Avaya Solution & Interoperability Test Lab

Application Notes for Avaya Aura® Communication Manager 6.3, Avaya Aura® Session Manager 6.3, and Avaya Session Border Controller for Enterprise 6.2 with Verizon Business IP Contact Center (IPCC) Services Suite – Issue 1.1

Abstract

These Application Notes describe a sample configuration of Avaya Aura® Communication Manager 6.3, Avaya Aura® Session Manager 6.3, and Avaya Session Border Controller for Enterprise 6.2 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. This service suite 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 Communication Manager. The Communication Manager 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 Communication Manager and 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 Private IP (PIP) 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 6.3, Avaya Aura® Session Manager 6.3, 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. This service suite 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 Communication Manager. The Communication Manager 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 [VZ-IPTF] and [VZ-IP-IVR] with a newer version of Session Manager, Communication Manager, and Avaya SBCE.

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

The Verizon Business IPCC Services suite described in these Application Notes is designed for business customers. The suite 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 Communication Manager can be avoided by requesting that the Verizon network transfer the inbound caller to an alternate destination. In addition, the Communication Manager 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 using Communication Manager.

Verizon Business IPCC Services suite is a portfolio of IP Contact Center (IPCC) interaction services that includes VoIP Inbound and IP Interactive Voice Response (IP IVR). Access to these features may use Internet Dedicated Access (IDA) or Private IP (PIP). PIP was used for the sample configuration described in these Application Notes. VoIP Inbound is the base service offering that offers core call routing and termination features. IP IVR is an enhanced service offering that includes features such as menu-routing, custom transfer, and additional media capabilities.

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 Services. 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 numbers, 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 PIP 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

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

See **Section 3.2** for an overview of key call flows and **Section 9** for detailed verifications and traces illustrating key call flows.

DevConnect Compliance Testing is conducted jointly by Avaya and DevConnect members. The jointly-defined test plan focuses on exercising APIs and/or standards-based interfaces pertinent to the interoperability of the tested products and their functionalities. DevConnect Compliance Testing is not intended to substitute full product performance or feature testing performed by DevConnect members, nor is it to be construed as an endorsement by Avaya of the suitability or completeness of a DevConnect member's solution.

2.1. Interoperability Compliance Testing

The interoperability compliance testing included the execution of test cases details in the Verizon-authored interoperability test plan.

- SIP OPTIONS monitoring of the health of the SIP trunks was verified. Both the Avaya enterprise equipment and Verizon Business can monitor health using SIP OPTIONS.
- Incoming calls from the PSTN were routed to the 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 IPCC 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. The Avaya CPE 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 IPCC with a media attribute “sendonly”. The Verizon 200 OK to this re-INVITE will include media attribute “recvonly”. While the call remains on hold, RTP will flow from the Avaya CPE to Verizon, but no RTP will flow from Verizon to the Avaya CPE (i.e., as intended). When the user resumes the call from hold, bi-directional media path resumes. 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 re-asserted the “sendonly” state.
- 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.

2.2. Test Results

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

- Verizon Business IPCC Services suite does not support fax.
- Verizon Business IPCC Services suite does not support History Info or Diversion Headers. The Avaya CPE will not send History-Info or Diversion header to Verizon IPCC in the sample configuration.
- Verizon Business IPCC Services suite does not support G.729 Annex b. When using G729, the Avaya CPE will always include "annexb=no" in SDP in the sample configuration.
- **Section 3.3.3** summarizes a call flow that would theoretically allow a call to remain in Communication Manager vector processing upon failure of a vector-triggered REFER attempt. However, such call scenarios could not be verified on the production Verizon circuit used for testing. On the production circuit, Verizon would send a BYE to terminate the call upon encountering REFER transfer failures, so there was no opportunity for the call to remain in Communication Manager vector processing. See **Section 3.3.3** for additional information.
- The presence of unnecessary headers such as P-Location in a SIP message to Verizon does not cause any user-perceivable problems. Nevertheless, SBC procedures are shown in **Section 7.7** to illustrate how headers such as P-Location that are not required by Verizon may be removed by the SBC.

2.3. Support

2.3.1 Avaya

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

2.3.2 Verizon

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

3. Reference Configuration

Figure 1 illustrates the sample configuration used for the DevConnect compliance testing. The configuration is comprised of the Avaya CPE location connected via a T1 Internet connection to the Verizon Business IPCC service node. The Avaya CPE location simulates a customer site. At the edge of the Avaya CPE location is an Avaya Session Border Controller for Enterprise. The Avaya SBCE receives traffic from the Verizon Business IPCC Services on port 5060 and sends traffic to the Verizon Business IPCC Services using destination port 5072, using UDP for transport. The PIP service defines a secure MPLS connection between the Avaya CPE T1 connection and the Verizon IPCC service node.

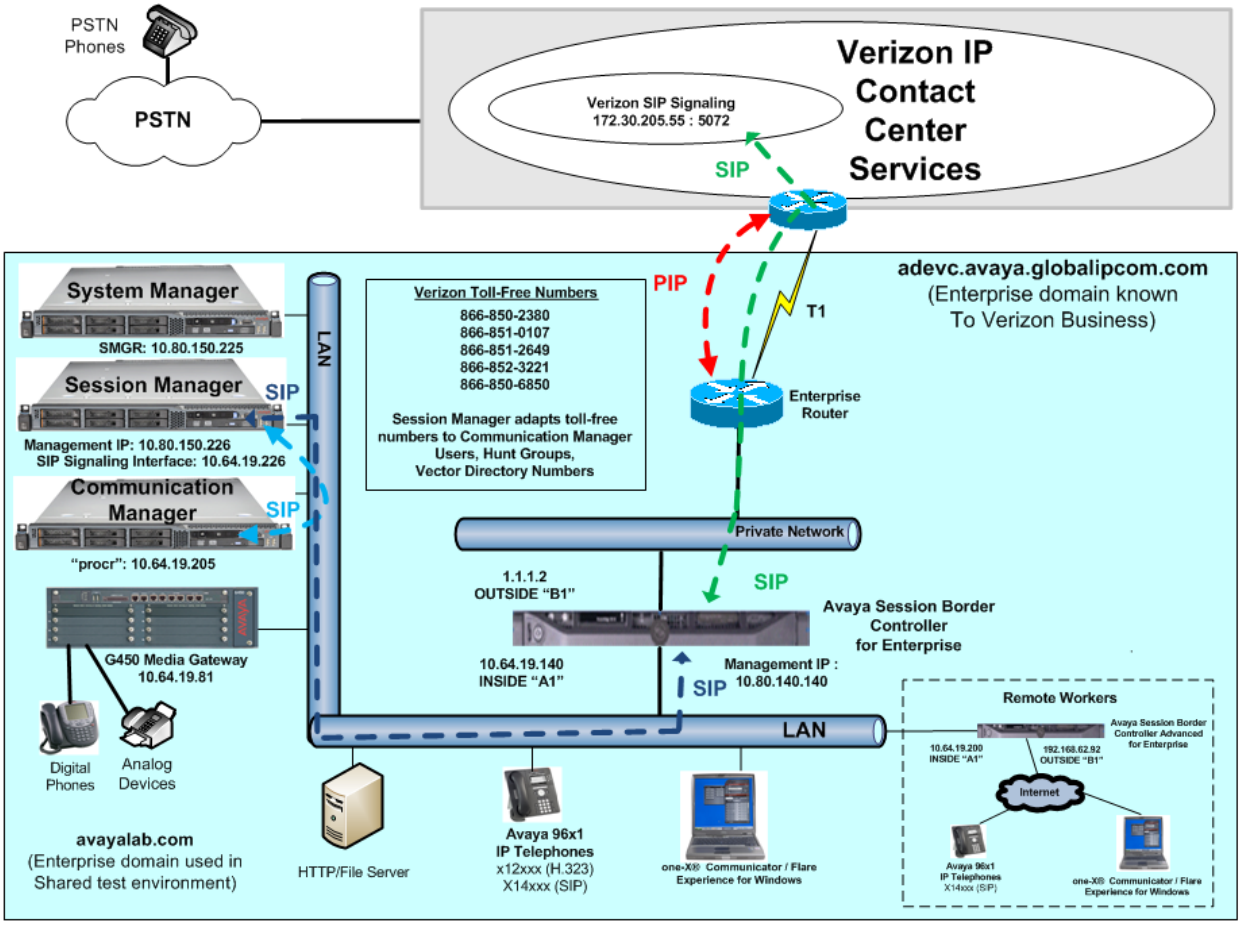


Figure 1: Avaya Interoperability Test Lab Configuration

The Verizon 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.

The Avaya CPE environment was known to Verizon Business IPCC Service as FQDN *adevc.avaya.globalipcom.com*. For efficiency, the Avaya CPE environment utilizing Session Manager Release 6.3 and Communication Manager Release 6.3 was shared among other ongoing test efforts at the Avaya Solutions and Interoperability Test lab. Access to the Verizon Business IPCC services was added to a configuration that already used domain “avayalab.com” at the enterprise. As such, the Avaya SBCE is used to adapt the domains as needed. These Application Notes indicate the configuration that would not be required in cases where the CPE domain in Communication Manager and Session Manager match the CPE domain known to Verizon.

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

- Verizon Business IPCC Services node sends the following in the initial INVITE to the CPE:
    - The CPE FQDN of ***adevc.avaya.globalipcom.com*** in the Request URI.
    - The Verizon IPCC Services gateway IP address in the From header.
    - The enterprise SBC outside IP address (i.e., 1.1.1.2) 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 contains ***avayalab.com.***
    - The host portion of the From header and PAI header contains ***avayalab.com***
    - The host portion of the To header contains ***avayalab.com***
    - Sends the packet to Session Manager using destination port 5060 via TCP
- Session Manager sends Communication Manager
    - The Request URI contains ***avayalab.com***, to match the shared Avaya SIL test environment.
    - Sends the packet to Communication Manager using destination port 5071 via TLS to allow Communication Manager to distinguish Verizon traffic from other traffic arriving from the same instance of Session Manager.

Note – The Fully Qualified Domain Names and IP addressing specified in these Application Notes apply only to the reference configuration shown in **Figure 1**. Verizon Business customers will use FQDNs and IP addressing appropriate for the unique customer environment.

3.1. Remote Workers

In the sample configuration, remote Avaya SIP endpoints connected through Avaya SBCE with Advanced Services licensing were used along with local Avaya endpoints in the verification of these Application Notes. The figure below illustrates a detailed view of the Remote Workers section previously shown in **Figure 1**. Although not the primary focus of these Application Notes, relevant configuration parameters of the Avaya SBCE for use with Remote Worker are illustrated in **Appendix A**.

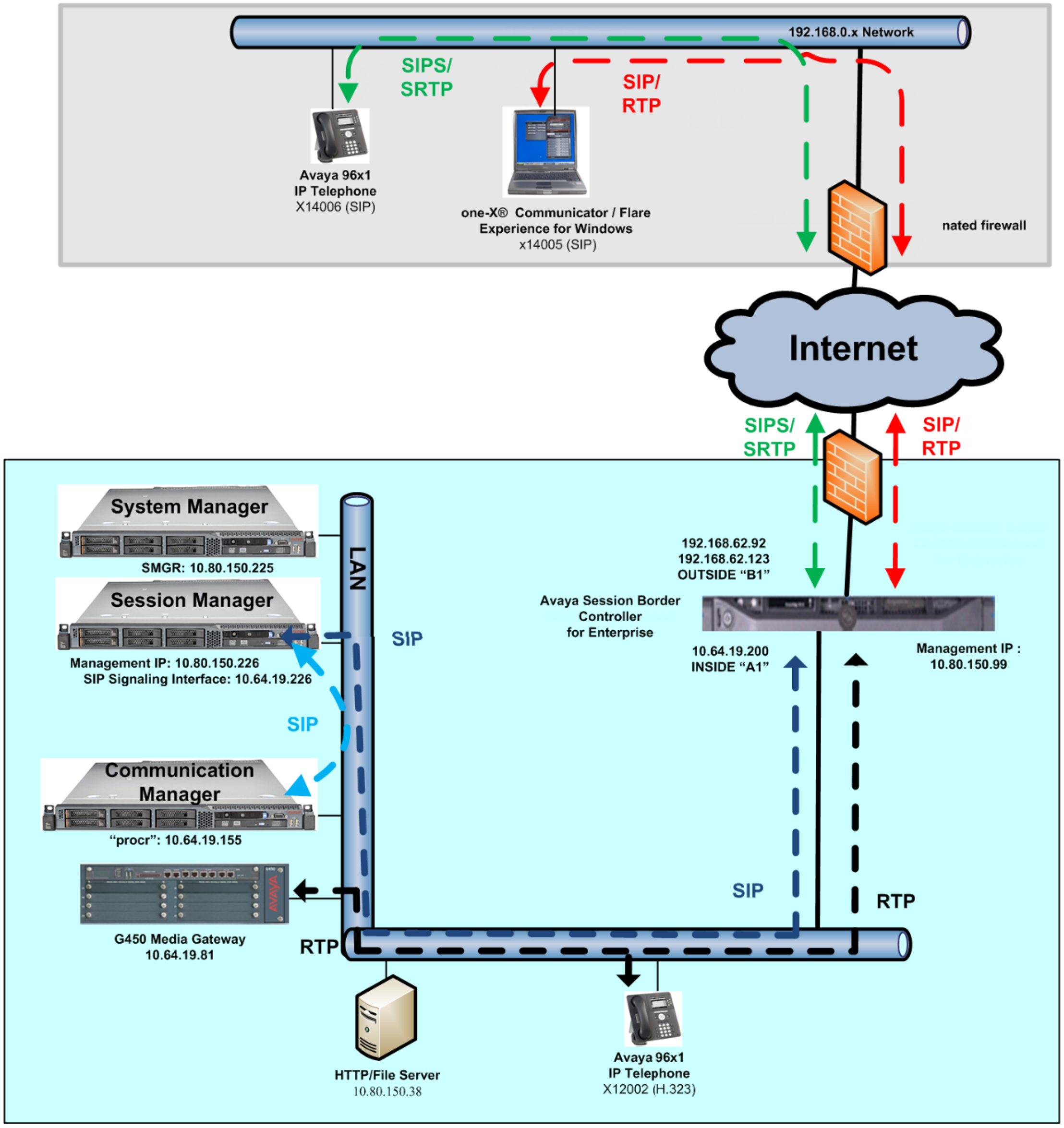


Figure 2: Remote Worker Lab Configuration

3.2. 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.

3.3. Call Flows

To understand how inbound Verizon toll-free calls are handled by Session Manager and Communication Manager, key call flows are summarized in this section.

3.3.1 Inbound IP Toll Free Call with no Network Call Redirection

The first call scenario illustrated in **Figure 3** is an inbound Verizon IP Toll Free call that is routed to Communication Manager, which in turn routes the call to a vector, agent, or phone. No redirection is performed in this simple scenario. A detailed verification of such a call with Communication Manager traces can be found in **Section 9.1.1**.

1. A PSTN phone originates a call to a Verizon IP Toll Free number.
2. The PSTN routes the call to the Verizon IP Toll Free service network.
3. The Verizon IP Toll Free service routes the call to the Avaya Session Border Controller for Enterprise.
4. The Avaya Session Border Controller for Enterprise performs any configured SIP header modifications, and routes the call to Session Manager.
5. Session Manager applies any configured SIP header adaptations and digit conversions, and based on configured Routing Policies, determines where the call should be routed. In this case, Session Manager routes the call to Communication Manager using a unique port so that Communication Manager can distinguish this call as having arrived from Verizon IPCC.
6. Depending on the called number, Communication Manager routes the call to a) a hunt group or vector, which in turn routes the call to an agent or phone, or b) directly to a phone.

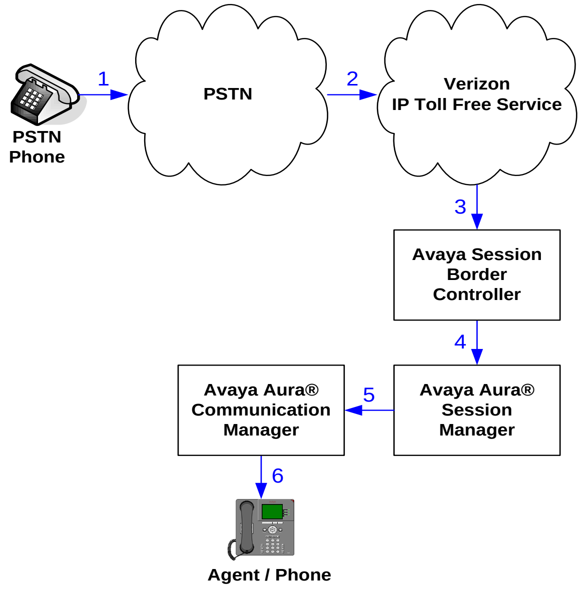

PSTN Phone
1
PSTN
2
Verizon IP Toll Free Service
3
Avaya Session Border Controller
4
Avaya Aura® Session Manager
5
Avaya Aura® Communication Manager
6
Agent / Phone

Figure 3: Inbound Verizon IP Toll Free Call – No Redirection

3.3.2 Inbound IP Toll Free Call with Post-Answer Network Call Redirection

The second call scenario illustrated in **Figure 4** is an inbound Verizon IP Toll Free call that is routed to a Communication Manager Vector Directory Number (VDN) to invoke call handling logic in a vector. The vector answers the call and then redirects the call back to the Verizon IP Toll Free service for routing to an alternate destination. Note that Verizon IP Toll Free service does not support redirecting a call before it is answered (using a SIP 302), and therefore the vector must include a step that results in answering the call, such as playing an announcement, prior to redirecting the call using REFER.

A detailed verification of such call with Communication Manager traces can be found in **Section 9.1.2** for a Verizon IP Toll Free SIP-connected alternate destination. In this example, the Verizon IP Toll Free service can be used to pass User to User Information (UUI) from the redirecting site to the alternate destination.

1. Same as the first five steps in **Figure 3**.
2. Communication Manager routes the call to a vector, which answers the call, plays an announcement, and attempts to redirect the call by sending a SIP REFER message out the SIP trunk from which the inbound call arrived. The SIP REFER message specifies the alternate destination in the Refer-To header. The SIP REFER message passes back through Session Manager and the Avaya SBCE to the Verizon IP Toll Free service network.
3. The Verizon IP Toll Free service places a call to the target party contained in the Refer-To header. Upon answer, the calling party is connected to the target party.
4. The Verizon IP Toll Free service notifies the Avaya CPE that the referred call has been answered (NOTIFY/sipfrag 200 OK). Communication Manager sends a BYE. The calling party and the target party can talk. The trunk upon which the call arrived in Step 1 is idle.

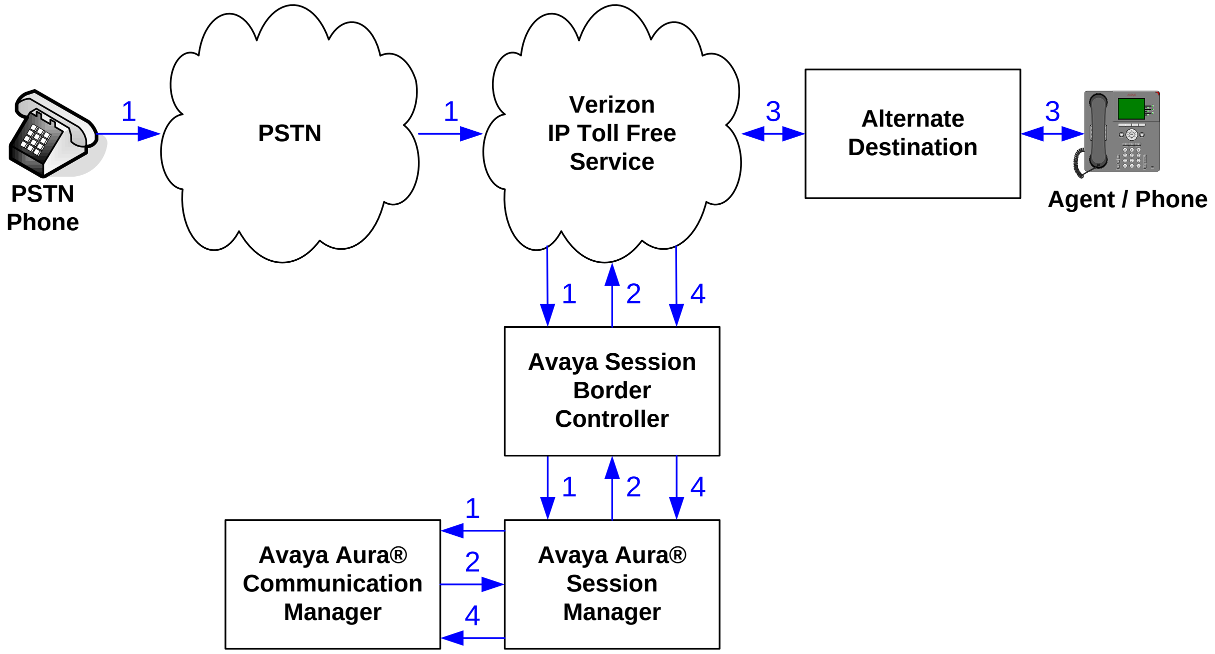


Figure 4: Inbound Verizon IP Toll Free– Post-Answer SIP REFER Redirection Successful

3.3.3 Inbound IP Toll Free Call with Unsuccessful Network Call Redirection

The next call scenario illustrated in **Figure 5** is similar to the previous call scenario, except that the redirection is unsuccessful. In theory, if redirection is successful, Communication Manager can "take the call back" and continue vector processing. For example, the call may route to an alternative agent, phone, or announcement after unsuccessful NCR.

1. Same as **Figure 4**.
2. Same as **Figure 4**.
3. The Verizon IP Toll Free service places a call to the target party (alternate destination), but the target party is busy or otherwise unavailable.
4. The Verizon IP Toll Free service notifies the redirecting/referring party (Communication Manager) of the error condition.
5. Communication Manager routes the call to a local agent, phone, or announcement.

However, as noted in **Section 2.2**, except for egregious configuration errors, this "REFER error handling" scenario could not be verified on the production Verizon circuit used for testing. On the production circuit, Verizon sends a SIP BYE which terminates Communication Manager vector processing for failure scenarios. For example, if a 486 Busy is received from the target of the REFER, Verizon will send a BYE immediately after a "NOTIFY/sipfrag 486", which precludes any further call processing by Communication Manager. As another example, in cases where mis-configuration is introduced to cause the Refer-To header to be malformed (e.g., no "+" in Refer-To), Verizon will send a BYE immediately after a "NOTIFY/sipfrag 603 Server Internal Error". If REFER is configured in the vector, but Network Call Redirection is not enabled for the SIP trunk group, Communication Manager will not send the REFER to Verizon, and vector processing will continue at the step following the route-to step that would normally trigger the REFER.

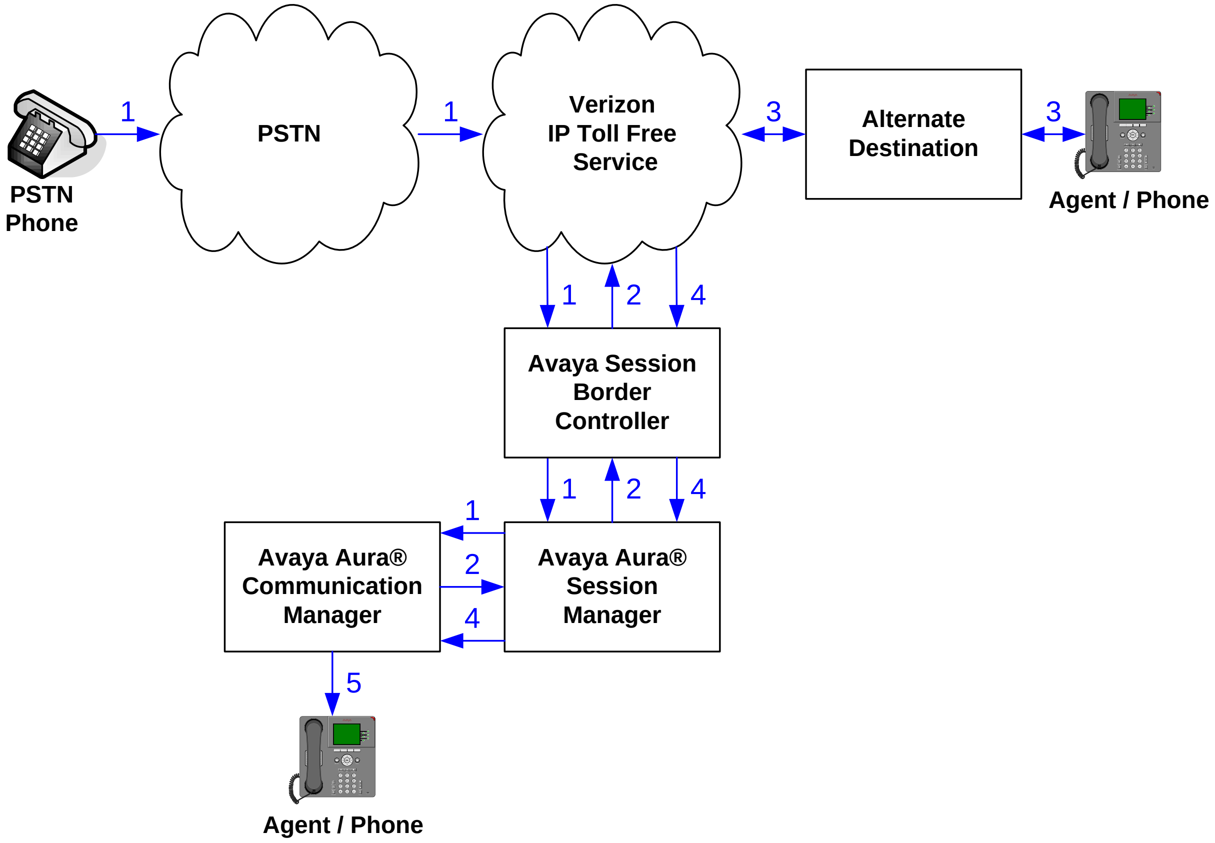

PSTN Phone
1
PSTN
1
Verizon IP Toll Free Service
3
Alternate Destination
3
Agent / Phone
1
2
4
Avaya Session Border Controller
1
2
4
1
2
4
Avaya Aura® Communication Manager
Avaya Aura® Session Manager
5
Agent / Phone

Figure 5: Inbound Verizon IP Toll Free– Post-Answer SIP REFER Redirection Unsuccessful

4. Equipment and Software Validated

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

Equipment:	Software:
HP ProLiant DL360 G7	Avaya Aura® Communication Manager Release 6.3 SP0
HP ProLiant DL360 G7	Avaya Aura® System Manager 6.3 SP2
HP ProLiant DL360 G7	Avaya Aura® Session Manager 6.3 SP2
G450 Gateway	33.13.0
DELL 210 RII	Avaya Session Border Controller for Enterprise Version 6.2 Q36
Avaya 9600-Series Telephones (H.323)	R 3.2
Avaya 96X1- Series Telephones (SIP)	R6.2.2.17
Avaya 96X1- Series Telephones (H323)	R6.2313
Avaya One-X Communicator (H.323)	6.1.8.06-SP8-40314
Avaya Flare® Experience for Windows	1.1.2.11
Avaya Desktop Video Device	Flare 1.1.3
Avaya 6400-Series Digital Telephones	N/A

Table 1: Equipment and Software Used in the Sample Configuration

5. Configure Avaya Aura® Communication Manager Release 6.3

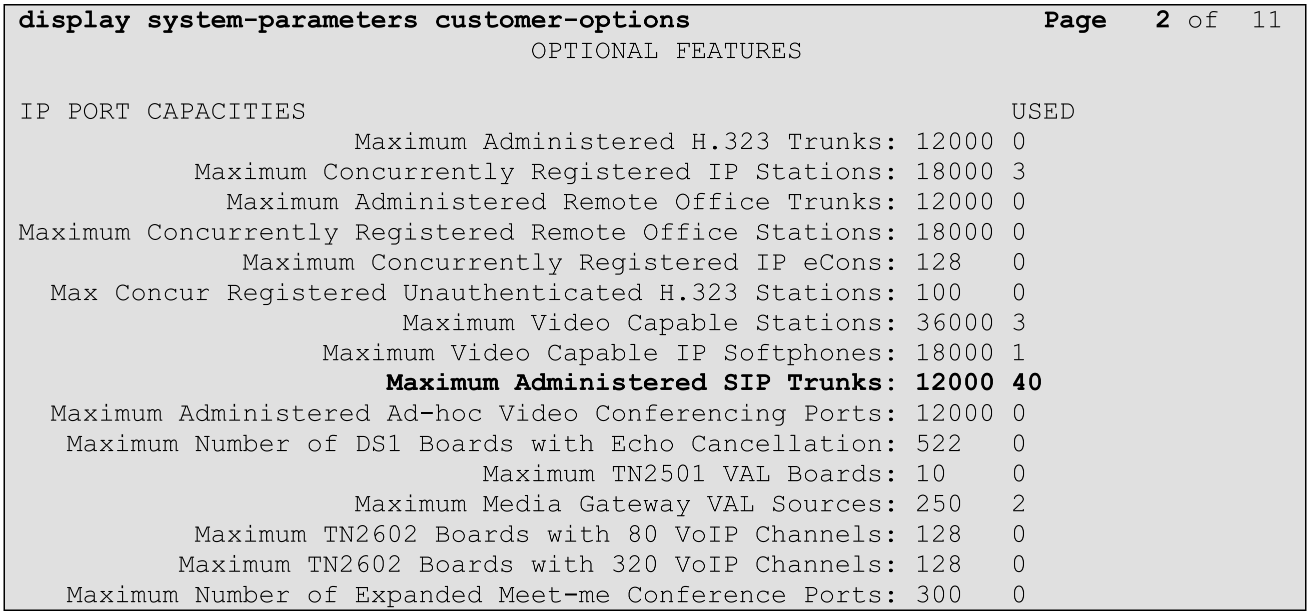
This section illustrates an example configuration allowing SIP signaling via the "Processor Ethernet" of Communication Manager to Session Manager. In configurations that use an Avaya G650 Media Gateway, it is also possible to use an Avaya C-LAN in the Avaya G650 Media Gateway for SIP signaling to Session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

Note - The initial installation, configuration, and licensing of the Avaya servers and media gateways for Communication Manager are assumed to have been previously completed and are not discussed in these Application Notes. These Application Notes focus on describing the sample configuration as it relates to SIP Trunking to Verizon IPCC.

5.1. Verify Licensed Features

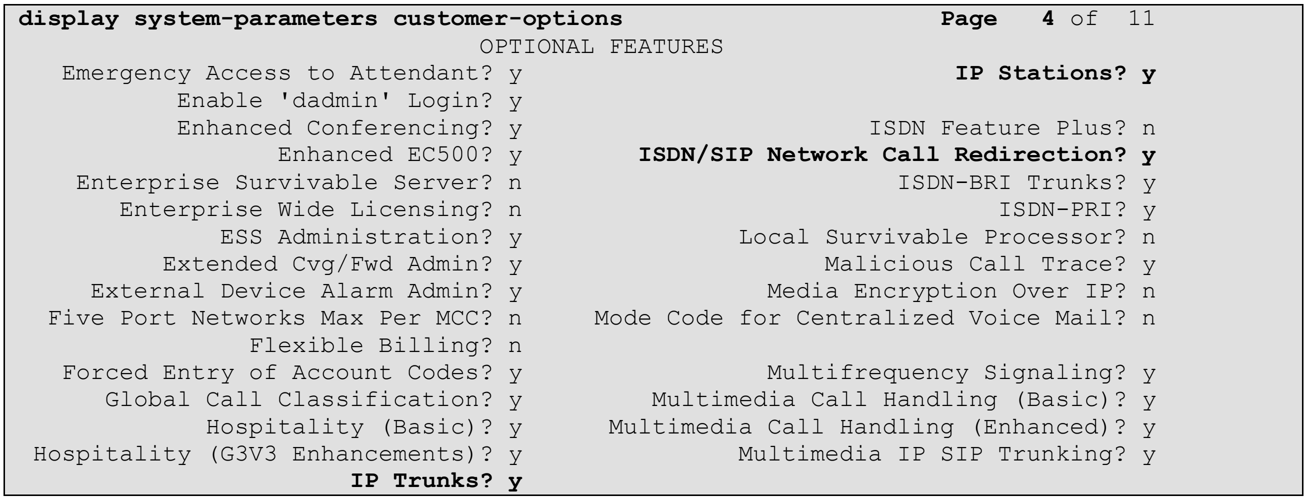
Communication Manager license file controls customer capabilities. Contact an authorized Avaya representative for assistance if a required feature needs to be enabled.

On **Page 2** of the ***display system-parameters customer-options*** form, verify that the **Maximum Administered SIP Trunks** is sufficient for the combination of trunks to the Verizon Business 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 3
             Maximum Administered Remote Office Trunks: 12000 0
Maximum Concurrently Registered Remote Office Stations: 18000 0
              Maximum Concurrently Registered IP eCons: 128   0
  Max Concur Registered Unauthenticated H.323 Stations: 100   0
                        Maximum Video Capable Stations: 36000 3
                   Maximum Video Capable IP Softphones: 18000 1
                       Maximum Administered SIP Trunks: 12000 40
  Maximum Administered Ad-hoc Video Conferencing Ports: 12000 0
   Maximum Number of DS1 Boards with Echo Cancellation: 522   0
                             Maximum TN2501 VAL Boards: 10    0
                     Maximum Media Gateway VAL Sources: 250   2
           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 ***display system-parameters customer-options*** form, verify that the **IP Trunks** and **IP Stations** features are enabled. If the use of SIP REFER messaging or send-only SDP attributes will be required verify that the **ISDN/SIP Network Call Redirection** feature is enabled.



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

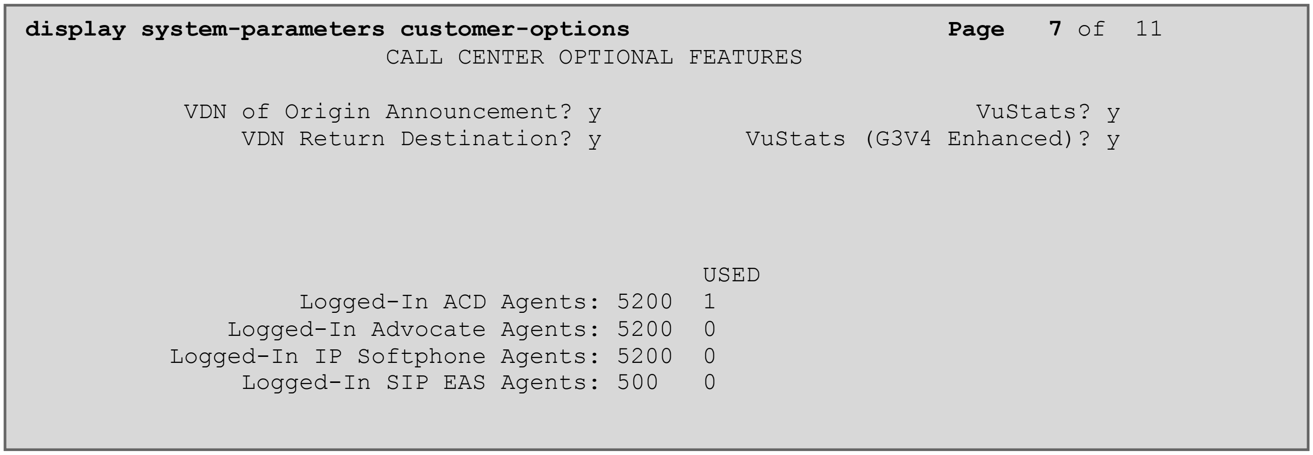
On **Page 5** of the ***display system-parameters customer-options*** form, verify that the **Private Networking** and **Processor Ethernet** features are enabled.

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

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

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.

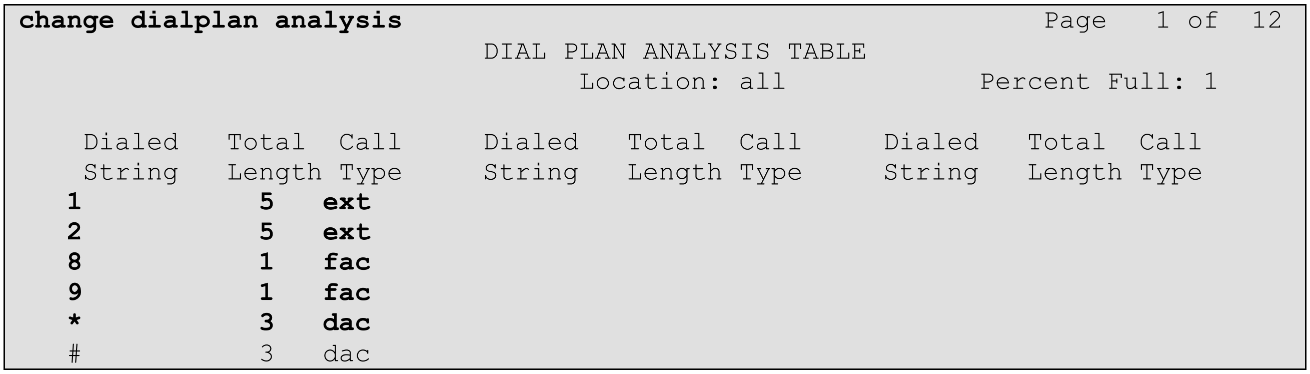


```
display system-parameters customer-options                      Page   7 of  11
                         CALL CENTER OPTIONAL FEATURES

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





                                               USED
                   Logged-In ACD Agents: 5200  1
              Logged-In Advocate Agents: 5200  0
          Logged-In IP Softphone Agents: 5200  0
               Logged-In SIP EAS Agents: 500   0
```

5.2. Dial Plan

In the reference configuration the Avaya CPE environment uses five digit local extensions, such as 12xxx, 14xxx or 20xxx. Trunk Access Codes (TAC) are 3 digits in length and begin with *. The Feature Access Code (FAC) to access ARS is the single digit 9. The Feature Access Code (FAC) to access AAR is the single digit 8. The dial plan illustrated here is not intended to be prescriptive; any valid dial plan may be used.

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



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

    Dialed   Total  Call     Dialed   Total  Call     Dialed   Total  Call
    String   Length Type     String   Length Type     String   Length Type
   1           5   ext
   2           5   ext
   8           1   fac
   9           1   fac
   *           3   dac
   #           3   dac
```

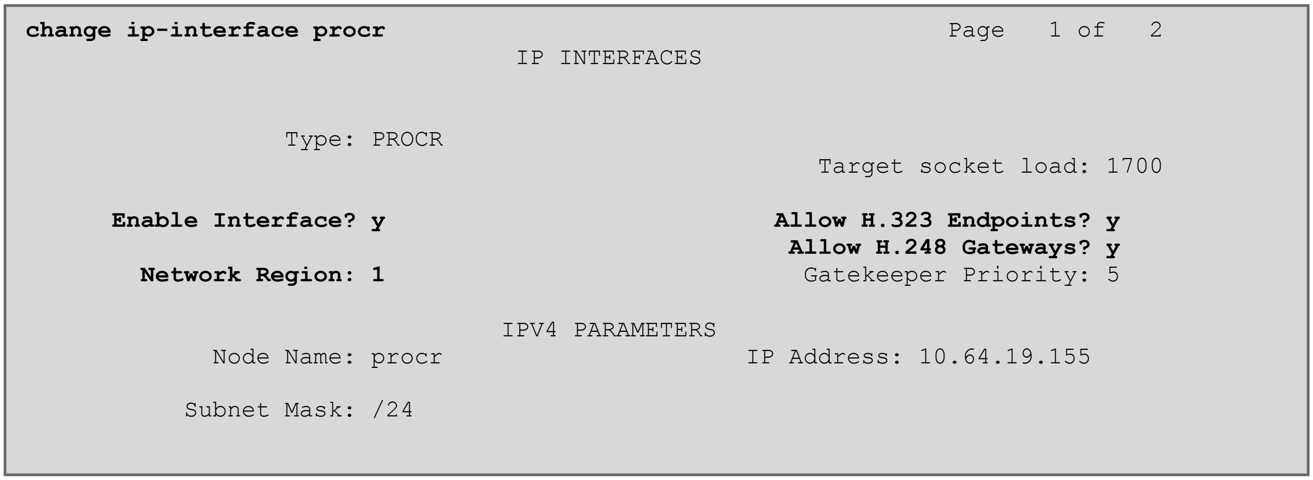
5.3. Node Names

Node names are mappings of names to IP addresses that can be used in various screens. The following ***change node-names ip*** output shows relevant node-names in the sample configuration. As shown in bold, the node name for Session Manager is “SM63” with IP address 10.64.19.226. The node name and IP address for the Processor Ethernet “procr” is 10.64.19.155.

```
change node-names ip                                                Page   1 of   2
                                          IP NODE NAMES
    Name                IP Address
SM63                  10.64.19.226
default               0.0.0.0
procr                 10.64.19.155
procr6                ::
```

5.4. Processor Ethernet Configuration on HP Common Server

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

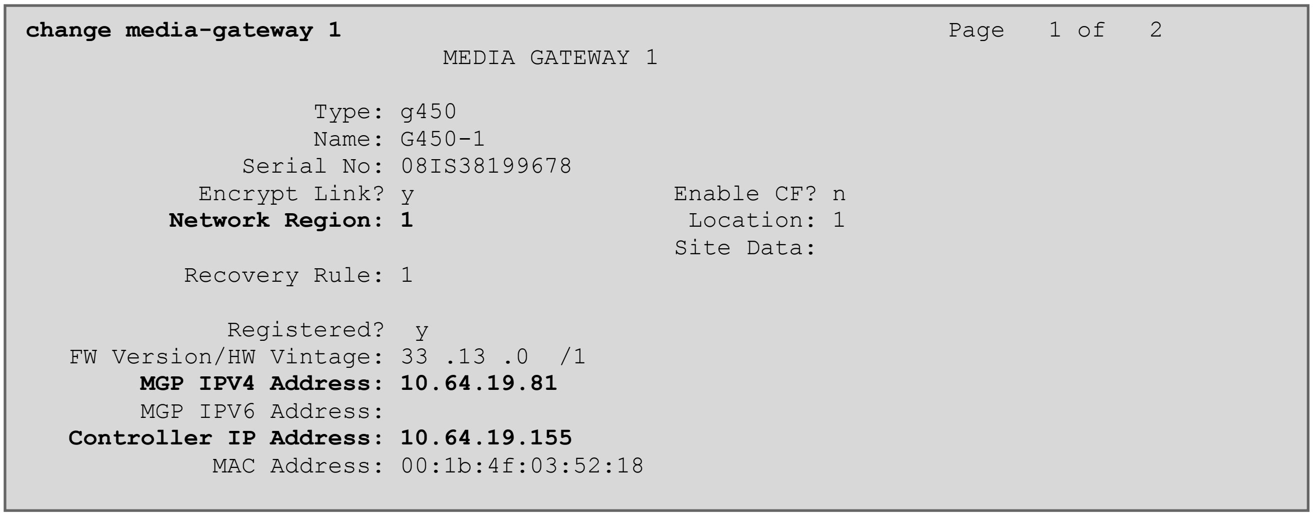


```
change ip-interface procr                                      Page   1 of   2
                                  IP INTERFACES


                  Type: PROCR
                                                        Target socket load: 1700

       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: 10.64.19.155

           Subnet Mask: /24
```

5.5. Network Regions for Gateway, Telephones

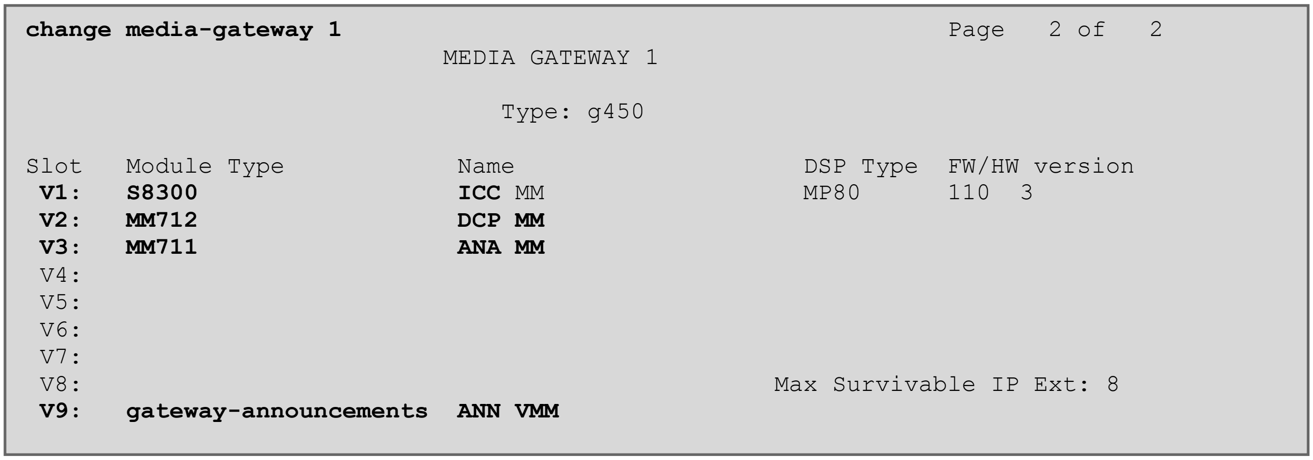
Network regions provide a means to logically group resources. In the shared Communication Manager configuration used for the testing, the Avaya G450 Media Gateway is in region 1. To provide testing flexibility, network region 2 was associated with other components used specifically for the Verizon testing.

Non-IP telephones (e.g., analog, digital) derive network region and location configuration from the Avaya gateway to which the device is connected. The following display command shows that **Media Gateway 1** is an Avaya G450 Media Gateway configured for network region 1. It can also be observed that the **Controller IP Address** is the Avaya Processor Ethernet (10.64.19.155), and that the gateway IP address is 10.64.19.81. These fields are not configured in this screen, but just display the current information for the Media Gateway.



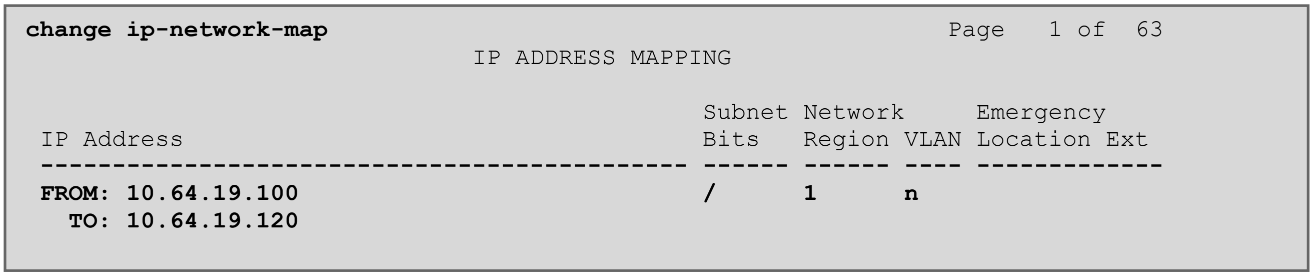
```
change media-gateway 1                                          Page   1 of   2
                             MEDIA GATEWAY 1

                    Type: g450
                    Name: G450-1
               Serial No: 08IS38199678
            Encrypt Link? y                  Enable CF? n
          Network Region: 1                   Location: 1
                                             Site Data:
           Recovery Rule: 1

              Registered?  y
   FW Version/HW Vintage: 33 .13 .0  /1
        MGP IPV4 Address: 10.64.19.81
        MGP IPV6 Address:
   Controller IP Address: 10.64.19.155
             MAC Address: 00:1b:4f:03:52:18
```

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



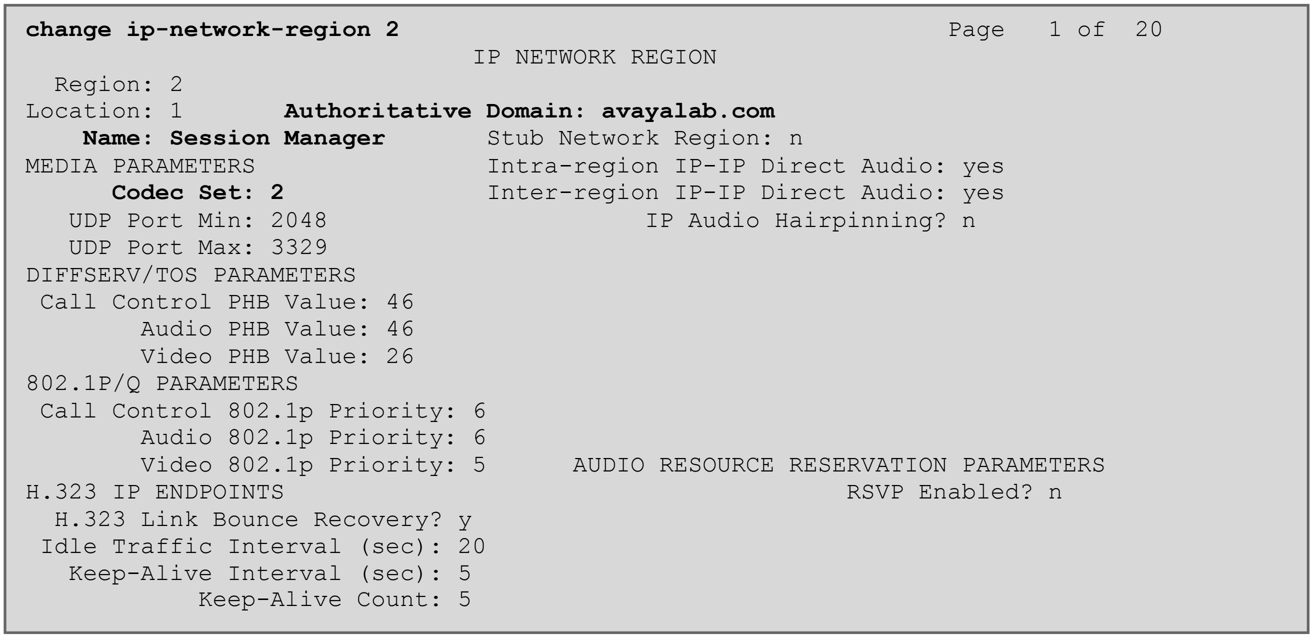
```
change media-gateway 1                                          Page   2 of   2
                             MEDIA GATEWAY 1

                                 Type: g450

Slot   Module Type            Name                    DSP Type  FW/HW version
 V1:   S8300                  ICC MM                  MP80      110  3
 V2:   MM712                  DCP MM
 V3:   MM711                  ANA MM
 V4:
 V5:
 V6:
 V7:
 V8:                                                Max Survivable IP Ext: 8
 V9:   gateway-announcements  ANN VMM
```

IP telephones can be assigned a network region based on an IP address mapping. The network region can also associate the IP telephone to a location for location-based routing decisions. The following screen illustrates a subset of the IP network map configuration used to verify these Application Notes. If the IP address of a registering IP Telephone does not appear in the ip-network-map, the phone is assigned the network region of the "gatekeeper" (e.g., CLAN or PE) to which it registers. When the IP address of a registering IP telephone is in the ip-network-map, the phone is assigned the network region assigned by the form shown below. For example, the IP address 10.64.19.109 would be mapped to network region 1, based on the configuration in bold below. In production environments, different sites will typically be on different networks, and ranges of IP addresses assigned by the DHCP scope serving the site can be entered as one entry in the network map, to assign all telephones in a range to a specific network region.



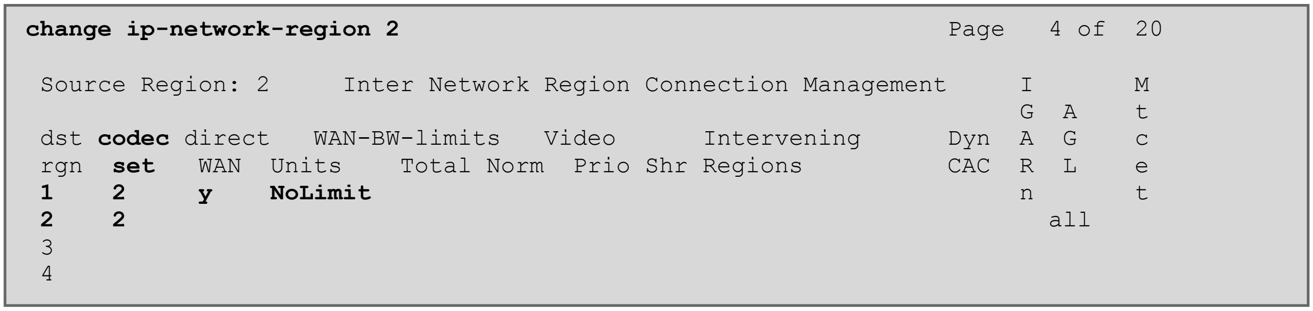
```
change ip-network-map                                           Page   1 of  63
                               IP ADDRESS MAPPING

                                               Subnet Network     Emergency
 IP Address                                    Bits   Region VLAN Location Ext
 --------------------------------------------- ------ ------ ---- -------------
 FROM: 10.64.19.100                            /      1      n
   TO: 10.64.19.120
```

The following screen shows IP Network Region 2 configuration. In the shared test environment, network region 2 is used to allow unique behaviors for the Verizon IPCC test environment. In this example, codec set 2 will be used for calls within region 2. The shared Avaya Interoperability Lab test environment uses the domain "avayalab.com" (i.e., for network region 1 including the region of the Processor Ethernet "procr"). Session Manager also uses this domain to determined routes for calls based on the domain information of the calls and for SIP phone registration.



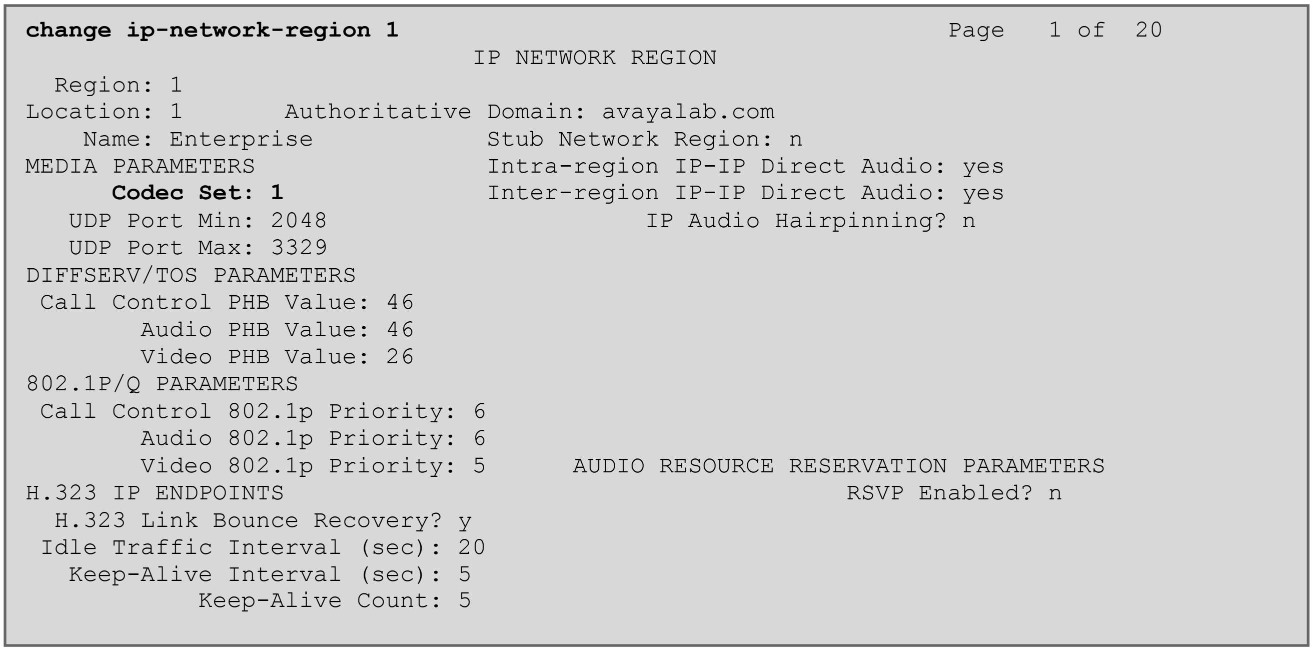
```
change ip-network-region 2                                      Page   1 of  20
                               IP NETWORK REGION
  Region: 2
Location: 1       Authoritative Domain: avayalab.com
    Name: Session Manager       Stub Network Region: n
MEDIA PARAMETERS                Intra-region IP-IP Direct Audio: yes
      Codec Set: 2              Inter-region IP-IP Direct Audio: yes
   UDP Port Min: 2048                      IP Audio Hairpinning? n
   UDP Port Max: 3329
DIFFSERV/TOS PARAMETERS
 Call Control PHB Value: 46
        Audio PHB Value: 46
        Video PHB Value: 26
802.1P/Q PARAMETERS
 Call Control 802.1p Priority: 6
        Audio 802.1p Priority: 6
        Video 802.1p Priority: 5      AUDIO RESOURCE RESERVATION PARAMETERS
H.323 IP ENDPOINTS                                       RSVP Enabled? n
  H.323 Link Bounce Recovery? y
 Idle Traffic Interval (sec): 20
   Keep-Alive Interval (sec): 5
            Keep-Alive Count: 5
```

The following screen shows the inter-network region connection configuration for region 2. The first bold row shows that network region 2 is directly connected to network region 1, and that codec set 2 will also be used for any connections between region 2 and region 1. For configurations where multiple remote gateways are used, each gateway will typically be configured for a different region, and this screen can be used to specify unique codec or call admission control parameters for the pairs of regions. If a different codec should be used for inter-region connectivity than for intra-region connectivity, a different codec set can be entered in the **codec set** column for the appropriate row in the screen shown below. Once submitted, the configuration becomes symmetric, meaning that network region 1, **Page 4** will also show codec set 2 for region 2 to region 1 connectivity.



```
change ip-network-region 2                                      Page   4 of  20

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

The following screen shows IP Network Region 1 configuration. In this example, codec set 1 will be used for calls within region 1 due to the **Codec Set** parameter on **Page 1**, but codec set 2 will be used for connections between region 1 and region 2 as noted previously.



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

The following screen shows the inter-network region connection configuration for region 1. The bold row shows that network region 1 is directly connected to network region 2, and that codec set 2 will be used for any connections between region 2 and region 1.

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

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

5.6. IP Codec Sets

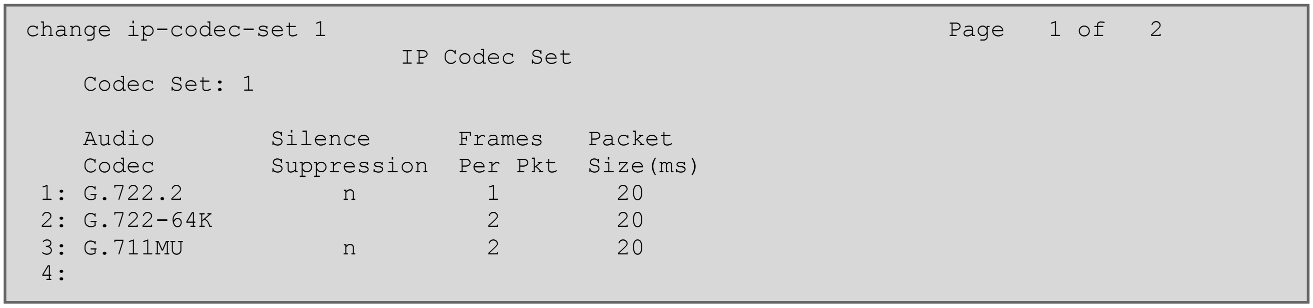
The following screen shows the configuration for codec set 2, the codec set configured to be used for calls within region 2 and for calls between region 1 and region 2. In general, an IP codec set is a list of allowable codecs in priority order. Using the example configuration shown below, all calls with Verizon IPCC via the SIP trunks would prefer to use **G.729A**, but also be capable of using **G.711MU** (The Verizon IPCC service will not include G.722 in SDP offers or SDP answers). Any calls using this same codec set that are between devices capable of the **G.722-64K** codec can use G.722. The specification of G.722 as the first choice is not required. That is, G.722 may be omitted from the codec set, but it is recommended that G.729A and G.711MU be included in the codec set for use with Verizon IPCC Services.

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

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

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

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

                          IP Codec Set

                              Allow Direct-IP Multimedia? n

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

Although codec set 1 is not used for connections with Verizon IPCC, the following screen shows the configuration for codec set 1. Codec set 1 is used for local Avaya CPE connections within region 1.

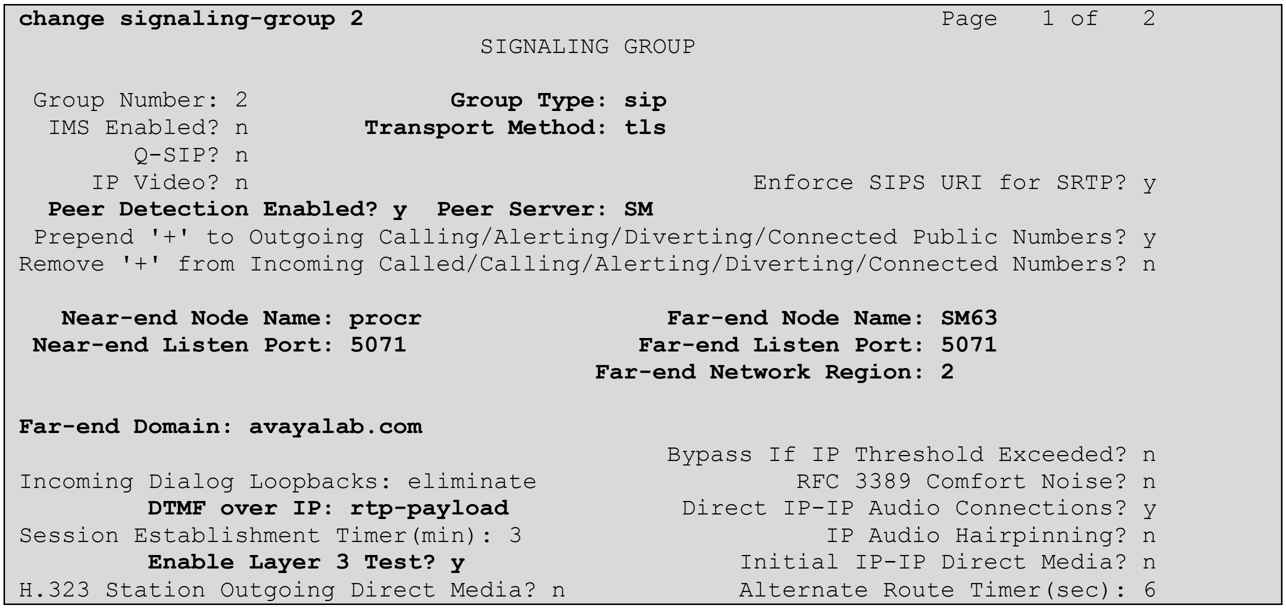


```
change ip-codec-set 1                                           Page   1 of   2
                          IP Codec Set
    Codec Set: 1

    Audio        Silence      Frames   Packet
    Codec        Suppression  Per Pkt  Size(ms)
 1: G.722.2           n         1        20
 2: G.722-64K                   2        20
 3: G.711MU           n         2        20
 4:
```

5.7. SIP Signaling Group

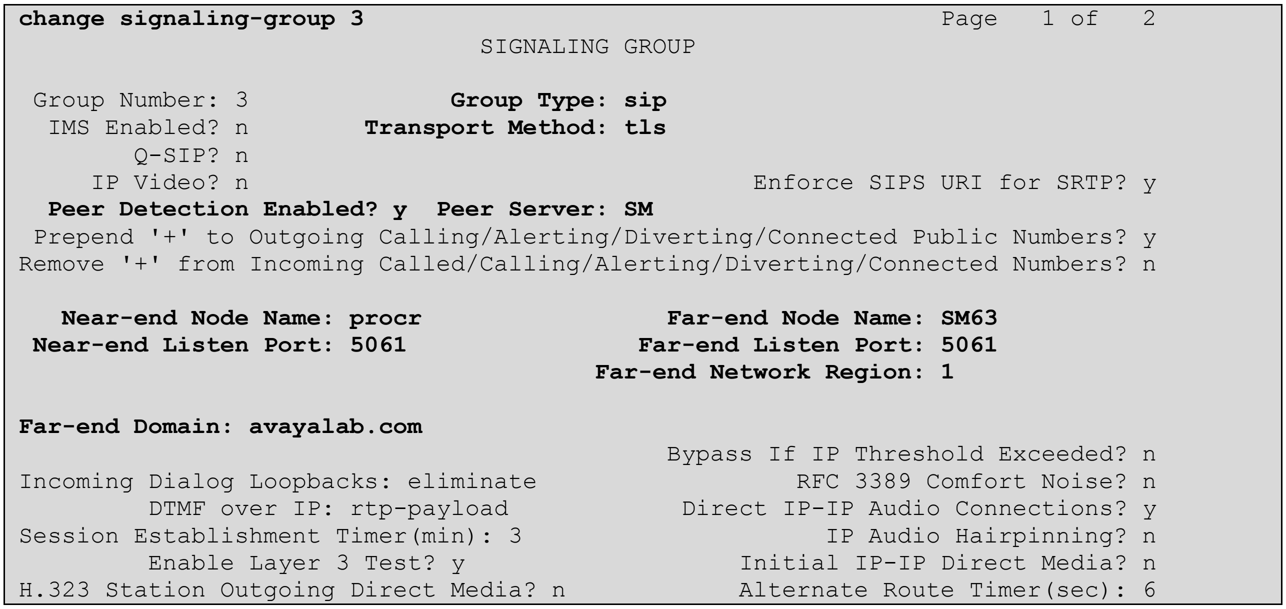
This section illustrates the configuration of the SIP Signaling Groups. Each signaling group has a **Group Type** of “sip”, a **Near-end Node Name** of “procr”, and a **Far-end Node Name** of “SM63”. In the example screens, the **Transport Method** for all signaling groups is “tls”. The **Peer Detection Enabled** field is set to “y” and a peer Session Manager has been previously detected. The **Far-end Domain** is set to “avayalab.com” matching the configuration in place prior to adding the Verizon IP SIP Trunking configuration. The **Enable Layer 3 Test** field is enabled on each of the signaling groups to allow Communication Manager to maintain the signaling group using the SIP OPTIONS method. Fields that are not referenced in the text below can be left at default values, including **DTMF over IP** set to “rtp-payload”, which corresponds to RFC 2833.

The following screen shows signaling group 2. Signaling group 2 will be used for processing incoming calls from Verizon IPCC via Session Manager. The **Far-end Network Region** is configured to region 2. Port 5071 has been configured as both the **Near-end Listen Port** and **Far-end Listen Port**. Session Manager will be configured to direct calls arriving from the PSTN with Verizon toll-free numbers to a route policy that uses a SIP entity link to Communication Manager specifying port 5071. The use of different ports is one means to allow Communication Manager to distinguish different types of calls arriving from the same Session Manager. Other parameters may be left at default values.



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

 Group Number: 2             Group Type: sip
  IMS Enabled? n       Transport Method: tls
        Q-SIP? n
     IP Video? n                                   Enforce SIPS URI for SRTP? y
  Peer Detection Enabled? y  Peer Server: SM
 Prepend '+' to Outgoing Calling/Alerting/Diverting/Connected Public Numbers? y
Remove '+' from Incoming Called/Calling/Alerting/Diverting/Connected Numbers? n

   Near-end Node Name: procr                 Far-end Node Name: SM63
 Near-end Listen Port: 5071                Far-end Listen Port: 5071
                                        Far-end Network Region: 2

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

The following screen shows signaling group 3, the signaling group to Session Manager that was in place prior to adding the Verizon IPCC configuration to the shared Avaya Solutions and Interoperability Test Lab configuration. This signaling group reflects configuration not specifically related to Verizon IPCC but will be used to enable SIP phones to register to Session Manager and to use features from Communication Manager. Again, the **Near-end Node Name** is “procr” and the **Far-end Node Name** is “SM63”, the node name of the Session Manager. Unlike the signaling group used for the Verizon IPCC signaling, the **Far-end Network Region** is “1”. The **Peer Detection Enabled** field is set to “y” and a peer Session Manager has been previously detected.



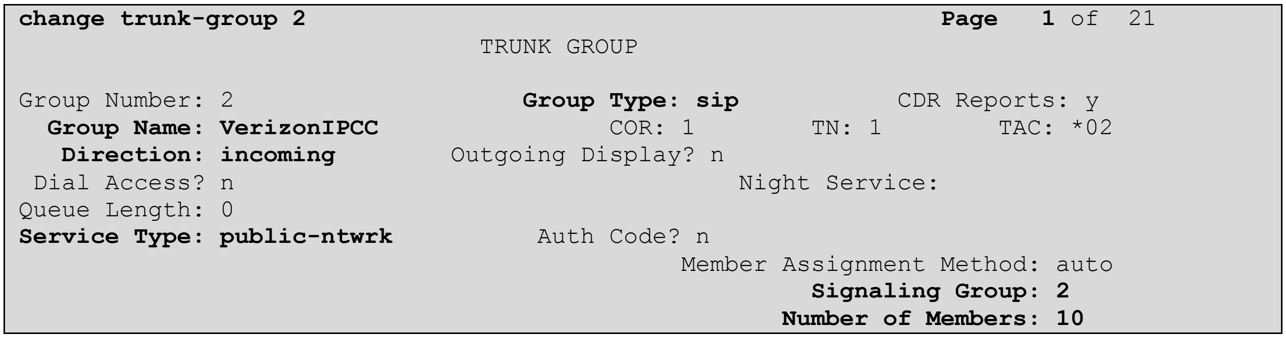
```
change signaling-group 3                                          Page   1 of   2
                                SIGNALING GROUP

 Group Number: 3              Group Type: sip
  IMS Enabled? n        Transport Method: tls
        Q-SIP? n
     IP Video? n                                   Enforce SIPS URI for SRTP? y
  Peer Detection Enabled? y  Peer Server: SM
 Prepend '+' to Outgoing Calling/Alerting/Diverting/Connected Public Numbers? y
Remove '+' from Incoming Called/Calling/Alerting/Diverting/Connected Numbers? n

   Near-end Node Name: procr                  Far-end Node Name: SM63
 Near-end Listen Port: 5061                 Far-end Listen Port: 5061
                                         Far-end Network Region: 1

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

5.8. SIP Trunk Group

This section illustrates the configuration of the SIP Trunk Groups corresponding to the SIP signaling group 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.

The following shows **Page 1** for trunk group 2, which will be used for incoming and outgoing PSTN calls from Verizon. The **Number of Members** field defines how many simultaneous calls are permitted for the trunk group. The **Service Type** field is set to “public-ntwrk” for the trunks that will handle calls with Verizon. Although not strictly necessary, the **Direction** has been configured to “incoming” to emphasize that trunk group 1 is used for incoming calls only in the sample configuration.



```
change trunk-group 2                                            Page   1 of  21
                                TRUNK GROUP

Group Number: 2                    Group Type: sip           CDR Reports: y
  Group Name: VerizonIPCC                COR: 1        TN: 1        TAC: *02
   Direction: incoming        Outgoing Display? n
 Dial Access? n                                    Night Service:
Queue Length: 0
Service Type: public-ntwrk          Auth Code? n
                                              Member Assignment Method: auto
                                                       Signaling Group: 2
                                                     Number of Members: 10
```

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

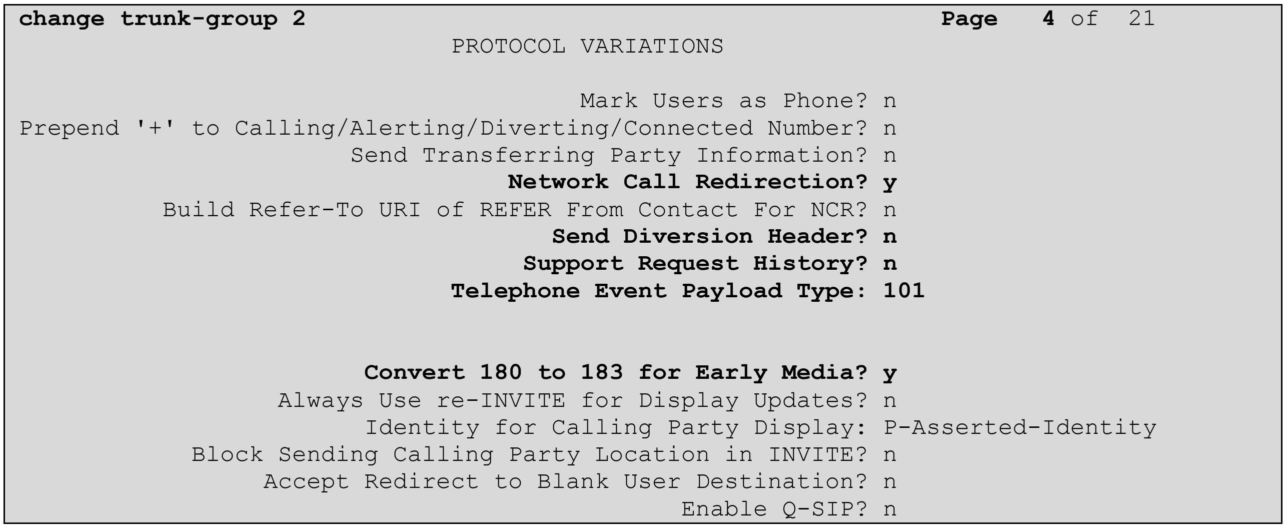
```
change trunk-group 2                                            Page   2 of  21
      Group Type: sip

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  Out? y


             XOIP Treatment: auto    Delay Call Setup When Accessed Via IGAR? n
```

The following screen shows **Page 3** for trunk group 2. All parameters except those in bold are default values. The **Numbering Format** will use “private” numbering, meaning that the private numbering table would be consulted for any mappings of Communication Manager extensions to alternate numbers to be sent to Session Manager. Replacement text strings can be configured using the “system-parameters features” screen (page 9, not shown), such that incoming “private” (anonymous) or “restricted” calls can display a configurable text string on called party telephones. If it is desired to see the configurable replacement text strings on user displays, the **Replace Restricted Numbers** and **Replace Unavailable Numbers** fields may be set to “y”.

```
change trunk-group 2                                            Page   3 of  21
TRUNK FEATURES
          ACA Assignment? n            Measured: none
                                                         Maintenance Tests? y



                     Numbering Format: private
                                                UUI Treatment: service-provider

                                                 Replace Restricted Numbers? y
                                                Replace Unavailable Numbers? y

                                Modify Tandem Calling Number: no

 Show ANSWERED BY on Display? y
```

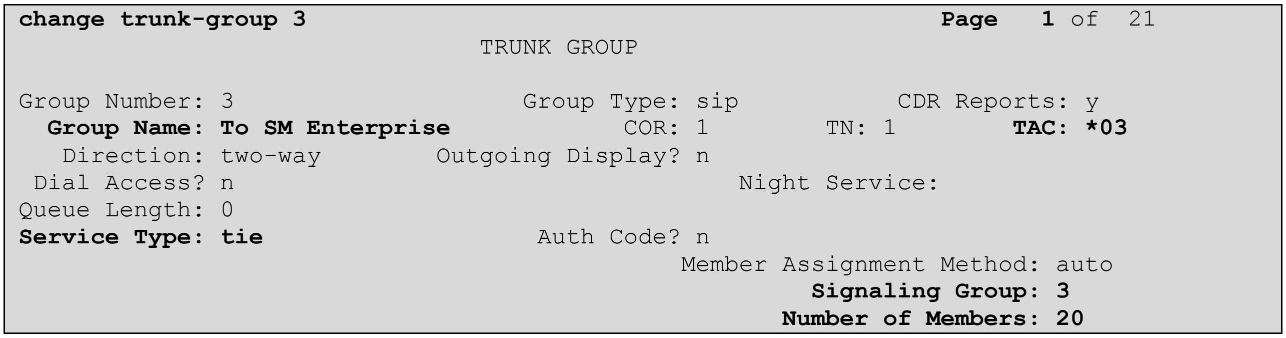
The following screen shows **Page 4** for trunk group 2. The bold fields have non-default values. The **Convert 180 to 183 for Early Media** field was a new in Communication Manager Release 6. Verizon recommends that inbound calls to the enterprise result in a 183 with SDP rather than a 180 with SDP, and setting this field to “y” for the trunk group handling inbound calls from Verizon produces this result. Although not strictly necessary, the **Telephone Event Payload Type** has been set to 101 to match Verizon configuration. Setting the **Network Call Redirection** flag to “y” enables advanced services associated with the use of the REFER message, while also implicitly enabling Communication Manager to signal “send-only” media conditions for calls placed on hold at the enterprise site. If neither REFER signaling nor “send-only” media signaling is required, this field may be left at the default “n” value. In the testing associated with these Application Notes, the **Network Call Redirection** flag was set to “y” to allow REFER to be exercised with the Verizon IPCC 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”



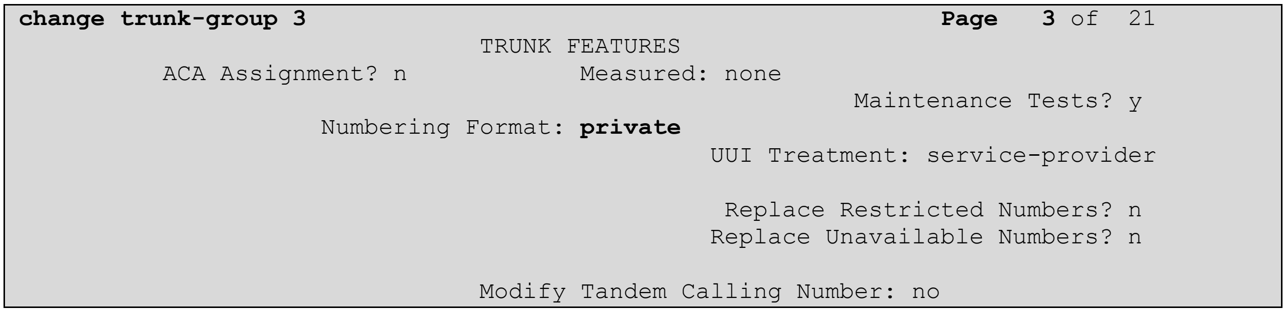
```
change trunk-group 2                                              Page   4 of  21
                              PROTOCOL VARIATIONS

                                       Mark Users as Phone? n
Prepend '+' to Calling/Alerting/Diverting/Connected Number? n
                       Send Transferring Party Information? n
                                  Network Call Redirection? y
          Build Refer-To URI of REFER From Contact For NCR? n
                                     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
            Block Sending Calling Party Location in INVITE? n
                 Accept Redirect to Blank User Destination? n
                                              Enable Q-SIP? n
```

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



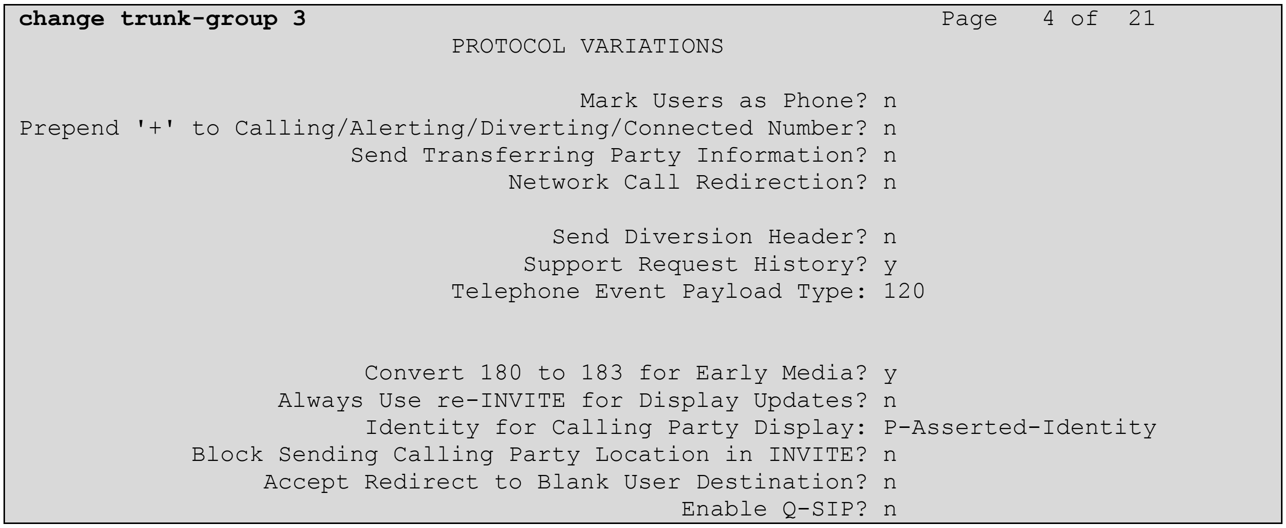
```
change trunk-group 3                                              Page   1 of  21
                                TRUNK GROUP

Group Number: 3                    Group Type: sip          CDR Reports: y
  Group Name: To SM Enterprise            COR: 1        TN: 1        TAC: *03
   Direction: two-way       Outgoing Display? n
 Dial Access? n                                  Night Service:
Queue Length: 0
Service Type: tie                    Auth Code? n
                                              Member Assignment Method: auto
                                                       Signaling Group: 3
                                                     Number of Members: 20
```

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



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

                                                 Replace Restricted Numbers? n
                                                Replace Unavailable Numbers? n

                                Modify Tandem Calling Number: no
```

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



```
change trunk-group 3                                            Page   4 of  21
                              PROTOCOL VARIATIONS

                                       Mark Users as Phone? n
Prepend '+' to Calling/Alerting/Diverting/Connected Number? n
                       Send Transferring Party Information? n
                                  Network Call Redirection? n

                                     Send Diversion Header? n
                                   Support Request History? y
                              Telephone Event Payload Type: 120


                        Convert 180 to 183 for Early Media? y
                  Always Use re-INVITE for Display Updates? n
                        Identity for Calling Party Display: P-Asserted-Identity
            Block Sending Calling Party Location in INVITE? n
                 Accept Redirect to Blank User Destination? n
                                              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
11001                 integrated callcenter-main            001V9       1
11002                 integ-mus  holdmusic                  001V9       1
11003                 integrated disconnect                 001V9       1
11004                 integrated no_agents                  001V9       1
11005                 integrated dtmf_test                  001V9       1
11006                 integrated please_wait                001V9       1
11007                 integrated REFER_Test                 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. A corresponding detailed verification is provided in **Section 9.2.2**. In this example, the inbound toll-free call is routed to VDN 10001 shown in the following screen. The originally dialed Verizon IP Toll Free number may be mapped to VDN 3698 by Session Manager digit conversion, or via the incoming call handling treatment for the Communication Manager trunk group handling the call.

```
display vdn 10001                                             Page   1 of   3
                            VECTOR DIRECTORY NUMBER

                             Extension: 10001
                                 Name*: Refer-to-PSTN
                           Destination: Vector Number        1
                   Attendant Vectoring? n
                  Meet-me Conferencing? n
                    Allow VDN Override? n
                                   COR: 1
                                   TN*: 1
                              Measured: none
```

VDN 10001 is associated with vector 1, which is shown below. Vector 1 plays an announcement (step 03) to answer the call. After the announcement, the “route-to number” (step 05) includes “~r+13035387024” where the number 303-538-7024 is a PSTN destination. This step causes a REFER message to be sent where the Refer-To header includes “+13035387024” 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 1                                              Page   1 of   6
                                  CALL VECTOR

    Number: 1                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 11006
04 #    Refer the call to PSTN Destination in step 5 below.
05 route-to     number ~r+13035387024   with cov n if unconditionally
06 #    If Refer fails queue to skill 1
07 queue-to     skill 1    pri m
08
```

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. A corresponding detailed verification is provided in **Section 9.2.3**. In this example, the inbound call is routed to VDN 10003 shown in the following screen. The originally dialed Verizon toll-free number may be mapped to VDN 10003 by Session Manager digit conversion, or via the incoming call handling treatment for the Communication Manager trunk group handling the call.

```
display vdn 10003                                             Page   1 of   3
                            VECTOR DIRECTORY NUMBER

                             Extension: 10003
                                 Name*: REFER with UUI
                           Destination: Vector Number        3
                   Attendant Vectoring? n
                  Meet-me Conferencing? n
                    Allow VDN Override? n
                                  COR: 1
                                  TN*: 1
                              Measured: none
```

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   uui                         asaiuui L     16     1
B   uui                         asaiuui L     16     17
C
```

VDN 10003 is associated with vector 3, which is shown below. Vector 3 sets data in the vector variables A and B (steps 03 and 04) and plays an announcement to answer the call (step 05). After the announcement, the “route-to” number step includes “~r+18668512649”. This step causes a REFER message to be sent where the Refer-To header includes “+18668512649” 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 “18668512649”. In the sample configuration, where only one location was used, 866-851-2649 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 3                                                Page   1 of   6
                                  CALL VECTOR

    Number: 3                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 wait-time    2   secs hearing ringback
02 set          A      = none   CATR  1234567890123456
03 set          B      = none   CATR  7890123456789012
04 #    Play announcement to answer call and route to ~r to cause Refer
05 announcement 11007
06 route-to     number ~r+18668512649   with cov n if unconditionally
07 #    If Refer fails play announcement and disconnect
08 disconnect   after announcement 11003
```

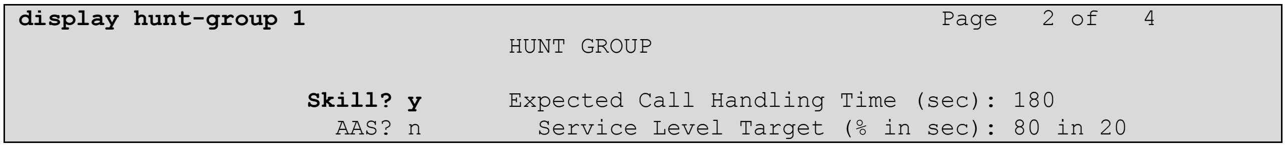
5.9.4 ACD Configuration for Call Queued for Handling by Agent

This section provides a simple example configuration for VDN, vector, hunt group, and agent logins used to queue inbound Verizon IPCC calls for handling by an agent.

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

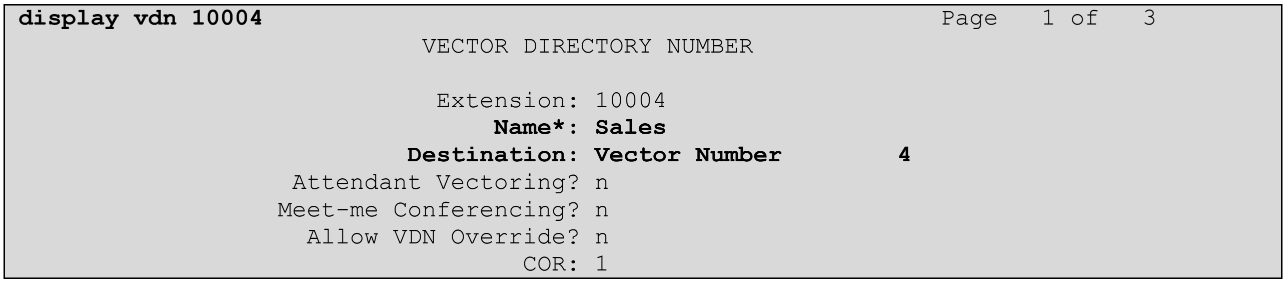
```
display hunt-group 1                                            Page   1 of   4
                                  HUNT GROUP

            Group Number: 1                                 ACD? y
              Group Name: Agent Group                     Queue? y
         Group Extension: 19991                          Vector? y
              Group Type: ucd-mia
                      TN: 1
                     COR: 1                        MM Early Answer? n
           Security Code:                    Local Agent Preference? n
 ISDN/SIP Caller Display:

             Queue Limit: unlimited
```

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



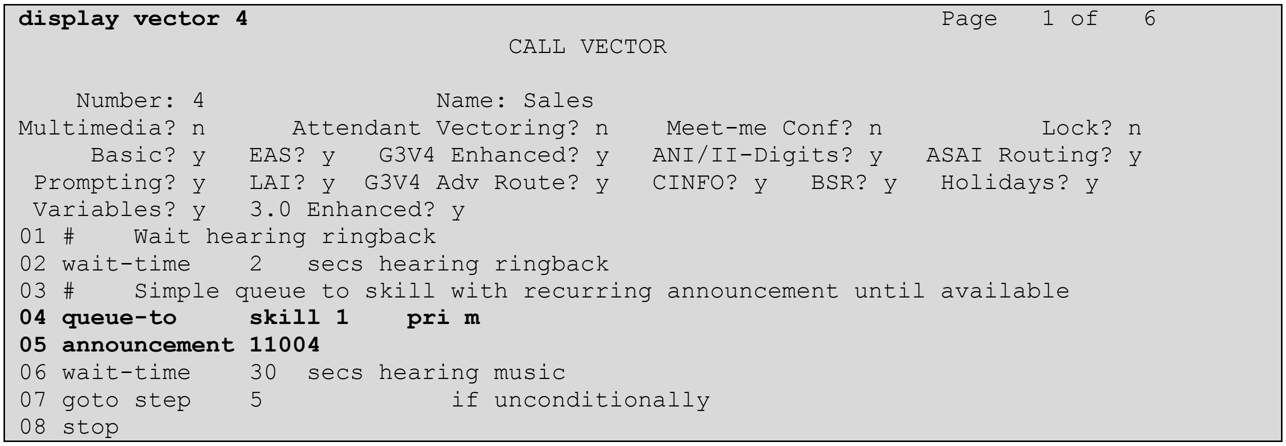
```
display hunt-group 1                                            Page   2 of   4
                                  HUNT GROUP

                    Skill? y      Expected Call Handling Time (sec): 180
                      AAS? n        Service Level Target (% in sec): 80 in 20
```

VDN 10004, shown below, is associated with vector 4.



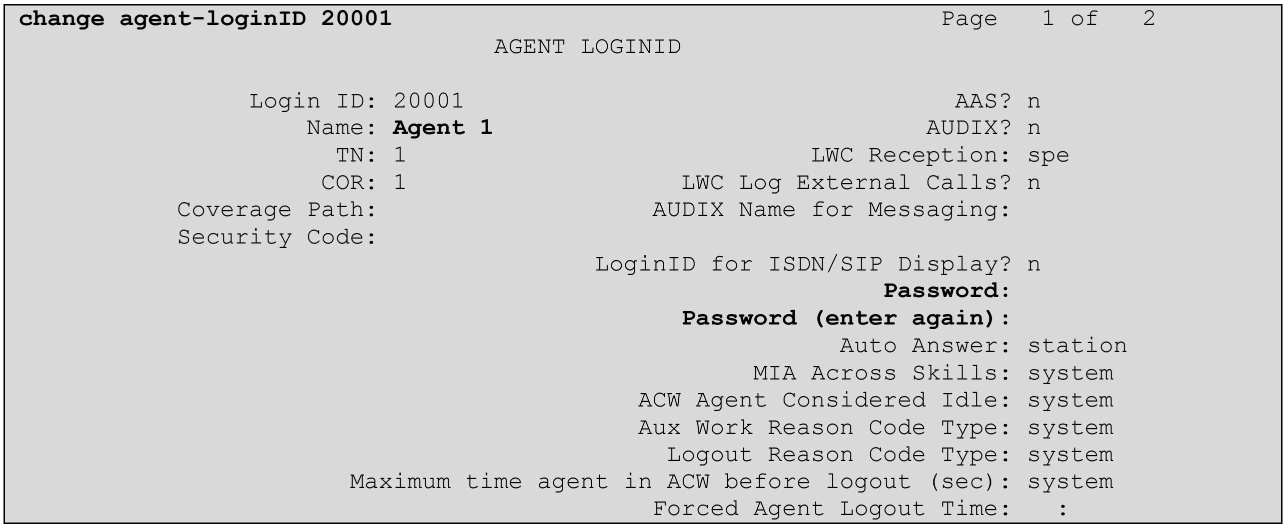
```
display vdn 10004                                               Page   1 of   3
                            VECTOR DIRECTORY NUMBER

                             Extension: 10004
                                 Name*: Sales
                           Destination: Vector Number        4
                   Attendant Vectoring? n
                  Meet-me Conferencing? n
                    Allow VDN Override? n
                                   COR: 1
```

In this simple example, vector 4 briefly plays ring back, then queues the call to skill 1. Announcement 11004 is a simple recurring announcement. If an agent is immediately available to handle the call, the call will be delivered to the agent. If an agent is not immediately available, the call will be queued, and the caller will hear the announcement. Once an agent becomes available, the call will be delivered to the agent.



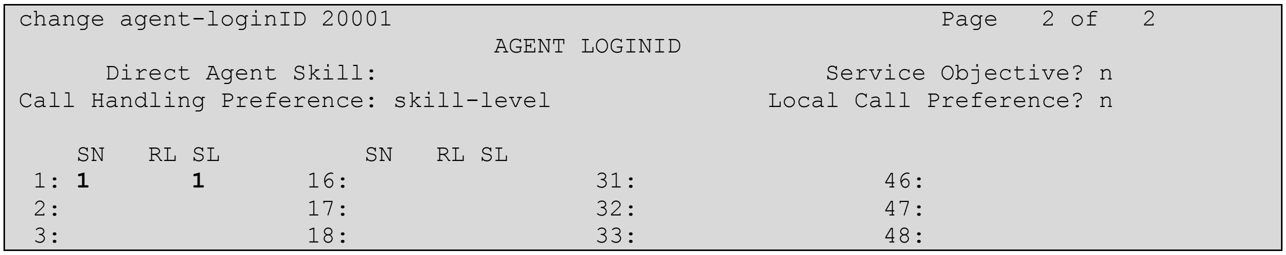
```
display vector 4                                                Page   1 of   6
                                  CALL VECTOR

    Number: 4                Name: Sales
Multimedia? n      Attendant Vectoring? n    Meet-me Conf? n           Lock? n
     Basic? y   EAS? y   G3V4 Enhanced? y   ANI/II-Digits? y   ASAI Routing? y
 Prompting? y   LAI? y  G3V4 Adv Route? y   CINFO? y   BSR? y   Holidays? y
 Variables? y   3.0 Enhanced? y
01 #    Wait hearing ringback
02 wait-time    2   secs hearing ringback
03 #    Simple queue to skill with recurring announcement until available
04 queue-to     skill 1    pri m
05 announcement 11004
06 wait-time    30  secs hearing music
07 goto step    5             if unconditionally
08 stop
```

The following screen illustrates an example agent-loginID 20001. In the sample configuration, an Avaya one-X® Deskphone logged in using agent-loginID 20001 and the configured Password to staff and take calls for skill 1.



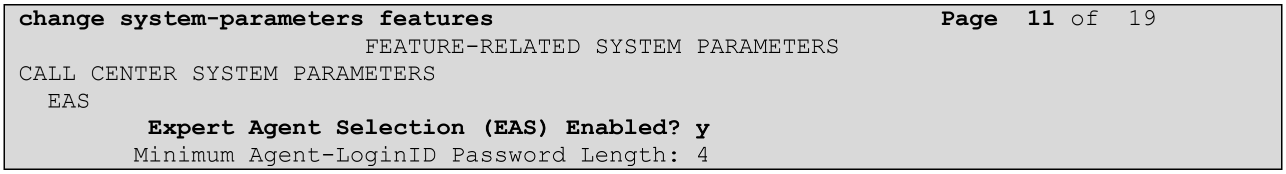
```
change agent-loginID 20001                                      Page   1 of   2
                                 AGENT LOGINID

                Login ID: 20001                                   AAS? n
                    Name: Agent 1                               AUDIX? n
                      TN: 1                             LWC Reception: spe
                     COR: 1                    LWC Log External Calls? n
           Coverage Path:                    AUDIX Name for Messaging:
           Security Code:
                                         LoginID for ISDN/SIP Display? n
                                                             Password:
                                               Password (enter again):
                                                          Auto Answer: station
                                                    MIA Across Skills: system
                                            ACW Agent Considered Idle: system
                                            Aux Work Reason Code Type: system
                                              Logout Reason Code Type: system
                       Maximum time agent in ACW before logout (sec): system
                                             Forced Agent Logout Time:   :
```

The following abridged screen shows Page 2 for agent-loginID 20001. Note that the Skill Number (**SN**) has been set to 1.



```
change agent-loginID 20001                                      Page   2 of   2
                                 AGENT LOGINID
      Direct Agent Skill:                                  Service Objective? n
Call Handling Preference: skill-level                  Local Call Preference? n

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

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



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

5.10. Private Numbering

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

In the bolded rows shown in the example abridged output below, entries are made for the specific Communication Manager Vector Directory Numbers (VDN) illustrated in the prior section. Without this configuration, calls to the VDNs would result in a 5-digit user portion of the Contact header in the 183 with SDP and 200 OK returned to Verizon. Although this did not present any user-perceivable problem in the sample configuration, the configuration in the bolded rows below illustrate how to cause Communication Manager to populate the Contact header with user portions that correspond with a Verizon IPCC number. In the course of the testing, multiple Verizon toll-free numbers were associated with different Communication Manager extensions and functions.

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

Ext Ext              Trk        Private          Total
Len Code             Grp(s)     Prefix           Len
 5  10                                           5     Total Administered: 7
 5  12                                           5        Maximum Entries: 540
 5  14                                           5
 5  20                                           5
 5  10001            2          8668523221       10
 5  10003            2          8668510107       10
 5  10004            2          8668508170       10
```

5.11. Incoming Call Handling Treatment for Incoming Calls

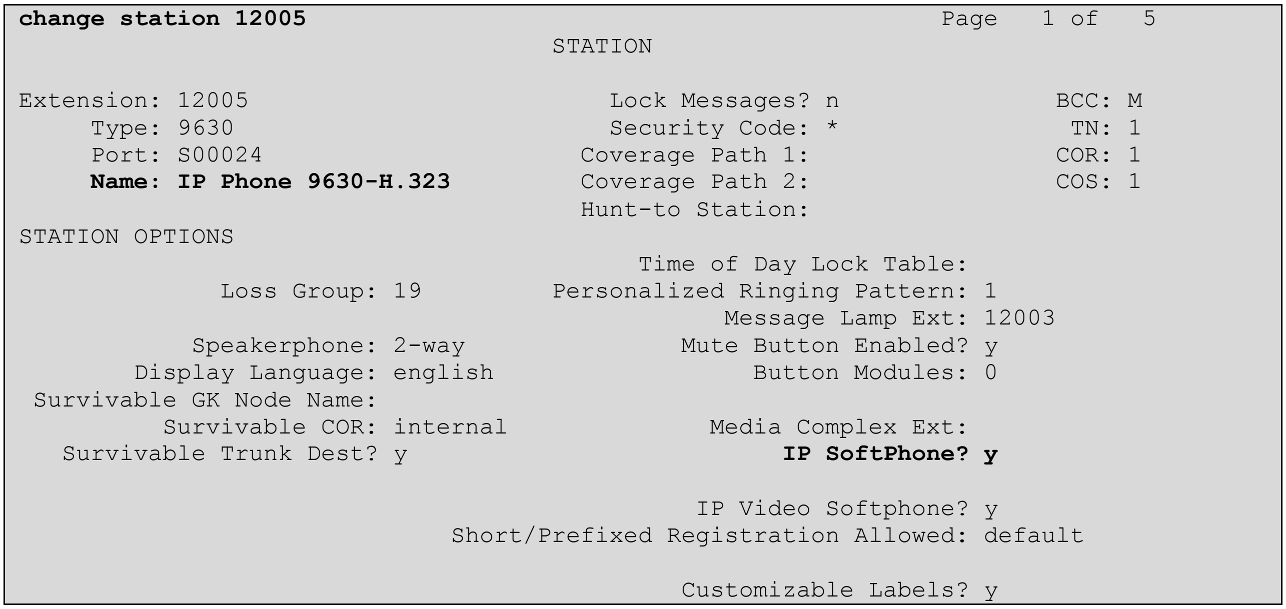
In general, the "incoming call handling treatment" for a trunk group can be used to manipulate the digits received for an incoming call if necessary. Since Session Manager is present, Session Manager can be used to perform digit conversion, and digit manipulation via the Communication Manager incoming 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 of the receiving trunk group. As an example, the following screen illustrates a conversion of toll-free number 8668502380 to extension 14000 when the call arrives on trunk group 1.

```
change inc-call-handling-trmt trunk-group 2                     Page   1 of  30
                       INCOMING CALL HANDLING TREATMENT
 Service/      Number   Number      Del Insert
 Feature        Len      Digits
 public-ntwrk    10 8668502380       10  14000

```

5.12. Communication Manager Stations

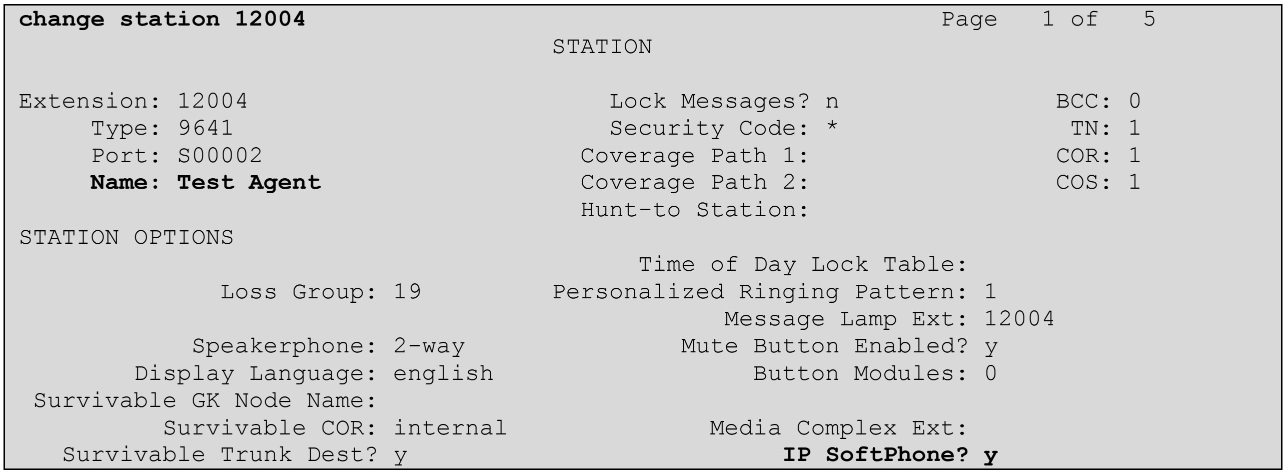
In the sample configuration, five digit station extensions were used with the format 120xx. Since this configuration is not unique to Verizon, a minimum of information is presented simply to assist in understanding verification traces presented in subsequent sections.

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



```
change station 12005                                            Page   1 of   5
                                     STATION

Extension: 12005                         Lock Messages? n                BCC: M
     Type: 9630                          Security Code: *                 TN: 1
     Port: S00024                      Coverage Path 1:                 COR: 1
     Name: IP Phone 9630-H.323         Coverage Path 2:                 COS: 1
                                       Hunt-to Station:
STATION OPTIONS
                                           Time of Day Lock Table:
              Loss Group: 19         Personalized Ringing Pattern: 1
                                                 Message Lamp Ext: 12003
            Speakerphone: 2-way                Mute Button Enabled? y
        Display Language: english                   Button Modules: 0
 Survivable GK Node Name:
          Survivable COR: internal                Media Complex Ext:
   Survivable Trunk Dest? y                             IP SoftPhone? y

                                               IP Video Softphone? y
                              Short/Prefixed Registration Allowed: default

                                              Customizable Labels? y
```

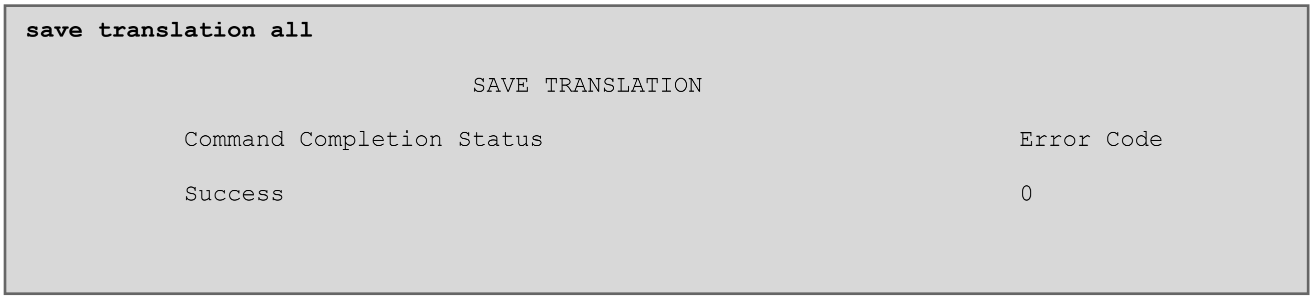
The following abbreviated screen shows an example extension used by an Avaya one-X® Agent client. Call appearances and appropriate features (e.g., uui-info, aux-work, etc.) can be assigned on page 4 (not shown).



```
change station 12004                                            Page   1 of   5
                                     STATION

Extension: 12004                         Lock Messages? n                BCC: 0
     Type: 9641                          Security Code: *                 TN: 1
     Port: S00002                      Coverage Path 1:                 COR: 1
     Name: Test Agent                  Coverage Path 2:                 COS: 1
                                       Hunt-to Station:
STATION OPTIONS
                                           Time of Day Lock Table:
              Loss Group: 19         Personalized Ringing Pattern: 1
                                                 Message Lamp Ext: 12004
            Speakerphone: 2-way                Mute Button Enabled? y
        Display Language: english                   Button Modules: 0
 Survivable GK Node Name:
          Survivable COR: internal                Media Complex Ext:
   Survivable Trunk Dest? y                             IP SoftPhone? y
```

5.13. Saving Communication Manager Configuration Changes

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



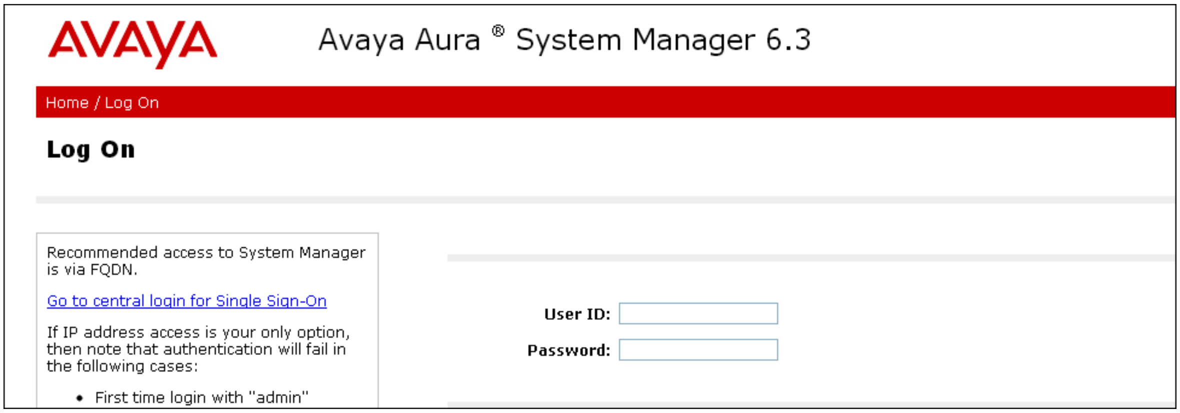
```
save translation all

                               SAVE TRANSLATION

           Command Completion Status                                 Error Code

           Success                                                   0
```

6. Configure Avaya Aura® Session Manager Release 6.3

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 (not shown).



Avaya Aura ® System Manager 6.3

Home / Log On

Log On

Recommended access to System Manager is via FQDN.

Go to central login for Single Sign-On

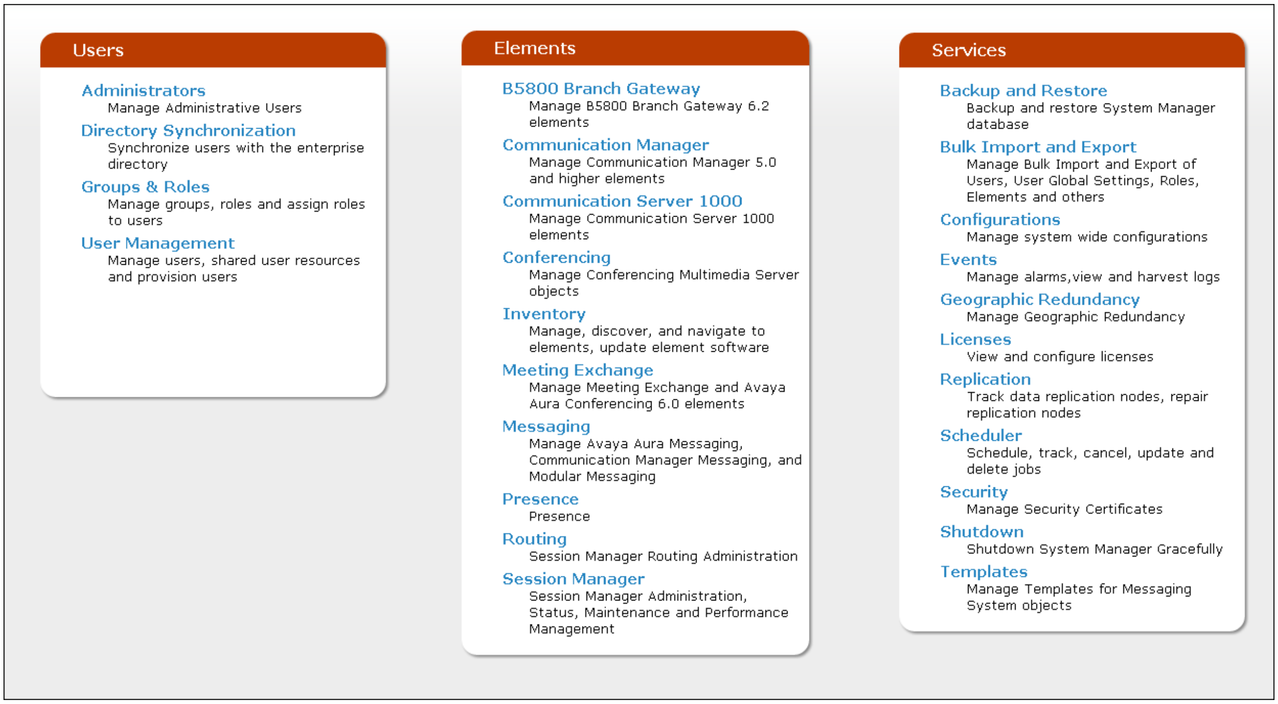
If IP address access is your only option, then note that authentication will fail in the following cases:

- First time login with "admin"

User ID:

Password:

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



Users

Administrators
Manage Administrative Users

Directory Synchronization
Synchronize users with the enterprise directory

Groups & Roles
Manage groups, roles and assign roles to users

User Management
Manage users, shared user resources and provision users

Elements

B5800 Branch Gateway
Manage B5800 Branch Gateway 6.2 elements

Communication Manager
Manage Communication Manager 5.0 and higher elements

Communication Server 1000
Manage Communication Server 1000 elements

Conferencing
Manage Conferencing Multimedia Server objects

Inventory
Manage, discover, and navigate to elements, update element software

Meeting Exchange
Manage Meeting Exchange and Avaya Aura Conferencing 6.0 elements

Messaging
Manage Avaya Aura Messaging, Communication Manager Messaging, and Modular Messaging

Presence
Presence

Routing
Session Manager Routing Administration

Session Manager
Session Manager Administration, Status, Maintenance and Performance Management

Services

Backup and Restore
Backup and restore System Manager database

Bulk Import and Export
Manage Bulk Import and Export of Users, User Global Settings, Roles, Elements and others

Configurations
Manage system wide configurations

Events
Manage alarms,view and harvest logs

Geographic Redundancy
Manage Geographic Redundancy

Licenses
View and configure licenses

Replication
Track data replication nodes, repair replication nodes

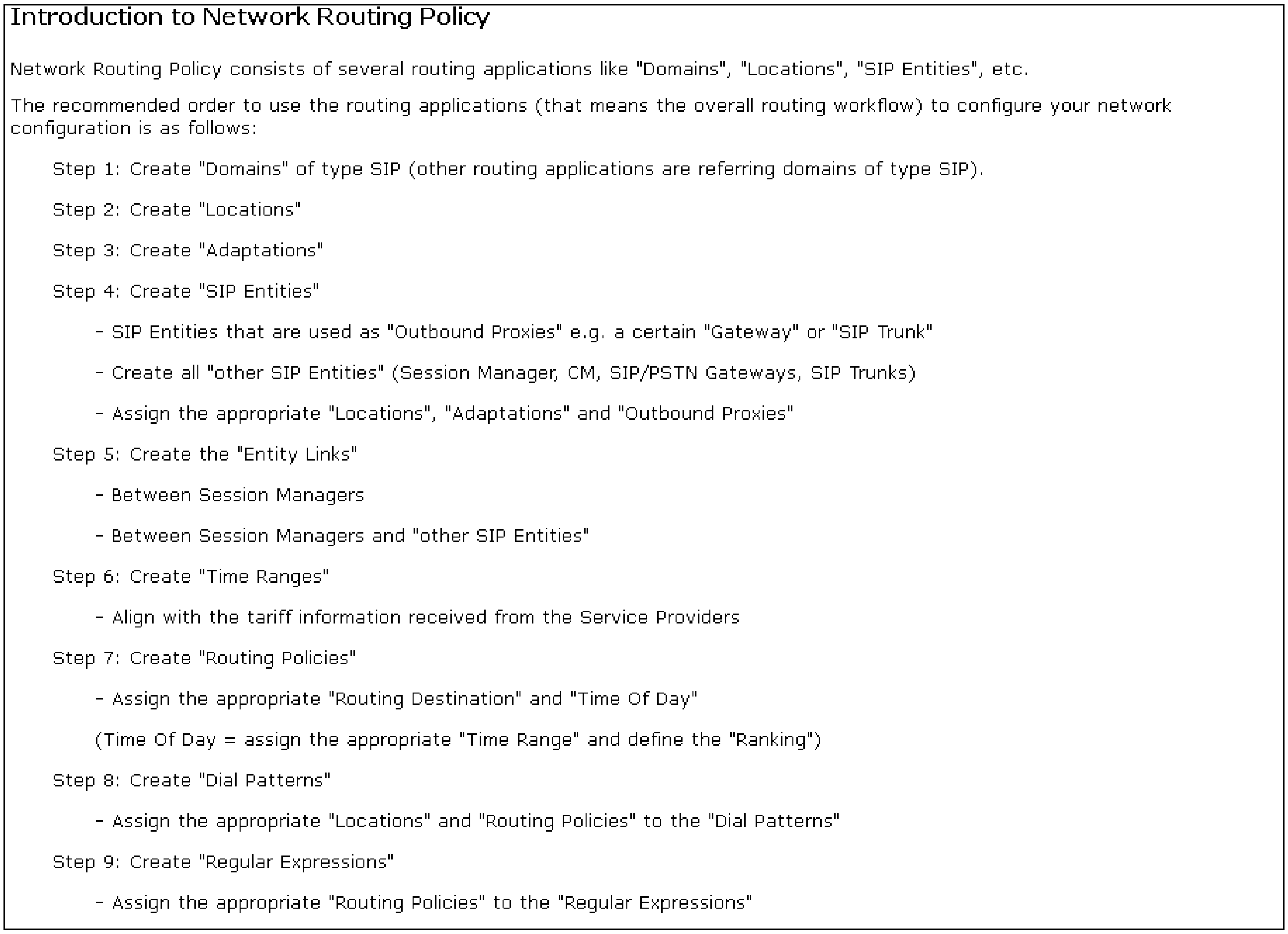
Scheduler
Schedule, track, cancel, update and delete jobs

Security
Manage Security Certificates

Shutdown
Shutdown System Manager Gracefully

Templates
Manage Templates for Messaging System objects

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



Introduction to Network Routing Policy

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

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

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

Step 2: Create "Locations"

Step 3: Create "Adaptations"

Step 4: Create "SIP Entities"

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

Step 5: Create the "Entity Links"

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

Step 6: Create "Time Ranges"

- Align with the tariff information received from the Service Providers

Step 7: Create "Routing Policies"

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

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

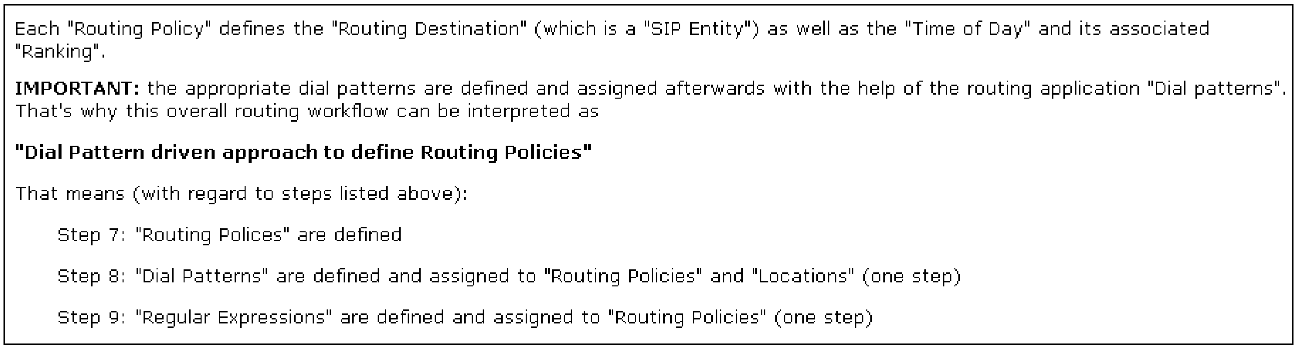
Step 8: Create "Dial Patterns"

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

Step 9: Create "Regular Expressions"

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

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



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

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

"Dial Pattern driven approach to define Routing Policies"

That means (with regard to steps listed above):

Step 7: "Routing Polices" are defined

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

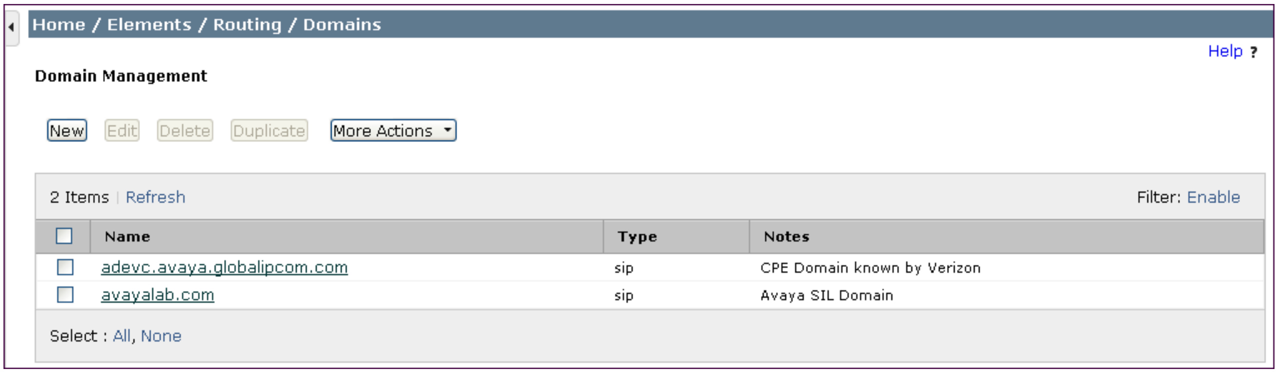
Step 9: "Regular Expressions" are defined and assigned to "Routing Policies" (one step)

6.1. Domains

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

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

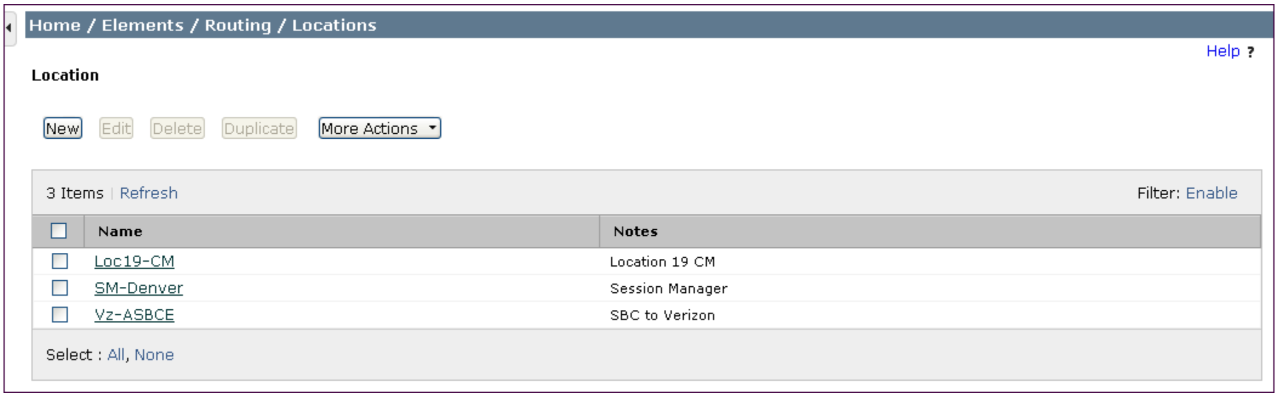
The domain "adevc.avaya.globalipcom.com" is the domain known to Verizon as the enterprise SIP domain. For example, for calls from the enterprise site to Verizon, this domain can appear in the From and P-Asserted-Identity headers in the INVITE message sent to Verizon.



□	Name	Type	Notes
□	adevc.avaya.globalipcom.com	sip	CPE Domain known by Verizon
□	avayalab.com	sip	Avaya SIL Domain

6.2. Locations

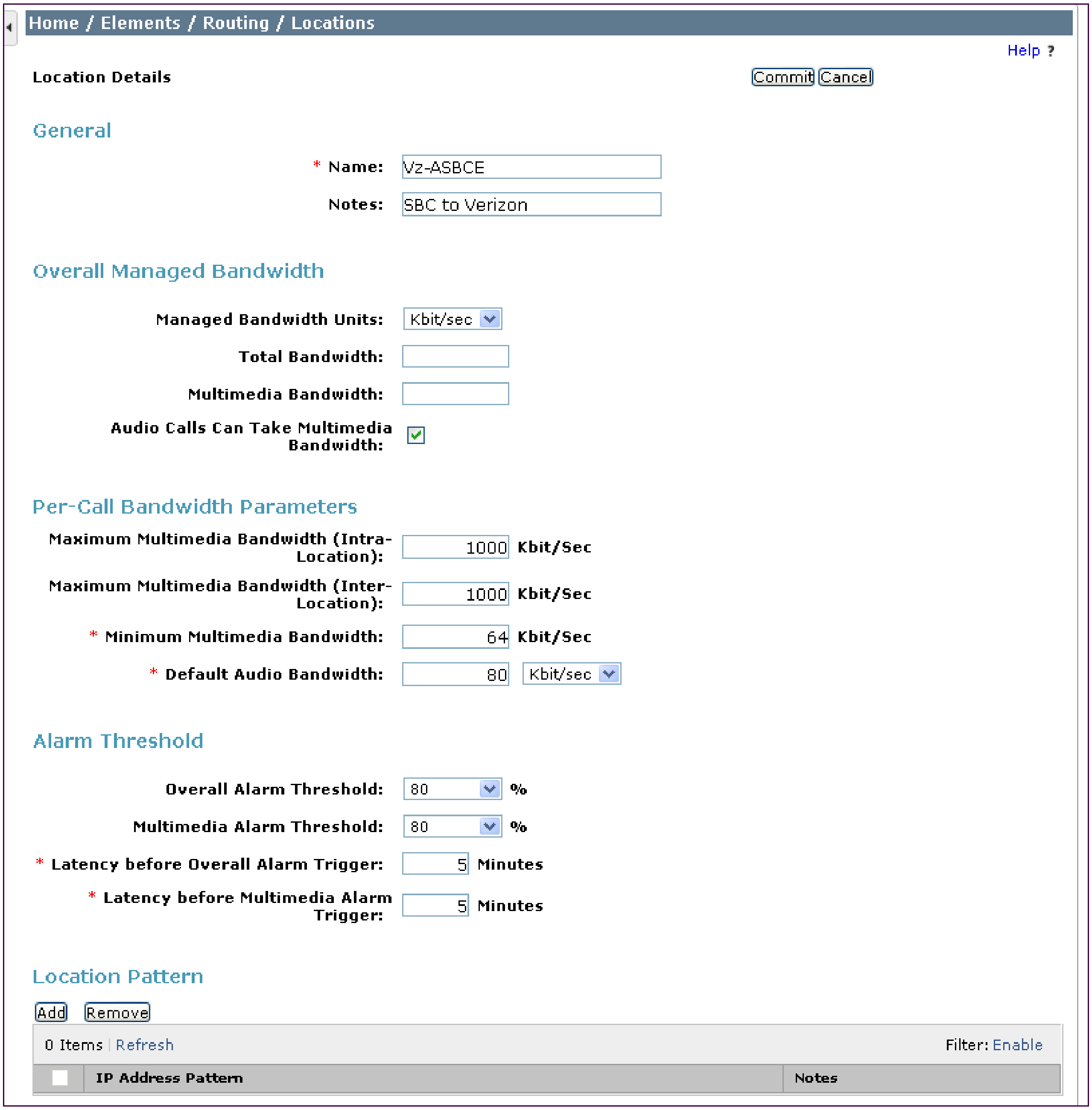
To view or change locations, select **Routing → Locations**. The following screen shows an abridged list of configured locations. Click on the checkbox corresponding to the name of a location and **Edit** to edit an existing location, or the **New** button to add a location. Click the **Commit** button (not shown) after changes are completed. Assigning unique locations can allow Session Manager to perform location-based routing, bandwidth management, and call admission control.



□	Name	Notes
□	Loc19-CM	Location 19 CM
□	SM-Denver	Session Manager
□	Vz-ASBCE	SBC to Verizon

The following screen shows the location details for the location named “Vz-ASBCE”, corresponding to the Avaya SBCE relevant to these Application Notes. Later, the location with name “Vz-ASBCE” will be assigned to the corresponding Avaya SBCE SIP Entity.

The **Location Pattern** is used to identify call routing based on IP address. Session Manager matches the IP address of SIP Entities 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 in the SIP Entity form. In this sample configuration Locations are added to SIP Entities in **Section 6.4**, so it was not necessary to add a pattern.



Location Details

General

* Name: Vz-ASBCE

Notes: SBC to Verizon

Overall Managed Bandwidth

Managed Bandwidth Units: Kbit/sec

Total Bandwidth:

Multimedia Bandwidth:

Audio Calls Can Take Multimedia Bandwidth: ☑

Per-Call Bandwidth Parameters

Maximum Multimedia Bandwidth (Intra-Location): 1000 Kbit/Sec

Maximum Multimedia Bandwidth (Inter-Location): 1000 Kbit/Sec

* Minimum Multimedia Bandwidth: 64 Kbit/Sec

* Default Audio Bandwidth: 80 Kbit/sec

Alarm Threshold

Overall Alarm Threshold: 80 %

Multimedia Alarm Threshold: 80 %

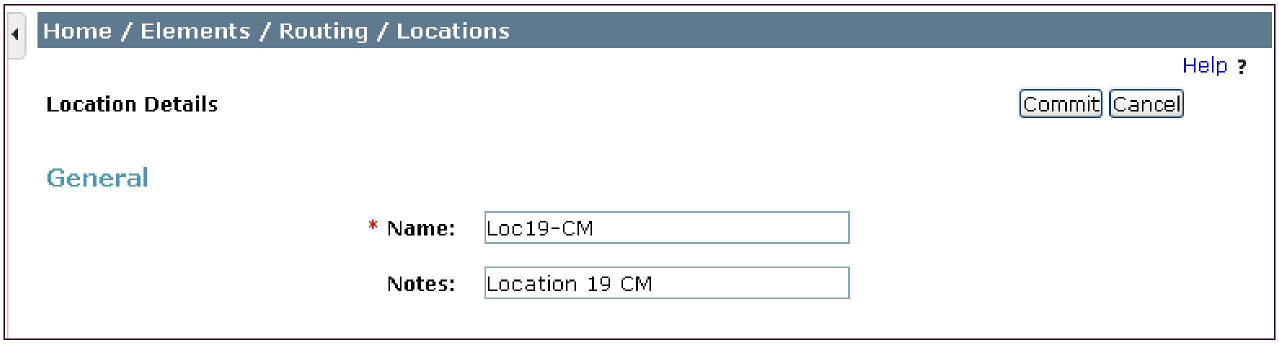
* Latency before Overall Alarm Trigger: 5 Minutes

* Latency before Multimedia Alarm Trigger: 5 Minutes

Location Pattern

□	IP Address Pattern	Notes

The location named “Loc19-CM” shown in the following screen will later be assigned to the corresponding Communication Manager SIP Entity. In the sample configuration, other location parameters (not shown) retained the default values.



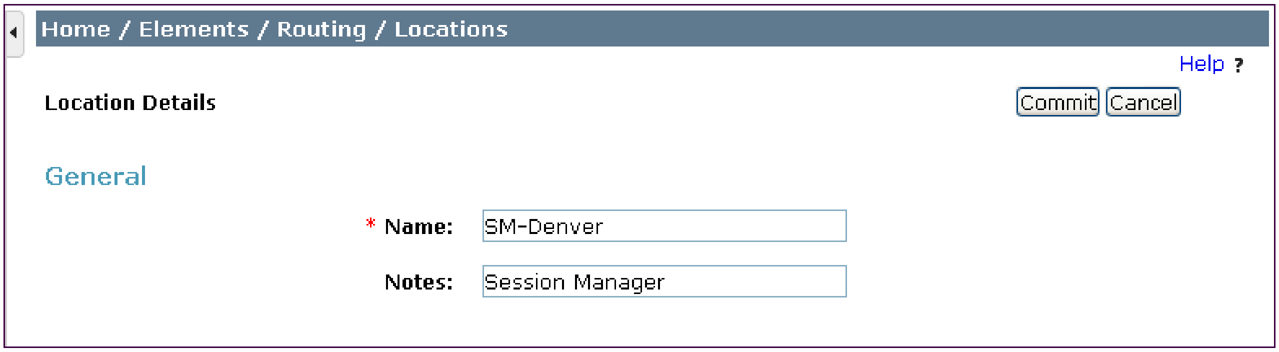
Location Details

General

* Name: Loc19-CM

Notes: Location 19 CM

The following screen shows the location details for the location named “SM-Denver”, corresponding to Session Manager. This location was created during the installation of Session Manager and was assigned to the Session Manager SIP Entity. In the sample configuration, other location parameters (not shown) retained the default values.



Location Details

General

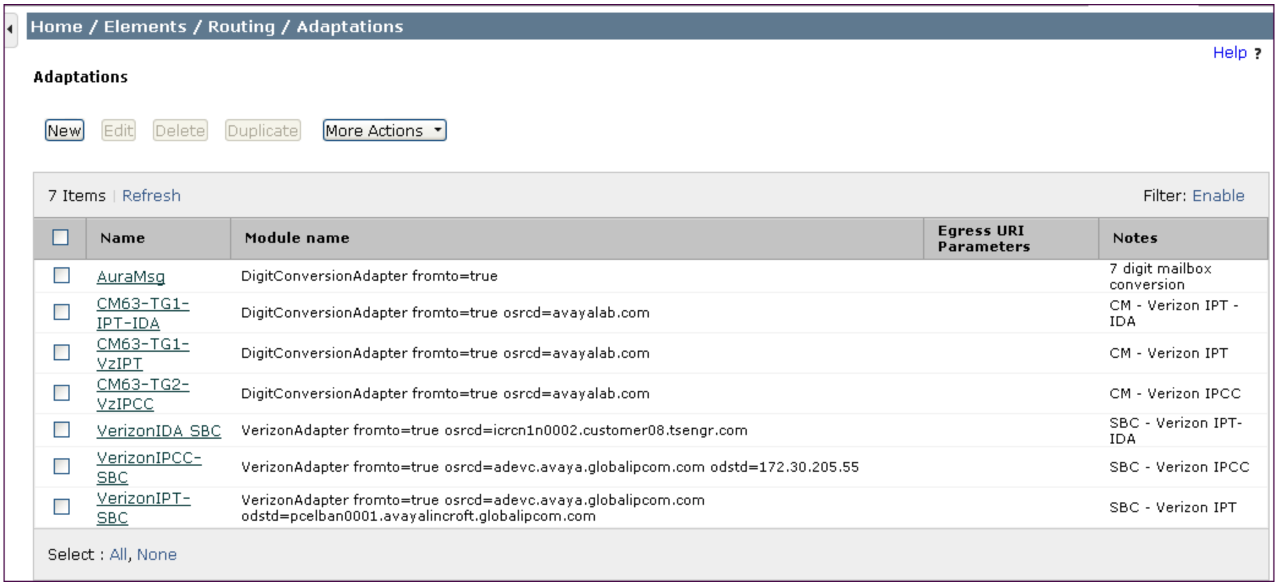
* Name: SM-Denver

Notes: Session Manager

6.3. Adaptations

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

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



Adaptations

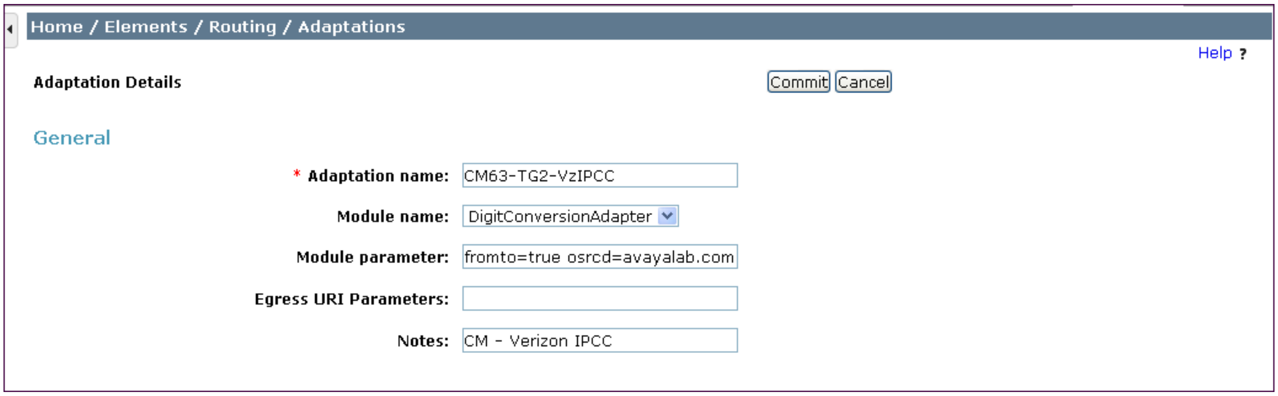
7 Items

□	Name	Module name	Egress URI Parameters	Notes
□	AuraMsg	DigitConversionAdapter fromto=true		7 digit mailbox conversion
□	CM63-TG1-IPT-IDA	DigitConversionAdapter fromto=true osrcd=avayalab.com		CM - Verizon IPT - IDA
□	CM63-TG1-VzIPT	DigitConversionAdapter fromto=true osrcd=avayalab.com		CM - Verizon IPT
□	CM63-TG2-VzIPCC	DigitConversionAdapter fromto=true osrcd=avayalab.com		CM - Verizon IPCC
□	VerizonIDA SBC	VerizonAdapter fromto=true osrcd=icrcn1n0002.customer08.tsengr.com		SBC - Verizon IPT-IDA
□	VerizonIPCC-SBC	VerizonAdapter fromto=true osrcd=adevc.avaya.globalipcom.com odstd=172.30.205.55		SBC - Verizon IPCC
□	VerizonIPT-SBC	VerizonAdapter fromto=true osrcd=adevc.avaya.globalipcom.com odstd=pcelban0001.avayalincroft.globalipcom.com		SBC - Verizon IPT

The adapter named "CM63-TG1-VzIPT" shown in the following screen will later be assigned to the SIP Entity linking Session Manager to Communication Manager for calls involving Verizon Business IP Trunk service. This adaptation uses the "DigitConversionAdapter" and specifies the following parameters:

- "fromto=true". This adapts the From and To headers along with the Request-Line and PAI headers.
- "osrcd=avayalab.com". This enables the source domain to be overwritten with "avayalab.com". For example, for inbound PSTN calls from Verizon to Communication Manager, the PAI header will contain "avayalab.com".

Depending on the Communication Manager configuration, it may not be necessary for Session Manager to adapt the domain in this fashion.



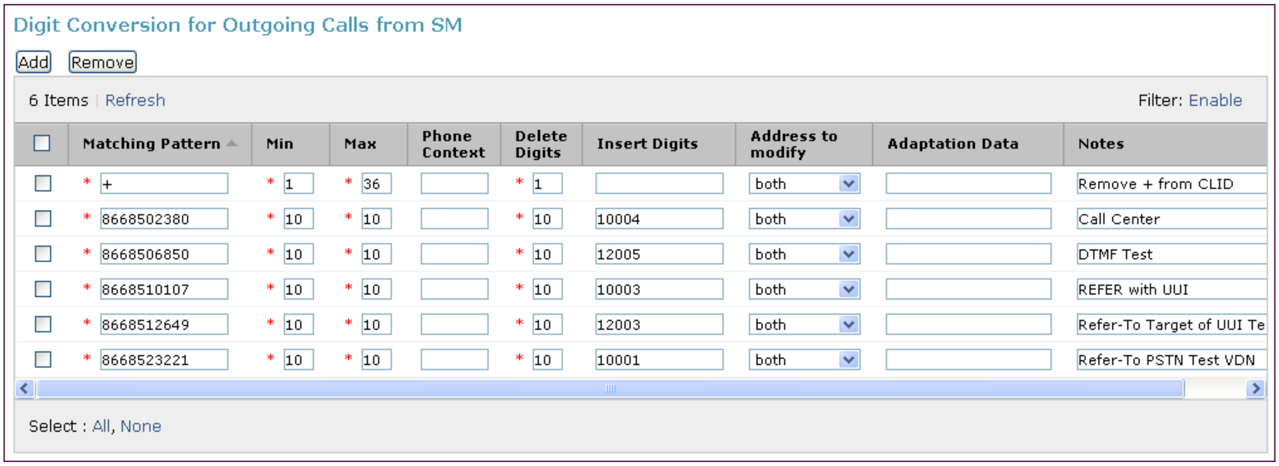
Adaptation Details

General

* Adaptation name:	CM63-TG2-VzIPCC
Module name:	DigitConversionAdapter
Module parameter:	fromto=true osrcd=avayalab.com
Egress URI Parameters:	
Notes:	CM - Verizon IPCC

Scrolling down, the following screen shows a portion of the "CM63-TG2-VzIPCC" adapter that can be used to convert digits between the Communication Manager extension numbers (user extensions, VDNs) and the toll-free numbers assigned by Verizon.

An example portion of the settings for "Digit Conversion for Outgoing Calls from SM" (i.e., inbound to Communication Manager) is shown below. During the testing, this digit conversion was varied to allow the same toll-free number to be used to test different Communication Manager destinations.



Digit Conversion for Outgoing Calls from SM

Add Remove

6 Items | Refresh Filter: Enable

□	Matching Pattern	Min	Max	Phone Context	Delete Digits	Insert Digits	Address to modify	Adaptation Data	Notes
□	* +	* 1	* 36		* 1		both		Remove + from CLID
□	* 8668502380	* 10	* 10		* 10	10004	both		Call Center
□	* 8668506850	* 10	* 10		* 10	12005	both		DTMF Test
□	* 8668510107	* 10	* 10		* 10	10003	both		REFER with UUI
□	* 8668512649	* 10	* 10		* 10	12003	both		Refer-To Target of UUI Te
□	* 8668523221	* 10	* 10		* 10	10001	both		Refer-To PSTN Test VDN

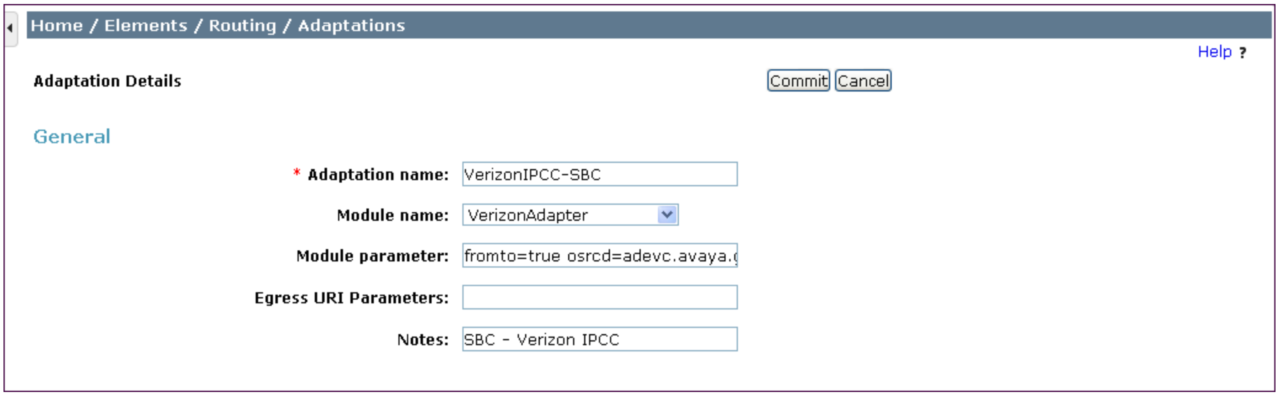
Select : All, None

In general, digit conversion such as this that converts a Verizon IPCC number to a Communication Manager extension can be performed in Communication Manager or in Session Manager. In the example screens shown above, before sending the SIP INVITE to Communication Manager, Session Manager would adapt a dialed number of 8668510107 to the VDN 10003 associated with testing Refer with UUI. As such, it would not be necessary to use the incoming call handling table of the receiving Communication Manager trunk group to convert the toll-free number to its corresponding extension

The adapter named “VerizonIPCC-SBC” shown below will later be assigned to the SIP Entity for the Avaya SBCE, specifying that all communication from Session Manager to the Avaya SBCEs will use this adapter.

This adaptation uses the “VerizonAdapter” module and specifies the following parameters:

- “fromto=true”. This adapts the From and To headers along with the Request-Line and PAI headers.
- “osrcd=adevc.avaya.globalipcom.com”. This enables the source domain to be overwritten with “adevc.avaya.globalipcom.com”. For example, for outbound PSTN calls from the Avaya CPE to Verizon, the PAI header will contain “adevc.avaya.globalipcom.com” as expected by Verizon.
- “odstd=172.30.205.55”. This enables the destination domain to be overwritten with “172.30.205.55”, the Verizon IPCC service node IP Address.

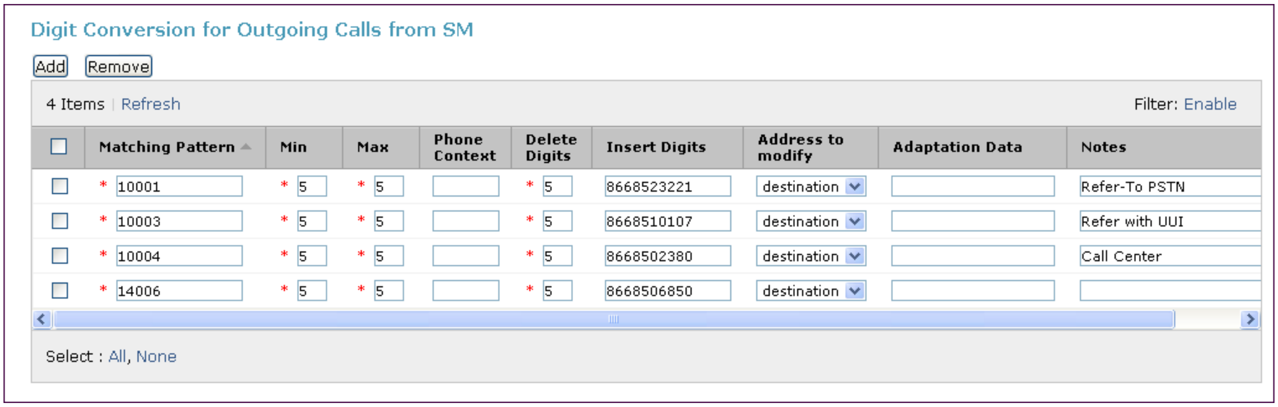


Adaptation Details

General

* Adaptation name:	VerizonIPCC-SBC
Module name:	VerizonAdapter
Module parameter:	fromto=true osrcd=adevc.avaya.(
Egress URI Parameters:	
Notes:	SBC - Verizon IPCC

Scrolling down, the following screen shows an abridged portion of the settings for “Digit Conversion for Outgoing Calls from SM”. Although the direction of actual calls involving Verizon IPCC service are “inbound” to Communication Manager, SIP headers in responses from Communication Manager can be adapted using the “Digit Conversion for Outgoing Calls from SM” area of the “VerizonIPCC-SBC” adaptation.



Digit Conversion for Outgoing Calls from SM

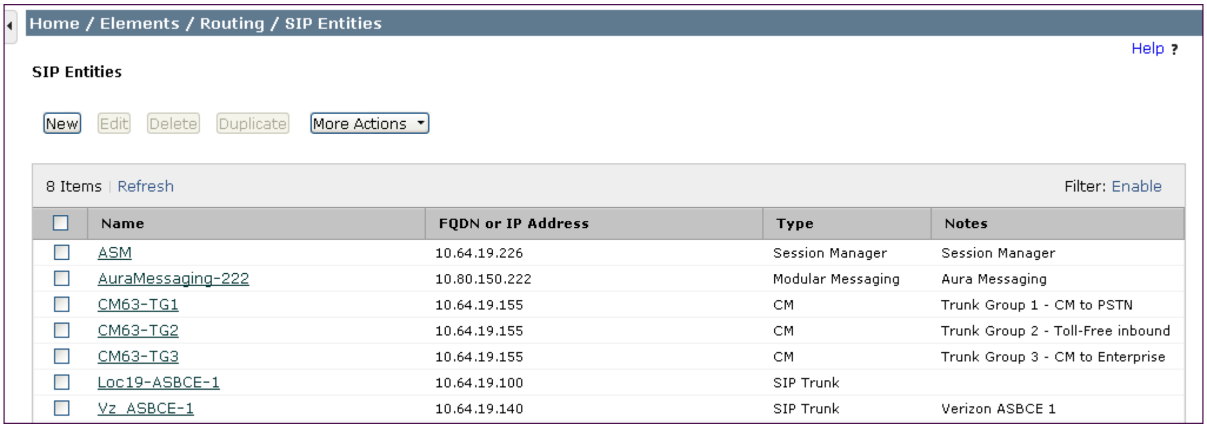
4 Items

□	Matching Pattern	Min	Max	Phone Context	Delete Digits	Insert Digits	Address to modify	Adaptation Data	Notes
□	* 10001	* 5	* 5		* 5	8668523221	destination		Refer-To PSTN
□	* 10003	* 5	* 5		* 5	8668510107	destination		Refer with UUI
□	* 10004	* 5	* 5		* 5	8668502380	destination		Call Center
□	* 14006	* 5	* 5		* 5	8668506850	destination		

6.4. SIP Entities

To view or change SIP entities, select **Routing → SIP Entities**. Click the checkbox corresponding to the name of an entity and **Edit** to edit an existing entity, or the **New** button to add an entity. Click the **Commit** button after changes are completed.

The following screen shows the list of configured SIP entities in the shared test environment.

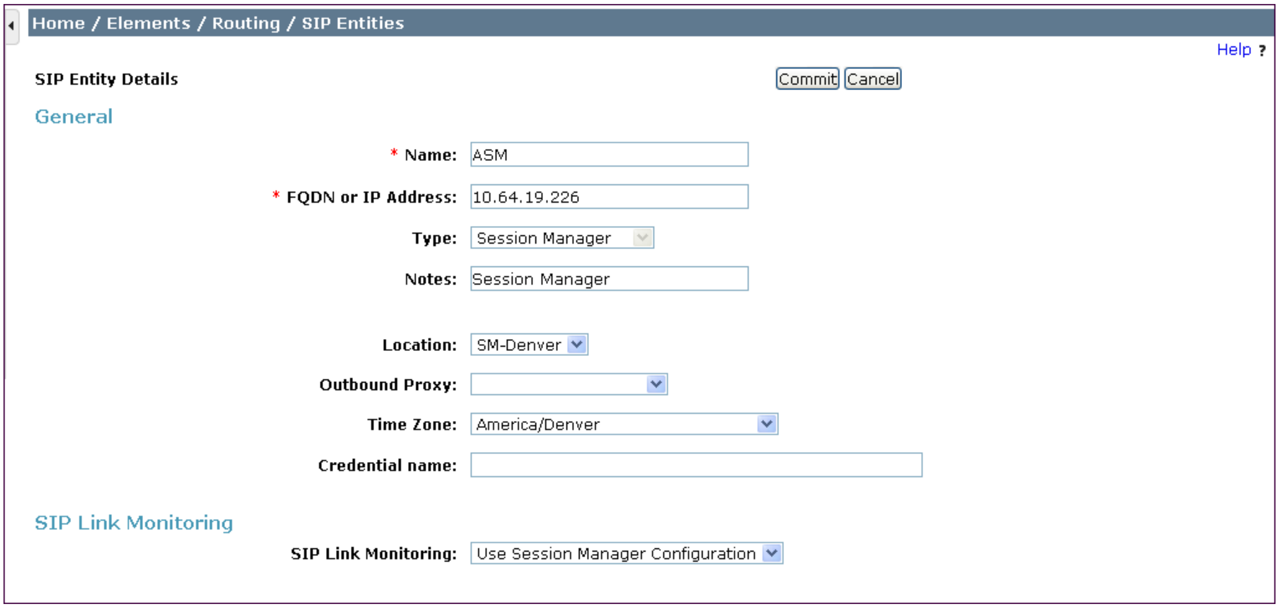


SIP Entities

8 Items

□	Name	FQDN or IP Address	Type	Notes
□	ASM	10.64.19.226	Session Manager	Session Manager
□	AuraMessaging-222	10.80.150.222	Modular Messaging	Aura Messaging
□	CM63-TG1	10.64.19.155	CM	Trunk Group 1 - CM to PSTN
□	CM63-TG2	10.64.19.155	CM	Trunk Group 2 - Toll-Free inbound
□	CM63-TG3	10.64.19.155	CM	Trunk Group 3 - CM to Enterprise
□	Loc19-ASBCE-1	10.64.19.100	SIP Trunk	
□	Vz_ASBCE-1	10.64.19.140	SIP Trunk	Verizon ASBCE 1

The following screen shows the upper portion of the **SIP Entity Details** corresponding to "ASM". The **FQDN or IP Address** field for "ASM" is the Session Manager Security Module IP Address (10.64.19.226), which is used for SIP signaling with other networked SIP entities. The **Type** for this SIP entity is "Session Manager". Select an appropriate location for the Session Manager from the **Location** drop-down menu. In the shared test environment, the Session Manager used location "SM-Denver". The default **SIP Link Monitoring** parameters may be used. Unless changed elsewhere, links from other SIP entities to this instance of Session Manager will use the default SIP Link Monitoring timers, configurable at the Session Manager level. If desired, these timers may be customized for each entity.



SIP Entity Details

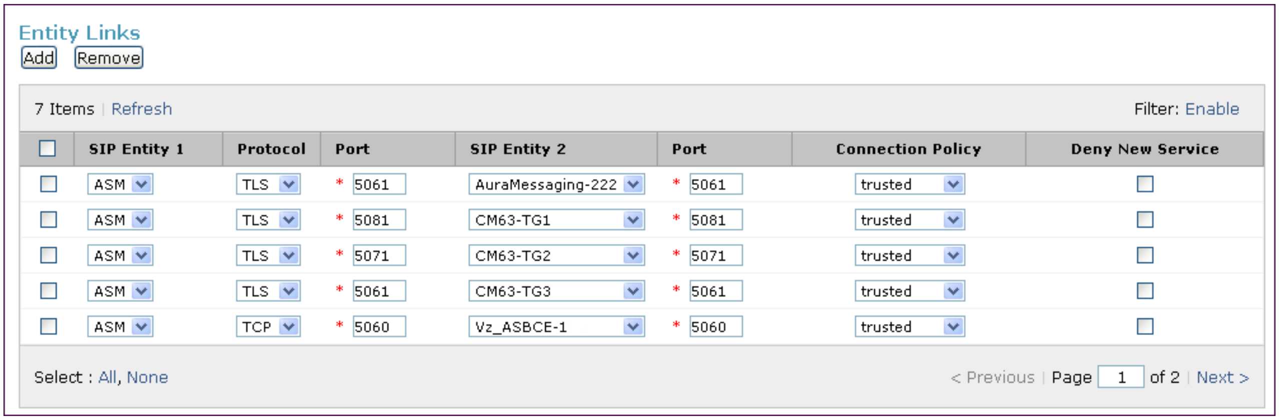
General

* Name:	ASM
* FQDN or IP Address:	10.64.19.226
Type:	Session Manager
Notes:	Session Manager
Location:	SM-Denver
Outbound Proxy:	
Time Zone:	America/Denver
Credential name:	

SIP Link Monitoring

SIP Link Monitoring:	Use Session Manager Configuration

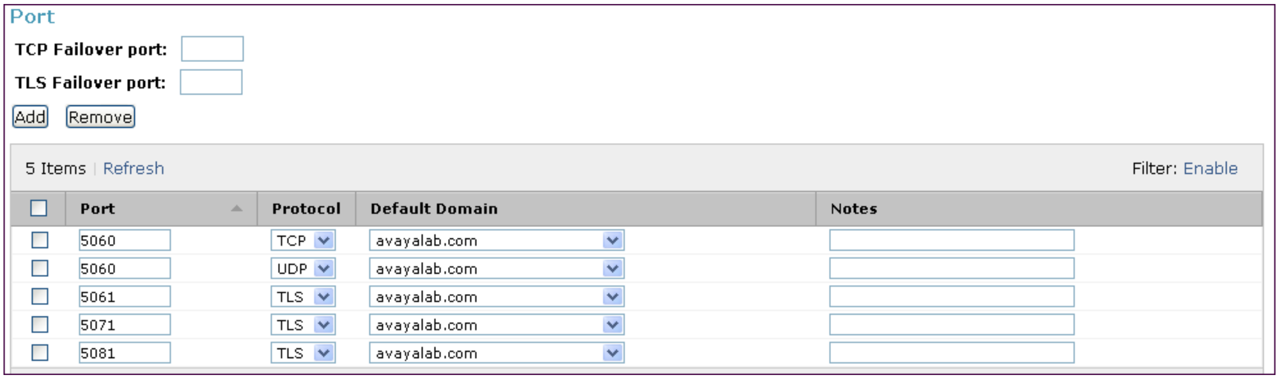
Scrolling down, the following screen shows the middle portion of the **SIP Entity Details**, a listing of the **Entity Links** previously configured for "ASM". The links relevant to these Application Notes are described in the subsequent section.



Entity Links

□	SIP Entity 1	Protocol	Port	SIP Entity 2	Port	Connection Policy	Deny New Service
□	ASM	TLS	* 5061	AuraMessaging-222	* 5061	trusted	□
□	ASM	TLS	* 5081	CM63-TG1	* 5081	trusted	□
□	ASM	TLS	* 5071	CM63-TG2	* 5071	trusted	□
□	ASM	TLS	* 5061	CM63-TG3	* 5061	trusted	□
□	ASM	TCP	* 5060	Vz_ASBCE-1	* 5060	trusted	□

Scrolling down, the following screen shows the lower portion of the **SIP Entity Details**, illustrating the configured ports for "ASM". 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.



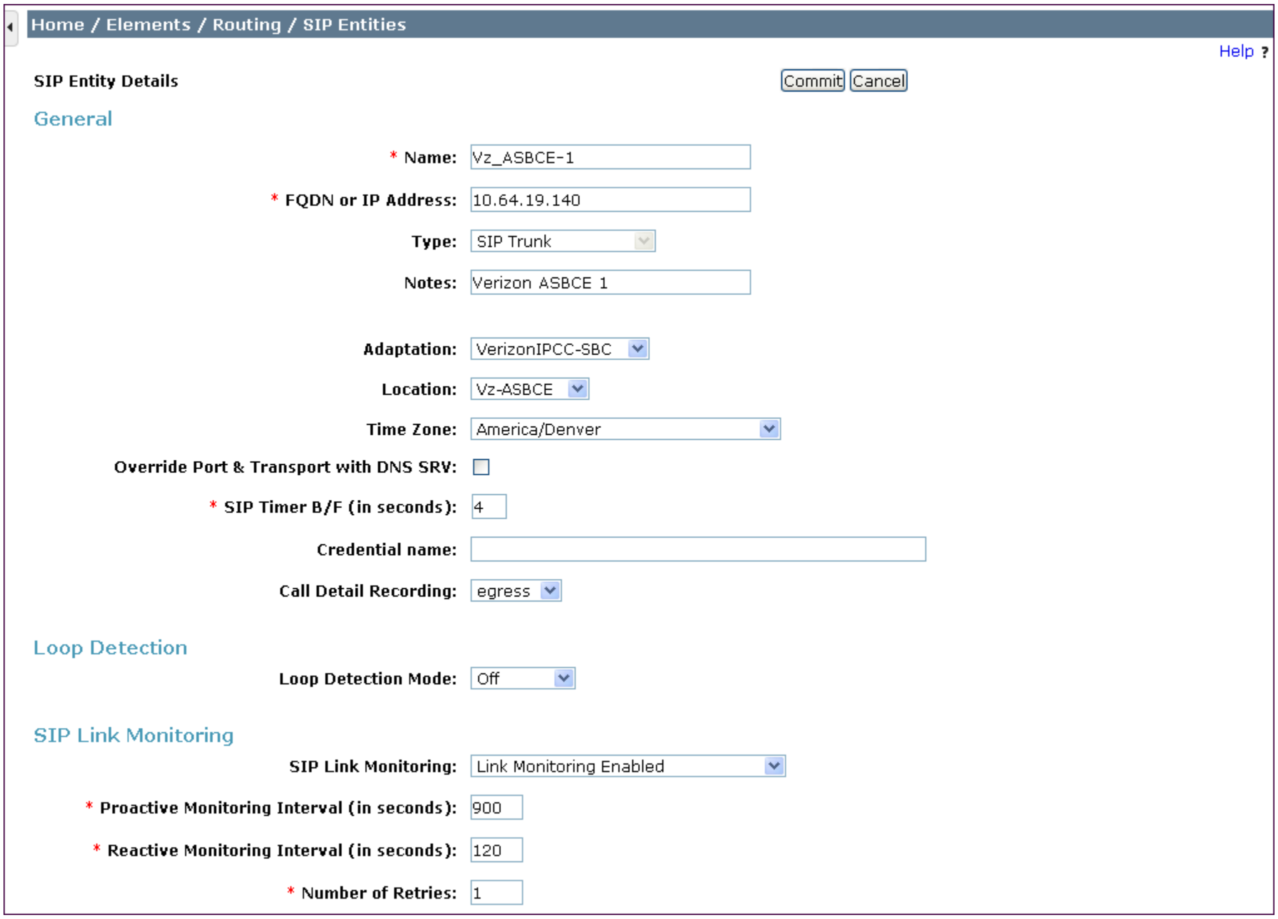
Port

TCP Failover port:

TLS Failover port:

□	Port	Protocol	Default Domain	Notes
□	5060	TCP	avayalab.com	
□	5060	UDP	avayalab.com	
□	5061	TLS	avayalab.com	
□	5071	TLS	avayalab.com	
□	5081	TLS	avayalab.com	

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 (10.64.19.140). "SIP Trunk" is selected from the **Type** drop-down menu. This Avaya SBCE has been assigned to **Location** "Vz-ASBCE", and the "VerizonIPCC-SBC" adapter is applied. Other parameters (not shown) retain default values.



SIP Entity Details

General

* Name:	Vz_ASBCE-1
* FQDN or IP Address:	10.64.19.140
Type:	SIP Trunk
Notes:	Verizon ASBCE 1
Adaptation:	VerizonIPCC-SBC
Location:	Vz-ASBCE
Time Zone:	America/Denver
Override Port & Transport with DNS SRV:	□
* SIP Timer B/F (in seconds):	4
Credential name:	
Call Detail Recording:	egress

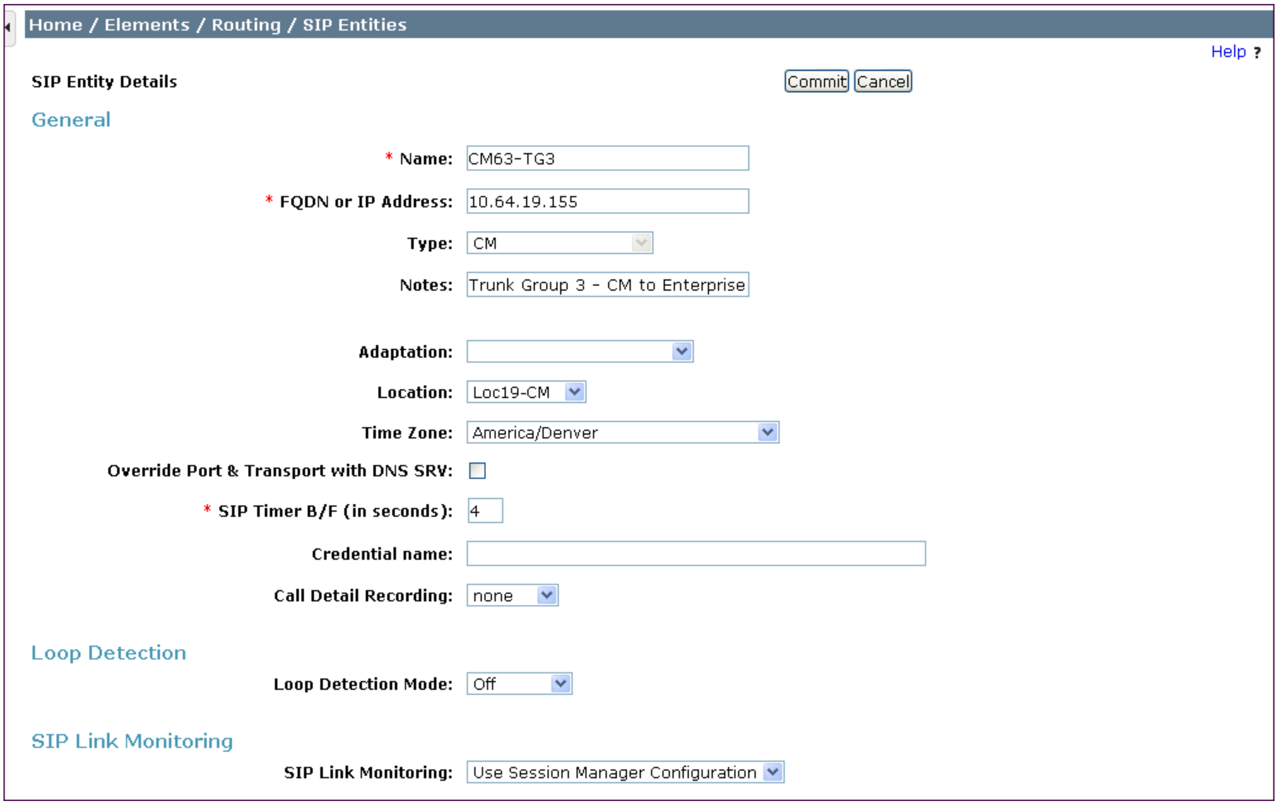
Loop Detection

Loop Detection Mode:	Off

SIP Link Monitoring

SIP Link Monitoring:	Link Monitoring Enabled
* Proactive Monitoring Interval (in seconds):	900
* Reactive Monitoring Interval (in seconds):	120
* Number of Retries:	1

The following screen shows a portion of the **SIP Entity Details** corresponding to a Communication Manager SIP Entity named “CM63-TG3” This is the SIP Entity that was already in place in the shared Avaya Interoperability Test Lab environment, prior to adding the Verizon IP Trunk configuration. The **FQDN or IP Address** field contains the IP Address of the “processor Ethernet” (10.64.19.155). In systems with Avaya G650 Media Gateways containing C-LAN cards, C-LAN cards may also be used as SIP entities, instead of, or in addition to, the “processor Ethernet”. “CM” is selected from the **Type** drop-down menu and “Loc19-CM” is selected for the **Location**.



SIP Entity Details

General

* Name: CM63-TG3

* FQDN or IP Address: 10.64.19.155

Type: CM

Notes: Trunk Group 3 - CM to Enterprise

Adaptation:

Location: Loc19-CM

Time Zone: America/Denver

Override Port & Transport with DNS SRV: □

* SIP Timer B/F (in seconds): 4

Credential name:

Call Detail Recording: none

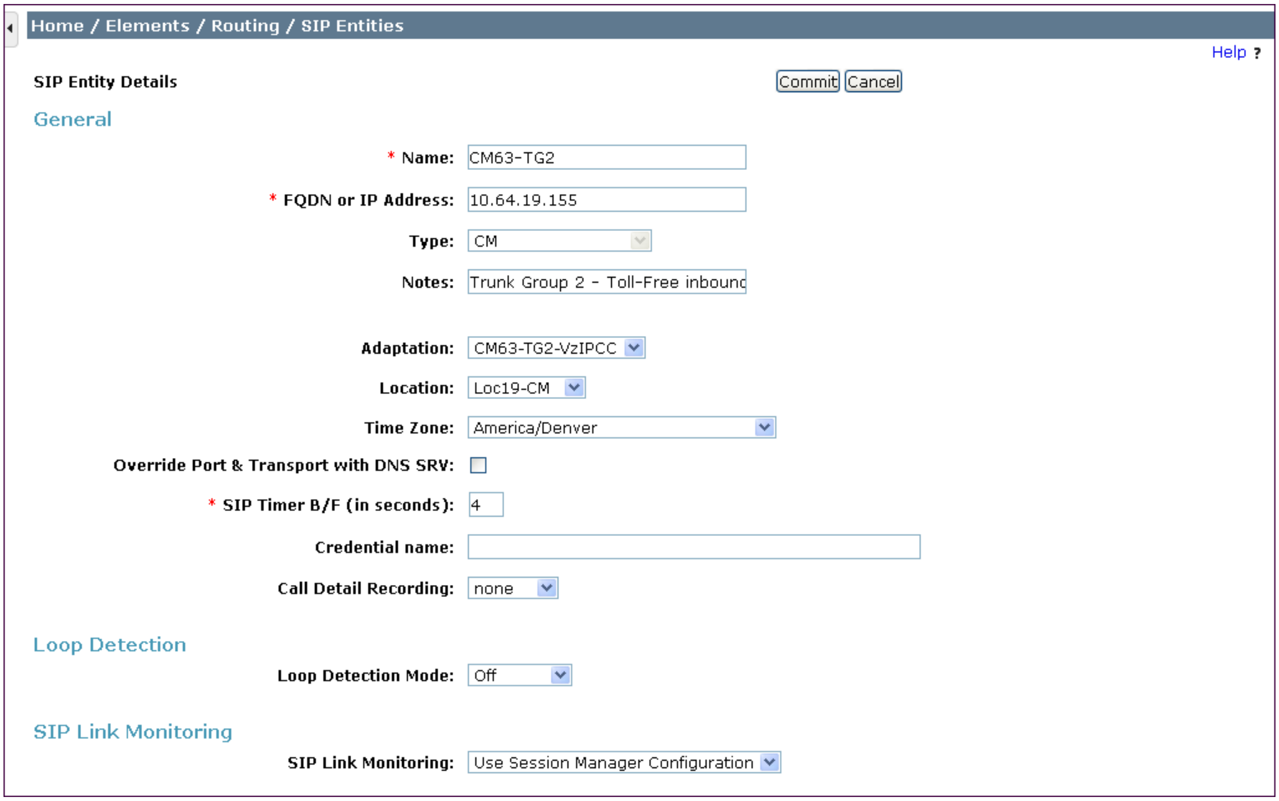
Loop Detection

Loop Detection Mode: Off

SIP Link Monitoring

SIP Link Monitoring: Use Session Manager Configuration

The following screen shows the **SIP Entity Details** for an entity named “CM63-TG2”. This entity uses the same **FQDN or IP Address** (10.64.19.155) as the prior entity with name “CM63-TG3”; both correspond to Communication Manager processor Ethernet IP address. Later, a unique port, 5071, will be used for the Entity Link to “CM63-TG2”. Using a different port is one approach that will allow Communication Manager to distinguish traffic originally from Verizon IPCC from other SIP traffic arriving from the same IP Address of the Session Manager, such as SIP traffic associated with SIP Telephones or other SIP-integrated applications. “CM” is selected from the **Type** drop-down menu. The **Adaptation** “CM63-TG2-VzIPCC” is applied to this SIP entity. Recall that this adapter is used to map the Verizon IPCC toll-free numbers to the corresponding Communication Manager extensions. “Loc19-CM” is selected for the **Location**.



SIP Entity Details

General

* Name: CM63-TG2

* FQDN or IP Address: 10.64.19.155

Type: CM

Notes: Trunk Group 2 - Toll-Free inbounc

Adaptation: CM63-TG2-VzIPCC

Location: Loc19-CM

Time Zone: America/Denver

Override Port & Transport with DNS SRV: □

* SIP Timer B/F (in seconds): 4

Credential name:

Call Detail Recording: none

Loop Detection

Loop Detection Mode: Off

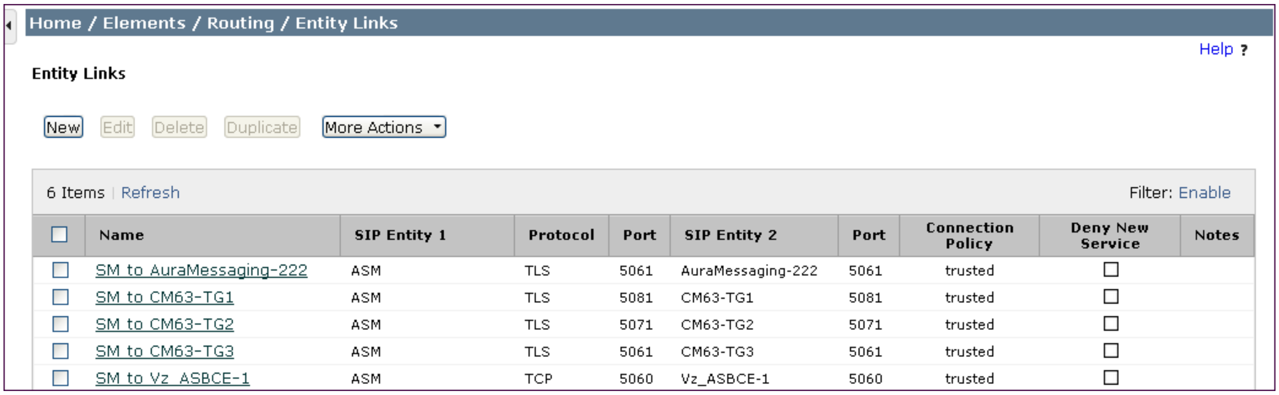
SIP Link Monitoring

SIP Link Monitoring: Use Session Manager Configuration

6.5. Entity Links

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

The following screen shows a list of configured links. In the screen below, the links named “SM to Vz_ASBCE-1” and “SM to CM63-TG2” are most relevant to these Application Notes. Each link uses the entity named “ASM” as **SIP Entity 1**, and the appropriate entity, such as “Vz_ASBCE-1”, for **SIP Entity 2**. Note that there are multiple SIP Entity Links, using different TLS ports, linking the same “ASM” with the processor Ethernet of Communication Manager. For example, for one link named “SM to CM63-TG3”, both entities use TLS and port 5061. For the entity link used by Verizon IPCC named “SM to CM63-TG2”, both entities use TLS and port 5071.



Entity Links

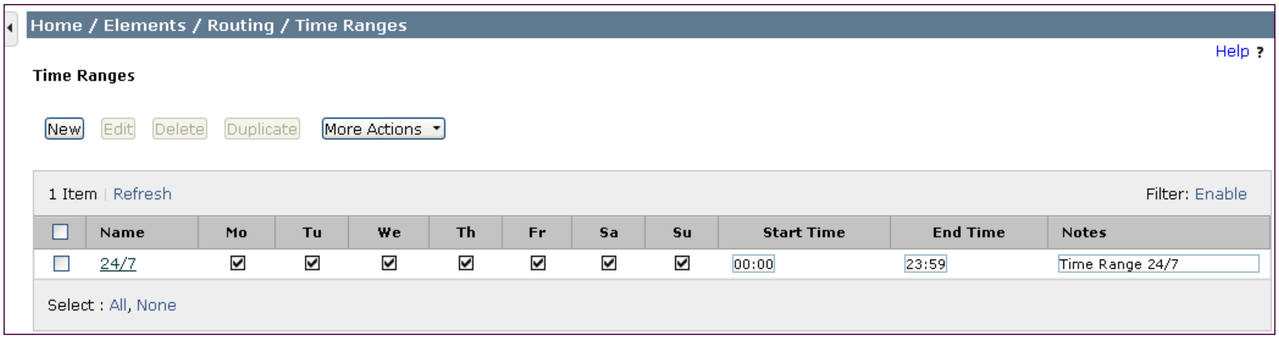
□	Name	SIP Entity 1	Protocol	Port	SIP Entity 2	Port	Connection Policy	Deny New Service	Notes
□	SM to AuraMessaging-222	ASM	TLS	5061	AuraMessaging-222	5061	trusted	□	
□	SM to CM63-TG1	ASM	TLS	5081	CM63-TG1	5081	trusted	□	
□	SM to CM63-TG2	ASM	TLS	5071	CM63-TG2	5071	trusted	□	
□	SM to CM63-TG3	ASM	TLS	5061	CM63-TG3	5061	trusted	□	
□	SM to Vz_ASBCE-1	ASM	TCP	5060	Vz_ASBCE-1	5060	trusted	□	

The link named “SM to CM63-TG3” links Session Manager “ASM” with Communication Manager processor Ethernet. This link existed in the configuration prior to adding the Verizon IPCC-related configuration. This link, using port 5061, can carry traffic between Session Manager and Communication Manager that is not necessarily related to calls with Verizon, such as traffic related to SIP Telephones registered to Session Manager.

The link named “SM to CM63-TG2” also links Session Manager “ASM” with Communication Manager processor Ethernet. However, this link uses port 5071 for both entities in the link. This link was created to allow Communication Manager to distinguish calls from Verizon IPCC from other calls that arrive from the same Session Manager. Other methods of distinguishing traffic could be used, if desired.

6.6. Time Ranges

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



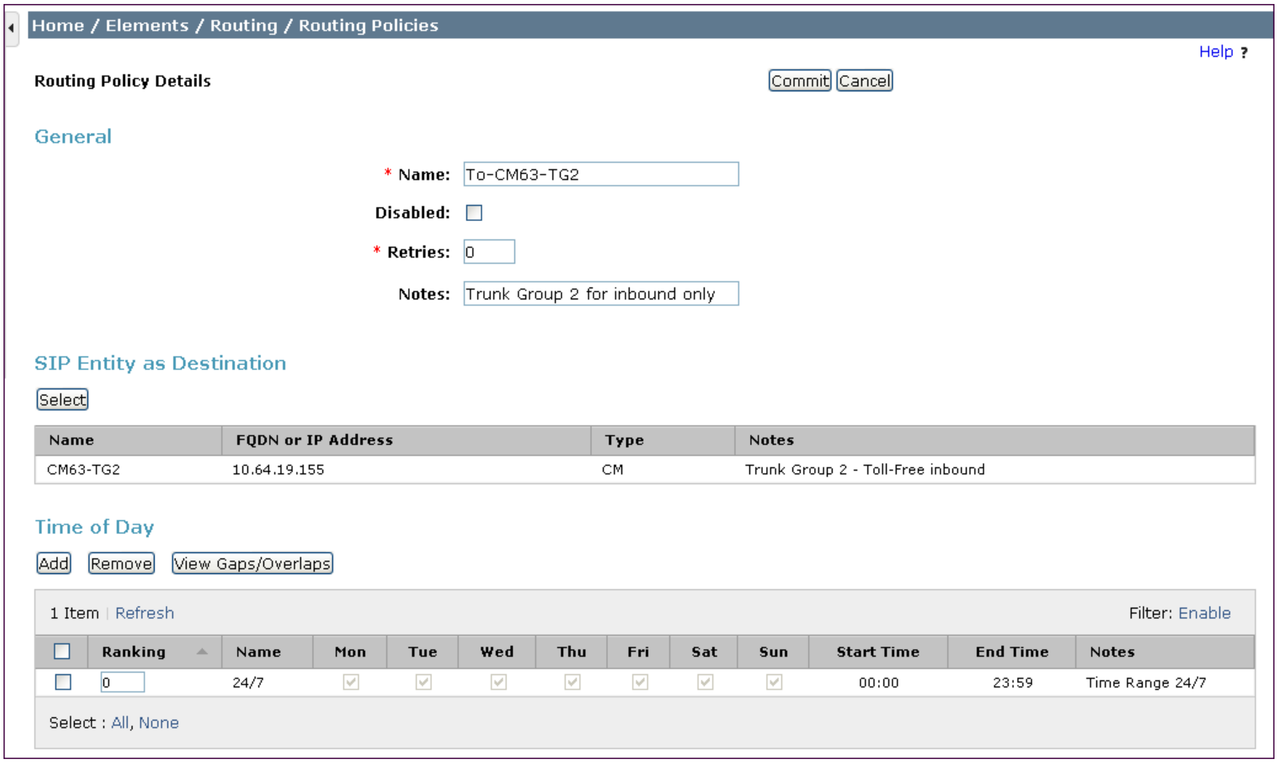
Time Ranges

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

6.7. Routing Policies

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

The following screen shows the **Routing Policy Details** for the policy named "To-CM63-TG2" associated with incoming toll-free calls from Verizon IPCC to Communication Manager. Observe the **SIP Entity as Destination** is the entity named "CM63-TG2".



Routing Policy Details

General

* Name: To-CM63-TG2
Disabled: □
* Retries: 0
Notes: Trunk Group 2 for inbound only

SIP Entity as Destination

Name	FQDN or IP Address	Type	Notes
CM63-TG2	10.64.19.155	CM	Trunk Group 2 - Toll-Free inbound

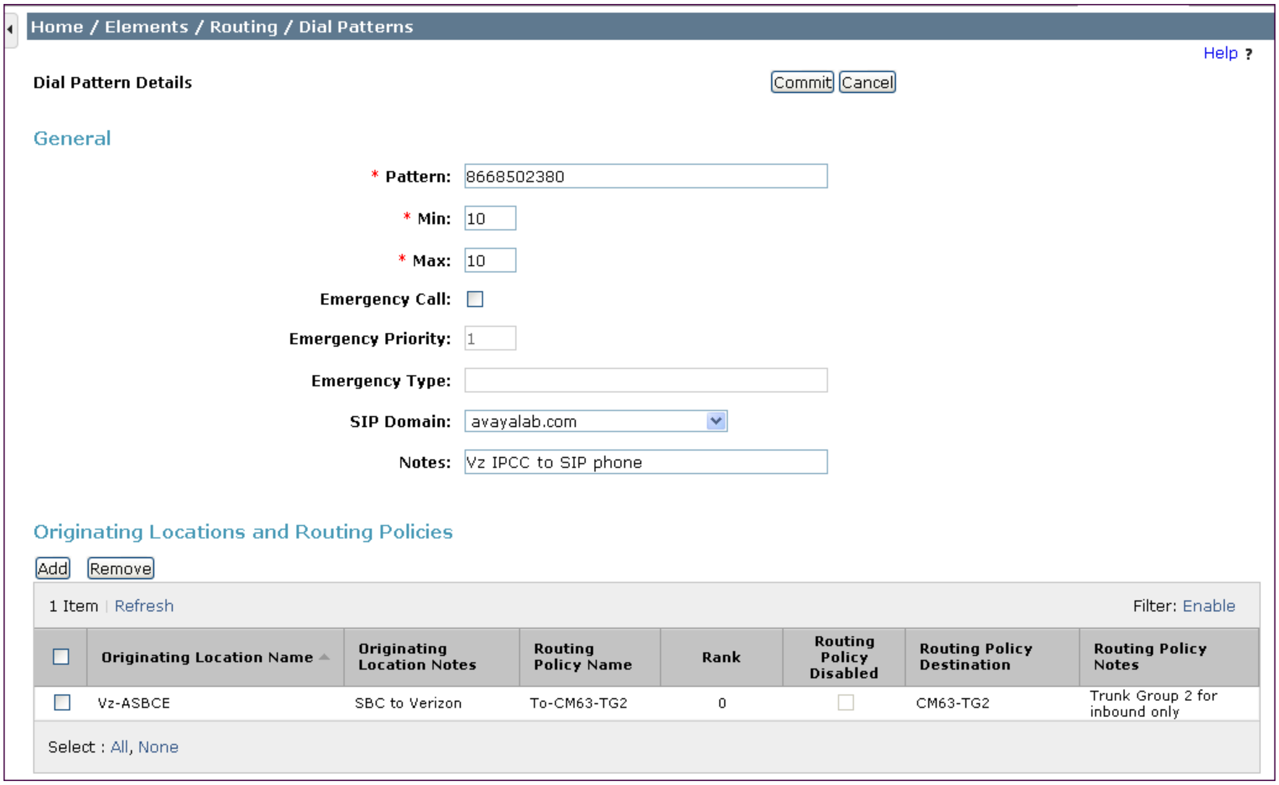
Time of Day

□	Ranking	Name	Mon	Tue	Wed	Thu	Fri	Sat	Sun	Start Time	End Time	Notes
□	0	24/7	☑	☑	☑	☑	☑	☑	☑	00:00	23:59	Time Range 24/7

6.8. Dial Patterns

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

The following screen illustrates an example dial pattern used to verify inbound PSTN calls to the enterprise. When a user on the PSTN dials a toll-free number such as 866-850-2380, Verizon delivers the number to the enterprise, and the Avaya SBCE sends the call to Session Manager. The dial pattern below matches on 866-850-2380 specifically. Dial patterns can alternatively match on ranges of numbers. Under **Originating Locations and Routing Policies**, the routing policy named “To-CM63-TG2” is chosen when the call originates from **Originating Location Name** “Vz-ASBCE”. This sends the call to Communication Manager using port 5071 as described previously.



Dial Pattern Details

General

* Pattern:	8668502380
* Min:	10
* Max:	10
Emergency Call:	□
Emergency Priority:	1
Emergency Type:	
SIP Domain:	avayalab.com
Notes:	Vz IPCC to SIP phone

Originating Locations and Routing Policies

1 Item | Refresh Filter: Enable

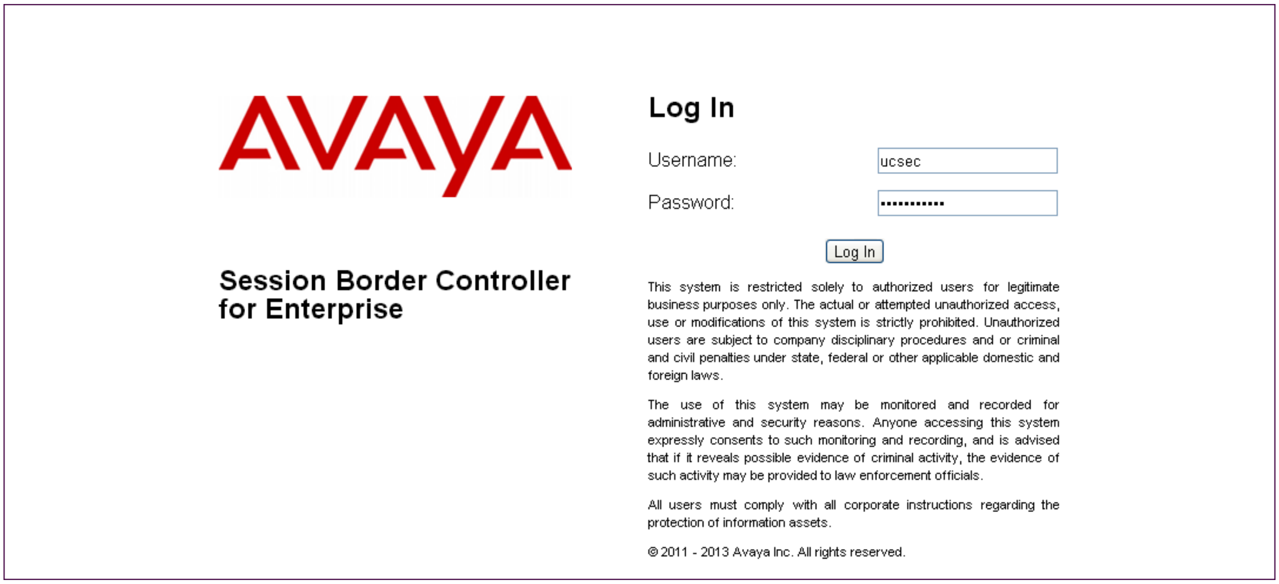
□	Originating Location Name	Originating Location Notes	Routing Policy Name	Rank	Routing Policy Disabled	Routing Policy Destination	Routing Policy Notes
□	Vz-ASBCE	SBC to Verizon	To-CM63-TG2	0	□	CM63-TG2	Trunk Group 2 for inbound only

Select : All, None

7. Configure Avaya Session Border Controller for Enterprise Release 6.2

These Application Notes assume that the installation of the Avaya SBCE and the assignment of all IP addresses have already been completed, including the management IP address.

In the sample configuration, the management IP is 10.80.140.140. Access the web management interface by entering https://<ip-address> where <ip-address> is the management IP address assigned during installation. Log in with the appropriate credentials. Click **Log In**.



Log In

Username: ucsec

Password: ••••••••••••

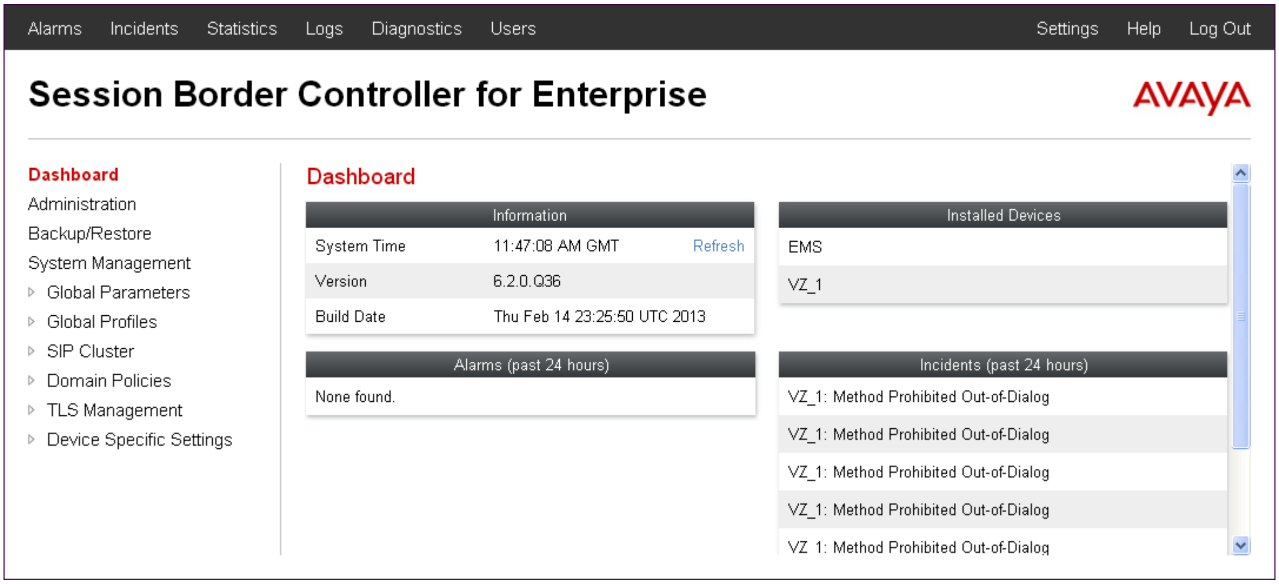
This system is restricted solely to authorized users for legitimate business purposes only. The actual or attempted unauthorized access, use or modifications of this system is strictly prohibited. Unauthorized users are subject to company disciplinary procedures and or criminal and civil penalties under state, federal or other applicable domestic and foreign laws.

The use of this system may be monitored and recorded for administrative and security reasons. Anyone accessing this system expressly consents to such monitoring and recording, and is advised that if it reveals possible evidence of criminal activity, the evidence of such activity may be provided to law enforcement officials.

All users must comply with all corporate instructions regarding the protection of information assets.

© 2011 - 2013 Avaya Inc. All rights reserved.

The main page of the Avaya SBCE will appear.



Dashboard

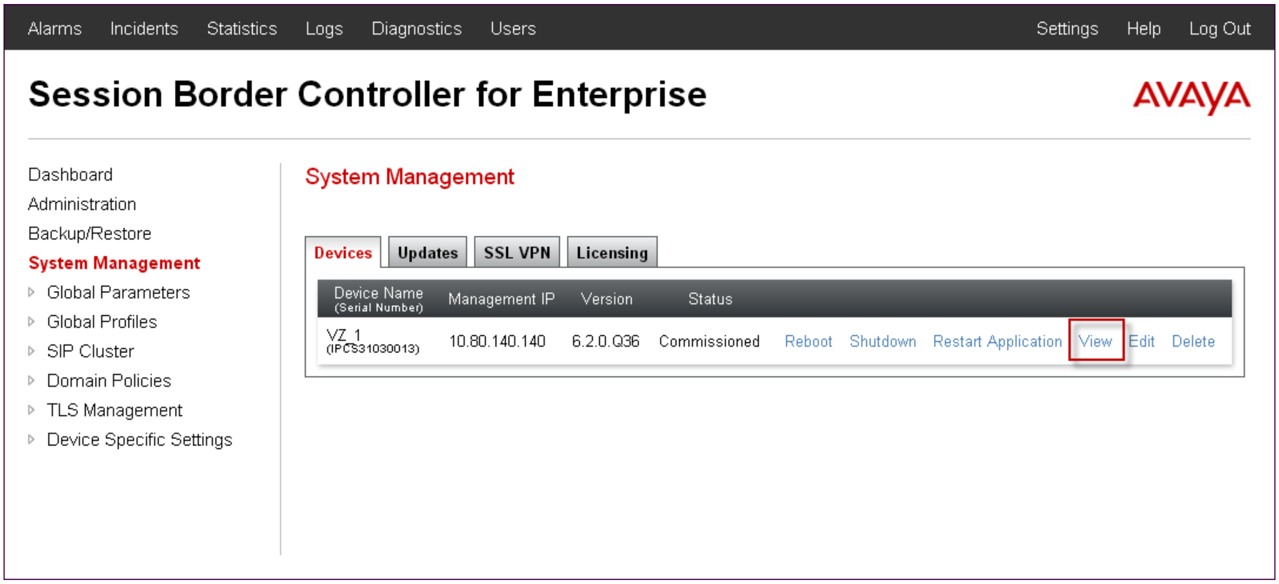
Information		
System Time	11:47:08 AM GMT	Refresh
Version	6.2.0.Q36	
Build Date	Thu Feb 14 23:25:50 UTC 2013	

Installed Devices
EMS
VZ_1

Alarms (past 24 hours)
None found.

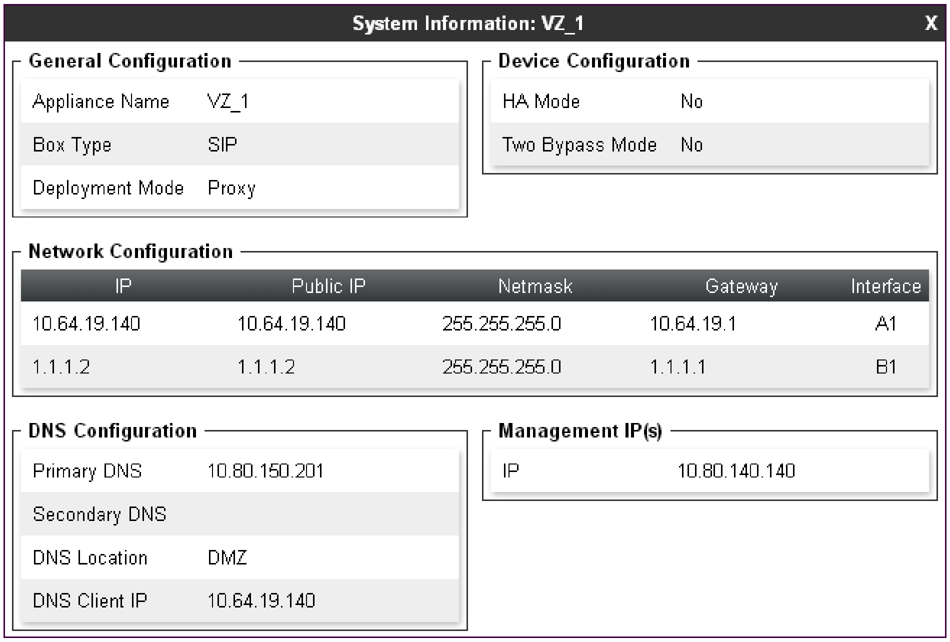
Incidents (past 24 hours)
VZ_1: Method Prohibited Out-of-Dialog
VZ_1: Method Prohibited Out-of-Dialog
VZ_1: Method Prohibited Out-of-Dialog
VZ_1: Method Prohibited Out-of-Dialog
VZ_1: Method Prohibited Out-of-Dialog

To view system information that was configured during installation, navigate to **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 **View** as highlighted below.



Device Name (Serial Number)	Management IP	Version	Status						
VZ_1 (IPCS31030013)	10.80.140.140	6.2.0.Q36	Commissioned	Reboot	Shutdown	Restart Application	View	Edit	Delete

The **System Information** screen shows the **Network Settings**, **DNS Configuration**, and **Management IP** 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. Note that the **Management IP** must be on a separate subnet from the IP interfaces designated for SIP traffic.



General Configuration

Appliance Name	VZ_1
Box Type	SIP
Deployment Mode	Proxy

Device Configuration

HA Mode	No
Two Bypass Mode	No

Network Configuration

IP	Public IP	Netmask	Gateway	Interface
10.64.19.140	10.64.19.140	255.255.255.0	10.64.19.1	A1
1.1.1.2	1.1.1.2	255.255.255.0	1.1.1.1	B1

DNS Configuration

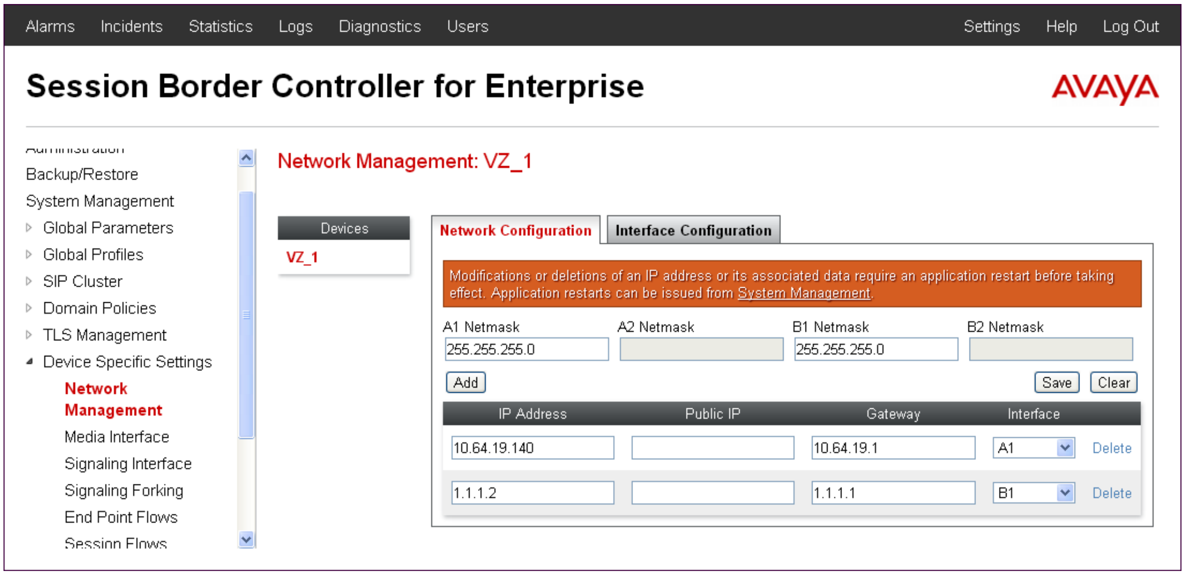
Primary DNS	10.80.150.201
Secondary DNS	
DNS Location	DMZ
DNS Client IP	10.64.19.140

Management IP(s)

IP	10.80.140.140

7.1. Network Management

The Network Management screen is where the network interface settings are configured and enabled. During the installation process, certain network-specific information is defined such as device IP address(es), public IP address(es), netmask, gateway, etc., to interface the device to the network. It is this information that populates the various Network Management tab displays, which can be edited as needed to optimize device performance and network efficiency. Navigate to **Device Specific Settings → Network Management** and verify the IP addresses assigned to the interfaces and that the interfaces are enabled. The following screen shows the internal interface is assigned to **A1** and the external interface is assigned to **B1**.



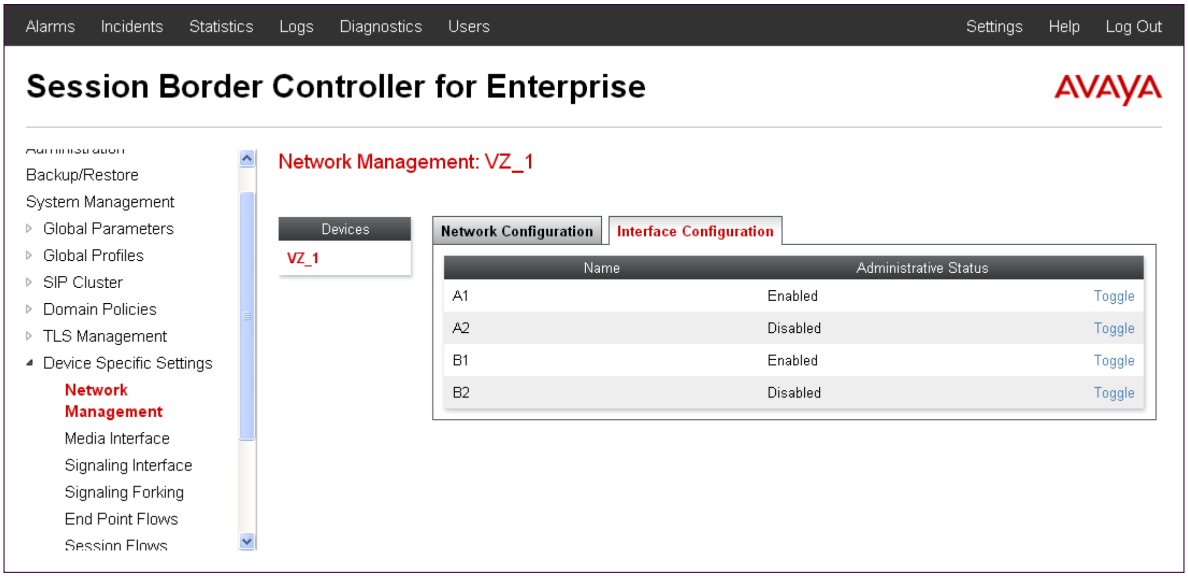
Network Management: VZ_1

Modifications or deletions of an IP address or its associated data require an application restart before taking effect. Application restarts can be issued from System Management.

A1 Netmask	A2 Netmask	B1 Netmask	B2 Netmask
255.255.255.0		255.255.255.0	

IP Address	Public IP	Gateway	Interface	
10.64.19.140		10.64.19.1	A1	Delete
1.1.1.2		1.1.1.1	B1	Delete

The following screen shows interface **A1** and **B1** are **Enabled**. To enable an interface click the corresponding **Toggle State** button.



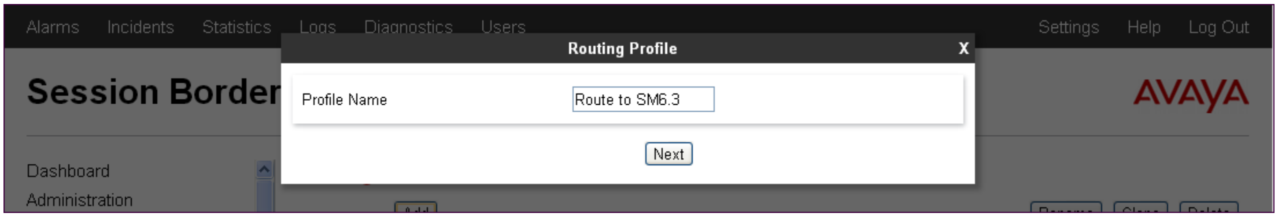
Network Management: VZ_1

Name	Administrative Status	
A1	Enabled	Toggle
A2	Disabled	Toggle
B1	Enabled	Toggle
B2	Disabled	Toggle

7.2. 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.

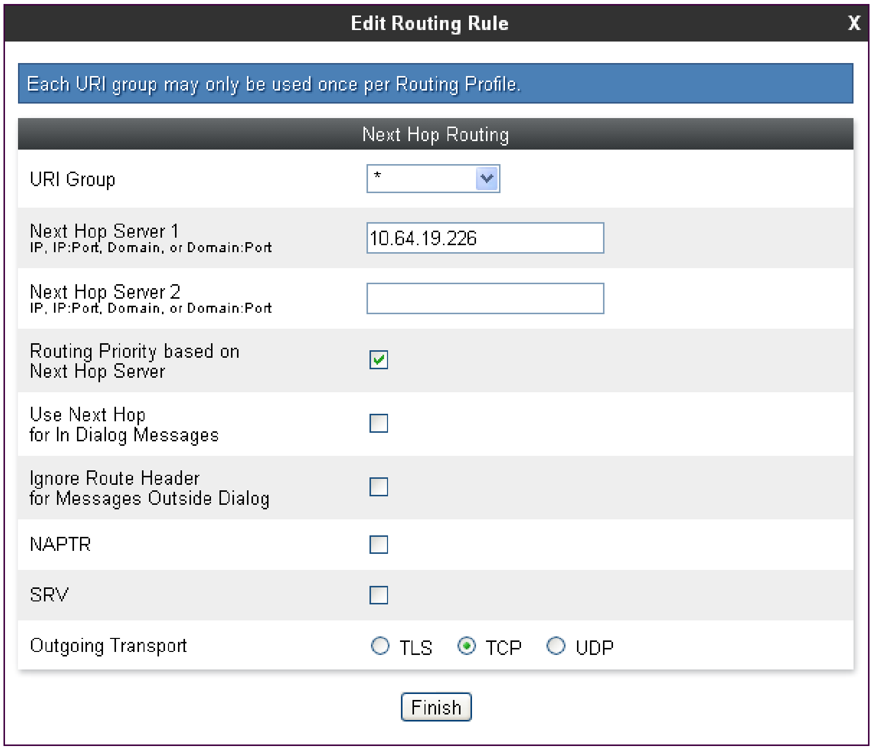
Create a Routing Profile for Session Manager and Verizon IP Trunk service. To add a routing profile, navigate to **Global Profiles → Routing** and select **Add**. Enter a **Profile Name** and click **Next** to continue.



Routing Profile

Profile Name: Route to SM6.3

In the shared test environment the following screen shows Routing Profile "Route to SM6.3" created for Session Manager. The **Next Hop Server 1** IP address must match the IP address of Session Manager Entity created for Avaya SBCE in **Section 6.4**. The **Outgoing Transport** is set to **TCP** and matched the **Protocol** set in the Session Manager Entity Link for Avaya SBCE in **Section 6.5**.

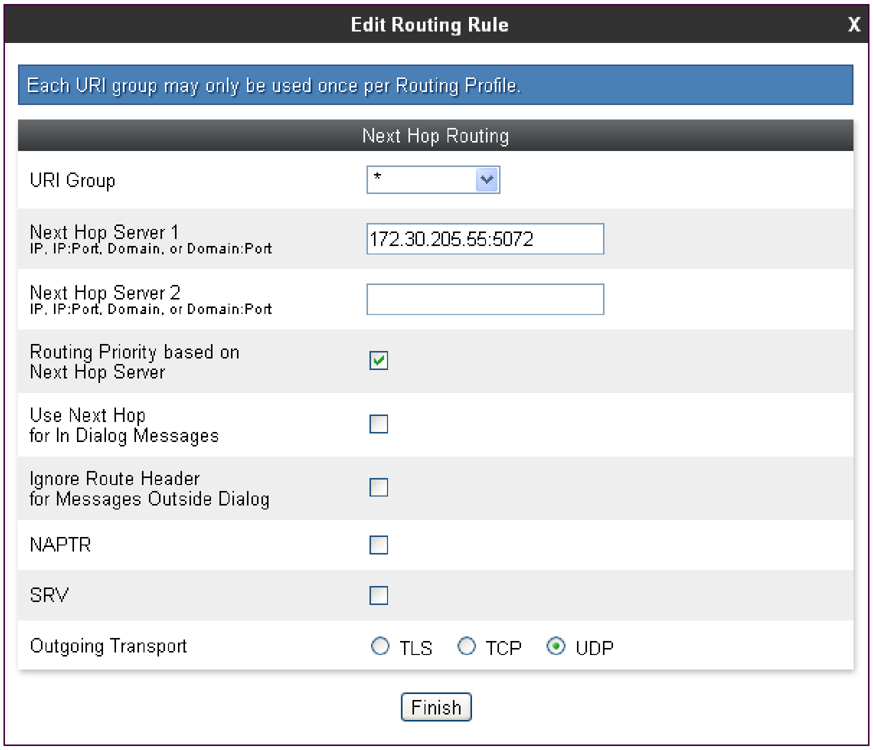


Edit Routing Rule

Each URI group may only be used once per Routing Profile.

Next Hop Routing	
URI Group	*
Next Hop Server 1 IP, IP:Port, Domain, or Domain:Port	10.64.19.226
Next Hop Server 2 IP, IP:Port, Domain, or Domain:Port	
Routing Priority based on Next Hop Server	☑
Use Next Hop for In Dialog Messages	□
Ignore Route Header for Messages Outside Dialog	□
NAPTR	□
SRV	□
Outgoing Transport	○ TLS ● TCP ○ UDP

The following screen shows Routing Profile "Route To Vz_IPCC" created for Verizon. Enter the IP address and port of the Verizon SIP signaling interface as **Next Hop Server 1**, as shown below. It is only necessary to include the port after the IP address when it is not the default SIP port. Choose **UDP** for **Outgoing Transport**, and click **Finish**.



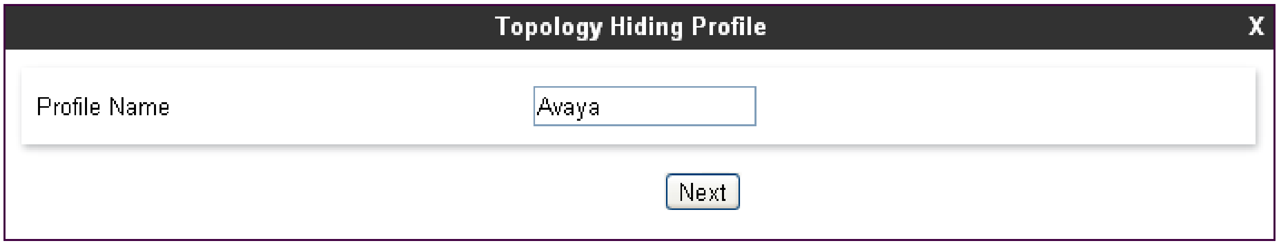
Each URI group may only be used once per Routing Profile.

Next Hop Routing	
URI Group	*
Next Hop Server 1 IP, IP:Port, Domain, or Domain:Port	172.30.205.55:5072
Next Hop Server 2 IP, IP:Port, Domain, or Domain:Port	
Routing Priority based on Next Hop Server	☑
Use Next Hop for In Dialog Messages	□
Ignore Route Header for Messages Outside Dialog	□
NAPTR	□
SRV	□
Outgoing Transport	○ TLS ○ TCP ● UDP

7.3. Topology Hiding Profile

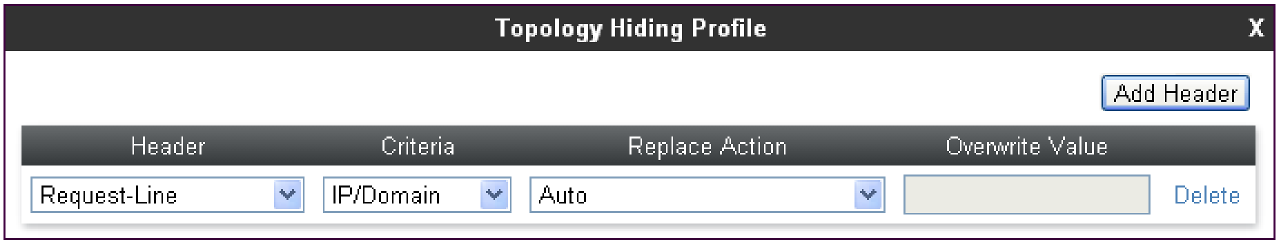
The Topology Hiding profile manages how various source, destination and routing information in SIP and SDP message headers are substituted or changed to maintain the integrity of the network. It hides the topology of the enterprise network from external networks.

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



Profile Name: Avaya

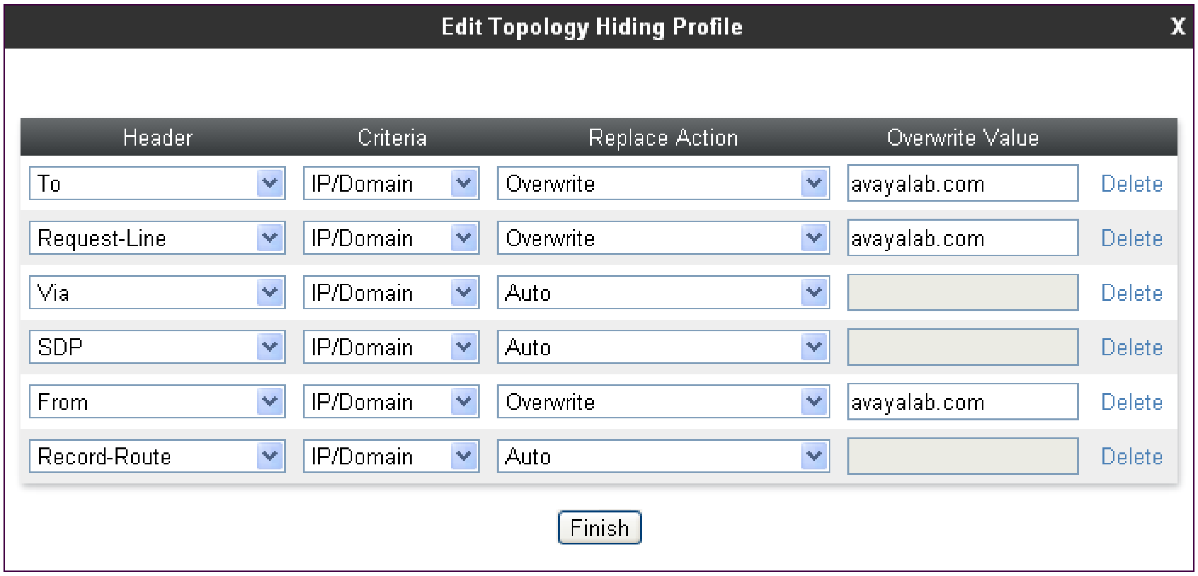
In the resultant screen, click the **Add Header** button in the upper right multiple times to reveal additional headers.



Topology Hiding Profile

Header	Criteria	Replace Action	Overwrite Value	
Request-Line	IP/Domain	Auto		Delete

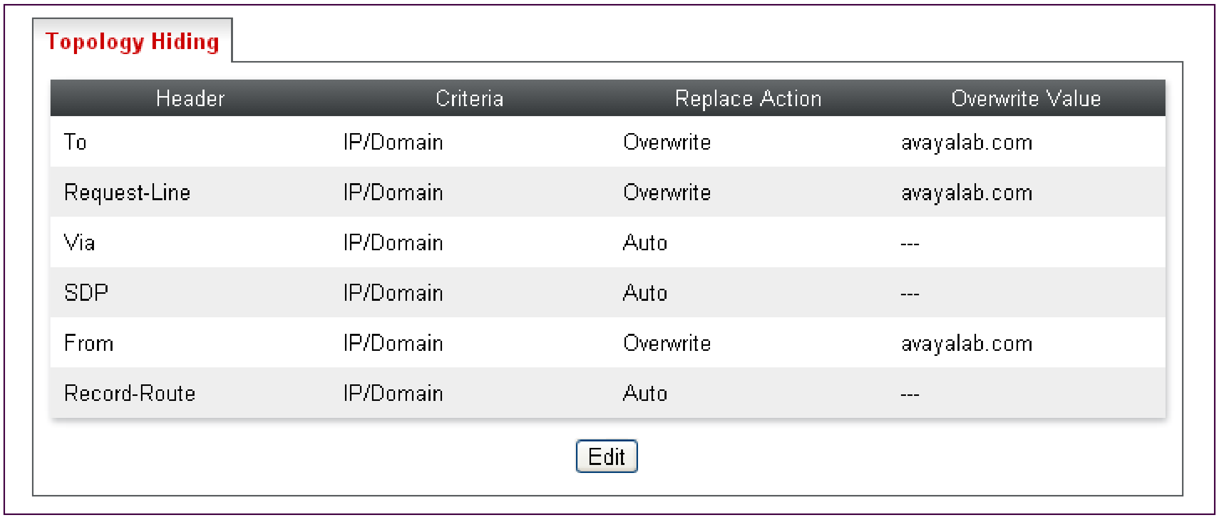
In the **Replace Action** column an action of "Auto" will replace the header field with the IP address of the Avaya SBCE interface and the "Overwrite" will use the value in the **Overwrite Value**. In the example shown, this profile will later be applied in the direction of the Session Manager and "Overwrite"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



Edit Topology Hiding Profile

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

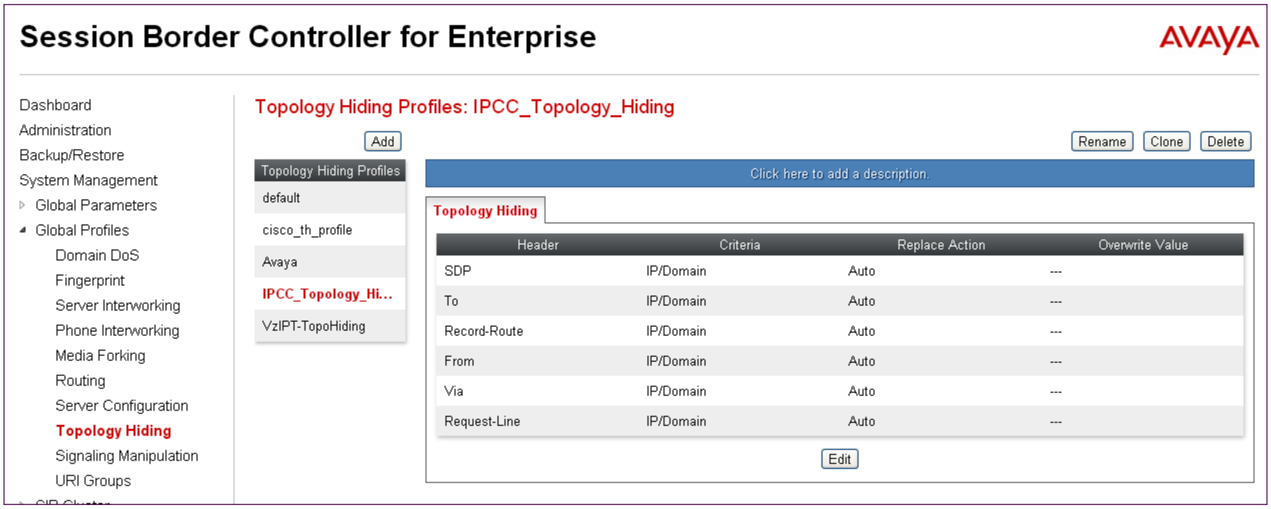
After configuration is completed, the Topology Hiding for profile "Avaya" will appear as follows. This profile will later be applied to the Server Flow for Avaya.



Topology Hiding

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

Similarly, create a Topology Hiding profile for Verizon. The following screen shows Topology Hiding profile "IPCC_Topology_Hiding" created for Verizon. This profile will later be applied to the Server Flow for Verizon.



Topology Hiding Profiles: IPCC_Topology_Hiding

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

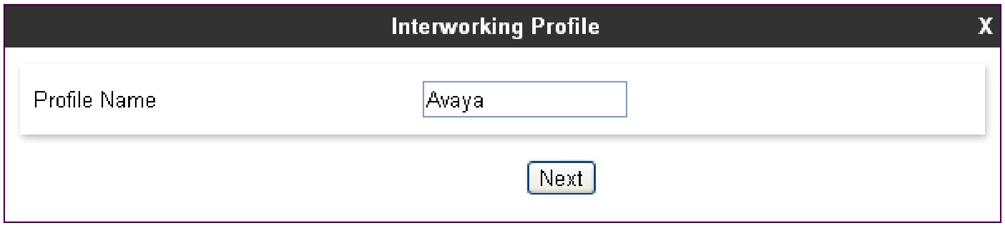
7.4. Server Interworking Profile

The Server Internetworking profile configures and manages various SIP call server-specific parameters such as TCP and UDP port assignments, heartbeat signaling parameters (for HA deployments), DoS security statistics, and trusted domains. Interworking Profile features are configured based on different Trunk Servers. There are default profiles available that may be used as is, or modified, or new profiles can be configured as described below.

In the sample configuration, separate Server Interworking Profiles were created for Avaya and Verizon IPCC.

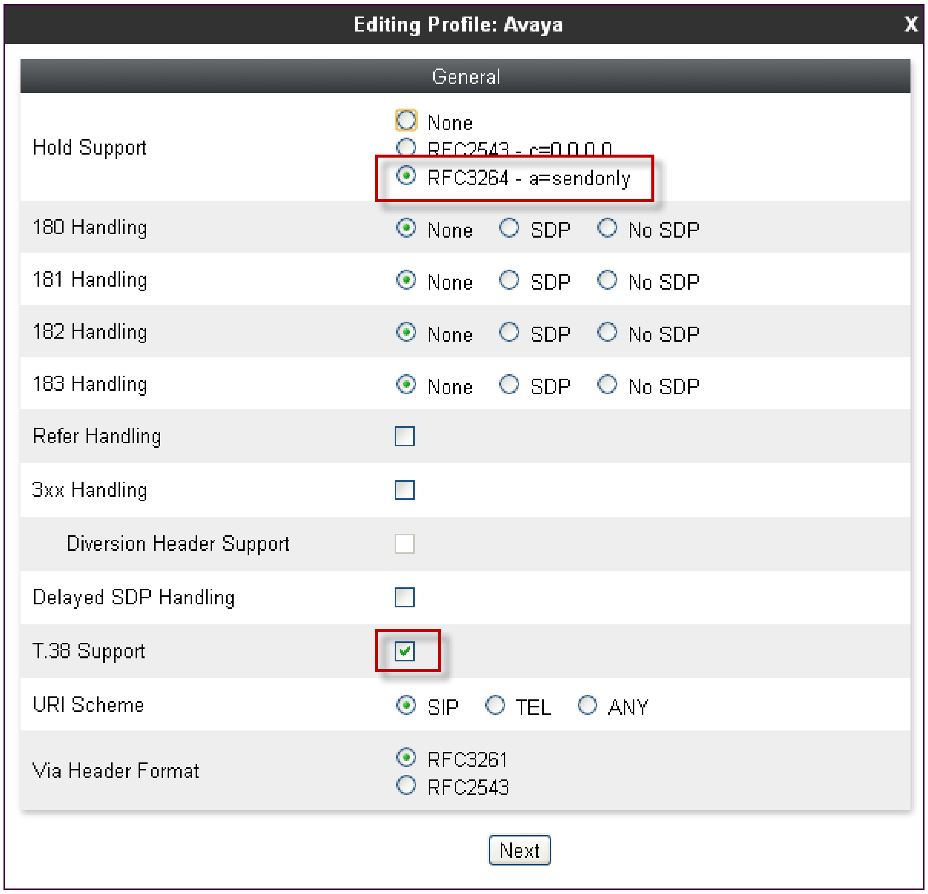
7.4.1 Server Interworking– Avaya

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



Profile Name	Avaya

The following screens illustrate the “General” parameters used in the sample configuration for the Interworking Profile named “Avaya”. Most parameters retain default values. In the sample configuration, **RFC3264 – a=sendonly** is selected and **T.38 support** is checked.

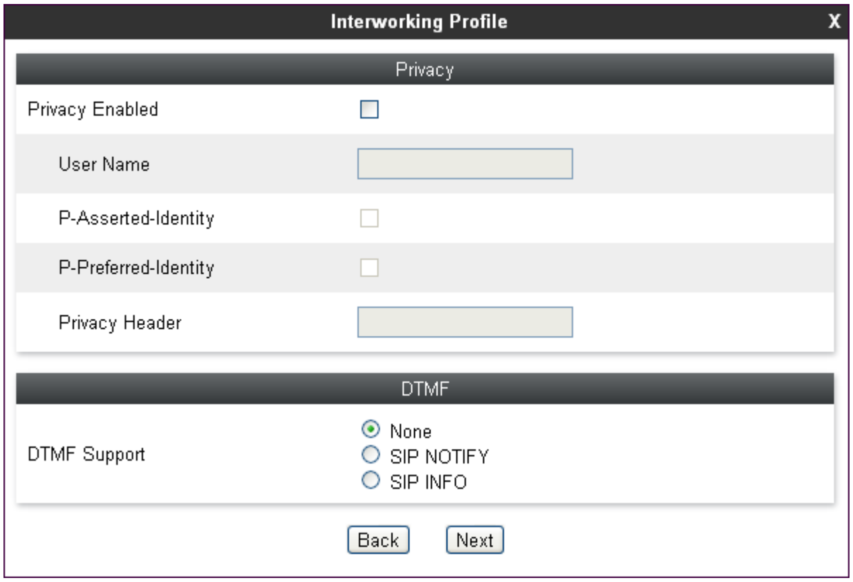


Editing Profile: Avaya

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

Click **Next** to advance to through both the Privacy / DTMF parameters screen, and the SIP / Transport Timers parameters screen, which may retain default values.



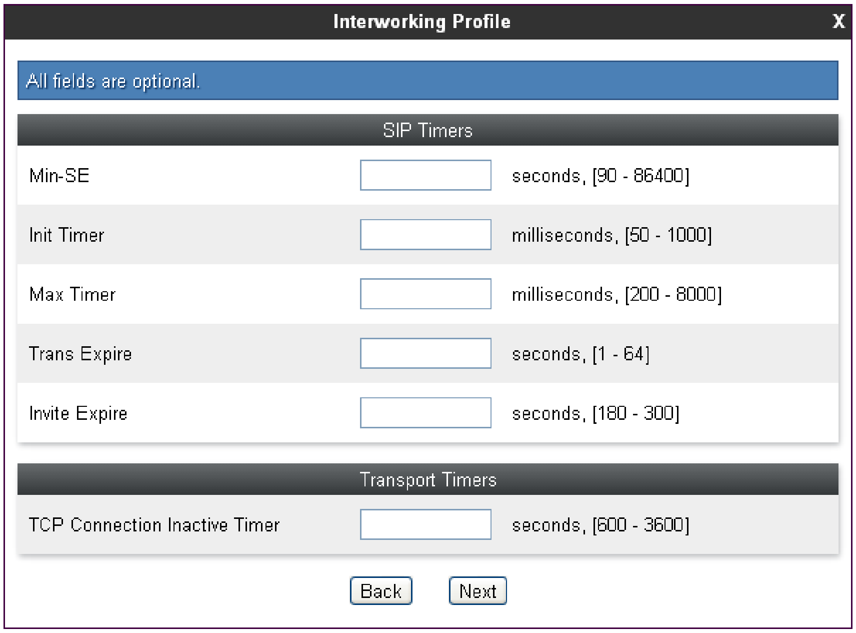
Interworking Profile

Privacy

Privacy Enabled	□
User Name	
P-Asserted-Identity	□
P-Preferred-Identity	□
Privacy Header	

DTMF

DTMF Support	● None ○ SIP NOTIFY ○ SIP INFO



Interworking Profile

All fields are optional.

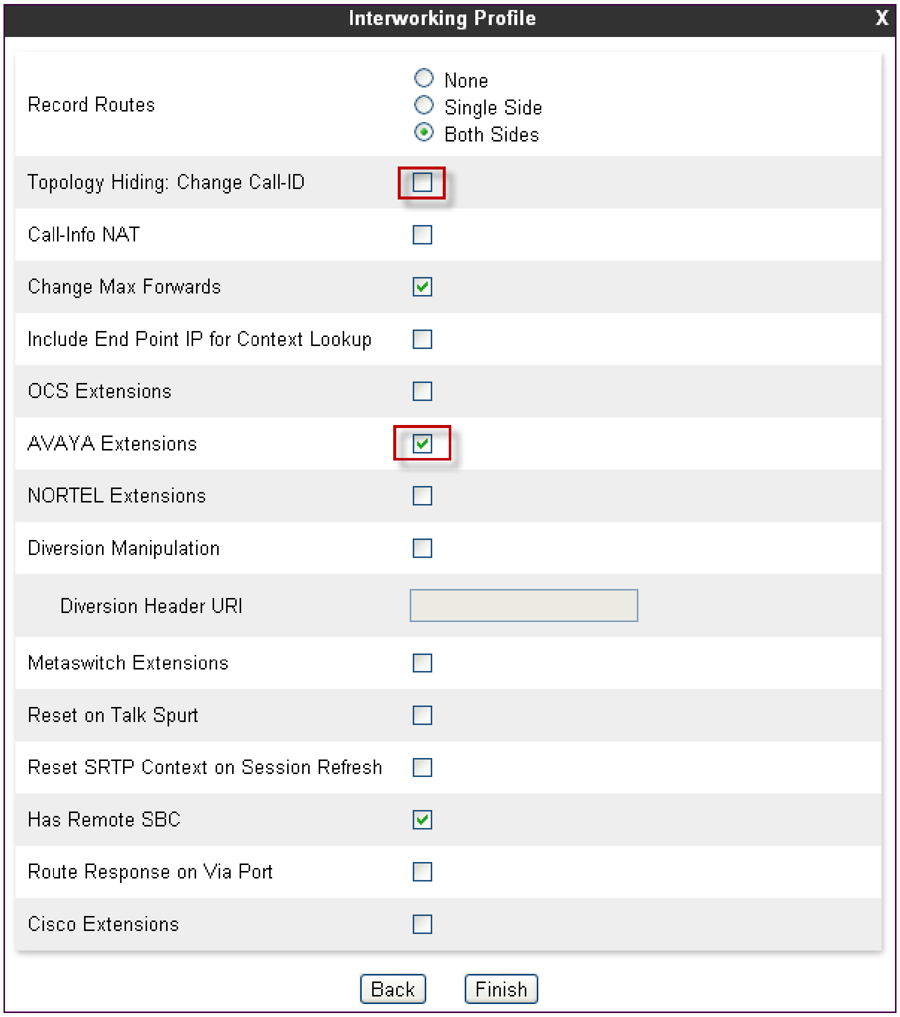
SIP Timers

Min-SE		seconds, [90 - 86400]
Init Timer		milliseconds, [50 - 1000]
Max Timer		milliseconds, [200 - 8000]
Trans Expire		seconds, [1 - 64]
Invite Expire		seconds, [180 - 300]

Transport Timers

TCP Connection Inactive Timer		seconds, [600 - 3600]

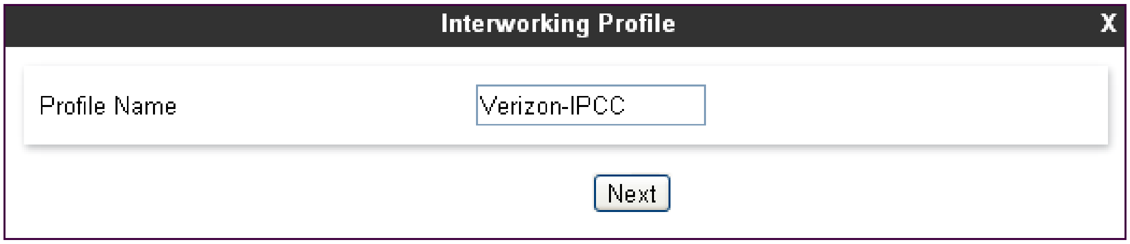
The following screen illustrates the **Advanced Settings** configuration. The **Topology Hiding: Change Call-ID** is unchecked and the **AVAYA Extensions** is checked. All other parameters shown are default values. Note that the default configuration will result in Record-Route headers in SIP messages.



Record Routes	○ None ○ Single Side ● Both Sides
Topology Hiding: Change Call-ID	□
Call-Info NAT	□
Change Max Forwards	☑
Include End Point IP for Context Lookup	□
OCS Extensions	□
AVAYA Extensions	☑
NORTEL Extensions	□
Diversion Manipulation	□
Diversion Header URI	
Metaswitch Extensions	□
Reset on Talk Spurt	□
Reset SRTP Context on Session Refresh	□
Has Remote SBC	☑
Route Response on Via Port	□
Cisco Extensions	□

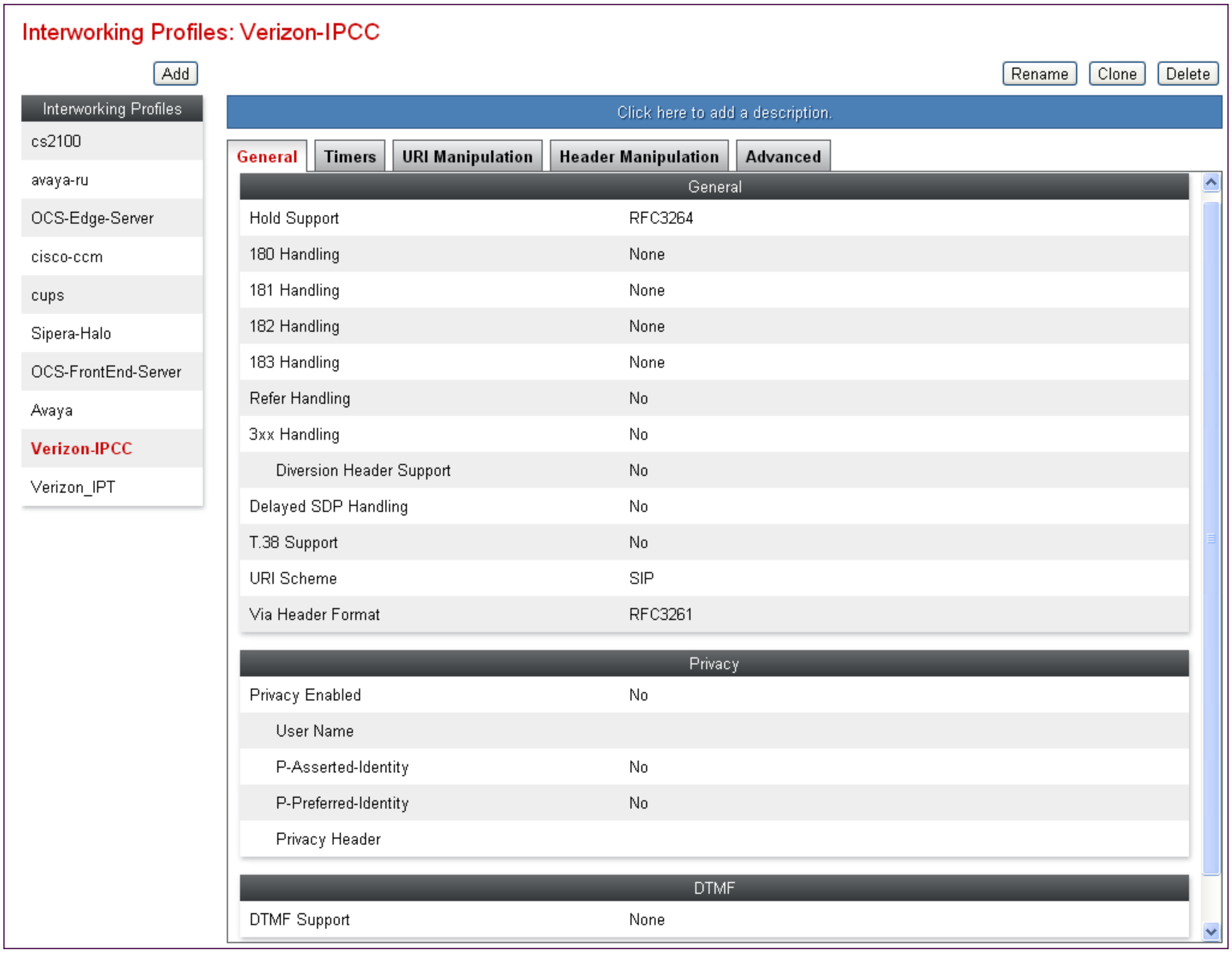
7.4.2 Server Interworking – Verizon IPCC

Click the **Add** 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**.



Profile Name	Verizon-IPCC

The following screens illustrate the "General" parameters used in the sample configuration for the Interworking Profile named "Verizon-IPCC". Most parameters retain default values. In the sample, **Hold Support** was set for RFC3264, and all other fields retained default values.

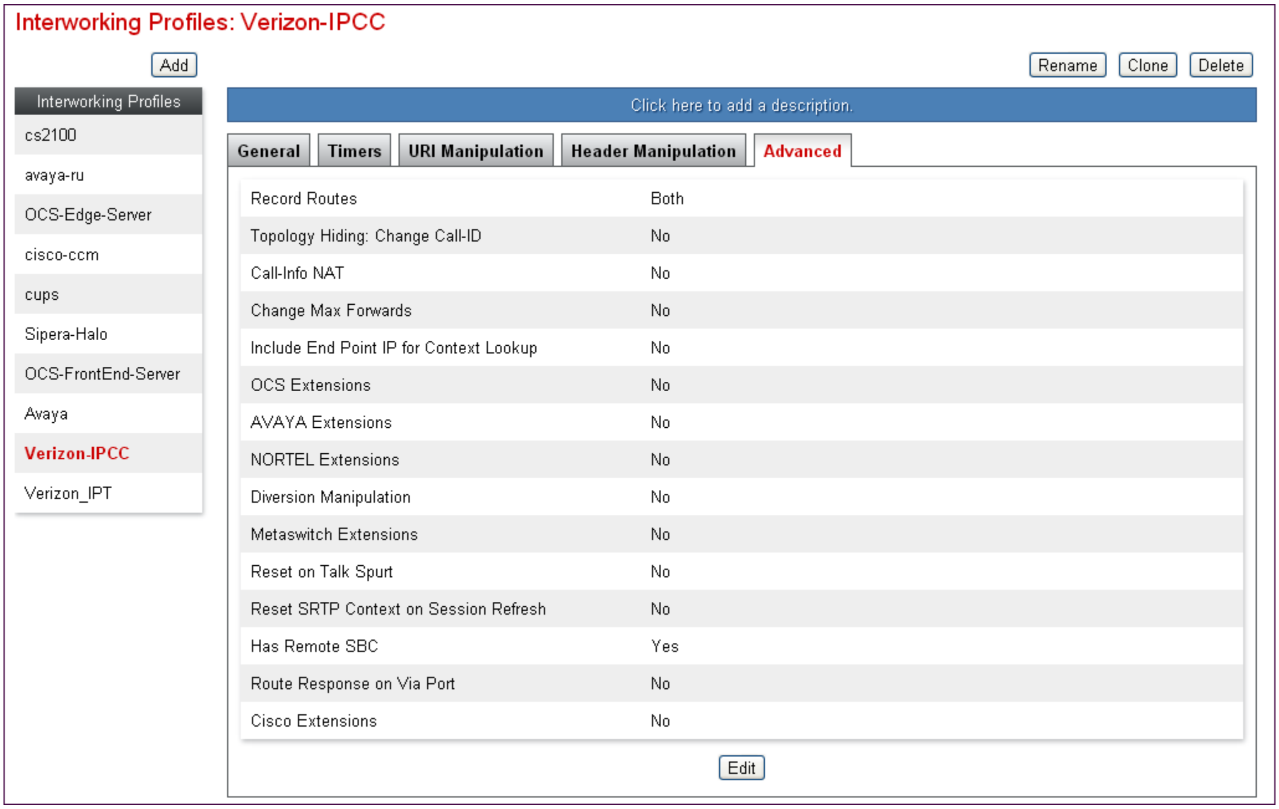


General	
Hold Support	RFC3264
180 Handling	None
181 Handling	None
182 Handling	None
183 Handling	None
Refer Handling	No
3xx Handling	No
Diversion Header Support	No
Delayed SDP Handling	No
T.38 Support	No
URI Scheme	SIP
Via Header Format	RFC3261

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

DTMF	
DTMF Support	None

The following screen illustrates the **Advanced Settings** configuration. The **Topology Hiding: Change Call-ID** and **Change Max Forwards** defaults were changed to "No". All other parameters shown are default values. Note that the default configuration will result in Record-Route headers in SIP messages.



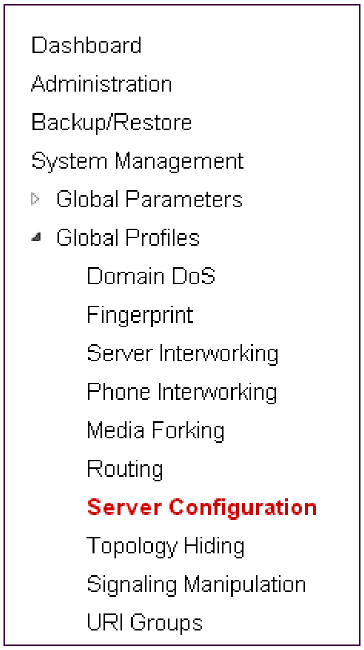
Interworking Profiles: Verizon-IPCC

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

7.5. Server Configuration

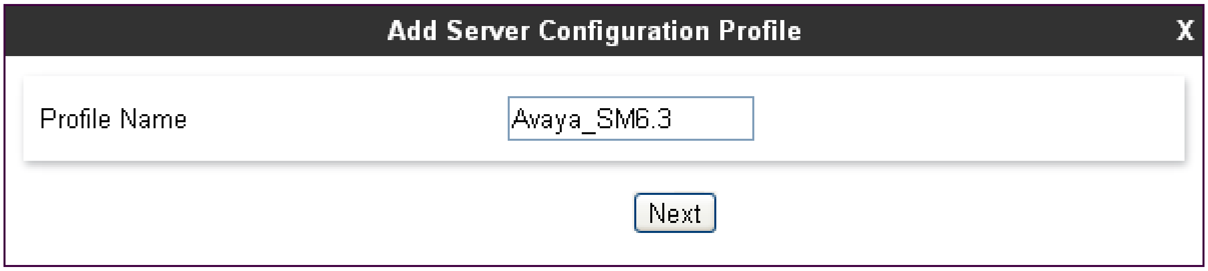
The **Server Configuration** screen contains four tabs: **General**, **Authentication**, **Heartbeat**, and **Advanced**. Together, these tabs configure and manage various SIP call server-specific parameters such as TCP and UDP port assignments, heartbeat signaling parameters, DoS security statistics, and trusted domains.

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



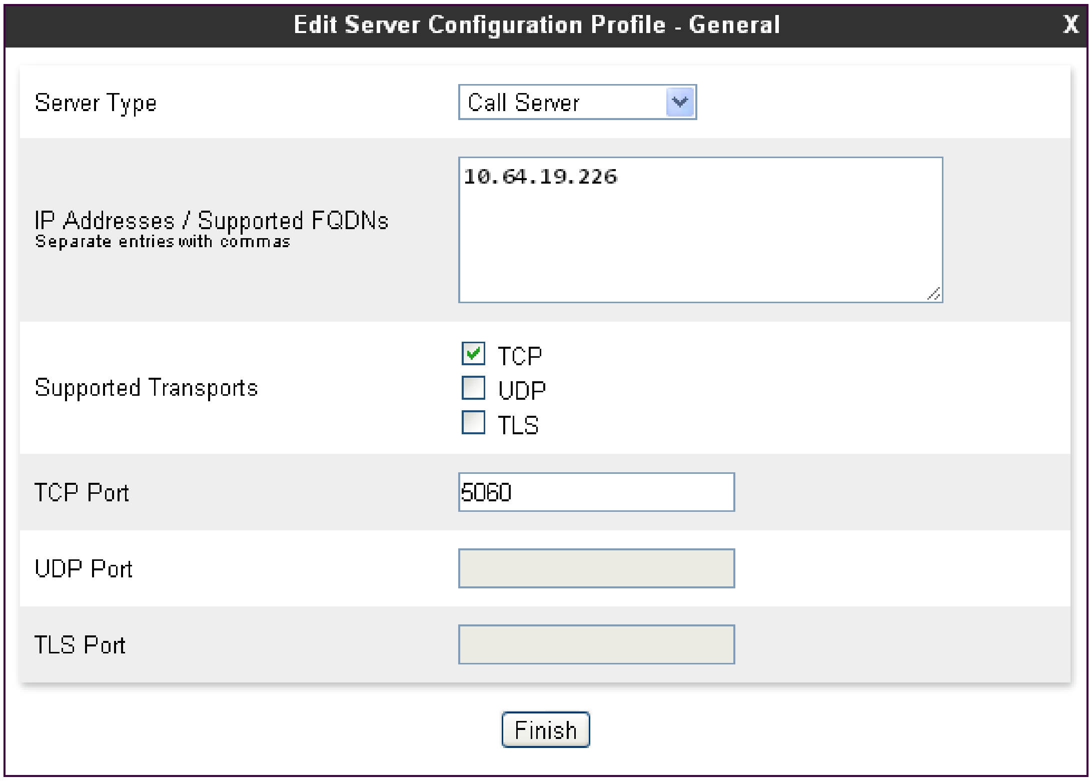
7.5.1 Server Configuration for Session Manager

Click the **Add** button (not shown) to add a new profile, or select an existing profile to edit. If adding a profile, a screen such as the following is displayed. Enter an appropriate Profile Name such as "Avaya_SM6.3" shown below. Click **Next**.



Profile Name: Avaya_SM6.3

The following screens illustrate the Server Configuration for the Profile name "Avaya_SM6.3". On the **General** tab, select "Call Server" from the **Server Type** drop-down menu. In the **IP Addresses / Supported FQDNs** area, the IP Address of the Session Manager SIP signaling interface in the sample configuration is entered. This IP Address is 10.64.19.226. In the **Supported Transports** area, **TCP** is selected, and the **TCP Port** is set to 5060. This configuration corresponds with the Session Manager entity link configuration for the entity link to the Avaya SBCE created in **Section 6.4**. If adding a new profile, click **Next** (not shown). If editing an existing profile, click **Finish**.



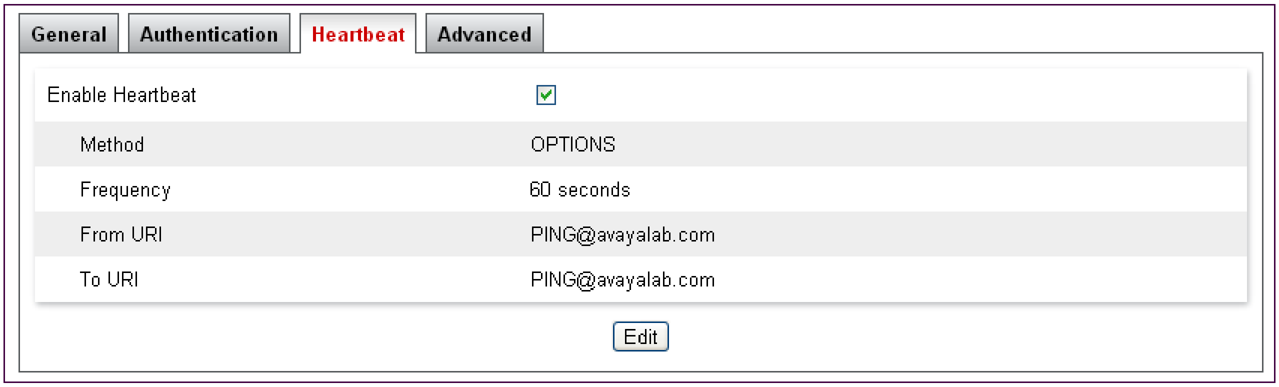
Edit Server Configuration Profile - General

Server Type	Call Server
IP Addresses / Supported FQDNs Separate entries with commas	10.64.19.226
Supported Transports	☑ TCP ☐ UDP ☐ TLS
TCP Port	5060
UDP Port	
TLS Port	

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

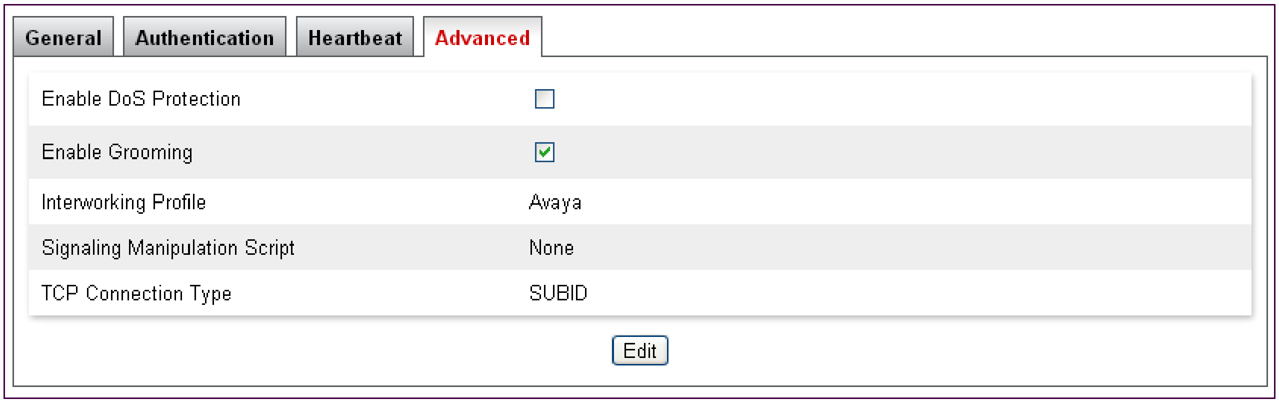
Avaya SBCE can be configured to source "heartbeats" in the form of SIP OPTIONS. In the sample configuration, with one Session Manager, this configuration is optional.

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



Enable Heartbeat	☑
Method	OPTIONS
Frequency	60 seconds
From URI	PING@avayalab.com
To URI	PING@avayalab.com

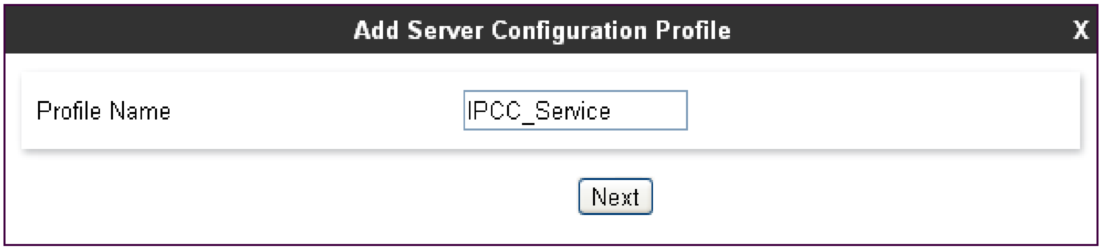
If adding a profile, click **Next** to continue to the "Advanced" settings (not shown). If editing an existing profile, select the **Advanced** tab and **Edit** (not shown). In the resultant screen, select **Enable Grooming** to allow the same TCP connection to be used for all SIP messages from this device. Select the **Interworking Profile** "Avaya" created previously. Click **Finish**.



Enable DoS Protection	☐
Enable Grooming	☑
Interworking Profile	Avaya
Signaling Manipulation Script	None
TCP Connection Type	SUBID

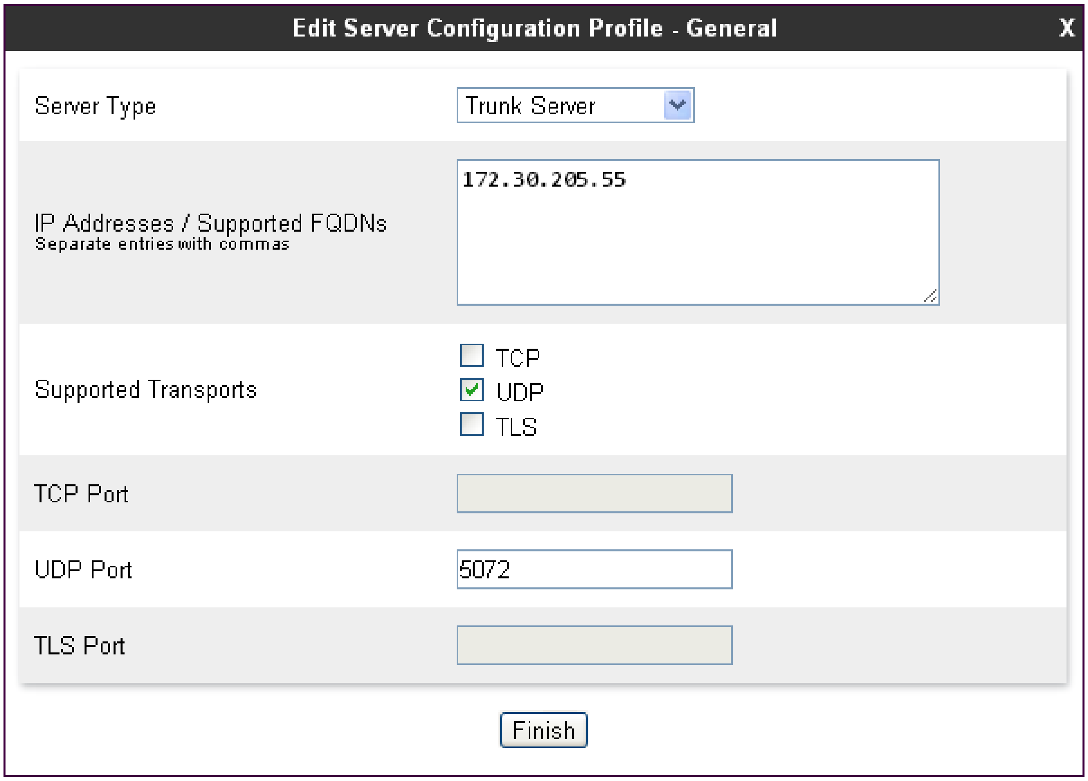
7.5.2 Server Configuration for Verizon IPCC

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



Profile Name: IPCC_Service

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



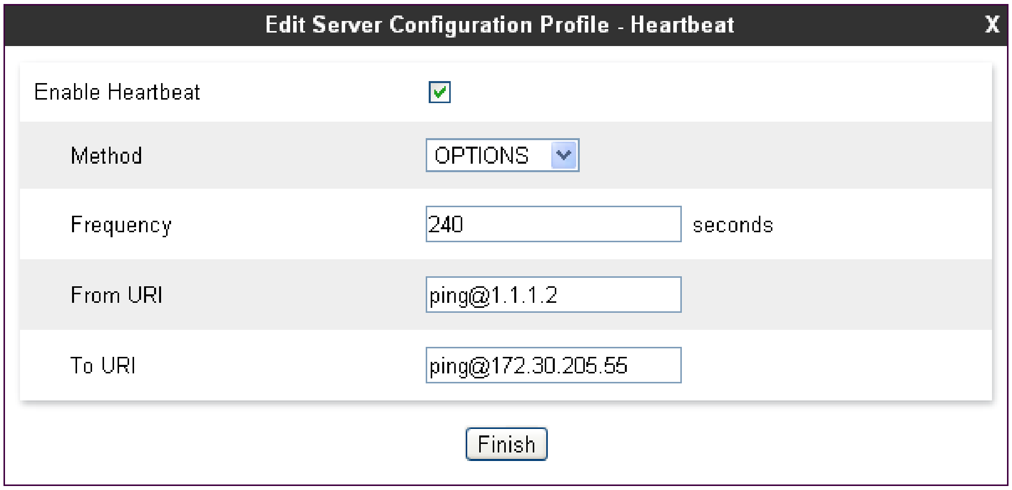
Edit Server Configuration Profile - General

Server Type	Trunk Server
IP Addresses / Supported FQDNs Separate entries with commas	172.30.205.55
Supported Transports	□ TCP ☑ UDP □ TLS
TCP Port	
UDP Port	5072
TLS Port	

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

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

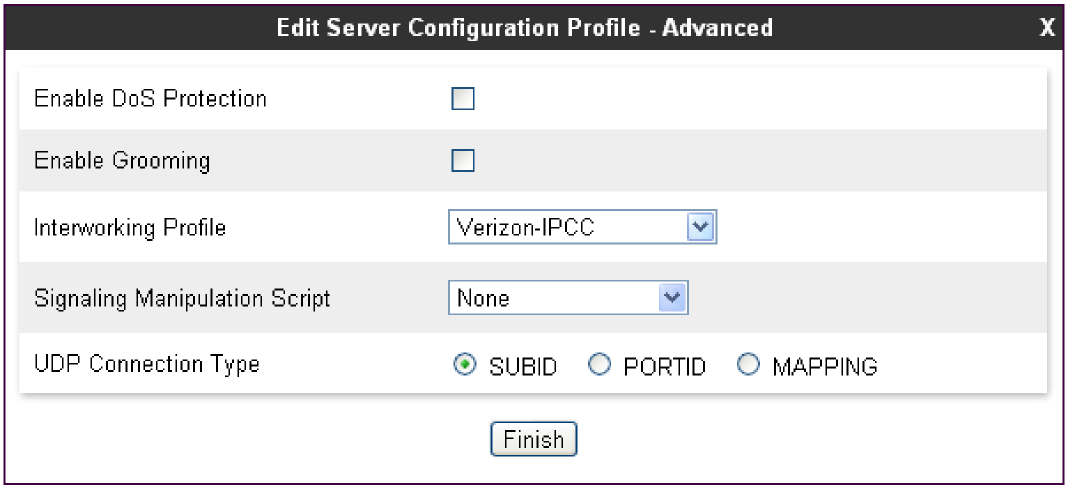
If Avaya SBCE sourced OPTIONS are desired, select “OPTIONS” from the **Method** drop-down menu. Select the desired frequency that the SBCE will source OPTIONS. The **From URI** and **To URI** may be filled in to configure easily identifiable URIs to appear in SIP OPTIONS sourced by the Avaya SBCE. If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



Edit Server Configuration Profile - Heartbeat

Enable Heartbeat	☑
Method	OPTIONS
Frequency	240 seconds
From URI	ping@1.1.1.2
To URI	ping@172.30.205.55

If editing an existing profile, highlight the desired profile and select the **Advanced** tab and then click the **Edit button** (not shown). In the resultant screen, **Enable Grooming** is not used for UDP connections and left unchecked. Select the **Interworking Profile** “Verizon_IPCC” created previously. Click **Finish**.



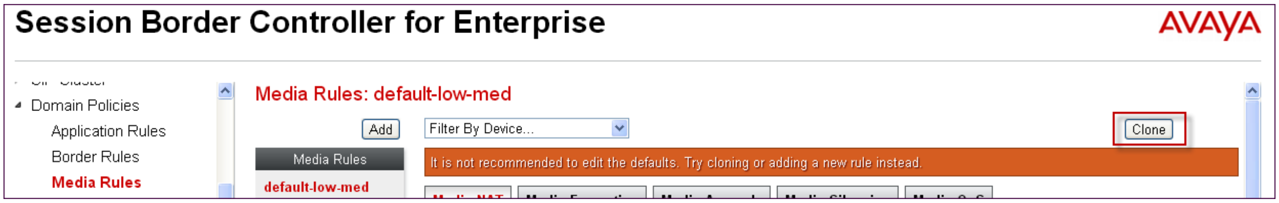
Edit Server Configuration Profile - Advanced

Enable DoS Protection	□
Enable Grooming	□
Interworking Profile	Verizon-IPCC
Signaling Manipulation Script	None
UDP Connection Type	● SUBID ○ PORTID ○ MAPPING

7.6. Media Rule

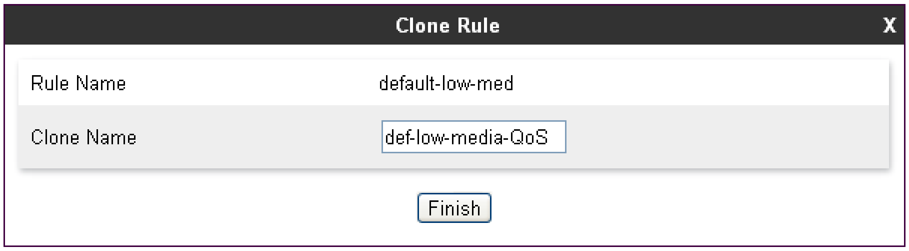
Media Rules define RTP media packet parameters such as prioritizing encryption techniques and packet encryption techniques. Together these media-related parameters define a strict profile that is associated with other SIP-specific policies to determine how media packets matching these criteria will be handled by the Avaya SBCE security product.

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.



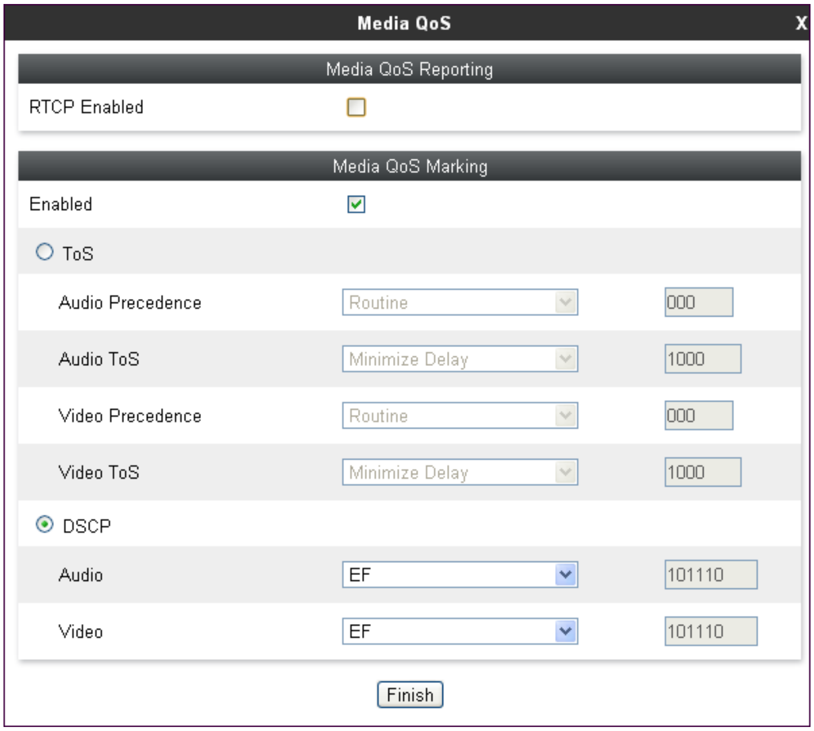
It is not recommended to edit the defaults. Try cloning or adding a new rule instead.

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



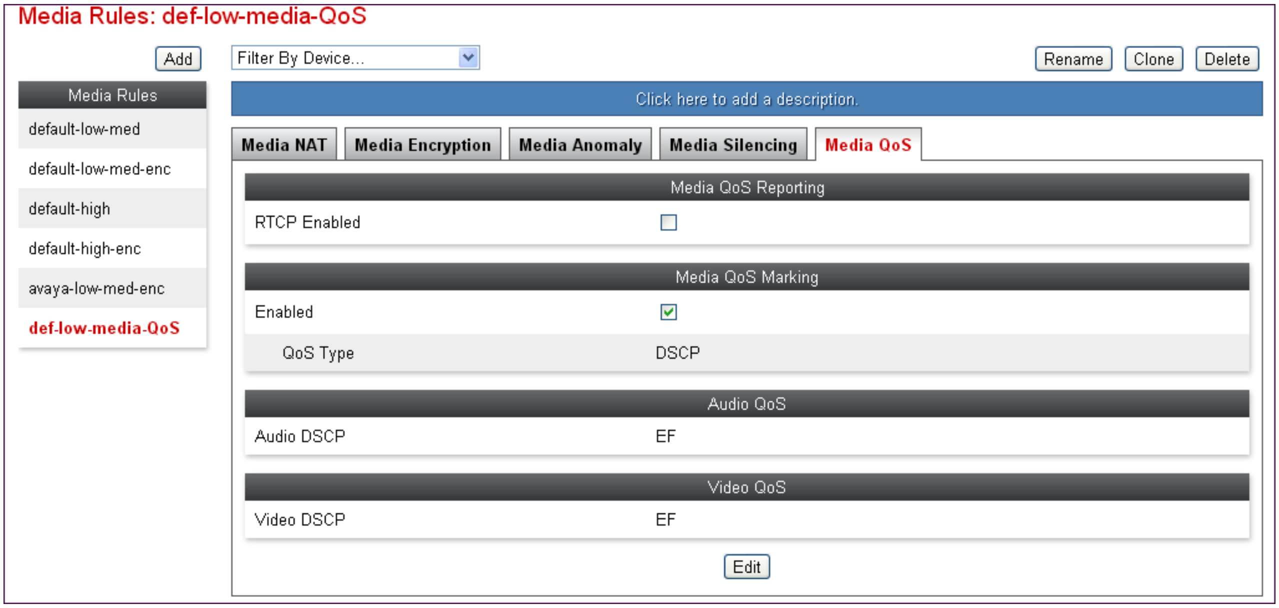
Rule Name	default-low-med
Clone Name	def-low-media-QoS

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



RTCP Enabled	□	
Enabled	☑	
○ ToS		
Audio Precedence	Routine	000
Audio ToS	Minimize Delay	1000
Video Precedence	Routine	000
Video ToS	Minimize Delay	1000
● DSCP		
Audio	EF	101110
Video	EF	101110

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



Media Rules: def-low-media-QoS

Media QoS Reporting

RTCP Enabled □

Media QoS Marking

Enabled ☑

QoS Type DSCP

Audio QoS

Audio DSCP EF

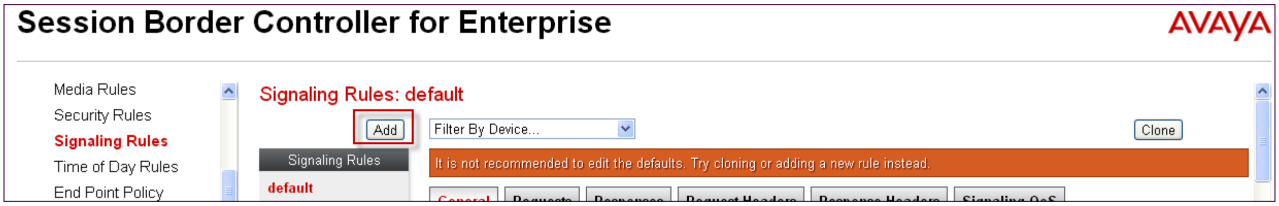
Video QoS

Video DSCP EF

7.7. Signaling Rule

Signaling Rules define the action to be taken (Allow, Block, Block with Response, etc.) for each type of SIP-specific signaling request and response message. When SIP signaling packets are received by Avaya SBCE, they are parsed and “pattern-matched” against the particular signaling criteria defined by these rules. Packets matching the criteria defined by the Signaling Rules are tagged for further policy matching.

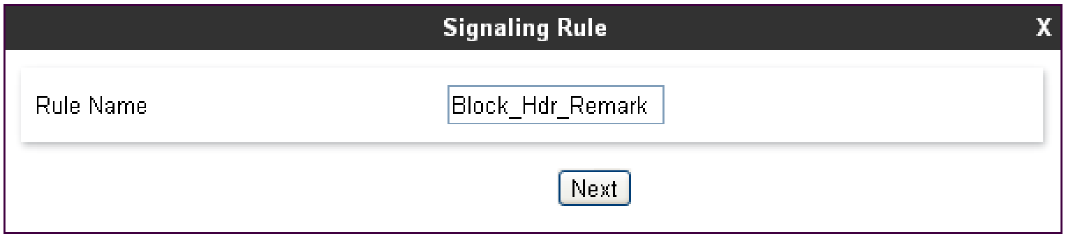
To add a signaling rule, navigate to **Domain Policies → Signaling Rules**. Click the **Add** button to add a new signaling rule.



Session Border Controller for Enterprise

It is not recommended to edit the defaults. Try cloning or adding a new rule instead.

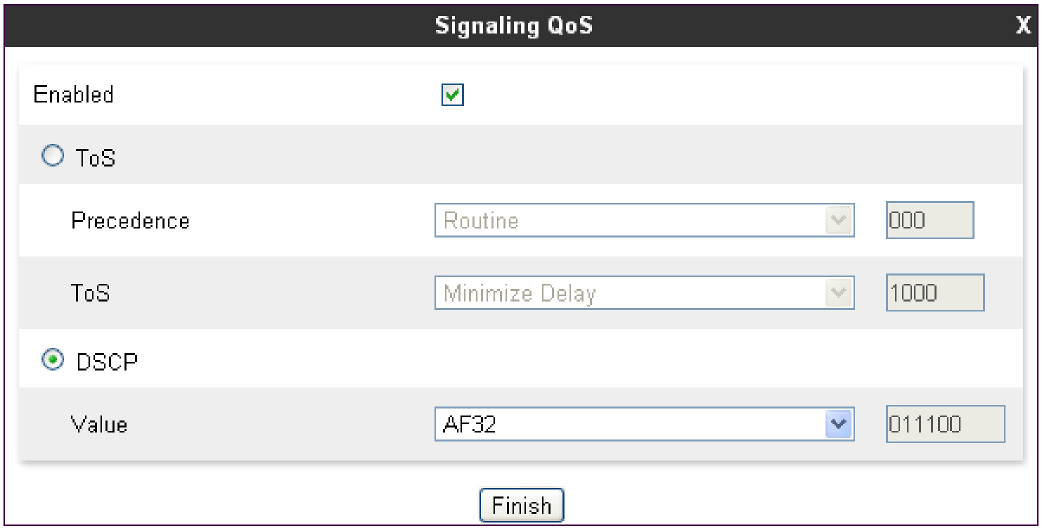
In the **Rule Name** field, enter an appropriate name, such as “Block_Hdr_Remark” and click **Next**.



Signaling Rule

Rule Name Block_Hdr_Remark

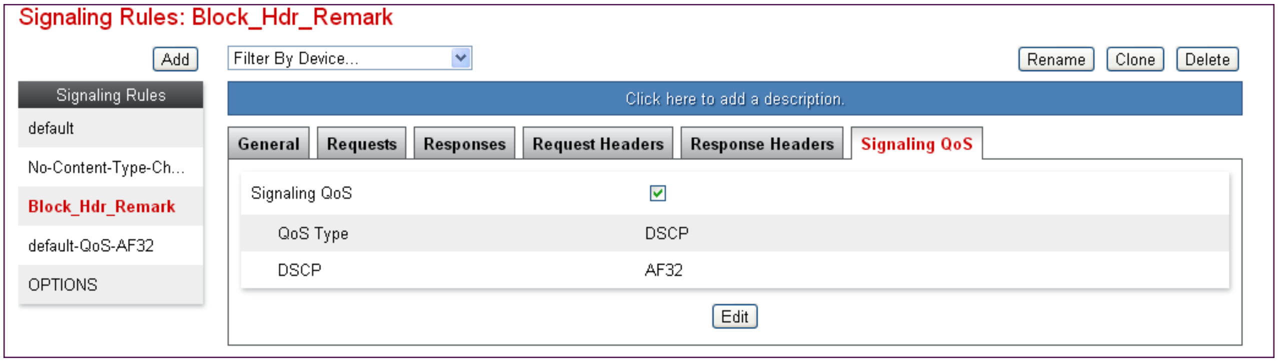
In the subsequent screen (not shown), click **Next** to accept defaults. In the Signaling QoS screen below, select **DSCP** and select the desired **Value** for Signaling QoS from the drop-down box. In the sample configuration, "AF32" is selected for Assured Forwarding 32. Click **Finish**.



Signaling QoS

Enabled	☑	
○ ToS		
Precedence	Routine	000
ToS	Minimize Delay	1000
● DSCP		
Value	AF32	011100

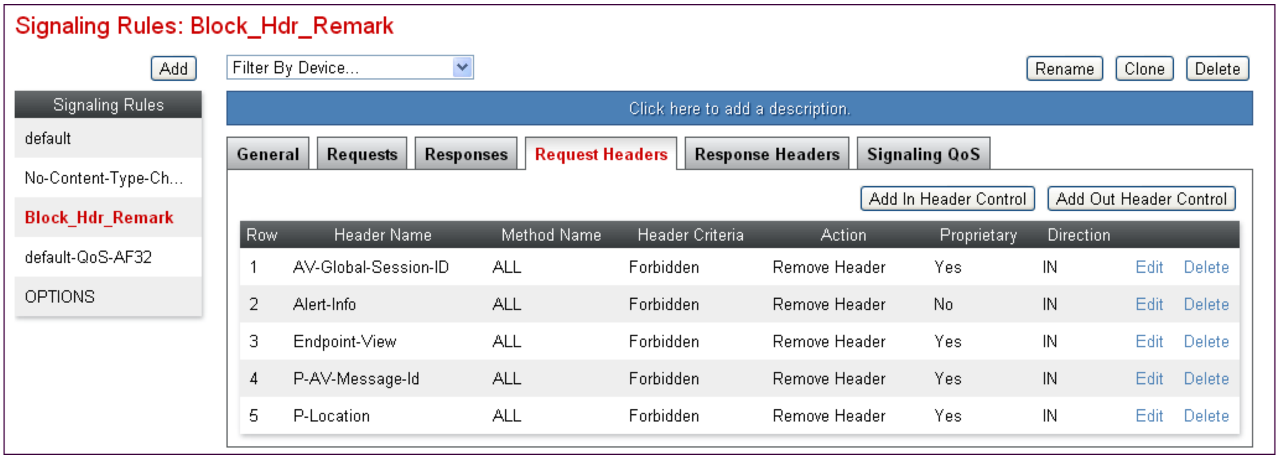
After this configuration, the new "Block_Hdr_Remark" will appear as follows.



Signaling Rules: Block_Hdr_Remark

Signaling QoS	☑
QoS Type	DSCP
DSCP	AF32

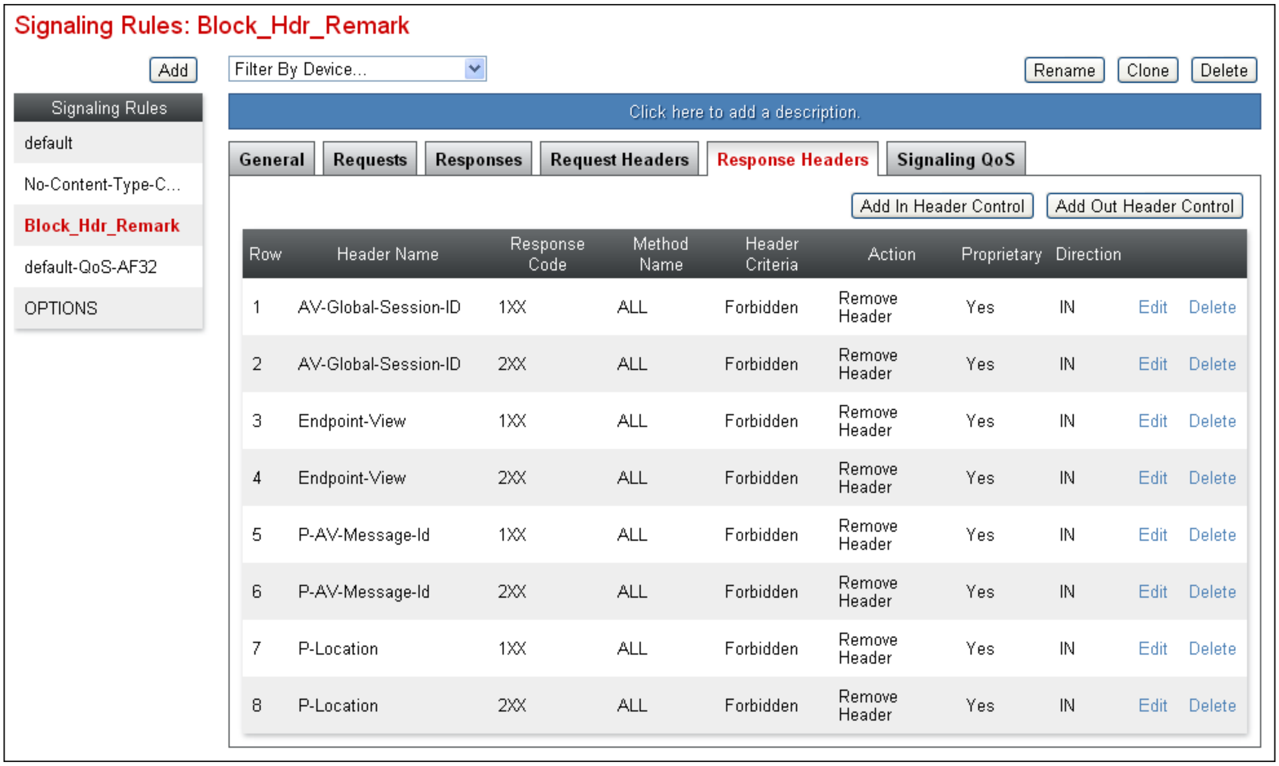
Select this rule in the center pane, then select the **Request Headers** tab to view the manipulations performed on the request messages such as the initial INVITE or UPDATE message. The following screen shows the “Alert-Info”, “Endpoint-View”, “P-Location" and other proprietary headers removed during the compliance test. This configuration is optional in that these headers do not cause any user-perceivable problems if presented to Verizon.



Signaling Rules: Block_Hdr_Remark

Row	Header Name	Method Name	Header Criteria	Action	Proprietary	Direction		
1	AV-Global-Session-ID	ALL	Forbidden	Remove Header	Yes	IN	Edit	Delete
2	Alert-Info	ALL	Forbidden	Remove Header	No	IN	Edit	Delete
3	Endpoint-View	ALL	Forbidden	Remove Header	Yes	IN	Edit	Delete
4	P-AV-Message-Id	ALL	Forbidden	Remove Header	Yes	IN	Edit	Delete
5	P-Location	ALL	Forbidden	Remove Header	Yes	IN	Edit	Delete

Similarly, manipulations can be performed on the SIP response messages. These can be viewed by selecting the **Response Headers** tab as shown below.



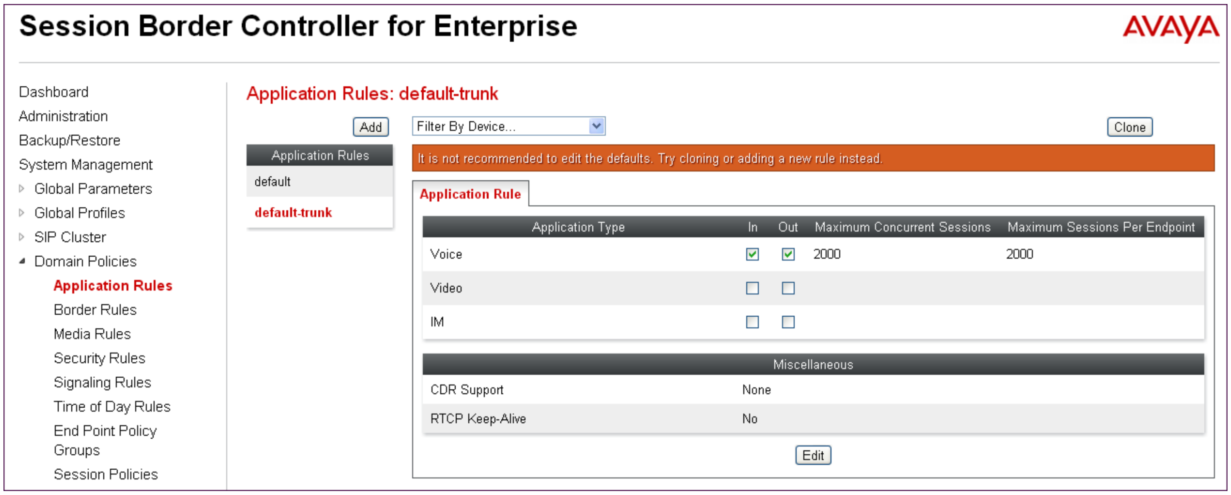
Signaling Rules: Block_Hdr_Remark

Row	Header Name	Response Code	Method Name	Header Criteria	Action	Proprietary	Direction		
1	AV-Global-Session-ID	1XX	ALL	Forbidden	Remove Header	Yes	IN	Edit	Delete
2	AV-Global-Session-ID	2XX	ALL	Forbidden	Remove Header	Yes	IN	Edit	Delete
3	Endpoint-View	1XX	ALL	Forbidden	Remove Header	Yes	IN	Edit	Delete
4	Endpoint-View	2XX	ALL	Forbidden	Remove Header	Yes	IN	Edit	Delete
5	P-AV-Message-Id	1XX	ALL	Forbidden	Remove Header	Yes	IN	Edit	Delete
6	P-AV-Message-Id	2XX	ALL	Forbidden	Remove Header	Yes	IN	Edit	Delete
7	P-Location	1XX	ALL	Forbidden	Remove Header	Yes	IN	Edit	Delete
8	P-Location	2XX	ALL	Forbidden	Remove Header	Yes	IN	Edit	Delete

7.8. Application Rule

Application Rules define which types of SIP-based Unified Communications (UC) applications the Avaya SBCE security device will protect: voice, video, and/or Instant Messaging (IM). In addition, the maximum number of concurrent voice and video sessions the network will process can be determined in order to prevent resource exhaustion.

Select **Domain Policies → Application Rules** from the left-side menu as shown below. In the sample configuration, a single default application rule “default-trunk” is used and will be applied to the Endpoint Policy Group in the next section.



Application Rules: default-trunk

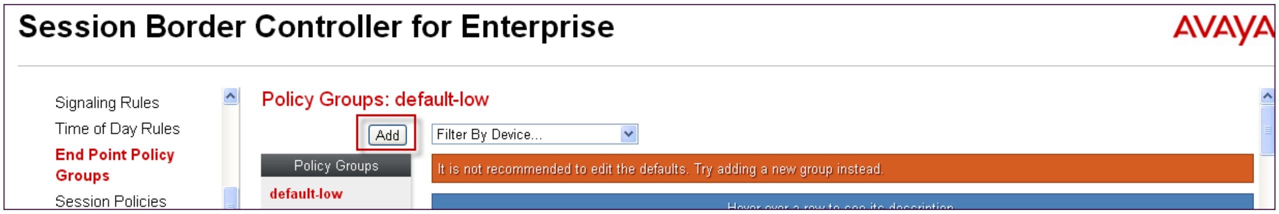
It is not recommended to edit the defaults. Try cloning or adding a new rule instead.

Application Type	In	Out	Maximum Concurrent Sessions	Maximum Sessions Per Endpoint
Voice	☑	☑	2000	2000
Video	□	□		
IM	□	□		

Miscellaneous	
CDR Support	None
RTCP Keep-Alive	No

7.9. Endpoint Policy Group

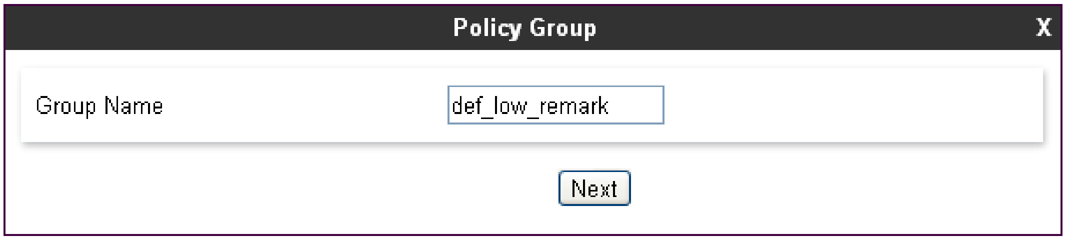
The rules created within the Domain Policy section are assigned to an Endpoint Policy Group. The Endpoint Policy Group is then applied to a Server Flow in **Section 7.12**. Create a separate Endpoint Policy Group for the enterprise and the Verizon IP Trunk. To create a new policy group, navigate to **Domain Policies → Endpoint Policy Groups**. Select the **Add** button.



Policy Groups: default-low

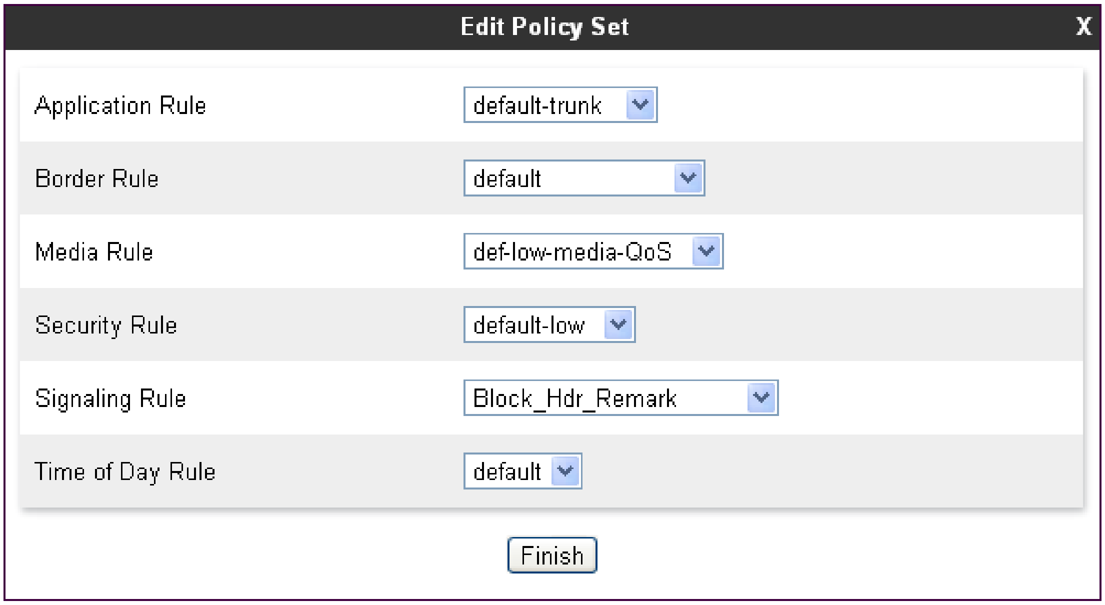
It is not recommended to edit the defaults. Try adding a new group instead.

Enter a name in the **Group Name** field, such as “def_low_remark” as shown below. Click **Next**.



Group Name: def_low_remark

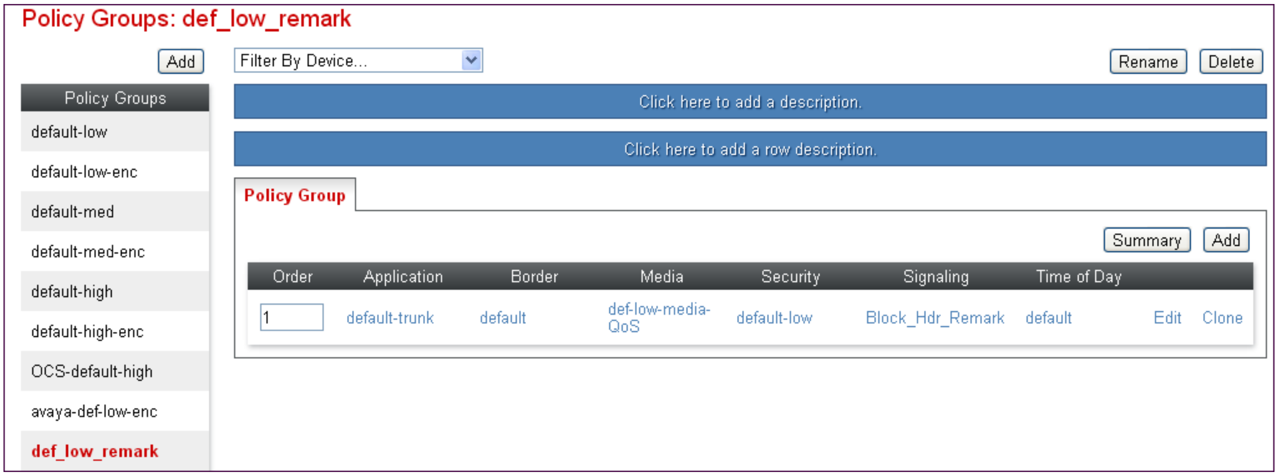
In the sample configuration, defaults were selected for all fields, with the exception of the **Application Rule** which is set to "default-trunk", **Media Rule** which is set to "default-low-media-QoS", and the **Signaling Rule**, which is set to "Block_Hdr_Remark" as shown below. The selected non-default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



Edit Policy Set

Application Rule	default-trunk
Border Rule	default
Media Rule	def-low-media-QoS
Security Rule	default-low
Signaling Rule	Block_Hdr_Remark
Time of Day Rule	default

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



Policy Groups: def_low_remark

Policy Groups: default-low, default-low-enc, default-med, default-med-enc, default-high, default-high-enc, OCS-default-high, avaya-def-low-enc, def_low_remark

Click here to add a description.

Click here to add a row description.

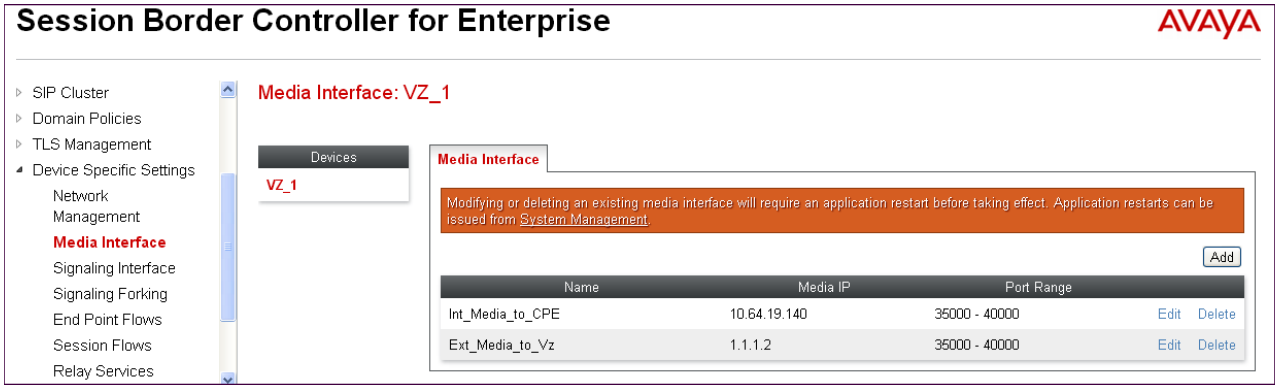
Policy Group

Order	Application	Border	Media	Security	Signaling	Time of Day		
1	default-trunk	default	def-low-media-QoS	default-low	Block_Hdr_Remark	default	Edit	Clone

7.10. Media Interface

The Media Interface screen is where the SIP media ports are defined. Avaya SBCE will send SIP media on the defined ports. Create a SIP Media Interface for both the inside and outside IP interfaces.

To create a new Signaling Interface, navigate to **Device Specific Settings → Media Interface** and click **Add Media Interface**. The following screen shows the media interfaces created in the sample configuration for the inside and outside IP interfaces.



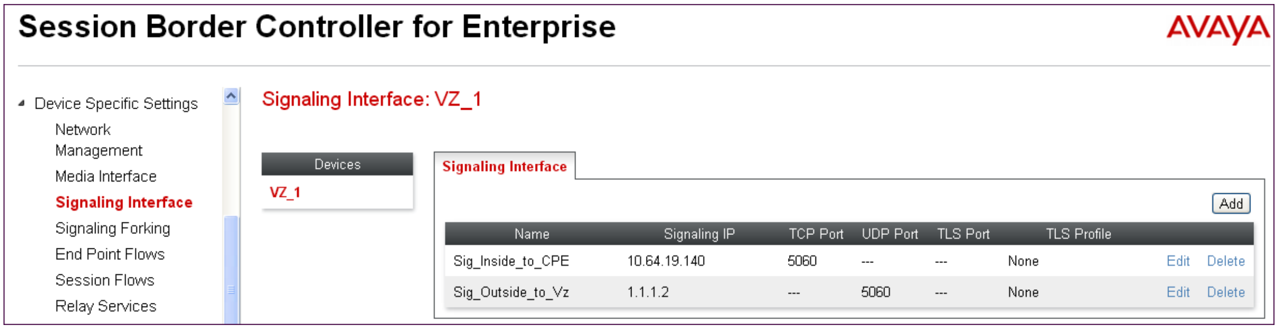
Modifying or deleting an existing media interface will require an application restart before taking effect. Application restarts can be issued from System Management.

Name	Media IP	Port Range		
Int_Media_to_CPE	10.64.19.140	35000 - 40000	Edit	Delete
Ext_Media_to_Vz	1.1.1.2	35000 - 40000	Edit	Delete

7.11. Signaling Interface

The Signaling Interface screen is where the SIP signaling ports are defined. Avaya SBCE will listen for SIP requests on the defined ports. Create a Signaling Interface for both the inside and outside IP interfaces.

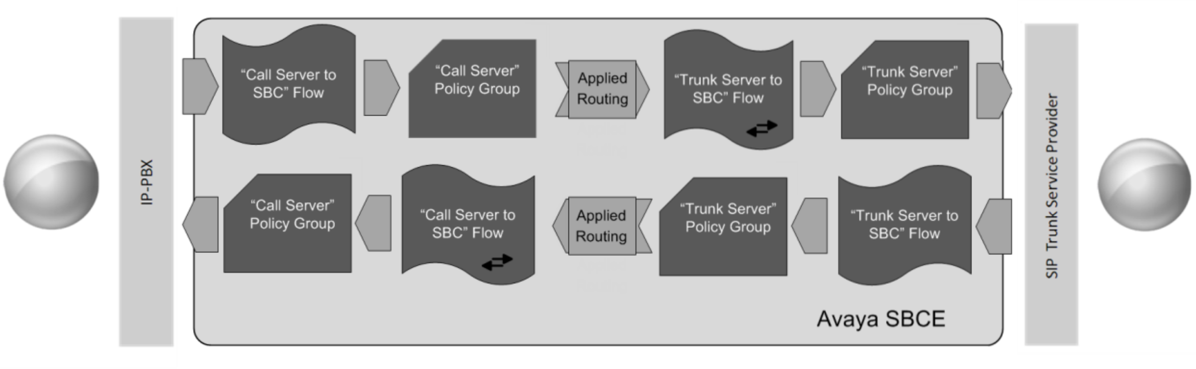
To create a new Signaling Interface, navigate to **Device Specific Settings → Signaling Interface** and click **Add Signaling Interface**. The following screen shows the signaling interfaces created in the sample configuration for the inside and outside IP interfaces.



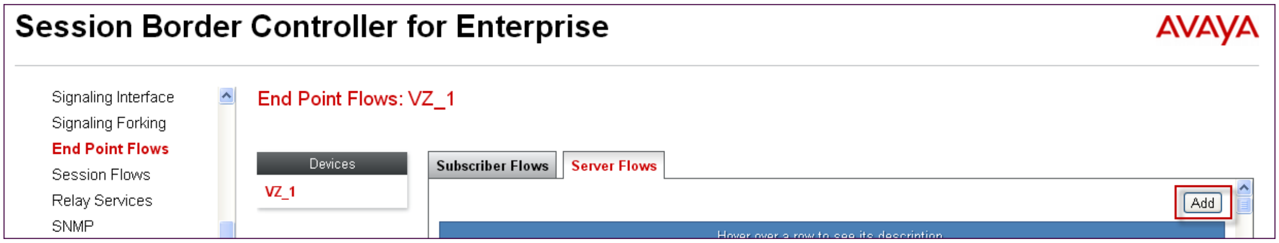
Name	Signaling IP	TCP Port	UDP Port	TLS Port	TLS Profile		
Sig_Inside_to_CPE	10.64.19.140	5060	---	---	None	Edit	Delete
Sig_Outside_to_Vz	1.1.1.2	---	5060	---	None	Edit	Delete

7.12. End Point Flows - Server Flow

When a packet is received by Avaya SBCE, the content of the packet (IP addresses, URIs, etc.) is used to determine which flow it matches. Once the flow is determined, the flow points to a policy which contains several rules concerning processing, privileges, authentication, routing, etc. Once routing is applied and the destination endpoint is determined, the policies for this destination endpoint are applied. The context is maintained, so as to be applied to future packets in the same flow. The following screen illustrates the flow through the Avaya SBCE to secure a SIP Trunk call.

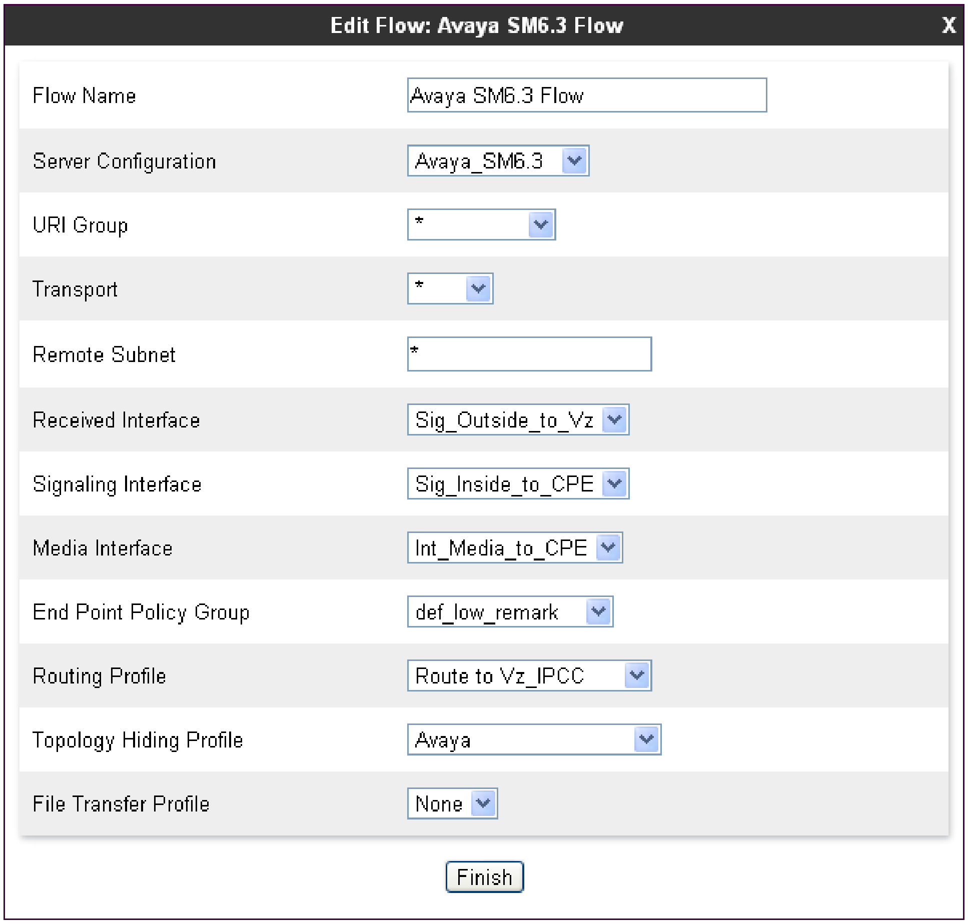

IP-PBX
"Call Server to SBC" Flow
"Call Server" Policy Group
Applied Routing
"Trunk Server to SBC" Flow
"Trunk Server" Policy Group
"Call Server" Policy Group
"Call Server to SBC" Flow
Applied Routing
"Trunk Server" Policy Group
"Trunk Server to SBC" Flow
Avaya SBCE
SIP Trunk Service Provider

Create a Server Flow for Session Manager and the Verizon IP Trunk. To create a Server Flow, navigate to **Device Specific Settings → End Point Flows**. Select the **Server Flows** tab and click **Add Flow** as shown below.


Session Border Controller for Enterprise

End Point Flows: VZ_1

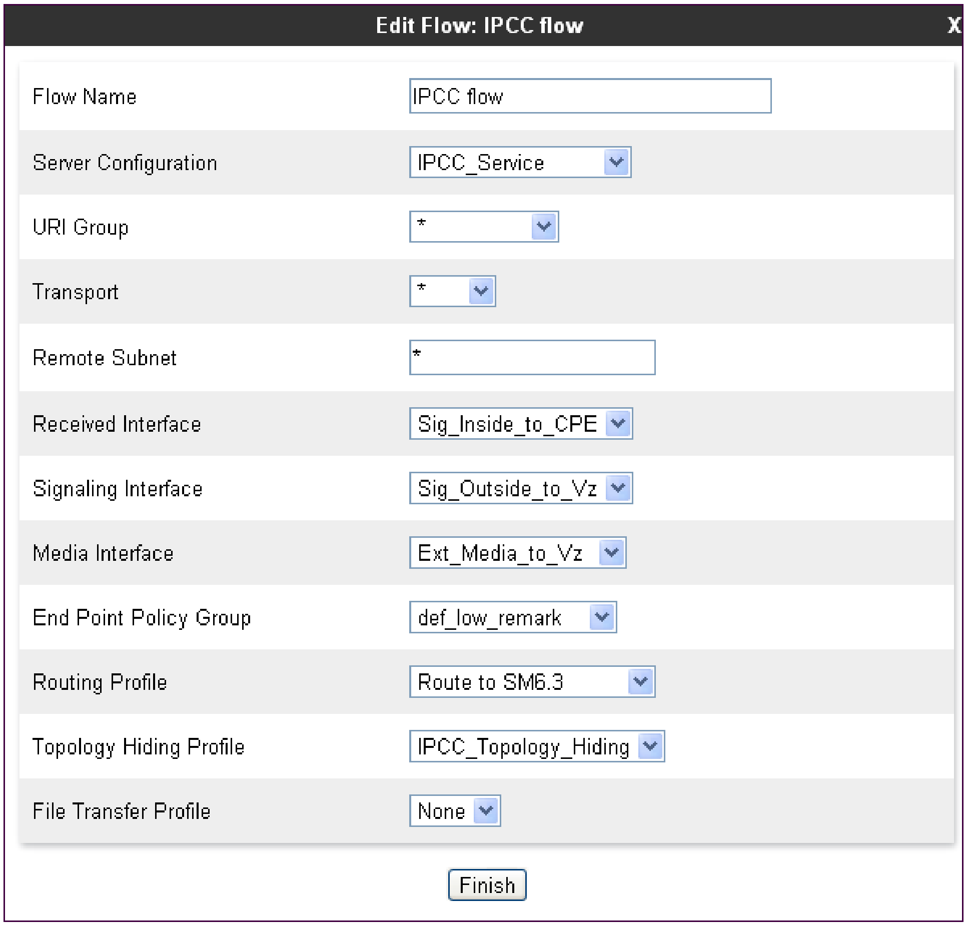
The following screen shows the flow named "Avaya SM6.3 Flow" used in the sample configuration. This flow uses the interfaces, policies, and profiles defined in previous sections. Click **Finish**.



Edit Flow: Avaya SM6.3 Flow

Flow Name	Avaya SM6.3 Flow
Server Configuration	Avaya_SM6.3
URI Group	*
Transport	*
Remote Subnet	*
Received Interface	Sig_Outside_to_Vz
Signaling Interface	Sig_Inside_to_CPE
Media Interface	Int_Media_to_CPE
End Point Policy Group	def_low_remark
Routing Profile	Route to Vz_IPCC
Topology Hiding Profile	Avaya
File Transfer Profile	None

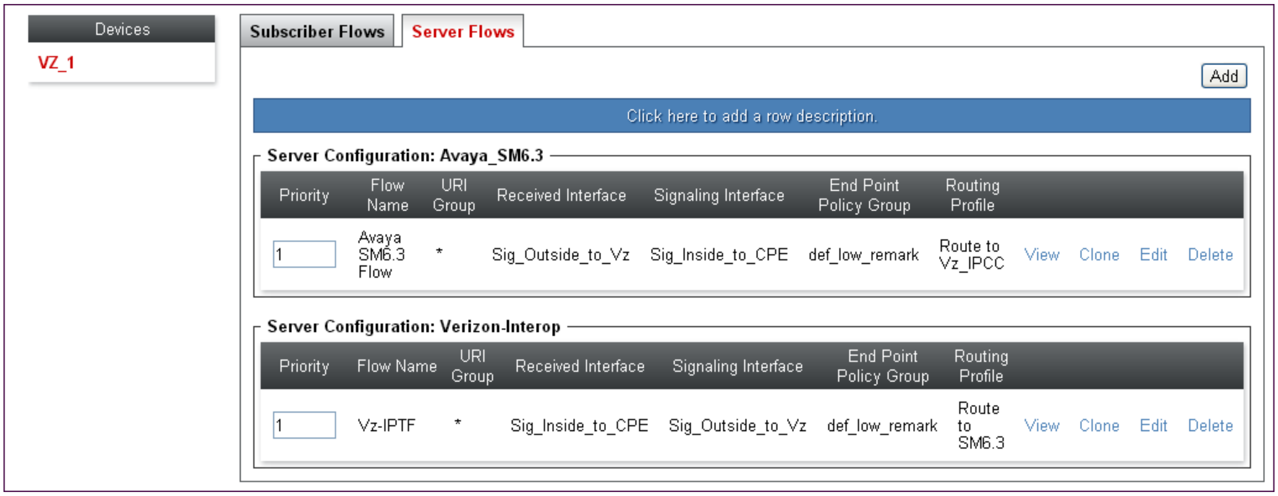
Once again, select the **Server Flows** tab and click **Add Flow**. The following screen shows the flow named “Verizon_IP_Trunk” created in the sample configuration. This flow uses the interfaces, policies, and profiles defined in previous sections. Click **Finish**.



Edit Flow: IPCC flow

Flow Name	IPCC flow
Server Configuration	IPCC_Service
URI Group	*
Transport	*
Remote Subnet	*
Received Interface	Sig_Inside_to_CPE
Signaling Interface	Sig_Outside_to_Vz
Media Interface	Ext_Media_to_Vz
End Point Policy Group	def_low_remark
Routing Profile	Route to SM6.3
Topology Hiding Profile	IPCC_Topology_Hiding
File Transfer Profile	None

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



Server Configuration: Avaya_SM6.3

Priority	Flow Name	URI Group	Received Interface	Signaling Interface	End Point Policy Group	Routing Profile				
1	Avaya SM6.3 Flow	*	Sig_Outside_to_Vz	Sig_Inside_to_CPE	def_low_remark	Route to Vz_IPCC	View	Clone	Edit	Delete

Server Configuration: Verizon-Interop

Priority	Flow Name	URI Group	Received Interface	Signaling Interface	End Point Policy Group	Routing Profile				
1	Vz-IPTF	*	Sig_Inside_to_CPE	Sig_Outside_to_Vz	def_low_remark	Route to SM6.3	View	Clone	Edit	Delete

8. Verizon Business IPCC Services Suite Configuration

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

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

8.1. Service Access Information

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

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

Toll Free Numbers
866-850-2380
866-851-0107
866-851-2649
866-852-3221
866-850-6850

9. Verification Steps

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

9.1. Avaya Aura® Communication Manager Verifications

This section illustrates verifications from Communication Manager.

9.1.1 Example Incoming Call from PSTN via Verizon IPCC to Telephone

Incoming PSTN calls arrive from Verizon at Avaya SBCE, which sends the call to Session Manager. Session Manager sends the call to Communication Manager. On Communication Manager, the incoming call arrives via signaling group 2 and trunk group 2.

The following edited Communication Manager ***list trace tac*** trace output shows a call incoming on trunk group 2. The PSTN telephone dialed 866-850-6850. Session Manager mapped the number received from Verizon to the extension of a Communication Manager telephone (x12005). Extension 12005 is an IP Telephone with IP address 10.64.19.101 in Region 1. Initially, the G450 Media Gateway (10.64.18.81) is used, but as can be seen in the final trace output, once the call is answered, the final RTP media path is "ip-direct" from the IP Telephone (10.64.19.101) to the "inside" of the Avaya SBCE (10.64.19.140) in Region 2.

```
list trace tac *02                                                  Page   1
                                LIST TRACE
time            data
/* Incoming call arrives to Communication Manager for x12005 */
10:40:01 TRACE STARTED 05/07/2013 CM Release String cold-02.0.823.0-20396
10:41:10 SIP<INVITE sip:12005@avayalab.com SIP/2.0
10:41:10     Call-ID: 11905073701052985101@63.64.24.199
10:41:10     active trunk-group 1 member 1    cid 0x18ba
/* Communication Manager sends 183 with SDP as a result of TG 1 configuration */
10:41:10 SIP>SIP/2.0 183 Session Progress
10:41:10     Call-ID: 11905073701052985101@63.64.24.199
10:41:10     dial 12005
10:41:10     ring station      12005 cid 0x18ba
/* G450 Gateway at 10.64.19.81, ringback tone heard by caller */
10:41:10     G711MU ss:off ps:20
             rgn:1 [10.64.19.101]:3314
             rgn:1 [10.64.19.81]:2050
10:41:10     G729 ss:off ps:20
             rgn:2 [10.64.19.140]:35004
             rgn:1 [10.64.19.81]:2054
10:41:10     xoip options: fax:T38 modem:off tty:US  uid:0x50009
             xoip ip: [10.64.19.81]:2054
/* User Answers call, Communication Manager sends 200 OK */
10:41:13 SIP>SIP/2.0 200 OK
10:41:13     Call-ID: 11905073701052985101@63.64.24.199
10:41:13     active station      12005 cid 0x18ba
/* Communication Manager receives ACK to 200 OK */
10:41:13 SIP<ACK sip:12005@10.64.19.205:5071;transport=tls SIP/2.0
10:41:13     Call-ID: 11905073701052985101@63.64.24.199

<continued on next page>
```

```
/* Communication Manager sends re-INVITE to begin shuffle to ip-direct */
10:41:13 SIP>INVITE sip:+13035387006@10.64.19.140:5060;transport=tcp
10:41:13 SIP>;gsid=ec2f2030-b734-11e2-b83f-9c8e992b0a68 SIP/2.0
10:41:13     Call-ID: 11905073701052985101@63.64.24.199
10:41:13 SIP<SIP/2.0 100 Trying
10:41:13     Call-ID: 11905073701052985101@63.64.24.199
/* Communication Manager receives 200 OK with SDP, sends ACK with SDP */
10:41:13 SIP<SIP/2.0 200 OK
10:41:13     Call-ID: 11905073701052985101@63.64.24.199
10:41:13 SIP>ACK sip:+13035387006@10.64.19.140:5060;transport=tcp;gs
10:41:13 SIP>id=ec2f2030-b734-11e2-b83f-9c8e992b0a68 SIP/2.0
10:41:13     Call-ID: 11905073701052985101@63.64.24.199
/* Final media path is ip-direct from answering IP (10.64.19.101) to inside of SBC
(10.64.19.140) */
10:41:13     G729A ss:off ps:20
             rgn:2 [10.64.19.140]:35004
             rgn:1 [10.64.19.101]:3314
10:41:13     G729 ss:off ps:20
             rgn:1 [10.64.19.101]:3314
             rgn:2 [10.64.19.140]:35004
```

The following screen shows **Page 2** of the output of the ***status trunk*** command pertaining to this same call. Note the signaling using port 5071 between Communication Manager and Session Manager. Note the media is "ip-direct" from the IP Telephone (10.64.19.109) to the inside IP address of Avaya SBCE (10.64.19.140) using codec G.729a.

```
status trunk 2/1                                                Page   2 of   3
                                CALL CONTROL SIGNALING

Near-end Signaling Loc: PROCR
  Signaling   IP Address                               Port
   Near-end:  10.64.19.155                           : 5071
    Far-end:  10.64.19.226                           : 5071
 H.245 Near:
  H.245 Far:
   H.245 Signaling Loc:           H.245 Tunneled in Q.931? no

 Audio Connection Type: ip-direct     Authentication Type: None
    Near-end Audio Loc:                        Codec Type: G.729
   Audio      IP Address                               Port
   Near-end:  10.64.19.101                           : 3314
    Far-end:  10.64.19.140                           : 35006
```

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

```
status trunk 2/1                                                Page   3 of   3
                      SRC PORT TO DEST PORT TALKPATH
src port: T00009
T00009:TX:10.64.19.140:35014/g729/20ms
S00003:RX:10.64.19.101:3314/g729a/20ms
```

9.1.2 Example Incoming Call Referred via Call Vector to PSTN Destination

The following edited and annotated Communication Manager ***list trace tac*** trace output shows a call incoming on trunk group 2. The call was routed to a Communication Manager vector directory number (VDN 10001) associated with a call vector (call vector 1). The vector answers the call, plays an announcement to the caller, and then uses a "route-to" step to cause a REFER message to be sent with a Refer-To header containing the number configured in the vector "route-to" step. The PSTN telephone dialed 866-852-3221. Session Manager can map the number received from Verizon to the VDN extension (x10001), or the incoming call handling table for trunk group 1 can do the same. In the trace below, Session Manager had already mapped the Verizon number to the Communication Manager VDN extension. The annotations in the edited trace highlight key behaviors. At the conclusion, the PSTN caller that dialed the Verizon toll-free number is talking to the Referred-to PSTN destination, and no trunks (i.e., from trunk 1 handling the call) are in use.

```
list trace tac *02                                                Page   1
/* Session Manager has adapted the dialed number 8668523221 to VDN 10001 */
14:21:06 SIP<INVITE sip:10001@avayalab.com SIP/2.0
14:21:06     Call-ID: 2036505164-1723268874@10.10.20.23
14:21:06     active trunk-group 1 member 1    cid 0x18dd
14:21:06    0  0 ENTERING TRACE cid 6365
14:21:06    2  1 vdn e10001 bsr appl   0 strategy 1st-found override n
14:21:06    2  1 wait 2 secs hearing ringback
14:21:06 SIP>SIP/2.0 183 Session Progress
14:21:06     Call-ID: 2036505164-1723268874@10.10.20.23
14:21:06     dial 10001
14:21:06     ring vector 2      cid 0x18dd
/* Vector step plays ringback. A 183 with SDP is sent*/
14:21:06     G729 ss:off ps:20
             rgn:2 [10.64.19.140]:35002
             rgn:1 [10.64.19.81]:2062
14:21:06     xoip options: fax:T38 modem:off tty:US  uid:0x50009
             xoip ip: [10.64.19.81]:2062
14:21:08    2  2 # Play announcement to caller i...
14:21:08    2  3 announcement 11006
14:21:08 SIP>SIP/2.0 183 Session Progress
14:21:08     Call-ID: 2036505164-1723268874@10.10.20.23
14:21:08    2  3      announcement: board 001V9 ann ext: 11006
/* Vector step answers call with announcement. 200 OK is sent */
14:21:08 SIP>SIP/2.0 200 OK
14:21:08     Call-ID: 2036505164-1723268874@10.10.20.23
14:21:08     active announcement      11006 cid 0x18dd
14:21:08     hear annc board 001V9 ext 11006 cid 0x18dd
14:21:08 SIP<ACK sip:8668523221@10.64.19.205:5071;transport=tls SIP/
14:21:08 SIP<2.0
14:21:08     Call-ID: 2036505164-1723268874@10.10.20.23
/* Caller hears pre-REFER announcement, announcement completes, REFER sent */
14:21:11     idle announcement       cid 0x18dd
14:21:11    2  4 # Refer the call to PSTN Destin...
14:21:11    2  5 route-to number ~r+13035387024 cov n if unconditionally
14:21:11 SIP>REFER sip:+13035387006@10.64.19.140:5060;transport=tcp;
14:21:11 SIP>gsid=a5787640-b753-11e2-b83f-9c8e992b0a68 SIP/2.0
14:21:11     Call-ID: 2036505164-1723268874@10.10.20.23
/* Communication Manager receives 202 Accepted sent by Verizon IPCC */
14:21:11 SIP<SIP/2.0 202 Accepted
14:21:11     Call-ID: 2036505164-1723268874@10.10.20.23

<continued on next page>
```

```
/* Verizon IPCC sends re-INVITE with c=0.0.0.0 SDP and 200 OK/ACK occur */
14:21:11 SIP<INVITE sip:8668523221@10.64.19.205:5071;transport=tls S
14:21:11 SIP<IP/2.0
14:21:11     Call-ID: 2036505164-1723268874@10.10.20.23
14:21:11 SIP>SIP/2.0 100 Trying
14:21:11     Call-ID: 2036505164-1723268874@10.10.20.23
14:21:11 SIP>SIP/2.0 200 OK
14:21:11     Call-ID: 2036505164-1723268874@10.10.20.23
/* Verizon IPCC sends NOTIFY with sipfrag 100 Trying,CM sends 200 OK */
14:21:11 SIP<NOTIFY sip:8668523221@10.64.19.205:5071;transport=tls S
14:21:11 SIP<IP/2.0
14:21:11     Call-ID: 2036505164-1723268874@10.10.20.23
14:21:11 SIP>SIP/2.0 200 OK
14:21:11     Call-ID: 2036505164-1723268874@10.10.20.23
14:21:11 SIP<ACK sip:8668523221@10.64.19.205:5071;transport=tls SIP/
14:21:11 SIP<2.0
14:21:11     Call-ID: 2036505164-1723268874@10.10.20.23
14:21:16 SIP<NOTIFY sip:8668523221@10.64.19.205:5071;transport=tls S
14:21:16 SIP<IP/2.0
14:21:16     Call-ID: 2036505164-1723268874@10.10.20.23
14:21:16 SIP>SIP/2.0 200 OK
* Note that caller does not hear ringback or any audible feedback until answer */
/* Verizon IPCC sends NOTIFY with sipfrag 200 OK and CM sends 200 OK and BYE */
14:21:16     Call-ID: 2036505164-1723268874@10.10.20.23
14:21:16    2  5 LEAVING VECTOR PROCESSING cid 6365
14:21:16 SIP>BYE sip:+13035387006@10.64.19.140:5060;transport=tcp;gs
14:21:16 SIP>id=a5787640-b753-11e2-b83f-9c8e992b0a68 SIP/2.0
14:21:16     Call-ID: 2036505164-1723268874@10.10.20.23
14:21:16     idle vector 0      cid 0x18dd
/* Trunks are now idle. Caller and refer-to target are connected by Verizon */
```

When the initial call arrived from Verizon, it used trunk member 1 from trunk group 2. In the final state when the PSTN caller is speaking with the answering agent at the Refer-To target, trunk member 1 is idle, reflecting the successful REFER.

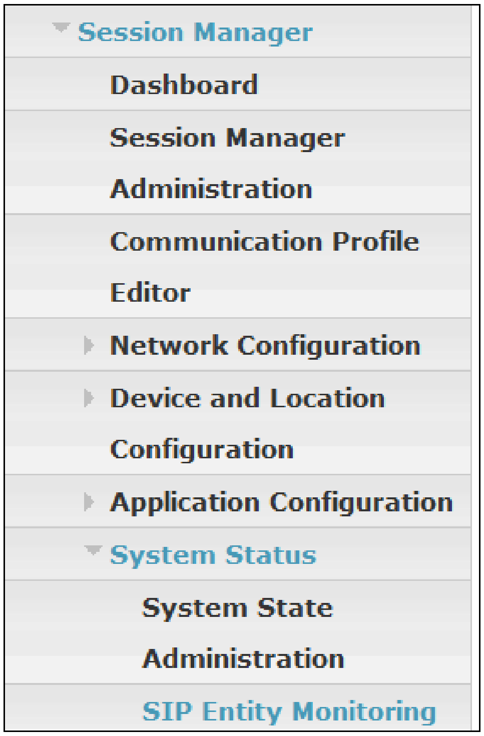
```
status trunk 2
                              TRUNK GROUP STATUS
Member   Port     Service State      Mtce Connected Ports
                                     Busy
0077/001 T00041   in-service/idle    no
0077/002 T00042   in-service/idle    no
0077/003 T00043   in-service/idle    no
0077/004 T00044   in-service/idle    no
0077/005 T00045   in-service/idle    no
0077/006 T00046   in-service/idle    no
0077/007 T00047   in-service/idle    no
0077/008 T00048   in-service/idle    no
0077/009 T00049   in-service/idle    no
0077/010 T00050   in-service/idle    no
```

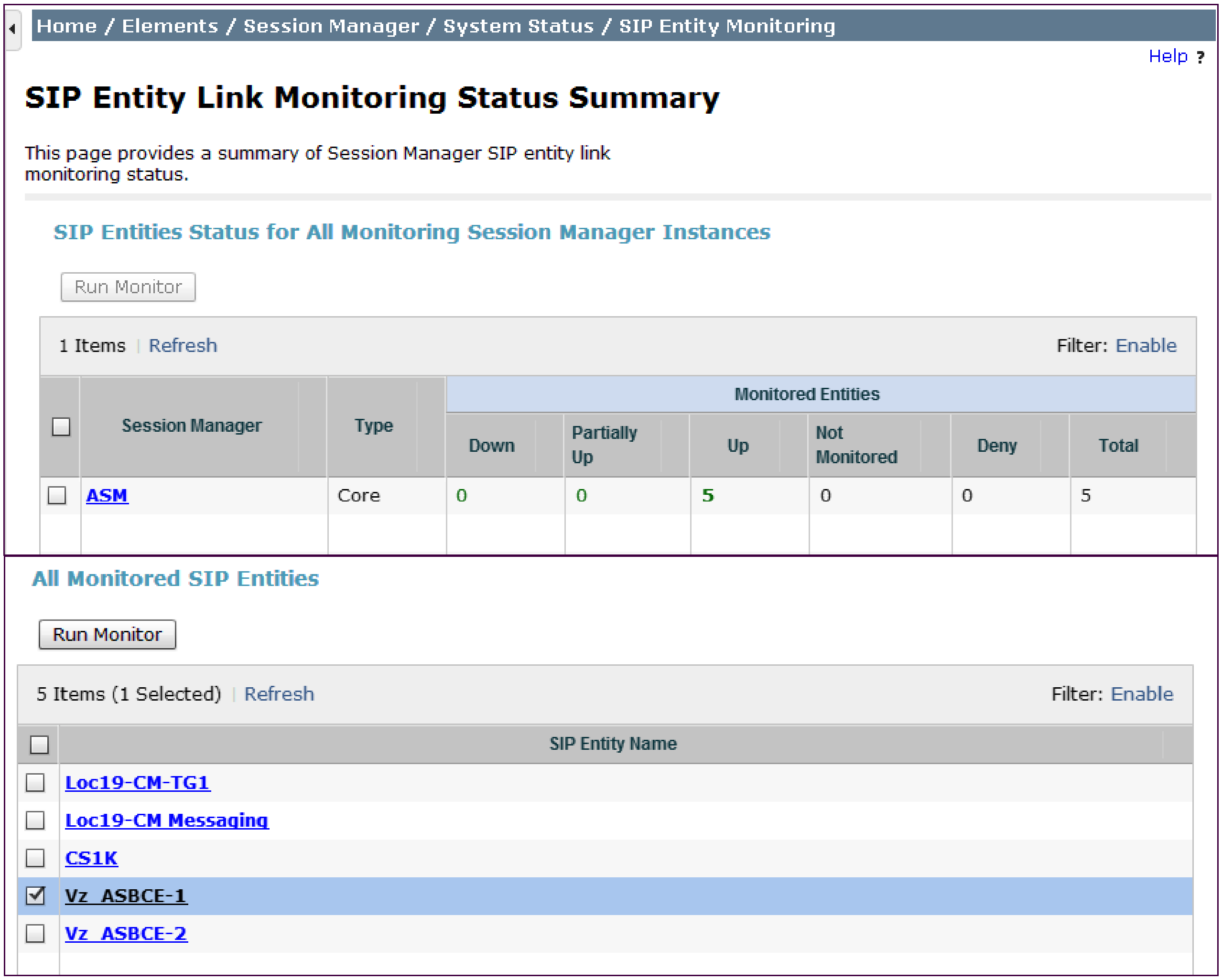
9.2. Avaya Aura® System Manager and Avaya Aura® Session Manager Verifications

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

9.2.1 Verify SIP Entity Link Status

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


Session Manager
Dashboard
Session Manager Administration
Communication Profile Editor
Network Configuration
Device and Location Configuration
Application Configuration
System Status
System State Administration
SIP Entity Monitoring



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

Help ?

SIP Entity Link Monitoring Status Summary

This page provides a summary of Session Manager SIP entity link monitoring status.

SIP Entities Status for All Monitoring Session Manager Instances

Run Monitor

1 Items | Refresh   Filter: Enable

□	Session Manager	Type	Monitored Entities					
			Down	Partially Up	Up	Not Monitored	Deny	Total
□	ASM	Core	0	0	5	0	0	5

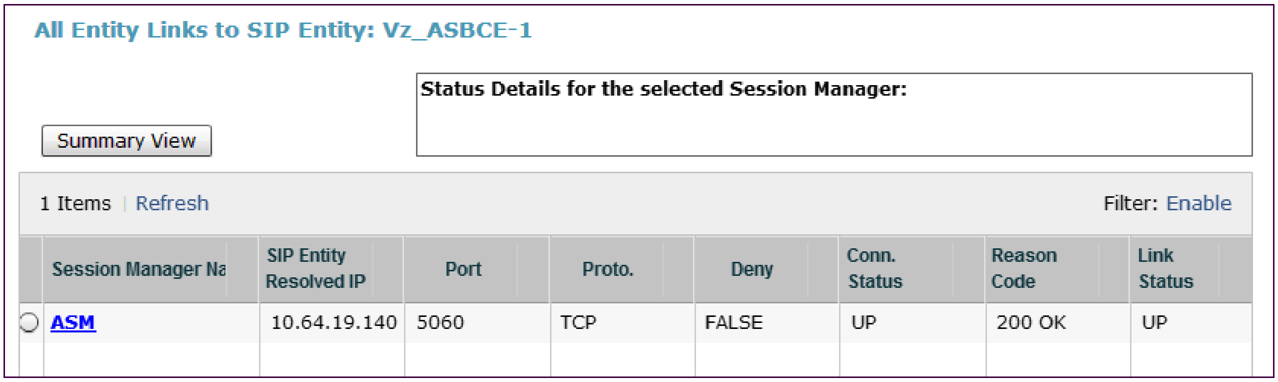
All Monitored SIP Entities

Run Monitor

5 Items (1 Selected) | Refresh   Filter: Enable

□	SIP Entity Name
□	Loc19-CM-TG1
□	Loc19-CM Messaging
□	CS1K
☑	Vz_ASBCE-1
□	Vz_ASBCE-2

From the list of monitored entities, select an entity of interest, such as “Vz_ASBCE-1”. Under normal operating conditions, the **Link Status** should be “UP” as shown in the example screen below.



All Entity Links to SIP Entity: Vz_ASBCE-1

Summary View

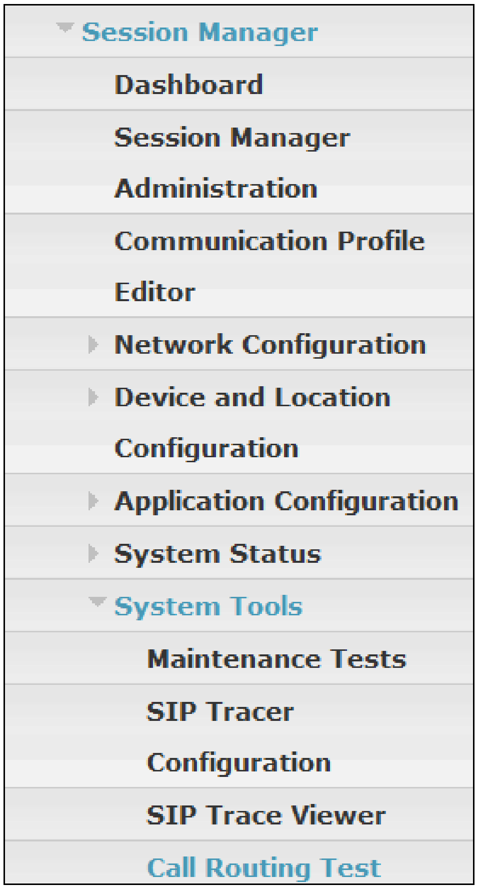
Status Details for the selected Session Manager:

1 Items | Refresh   Filter: Enable

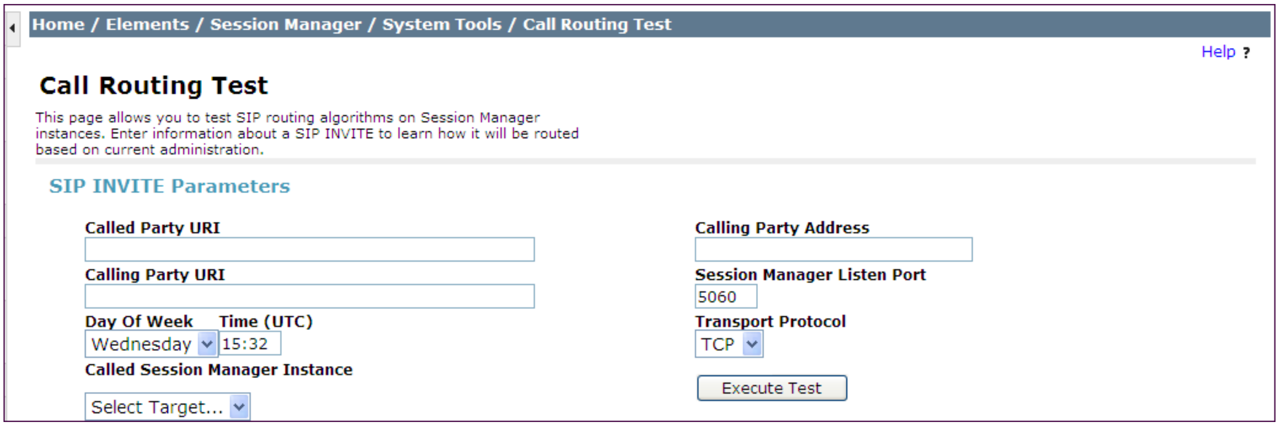
	Session Manager Na	SIP Entity Resolved IP	Port	Proto.	Deny	Conn. Status	Reason Code	Link Status
○	ASM	10.64.19.140	5060	TCP	FALSE	UP	200 OK	UP

9.2.2 Call Routing Test

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



A screen such as the following is displayed.


Home / Elements / Session Manager / System Tools / Call Routing Test
Help ?

Call Routing Test

This page allows you to test SIP routing algorithms on Session Manager instances. Enter information about a SIP INVITE to learn how it will be routed based on current administration.

SIP INVITE Parameters

Called Party URI

Calling Party URI

Day Of Week: Wednesday   Time (UTC): 15:32

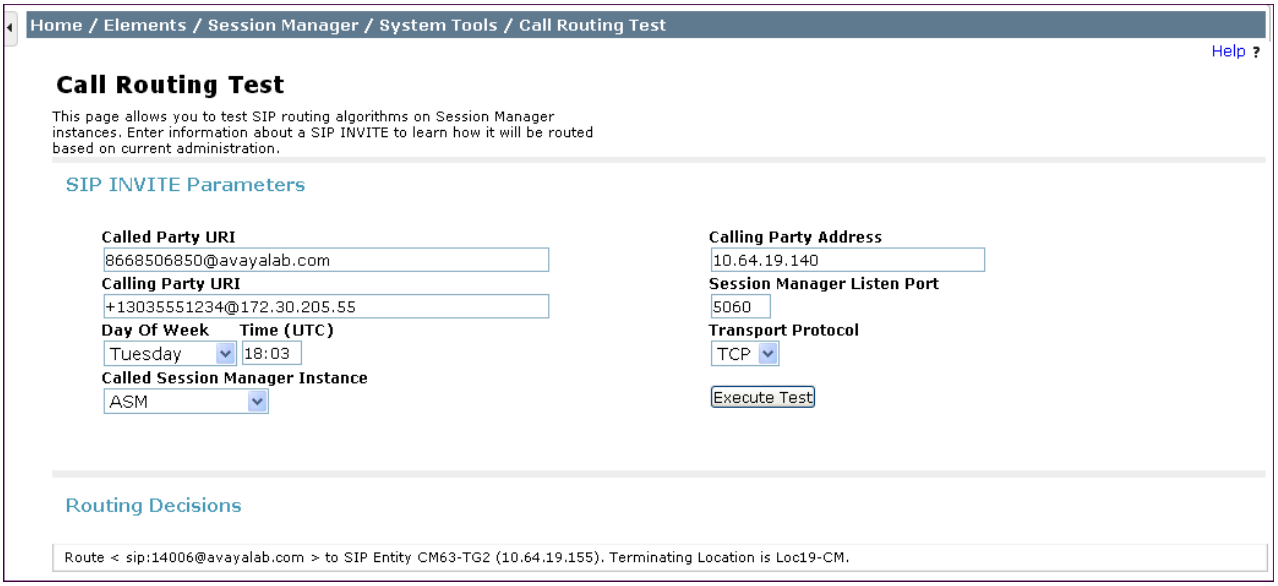
Called Session Manager Instance: Select Target...

Calling Party Address

Session Manager Listen Port: 5060

Transport Protocol: TCP

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 (10.64.19.140). Under **Routing Decisions**, observe that the call will route to the Communication Manager using the SIP entity named "CM63-TG2". The digits are manipulated such that the Verizon toll-free number (i.e., 866-850-6850) is converted to a Communication Manager extension (i.e., 14006) by the adapter assigned to the Communication Manager entity. Scroll down to inspect the details of the **Routing Decision Process** if desired (not shown).


Home / Elements / Session Manager / System Tools / Call Routing Test
Help ?

Call Routing Test

This page allows you to test SIP routing algorithms on Session Manager instances. Enter information about a SIP INVITE to learn how it will be routed based on current administration.

SIP INVITE Parameters

Called Party URI: 8668506850@avayalab.com
Calling Party URI: +13035551234@172.30.205.55
Day Of Week: Tuesday
Time (UTC): 18:03
Called Session Manager Instance: ASM
Calling Party Address: 10.64.19.140
Session Manager Listen Port: 5060
Transport Protocol: TCP

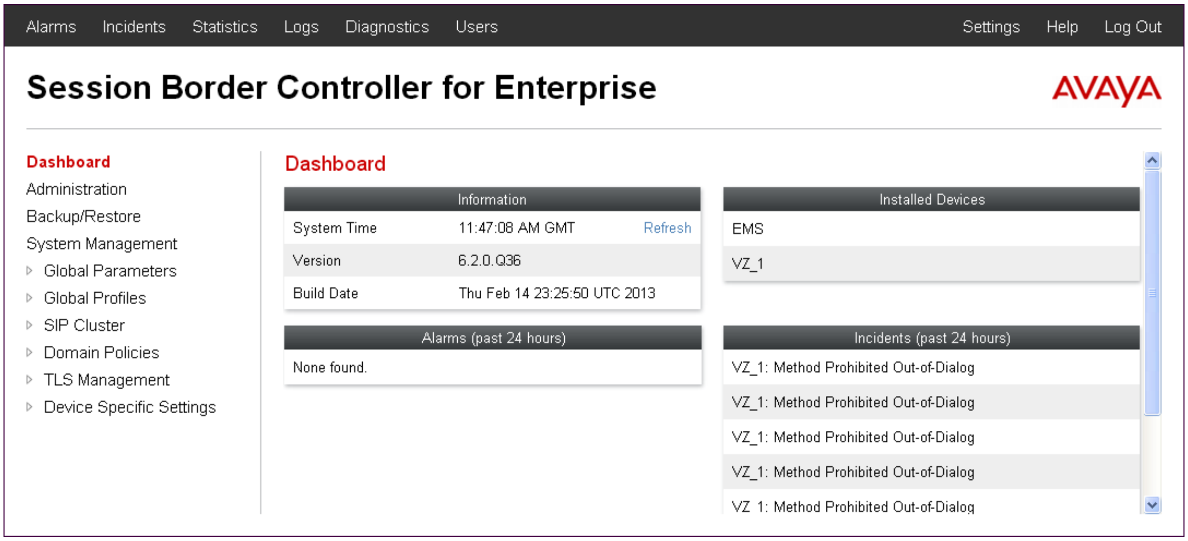
Routing Decisions

Route < sip:14006@avayalab.com > to SIP Entity CM63-TG2 (10.64.19.155). Terminating Location is Loc19-CM.

9.3. Avaya Session Border Controller for Enterprise Verification

9.3.1 Welcome Screen

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



Dashboard

Information		
System Time	11:47:08 AM GMT	Refresh
Version	6.2.0.Q36	
Build Date	Thu Feb 14 23:25:50 UTC 2013	

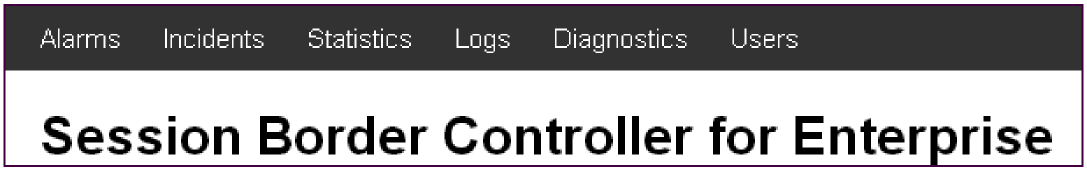
Installed Devices
EMS
VZ_1

Alarms (past 24 hours)
None found.

Incidents (past 24 hours)
VZ_1: Method Prohibited Out-of-Dialog
VZ_1: Method Prohibited Out-of-Dialog
VZ_1: Method Prohibited Out-of-Dialog
VZ_1: Method Prohibited Out-of-Dialog
VZ_1: Method Prohibited Out-of-Dialog

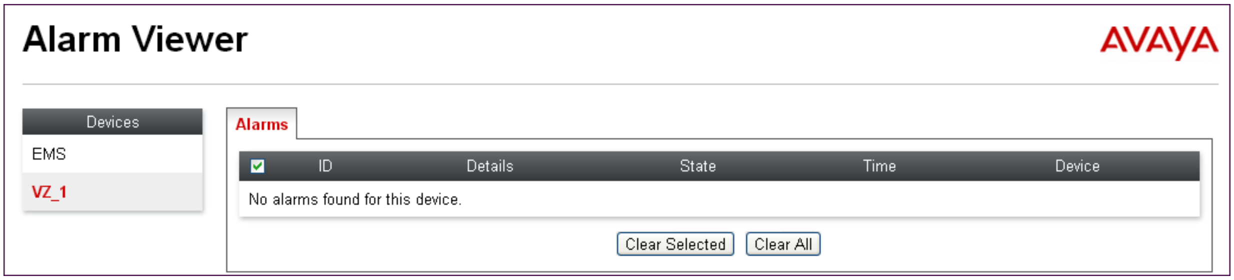
9.3.2 Alarms

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



Session Border Controller for Enterprise

Alarm Viewer.

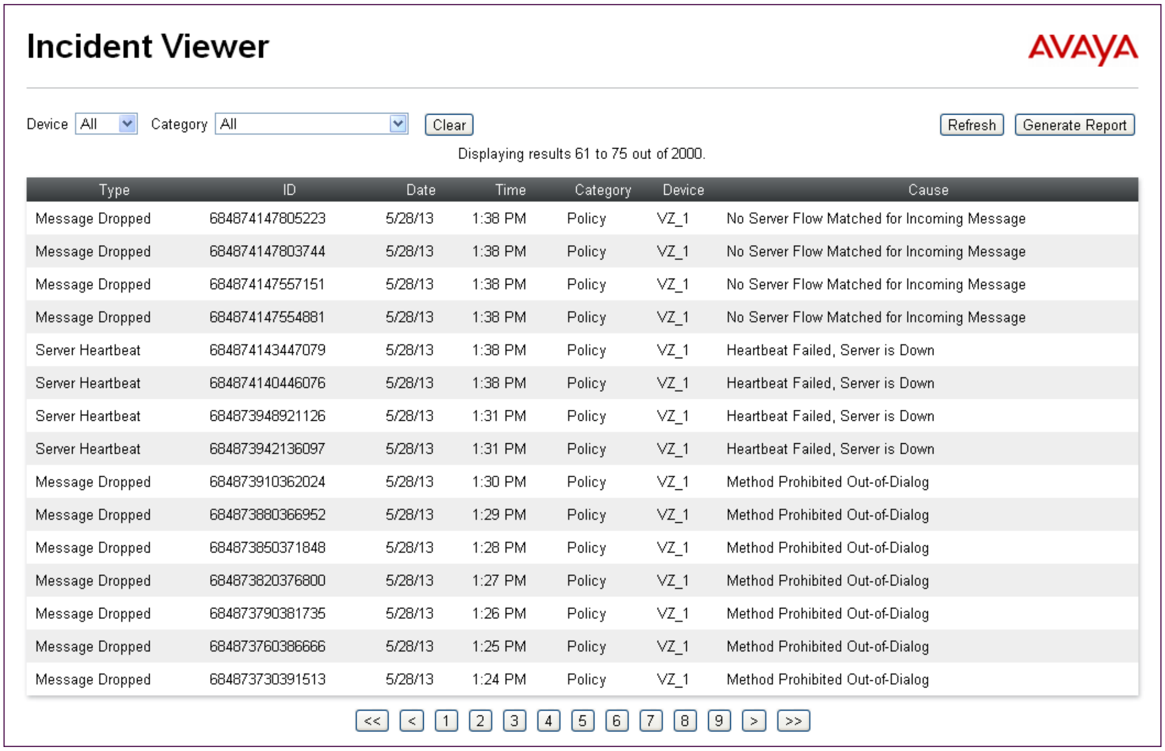

Alarm Viewer

☑	ID	Details	State	Time	Device
No alarms found for this device.					

9.3.3 Incidents

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

Incident Viewer.

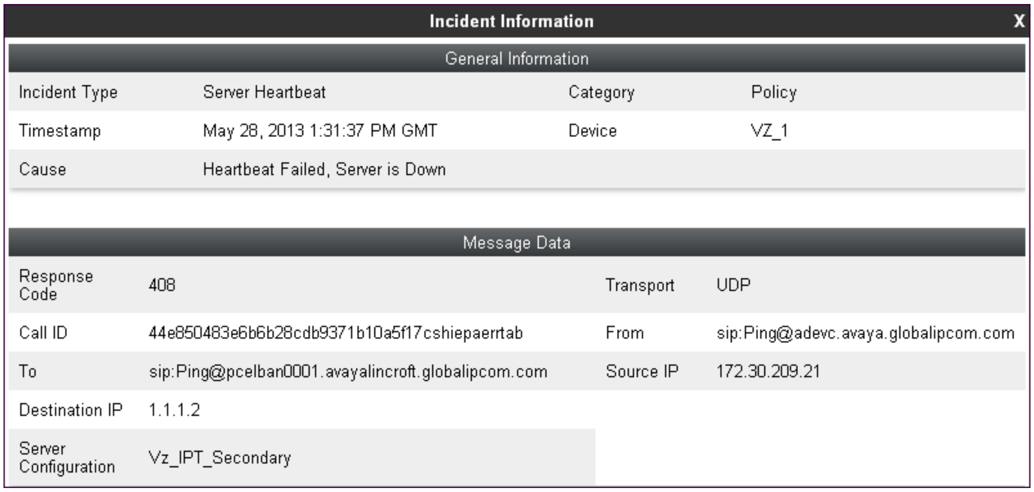

Incident Viewer

Device: All Category: All

Displaying results 61 to 75 out of 2000.

Type	ID	Date	Time	Category	Device	Cause
Message Dropped	684874147805223	5/28/13	1:38 PM	Policy	VZ_1	No Server Flow Matched for Incoming Message
Message Dropped	684874147803744	5/28/13	1:38 PM	Policy	VZ_1	No Server Flow Matched for Incoming Message
Message Dropped	684874147557151	5/28/13	1:38 PM	Policy	VZ_1	No Server Flow Matched for Incoming Message
Message Dropped	684874147554881	5/28/13	1:38 PM	Policy	VZ_1	No Server Flow Matched for Incoming Message
Server Heartbeat	684874143447079	5/28/13	1:38 PM	Policy	VZ_1	Heartbeat Failed, Server is Down
Server Heartbeat	684874140446076	5/28/13	1:38 PM	Policy	VZ_1	Heartbeat Failed, Server is Down
Server Heartbeat	684873948921126	5/28/13	1:31 PM	Policy	VZ_1	Heartbeat Failed, Server is Down
Server Heartbeat	684873942136097	5/28/13	1:31 PM	Policy	VZ_1	Heartbeat Failed, Server is Down
Message Dropped	684873910362024	5/28/13	1:30 PM	Policy	VZ_1	Method Prohibited Out-of-Dialog
Message Dropped	684873880366952	5/28/13	1:29 PM	Policy	VZ_1	Method Prohibited Out-of-Dialog
Message Dropped	684873850371848	5/28/13	1:28 PM	Policy	VZ_1	Method Prohibited Out-of-Dialog
Message Dropped	684873820376800	5/28/13	1:27 PM	Policy	VZ_1	Method Prohibited Out-of-Dialog
Message Dropped	684873790381735	5/28/13	1:26 PM	Policy	VZ_1	Method Prohibited Out-of-Dialog
Message Dropped	684873760386666	5/28/13	1:25 PM	Policy	VZ_1	Method Prohibited Out-of-Dialog
Message Dropped	684873730391513	5/28/13	1:24 PM	Policy	VZ_1	Method Prohibited Out-of-Dialog

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



General Information

Incident Type	Server Heartbeat	Category	Policy
Timestamp	May 28, 2013 1:31:37 PM GMT	Device	VZ_1
Cause	Heartbeat Failed, Server is Down		

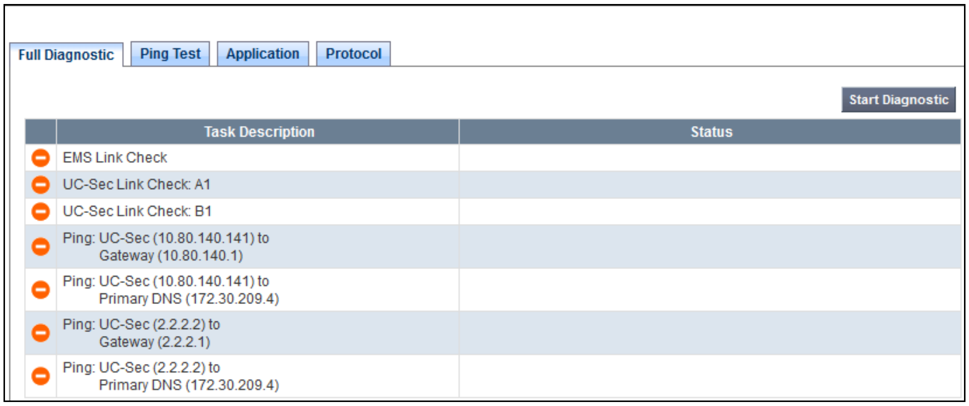
Message Data

Response Code	408	Transport	UDP
Call ID	44e850483e6b6b28cdb9371b10a5f17cshiepaerrtab	From	sip:Ping@adevc.avaya.globalipcom.com
To	sip:Ping@pcelban0001.avayalincroft.globalipcom.com	Source IP	172.30.209.21
Destination IP	1.1.1.2		
Server Configuration	Vz_IPT_Secondary		

9.3.4 Diagnostics

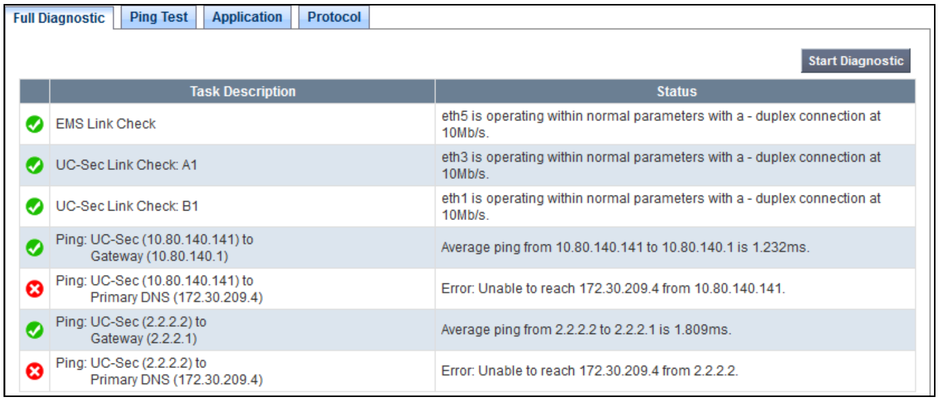
The full diagnostics check that can be run can run line checks in both directions.

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



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

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

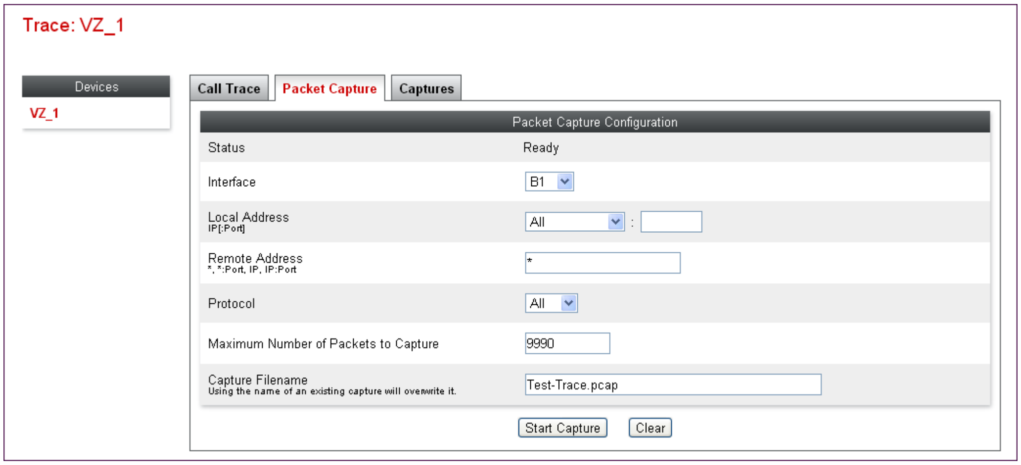


	Task Description	Status
✓	EMS Link Check	eth5 is operating within normal parameters with a - duplex connection at 10Mb/s.
✓	UC-Sec Link Check: A1	eth3 is operating within normal parameters with a - duplex connection at 10Mb/s.
✓	UC-Sec Link Check: B1	eth1 is operating within normal parameters with a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

9.3.5 Tracing

To take a call trace, Select **Device Specific Settings → Troubleshooting → Tracing** from the left-side menu (not shown).

Select the Packet Capture tab and set the desired configuration for a call trace and click **Start Capture**.



Trace: VZ_1

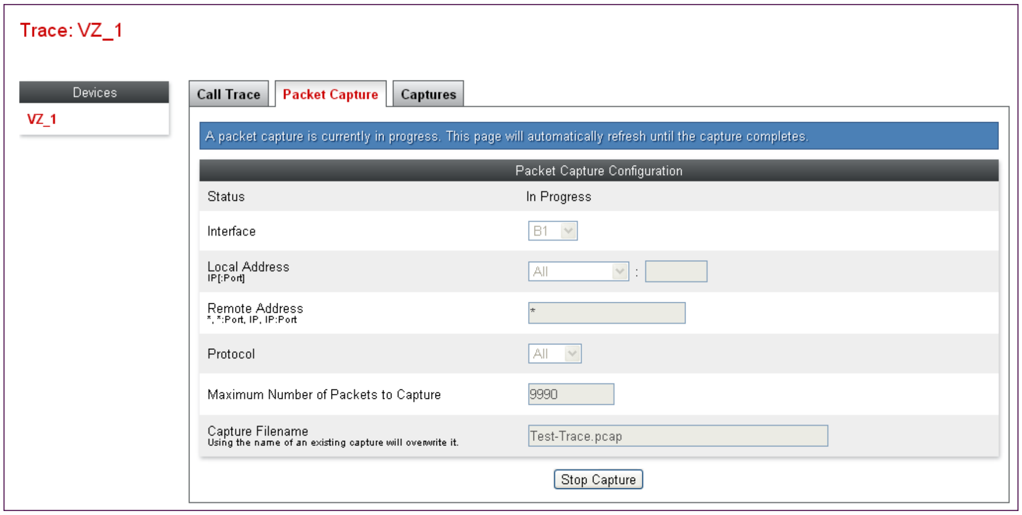
Devices: VZ_1

Call Trace | Packet Capture | Captures

Packet Capture Configuration

Status	Ready
Interface	B1
Local Address IP[:Port]	All :
Remote Address *, *:Port, IP, IP:Port	*
Protocol	All
Maximum Number of Packets to Capture	9990
Capture Filename Using the name of an existing capture will overwrite it.	Test-Trace.pcap

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



Trace: VZ_1

Devices: VZ_1

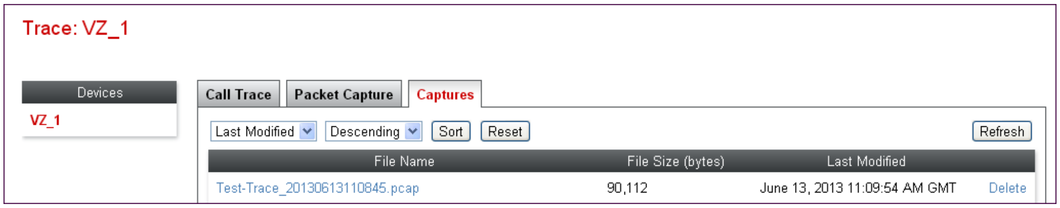
Call Trace | Packet Capture | Captures

A packet capture is currently in progress. This page will automatically refresh until the capture completes.

Packet Capture Configuration

Status	In Progress
Interface	B1
Local Address IP[:Port]	All :
Remote Address *, *:Port, IP, IP:Port	*
Protocol	All
Maximum Number of Packets to Capture	9990
Capture Filename Using the name of an existing capture will overwrite it.	Test-Trace.pcap

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



Trace: VZ_1

Devices: VZ_1

Call Trace | Packet Capture | Captures

File Name	File Size (bytes)	Last Modified	
Test-Trace_20130613110845.pcap	90,112	June 13, 2013 11:09:54 AM GMT	Delete

10. Conclusion

As illustrated in these Application Notes, Avaya Aura® Communication Manager 6.3, Avaya Aura® Session Manager 6.3, and Avaya Session Border Controller for Enterprise can be configured to interoperate successfully with Verizon Business IP Contact Center Services suite. 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's Business IP Contact Center services 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] *Implementing Avaya Aura® Communication Manager*, Doc ID 03-603558, Release 6.3
[2] *Administering Avaya Aura® Communication Manager*, Doc ID 03-300509, Release 6.3
[3] *Implementing Avaya Aura® Session Manager*, Release 6.3
[4] *Installing Service Packs for Avaya Aura® Session Manager*, Release 6.3
[5] *Upgrading Avaya Aura® Session Manager*, Release 6.3
[6] *Maintaining and Troubleshooting Avaya Aura® Session Manager*, Release 6.3
[7] *Implementing Avaya Aura® System Manager*, Release 6.3
[8] *Installing Avaya Session Border Controller for Enterprise*, Release 6.2
[9] *Administering Avaya Session Border Controller for Enterprise*, Release 6.2

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

The following Application Notes cover Session Manager 6.2 with Verizon Business IP Toll Free VoIP Inbound Service.
[VZ-IPTF] – Application Notes for Avaya Aura® Communication Manager 6.2, Avaya Aura® Session Manager 6.2, and Avaya Session Border Controller for Enterprise with Verizon Business IP Toll Free VoIP Inbound – Issue 1.1

The following Application Notes cover Session Manager 6.2 with Verizon Business IP Contact Center IP-IVR Service.
[VZ-IP-IVR] – Application Notes for Avaya Aura® Communication Manager 6.2, Avaya Aura® Session Manager 6.2, and Avaya Session Border Controller for Enterprise with Verizon Business IP Contact Center IP-IVR – Issue 1.1

11.2. Verizon Business

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

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

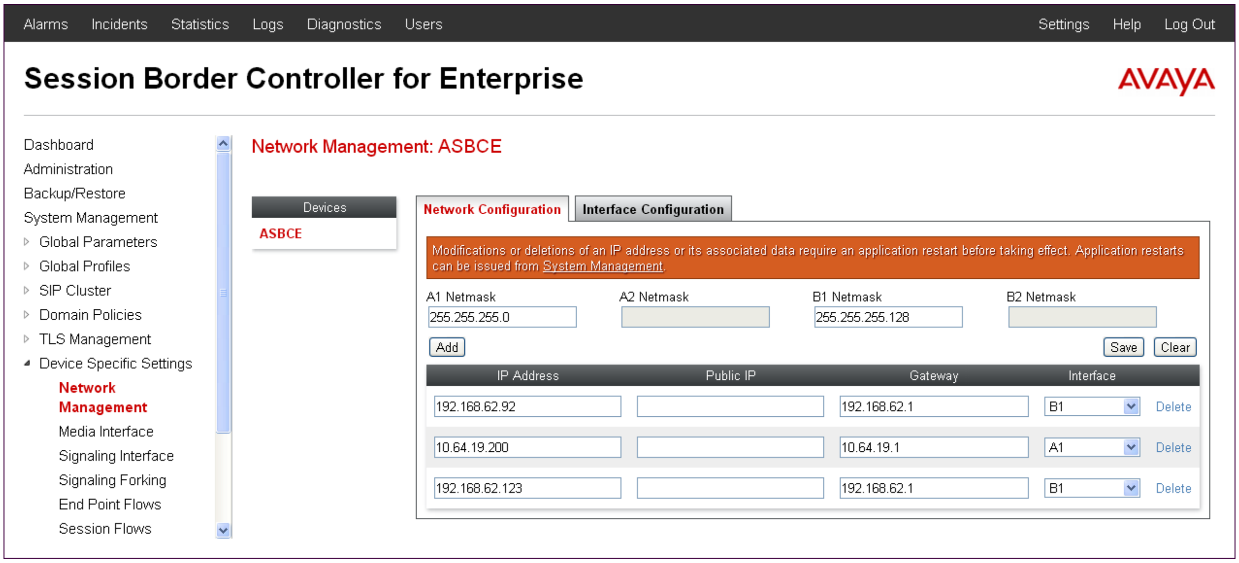
Appendix A

This section covers the configuration settings of Avaya SBCE, Session Manager, and a sample endpoint as used for Remote Workers during compliance testing. In the test environment, a dedicated Avaya SBCE with private IP addresses was used to access the Verizon Business IP Contact Center (IPCC) Services suite. To allow remote SIP endpoints access to the test environment through a public network, a separate Avaya SBCE with public IP addresses was utilized. The settings presented here simply illustrate the sample configuration used during compliance testing with Verizon IPCC, and are not intended to be prescriptive. Other routing criteria and policies may be appropriate based on different customer needs.

Standard and Advanced Session Licenses are required for Remote Worker. Contact an authorized Avaya representative for assistance if additional licensing is required.

The following screen shows the **Network Management** of the Avaya SBCE. The internal interface is assigned to **A1** and the external interfaces are assigned to **B1**. Avaya SIP endpoints registered to IP address "192.168.62.92" and retrieved firmware and configuration data from IP address "192.168.63.123". For security reasons, any actual public IP addresses used in the configuration have been replaced with private IP addresses.

Note – A SIP Entity in Session Manager was *not* configured for the Avaya SBCE's internal IP address used for Remote Worker. This keeps the interface untrusted in Session Manager, thereby allowing Session Manager to properly challenge user registration requests.



Network Management: ASBCE

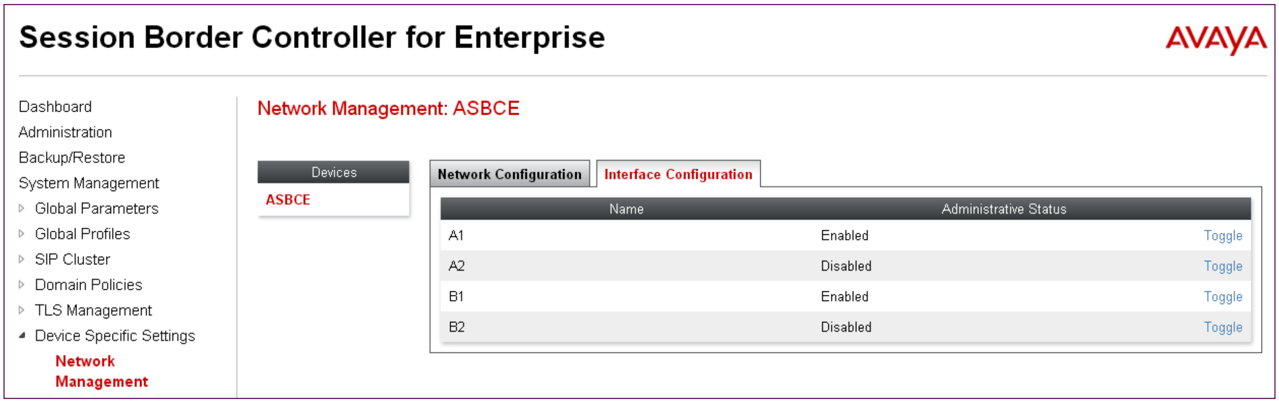
Modifications or deletions of an IP address or its associated data require an application restart before taking effect. Application restarts can be issued from System Management.

A1 Netmask	A2 Netmask	B1 Netmask	B2 Netmask
255.255.255.0		255.255.255.128	

IP Address	Public IP	Gateway	Interface	
192.168.62.92		192.168.62.1	B1	Delete
10.64.19.200		10.64.19.1	A1	Delete
192.168.62.123		192.168.62.1	B1	Delete

It is possible to deploy Remote Worker using the same Avaya SBCE as the one used for SIP trunking. However, separate IP addresses are needed for each function. This allows the Avaya SBCE to enforce proper security policies as if it were two different Avaya SBCEs. Only two network interfaces on the Avaya SBCE may be active at one time, so this requires all external IP addresses to be on the same subnet so they may be applied to the same network interface. Similarly, additional internal IP addresses must be on the same internal subnet.

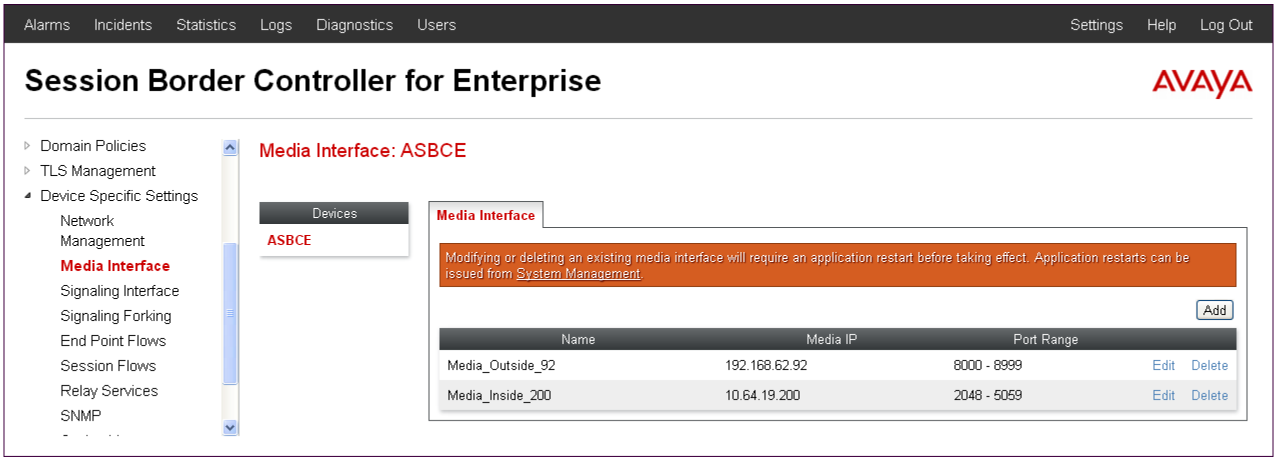
Interfaces **A1** and **B1** were both set to **Enabled**.



Network Management: ASBCE

Name	Administrative Status	
A1	Enabled	Toggle
A2	Disabled	Toggle
B1	Enabled	Toggle
B2	Disabled	Toggle

The following screen shows the **Media Interface** settings. Media interfaces were created for the inside and outside IP interfaces used for Remote Worker SIP traffic.

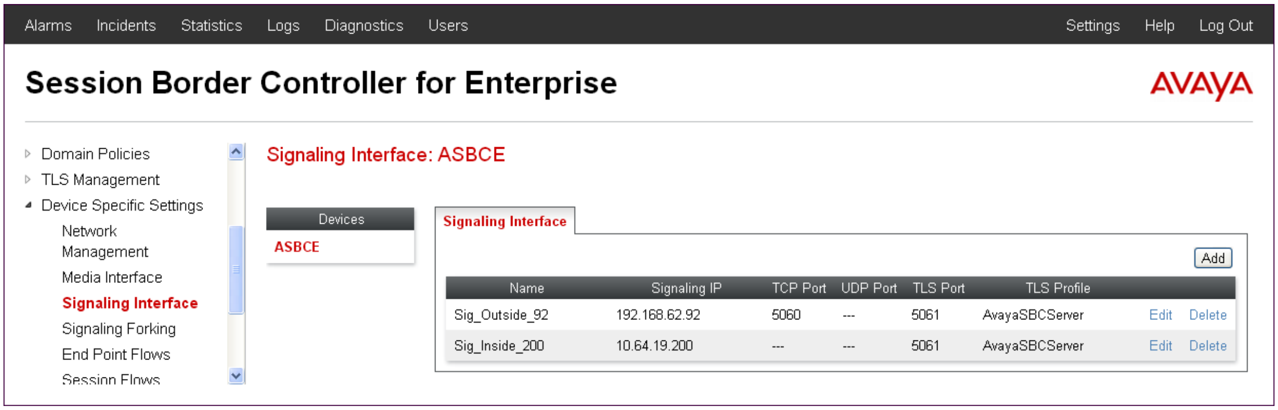


Media Interface: ASBCE

Modifying or deleting an existing media interface will require an application restart before taking effect. Application restarts can be issued from System Management.

Name	Media IP	Port Range	
Media_Outside_92	192.168.62.92	8000 - 8999	Edit Delete
Media_Inside_200	10.64.19.200	2048 - 5059	Edit Delete

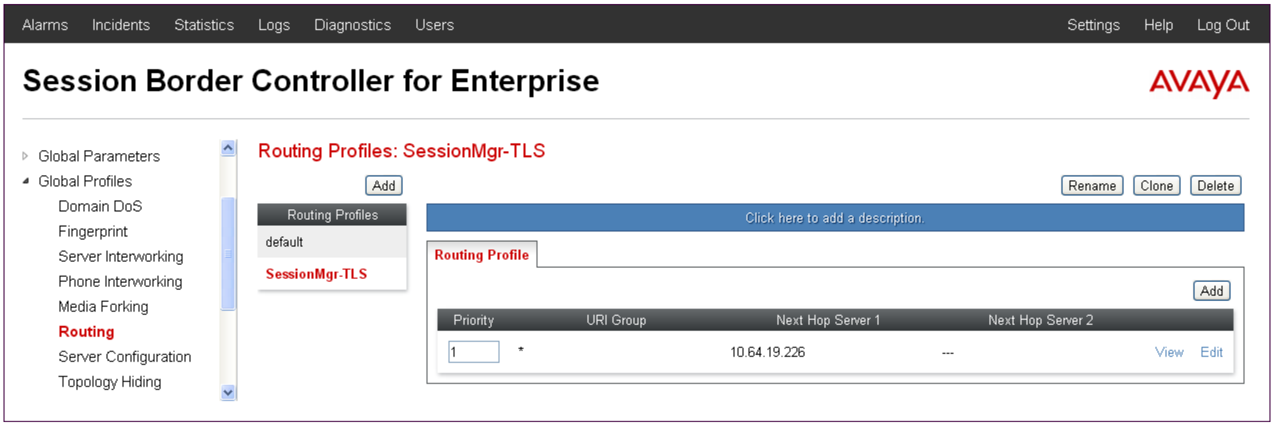
The following screen shows the **Signaling Interface** settings. Signaling interfaces were also created for the inside and outside IP interfaces used for Remote Worker SIP traffic. The interface named “Sig_Outside_92” supports TCP and TLS, while the interface named “Sig_Inside_200” supports TLS only.



Signaling Interface: ASBCE

Name	Signaling IP	TCP Port	UDP Port	TLS Port	TLS Profile	
Sig_Outside_92	192.168.62.92	5060	---	5061	AvayaSBCServer	Edit Delete
Sig_Inside_200	10.64.19.200	---	---	5061	AvayaSBCServer	Edit Delete

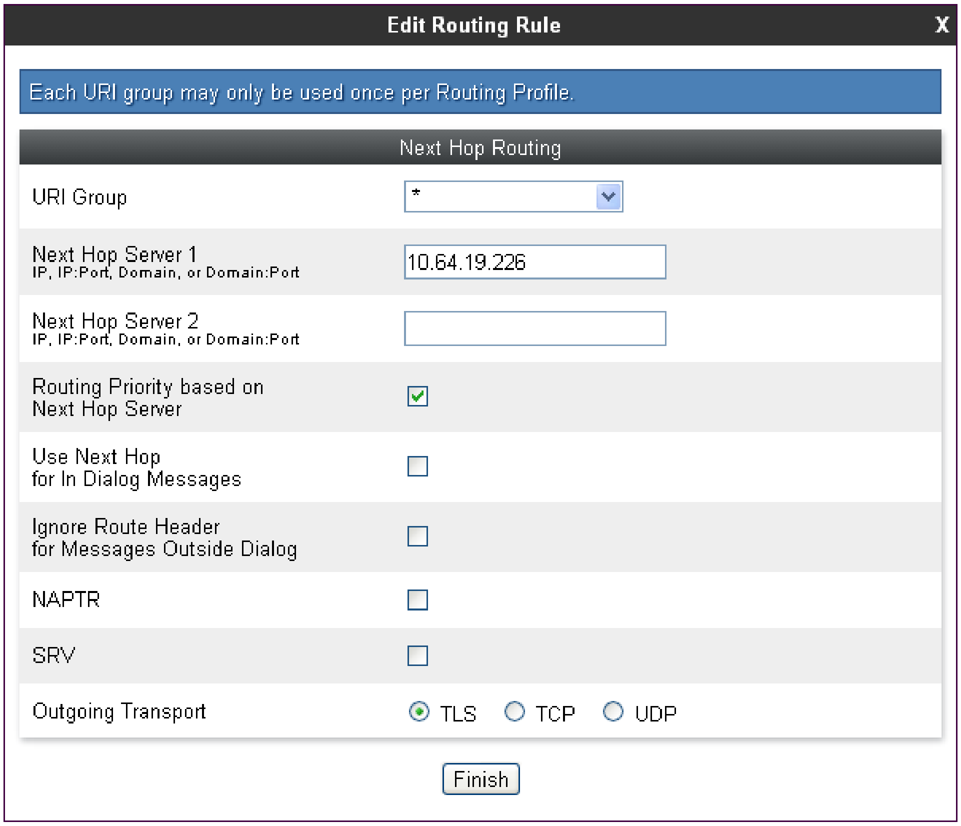
Routing Profile “SessionMgr-TLS” was created for Session Manager as shown in the following screens.



Routing Profiles: SessionMgr-TLS

Routing Profiles
default
SessionMgr-TLS

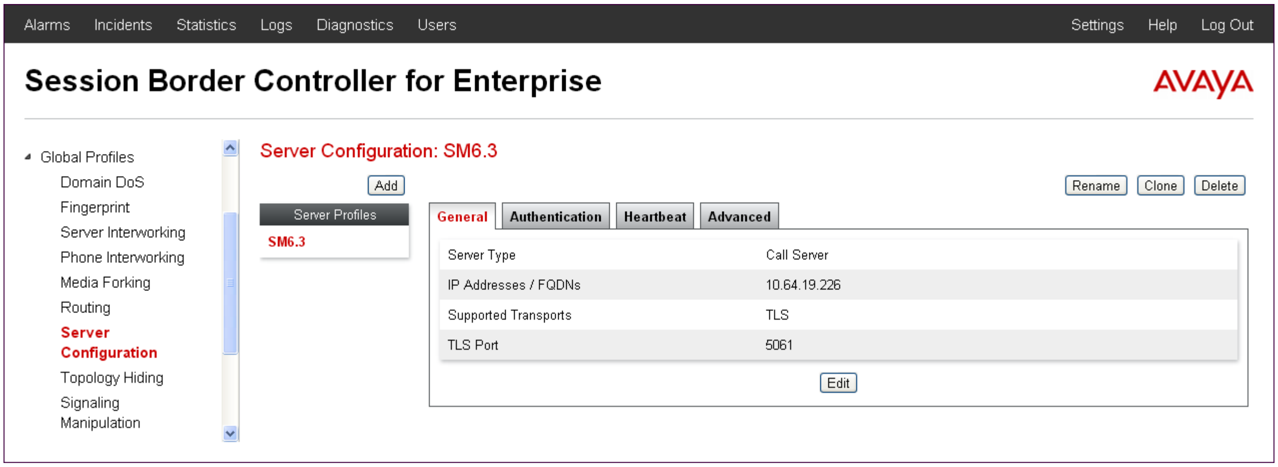
Priority	URI Group	Next Hop Server 1	Next Hop Server 2		
1	*	10.64.19.226	---	View	Edit



Each URI group may only be used once per Routing Profile.

Next Hop Routing	
URI Group	*
Next Hop Server 1 IP, IP:Port, Domain, or Domain:Port	10.64.19.226
Next Hop Server 2 IP, IP:Port, Domain, or Domain:Port	
Routing Priority based on Next Hop Server	☑
Use Next Hop for In Dialog Messages	□
Ignore Route Header for Messages Outside Dialog	□
NAPTR	□
SRV	□
Outgoing Transport	● TLS ○ TCP ○ UDP

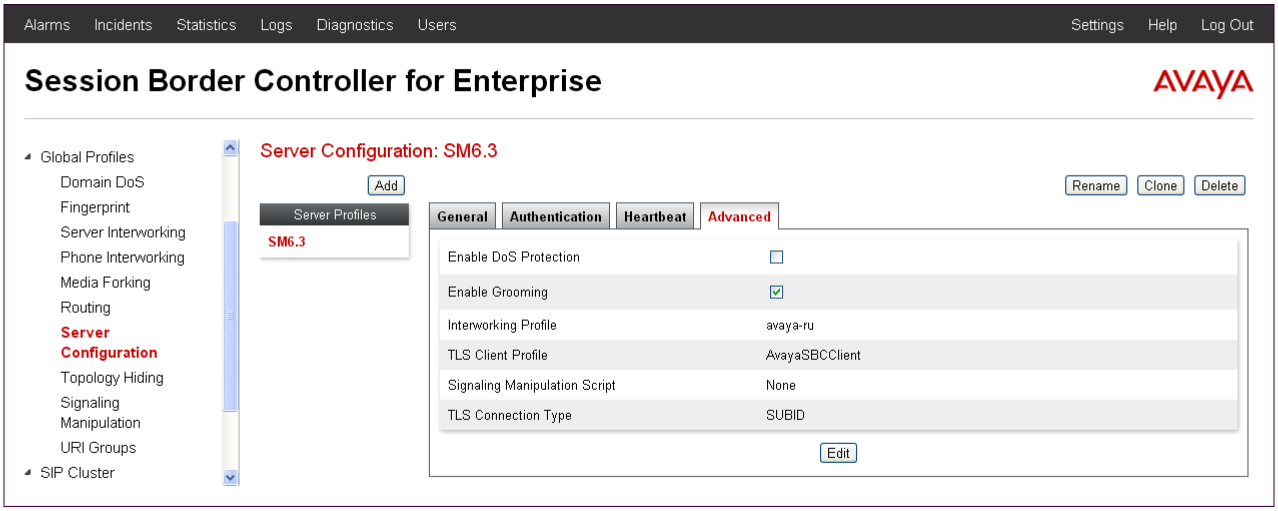
The following screens illustrate the **Server Configuration** for the Profile named “SM6.3” created for Session Manager. The **Authentication** and **Heartbeat** tabs were kept at the default disabled setting.



Server Configuration: SM6.3

Server Type	Call Server
IP Addresses / FQDNs	10.64.19.226
Supported Transports	TLS
TLS Port	5061

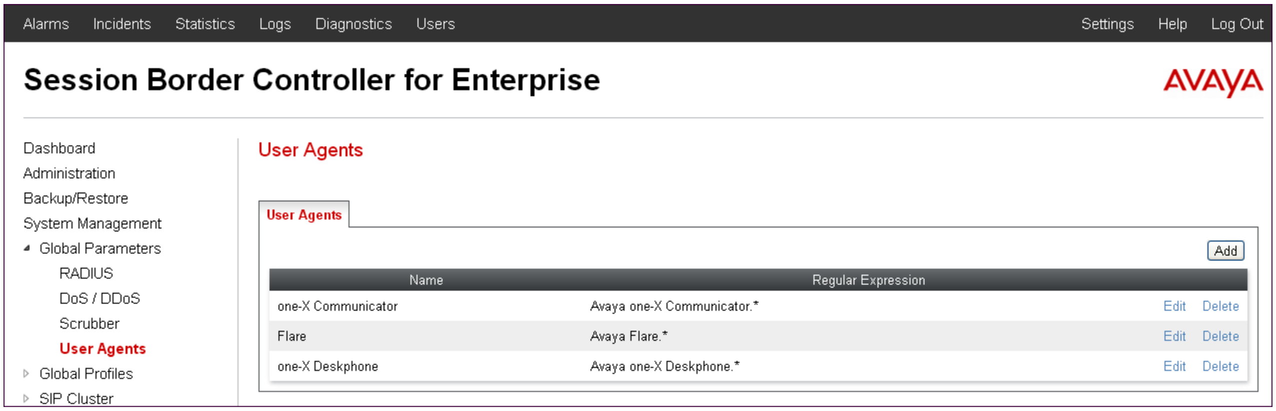
On the **Advanced** tab, default profiles were specified that applies to traffic between the Avaya SBCE and Session Manager as shown below.



Server Configuration: SM6.3

Enable DoS Protection	□
Enable Grooming	☑
Interworking Profile	avaya-ru
TLS Client Profile	AvayaSBCClient
Signaling Manipulation Script	None
TLS Connection Type	SUBID

User Agents were created for each type of endpoint tested. This allows for different policies to be applied based on the type of device. For example, Avaya one-X Deskphones will use TLS and SRTP, while one-X® Communicator and Avaya Flare® will use TCP and RTP.

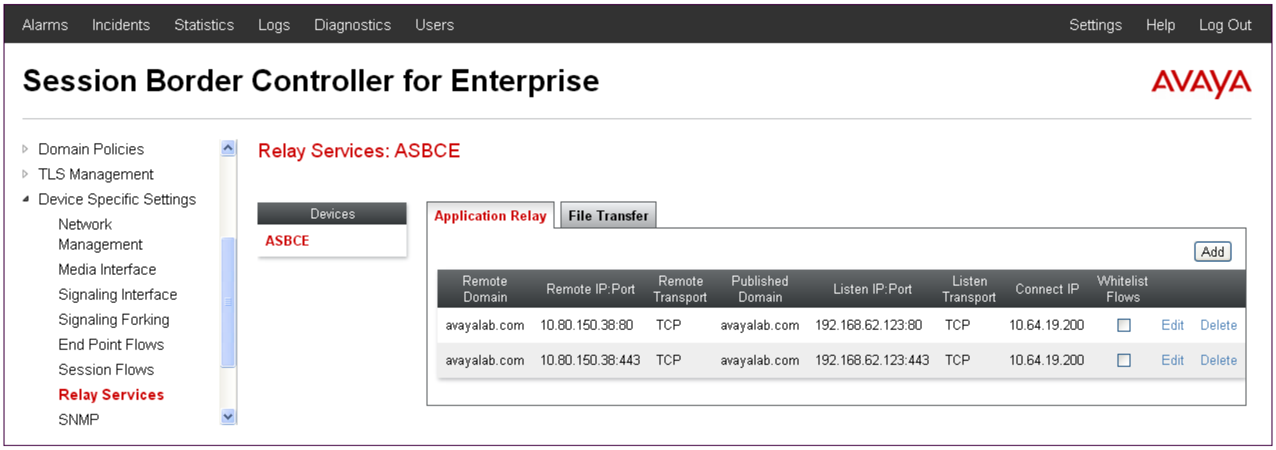


Name	Regular Expression		
one-X Communicator	Avaya one-X Communicator.*	Edit	Delete
Flare	Avaya Flare.*	Edit	Delete
one-X Deskphone	Avaya one-X Deskphone.*	Edit	Delete

The following abridged output of Session Manager's traceSM command shows the details of an Invite from an Avaya one-X Deskphone. The **User-Agent** shown in this trace will match "one-X Deskphone" shown above with a **Regular Expression** of "Avaya one-X Deskphone.*". In this expression, ".*" will match any software version listed after the user agent name.

```
INVITE sip:12002@avayalab.com SIP/2.0
From: <sip:14006@avayalab.com>;tag=-76557dff51bb3900-5c89896d_F1400610.80.150.111
To: <sip:12002@avayalab.com>
CSeq: 357 INVITE
Call-ID: 161_51bb3900-2ff0c2ff-5c898dda_I@10.80.150.111
Contact: <sip:14006@10.64.19.200:5061;transport=tls;subid_ipcs=448140782>;+avaya-cm-line=1
Record-Route: <sip:10.64.19.200:5061;ipcs-line=930;lr;transport=tls>
Record-Route: <sips:205.168.62.92:5061;ipcs-line=930;lr;transport=tls>
Allow:
INVITE,ACK,BYE,CANCEL,SUBSCRIBE,NOTIFY,MESSAGE,REFER,INFO,PRACK,PUBLISH,UPDATE
Supported: 100rel,eventlist,feature-ref,replaces
User-Agent: Avaya one-X Deskphone 6.2.2.17 (40235)
Max-Forwards: 69
Via: SIP/2.0/TLS 10.64.19.200:5061;branch=z9hG4bK-s1632-001744755540-1--s1632-
Via: SIP/2.0/TLS 10.80.150.111:5061;branch=z9hG4bK165_51bb39027017c28d-5c899bb5_I14006
Accept-Language: en
Content-Type: application/sdp
Content-Length: 416
```

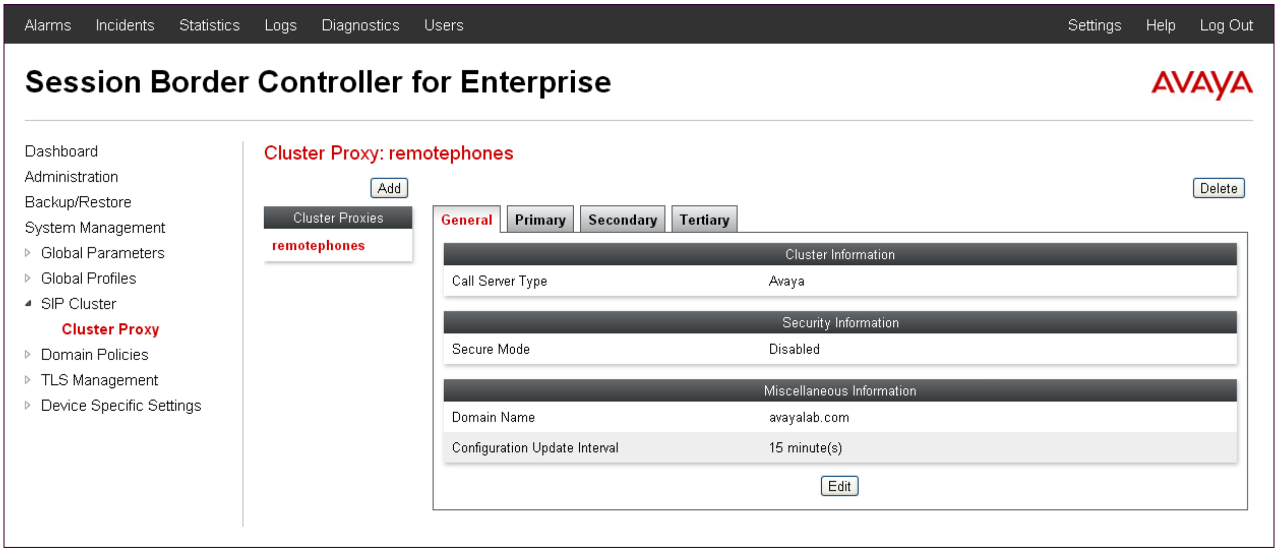
Relay Services are used to define how firmware updates and configuration data are routed for remote endpoints. The following screen shows the **Application Relay** tab with the two application relays created for the sample configuration. This allows for both HTTP and HTTPS traffic to be routed to the appropriate internal file server. The **Remote IP:Port** was set to the IP address and port of the internal file server used to provide the firmware updates and configuration data for the remote endpoints. The **Listen IP:Port** was set to the IP address and port of the Avaya SBCE's external IP address designated for file transfers. The **Connected IP** was set to the internal IP address of the Avaya SBCE.



Relay Services: ASBCE

Remote Domain	Remote IP:Port	Remote Transport	Published Domain	Listen IP:Port	Listen Transport	Connect IP	Whitelist Flows		
avayalab.com	10.80.150.38:80	TCP	avayalab.com	192.168.62.123:80	TCP	10.64.19.200	□	Edit	Delete
avayalab.com	10.80.150.38:443	TCP	avayalab.com	192.168.62.123:443	TCP	10.64.19.200	□	Edit	Delete

A **Cluster Proxy** is used for Personal Profile Manager (PPM) data and Presence services. The following screen shows the cluster proxy "remotephones" created in the sample configuration. A Presence Services server was not part of the sample configuration. Therefore, configuration of the cluster proxy for use with Presence is not shown and only configuration related to PPM data is present.



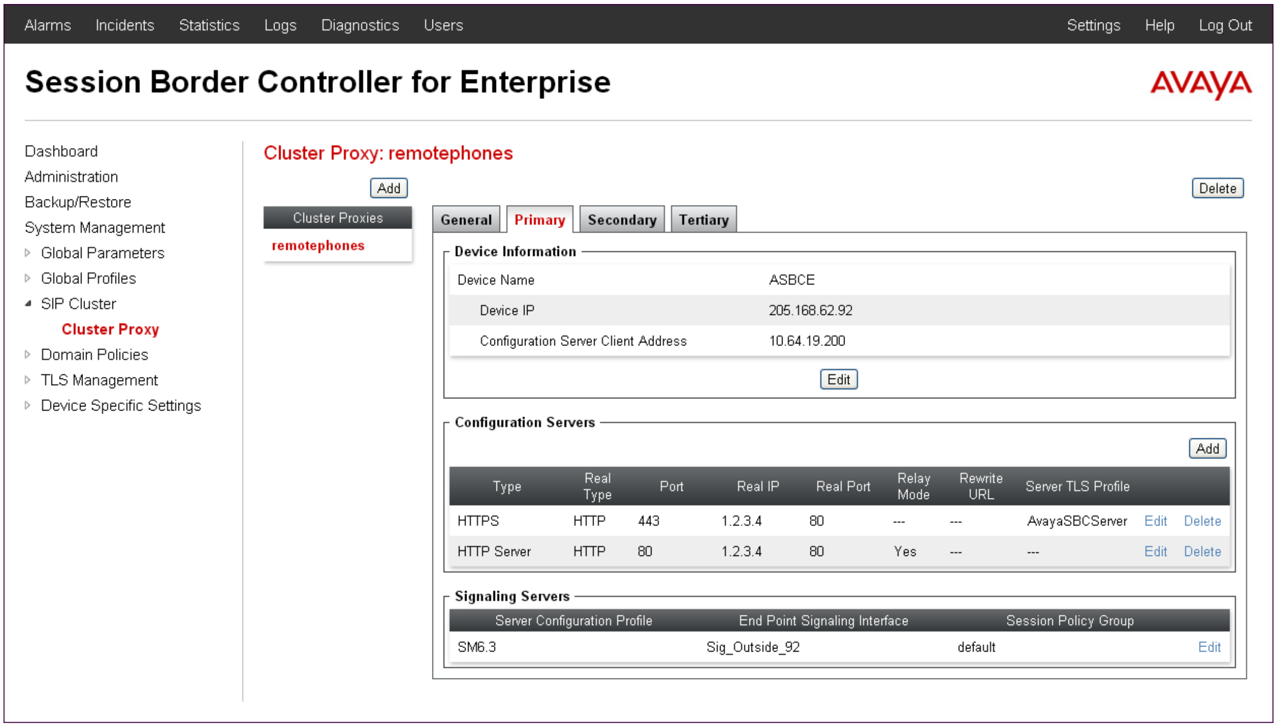
Cluster Proxy: remotephones

Cluster Information	
Call Server Type	Avaya

Security Information	
Secure Mode	Disabled

Miscellaneous Information	
Domain Name	avayalab.com
Configuration Update Interval	15 minute(s)

On the **Primary** tab, PPM traffic received on **Device IP** “192.168.62.92” will be routed to the **Configuration Server Client Address** “10.64.19.200”. The **Real IP** field is not used for PPM, so any IP address can be entered, e.g., “1.2.3.4”. This enables the remote Avaya SIP endpoints to send and receive PPM information to and from Session Manager via the Avaya SBCE.



Cluster Proxy: remotephones

Device Information

Device Name	ASBCE
Device IP	205.168.62.92
Configuration Server Client Address	10.64.19.200

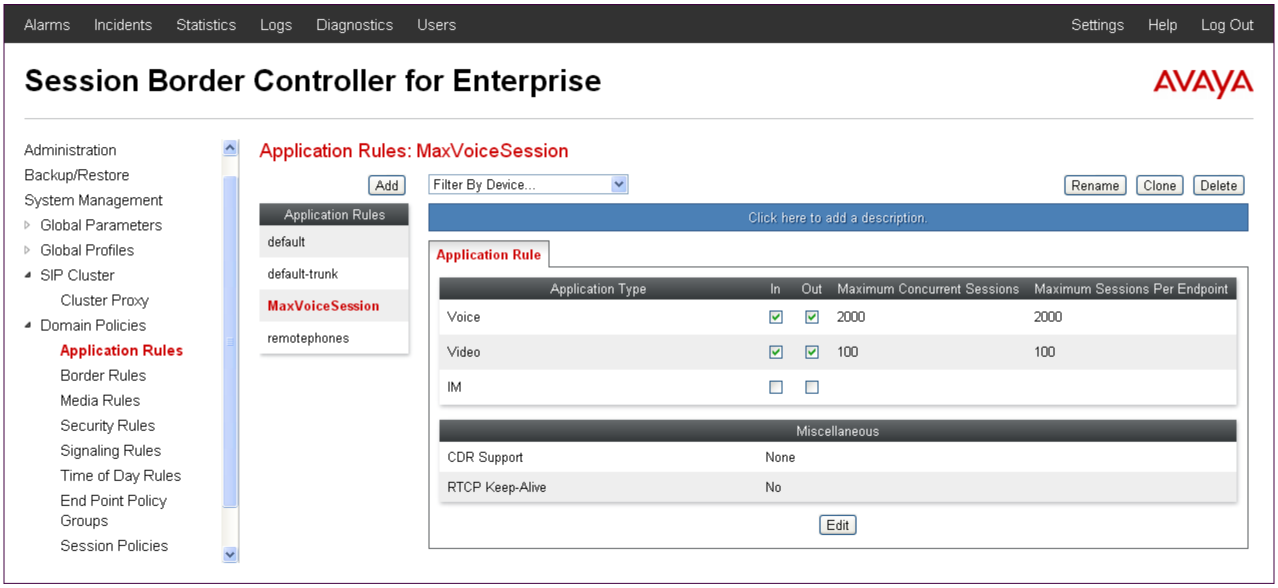
Configuration Servers

Type	Real Type	Port	Real IP	Real Port	Relay Mode	Rewrite URL	Server TLS Profile		
HTTPS	HTTP	443	1.2.3.4	80	---	---	AvayaSBCServer	Edit	Delete
HTTP Server	HTTP	80	1.2.3.4	80	Yes	---	---	Edit	Delete

Signaling Servers

Server Configuration Profile	End Point Signaling Interface	Session Policy Group	
SM6.3	Sig_Outside_92	default	Edit

The following screens show the **Application Rules** "MaxVoiceSession" and "remotephones" used in the sample configuration. In an actual customer installation, set the **Maximum Concurrent Sessions** for the **Voice** application to a value slightly larger than the licensed sessions. For example, if licensed for 300 session set the values to "500". For the "MaxVoiceSession" rule, the **Maximum Session Per Endpoint** matches the **Maximum Concurrent Sessions**. For the application rule applied to the Remote Workers subscriber flows, a value of "10" is recommended for the **Maximum Session Per Endpoint**.



Session Border Controller for Enterprise

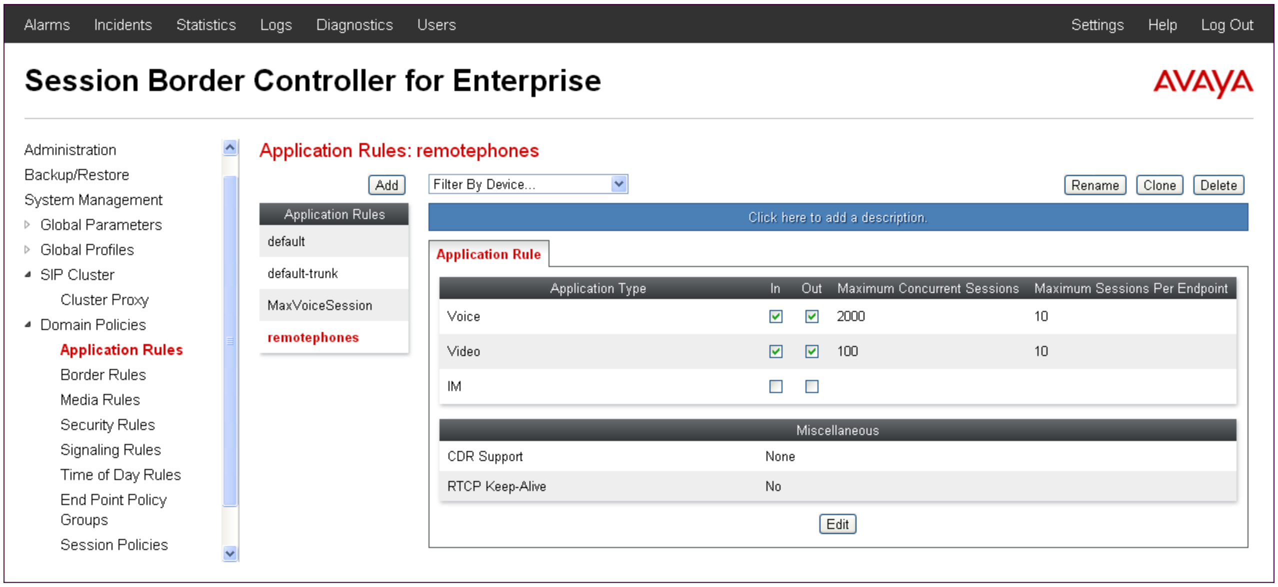
Application Rules: MaxVoiceSession

Application Rules
default
default-trunk
MaxVoiceSession
remotephones

Application Rule

Application Type	In	Out	Maximum Concurrent Sessions	Maximum Sessions Per Endpoint
Voice	☑	☑	2000	2000
Video	☑	☑	100	100
IM	□	□		

Miscellaneous	
CDR Support	None
RTCP Keep-Alive	No



Session Border Controller for Enterprise

Application Rules: remotephones

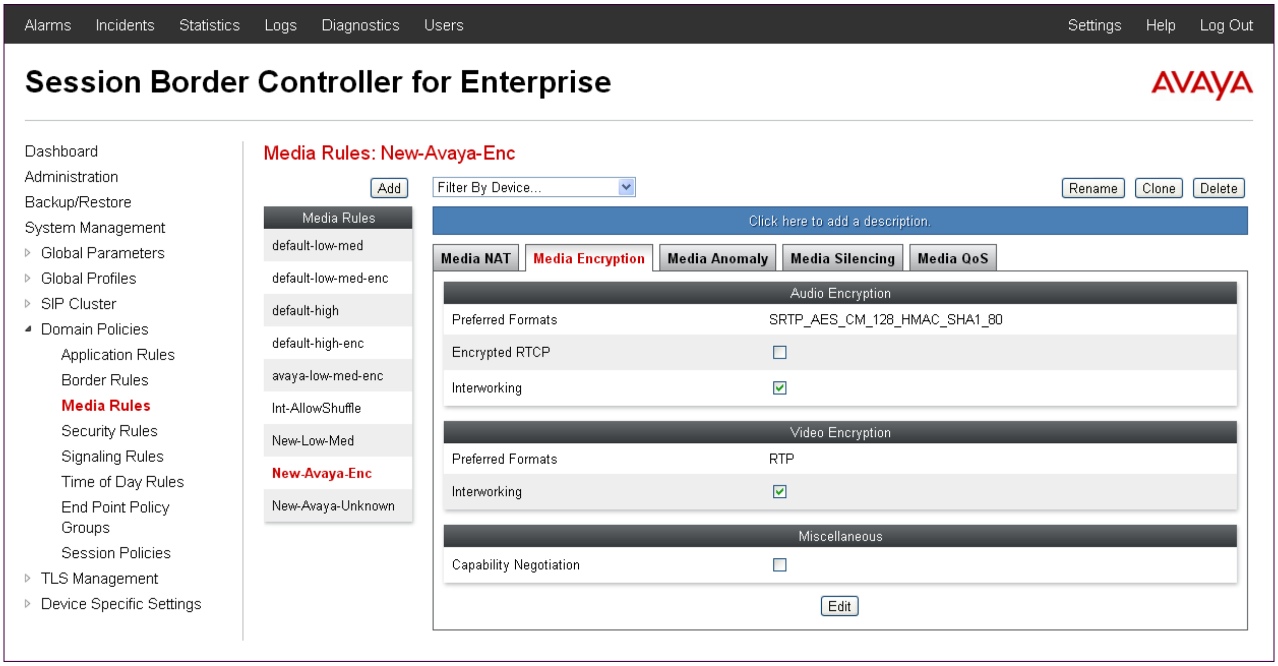
Application Rules
default
default-trunk
MaxVoiceSession
remotephones

Application Rule

Application Type	In	Out	Maximum Concurrent Sessions	Maximum Sessions Per Endpoint
Voice	☑	☑	2000	10
Video	☑	☑	100	10
IM	□	□		

Miscellaneous	
CDR Support	None
RTCP Keep-Alive	No

The following screens show **Media Rules** “New-Avaya-Enc” and “default-low-med” that will later be assigned to the End Point Policy Groups. Note that both rules have **Interworking** checked. Based on how calls are routed through Avaya SBCE, this will convert SRTP media to RTP and vice versa. In the sample configuration, Avaya SBCE will convert the SRTP media stream from remote Avaya 96x1 SIP Telephones to RTP towards the enterprise and also towards remote endpoints using TCP. Avaya SBCE will also convert RTP media from calls originating from Session Manager to SRTP towards Avaya 96x1 SIP Telephones using TLS through the external IP interface. The “New-Avaya-Enc” policy was cloned from the existing “default-low-med” policy. The parameters on the other tabs not shown retained their default values.

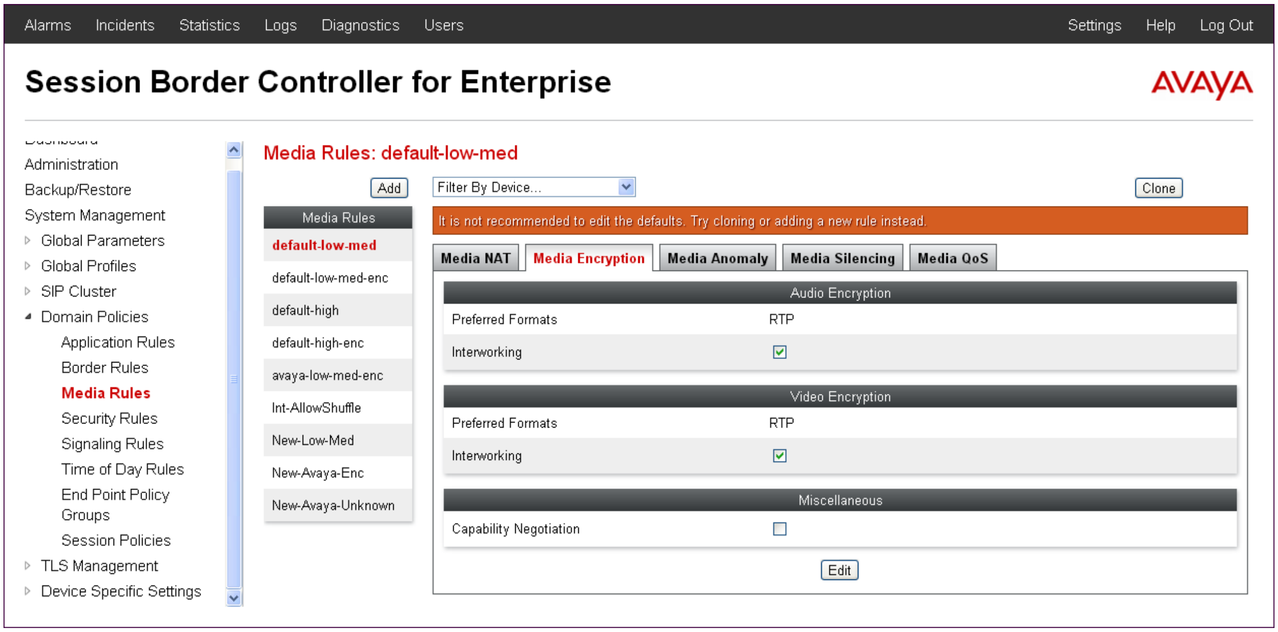


Media Rules: New-Avaya-Enc

Audio Encryption	
Preferred Formats	SRTP_AES_CM_128_HMAC_SHA1_80
Encrypted RTCP	☐
Interworking	☑

Video Encryption	
Preferred Formats	RTP
Interworking	☑

Miscellaneous	
Capability Negotiation	☐



Media Rules: default-low-med

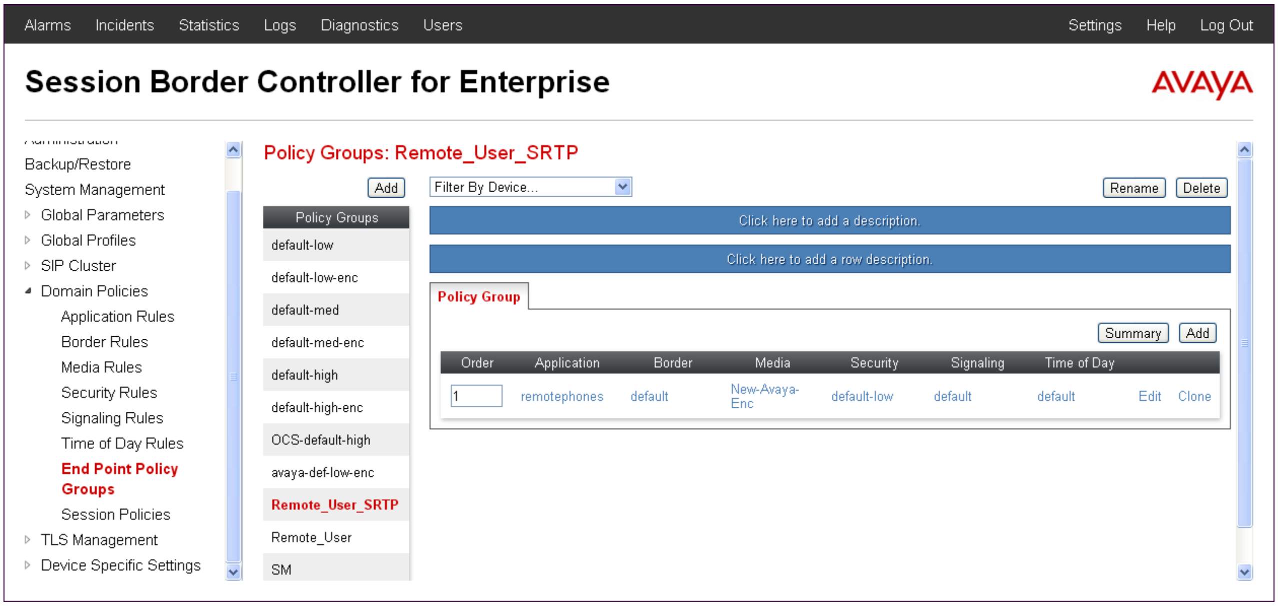
It is not recommended to edit the defaults. Try cloning or adding a new rule instead.

Audio Encryption	
Preferred Formats	RTP
Interworking	☑

Video Encryption	
Preferred Formats	RTP
Interworking	☑

Miscellaneous	
Capability Negotiation	☐

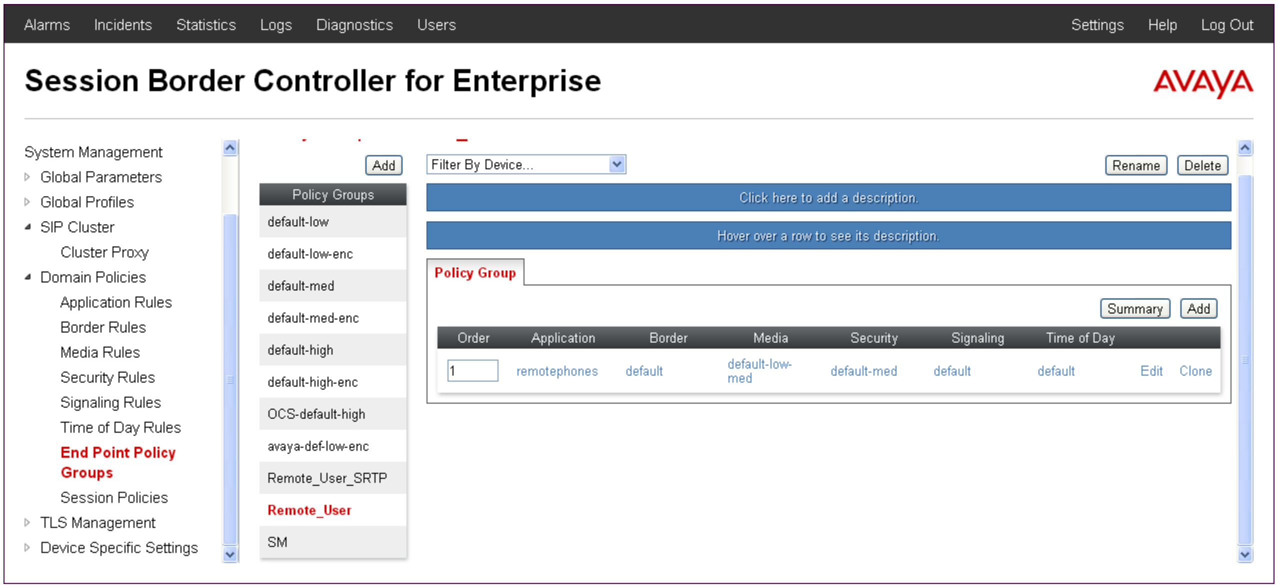
The following **End Point Policy Groups** will later be assigned to the subscriber and server flows. The “Remote_User_SRTP” policy uses the “remotephones” **Application** rule and the “New-Avaya-Enc” **Media** rule.



Policy Groups: Remote_User_SRTP

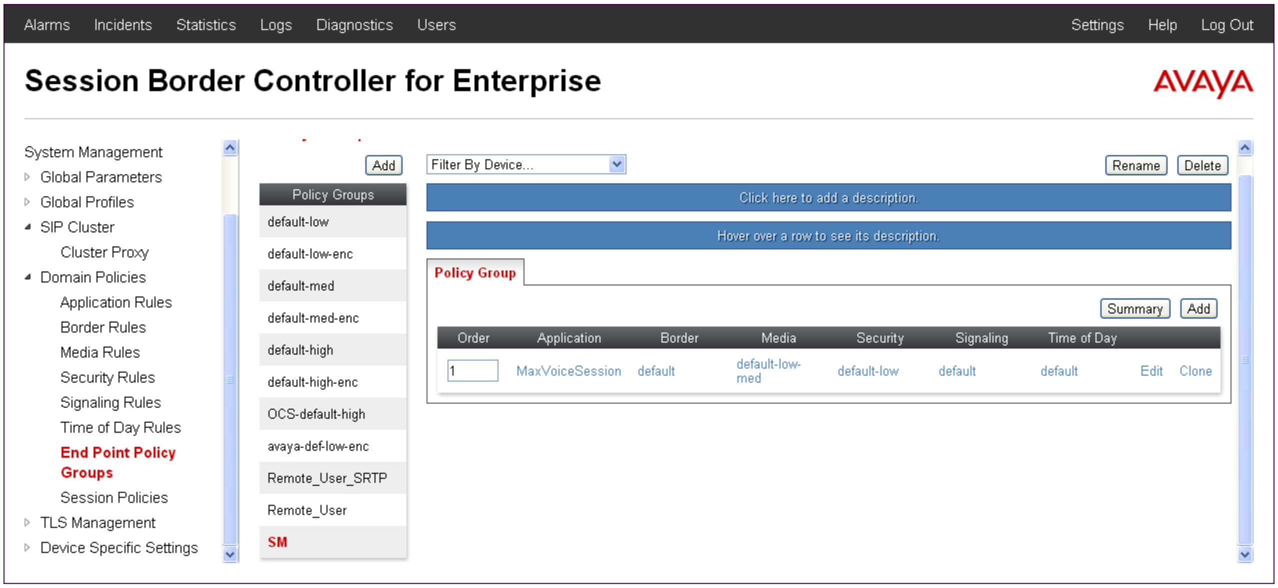
Order	Application	Border	Media	Security	Signaling	Time of Day		
1	remotephones	default	New-Avaya-Enc	default-low	default	default	Edit	Clone

The “Remote_User” policy uses the “remotephones” **Application** rule and the “default-low-med” **Media** rule.



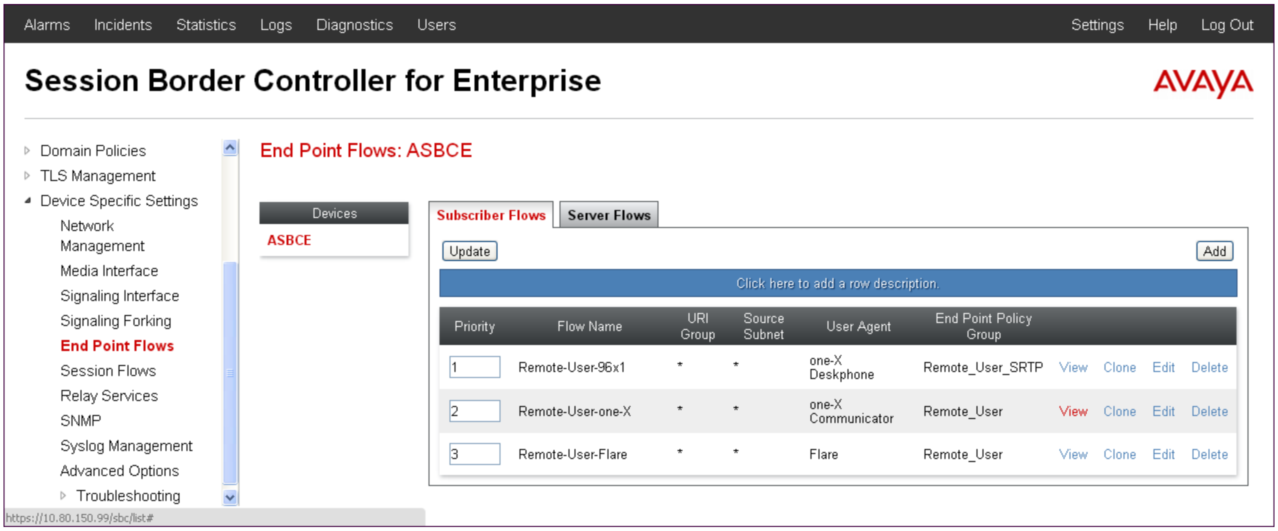
Order	Application	Border	Media	Security	Signaling	Time of Day		
1	remotephones	default	default-low-med	default-med	default	default	Edit	Clone

The “SM” policy uses the “MaxVoiceSession” **Application** rule and the “default-low-med” **Media** rule.



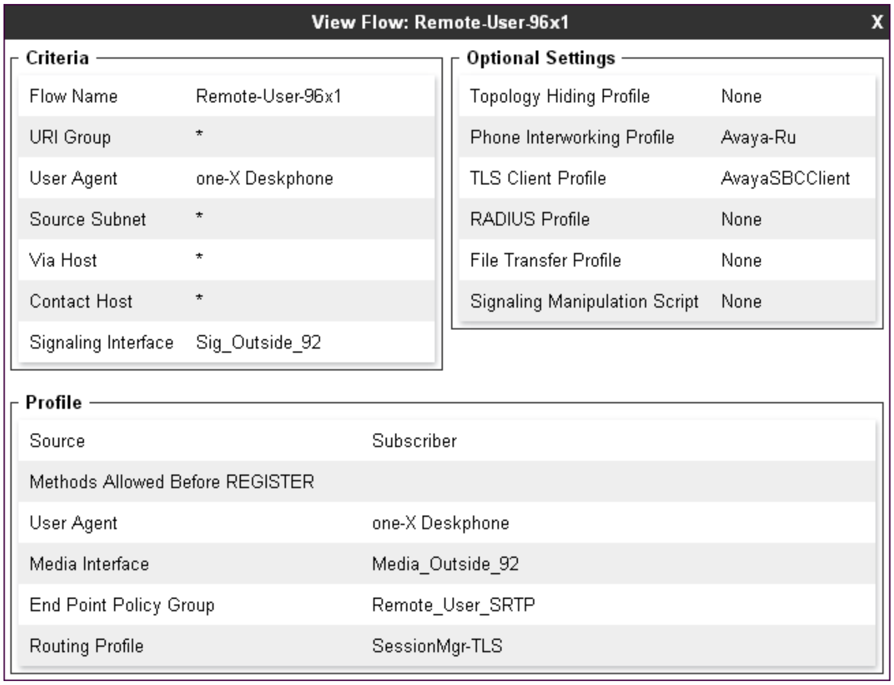
Order	Application	Border	Media	Security	Signaling	Time of Day		
1	MaxVoiceSession	default	default-low-med	default-low	default	default	Edit	Clone

Three **Subscriber Flows** were created for Remote Workers. One for each **User Agent** previously created.



Priority	Flow Name	URI Group	Source Subnet	User Agent	End Point Policy Group				
1	Remote-User-96x1	*	*	one-X Deskphone	Remote_User_SRTP	View	Clone	Edit	Delete
2	Remote-User-one-X	*	*	one-X Communicator	Remote_User	View	Clone	Edit	Delete
3	Remote-User-Flare	*	*	Flare	Remote_User	View	Clone	Edit	Delete

The following screen shows the details of the flow named “Remote-User-96x1” used in the sample configuration. This flow will match traffic from remote Avaya 96x1 Series IP Telephones set to use TLS. Note that the **User Agent** was set to “one-X Deskphone” and that the **End Point Policy Group** was set to “Remote_User_SRTP”.



View Flow: Remote-User-96x1

Criteria

Flow Name	Remote-User-96x1
URI Group	*
User Agent	one-X Deskphone
Source Subnet	*
Via Host	*
Contact Host	*
Signaling Interface	Sig_Outside_92

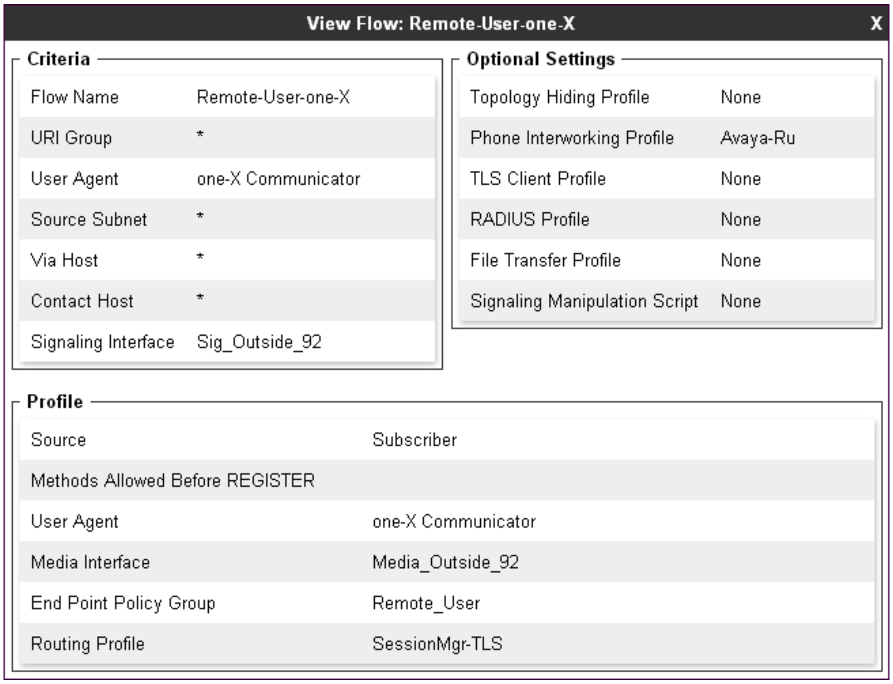
Optional Settings

Topology Hiding Profile	None
Phone Interworking Profile	Avaya-Ru
TLS Client Profile	AvayaSBCClient
RADIUS Profile	None
File Transfer Profile	None
Signaling Manipulation Script	None

Profile

Source	Subscriber
Methods Allowed Before REGISTER	
User Agent	one-X Deskphone
Media Interface	Media_Outside_92
End Point Policy Group	Remote_User_SRTP
Routing Profile	SessionMgr-TLS

The “Remote-User-one-X” flow will match traffic from remote one-X® Communicator devices set to use TCP. Note that the **User Agent** was set to “one-X Communicator” and that the **End Point Policy Group** was set to “Remote_User”.



View Flow: Remote-User-one-X

Criteria

Flow Name	Remote-User-one-X
URI Group	*
User Agent	one-X Communicator
Source Subnet	*
Via Host	*
Contact Host	*
Signaling Interface	Sig_Outside_92

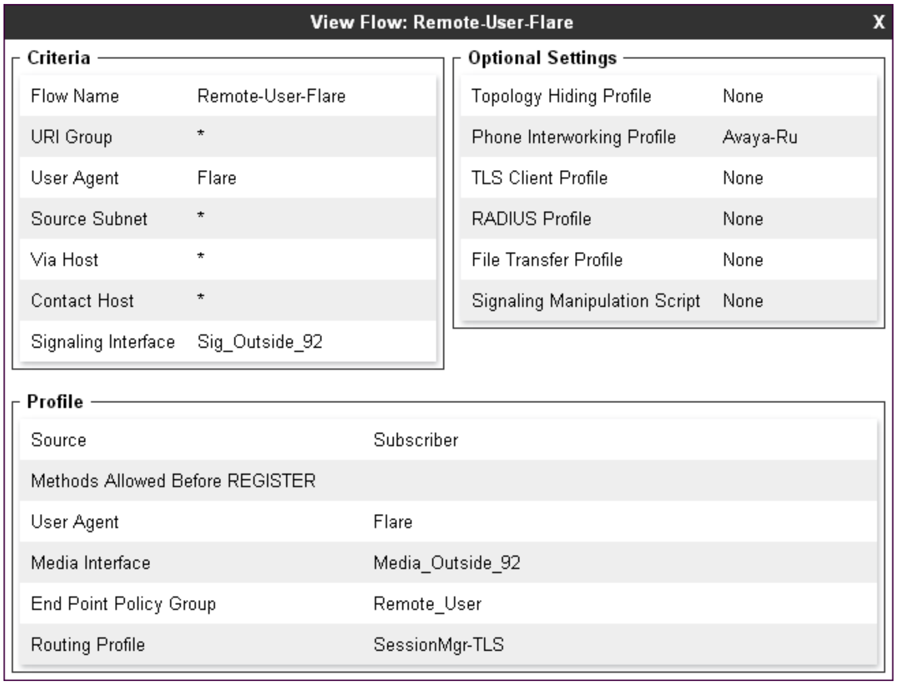
Optional Settings

Topology Hiding Profile	None
Phone Interworking Profile	Avaya-Ru
TLS Client Profile	None
RADIUS Profile	None
File Transfer Profile	None
Signaling Manipulation Script	None

Profile

Source	Subscriber
Methods Allowed Before REGISTER	
User Agent	one-X Communicator
Media Interface	Media_Outside_92
End Point Policy Group	Remote_User
Routing Profile	SessionMgr-TLS

The “Remote-User-Flare” flow will match traffic from remote Avaya Flare® devices set to use TCP. Note that the **User Agent** was set to “Flare” and that the **End Point Policy Group** was set to “Remote_User”.



View Flow: Remote-User-Flare

Criteria

Flow Name	Remote-User-Flare
URI Group	*
User Agent	Flare
Source Subnet	*
Via Host	*
Contact Host	*
Signaling Interface	Sig_Outside_92

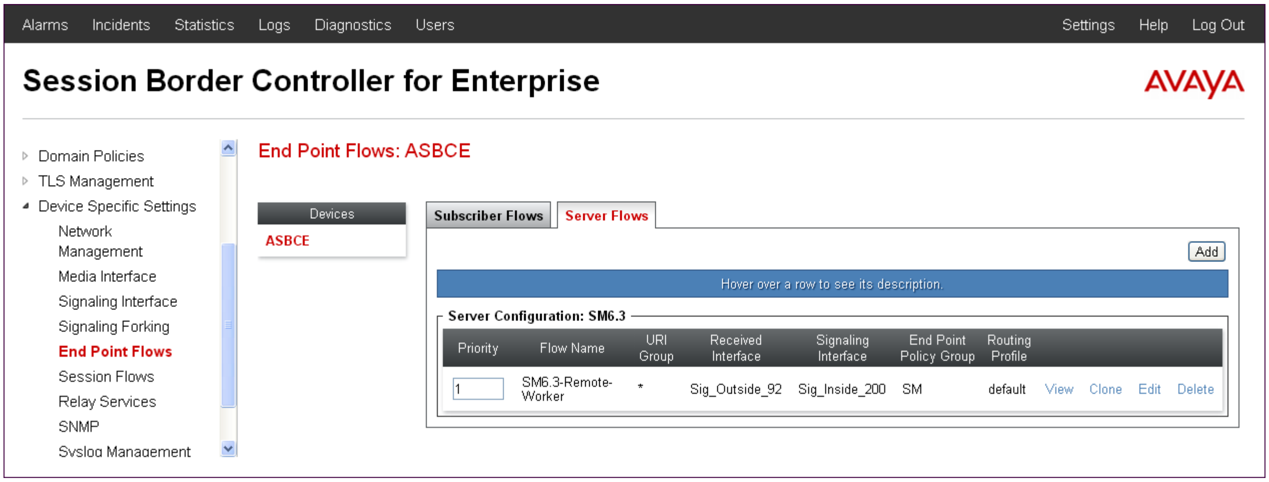
Optional Settings

Topology Hiding Profile	None
Phone Interworking Profile	Avaya-Ru
TLS Client Profile	None
RADIUS Profile	None
File Transfer Profile	None
Signaling Manipulation Script	None

Profile

Source	Subscriber
Methods Allowed Before REGISTER	
User Agent	Flare
Media Interface	Media_Outside_92
End Point Policy Group	Remote_User
Routing Profile	SessionMgr-TLS

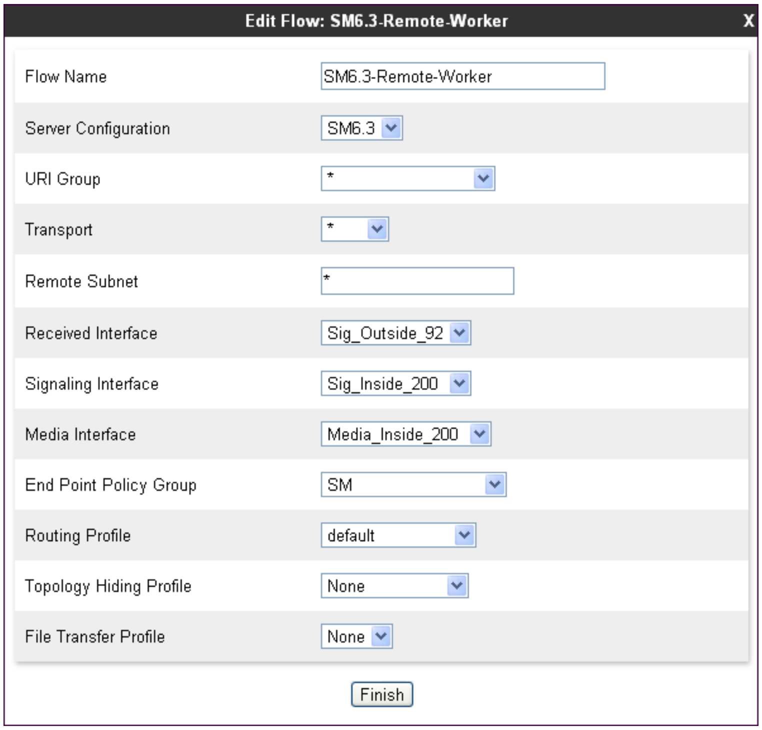
The following screens show the **Server Flows** settings for Session Manager.



End Point Flows: ASBCE

Server Configuration: SM6.3

Priority	Flow Name	URI Group	Received Interface	Signaling Interface	End Point Policy Group	Routing Profile				
1	SM6.3-Remote-Worker	*	Sig_Outside_92	Sig_Inside_200	SM	default	View	Clone	Edit	Delete

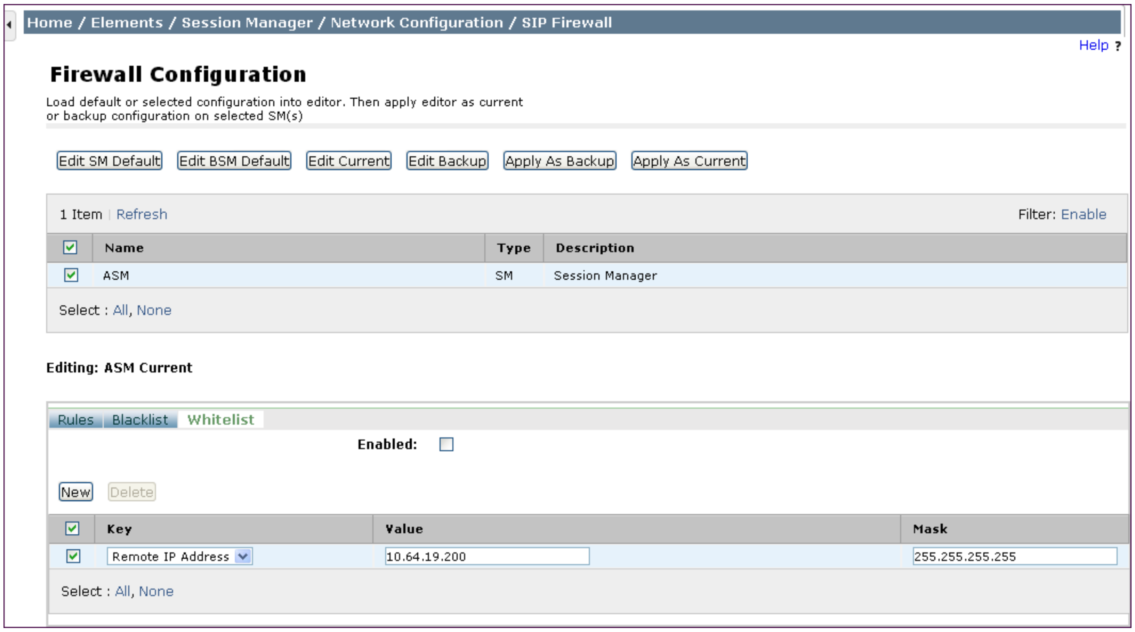


Edit Flow: SM6.3-Remote-Worker

Flow Name	SM6.3-Remote-Worker
Server Configuration	SM6.3
URI Group	*
Transport	*
Remote Subnet	*
Received Interface	Sig_Outside_92
Signaling Interface	Sig_Inside_200
Media Interface	Media_Inside_200
End Point Policy Group	SM
Routing Profile	default
Topology Hiding Profile	None
File Transfer Profile	None

In the sample configuration, the internal IP address of the Avaya SBCE used for Remote Worker was added to Session Manager's SIP Firewall Whitelist and PPM limiting was disabled.

To add an IP address to the Whitelist, log into System Manager and navigate to **Session Manager → Network Configuration → SIP Firewall**. Select the Session Manager listed in the top section and click **Edit SM Default**. Select the **Whitelist** tab towards the bottom of the screen and click **New**. Enter the internal IP address of Avaya SBCE used for Remote Workers in the **Value** field and "255.255.255.255" in the **Mask** field. Click **Apply As Current** to save the configuration.



Home / Elements / Session Manager / Network Configuration / SIP Firewall

Help ?

Firewall Configuration

Load default or selected configuration into editor. Then apply editor as current or backup configuration on selected SM(s)

1 Item | Refresh Filter: Enable

☑	Name	Type	Description
☑	ASM	SM	Session Manager

Select : All, None

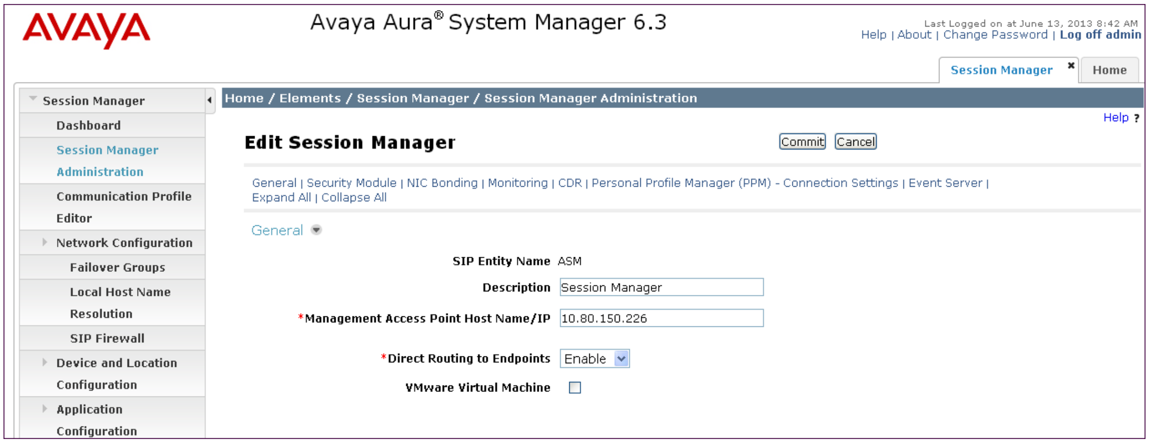
Editing: ASM Current

Enabled: □

☑	Key	Value	Mask
☑	Remote IP Address	10.64.19.200	255.255.255.255

Select : All, None

To disable PPM limiting, navigate to **Session Manager → Session Manager Administration** in the left-hand navigation pane and click **View** (not shown). A screen such as the following is displayed.



AVAYA
Avaya Aura® System Manager 6.3
Last Logged on at June 13, 2013 8:42 AM
Help | About | Change Password | Log off admin
Session Manager
Home
Session Manager
Dashboard
Session Manager Administration
Communication Profile Editor
Network Configuration
Failover Groups
Local Host Name Resolution
SIP Firewall
Device and Location Configuration
Application Configuration

Home / Elements / Session Manager / Session Manager Administration

Help ?

Edit Session Manager

Commit
Cancel
General | Security Module | NIC Bonding | Monitoring | CDR | Personal Profile Manager (PPM) - Connection Settings | Event Server |
Expand All | Collapse All

General

SIP Entity Name: ASM

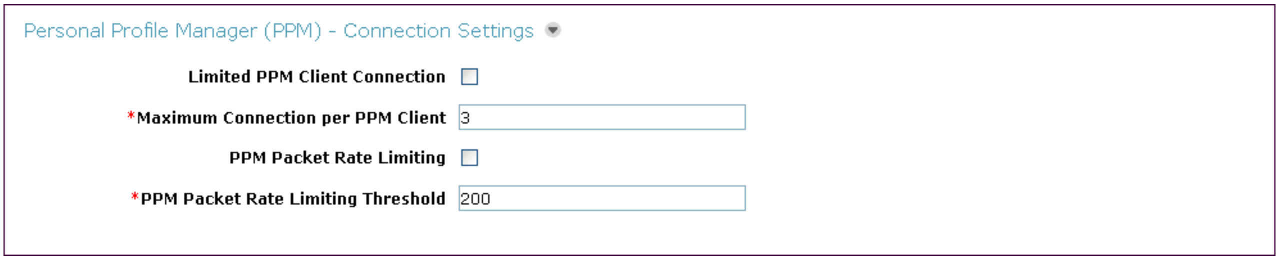
Description: Session Manager

*Management Access Point Host Name/IP: 10.80.150.226

*Direct Routing to Endpoints: Enable

VMware Virtual Machine: □

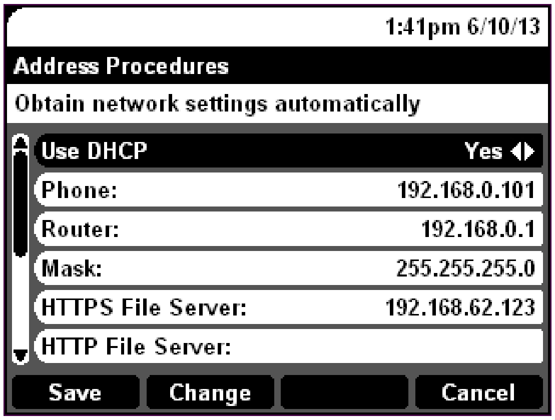
Scroll down to the **Personal Profile manager (PPM) – Connection Settings**. Uncheck **Limited PPM Client Connections** and **PPM Packet Rate Limiting**.



Personal Profile Manager (PPM) - Connection Settings

Limited PPM Client Connection	☐
*Maximum Connection per PPM Client	3
PPM Packet Rate Limiting	☐
*PPM Packet Rate Limiting Threshold	200

The following screens show an Avaya one-X® Deskphone SIP Emulator illustrating the administration settings of a SIP endpoint used for Remote Worker. Note that the **HTTPS File Server** is set to the external IP address of the Avaya SBCE designated for firmware and configuration file transfers. Under **SIP Global Settings**, the **SIP Domain** is set to “avayalab.com”. The domain expected by Session Manager.

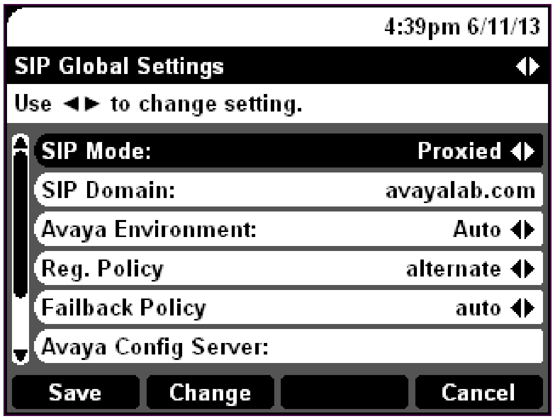


1:41pm 6/10/13

Address Procedures

Obtain network settings automatically

Use DHCP	Yes ◀▶
Phone:	192.168.0.101
Router:	192.168.0.1
Mask:	255.255.255.0
HTTPS File Server:	192.168.62.123
HTTP File Server:	



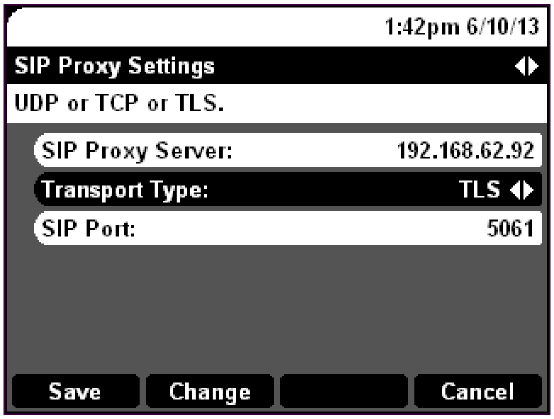
4:39pm 6/11/13

SIP Global Settings ◀▶

Use ◀▶ to change setting.

SIP Mode:	Proxied ◀▶
SIP Domain:	avayalab.com
Avaya Environment:	Auto ◀▶
Reg. Policy	alternate ◀▶
Failback Policy	auto ◀▶
Avaya Config Server:	

Under **SIP Proxy Settings**, the **SIP Proxy Server** is set to the external IP address of Avaya SBCE designated for Remote Worker SIP traffic. The Transport Type and SIP Port should be set according to device type. For example, “TLS” and “5061” for one-X® Deskphones, and “TCP” and “5060” for one-X® Communicator and Flare® Experience.



1:42pm 6/10/13

SIP Proxy Settings ◀▶

UDP or TCP or TLS.

SIP Proxy Server:	192.168.62.92
Transport Type:	TLS ◀▶
SIP Port:	5061

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.