Avaya Solution & Interoperability Test Lab

Application Notes for Avaya Aura™ Communication Manager 6.0, Avaya Aura™ Session Manager 6.0, and Acme Packet Net-Net with Verizon Business IP Trunk SIP Trunk Service – Issue 1.2

Abstract

These Application Notes illustrate a sample configuration using Avaya Aura™ Session Manager Release 6 and Avaya Aura™ Communication Manager Release 6 with the Verizon Business Private IP (PIP) IP Trunk service. These Application Notes update previously published Application Notes with newer versions of Communication Manager and Session Manager, **including a declaration of support for Communication Manager Release 6.0.1 and Session Manager Release 6.1, as noted in Section 3**. The Verizon Business SIP trunk redundant architecture (2-CPE) is supported by dual Acme Packet Net-Net Session Border Controllers.

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

Information in these Application Notes has been obtained through DevConnect compliance testing and additional technical discussions. Testing was conducted via the DevConnect Program at the Avaya Solution and Interoperability Test Lab., utilizing a Verizon Business Private IP (PIP) circuit connection to the production Verizon Business IP Trunking service.

Table of Contents

1. Introduction

These Application Notes illustrate a sample configuration using Avaya Aura™ Session Manager Release 6 and Avaya Aura™ Communication Manager Release 6 with the Verizon Business Private IP (PIP) IP Trunk service. The Verizon Business IP Trunk service provides local and/or long-distance calls (with PSTN endpoints) via standards-based SIP trunks. These Application Notes update previously published Application Notes [JF-JRR-VZIPT] with newer versions of Communication Manager and Session Manager. The Verizon Business SIP trunk redundant architecture (2-CPE) is supported by dual Acme Packet Net-Net Session Border Controllers (SBCs). The Verizon Business SIP Trunk redundant (2-CPE) architecture provides for redundant SIP trunk access between the Verizon Business IP Trunk service offer and the customer premises equipment (CPE).

As in reference [JF-JRR-VZIPT], dual Acme Packet Net-Net SBCs are used as edge devices between the Avaya CPE and the Verizon Business network, and provide for Verizon Business 2-CPE redundancy. In addition, the Acme Packet SBCs provide Network Address Translation (NAT) functionality to convert the addresses used within the enterprise to the Verizon routable addresses.

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

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

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

1.1. Interoperability Compliance Testing

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

- Inbound and outbound voice calls between telephones controlled by Avaya Aura™ Communication Manager and the PSTN can be made using G.711MU or G.729A codecs.
- Direct IP-to-IP Media (also known as "Shuffling") when applicable.
- DTMF using RFC 2833
    - Outbound call to PSTN application requiring post-answer DTMF (e.g., an IVR or voice mail system)

    - Inbound call from PSTN to Avaya CPE application requiring post-answer DTMF (e.g., Avaya Modular Messaging, Avaya vector digit collection steps)
- Additional PSTN numbering plans (e.g., International, operator assist, 411)
- Hold / Retrieve with music on hold
- Call transfer using two approaches
    - REFER approach (Communication Manager Network Call Redirection flag on trunk group form set to "y")
    - INVITE approach (Communication Manager Network Call Redirection flag on trunk group form set to "n")
- Conference calls
- Modular Messaging voicemail coverage, retrieval, and Find-Me application.
- SIP Diversion Header for call redirection
    - Call Forwarding
    - EC500
- Long hold time calls
- Automatic fail-over testing associated with the 2-CPE redundancy (i.e., calls automatically re-routed around component outages).

1.2. Support

1.2.1 Avaya

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

1.2.2 Verizon

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

1.3. Known Limitations

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

- Although Avaya Aura™ Session Manager 6.0 supports the use of SIP phones, and SIP phones were present in the sample configuration, the configuration of SIP phones is not covered by these Application Notes.
- At the time of original publication of these Application Notes, Verizon Business IP Trunking service supported fax over G.711 but did not support T.38 fax. As noted in reference [JF-JRR-VZIPT], the use of an AudioCodes SIP Gateway between Communication Manager and the fax device has long been recommended for G.711 fax with Verizon IP Trunk service. Since original publication of these Application Notes, Verizon Business IP Trunking service has been enhanced to support T.38 fax. A customer connecting fax devices to an AudioCodes SIP Gateway may continue to use fax over G.711. Alternatively, if the AudioCodes gateway version and Communication Manager Service Pack are up to date, the customer may now choose to enable T.38 on the AudioCodes gateway and Communication Manager codec set. For example, for an AudioCodes MP-114, the AudioCodes gateway should use version 6.20A.035.001 or later. If T.38 fax will be used with Verizon IP Trunk service, and the fax

device will be connected to a SIP gateway, Communication Manager 6.0.1 Service Pack 6 (SP6) is recommended. Communication Manager 6.0.1 SP6 includes a change that enables Communication Manager to relay a SIP 488 response from Verizon to the SIP gateway for call scenarios where the SIP gateway requests T.38 but Verizon can not comply. By relaying the SIP 488 response from Verizon to the SIP gateway, Communication Manager 6.0.1 SP6 gives the SIP gateway the opportunity to "fallback to G.711" to complete the fax call using fax over G.711, if T.38 is not available for a particular fax call.

- If calls requiring in-band DTMF (rather than RFC 2833 signaling) will be required, the "DTMF over IP" parameter on the Avaya Aura™ Communication Manager SIP signaling group carrying such calls can be set to "in-band" rather than "rtp-payload". If the Communication Manager SIP signaling group is set to "rtp-payload", and a call is established using RFC 2833, Communication Manager will not subsequently switch to using "in-band" procedures to signal DTMF. Avaya is considering an enhancement for a future release of Communication Manager that would allow a call initially established with RFC 2833 to switch to using in-band DTMF based on subsequent SIP SDP exchanges.
- Verizon Business IP Trunking service does not support G.711a codec for domestic service (EMEA only).
- Verizon Business IP Trunking service does not support G.729B codec.

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

2. Reference Configuration

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

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

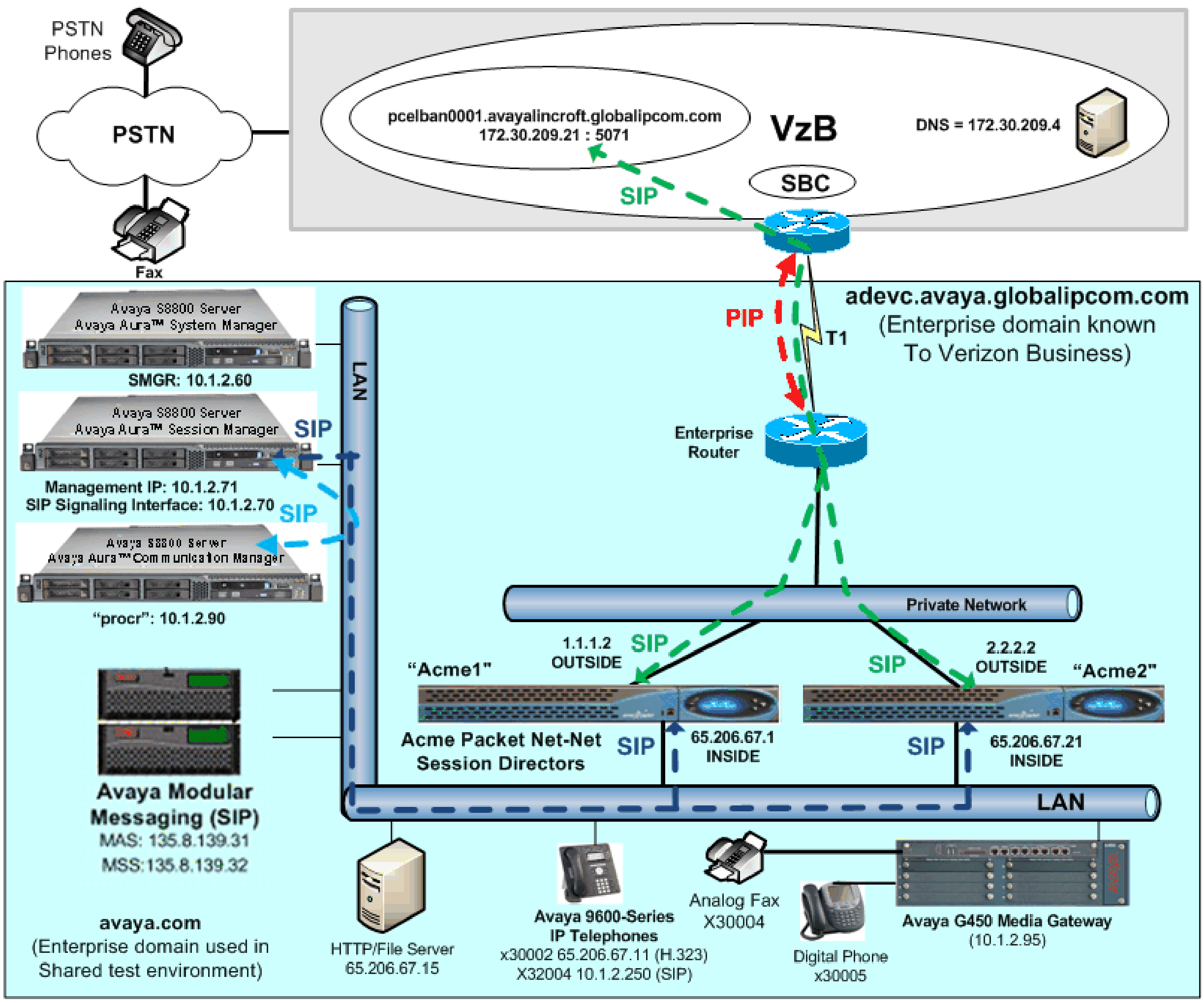


Figure 1: Avaya Interoperability Test Lab Configuration

The Verizon Business IP Trunk service used FQDN *pcelban0001.avayalincroft.globalipcom.com*. The Avaya CPE environment was known to Verizon Business IP Trunk service as FQDN *adevc.avaya.globalipcom.com*, as in reference [JF-JRR-VZIPT]. For efficiency, the Avaya CPE environment utilizing Session Manager Release 6 and Communication Manager Release 6 was shared among many ongoing test efforts at the Avaya Solution Interoperability Lab. Access to the Verizon Business IP Trunk service was added to a configuration that already used domain "avaya.com" at the enterprise. As such, Session Manager or the SBC are used to adapt the "avaya.com" domain to the domain known to Verizon. 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 the Verizon Business IP Trunk service.

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

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

- Verizon Business IP Trunk network Fully Qualified Domain Name (FQDN)
  - *pcelban0001.avayalincroft.globalipcom.com*
- Avaya CPE Fully Qualified Domain Name (FQDN) known to Verizon
  - *adevc.avaya.globalipcom.com*
- Primary and Secondary Acme Packet Net-Net SBCs.
- Avaya Aura™ Communication Manager Release 6
- Avaya Aura™ Session Manager Release 6
- Avaya 4600 Series IP telephones using the H.323 software bundle.
- Avaya 9600 Series IP telephones using the H.323 software bundle.
- Avaya Digital phones

2.1. History Info and Diversion Headers

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

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

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

3. Equipment and Software Validated

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

Equipment	Software
Avaya S8800 Server (Communication Manager)	Avaya Aura™ Communication Manager Release 6.0 (load 345.0, patch 18246)
Avaya S8800 Server (System Manager)	Avaya Aura™ System Manager Release 6.0 (load 6.0.0.0.556-3.0.6.1)
Avaya S8800 Server (Session Manager)	Avaya Aura™ Session Manager Release 6.0 (load 6.0.0.0.600020)
Avaya 9600-Series Telephones (H.323)	Release 3.1.1 – H.323
Avaya 2400-Series and 6400-Series Digital Telephones	N/A
Avaya Modular Messaging (Application Server)	Avaya Modular Messaging (MAS) 5.2 Service Pack 3 Patch 1
Avaya Modular Messaging (Storage Server)	Avaya Modular Messaging (MSS) 5.2, Build 5.2-11.0
Acme Packet Net-Net 4250[1]	nnSC620m3p1.xz
Brother Intellifax 1360	N/A

Table 1: Equipment and Software Used in the Sample Configuration

Note - The solution integration validated in these Application Notes should be considered valid for deployment with Avaya Aura® Communication Manager release 6.0.1 and Avaya Aura® Session Manager release 6.1. Avaya agrees to provide service and support for the integration of Avaya Aura® Communication Manager release 6.0.1 and Avaya Aura® Session Manager release 6.1 with Verizon Business IP Trunk service offer, in compliance with existing support agreements for Avaya Aura® Communication Manager release 6.0 and Avaya Aura® Session Manager 6.0, and in conformance with the integration guidelines as specified in this document. As noted in Section 1.3, Communication Manager 6.0.1 Service Pack 6 (SP6) is recommended if fax devices will be connected to a SIP gateway, and T.38 fax will be used.

4. Configure Avaya Aura™ Communication Manager Release 6

This section illustrates an example configuration allowing SIP signaling via the "Processor Ethernet" of the Avaya S8800 Servers 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.

[1] Although an Acme Net-Net 4250 was used in the sample configuration, the 3800, 4500, and 9200 platforms are also supported.

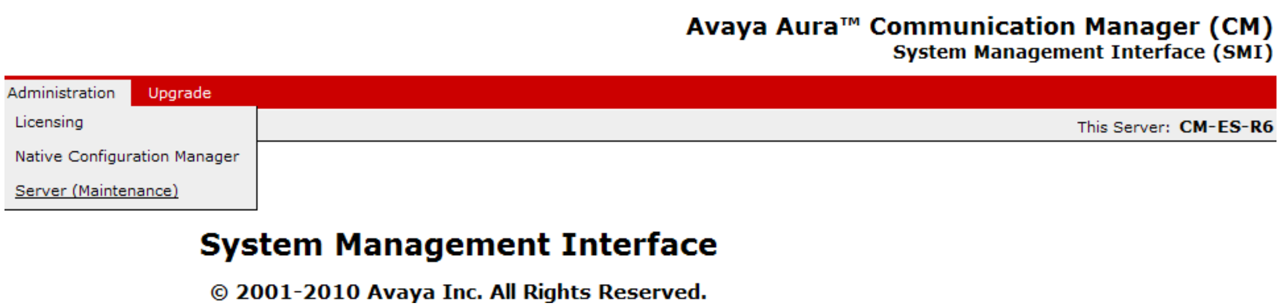
Note - The initial installation, configuration, and licensing of the Avaya servers and media gateways for Communication Manager are assumed to have been previously completed and are not discussed in these Application Notes.

Except for the web configuration shown in Section 4.1, all remaining configuration is performed via the Communication Manager SAT interface of the Avaya S8800 Server. Screens are abridged for brevity in presentation.

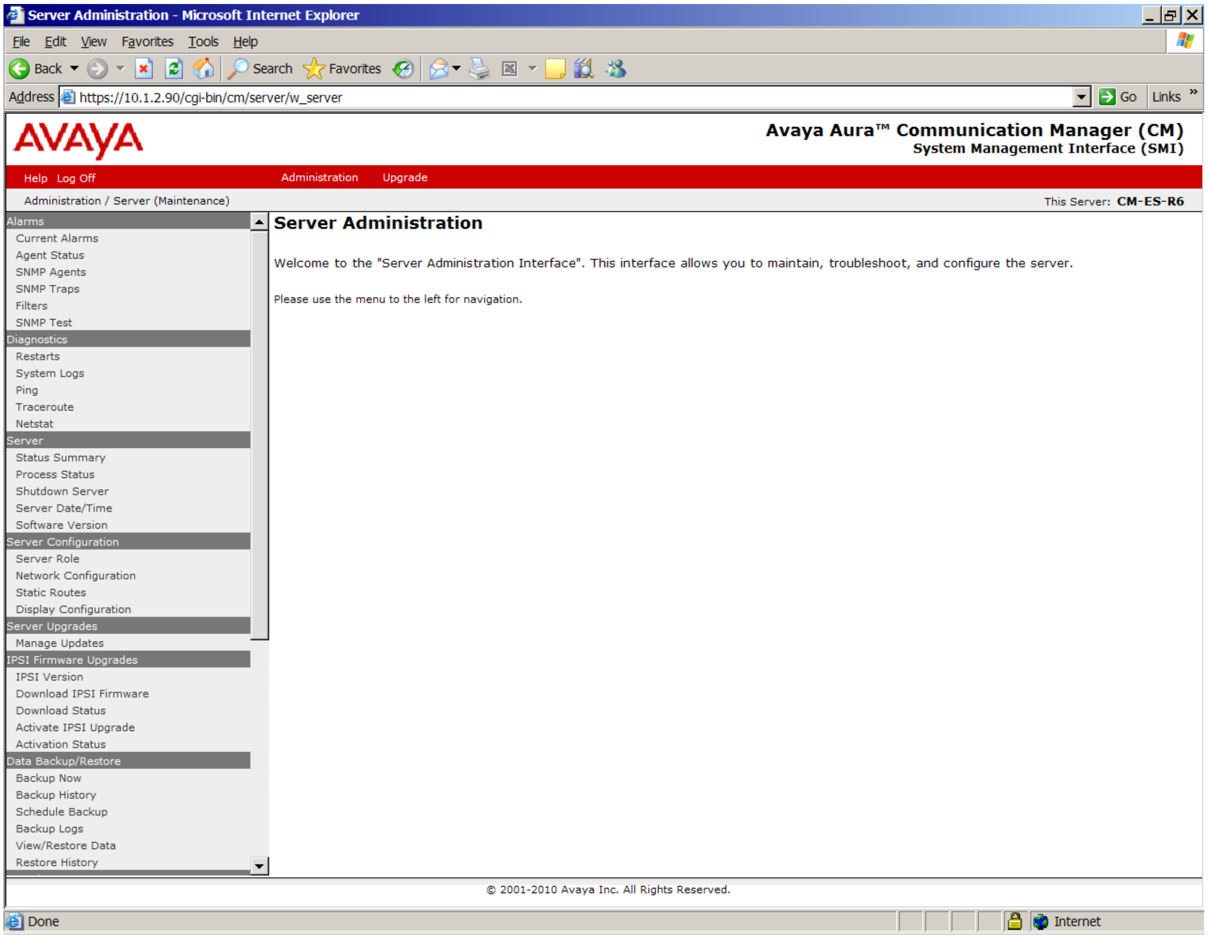
4.1. Processor Ethernet Configuration on S8800 Server

The screens in this section illustrate a previously completed configuration. Consult product documentation for further procedural guidance.

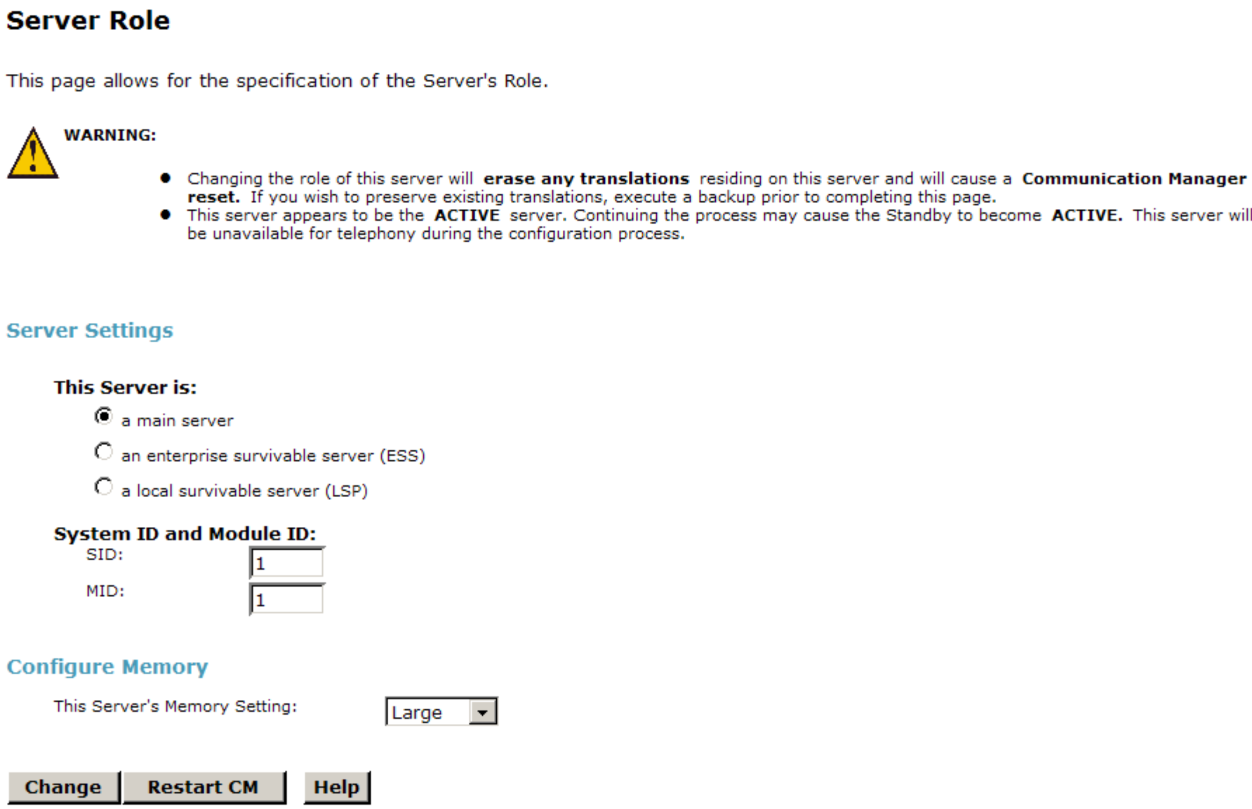
The S8800 Server can be accessed via a web interface in an internet browser. In the sample configuration, enter http://10.1.2.90 and log in with appropriate credentials (not shown). From the **System Management Interface** screen, select **Administration → Server (Maintenance)** as shown below.



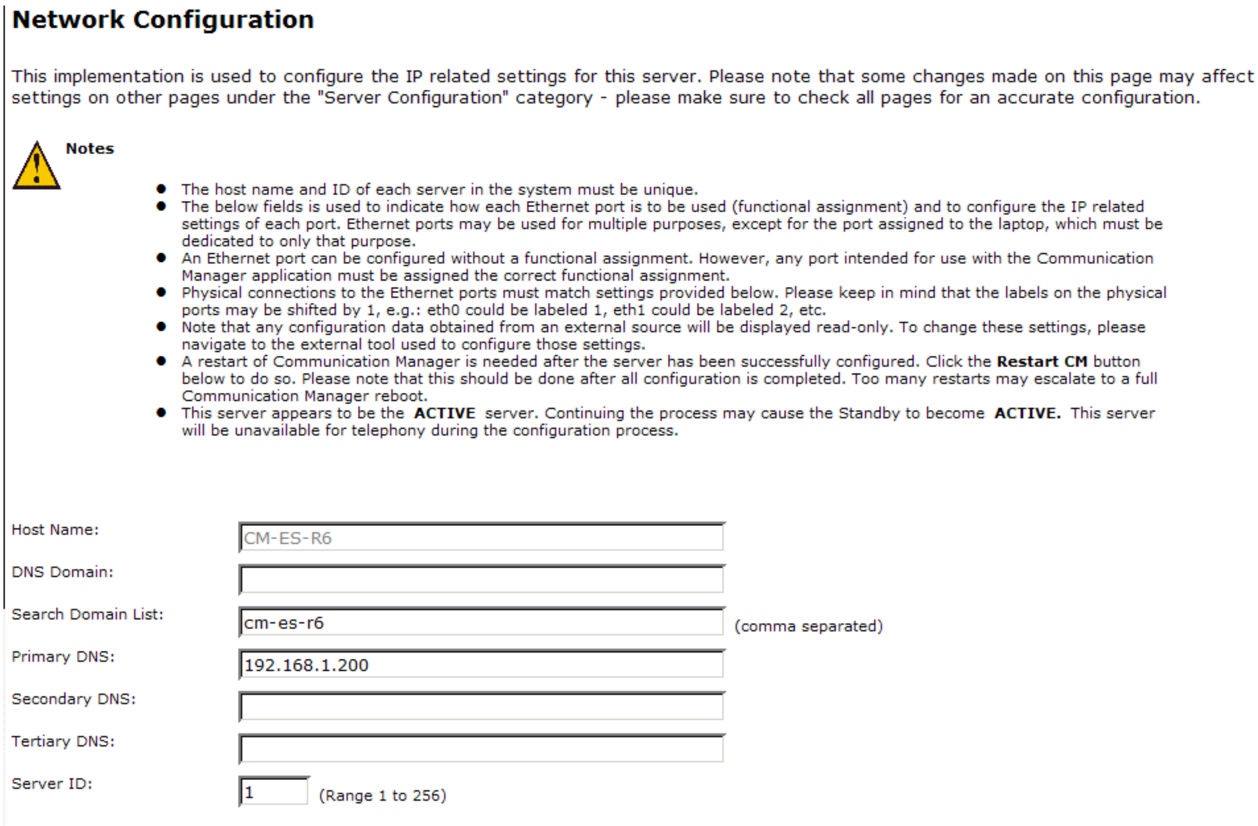
The resulting **Server Administration** screen is shown below.



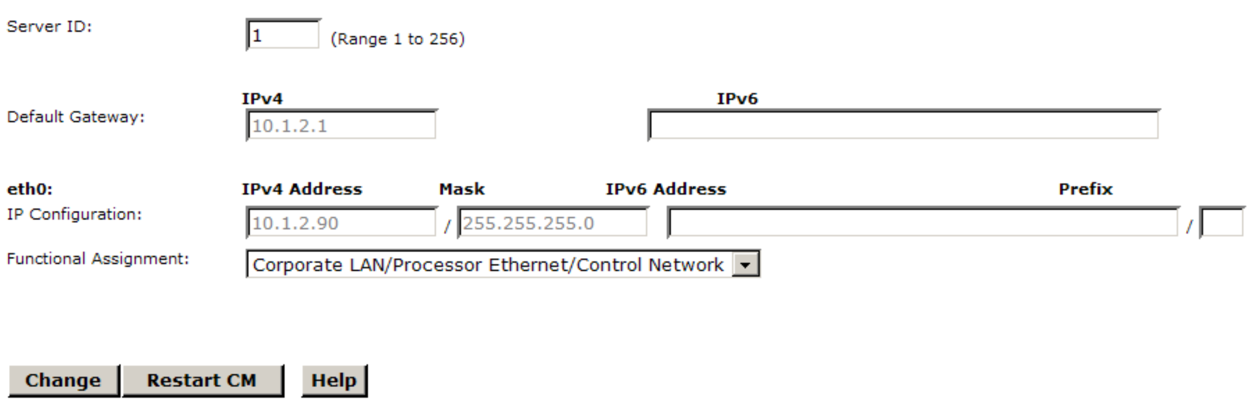
Under **Server Configuration**, select **Server Role** to view or configure the server role. In the sample configuration, the Avaya S8800 server is **a main server**, as shown below.



Under **Server Configuration**, select **Network Configuration** to view the network configuration. The following screen shows the upper portion of the **Network Configuration**.



Scrolling down, the following screen shows the lower portion of the Network Configuration. Note that the **IPv4 Address** of the server is 10.1.2.90, and that the **Functional Assignment** drop-down has assigned the **Corporate LAN/Processor Ethernet/Control Network** to the same “eth0” interface.



4.2. Verify Licensed Features

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

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

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

IP PORT CAPACITIES                                            USED
                     Maximum Administered H.323 Trunks: 12000 100
           Maximum Concurrently Registered IP Stations: 18000 3
             Maximum Administered Remote Office Trunks: 12000 0
Maximum Concurrently Registered Remote Office Stations: 18000 0
              Maximum Concurrently Registered IP eCons: 414   0
  Max Concur Registered Unauthenticated H.323 Stations: 100   0
                        Maximum Video Capable Stations: 18000 0
                   Maximum Video Capable IP Softphones: 18000 0
                       Maximum Administered SIP Trunks: 24000 146
  Maximum Administered Ad-hoc Video Conferencing Ports: 24000 0
   Maximum Number of DS1 Boards with Echo Cancellation: 522   0
                             Maximum TN2501 VAL Boards: 128   0
                     Maximum Media Gateway VAL Sources: 250   1
           Maximum TN2602 Boards with 80 VoIP Channels: 128   0
          Maximum TN2602 Boards with 320 VoIP Channels: 128   0
   Maximum Number of Expanded Meet-me Conference Ports: 300   0
```

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

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

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

On **Page 4** of the ***display system-parameters customer-options*** form, verify that the **Enhanced EC500**, **IP Trunks**, **IP Stations**, and **ISDN-PRI** features are enabled. If the use of SIP REFER messaging or send-only SDP attributes will be required (see also Section 4.9), verify that the **ISDN/SIP Network Call Redirection** feature is enabled.

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

           IP Attendant Consoles? y
```

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

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

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

4.3. Dial Plan

In the reference configuration the Avaya CPE environment uses five digit local extensions, such as 30xxx. Trunk Access Codes (TAC) are 3 digits in length and begin with 1. 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: 2

    Dialed   Total  Call      Dialed   Total  Call      Dialed   Total  Call
    String   Length Type      String   Length Type      String   Length Type
   0           3   fac
   1           3   dac
   2           5   ext
   3           5   ext
   4           4   ext
   5           5   ext
   6           3   fac
   60          5   ext
   7           5   ext
   8           1   fac
   9           1   fac
   *           2   fac
   #           2   fac
```

4.4. Node Names

Node names are mappings of names to IP addresses that can be used in various screens. The following abridged ***change node-names ip*** output shows relevant node-names in the sample configuration. As shown in bold, the node name for Session Manager is “SM1” with IP address 10.1.2.70. The node name and IP address (10.1.2.90) for the Processor Ethernet “procr” appears automatically due to the web configuration in Section 4.1.

```
change node-names ip                                        Page   1 of   2
                                   IP NODE NAMES
    Name                 IP Address
SM1                    10.1.2.70
procr                  10.1.2.90
```

4.5. IP Interface for procr

The ***add ip-interface procr*** or ***change ip-interface procr*** command can be used to configure the Processor Ethernet (PE) parameters. The following screen shows the parameters used in the sample configuration. While the focus here is the use of the PE for SIP Trunk Signaling, observe that the Processor Ethernet will also be used for registrations from H.323 IP Telephones and H.248 gateways in the sample configuration.

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

                  Type: PROCR
                                                         Target socket load: 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: 10.1.2.90

           Subnet Mask: /24
```

4.6. Network Regions for Gateway, Telephones

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

Non-IP telephones (e.g., analog, digital) derive network region and location configuration from the Avaya gateway to which the device is connected. The following display command shows that media gateway 1 is an Avaya G450 Media Gateway configured for network region 1. It can also be observed that the **Controller IP Address** is the Avaya S8800 Processor Ethernet (10.1.2.90), and that the gateway IP address is 10.1.2.95. These fields are not configured in this screen, but rather simply display the current information for the gateway.

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

                    Type: g450
                    Name: G450 Evolution Srvr
               Serial No: 08IS43202588
            Encrypt Link? y                  Enable CF? n
          Network Region: 1                   Location: 1
                                             Site Data:
           Recovery Rule: none

             Registered?  y
   FW Version/HW Vintage: 30 .13 .2  /1
        MGP IPV4 Address: 10.1.2.95
        MGP IPV6 Address:
   Controller IP Address: 10.1.2.90
             MAC Address: 00:1b:4f:03:57:b0
```

The following screen shows **Page 2** for media gateway 1. The gateway has an MM712 media module supporting Avaya digital phones in slot v3, an MM714 supporting analog devices in slot v5, and the capability to provide announcements and music on hold via "gateway-announcements" in logical slot v9.

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

                                 Type: g450

Slot   Module Type             Name                    DSP Type  FW/HW version
 V1:                                                   MP80      45   3
 V2:
 V3:   MM712                   DCP MM
 V4:
 V5:   MM714                   ANA MM
 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 65.206.67.11 would be mapped to network region 4, based on the bold configuration below. In production environments, different sites will typically be on different networks, and ranges of IP addresses assigned by the DHCP scope serving the site can be entered as one entry in the network map, to assign all telephones in a range to a specific network region.

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

                                               Subnet Network     Emergency
 IP Address                                    Bits   Region VLAN Location Ext
 --------------------------------------------- ------ ------ ---- -------------
 FROM: 10.1.2.0                                /24    1      n
   TO: 10.1.2.255
 FROM: 65.206.67.0                             /24    4      n
   TO: 65.206.67.255
```

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

```
change ip-network-region 4                                      Page   1 of  20
                               IP NETWORK REGION
  Region: 4
Location:          Authoritative Domain: adevc.avaya.globalipcom.com
    Name: Verizon testing
MEDIA PARAMETERS                Intra-region IP-IP Direct Audio: yes
      Codec Set: 4              Inter-region IP-IP Direct Audio: yes
   UDP Port Min: 2048                      IP Audio Hairpinning? y
   UDP Port Max: 3029
DIFFSERV/TOS PARAMETERS
 Call Control PHB Value: 46
        Audio PHB Value: 46
        Video PHB Value: 26
802.1P/Q PARAMETERS
 Call Control 802.1p Priority: 6
        Audio 802.1p Priority: 6
        Video 802.1p Priority: 5      AUDIO RESOURCE RESERVATION PARAMETERS
H.323 IP ENDPOINTS                                        RSVP Enabled? n
  H.323 Link Bounce Recovery? y
 Idle Traffic Interval (sec): 20
   Keep-Alive Interval (sec): 5
            Keep-Alive Count: 5
```

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

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

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

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

```
change ip-network-region 1                                     Page   1 of  20
                               IP NETWORK REGION
  Region: 1
Location:          Authoritative Domain: avaya.com
    Name: HQ CM and SIP Phones
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? y
   UDP Port Max: 65535
DIFFSERV/TOS PARAMETERS
 Call Control PHB Value: 46
        Audio PHB Value: 46
        Video PHB Value: 26
802.1P/Q PARAMETERS
 Call Control 802.1p Priority: 6
        Audio 802.1p Priority: 6
        Video 802.1p Priority: 5      AUDIO RESOURCE RESERVATION PARAMETERS
H.323 IP ENDPOINTS                                       RSVP Enabled? n
  H.323 Link Bounce Recovery? y
 Idle Traffic Interval (sec): 20
   Keep-Alive Interval (sec): 5
            Keep-Alive Count: 5
```

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

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

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

4.7. IP Codec Sets

The following screen shows the configuration for codec set 4, the codec set configured to be used for calls within region 4 and for calls between region 1 and region 4. In general, an IP codec set is a list of allowable codecs in priority order. Using the example configuration shown below, all calls to and from the PSTN via the SIP trunks would use G.729A, since G.729A is preferred by both Verizon and the Avaya ip-codec-set. Any calls using this same codec set that are between devices capable of the G.722-64K codec (e.g., Avaya 9600-Series IP Telephone) can use G.722. Note that if G.711MU is omitted from the list of allowed codecs in ip-codec-set 4, calls from

Verizon that are answered by Avaya Modular Messaging will use G450 VoIP resources to convert from G.729a (facing Verizon) to G.711MU (facing Modular Messaging). If G.711MU is included in ip-codec-set 4, then calls from Verizon that are answered by Modular Messaging will not use G450 VoIP resources, but rather be "ip-direct" using G.711MU from Modular Messaging to the inside of the Acme Packet Net-Net SBC. Include G.711MU in the ip-codec-set if fax will be used.

```
change ip-codec-set 4                                          Page   1 of   2
                          IP Codec Set
    Codec Set: 4

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

On **Page 2** of the form:

- Configure the Fax **Mode** field to "off". See Section 1.3 for additional fax considerations arising from Verizon's introduction of support for T.38 fax.
- Configure the Fax **Redundancy** field to "0**".**

```
change ip-codec-set 4                                          Page   2 of   2
                          IP Codec Set

                              Allow Direct-IP Multimedia? n

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

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

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

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

4.8. SIP Signaling Groups

This section illustrates the configuration of the SIP Signaling Groups. Each signaling group has a **Group Type** of “sip”, a **Near-end Node Name** of “procr”, and a **Far-end Node Name** of “SM1”. In the example screens, the **Transport Method** for all signaling groups is “tcp”. In production, TLS transport between Communication Manager and Session Manager can be used. The **Enable Layer 3 Test** field is enabled on each of the signaling groups to allow Communication Manager to maintain the signaling group using the SIP OPTIONS method. Fields that are not referenced in the text below can be left at default values, including **DTMF over IP** set to “rtp-payload”, which corresponds to RFC 2833.

The following screen shows signaling group 67. Signaling group 67 will be used for processing incoming PSTN calls from Verizon via Session Manager. The **Far-end Network Region** is configured to region 4. Port 5062 has been configured as both the **Near-end Listen Port** and **Far-end Listen Port**. Session Manager will be configured to direct calls arriving from the PSTN with Verizon DID numbers to a route policy that uses a SIP entity link to Communication Manager specifying port 5062. The use of different ports is one means to allow Communication Manager to distinguish different types of calls arriving from the same Session Manager. In the sample configuration, the **Peer Detection Enabled** field was set to “n”. Other parameters may be left at default values.

```
change signaling-group 67                                       Page   1 of   1
                                SIGNALING GROUP

 Group Number: 67             Group Type: sip
  IMS Enabled? n        Transport Method: tcp
        Q-SIP? n                                              SIP Enabled LSP? n
     IP Video? n                                   Enforce SIPS URI for SRTP? y
  Peer Detection Enabled? n  Peer Server: Others

   Near-end Node Name: procr                 Far-end Node Name: SM1
 Near-end Listen Port: 5062                Far-end Listen Port: 5062
                                        Far-end Network Region: 4

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

The following screen shows signaling group 68. Again, the **Near-end Node Name** is “procr”, the **Far-end Node Name** is “SM1”, the node name of the Session Manager, and the **Far-end Network Region** is 4. Signaling group 68 will be used for outgoing calls to Session Manager destined for the PSTN via Verizon. Although not strictly necessary in the sample configuration since Session Manager is adapting the Request-URI to the expected Verizon network domain, the **Far-end Domain** is set to “pcelban0001.avayalincroft.globalipcom.com”. In the sample configuration, the **Peer Detection Enabled** field was set to “n”. Other parameters may be left at default values.

Note that the **Alternate Route Timer** that defaults to 6 seconds impacts fail-over timing for outbound calls. If Communication Manager does not get an expected response, Look-Ahead

Routing (LAR) can be triggered, after the expiration of the Alternate Route Timer. Detailed examples of the use of LAR can be found in reference [PE] and reference [LAR].

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

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

   Near-end Node Name: procr                  Far-end Node Name: SM1
 Near-end Listen Port: 5062                 Far-end Listen Port: 5062
                                         Far-end Network Region: 4

Far-end Domain: pcelban0001.avayalincroft.globalipcom.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 60, the signaling group to Session Manager that was in place prior to adding the Verizon SIP Trunking configuration to the shared Avaya Interoperability Lab configuration. This signaling group reflects configuration not specifically related to Verizon trunking. For example, calls using Avaya SIP Telephones and calls routed to other Avaya applications, such as Avaya Modular Messaging, use this signaling group. Again, the **Near-end Node Name** is "procr" and the **Far-end Node Name** is "SM1", the node name of the Session Manager. Unlike the signaling groups used for the Verizon signaling, the **Far-end Network Region** is 1. The **Peer Detection Enabled** field is set to "y" and a peer Session Manager has been previously detected. The **Far-end Domain** is set to "avaya.com" matching the configuration in place prior to adding the Verizon SIP Trunking configuration.

```
change signaling-group 60                                          Page   1 of   1
                                SIGNALING GROUP

 Group Number: 60             Group Type: sip
  IMS Enabled? n        Transport Method: tcp
        Q-SIP? n                                                SIP Enabled LSP? n
     IP Video? n                                      Enforce SIPS URI for SRTP? y
  Peer Detection Enabled? y  Peer Server: SM

   Near-end Node Name: procr                  Far-end Node Name: SM1
 Near-end Listen Port: 5060                 Far-end Listen Port: 5060
                                         Far-end Network Region: 1

Far-end Domain: avaya.com
                                              Bypass If IP Threshold Exceeded? n
Incoming Dialog Loopbacks: eliminate                   RFC 3389 Comfort Noise? n
         DTMF over IP: rtp-payload             Direct IP-IP Audio Connections? y
Session Establishment Timer(min): 3                      IP Audio Hairpinning? n
         Enable Layer 3 Test? y                     Initial IP-IP Direct Media? n
H.323 Station Outgoing Direct Media? n              Alternate Route Timer(sec): 10
```

4.9. SIP Trunk Groups

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

The following shows **Page 1** for trunk group 67, which will be used for incoming PSTN calls from Verizon. The **Number of Members** field defines how many simultaneous calls are permitted for the trunk group. The **Service Type** field should be set to "public-ntwrk" for the trunks that will handle calls with Verizon. Although not strictly necessary, the **Direction** has been configured to "incoming" to emphasize that trunk group 67 is used for incoming calls only in the sample configuration.

```
change trunk-group 67                                          Page   1 of  21
                                TRUNK GROUP

Group Number: 67                  Group Type: sip           CDR Reports: y
  Group Name: From-SM-Acme-VZ            COR: 1        TN: 1        TAC: 167
   Direction: incoming       Outgoing Display? n
 Dial Access? n                                   Night Service:

Service Type: public-ntwrk          Auth Code? n
                                                       Signaling Group: 67
                                                     Number of Members: 6
```

The following shows **Page 2** for trunk group 67. 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 the Communication Manager default value, which can result in unnecessary SIP messages to re-establish a higher refresh interval for each call.

```
change trunk-group 67                                          Page   2 of  21
      Group Type: sip

TRUNK PARAMETERS
     Unicode Name: auto
                                            Redirect On OPTIM Failure: 5000

            SCCAN? n                               Digital Loss Group: 18
                      Preferred Minimum Session Refresh Interval(sec): 900

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

The following shows **Page 3** for trunk group 67. All parameters except those in bold are default values. Optionally, replacement text strings can be configured using the "system-parameters features" screen, such that incoming "private" (anonymous) or "restricted" calls can display an Avaya-configured text string on called party telephones.

```
change trunk-group 67                                           Page   3 of  21
TRUNK FEATURES
          ACA Assignment? n            Measured: none
                                                          Maintenance Tests? y

                     Numbering Format: public
                                                UUI Treatment: service-provider

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

The following shows **Page 4** for trunk group 67. The **PROTOCOL VARIATIONS** page is one reason why it can be advantageous to configure incoming calls from Verizon to arrive on specific signaling groups and trunk groups. The bold fields have non-default values. The **Convert 180 to 183 for Early Media** field is new in Communication Manager Release 6. Verizon recommends that inbound calls to the enterprise result in a 183 with SDP rather than a 180 with SDP, and setting this field to "y" for the trunk group handling inbound calls from Verizon produces this result. Although not strictly necessary, the **Telephone Event Payload Type** has been set to 101 to match Verizon configuration. Setting the **Network Call Redirection** flag to "y" enables advanced services associated with the use of the REFER message, while also implicitly enabling Communication Manager to signal "send-only" media conditions for calls placed on hold at the enterprise site. If neither REFER signaling nor "send-only" media signaling is required, this field may be left at the default "n" value. In the testing associated with these Application Notes, transfer testing using REFER was successfully completed with the **Network Call Redirection** flag set to "y", and transfer testing using INVITE was successfully completed with the **Network Call Redirection** flag set to "n".

For redirected calls, Verizon supports the Diversion header, but not the History-Info header. Communication Manager can send the Diversion header by marking **Send Diversion Header** to "y". Alternatively, Communication can send the History-Info header by setting **Support Request History** to "y", and Session Manager can adapt the History-Info header to the Diversion header using the "VerizonAdapter". In the testing associated with these Application Notes, call redirection testing with Communication Manager sending Diversion Header was completed successfully. Communication Manager configuration was then changed (i.e., for outbound trunk-group 68), and call redirection testing with Communication Manager sending History-Info and Session Manager adapting to Diversion Header was completed successfully.

```
change trunk-group 67                                           Page   4 of  21
                              PROTOCOL VARIATIONS

                        Mark Users as Phone? n
              Prepend '+' to Calling Number? n
        Send Transferring Party Information? n
                   Network Call Redirection? y
                      Send Diversion Header? y
                    Support Request History? n
               Telephone Event Payload Type: 101

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

The following shows **Page 1** for trunk group 68. The **Number of Members** field defines how many simultaneous calls are permitted for the trunk group. The **Service Type** field should be set to “public-ntwrk” for the trunks that will handle calls with Verizon. Although not strictly necessary, the **Direction** has been configured to “outgoing” to emphasize that trunk group 68 is used for outgoing calls to Session Manager destined for the PSTN. The remaining pages for trunk group 68 can match trunk group 67 and therefore will not be illustrated here.

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

Group Number: 68                  Group Type: sip           CDR Reports: y
  Group Name: To-ASM-6-VZ                COR: 1        TN: 1        TAC: 168
   Direction: outgoing       Outgoing Display? n
 Dial Access? n                                Night Service:
Queue Length: 0
Service Type: public-ntwrk          Auth Code? n
                                                    Signaling Group: 68
                                                  Number of Members: 10
```

The following shows **Page 1** for trunk group 60, 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 for communication with other Avaya applications, such as Avaya Modular Messaging, and does not reflect any unique Verizon configuration.

```
change trunk-group 60                                           Page   1 of  21
                                TRUNK GROUP

Group Number: 60                  Group Type: sip           CDR Reports: y
  Group Name: SM1                        COR: 1        TN: 1        TAC: 160
   Direction: two-way        Outgoing Display? n
 Dial Access? n                                Night Service:
Queue Length: 0
Service Type: tie                   Auth Code? n
                                                    Signaling Group: 60
                                                  Number of Members: 100
```

The following shows **Page 3** for trunk group 60. Note that unlike the trunks associated with Verizon calls that use “public” numbering, this tie trunk group uses a “private” **Numbering Format**.

```
change trunk-group 60                                           Page   3 of  21
TRUNK FEATURES
          ACA Assignment? n            Measured: none
                                                          Maintenance Tests? y

                     Numbering Format: private
                                               UUI Treatment: service-provider

                                                Replace Restricted Numbers? n
                                               Replace Unavailable Numbers? n

                                Modify Tandem Calling Number: no

 Show ANSWERED BY on Display? y
```

The following shows **Page 4** for trunk group 60. 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 Avaya Modular Messaging.

```
change trunk-group 60                                           Page   4 of  21
                              PROTOCOL VARIATIONS

                      Mark Users as Phone? n
            Prepend '+' to Calling Number? n
      Send Transferring Party Information? n
                 Network Call Redirection? n
                    Send Diversion Header? n
                  Support Request History? y
             Telephone Event Payload Type:

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

4.10. Route Pattern Directing Outbound Calls to Verizon

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

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

```
change route-pattern 68                                         Page   1 of   3
                    Pattern Number: 68  Pattern Name: To-VZ-IP-Trunk
                             SCCAN? n     Secure SIP? n
    Grp FRL NPA Pfx Hop Toll No.  Inserted                            DCS/ IXC
    No          Mrk Lmt List Del  Digits                              QSIG
                             Dgts                                     Intw
 1: 68   0                                                             n   user
 2:                                                                    n   user
 3:                                                                    n   user
 4:                                                                    n   user
 5:                                                                    n   user
 6:                                                                    n   user

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

4.11. Public Numbering

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

In the bolded row shown in the example abridged output below, a specific Communication Manager extension (x30002) is mapped to a DID number that is known to Verizon for this SIP Trunk connection (7329450285), when the call uses trunk group 67 or 68. Alternatively, Communication Manager can send the five digit extension to Session Manager, and Session Manager can adapt the number to the Verizon DID. Both methods were tested successfully.

```
change public-unknown-numbering 5                                Page   1 of   2
                      NUMBERING - PUBLIC/UNKNOWN FORMAT
                                           Total
Ext Ext           Trk       CPN             CPN
Len Code          Grp(s)    Prefix          Len
                                                  Total Administered: 3
 5  3             60                        5        Maximum Entries: 9999
 5  556                                     5
 5  30002         67-68        7329450285   10    Note: If an entry applies to
                                                  a SIP connection to Avaya
                                                  Aura(tm) Session Manager,
                                                  the resulting number must
                                                  be a complete E.164 number.
```

4.12. ARS Routing For Outbound Calls

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

The following screen shows a specific ARS configuration as an example. If a user dials the ARS access code followed by 1-908-848-5704, the call will select route pattern 68. Of course, matching of the dialed string need not be this specific. The ARS configuration shown here is not intended to be prescriptive.

```
change ars analysis 19088485704                                  Page   1 of   2
                             ARS DIGIT ANALYSIS TABLE
                                   Location: all           Percent Full: 0

          Dialed            Total      Route     Call   Node  ANI
          String          Min  Max   Pattern    Type   Num   Reqd
    19088485704           11   11     68        hnpa         n
```

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

```
list ars route-chosen 19088485704
                          ARS ROUTE CHOSEN REPORT
     Location:  1                    Partitioned Group Number:  1

      Dialed            Total        Route     Call      Node
      String          Min    Max    Pattern    Type     Number    Location
 19088485704          11    11        68       hnpa                 all
```

4.13. Incoming Call Handling Treatment for Incoming Calls

In general, the incoming call handling treatment for a trunk group can be used to manipulate the digits received for an incoming call if necessary. Since Session Manager is present, Session Manager can be used to perform digit conversion, and digit manipulation via the Communication Manager incoming call handling table may not be necessary. If the DID number sent by Verizon is unchanged by Session Manager, then the DID number can be mapped to an extension using the incoming call handling treatment of the receiving trunk group. As an example, the following screen illustrates a conversion of DID number 7329450285 to extension 30002. Both Session Manager digit conversion and Communication Manager incoming call handling treatment methods were tested successfully.

```
change inc-call-handling-trmt trunk-group 67                   Page   1 of  30
                      INCOMING CALL HANDLING TREATMENT
 Service/      Number   Number      Del Insert
 Feature        Len      Digits
 public-ntwrk    10 7329450285       all 30002
```

4.14. Modular Messaging Hunt Group

Although not specifically related to Verizon, this section shows the hunt group used for access to Avaya Modular Messaging. In the sample configuration, users with voice mail have a coverage path containing hunt group 60. Users can dial extension 33000 to reach Modular Messaging (e.g., for message retrieval). The following screen shows **Page 1** of hunt-group 60.

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

            Group Number: 60                            ACD? n
              Group Name: MM Coverage                 Queue? n
         Group Extension: 33000                      Vector? n
              Group Type: ucd-mia             Coverage Path:
                      TN: 1          Night Service Destination:
                     COR: 1                 MM Early Answer? n
           Security Code:              Local Agent Preference? n
 ISDN/SIP Caller Display: mbr-name
```

The following screen shows **Page 2** of hunt-group 60, which routes to the AAR access code 8 and **Voice Mail Number** 33000.

```
display hunt-group 60                                          Page   2 of  60
                                  HUNT GROUP
                      Message Center: sip-adjunct

     Voice Mail Number        Voice Mail Handle         Routing Digits
                                                  (e.g., AAR/ARS Access Code)
     33000                    33000                     8
```

4.15. AAR Routing to Modular Messaging via Session Manager

Although not specifically related to Verizon, this section shows the AAR routing for the number used in the hunt group in the previous section. The bold row shows that calls to the number range 33xxx, which includes the Modular Messaging hunt group 33000, will use **Route Pattern** 60. As can be observed from the other rows, various other dial strings also route to other internal destinations (i.e., not to Verizon) via route pattern 60.

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

          Dialed            Total     Route    Call   Node  ANI
          String          Min  Max   Pattern   Type   Num   Reqd
    205                   5    5      60       unku         n
    300                   5    5      60       unku         n
    301                   5    5      60       unku         n
    305                   5    5      60       unku         n
    3100                  5    5      60       unku         n
    32                    5    5      60       unku         n
    33                    5    5      60       unku         n
    3400                  5    5      60       unku         n
```

4.16. Uniform Dial Plan (UDP) Configuration

Although not specifically related to Verizon, this section shows the UDP configuration, with the bold row showing the calls of the form 33xxx will be routed via AAR.

```
change uniform-dialplan 3                                     Page   1 of   2

                       UNIFORM DIAL PLAN TABLE
                                                           Percent Full: 0
  Matching                    Insert              Node
  Pattern        Len Del      Digits     Net Conv Num
 30001            5   0                  aar  n
 30002            5   0                  aar  n
 30008            5   0                  aar  n
 30009            5   0                  aar  n
 30015            5   0                  aar  n
 301              5   0                  aar  n
 30101            5   0                  aar  n
 31               5   0                  aar  n
 3100             5   0                  aar  n
 33               5   0                  aar  n
 3400             5   0                  aar  n
```

4.17. Route Pattern for Internal Calls via Session Manager

Although not specifically related to Verizon, this section shows the AAR routing for the number used in the hunt group for Modular Messaging. Route pattern 60 contains trunk group 60, the "private" tie trunk group to Session Manager.

```
change route-pattern 60                                           Page   1 of   3
                    Pattern Number: 60  Pattern Name: SM FS
                             SCCAN? n     Secure SIP? n
    Grp FRL NPA Pfx Hop Toll No.  Inserted                            DCS/ IXC
    No          Mrk Lmt List Del  Digits                              QSIG
                             Dgts                                     Intw
 1: 60   0                    0                                        n   user
 2:                                                                    n   user
 3:                                                                    n   user
 4:                                                                    n   user
 5:                                                                    n   user
 6:                                                                    n   user

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

4.18. Private Numbering

Although not specifically related to Verizon, this section shows the private numbering configuration associated with the calls using trunk group 60. The bold row configures any five digit number beginning with 3 (i.e., 3xxxx) that uses trunk group 60 to retain the original 5 digit number (i.e., no digit manipulation is specified, and the **Total Len** is 5).

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

Ext Ext              Trk        Private          Total
Len Code             Grp(s)     Prefix           Len
 5  2                                            5     Total Administered: 5
 5  3                60                          5        Maximum Entries: 540
 5  4                                            5
 5  5                                            5
```

4.19. Avaya Aura™ Communication Manager Stations

In the sample configuration, five digit station extensions were used with the format 3xxxx. The following abbreviated screen shows an example extension for an Avaya H.323 IP telephone. Coverage path 60 is assigned to give this user coverage to Avaya Modular Messaging.

```
change station 30002                                          Page   1 of   5
                                     STATION
Extension: 30002                         Lock Messages? n               BCC: 0
     Type: 9620                          Security Code: *                TN: 1
     Port: S00038                      Coverage Path 1: 60              COR: 1
     Name: Joey Votto                  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: 30002
            Speakerphone: 2-way               Mute Button Enabled? y
```

On **Page 2**, the **MWI Served User Type** is set to "sip-adjunct" for the SIP integration to Avaya Modular Messaging.

```
change station 30002                                          Page   2 of   5
                                     STATION
FEATURE OPTIONS
           LWC Reception: spe              Auto Select Any Idle Appearance? n
          LWC Activation? y                         Coverage Msg Retrieval? y
  LWC Log External Calls? n                                    Auto Answer:
none
             CDR Privacy? n                               Data Restriction? n
   Redirect Notification? y                     Idle Appearance Preference? n
 Per Button Ring Control? n                   Bridged Idle Line Preference? n
   Bridged Call Alerting? n                       Restrict Last Appearance? y
  Active Station Ringing: single
                                                         EMU Login Allowed? n
        H.320 Conversion? n          Per Station CPN - Send Calling Number?
       Service Link Mode: as-needed                     EC500 State: enabled
         Multimedia Mode: enhanced                 Audible Message Waiting? n
    MWI Served User Type: sip-adjunct           Display Client Redirection? n
                                               Select Last Used Appearance? n
                                                 Coverage After Forwarding? s
                                                   Multimedia Early Answer? n
                                            Direct IP-IP Audio Connections? y
  Emergency Location Ext: 30002        Always Use? n IP Audio Hairpinning? n
```

4.20. Coverage Path

This section illustrates an example coverage path for a station with a mailbox on Avaya Modular Messaging. Hunt group 60, the hunt group to Modular Messaging, is **Point1** in coverage path 60.

```
change coverage path 60                                         Page   1 of   1
                                 COVERAGE PATH
                   Coverage Path Number: 60
     Cvg Enabled for VDN Route-To Party? y        Hunt after Coverage? n
                       Next Path Number:          Linkage
COVERAGE CRITERIA
    Station/Group Status    Inside Call     Outside Call
             Active?             n               n
               Busy?             y               y
       Don't Answer?             y               y        Number of Rings: 2
                All?             n               n
 DND/SAC/Goto Cover?             y               y
   Holiday Coverage?             n               n

COVERAGE POINTS
    Terminate to Coverage Pts. with Bridged Appearances? n
  Point1: h60             Rng:    Point2:
  Point3:                         Point4:
  Point5:                         Point6:
```

4.21. EC500 Configuration for Diversion Header Testing

When EC500 is enabled for a Communication Manager station, a call to that station will generate a new outbound call from Avaya Aura™ Communication Manager to the configured EC500 destination, typically a mobile phone. The following screen shows an example EC500 configuration for the user with station extension 30002. Use the command ***change off-pbx-telephone station mapping x*** where ***x*** is the Communication Manager station (e.g. 30002).

- **Station Extension** – This field will automatically populate
- **Application** – Enter **"**EC500"
- **Dial Prefix** – Enter a prefix (e.g., 1) if required by the routing configuration
- **Phone Number** – Enter the phone that will also be called (e.g., 7326870755)
- **Trunk Selection** – Enter "ars". This means ARS will be used to determine how Communication Manager will route to the **Phone Number** destination.
- **Config Set** – Enter "1"
- Other parameters can retain default values

```
change off-pbx-telephone station-mapping 30002                  Page   1 of   3
                  STATIONS WITH OFF-PBX TELEPHONE INTEGRATION
 Station        Application Dial   CC  Phone Number    Trunk        Config  Dual
 Extension                  Prefix                     Selection    Set     Mode
 30002             EC500    1     -    7326870755       ars         1
```

4.22. Saving Communication Manager Configuration Changes

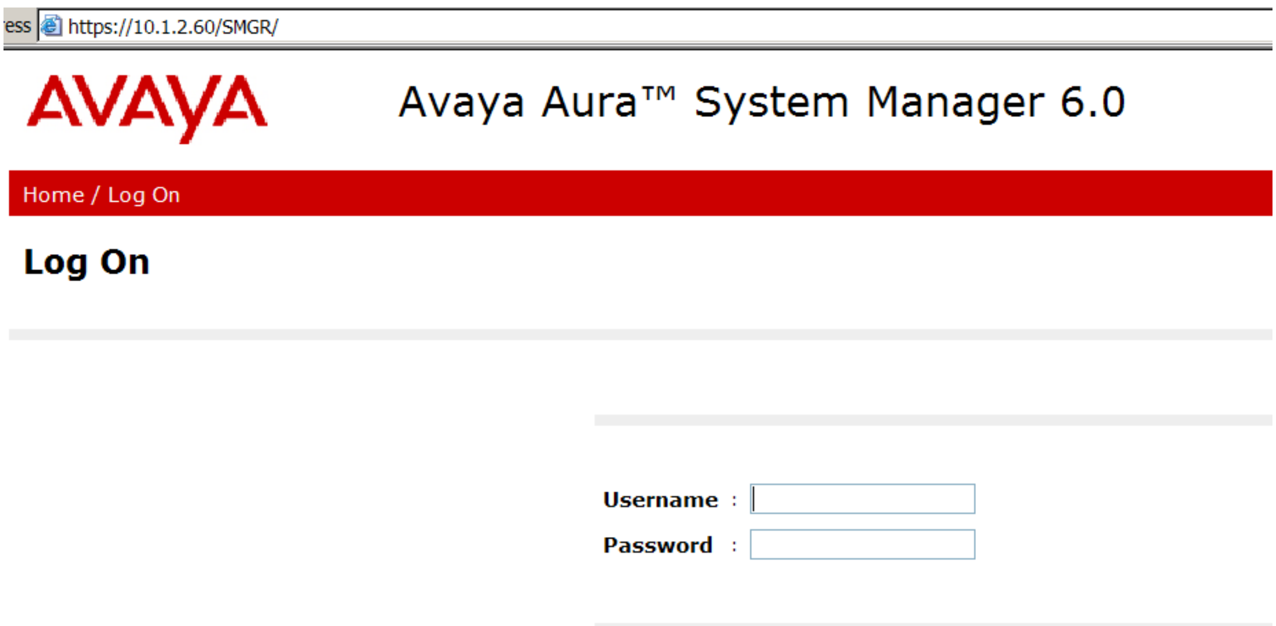
The command ***save translation all*** can be used to save the configuration.

5. Configure Avaya Aura™ Session Manager Release 6

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

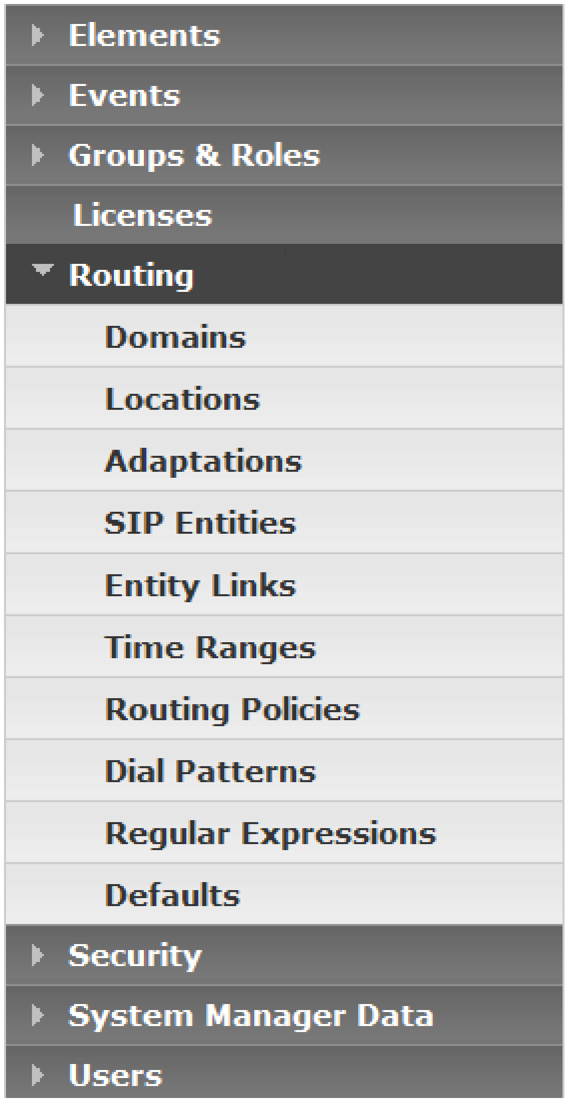
Note – The following sections assume that Session Manager and System Manager have been installed and that network connectivity exists between the two. For more information on Session Manager see **[3]**.

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 **Username** and **Password** and press the **Log On** button (not shown).



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

For readers familiar with prior releases of Session Manager, the configurable items under **Routing** in Release 6 were located under a heading called **Network Routing Policy** in prior releases. Select **Routing.** The screen shown below shows the various sub-headings.



When Routing is selected, the right side 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"

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

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"

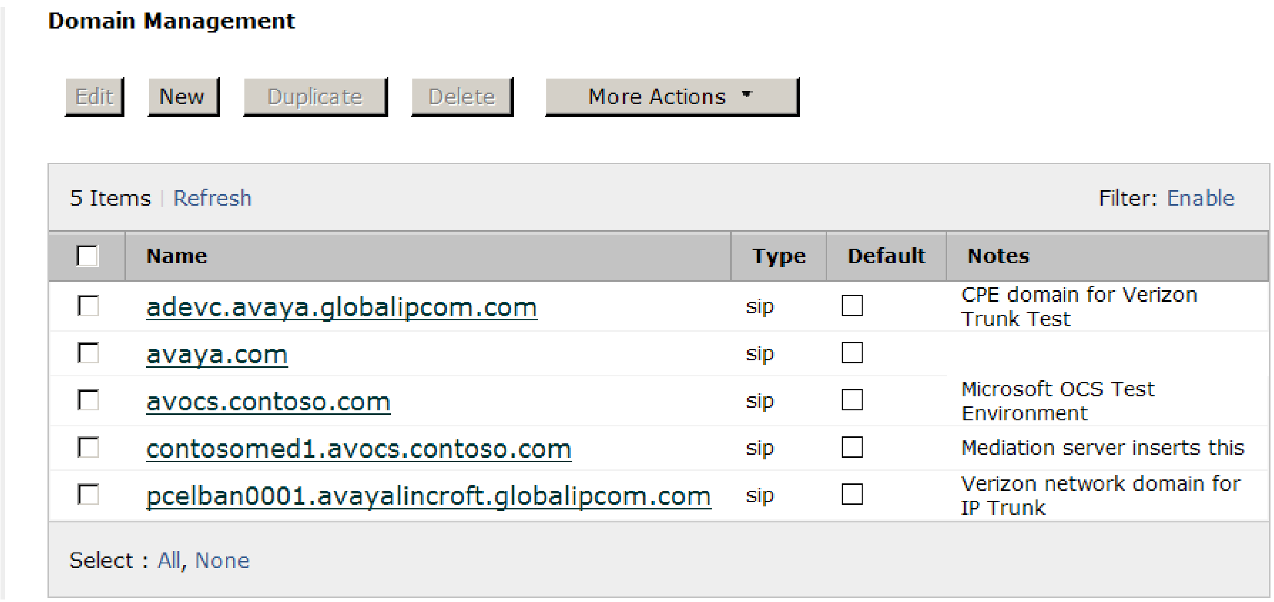
- Assign the appropriate "Routing Policies" to the "Regular Expressions"

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

5.1. Domains

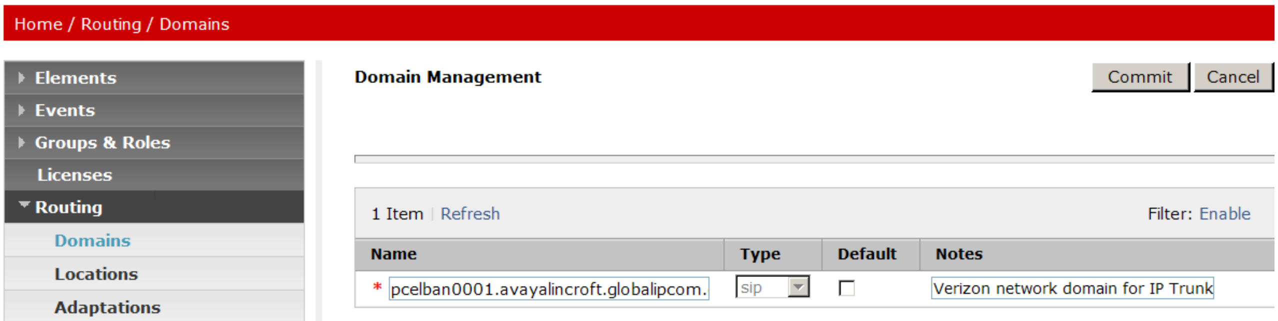
To view or change SIP domains, select **Routing → Domains**. Click on the checkbox next to the name of the SIP domain and **Edit** to edit an existing domain, or the **New** button to add a domain. Click the **Commit** button after changes are completed.

The following screen shows the list of configured SIP domains. The Session Manager used in the verification of these Application Notes was shared among many Avaya interoperability test efforts. The domain "avaya.com" was already being used for communication among a number of Avaya systems and applications, including an Avaya Modular Messaging system with SIP integration to Session Manager. The domain "avaya.com" is not known to the Verizon production service.



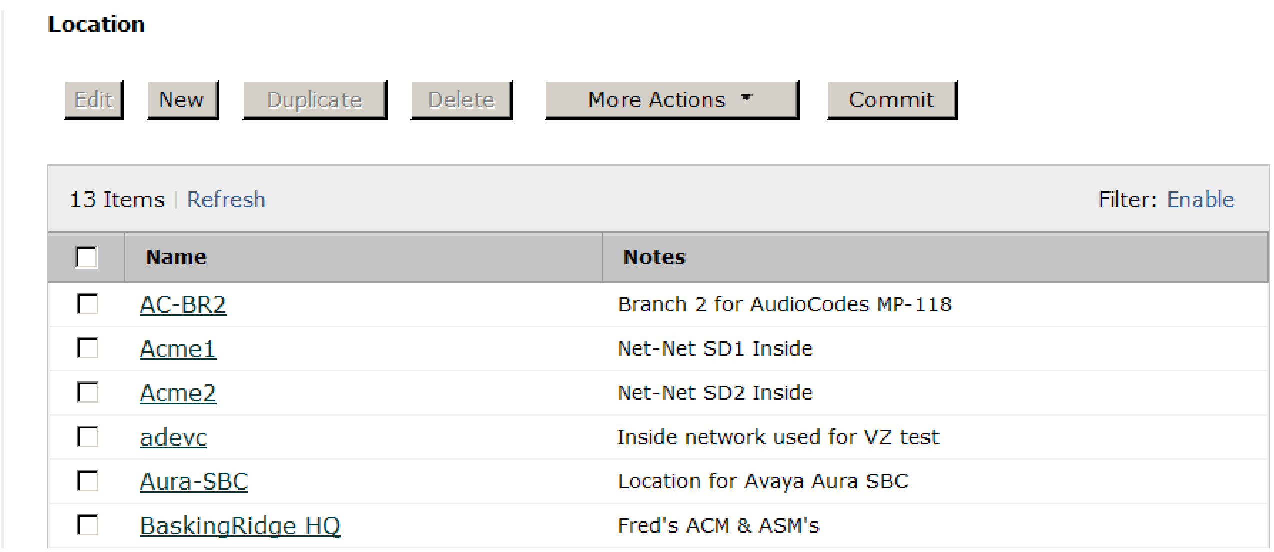
The domain "adevc.avaya.globalipcom.com" is the domain known to Verizon as the enterprise SIP domain. For example, for calls from the enterprise site to Verizon, this domain can appear in the P-Asserted-Identity in the INVITE message sent to Verizon.

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

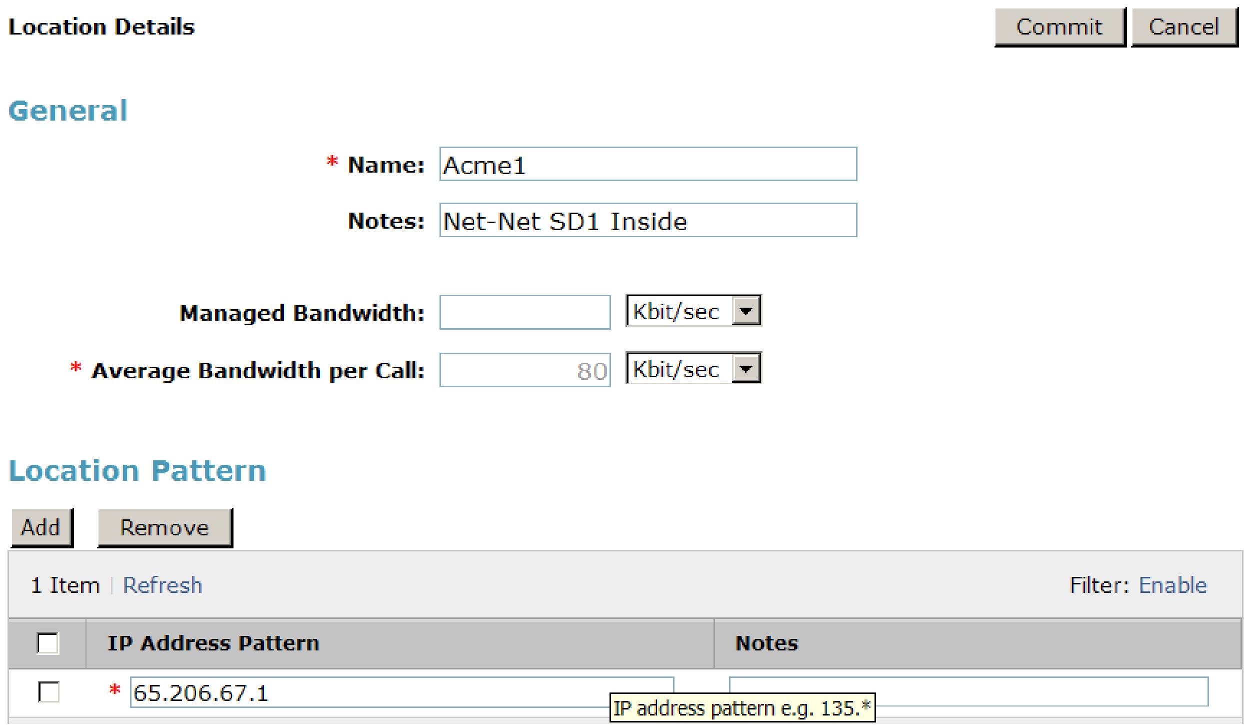


5.2. Locations

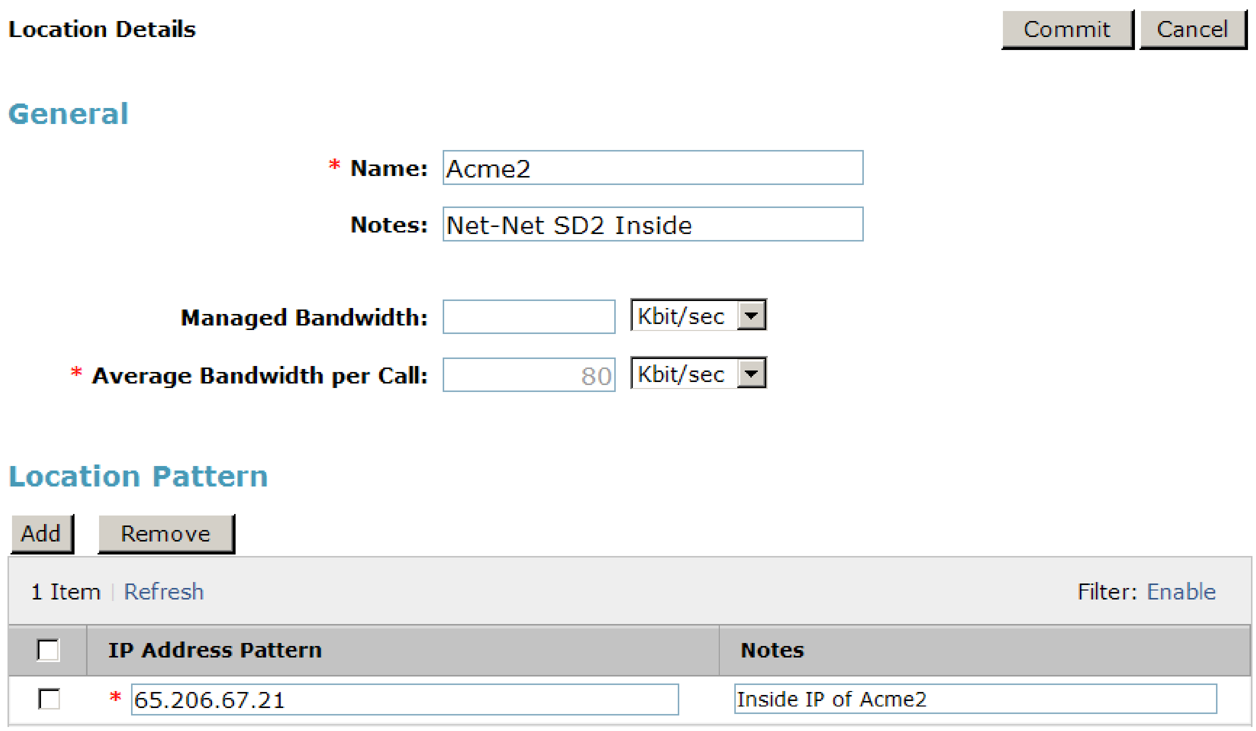
To view or change locations, select **Routing → Locations**. The following screen shows an abridged list of configured locations. Click on the checkbox corresponding to the name of a location and **Edit** to edit an existing location, or the **New** button to add a location. Click the **Commit** button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



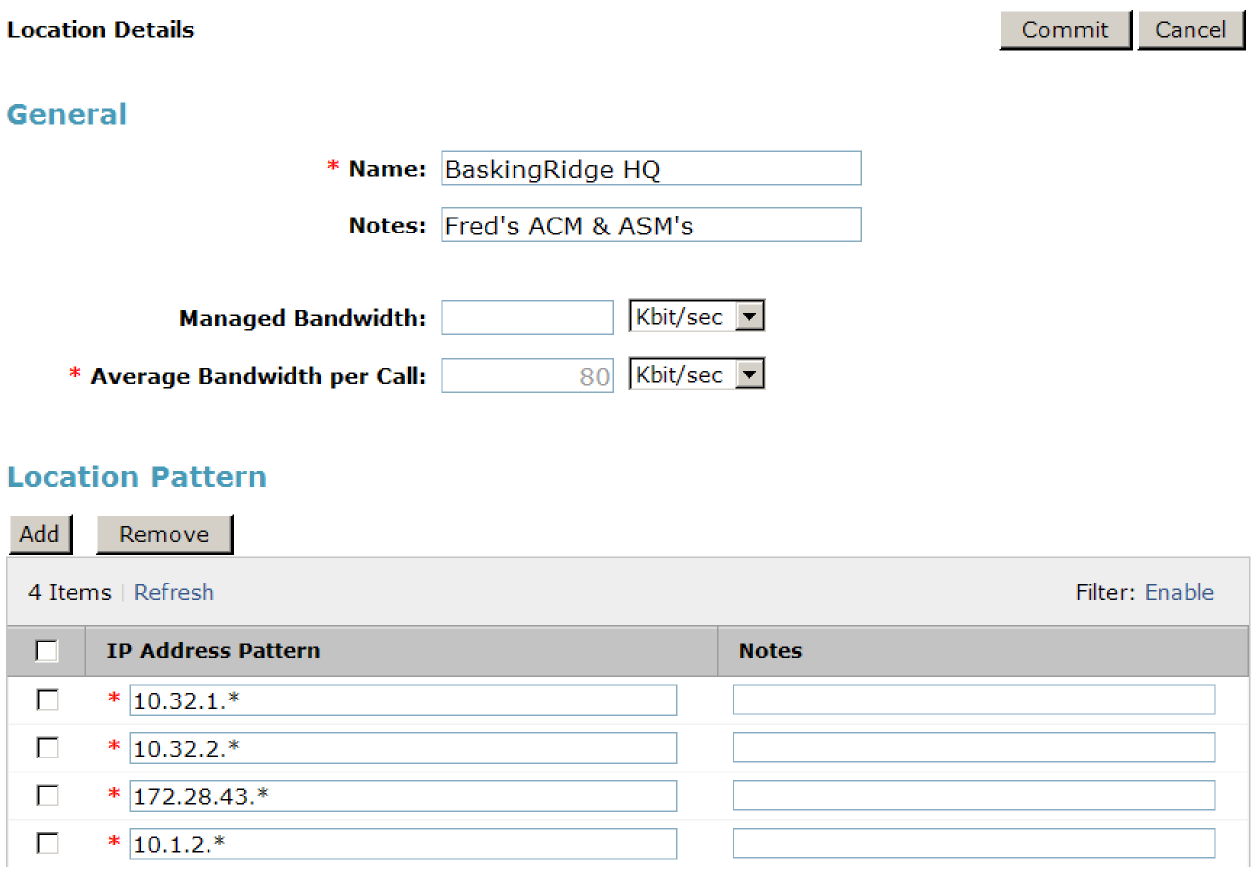
The following screen shows the location details for the location named "Acme1", corresponding to the primary Acme Packet Net-Net SBC. Later, the location with name "Acme1" will be assigned to the corresponding SIP Entity. The IP address 65.206.67.1 of the inside (private) interface of "Acme1" is entered in the **IP Address Pattern** field. Mouse-over help is available for Session Manager input fields and can be observed in the sample screen below.



The following screen shows the location details for the location named “Acme2”, corresponding to the second Acme Packet Net-Net SBC. Later, the location with name “Acme2” will be assigned to the corresponding SIP Entity. The IP address 65.206.67.21 of the inside (private) interface of “Acme2” is entered in the **IP Address Pattern** field.



The following screen shows the location details for the location named "BaskingRidgeHQ". The SIP Entities and associated IP addresses for this location correspond to the shared components of the Avaya Interoperability Lab test environment, such as Communication Manager Release 6, Session Manager Release 6, and Avaya Modular Messaging servers.



5.3. Adaptations

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

The following screen shows a portion of the list of adaptations in the sample configuration.

Adaptations

Edit | New | Duplicate | Delete | More Actions ▾ | Commit

14 Items | Refresh — Filter: Enable

☐	Name	Module name	Egress URI Parameters	Notes
☐	Avaya-R6.0	DigitConversionAdapter odstd=avaya.com osrcd=avaya.com		
☐	Cisco-UCM6	CiscoAdapter avaya.com		
☐	Cisco-UCM7	CiscoAdapter avaya.com		
☐	CiscoUCME	CiscoAdapter avaya.com		
☐	CM-ES Inbound	DigitConversionAdapter odstd=avaya.com osrcd=avaya.com		
☐	CM-ES-VZ Inbound	DigitConversionAdapter odstd=avaya.com		Avaya.com for shared SIL ntwk

After scrolling down, the following screen shows another portion of the list of adaptations in the sample configuration.

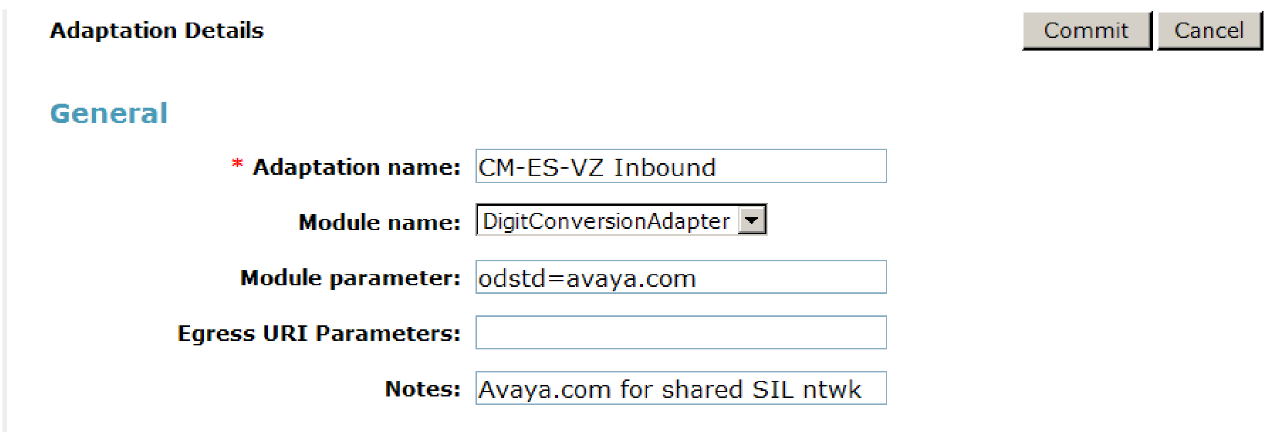
☐	History_Diversion_IPT	VerizonAdapter osrcd=adevc.avaya.globalipcom.com odstd=pcelban0001.avayalincroft.globalipcom.com
☐	MM Normalized	DigitConversionAdapter avaya.com

The adapter named "History_Diversion_IPT" will later be assigned to the Acme SIP Entities. This adaptation uses the "VerizonAdapter" and specifies two parameters that are used to adapt the FQDN to the domains expected by the Verizon network in the sample configuration.

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

Depending on the Communication Manager configuration, it may not be necessary for Session Manager to adapt the domains in this fashion. In the sample configuration, where "avaya.com" was already in use in a shared Avaya environment, it was necessary for Session Manager to adapt the domain from "avaya.com" to "adevc.avaya.globalipcom.com" where the latter is the CPE domain known to Verizon.

The adapter named "CM-ES-VZ Inbound" shown below will later be assigned to the SIP Entity linking Session Manager to Communication Manager for calls to and from Verizon. This adaptation uses the "DigitConversionAdapter" and specifies the "odstd=avaya.com" parameter to adapt the domain to the domain expected by Communication Manager in the sample configuration. More specifically, this configuration enables the destination domain to be overwritten with "avaya.com" for calls that egress to a SIP entity using this adapter. For example, for inbound PSTN calls from Verizon to the Avaya CPE, the Request-URI header sent to Communication Manager will contain "avaya.com" as expected by Communication Manager in the shared Avaya Interoperability Lab configuration. Depending on the Communication Manager configuration, it may not be necessary for Session Manager to adapt the domain in this fashion.



Scrolling down, the following screen shows a portion of the "CM-ES-VZ Inbound" adapter that can be used to convert digits between the extension numbers used on Communication Manager and the 10 digit DID numbers assigned by Verizon. Since this adapter will be assigned to the SIP Entity receiving calls from Communication Manager for routing to the PSTN, the settings for "incoming calls to SM" correspond with outgoing calls from Communication Manager to the PSTN using the Verizon IP Trunk service. Similarly, the settings for "outgoing calls from SM" correspond to incoming calls from the PSTN to Communication Manager. In general, digit conversion such as this, that converts a Communication Manager extension (e.g., 30002) to a corresponding LDN or DID number known to the PSTN (e.g., 7329450285), can be performed in Communication Manager (e.g., using "public unknown numbering" and "incoming call handling treatment" for the Communication Manager trunk group) or in Session Manager as shown below.

Digit Conversion for Incoming Calls to SM

Add | Remove

1 Item | Refresh — Filter: Enable

	Matching Pattern	Min	Max	Delete Digits	Insert Digits	Address to modify	Notes
	* 30002	* 5	* 5	* 5	7329450285	both	

Select : All, None

Digit Conversion for Outgoing Calls from SM

Add | Remove

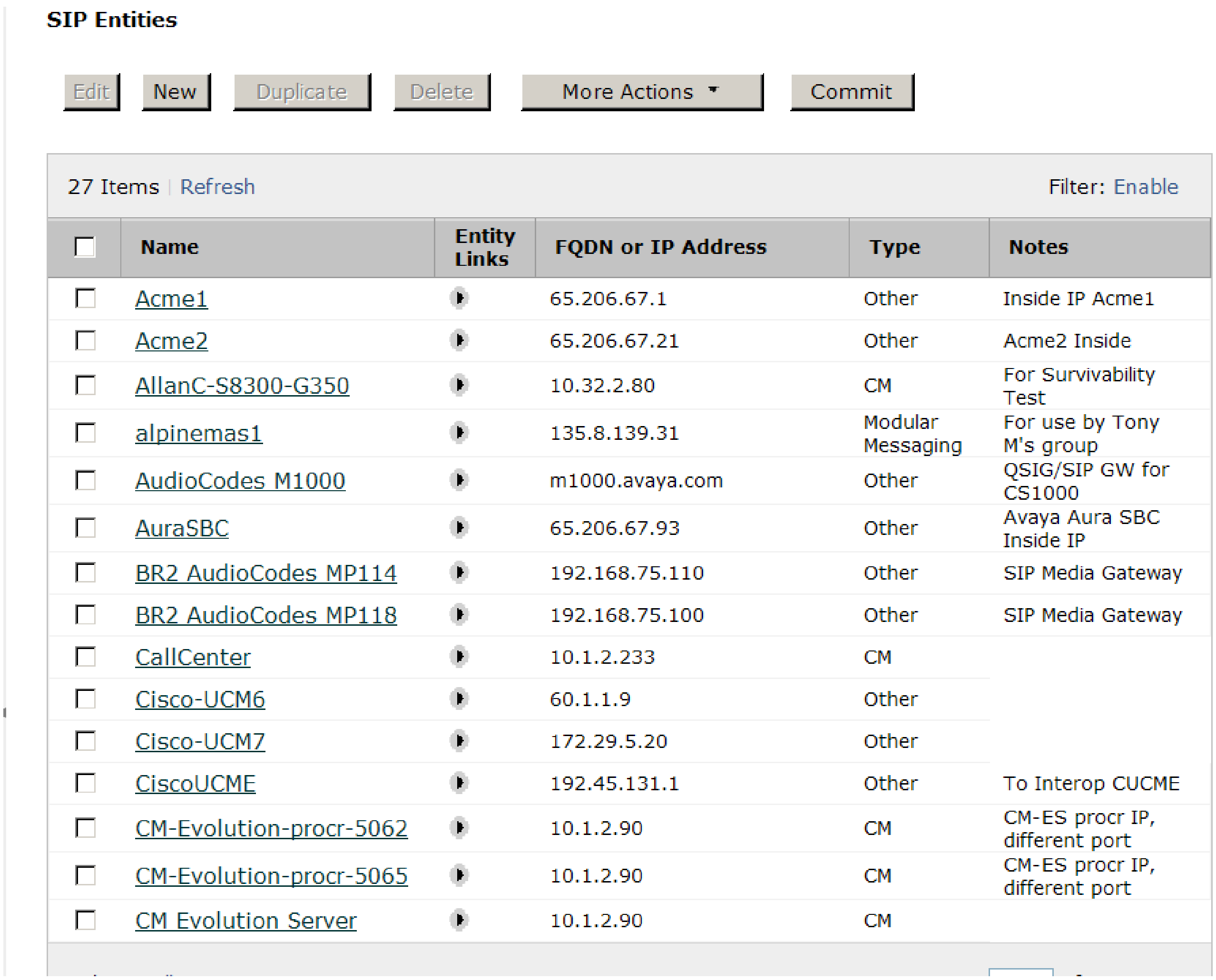
6 Items | Refresh — Filter: Enable

	Matching Pattern	Min	Max	Delete Digits	Insert Digits	Address to modify	Notes
	* 7329450285	* 10	* 10	* 10	30002	both	

In the example shown above, if a user on the PSTN dials 732-945-0285, Session Manager will convert the number to 30002 before sending the SIP INVITE to Communication Manager. As such, it would not be necessary to use the incoming call handling table of the receiving Communication Manager trunk group to convert the DID number to its corresponding extension. For an outbound call, if extension 30002 dials the PSTN, and if Communication Manager sends the extension 30002 to Session Manager as the calling number, Session Manager would convert the calling number to 7329450285. Alternatively, the Communication Manager public-unknown numbering form could have an entry to convert 30002 to 7329450285 before sending the call on the trunk group to Session Manager. Both methods were verified successfully in the testing associated with these Application Notes.

5.4. SIP Entities

To view or change SIP entities, select **Routing → SIP Entities**. Click the checkbox corresponding to the name of an entity and **Edit** to edit an existing entity, or the **New** button to add an entity. Click the **Commit** button after changes are completed. The following screen shows a portion of the list of configured SIP entities. In this screen, the SIP Entities named "Acme1", "Acme2", "alpinemas1", "CM-Evolution-procr-5062", and "CM Evolution Server" are relevant to these Application Notes.

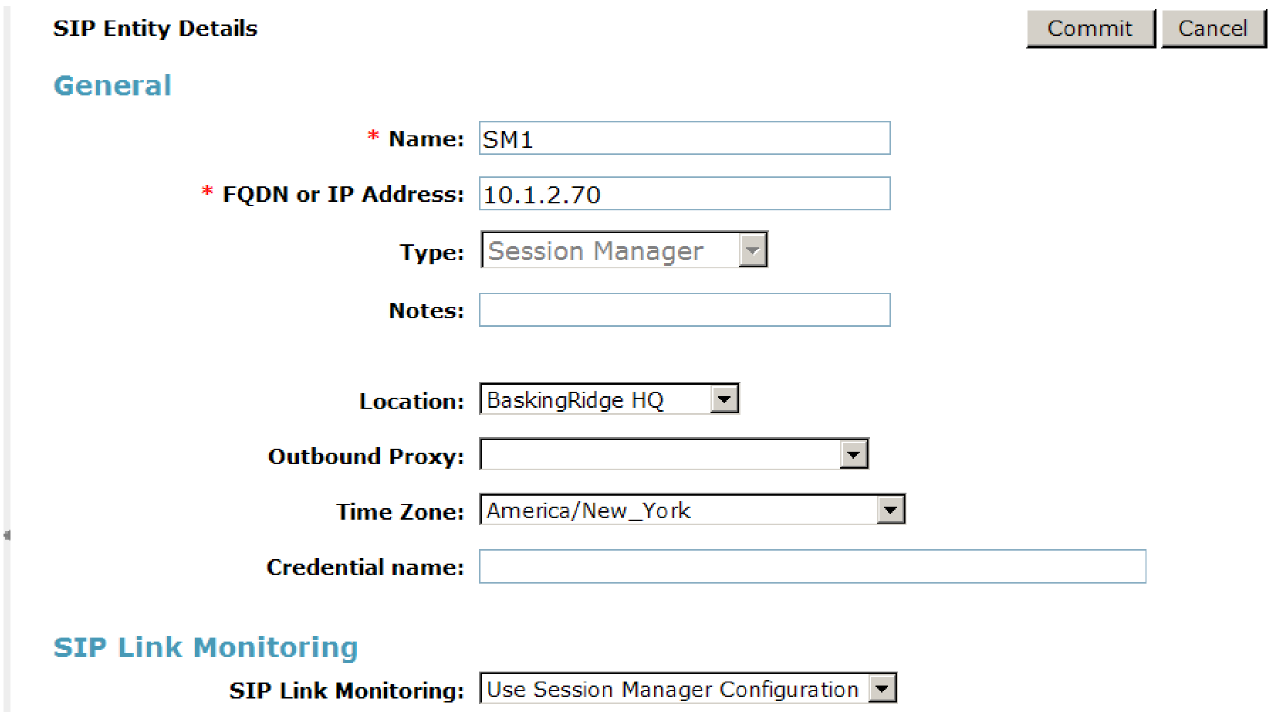


Name	Entity Links	FQDN or IP Address	Type	Notes
Acme1		65.206.67.1	Other	Inside IP Acme1
Acme2		65.206.67.21	Other	Acme2 Inside
AllanC-S8300-G350		10.32.2.80	CM	For Survivability Test
alpinemas1		135.8.139.31	Modular Messaging	For use by Tony M's group
AudioCodes M1000		m1000.avaya.com	Other	QSIG/SIP GW for CS1000
AuraSBC		65.206.67.93	Other	Avaya Aura SBC Inside IP
BR2 AudioCodes MP114		192.168.75.110	Other	SIP Media Gateway
BR2 AudioCodes MP118		192.168.75.100	Other	SIP Media Gateway
CallCenter		10.1.2.233	CM	
Cisco-UCM6		60.1.1.9	Other	
Cisco-UCM7		172.29.5.20	Other	
CiscoUCME		192.45.131.1	Other	To Interop CUCME
CM-Evolution-procr-5062		10.1.2.90	CM	CM-ES procr IP, different port
CM-Evolution-procr-5065		10.1.2.90	CM	CM-ES procr IP, different port
CM Evolution Server		10.1.2.90	CM	

The following screen shows Page 2 of the list of SIP Entities. In this screen, only the SIP Entity named "SM1" (corresponding to Session Manager) is relevant to these Application Notes.

☐	Name	Entity Links	FQDN or IP Address	Type	Notes
☐	Denver Nortel CS1000e	▸	CS1KGateway.avaya.com	Other	
☐	Juniper-SRX240	▸	1.0.0.2	Other	
☐	Microsoft-OCS-Mediation-Server	▸	135.8.19.139	SIP Trunk	MS OCS Mediation Server in WM
☐	MikeH-S8300-G450	▸	10.32.2.20	CM	For Survivability Test
☐	OITT Test Tool	▸	135.8.19.109	Other	OITT Test Tool
☐	RobertIP500	▸	10.1.2.190	SIP Trunk	Robert's IP500
☐	S8300-G250-JRWB	▸	172.28.40.5	CM	S8300-in-G250 at JRR workbench
☐	S8300-G450-BR1	▸	135.8.139.118	CM	S8300 is an LSP
☐	S87x0-Procr-CM521-VZ	▸	65.206.67.3	CM	CM 5.2.1 Verizon Testbed
☐	SM1	▸	10.1.2.70	Session Manager	

The following screen shows the upper portion of the **SIP Entity Details** corresponding to "SM1". The **FQDN or IP Address** field for "SM1" is the Session Manager Security Module IP address (10.1.2.70), 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 "BaskingRidge HQ". The default **SIP Link Monitoring** parameters may be used. Unless changed elsewhere, links from other SIP entities to this instance of Session Manager will use the default SIP Link Monitoring timers, configurable at the Session Manager level. If desired, these timers may be customized for each entity.



Scrolling down, the following screen shows the middle portion of the **SIP Entity Details**, a listing of the **Entity Links** previously configured for "SM1". The links relevant to these Application Notes are described in the following section.

Entity Links

Add | Remove

27 Items | Refresh — Filter: Enable

☐	SIP Entity 1	Protocol	Port	SIP Entity 2	Port	Trusted
☐	SM1	TCP	* 5060	Acme1	* 5060	☑
☐	SM1	TCP	* 5060	Acme2	* 5060	☑
☐	SM1	TCP	* 5060	AuraSBC	* 5060	☑
☐	SM1	TCP	* 5060	CallCenter	* 5060	☑
☐	SM1	TCP	* 5060	Cisco-UCM6	* 5060	☑
☐	SM1	TCP	* 5060	Cisco-UCM7	* 5060	☑
☐	SM1	TCP	* 5060	CiscoUCME	* 5060	☑
☐	SM1	TCP	* 5060	CM Evolution Server	* 5060	☑
☐	SM1	TCP	* 5062	CM-Evolution-procr-5062	* 5062	☑
☐	SM1	TCP	* 5060	Denver Nortel CS1000e	* 5060	☑
☐	SM1	TCP	* 5060	alpinemas1	* 5060	☑

Scrolling down, the following screen shows the lower portion of the **SIP Entity Details**, a listing of the configured ports for "SM1". In the sample configuration, TCP port 5060 was already in place for the shared test environment, using **Default Domain** "avaya.com". To enable Communication Manager to distinguish inbound calls from Verizon from other types of SIP calls arriving from the same Session Manager, TCP port 5062 was added, with default domain "adevc.avaya.globalipcom.com". Click the **Add** button to configure a new port. TCP is used in the sample configuration for improved visibility during testing; TLS may be used in production.

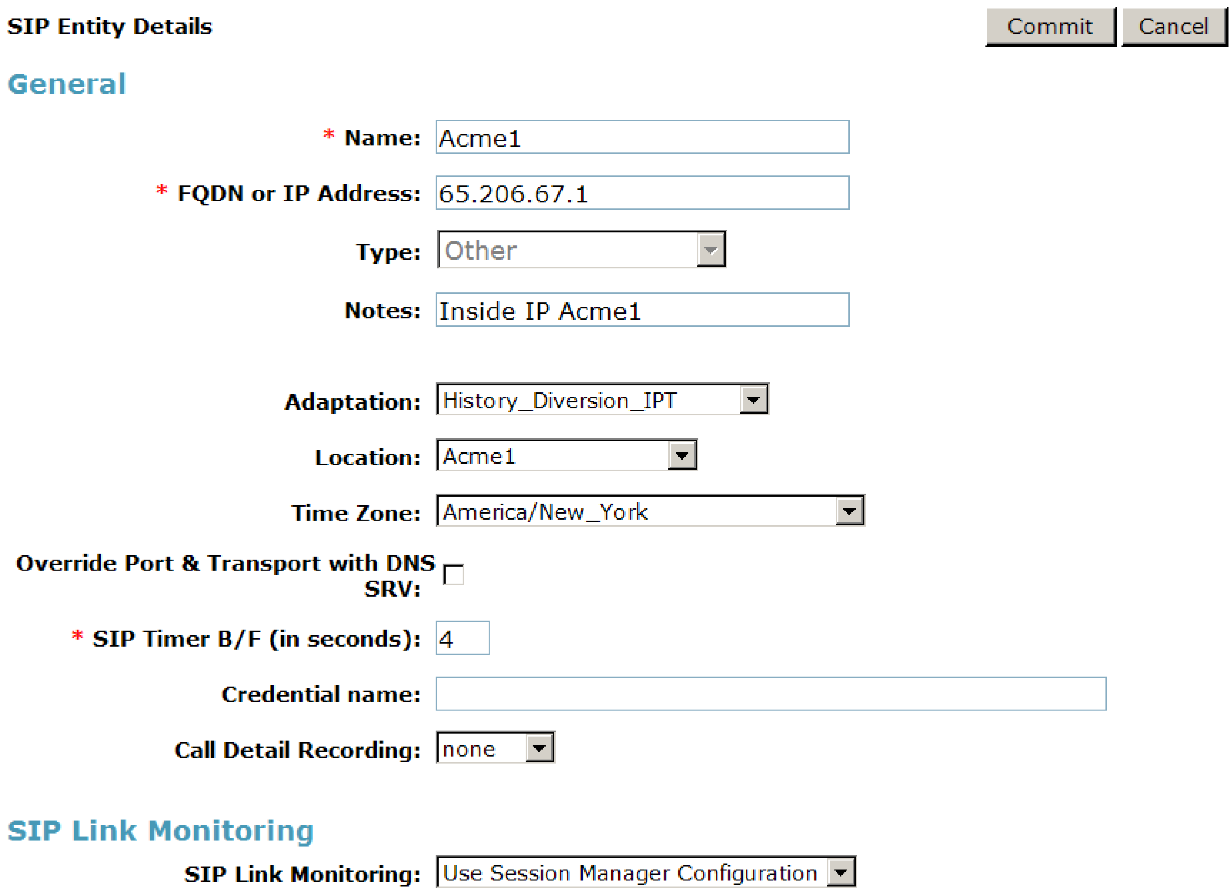
Port

Add | Remove

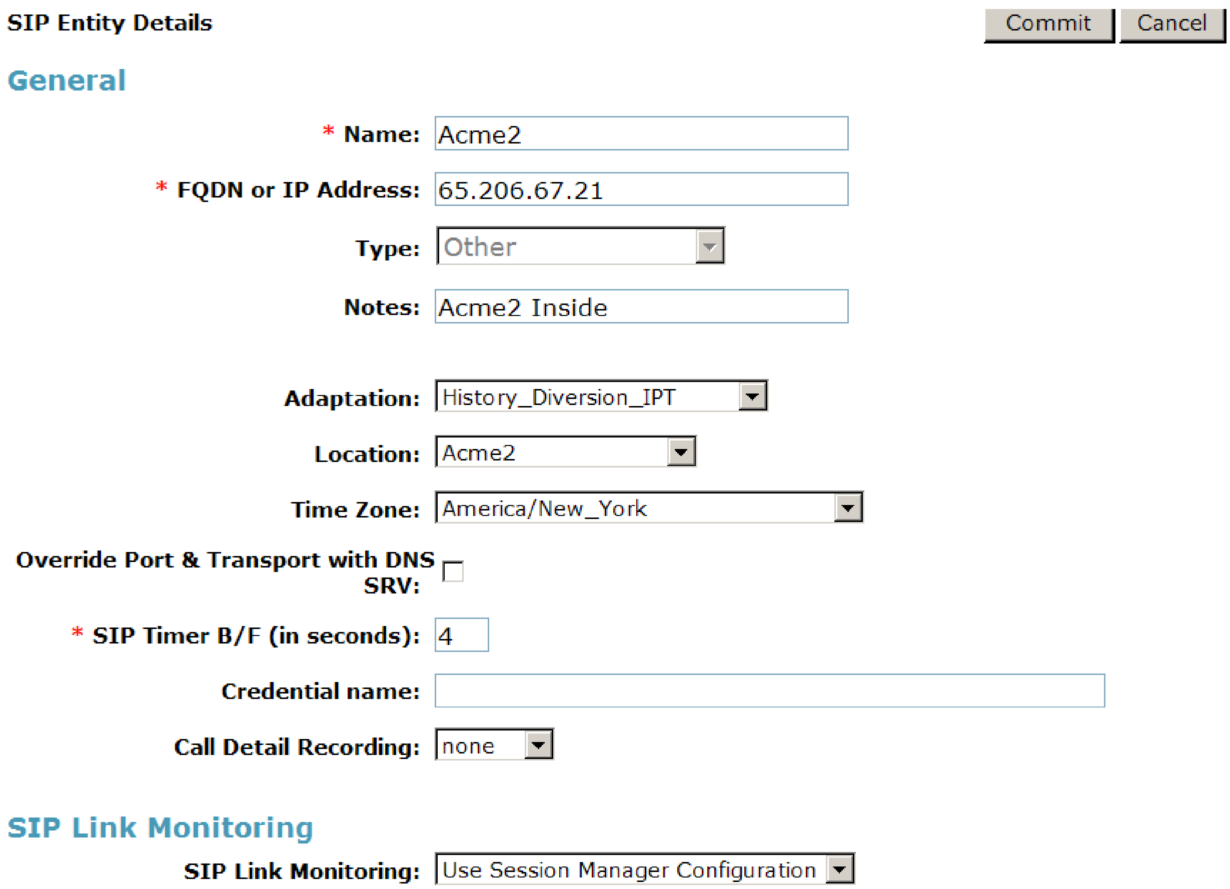
5 Items | Refresh — Filter: Enable

☐	Port	Protocol	Default Domain	Notes
☐	5060	TCP	avaya.com	
☐	5060	UDP	avaya.com	
☐	5061	TLS	avaya.com	
☐	5062	TCP	adevc.avaya.globalipcom.com	Verizon testing CPE-domain
☐	5070	TCP	avocs.contoso.com	

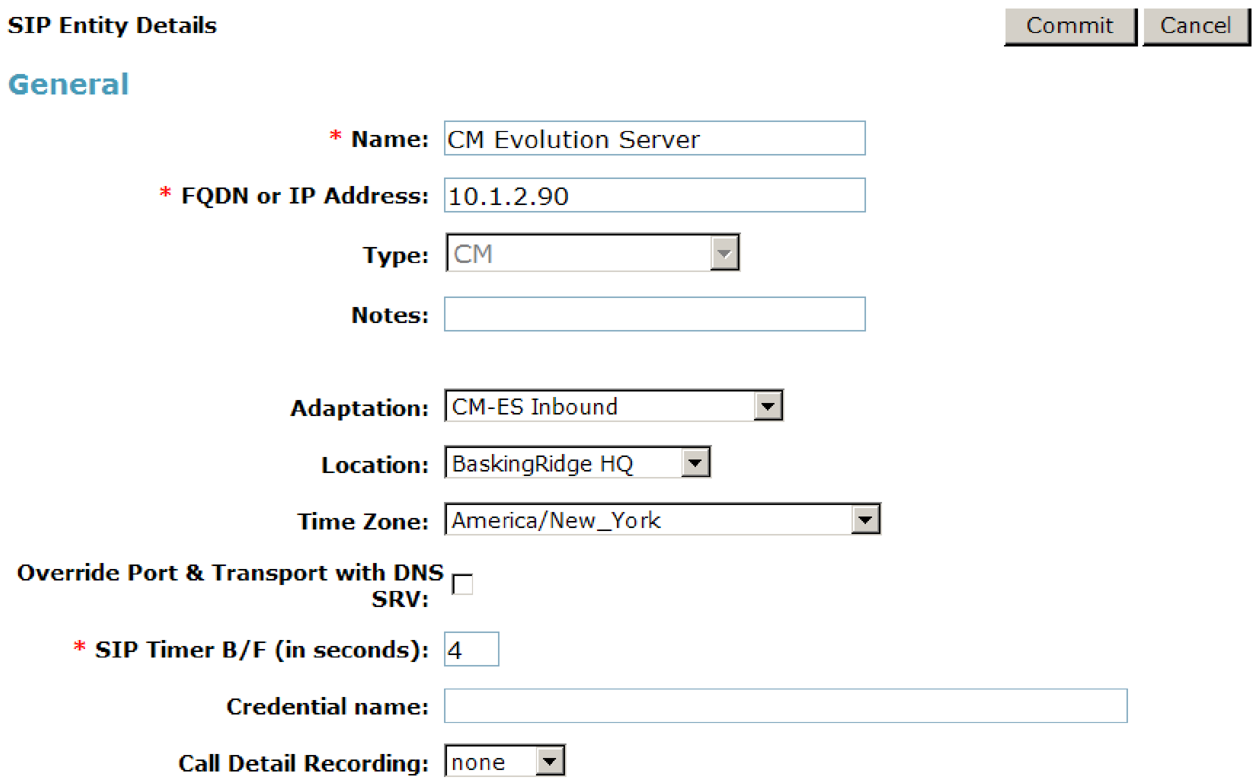
The following screen shows the **SIP Entity Details** corresponding to "Acme1". The **FQDN or IP Address** field is configured with the Acme Packet Net-Net SBC inside IP address (65.206.67.1). "Other" is selected from the **Type** drop-down menu for SBC SIP Entities. This Acme Packet Net-Net SBC has been assigned to **Location** "Acme1", and the "History_Diversion_IPT" adapter is applied. This adaptation uses the "VerizonAdapter".



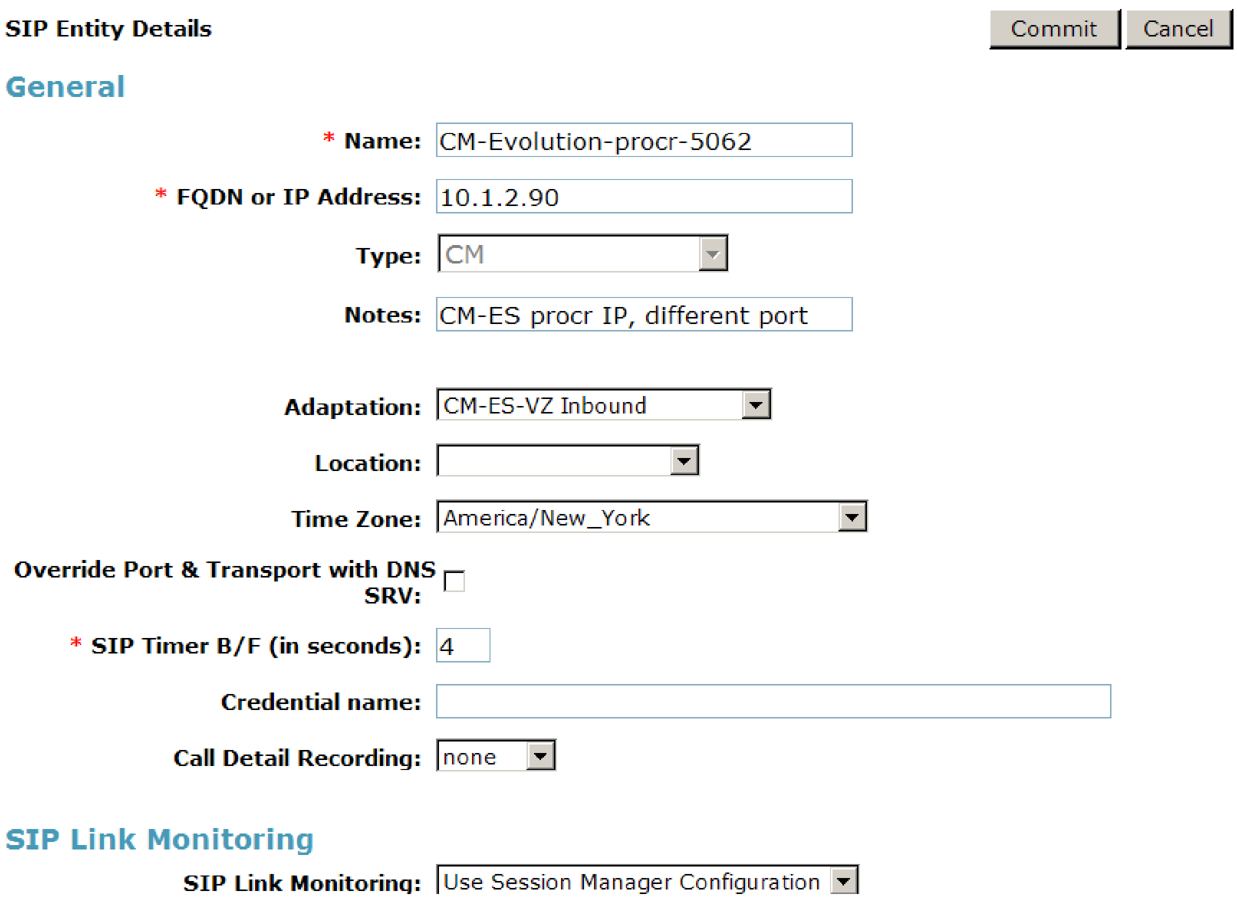
The following screen shows the **SIP Entity Details** corresponding to "Acme2". The **FQDN or IP Address** field is configured with the second Acme Packet Net-Net SBC inside IP address (65.206.67.21). "Other" is selected from the **Type** drop-down menu for SBC SIP Entities. This Acme Packet Net-Net SBC has been assigned to **Location** "Acme2", and the "History_Diversion_IPT" adapter is applied. This adaptation uses the "VerizonAdapter".



The following screen shows a portion of the **SIP Entity Details** corresponding to a Communication Manager SIP Entity named "CM Evolution Server" This is the SIP Entity that was already in place in the shared Avaya Interoperability Lab test environment, prior to adding the Verizon IP Trunk configuration. The **FQDN or IP Address** field contains the IP address of the "Processor Ethernet" (10.1.2.90). 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. In the shared test environment, the **Adaptation** "CM-ES Inbound" and **Location** "BaskingRidge HQ" had already been assigned to the Communication Manager SIP entity.



The following screen shows the **SIP Entity Details** for an entity named “CM-Evolution-procr-5062”. This entity uses the same **FQDN or IP Address** (10.1.2.90) as the prior entity with name “CM Evolution Server”; both correspond to the S8800 Processor Ethernet. Later, a unique port, 5062, will be used for the Entity Link to “CM-Evolution-procr-5062”. Using a different port is one approach that will allow Communication Manager to distinguish traffic originally from Verizon from other SIP traffic arriving from the same IP address of the Session Manager. The adapter “CM-ES-VZ Inbound” is applied to this SIP entity. Recall that this adapter is used to adapt the domain as well as map the Verizon 10 digit DID numbers to the corresponding Communication Manager extensions. If desired, a location can be assigned if location-based routing criteria will be used. In the sample configuration, no location was assigned to this entity, and “all locations” routing was used for outbound calls to Verizon.



5.5. 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 partial list of configured links. In the screen below, the links named "Acme1", "Acme2", "CM-ES-VZ-5062", and "CM Evolution Server" are relevant to these Application Notes. Each of the links uses the entity named "SM1" as **SIP Entity 1**, and the appropriate entity, such as "Acme1" or "Acme2" for **SIP Entity 2**. Note that there are two SIP Entity Links, using different TCP ports, linking the same SM1 with the Processor Ethernet of Communication Manager. For one link, named "CM Evolution Server", both entities use port 5060. For the other, named "CM-ES-VZ-5062", both entities use port 5062.

Entity Links

Edit | New | Duplicate | Delete | More Actions | Commit

27 Items | Refresh   Filter: Enable

	Name	SIP Entity 1	Protocol	Port	SIP Entity 2	Port	Trusted	Notes
☐	Acme1	SM1	TCP	5060	Acme1	5060	☑	
☐	Acme2	SM1	TCP	5060	Acme2	5060	☑	
☐	AuraSBC	SM1	TCP	5060	AuraSBC	5060	☑	
☐	Call Center	SM1	TCP	5060	CallCenter	5060	☑	
☐	Cisco-UCM6	SM1	TCP	5060	Cisco-UCM6	5060	☑	
☐	Cisco-UCM7	SM1	TCP	5060	Cisco-UCM7	5060	☑	
☐	CiscoUCME-Link	SM1	TCP	5060	CiscoUCME	5060	☑	
☐	CM-ES-VZ-5062	SM1	TCP	5062	CM-Evolution-procr-5062	5062	☑	Same IP, diff port
☐	CM Evolution Server	SM1	TCP	5060	CM Evolution Server	5060	☑	
☐	Denver CS1000e	SM1	TCP	5060	Denver Nortel CS1000e	5060	☑	

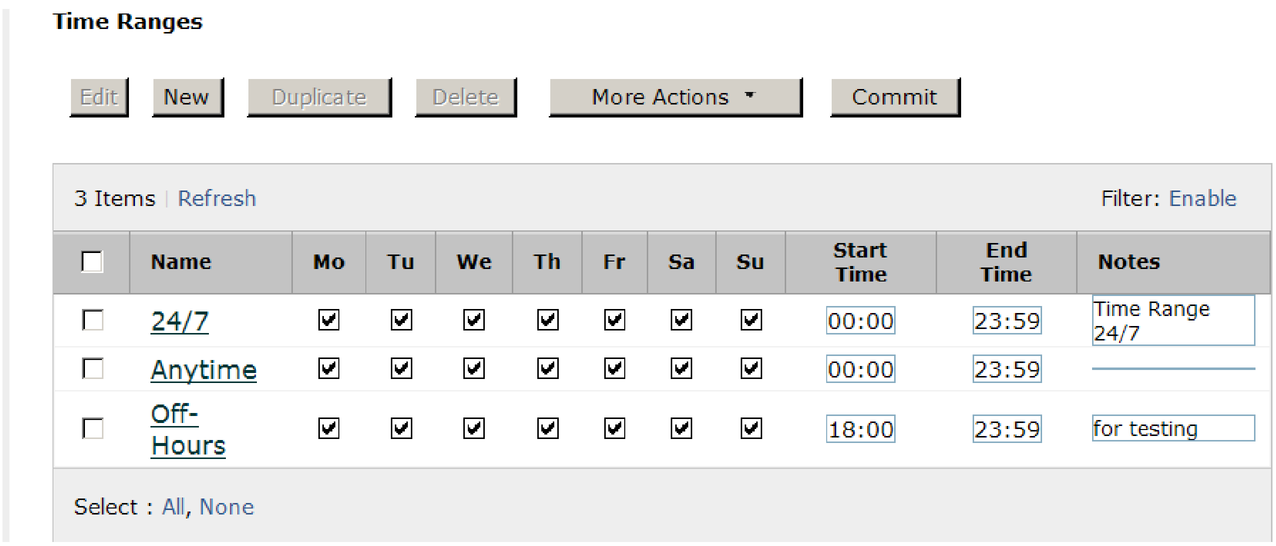
The link named "CM Evolution Server" links Session Manager "SM1" with the Communication Manager Processor Ethernet. This link existed in the shared configuration prior to adding the Verizon IP Trunk-related configuration. This link, using port 5060, can carry traffic between Session Manager and Communication Manager that is not necessarily related to calls with

Verizon, such as traffic related to SIP Telephones registered to Session Manager, or traffic related to Avaya Modular Messaging, which has SIP integration to Session Manager.

The link named "CM-ES-VZ-5062" also links Session Manager "SM1" with the Communication Manager Processor Ethernet. However, this link uses port 5062 for both entities in the link. This link was created to allow Communication Manager to distinguish calls from Verizon from other calls that arrive from the same Session Manager. Other methods of distinguishing traffic could be used, if desired. For example, in a configuration using G650 Media Gateways, the use of one or more TN799DP C-LAN interface cards can provide additional Communication Manager SIP Signaling alternatives.

5.6. Time Ranges

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

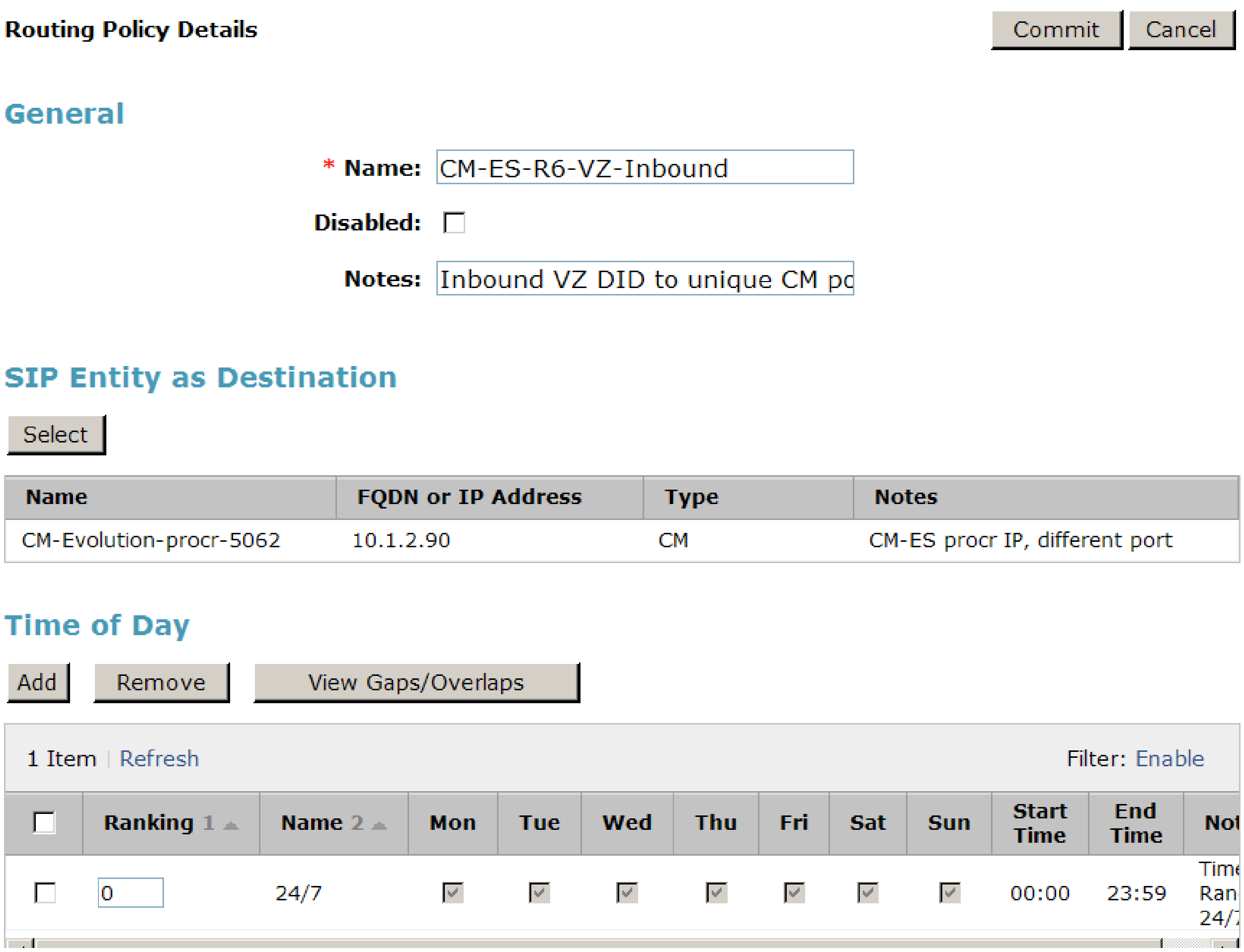


	Name	Mo	Tu	We	Th	Fr	Sa	Su	Start Time	End Time	Notes
☐	24/7	☑	☑	☑	☑	☑	☑	☑	00:00	23:59	Time Range 24/7
☐	Anytime	☑	☑	☑	☑	☑	☑	☑	00:00	23:59	
☐	Off-Hours	☑	☑	☑	☑	☑	☑	☑	18:00	23:59	for testing

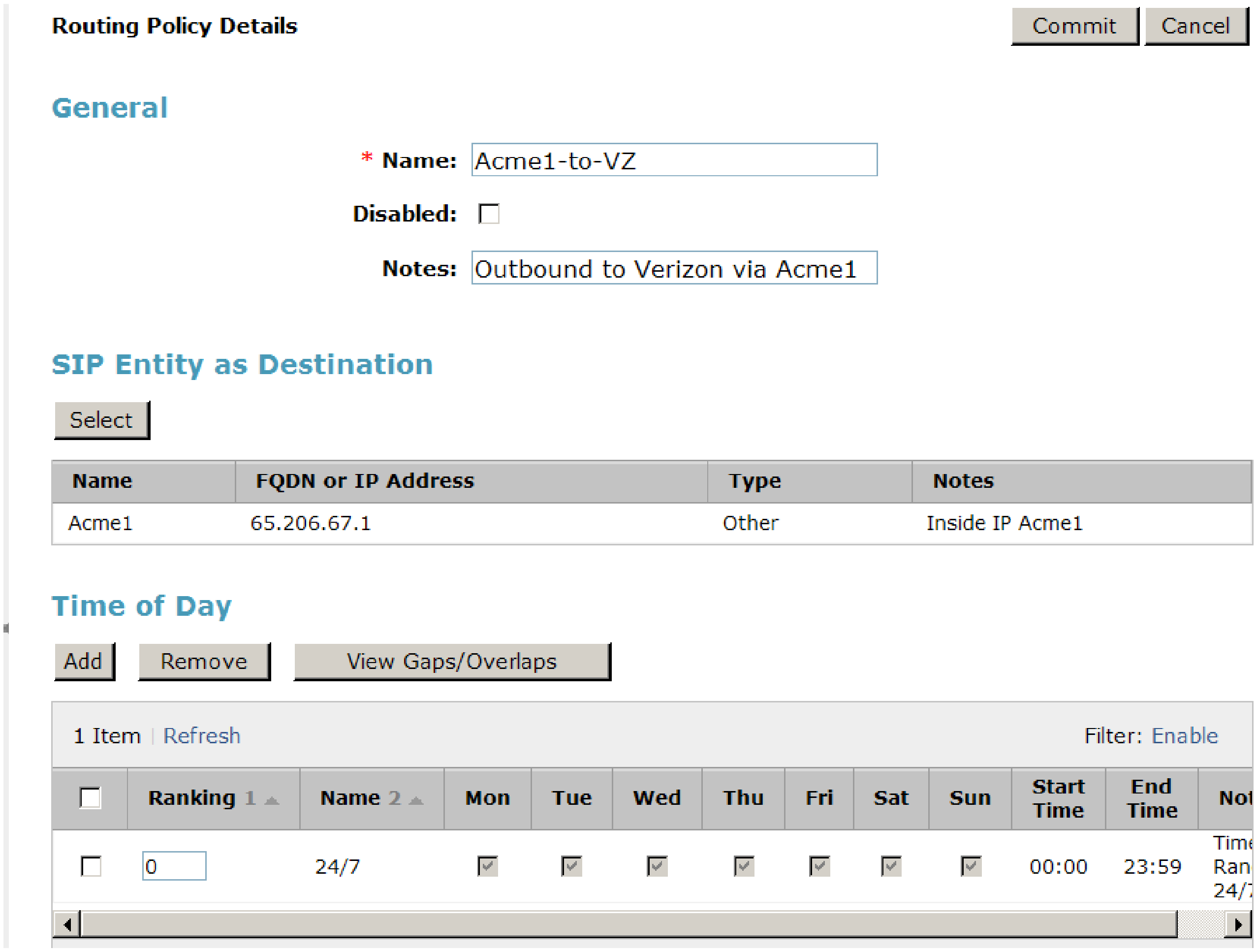
5.7. Routing Policies

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

The following screen shows the **Routing Policy Details** for the policy named "CM-ES-R6-VZ-Inbound" associated with incoming PSTN calls from Verizon to Communication Manager, using the Avaya S8800 PE. Observe the **SIP Entity as Destination** is the entity named "CM-Evolution-procr-5062".



The following screen shows the **Routing Policy Details** for the policy named “Acme1-to-VZ” associated with outgoing calls from Communication Manager to the PSTN via Verizon through Acme1. Observe the **SIP Entity as Destination** is the entity named “Acme1”. After dial patterns are assigned to use this routing policy, the lower portion of the screen will show the dial patterns using the routing policy.



The following screen shows the **Routing Policy Details** for the policy named "Acme2-to-VZ" associated with outgoing calls from Communication Manager to the PSTN via Verizon through Acme2. Observe the **SIP Entity as Destination** is the entity named "Acme2". In the **Time of Day** area, note that a **Ranking** can be configured. To allow Acme2 to receive calls from Session Manager even when Acme1 is operational, the default rank of 0 (also assigned to Acme1) can be retained.

Routing Policy Details

Commit Cancel

General

* **Name:** Acme2-to-VZ

Disabled: ☐

Notes: Out to Verizon via Acme2

SIP Entity as Destination

Select

Name	FQDN or IP Address	Type	Notes
Acme2	65.206.67.21	Other	Acme2 Inside

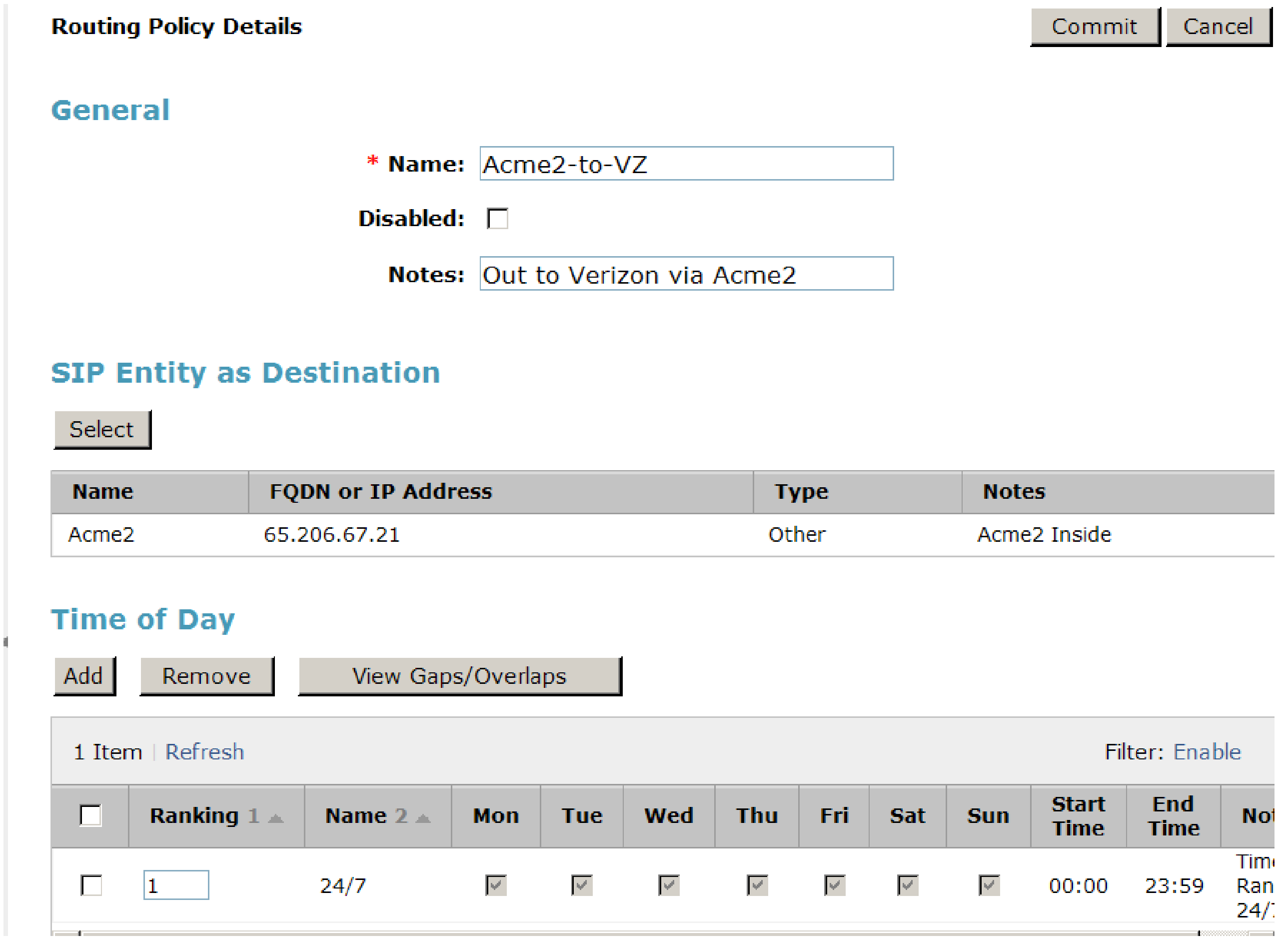
Time of Day

Add Remove View Gaps/Overlaps

1 Item | Refresh Filter: Enable

☐	Ranking 1	Name 2	Mon	Tue	Wed	Thu	Fri	Sat	Sun	Start Time	End Time	Not
☐	0	24/7	☑	☑	☑	☑	☑	☑	☑	00:00	23:59	Time Ran 24/7

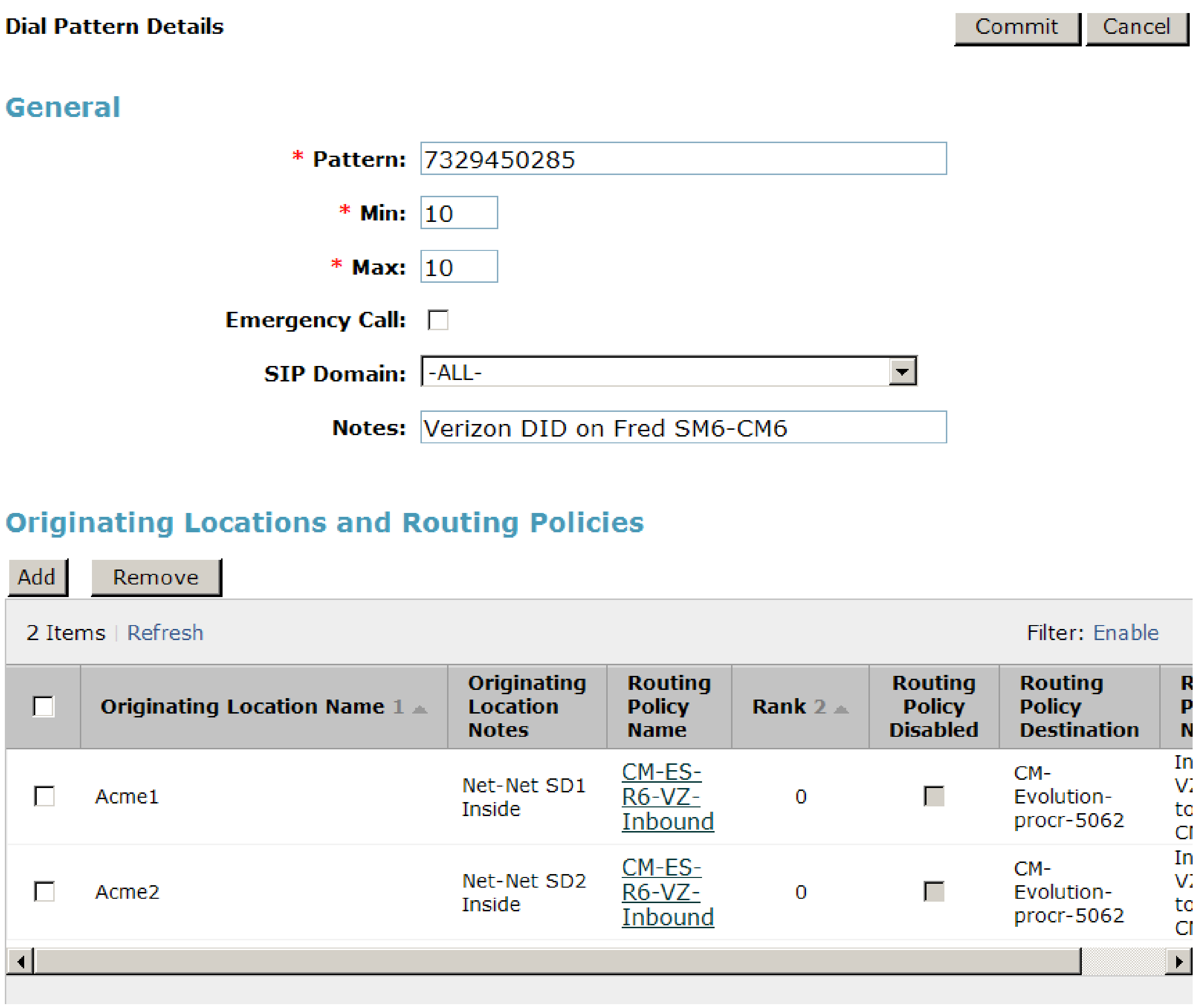
If it is intended that Acme1 should always be tried by Session Manager before Acme2, the rank of Acme2 can be changed to 1 as shown below. Both the “load sharing” approach where Acme1 and Acme2 use the same rank, and the strict rank order priority of Acme1 over Acme2 were successfully tested in the sample configuration.



5.8. Dial Patterns

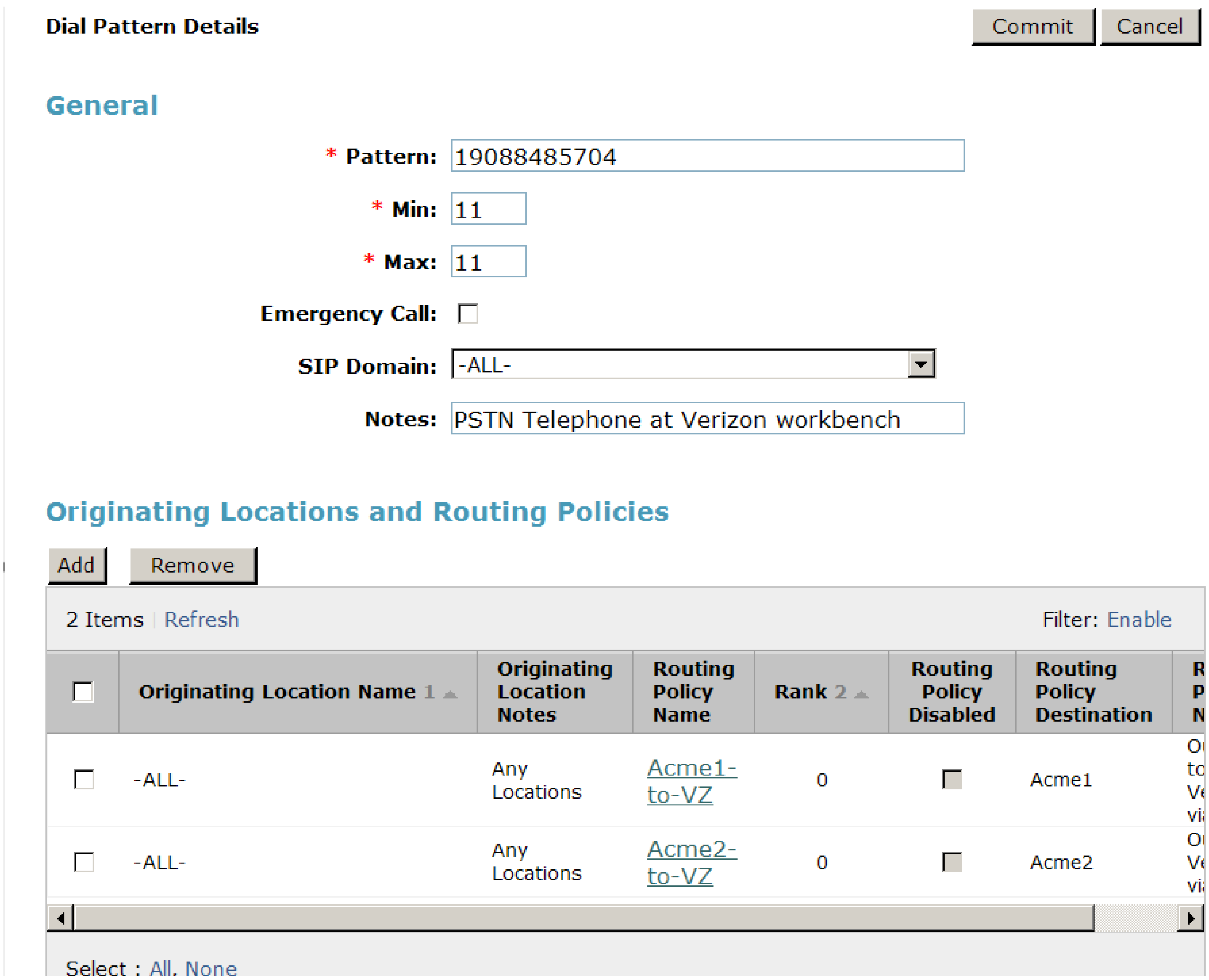
To view or change dial patterns, select **Routing → Dial Patterns**. Click on the checkbox corresponding to the name of a pattern and **Edit** to edit an existing pattern, or **New** to add a pattern. Click the **Commit** button after changes are completed.

The following screen illustrates an example dial pattern used to verify inbound PSTN calls to the enterprise via the Avaya S8800 Processor Ethernet. When a user on the PSTN dials a number assigned to the Verizon IP Trunk service, such as 732-945-0285, Verizon delivers the number to the enterprise, and the Acme Packet Net-Net SBC sends the call to Session Manager. The pattern below matches on 732-945-0285 specifically. Dial patterns can alternatively match on ranges of numbers (e.g., a DID block). Under **Originating Location and Routing Policies**, the routing policy named “CM-ES-R6-VZ-Inbound” is selected, which sends the call to Communication Manager using port 5062 as described previously. Two entries are created, one for **Originating Location Name** “Acme1” and the other for “Acme2”.

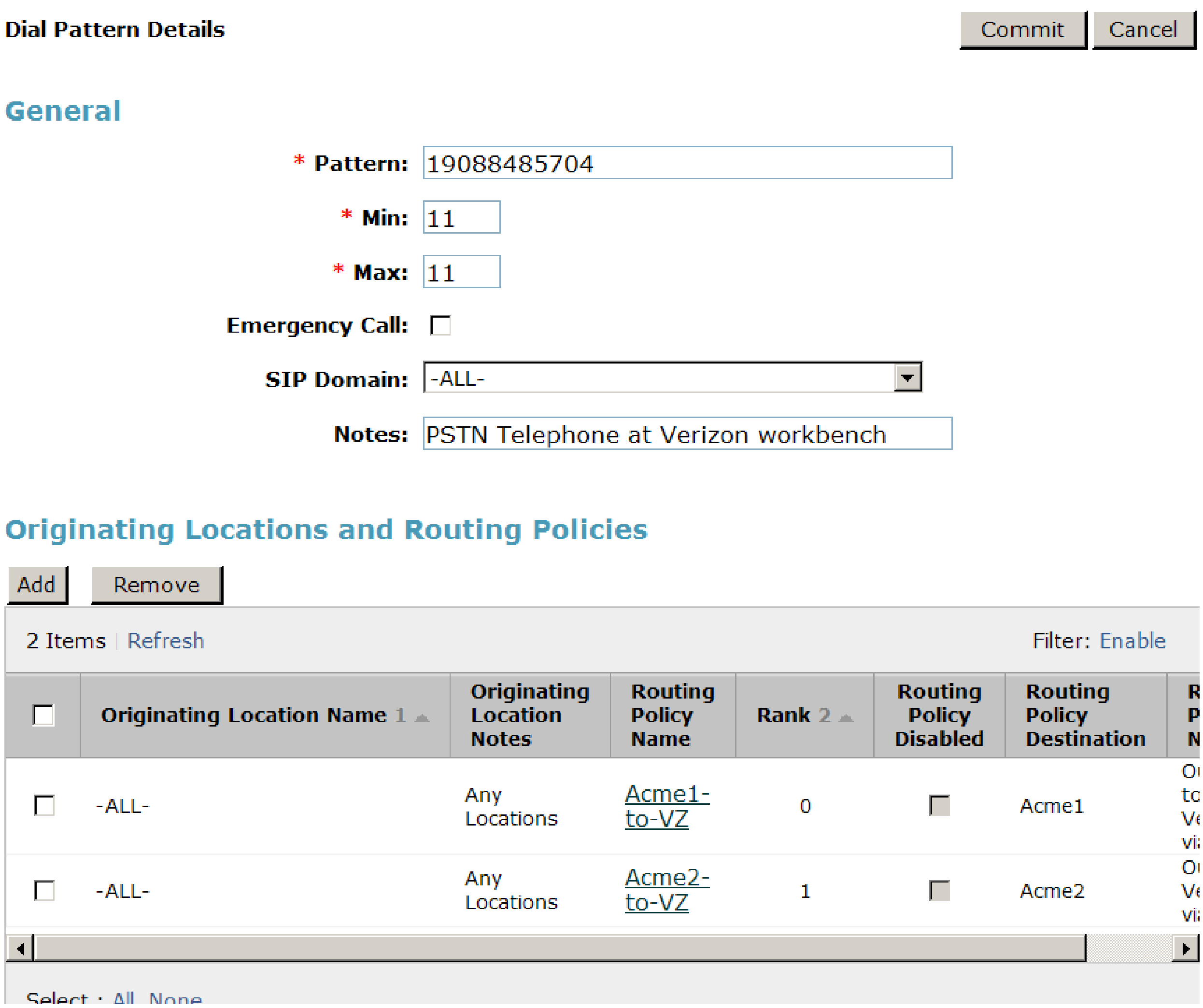


The following screen illustrates an example dial pattern used to verify outbound calls from the enterprise to the PSTN. When a Communication Manager user dials a PSTN number via ARS such as 1-908-848-5704, Communication Manager sends the call to Session Manager via the S8800 PE. Session Manager will match the dial pattern shown below and send the call to one of the Acme Packet Net-Net SBCs. If the call cannot be routed via the first Acme Packet Net-Net SBC that is tried first for a particular call, the call can automatically re-route to the other.

In the screen shown below, the routing policies for Acme1 and Acme2 have the same rank. With this configuration, some calls will use Acme1 first, and other calls will use Acme2 first (i.e., even if Acme1 is operational).



In the alternative screen shown below, the routing policy associated with Acme2 has a rank of 1. With this configuration, all calls will use Acme1 first, and only try Acme2 if the call attempt through Acme1 is unsuccessful. Session Manager can be configured to distribute the calls among the SBCs (same rank) or prefer one SBC over another (different ranks).



As mentioned previously, once Dial Patterns are configured that associate dialed numbers with routing policies, a return to the routing policy screen will list the Dial Patterns associated with the policy.

For example, the following screen shows the bottom portion of the Routing Policy Details screen for the policy named "Acme2-to-VZ" after a number of dial patterns for the testing associated with these Application Notes had been added.

☐	Pattern	Min	Max	Emergency Call	SIP Domain	Originating Location	Notes
☐	0	1	1	☐	-ALL-	-ALL-	Verizon IP Trunk Test Plan TC29
☐	0	11	11	☐	-ALL-	-ALL-	Verizon IP Trunk Test Plan TC27,TC28
☐	00	2	2	☐	-ALL-	-ALL-	Verizon IP Trunk Test Plan TC30
☐	01	12	15	☐	-ALL-	-ALL-	Verizon IP Trunk Test Plan TC31
☐	011	13	15	☐	-ALL-	-ALL-	Verizon IP Trunk Test Plan TC18
☐	1411	4	4	☐	-ALL-	-ALL-	Verizon IP Trunk Test Plan TC22
☐	17124329999	11	11	☐	-ALL-	-ALL-	Verizon Test Number for Fast Answer TC34
☐	17326870755	11	11	☐	-ALL-	-ALL-	John R Cell Phone
☐	18004337300	11	11	☐	-ALL-	-ALL-	Verizon Early Media TC59 AA Reservations
☐	18005233273	11	11	☐	-ALL-	-ALL-	Verizon IP Trunk Test Plan, TC26
☐	1900	11	11	☐	-ALL-	-ALL-	Verizon IP Trunk Test Plan TC31
☐	19088485579	11	11	☐	-ALL-	-ALL-	John R Real Number used for testing VZ
☐	19088485704	11	11	☐	-ALL-	-ALL-	PSTN Telephone at Verizon workbench
☐	1976	11	11	☐	-ALL-	-ALL-	Verizon IP Trunk Test Plan TC38
☐	411	3	3	☐	-ALL-	-ALL-	Verizon IP Trunk Test Plan TC21

Select : All, None   < Previous | Page 1 of 2 | Next >

The following screen shows Page 2.

Dial Patterns

Add   Remove

18 Items | Refresh   Filter: Enable

☐	Pattern	Min	Max	Emergency Call	SIP Domain	Originating Location	Notes
☐	511	3	3	☐	-ALL-	-ALL-	Verizon IP Trunk Test Plan TC25
☐	5551212	7	7	☐	-ALL-	-ALL-	Verizon IP Trunk Test Plan TC20
☐	711	3	3	☐	-ALL-	-ALL-	Verizon IP Trunk Test Plan TC23

Select : All, None   < Previous | Page 2 of 2 | Next >

6. Configure Acme Packet Net-Net SBCs

The Acme Packet Net-Net SBC configuration is similar to the configuration described in previously published Application Notes covering the testing of prior releases of Session Manager and Communication Manager with the same Verizon IP Trunk PIP access circuit. See reference [JF-JRR-VZIPT] for detailed configuration steps covering the Acme Packet Net-Net SBC as it relates to the outside or public interface facing the Verizon network, which has not changed.

This section focuses on new recommendations for the Acme Packet Net-Net SBC configuration due to the new releases of Session Manager and Communication Manager, or differences in the sample configuration described in these Application Notes compared with reference [JF-JRR-VZIPT]. The changes to the Acme Packet configuration documented in [JF-JRR-VZIPT] shown below should be made to both "Acme1" and "Acme2" in the 2-CPE configuration depicted in **Figure 1**.

6.1. P-Site Header Removal

Session Manager Release 6 inserts a P-Site header which contains the IP-Address of System Manager as a parameter. Since there is no value in sending this header to Verizon in the sample configuration, the header is stripped by the SBC. Calls can still be completed successfully if the configuration in this section is not performed and the P-Site header is sent to Verizon. This information is included to allow the reader to delete the P-Site header if desired so that the private IP address of System Manager is not revealed on the public side of the SBC.

In Section 5.3.11 of reference [JF-JRR-VZIPT], a SIP header manipulation named "NAT_IP" is defined and applied to the outside realm towards Verizon. This sip-manipulation contains various header rules mainly to replace inside or private IP addresses in headers with the appropriate outside or public IP addresses in the SIP messages sent to Verizon. To remove the P-Site header, an additional header rule is added to the existing NAT_IP header retained from reference [JF-JRR-VZIPT]. This new header-rule to delete the P-Site header is shown below.

```
header-rule
          name               delPsite
          header-name        P-Site
          action             delete
          comparison-type    pattern-rule
          match-value
          msg-type           request
          new-value
          methods
```

With this header rule configured and activated, the P-Site header inserted by Session Manager will not be sent to Verizon.

6.2. Diversion Header Domain Mapping

The configuration in this section is not required if the Avaya CPE domain configured in Communication Manager matches the domain configured in the Verizon network for the Avaya CPE.

Session Manager can adapt the domain in various SIP headers such as the Request-URI and P-Asserted-Identity headers. As described in these Application Notes, the Session Manager capability to adapt the domain in various headers allowed a shared Avaya Interoperability Lab configuration already configured for the CPE domain "avaya.com" to be used for Verizon IP Trunk testing, even though the Verizon IP Trunk service understood the CPE domain to be "adevc.avaya.globalipcom.com". To allow diverted calls to be processed properly in the shared configuration, the SBC was used to convert the domain in the Diversion header to the Verizon expected "adevc.avaya.globalipcom.com".

As described in Section 6.1, the "NAT_IP" sip-manipulation already present on the outside realm is a natural place to modify the domain in the Diversion header sent to Verizon for redirected calls. The new header-rule named "manipDiversion" and related element-rule "DIVERSION" are added to the NAT_IP sip-manipulation to modify the host portion of the Diversion header. As shown below, the "new-value" is changed to "adevc.avaya.globalipcom.com", the enterprise domain known to Verizon in the sample configuration.

```
header-rule
        name                    manipDiversion
        header-name             Diversion
        action                  manipulate
        comparison-type         case-sensitive
        match-value
        msg-type                request
        new-value
        methods
        element-rule
            name                    DIVERSION
            parameter-name
            type                    uri-host
            action                  replace
            match-val-type          any
            comparison-type         case-sensitive
            match-value
            new-value               adevc.avaya.globalipcom.com
```

With this changed header rule configured and activated, calls diverted to the PSTN via Verizon requiring the Diversion header are successful. Examples are inbound PSTN calls that are call forwarded to Verizon, or inbound PSTN calls to a user that has Extension to Cellular activated to a PSTN destination through Verizon.

6.3. Modular Messaging Find-Me PAI Insertion

The configuration in this section is not required unless the Modular Messaging Find-Me application will be used to direct Find-Me calls out to the PSTN via the Verizon IP Trunk service. The Modular Messaging Find-Me feature allows a subscriber to set Find-Me reach number(s). If a caller is directed to the mailbox of a Modular Messaging subscriber with Find-Me active, the caller will have the option to leave a voice message or allow Modular Messaging to try to "find" the subscriber. If the caller opts to have Modular Messaging find the subscriber, Modular Messaging generates an outbound Find-Me call to the reach number active at that time. The P-Asserted-Identity in the INVITE for this outbound find-me call generated by Modular Messaging will not necessarily contain a DID number provisioned in the Verizon network for the IP Trunk service. To allow Verizon to route the outbound find-me call, the SBC can be used to insert a PAI with a DID number provisioned for the IP Trunk service. The DID number inserted in the PAI can be the external number callers would use to reach Modular Messaging. With the new sip-manipulation in place, the call will be routed by Verizon to the Find-Me reach number, and the caller ID presented to the Find-me destination will be the Verizon DID associated with Modular Messaging (i.e., rather than the caller's information). Note that the Modular Messaging Find-Me application announces the caller's spoken name when the Find-Me call is answered, so the answering user can still identify the caller to decide whether to connect to the caller. If the user answering the Find-Me call does not opt to connect to the caller, the caller is returned to the subscriber's mailbox greeting to leave a message.

As described in Section 6.1, the "NAT_IP" sip-manipulation already present on the outside realm is a natural place to add header-rules to check for calls from Modular Messaging and create the proper PAI. The header-rule "checkUA" below will look for the presence of "Modular Messaging" in the User-Agent header of an INVITE message, and the header-rule "modPAI" will ensure a specific PAI header is sent to Verizon. In the sample configuration, the PAI sent to Verizon contains "sip:7329450287@adevc.avaya.globalipcom.com" where the number "732-945-0287" is a DID number on the Verizon IP Trunk circuit that is associated with Modular Messaging, and the host portion of the PAI is the enterprise domain known to Verizon.

```
header-rule
        name                    checkUA
        header-name             User-Agent
        action                  manipulate
        comparison-type         case-sensitive
        match-value
        msg-type                any
        new-value
        methods                 INVITE
        element-rule
                name                    checkUA
                parameter-name
                type                    header-value
                action                  store
                match-val-type          any
                comparison-type         case-sensitive
```

```
                    match-value           Modular Messaging
                    new-value
header-rule
            name                  modPAI
            header-name           P-Asserted-Identity
            action                manipulate
            comparison-type       boolean
            match-value           $checkUA.$checkUA
            msg-type              any
            new-value
            methods               INVITE
            element-rule
                    name                  modPAI
                    parameter-name
                    type                  header-value
                    action                replace
                    match-val-type        any
                    comparison-type       pattern-rule
                    match-value           .*
                    new-value             sip:7329450287@adevc.avaya.globalipcom.com
```

6.4. Session Agent for Session Manager Release 6

Conceptually, the session agent configured for Session Manager Release 6 is the same as the one configured in Section 5.3.7.2 of reference [JF-JRR-VZIPT], which defined a session agent to a prior release of Session Manager. The relevant part of the session agent configuration is included below, since the IP address of Session Manager is different in these Application Notes.

```
session-agent
      hostname                10.1.2.70
      ip-address              10.1.2.70
      port                    5060
      state                   enabled
      app-protocol            SIP
      transport-method        StaticTCP
      realm-id                INSIDE
      description             Session-Manager-R6
      allow-next-hop-lp       enabled
      loose-routing           enabled
      send-media-session      enabled
      ping-method             OPTIONS;hops=0
      ping-interval           60
      ping-send-mode          keep-alive
      options                 trans-timeouts=1
      reuse-connections       TCP
      tcp-keepalive           enabled
      tcp-reconn-interval     10
```

6.5. Session Agent Group for Session Manager Release 6

Conceptually, the session agent group "ENTERPRISE" configured for the Avaya CPE is the same as the one configured in Section 5.3.8.2 of reference [JF-JRR-VZIPT], which defined a session agent group whose destination was the session agent corresponding to a prior release of Session Manager. The relevant portion of the configuration is included here, since the IP address of the destination Session Manager is different in these Application Notes. When more than one instance of Session Manager is included in a configuration, the use of a session-group allows each of the Session Manager instances to be included in the session group. The Session Manager instance selected for a given call is based on the "strategy" parameter (e.g., "Hunt" or "RoundRobin"). In the sample configuration with only one Session Manager instance, the strategy is moot.

```
session-group
        group-name          ENTERPRISE
        state               enabled
        app-protocol        SIP
        strategy            RoundRobin
        dest                10.1.2.70
```

7. Verizon Business IP Trunk Service Offer Configuration

Information regarding Verizon Business IP Trunk service offer can be found at http://www.verizonbusiness.com/us/products/voip/trunking/ or by contacting a Verizon Business sales representative.

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

7.1. Fully Qualified Domain Name (FQDN)s

The following Fully Qualified Domain Name (FQDN)s were provided by Verizon for the sample configuration.

CPE (Avaya)	Verizon Network
adevc.avaya.globalipcom.com	*pcelban0001.avayalincroft.globalipcom.com*

8. General Test Approach and Test Results

The test approach was manual testing of inbound and outbound calls using the Verizon IP Trunk service on a production Verizon PIP access circuit, as shown in **Figure 1**. Testing was successful. Examples of the verified call scenarios are detailed in Section 9.

9. Verification Steps

This section provides example verifications of the Avaya configuration with Verizon Business Private IP (PIP) IP Trunk service. Verification scenarios for the configuration described in these Application Notes included the following:

- Inbound and outbound voice calls between telephones controlled by Communication Manager and the PSTN can be made using G.711MU and/or G.729A codecs.
- Direct IP-to-IP Media (also known as "Shuffling") when applicable.
- DTMF Tone Support
  - Outbound call to PSTN application requiring post-answer DTMF (e.g., an IVR or voice mail system)
  - Inbound call from PSTN to Avaya CPE application requiring post-answer DTMF (e.g., Avaya Modular Messaging, Avaya vector digit collection steps)
- Additional PSTN numbering plans (e.g. International, operator call types, 511, etc.)
- Verizon Business IP Trunk service 2-CPE architecture
- Hold / Retrieve with music on hold
- Call transfer using two approaches
  - REFER approach (Communication Manager Network Call Redirection flag on trunk group form set to "y")
  - INVITE approach (Communication Manager Network Call Redirection flag on trunk group form set to "n")
- Conference calls
- Modular Messaging voicemail coverage, retrieval, and Find-Me application.
- SIP Diversion Header for call redirection
  - Call Forwarding
  - EC500
- Long hold time calls

9.1. Avaya Aura™ Communication Manager Verifications

This section illustrates verifications from Communication Manager.

9.1.1 Example Incoming Call from PSTN via Verizon SIP Trunk

Incoming PSTN calls arrive from Verizon at an Acme Packet Net-Net SBC, which sends the call to Session Manager. In the sample configuration, when Acme1 is in-service, Verizon sends all inbound calls to Acme1 (i.e., not load balanced). Session Manager sends the call to Communication Manager via the entity link corresponding to the Avaya S8800 PE using port 5062. On Communication Manager, the incoming call arrives via signaling group 67 and trunk group 67.

The following edited Communication Manager ***list trace tac*** trace output shows a call incoming on trunk group 67. The PSTN telephone dialed 732-945-0285. Session Manager can map the number received from Verizon to the extension of a Communication Manager telephone (x30002), or the incoming call handling table for trunk group 67 can do the same. In the trace below, Session Manager had already mapped the Verizon DID to the Communication Manager extension.

Extension 30002 is an IP Telephone with IP address 65.206.67.11 in Region 4. Initially, the G450 Media Gateway (10.1.2.95) 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 (65.206.67.11) to the "inside" of an Acme Packet Net-Net SBC (65.206.67.1).

In Communication Manager Release 6, the tracing prints the Communication Manager release version at the start of the trace, and intersperses the SIP messaging with the Communication Manager processing.

```
list trace tac 167                                                  Page   1
                                LIST TRACE
time            data
12:59:46 TRACE STARTED 06/24/2010 CM Release String cold-00.0.345.0-18246
13:00:21 SIP<INVITE sip:30002@avaya.com:5060;transport=tcp SIP/2.0
13:00:21     active trunk-group 67 member 1  cid 0x8af
13:00:21 SIP>SIP/2.0 183 Session Progress
13:00:21     dial 30002
13:00:21     ring station    30002 cid 0x8af
13:00:21     G729A ss:off ps:20
             rgn:4 [65.206.67.11]:2250
             rgn:1 [10.1.2.95]:2054
13:00:21     G729 ss:off ps:20
             rgn:4 [65.206.67.1]:49570
             rgn:1 [10.1.2.95]:2050
13:00:21     xoip options: fax:off modem:off tty:US  uid:0x500f1
             xoip ip: [10.1.2.95]:2050
13:00:23 SIP>SIP/2.0 200 OK
13:00:23     active station    30002 cid 0x8af
13:00:23 SIP<ACK sip:30002@10.1.2.90:5062;transport=tcp SIP/2.0
13:00:23 SIP>INVITE sip:9088485704@65.206.67.1:5060;transport=tcp SIP/2.0
13:00:23 SIP<SIP/2.0 100 Trying
13:00:23 SIP<SIP/2.0 200 OK
13:00:23 SIP>ACK sip:9088485704@65.206.67.1:5060;transport=tcp SIP/2.0
13:00:23     G729A ss:off ps:20
             rgn:4 [65.206.67.1]:49570
             rgn:4 [65.206.67.11]:2250
13:00:23     G729 ss:off ps:20
             rgn:4 [65.206.67.11]:2250
             rgn:4 [65.206.67.1]:49570
```

The following screen shows **Page 2** of the output of the ***status trunk*** command pertaining to this same call. Note the signaling using port 5062 between Communication Manager and Session Manager. Note the media is "ip-direct" from the IP Telephone (65.206.67.11) to the inside IP address of Acme1 (65.206.67.1) using G.729.

```
status trunk 67/1                                              Page    2 of    3
                                CALL CONTROL SIGNALING
Near-end Signaling Loc: PROCR
  Signaling   IP Address                                    Port
   Near-end:  10.1.2.90                                   : 5062
    Far-end:  10.1.2.70                                   : 5062
 H.245 Near:
  H.245 Far:
   H.245 Signaling Loc:          H.245 Tunneled in Q.931? no

 Audio Connection Type: ip-direct     Authentication Type: None
    Near-end Audio Loc:                         Codec Type: G.729
   Audio      IP Address                                    Port
   Near-end:  65.206.67.11                                : 2250
    Far-end:  65.206.67.1                                 : 49570
```

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 is used.

```
status trunk 67/1                                              Page    3 of    3
                      SRC PORT TO DEST PORT TALKPATH
src port: T00241
T00241:TX:65.206.67.1:49570/g729/20ms
S00038:RX:65.206.67.11:2250/g729a/20ms
dst port: S00038
```

The following portion of a filtered Wireshark trace (tracing SIP messages on the private inside interface only) shows the same incoming PSTN call. In frame 159, an Acme Packet Net-Net SBC (65.206.67.1) sends an INVITE to Session Manager (10.1.2.70). In frame 163, Session Manager sends the INVITE to the S8800 PE. Observe that Session Manager has already adapted the Verizon DID to its corresponding Communication Manager extension (30002). In frame 168, Communication Manager sends a 183 Session Progress with SDP. Note that in prior releases of Communication Manager, a 180 with SDP would have been sent, but enhancements in Communication Manager Release 6 allow a 183 with SDP to be configured to be sent, as desired by Verizon. In frame 221, Communication Manager sends the 200 OK when the user answers the call. In frame 234, Communication Manager sends the INVITE to begin the process of shuffling the media paths to "ip-direct", which concludes with the ACKs in frames 255 and 256.

Filter: sip Expression... Clear Apply

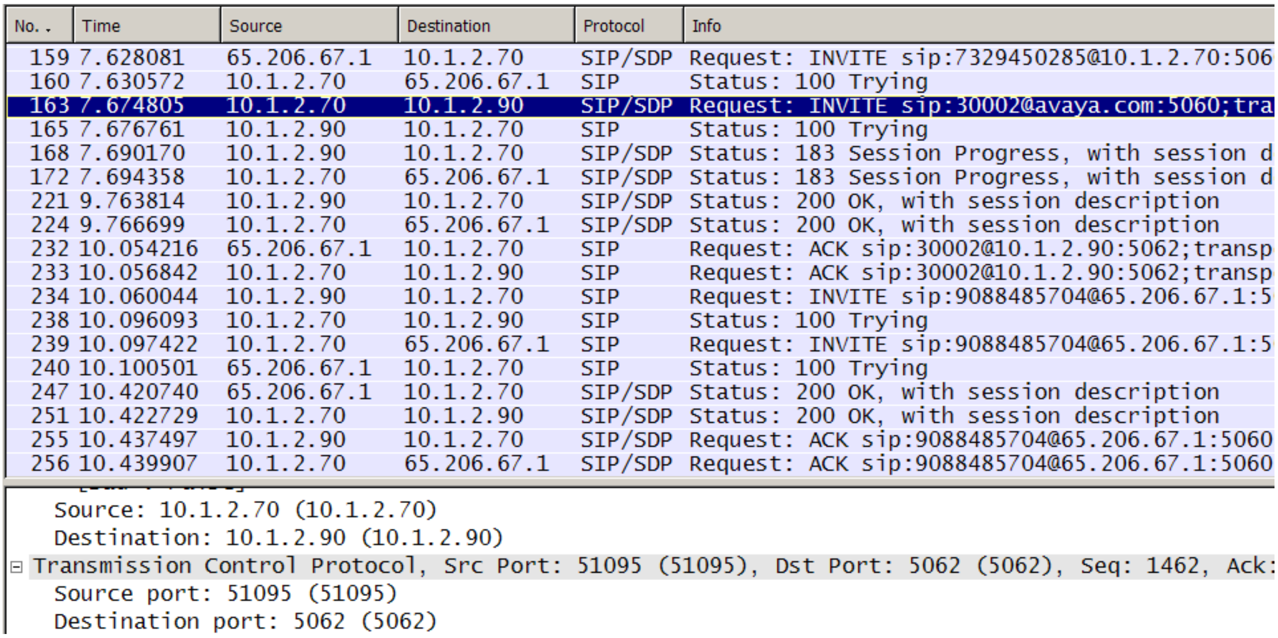
No.	Time	Source	Destination	Protocol	Info
159	7.628081	65.206.67.1	10.1.2.70	SIP/SDP	Request: INVITE sip:7329450285@10.1.2.70:506
160	7.630572	10.1.2.70	65.206.67.1	SIP	Status: 100 Trying
163	7.674805	10.1.2.70	10.1.2.90	SIP/SDP	Request: INVITE sip:30002@avaya.com:5060;tra
165	7.676761	10.1.2.90	10.1.2.70	SIP	Status: 100 Trying
168	7.690170	10.1.2.90	10.1.2.70	SIP/SDP	Status: 183 Session Progress, with session d
172	7.694358	10.1.2.70	65.206.67.1	SIP/SDP	Status: 183 Session Progress, with session d
221	9.763814	10.1.2.90	10.1.2.70	SIP/SDP	Status: 200 OK, with session description
224	9.766699	10.1.2.70	65.206.67.1	SIP/SDP	Status: 200 OK, with session description
232	10.054216	65.206.67.1	10.1.2.70	SIP	Request: ACK sip:30002@10.1.2.90:5062;transp
233	10.056842	10.1.2.70	10.1.2.90	SIP	Request: ACK sip:30002@10.1.2.90:5062;transp
234	10.060044	10.1.2.90	10.1.2.70	SIP	Request: INVITE sip:9088485704@65.206.67.1:5
238	10.096093	10.1.2.70	10.1.2.90	SIP	Status: 100 Trying
239	10.097422	10.1.2.70	65.206.67.1	SIP	Request: INVITE sip:9088485704@65.206.67.1:5
240	10.100501	65.206.67.1	10.1.2.70	SIP	Status: 100 Trying
247	10.420740	65.206.67.1	10.1.2.70	SIP/SDP	Status: 200 OK, with session description
251	10.422729	10.1.2.70	10.1.2.90	SIP/SDP	Status: 200 OK, with session description
255	10.437497	10.1.2.90	10.1.2.70	SIP/SDP	Request: ACK sip:9088485704@65.206.67.1:5060
256	10.439907	10.1.2.70	65.206.67.1	SIP/SDP	Request: ACK sip:9088485704@65.206.67.1:5060

The following portion of the same filtered Wireshark trace shows frame 168 expanded to illustrate the SDP in the 183 Session Progress from Communication Manager. In the sample configuration, ip-codec-set 4 is chosen and the preferred codec that matches a Verizon supported codec is G.729a, as shown in the trace.

No.	Time	Source	Destination	Protocol	Info
159	7.628081	65.206.67.1	10.1.2.70	SIP/SDP	Request: INVITE sip:7329450285@10.1.2.70:506
160	7.630572	10.1.2.70	65.206.67.1	SIP	Status: 100 Trying
163	7.674805	10.1.2.70	10.1.2.90	SIP/SDP	Request: INVITE sip:30002@avaya.com:5060;tra
165	7.676761	10.1.2.90	10.1.2.70	SIP	Status: 100 Trying
168	7.690170	10.1.2.90	10.1.2.70	SIP/SDP	Status: 183 Session Progress, with session d
172	7.694358	10.1.2.70	65.206.67.1	SIP/SDP	Status: 183 Session Progress, with session d
221	9.763814	10.1.2.90	10.1.2.70	SIP/SDP	Status: 200 OK, with session description
224	9.766699	10.1.2.70	65.206.67.1	SIP/SDP	Status: 200 OK, with session description
232	10.054216	65.206.67.1	10.1.2.70	SIP	Request: ACK sip:30002@10.1.2.90:5062;transp
233	10.056842	10.1.2.70	10.1.2.90	SIP	Request: ACK sip:30002@10.1.2.90:5062;transp
234	10.060044	10.1.2.90	10.1.2.70	SIP	Request: INVITE sip:9088485704@65.206.67.1:5
238	10.096093	10.1.2.70	10.1.2.90	SIP	Status: 100 Trying
239	10.097422	10.1.2.70	65.206.67.1	SIP	Request: INVITE sip:9088485704@65.206.67.1:5
240	10.100501	65.206.67.1	10.1.2.70	SIP	Status: 100 Trying
247	10.420740	65.206.67.1	10.1.2.70	SIP/SDP	Status: 200 OK, with session description
251	10.422729	10.1.2.70	10.1.2.90	SIP/SDP	Status: 200 OK, with session description
255	10.437497	10.1.2.90	10.1.2.70	SIP/SDP	Request: ACK sip:9088485704@65.206.67.1:5060
256	10.439907	10.1.2.70	65.206.67.1	SIP/SDP	Request: ACK sip:9088485704@65.206.67.1:5060

```
⊟ Media Description, name and address (m): audio 2050 RTP/AVP 18 101
    Media Type: audio
    Media Port: 2050
    Media Protocol: RTP/AVP
    Media Format: ITU-T G.729
    Media Format: DynamicRTP-Type-101
⊟ Media Attribute (a): rtpmap:18 G729/8000
    Media Attribute Fieldname: rtpmap
    Media Format: 18
    MIME Type: G729
    Sample Rate: 8000
⊟ Media Attribute (a): fmtp:18 annexb=no
    Media Attribute Fieldname: fmtp
    Media Format: 18 [G729]
    Media format specific parameters: annexb=no
```

The following portion of the same filtered Wireshark trace shows the INVITE in frame 163 expanded to illustrate the use of destination port 5062 on the S8800 PE (10.1.2.90) of Communication Manager. Communication Manager can apply Verizon-appropriate behaviors, such as the use of 183 with SDP rather than 180 with SDP, since it can distinguish that the call is inbound from Verizon by the use of port 5062 (i.e., arriving from the same Session Manager as other non-Verizon traffic).



No.	Time	Source	Destination	Protocol	Info
159	7.628081	65.206.67.1	10.1.2.70	SIP/SDP	Request: INVITE sip:7329450285@10.1.2.70:506
160	7.630572	10.1.2.70	65.206.67.1	SIP	Status: 100 Trying
163	7.674805	10.1.2.70	10.1.2.90	SIP/SDP	Request: INVITE sip:30002@avaya.com:5060;tra
165	7.676761	10.1.2.90	10.1.2.70	SIP	Status: 100 Trying
168	7.690170	10.1.2.90	10.1.2.70	SIP/SDP	Status: 183 Session Progress, with session d
172	7.694358	10.1.2.70	65.206.67.1	SIP/SDP	Status: 183 Session Progress, with session d
221	9.763814	10.1.2.90	10.1.2.70	SIP/SDP	Status: 200 OK, with session description
224	9.766699	10.1.2.70	65.206.67.1	SIP/SDP	Status: 200 OK, with session description
232	10.054216	65.206.67.1	10.1.2.70	SIP	Request: ACK sip:30002@10.1.2.90:5062;transp
233	10.056842	10.1.2.70	10.1.2.90	SIP	Request: ACK sip:30002@10.1.2.90:5062;transp
234	10.060044	10.1.2.90	10.1.2.70	SIP	Request: INVITE sip:9088485704@65.206.67.1:5
238	10.096093	10.1.2.70	10.1.2.90	SIP	Status: 100 Trying
239	10.097422	10.1.2.70	65.206.67.1	SIP	Request: INVITE sip:9088485704@65.206.67.1:5
240	10.100501	65.206.67.1	10.1.2.70	SIP	Status: 100 Trying
247	10.420740	65.206.67.1	10.1.2.70	SIP/SDP	Status: 200 OK, with session description
251	10.422729	10.1.2.70	10.1.2.90	SIP/SDP	Status: 200 OK, with session description
255	10.437497	10.1.2.90	10.1.2.70	SIP/SDP	Request: ACK sip:9088485704@65.206.67.1:5060
256	10.439907	10.1.2.70	65.206.67.1	SIP/SDP	Request: ACK sip:9088485704@65.206.67.1:5060

```
    Source: 10.1.2.70 (10.1.2.70)
    Destination: 10.1.2.90 (10.1.2.90)
⊟ Transmission Control Protocol, Src Port: 51095 (51095), Dst Port: 5062 (5062), Seq: 1462, Ack:
    Source port: 51095 (51095)
    Destination port: 5062 (5062)
```

9.1.2 Example Outgoing Calls to PSTN via Verizon IP Trunk

Depending on Session Manager configuration of the "rank" for the routing policies as shown in Section 5.7, outbound calls can either use Acme1 preferentially or distribute calls across Acme1 and Acme2. At the time of the following trace, Session Manager was configured such that both Acme1 and Acme2 had the same "rank" and for this particular call, Acme2 was used. Outbound calls using Acme1 look similar and will not be repeated here.

The following edited trace shows an outbound ARS call from IP Telephone x30002 to the PSTN number 9-1-908-848-5704. The call is routed to route pattern 68 and trunk group 68. The call initially uses the gateway (10.1.2.95), but after the call is answered, the call is "shuffled" to become an "ip-direct" connection between the IP Telephone (65.206.67.11) and the "inside" of the Acme Packet Net-Net SBC (65.206.67.21).

```
list trace tac 168                                                   Page   1
                                LIST TRACE
time            data
12:52:32 TRACE STARTED 06/24/2010 CM Release String cold-00.0.345.0-18246
12:52:39     Calling party station    30002 cid 0x8ad
12:52:39     Calling Number & Name 30002 Joey Votto
12:52:39     dial 919088485704 route:PREFIX|HNPA|ARS
12:52:39     term trunk-group 68    cid 0x8ad
12:52:39     dial 919088485704 route:PREFIX|HNPA|ARS
12:52:39     route-pattern  68 preference 1  cid 0x8ad
12:52:39     seize trunk-group 68 member 1  cid 0x8ad
12:52:39     Calling Number & Name NO-CPNumber NO-CPName
12:52:39 SIP>INVITE sip:19088485704@pcelban0001.avayalincroft.gl
12:52:39 SIP>obalipcom.com SIP/2.0
12:52:39     Setup digits 19088485704
12:52:39     Calling Number & Name 30002 Joey Votto
12:52:39 SIP<SIP/2.0 100 Trying
12:52:39     Proceed trunk-group 68 member 1  cid 0x8ad
12:52:40 SIP<SIP/2.0 183 Session Progress
12:52:40     G729 ss:off ps:20
             rgn:4 [65.206.67.21]:49552
             rgn:1 [10.1.2.95]:2054
12:52:40     xoip options: fax:off modem:off tty:US  uid:0x500e7
             xoip ip: [10.1.2.95]:2054
12:52:46 SIP<SIP/2.0 200 OK
12:52:46 SIP>ACK sip:19088485704@65.206.67.21:5060;transport=tcp SIP/2.0
12:52:46     active trunk-group 68 member 1  cid 0x8ad
12:52:46 SIP>INVITE sip:19088485704@65.206.67.21:5060;transport=tcp SIP/2.0
12:52:46 SIP<SIP/2.0 100 Trying
12:52:47 SIP<SIP/2.0 200 OK
12:52:47     G729 ss:off ps:20
             rgn:4 [65.206.67.11]:2250
             rgn:4 [65.206.67.21]:49552
12:52:47 SIP>ACK sip:19088485704@65.206.67.21:5060;transport=tcp SIP/2.0
12:52:47     G729A ss:off ps:20
             rgn:4 [65.206.67.21]:49552
             rgn:4 [65.206.67.11]:2250
```

The following screen shows **Page 2** of the output of the ***status trunk*** command pertaining to this same call. Note the media is "ip-direct" from the IP Telephone (65.206.67.11) to the inside IP address of Acme2 (65.206.67.21) using G.729.

```
status trunk 68/1                                             Page   2 of   3
                                CALL CONTROL SIGNALING
Near-end Signaling Loc: PROCR
  Signaling   IP Address                              Port
   Near-end:  10.1.2.90                             : 5062
    Far-end:  10.1.2.70                             : 5062
 H.245 Near:
  H.245 Far:
   H.245 Signaling Loc:          H.245 Tunneled in Q.931? no

 Audio Connection Type: ip-direct     Authentication Type: None
    Near-end Audio Loc:                        Codec Type: G.729
   Audio      IP Address                              Port
   Near-end:  65.206.67.11                          : 2250
    Far-end:  65.206.67.21                          : 49552
```

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 is used.

```
status trunk 68/1                                           Page   3 of   3
                      SRC PORT TO DEST PORT TALKPATH
src port: T00231
T00231:TX:65.206.67.21:49552/g729/20ms
S00038:RX:65.206.67.11:2250/g729a/20ms
dst port: S00038
```

The following portion of a filtered Wireshark trace (tracing the private or inside network only) shows the same outgoing call to Verizon. In frame 267, Communication Manager uses the S8800 PE to send an INVITE to Session Manager. This frame is selected so that it is evident from the center pane that destination port 5062 was used. In frame 271, Session Manager sends the INVITE to the Acme Packet Net-Net SBC “Acme2”. The call proceeds with 100 Trying, 183 Session Progress, and 200 OK upon answer by the PSTN phone. In frame 440, Communication Manager sends an INVITE to begin the shuffling process, which concludes with the ACKs in frames 454 and 455.

Filter: sip   Expression... Clear Apply

No.	Time	Source	Destination	Protocol	Info
267	9.266559	10.1.2.90	10.1.2.70	SIP/SDP	Request: INVITE sip:19088485704@pcelban0001.
269	9.269097	10.1.2.70	10.1.2.90	SIP	Status: 100 Trying
271	9.272414	10.1.2.70	65.206.67.21	SIP/SDP	Request: INVITE sip:19088485704@pcelban0001.
272	9.277452	65.206.67.21	10.1.2.70	SIP	Status: 100 Trying
309	10.956509	65.206.67.21	10.1.2.70	SIP/SDP	Status: 183 Session Progress, with session d
311	10.958998	10.1.2.70	10.1.2.90	SIP/SDP	Status: 183 Session Progress, with session d
430	16.889076	65.206.67.21	10.1.2.70	SIP/SDP	Status: 200 OK, with session description
432	16.892003	10.1.2.70	10.1.2.90	SIP/SDP	Status: 200 OK, with session description
434	16.894897	10.1.2.90	10.1.2.70	SIP	Request: ACK sip:19088485704@65.206.67.21:50
435	16.912736	10.1.2.70	65.206.67.21	SIP	Request: ACK sip:19088485704@65.206.67.21:50
440	16.987411	10.1.2.90	10.1.2.70	SIP	Request: INVITE sip:19088485704@65.206.67.21
443	16.989559	10.1.2.70	10.1.2.90	SIP	Status: 100 Trying
444	16.990806	10.1.2.70	65.206.67.21	SIP	Request: INVITE sip:19088485704@65.206.67.21
451	17.297347	65.206.67.21	10.1.2.70	SIP/SDP	Status: 200 OK, with session description
452	17.299186	10.1.2.70	10.1.2.90	SIP/SDP	Status: 200 OK, with session description
454	17.314252	10.1.2.90	10.1.2.70	SIP/SDP	Request: ACK sip:19088485704@65.206.67.21:50
455	17.316509	10.1.2.70	65.206.67.21	SIP/SDP	Request: ACK sip:19088485704@65.206.67.21:50

```
    Source: 10.1.2.90 (10.1.2.90)
    Destination: 10.1.2.70 (10.1.2.70)
⊟ Transmission Control Protocol, Src Port: 30389 (30389), Dst Port: 5062 (5062), Seq: 1, Ack: 2,
```

The following portion of the same filtered Wireshark trace shows frame 271 selected and expanded so that the contents of the PAI can be observed. In the selected row, observe that the Request URI contains the Verizon domain “pcelban0001.avayalincroft.globalipcom.com”. In the details in the center, observe that the PAI contains the enterprise FQDN known to Verizon, “adevc.avaya.globalipcom.com”. A Session Manager Adaptation has ensured that these domains expected by Verizon are present.

No. .	Time	Source	Destination	Protocol	Info
267	9.266559	10.1.2.90	10.1.2.70	SIP/SDP	Request: INVITE sip:19088485704@pcelban0001.
269	9.269097	10.1.2.70	10.1.2.90	SIP	Status: 100 Trying
271	9.272414	10.1.2.70	65.206.67.21	SIP/SDP	Request: INVITE sip:19088485704@pcelban0001.
272	9.277452	65.206.67.21	10.1.2.70	SIP	Status: 100 Trying
309	10.956509	65.206.67.21	10.1.2.70	SIP/SDP	Status: 183 Session Progress, with session d
311	10.958998	10.1.2.70	10.1.2.90	SIP/SDP	Status: 183 Session Progress, with session d
430	16.889076	65.206.67.21	10.1.2.70	SIP/SDP	Status: 200 OK, with session description
432	16.892003	10.1.2.70	10.1.2.90	SIP/SDP	Status: 200 OK, with session description
434	16.894897	10.1.2.90	10.1.2.70	SIP	Request: ACK sip:19088485704@65.206.67.21:50
435	16.912736	10.1.2.70	65.206.67.21	SIP	Request: ACK sip:19088485704@65.206.67.21:50
440	16.987411	10.1.2.90	10.1.2.70	SIP	Request: INVITE sip:19088485704@65.206.67.21
443	16.989559	10.1.2.70	10.1.2.90	SIP	Status: 100 Trying
444	16.990806	10.1.2.70	65.206.67.21	SIP	Request: INVITE sip:19088485704@65.206.67.21
451	17.297347	65.206.67.21	10.1.2.70	SIP/SDP	Status: 200 OK, with session description
452	17.299186	10.1.2.70	10.1.2.90	SIP/SDP	Status: 200 OK, with session description
454	17.314252	10.1.2.90	10.1.2.70	SIP/SDP	Request: ACK sip:19088485704@65.206.67.21:50
455	17.316509	10.1.2.70	65.206.67.21	SIP/SDP	Request: ACK sip:19088485704@65.206.67.21:50

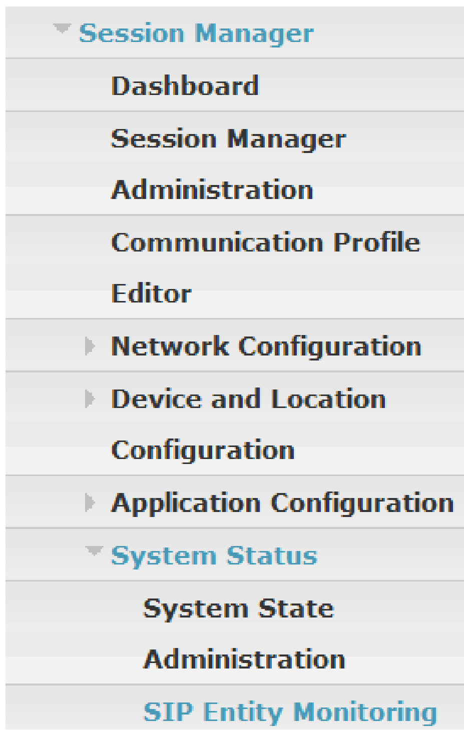
```
⊟ P-Asserted-Identity: "Joey Votto" <sip:7329450285@adevc.avaya.globalipcom.com>
    SIP Display info: "Joey Votto"
  ⊟ SIP PAI Address: sip:7329450285@adevc.avaya.globalipcom.com
      SIP PAI User Part: 7329450285
      SIP PAI Host Part: adevc.avaya.globalipcom.com
```

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

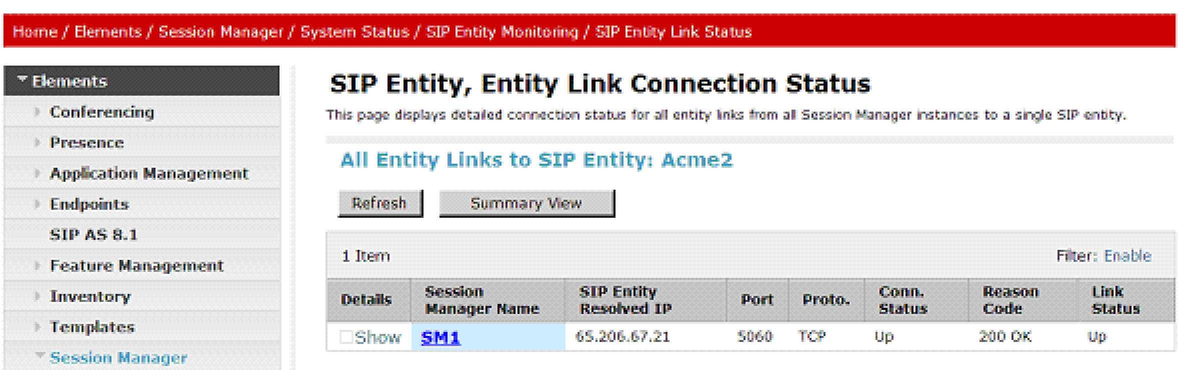
This section contains verification steps that may be performed using System Manager for Session Manager.

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.



From the list of monitored entities, select an entity of interest, such as "Acme2". Under normal operating conditions, the **Link Status** should be "Up" as shown in the example screen below.



Return to the list of monitored entities, and select another entity of interest, such as “Acme1”. Under normal operating conditions, the **Link Status** should be “Up” as shown in the example screen below.

All Entity Links to SIP Entity: Acme1

Refresh | Summary View

1 Item — Filter: Enable

Details	Session Manager Name	SIP Entity Resolved IP	Port	Proto.	Conn. Status	Reason Code	Link Status
Show	SM1	65.206.67.1	5060	TCP	Up	200 OK	Up

Return to the list of monitored entities, and select another entity of interest, such as “CM-Evolution-procr-5062”. Under normal operating conditions, the **Link Status** should be “Up” as shown in the example screen below. In this case, “Show” under **Details** was selected to view additional information. Note the use of port 5062.

SIP Entity, Entity Link Connection Status

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

All Entity Links to SIP Entity: CM-Evolution-procr-5062

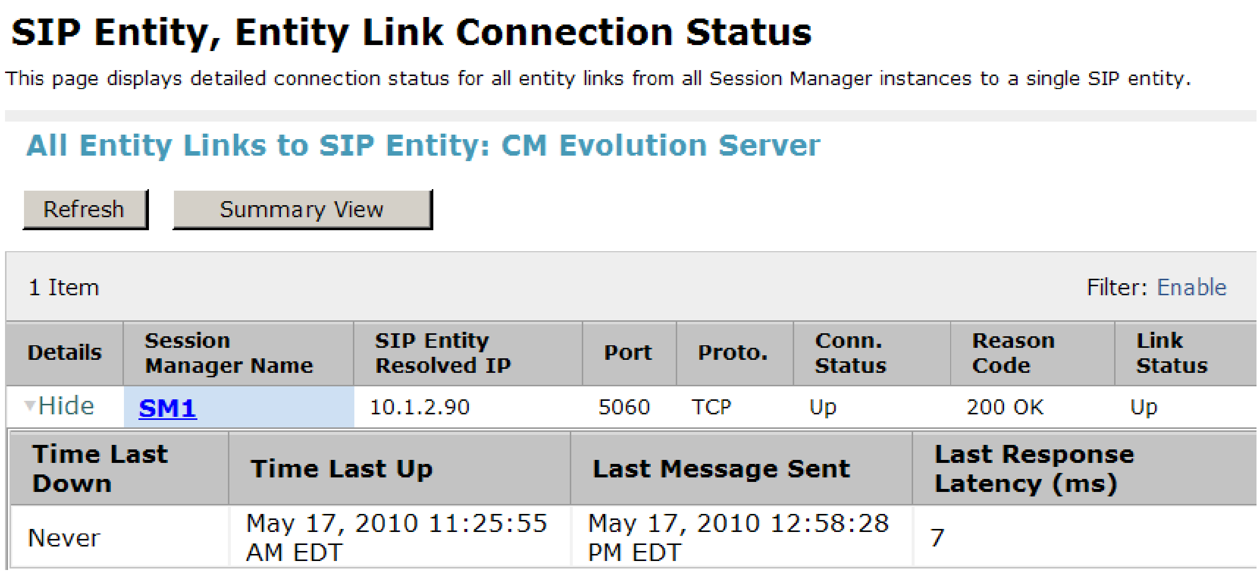
Refresh | Summary View

1 Item — Filter: Enable

Details	Session Manager Name	SIP Entity Resolved IP	Port	Proto.	Conn. Status	Reason Code	Link Status
Hide	SM1	10.1.2.90	5062	TCP	Up	200 OK	Up

Time Last Down	Time Last Up	Last Message Sent	Last Response Latency (ms)
Never	May 17, 2010 11:27:44 AM EDT	May 17, 2010 12:46:56 PM EDT	8

Return to the list of monitored entities, and select another entity of interest, such as “CM Evolution Server”. Under normal operating conditions, the **Link Status** should be “Up” as shown in the example screen below. In this case, “Show” under **Details** was selected to view additional information. Note the use of port 5060 using the same IP address as “CM-Evolution-procr-5062” shown in the prior screen.


SIP Entity, Entity Link Connection Status

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

All Entity Links to SIP Entity: CM Evolution Server

Refresh | Summary View

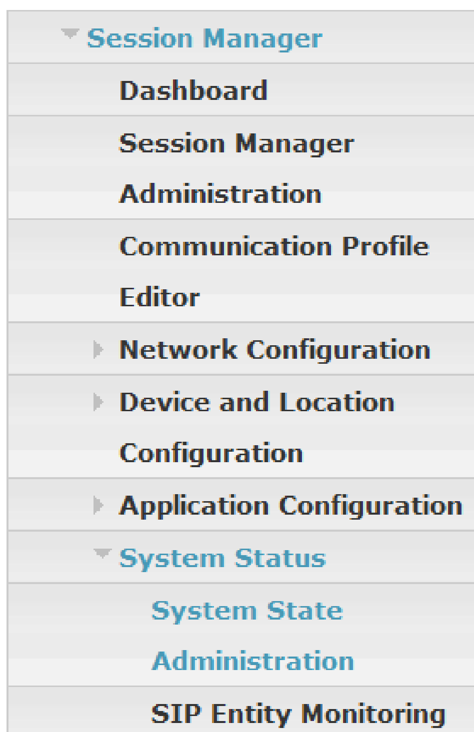
1 Item | Filter: Enable

Details	Session Manager Name	SIP Entity Resolved IP	Port	Proto.	Conn. Status	Reason Code	Link Status
Hide	SM1	10.1.2.90	5060	TCP	Up	200 OK	Up

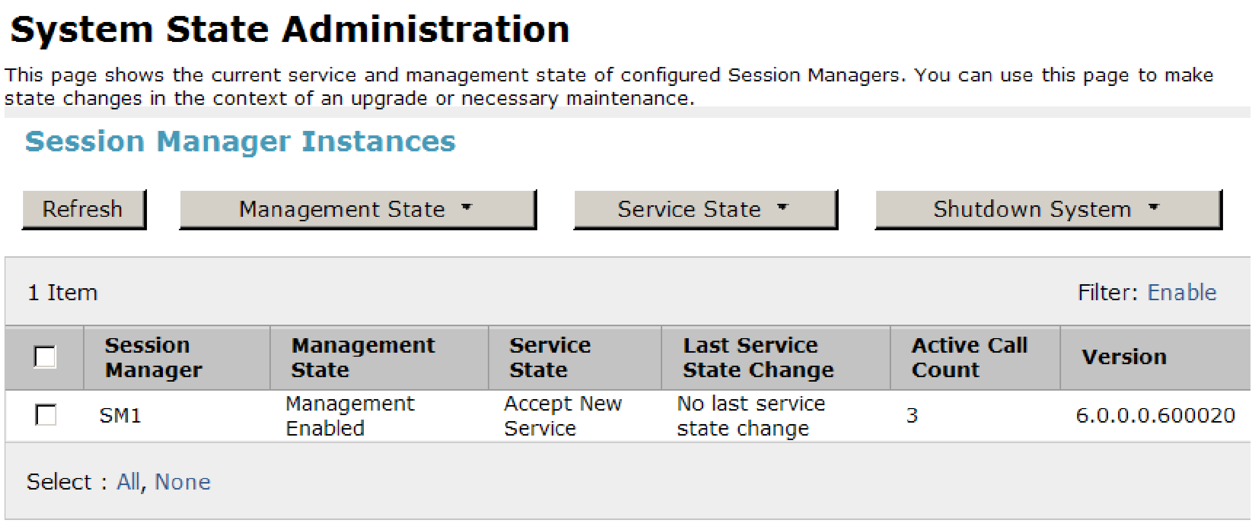
Time Last Down	Time Last Up	Last Message Sent	Last Response Latency (ms)
Never	May 17, 2010 11:25:55 AM EDT	May 17, 2010 12:58:28 PM EDT	7

9.2.2 Verify System State

Expand **Elements** → **Session Manager** → **System Status** → **System State Administration**, as shown below.

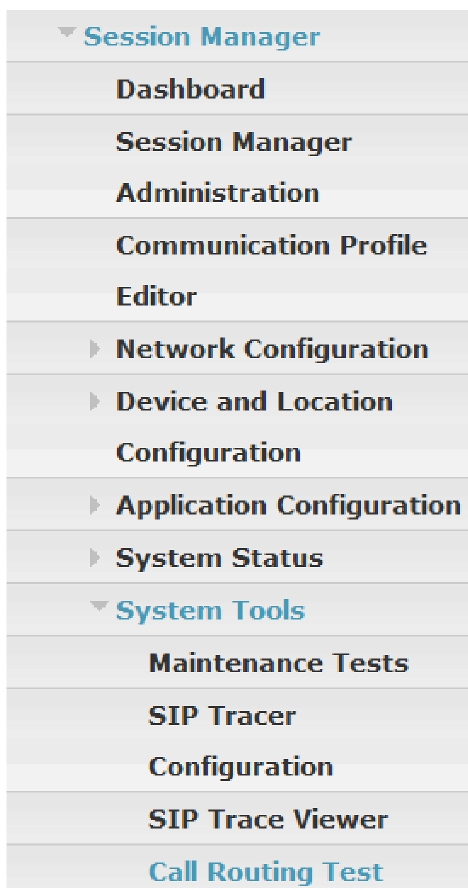


Verify that the **Management State** is "Management Enabled" and the **Service State** is "Accept New Service." The **Version** can also be observed.

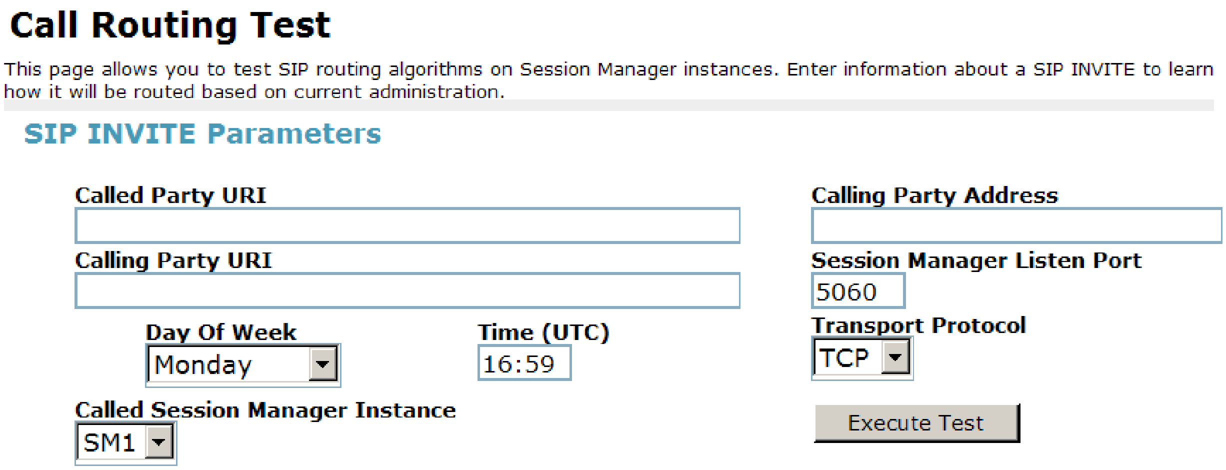


9.2.3 Call Routing Test

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

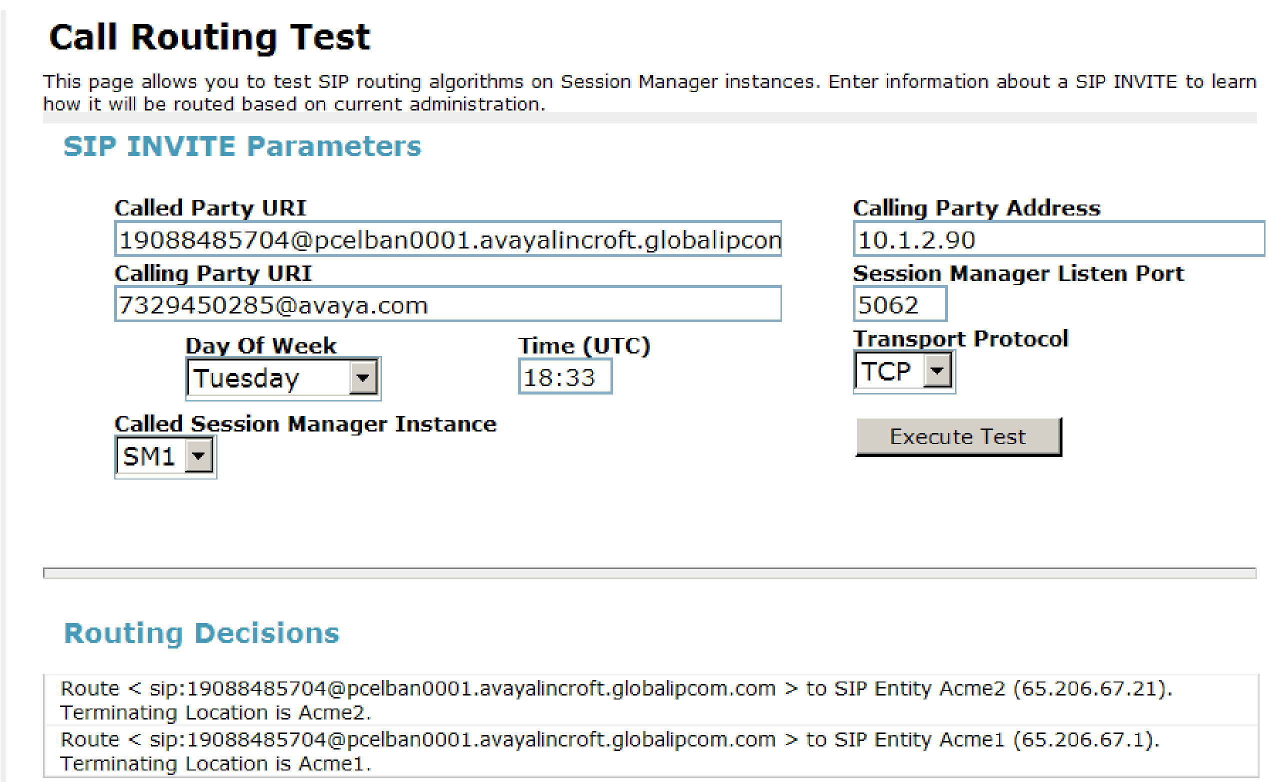


A screen such as the following is displayed.

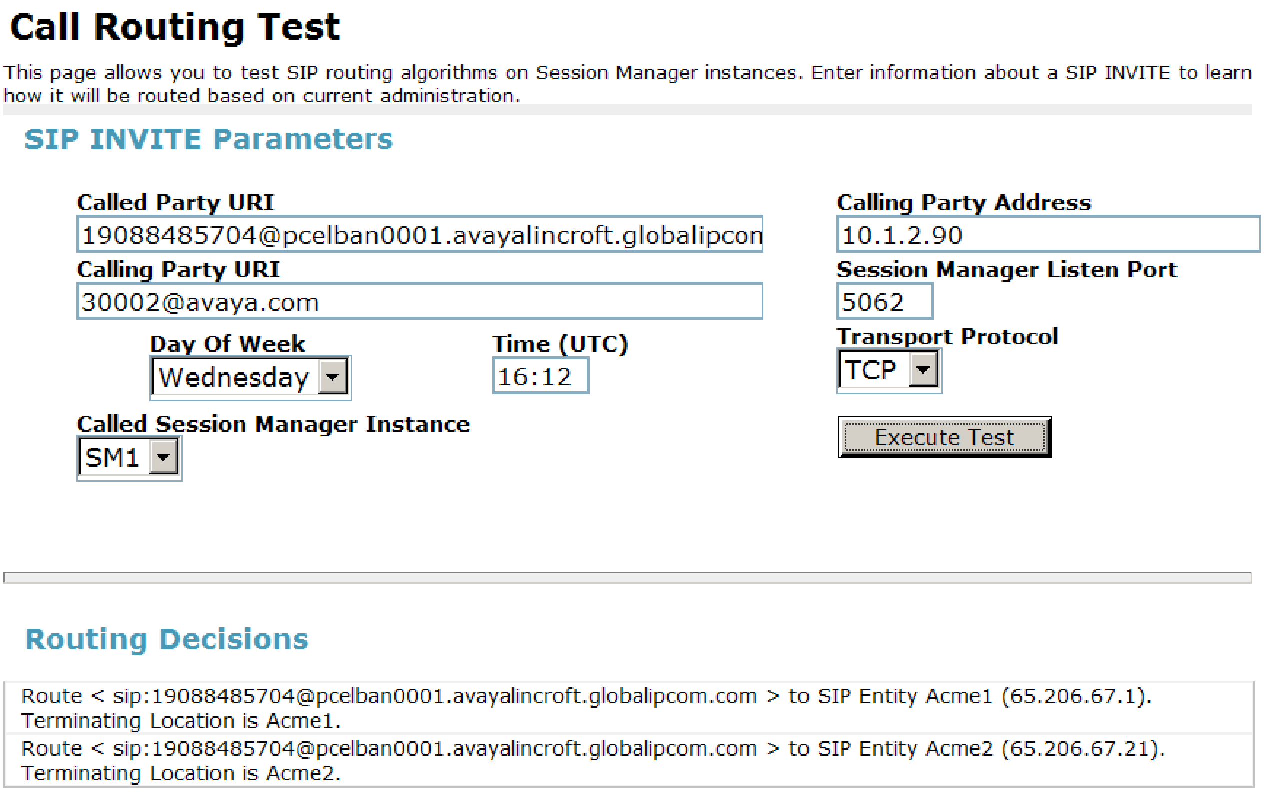


Populate the fields for the call parameters of interest. For example, the following screen shows an example call routing test for an outbound call to the PSTN via Verizon. In this case, the "Rank" in the Routing Policy for Acme1 and Acme2 were the same (default 0). Under **Routing Decisions**, observe that the call will route via an Acme Packet Net-Net SBC on the path to Verizon. In this example, Acme2 would have been selected before Acme1. If the "Execute Test" button is pressed multiple times without changing the request parameters, some results will list Acme1 before Acme2, and other results will list Acme2 before Acme1.

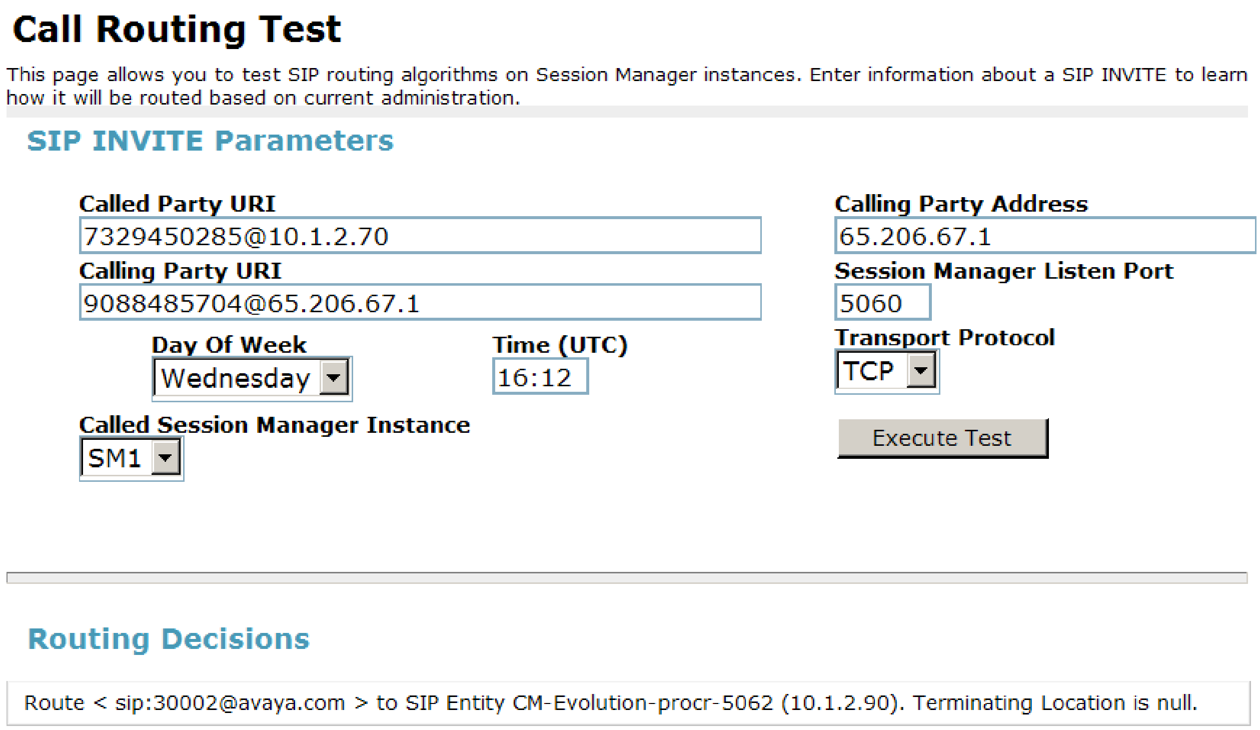
Scroll down to inspect the details of the **Routing Decision Process** if desired (not shown).



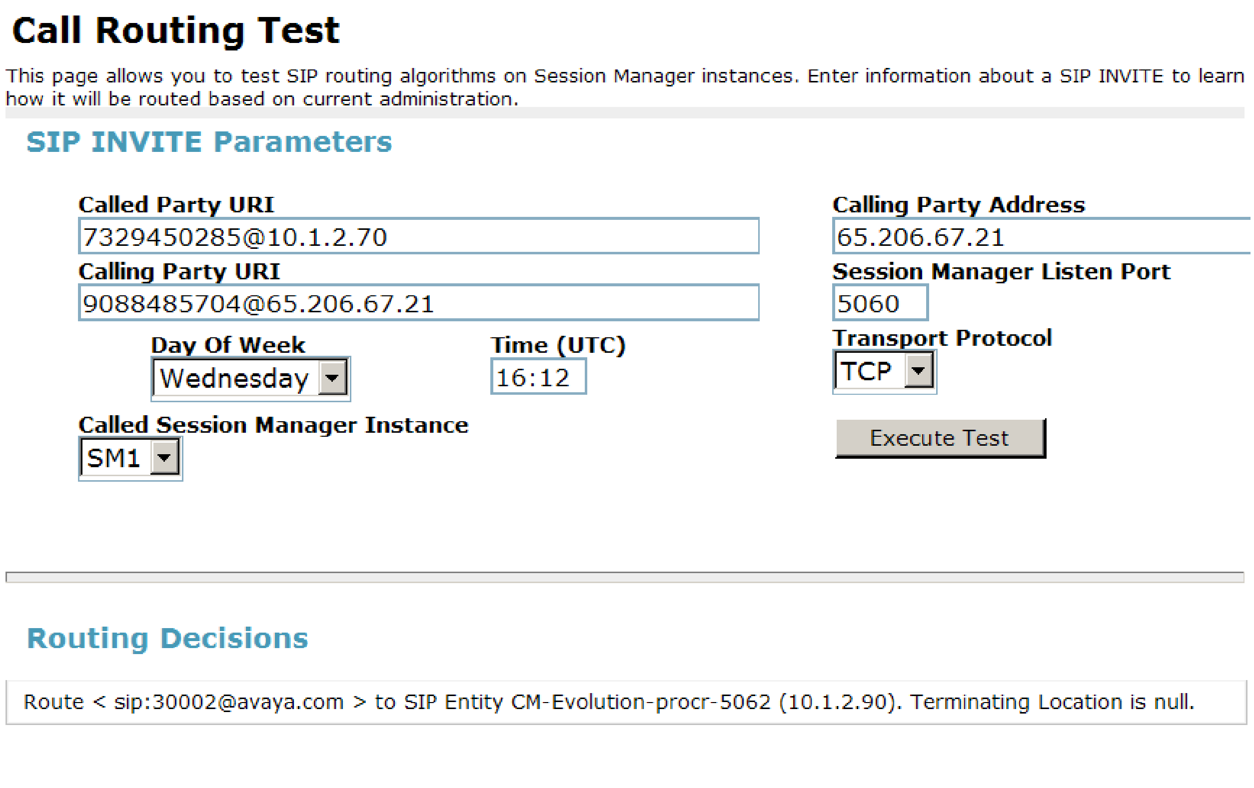
As another example of an outbound routing test, the following screen shows an example call routing test for an outbound call to the PSTN via Verizon. At the time of this test, the "Rank" in the Routing Policy for Acme1 was the default 0, but the rank associated with the Routing Policy to Acme2 was 1. Under **Routing Decisions**, observe that the call will route via Acme1 first. If the "Execute Test" button is pressed multiple times without changing the request parameters, all results will list Acme1 before Acme2.



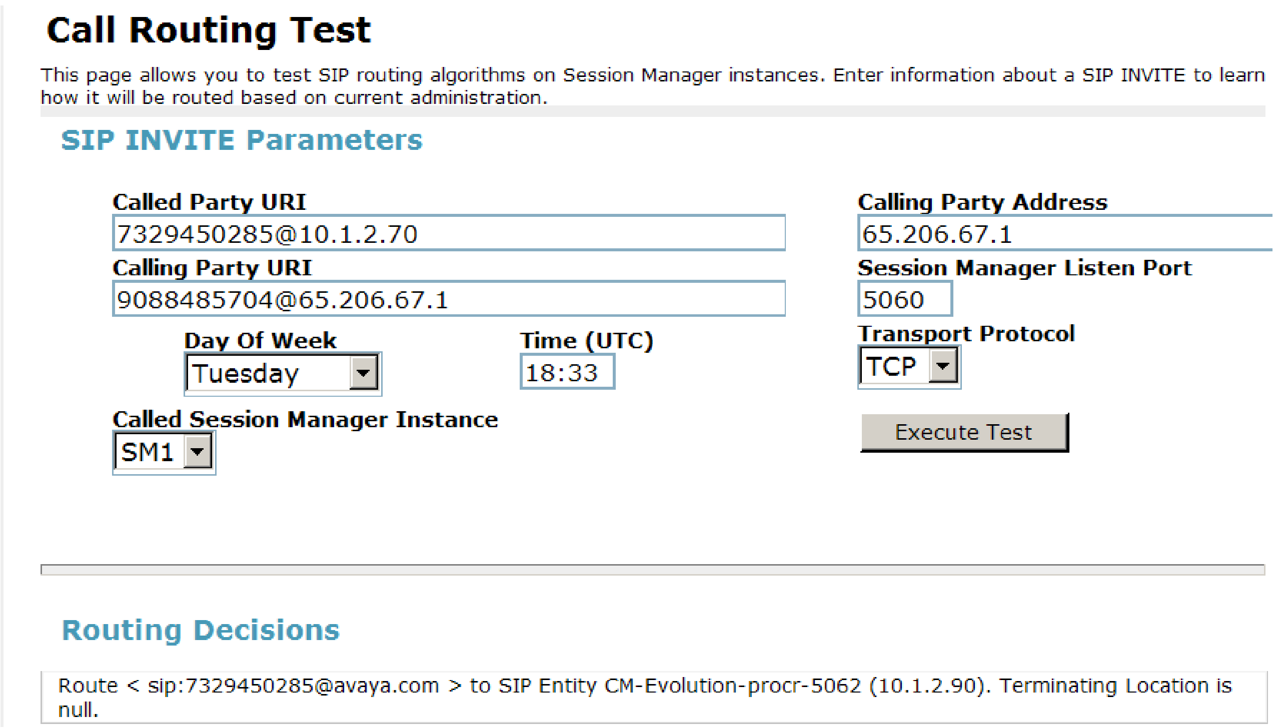
The following shows an example call routing test for an inbound call from the PSTN to the enterprise via Acme1 (65.206.67.1). Under **Routing Decisions**, observe that the call will route to the S8800 Processor Ethernet (10.1.2.90) using the SIP entity named “CM-Evolution-procr-5062”. The domain in the Request-URI is converted to “avaya.com”, and the digits are manipulated such that the Verizon DID number (i.e., 7329450285) is converted to a Communication Manager extension (i.e., 30002) by the adapter assigned to the Communication Manager entity. Scroll down to inspect the details of the **Routing Decision Process** if desired (not shown).



The following shows an example call routing test for an inbound call from the PSTN to the enterprise via Acme2 (65.206.67.21). Under **Routing Decisions**, observe that the call will route to the S8800 Processor Ethernet (10.1.2.90) using the SIP entity named "CM-Evolution-procr-5062". The domain in the Request-URI is converted to "avaya.com", and the digits are manipulated such that the Verizon DID number (i.e., 7329450285) is converted to a Communication Manager extension (i.e., 30002) by the adapter assigned to the Communication Manager entity. Scroll down to inspect the details of the **Routing Decision Process** if desired (not shown).



After a configuration change that removed the Verizon DID to Communication Manager extension digit manipulation from the adapter, the following example shows a call routing test for an inbound call from the PSTN to the enterprise via Acme1. Under **Routing Decisions**, observe that the call will still route to the S8800 Processor Ethernet (10.1.2.90) using the SIP entity named "CM-Evolution-procr-5062", but the Request-URI contains the full 10 digit DID number. With configuration like this, the incoming call handling table of the Communication Manager trunk group receiving the incoming call (i.e., trunk group 67 in the sample configuration) would need to map the Verizon DID to a Communication Manager extension.



10. Conclusion

As illustrated in these Application Notes, Avaya Aura™ Communication Manager 6.0, Avaya Aura™ Session Manager 6.0, and Acme Packet Net-Net SBC can be configured to interoperate successfully with Verizon Business IP Trunk service, inclusive of the "2-CPE" SIP trunk redundancy architecture. This solution allows Avaya Aura™ Communication Manager and Avaya Aura™ Session Manager users access to the PSTN using a Verizon Business IP Trunk public SIP trunk service connection.

11. Additional References

11.1. Avaya

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

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

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

[3] *Administering Avaya Aura™ Session Manager*, Doc ID 03-603324, Release 6.0, June 2010 available at http://support.avaya.com/css/P8/documents/100082630

[4] *Installing and Configuring Avaya Aura™ Session Manager,* Doc ID 03-603473 Release 6.0, June 2010 available at http://support.avaya.com/css/P8/documents/100089152

[5] *Maintaining and Troubleshooting Avaya Aura™ Session Manager,* Doc ID 03-603325, Release 6.0, June 2010 available at http://support.avaya.com/css/P8/documents/100089154

[6] *Administering Avaya Aura™ System Manager*, Document Number 03-603324, Release 5.2, November 2009 available at http://support.avaya.com/css/P8/documents/100089681

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

Application Notes Reference [JF-JRR-VZIPT] documents Verizon IP Trunk Service with previous versions of Avaya Aura™ Communication Manager and Avaya Aura™ Session Manager. The version coverage in [JF-JRR-VZIPT] goes beyond the versions in the title, with the addition of Addendum 2 in Issue 1.3 covering Communication Manager 5.2.1 and Session Manager 5.2.
[JF-JRR-VZIPT] Application Notes for Avaya Aura™ Communication Manager 5.2, Avaya Aura™ Session Manager 1.1, and Acme Packet Net-Net Session Director with Verizon Business IP Trunk SIP Trunk Service – Issue 1.3
https://devconnect.avaya.com/public/download/dyn/AvayaSM_VzB_IPT.pdf

Application Notes Reference [PE] documents a configuration with testing results using Processor Ethernet on a main Communication Manager and an ESS for survivable SIP Trunking. The verifications in this document illustrate additional survivability considerations.
[PE] Sample Configuration Illustrating Avaya Aura™ Communication Manager SIP Trunking Using Processor Ethernet and Acme Packet Net-Net 4500 Session Director – Issue 1.0
https://devconnect.avaya.com/public/flink.do?f=/public/download/interop/CM-PE-NN4500.pdf

Application Notes Reference [CLAN] documents a similar configuration to [PE] using survivable SIP Trunks signaled from C-LAN interfaces rather than processor Ethernet.
[CLAN] Sample Configuration Illustrating Avaya Aura™ Communication Manager SIP Trunk Survivability with Enterprise Survivable Server and Acme Packet Net-Net 4500 Session Director, Issue 1.0
https://devconnect.avaya.com/public/flink.do?f=/public/download/interop/CM-ESS-NN4500.pdf

Application Notes Reference [LAR] contains additional information on Communication Manager Look-Ahead Routing.
[LAR] Sample Configuration for SIP Private Networking and SIP Look-Ahead Routing Using Avaya Communication Manager, Issue 1.0
http://www.avaya.com/master-usa/en-us/resource/assets/applicationnotes/sip-pvt-lar.pdf

11.2. Verizon Business

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

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

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.