Avaya Solution & Interoperability Test Lab

Application Notes for Avaya Aura™ Communication Manager 5.2, Avaya Aura™ Session Manager 1.1, and Acme Packet 3800 Net-Net Session Director integration with Verizon Business IP Contact Center (IPCC) Services Suite – Issue 1.2

Abstract

These Application Notes describe the steps used to configure the Avaya Aura™ Communication Manager 5.2, Avaya Aura™ Session Manager 1.1, and Acme Packet Net-Net Session Director integration with Verizon Business IP Contact Center (IPCC) Services suite. The Verizon Business IPCC Services suite is comprised of the VoIP Inbound, IP Contact Center, and IP-IVR SIP trunk service offers.

The Verizon Business IPCC Services suite referenced within these Application Notes is designed for business customers with an Avaya SIP trunk solution. This service suite provides toll free inbound calling via standards-based SIP trunks as well as SIP Network Call Redirection (NCR).

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

Table of Contents

1. Introduction

These Application Notes describe the steps used to configure the Avaya SIP trunk solution with the Verizon Business IPCC Services suite via a Verizon Business Private IP (PIP) circuit connection. The Avaya SIP trunk architecture consists of Avaya Aura™ Communication Manager (version 5.2), Avaya Aura™ Session Manager (version 1.1), and Avaya Aura™ System Manager (version 1.0). Various Avaya H.323, digital, and analog stations are also included.

An Acme Packet 3800 Net-Net Session Director is used as edge device between the Avaya CPE and the Verizon Business. The Acme Packet SBC provides Network Address Translation (NAT) functionality to convert the private Avaya CPE IP addressing to public addressing, as well as performing SIP header manipulation.

Avaya Aura™ Session Manager performs as the SIP trunking "hub" where all inbound and outbound SIP call routing (and other call processing) decisions is made. Avaya Aura™ ™ Communication Manager SIP trunks and Acme Packet "session-agents" are provisioned to terminate at Avaya Aura™ Session Manager.

The Verizon Business IPCC Services suite described in these Application Notes is designed for business customers using Avaya Aura™ Communication Manager and Avaya Aura™ Session Manager. The service provides inbound toll free service via standards-based SIP trunks. Verizon Business IPCC Services suite is a portfolio of IP Contact Center (IPCC) interaction services that includes VoIP Inbound and IP Interactive Voice Response (IP IVR). These feature sets add the capability to support SIP terminations over Internet Dedicated Access (IDA) or Private IP (PIP) to the existing Verizon Business IPCC Services suite. PIP was used for the reference configuration described in these Application Notes. VoIP Inbound is the base service offering, that offers core call routing and termination features. IPIVR is an enhanced service offering that is built on top of VoIP Inbound, and includes features such as menu-routing, custom transfer, and additional media capabilities. Although both VoIP Inbound and IPIVR are inbound services, they do support outbound calls for specific call scenarios (e.g. transfers).

For more information on Verizon Business IPCC Services suite interoperability with the Avaya SIP trunking, see **Section 9.2**.

1.1. Reference Configuration

Figure 1 illustrates the reference configuration used for the DevConnect compliance testing. The testing was performed using the Verizon Business *Retail VoIP Interoperability Test Plan* [**9**]. The reference configuration is comprised of the Avaya CPE location connected via a T1 Internet connection to the Verizon Business IPCC service node. The Avaya CPE location simulates a customer site and uses private IP addressing. At the edge of the Avaya CPE location, an Acme Packet SBC provides NAT functionality that converts the private IP addressing to public addressing that is passed to Verizon Business as well as performing SIP header manipulation. Further network security is provided by the Verizon Business Private IP (PIP) service. The PIP service defines a secure MPLS connection between the Avaya CPE T1 connection and the Verizon IPCC service node.

The following components were used in the reference configuration and are discussed in detail in subsequent Sections.

- Acme Packet 3800 SBC.
  - Private/Public Network Address translation (NAT)
  - SIP header manipulation (see **Section 1.1.1**).
- Avaya Aura™ Communication Manager.
  - SIP trunks for Inbound Voice traffic.
    - Inbound Signaling Group defined with <blank> Far-end Domain field.
    - Voice components assigned to IP-Network-Region 2
    - IP-Network-Region 2 specifies Avaya CPE FQDN and IP-Codec 2
    - IP-Codec 2 specifies G.729A and G.711Mu
  - SIP trunk for Outbound Voice traffic.
    - Outbound Signaling Group defined with Far-end Domain field specifying the Avaya CPE FQDN (See **Section 3.1.5**).
    - Voice components assigned to IP-Network-Region 2
    - IP-Network-Region 2 specifies Avaya CPE FQDN and IP-Codec 2
    - IP-Codec 2 specifies G.729A and G.711Mu
  - Disable the use of History Info Headers
  - Disable the use of Diversion Headers (default).
- Avaya Aura™ Session Manager.
  - Route all Inbound and Outbound SIP calls based on request URI header information
  - Provided digit conversion functionality (converting Verizon 10 digit numbers to 5 digit Avaya Aura™ Communication Manager extensions and vice-versa) for inbound and outbound calls (see **Section 4.3.2**)
  - For outbound calls (transfers), convert the local Avaya CPE FQDN sent by Avaya Aura™ Communication Manager in the request URI to the Verizon Business IPCC Services node IP address (see **Section 1.1.1**).
- Avaya S8720 Media Servers with an Avaya G650 Media Gateway. The S8720s served as the host processor for Avaya Aura™ Communication Manager.
- Avaya 4600 Series IP telephones using the H.323 software bundle.
- Avaya 9600 Series IP telephones using the H.323 software bundle.
- Avaya 6408 Digital phones

1.1.1 SIP Domains

In the reference configuration the Avaya CPE had a local Fully Qualified Domain name (FQDN) of, ***adevc.avaya.globalipcom.com*** (simulating a customer with an existing FQDN**)**. However Verizon Business IPCC Services assigned a service FQDN of ***loc1.interoplab3.21sip.com*** to the Avaya CPE for call routing purposes.

The Verizon Business IPCC Services node used the IP address of 63.79.179.178 instead of an FQDN (they also require inbound packets sent by the Avaya CPE to be sent to port 5112 using UDP transport protocol).

To keep the customer site (Avaya CPE) from having to change its' local FQDN, and to satisfy the Verizon Business IPCC Services suite requirements, SIP headers had to be modified by the Avaya CPE. The following SIP header manipulations are performed by the Avaya CPE.

- Outbound calls (transfers)
  - Avaya Aura™ Communication Manager inserts the local FQDN of ***adevc.avaya.globalipcom.com*** into the Request URI, From, To, and PAI headers (see **Section 3.1.5**).
  - Avaya Aura™ Session Manager modifies the Request URI from ***adevc.avaya.globalipcom.com*** to ***63.79.179.178*** (see **Section 4.3.2**).
  - Acme SBC modifies (see **Section 5**):
    - The From header of ***adevc.avaya.globalipcom.com*** to ***1.1.1.2*** (the outside IP address of the Acme)
    - The To header from ***adevc.avaya.globalipcom.com*** to ***63.79.179.178***
    - The PAI header of ***adevc.avaya.globalipcom.com*** to ***1.1.1.2***
    - Sends the packet to Verizon using destination port 5112 via UDP
- Inbound calls
  - Verizon Business IPCC Services node inserts the following:
    - The assigned CPE FQDN of ***loc1.interoplab3.21sip.com*** into the Request URI.
    - The Verizon Business IPCC Services gateway IP address in the From header.
    - The Acme SBC outside IP address in the To header.
    - Sends the packet to Avaya CPE using destination port 5060 via UDP
  - Acme SBC modifies(see **Section 5**):
    - The Request URI to the IP address ***65.206.67.2*** (Avaya Aura™ Session Manager)
    - The From header to ***65.206.67.1*** (Acme inside address).
    - The To header to ***65.206.67.2***
    - The PAI header to ***65.206.67.1***
    - Changes the transport protocol to TCP
  - Avaya Aura™ Session Manager modifies the Request URI from ***65.206.67.2*** to ***adevc.avaya.globalipcom.com***.

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

1.1.2 Dialing Examples

The following are examples of outbound and inbound voice calls.

Given:

- Avaya Aura™ Communication Manager
  - Station 30001
  - Inbound SIP trunk 4
  - Outbound SIP trunk 2

Inbound

- PSTN dials Verizon Business IPCC Services suite toll free number and the associated Verizon Business IPCC Services suite component sends the call to the Acme Packet SBC.
- The Acme Packet provides SIP header manipulation and passes the call to Avaya Aura™ Session Manager.
- Avaya Aura™ Session Manager performs digit conversion, (changes the 10 digit toll free number to the associated Avaya Aura™ Communication Manager extension 30001), performs SIP header manipulation, and sends the call to Avaya Aura™ Communication Manager Clan board to port 5060.
- The call arrives on inbound voice trunk 4 and connects to station 30001 using either G729A or G711Mu codecs.

Outbound

- Avaya Aura™ Communication Manager voice stations dial 9 and a 10 digit number.
    - ARS sends the call to Route Pattern 2. Route Pattern 2 specifies Outbound trunk 2.
    - The call will select trunk 2 and Avaya Aura™ Communication Manager Clan sends the call to Avaya Aura™ Session Manager specifying:
        - Port 5060
        - G729A or G711Mu codecs.
        - The Avaya CPE FQDN *adevc.avaya.globalipcom.com*
    - Public Unknown Numbering will convert extension 30001 to its' associated toll free number (to pass Verizon admission control).
- Avaya Aura™ Session Manager performs SIP header manipulation and sends the call to the Acme.
- The Acme Packet performs SIP header manipulation and sends the call to the Verizon Business IP Trunk network service node IP address 63.79.179.178, using port 5112 and UDP.

1.1.3 History Info and Diversion Headers

The Verizon Business IPCC Services suite does not support SIP History Info Headers or Diversion Headers. Therefore, in the reference configuration Avaya Aura™ Communication Manager was provisioned ***not*** to send History Info Headers or Diversion Headers (see **Section 3.1.5**).

1.2. Known Limitations

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

- Verizon Business recommends that Avaya Aura™ Session Manager be provisioned using the "Source Based Routing" method described in the addendum section of this document (**Section 8**). This call routing method minimizes routing loops from occurring should the sequence of Verizon network and CPE provisioning cause conflicting call routing.
- Although Avaya Aura™ Communication Manager release 5.2 supports the possibility of using SIP phones, SIP phones were not tested as part of the reference configuration used to validate this solution. To use SIP phones with this solution, Avaya Aura™ SIP Enablement Services is required to support the SIP registrar services for the SIP stations.

- Avaya Aura™ Communication Manager sends SIP 180 RINGING messages with SDP. Although this does not meet the Verizon Business Product Integration Requirements [**8**], no impact to call processing was observed.
- Verizon Business IPCC Services suite does not support fax.
- Verizon Business IPCC Services suite does not support History Info or Diversion Headers.
- Verizon Business IP Trunking service does not support G.729B codec.

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

2. Equipment and Software Validated

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

Equipment	Firmware	Software
Avaya S8720 Servers	-	-
Avaya Aura™ Communication Manager	-	R015x.02.0.947.3 with patch 02.0.947.3-9090
Avaya G650 Media Gateway IPSI – TN2312BP CLAN – TN799DP MedPro – TN2302AP	 HW3 FW45 HW13 FW32 HW2 FW47	 - - -
Avaya Aura™ Session Manager	-	1.1 with SP1
Avaya Aura™ System Manager		1.0 with SP1
Avaya 4610 and 4620 SW IP Telephones	-	a10d01b2-9-1.bin (H.323)
Avaya 9620 and 9630 IP Telephones	-	1.5 (H323)
Avaya 6408D+ Digital Phones	-	-
Avaya One-X Communicator	-	1.0 (H.323)
Acme Packet 3800 Net-Net Session Director	-	SC6.1.0 patch 6 build 377

Table 1: Equipment and Software Used in the Reference Configuration

Note - The solution integration validated in these Application Notes should be considered valid for deployment with Avaya Aura™ Communication Manager release 5.2.1 and Avaya Aura™ Session Manager release 5.2. Avaya agrees to provide service and support for the integration of Avaya Aura™ Communication Manager release 5.2.1 and Avaya Aura™ Session Manager release 5.2 with Verizon Business IPCC Services suite, in compliance with existing support agreements for Avaya Communication Manager release 5.2 and Avaya Aura™ Session Manager 1.1, and in conformance with the integration guidelines as specified in the body of this document.

2.1.1 Reference Configuration - Avaya Interoperability Test Lab

Figure 1 show the Avaya interoperability reference configuration located in the Solution Interoperability Test Lab in Lincroft, New Jersey. All the Avaya CPE is located on the same private IP subnet. The “inside” interfaces of the Acme Packet SBCs are also connected to this private subnet. The “outside” interfaces of the Acme Packet SBCs are connected to a Juniper edge router providing access to the Verizon Business IPCC Services network via a Verizon Business T1 circuit. This circuit is provisioned using the Verizon Business Private IP (PIP) service. The Acme Packet SBCs receive traffic from the Verizon Business IPCC Services on port 5060 and send traffic to the Verizon Business IPCC Services on port 5112, using UDP protocol for network transport (required by the Verizon Business IPCC Services suite).

Verizon Business IPCC Services provided toll free 10 digit numbers for use during the testing. These numbers were mapped by Avaya Aura™ Session Manager to their associated Avaya Aura™ Communication Manager extensions.

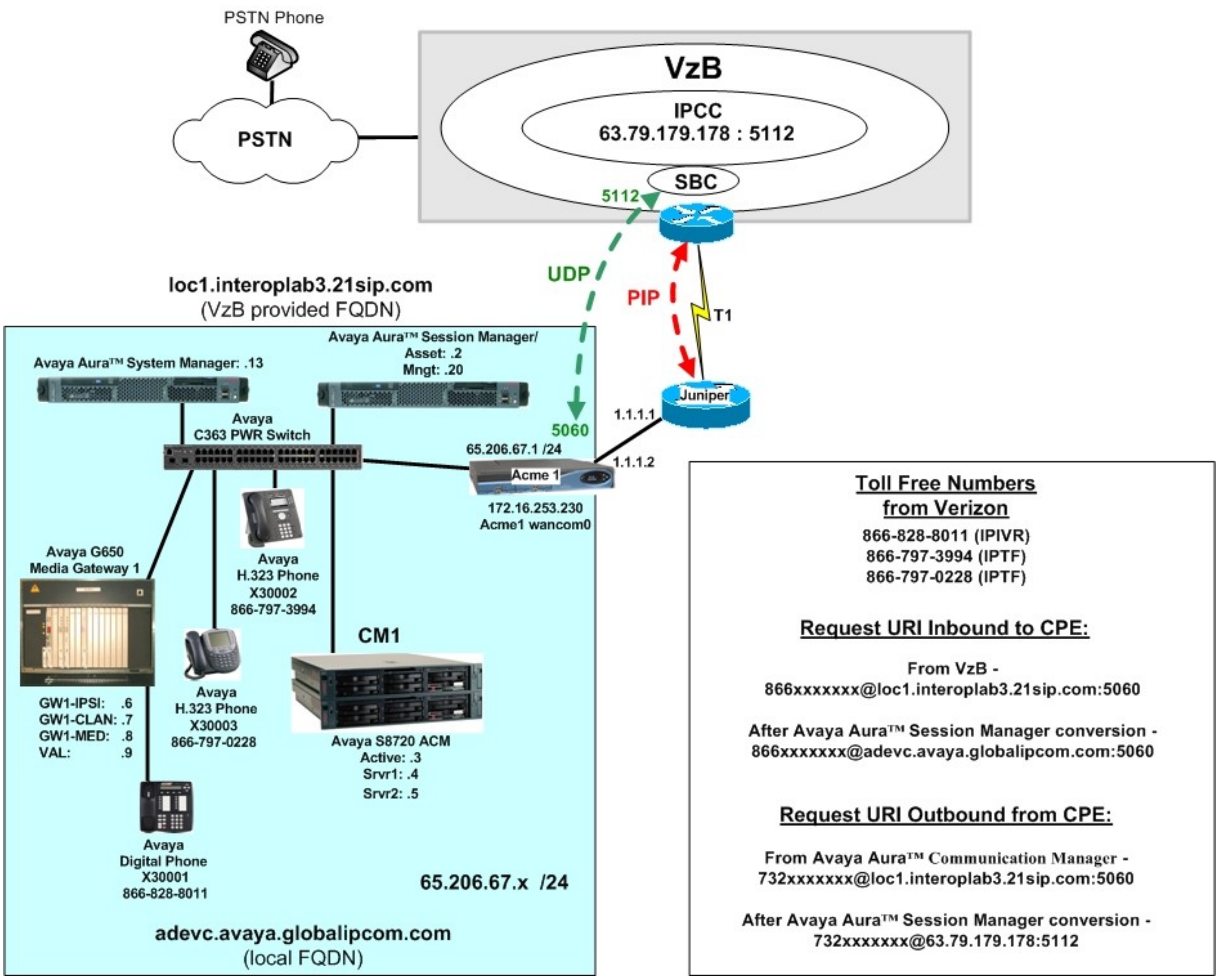

Figure 1: Avaya Interoperability Test Lab Reference Configuration

3. Configure Avaya Aura™ Communication Manager for SIP Trunking

This Section describes the steps for configuring Avaya Aura™ Communication Manager with the necessary signaling and media characteristics for the SIP trunk connection with the Verizon Business IPCC Services suite offer.

Note - The initial installation, configuration, and provisioning of the Avaya servers for Avaya Aura^{TM} Communication Manager, Avaya Media Gateways and their associated boards, as well as Avaya telephones, are presumed to have been previously completed and are not discussed in these Application Notes.

The Avaya CPE site utilized Avaya Aura^{TM} Communication Manager running on Avaya S8720 servers. Collocated with these servers is an Avaya G650 Media Gateway containing a C-LAN signaling processor card, a MedPro media processor card, and an IPSI controller card for communicating to the Avaya S8720 servers. The Avaya CPE site also contained Avaya H.323, and Avaya Digital endpoints.

Note – The Avaya Aura^{TM} Communication Manager commands described in these Application Notes were administered using the System Access Terminal (SAT). SSH was used connect to SAT via the appropriate IP address, login and password.

3.1. Verify System Capacity and Features

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

1. On **Page 2** of the ***display system-parameters customer-options*** form, verify that the **Maximum Administered SIP Trunks** is sufficient for the combination of trunks to the Verizon Business IPCC Services suite offer and any other SIP trunking applications. Be aware that for each call from a non-SIP endpoint to the Verizon Business IPCC Services suite offer one SIP trunk is used 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    4
           Maximum Concurrently Registered IP Stations: 2400   3
             Maximum Administered Remote Office Trunks: 800    0
Maximum Concurrently Registered Remote Office Stations: 2400   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: 75     66
  Maximum Administered Ad-hoc Video Conferencing Ports: 0      0
   Maximum Number of DS1 Boards with Echo Cancellation: 80     0
                             Maximum TN2501 VAL Boards: 10     1
                     Maximum Media Gateway VAL Sources: 250    0
           Maximum TN2602 Boards with 80 VoIP Channels: 128    0
          Maximum TN2602 Boards with 320 VoIP Channels: 128    0
```

Figure 2: System-Parameters Customer-Options Form – Page 2

2. On **Page 3** of the **System-Parameters Customer-Options** form, verify that the **ARS** feature is enabled.

```
display system-parameters customer-options                      Page   3 of  10
                                OPTIONAL FEATURES
    Abbreviated Dialing Enhanced List? y          Audible Message Waiting? y
        Access Security Gateway (ASG)? n              Authorization Codes? y
        Analog Trunk Incoming Call ID? y                       CAS Branch? n
  A/D Grp/Sys List Dialing Start at 01? y                        CAS Main? n
Answer Supervision by Call Classifier? y                Change COR by FAC? n
                                  ARS? y  Computer Telephony Adjunct Links? n
                 ARS/AAR Partitioning? y   Cvg Of Calls Redirected Off-net? y
          ARS/AAR Dialing without FAC? y                      DCS (Basic)? y
          ASAI Link Core Capabilities? n                 DCS Call Coverage? y
          ASAI Link Plus Capabilities? n                DCS with Rerouting? y
       Async. Transfer Mode (ATM) PNC? n
  Async. Transfer Mode (ATM) Trunking? n    Digital Loss Plan Modification? y
              ATM WAN Spare Processor? n                          DS1 MSP? n
                                ATMS? y             DS1 Echo Cancellation? y
                  Attendant Vectoring? y
```

Figure 3: System-Parameters Customer-Options Form – Page 3

3. On **Page 4** of the **System-Parameters Customer-Options** form, verify that the **IP Trunks**, and **ISDN/SIP Network Call Redirection,** and **ISDN-PRI** features are 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? y                   Malicious Call Trace? y
     External Device Alarm Admin? y               Media Encryption Over IP? y
  Five Port Networks Max Per MCC? n    Mode Code for Centralized Voice Mail? n
                Flexible Billing? y
   Forced Entry of Account Codes? y                Multifrequency Signaling? y
      Global Call Classification? y        Multimedia Call Handling (Basic)? y
             Hospitality (Basic)? y     Multimedia Call Handling (Enhanced)? y
 Hospitality (G3V3 Enhancements)? y              Multimedia IP SIP Trunking? n
                       IP Trunks? y
          IP Attendant Consoles? y
         (NOTE: You must logoff & login to effect the permission changes.)
```

Figure 4: System-Parameters Customer-Options Form – Page 4

3.1.1 Dial Plan

In the reference configuration the Avaya CPE environment uses five digit local extensions, 300xx. Trunk Access Codes (TAC) are 3 digits in length and begin with 6. The Feature Access Code (FAC) to access ARS is one digit in length (9).

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

1. On **Page 1** of the form:
   - Local extensions:
     1. In the **Dialed String** field enter **3**
     2. In the **Total Length** field enter **5**
     3. In the **Call Type** field enter **ext**
   - TAC codes:
     1. In the **Dialed String** field enter **1**
     2. In the **Total Length** field enter **3**
     3. In the **Call Type** field enter **dac**
   - FAC code – ARS access:
     1. In the **Dialed String** field enter **9**
     2. In the **Total Length** field enter **1**
     3. In the **Call Type** field enter **fac**

```
change dialplan analysis                                        Page   1 of  12
                             DIAL PLAN ANALYSIS TABLE
                                   Location:  all          Percent Full:    0
       Dialed   Total  Call    Dialed   Total  Call     Dialed   Total  Call
       String   Length Type    String   Length Type     String   Length Type
     3            4    ext
     1            3    dac
     9            1    fac
```

Figure 5: Change Dialplan Analysis Form – Page 1

3.1.2 Node Names

In the **IP Node Names** form, verify (or assign) the node names to be used in this configuration using the ***change node-names ip*** command.

- **ASM** and **65.206.67.2** are the **Name** and **IP Address** of Avaya Aura™ Session Manager.
- **GW1-CLAN1** and **65.206.67.7** are the **Name** and **IP Address** of the C-LAN signaling processor in the G650 Media Gateway.
- **GW1-MEDPRO1** and **65.206.67.8** are the **Name** and **IP Address** of the Media Processor in the G650 Media Gateway.
- **Gateway001** and **65.206.67**.1 are the **Name** and **IP Address** of the default gateway.
- All other values are default.

```
display node-names ip                                          Page   1 of   2
                                 IP NODE NAMES
    Name              IP Address
ASM                 65.206.67.2
GW1-CLAN1           65.206.67.7
GW1-MEDPRO1         65.206.67.8
Gateway001          65.206.67.1
default             0.0.0.0
procr               0.0.0.0
```

Figure 6: IP Node Names Form

3.1.3 IP-Network-Regions

Three network regions were defined in the reference configuration. Avaya Aura™ Communication Manager components are assigned to ip-network-region 1. Voice trunks are assigned to ip-network-region 2.

Avaya Component	IP_Network-Region
C-LAN	1
MedPro	1
Voice SIP Trunks 2 & 4	2

Table 2 –IP Network Regions

The SIP trunk ip-network-regions are defined in the SIP Signaling Group form Far-end Region parameter (see **Section 3.1.5**).

Network region assignments for ip-interfaces may be verified with the ***list ip-interface all*** command.

```
list ip-interface all
                                IP INTERFACES
                                                                       Net
ON Type   Slot  Code/Sfx      Node Name/       Mask  Gateway Node      Rgn  VLAN
                              IP-Address
-- ------ ----- --------      ---------------  ----  ---------------   ---  ----
 y C-LAN  01A02 TN799  D      GW1-CLAN1        /24   Gateway001        1    n
                              65.206.67.7
 y MEDPRO 01A03 TN2602        GW1-MEDPRO1      /24   Gateway001        1    n
                              65.206.67.8
```

Figure 7: IP-Interface IP-Network-Region Assignments

The network-region for an ip-interface may be modified with the ***change ip-interface x*** command where **x** is the board location (the C-LAN interface is shown in the example below).

```
change ip-interface 01a02                                      Page   1 of   3
                                IP INTERFACES
                  Type: C-LAN
                  Slot: 01A02      Target socket load and Warning level: 400
           Code/Suffix: TN799  D         Receive Buffer TCP Window Size: 8320
      Enable Interface? y                        Allow H.323 Endpoints? y
                  VLAN: n                         Allow H.248 Gateways? y
        Network Region: 1                          Gatekeeper Priority: 5

                             IPV4 PARAMETERS
             Node Name: GW1-CLAN1
           Subnet Mask: /24
     Gateway Node Name: Gateway001
         Ethernet Link: 1
         Network uses 1's for Broadcast Addresses? Y
```

Figure 8: IP-Interface IP-Network-Region Assignment.

The **IP-Network-Region** form specifies the parameters used by the Avaya Aura™ Communication Manager components and how components defined to different regions interact with each other. The following ip-network-region assignments were used in the reference configuration. Other combinations are possible. In addition, specific codecs are used to communicate between these regions. See **Section 3.1.4** for the Codec form configurations.

Inter Region Communication	IP-Codec used
Region 1 to Region 1	Codec 1
Region 1 to Region 2	Codec 2
Region 2 to Region 2	Codec 2

Table 3: Inter Region Codec Assignments

Note – Avaya IP telephones inherit the ip-network-region of the C-LAN (or procr for an Avaya S8300 based system) they register to. So if an IP phone registers to a C-LAN, that phone will become part of region 1. If an IP phone needs to be defined to a different region regardless of registration, this may be performed with the ***ip-network-map*** command. **[2]**

3.1.3.1 IP-Network-Region 1

Ip-network-region 1 is defined for Avaya Aura^{TM} Communication Manager components. The network regions are modified with the ***change ip-network-region x*** command, where x is the network region number (**Figure 9**).

1. On **Page 1** of the **IP Network Region** form:
    - Configure the **Authoritative Domain** field to match the Avaya CPE location. In the reference configuration, the FQDN is ***adevc.avaya.globalipcom.com***. (see **Section 1.1.1**)
    - By default, Intra-Region and Inter-Region IP-IP Direct Audio (media shuffling) is set to **yes** to allow audio traffic to be sent directly between SIP endpoints to reduce the use of media resources.
    - Set the **Codec Set** to **1** for the corresponding calls within the IP Network Region.
    - All other values are default.

```
change ip-network-region 1                                    Page   1 of  19
                               IP NETWORK REGION
  Region: 1
Location: 1      Authoritative Domain: adevc.avaya.globalipcom.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: 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
```

Figure 9: IP Network Region 1 – Page 1

2. On **Page 3** of the **IP Network Region** form:
    - Define the **Codec Set** used for inter-region communications. **Codec Set *2*** is entered for communications with region **2**.
    - Set the **direct WAN** field to **y**, indicating that devices in each region can directly communicate with each other.
    - Set the **WAN-BW-Limits** fields to **NoLimit** indicating that the Inter Network Region Connections are not constrained by bandwidth limits.
    - Set the **IGAR** (Inter-Gateway-Alternate-Routing) field to **n** because this field is not used in these Application Notes.

```
change ip-network-region 1                                   Page   3 of  19
 Source Region: 1     Inter Network Region Connection Management     I       M
                                                                     G  A    e
 dst codec direct   WAN-BW-limits   Video      Intervening      Dyn  A  G    a
 rgn  set   WAN  Units    Total Norm  Prio Shr Regions          CAC  R  L    s
 1    1                                                                all
 2    2     y    NoLimit                                             n
```

Figure 10: IP Network Region 1 – Page 3

3.1.3.2 IP-Network-Region 2

Ip-network-region 2 is defined for voice SIP trunks. Provisioning is the same as for ip-network-region 1 except:

1. On **Page 1** of the **IP Network Region** form:
    - Set the **Codec Set** to **IP Codec Set 2** to be used for the corresponding calls within the IP Network Region.

```
change ip-network-region 2                                   Page   1 of  19
                               IP NETWORK REGION
  Region: 2
Location: 1       Authoritative Domain: adevc.avaya.globalipcom.com
    Name: Site 2
MEDIA PARAMETERS                Intra-region IP-IP Direct Audio: yes
      Codec Set: 2              Inter-region IP-IP Direct Audio: yes
   UDP Port Min: 2048                      IP Audio Hairpinning? n
   UDP Port Max: 3329
DIFFSERV/TOS PARAMETERS                   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
```

Figure 11: IP Network Region 2 – Page 1

2. On **Page 3** of the **IP Network Region** form:
   - Define the **Codec Set** used for inter-region communications. **Codec Set 2** is entered for communications with region **1**.

```
change ip-network-region 2                                     Page   3 of  19
 Source Region: 2     Inter Network Region Connection Management     I       M
                                                                     G  A    e
 dst codec direct   WAN-BW-limits   Video      Intervening      Dyn  A  G    a
 rgn  set   WAN  Units    Total Norm  Prio Shr Regions          CAC  R  L    s
 1    2     y    NoLimit                                             n
 2    2                                                                all
```

Figure 12: IP Network Region 2 – Page 3

3.1.4 IP Codec Sets

Two codec sets are defined in the reference configuration. One for local intra customer location calls (ip-network-region 1), and voice calls (ip-network-region 2). **Table 4** shows the codecs defined to each of these codec sets.

IP-Codec Form	IP-Network-Region	Codecs Defined
Codec Form 1	1	G.711MU / G.729A
Codec Form 2	2	G.729A /G.711MU

Table 4: Codec Form Codec Assignments

3.1.4.1 Intra Customer Location – IP-Codec-Set 1

G.711MU is typically used within the same location and is often specified first. G.729A is also specified as an option. Other codecs could be specified as well depending on local requirements. This codec set is associated with ip-network-region 1.

The **IP-Codec-Set** form is modified with the ***change ip-codec x*** command, where ***x*** is the codec form number.

1. On **Page 1** of the form:
   - Configure the **Audio Codec** field **1** to **G.711MU.**
   - Configure the **Audio Codec** field **1** to **G.729A.**

```
change ip-codec-set 1                                          Page   1 of   2
                         IP Codec Set
    Codec Set: 1
    Audio         Silence      Frames   Packet
    Codec         Suppression  Per Pkt  Size(ms)
 1: G.711MU           n          2        20
 2: G.729A            n          2        20
```

Figure 13: IP Codec Set 1

2. On **Page 2** of the form:
   - Configure the **Fax** field to **off.**
   - Configure the **Fax Redundancy** field to **0.**
   - Let all other fields default.

```
change ip-codec-set 1                                          Page   2 of   2
                          IP Codec Set
                              Allow Direct-IP Multimedia? n
                    Mode                 Redundancy
    Fax             off                   0
    Modem           off                   0
    TDD/TTY         off                   3
    Clear-channel   n                     0
```
Figure 14: IP Codec Set 1 – Page 2

3.1.4.2 Outbound Calls – IP-Codec-Set 2

G.729A was picked as the first option as it uses less bandwidth. G.711Mu was used as the second choice. This codec set is associated with ip-network-region 2.

1. On **Page 1** of the form:
   - Configure the **Audio Codec** field **1** to **G.729A.**
   - Configure the **Audio Codec** field **2** to **G.711MU.**

```
display ip-codec-set 2                                            Page   1 of   2
                          IP Codec Set
    Codec Set: 2
    Audio        Silence      Frames   Packet
    Codec        Suppression  Per Pkt  Size(ms)
 1: G.729A          n          2        20
 2: G.711MU         n          2        20
```
Figure 15: Outbound Call IP Codec Set 2

2. On **Page 2** of the form set the values shown in **Figure 14** for codec set 1.

3.1.5 SIP Trunk Groups

SIP trunks are defined for off network voice calls to the Verizon Business IPCC Service suite. **Table 5** lists the SIP trunks used in the reference configuration. A SIP trunk is created in Avaya Aura^{TM} Communication Manager by provisioning a SIP Trunk Group as well as a SIP Signaling Group.

NOTE: For Verizon Business customers utilizing either Verizon's **IP Contact Center** or **IP-IVR** service offers, at least one **Elite Agent license is required** to support the ability to utilize the Network Call Redirection capabilities of those services with Avaya Aura(TM) Communication Manager. This license is required to enable the **System-Parameters Customer-Options** form which contains the **"ISDN/SIP Network Call Redirection"** feature that must be turned **ON** to support Network Call Redirection. Additional details on how to configure Network Call Redirection in Avaya Aura(TM) Communication Manager can be found within the supporting text and figures contained within this section.

SIP Trunk Function	Avaya Aura™ Communication Manager SIP Signaling Group/Trunk Group	Avaya Aura™ Communication Manager SIP Signaling Group *Far-End Domain*	Avaya Aura™ Communication Manager IP Network Region
Inbound	Trunk 4	<blank>	2
Outbound	Trunk 2	Avaya CPE FQDN ***adevc.avaya.globaipcom.com***	2

Table 5: Avaya SIP Trunk Configuration

Note – In the SIP trunk configurations below (and in the Avaya Aura™ Session Manager SIP Entity configuration, **Section 4.3.4**), TCP was selected as the transport protocol for the Avaya CPE in the reference configuration. TCP was used to facilitate trace analysis during network verification. The use of TLS protocol is recommended by Avaya in customer deployments.

3.1.5.1 Configure Public Inbound SIP Trunk

1. Using the ***add signaling-group 4*** command, configure the inbound voice Signaling Group as follows:

   - Set the **Group Type** field to **sip**.
   - Set the **Transport Method** field to **tcp**. Note that this specifies the transport method used between Avaya Aura™ Communication Manager and Avaya Aura™ Session Manager, not the transport method used to the Verizon network.
   - Specify the C-LAN used for SIP signaling (node name **GW1-CLAN1**) and the Avaya Aura™ Session Manager (node name **ASM**) as the two ends of the signaling group in the **Near-end Node Name** and **Far-end Node Name** fields, respectively. These field values are taken from the **IP Node Names** form shown in **Section 3.1.2.**
   - Specify **5060** in the **Near-End** and **Far-end Listen Port** fields.
   - Enter the value **2** into the **Far-end Network Region** field. This value is for the **IP Network Region** defined in **Section 3.1.3**.
   - Leave the **Far-end Domain** field blank. This permits inbound calls from any foreign domain.
   - The **Direct IP-IP Audio Connections** field should be set to **y** to allow RTP voice paths to be established directly between IP telephones and the Verizon Business IPCC Services suite offer.
   - The **DTMF over IP** field should remain set to the default value of **rtp-payload**. This value enables Avaya Aura™ Communication Manager to send DTMF tones using RFC 2833.
   - The default values for the other fields may be used.

```
add signaling-group 4                                           Page   1 of  1
                                SIGNALING GROUP
 Group Number: 4              Group Type: sip
                        Transport Method: tcp
  IMS Enabled? n
   Near-end Node Name: GW1-CLAN1            Far-end Node Name: ASM
 Near-end Listen Port: 5060               Far-end Listen Port: 5060
                                       Far-end Network Region: 2
Far-end Domain:
                                            Bypass If IP Threshold Exceeded? 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
```

Figure 16: Public Inbound SIP Trunk - Signaling Group 4

2. Using the ***add trunk-group 4*** command, add the inbound voice Trunk Group as follows:
   a. On Page 1 of the Trunk Group form:
      - Set the **Group Type** field to **sip**.
      - Choose a descriptive **Group Name.**
      - Specify an available trunk access code (**TAC**) such as **104**.
      - Set the **Service Type** field to **public-ntwrk.**
      - Enter **4** as the **Signaling Group** number.
      - Specify the **Number of Members** used by this SIP trunk group (e.g. **5**).

```
add trunk-group 4                                          Page   1 of  21
                                TRUNK GROUP
Group Number: 4                   Group Type: sip           CDR Reports: y
  Group Name: Inbound_blank              COR: 1        TN: 1        TAC: 104
   Direction: two-way       Outgoing Display? n
 Dial Access? n                                 Night Service:
Queue Length: 0
Service Type: public-ntwrk          Auth Code? n
                                                       Signaling Group: 4
                                                     Number of Members: 10
```

Figure 17: Public Inbound Trunk Group 4 – Page 1

   b. On Page 3 of the **Trunk Group** form:
      - Set the **Numbering Format** field to **public.** This field specifies the format of the calling party number sent to the far-end.

```
add trunk-group 4                                          Page   3 of  21
TRUNK FEATURES
          ACA Assignment? n            Measured: none
                                                       Maintenance Tests? y
                     Numbering Format: public
                                                UUI Treatment: service-provider
                                                 Replace Restricted Numbers? n
                                                Replace Unavailable Numbers? n
```

Figure 18: Public Inbound Trunk Group 4 – Page 3

c. On Page 4 of the **Trunk Group** form:
   - Set the **Telephone Event Payload Type** to **101** to match the configuration on the Verizon Business IPCC Services suite offer.
   - Set **Network Call Redirection** to **Y**. While this parameter is usually set to support Avaya Network Call redirection features such as REFER, it also enables SIP signaling to be sent when an Avaya station presses Hold (Media Attribute=SendOnly).
   - Set **Support Request History?** to **N**.
   - Let all other values default.

```
add trunk-group 10                                           Page   4 of  21
                              PROTOCOL VARIATIONS
                      Mark Users as Phone? n
            Prepend '+' to Calling Number? n
      Send Transferring Party Information? n
                 Network Call Redirection? y
                    Send Diversion Header? n
                  Support Request History? n
             Telephone Event Payload Type: 101
```

Figure 19: Public Inbound Trunk Group 4 – Page 4

3.1.5.2 Configure Public Outbound Voice SIP Trunk

Note – As described in **Section 1**, the Verizon Business IPCC Services suite supports only inbound calling. However outbound calling is supported for specific call scenarios (e.g. transfers), therefore an outbound SIP trunk is required. The outbound SIP trunk is configured in the same fashion as the inbound SIP Trunk except that the voice Signaling Group Far-End Domain specifies the Avaya CPE FQDN instead of being blank.

1. Using the ***add signaling-group 2*** command, configure the inbound voice Signaling Group as follows:

   - Set the **Far-end Domain** field to ***adevc.avaya.globalipcom.com***.

2. Using the ***add trunk-group 2*** command, add the inbound voice Trunk Group as follows:
   1. On Page 1 of the Trunk Group form:
      - Specify an available trunk access code (**TAC**) such as **102**.
      - Enter **2** as the **Signaling Group** number.

All other values should match those shown in **Section 3.1.5.1**.

3.1.6 Public Unknown Numbering

In the reference configuration, the extensions on Avaya Aura^{TM} Communication Manager use a 5 digit dialing plan using extensions 3xxxx. The **Public-Unknown-Numbering** form allows Avaya Aura^{TM} Communication Manager to use these extensions as the calling party number for outbound calls. Otherwise *Anonymous* is displayed as the calling number. However the Verizon Business IPCC Services suite uses the calling party number fields as admission control. Therefore the Avaya Aura^{TM} Communication Manager extension must be converted to its associated Verizon Business IPCC Services suite toll free number. Each extension string is defined for the *outbound* trunk group that the extensions may use. SIP trunk 2 is used for outbound calls n the reference configuration. The following extension mapping was used in the reference configuration.

Extension	Toll Free Number
30001	866-797-8011
30002	866-797-3994
30003	866-797-5598

3.1.6.1 Public Unknown Numbering

Use the ***change public-unknown-numbering x*** command, where *x* is the leading digit of the dial plan extensions (e.g. **3**).

1. Set the **Ext Len** field to **5**.
2. Set the **Ext Code** field to an extension (e.g. **30001)**.
3. Set the **Trk Grp(s)** field to **2.**
4. Set the **CPN Prefix** field to the extensions' corresponding toll free number (e.g. 866-797-8011)
5. Set the **Total CPN Len** field to **10**. This is the total number of digits in the toll free number.
6. Repeat steps 1 through 5 for extensions 30002 (866-797-3994) and 30003 (866-797-5598).

All provisioned public-unknown-numbering entries can be displayed by entering the command ***display public-unknown-numbering 0*** as show in **Figure 23**.

```
display 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: 3
 5  30001          2        8667978011         10           Maximum Entries: 9999
 5  30002          2        8667973994         10
 5  30003          2        8667975598         10
```

Figure 20: Public-unknown-numbering Form

3.1.7 Call Routing

3.1.7.1 Outbound Calls

Note – As described in **Section 1**, the Verizon Business IPCC Services suite only supports outbound dialing for specific call scenarios (e.g. transfers).

The following Sections describe Avaya Aura™ Communication Manager provisioning required for outbound dialing. Avaya Aura™ Communication Manager uses ARS to direct outbound calls to Avaya Aura™ Session Manager.

3.1.7.1.1 ARS

The Automatic Route Selection feature is used to route calls via the SIP trunks to the Avaya Aura™ Session Manager, which in turn completes the calls to the Verizon Business IPCC Service suite. In the reference configuration ARS is triggered by dialing a 9 (feature access code or FAC) and then dialing the called number. ARS matches on the called number and sends the call to a specified route pattern.

1. Verify that the appropriate extensions are defined in the **Public-Unknown-Numbering** form (see **Section 3.1.6**).
2. Use the ***change dialplan analysis*** command to add **9** as a feature access code (**fac**).
   - Set **Dialed String** to **9**.
   - Set **Total Length** to **1**.
   - Set **Call Type** to **fac**.

```
change dialplan analysis                                      Page   1 of  12
                             DIAL PLAN ANALYSIS TABLE
                                   Location:  all          Percent Full:    1
       Dialed   Total  Call    Dialed   Total  Call      Dialed   Total  Call
       String   Length Type    String   Length Type      String   Length Type
         9        1    fac
```

Figure 21: Dialplan Analysis Form

3. Use the ***change feature-access-codes*** command to specify **9** as the access code for external dialing.
   - Set **Auto Route Selection (ARS) – Access Code 1:** to **9**.

```
change feature-access-codes                                    Page   1 of   8
                              FEATURE ACCESS CODE (FAC)
         Abbreviated Dialing List1 Access Code:
         Abbreviated Dialing List2 Access Code:
         Abbreviated Dialing List3 Access Code:
Abbreviated Dial - Prgm Group List Access Code:
                      Announcement Access Code:
                       Answer Back Access Code:
                         Attendant Access Code:
      Auto Alternate Routing (AAR) Access Code:
    Auto Route Selection (ARS) - Access Code 1: 9     Access Code 2:
                 Automatic Callback Activation:        Deactivation:
Call Forwarding Activation Busy/DA:        All:     Deactivation:
   Call Forwarding Enhanced Status:        Act:        Deactivation:
                         Call Park Access Code:
                       Call Pickup Access Code:
CAS Remote Hold/Answer Hold-Unhold Access Code:
                  CDR Account Code Access Code:
                        Change COR Access Code:
                   Change Coverage Access Code:
```

Figure 22: Feature-Access-Codes Form – Page 1

4. Use the ***change ars analysis*** command to configure the route pattern selection rule based upon the number dialed following the ARS access digit "9". In the reference configuration, outbound calls are placed to PSTN:

- 732xxxxxxx (voice destination beginning with 732)

To specify the 732 calls, enter the command ***change ars analysis 732*** and enter the following values:

- Set the **Dialed String** field to **732**
- Set the **Total Min** field to **10**
- Set the **Total Max** field to **10**
- Set the **Route Pattern** field to **2** (will direct to outbound trunk)
- Set the **Type** field to **hnpa**

Note – ARS will route based on the most complete match. For example 732555xxxx would match before 732xxxxxxx.

```
display ars analysis 7                                        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
    732                   10   10     2         hnpa         n
```

Figure 23: ARS Analysis Form

3.1.7.1.2 Route Patterns

Outbound voice calls use route-pattern 2.

Note - Route patterns may also be used to add or delete digits prior to sending them out the specified trunk(s). This feature was not used in the reference configuration.

1. Use the **change route-pattern** command to define the outbound SIP trunk groups included in the route pattern that ARS selects.
   - **Outbound trunk**
     - Set the first **Grp No** field to ***2***.
   - Let all other parameters default.

```
change route-pattern 2                                      Page   1 of   3
                    Pattern Number: 16  Pattern Name: Outbound
                             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: 2    0                                                           n   user
 2:
```

Figure 24: Route Pattern 2 – Outbound Calls

3.1.7.2 Incoming Calls

SIP trunk 4 is used for inbound calls. In the reference configuration the Avaya Aura™ Session Manager is used to convert inbound Verizon toll free numbers to Avaya Aura™ Communication Manager extensions (see **Section 4.3.2**). Therefore no incoming digit manipulation was required on Avaya Aura™ Communication Manager.

Note - Incoming called numbers may be changed to match a provisioned extension if necessary, with the Avaya Aura™ Communication Manager *change inc-call-handling-trmt trunk-group x* command, where **x** is the receiving trunk.

3.1.8 Avaya Aura™ Communication Manager Stations

In the reference configuration 5 digit voice and fax stations were provisioned with the extension format 300xx.

3.1.8.1 Voice Stations

Figure 28 shows an example of a voice extension (Avaya H.323 IP phone). Note that the **COR** value is ***1*** (default). Since the phone is an IP device, a virtual port **S00000** is automatically assigned by the system. By default three call appearances are defined on page 4 of the form.

On page 1 of the form:

- Set the **Type** field to match the station type (e.g. 9620)
- Set the **Name** field to some value (e.g. Avaya H.323)

```
display station 30002                                          Page   1 of   6
                                     STATION
Extension: 30002                          Lock Messages? n               BCC: 0
     Type: 9620                        Security Code:                    TN: 1
     Port: S00000                      Coverage Path 1:                 COR: 1
     Name: Avaya H.323                 Coverage Path 2:                 COS: 1
                                       Hunt-to Station:
STATION OPTIONS
                                           Time of Day Lock Table:
              Loss Group: 19         Personalized Ringing Pattern: 1
                                                 Message Lamp Ext: 30002
            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
                                             Customizable Labels? y
```

Figure 25: Avaya H.323 IP Phone – Page 1

On page 4 of the form:

- Call appearances (**call-appr**) will appear automatically based on the station type.

```
display station 30002                                           Page   4 of   6
                                    STATION
 SITE DATA
       Room:                                                   Headset? n
       Jack:                                                   Speaker? n
      Cable:                                                  Mounting: d
      Floor:                                               Cord Length: 0
   Building:                                                 Set Color:
ABBREVIATED DIALING
     List1:                    List2:                    List3:
BUTTON ASSIGNMENTS
 1: call-appr                           5:
 2: call-appr                           6:
 3:                                     7:
 4:                                     8:
    voice-mail Number:
```

Figure 26: Avaya H.323 IP Phone – Page 4

3.1.9 Save Avaya Aura™ Communication Manager Provisioning

Enter the ***save translation*** command to make the changes permanent.

4. Avaya Aura™ Session Manager Provisioning

This section provides the procedures for configuring Avaya Aura™ Session Manager as provisioned in the reference configuration. Avaya Aura™ Session Manager is comprised of two functional components: the Avaya Aura™ Session Manager server and the Avaya Aura™ System Manager management server. All SIP call provisioning for Avaya Aura™ Session Manager is performed via the Avaya Aura™ System Manager web interface and are then downloaded into Avaya Aura™ Session Manager.

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 platforms. For more information on provisioning Avaya Aura™ Session Manager see **[3]**.

4.1. Network Interfaces

Avaya Aura™ Session Manager is comprised of two main components, the server itself and the SM-100 card. **Figure 27** shows the backplane of Avaya Aura™ Session Manager.

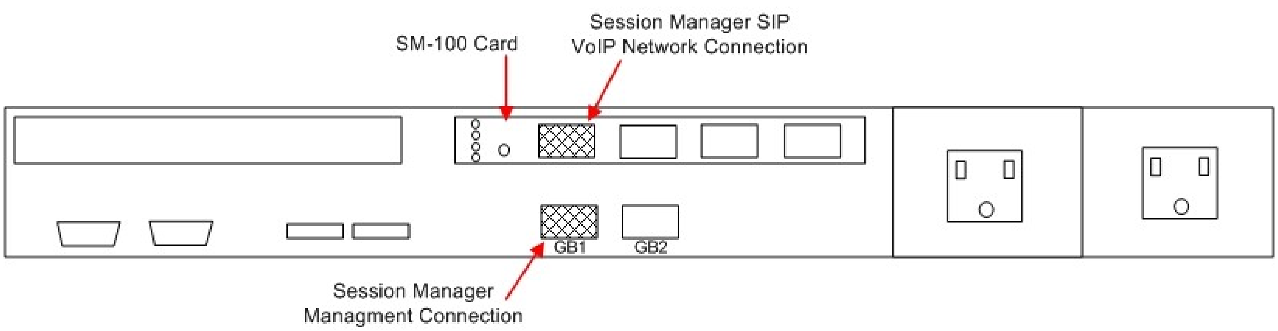

Figure 27 – Avaya Aura™ Session Manager Network Connections

The Avaya Aura™ Session Manager SM-100 card has four network interface ports. The first port is the Avaya Aura™ Session Manager connection to the SIP VoIP network. This interface is used for all inbound and outbound SIP signaling and must have network connectivity to all provisioned SIP Entities (see **Section 4.3.4**).

The Avaya Aura™ Session Manager server has two network interface ports labeled "GB1" and "GB2". The "GB1" port is used for management/provisioning of Avaya Aura™ Session Manager. This port must have network connectivity to Avaya Aura™ System Manager.

Note –In the reference configuration the SM-100 interface and the Avaya Aura™ Session Manager server interface were both connected to the same IP network. If desired, the Avaya Aura™ System Manager/Avaya Aura™ Session Manager management connection may use a different network than the SM-100 connection.

4.2. Logging Into Avaya Aura™ System Manager

The following provisioning is performed via Avaya Aura™ System Manager to enable SIP trunking:

- **Network Routing Policy**
  - **SIP Domains -** Define FQDNs that may send calls to Avaya Aura™ Session Manager.
  - **Locations** – Logical/physical areas that may be occupied by SIP Entities
  - **SIP Entities** – Typically devices corresponding to the SIP telephony systems including Avaya Aura™ Session Manager itself, however they may includes other devices such as SBCs.
  - **Entity Links** – Connection information which define the SIP trunk parameters used by Avaya Aura™ Session Manager when routing calls to/from other SIP Entities.
  - **Dial Patterns** – Matching digit patterns which govern to which SIP Entity a call is routed.
  - **Routing Policies** - Policies that determine which control call routing between the SIP Entities based on applicable Dial Patterns.
  - **Time Ranges** – Specified windows during which SIP call processing is permitted for a particular Routing Policies.
- **Avaya Aura™ Session Manager** – Information corresponding to the Avaya Aura™ Session Manager Server to be managed by Avaya Aura™ System Manager.

Configuration is accomplished by accessing the browser-based GUI of Avaya Aura™ System Manager, using the URL ***http://<ip-address>/IMSM***, where "<ip-address>" is the IP address of Avaya Aura™ System Manager. Log in with the appropriate credentials.

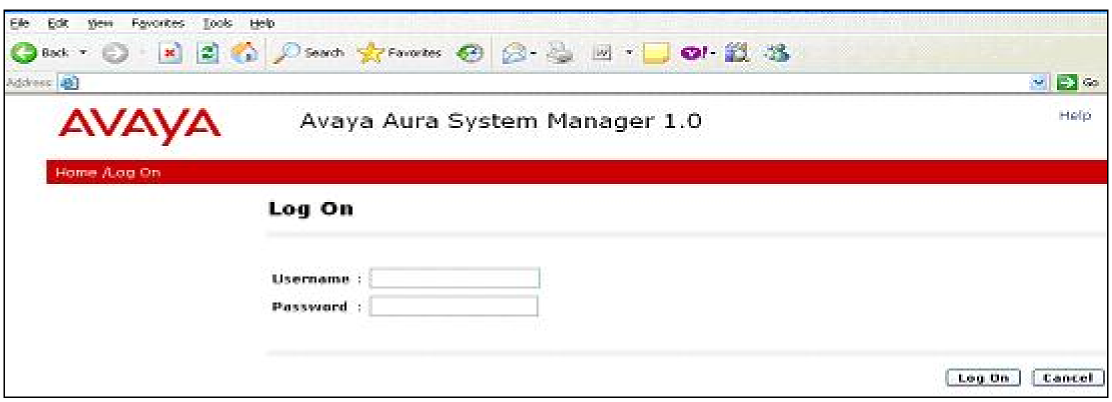

Figure 28: Avaya Aura™ **System Manager GUI Log On Screen**

4.3. Network Routing Policy

After logging in, the menu shown in **Figure 29** is displayed. Expand the **Network Routing Policy Link** on the left side as shown.

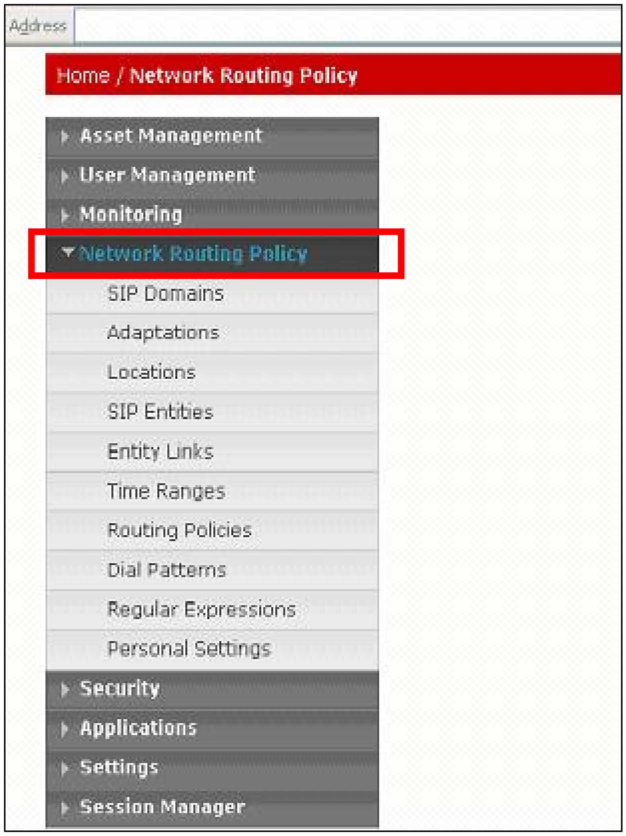

Figure 29: Network Routing Policy Menu

4.3.1 SIP Domains

As described in **Section 1.1.1** the Avaya CPE already has a local Fully Qualified Domain name (FQDN) of, *adevc.avaya.globalipcom.com* (simulating a customer with an existing FQDN) and The Verizon Business IPCC Services node used the IP address of 63.79.179.178 instead of an FQDN.

Therefore only the Avaya CPE FQDN needed to be provisioned in Avaya Aura™ Session Manager.

1. Select **SIP Domains** from the menu.
2. Select **New**.
3. Enter the SIP Domain FQDN in the **Name** field.
4. Enter a description in the **Notes** field if desired.
5. When completed, the SIP Domain window will look like **Figure 30**.
6. Click on the **Commit** button.

Note – On most of the following forms, to edit or delete an entry, click the box next to the item to select it, to make the Edit and Delete buttons available.

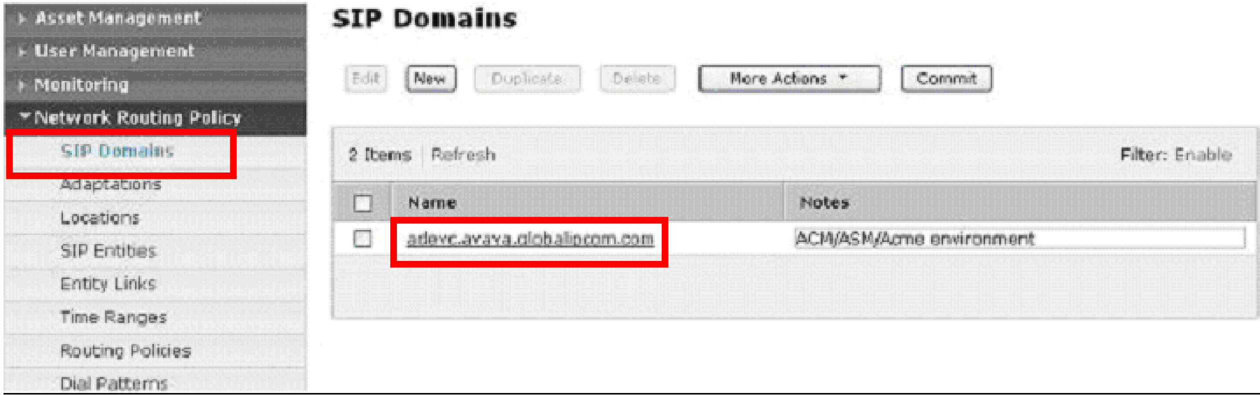

Figure 30: SIP Domain Menu

4.3.2 Adaptations

Avaya Aura™ Session Manager provides for specialized code modules to process specific call processing requirements of various vendors and/or services. These pre-defined modules are called adaptations. One of these pre-defined adaptations is used in the reference configuration: ***DigitConversionAdapter*** (see **Section 4.3.2.1**). This adaptation may be specifically added, or if any other adaptation is provisioned, the DigitConversionAdapter functionality is automatically added.

In the reference configuration, the DigitConversionAdapter adaptation is used twice. It is used to perform digit conversion for Avaya Aura™ Communication Manager between its local extensions and associated Verizon toll free numbers (see **Section 4.3.2.1**). It is also used as a mechanism to convert the Avaya CPE FQDN to the Verizon Business IPCC Services node IP address in the outbound Request URI headers (see **Section 4.3.2.2**). In this second case no digit conversion is performed.

4.3.2.1 DigitConversionAdapter - Avaya Aura™ Communication Manager / Avaya Aura™ Session Manager

This adaptation allows Avaya Aura™ Session Manager to convert inbound and/or outbound digits in SIP Request-URI, History-Info header, P-Asserted-Identity header, and Notify messages, based on the SIP Entities to which this adaptation is defined. This functionality is similar to the Avaya Aura™ Communication Manager public-unknown-numbering and incoming-call-handling-treatment capabilities.

Avaya Aura™ Session Manager will perform digit conversion based on whether the digits are being received by (incoming) or sent from (outgoing) Avaya Aura™ Session Manager with another SIP Entity. For example, on a call from Avaya Aura™ Communication Manager to Verizon, the call leg from Avaya Aura™ Communication Manager to Avaya Aura™ Session Manager is incoming, while the call leg from Avaya Aura™ Session Manager to the Acme Packet is outgoing.

In the reference configuration the DigitConversionAdapter is used convert Avaya Aura™ Communication Manager extensions to their associated toll free numbers, and is applied to the Avaya Aura™ Communication Manager Clan SIP Entity (see **Section 4.3.4**). This means the specified digit conversions will take place during Avaya Aura™ Communication Manager and Avaya Aura™ Session Manager call processing.

Extension	Toll Free Number
30001	866-797-8011
30002	866-797-3994
30003	866-797-5598

1. Select **Adaptations** from the menu.
2. Select **New**.
3. Enter a descriptive name (e.g. **Digit Conversion**)
4. Specify **DigitConversionAdapter** in the Adaptation Module field.
5. Leave the **Egress URI Parameters** field blank (this is for adding additional parameters such as user=phone).
6. Enter a description in the **Notes** field if desired.

4.3.2.1.1 Outbound - Avaya Aura™ Communication Manager to Avaya Aura™ Session Manager

In this example Avaya Aura™ Communication Manager extension 30001 will be converted to Verizon toll free number **866-828-8011** for calls going from Avaya Aura™ Communication Manager to Avaya Aura™ Session Manager.

7. Click the **Add** button and enter:
    a. **Matching Pattern** – The digit string to match → **30001**
    b. **Min** – The minimum number of digits → **5**
    c. **Max** – The maximum number of digits → **5**
    d. **Delete Digits** – The number of digits to delete → **5**
    e. **Insert Digits** – The digit to be inserted → **866-828-8011**
    f. **Address to Modify - origination/destination/both** – Associated headers to be monitored for matching digits. → **Both**
    g. **Notes** - Enter a description in the **Notes** field if desired.
    h. Repeat a thru g for each incoming digit conversion.

4.3.2.1.2 Inbound - Avaya Aura™ Session Manager to Avaya Aura™ Communication Manager

In the outgoing example Verizon toll free number **866-828-8011** will be converted to Avaya Aura™ Communication Manager extension 30001 for calls going from Avaya Aura™ Session Manager to Avaya Aura™ Communication Manager.

8. Click the **Add** button and enter:
    a. **Matching Pattern** – The digit string to match → **866-828-8011**
    b. **Min** – The minimum number of digits → **10**
    c. **Max** – The maximum number of digits → **10**
    d. **Delete Digits** – The number of digits to delete → **10**
    e. **Insert Digits** – The digit to be inserted → **30001**
    f. **Address to Modify - origination/destination/both** – Associated headers to be monitored for matching digits. → **Both**
    g. **Notes** - Enter a description in the **Notes** field if desired.

h. Repeat a thru g for each outgoing digit conversion.

9. Repeat steps 7 and 8 for extensions 30002 and 30003.
10. When completed, the Adaptation Details window for DigitConversionAdapter will look like **Figure 31**.
11. Click on the **Commit** button.

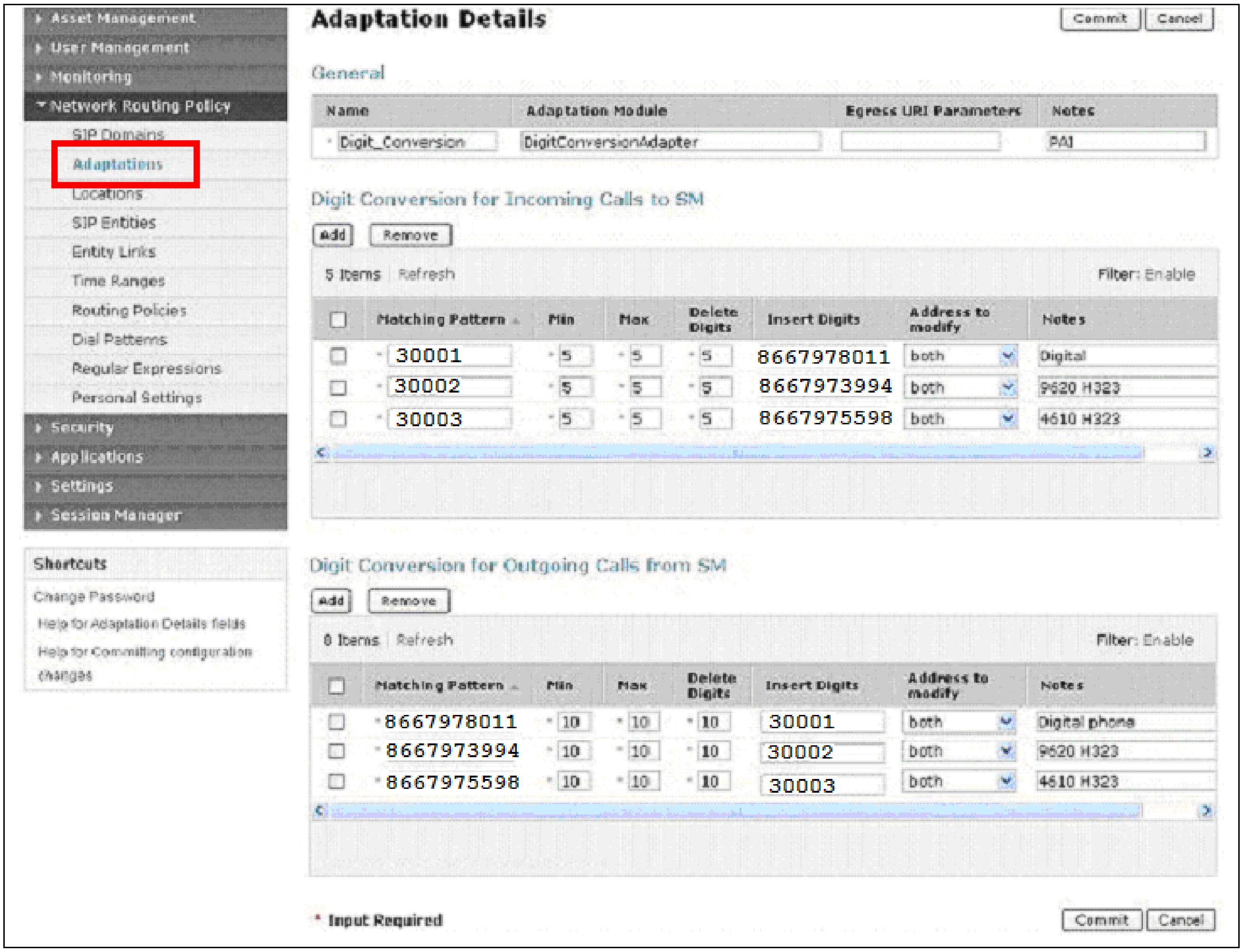

Figure 31: DigitConversionAdapter Adaptation

4.3.2.2 DigitConversionAdapter - Avaya Aura™ Session Manager / Acme SBC

As described in **Section 1.1.1**, Avaya Aura™ Communication Manager will put its local FQDN *adevc.avaya.globalipcom.com* in Request URIs of outbound calls; however the Verizon Business IPCC Services suite requires that the IP address of their service node be in the Request URI (*63.79.179.178*). This function may be performed by Avaya Aura™ Session Manager. Since this operation is only required for outbound calls, this operation should be applied as Avaya Aura™ Session Manager sends calls out to the Acme SBC. Therefore an adaptation must be defined for the Acme SIP Entity (see **Section 4.3.4**) that will perform this SIP header modification. In the reference configuration the DigitConversion Adaptation was used (although no digit conversion was performed here) using the following format:

DigitConversionAdapter 63.79.179.178

1. Select **Adaptations** from the menu.
2. Select **New**.
3. Enter a descriptive name (e.g. **VzB_IPCC_Lab**)
4. Specify **DigitConversionAdapter 63.79.179.178** in the Adaptation Module field (note the space between the two parameters).
5. Leave the **Egress URI Parameters** field blank (this is for adding additional parameters such as user=phone).
6. Enter a description in the **Notes** field if desired.
7. Click on the **Commit** button.

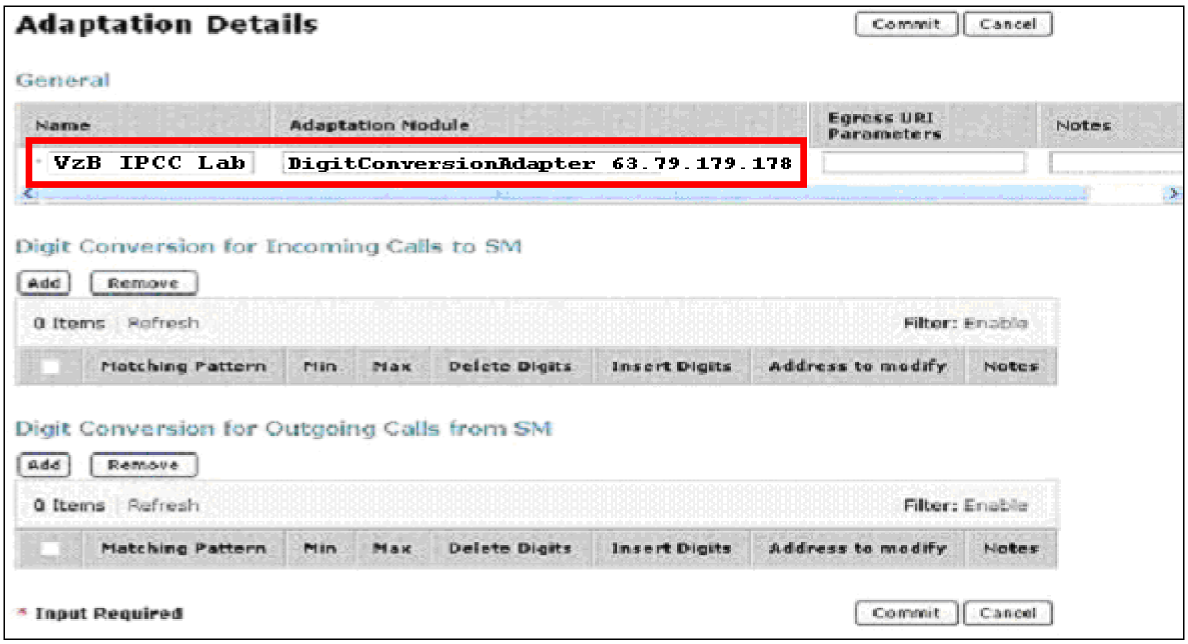

Figure 32: DigitConversionAdapter Adaptation with FQDN Replacement

Note - The DigitConversionAdapter was chosen for the FQDN replacement function, however the FQDN replacement function may be specified with any adaptation.

When completed the Adaptations page will look like **Figure 33**.

1. Click on the **Commit** button.

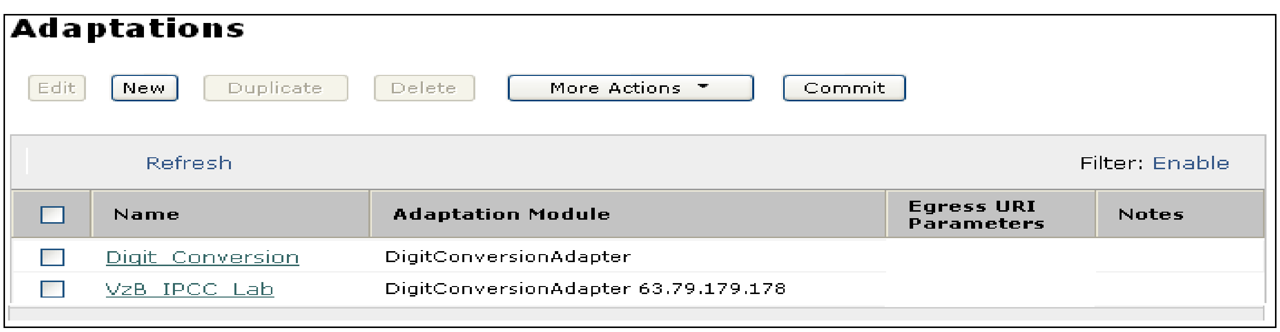

Figure 33: Completed Adaptations page

4.3.3 Locations

Locations are used to identify logical and/or physical locations where SIP Entities reside, by specifying the IP addressing for the locations as well as for purposes of bandwidth management if required. In the reference configuration only the Avaya CPE location was defined. This was done because from the Avaya Aura™ Session Manager perspective, there was only one IP subnet. The Acme Packet SBC was the only device that was connected to an "outside" IP segment.

To add a location, select **Locations** in the left **Network Routing Policy** menu and click on the **New** button on the right. The screen shown in **Figure 34** will open.

1. Enter a descriptive location name in the **Name** field (e.g. **adevc**).
2. Enter a description in the **Notes** field if desired.
3. Under the **Location Pattern** heading, click on **Add**.
4. Enter IP address information for the location (e.g. **65.206.67.***)
5. Enter a description in the **Notes** field if desired.
6. Repeat steps 3 thru 5 if the location has multiple IP segments.
7. Modify the remaining values on the form if necessary, otherwise use all the default values.
8. Click on the **Commit** button.
9. Repeat all the steps for each new location.

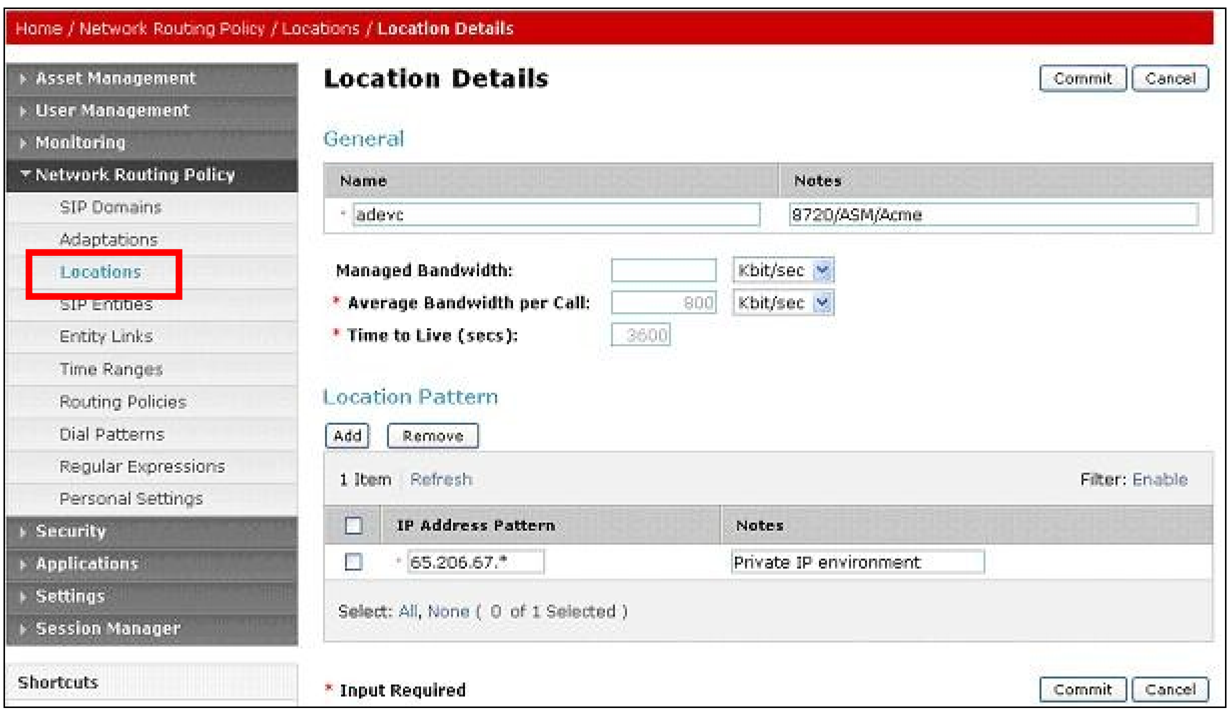

Figure 34: Locations Menu

4.3.4 SIP Entities

A SIP Entity must be added for Avaya Aura™ Session Manager and for each network component that has a SIP trunk provisioned to Avaya Aura™ Session Manager. In the reference configuration the SIP Entities are provisioned for:

- Avaya Aura™ Communication Manager (C-LAN) voice SIP trunk
- The Acme Packet SBC
- Avaya Aura™ Session Manager itself.

To add a SIP Entity, select **SIP Entities** on the left **Network Routing Policy** menu and click on the **New** button on the right. The screen shown in **Figure 35** is displayed.

1. **General** Section
   a. Enter a descriptive location name in the **Name** field.
   b. Enter the IP address for the SIP Entity (e.g. **65.206.67.7** for the C-LAN).
   c. From the **Type** drop down menu select a type that best matches the SIP Entity (e.g. **CM**).
   d. Enter a description in the **Notes** field if desired.
   e. From the **Adaptations** drop down menu, select the adaption required for this Entity (see **Section X**).
      i. For the voice C-LAN Entity, the DigitConversion adaptation is selected. This function is applied to the C-LAN Entities to convert Avaya extensions to Verizon toll free numbers and vice versa depending on whether the call is inbound from Avaya Aura™ Communication Manager to Avaya Aura™ Session Manager or outbound from Avaya Aura™ Session Manager to Avaya Aura™ Communication Manager.
      ii. For the Acme Packet Entity, the **VzB_IPCC_Lab** adaptation was selected. This function is applied to the Acme Packet Entities to convert the outbound call (Avaya Aura™ Session Manager to Acme) request URI FQDN, from the Avaya CPE FQDN used by Avaya Aura™ Communication Manager to the Verizon service node IP address.
   f. From the Locations drop down menu select **adevc**.
   g. Select the appropriate time zone.
   h. Accept the other default values.
2. **Sip Link Monitoring** section
   a. Accept the default values.
3. Click on **Commit**.
4. Repeat these steps for each SIP Entity

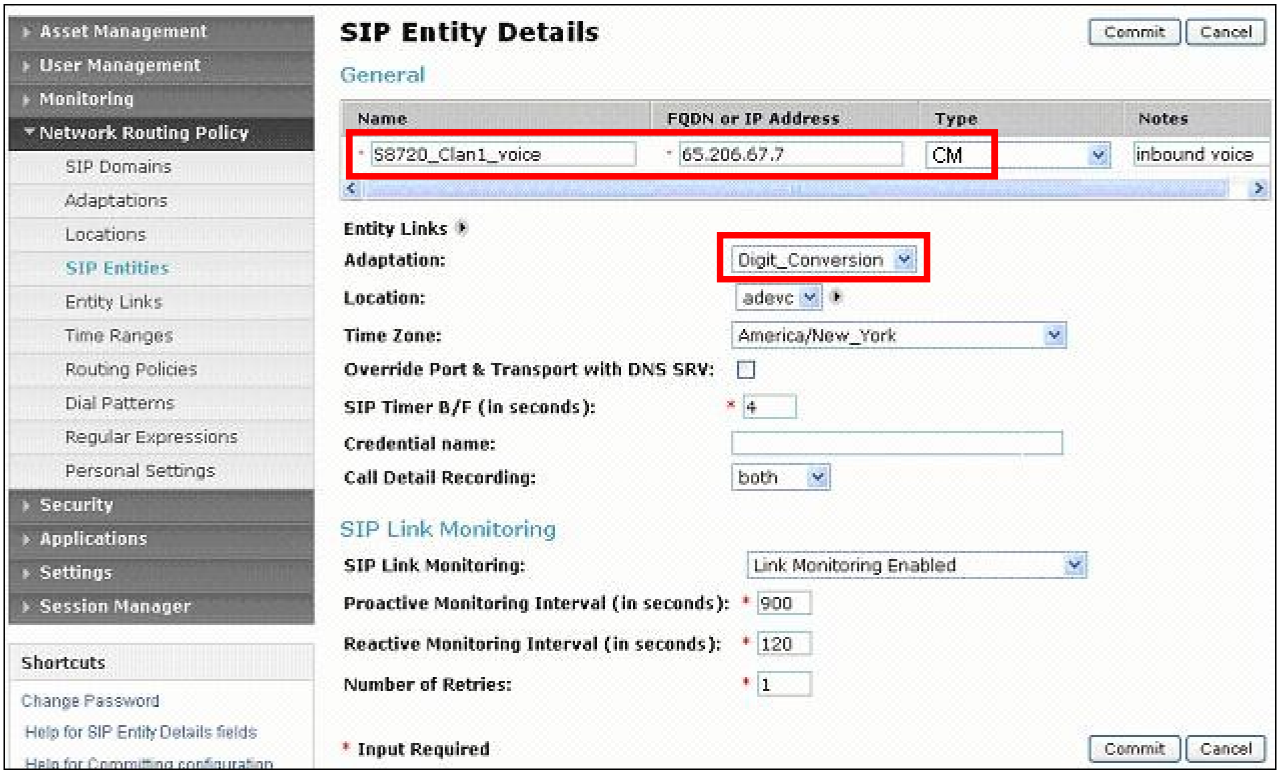

Figure 35: C-LAN SIP Entity Details

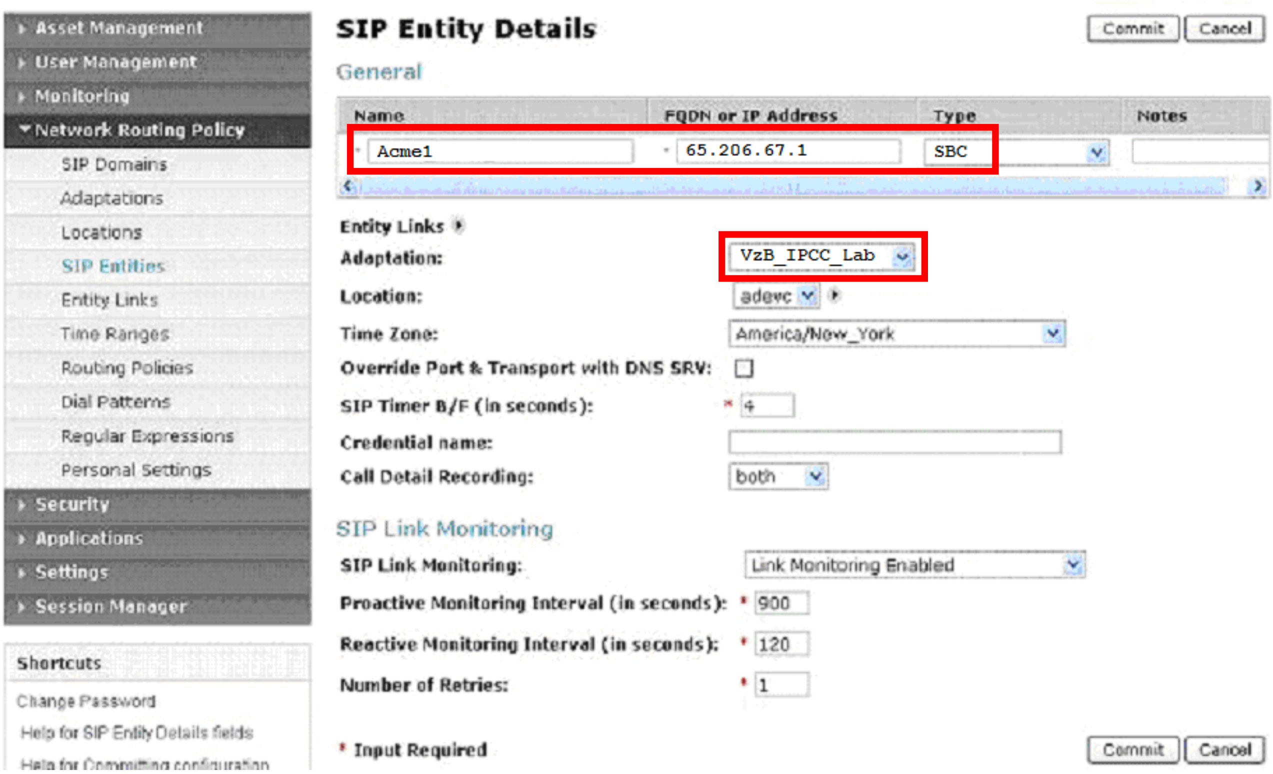

Figure 36: Acme1 SIP Entity Details

Note – When defining a SIP Entity for Avaya Aura™ Session Manager itself and the "SM" option is selected from the Type drop down menu, and addition section called Ports will appear. In this section add the transport protocol, port and FQDN used by Avaya Aura™ Session Manager. In the reference configuration the values used were 5060, TCP and the Avaya CPE FQDN.

The following SIP Entity values were specified in the reference configuration:

Name	IP Address	Type	Adaptation	Location	Port	Protocol	Domain
Acme1	65.206.67.1	SBC	VzB_IPCC_Lab	adevc	-	-	Avaya CPE
ASM1	65.206.67.2	SM	-	adevc	5060	TCP	Avaya CPE
CLAN-Voice	65.206.67.7	CM	DigitConversion	adevc	-	-	Avaya CPE

Table 6: SIP Entity Provisioning

Figure 37 show the completed SIP Entities form.

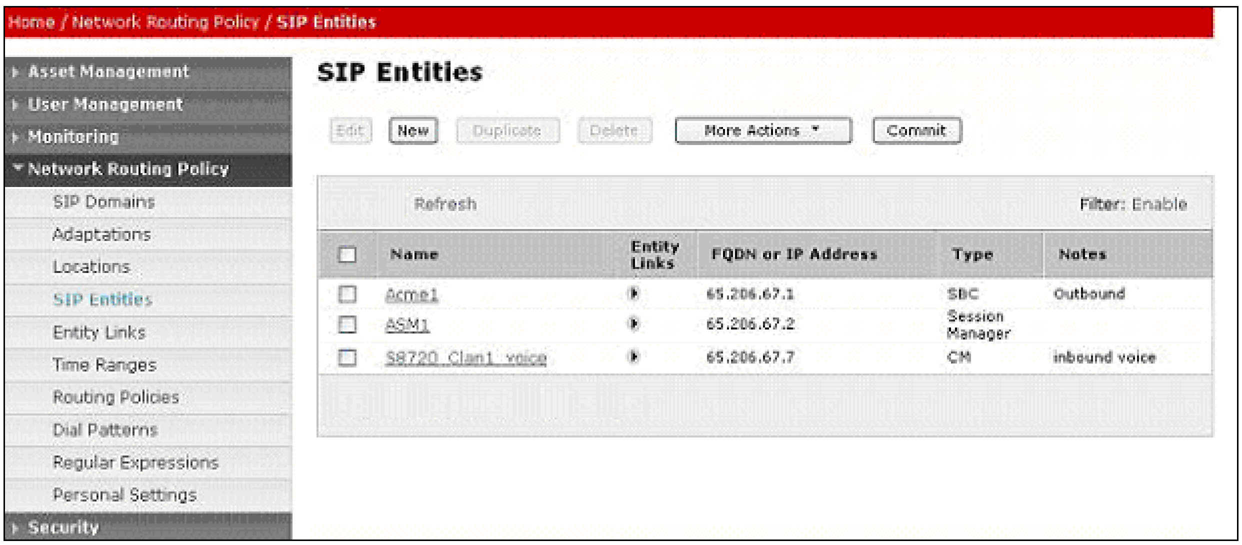

Figure 37: Completed SIP Entities Form

Note – As described in this section, both the "DigitConversion" and "VzB_IPCC_Lab" adaptations are defined in SIP Entities.

The "DigitConversion" adaptation is provisioned on the Avaya Aura™ Communication Manager Clan SIP Entity (S8720_Clan1_voice). This means that the digit conversion from Verizon toll free numbers to Avaya Aura™ Communication Manager extensions is performed ***after*** the dial pattern match for <u>inbound</u> calls to Avaya Aura™ Communication Manager, and ***before*** the dial pattern match for <u>outbound</u> calls to Verizon/PSTN.

The "VzB_IPCC_Lab" adaptation is provisioned on the Acme SIP Entity (Acme1). This means that the Request URI manipulation from the Avaya CPE FQDN to the Verizon service node IP address is performed ***after*** the dial pattern match for <u>outbound</u> calls to Verizon/PSTN.

4.3.5 Entity Links

Note – In the Entity Link configurations below (and in the Avaya Aura™ Communication Manager SIP trunk configuration, **Section 3.1.5**), TCP was selected as the transport protocol for the Avaya CPE in the reference configuration. TCP was used to facilitate trace analysis during network verification. The use of TLS protocol is recommended by Avaya in customer deployments.

Entity Links defined the connections between the SIP Entities and Avaya Aura™ Session Manager. In the reference configuration Entity Links are defined between Avaya Aura™ Session Manager and:

- The Acme Packet (Acme1)
- The Avaya Aura™ Communication Manager C-LAN for voice calls (S8720_Clan1_voice)

To add an Entity Link, select **Entity Links** on the left **Network Routing Policy** menu and click on the **New** button on the right. The screen shown in **Figure 38** is displayed.

1. Enter a descriptive location name in the **Name** field.
2. In the **SIP Entity 1** drop down menu select the Avaya Aura™ Session Manager SIP Entity created in **Section 4.3.4** (e.g. **ASM1**).
3. In the **Port** field enter **5060**.
4. In the **SIP Entity 2** drop down menu select the **Acme1** SIP Entity created in **Section 4.3.4**.
5. In the **Port** field enter **5060**.
6. Check the **Trusted** box.
7. In the **Protocol** drop down menu select **TCP**.
8. Enter a description in the **Notes** field if desired (not shown).
9. Click on the **Commit** button.

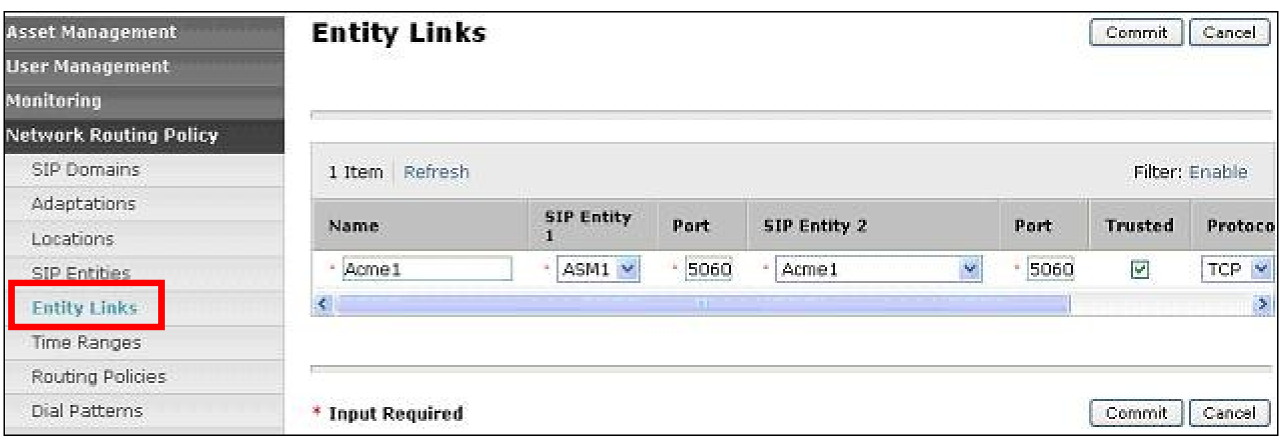

Figure 38: Entity Link – Primary Acme Packet

When completed, the Entity Links form will look like **Figure 39**.

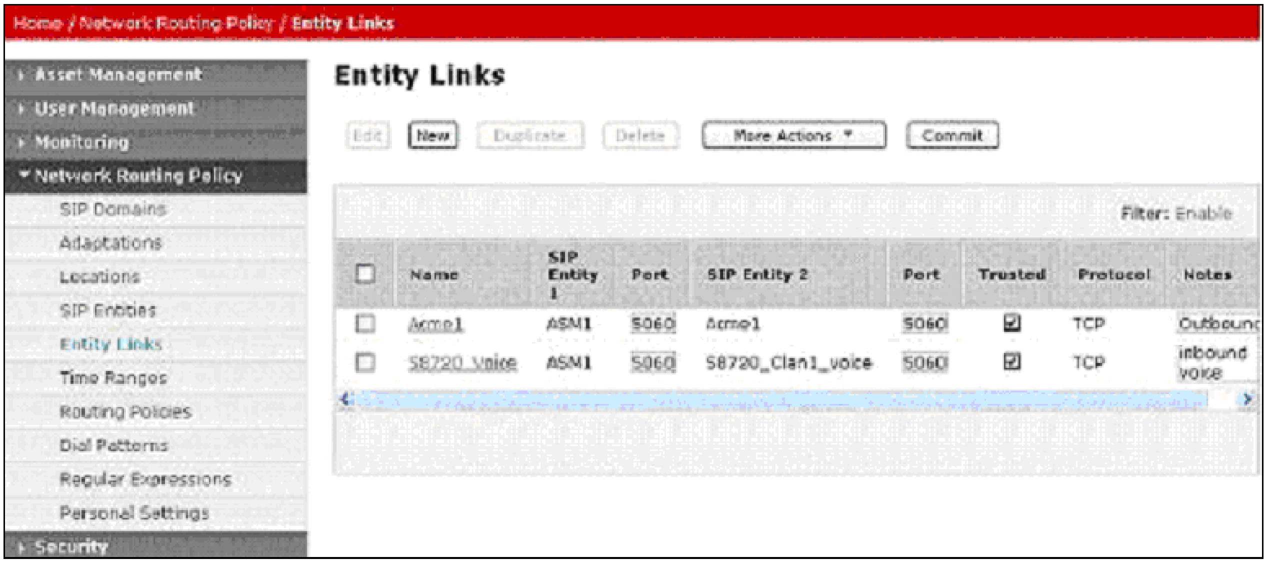

Figure 39: Completed Entity Links Form

4.3.6 Time Ranges

The Time Ranges form allows admission control criteria to be specified for Routing Policies (**Section 4.3.7**). In the reference configuration no restrictions were used.

To add a Time Range, select **Time Ranges** on the left **Network Routing Policy** menu and click on the **New** button on the right. The screen shown in **Figure 40** is displayed.

1. Enter a descriptive location name in the **Name** field (e.g. **Anytime**).
2. Check each day of the week.
3. In the **Start Time** field enter **00:00**.
4. In the **End Time** field enter **23:59**.
5. Enter a description in the **Notes** field if desired.
6. Click the **Commit** button.

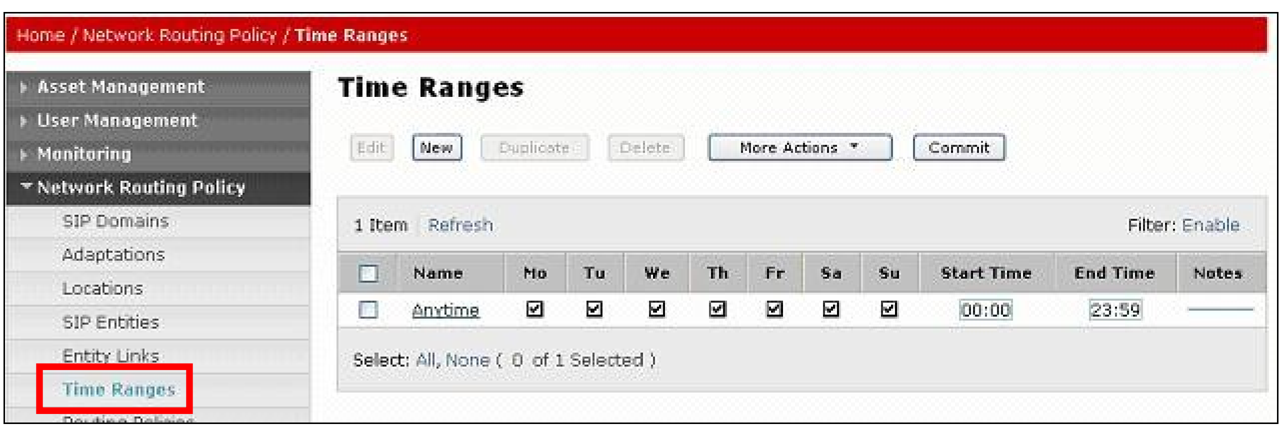

Figure 40: Time Ranges

4.3.7 Routing Policies

Routing Policies associate destination SIP Entities (**Section 4.3.4**) with Time of Day admission control parameters (**Section 4.3.6**) and Dial Patterns (**Section 4.3.8**). In the reference configuration Routing Policies are defined for:

- Inbound voice calls (to Avaya Aura™ Communication Manager)
- Outbound calls to Acme1 (outbound calls to Verizon)

Note – In the reference configuration the **Regular Expressions** parameters was not used.

Name	SIP Entity Destination	Time Of Day	Dial Pattern(s)	Notes
Inbound	S8720_Clan1_Voice	Anytime	866797 - 10 digits	Any call to 866797xxxx will be sent to Avaya Aura™ Communication Manager stations (after digit conversion), and use port 5060.
Outbound	Acme1	Anytime	732 -10 digits	All matching dial patterns will route to Acme1 to be sent to Verizon/PSTN.

Table 7: Routing Policy Provisioning

To add a Routing Policy, select **Routing Policies** on the left **Network Routing Policy** menu and click on the **New** button on the right. The window shown in **Figure 41** will open.

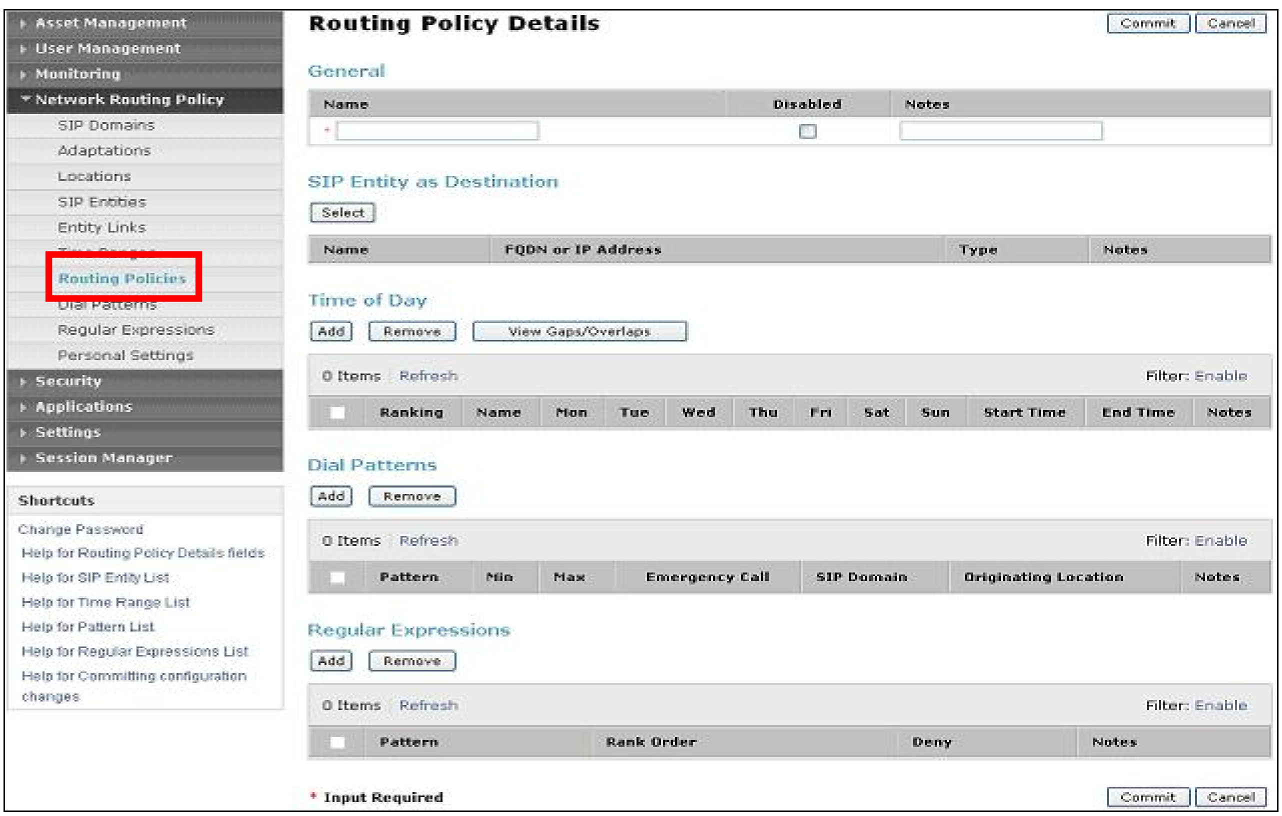

Figure 41: Routing Policy Details

1. **General** section
    a. Enter a descriptive location name in the **Name** field (e.g. **Inbound**).
    b. Enter a description in the **Notes** field if desired.
2. **SIP Entity as Destination** section
    a. Click the **Select** button.
    b. Select the SIP Entity that will be the destination for this call (e.g. **S8720_Clan1_voice**)
    c. Click the **Select** button and return to the Routing Policy Details form.
3. **Time of Day** section
    a. Click the **Add** button and select the **Time Range** for this Routing Policy.
    b. Click on **Select** and return to the Routing Policy Details form.

Note – Multiple time ranges may be selected and a Ranking value applied (0 is the highest).

4. **Dial Pattern** section
    a. Click the **Add** button and select the **Dial Pattern(s)** for this Routing Policy (dial patterns are discussed in the next section).
    b. Click on **Select** and return to the Routing Policy Details form. The form will look like **Figure 42**.

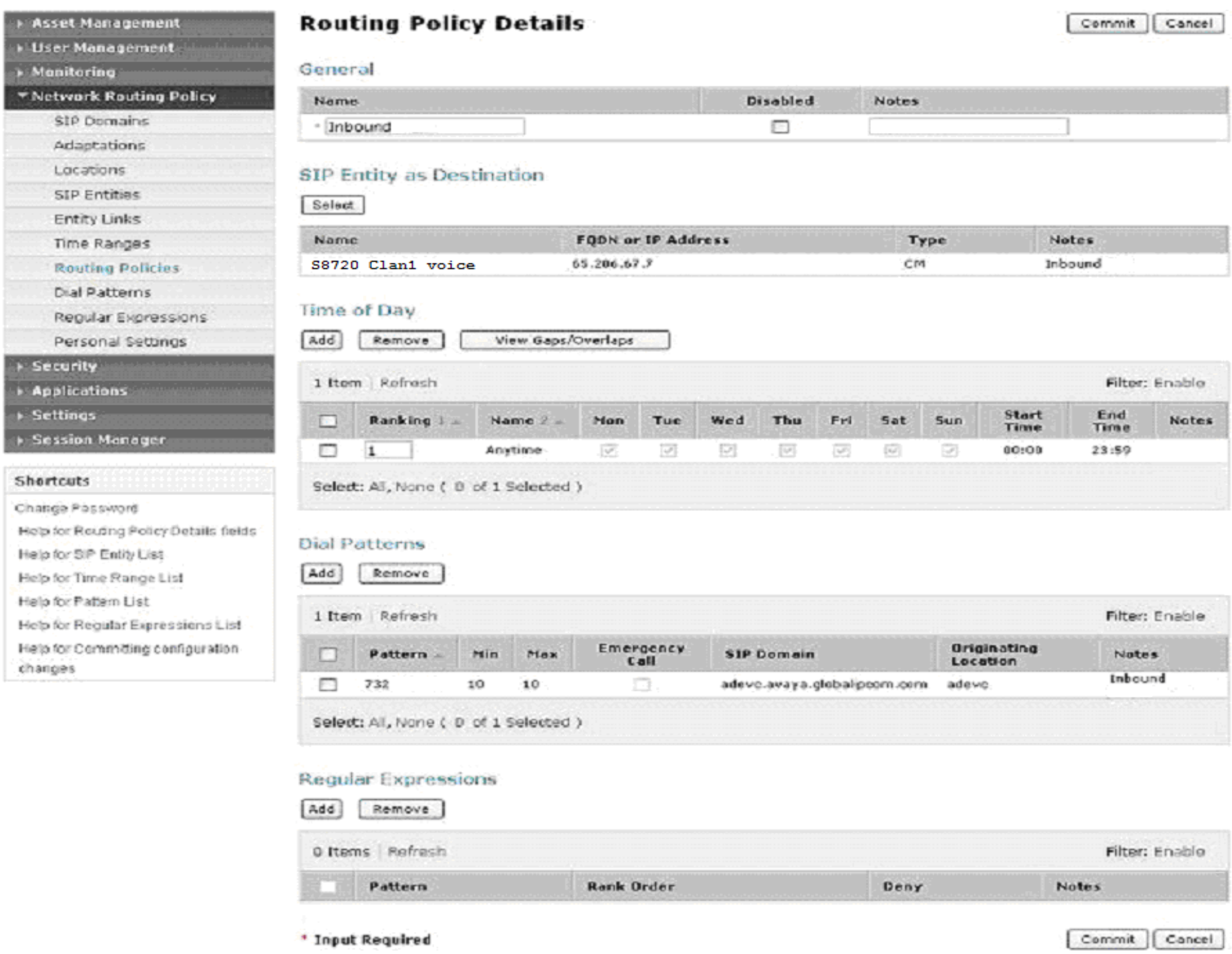

Figure 42: Inbound Routing Policy Details - Completed

5. Click the **Commit** button.
6. Repeat steps 1 thru 5 for the outbound Routing Policy (e.g. 732xxxxxxx). When completed the form will look like **Figure 43**.

Figure 43: Routing Policies- Completed

7. Click the **Commit** button.

4.3.8 Dial Patterns

Dial Patterns define digit strings to be matched for inbound and outbound calls. In addition, the FQDN in the request URI is also examined.

Note – The Dial Pattern digit string with the most complete match will be selected. For example if the 10 digit string 732 is defined first in the list, and the 10 digit string 732555 is defined last, an outbound call to 7325551212 will match on the 732555 entry.

The following Dial Patterns were provisioned in the reference configuration.

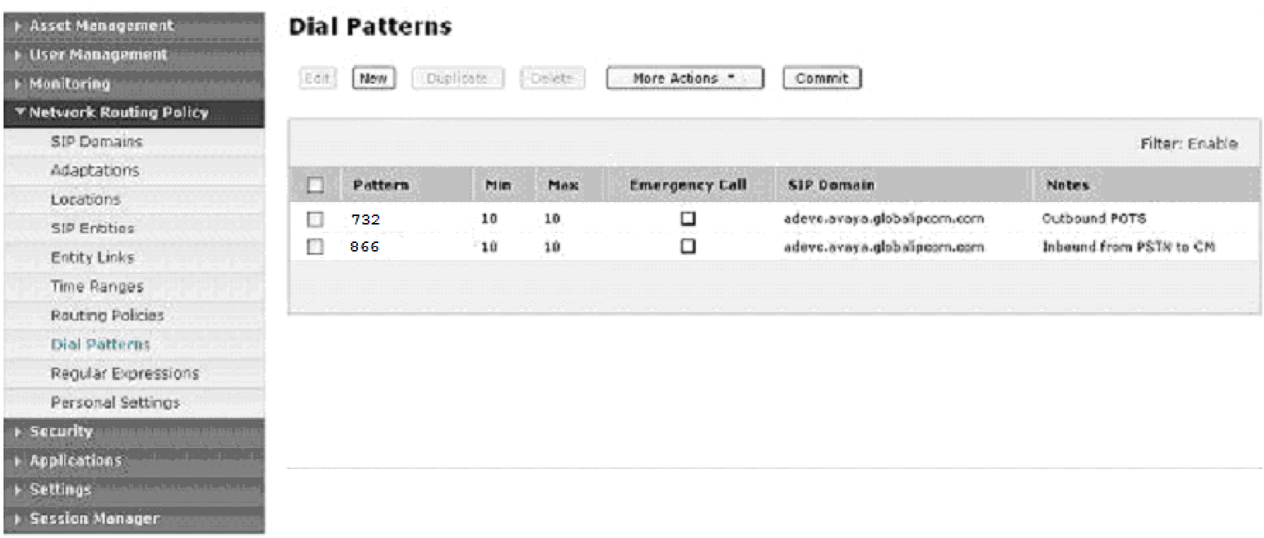

Figure 44: Completed Dial Pattern Form

To add a Dial Pattern, select **Dial Patterns** on the left **Network Routing Policy** menu and click on the **New** button on the right. The screen shown in **Figure 45** is displayed. In this example a Request URI to a 10 digit number beginning with *732*, and sent by is defined (this would be an outbound call from Avaya Aura™ Communication Manager to Avaya Aura™ Session Manager, destined for Verizon).

1. **General** section
    a. Enter a unique pattern in the **Pattern** field (e.g. **732**).
    b. In the **Min** column enter the minimum number of digits (e.g. **10**).
    c. In the **Max** column enter the maximum number of digits (e.g. **10**).
    d. In the **SIP Domain** field drop down menu select the FQDN that will be contained in the Request URI *received* by Avaya Aura™ Session Manager from Avaya Aura™ Communication Manager (see **Sections 3.1.3 & 3.1.5**).
    e. Enter a description in the **Notes** field if desired.

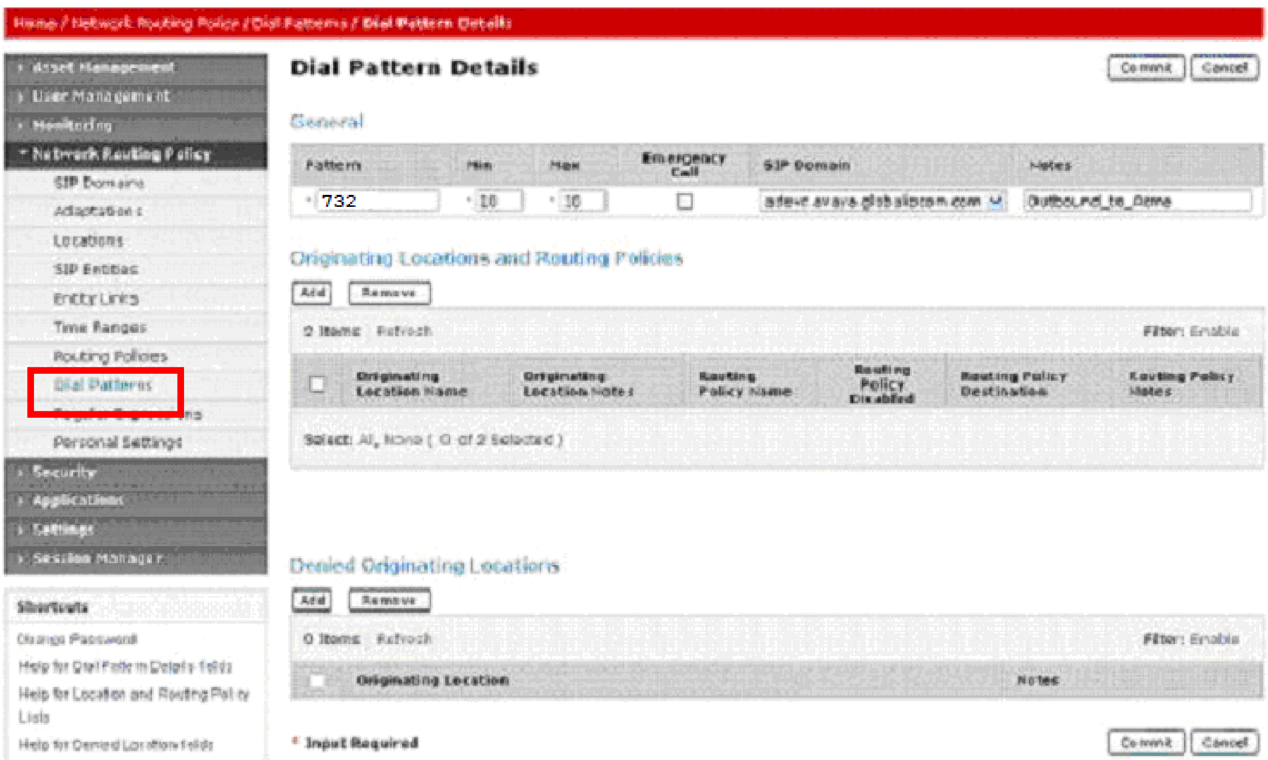

Figure 45: Dial Pattern Details - General

2. **Originating Locations and Routing Policies** Section
    a. Click on the Add button and the window in **Figure 46** will open.
    b. Click on the boxes for the appropriate Originating Locations (see **Section 4.3.3**), and Routing Policies (see **Section 4.3.7**) that pertain to this Dial Pattern.
        i. Location **adevc**
        ii. Routing Policy **Oubound1** (Acme1).
    c. Click on the **Select** button and return to the Dial Pattern window.

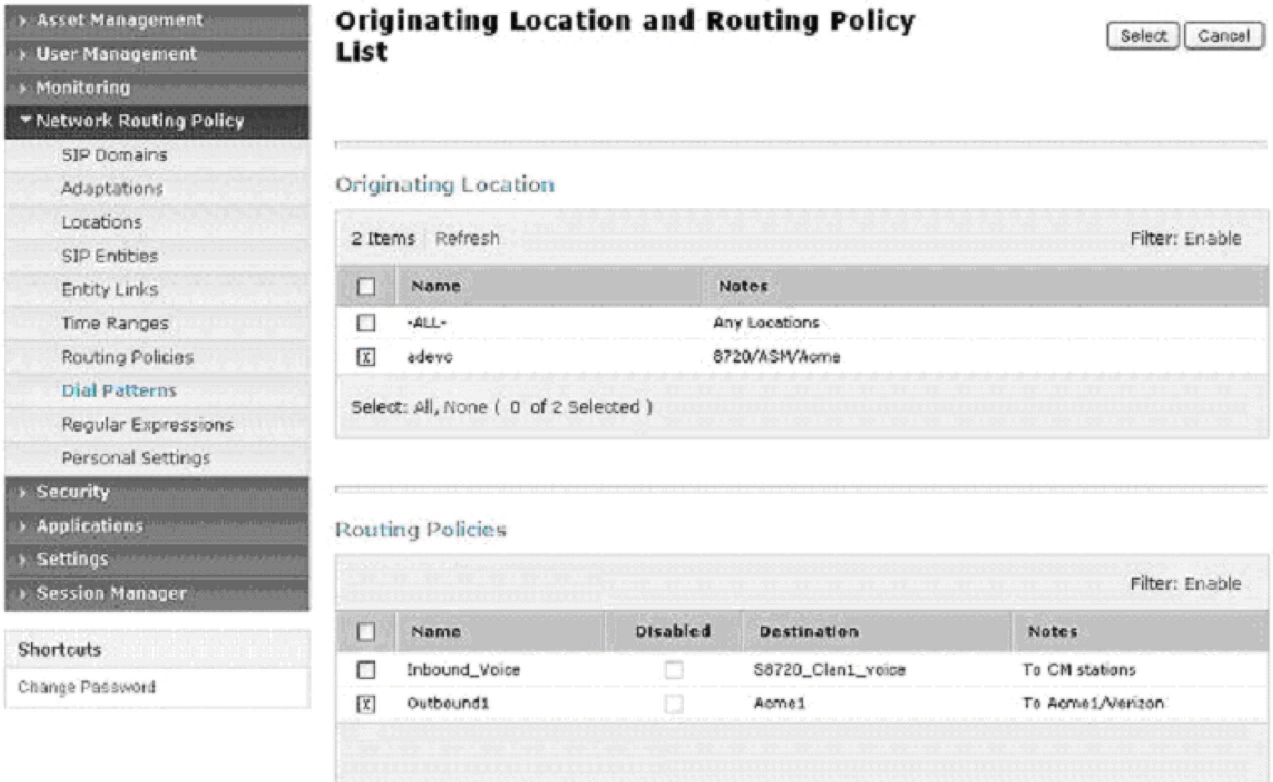

Figure 46: Dial Pattern Details – Originating Locations and Routing Policies

In the reference configuration a request URI of *7325551212@adevc.avaya.globalipcom.com* would match and be sent to Acme1.

3. Click the **Commit** button
4. Repeat steps 1 thru 3 for the inbound Dial Patterns (e.g. 866797xxxx toll free numbers). The completed Dial Pattern screen will look like **Figure 44** above.

4.4. Avaya Aura™ Session Manager

To complete the Avaya Aura™ Session Manager configuration, add an Avaya Aura™ Session Manager instance. To add an Avaya Aura™ Session Manager, select **Session Manager** on the left **Network Routing Policy** menu and click on the **New** button. The screen shown in **Figure 47** is displayed.

1. **General** section
   a. Enter a name in the **SIP Entity Name** field (e.g. **ASM1**).
   b. Enter an optional description in the **Description** field.
   c. In the **Management Access Point Host Name/IP** field enter the IP address of the management interface of the Avaya Aura™ Session Manager server. (e.g. **65.206.67.20**).
2. **Security Module** section
   a. Enter the **Network Mask** (e.g. **255.255.255.0**)
   b. Enter the **Default Gateway** (e.g. **65.206.67.1**)

c. In the **Speed & Duplex** drop down menu verify **Auto** is selected (default).

3. Use all other default parameters.

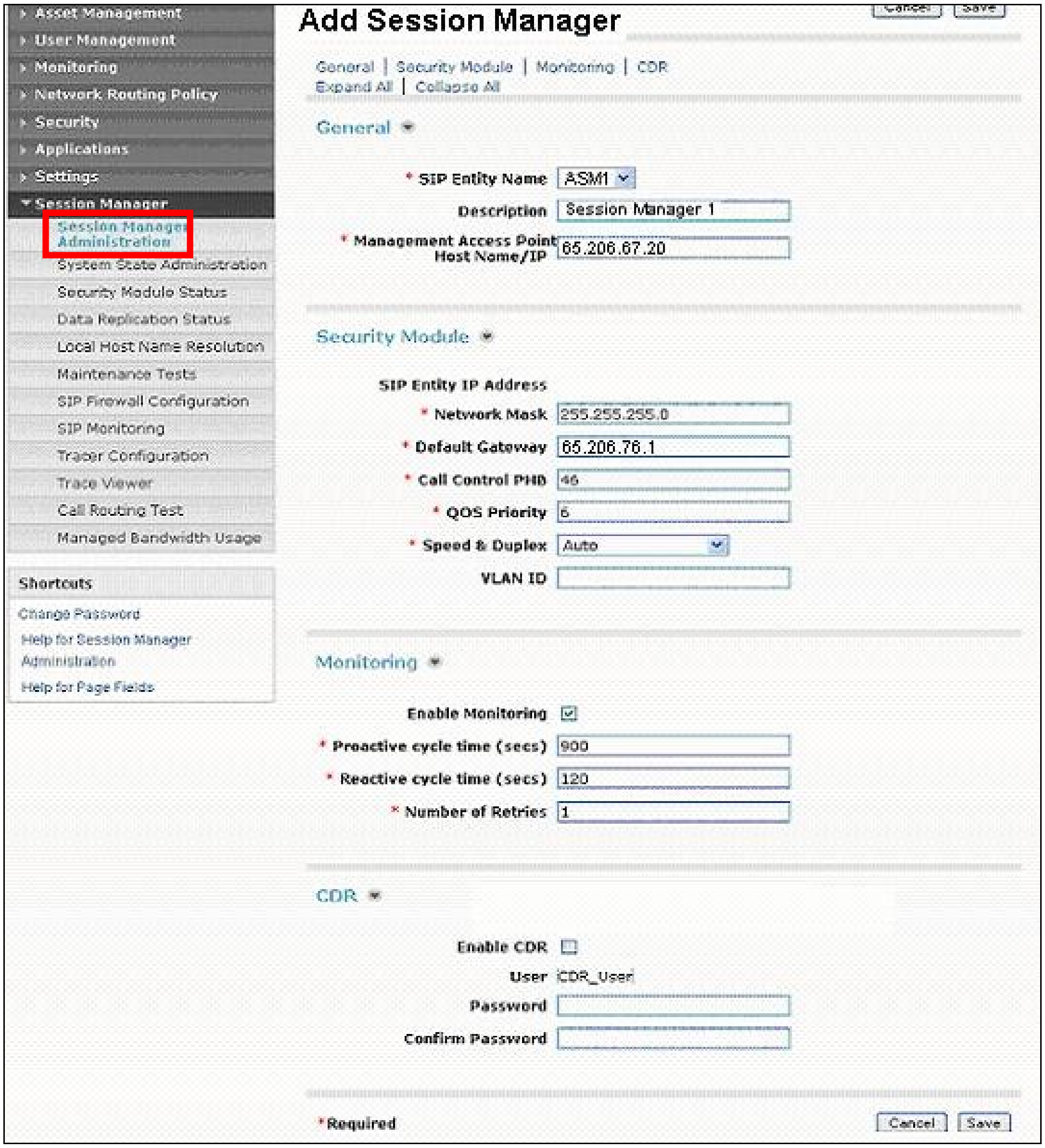

Figure 47: Add Session Manager

4. Click the **Save** button and the completed form shown in **Figure 48** will be displayed.

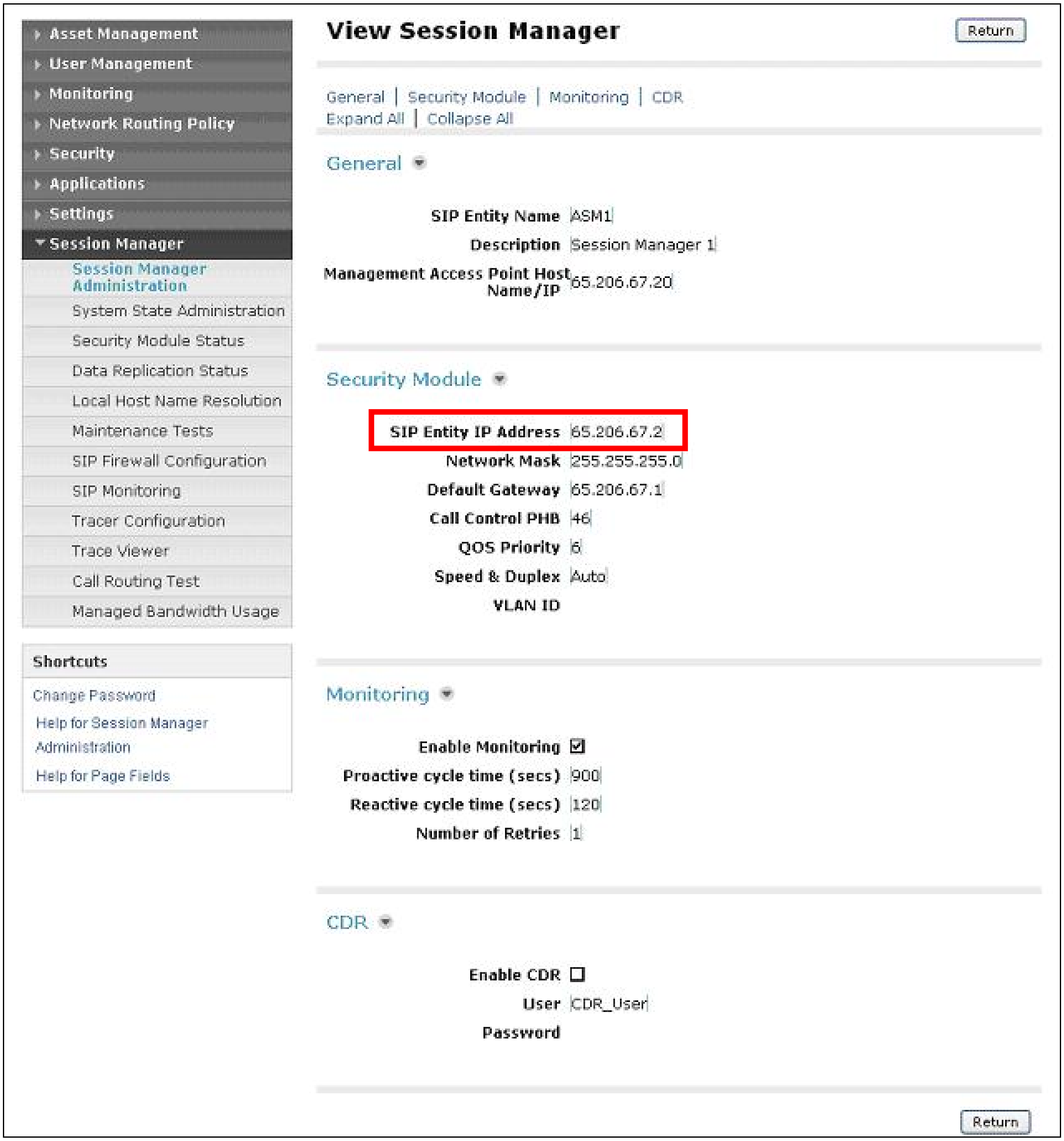

Figure 48: Completed Session Manager Form

Note – The SIP Entity IP address (under the Security Module heading) is automatically populated with the IP address defined for this SIP Entity (**ASM1**) in **Section 4.3.4**.

5. Acme Packet 3800 Net-Net Session Director

In the reference configuration an Acme Packet 3800 Net-Net Session Director is used as the edge device between the Avaya CPE and the Verizon Business. The Acme Packet SBC provides Network Address Translation (NAT) functionality to convert the private Avaya CPE IP addressing to public addressing, as well as performing SIP header manipulation.

5.1. Acme Packet Service State

The Acme SBC requests and provides service states by sending out and responding to SIP *OPTIONS* messages. The Acme sends the OPTIONS message with the hop count (SIP Max-Forwards) set to zero.

- Acme/Avaya Aura™ Session Manager
  - Acme Packet sends OPTIONS → Avaya Aura™ Session Manager responds with 200 OK
  - Avaya Aura™ Session Manager sends OPTIONS → Acme Packet responds with 200 OK
- Acme/Verizon
  - Acme Packet sends OPTIONS → Verizon responds with 483 Too Many Hops[1]
  - Verizon sends OPTIONS → Acme Packet responds with 200 OK

5.2. Acme Packet Network Interfaces

Figure 49 shows the Acme Packet network interface connections used in the reference configuration. The physical and network interface provisioning for the "OUTSIDE" (to Verizon) and "INSIDE" (to Avaya CPE) interfaces is described in **Sections 5.3.3 and 5.3.4**.

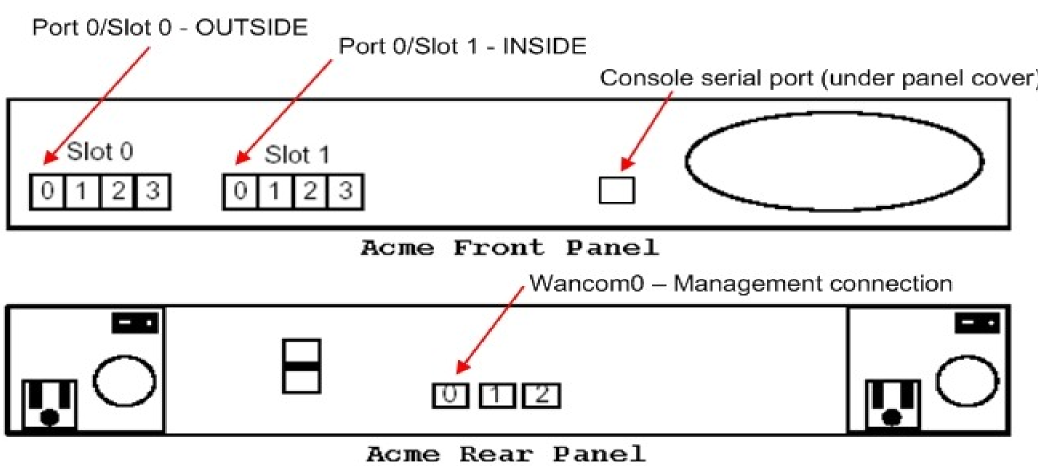

Figure 49: Acme Packet Network Interfaces

[1] In the reference configuration Acme sends the OPTIONS message with the hop count (SIP Max-Forwards) set to zero (unlimited). The Verizon Business IPCC Services node responds to this parameter with 483 Too Many Hops. This is an expected response and the Acme treats this response as a positive acknowledgement.

5.3. Acme Packet Provisioning

Note – Only the Acme Packet provisioning required for the reference configuration is described in these Application Notes. For more information on Acme Packet configuration see **[11 & 12]**.

The Acme Packet SBC was configured using the Acme Packet CLI via a serial console port connection. An IP remote connection to a management port is also supported. The following are the generic steps for configuring various elements.

1. Log in with the appropriate credentials.
2. Enable the Superuser mode by entering **enable** command and the appropriate password (prompt will end with #).
3. In Superuser mode, type **configure terminal** and press <ENTER>. The prompt will change to (*configure)#*.
4. Type the name of the element that will be configured (e.g., **session-router**).
5. Type the name of the sub-element, if any (e.g., **session-agent**).
6. Type the name of the parameter followed by its value (e.g., **ip-address**).
7. Type **done**.
8. Type **exit** to return to the previous menu.
9. Repeat steps 4-8 to configure all the elements. When finished, exit from the configuration mode by typing **exit** until returned to the Superuser prompt.
10. Type **save-configuration** to save the configuration.
11. Type **activate-configuration** to activate the configuration.

Once the provisioning is complete, the configuration may be verified by entering the ***show running-config*** command.

5.3.1 Acme Packet Management

Initial Acme Packet provisioning is performed via the console serial port (115200, 8/None/1/None). Network management is enabled by provisioning interface "Wancom0". In the reference configuration, the management IP address 172.16.253.230 is assigned.

From the *configure* prompt (steps 1 thru 3 in **Section 5.3**):

1. Enter **bootparam**

   Note - This command will prompt one line at a time showing the existing value. Enter the new value next to the existing value. If there is no change to a value, hit the enter key and the next line will be presented. Be careful not to modify any values other than those listed below, or the Acme Packet may not recover after a reboot.

   Console output will appear as follows:

```
acmesbc-pri(configure)# bootparam

'.' = clear field;  '-' = go to previous field;  q = quit

boot device          : wancom0
```

2. Press Enter at the **boot device : wancom0** line, and the next 4 lines until the following is displayed:

inet on ethernet (e)   :

3. Enter the IP address and mask (in hex) to be used for network management (e.g. **172.16.253.230:ffffff00**) and press Enter 3 more times until the following is displayed:

gateway inet (g)   :

4. Enter the management network gateway IP address (e.g. **172.16.253.4**) and press Enter.
5. Continue to press Enter until returned to the "configure" prompt. After the last bootparam line, the following message is displayed:

NOTE: These changed parameters will not go into effect until reboot. Also, be aware that some boot parameters may also be changed through PHY and Network Interface Configurations.

6. At the "configure" prompt enter **exit**
7. Reboot the Acme Packet by entering **reboot** at the Superuser "#" prompt.

5.3.2 Local Policies

Allows any SIP requests from the **INSIDE** realm to be routed to the SERV_PROVIDER Session Agent Group in the OUTSIDE realm (and vice-versa).

5.3.2.1 INSIDE to OUTSIDE

From the *configure* prompt (steps 1 thru 3 in **Section 5.3**):

1. Create a local-policy for the INSIDE realm
   a. Enter **session-router → local-policy**
   b. Enter **from-address → ***
   c. Enter **to-address → ***
   d. Enter **source-realm → INSIDE**
   e. Enter **state → enabled**
   f. Enter **policy-attributes**
   g. Enter **next-hop → SAG:SERV_PROVIDER**
   h. Enter **realm → OUTSIDE**
   i. Enter **action → none**
   j. Enter **start-time → 0000**
   k. Enter **end-time → 2400**
   l. Enter **days-of-week → U-S**
   m. Enter **app-protocol → SIP**
   n. Enter **state → enabled**
   o. Enter **exit**
   p. Enter **done**

5.3.2.2 OUTSIDE to INSIDE

1. Create a local-policy for the **OUTSIDE** realm. Procedures are the same as for the INSIDE local-policy except:
   a. Enter **source-realm → OUTSIDE**
   b. Enter **policy-attributes**
   c. Enter **next-hop → SAG:ENTERPRISE**
   d. Enter **realm → INSIDE**
   a. Enter **action → replace-uri**

5.3.3 Network Interfaces

This Section defines the network interfaces to the private (Avaya CPE) and public (Verizon) IP networks.

5.3.3.1 Public Interface

1. Create a network-interface to the public (Internet/Verizon) side of the Acme.
   a. Enter **system → network-interface**
   b. Enter **name → Public**
   c. Enter **ip-address → 1.1.1.2**
   d. Enter **netmask → 255.255.255.0**
   e. Enter **gateway → 1.1.1.1**
   f. Enter **exit**
   g. Enter **done**

5.3.3.2 Private Interface

1. Create a network-interface to the private (Avaya CPE) side of the Acme. Procedures are the same as for the public network-interface except:
   a. Enter **system → network-interface**
   b. Enter **name → Private**
   c. Enter **ip-address → 65.206.67.1**
   d. Enter **netmask → 255.255.255.0**
   e. Enter **gateway → 65.206.67.100**
   f. Enter **exit**
   g. Enter **done**

5.3.4 Physical Interfaces

This Section defines the physical interfaces to the private (Avaya CPE) and public (Verizon) networks.

5.3.4.1 Public Interface

1. Create a network-interface to the public (Internet/Verizon) side of the Acme.
   a. Enter **system → phy-interface**
   b. Enter **name → Public**
   c. Enter **operation-type → media**
   d. Enter **port → 0**
   e. Enter **slot → 0**
   f. **virtual-mac → 00:08:25:01:be:e8**

i. Virtual MAC addresses are assigned based on the MAC address assigned to the Acme. This MAC address is found by entering the command → *show prom-info mainboard* (e.g. **00 08 25 01 be e0**). To define a virtual MAC address, replace the last digit with **8** thru **f**.

g. Enter **duplex-mode → full**
h. Enter **speed → 100**
i. Enter **exit**
j. Enter **done**

5.3.4.2 Private Interface

1. Create a phy-interface to the private (Avaya CPE) side of the Acme. Procedures are the same as for the public phy-interface except:
   a. Enter **system → phy-interface**
   b. Enter **name → Private**
   c. Enter **port → 0**
   d. Enter **slot → 1**
   e. **virtual-mac → 00:08:25:01:be:ee**
   a. Enter **exit**
   b. Enter **done**

5.3.5 Realms

Realms are used as a basis for determining egress and ingress associations between physical and network interfaces as well as applying header manipulation such as NAT.

5.3.5.1 Outside Realm

1. Create a realm for the outside network.
   a. Enter **media-manager → realm-config**
   b. Enter **identifier → OUTSIDE**
   c. Enter **addr-prefix → 0.0.0.0**
   d. Enter **network-interfaces → Public:0**
   e. Enter **out-manipulationid → outManipOutside**
   f. Enter **mm-in-realm → enabled**
   g. Enter **mm-in-network → enabled**
   h. Enter **mm-same-ip → enabled**
   i. Enter **mm-in-system → enabled**
   j. Enter **access-control-trust-level → medium**
   k. Enter **invalid-signal-threshold → 1**
   l. Enter **maximum-signal-threshold → 1**
   m. Enter **untrusted-signal-threshold → 1**
   n. Enter **exit**
   o. Enter **done**

5.3.5.2 Inside Realm

1. Create a realm for the inside network. Procedures are the same as for the outside realm except:
   a. Enter **media-manager → realm-config**

b. Enter **identifier → INSIDE**
c. Enter **addr-prefix → 0.0.0.0**
d. Enter **network-interfaces → Private:0**
e. Enter **out-manipulationid → NAT_IP**
f. Enter **access-control-trust-level → high**
g. Enter **invalid-signal-threshold → 0**
h. Enter **maximum-signal-threshold → 0**
i. Enter **untrusted-signal-threshold → 0**
j. Enter **exit**
k. Enter **done**

5.3.6 Steering-Pools

Steering pools define sets of ports that are used for steering media flows thru the Acme.

5.3.6.1 Outside Steering-Pool

1. Create a steering-pool for the outside network.
   a. Enter **media-manager → steering-pool**
   b. Enter **ip-address → 1.1.1.2**
   c. Enter **start-port → 49152**
   d. Enter **end-port → 65535**
   e. Enter **realm-id → OUTSIDE**
   f. Enter **exit**
   g. Enter **done**

5.3.6.2 Inside Steering-Pool

1. Create a steering-pool for the inside network. Procedures are the same as for the outside steering-pool except:
   a. Enter **media-manager → steering-pool**
   b. Enter **ip-address → 65.206.67.1**
   c. Enter **start-port → 49152**
   d. Enter **end-port → 65535**
   e. Enter **realm-id → INSIDE**
   f. Enter **exit**
   g. Enter **done**

5.3.7 Session-Agents

A session-agent defines an internal "next hop" signaling entity for the SIP traffic. A realm is associated with a session-agent to identify sessions coming from or going to the session-agent. A session-agent id defined for the Verizon service node (outside) and the Avaya Aura™ Session Manager (inside).

5.3.7.1 Outside Session-Agent

Note – As mentioned previously 63.79.179.178 is the IP address of the Verizon service node (no FQDN) and port 5112 is the service node destination port.

1. Create a session-agent for the outside network.

a. Enter **session-router → session-agent**
b. Enter **hostname → 63.79.179.178**
c. Enter **ip-address → 63.79.179.178**
d. Enter **port → 5112**
e. Enter **state → enabled**
f. Enter **app-protocol → SIP**
g. Enter **transport-method → UDP**
h. Enter **realm-id → OUTSIDE**
i. Enter **description → To IPCC**
j. Enter **ping-method → Options;hops=0**
k. Enter **ping-interval → 60**
l. Enter **ping-send-mode → keep-alive**
m. Enter **exit**
n. Enter **done**

5.3.7.2 Inside Session-Agent

1. Create a session-agent for the inside network. Procedures are the same as for the outside session-agent except:
   a. Enter **session-router → session-agent**
   b. Enter **hostname → 65.206.67.2**
   c. Enter **ip-address → 65.206.67.2**
   d. Enter **port → 5060**
   e. Enter **transport-method → staticTCP**
   f. Enter **realm-id → INSIDE**
   g. Enter **description → To Session Manager**
   h. Enter **tcp-keepalive → enabled**
   i. Enter **tcp-reconn-interval → 10**
   a. Enter **exit**
   b. Enter **done**

5.3.8 Session Groups

Session-groups (SAG) define single or multiple destinations that are referenced in provisioning session-agents.

5.3.8.1 Verizon Session-group

1. Create a session-group for the Verizon network.
   a. Enter **session-router → session-group**
   b. Enter **groupname → SERV_PROVIDER**
   c. Enter **state → enabled**
   d. Enter **app-protocol → SIP**
   e. Enter **strategy → hunt**
   f. Enter **dest → 63.79.179.178**
   g. Enter **exit**
   h. Enter **done**

5.3.8.2 Avaya CPE Session-group

1. Create a session-group for the Avaya CPE network. Procedures are the same as for the Verizon session-group except:
   a. Enter **session-router → session-group**
   b. Enter **groupname → ENTERPRISE**
   c. Enter **dest → 65.206.67.2**
   c. Enter **exit**
   d. Enter **done**

5.3.9 SIP Configuration

This command sets the values for the Acme Packet SIP operating parameters. The home-realm defines the SIP daemon location, and the egress-realm is the realm that will be used to send a request if a realm is not specified elsewhere.

1. Enter **session-router → sip-config**
2. Enter **state → enabled**
3. Enter **operation-mode → dialog**
4. Enter **home-realm-id → INSIDE**
5. Enter **egress-realm-id → INSIDE**
6. Enter **exit**
7. Enter **done**

5.3.10 SIP Interfaces

The SIP interface defines the signaling interface (IP address and port) to which the Acme Packet sends and receives SIP messages.

5.3.10.1 Outside SIP- interface

1. Create a sip-interface for the outside network.
   a. Enter **session-router → sip-interface**
   b. Enter **state → enabled**
   c. Enter **realm-id → OUTSIDE**
   d. Enter **sip-port →**
      1. Enter **address → 1.1.1.2**
      2. Enter **port → 5060**
      3. Enter **transport-protocol → UDP**
   e. Enter **exit**
   f. Enter **exit**
   g. Enter **done**

5.3.10.2 Inside SIP- interface

1. Create a sip-interface for the inside network. Procedures are the same as for the outside sip-interface except:
   a. Enter **session-router → sip-interface**
   b. Enter **realm-id → INSIDE**
   c. Enter **sip-port →**

    1. Enter **address → 65.206.67.1**
    2. Enter **port → 5060**
    3. Enter **transport-protocol → TCP**

  d. Enter **exit**
  e. Enter **exit**
  f. Enter **done**

5.3.11 SIP Manipulation

SIP- manipulation specifies rules for manipulating the contents of specified SIP headers. In the reference configuration the following header manipulations are performed:

- NAT IP addresses in the From header of SIP requests.
- NAT IP addresses in the To header of SIP requests.
- NAT IP addresses in the Remote-Party-ID header of SIP requests.
- NAT IP addresses in the Alert-Info header of SIP requests. This is different from other rules because it will NAT CID (caller ID) URIs in addition to SIP URIs.
- Avaya CPE FQDN in Refer-To header

1. Enter **session-router → sip-manipulation**
2. Enter **name → NAT_IP**
3. Enter **description → Topology hiding SIP headers**
4. Enter **session-router → sip-manipulation → header-rule**
5. Proceed to the following sections

5.3.11.1 From Header

1. Enter **session-router → sip-manipulation → header-rule**
2. Enter **name → manipFrom**
3. Enter **action → manipulate**
4. Enter **comparison-type → case-sensitive**
5. Enter **msg-type → request**
6. Enter **element-rule →**
    a. Enter **name → FROM**
    b. Enter **type → uri-host**
    c. Enter **action → replace**
    d. Enter **match-val-type → ip**
    e. Enter **comparison-type → uri-host**
    f. Enter **new-value → $LOCAL_IP**
7. Enter **exit**
8. Enter **done**

5.3.11.2 To Header

1. Enter **session-router → sip-manipulation → header-rule**
2. Enter **name → manipTo**
3. Enter **action → manipulate**
4. Enter **comparison-type → case-sensitive**

5. Enter **msg-type → request**
6. Enter **element-rule →**
    a. Enter **name → TO**
    b. Enter **type → uri-host**
    c. Enter **action → replace**
    d. Enter **match-val-type → ip**
    e. Enter **comparison-type → case-sensitive**
    f. Enter **new-value → $REMOTE_IP**
7. Enter **exit**
8. Enter **done**

5.3.11.3 Remote Party ID Header

1. Enter **session-router → sip-manipulation → header-rule**
2. Enter **name → manipRpid**
3. Enter **header-name → Remote-Party-ID**
4. Enter **action → manipulate**
5. Enter **comparison-type → case-sensitive**
6. Enter **msg-type → request**
7. Enter **element-rule →**
    a. Enter **name → RPID**
    b. Enter **type → uri-host**
    c. Enter **action → replace**
    d. Enter **match-val-type → ip**
    e. Enter **comparison-type → case-sensitive**
    f. Enter **new-value → $LOCAL_IP**
8. Enter **exit**
9. Enter **done**

5.3.11.4 Alert-info Header

1. Enter **session-router → sip-manipulation → header-rule**
2. Enter **name → storeAlertInfo**
3. Enter **header-name → Alert-Info**
4. Enter **action → store**
5. Enter **comparison-type → pattern-rule**
6. Enter **match-value → (.+@) ([0-9.]+) (.+)**
7. Enter **msg-type → request**
8. Enter **exit**
9. Enter **header-rule**
10. Enter **name → manipAlertInfo**
11. Enter **header-name → Alert-Info**
12. Enter **action → manipulate**
13. Enter **comparison-type → boolean**
14. Enter **match-value → $storeAlertInfo**
15. Enter **msg-type → request**
16. Enter **new-value → $storeAlertInfo.$1+$REMOTE_IP+$storeAlertInfo.$3**
17. Enter **exit**

18. Enter **done**

5.3.11.5 Refer Header

1. Enter **session-router → sip-manipulation →**
2. Enter **name → outManipOutside**
3. Enter description→ IPTF-Refer
4. **Enter → header-rule**
5. Enter **name → NatIp**
6. Enter **header-name → To**
7. Enter **action → sip-manip**
8. Enter **comparison-type → case-sensitive**
9. Enter **msg-type → request**
10. **Enter new-value → NAT_IP**
11. Enter **exit**
12. Enter **header-rule**
13. Enter **name → manipReferTo**
14. Enter **header-name → Refer-To**
15. Enter **action → manipulate**
16. Enter **comparison-type → case-sensitive**
17. Enter **msg-type → request**
18. Enter **methods → REFER**
19. **Enter → element-rule**
20. **Enter name → REFERTO**
21. **Enter type → uri-host**
22. **Enter action → replace**
23. **Enter match-val-type → ip**
24. **Enter comparison-type → case-sensitive**
25. **Enter new-value → loc1.interoplab3.21sip.com**
26. Enter **exit**
27. Enter **done**

5.3.12 Other Acme Packet provisioning

5.3.12.1 Access-control

This is a static Access Control List that is used to limit SIP access to only known devices.

1. Enter **session-router → access-control**
2. Enter **realm-id → OUTSIDE**
3. Enter **source-address → 63.79.179.178:5112**
4. **Enter destination address → 0.0.0.0**
5. Enter **application-protocol → SIP**
6. Enter **transport-protocol → UDP**
7. Enter **access → permit**
8. Enter **exit**
9. Enter **done**

5.3.12.2 Media-Manager

Verify that the media-manager process is enabled.

1. Enter **media-manager** → **media-manager**
2. Enter **select** → **show** → Verify that the media-manager state is enabled. If not, enter:
3. Enter **state** → **enabled**
4. Enter **exit**
5. Enter **done**

5.3.12.3 System-config

In the system-config, specify a hostname and the default gateway of the management interface.

1. Enter **system** → **system-config**
2. Enter **hostname** → **acmesbc**
3. Enter **default-gateway** → **172.16.253.4**
4. Enter **exit**
5. Enter **done**

6. Verizon Business IPCC Services suite Offer Configuration

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

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

6.1. Service access information

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

CPE (Avaya)	Verizon Network
loc1.interoplab3.21sip.com port 5060	***63.79.179.178 Port 5112***

Toll Free Numbers
866-797-8011
866-797-3994
866-797-5598

7. Verification Steps

This Section provides the verification steps that may be performed to verify basic operation of the Avaya Aura™ SIP trunk solution with Verizon Business IPCC service.

7.1. Verify Avaya Aura™ Communication Manager 5.2

Verify the status of the SIP trunk group by using the "status trunk n" command, where "n" is the trunk group numbers administered in **Section 3.1.5**. Verify that all trunks are in the "in-service/idle" state as shown below.

```
status trunk 2
                             TRUNK GROUP STATUS
Member   Port     Service State      Mtce Connected Ports
                                     Busy
0002/001 T00011   in-service/idle    no
0002/002 T00012   in-service/idle    no
0002/003 T00013   in-service/idle    no
0002/004 T00014   in-service/idle    no
0002/005 T00015   in-service/idle    no
0002/006 T00016   in-service/idle    no
0002/007 T00017   in-service/idle    no
0002/008 T00018   in-service/idle    no
0002/009 T00019   in-service/idle    no
0002/010 T00020   in-service/idle    no
```

Figure 50: Status Trunk

Verify the status of the SIP signaling groups by using the "status signaling-group n" command, where "n" is the signaling group number administered in **Section 3.1.5**. Verify the signaling group is "in-service" as indicated in the **Group State** field shown below.

```
status signaling-group 2
                         STATUS SIGNALING GROUP
        Group ID: 2                              Active NCA-TSC Count: 0
      Group Type: sip                              Active CA-TSC Count: 0
  Signaling Type: facility associated signaling
     Group State: in-service
```

Figure 51: Status Signaling Group

Make a call between an Avaya Aura™ Communication Manager H.323 station and PSTN. Verify the status of connected SIP trunk by using the "***status trunk x/y***"command, where "x" is the number of the outbound SIP trunk group, and "y" is the active member number of a connected trunk. Verify on Page 1 that the **Service State** is "**in-service/active**". On Page 2, verify that the IP addresses of the C-LAN and Avaya Aura™ Session Manager are shown in the **Signaling** section. In addition, the **Audio** section shows the G.729 codec and the IP address of the Avaya H.323 endpoint and the Acme Packet SBC. The **Audio Connection Type** displays "**ip-direct**", indicating direct media between the two endpoints.

```
 status trunk 2/2                                              Page   1 of   3
                                TRUNK STATUS
  Trunk Group/Member: 0002/002            Service State: in-service/active
                Port: T00012            Maintenance Busy? no
  Signaling Group ID: 2
    IGAR Connection? no
     Connected Ports: S00001
```

Figure 52: Status Trunk – Active Call – Page 1

```
status trunk 2/2                                                Page   2 of   3
                                CALL CONTROL SIGNALING
Near-end Signaling Loc: 01A0217
  Signaling    IP Address                           Port
   Near-end:   65.206.67.7                        : 5060
    Far-end:   65.206.67.2                        : 5060
 H.245 Near:
  H.245 Far:
   H.245 Signaling Loc:          H.245 Tunneled in Q.931? no
 Audio Connection Type: ip-direct     Authentication Type: None
    Near-end Audio Loc:                        Codec Type: G.729
   Audio       IP Address                           Port
   Near-end:   65.206.67.12                       : 2776
    Far-end:   65.206.67.1                        : 49428
 Video Near:
  Video Far:
 Video Port:
  Video Near-end Codec:                 Video Far-end Codec:
```

Figure 53: Status Trunk – Active Call – Page 2

7.2. Verify Avaya Aura™ Session Manager

Monitoring of Avaya Aura™ Session Manager is performed via Avaya Aura™ System Manager.

7.2.1 Verify SIP Entity Link Status

Expand the **Session Manager** menu and click SIP Monitoring. Verify that none of the links to the defined SIP entities are down (as indicated by **0/2** in **Figure 54**), indicating that they are all reachable for call routing.

Figure 54: SIP Entity Link Monitoring - Summary

Selecting a monitored SIP Entity from the list will display its status (e.g. **S8720_Clan1_voice**).

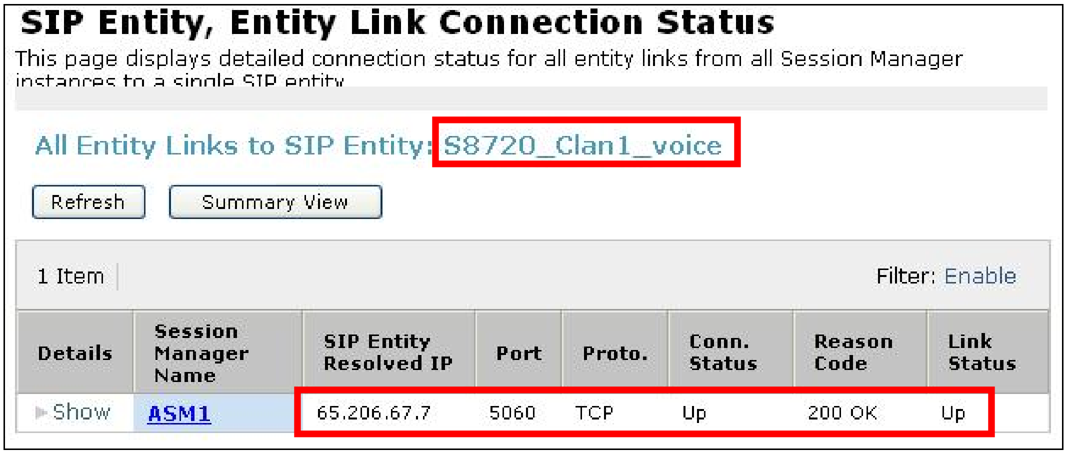

Figure 55: SIP Entity Link Connection Status

7.2.2 Verify System State

Expand the **Session Manager** menu and click **System State Administration**. Verify that the Management State is Management Enabled and the Service State is Accept New Service.

Figure 56: System State

7.2.3 Call Routing Test

The Call Routing Test verifies that the call routing/dial pattern for a particular source and destination is correctly provisioned. In this example a call from Avaya Aura™ Communication Manager station 30001 to PSTN number 7328521642 is provisioned correctly.

Note - Since the DigitConversionAdapter is provisioned for the Avaya Aura™ Communication Manager Clan SIP Entity (e.g. S8720_Clan1_voice), station 30001 will be converted to its Verizon toll free number (8667978011) prior to the routing policies being applied, therefore the toll free number associated with the extension must be specified as the calling number in the test.

Expand the Session Manager menu and click **Call Routing Test**. Populate the fields as follows:

- **Called party URI – 7328521642@adevc.avaya.globalipcom.com** → This is the request URI sent by Avaya Aura™ Communication Manager to Avaya Aura™ Session Manager.
- **Calling Party URI – 8667978011@adevc.avaya.globalipcom.com** → This is the contents of the Avaya Aura™ Communication Manager From header.
- **Calling Party Address – 65.206.67.7** → This is the source IP address of the call (Avaya Aura™ Communication Manager Clan).
- **Session Manager Listening Port – 5060** → This is the port provisioned for Session Manager.
- **Day of the week** – Since no time restrictions were defined for the reference configuration (see **Section 4.3.6**) any day value may be selected.
- **Time** – Since no time restrictions were defined for the reference configuration (see **Section 4.3.6**) any time value may be selected.
- **Transport Protocol** – Select the transport protocol used (e.g., **TCP**).
- **Called Session Manager Instance** – Select the Session Manager used for the call. In the reference configuration only one Session Manager is defined (**ASM1**).

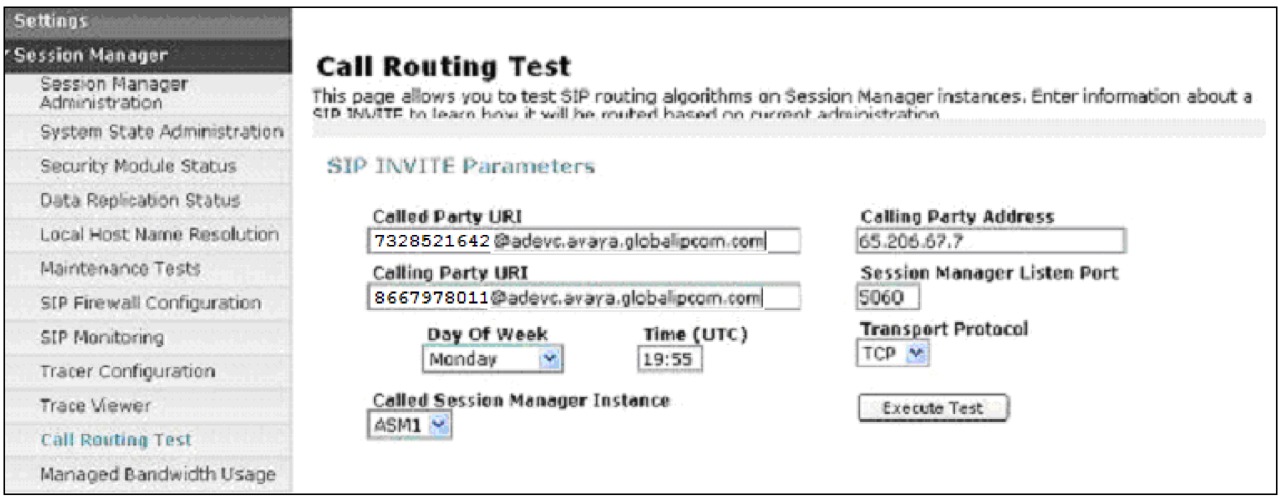

Figure 57: Call Routing Test

Then click on the **Execute Test** button. Avaya Aura™ System Manager will check the routing algorithms and report on the success or failure of the provisioning.

The results of the test are then displayed. At the top of the list, the heading **Routing Decisions** shows the final result. In the example, the call will be sent to Acme1. The next heading Routing Decision Process shows all the routing algorithm calculations.

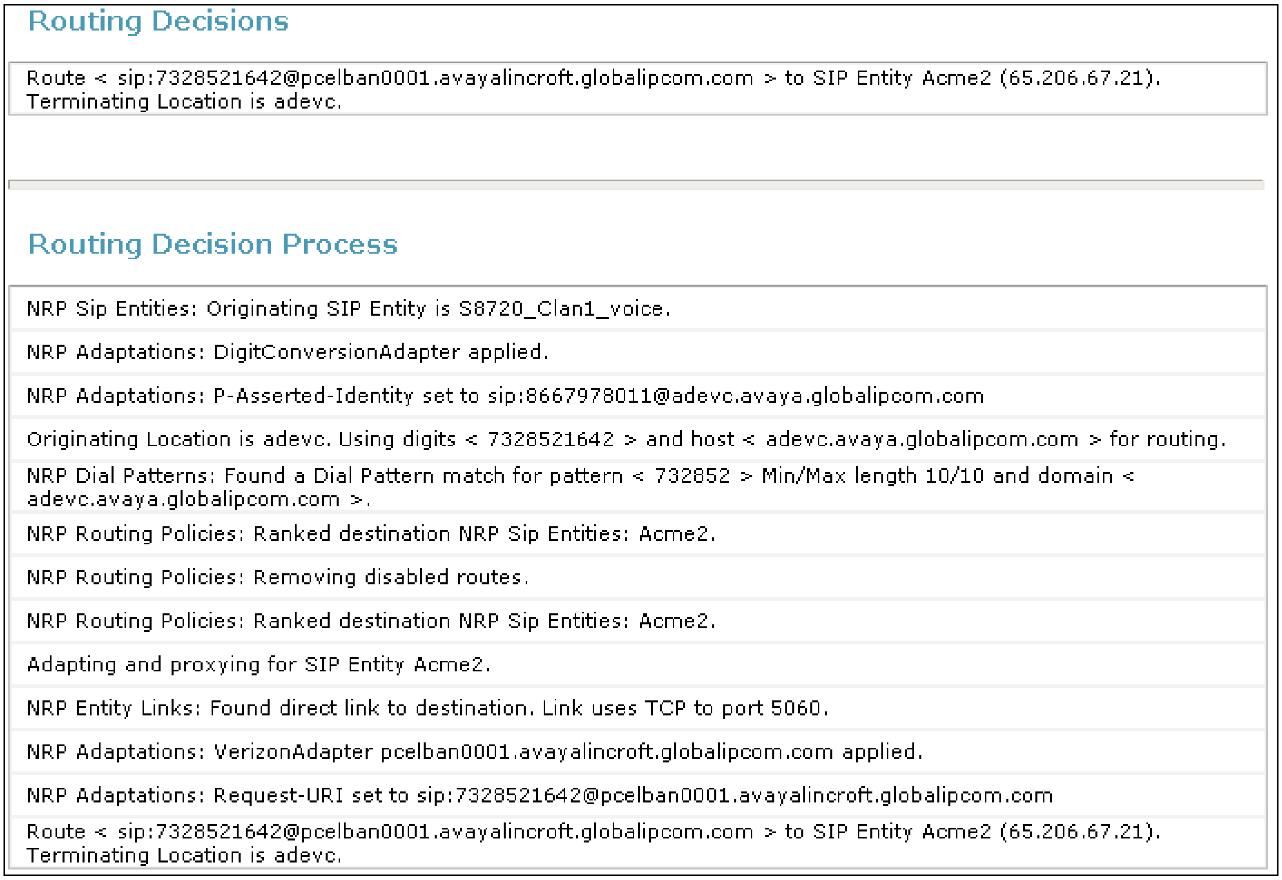

Figure 58: Call Routing Test - Results

7.3. Verification Call Scenarios

Verification scenarios for the configuration described in these Application Notes included:

- Inbound and outbound voice calls between PSTN and Avaya SIP trunking CPE via the Verizon Business IPCC Services suite.
- Call redirection via Refer or Refer with Replaces SIP signaling.
- Direct IP-to-IP Media (also known as “Shuffling”) when applicable.
- DTMF Tone Support.

7.4. Conclusion

As illustrated in these Application Notes, Avaya Aura™ Session Manager, Avaya Aura™ Communication Manager, and the Acme Packet Net-Net Session Director can be configured to interoperate successfully with Verizon Business's IP Contact Center services suite inclusive of VoIP Inbound, IP Contact Center, IP-IVR SIP trunk services. This solution provides users of Avaya Aura™ Communication Manager the ability to support inbound toll free calls over a Verizon Business VoIP Inbound SIP trunk service connection. In addition, these application notes further demonstrate that the Avaya Aura™ Communication Manager's implementation of SIP Network Call Redirection (SIP-NCR), can work in compliment with Verizon's Business's IP Contact Center and IP-IVR services implementation of SIP-NCR to support call redirection over SIP trunks. This capability includes support of outbound calls for the specific call redirection scenarios documented in this application note.

Please note that the sample configurations shown in these application notes are representative of a basic enterprise customer configuration and as such are intended to provide configuration guidance to supplement other Avaya product documentation. Finally, the test results indicated in these application notes are based upon formal interoperability compliance testing that was conducted as part of the Avaya DevConnect Service Provider program. As part of this program, compliance testing of this solution was conducted with the full support and collaboration with Verizon's CPE Systems Interoperability Test Lab.

8. Addendum – Alternate method for defining Avaya Aura™ Session Manager Locations for Call Routing

In **Section 4.3.3** the provisioning of Avaya Aura™ Session Manager Locations is discussed. Locations are used by Avaya Aura™ Session Manager as part of the call routing algorithm to determine the source of a call. These Locations, plus other criteria such as digit strings and Routing Policies, are used to determine the destination for the call. In **Section 4.3.3** the entire CPE private IP subnet was defined as a “general” Location from which Avaya Aura™ Session Manager would receive SIP calls. In this section the method of using a general Location is compared with an alternate method called “Source Based Routing”. While either method is acceptable, variations in calling requirements may determine the best method to use.

8.1. General Location

As shown in **Figure 1**, Avaya Aura™ Session Manager would receive outbound calls from Avaya Aura™ Communication Manager and receive inbound calls from either Acme1 or Acme2. In the reference configuration, Avaya Aura™ Communication Manager, Avaya Aura™ Session Manager, Acme1, and Acme2 are all part of the 65.206.67.x subnet. In addition, specific dial patterns (digits) were identified as being either for “inbound” (e.g. 866xxxxxxx) or “outbound” (e.g. 800xxxxxxx) dialing. Since the dialing patterns were clearly defined, only a single general Location was provisioned (called *adevc* in the reference configuration) that specified to Avaya Aura™ Session Manager that all calls it received would come from 65.206.67.x. Therefore only scrutiny of the called digits would be needed for Avaya Aura™ Session Manager to determine whether to send the call inbound to Avaya Aura™ Communication Manager (the call came from one of the Acmes), or to send the call outbound to one of the Acmes (the call came from Avaya Aura™ Communication Manager).

This method works well as long as the dialing patterns are clearly defined as being either inbound or outbound. However there may be cases where overlapping dial patterns may be used for inbound and outbound calls. In these cases Avaya Aura™ Session Manager needs clearer criteria for how to route the calls. This can be accomplished by using Source Based Routing and individual Locations.

8.2. Source Based Routing

As the name implies, with Sourced Based Routing Avaya Aura™ Session Manager uses Locations (sources) to determine how to route a call. In this example calls for 866xxxxxxx are normally sent inbound from Verizon to the CPE (Avaya Aura™ Communication Manager). However the customer wants to be able to transfer calls back out to the Verizon network also using numbers that fall into the 866xxxxxxx pattern. In the configuration described in **Section 8.1**, this would result in a routing loop since Avaya Aura™ Session Manager had been provisioned that if a call for 866xxxxxxx comes from any device in the subnet 65.206.67.x (Location *adevc*), send the call to Avaya Aura™ Communication Manager. The solution is to use Source Based Routing.

In the reference configuration the Avaya Aura™ Communication Manager Clan board has the IP address 65.207.67.7, Acme1 has the IP address 65.206.67.1 and Acme2 has the IP address

65.206.67.21. Using the procedures described in **Section 4.3.3**, an individual Location is defined for each. Then when the dial pattern is defined for 866xxxxxxx (see **Section 4.3.8**), these three Locations are also defined in the following manner:

Digit String	Originating Location	Routing Policy
866xxxxxxx	Clan	*Outbound*
866xxxxxxx	Acme1	*Inbound*

Table 8

- If 866xxxxxxx is sent by Location "Clan", route the call outbound using the Routing Policy *Outbound* (Acme1).
- If 866xxxxxxx is sent by Location "Acme1", route the call inbound using the Routing Policy *Inbound* (the Clan).

Note - The Routing Policies described in **Section 4.3.7** are used in this example.

8.2.1 New Locations

Three Locations need to be added: Clan (65.206.67.7), Acme1 (65.206.67.1), and Acme2 (65.206.67.21). To add a Location, select **Locations** in the left **Network Routing Policy** menu and click on the **New** button on the right.

1. Enter "Clan" in the **Name** field.
2. Enter a description in the **Notes** field if desired.
3. Under the **Location Pattern** heading, click on **Add**.
4. Enter IP address **65.206.67.7**
5. Enter a description in the **Notes** field if desired.
6. Modify the remaining values on the form if necessary; otherwise use all the default values.
7. Click on the **Commit** button. The completed form will look like **Figure 59**.

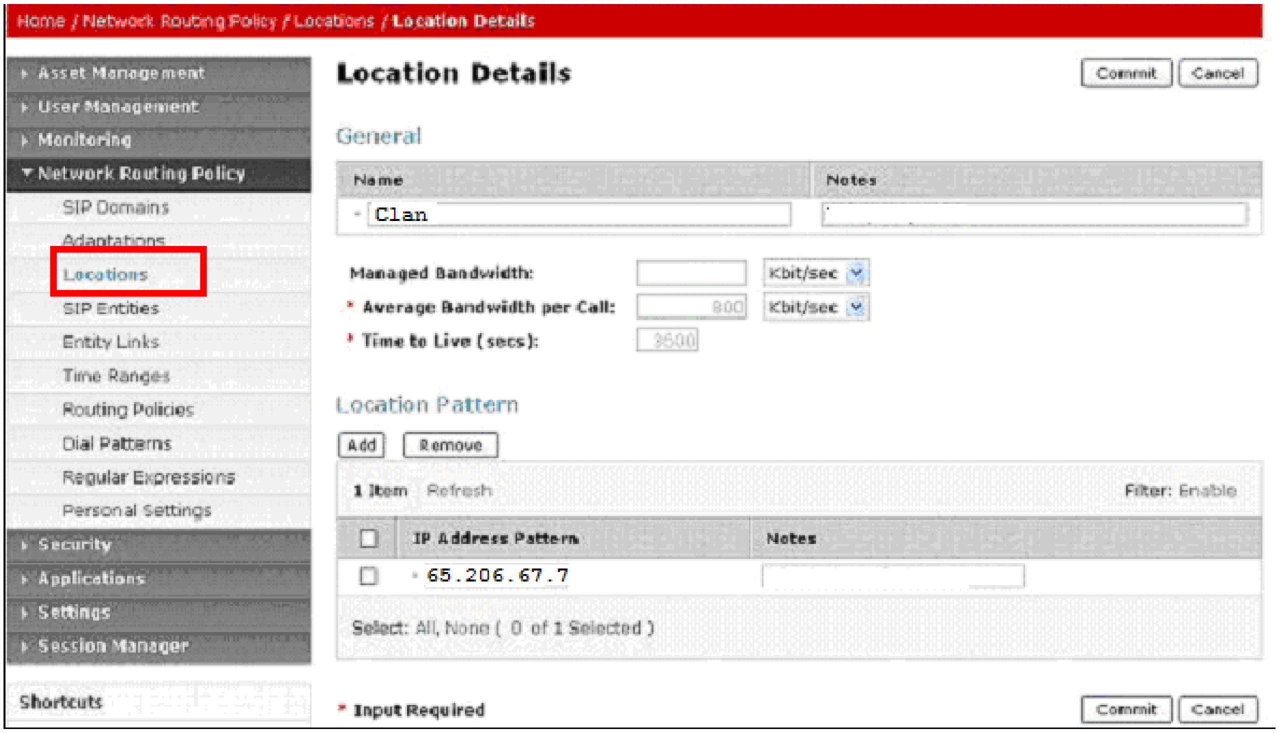

Figure 59: Adding Location "Clan"

8. Repeat steps 3 thru 7 to add Location **Acme1**.

The completed Location form will look like **Figure 60**.

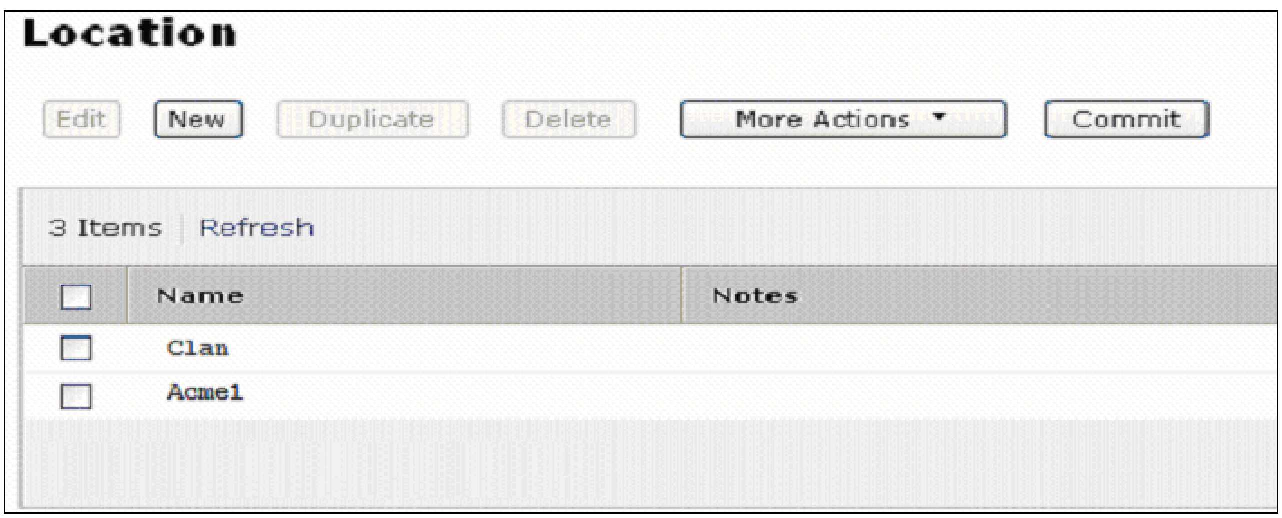

Figure 60: Completed Location Form

Once the three new Locations are defined, the dial pattern 866xxxxxxx must be provisioned.

8.2.2 Dial Pattern 866xxxxxxx

The Dial pattern 866xxxxxxx must now be associated with the source Locations defined in **Section 8.2.1**. Select **Dial Patterns** on the left **Network Routing Policy** menu and click on the **New** button on the right. The screen shown in **Figure 61** is displayed. In this example a Request URI to a 10 digit number beginning with *866xxxxxxx*, and sent by *adevc.avaya.globalipcom.com* (the Avaya CPE FQDN, see **Section 1.2**), are defined.

1. **General** section
   a. Enter 866xxxxxx in the **Pattern** field.
   b. In the **Min** column enter **10**.
   c. In the **Max** column enter **10**.
   d. In the **SIP Domain** field drop down menu select the Avaya CPE FQDN.
   e. Enter a description in the **Notes** field if desired.

Figure 61: Dial Pattern Details - General

2. **Originating Locations and Routing Policies** Section
   a. Click on the Add button and the window in **Figure 62** will open. All the provisioned Locations and Routing Policies will be listed.
   b. Click on the box for the Originating Location **Clan** (see **Section 8.2.1**).
   c. Select Routing Policies **Oubound1** (Acme1) and **Outbound2** (Acme2) (see **Table 8** and **Section 4.3.7**).

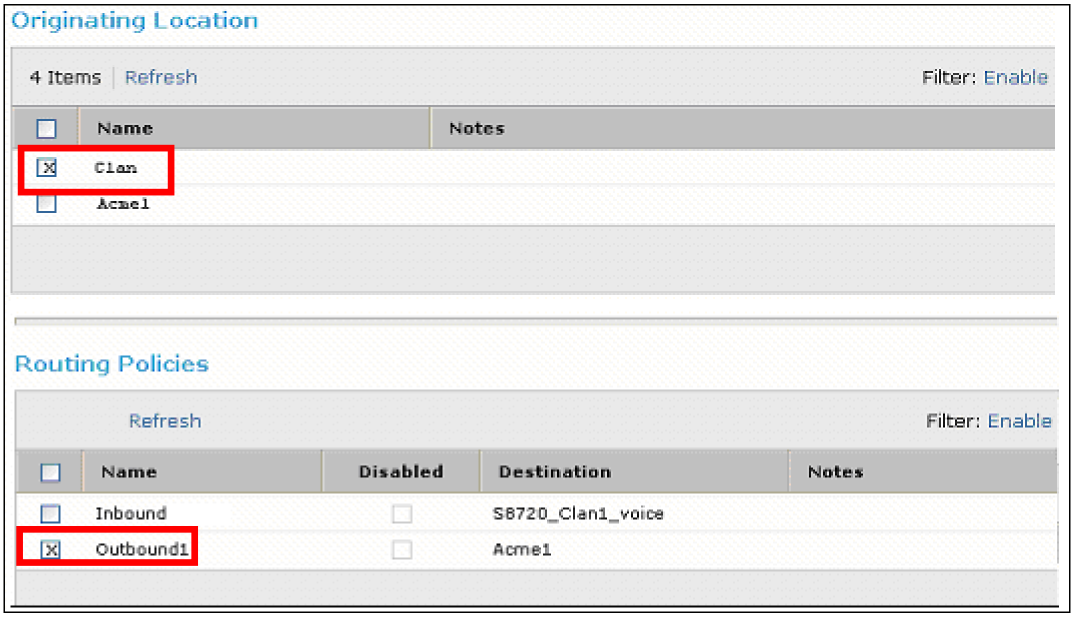

Figure 62: Dial Pattern Details – Originating Locations and Routing Policies

d. Click on the **Select** button and repeat **steps a** thru **c** specifying **Acme1** as the Originating Location and Routing Policy **Inbound**.

5. Click the **Commit** button
6. The completed Dial Pattern screen will look like **Figure 63**.

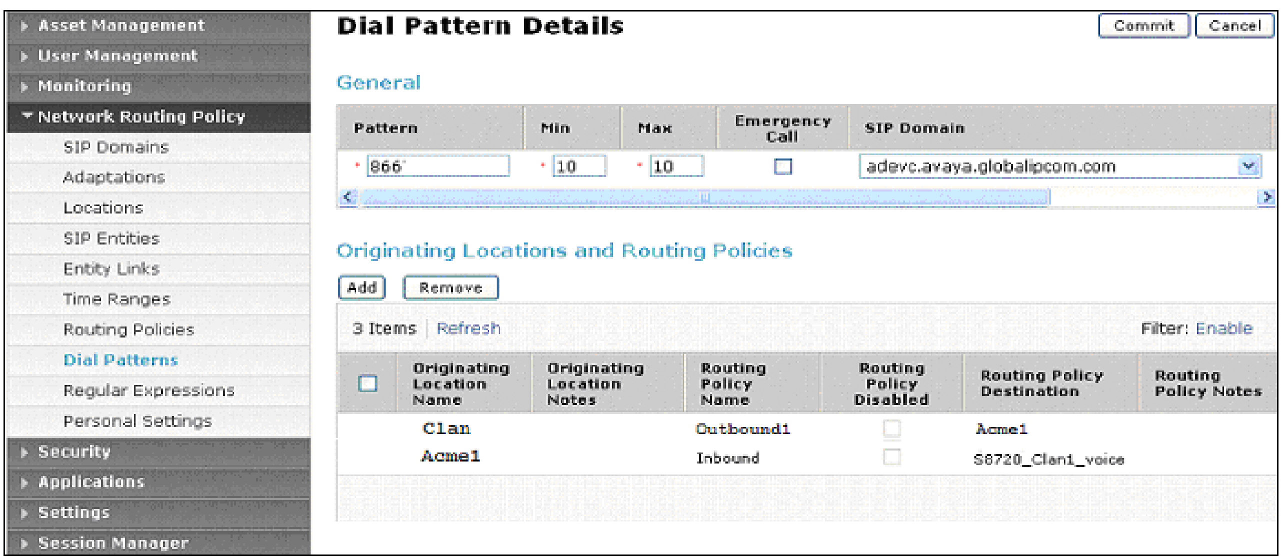

Figure 63: Completed Dial Pattern Form

The Source Based Routing for dial string 866xxxxxxx is completed.

8.3. Routing Conflicts

Routing conflicts may occur if specific Locations (Source Based Routing) and general Locations are used together and their IP addressing overlaps. As described in **Section 8.1**, the general Location *adevc* was defined with the IP subnet 65.206.67.x. The Source Based Routing Locations described in **Section 8.2** (*Clan, Acme1,* and *Acme2*) are part of that subnet. The Avaya Aura™ Session Manager routing algorithm will always match on a Location with a specific IP address (e.g. 65.206.67.1) over a Location with a "wild card" address (65.206.67.x). Therefore if a call comes from an IP address that matches a Location with a specific address, and that Location does not have an associated Dial Pattern defined, the call will be denied even though a general Location may have a matching Dial Pattern.

For example:

- Given:
    - Location Acme1 (65.206.67.1) is provisioned
    - Location adevc (65.206.67.x) is provisioned.
    - Dial Pattern 5551212 is associated with Location adevc

- Acme 1 (65.206.67.1) sends a call to Avaya Aura™ Session Manager for 5551212
- Avaya Aura™ Session Manager matches Dial Pattern 5551212 but it is associated with Location adevc (65.206.67.x), not Location Acme1 (65.206.67.1).
- Avaya Aura™ Session Manager will deny the call.

Therefore care must be taken that IP address overlap does not occur if both general Locations and specific Locations are provisioned.

9. Support

9.1. Avaya

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

9.2. Verizon

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

10. References

10.1. Avaya

The following Avaya product documentation is available at http://support.avaya.com.

[1] *SIP Support in Avaya Aura™ Communication Manager Running on Avaya S8xxx Servers*, Doc ID 555-245-206, May, 2009.
[2] *Administering Avaya Aura™ Communication Manager*, Doc ID 03-300509, May 2009.
[3] *Installing and Administering Avaya Aura™ Session Manager, 03-603324, Issue 1.1, Release 1.1, June 2009*
[4] *Installing and Administering Avaya Aura™ Session Manager, Doc ID 03-603324.*
[5] *Maintaining and Troubleshooting Avaya Aura™ Session Manager, Doc ID 03-603325.*
[6] *Feature Description and Implementation for Avaya Communication Manager, 555-245-205, Issue 6, January 2008*
[7] *Application Notes for Avaya Aura™ Communication Manager 5.2, Avaya Aura™ Session Manager 1.1,and Acme Packet 3800 Net-Net Session Director integration with Verizon Business IP Trunk SIP trunk service offer – Issue 1.0*

10.2. Verizon Business

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

[8] *Verizon Business Retail VoIP Network Interface Specification (for non-registering devices) Document, Version:3.3, 2009-05-1*
[9] *Retail VoIP Interoperability Test Plan version 1.9.1, Date:2009-01-05*
[10] *Additional information regarding Verizon Business IPCC Services suite offer can be found at http://www.verizonbusiness.com/us/products/voip/trunking/*

10.3. Acme Packet

The following Acme Packet product documentation is available at: https://support.acmepacket.com/

[11] *Net-Net® 4000, ACLI Reference Guide, Release Version S-C6.1.0*
[12] *Net-Net® 4000 ACLI, Configuration Guide, Release Version S-C6.1.0*

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.