has ended.

```
status trunk 5

                              TRUNK GROUP STATUS

Member   Port     Service State      Mtce Connected Ports
                                     Busy

0001/001 T00001   in-service/idle    no
0001/002 T00002   in-service/idle    no
0001/003 T00003   in-service/idle    no
0001/004 T00004   in-service/idle    no
```

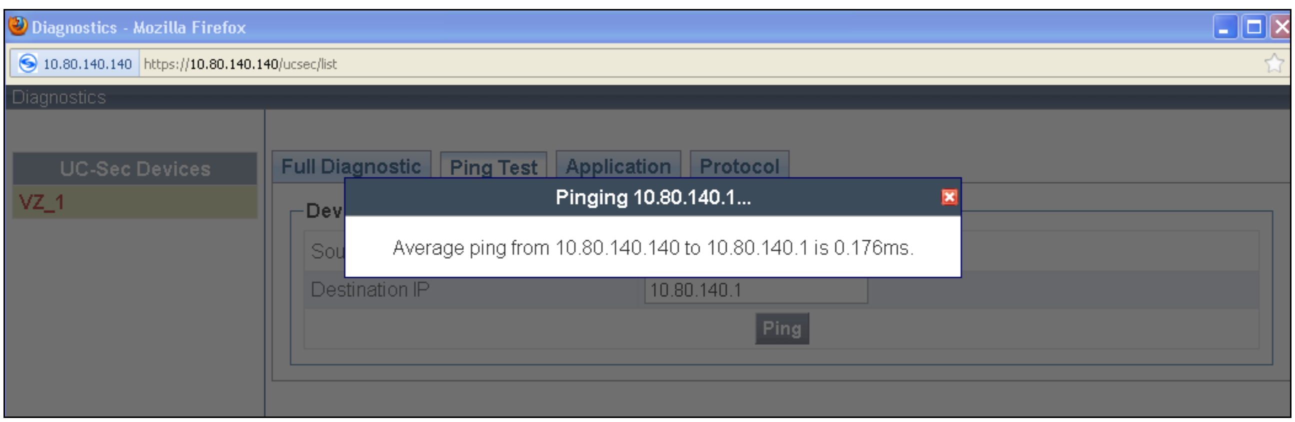
9.3. Troubleshooting

1. Communication Manager:
   - **list trace station** <extension number> - Traces calls to and from a specific station.
   - **list trace tac** <trunk access code number> - Trace calls over a specific trunk group.
   - **status station** <extension number> - Displays signaling and media information for an active call on a specific station.
   - **status trunk** <trunk number> - Displays real-time trunk group status.
2. Session Manager:
   - **traceSM -x -uni** - Session Manager command line tool for traffic analysis. Log in to the Session Manager management interface to run this command.
3. Avaya SBCE:
   - **Incidents** - Displays alerts captured by the UC-Sec appliance.

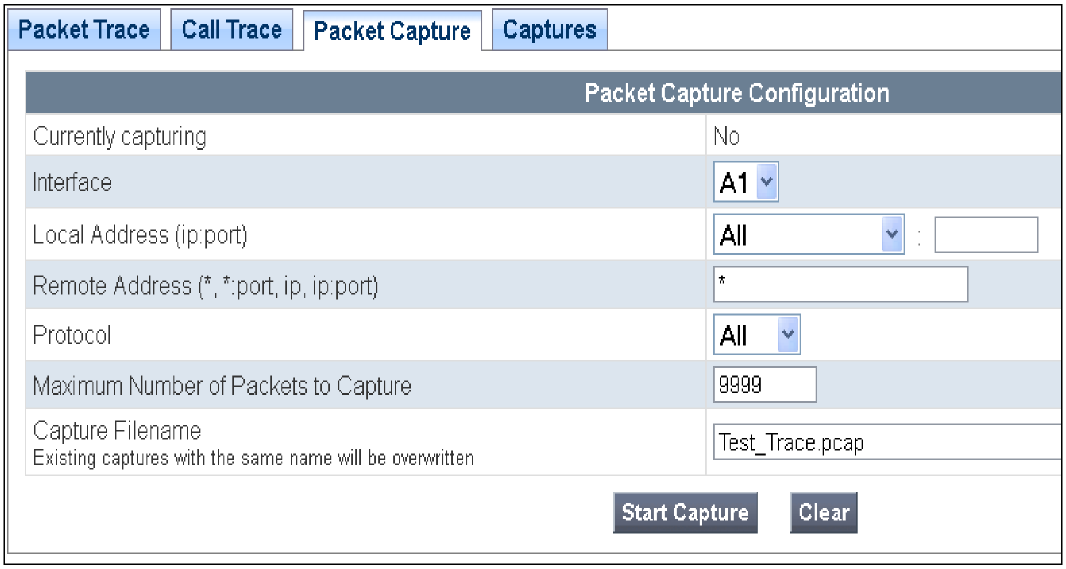


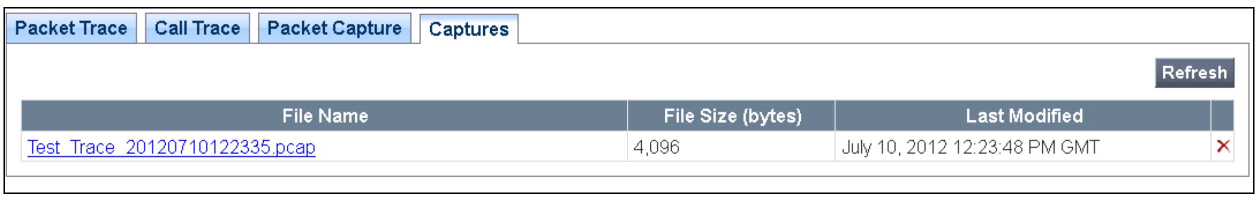
Incident Type	Incident ID	Date	Time	Category	Device	Cause
Call Denied	670662031896742	7/3/12	2:01 PM	Policy	VZ_1	No Server Flow Matched for Outgoing Message
Call Denied	670661994168844	7/3/12	1:59 PM	Policy	VZ_1	No Server Flow Matched for Outgoing Message
Call Denied	670661954276260	7/3/12	1:58 PM	Policy	VZ_1	No Server Flow Matched for Outgoing Message
Call Denied	670661945964975	7/3/12	1:58 PM	Policy	VZ_1	No Server Flow Matched for Outgoing Message
Call Denied	670661925281781	7/3/12	1:57 PM	Policy	VZ_1	No Server Flow Matched for Outgoing Message
Call Denied	670661836385435	7/3/12	1:54 PM	Policy	VZ_1	No Server Flow Matched for Outgoing Message
Server Heartbeat	670544586913020	6/30/12	8:46 PM	Policy	VZ_1	Server Heartbeat is UP
Server Heartbeat	670544560072813	6/30/12	8:45 PM	Policy	VZ_1	Server Heartbeat is failed
Server Heartbeat	670395413600112	6/27/12	9:53 AM	Policy	VZ_1	Server Heartbeat is UP
Call Denied	670395398129528	6/27/12	9:53 AM	Policy	VZ_1	No Server Flow Matched for Incoming Message
Call Denied	670395390129764	6/27/12	9:53 AM	Policy	VZ_1	No Server Flow Matched for Incoming Message
Call Denied	670395389651406	6/27/12	9:52 AM	Policy	VZ_1	No Server Flow Matched for Incoming Message
Server Heartbeat	670395386597209	6/27/12	9:52 AM	Policy	VZ_1	Server Heartbeat is failed
Call Denied	670395386129139	6/27/12	9:52 AM	Policy	VZ_1	No Server Flow Matched for Incoming Message
Call Denied	670395384128531	6/27/12	9:52 AM	Policy	VZ_1	No Server Flow Matched for Incoming Message

- **Diagnostics** - Allows for PING tests and displays application and protocol use.

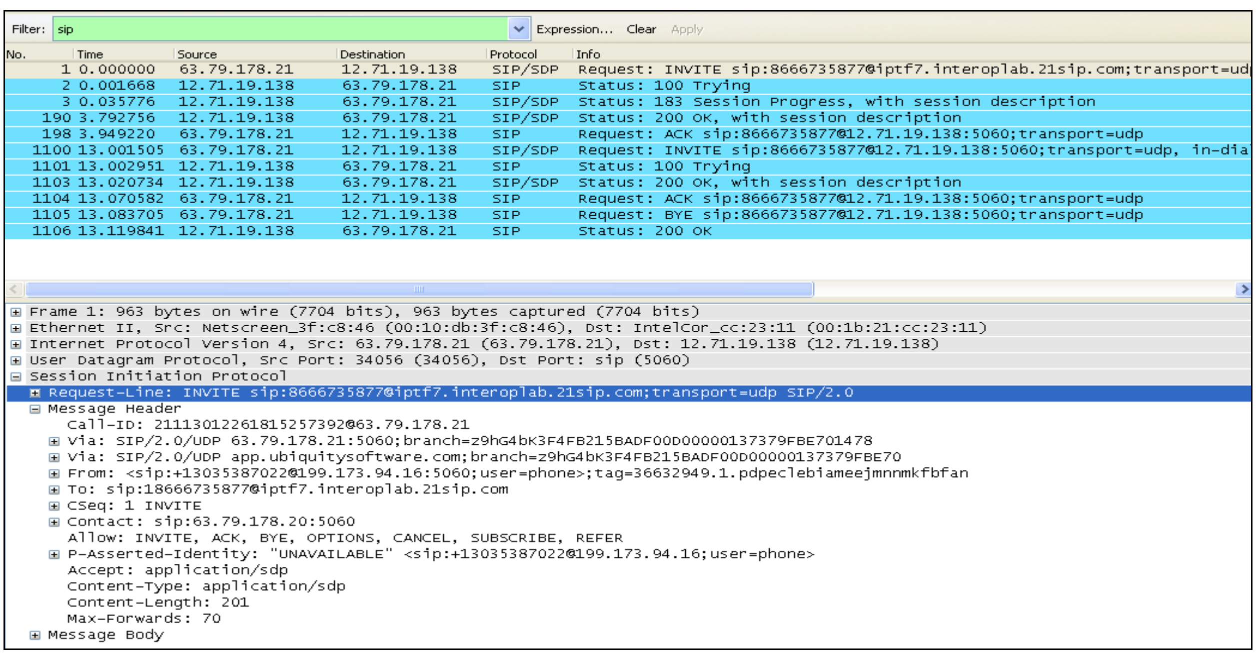


- **Troubleshooting → Trace Settings** - Configure and display call traces and packet captures for the UC-Sec appliance.





The packet capture file can be downloaded and viewed using a Network Protocol Analyzer such as Wireshark:



10. Conclusion

As illustrated in these Application Notes, Avaya Aura® Communication Manager 6.0.1, Avaya Aura® Session Manager 6.1, and Avaya Session Border Controller for Enterprise can be configured to interoperate successfully with Verizon Business IP Contact Center Services IP Toll Free VoIP Inbound service. This solution enables inbound toll free calls over a Verizon Business VoIP Inbound SIP trunk service connection. In addition, these Application Notes further demonstrate that the Avaya Aura® Communication Manager implementation of SIP Network Call Redirection (SIP-NCR) can work in conjunction with Verizon Business IP Contact Center service's implementation of SIP-NCR to support call redirection over SIP trunks inclusive of passing User-User Information (UUI).

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

11. Additional References

11.1. Avaya

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

[1] *Installing and Configuring Avaya Aura™ Communication Manager*, Doc ID 03-603558, Release 6.0 June, 2010 available at http://support.avaya.com/css/P8/documents/100089133

[2] *Administering Avaya Aura™ Communication Manager*, Doc ID 03-300509, Issue 6.0 June 2010 available at http://support.avaya.com/css/P8/documents/100089333

[3] *Administering Avaya Aura® System Platform*, Release 6, June 2010.

[4] *Installing and Upgrading Avaya Aura® System ManagerRelease6.1*, November 2010.

[5] *Installing and Configuring Avaya Aura® Session Manager*, January 2011, Document Number 03-603473

[6] *Administering Avaya Aura® Session Manager,* March 2011, Document Number 03-603324.

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

Appendix A

Included below is the Sigma Script used during the compliance testing.

```
// Verizon

//Remove unwanted headers to assist in topology hiding.

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

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

   }
 }
```

Please e-mail any questions or comments pertaining to these Application Notes along with the full title name and filename, located in the lower right corner, directly to the Avaya DevConnect Program at devconnect@avaya.com.