Avaya Solution & Interoperability Test Lab

Application Notes for Avaya Aura® Communication Manager Release 5.2.1, Avaya Aura® Session Manager Release 6.1, and Acme Packet Net-Net with Verizon Business IP Trunk SIP Trunk Service – Issue 1.0

Abstract

These Application Notes illustrate a sample configuration using Avaya Aura® Session Manager Release 6.1 and Avaya Aura® Communication Manager Release 5.2.1 with the Verizon Business Private IP (PIP) IP Trunk service. These Application Notes supplement previously published Application Notes with other versions of Avaya Aura® Communication Manager and Avaya Aura® Session Manager. 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.

Avaya Aura® SIP Solution using Avaya Aura® Communication Manager Release 5.2.1 has not been certified independently by Verizon labs. These Application Notes can be used to facilitate customer engagements via the Verizon field trial process, pending Verizon labs independent certification.

Table of Contents

1. Introduction

These Application Notes illustrate a sample configuration using Avaya Aura® Session Manager Release 5.2.1 and Avaya Aura® Communication Manager Release 6.1 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 supplement previously published Application Notes [JF-JRR-VZIPT] and [JRR-VZIPT] with other versions of Avaya Aura® Communication Manager and Avaya Aura® 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 references [JF-JRR-VZIPT] and [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.

Avaya Aura® SIP Solution using Avaya Aura® Communication Manager Release 5.2.1 has not been independently certified by Verizon labs. These Application Notes can be used to facilitate customer engagements via the Verizon field trial process, pending Verizon labs independent certification.

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 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 and retrieval.
- 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:

- With Communication Manager Release 5.2.1, an additional Communication Manager configured as a Feature Server is required to support enterprise SIP phones and their inter-working with endpoints of other types (i.e., H.323, digital and/or analog) controlled by the Communication Manager Access Element (this limitation was lifted in Communication Manager Release 6.0 and later releases). Since Communication Manager configured as an Access Element plus a separate Communication Manager Feature Server in the Release 5.2.1 environment is not a typical deployment configuration, Communication Manager Feature Server (and therefore enterprise SIP phones) was not included in the sample configuration described in these Application Notes.

- Verizon Business IP Trunking service does not support T.38 fax on the production circuit used to verify these Application Notes. The approach to using fax over G.711MU documented in reference [JF-JRR-VZIPT] may be used. However, as noted in reference [JF-JRR-VZIPT], the use of an AudioCodes MP-202 Gateway between Communication Manager and the fax device is recommended for G.711 fax.
- If calls requiring in-band DTMF (rather than RFC 2833 signaling) will be required, the "DTMF over IP" parameter on the 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 plans to implement 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.

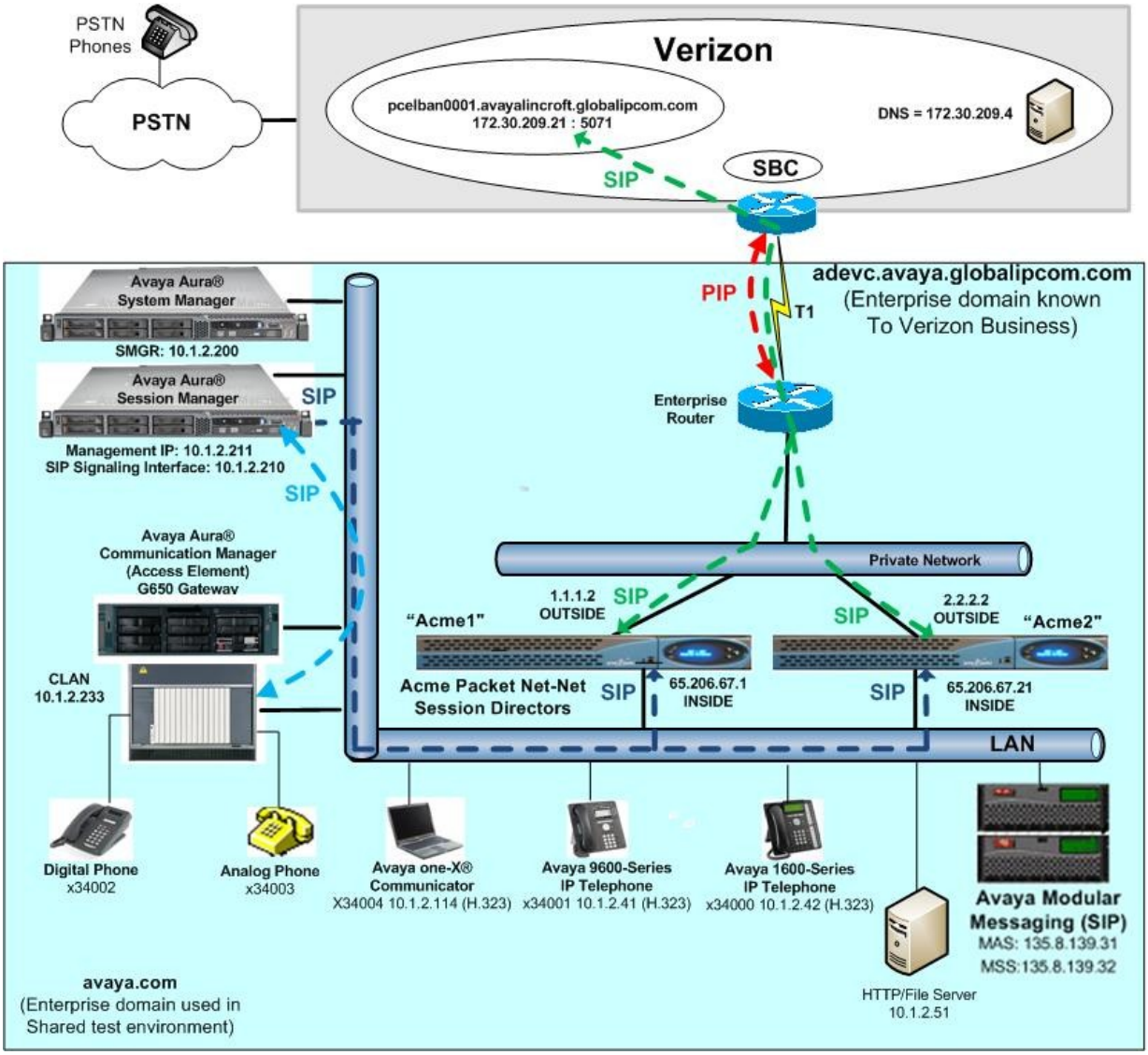


Figure 1: Avaya Solution and Interoperability Test Lab Configuration

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 references [JF-JRR-VZIPT] and [JRR-VZIPT]. For efficiency, the Avaya CPE environment utilizing Avaya Aura® Session Manager Release 6.1 and Avaya Aura® Communication Manager Release 5.2.1 was shared among many ongoing test efforts at the Avaya Solution and Interoperability Test 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, Avaya Aura® 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 Avaya Aura® Communication Manager and Avaya Aura® 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 5.2.1
- Avaya Aura® System Manager Release 6.1
- Avaya Aura® Session Manager Release 6.1
- Avaya 1600 Series IP telephones using the H.323 software bundle.
- Avaya 9600 Series IP telephones using the H.323 software bundle.
- Avaya one-X® Communicator Soft phone (configured for H.323).
- Avaya Digital phones
- Avaya Analog 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 Communication Manager SIP trunk group form provides options for specifying whether History Info Headers or Diversion Headers are sent.

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

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	Avaya Aura® Communication Manager 5.2.1 (R015x.02.1.016.4 + patch 18576)
Avaya G650 Media Gateway – CONTROL-LAN – IP MEDIA PROCESSOR – IP SERVER INTFC	 TN799DP – HW01 FW032 TN2602AP – HW02 FW047 TN2312BP – HW15 FW046
Avaya S8800 Server	Avaya Aura® System Manager 6.1 Build 6.1.0.0.7345, Patch 6.1.5.2
Avaya S8800 Server	Avaya Aura® Session Manager 6.1 6.1.0.0.610023
Avaya 9600-Series Telephone (H.323)	Avaya one-X® Deskphone Edition 3.1.1
Avaya 1600-Series Telephone (H.323)	Avaya one-X® Deskphone Value Edition 1.2.2
Avaya one-X® Communicator (H.323)	6.0 with SP1 (6.0.1.16)
Avaya 6408-D Digital Telephone	N/A
Avaya 6210 Analog Telephone	N/A
Avaya Modular Messaging (Application Server)	Avaya Modular Messaging (MAS) 5.2 SP6 Patch 2 (9.2.357.6022)
Avaya Modular Messaging (Storage Server)	Avaya Modular Messaging (MSS) 5.2 SP6 Patch 2
Acme Packet Net-Net 4250[1]	SC6.2.0 MR-3 Patch 5 (Build 687)

Table 1: Equipment and Software Used in the Sample Configuration

4. Configure Avaya Aura® Communication Manager Release 5.2.1

This section illustrates a sample configuration allowing SIP signaling between Communication Manager and Session Manager via an Avaya C-LAN in the Avaya G650 Media Gateway.

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.

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

All Communication Manager configuration is performed via the Communication Manager SAT interface of the Avaya S8800 Server. Screens are abridged for brevity in presentation.

4.1. Verify Licensed Features

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

On **Page 2** of the ***display system-parameters customer-options*** form, verify that the **Maximum Administered SIP Trunks** is sufficient for the combination of trunks to the Verizon Business 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  10
                                OPTIONAL FEATURES

IP PORT CAPACITIES                                          USED
                     Maximum Administered H.323 Trunks: 800   200
           Maximum Concurrently Registered IP Stations: 18000 3
             Maximum Administered Remote Office Trunks: 0     0
Maximum Concurrently Registered Remote Office Stations: 0     0
              Maximum Concurrently Registered IP eCons: 0     0
  Max Concur Registered Unauthenticated H.323 Stations: 0     0
                  Maximum Video Capable H.323 Stations: 0     0
                   Maximum Video Capable IP Softphones: 0     0
                       Maximum Administered SIP Trunks: 800   198
  Maximum Administered Ad-hoc Video Conferencing Ports: 0     0
   Maximum Number of DS1 Boards with Echo Cancellation: 0     0
                            Maximum TN2501 VAL Boards: 10    1
                     Maximum Media Gateway VAL Sources: 0     0
           Maximum TN2602 Boards with 80 VoIP Channels: 128   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  10
                                OPTIONAL FEATURES

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

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 4.8**), verify that the **ISDN/SIP Network Call Redirection** feature is enabled.

```
display system-parameters customer-options                      Page   4 of  10
                                OPTIONAL FEATURES

   Emergency Access to Attendant? y                             IP Stations? y
           Enable 'dadmin' Login? y
           Enhanced Conferencing? y                       ISDN Feature Plus? y
                  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? n               Local Survivable Processor? n
          Extended Cvg/Fwd Admin? n                    Malicious Call Trace? n
     External Device Alarm Admin? n                 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? n                 Multifrequency Signaling? y
      Global Call Classification? n         Multimedia Call Handling (Basic)? n
             Hospitality (Basic)? y      Multimedia Call Handling (Enhanced)? n
 Hospitality (G3V3 Enhancements)? n               Multimedia IP SIP Trunking? n
                       IP Trunks? y

           IP Attendant Consoles? n
```

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

```
display system-parameters customer-options                      Page   5 of  10
                                OPTIONAL FEATURES

                Multinational Locations? n             Station and Trunk MSP? y
 Multiple Level Precedence & Preemption? n      Station as Virtual Extension? n
                     Multiple Locations? n
                                              System Management Data Transfer? n
          Personal Station Access (PSA)? n               Tenant Partitioning? n
                        PNC Duplication? n       Terminal Trans. Init. (TTI)? n
                  Port Network Support? y               Time of Day Routing? n
                        Posted Messages? n       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? n
                                                                    Wireless? n
                          Remote Office? n
          Restrict Call Forward Off Net? y
                  Secondary Data Module? y
```

4.2. Dial Plan

In the reference configuration the Avaya CPE environment uses five digit local extensions, such as 34xxx. 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
     1            3    dac
     2            5    ext
     222          5    aar
     3            5    ext
     3234         7    ext
     4            5    ext
     5            5    ext
     6            5    ext
     7            7    ext
     8            1    fac
     9            1    fac
     *            3    fac
     #            3    fac
```

4.3. System Features

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

```
change system-parameters features                               Page   1 of  19
                           FEATURE-RELATED SYSTEM PARAMETERS
                              Self Station Display Enabled? y
                                   Trunk-to-Trunk Transfer: all
               Automatic Callback with Called Party Queuing? n
    Automatic Callback - No Answer Timeout Interval (rings): 3
                      Call Park Timeout Interval (minutes): 10
        Off-Premises Tone Detect Timeout Interval (seconds): 20
                                AAR/ARS Dial Tone Required? y
                           Music/Tone on Hold: music Type: ext   65021
              Music (or Silence) on Transferred Trunk Calls? no
                      DID/Tie/ISDN/SIP Intercept Treatment: attd
    Internal Auto-Answer of Attd-Extended/Transferred Calls: transferred
                  Automatic Circuit Assurance (ACA) Enabled? N


             Abbreviated Dial Programming by Assigned Lists? n
       Auto Abbreviated/Delayed Transition Interval (rings): 2
                    Protocol for Caller ID Analog Terminals: Bellcore
    Display Calling Number for Room to Room Caller ID Calls? n
```

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

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

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

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

4.4. IP 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 "sm61" with IP address 10.1.2.210; the node name for the CLAN in the Avaya G650 Media Gateway controlled by Communication Manager is "clan1" with IP address 10.1.2.233.

```
change node-names ip                                            Page   1 of  2
                              IP NODE NAMES
    Name              IP Address
sm61                10.1.2.210
clan1               10.1.2.233
```

4.5. Network Regions for Gateway and Telephones

Network regions provide a mean to logically group resources. In the shared Communication Manager configuration used for the testing, the Avaya G650 Media Gateway is in region 1. To provide testing flexibility, network region 54 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. 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. The screen below shows 3 IP telephones used for the compliance test: they are all assigned to network region 54 with IP address in the 10.1.2.0/24 subnet based on the bold configuration entries. 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: 10.1.2.41                                   /32    54     n
   TO: 10.1.2.41
 FROM: 10.1.2.42                                   /32    54     n
   TO: 10.1.2.42
 FROM: 10.1.2.114                                  /32    54     n
   TO: 10.1.2.114
 FROM: 65.206.67.0                                 /24    54     n
   TO: 65.206.67.255
 FROM: 192.168.49.0                                /24    54     n
   TO: 192.168.49.255
```

The following screen shows IP network region 54 configuration. In the shared test environment, network region 54 is used to allow unique behaviors for the Verizon test environment. In this example, codec set 4 will be used for calls within region 54. The shared Avaya Solution and Interoperability Test Lab test environment uses the domain "avaya.com". 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 54                                    Page   1 of  19
                              IP NETWORK REGION
  Region: 54
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? n
   UDP Port Max: 3329
DIFFSERV/TOS PARAMETERS                  RTCP Reporting Enabled? y
 Call Control PHB Value: 46      RTCP MONITOR SERVER PARAMETERS
        Audio PHB Value: 46       Use Default Server Parameters? y
        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 54. The bold row shows that network region 54 is directly connected to network region 1, and that codec set 4 will 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 1will also show codec set 4 for region 1 to region 54 connectivity.

```
change ip-network-region 54                                     Page   3 of  19

 Source Region: 54    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
```

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 setting. 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  19
                              IP NETWORK REGION
  Region: 1
Location:         Authoritative Domain: avaya.com
    Name:
MEDIA PARAMETERS                Intra-region IP-IP Direct Audio: yes
      Codec Set: 1              Inter-region IP-IP Direct Audio: yes
   UDP Port Min: 2048                     IP Audio Hairpinning? n
   UDP Port Max: 10001
DIFFSERV/TOS PARAMETERS                  RTCP Reporting Enabled? y
 Call Control PHB Value: 46      RTCP MONITOR SERVER PARAMETERS
        Audio PHB Value: 46       Use Default Server Parameters? y
        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 54, and that codec set 4 will be used for any connections between region 54 and region 1.

```
change ip-network-region 1                                      Page   6 of  19

 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
 46
 47
 48
 49
 50
 51
 52
 53
 54   4     y    NoLimit                                          n       t
 55
```

4.6. IP Codec Sets

The following screen shows the configuration for codec set 4, the codec set configured to be used for calls within region 4 and for calls between region 1 and region 4. In general, an IP codec set is a list of allowable codecs in priority order. Using the example configuration shown below, all calls to and from the PSTN via the SIP trunks would use G.729A, since G.729A is preferred by both Verizon and the Avaya ip-codec-set. Any calls using this same codec set that are placed 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 VoIP resources on the Avaya G650 Media Gateway 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 G650 VoIP resources, but rather be "ip-direct" using G.711MU from Modular Messaging to the inside of the Acme Packet Net-Net SBC. If G.711MU is not included in ip-codec-set 4, and the Verizon network sends a re-INVITE to transition a call initially established using G.729a to G.711MU, the call may fail. For example, the Verizon network may send a re-INVITE for a voice call to G.711MU if ambient noise on the call causes the Verizon network to detect tones such as fax tone. For this reason, it is recommended that G.711MU be included in ip-codec-set 4.

```
change ip-codec-set 4                                           Page   1 of   2

                          IP Codec Set

    Codec Set: 4

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

On **Page 2** of the form:

- Configure the Fax **Mode** field to "off". Verizon does not support 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.

```
display 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:
```

4.7. SIP Signaling Groups

This section illustrates the configuration of the SIP signaling groups. Each signaling group has a **Group Type** of "sip", a **Near-end Node Name** of "clan1", and a **Far-end Node Name** of "sm61". 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 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 54. Port 5067 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 5067. The use of different ports is one means to allow Communication Manager to

distinguish different types of calls arriving from the same Session Manager. Other parameters may be left at default values.

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

 Group Number: 67             Group Type: sip
                        Transport Method: tcp
  IMS Enabled? n


   Near-end Node Name: clan1                  Far-end Node Name: sm61
 Near-end Listen Port: 5067                 Far-end Listen Port: 5067
                                         Far-end Network Region: 54
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                      Direct IP-IP Early 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 "clan1", the **Far-end Node Name** is "sm61", and the **Far-end Network Region** is 54. 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". Other parameters may be left at default values.

Note that the **Alternate Route Timer** settting that defaults to 6 seconds impacts fail-over timing for outbound calls. If Communication Manager does not get an expected response after the expiration of the Alternate Route Timer, Look-Ahead Routing (LAR) can be triggered. Detailed examples of the use of LAR can be found in reference [CLAN] and reference [LAR].

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

 Group Number: 68             Group Type: sip
                        Transport Method: tcp
  IMS Enabled? n


   Near-end Node Name: clan1                  Far-end Node Name: sm61
 Near-end Listen Port: 5067                 Far-end Listen Port: 5067
                                         Far-end Network Region: 54
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                      Direct IP-IP Early Media? n
H.323 Station Outgoing Direct Media? n            Alternate Route Timer(sec):20
```

The following screen shows signaling group 32, the signaling group to Session Manager that was in place prior to adding the Verizon SIP Trunking configuration to the shared Avaya Solution and Interoperability Test Lab configuration. This signaling group reflects configuration not specifically related to Verizon trunking. For example, calls routed to other Avaya applications, such as Avaya Modular Messaging, use this signaling group. Again, the **Near-end Node Name** is "clan1" and the **Far-end Node Name** is "sm61", the node name of the Session Manager. Unlike the signaling groups used for the Verizon signaling, the **Far-end Network Region** is 1. The **Far-end Domain** is set to "avaya.com" matching the configuration in place prior to adding the Verizon SIP Trunking configuration.

```
display signaling-group 32
                               SIGNALING GROUP

 Group Number: 32             Group Type: sip
                        Transport Method: tcp
  IMS Enabled? n



   Near-end Node Name: clan1                 Far-end Node Name: sm61
 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? n                     Direct IP-IP Early Media? n
H.323 Station Outgoing Direct Media? n            Alternate Route Timer(sec):15
```

4.8. SIP Trunk Groups

This section illustrates the configuration of the SIP trunks groups corresponding to the SIP signaling groups from **Section 4.7**.

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-CPESBC-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: 10
```

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 refresh SIP call sessions.

```
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
```

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 as in **Section 4.3**, such that incoming "private" (anonymous) or "restricted" calls can display an Avaya-configured text string on called party telephones. The sample configuration uses the "public" Numbering Format for sending the calling party numbers (CPN) to the far-end (see **Section 4.10** for details).

```
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
```

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. 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 the use of the SIP REFER method, while also implicitly enabling

Communication Manager to signal "send-only" media conditions for calls placed on hold at the enterprise site. If neither REFER signaling nor "send-only" media signaling is required, this field may be left at the default "n" value. In the testing associated with these Application Notes, the transfer feature 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 Manager 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. The 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
```

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-SM-CPESBC-VZ             COR: 1        TN: 1        TAC: 168
   Direction: outgoing       Outgoing Display? n
 Dial Access? n
Queue Length: 0
Service Type: public-ntwrk

                                                     Signaling Group: 68
                                                   Number of Members: 10
```

The following shows **Page 1** for trunk group 32, the bi-directional "tie" trunk group to Session Manager that existed before adding the Verizon SIP Trunk configuration to the shared Avaya Solution and Interoperability Test 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.

```
display trunk-group 32                                          Page   1 of  21
                                TRUNK GROUP

Group Number: 32                   Group Type: sip           CDR Reports: y
  Group Name: To SM61                       COR: 1        TN: 1        TAC: 132
   Direction: two-way        Outgoing Display? n
 Dial Access? n                                   Night Service:
Queue Length: 0
Service Type: tie                   Auth Code? n

                                                        Signaling Group: 32
                                                      Number of Members: 100
```

The following shows **Page 4** for trunk group 32. 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.

```
display trunk-group 32                                          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:
```

4.9. Route Pattern Directing Outbound Calls to Verizon

Route pattern 68 will be used for calls destined for the PSTN via the Verizon IP Trunk service. Digit manipulation can be performed on the called number, if needed, using the **No. Del Dgts** and **Inserted Digits** parameters. Digit manipulation can also be performed by Session Manager. The Facility Restriction Level (**FRL**) field can be set to a level that allows access to this trunk for all users that require it. The value of 0 is the least restrictive level.

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 [CLAN], [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
```

4.10. 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 the public-unknown-numbering form for outbound calls, and incoming call handling treatment form for the inbound trunk group).

In the bolded rows shown in the example abridged output below, several specific Communication Manager extensions (x34xxx) are mapped to DID numbers known to Verizon for this SIP Trunk connection (73294502xx), 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 0                                Page   1 of   2
                      NUMBERING - PUBLIC/UNKNOWN FORMAT
                                            Total
Ext Ext           Trk       CPN             CPN
Len Code          Grp(s)    Prefix          Len
                                                     Total Administered: 15
 5  3                                       5           Maximum Entries: 9999
 5  34000         67-68     7329450285      10
 5  34001         67-68     7329450286      10
 5  34002         67-68     7329450244      10
 5  34003         67-68     7329450242      10
 5  34004         67-68     7329450243      10
```

4.11. 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 [CLAN]. 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 1-908-848-5703, 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 19088485703                                  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
    19088485703           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 19088485703
                            ARS ROUTE CHOSEN REPORT
     Location:  1                      Partitioned Group Number:  1

      Dialed            Total        Route    Call      Node
      String          Min    Max    Pattern   Type     Number    Location
 19088485703          11    11       68       hnpa                 all
```

4.12. 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 7329450286 to extension 34001. 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 7329450286       all 34001
```

4.13. 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 32. Users can dial extension 33000 to reach Modular Messaging (e.g., for message retrieval). The following screen shows **Page 1** of hunt-group 32.

```
display hunt-group 32                                          Page   1 of  60
                                   HUNT GROUP

            Group Number: 32                                ACD? n
              Group Name: Modular Messaging               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 32, which routes to the AAR access code 8 and **Voice Mail Number** 33000.

```
display hunt-group 32                                          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
```

4.14. 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 **Section 4.13**. 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 32.

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

          Dialed           Total     Route    Call   Node  ANI
          String          Min  Max  Pattern   Type   Num   Reqd
    301                   5    5     32       aar          n
    305                   5    5     32       aar          n
    3100                  5    5     32       aar          n
    3101                  5    5     32       aar          n
    3200                  5    5     32       aar          n
    33                    5    5     32       aar          n
```

4.15. 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 32 contains trunk group 32, the "private" tie trunk group to Session Manager.

```
display route-pattern 32                                          Page   1 of   3
                    Pattern Number: 32  Pattern Name: To ASM
                              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: 32   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
```

4.16. Avaya Aura® Communication Manager Stations

In the sample configuration, five digit station extensions were used with the format 34xxx. The following abbreviated screen shows an example extension for an Avaya H.323 IP telephone. Coverage path 32 is assigned to give this user coverage to Avaya Modular Messaging.

```
change station 34001                                              Page   1 of   5
                                      STATION

Extension: 34001                         Lock Messages? n               BCC: 0
     Type: 9630                          Security Code: 123456           TN: 1
     Port: S00520                      Coverage Path 1: 32              COR: 1
     Name: Allan-96xxH                 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: 34001
            Speakerphone: 2-way              Mute Button Enabled? y
        Display Language: english                 Button Modules: 0
 Survivable GK Node Name:
          Survivable COR: internal              Media Complex Ext:
   Survivable Trunk Dest? y                          IP SoftPhone? n
```

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

```
change station 34001                                          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 - Send Calling Number and Name?
       Service Link Mode: as-needed                     EC500 State: disabled
         Multimedia Mode: enhanced
    MWI Served User Type: sip-adjunct           Display Client Redirection? n
                                               Select Last Used Appearance? n
                                                 Coverage After Forwarding? s

                                             Direct IP-IP Audio Connections? y
  Emergency Location Ext: 34001         Always Use? n IP Audio Hairpinning? n
```

4.17. Coverage Path

This section illustrates an example coverage path for a station with a mailbox on Avaya Modular Messaging. Hunt group 32, the hunt group to Modular Messaging, is **Point1** in coverage path 32.

```
change coverage path 32                                       Page   1 of   1
                                 COVERAGE PATH

                   Coverage Path Number: 32
     Cvg Enabled for VDN Route-To Party? n        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: h32            Rng:    Point2:
  Point3:                        Point4:
  Point5:                        Point6:
```

4.18. EC500 Configuration for Diversion Header Testing

When EC500 is enabled for a Communication Manager station, a call to that station will generate a new outbound call from Communication Manager to the configured EC500 destination, typically a mobile phone. The following screen shows a sample EC500 configuration for the user with station extension 34001. Use the command ***change off-pbx-telephone station mapping x*** where ***x*** is the Communication Manager station extension (e.g. 34001).

- **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., 9086309723)
- **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 34001                  Page   1 of   3
                  STATIONS WITH OFF-PBX TELEPHONE INTEGRATION

 Station       Application Dial   CC  Phone Number    Trunk       Config  Dual
 Extension                 Prefix                    Selection   Set     Mode
 34001            EC500    1    -     9086309723       ars        1
                                -
```

4.19. Saving Communication Manager Configuration Changes

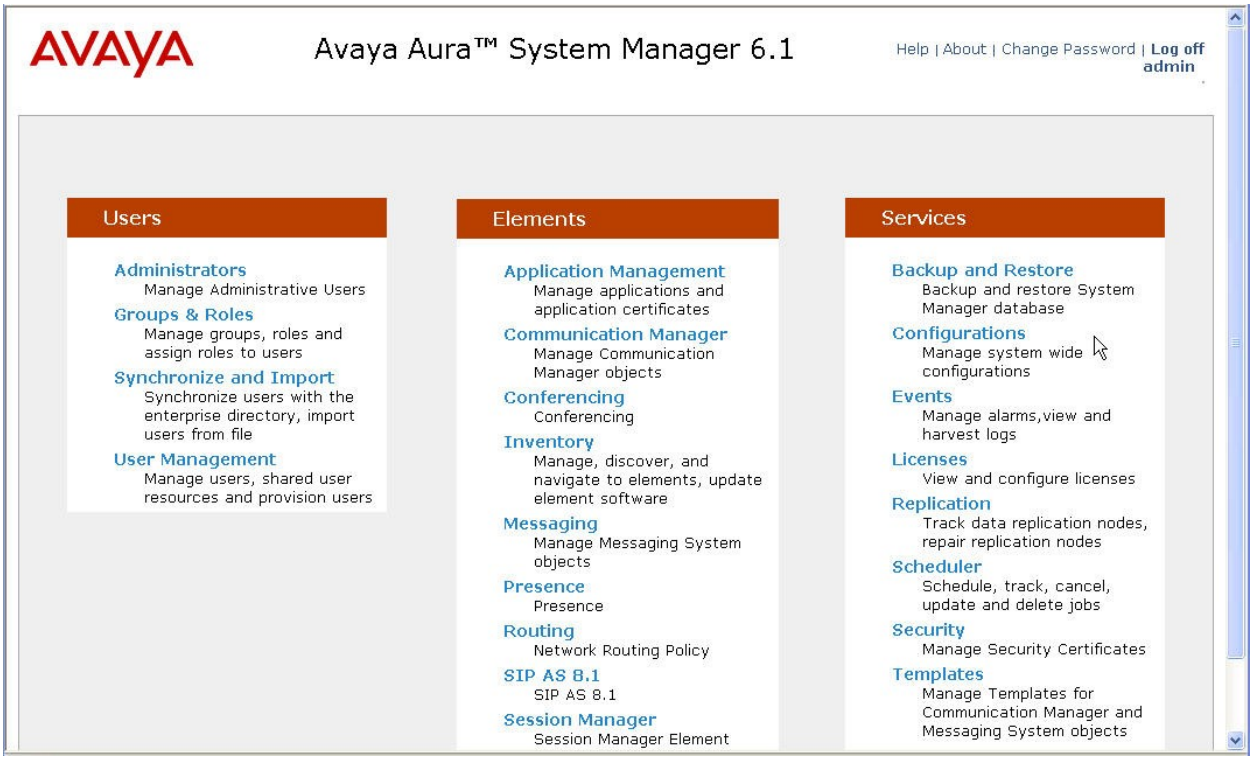
The command ***save translation all*** can be used to save the configuration.

5. Configure Avaya Aura® Session Manager Release 6.1

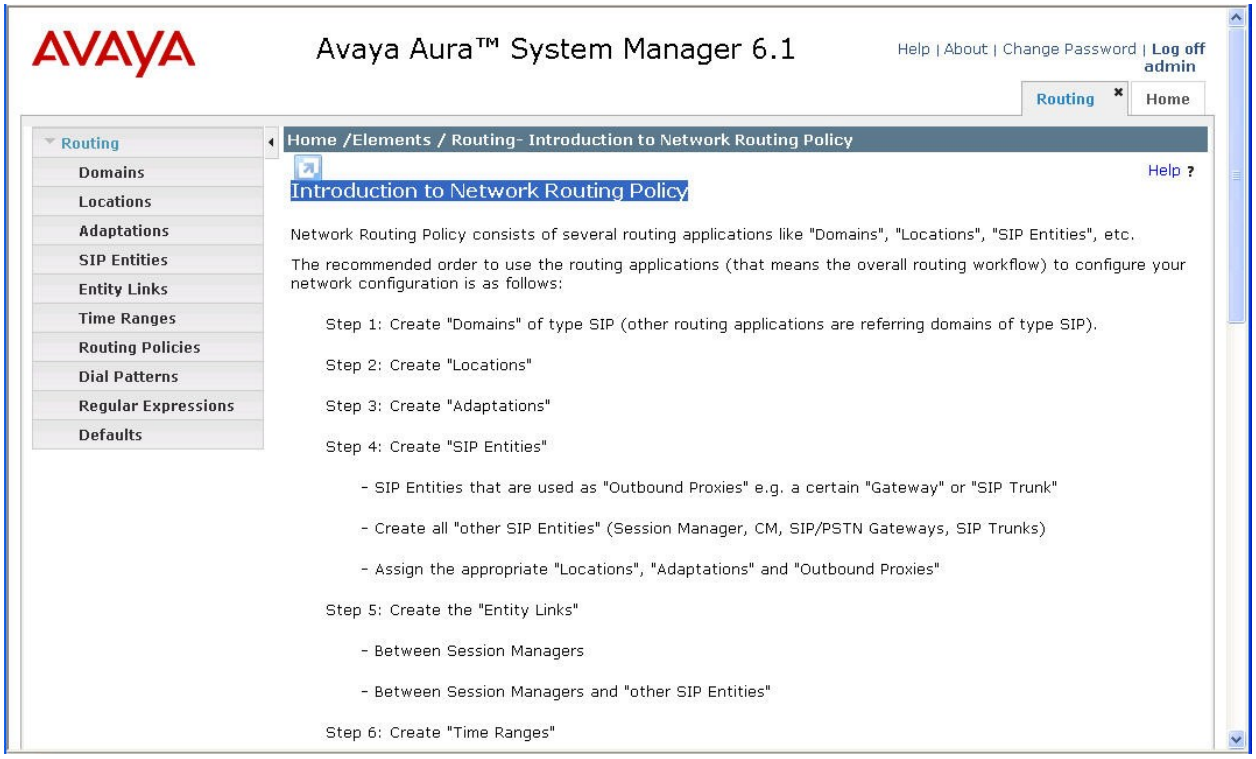
This section illustrates relevant aspects of the Avaya Aura® Session Manager configuration used in the verification of these Application Notes.

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

Session Manager configuration is accomplished by accessing the browser-based GUI of System Manager, using the URL "https://<ip-address>/SMGR", where "<ip-address>" is the IP address of System Manager. At the **Session Manager Log On** screen, provide the appropriate credentials and click on **Login** (not shown). The initial screen shown below is then displayed.



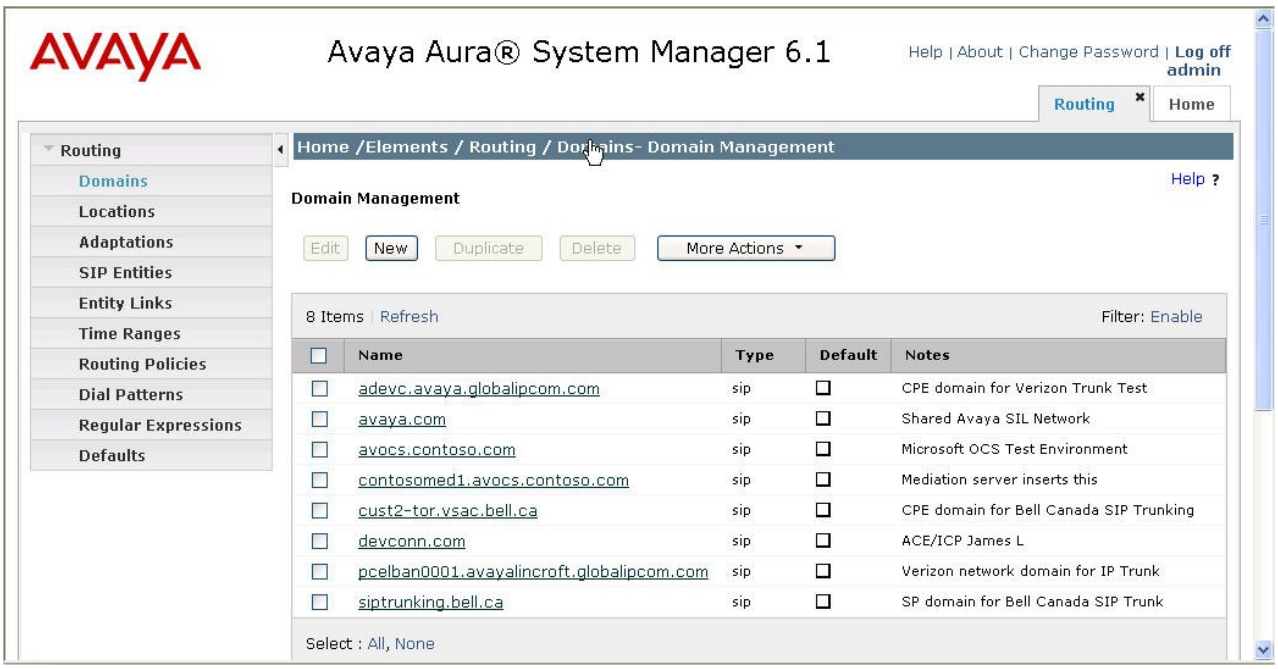
Most of the configuration items are performed in the Routing Element. Click on **Routing** in the **Elements** column to bring up the **Introduction to Network Routing Policy** screen. The navigation tree displayed in the left pane will be referenced in subsequent sections to navigate to items requiring configuration.



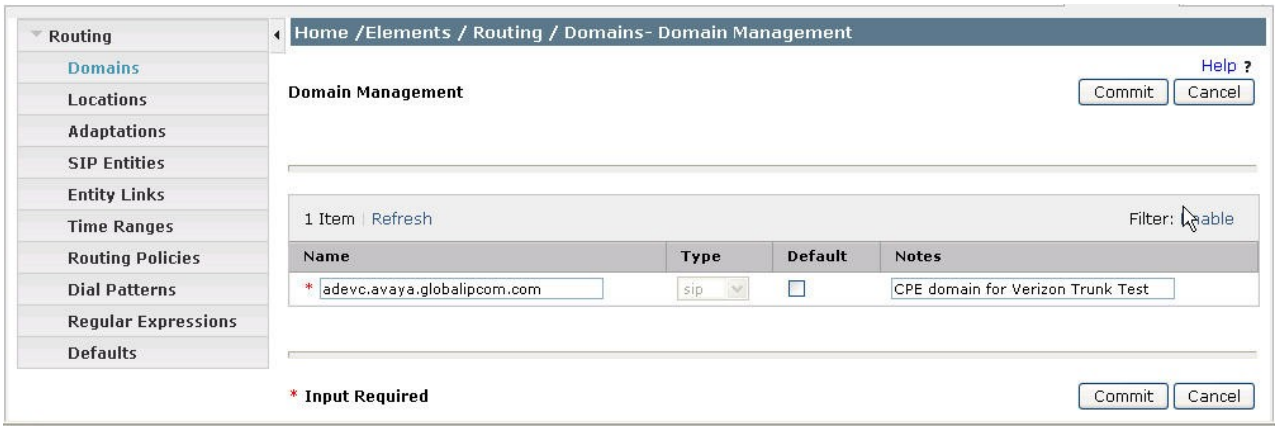
5.1. Domains

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.

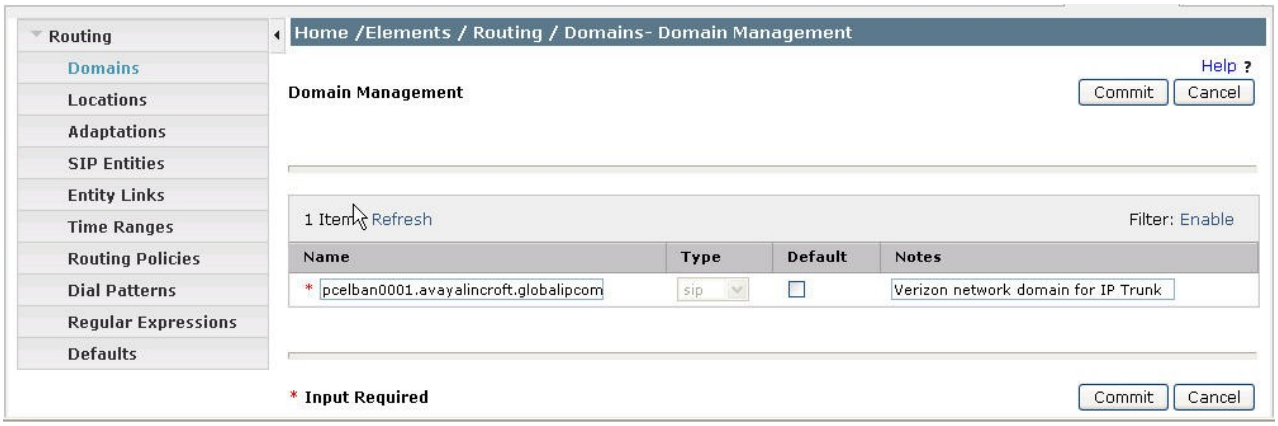
The following screen shows the list of configured SIP domains. The Session Manager used in the verification of these Application Notes was shared among many Avaya interoperability test efforts. The domain "avaya.com" was already being used for communication among a number of Avaya systems and applications, 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.



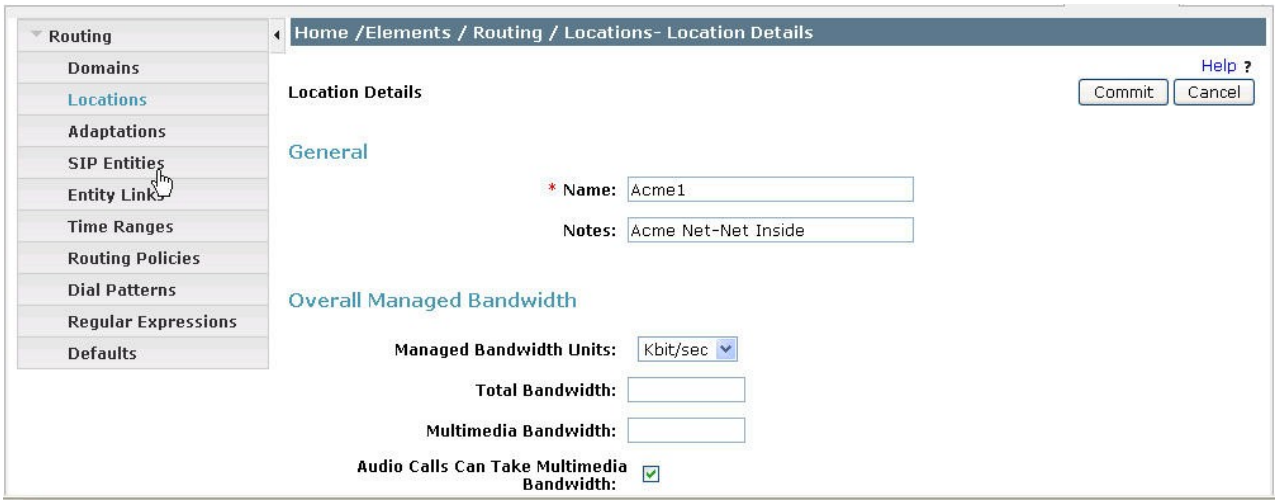
The domain "pcelban0001.avayalincroft.globalipcom.com" is associated with the Verizon network in the sample configuration. For example, for calls from the enterprise site to Verizon, this domain can appear in the Request-URI in the INVITE message sent to Verizon. The following screen shows the relevant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

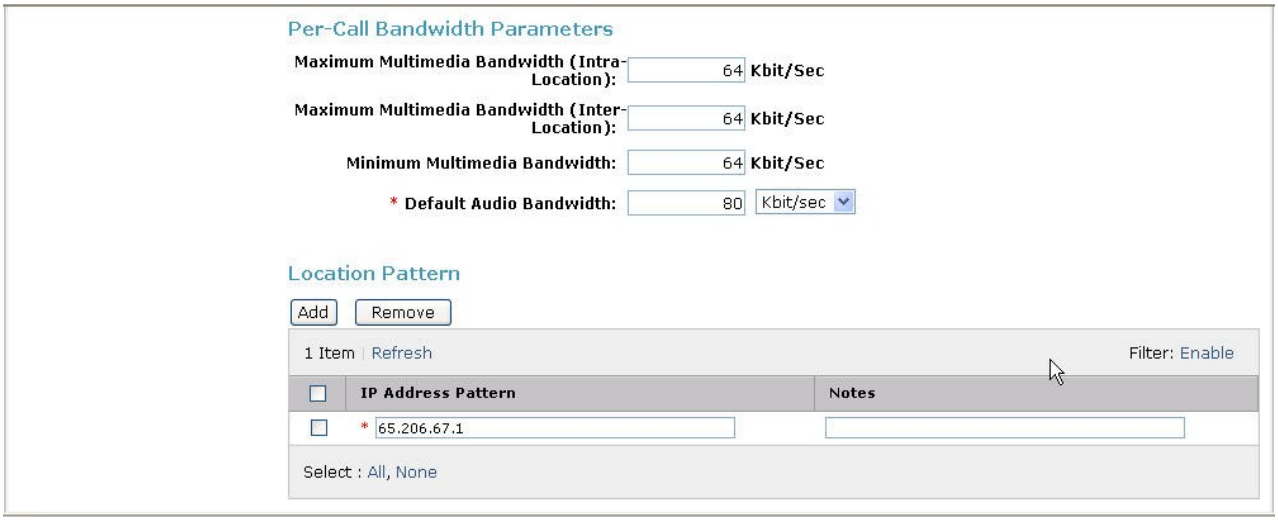


5.2. Locations

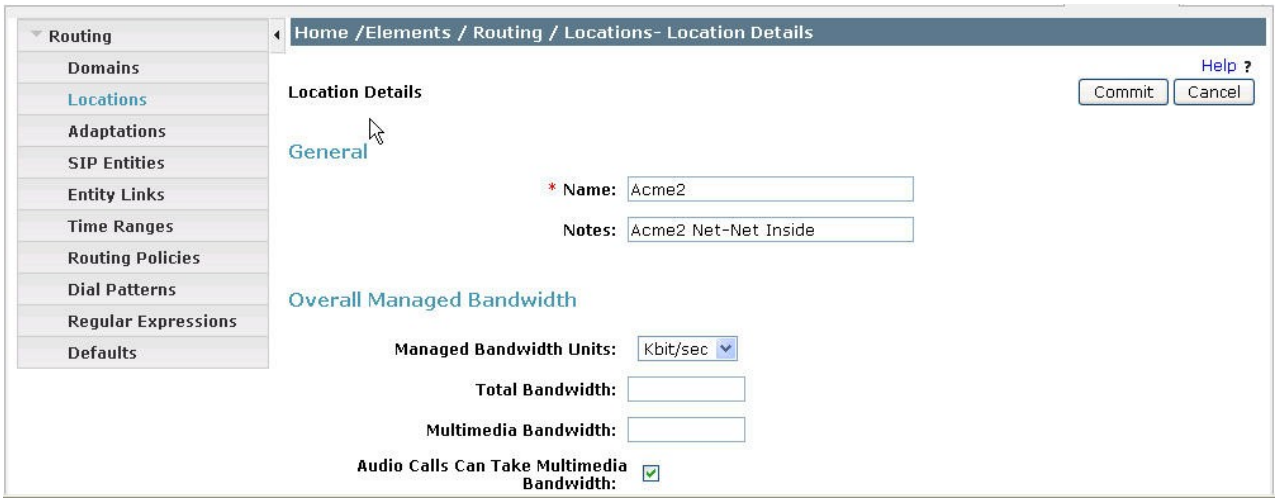
To view or change locations, select **Routing → Locations**. The following screen shows an abridged list of configured locations. Click on the checkbox corresponding to the name of a location and **Edit** to edit an existing location, or the **New** button to add a location. Click the **Commit** button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

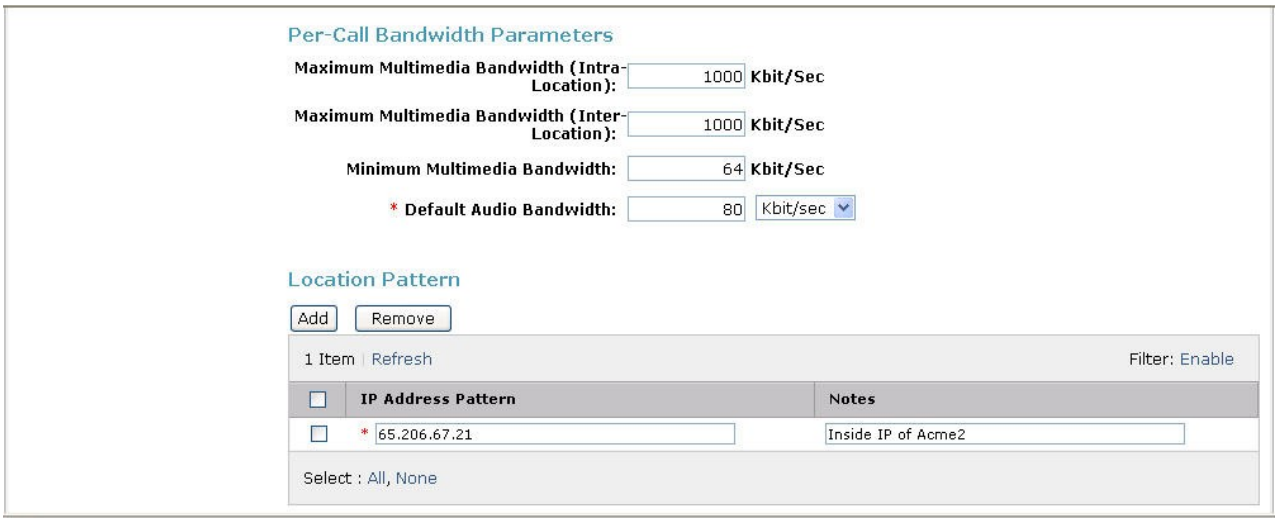
The following screens show upper and lower portions of the location details for the location named "Acme1", corresponding to the primary Acme Packet Net-Net SBC. Later, the location with name "Acme1" will be assigned to the corresponding SIP Entity. The IP address 65.206.67.1 of the inside (private) interface of "Acme1" is entered in the **IP Address Pattern** field. See Appendix, Section 12.4.2 in reference [JRR-VZIPT] if interested in using enhanced Call Admission Control with Overall Managed Bandwidth and Per-Call bandwidth Parameters in Session Manager 6.1.



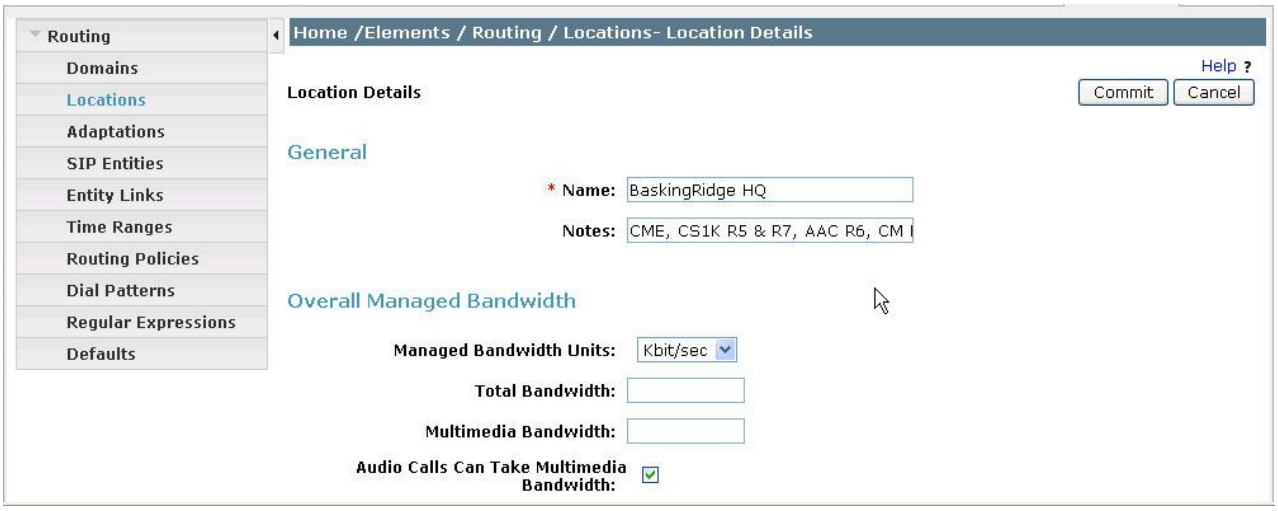


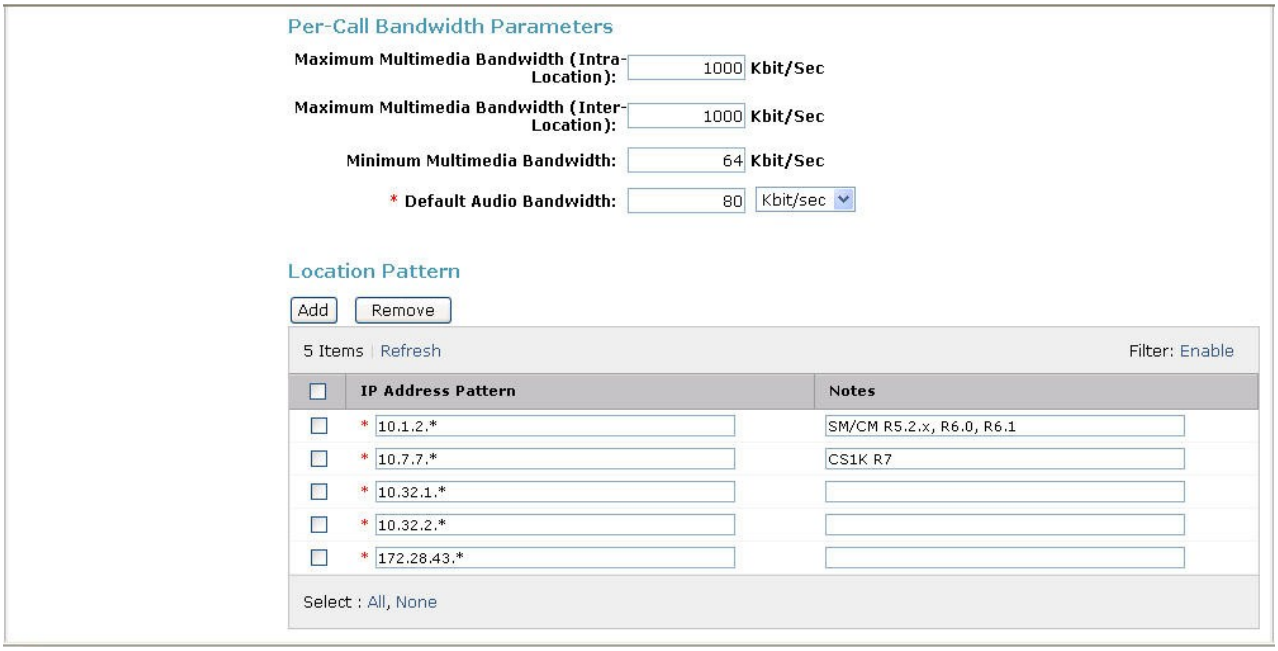
The following screens show the upper and lower portions of the location details for the location named "Acme2", corresponding to the second Acme Packet Net-Net SBC. Later, the location with name "Acme2" will be assigned to the corresponding SIP Entity. The IP address 65.206.67.21 of the inside (private) interface of "Acme2" is entered in the **IP Address Pattern** field.





The following screens show the upper and lower portions of the location details for the location named "BaskingRidgeHQ". The IP addresses administered for this location correspond to the shared components in the Avaya Solution and Interoperability Test Lab test environment, such as Communication Manager Release 5.2.1, Session Manager Release 6.1, and Avaya Modular Messaging servers.

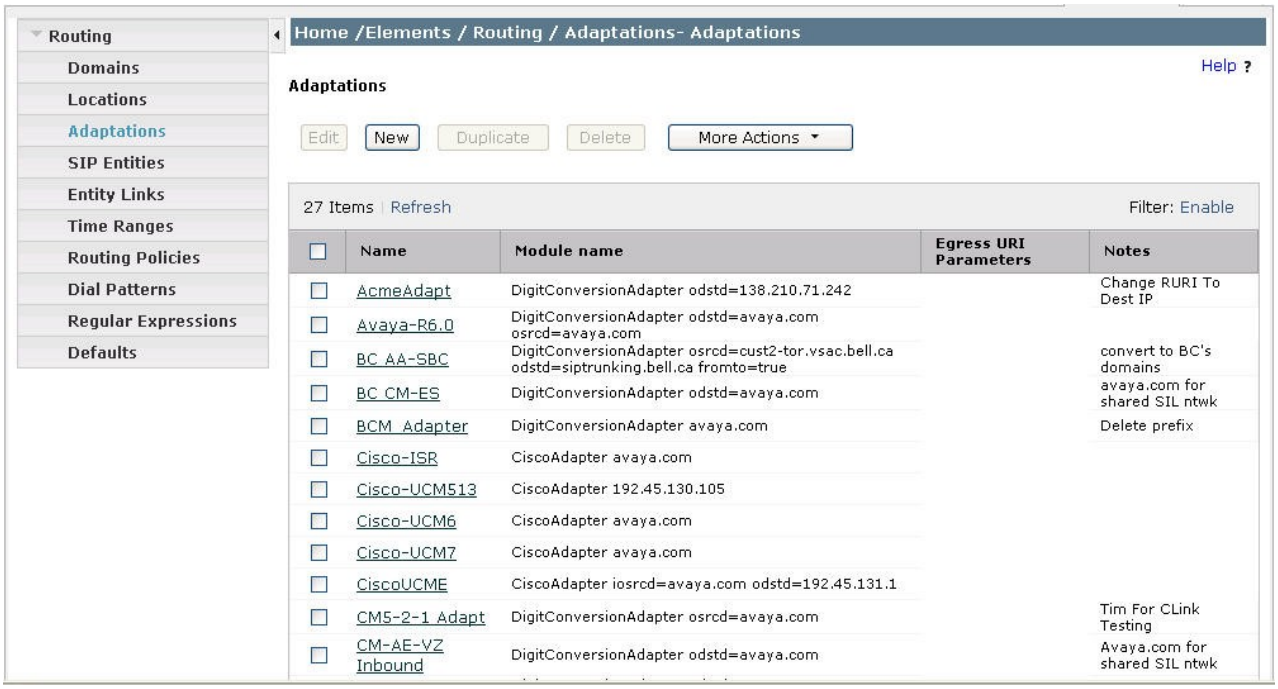




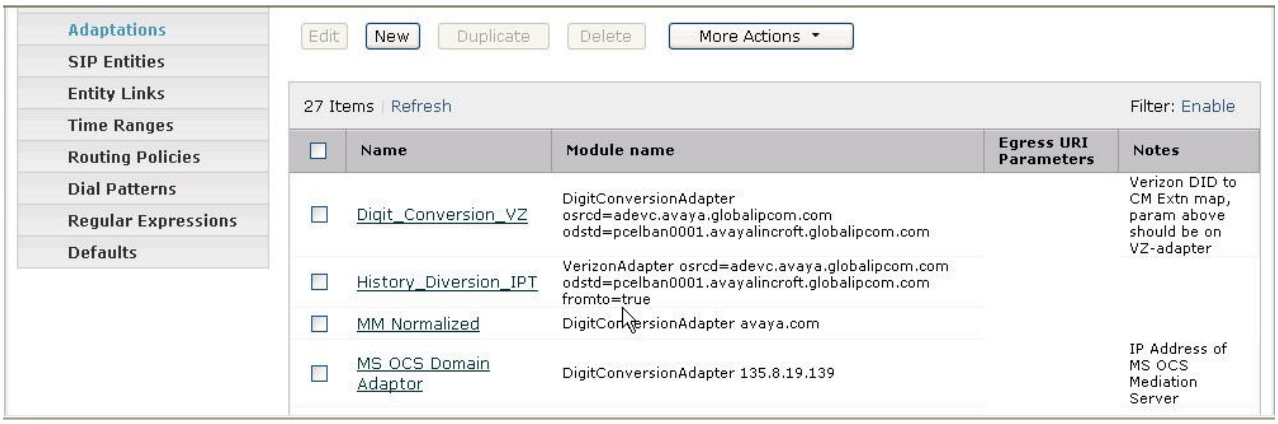
5.3. Adaptations

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.



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

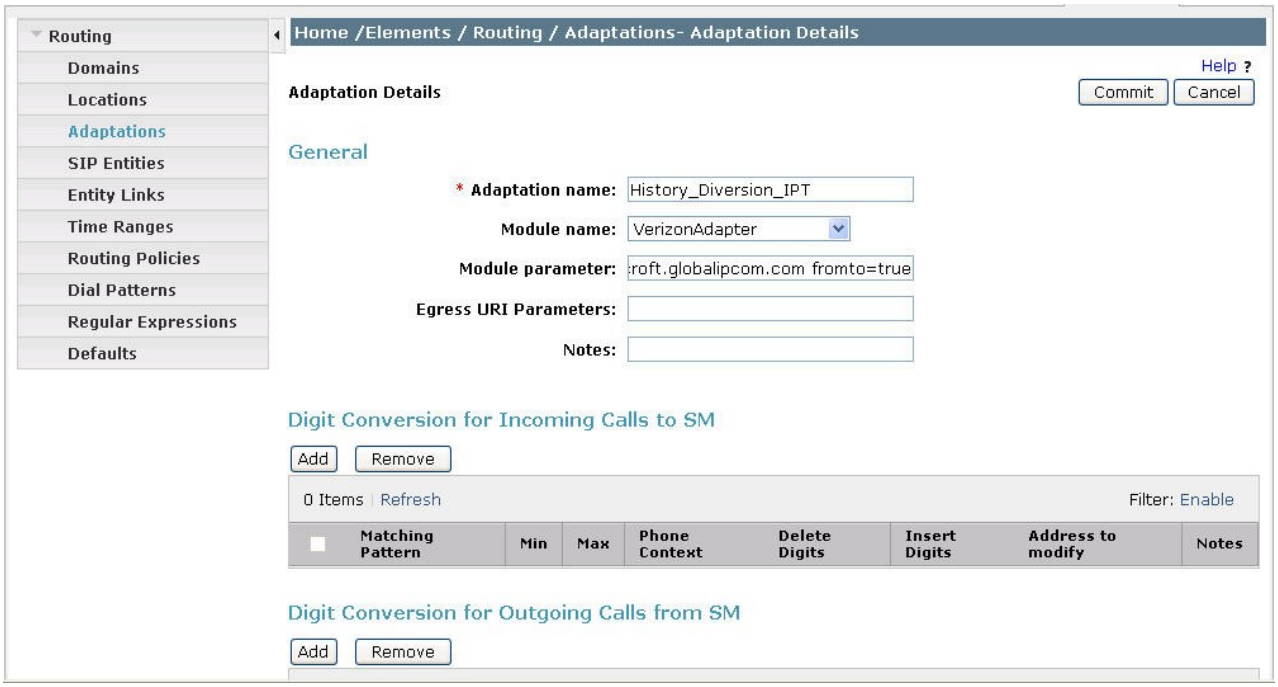


The adapter named "History_Diversion_IPT" listed in the second screen above will later be assigned to the Acme SIP Entities. This adaptation uses the "VerizonAdapter" and specifies three parameters that are used to adapt the FQDN to the domains expected by the Verizon network in the sample configuration.

- “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 will contain “pcelban0001.avayalincroft.globalipcom.com” as expected by Verizon.
- “fromto”=true”. With this configuration, for an outbound call to Verizon, Session Manager 6.1 will set the host portion of both the PAI and the From headers to “adevc.avaya.globalipcom.com”, and the host portion of the Request-URI and To headers to “pcelban0001.avayalincroft.globalipcom.com”

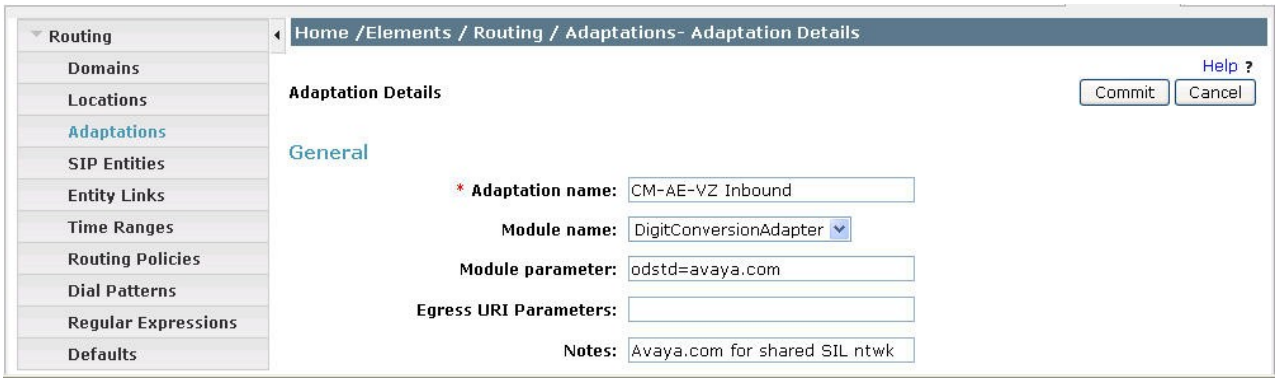
Depending on the Communication Manager configuration, it may not be necessary for Session Manager to adapt the domains in this fashion. In the sample configuration, where “avaya.com” was already in use in a shared Avaya environment, Session Manager was used to adapt the domain from “avaya.com” to “adevc.avaya.globalipcom.com”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

The screen below shows the History_Diversion_IPT adapter configured for the testing associated with these Application Notes:

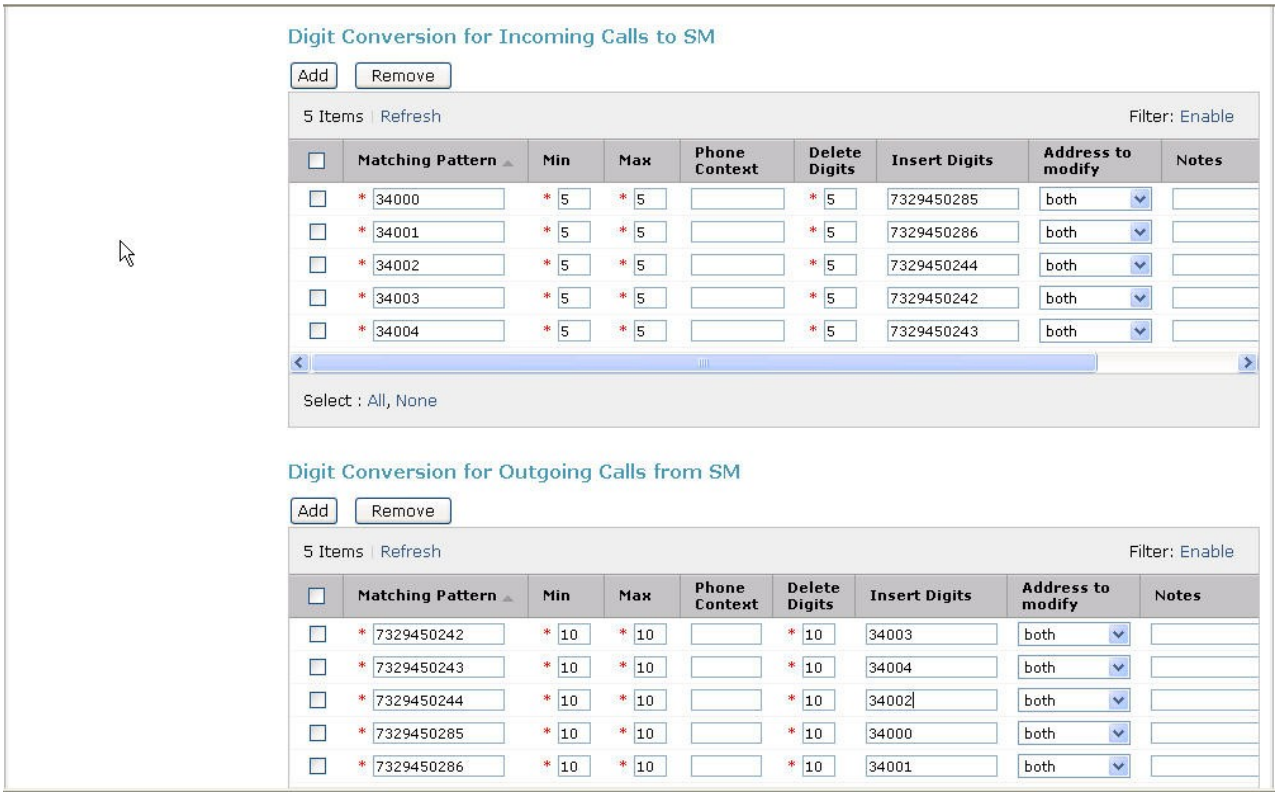


The adapter named “CM-AE-VZ Inbound” shown below will later be assigned to the Communication Manager SIP Entity for calls to and from Verizon. This adaptation uses the “DigitConversionAdapter” and specifies the “odstd=avaya.com” parameter to adapt the domain to the domain expected by Communication Manager 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 Solution and Interoperability Test 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-AE-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 applied to the Communication Manager SIP Entity later on, 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 that are routed by Session Manager to Communication Manager. In general, digit conversion such as this, that converts a Communication Manager extension (e.g., 34000) 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

5 Items | Refresh Filter: Enable

Matching Pattern	Min	Max	Phone Context	Delete Digits	Insert Digits	Address to modify	Notes
* 34000	* 5	* 5		* 5	7329450285	both	
* 34001	* 5	* 5		* 5	7329450286	both	
* 34002	* 5	* 5		* 5	7329450244	both	
* 34003	* 5	* 5		* 5	7329450242	both	
* 34004	* 5	* 5		* 5	7329450243	both	

Select : All, None

Digit Conversion for Outgoing Calls from SM

Add Remove

5 Items | Refresh Filter: Enable

Matching Pattern	Min	Max	Phone Context	Delete Digits	Insert Digits	Address to modify	Notes
* 7329450242	* 10	* 10		* 10	34003	both	
* 7329450243	* 10	* 10		* 10	34004	both	
* 7329450244	* 10	* 10		* 10	34002	both	
* 7329450285	* 10	* 10		* 10	34000	both	
* 7329450286	* 10	* 10		* 10	34001	both	

In the example shown above, if a user on the PSTN dials 732-945-0285, Session Manager will convert the number to 34000 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 34000 dials the PSTN, and if Communication Manager sends the extension 34000 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 34000 to 7329450285 before sending the call on the trunk group to Session Manager (as shown in **Section 4.10**). 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.

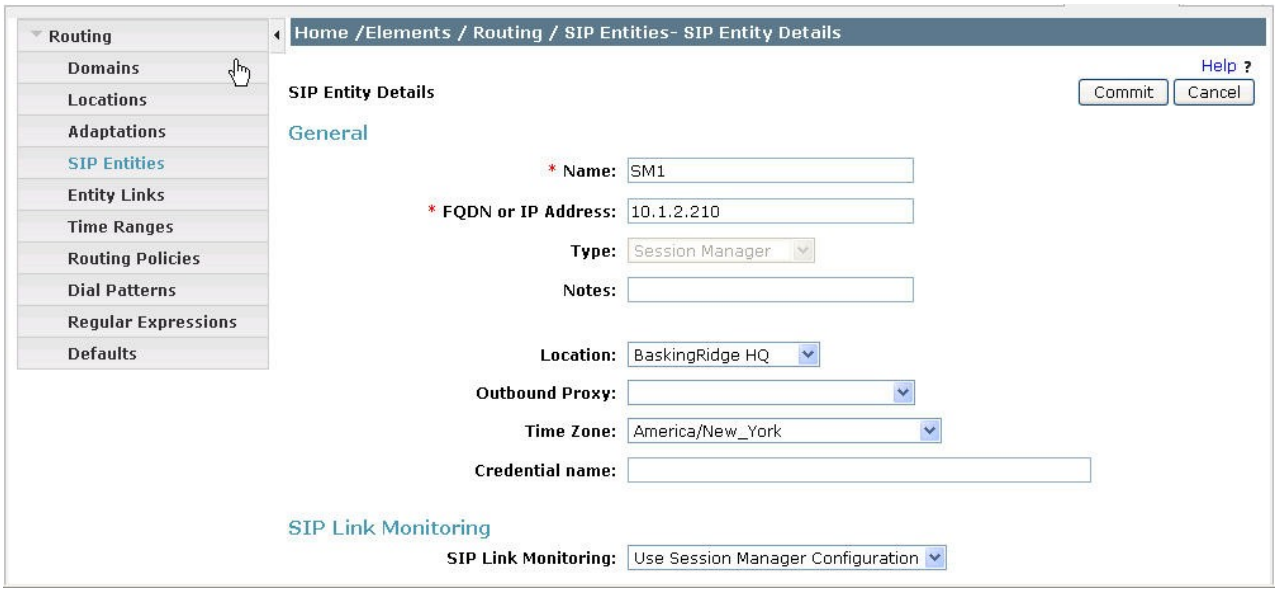
The following screen shows a portion of the list of configured SIP entities. In this screen, the SIP Entities named "Acme1", "Acme2" (corresponding to the two Acme Packet Net-Net SBC's) and "alpinemas1" (corresponding to Modular Messaging Application Server) are relevant to these Application Notes. Other relevant SIP Entities named "CM521-AE-clan1-5067" for Communication Manager (configured as Access Element) and "SM1" for Session Manager are listed in other pages of the SIP Entity list (not shown).

47 Items | Refresh Filter: Enable

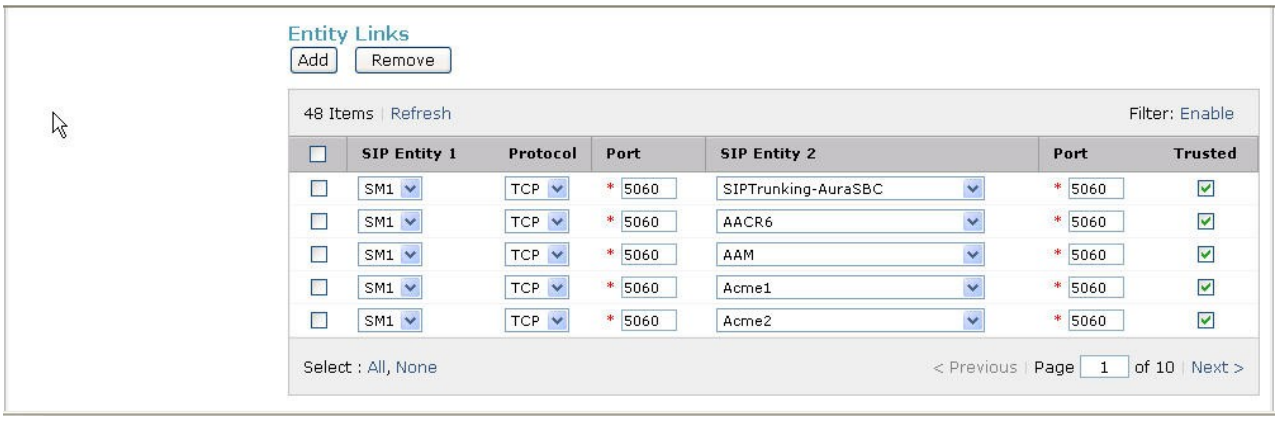
Name	FQDN or IP Address	Type	Notes
AACR6	10.7.7.185	Other	Avaya Aura Conferencing R6
AAM	135.8.139.136	Modular Messaging	For use by Tony M's group
ACE	10.32.48.26	SIP Trunk	ACE R2.2.3 James Liu
Acme1	65.206.67.1	Other	Inside IP Acme1
Acme2	65.206.67.21	Other	Acme2 Inside
AG2330	192.168.75.160	Other	
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
BCM50 R6	10.7.7.221	Other	
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 2921 SRST	120.1.1.1	Other	Branch 2

Select : All, None < Previous | Page 1 of 4 | Next >

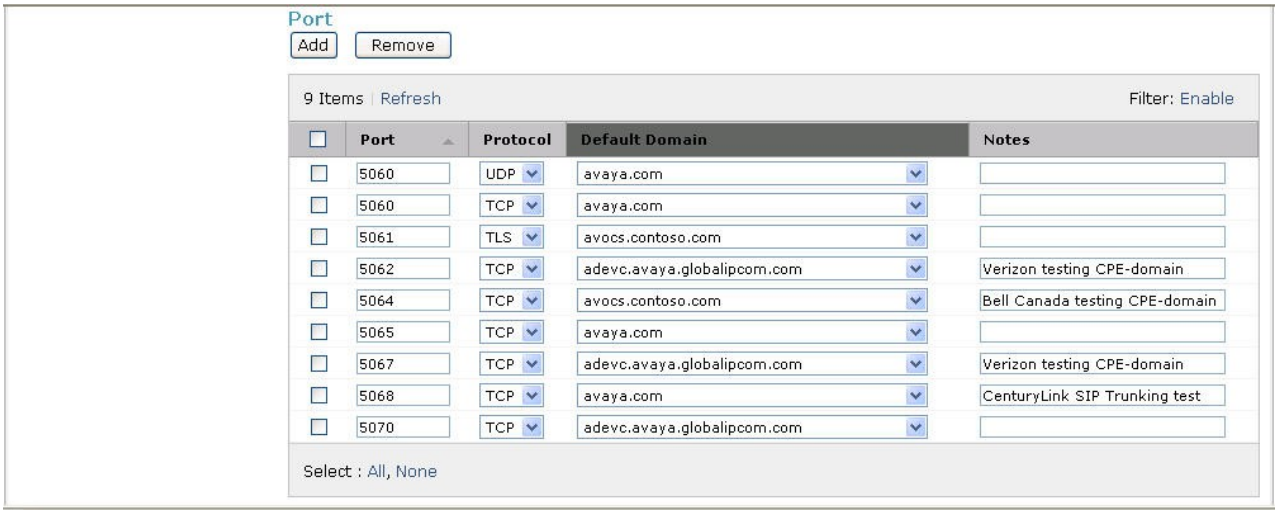
The following screen shows the upper portion of the **SIP Entity Details** corresponding to "SM1". The **FQDN or IP Address** field for "SM1" is the Session Manager signaling interface IP address (10.1.2.210), which is used for SIP signaling with other networked SIP entities. The **Type** for this SIP 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.



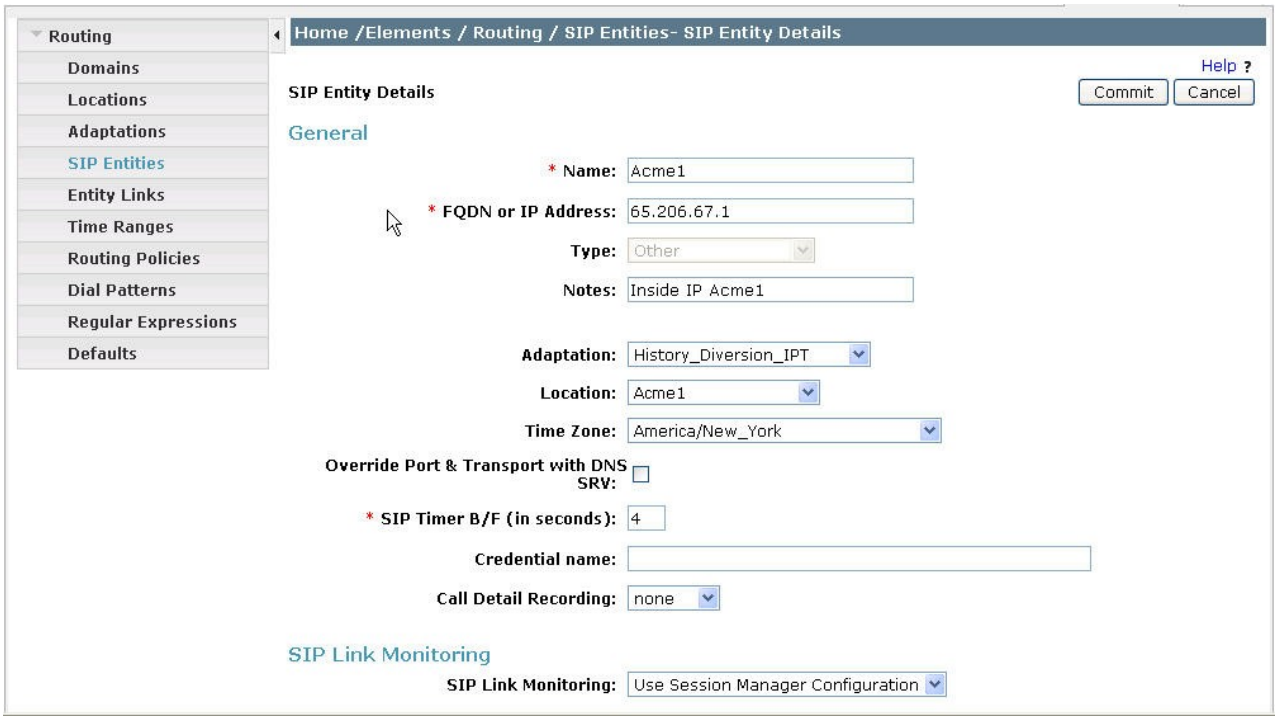
Scrolling down, the following screen shows the middle portion of the **SIP Entity Details**, a listing of the **Entity Links** previously configured for "SM1". The links relevant to these Application Notes are described in the following section.



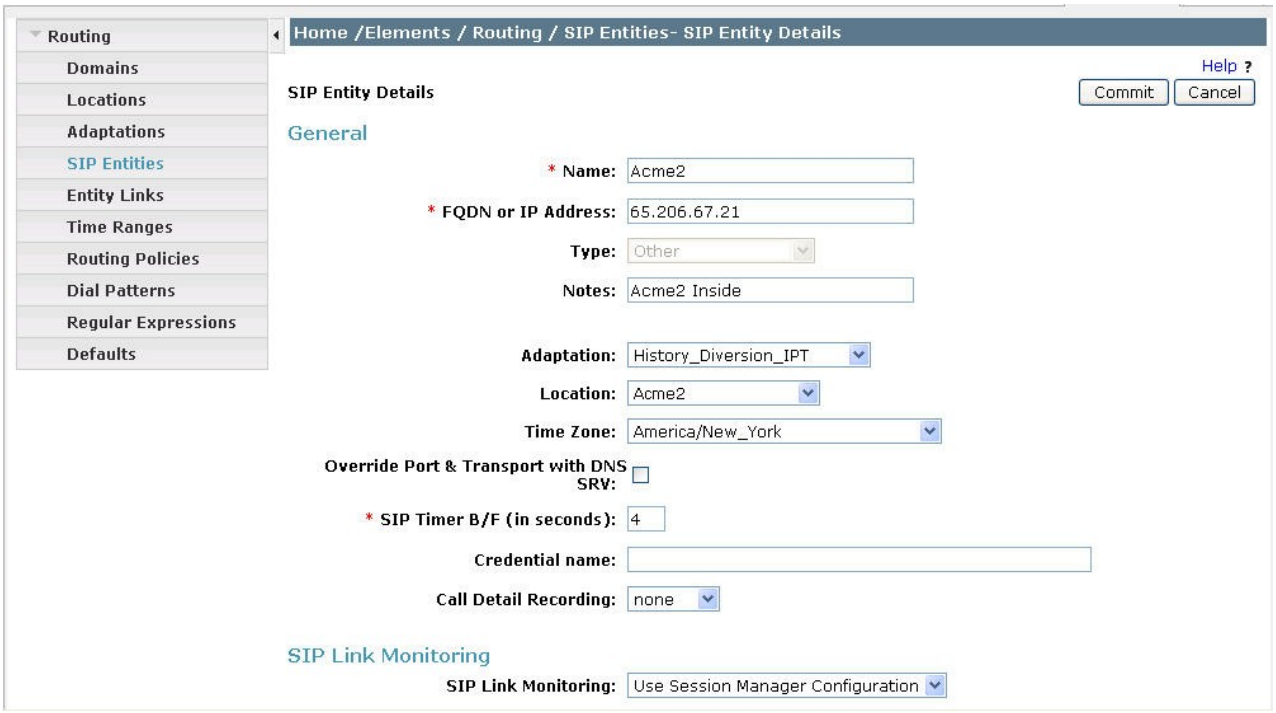
Scrolling down, the following screen shows the lower portion of the **SIP Entity Details**, a listing of the configured ports for "SM1". In the sample configuration, TCP port 5060 was already in place for the shared test environment, using **Default Domain** "avaya.com". To enable Communication Manager to distinguish inbound calls from Verizon from other types of SIP calls arriving from the same Session Manager, TCP port 5067 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 for debugging/tracing purposes during testing; TLS may be used in production.



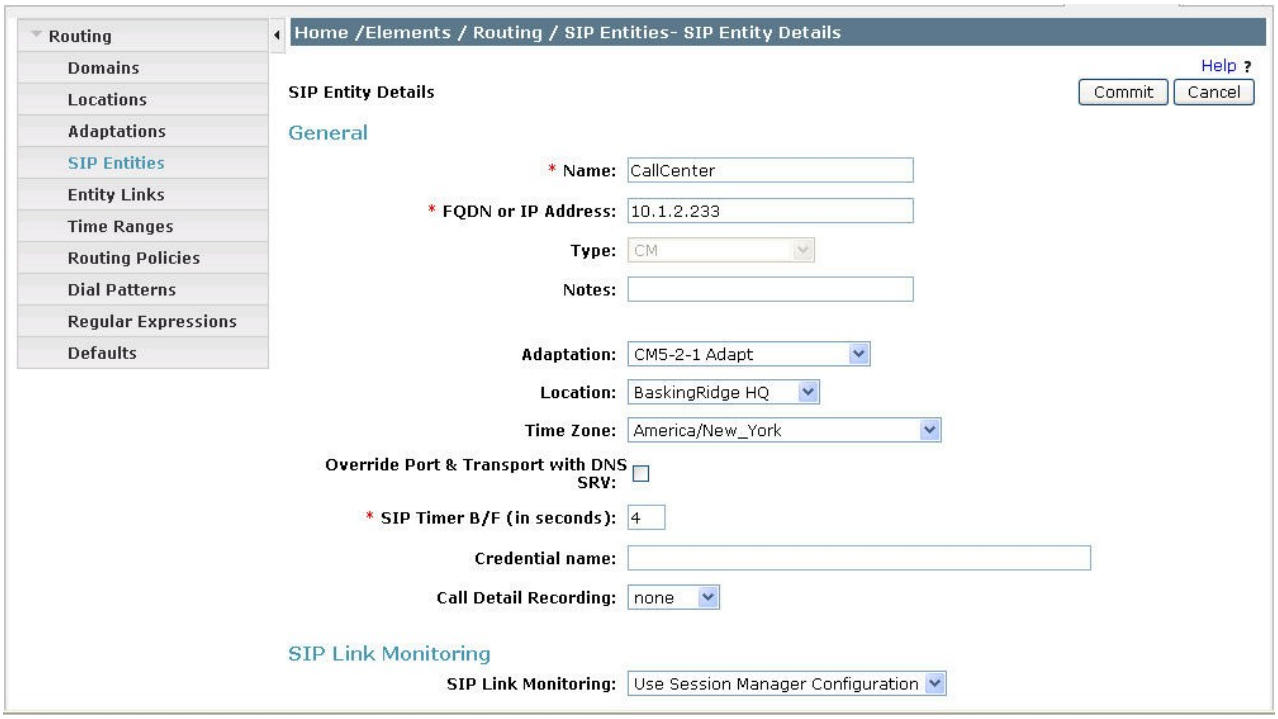
The following screen shows the **SIP Entity Details** corresponding to "Acme1". The **FQDN or IP Address** field is configured with the Acme Packet Net-Net SBC inside IP address (65.206.67.1). "Other" is selected from the **Type** drop-down menu for SBC SIP Entities. This Acme Packet Net-Net SBC has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



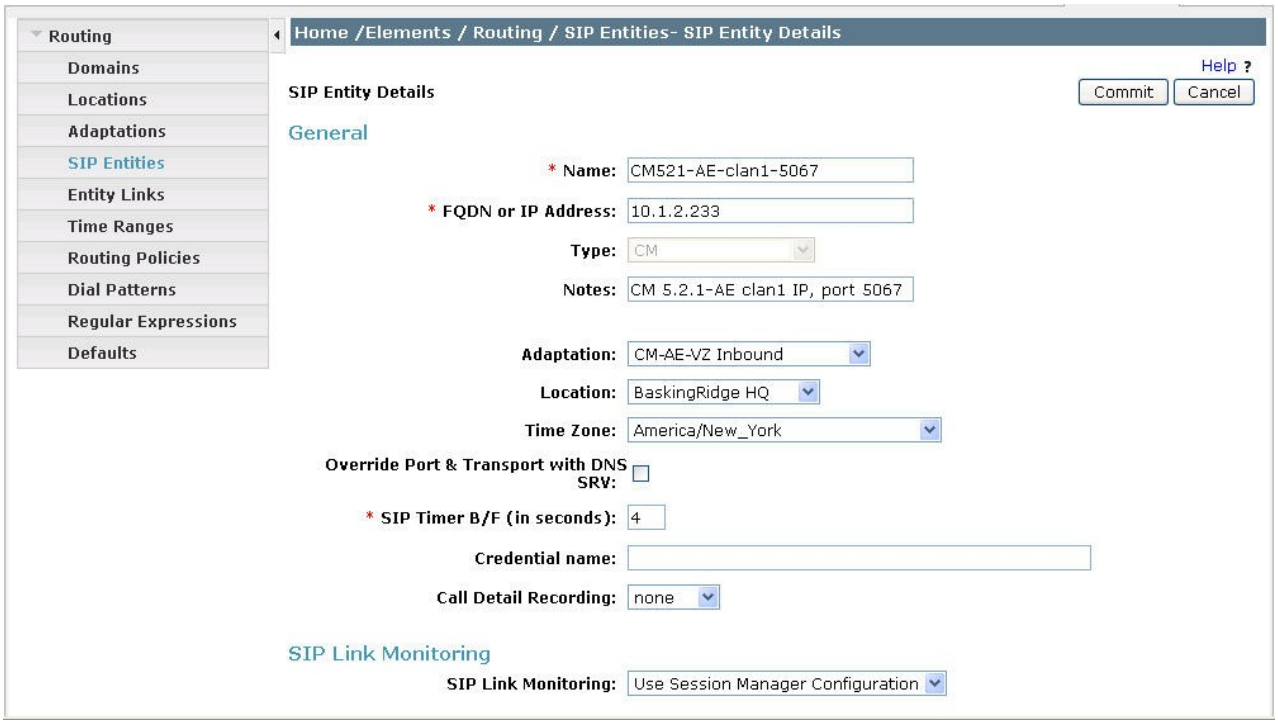
The following screen shows the **SIP Entity Details** corresponding to "Acme2". The **FQDN or IP Address** field is configured with the second Acme Packet Net-Net SBC inside IP address (65.206.67.21). "Other" is selected from the **Type** drop-down menu for SBC SIP Entities. This Acme Packet Net-Net 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 "CallCenter" This is the SIP Entity that was already in place in the shared Avaya Solution and Interoperability Test Lab test environment, prior to adding the Verizon IP Trunk configuration. The **FQDN or IP Address** field contains the IP address of the CLAN card in the Avaya G650 Media Gateway controlled by Communication Manager. "CM" is selected from the **Type** drop-down menu. In the shared test environment, the **Adaptation** "CM5-2-1 Adapt" and **Location** "BaskingRidge HQ" had already been assigned to this Communication Manager SIP entity.



The following screen shows the **SIP Entity Details** for an entity named "CM521-AE-clan1-5067". This entity uses the same **FQDN or IP Address** (10.1.2.233) as the prior entity with name "CallCenter"; both correspond to the IP address of the CLAN card in the Avaya G650 Media Gateway controlled by Communication Manager. Later, a unique port, 5067, will be used for the Entity Link between Session Manager and Communication Manager named "CM521-AE-clan1-5067". 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-AE-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.



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", "CM521-AE-clan1-5067", and "CallCenter" 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**.

48 Items | Refresh Filter: Enable

Name	SIP Entity 1	Protocol	Port	SIP Entity 2	Port	Trusted	Notes
AACR6	SM1	TCP	5060	AACR6	5060	☑	
AAM-SM1-TCP	SM1	TCP	5060	AAM	5060	☑	Between SM1 and AAM
Acme1	SM1	TCP	5060	Acme1	5060	☑	
Acme2	SM1	TCP	5060	Acme2	5060	☑	
AG2330	SM1	TCP	5060	AG2330	5080	☑	
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	☑	
Cisco UCME 513	SM1	TCP	5060	CUCM-513	5060	☑	
CiscoUCME-Link	SM1	TCP	5060	CiscoUCME	5060	☑	
CiscoUCME-Link-UDP	SM1	UDP	5060	CiscoUCME	5060	☑	
CM521-AE-clan1-5067	SM1	TCP	5067	CM521-AE-clan1-5067	5067	☑	For Verizon IP Trunk testing
CM521-AE-clan1-5068	SM1	TCP	5068	CM521-AE-clan1-5068	5068	☑	
CM521-ForSPs	SM1	TLS	5066	CM5-2-1	5066	☑	Tim Link to CM for SPs

Select : All, None < Previous | Page 1 of 4 | Next >

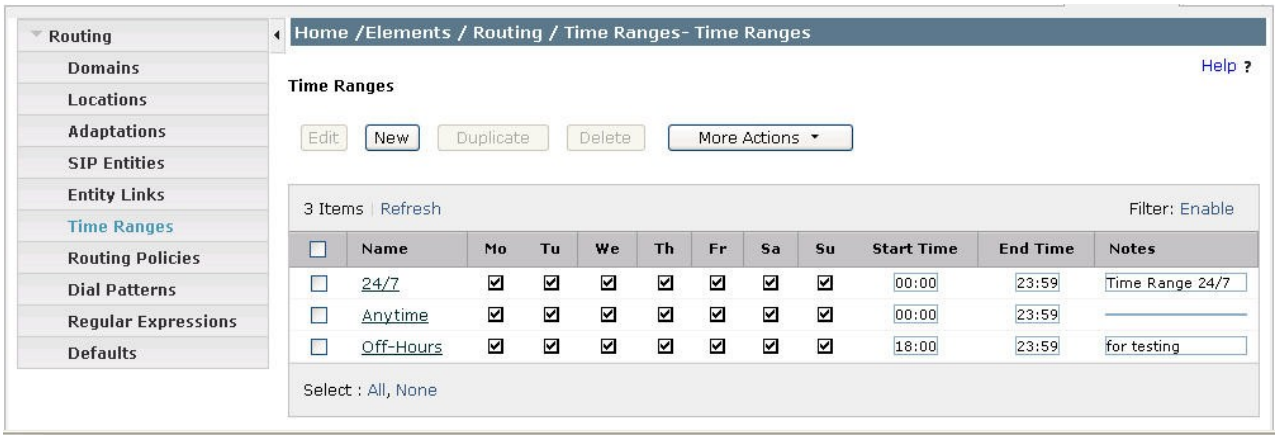
The link named "CallCenter" existed in the shared configuration prior to adding the Verizon IP Trunk-related configuration. This link, using port 5060, can carry traffic between Session Manager and Communication Manager that is not necessarily related to calls with Verizon, such as traffic related to SIP Telephones registered to Session Manager, or traffic related to Avaya Modular Messaging, which has SIP integration to Session Manager.

The link named "CM521-AE-clan1-5067" also links Session Manager "SM1" with the same Communication Manager. However, this link uses port 5067 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.

5.6. Time Ranges

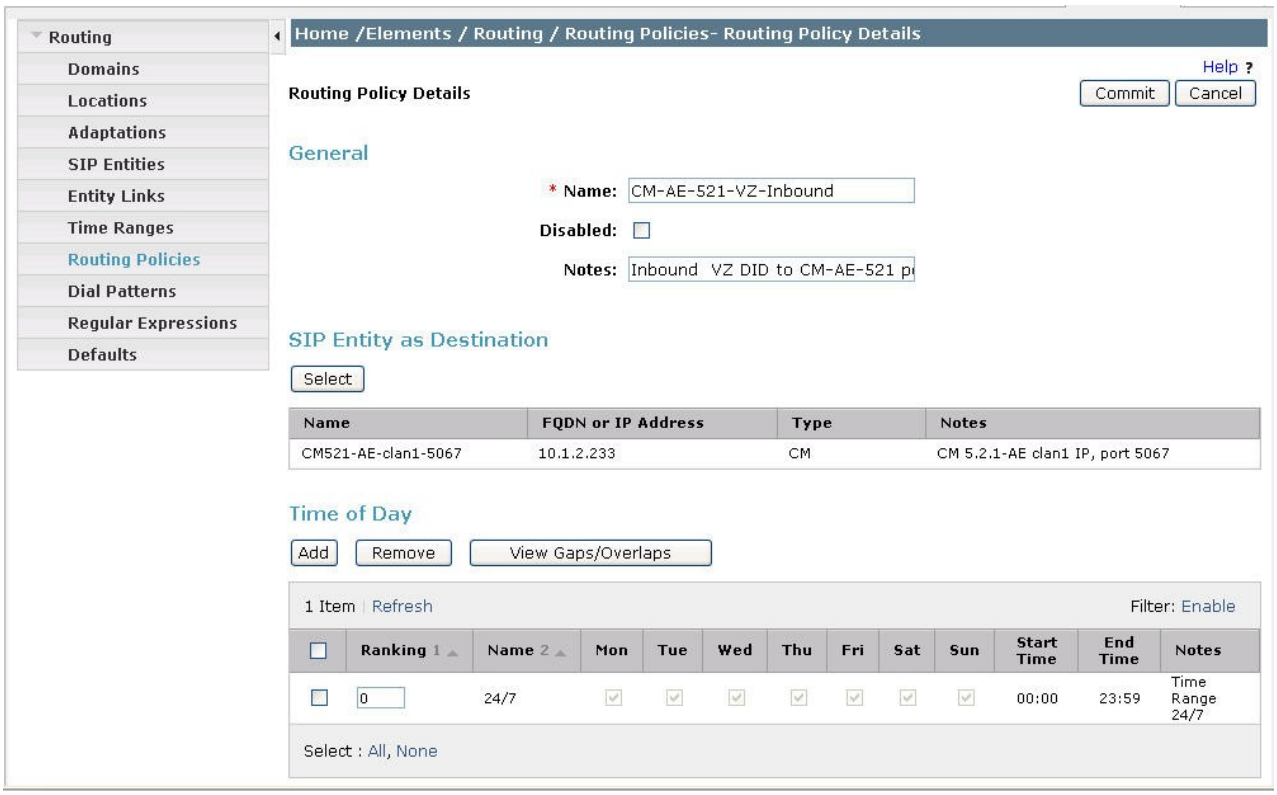
To view or change Time Ranges, select **Routing → Time Ranges**. The Routing Policies shown subsequently will use the "24/7" range since time-based routing was not the focus of these Application Notes.



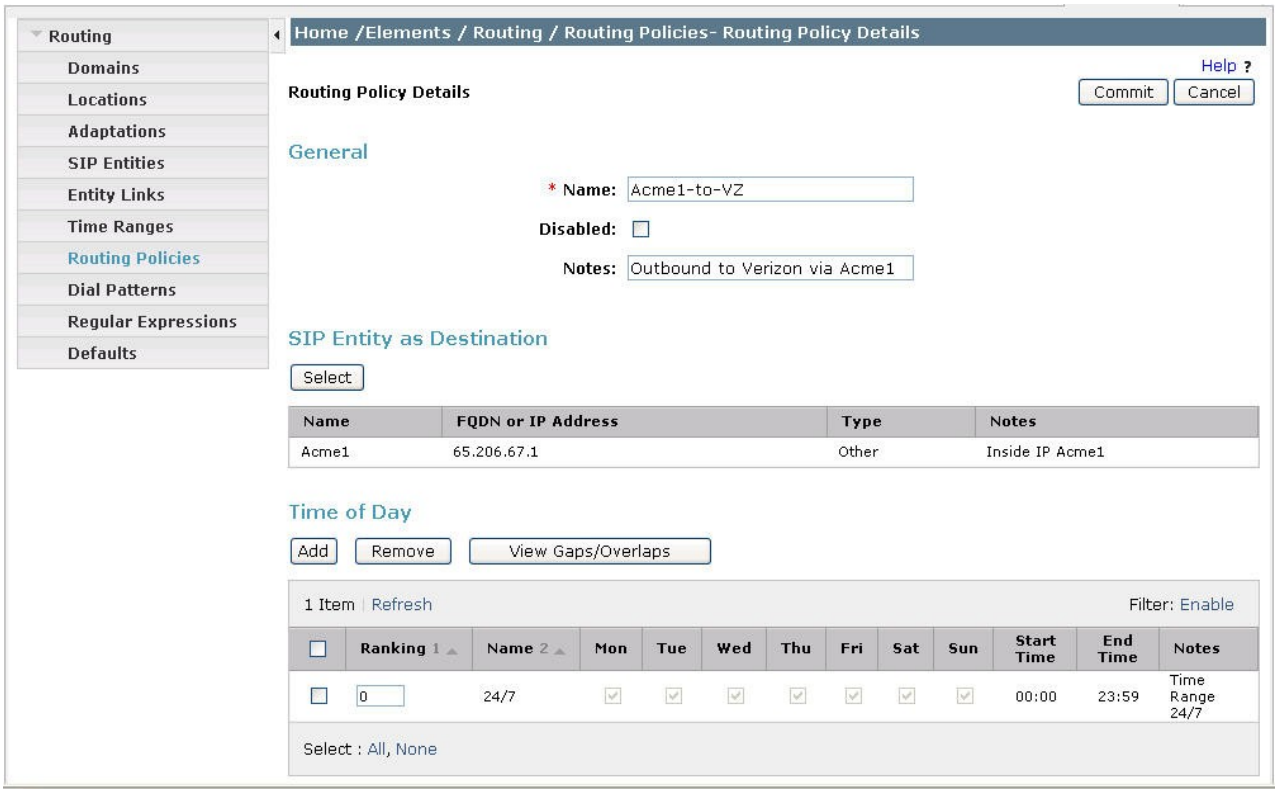
5.7. Routing Policies

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.

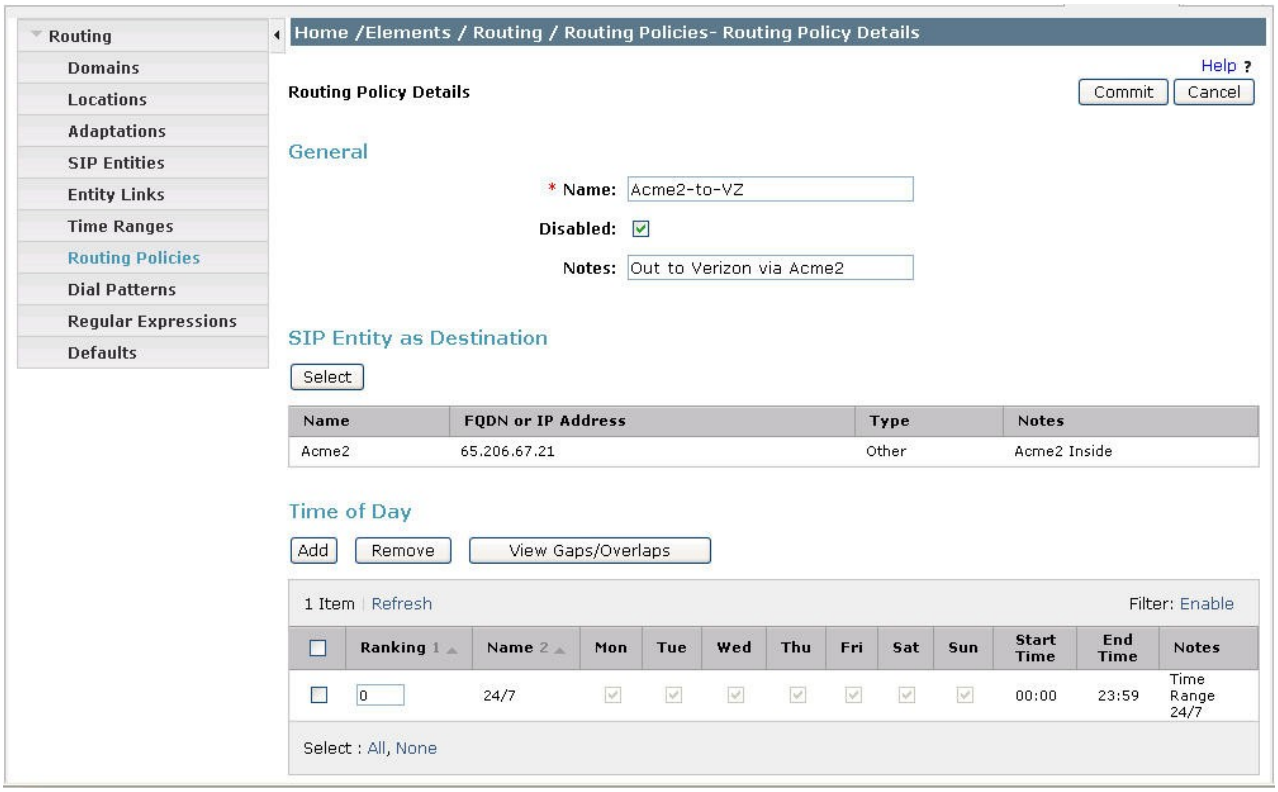
The following screen shows the **Routing Policy Details** for the policy named "CM-AE-521-VZ-Inbound" associated with incoming PSTN calls from Verizon to Communication Manager. Observe the **SIP Entity as Destination** is the entity named "CM521-AE-clan1-5067". After dial patterns are assigned to use this routing policy, the lower portion of the screen will show the dial patterns using the routing policy.



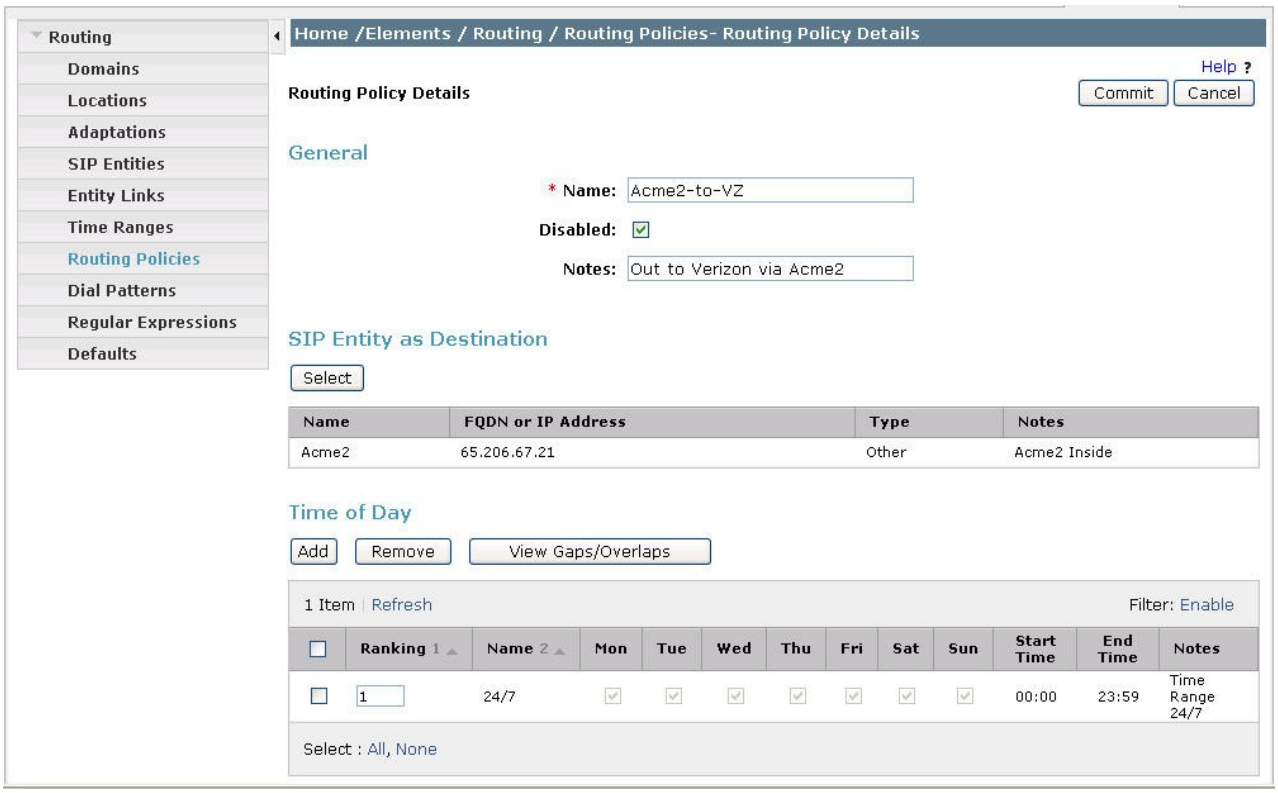
The following screen shows the **Routing Policy Details** for the policy named "Acme1-to-VZ" associated with outgoing calls from Communication Manager to the PSTN via Verizon through Acme1. Observe the **SIP Entity as Destination** is the entity named "Acme1". After dial patterns are assigned to use 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.



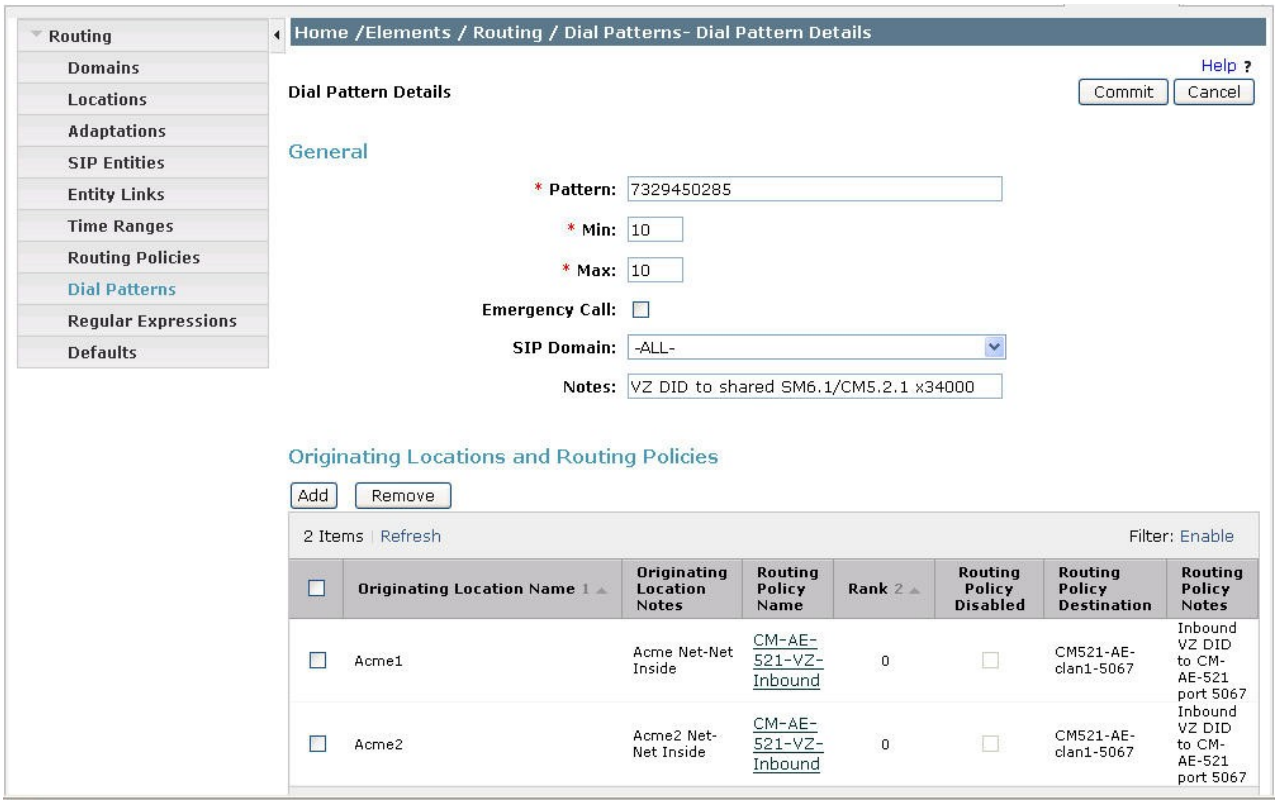
If it is intended that Acme1 should always be tried by Session Manager before Acme2, the rank of Acme2 can be changed to 1 as shown below. Both the "load sharing" approach where Acme1 and Acme2 use the same rank, and the strict rank order priority of Acme1 over Acme2 were successfully tested in the sample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



5.8. Dial Patterns

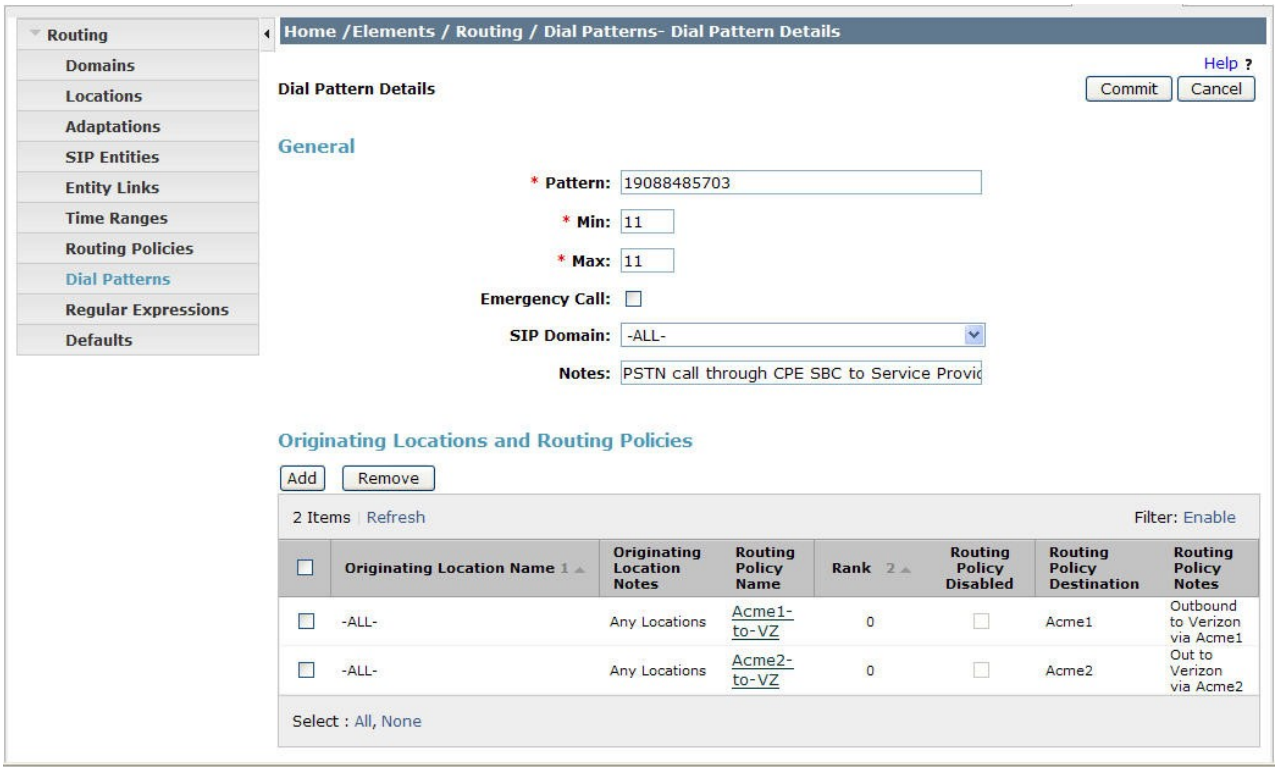
To view or change dial patterns, select **Routing → Dial Patterns**. Click on the checkbox corresponding to the name of a pattern and **Edit** to edit an existing pattern, or **New** to add a pattern. Click the **Commit** button after changes are completed.

The following screen illustrates a sample dial pattern used to verify inbound PSTN calls to the enterprise. When a user on the PSTN dials a number assigned to the Verizon IP Trunk service, such as 732-945-0285, 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-AE-521-VZ-Inbound" is selected, which sends the call to Communication Manager using port 5067 as described previously. Two entries are created, one for **Originating Location Name** "Acme1" and the other for "Acme2".

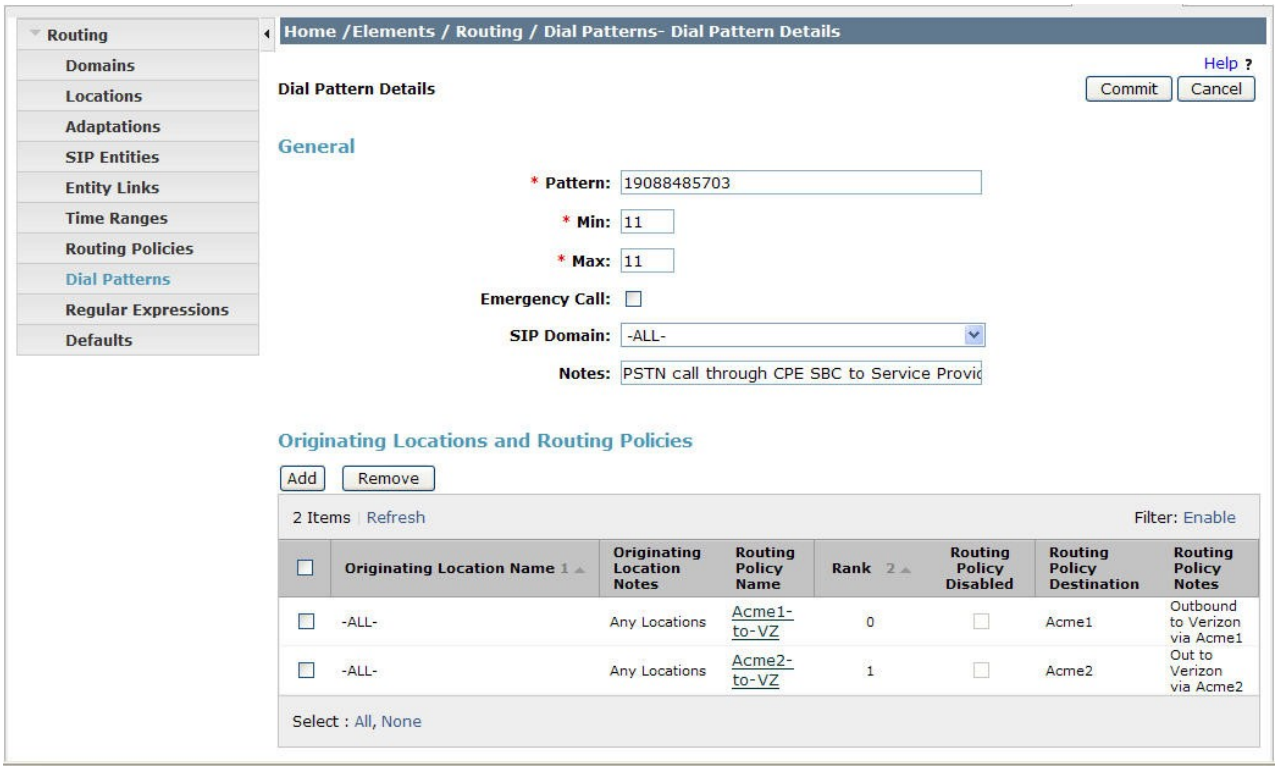


The following screen illustrates an example dial pattern used to verify outbound calls from the enterprise to the PSTN. When a Communication Manager user dials a PSTN number via ARS such as 1-908-848-5703, Communication Manager sends the call to Session Manager. Session Manager will match the dial pattern 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.

Dial Patterns

Add Remove

17 Items | Refresh Filter: Enable

Pattern	Min	Max	Emergency Call	SIP Domain	Originating Location	Notes
0	1	1		pcelban0001.avayalincroft.globalipcom.com	-ALL-	To Tim's SP
0	11	11		-ALL-	-ALL-	Verizon IP Trunk Test Plan TC30, TC31
00	2	2		-ALL-	-ALL-	Verizon IP Trunk Test Plan TC33
01	12	20		-ALL-	-ALL-	Verizon IP Trunk Test Plan TC34
011	13	15		pcelban0001.avayalincroft.globalipcom.com	-ALL-	Verizon IP Trunk Test Plan TC18
1411	4	4		-ALL-	-ALL-	Verizon IP Trunk Test Plan TC25
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 TC40
19088485579	11	11		-ALL-	-ALL-	John R Real Number used for testing VZ
19088485703	11	11		-ALL-	-ALL-	PSTN call through CPE SBC to Service Provider
19088485704	11	11		-ALL-	-ALL-	PSTN Telephone at Verizon workbench
1976	11	11		-ALL-	-ALL-	Verizon IP Trunk Test Plan TC41
411	3	3		-ALL-	-ALL-	Verizon IP Trunk Test Plan TC24
511	3	3		-ALL-	-ALL-	Verizon IP Trunk Test Plan TC28

Select : All, None < Previous | Page 1 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 Avaya Aura® Session Manager and Avaya Aura® 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 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 may be 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. P-Location Header Removal

For an outbound call from a Communication Manager user to the PSTN, Session Manager Release 6.1 inserts a P-Location header into the INVITE message sent to the SBC. For an inbound call from the PSTN to a Communication Manager user, Session Manager Release 6.1 inserts a P-Location header into the 200 OK message sent to the SBC when the call is answered. The presence of the P-Location header does not present a problem for calls to or from the Verizon IP Trunk Service. However, since there may be no value in sending this header to Verizon, and since tracing tools may flag this header as an unknown header, this section shows a sample SBC configuration to strip the P-Location header in the SBC so that Verizon does not receive it.

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-Location header, an additional header rule is added to the existing NAT_IP manipulation retained from reference [JF-JRR-VZIPT]. This new header-rule to delete the P-Location header is shown below.

```
header-rule
```

```
name                delPLocation
header-name          P-Location
action              delete
comparison-type     pattern-rule
match-value
msg-type             any
new-value
methods
```

With this header rule configured and activated, the P-Location header inserted by Session Manager Release 6.1 will not be sent to Verizon.

6.3. 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 Solution and Interoperability Test 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.

6.4. 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 "7329450287" 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
```

6.5. Session Agent for Session Manager Release 6.1

Conceptually, the session agent configured for Session Manager Release 6.1 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                10.1.2.210
        ip-address              10.1.2.210
        port                    5060
        state                   enabled
        app-protocol            SIP
        transport-method        StaticTCP
        realm-id                INSIDE
```

```
description              Fred-SM61
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
```

6.6. Session Agent Group for Session Manager Release 6.1

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            Hunt
        dest                10.1.2.210
```

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 Test 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 sample 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 and retrieval.
- 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 Avaya Aura® Communication Manager.

9.1.1 Sample 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 connecting Session Manager to Communication Manager using port 5067. On Communication Manager, the incoming call arrives via signaling group 67 and trunk group 67.

The following 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 (x34000), 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 34000 is an IP soft phone with IP address 10.1.2.42 in Region 54. Initially, the G650 Media Gateway provides the media resources for the call, but as can be seen in the final trace output, once the call is answered, the final RTP media path is "ip-direct" from the IP Telephone (10.1.2.42) to the "inside" of an Acme Packet Net-Net SBC (65.206.67.1).

```
list trace tac 167                                                    Page   1

                                LIST TRACE

time            data

08:41:52 SIP<INVITE sip:34000@avaya.com:5060;transport=tcp  SIP/
08:41:52 SIP<2.0
08:41:52     active trunk-group 67 member 1  cid 0x6f1
08:41:52 SIP>SIP/2.0 180 Ringing
08:41:52     dial 34000
08:41:52     ring station    34000 cid 0x6f1
08:41:52     G729A ss:off ps:20
             rgn:54 [10.1.2.42]:2740
             rgn:1 [10.1.2.235]:6000
08:41:52     G729 ss:off ps:20
             rgn:54 [65.206.67.1]:50226
             rgn:1 [10.1.2.235]:5992
08:41:52     xoip options: fax:off modem:off tty:US  uid:0x5011d
             xoip ip: [10.1.2.235]:5992
08:41:54 SIP>SIP/2.0 200 OK
```

```
list trace tac 167                                                    Page   2

                                LIST TRACE

time            data
08:41:54     active station    34000 cid 0x6f1
08:41:55 SIP<ACK sip:7329450285@10.1.2.233:5067;transport=tcp  S
08:41:55 SIP<IP/2.0
08:41:55 SIP>INVITE sip:9088485703@65.206.67.1:5060;transport=tc
08:41:55 SIP>p SIP/2.0
08:41:55 SIP<SIP/2.0 100 Trying
08:41:55 SIP<SIP/2.0 200 OK
08:41:55 SIP>ACK sip:9088485703@65.206.67.1:5060;transport=tcp S
08:41:55 SIP>IP/2.0
08:41:55     G729A ss:off ps:20
             rgn:54 [65.206.67.1]:50226
             rgn:54 [10.1.2.42]:2740
08:41:55     G729 ss:off ps:20
             rgn:54 [10.1.2.42]:2740
             rgn:54 [65.206.67.1]:50226
```

The following screen shows **Page 2** of the output of the ***status trunk*** command pertaining to this same call. Note the signaling using port 5067 between Communication Manager and Session Manager. Note also that the media is "ip-direct" from the IP Telephone (10.1.2.42) 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: 01A0217
  Signaling   IP Address                                Port
   Near-end:  10.1.2.233                              : 5067
    Far-end:  10.1.2.210                              : 5067
 H.245 Near:
  H.245 Far:
   H.245 Signaling Loc:           H.245 Tunneled in Q.931? no

 Audio Connection Type: ip-direct     Authentication Type: None
    Near-end Audio Loc:                        Codec Type: G.729
   Audio      IP Address                                Port
   Near-end:  10.1.2.42                               : 2740
    Far-end:  65.206.67.1                             : 50226
```

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: T00285
T00285:TX:65.206.67.1:50226/g729/20ms
S00527:RX:10.1.2.42:2740/g729a/20ms
```

The following portion of a filtered Wireshark trace (tracing SIP messages on the private inside interface only) shows the incoming PSTN call. In frame 251, an Acme Packet Net-Net SBC (65.206.67.1) sends an INVITE to Session Manager (10.1.2.210). In frame 254, Session Manager sends the INVITE to Communication Manager. Observe that Session Manager has already adapted the Verizon DID to its corresponding Communication Manager extension (34000). In frame 289, Communication Manager sends a 180 Ringing with SDP. Note that enhancements in Communication Manager Release 6 and later allow a 183 with SDP to be configured to be sent instead of 180. In frame 525, Communication Manager sends the 200 OK when the user answers the call. In frame 592, Communication Manager sends the INVITE to begin the process of shuffling the media paths to "ip-direct", which concludes with the ACKs in frames 657 and 659.

Filter: sip && (ip.addr==65.206.67.1 || ip.addr==10.1.2.233) Expression... Clear Apply

No.	Time	Source	Destination	Protocol	Info
251	11:51:29.658631	65.206.67.1	10.1.2.210	SIP/SDP	Request: INVITE sip:7329450285@10.1.2.210:5060;transport=t
252	11:51:29.661341	10.1.2.210	65.206.67.1	SIP	Status: 100 Trying
254	11:51:29.663843	10.1.2.210	10.1.2.233	SIP/SDP	Request: INVITE sip:34000@avaya.com:5060;transport=tcp, wi
256	11:51:29.707727	65.206.67.1	10.1.2.70	SIP	Request: OPTIONS sip:10.1.2.70:5060;transport=tcp
258	11:51:29.712164	10.1.2.70	65.206.67.1	SIP	Status: 200 OK
265	11:51:29.721830	10.1.2.233	10.1.2.210	SIP	Status: 100 Trying
289	11:51:29.748870	10.1.2.233	10.1.2.210	SIP/SDP	Status: 180 Ringing, with session description
291	11:51:29.750912	10.1.2.210	65.206.67.1	SIP/SDP	Status: 180 Ringing, with session description
525	11:51:32.592911	10.1.2.233	10.1.2.210	SIP/SDP	Status: 200 OK, with session description
527	11:51:32.595740	10.1.2.210	65.206.67.1	SIP/SDP	Status: 200 OK, with session description
577	11:51:32.880954	65.206.67.1	10.1.2.210	SIP	Request: ACK sip:7329450285@10.1.2.233:5067;transport=tcp
579	11:51:32.883177	10.1.2.210	10.1.2.233	SIP	Request: ACK sip:7329450285@10.1.2.233:5067;transport=tcp
592	11:51:32.924146	10.1.2.233	10.1.2.210	SIP	Request: INVITE sip:9088485703@65.206.67.1:5060;transport=
593	11:51:32.925625	10.1.2.210	10.1.2.233	SIP	Status: 100 Trying
594	11:51:32.926808	10.1.2.210	65.206.67.1	SIP	Request: INVITE sip:9088485703@65.206.67.1:5060;transport=
595	11:51:32.930602	65.206.67.1	10.1.2.210	SIP	Status: 100 Trying
640	11:51:33.253013	65.206.67.1	10.1.2.210	SIP/SDP	Status: 200 OK, with session description
642	11:51:33.255066	10.1.2.210	10.1.2.233	SIP/SDP	Status: 200 OK, with session description
657	11:51:33.304155	10.1.2.233	10.1.2.210	SIP/SDP	Request: ACK sip:9088485703@65.206.67.1:5060;transport=tcp
659	11:51:33.306420	10.1.2.210	65.206.67.1	SIP/SDP	Request: ACK sip:9088485703@65.206.67.1:5060;transport=tcp

The following portion of the same filtered Wireshark trace shows frame 289 expanded to illustrate the SDP in the Ringing with SDP 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
251	11:51:29.658631	65.206.67.1	10.1.2.210	SIP/SDP	Request: INVITE sip:7329450285@10.1.2.210:5060;transport=t
252	11:51:29.661341	10.1.2.210	65.206.67.1	SIP	Status: 100 Trying
254	11:51:29.663843	10.1.2.210	10.1.2.233	SIP/SDP	Request: INVITE sip:34000@avaya.com:5060;transport=tcp, wi
256	11:51:29.707727	65.206.67.1	10.1.2.70	SIP	Request: OPTIONS sip:10.1.2.70:5060;transport=tcp
258	11:51:29.712164	10.1.2.70	65.206.67.1	SIP	Status: 200 OK
265	11:51:29.721830	10.1.2.233	10.1.2.210	SIP	Status: 100 Trying
289	11:51:29.748870	10.1.2.233	10.1.2.210	SIP/SDP	Status: 180 Ringing, with session description
291	11:51:29.750912	10.1.2.210	65.206.67.1	SIP/SDP	Status: 180 Ringing, with session description
525	11:51:32.592911	10.1.2.233	10.1.2.210	SIP/SDP	Status: 200 OK, with session description
527	11:51:32.595740	10.1.2.210	65.206.67.1	SIP/SDP	Status: 200 OK, with session description

```
⊟ Media Description, name and address (m): audio 2988 RTP/AVP 18 101
    Media Type: audio
    Media Port: 2988
    Media Proto: RTP/AVP
    Media Format: ITU-T G.729
    Media Format: 101
⊟ Media Attribute (a): rtpmap:18 G729/8000
    Media Attribute Fieldname: rtpmap
    Media Format: 18
    MIME Type: G729
⊟ 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 254 expanded to illustrate the use of destination port 5067 on Communication Manager. Communication Manager can apply Verizon-appropriate behaviors since it can distinguish that the call is inbound from Verizon by the use of port 5067 (i.e., arriving from the same Session Manager as other non-Verizon traffic).

No.	Time	Source	Destination	Protocol	Info
251	11:51:29.658631	65.206.67.1	10.1.2.210	SIP/SDP	Request: INVITE sip:7329450285@10.1.2.210:5060;transport=t
252	11:51:29.661341	10.1.2.210	65.206.67.1	SIP	Status: 100 Trying
254	11:51:29.663843	10.1.2.210	10.1.2.233	SIP/SDP	Request: INVITE sip:34000@avaya.com:5060;transport=tcp, wi
256	11:51:29.707727	65.206.67.1	10.1.2.70	SIP	Request: OPTIONS sip:10.1.2.70:5060;transport=tcp
258	11:51:29.712164	10.1.2.70	65.206.67.1	SIP	Status: 200 OK
265	11:51:29.721830	10.1.2.233	10.1.2.210	SIP	Status: 100 Trying
289	11:51:29.748870	10.1.2.233	10.1.2.210	SIP/SDP	Status: 180 Ringing, with session description
291	11:51:29.750912	10.1.2.210	65.206.67.1	SIP/SDP	Status: 180 Ringing, with session description
525	11:51:32.592911	10.1.2.233	10.1.2.210	SIP/SDP	Status: 200 OK, with session description
527	11:51:32.595740	10.1.2.210	65.206.67.1	SIP/SDP	Status: 200 OK, with session description

```
⊞ Frame 254 (343 bytes on wire, 343 bytes captured)
⊞ Ethernet II, Src: e4:1f:13:33:67:48 (e4:1f:13:33:67:48), Dst: Avaya_4a:f5:42 (00:04:0d:4a:f5:42)
⊞ Internet Protocol, Src: 10.1.2.210 (10.1.2.210), Dst: 10.1.2.233 (10.1.2.233)
⊟ Transmission Control Protocol, Src Port: 53728 (53728), Dst Port: authentx (5067), Seq: 1457, Ack: 1, Len: 289
    Source port: 53728 (53728)
    Destination port: authentx (5067)
    Sequence number: 1457    (relative sequence number)
    [Next sequence number: 1746    (relative sequence number)]
    Acknowledgement number: 1    (relative ack number)
    Header length: 20 bytes
```

9.1.2 Sample 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, Acme1 was used. Outbound calls using Acme2 look similar and will not be repeated here.

The following edited trace shows an outbound ARS call from IP Telephone x34000 to the PSTN number 9-1-908-848-5703. The call is routed to route pattern 68 and trunk group 68. The calling party number sent is 9089540285 that maps to extension x34000 as specified in the "NUMBERING - PUBLIC/UNKNOWN FORMAT" form on Communication Manager. The call initially uses the media resources on the Avaya G650 Media Gateway for the call, but after the call is answered, the call is "shuffled" to become an "ip-direct" connection between the IP Telephone (10.1.2.42) and the "inside" of the Acme Packet Net-Net SBC (65.206.67.21).

```
list trace tac 168                                                    Page   1

                                LIST TRACE

time            data

08:52:26 SIP>INVITE sip:19088485703@pcelban0001.avayalincroft.gl
08:52:26 SIP>obalipcom.com SIP/2.0
08:52:26     dial 919088485703 route:PREFIX|HNPA|ARS
08:52:26     term trunk-group 68    cid 0x6f5
08:52:26     dial 919088485703 route:PREFIX|HNPA|ARS
08:52:26     route-pattern  68 preference 1  cid 0x6f5
08:52:26     seize trunk-group 68 member 3  cid 0x6f5
08:52:26     Setup digits 19088485703
08:52:26     Calling Number & Name 7329450285 Allan-16xxH
08:52:26 SIP<SIP/2.0 100 Trying
08:52:26     Proceed trunk-group 68 member 3  cid 0x6f5
08:52:28 SIP<SIP/2.0 183 Session Progress
08:52:28     G729 ss:off ps:20
             rgn:54 [65.206.67.1]:50236
             rgn:1 [10.1.2.235]:6096
```

```
list trace tac 168                                                    Page   2

                                LIST TRACE

time            data
08:52:28     xoip options: fax:off modem:off tty:US  uid:0x5013d
             xoip ip: [10.1.2.235]:6096
08:52:30 SIP<SIP/2.0 200 OK
08:52:30 SIP>ACK sip:19088485703@65.206.67.1:5060;transport=tcp
08:52:30 SIP>SIP/2.0
08:52:30     active trunk-group 68 member 3  cid 0x6f5
08:52:31 SIP>INVITE sip:19088485703@65.206.67.1:5060;transport=t
08:52:31 SIP>cp SIP/2.0
08:52:31 SIP<SIP/2.0 100 Trying
08:52:31 SIP<SIP/2.0 200 OK
08:52:31     G729 ss:off ps:20
             rgn:54 [10.1.2.42]:2740
             rgn:54 [65.206.67.1]:50236
08:52:31 SIP>ACK sip:19088485703@65.206.67.1:5060;transport=tcp
08:52:31 SIP>SIP/2.0
08:52:31     G729A ss:off ps:20
             rgn:54 [65.206.67.1]:50236
             rgn:54 [10.1.2.42]:2740
```

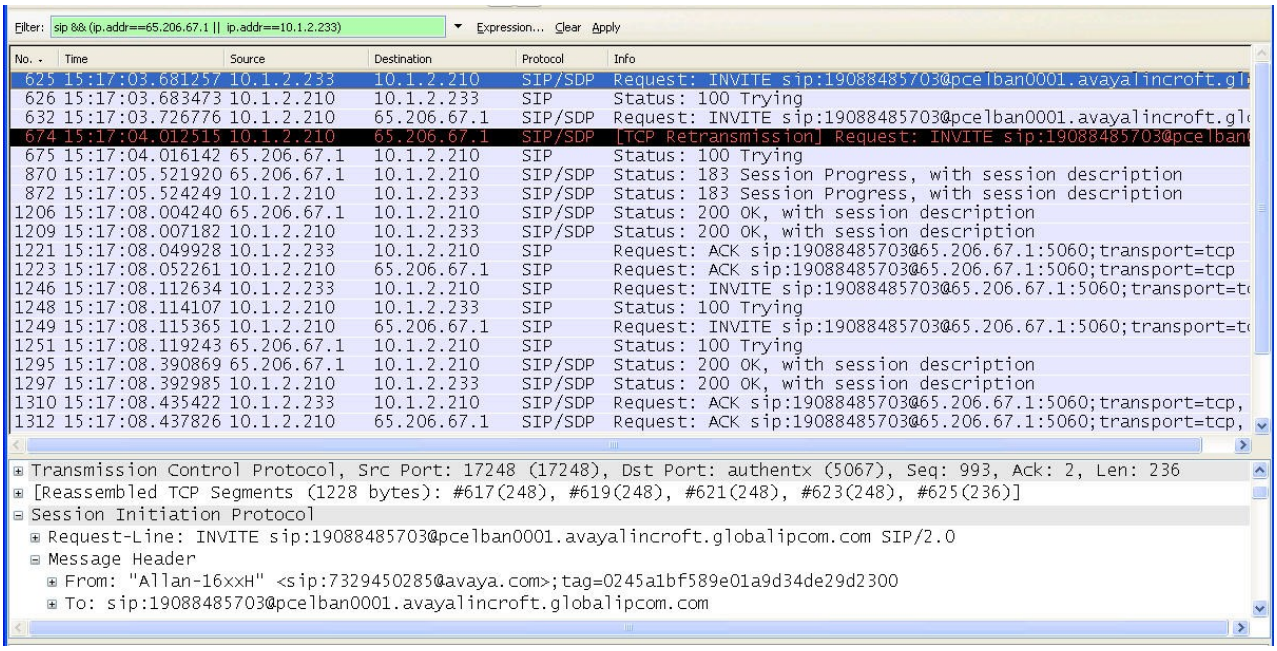
The following screen shows **Page 2** of the output of the ***status trunk*** command pertaining to this same call. Note the media is "ip-direct" from the IP Telephone (10.1.2.42) to the inside IP address of Acme1 (65.206.67.1) using G.729.

```
status trunk 68/3                                                  Page   2 of   3
                                CALL CONTROL SIGNALING

Near-end Signaling Loc: 01A0217
  Signaling   IP Address                                Port
   Near-end:  10.1.2.233                              : 5067
    Far-end:  10.1.2.210                              : 5067
 H.245 Near:
  H.245 Far:
   H.245 Signaling Loc:           H.245 Tunneled in Q.931? no

 Audio Connection Type: ip-direct     Authentication Type: None
    Near-end Audio Loc:                          Codec Type: G.729
   Audio      IP Address                                Port
   Near-end:  10.1.2.42                               : 2740
    Far-end:  65.206.67.1                             : 50236
```

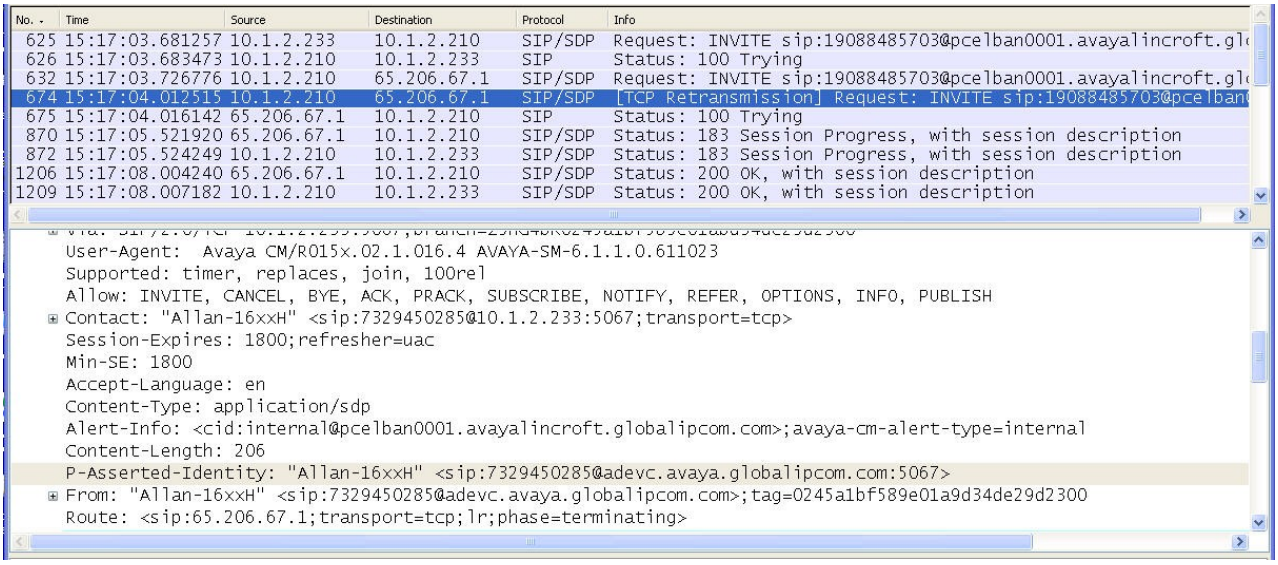
The following screen shows **Page 3** of the output of the ***status trunk*** command pertaining to this same call. Here it can be observed that G.729a is used.

```
status trunk 68/3                                                  Page   3 of   3
                       SRC PORT TO DEST PORT TALKPATH
src port: T00317
T00317:TX:65.206.67.1:50236/g729/20ms
S00527:RX:10.1.2.42:2740/g729a/20ms
```

The following portion of a filtered Wireshark trace (tracing the private or inside network only) shows the outgoing call to Verizon. In frame 625, Communication Manager sends an INVITE to Session Manager. This frame is selected so that it is evident from the bottom pane that destination port 5067 was used. In frame 632, Session Manager sends the INVITE to the Acme Packet Net-Net SBC "Acme1". The call proceeds with 100 Trying, 183 Session Progress, and 200 OK upon answer by the PSTN phone. In frame 1246, Communication Manager sends an INVITE to begin the shuffling process, which concludes with the ACKs in frames 1310 and 1312.



The following portion of the same filtered Wireshark trace shows frame 674 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 bottom pane, 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
625	15:17:03.681257	10.1.2.233	10.1.2.210	SIP/SDP	Request: INVITE sip:19088485703@pcelban0001.avayalincroft.gl
626	15:17:03.683473	10.1.2.210	10.1.2.233	SIP	Status: 100 Trying
632	15:17:03.726776	10.1.2.210	65.206.67.1	SIP/SDP	Request: INVITE sip:19088485703@pcelban0001.avayalincroft.gl
674	15:17:04.012515	10.1.2.210	65.206.67.1	SIP/SDP	[TCP Retransmission] Request: INVITE sip:19088485703@pcelban
675	15:17:04.016142	65.206.67.1	10.1.2.210	SIP	Status: 100 Trying
870	15:17:05.521920	65.206.67.1	10.1.2.210	SIP/SDP	Status: 183 Session Progress, with session description
872	15:17:05.524249	10.1.2.210	10.1.2.233	SIP/SDP	Status: 183 Session Progress, with session description
1206	15:17:08.004240	65.206.67.1	10.1.2.210	SIP/SDP	Status: 200 OK, with session description
1209	15:17:08.007182	10.1.2.210	10.1.2.233	SIP/SDP	Status: 200 OK, with session description

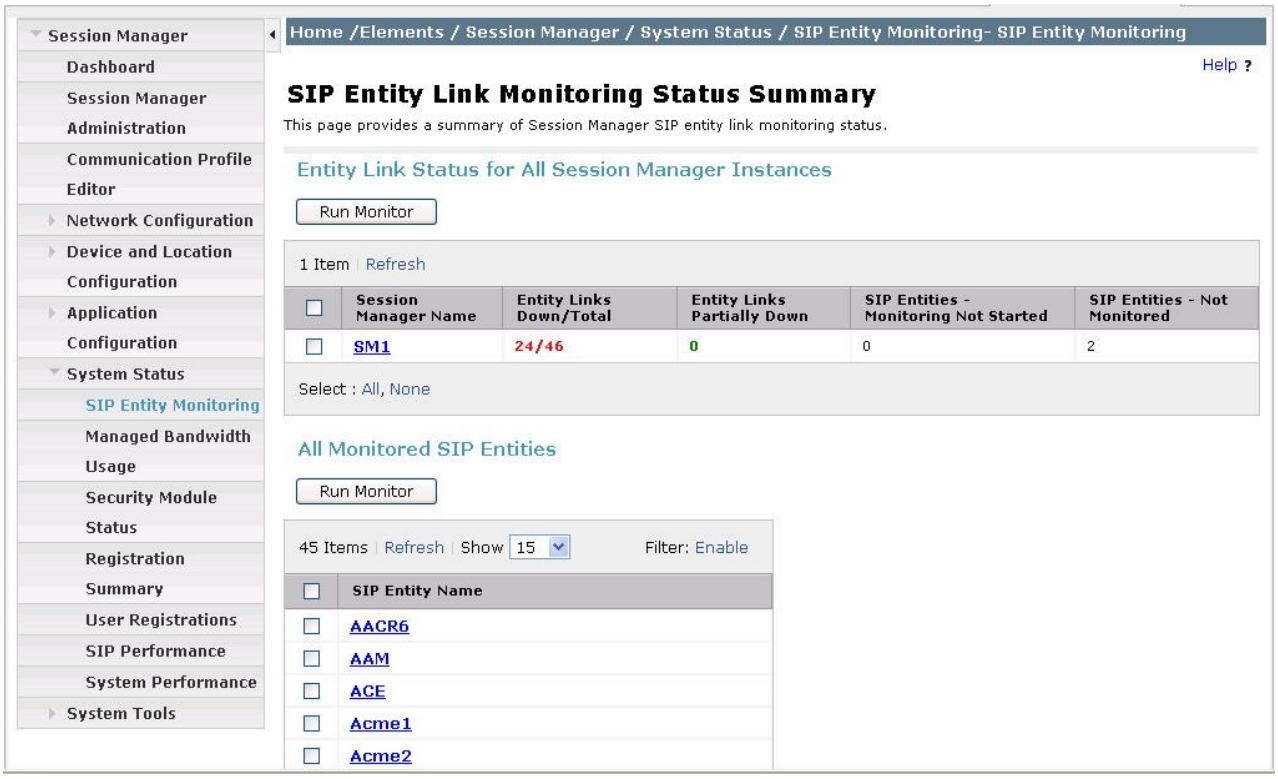
```
User-Agent:  Avaya CM/R015x.02.1.016.4 AVAYA-SM-6.1.1.0.611023
Supported: timer, replaces, join, 100rel
Allow: INVITE, CANCEL, BYE, ACK, PRACK, SUBSCRIBE, NOTIFY, REFER, OPTIONS, INFO, PUBLISH
⊞ Contact: "Allan-16xxH" <sip:7329450285@10.1.2.233:5067;transport=tcp>
Session-Expires: 1800;refresher=uac
Min-SE: 1800
Accept-Language: en
Content-Type: application/sdp
Alert-Info: <cid:internal@pcelban0001.avayalincroft.globalipcom.com>;avaya-cm-alert-type=internal
Content-Length: 206
P-Asserted-Identity: "Allan-16xxH" <sip:7329450285@adevc.avaya.globalipcom.com:5067>
⊞ From: "Allan-16xxH" <sip:7329450285@adevc.avaya.globalipcom.com>;tag=0245a1bf589e01a9d34de29d2300
Route: <sip:65.206.67.1;transport=tcp;lr;phase=terminating>
```

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

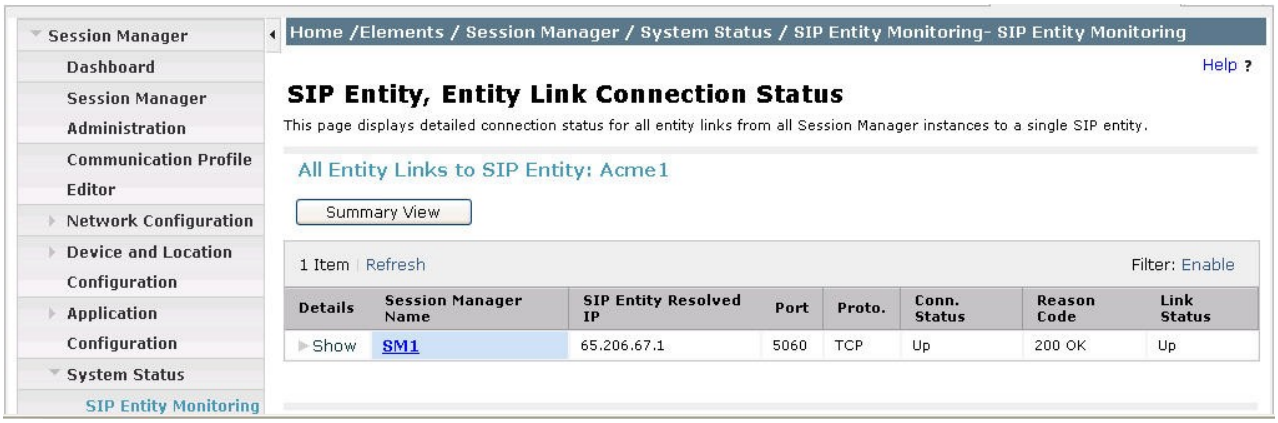
This section contains verification steps that may be performed using System Manager for Session Manager.

9.2.1 Verify SIP Entity Link Status

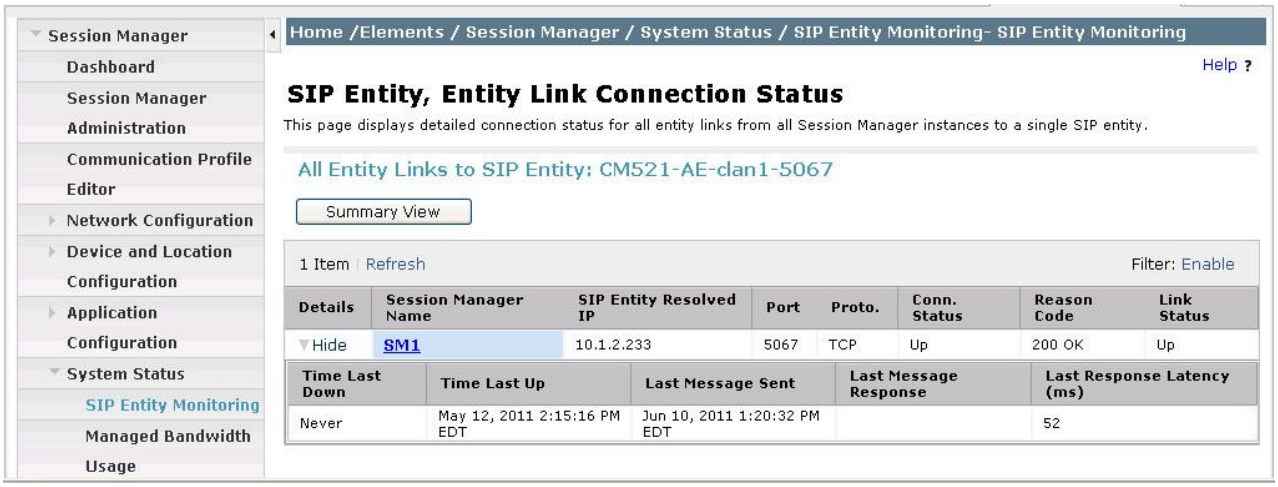
Log in to System Manager. Navigate to **Home → Elements → Session Manager → System Status → SIP Entity Monitoring**, as shown below.



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

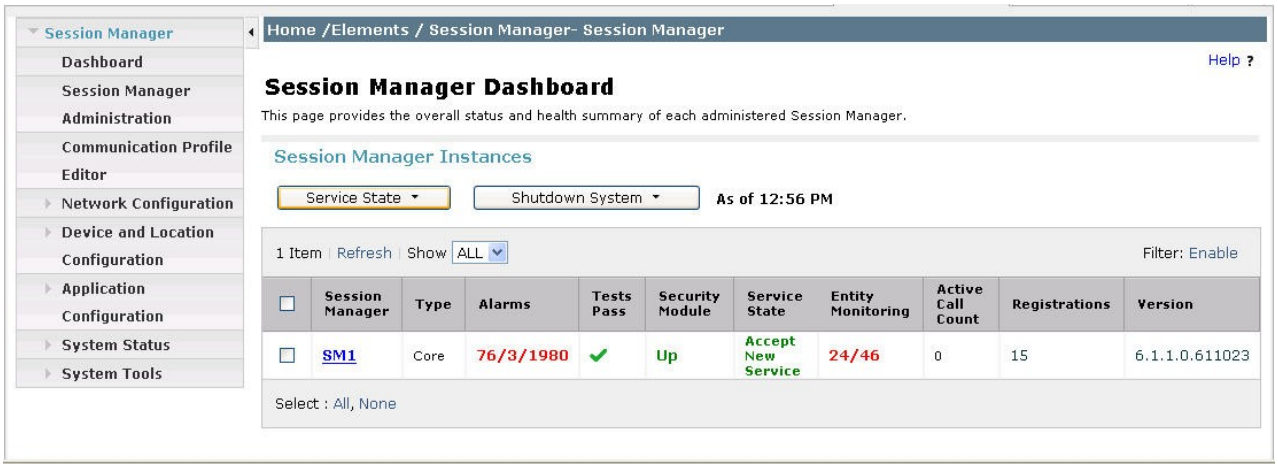


Return to the list of monitored entities, and select another entity of interest, such as “Acme2” or “CM521-AE-clan1-5067”. Under normal operating conditions, the **Link Status** should be “Up” as shown in the example screen below for “CM521-AE-clan1-5067”. In this case, “Show” under **Details** was selected to view additional information. Note the use of port 5067.



9.2.2 Verify System State

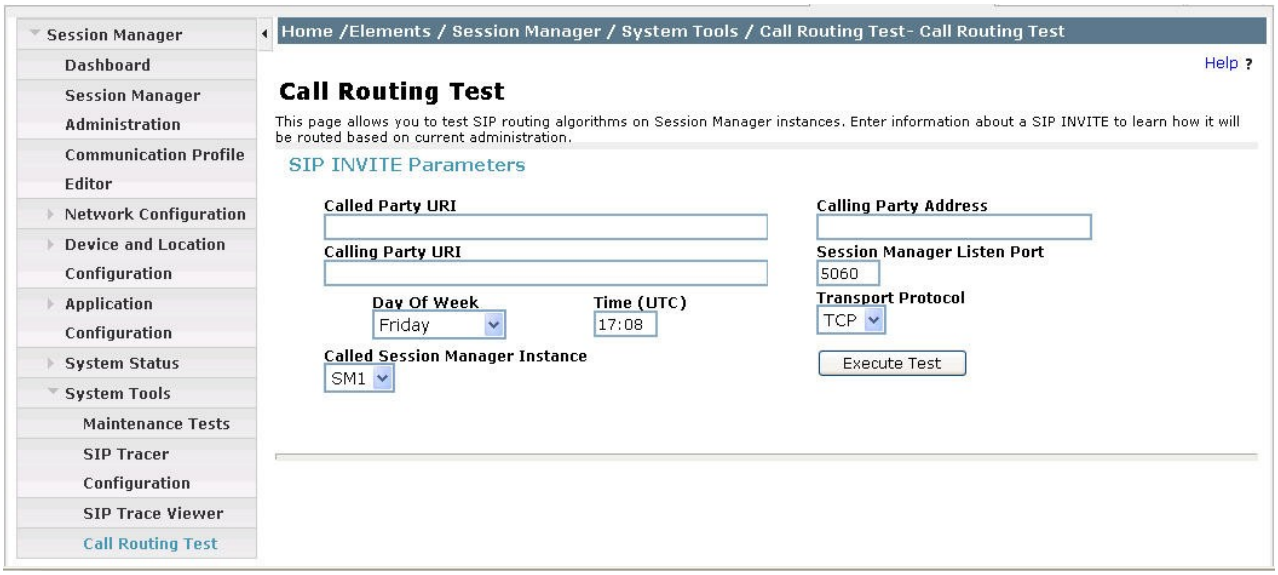
Navigate to **Home → Elements → Session Manager**, as shown below.



Verify that a green check mark is placed under **Tests Pass** and the **Service State** is "Accept New Service." The **Version** can also be observed.

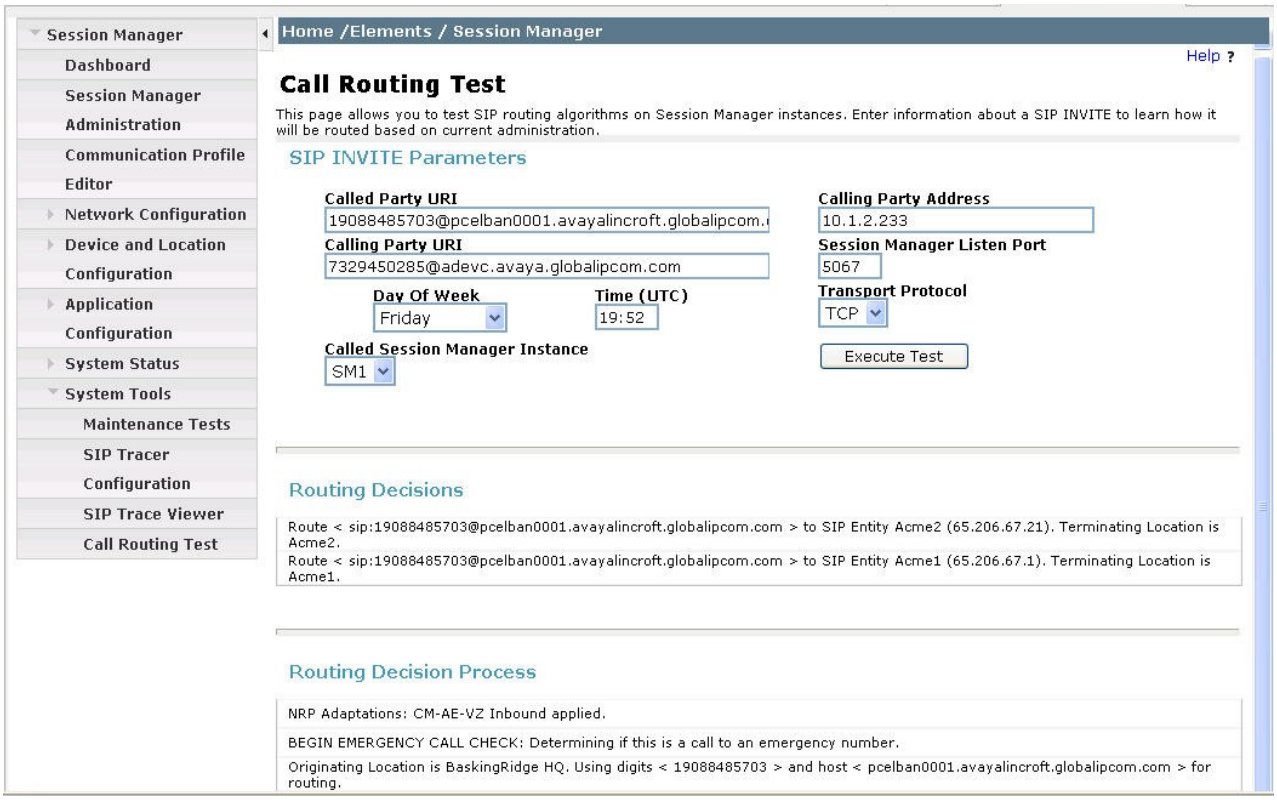
9.2.3 Call Routing Test

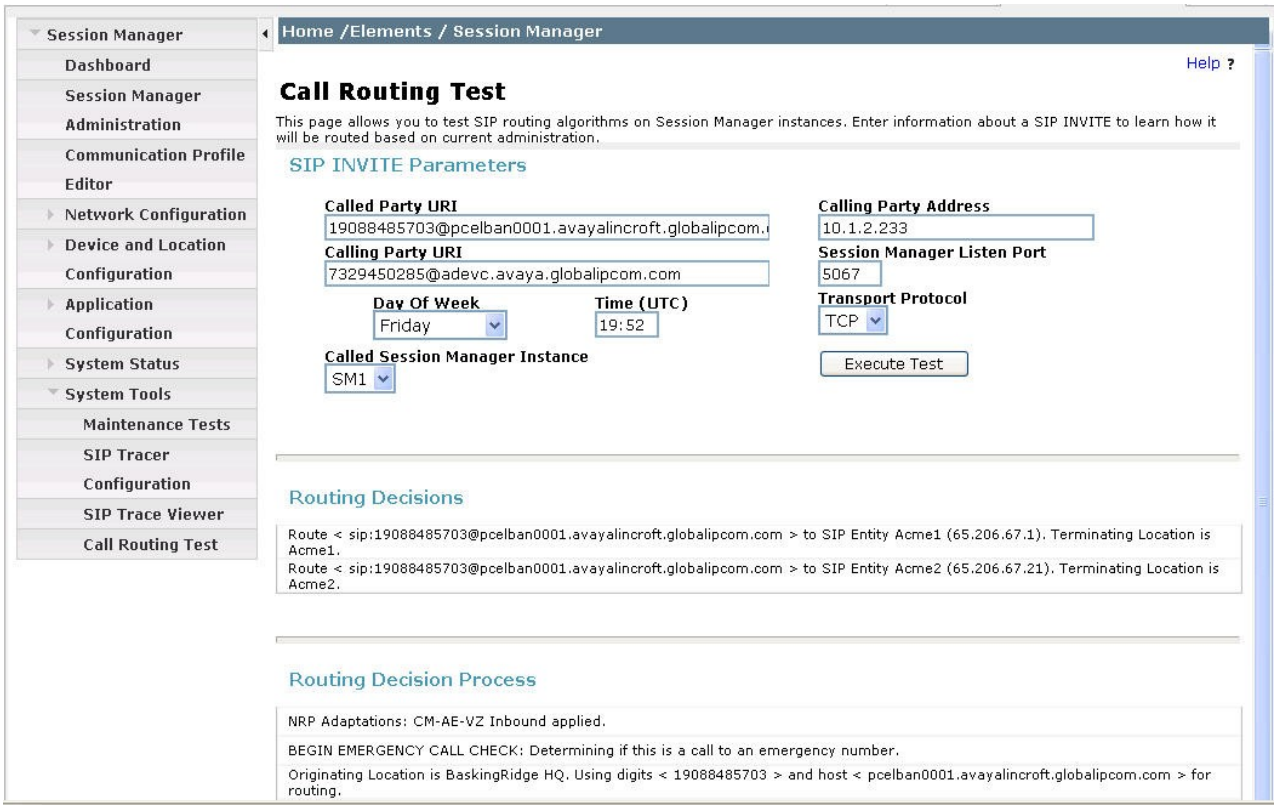
The **Call Routing Test** verifies the routing for a particular source and destination. To run the routing test, navigate to **Home → Elements → Session Manager → System Tools → Call Routing Test**, as shown below.



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 one of the two Acme Packet Net-Net SBCs 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 Acme2 before Acme1, and other results will list Acme1 before Acme2 as shown in the second screen below.

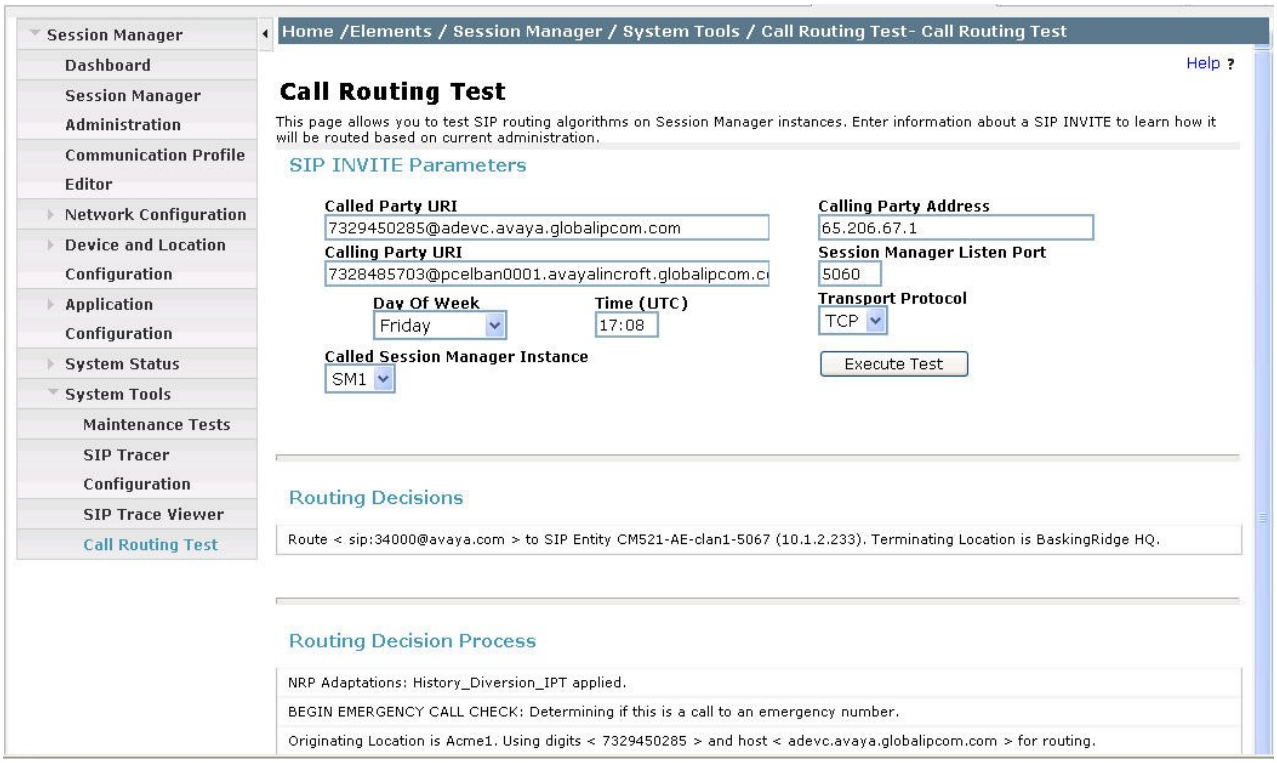
Scroll down to inspect the details of the **Routing Decision Process** if desired (partially shown).





If at the time of this routing 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, the call will always 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 SIP entity named "CM521-AE-clan1-5067" at 10.1.2.233. 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., 34000) by the adapter assigned to the Communication Manager entity. Scroll down to inspect the details of the **Routing Decision Process** if desired (partially shown).



10. Conclusion

As illustrated in these Application Notes, Avaya Aura® Communication Manager Release 5.2.1, Avaya Aura® Session Manager Release 6.1, 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 user access to the PSTN using a Verizon Business IP Trunk public SIP trunk service connection.

Avaya Aura® SIP Solution using Avaya Aura® Communication Manager Release 5.2.1 has not been independently certified by Verizon labs. These Application Notes can be used to facilitate customer engagements via the Verizon field trial process, pending Verizon labs independent certification.

11. Additional References

11.1. Avaya

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

[1] *Administering Avaya Aura® Communication Manager*, Release 5.2, May 2009, Document Number 03-300509, available at https://support.avaya.com/css/P8/documents/100059292

[2] *Administering Avaya Aura® Session Manager,* Release 6.1, November 2010, Document Number 03-603324, available at https://support.avaya.com/css/P8/documents/100121656

[3] *Installing and Configuring Avaya Aura® Session Manager*, Release 6.1, April 2011, Number 03-603473, available at https://support.avaya.com/css/P8/documents/100120934

[4] *Maintaining and Troubleshooting Avaya Aura® Session Manager,* Doc ID 03-603325, Release 6.1, March 2011, available at https://support.avaya.com/css/P8/documents/100120937

[5] *Administering Avaya Aura® System Manager*, Release 6.1, November 2010, available at https://support.avaya.com/css/P8/documents/100120857

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 [JRR-VZIPT] documents Verizon IP Trunk Service with Avaya Aura® Communication Manager Release 6 and Avaya Aura® Session Manager Release 6. The version coverage in [JRR-VZIPT] goes beyond the versions in the title, with the addition of Addendum in Issue 1.0 covering Communication Manager 6.0.1 and Session Manager 6.1.
[JRR-VZIPT] Application Notes for Avaya Aura® Communication Manager Release 6, Avaya Aura® Session Manager Release 6, and Acme Packet Net-Net with Verizon Business IP Trunk SIP Trunk Service – Issue 1.0
https://devconnect.avaya.com/public/download/dyn/SM61AcmeVzB-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.

[6] *Retail VoIP Interoperability Test Plan*
[7] *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.