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 Trunk SIP trunk service offer – Issue 1.3

Abstract

These Application Notes describe the steps to configure the Avaya Aura™ SIP trunk solution with Verizon Business Private IP (PIP) IP Trunk service. The Avaya SIP trunk architecture consists of Avaya Aura™ Communication Manager (version 5.2), and Avaya Aura™ Session Manager (version 1.1). In addition, the Verizon Business SIP trunk redundant architecture (2-CPE) is supported by dual Acme Packet 3800 Net-Net Session Directors.

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

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

Table of Contents

1. Introduction

These Application Notes describe the steps to configure the Avaya SIP trunk solution with the Verizon Business Private IP (PIP) IP Trunk service offer in a SIP Trunk redundant (2-CPE) environment. The Verizon Business SIP Trunk redundant (2-CPE) architecture provides for redundant SIP trunk access between the Verizon Business IP Trunk service offer and the Avaya SIP trunk architecture customer premises equipment (CPE). 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.

Dual Acme Packet 3800 Net-Net Session Directors are used as edge devices between the Avaya CPE and the Verizon Business network and provide for Verizon Business 2-CPE redundancy. In addition the Acme Packet SBCs provide Network Address Translation (NAT) functionality to convert the private Avaya CPE IP addressing to public addressing.

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

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

The Verizon Business IP Trunk service offer described in these Application Notes is designed for business customers using Avaya Aura™ Communication Manager and Avaya Aura™ Session Manager. The service provides local and/or long-distance calls (with PSTN endpoints) via standards-based SIP trunks.

Voice and fax calls have dedicated Inbound and outbound SIP trunks provisioned on Avaya Aura™ Communication Manager. This allows specific voice and fax parameters to be provisioned (e.g. codec selection).

For more information on Verizon Business IP Trunk service interoperability with the Avaya SIP trunking, see [**6**].

1.1. The SIP Trunk Redundant (2-CPE) Architecture Option

Verizon Business and Avaya developed the SIP Trunk Redundant (2-CPE) architecture to ensure that SIP trunk calls can be automatically rerouted to bypass SIP trunk failures due to network or component outages. The 2-CPE architecture described in these Application Notes is based on a customer location having two Acme Packet 3800 Net-Net Session Directors. One Acme Packet 3800 is designated as Primary and one as Secondary. The Acme Packet 3800s reside at the edge of the customer network.

Avaya Aura™ Session Manager is provisioned to attempt outbound calls to the Primary Acme Packet 3800 first. If that attempt fails, the Secondary Acme Packet 3800 is used. Similarly, the Verizon Business Private IP Trunk service node will send inbound calls to the Primary Acme Packet 3800. If there is no response then the call will be sent to the Secondary Acme Packet 3800.

1.2. Reference Configuration

Figure 1 illustrates the 2-CPE reference configuration used for the DevConnect compliance testing. The reference configuration is comprised of the Avaya CPE location connected via a T1 Internet connection to the Verizon Business IP trunking service. The Avaya CPE location simulates a customer site and uses private IP addressing. At the edge of the Avaya CPE location, Acme Packet SBCs provide NAT functionality that converts the private IP addressing to public addressing that is passed to Verizon Business. 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 service node.

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

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

- Verizon Business IP Trunk network Fully Qualified Domain Name (FQDN)
  - *pcelban0001.avayalincroft.globalipcom.com*
- Avaya CPE Fully Qualified Domain Name (FQDN)
  - *adevc.avaya.globalipcom.com*
- Primary and Secondary Acme Packet 3800 SBCs.
- Avaya Aura™ Communication Manager.
  - Separate SIP trunks for Inbound Voice and Fax traffic.
    - Voice
      - Voice Signaling Group defined with <blank> Far-end Domain field.
      - Voice Signaling Group defined with Near-end port 5060.
      - Voice trunk assigned Facility Restriction Level (FRL) 2
      - 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
    - Fax
      - Fax Signaling Group defined with <blank> Far-end Domain field.
      - Fax Signaling Group defined with Near-end port 5062.
      - Fax trunk assigned FRL 1
      - Fax components assigned to IP-Network-Region 3
      - IP-Network-Region 3 specifies Avaya CPE FQDN and IP-Codec 3
      - IP-Codec 3 specifies G.711Mu
  - Separate SIP trunks for Outbound Voice and Fax traffic.
    - Voice

        - Voice Signaling Group defined with Far-end Domain field specifying either the Avaya CPE FQDN or the Verizon Business IP Trunk service FQDN (See **Section 1.2.4**).
        - Voice Signaling Group defined with Near-end port 5060.
        - Voice trunk assigned FRL 2
        - 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
    - Fax
        - Fax Signaling Group defined with Far-end Domain field specifying either the Avaya CPE FQDN or the Verizon Business IP Trunk service FQDN (See **Section 1.2.4**).
        - Fax Signaling Group defined with Near-end port 5060.
        - Fax trunk assigned FRL 1
        - IP-Network-Region 3 specifies Avaya CPE FQDN and IP-Codec 3
        - IP-Codec 3 specifies G.711Mu
  - Voice stations assigned a Class of Restriction (COR) with an FRL of 2.
  - Fax stations assigned a Class of Restriction (COR) with an FRL of 1.
- 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**)
  - Conversion of any SIP History Info Headers sent Avaya Aura™ Communication Manager to SIP Diversion Headers (see **Section 4.3.2**).
  - For outbound calls, convert the local Avaya CPE FQDN sent by Avaya Aura™ Communication Manager in the request URI to the Verizon Business IP Trunk service FQDN (see **Section 4.3.2**).
- 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
- Avaya One-X Communicator (H.323 running on a Windows laptop).

1.2.1 Voice and Fax calls

Inbound and outbound voice and fax calls must be differentiated by Avaya Aura™ Communication Manager so that different codecs can be specified for these call types, (G.729A/G.711Mu for voice and G.711Mu only for Fax).

1.2.1.1 Inbound Calls to Avaya Aura™ Communication Manager

In order to differentiate between inbound voice and fax calls, Avaya Aura™ Communication Manager will listen on different ports for these calls. The voice Signaling Group Near-End port specifies port 5060. The fax Signaling Group specifies port 5062 (see **Section 3.1.5**). These Signaling Groups are provisioned to different ip-network-regions (2 for voice and 3 for fax) that specify the appropriate ip-codecs (see **Section 3.1.4**). Avaya Aura™ Session Manager has "Entity

Links” defined for voice and fax calls that specify these ports before sending the call on to Avaya Aura™ Communication Manager (see **Section 4.3.5**). This means that specific fax Avaya Aura™ Communication Manager station extensions must be provisioned in the Avaya Aura™ Session Manager “Dial Patterns” (see **Section 4.3.8**) for these inbound calls

1.2.1.2 Outbound Calls from Avaya Aura™ Communication Manager

Outbound and outbound voice and fax calls are differentiated by Avaya Aura™ Communication Manager based on Automatic Route Selection (ARS) of the called number (see **Section 3.1.7**). This requires that specific fax destination endpoint numbers be specified in the ARS table. The ARS table selects different ip-route-patterns based on the called number and the ip-route-patterns will direct the outbound call to the appropriate voice or fax outbound trunk. The Signaling Group associated with the voice or fax trunk will specify an ip-network-region (2 for voice and 3 for fax). These ip-network-regions will determine the ip-codec used (see **Section 3.1.3**).

1.2.2 Dialing Examples

The following are examples of outbound and inbound voice and fax calls.

Given:

- Voice station 30001
- Fax station 30004
- Voice Inbound SIP trunk 4
- Voice Outbound SIP trunk 2
- Fax Inbound SIP trunk 5
- Fax Outbound SIP trunk 3

Inbound

- Voice
  - PSTN dials Verizon Business IP Trunk service DID number and the Verizon Business IP Trunk service sends the call to the Acme Packet SBC.
  - The Acme Packet passes the call to Avaya Aura™ Session Manager. Avaya Aura™ Session Manager performs digit conversion, changes the 10 digit DID number to the associated Avaya Aura™ Communication Manager extension (30001), 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.
- Fax
  - Inbound fax calls are processed the same way except Avaya Aura™ Session Manager converts a DID to extension 30004 to port 5062.
  - The call arrives on inbound fax trunk 5 on port 5062 and connects to fax station 30004 using G711Mu codec.
  - All inbound Avaya Aura™ Communication Manager Signaling groups use a <blank> Far-end domain to accept calls from all foreign domains.

Outbound

- Voice
  - Voice stations are set to COR 1 which has the higher FRL priority 2 set.

    - 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 the following:
        - Voice outbound trunk 2
        - FRL 2
    - The voice calls 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.
        - Either the Avaya CPE FQDN
            - *adevc.avaya.globalipcom.com*
        - Or the Verizon Business IP Trunk network FQDN (based on the provisioning described in **Section 1.2.4**)
            - *pcelban0001.avayalincroft.globalipcom.com*
    - Avaya Aura™ Session Manager sends the call to the Acme.
    - The Acme Packet sends the call to the Verizon Business IP Trunk network service node.
- Fax
    - Fax stations are set to COR 2 which has the lower FRL priority 1 set.
    - Avaya Aura™ Communication Manager fax stations dial 9 and a 10 digit number.
    - ARS sends the call to Route Pattern 3. Route Pattern 3 specifies the following:
        - Voice outbound trunk 3
        - FRL 1
    - The fax calls will select trunk 3 and Avaya Aura™ Communication Manager Clan sends the call to Avaya Aura™ Session Manager specifying:
        - Port 5060
        - G711Mu codec.
        - Either the Avaya CPE FQDN
            - *adevc.avaya.globalipcom.com*
        - Or the Verizon Business IP Trunk network FQDN (based on the provisioning described in **Section 1.2.4**)
            - *pcelban0001.avayalincroft.globalipcom.com*
    - Avaya Aura™ Session Manager sends the call to the Acme.
    - The Acme Packet sends the call to the Verizon Business IP Trunk network service node.

1.2.3 History Info and Diversion Headers

The Verizon Business IP Trunk service does not support SIP History Info Headers. Instead the Verizon Business IP Trunk service requires that SIP Diversion Header be sent for any call redirection events. Avaya Aura™ Communication Manager version 5.2 SIP trunk form provides options for specifying whether History Info Headers or Diversion Headers are sent (see **Section 3.1.6.1**).

If the Avaya Aura™ Communication Manager sends History Info Header for a call-redirection event, Avaya Aura™ Session Manager has the capability for converting these History Info headers into Diversion Headers. This is performed by specifying the "*VerizonAdapter*" adaptation in

Avaya Aura™ Session Manager (see **Section 4.3.2**). If Avaya Aura™ Communication Manager sends History Info Header for any other type of call event; the Avaya Aura™ Session Manager "*VerizonAdapter*" adaptation will remove the History Info Header.

The Avaya Aura™ Communication Manager Extension to Cellular (EC500) feature was used in the reference configuration to provide the call redirection events necessary to generate Diversion Headers (see **Section 3.1.10**).

In the reference configuration Avaya Aura™ Communication Manager was provisioned to send History Info Headers and Avaya Aura™ Session Manager performed the conversion to Diversion Header for call redirection.

1.2.4 Local to Foreign FQDN Conversion for Outbound Calls.

As mentioned in **Section 1.2**, the Avaya CPE environment was assigned the FQDN *adevc.avaya.globalipcom.com* by Verizon, and the Verizon Business IP Trunk network FQDN is *pcelban0001.avayalincroft.globalipcom.com*. Therefore, for outbound calls the destination specified in the SIP request URI should be *pcelban0001.avayalincroft.globalipcom.com*. There are two methods to accomplish this.

1. Avaya Aura™ Communication Manager method – Avaya Aura™ Communication Manager would specify the Verizon FQDN in the Far-End Domain field of the outbound voice and fax Signaling Group forms. This would result in Avaya Aura™ Communication Manager sending a SIP request URI to Avaya Aura™ Session Manager with the format:

   <called number>@ pcelban0001.avayalincroft.globalipcom.com

   Avaya Aura™ Session Manager would forward this URI to the Acme Packet for transmission to Verizon.

2. Avaya Aura™ Session Manager method – Avaya Aura™ Communication Manager would specify the Avaya CPE FQDN in the Far-End Domain field of the outbound voice and fax Signaling Group forms. This would result in Avaya Aura™ Communication Manager sending a SIP request URI to Avaya Aura™ Session Manager with the format:

   <called number>@ adevc.avaya.globalipcom.com

   By adding the Verizon FQDN to the VerizonAdapter adaptation (**see Section 4.3.2**), using the format:

   VerizonAdapter pcelban0001.avayalincroft.globalipcom.com

   Avaya Aura™ Session Manager will convert the Avaya CPE FQDN to the Verizon FQDN and send the following request URI to the Acme:

   <called number>@ pcelban0001.avayalincroft.globalipcom.com

Note - In the reference configuration method 2 was chosen.

1.3. 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 IP Trunking service does not support T.38 fax.
- The use of an Audio Codes MP-202 Gateway between Avaya Aura™ Communication Manager and the fax device is recommended for G.711 fax.
- Verizon Business IP Trunking service does not support G.711a codec for domestic service (EMEA only).
- Verizon Business IP Trunking service does not support G.729B codec.

Note – These Application Notes describe the provisioning used for the 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 IP Trunk service offer, 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 IP Trunk service 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 IP Trunk service on port 5060 and send traffic to the Verizon Business IP trunk service on port 5071, using UDP protocol for network transport (required by the Verizon Business IP Trunk service).

The Verizon Business IP Trunk service provided Direct Inward Dial (DID) 10 digit numbers for use during the testing. These DIDs were mapped by Avaya Aura™ Session Manager to their associated Avaya Aura™ Communication Manager extensions.

The Verizon Business IP Trunk service used FQDN *pcelban0001.avayalincroft.globalipcom.com*. The Avaya CPE environment was assigned FQDN *adevc.avaya.globalipcom.com* by Verizon Business IP Trunk service.

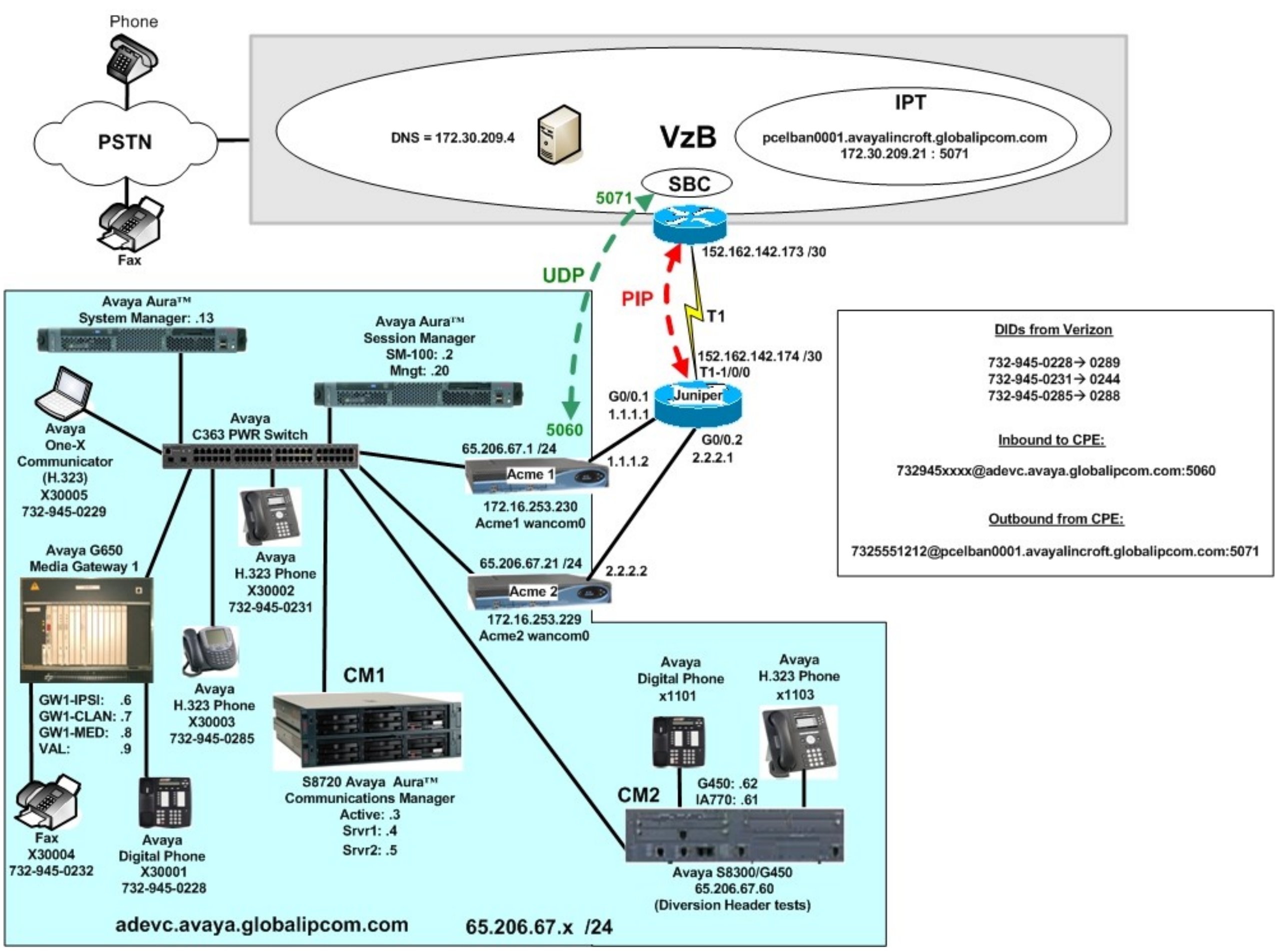


Figure 1: Avaya Interoperability Test Lab Reference Configuration

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 IP Trunk service offer.

Note - The initial installation, configuration, and provisioning of the Avaya servers for Avaya Aura™ 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™ 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, Avaya Digital and analog fax endpoints.

Note – The Avaya Aura™ 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.

Note – The Avaya Aura™ Communication Manager, Avaya Aura™ Session Manager, and Acme Packet SBC provisioning described in these Application Notes are also applicable on non SIP Trunk Redundant (2-CPE) architectures.

3.1. Verify System Capacity and Features

The Avaya Aura™ 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 IP Trunk service offer and any other SIP trunking applications. Be aware that for each call from a non-SIP endpoint to the Verizon Business IP Trunk service 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

Note – If any changes are made to the **system-parameters customer-options** form, you must log out of SAT and log back in for the changes to take effect.

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 **Enhanced EC500**, **IP Trunks,** 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? n
    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 (this IP address is defined during Avaya Aura™ Communication Manager installation).
- 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. Fax trunks are assigned to ip-network-region 3.

Avaya Component	IP_Network-Region
C-LAN	1
MedPro	1
Voice SIP Trunks 2 & 4	2
Fax SIP Trunks 3 & 5	3

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^{TM} 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 1 to Region 3	Codec 3
Region 2 to Region 2	Codec 2
Region 2 to Region 3	Codec 3
Region 3 to Region 3	Codec 3

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™ 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 FQDN provided by Verizon for the Avaya CPE location. In the reference configuration, the FQDN is ***adevc.avaya.globalipcom.com***.
   - 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**. **Codec Set *3*** is used for inter-region communication with region **3**.
   - 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
 3    3     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**. **Codec Set 3** is used for inter-region communication with region **3**.

```
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
 3    3     y    NoLimit                                             n
```

Figure 12: IP Network Region 2 – Page 3

3.1.3.3 IP-Network-Region 3

Ip-network-region 3 is defined for fax 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 3** to be used for the corresponding calls within the IP Network Region.

```
change ip-network-region 3                                    Page   1 of  19
                               IP NETWORK REGION
  Region: 3
Location: 1       Authoritative Domain: adevc.avaya.globalipcom.com
    Name:
MEDIA PARAMETERS                Intra-region IP-IP Direct Audio: yes
      Codec Set: 3              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 13: IP Network Region 3 – Page 1

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

```
display ip-network-region 3                                    Page   3 of  19
 Source Region: 3     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    3     y    NoLimit                                             n
 2    3     y    NoLimit                                             n
 3    3                                                                all
```

Figure 14: IP Network Region 3 – Page 3

3.1.4 IP Codec Sets

Three codec sets are defined in the reference configuration. One for local intra customer location calls (ip-network-region 1), off network voice calls (ip-network-region 2), and off network fax calls (ip-network-region 3). **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
Codec Form 3	3	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 15: 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 16: IP Codec Set 1 – Page 2

3.1.4.2 Voice 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
 3:
```

Figure 17: Voice Call IP Codec Set 2

2. On **Page 2** of the form set the values shown in **Figure 16** for codec set 1.

3.1.4.3 Fax Calls – IP-Codec-Set 3

G.711Mu was picked as the only option. This codec set is associated with ip-network-region 3.

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

```
change ip-codec-set 3                                            Page   1 of   2
                          IP Codec Set
    Codec Set: 3
    Audio        Silence      Frames   Packet
    Codec        Suppression  Per Pkt  Size(ms)
 1: G.711MU           n          2        20
 2:
```

Figure 18: Fax Call IP Codec Set 3

2. On **Page 2** of the form set the values shown in **Figure 16** for codec set 1.

3.1.5 SIP Trunk Groups

SIP trunks are defined for off network voice and fax calls to Verizon Business IP Trunk service. **Table x** lists the SIP trunks used in the reference configuration. A SIP trunk is created in Avaya

Aura™ Communication Manager by provisioning a SIP Trunk Group as well as a SIP Signaling Group.

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 Voice	Trunk 4	<blank>	2
Outbound Voice	Trunk 2	Avaya CPE FQDN *adevc.avaya.globaipcom.com*	2
Inbound Fax	Trunk 5	<blank>	3
Outbound Fax	Trunk 3	Avaya CPE FQDN *adevc.avaya.globalipcom.com*	3

Table 5: Avaya SIP Trunk Configuration

Note – In the SIP trunk configurations below (and in the Avaya Aura™ Session Manager configuration, **Section 4**), TCP was selected as the transport protocol in the reference configuration. TLS protocol could have been used instead.

3.1.5.1 Configure Public Inbound Voice 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 IP Trunk service 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 19: Public Inbound Voice 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-netwrk.**
      - 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: In_voice_blank               COR: 1        TN: 1        TAC: 104
   Direction: two-way       Outgoing Display? n
 Dial Access? n                                  Night Service:
Queue Length: 0
Service Type: public-netwrk          Auth Code? n
                                                      Signaling Group: 4
                                                    Number of Members: 10
```

Figure 20: Public Inbound Voice 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 21: Public Inbound Voice 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 IP Trunk service offer.
   - Let all other values default.

Note – History Info Headers are enabled by default (**Support Request History? y**). In the reference configuration this default value is used since Avaya Aura™ Session Manager is configured to generate Diversion Header (see **Sections 1.2.3** and **4.3.2**). If Avaya Aura™ Communication Manager is required to generate Diversion Header, this field must be set to "**n**" and the field **Send Diversion Header?** must be set to "**y**".

```
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? n
                    Send Diversion Header? n
                  Support Request History? y
             Telephone Event Payload Type: 101
```

Figure 22: Public Inbound Voice Trunk Group 4 – Page 4

3.1.5.2 Configure Public Inbound Fax SIP Trunk

The inbound Fax SIP trunk is configured in the same fashion as the inbound voice SIP Trunk except that the Fax Signaling Group Near-End port is 5062. This is the port Avaya Aura^{TM} Session Manager will specify for inbound fax calls.

1. Using the ***add signaling-group 5*** command, configure the inbound voice Signaling Group as follows:

   - Specify **5062** in the **Near-End** and **Far-end Listen Port** fields.
   - Enter the value **3** 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.
2. Using the ***add trunk-group 5*** command, add the inbound voice Trunk Group as follows:
   a. On Page 1 of the Trunk Group form:
      - Specify an available trunk access code (**TAC**) such as **105**.
      - Enter **5** as the **Signaling Group** number.

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

3.1.5.3 Configure Public Outbound Voice SIP Trunk

The outbound voice SIP trunk is configured in the same fashion as the inbound voice 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:
    b. 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**.

3.1.5.4 Configure Public Outbound Fax SIP Trunk

The outbound Fax SIP trunk is configured in the same fashion as the outbound voice SIP Trunk.

1. Using the ***add signaling-group 3*** 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 3*** command, add the inbound voice Trunk Group as follows:
    c. On Page 1 of the Trunk Group form:
        - Specify an available trunk access code (**TAC**) such as **103**.
        - Enter **3** as the **Signaling Group** number.

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

3.1.6 Public Unknown Numbering – Basic Configuration

In the reference configuration, the extensions on Avaya Aura™ Communication Manager use a 5 digit dialing plan using extensions 3xxxx. The **Public-Unknown-Numbering** form allows Avaya Aura™ Communication Manager to use these extensions as the calling party number for outbound calls. Otherwise *Anonymous* is displayed as the calling number. Each extension string is defined for the *outbound* trunk group that the extensions may use. These trunks may be defined individually or in contiguous ranges.

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

- Set the **Ext Len** field to **5**.
- Set the **Ext Code** field to **3**.
- Set the **Trk Grp(s)** field to **2-3** (voice = 2, fax =3)**.**
- Set the **Total CPN Len** field to **5**. This is the total number of digits in the extension.

All provisioned public-unknown-numbering entries can be displayed by entering the command ***display public-unknown-numbering 0*** as shown 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: 2
 5  3             2-3                        5          Maximum Entries: 9999
```

Figure 23: Public-unknown-numbering Form – Basic Configuration

3.1.6.1 Public Unknown Numbering – History Info/Diversion Header

As mentioned in **Section** 1.2.3, the Verizon Business IP Trunk service does not support History Info but does use the contents of the Diversion Header for admission control (the calling number specified in the Diversion Header must match a Verizon Business IP Trunk service DID or the redirected call will be rejected).

Since Avaya Aura™ Communication Manager or Avaya Aura™ Session Manager may generate Diversion Headers, the contents of the public-unknown-numbering form may differ based on the method used.

3.1.6.1.1 If Avaya Aura™ Communication Manager Creates Diversion Header

If Avaya Aura™ Communication Manager is provisioned to generate the Diversion Header, (see **Section 3.1.5.1**), then the public-unknown-numbering form must be configured to convert the local calling extension to its associated Verizon Business IP trunk service DID. In this manner the Diversion Header will contain a calling number that will pass Verizon Business IP trunk service admission control. **Figure 24** shows an example of this configuration. Extension 30001 is a fax endpoint and 30002 is an H.323 endpoint. Avaya Aura™ Communication Manager will insert 7329450228 in the Diversion Header for station 30001 and 7329450285 for station 30002.

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

- Set the **Ext Len** field to **5**.
- Set the **Ext Code** field to **30001** and **30002**.
- Set the **Trk Grp(s)** field to **2** or **3** (voice = 2, fax =3)**.**
- Set the **CPN Prefix** field to the Verizon DID (e.g. 7329450228)
- Set the **Total CPN Len** field to **10**. This is the total number of digits in the DID.

All provisioned public-unknown-numbering entries can be displayed by entering the command ***display public-unknown-numbering 0*** as show in **Figure 24**.

```
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: 2
 5  30001            3        7329450228     10           Maximum Entries: 9999
 5  30002            2        7329450285     10
```

Figure 24: Public-unknown-numbering Form

3.1.6.1.2 If Avaya Aura™ Session Manager Creates Diversion Header

If Avaya Aura™ Session Manager is used to generate the Diversion Header, then the Avaya Aura™ Communication Manager public-unknown-numbering form need not be changed from the basic configuration shown in **Section 3.1.6**. However Avaya Aura™ Session Manager must be provisioned to convert the local calling extension contained in the History Info Header to its associated Verizon Business IP trunk service DID (see **Section 4.3.2**). In this manner the Diversion Header sent by Avaya Aura™ Session Manager will contain a calling number that will pass Verizon Business IP trunk service admission control.

3.1.7 Call Routing

3.1.7.1 Outbound Calls

The following Sections describe Avaya Aura™ Communication Manager provisioning required for outbound dialing. Although Avaya Aura™ Session Manager routes all inbound and outbound SIP trunk calls, Avaya Aura™ Communication Manager uses ARS to direct outbound calls to Avaya Aura™ Session Manager based on whether they are voice or fax calls. This routing is used to determine the codec type used for these calls (see **Section 3.1.3**).

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 IP Trunk service. 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 25: 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 26: 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 the following numbers:

   - 732 (voice destination beginning with 732)
   - 800 (voice destination beginning with 800)
   - 7324509213 (fax destination)
   - 011 (international voice destination)
   - 0 (operator call)

   For example, to specify the 732 voice 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 voice trunk)
   - Set the **Type** field to **hnpa**

   To specify the 7324509213 fax call, enter the command ***change ars analysis 732***4509213 and enter the following values:
   - Set the **Dialed String** field to **7324509213**
   - Set the **Total Min** field to **10**
   - Set the **Total Max** field to **10**

- Set the **Route Pattern** field to **3** (will direct to fax trunk)
- Set the **Type** field to **hnpa**

> **Note** – ARS will route based on the most complete match. For example 7324509213 will match before 732.

Using the same procedure, specify the other called number patterns in the ARS table. **Figure 27** shows the completed ARS table.

```
display ars analysis 0                                     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
    0                      1    1      2         op           n
    011                    11   20     2         intl         n
    732                    10   10     2         hnpa         n
    7324509213             10   10     3         hnpa         n
```

Figure 27: ARS Analysis Form

3.1.7.1.2 Route Patterns

The reference configuration used Facility Restriction Level (FRL) to determine which outbound trunks could be used for voice and fax calls. Each outbound trunk is assigned an FRL on the route pattern form. Outbound voice calls use route-pattern 2 while outbound fax calls use route-pattern 3. In addition, all voice extensions were provisioned with an FRL of 2 and all fax extensions were provisioned with an FRL of 1 (see **Section 3.1.8**). The higher the FRL, the higher the access level (e.g. an extension with an FRL of 1 cannot access a trunk specified with an FRL of 2. However an extension with an FRL of 2 can access trunks with FRLs of 2 and 1). In this manner outbound G.711Mu fax calls will use trunk 3, while outbound G.729A and G.711Mu voice calls will use trunk2.

> **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. Voice calls - Use the **change route-pattern** command to define the outbound SIP trunk groups included in the route pattern that ARS selects.
   - **Voice trunk** - This trunk will be selected for outbound voice calls.
     - Set the first **Grp No** field to *2*.
     - Set the **FRL** field to *2*.
   - Let all other parameters default.

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

Figure 28: Route Pattern 2 – Outbound Voice Calls

2. Fax calls - Use the **change route-pattern** command to define the outbound SIP trunk groups included in the route pattern that ARS selects.
   - **Fax trunk** - This trunk will be selected for outbound fax calls.
     - Set the third **Grp No** field to ***3***.
     - Set the **FRL** field to ***1***.
   - Let all other parameters default.

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

Figure 29: Route Pattern 3 – Outbound Fax Calls

3.1.7.2 Incoming Calls

SIP trunk 4 is used for inbound voice calls and SIP trunk 5 is used for inbound fax calls. In the reference configuration the Avaya Aura™ Session Manager is used to convert inbound Verizon DID 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 30 shows an example of a voice extension (Avaya H.323 IP phone). Note that the **COR** value is ***1*** (default) for the voice extension. COR 1 is provisioned to assign FRL 2 to the voice stations. 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)
- Set the **COR** field to **1**

```
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 30: Voice Extension – Avaya H.323 IP Phone – Page 1

On page 4 of the form:

- Select an empty button assignment and enter **ec500** and let the **timer** field default to **N**. This button will enable EC500 capability on the phone (see **Section 3.1.10**).
- 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: ec500      Timer? n                 7:
 4:                                     8:
    voice-mail Number:
```

Figure 31: Voice Extension – Avaya H.323 IP Phone – Page 4

3.1.8.2 Fax Stations

Figure 32 shows an example of a fax extension. Note that the **COR** value is **2**. COR 2 is provisioned to assign FRL 1 to the voice stations. In the reference configuration an analog board is located in slot 01a07 (the command ***list configuration all*** may be used to find board locations on Avaya Aura™ Communication Manager). The fax station is connected to port 7 of the analog board. Therefore, the port specified for this fax extension is ***01A0707***. By default one call appearance is define on page 4 of the form.

On page 1 of the form:

- Set the **Type** field to match the station type (e.g. 2500)

- Set the **Port** field to **01a0707**
- Set the **Name** field to some value (e.g. Fax-port)
- Set the **COR** field to **2**
- Allow all other fields to default.

```
display station 30001                                           Page   1 of   4
                                     STATION
Extension: 30001                          Lock Messages? n               BCC: 0
     Type: 2500                          Security Code: *                 TN: 1
     Port: 01A0707                     Coverage Path 1:                  COR: 2
     Name: Fax-port                    Coverage Path 2:                  COS: 1
                                       Hunt-to Station:               Tests? y
STATION OPTIONS
      XOIP Endpoint type: auto             Time of Day Lock Table:
              Loss Group: 1             Message Waiting Indicator: none
    Off Premises Station? n
          Survivable COR: internal
   Survivable Trunk Dest? y                  Remote Office Phone? n
```

Figure 32: Fax Extension – Analog Port

3.1.9 Avaya Aura™ Communication Manager Class Of Restriction (COR)

As described in above, outbound calls from voice and fax extensions were provisioned with different FRLs. These FRLs are associated with an extension via the **Class of Restriction** (COR) form. Voice extensions are assigned a COR of 1 (default) and fax extensions are defined with a COR of 2 (**Figure 33**).

For the voice COR 1 use the **change cor 1** command and enter the following:

- Enter ***Voice Calls*** in the **cor description** field.
- Enter ***2*** into the **FRL** field.

```
change cor 1                                                   Page   1 of  23
                                  CLASS OF RESTRICTION
               COR Number: 1
          COR Description: Voice calls
                      FRL: 2                                 APLT? y
  Can Be Service Observed? n          Calling Party Restriction: none
Can Be A Service Observer? n           Called Party Restriction: none
        Time of Day Chart: 1      Forced Entry of Account Codes? n
         Priority Queuing? n                Direct Agent Calling? n
     Restriction Override: all       Facility Access Trunk Test? n
     Restricted Call List? n                 Can Change Coverage? y
            Access to MCT? y           Fully Restricted Service? n
Group II Category For MFC: 7           Hear VDN of Origin Annc.? n
         Send ANI for MFE? n            Add/Remove Agent Skills? n
            MF ANI Prefix:             Automatic Charge Display? n
Hear System Music on Hold? y   PASTE (Display PBX Data on Phone)? n
                        Can Be Picked Up By Directed Call Pickup? n
                                    Can Use Directed Call Pickup? y
                                    Group Controlled Restriction: inactive
```

Figure 33: COR 1 – Voice Extensions

For the fax extension COR 2 (**Figure 34**) use the **change cor 2** command and enter the following:

- Enter ***Fax Calls*** in the **cor description** field.
- Enter ***1*** into the **FRL** field.

```
change cor 2                                                  Page   1 of  23
                              CLASS OF RESTRICTION
               COR Number: 2
          COR Description: Fax calls
                      FRL: 1                                APLT? y
  Can Be Service Observed? n           Calling Party Restriction: none
Can Be A Service Observer? n            Called Party Restriction: none
        Time of Day Chart: 1       Forced Entry of Account Codes? n
         Priority Queuing? n                Direct Agent Calling? n
     Restriction Override: none       Facility Access Trunk Test? n
     Restricted Call List? n                 Can Change Coverage? n
            Access to MCT? y            Fully Restricted Service? n
Group II Category For MFC: 7            Hear VDN of Origin Annc.? n
         Send ANI for MFE? n             Add/Remove Agent Skills? n
            MF ANI Prefix:              Automatic Charge Display? n
Hear System Music on Hold? y   PASTE (Display PBX Data on Phone)? n
                        Can Be Picked Up By Directed Call Pickup? n
                                    Can Use Directed Call Pickup? n
                                    Group Controlled Restriction: inactive
```

Figure 34: COR 2 – Fax Extensions

3.1.10 EC500 Provisioning for Diversion Header Testing.

Avaya Aura™ Communication Manager EC500 feature was used to generate Diversion Headers (see **Section 3.1.10**). EC500 provides call coverage for an Avaya Aura™ Communication Manager station to a second destination endpoint. Typically this endpoint is a cell phone. When EC500 is enabled on the Avaya Aura™ Communication Manager station (by pressing the EC500 button), any inbound call to that station will generate a new outbound call from Avaya Aura™ Communication Manager to the provisioned EC500 destination endpoint. In the reference configuration EC500 was provisioned on an H.323 station (see **Section 3.1.8**).

Note – Only the basic EC500 call redirection functionality was used in the reference configuration. EC500 supports significantly more features. For more information on EC500 see **[7]**.

1. Verify that EC500 has been enabled on Avaya Aura™ Communication Manager (see **Section 3.1**).
2. Use the command **change off-pbx-telephone station mapping x** where *x* is the Avaya Aura™ Communication Manager station (e.g. **30003**).
    - **Station Extension** – This field will automatically populate
    - **Application** – Enter **EC500**
    - **Phone Number** – Enter the phone that will also be called (e.g. **732-4509213**)
    - **Trunk Selection** – Enter **ARS**. This means ARS will be used to determine how Avaya Aura™ Communication Manager will place this new outbound call.
    - **Config Set** – Enter **1**
    - Let all other parameters default.

```
change off-pbx-telephone station-mapping 30003                  Page   1 of   3
                  STATIONS WITH OFF-PBX TELEPHONE INTEGRATION

 Station       Application Dial   CC  Phone Number    Trunk       Config  Dual
 Extension                 Prefix                     Selection   Set     Mode
 30003            EC500        -      7324509213       ars        1
                               -
```

Figure 35: EC500 Station Mapping

3.1.11 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 System Manager management server. All SIP call provisioning for Avaya Aura™ Session Manager is performed via the System Manager web interface and are then downloaded into Avaya Aura™ Session Manager.

Note – The following sections assume that Avaya Aura™ Session Manager and System Manager have been installed and that network connectivity exists between the two platforms. For more information on 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 36** shows the backplane of Avaya Aura™ Session Manager.

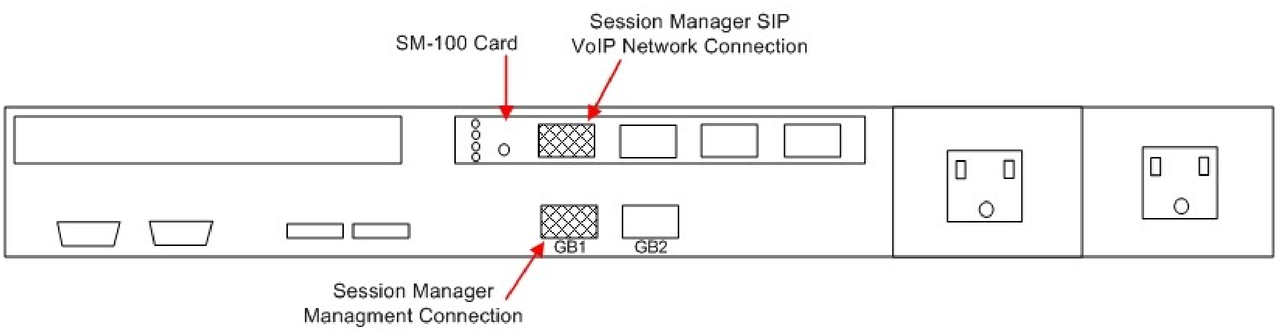


Figure 36 – Avaya Aura™ Session Manager Network Connections

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 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 System Manager/Avaya Aura™ Session Manager management connection use a different network than the SM-100 connection.

4.2. Logging Into System Manager

The following provisioning is performed via 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 System Manager.

In System Manager Release 1, configuration is accomplished by accessing the browser-based GUI of System Manager, using the URL ***http://<ip-address>/IMSM***, where "<ip-address>" is the IP address of System Manager.   In System Manager Release 5.2, the URL to access the browser-based GUI of System Manager is ***https://<ip-address>/SMGR***. Log in with the appropriate credentials.

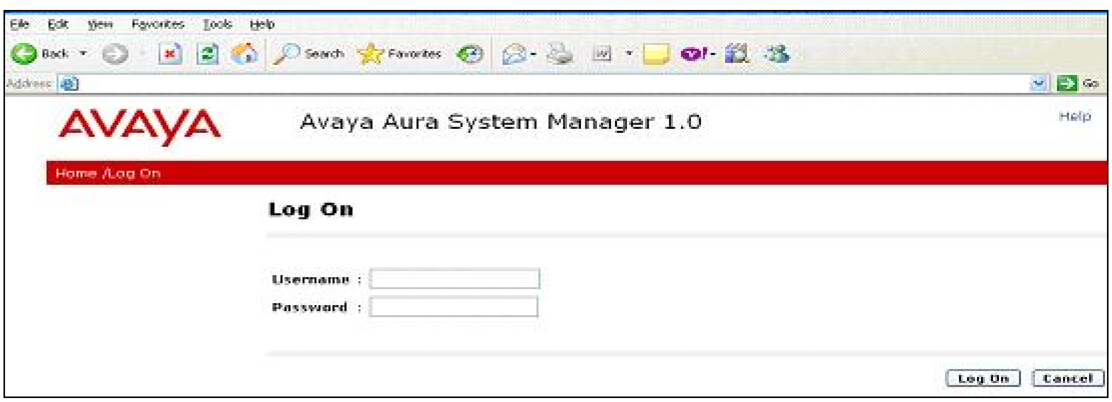


Figure 37: System Manager GUI Log On Screen

4.3. Network Routing Policy

After logging in, the menu shown in **Figure 38** is displayed. Expand the **Network Routing Policy Link** on the left side as shown.

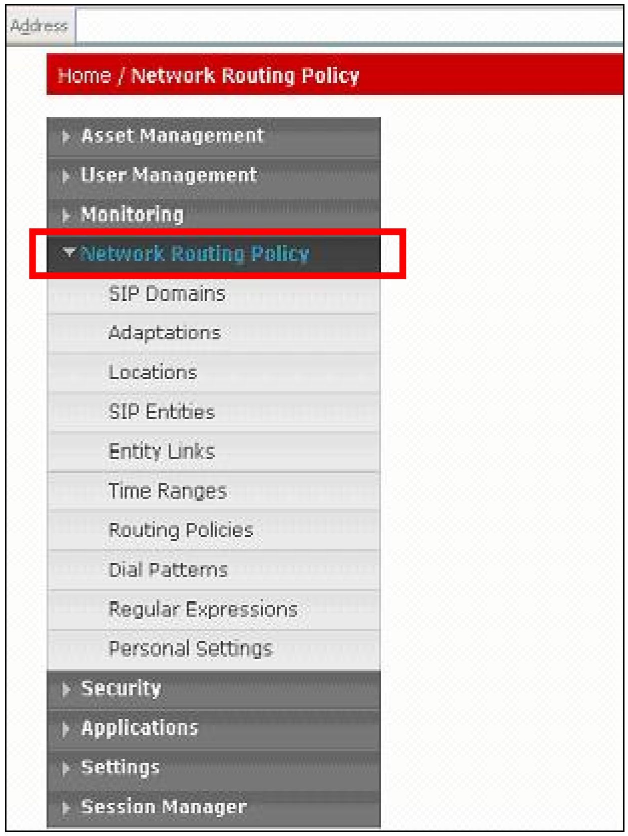


Figure 38: Network Routing Policy Menu

4.3.1 SIP Domains

In the reference configuration two SIP domains (FQDNs) were used. The Avaya CPE location is *adevc.avaya.globalipcom.com* and the Verizon Business IP Trunk service node is *pcelban0001.avayalincroft.globalipcom.com*. The Avaya CPE will send calls to the Verizon FQDN and the Verizon Business IP Trunk service will send calls to the Avaya FQDN. Therefore both of these FQDNs must 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. Repeat these steps for each SIP Domain. When completed, the SIP Domain window will look like **Figure 39**.
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 39: 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 modules are called adaptations. Two of these adaptations are used in the reference configuration: DigitConversionAdapter and VerizonAdapter

4.3.2.1 DigitConversionAdapter

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 (incoming) or sent (outgoing) by 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.

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.

In the incoming example Avaya Aura™ Communication Manager extension 30001 will be converted to Verizon DID 7329450228 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 → **7329450228**
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.

In the outgoing example Verizon DID 7329450228 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 → **7329450228**
   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. When completed, the Adaptation Details window for DigitConversionAdapter will look like **Figure 40**.
10. Click on the **Commit** button.

In the reference configuration Avaya Aura™ Communication Manager extensions were converted to Verizon DID numbers and vice versa. Verizon Business IP Trunk service uses its DID numbers for admission control.

Extension	DID
30001	732-945-0228
30002	732-945-0231
30003	732-945-0285
30004	732-945-0232
30005	732-945-0229

Table 6: Extension/DID assignments

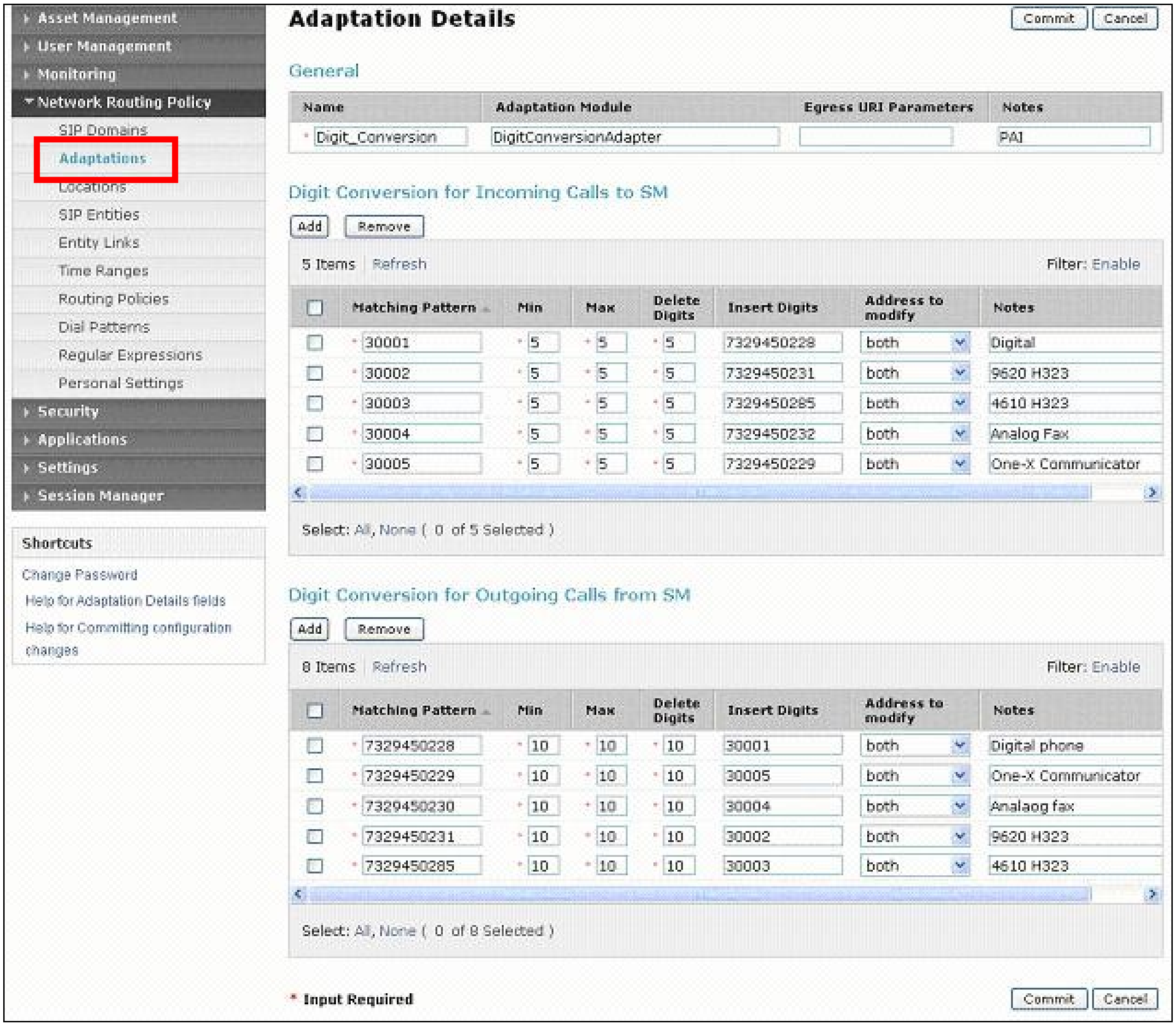


Figure 40: DigitConversionAdapter Adaptation

4.3.2.2 VerizonAdapter

Verizon Business IP Trunk service supports Diversion Header for call redirection scenarios, and does not use History Info header. Although Avaya Aura™ Communication Manager 5.2 supports both headers, earlier versions only support History Info and will send them for direct and redirected calls. The VerizonAdapter adaptation when provisioned will strip off the History Info headers for direct calls or replace them with Diversion Headers for redirected calls.

4.3.2.3 Additional Options

There are additional options that can be specified with the adaptations. The reference configuration required that the Avaya CPE FQDN contained in the Request URI sent by Avaya Aura™ Communication Manager to Avaya Aura™ Session Manager be replaced with the Verizon FQDN before being sent out to Verizon via the Acme. The FQDN replacement was performed by specifying the Verizon FQDN after the **VerizonAdapter** adaptation with the format –

VerizonAdapter pcelban0001.avayalincroft.globalipcom.com

1. Select **Adaptations** from the menu.
2. Select **New**.
3. Enter a descriptive name (e.g. **History Diversion**)
4. Specify **VerizonAdapter pcelban0001.avayalincroft.globalipcom.com** 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.

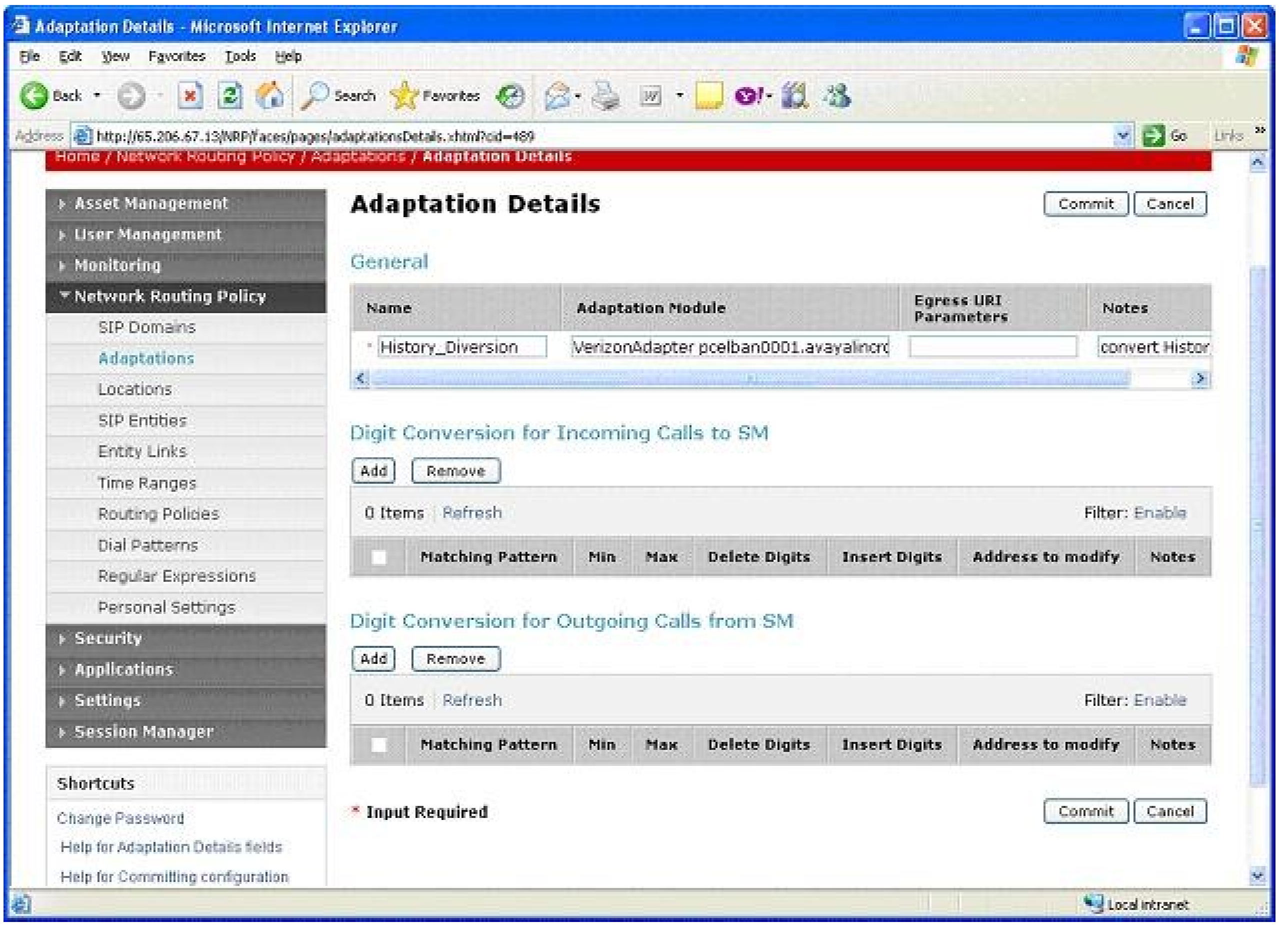


Figure 41: VerizonAdapter Adaptation with FQDN Replacement

Note - The VerizonAdapter was chosen for the FQDN replacement function since it was specified on the Acme Packet SIP Entity for outbound calls (see **Section 5**). However the FQDN replacement function may be specified with any adaptation.

When completed the Adaptations page will look like **Figure 42**.

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

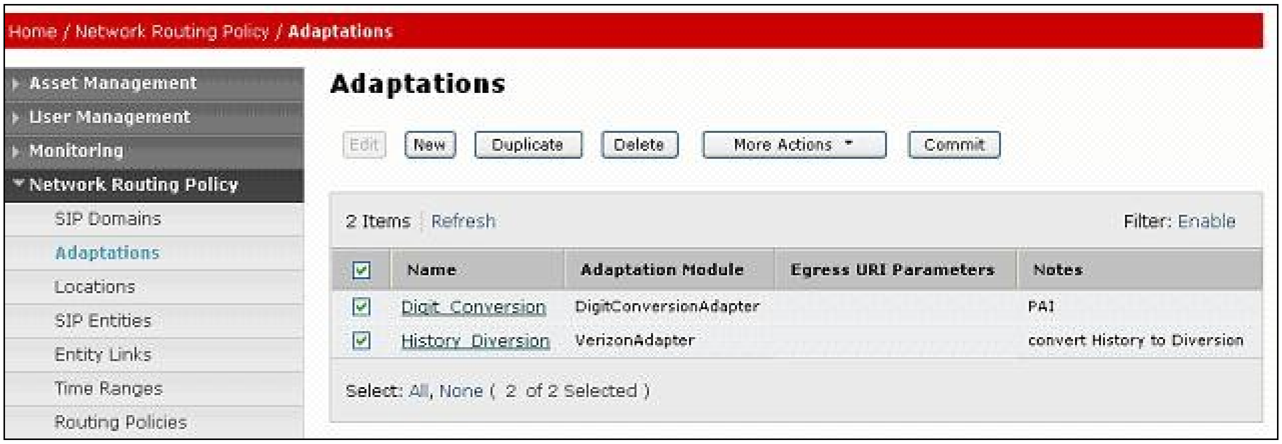


Figure 42: Completed Adaptations page

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 site was defined as a Location. 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 43** 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.

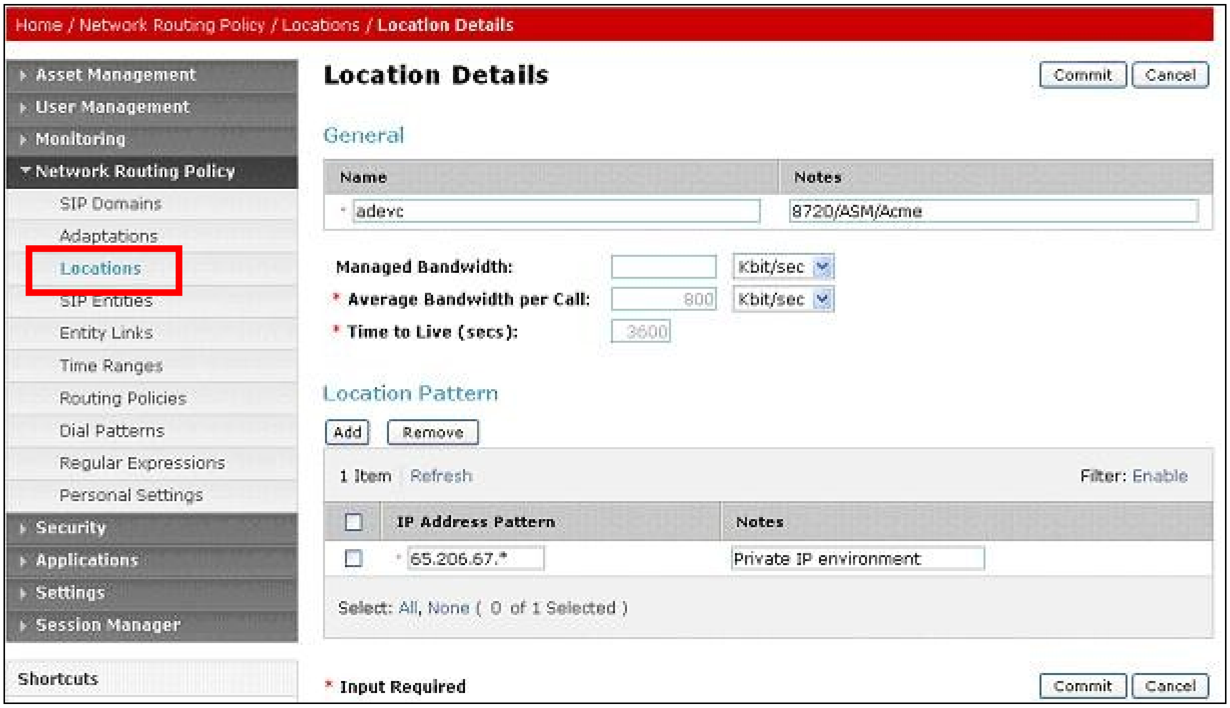


Figure 43: Locations Menu

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
- Avaya Aura™ Communication Manager (C-LAN) fax SIP trunk
- The Primary Acme Packet SBC
- The Secondary 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 44** 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 adaptation required for this Entity (see **Section X**).
      i. For the voice and fax C-LAN Entities, the DigitConversion adaptation is selected. This function is applied to the C-LAN Entities to convert Avaya extensions to Verizon DIDs 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 Primary and Secondary Acme Packet Entities, the VerizonAdapter 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 FQDN.

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

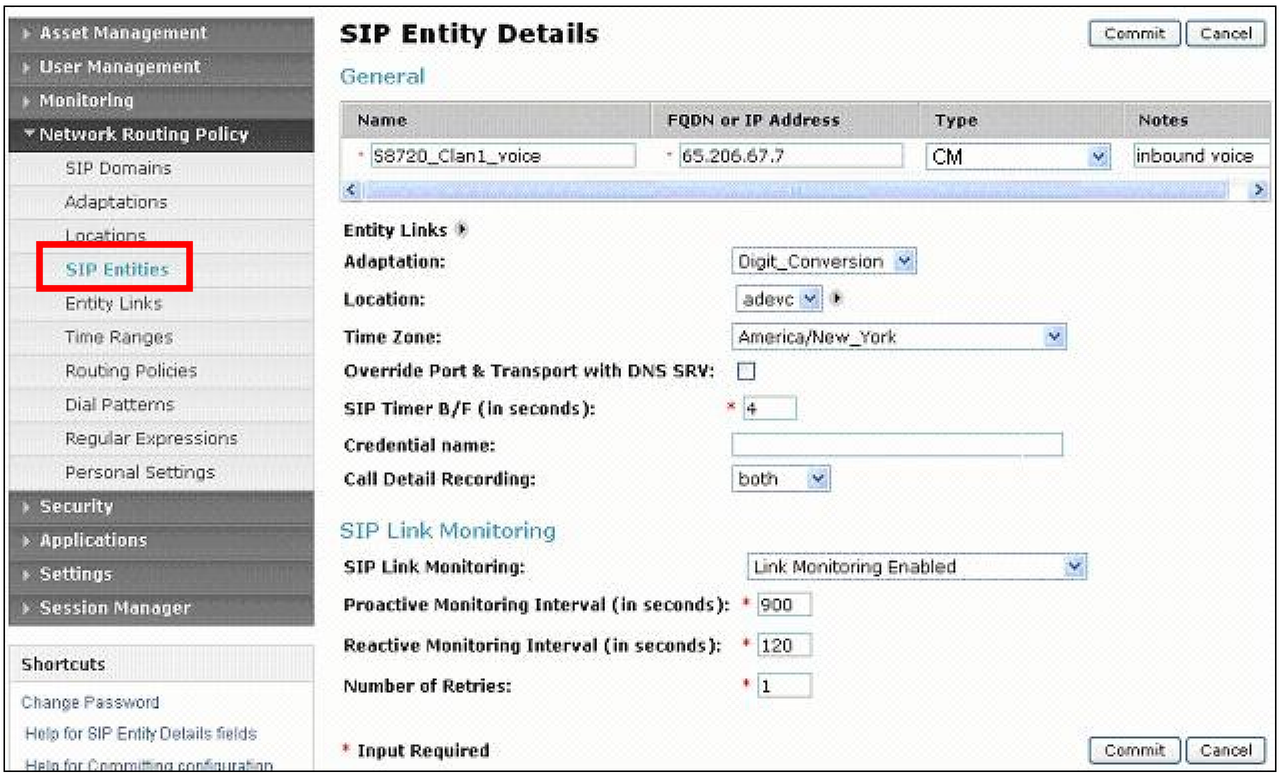


Figure 44: C-LAN SIP Entity Details

Note – When defining a SIP Entity for Avaya Aura™ Session Manager itself and SM is selected from the Type drop down menu, an additional 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. Note that the SIP Entity Type "SBC", available in Release 1, is not used in Release 5.2. For Release 5.2, SIP Entity Type "Other" can be used for the Acme Packet SBC SIP Entities.

Name	IP Address	Type (R1)	Type (R5.2)	Adaptation	Location	Port	Protocol	Domain
Acme1	65.206.67.1	SBC	Other	Verizon	adevc	-	-	Avaya CPE
Acme2	65.206.67.21	SBC	Other	Verizon	adevc	-	-	Avaya CPE
ASM1	65.206.67.2	SM	SM	-	adevc	5060	TCP	Avaya CPE
CLAN-Fax	65.206.67.7	CM	CM	DigitConv	adevc	-	-	Avaya CPE
CLAN-Voice	65.206.67.7	CM	CM	DigitConv	adevc	-	-	Avaya CPE

Table 7: SIP Entity Provisioning

Figure 45 show the completed SIP Entities form.

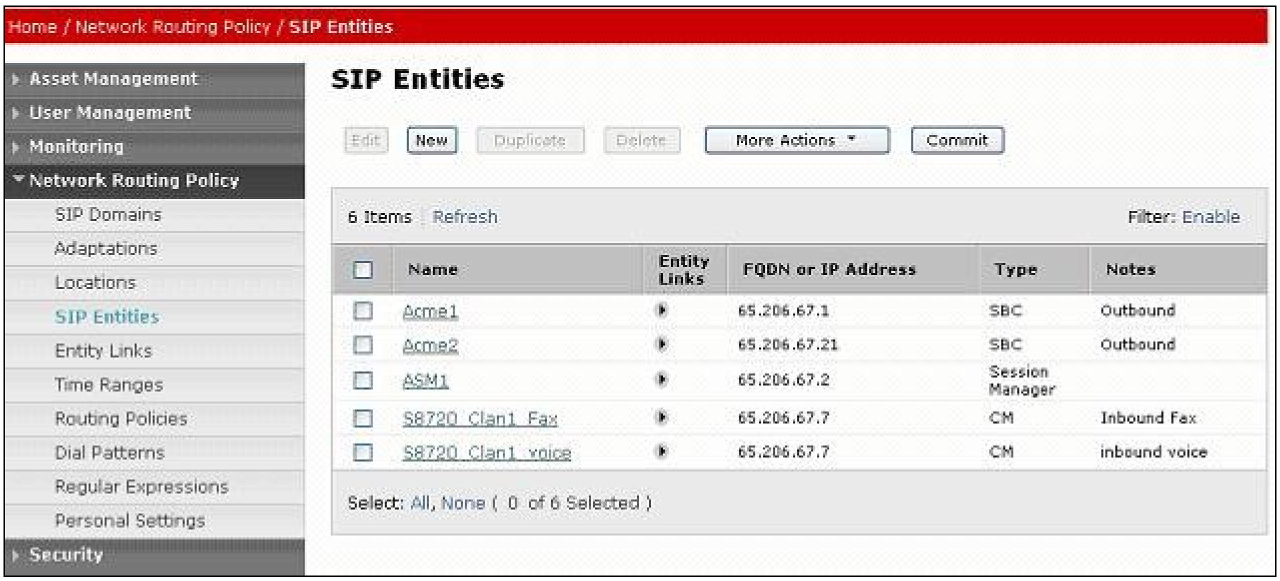


Figure 45: Completed SIP Entities Form

4.3.5 Entity Links

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 Primary Acme Packet (Acme1)
- The Secondary Acme Packet (Acme2)
- The Avaya Aura™ Communication Manager C-LAN for voice calls (S8720_Clan1_voice)
- The Avaya Aura™ Communication Manager C-LAN for fax calls (S8720_Clan1_fax)

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 46** 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.

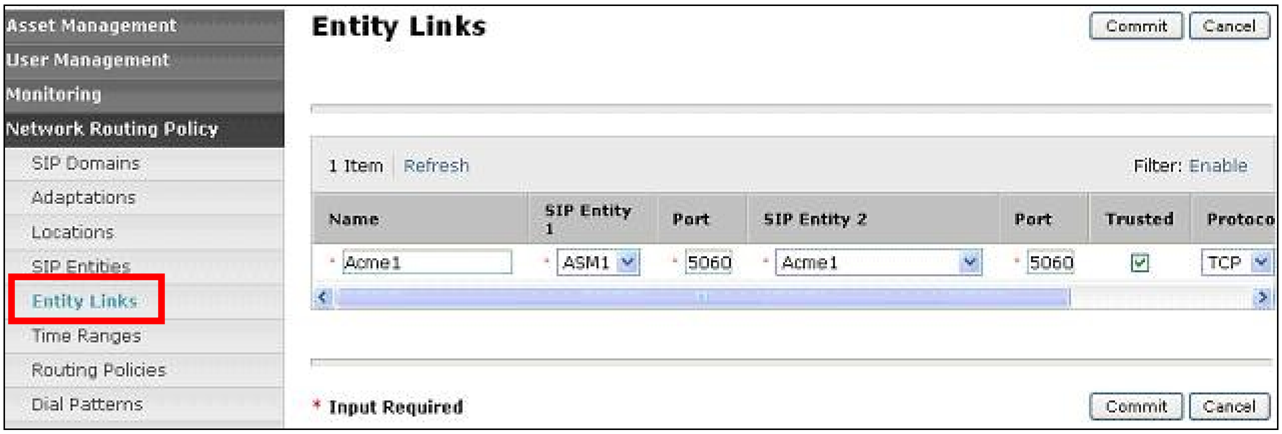


Figure 46: Entity Link – Primary Acme Packet

10. Click on **New** and repeat steps 1 thru 9 for the **Acme2** Entity Link, specifying Acme2 in the **SIP Entity 2** drop down menu.
11. Click on **New** and repeat steps 1 thru 9 for the **Voice** Entity Link, specifying **S8720_Clan1_voice** in the **SIP Entity 2** drop down menu.
12. Click on **New** and repeat steps 1 thru 9 for the **Fax** Entity Link, specifying **S8720_Clan1_fax** in the **SIP Entity 2** drop down menu and port **5062** for the port values.

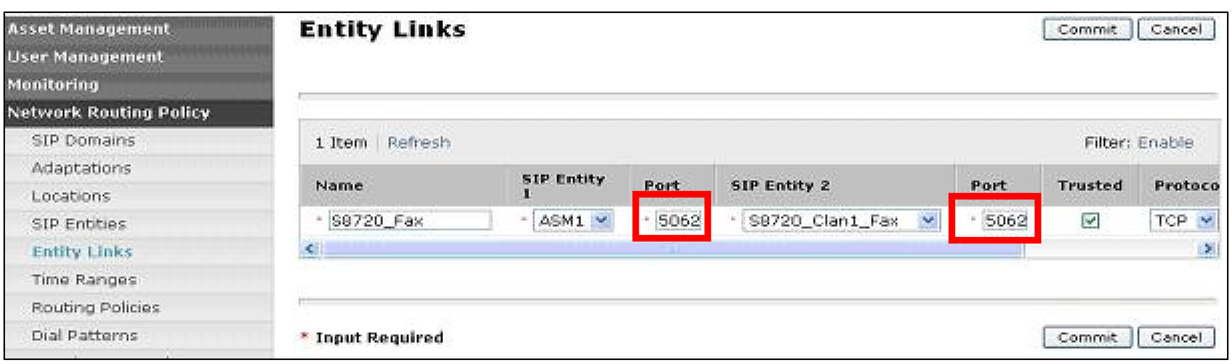


Figure 47: Entity Link – Fax Calls

When completed, the Entity Links form will look like **Figure 48**.

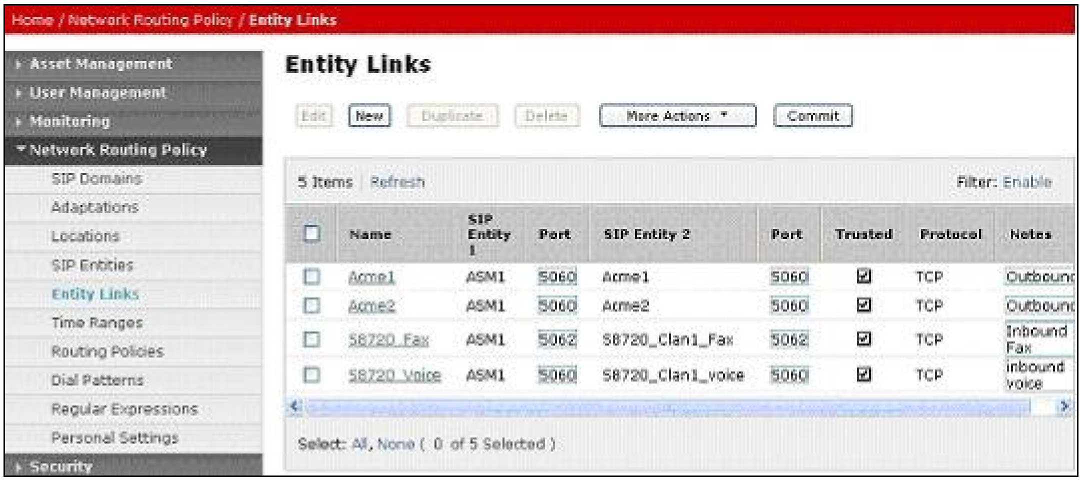


Figure 48: Completed Entity Links Form

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 49** 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 49: 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 Fax calls (to Avaya Aura™ Communication Manager)
- Inbound voice calls (to Avaya Aura™ Communication Manager)
- Outbound calls to Acme1 (all outbound calls to Verizon)
- Outbound calls to Acme2 (if Acme1 is out of service).

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

Name	SIP Entity Destination	Time Of Day	Dial Pattern(s)	Notes
Inbound_Fax	S8720_Clan1_Fax	Anytime	7329450228 – 10 digits	This call will route to Avaya Aura™ Communication Manager fax station 30001 (after digit conversion), and use port 5062.
Inbound_Voice	S8720_Clan1_Voice	Anytime	732945 – 10 digits	Any call to 732945xxxx (excluding the Fax number above) will route to Avaya Aura™ Communication Manager stations (after digit conversion), and use port 5060.
Outbound1	Acme1	Anytime	0 -1 digit 011 -14 digits 800 -10 digits 1800 -11 digits 411- 3 digits 732450 -10 digits 732852 -10 digits	All matching dial patterns will route to Acme1 to be sent to Verizon.
Outbound2	Acme2	Anytime	Same as Outbound1	All matching dial patterns will route to Acme2 if Avaya Aura™ Session Manager determines that Acme1 is out of service.

Table 8: 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 50** will open.

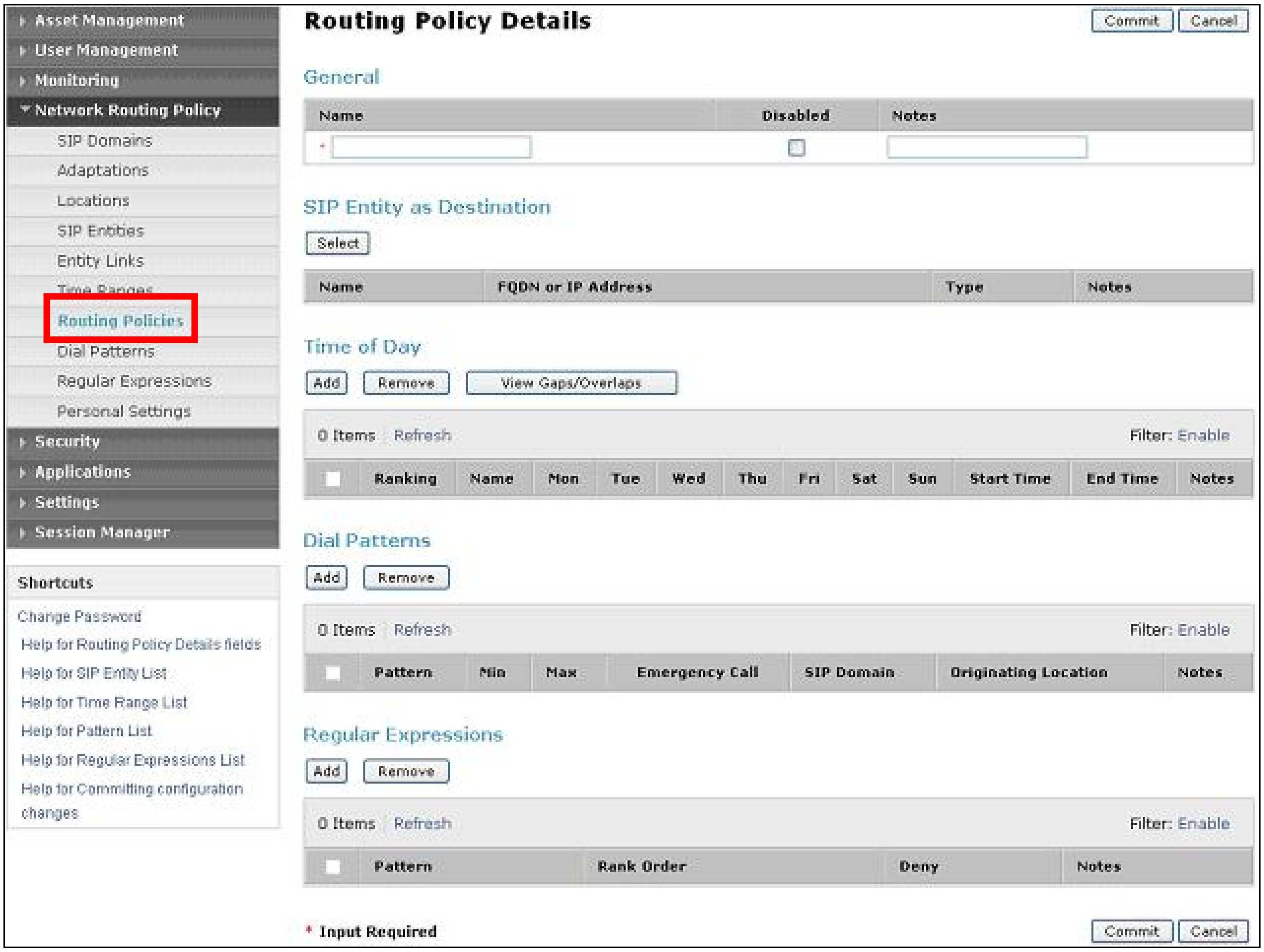


Figure 50: Routing Policy Details

1. **General** section
   a. Enter a descriptive Location name in the **Name** field (e.g. **Inbound_Fax**).
   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_fax**)
   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** for this Routing Policy.
   b. Click on **Select** and return to the Routing Policy Details form. The form will look like **Figure 51**.

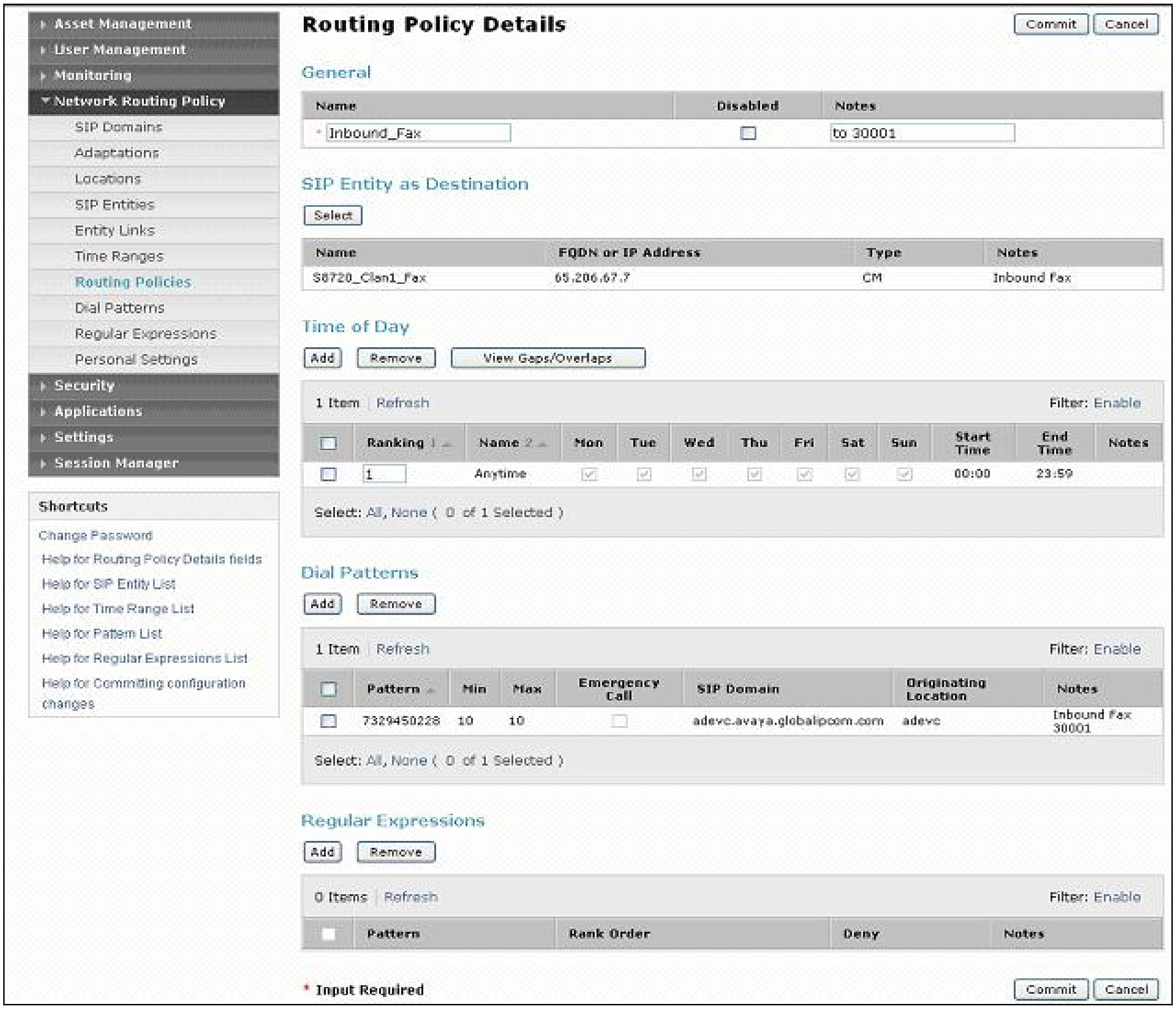


Figure 51: Routing Policy Details - Completed

5. Click the **Commit** button.
6. Repeat steps 1 thru 5 for each Routing Policy. When completed the form will look like **Figure 52**.

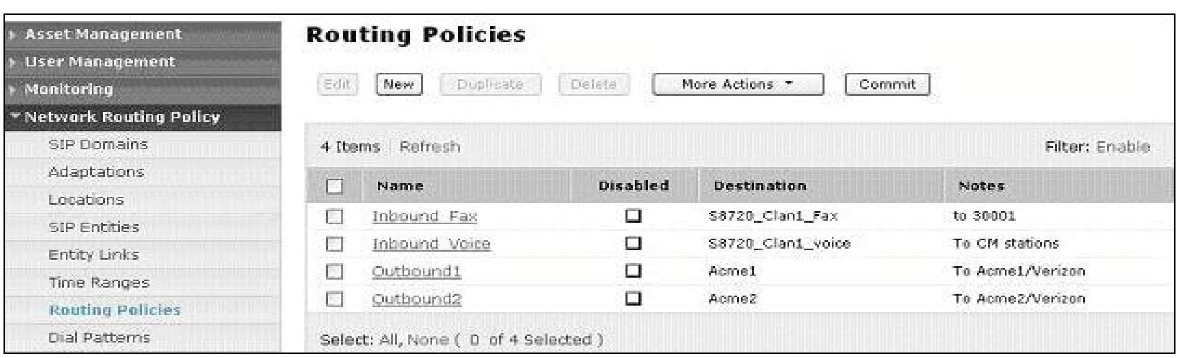


Figure 52: Routing Policies- Completed

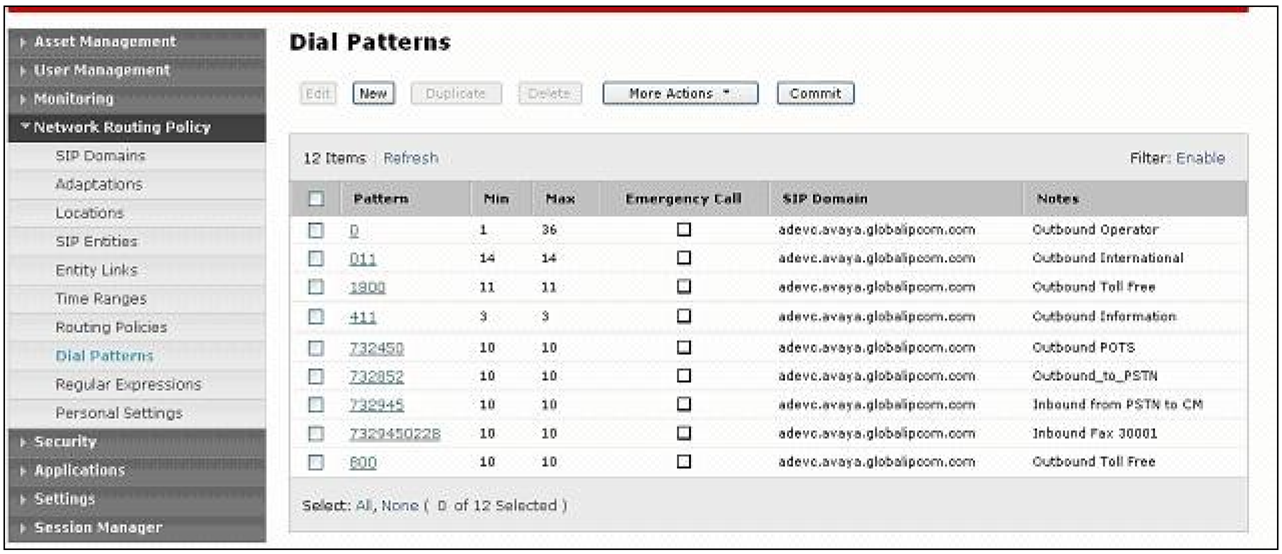
7. Click the **Commit** button.

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 5 digit string 300 is defined first in the list, and the 5 digit string 30001 is defined last, a call for 30001 will match on the 30001 string.

The following Dial Patterns were provisioned in the reference configuration.



Pattern	Min	Max	Emergency Call	SIP Domain	Notes
0	1	36	☐	adevc.avaya.globalipcom.com	Outbound Operator
011	14	14	☐	adevc.avaya.globalipcom.com	Outbound International
1800	11	11	☐	adevc.avaya.globalipcom.com	Outbound Toll Free
411	3	3	☐	adevc.avaya.globalipcom.com	Outbound Information
732450	10	10	☐	adevc.avaya.globalipcom.com	Outbound POTS
732852	10	10	☐	adevc.avaya.globalipcom.com	Outbound_to_PSTN
732945	10	10	☐	adevc.avaya.globalipcom.com	Inbound from PSTN to CM
7329450228	10	10	☐	adevc.avaya.globalipcom.com	Inbound Fax 30001
800	10	10	☐	adevc.avaya.globalipcom.com	Outbound Toll Free

Figure 53: Completed Dial Pattern Form

Note – The DigitConversionAdapter adaptation is provisioned on the Avaya Aura™ Communication Manager Clan SIP Entities for voice and fax calls. This means that the conversion from Verizon DIDs to Avaya Aura™ Communication Manager extensions is performed ***after*** the dial pattern match for inbound calls, and ***before*** the dial pattern match for outbound calls.

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 54** is displayed. In this example a Request URI to a 10 digit number beginning with *732852xxxx*, and sent by *adevc.avaya.globalipcom.com*, 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. **732852**).
   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.

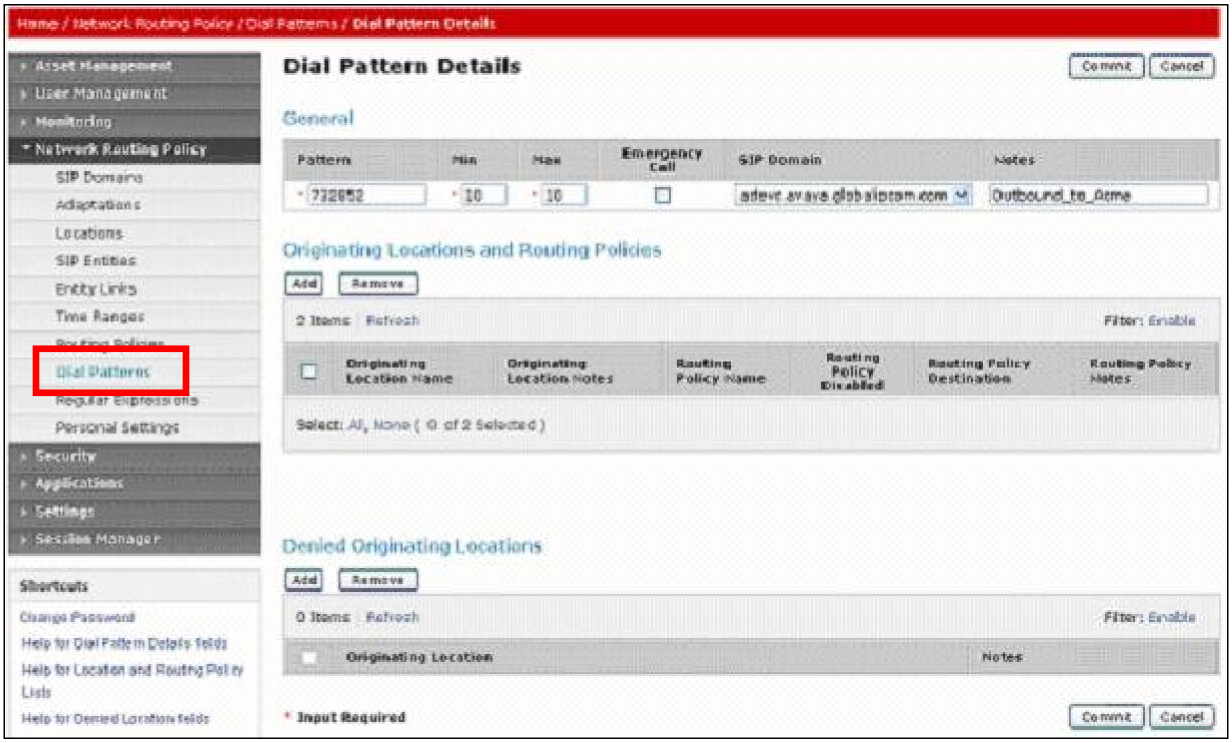


Figure 54: Dial Pattern Details - General

2. **Originating Locations and Routing Policies** Section
   a. Click on the Add button and the window in **Figure 55** 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 Policies **Oubound1** (Acme1) and **Outbound2** (Acme2).
   c. Click on the **Select** button and return to the Dial Pattern window.

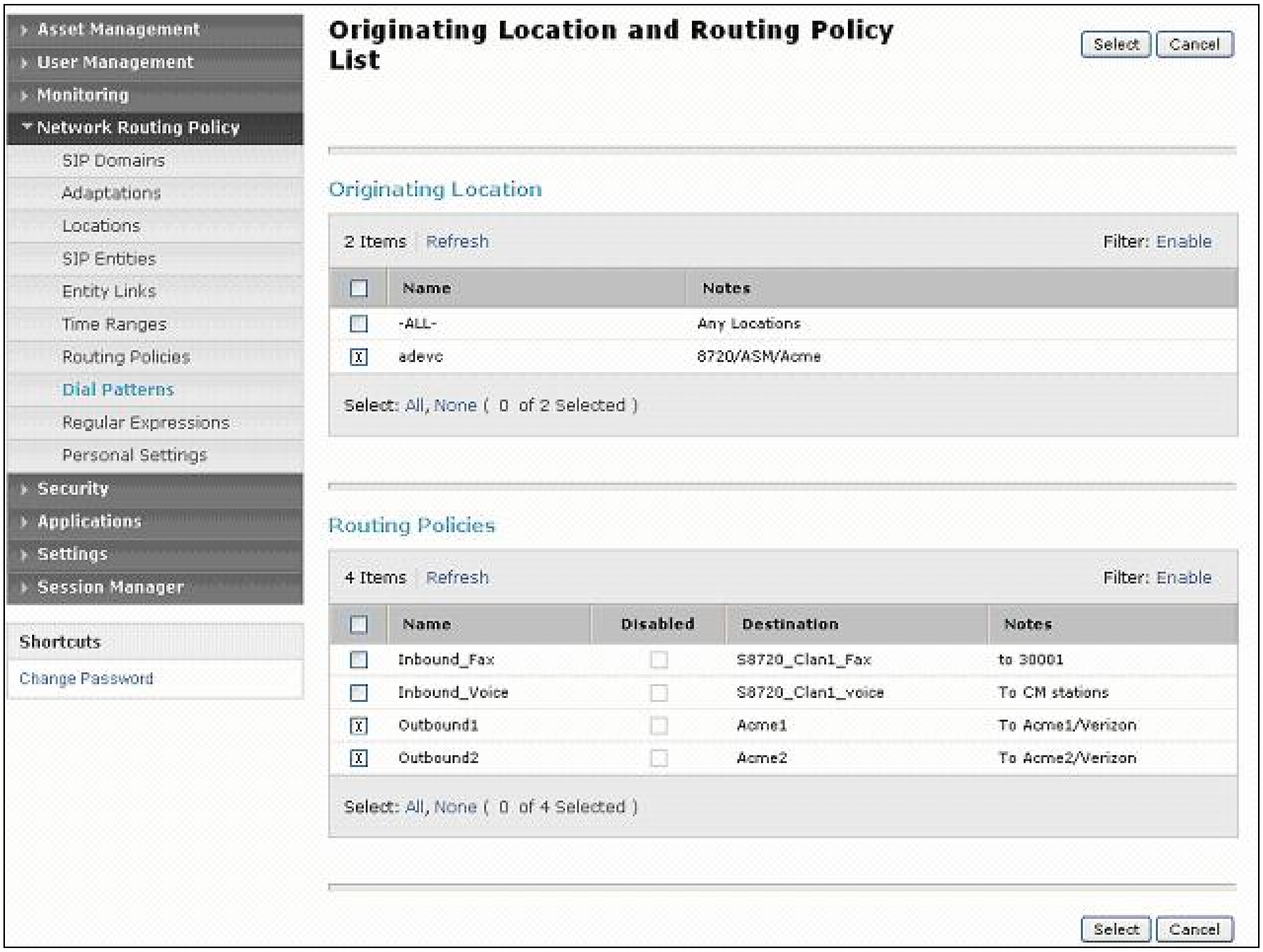


Figure 55: Dial Pattern Details – Originating Locations and Routing Policies

In the reference configuration a request URI of *732852xxxx@adevc.avaya.globalipcom.com* would match and be sent to Acme1 or Acme2.

3. Click the **Commit** button
4. Repeat steps 1 thru 3 for the remaining Dial Patterns. The completed Dial Pattern screen will look like **Figure 53**.

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 56** 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.
4. Click the **Save** button and the completed form shown in **Figure 56** will be displayed.

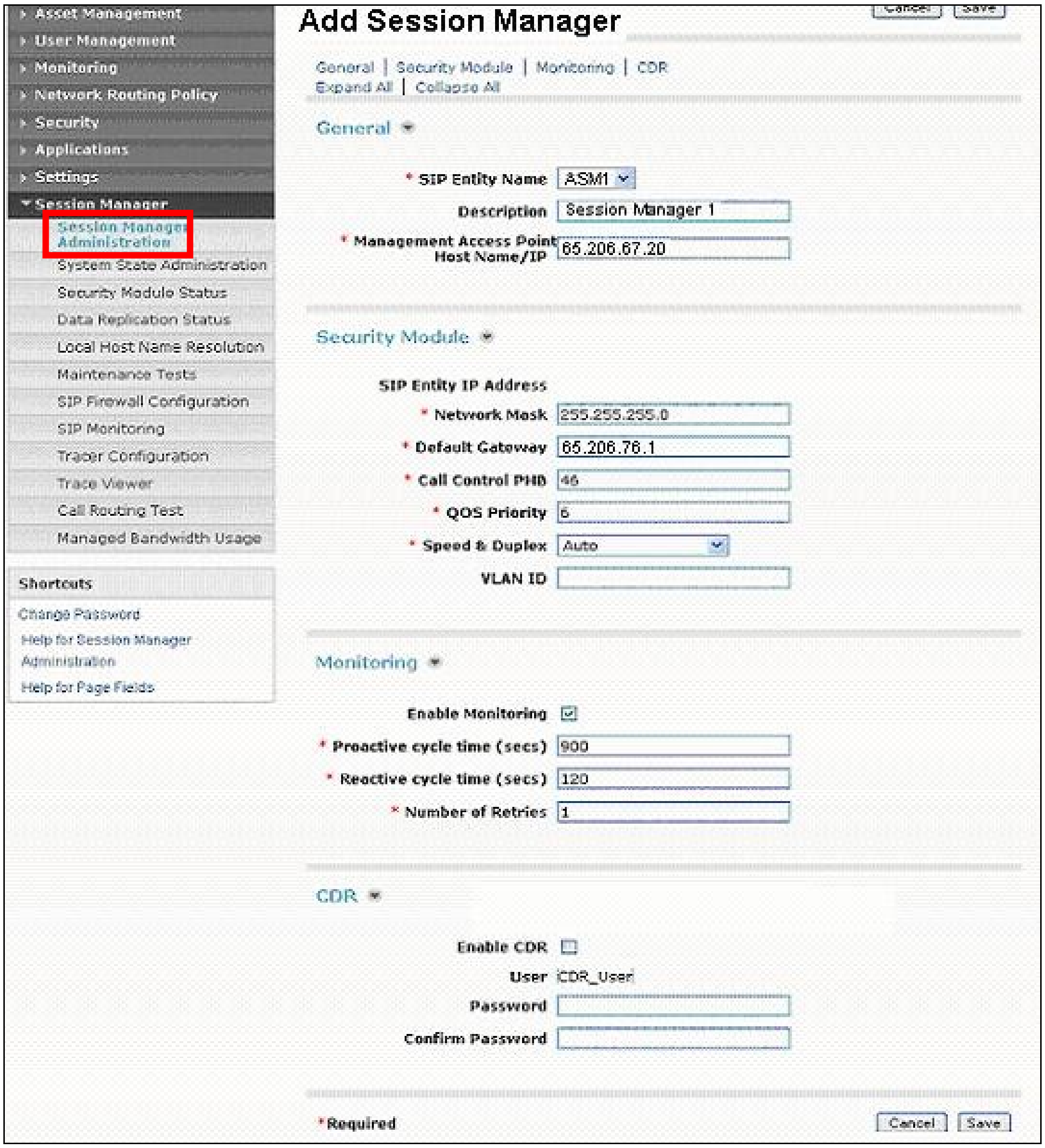


Figure 56: Add Session Manager

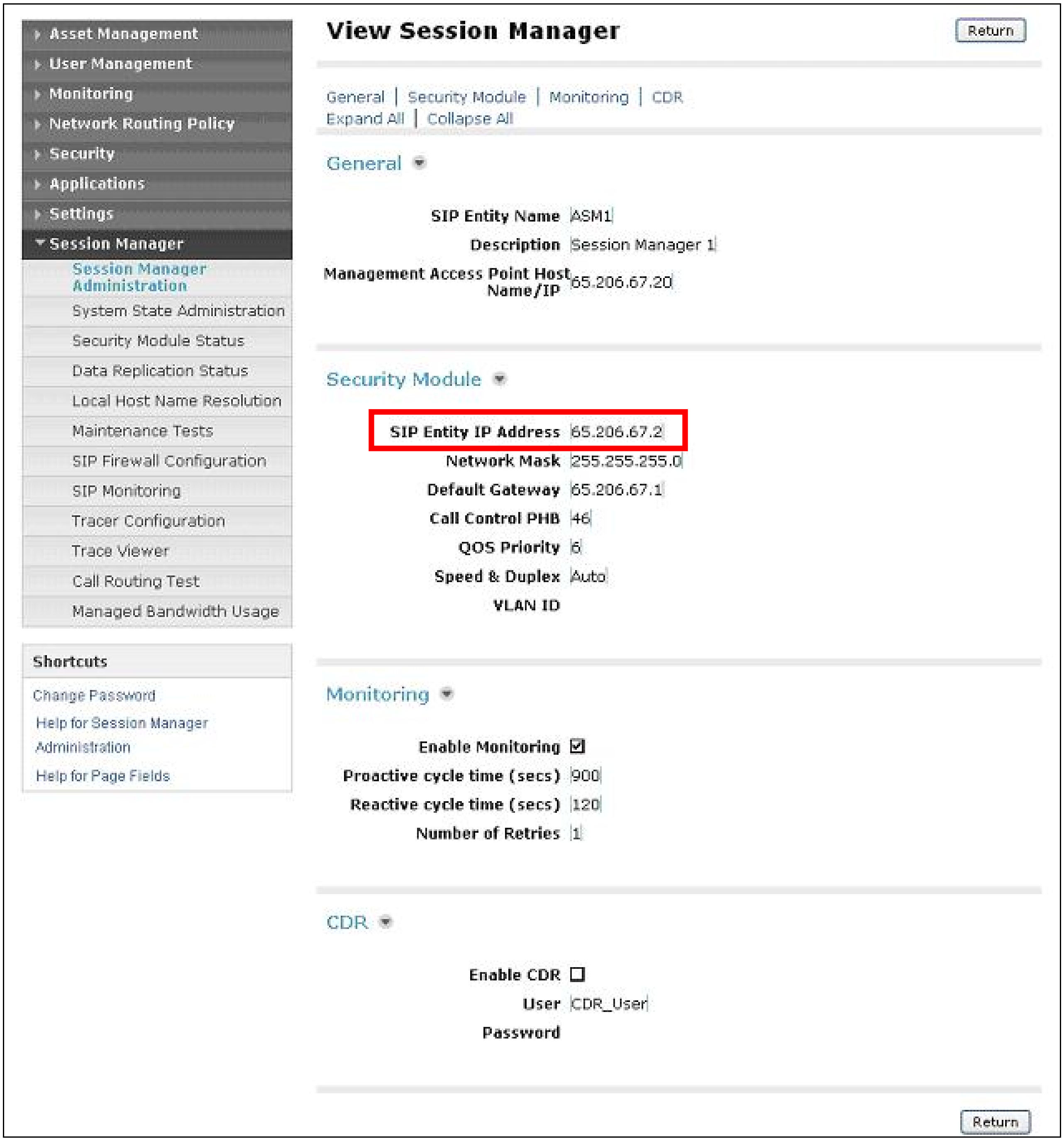


Figure 57: Completed Session Manager Form

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

As described in **Section 1**, Verizon Business IP Trunking supports a redundant (2-CPE) architecture that provides for redundant SIP trunk access between the Verizon Business IP Trunk service offer and the Avaya SIP trunk architecture customer premises equipment (CPE). In the reference configuration two Acme Packet Session Border Controllers (SBCs) were used to provide the 2-CPE redundant access. Both Acme Packet SBCs are provisioned with identical configurations except where noted in the following Sections (e.g. IP addressing).

Note – The 2-CPE redundant configuration is not the same as the Acme Packet high-availability configuration. In the 2-CPE configuration, the two Acme Packet SBCs are independent devices that are redundant in the sense that they provide alternate access between Verizon and the Avaya CPE. Acme Packet high-availability calls for two fully synchronized Acme Packet SBCs that share configurations and operational states.

5.1. Acme Packet Service States

In the reference configuration one Acme Packet SBC is identified as the "Primary" and the other is identified as the "Secondary". These names refer to the selection process by the Avaya Aura™ Session Manager (outbound calls) and the Verizon service node (inbound calls). Both Acmes request and provide service states by sending out and responding to, SIP *OPTIONS* messages. Acme Packet 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

If the Primary Acme Packet fails to respond to the Avaya Aura™ Session Manager or Verizon OPTIONS message, the calls will be sent to the Secondary Acme Packet instead. Once the Primary Acme Packet does respond, it will be used again instead of the Secondary Acme.

5.2. Acme Packet Network Interfaces

Figure 58 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**.

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

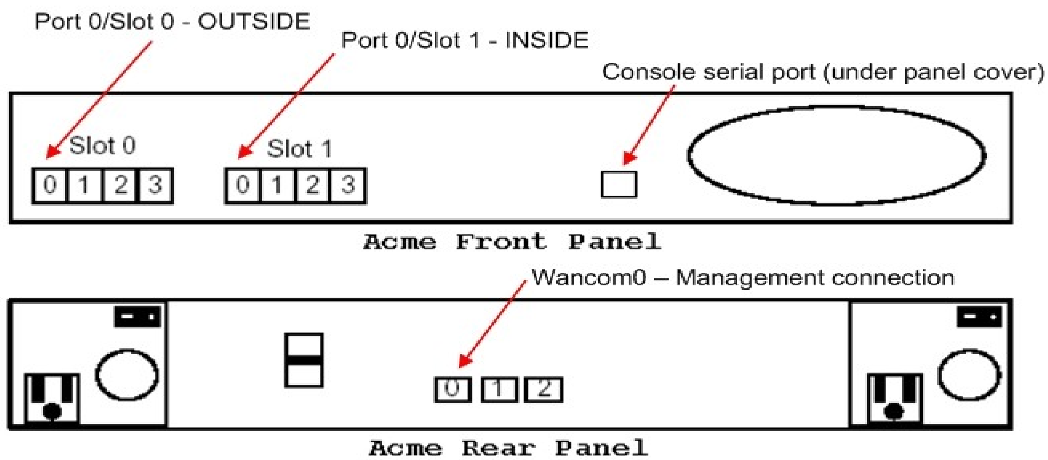


Figure 58: Acme Packet Network Interfaces

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 **[12 & 13]**.

Note – The following Sections describe the provisioning of the Primary Acme Packet SBC. The configuration of the Secondary Acme Packet is identical unless otherwise noted.

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 **start-time → 0000**
   j. Enter **end-time → 2400**
   k. Enter **days-of-week → U-S**
   l. Enter **app-protocol → SIP**
   m. Enter **state → enabled**
   n. Enter **exit**
   o. 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**

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 → NAT_IP**
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 **access-control-trust-level → high**
   f. Enter **invalid-signal-threshold → 0**
   g. Enter **maximum-signal-threshold → 0**
   h. Enter **untrusted-signal-threshold → 0**
   i. Enter **exit**
   j. 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

1. Create a session-agent for the outside network.
   a. Enter **session-router → session-agent**
   b. Enter **hostname → pcelban0001.avayalincroft.globalipcom.com**
   c. Enter **ip-address → 172.30.209.21**
   d. Enter **port → 5071**
   e. Enter **state → enabled**
   f. Enter **app-protocol → SIP**
   g. Enter **transport-method → UDP**
   h. Enter **realm-id → OUTSIDE**
   i. Enter **description → To Verizon**
   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 → pcelban0001.avayalincroft.globalipcom.com**
   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 History-Info 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.

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 History Info Header

1. Enter **session-router → sip-manipulation → header-rule**
2. Enter **name → manipHistInfo**
3. Enter **header-name → History-Info**
4. Enter **action → manipulate**
5. Enter **comparison-type → case-sensitive**
6. Enter **msg-type → request**

7. Enter **element-rule →**
    a. Enter **name → HISTORYINFO**
    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**
8. Enter **exit**
9. Enter **done**

5.3.11.5 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**

5.3.12 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 → 172.30.209.21:5071**
4. Enter **application-protocol → SIP**
5. Enter **transport-protocol → UDP**
6. Enter **access → permit**
7. Enter **exit**
8. 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 IP Trunk Service Offer Configuration

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

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

6.1. Fully Qualified Domain Name (FQDN)s

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

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

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 Private IP (PIP) IP Trunk 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 59: 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 60: 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 61: 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 62: 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 **0/4** in **Figure 62**), indicating that they are all reachable for call routing.

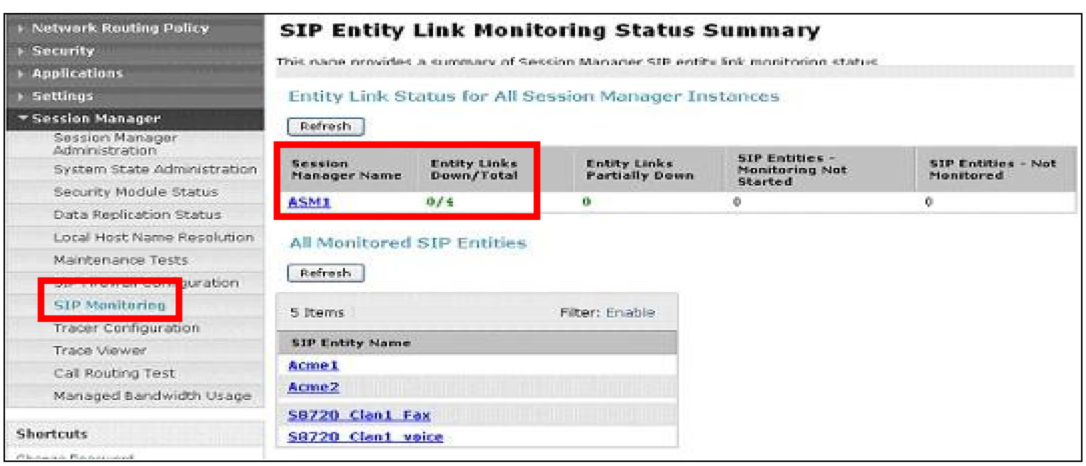


Figure 62: SIP Entity Link Monitoring - Summary

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

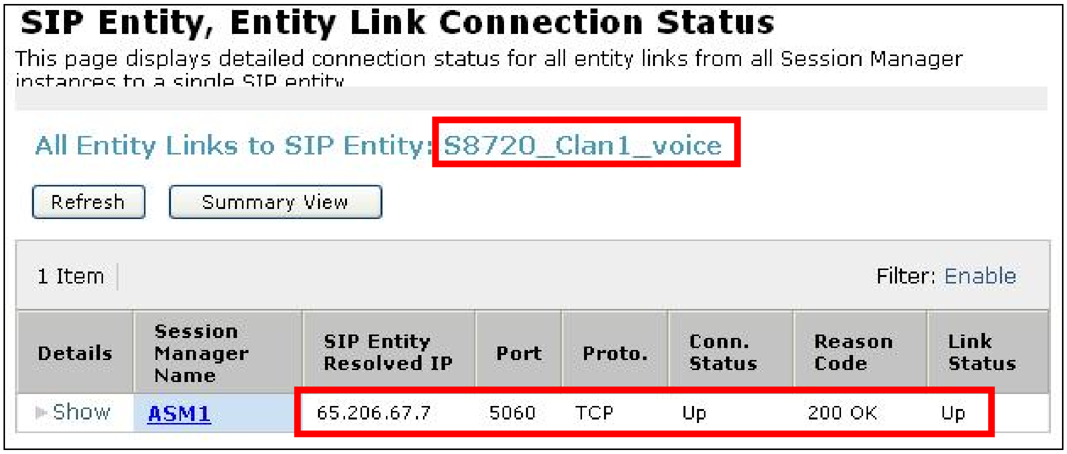


Figure 63: SIP Entity Link Connection Status

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 64: 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 7328523168 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 DID (7329450228) prior to the routing policies being applied, therefore the DID 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** – **7329450228@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**).

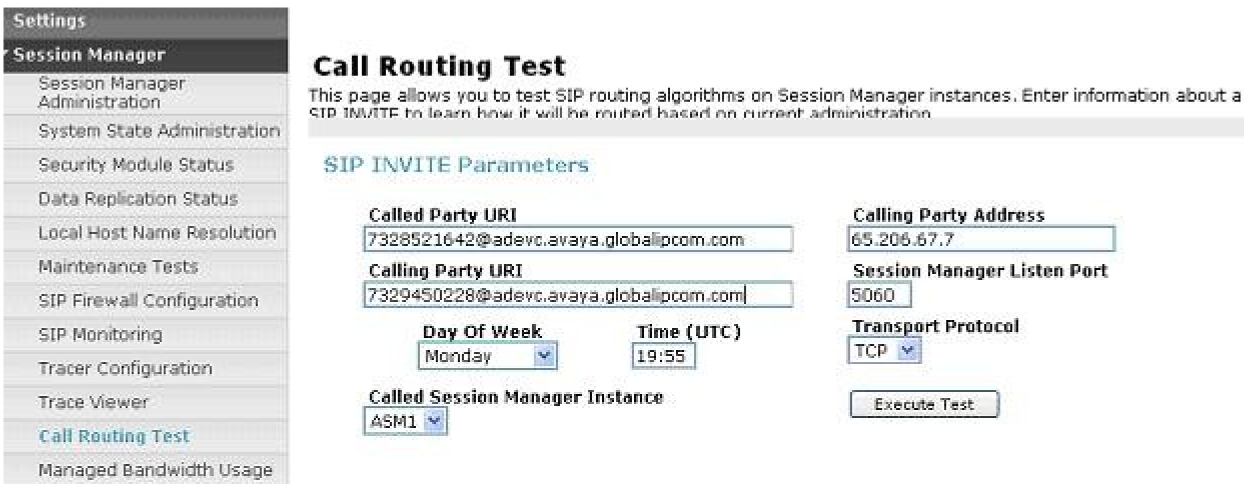


Figure 65: Call Routing Test

Then click on the **Execute Test** button. 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 or Acme2. The next heading Routing Decision Process shows all the routing algorithm calculations.

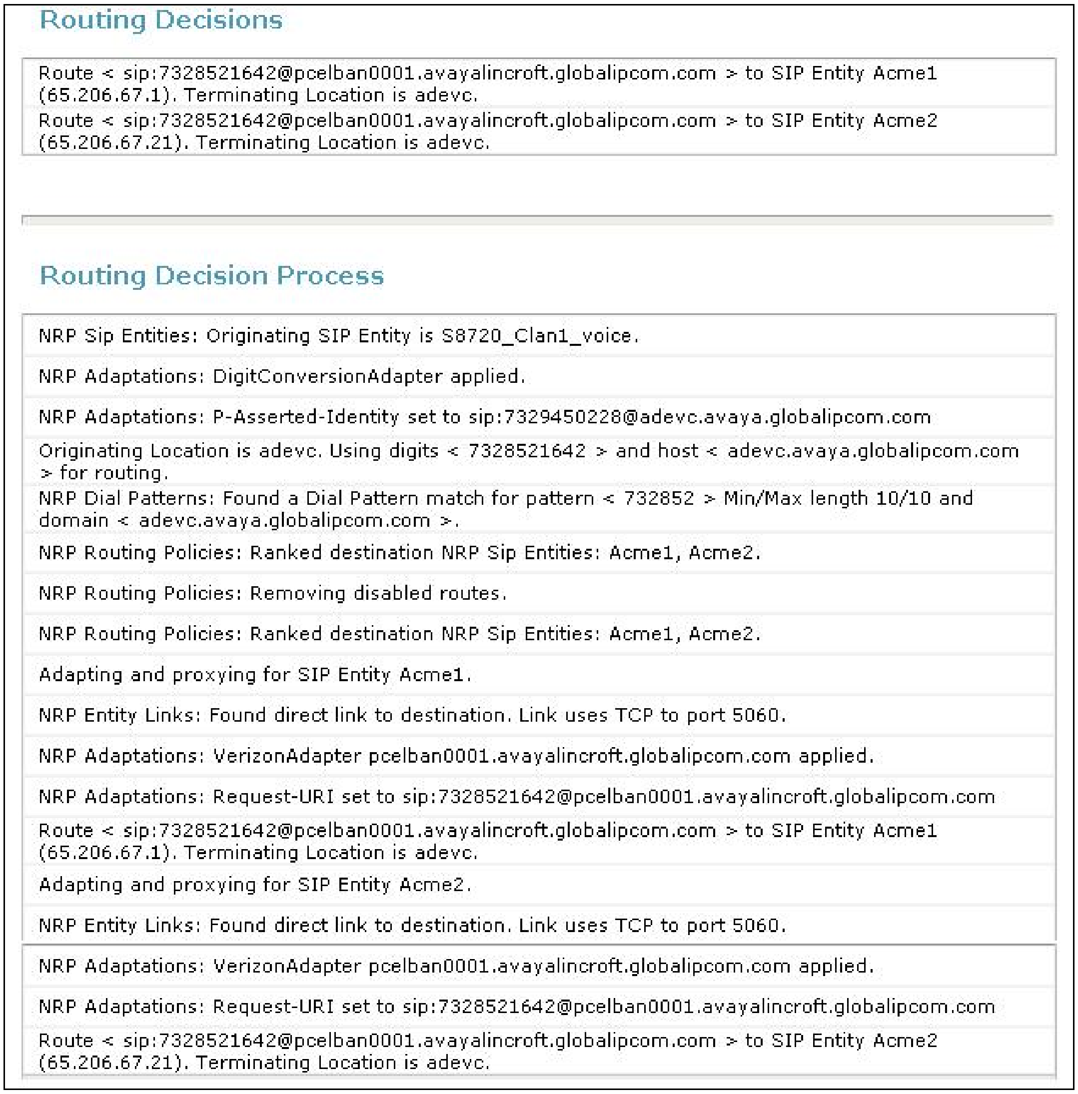


Figure 66: Call Routing Test - Results

7.3. Verification Call Scenarios

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

- Inbound and outbound basic voice calls between various telephones on the Avaya Aura™ Communication Manager and PSTN can be made in both directions using G.711MU and/or G.729A codecs.
  - Avaya One-X Communicator (H.323 Softphone) and Avaya IP Softphone (H.323) as well as traditional analog and digital TDM phones.
- Inbound and outbound Fax calls between Avaya Aura™ Communication Manager and PSTN can be made in both directions using G.711MU codec.
- Direct IP-to-IP Media (also known as "Shuffling") when applicable.
- DTMF Tone Support.
- Additional PSTN numbering plans (e.g. International, 0, 411).

- Verizon Business IP Trunk service 2-CPE architecture (dual Acme Packet 3800 Session Border Controllers at the CPE), including Verizon inbound call fail-over between the dual Acme Packet SBC.
    - Avaya Aura™ Session Manager selects Primary, then Secondary Acme Packet SBC for outbound calls to PSTN.
    - Verizon Business IP Trunk service selects Primary, then Secondary Acme Packet SBC for inbound calls from PSTN.
- Supplementary calling features were verified. The supplementary calling features verified are:
    - Hold, Call transfer, Conference .
    - Voicemail Coverage and Retrieval.
    - SIP Diversion Header for call re-direction.
        - Call Forwarding.
        - Call Coverage.
        - Extend Call.
        - EC500 (call forking).

7.4. Conclusion

As illustrated in these Application Notes, Avaya Aura™ Communication Manager 5.2, Avaya Aura™ Session Manager 1.1, and Acme Packet Session Border Controllers can be configured to interoperate successfully with Verizon Business IP trunk service. This solution provides users of Avaya Aura™ Communication Manager the ability to support inbound and outbound as well as on-net and off-net calling over a Verizon Business IP Trunk public SIP trunk service connection.

This application note further demonstrated that Avaya Aura™ Communication Manager and Avaya Aura™ Session Manager's Verizon Adaptation module could be utilized to convert SIP History Info to SIP Diversion Header in support of establishing off-net call routing over a Verizon Business IP Trunk service connection. This capability now provides users the ability to use application services that utilize off-net call routing, such as Avaya's Extension to Cellular (EC) application feature of Avaya Aura™ Communication Manager, when connecting through Verizon Business IP Trunk service.

Finally, this application note demonstrated that the Verizon Business's "2-CPE" SIP trunk redundancy architecture could be implemented in the enterprise utilizing two Acme Packet Net-Net Session Border Controllers in conjunction with Avaya Aura™ Communication Manager 5.2 and Avaya Aura™ Session Manager 1.1 to support a redundant connection to the Verizon Business IP Trunk service.

8. Addendum 1 – 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	*Outbound1*
866xxxxxxx	Clan	*Outbound2*
866xxxxxxx	Acme1	*Inbound_Voice*
866xxxxxxx	Acme2	*Inbound_Voice*

Table 9

- If 866xxxxxxx is sent by Location "Clan", route the call outbound using the Routing Policy *Outbound1* (Acme1) or *Outbound2* (Acme2).
- If 866xxxxxxx is sent by either Location "Acme1" or "Acme2", route the call inbound using the Routing Policy *Inbound_Voice* (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 67**.

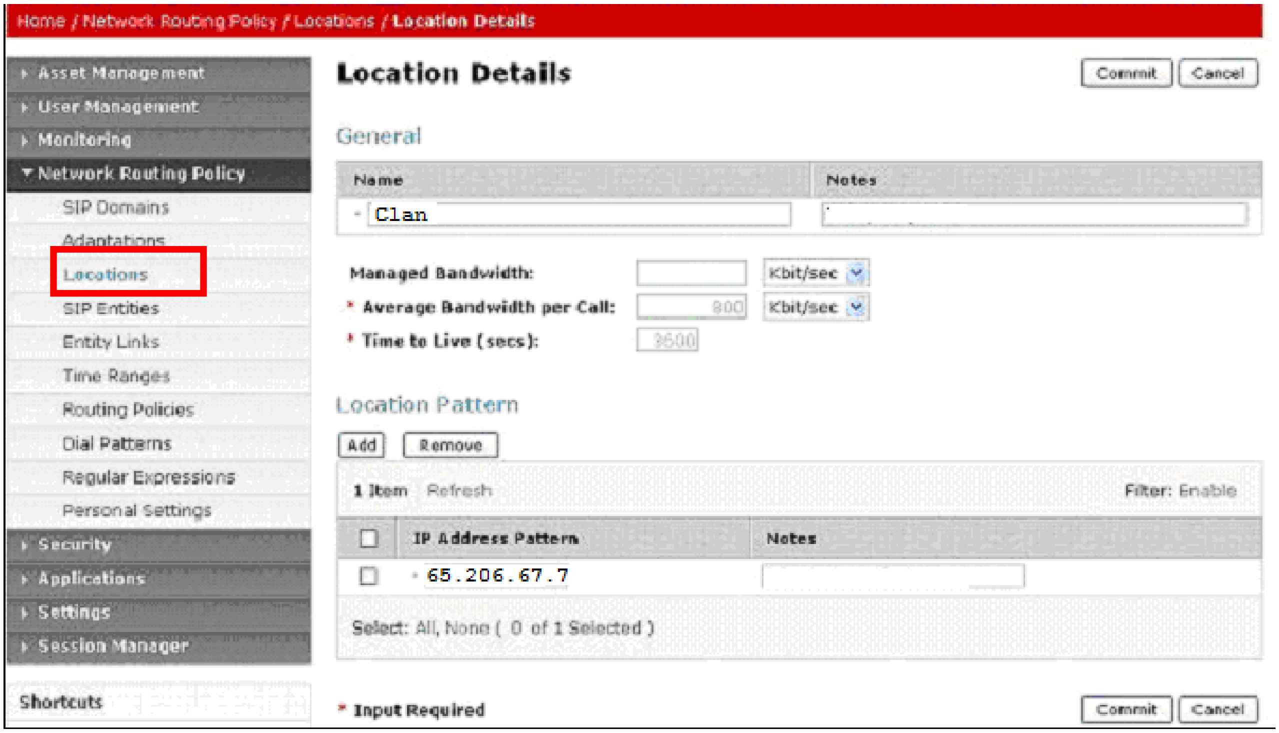


Figure 67: Adding Location "Clan"

8. Repeat steps 3 thru 7 to add Locations for Acme1 and Acme2.

The completed Location form will look like **Figure 68**.

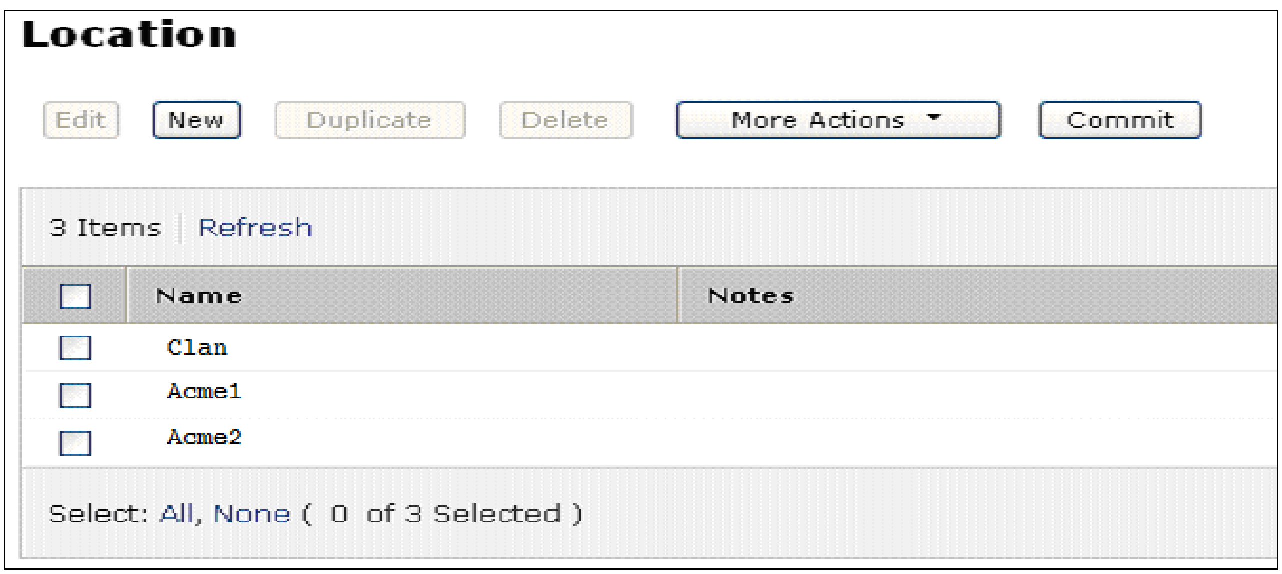


Figure 68: Completed Location Form

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 69** 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 69: Dial Pattern Details - General

2. **Originating Locations and Routing Policies** Section
   a. Click on the Add button and the window in **Figure 70** 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 9** and **Section 4.3.7**).

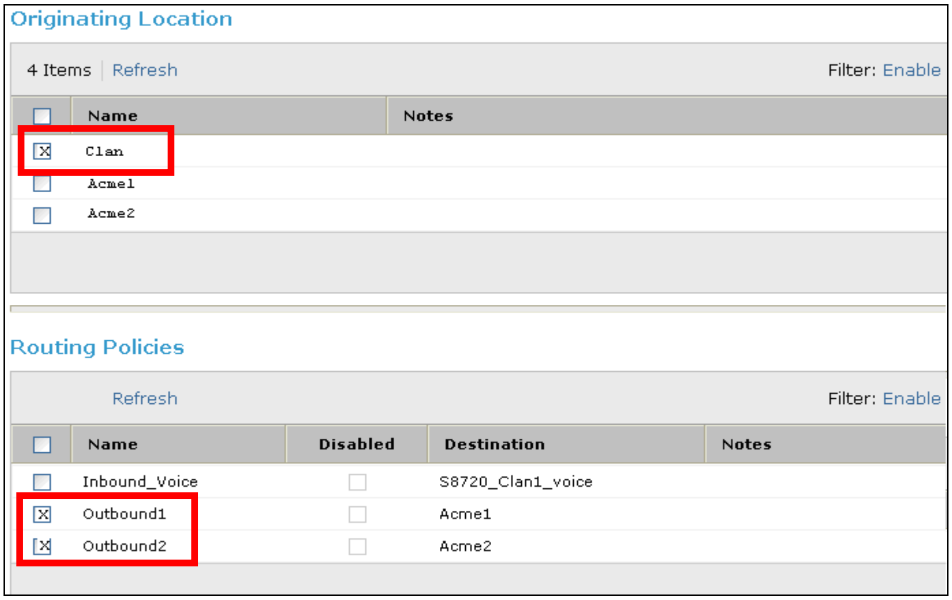


Figure 70: Dial Pattern Details – Originating Locations and Routing Policies

d. Click on the **Select** button and repeat **steps a** thru **c** specifying **Acme1** as the Originating Location and Routing Policy **Inbound_Voice**.
e. Click on the **Select** button and repeat **steps a** thru **c** specifying **Acme2** as the Originating Location and Routing Policy **Inbound_Voice**.

5. Click the **Commit** button
6. The completed Dial Pattern screen will look like **Figure 71**.

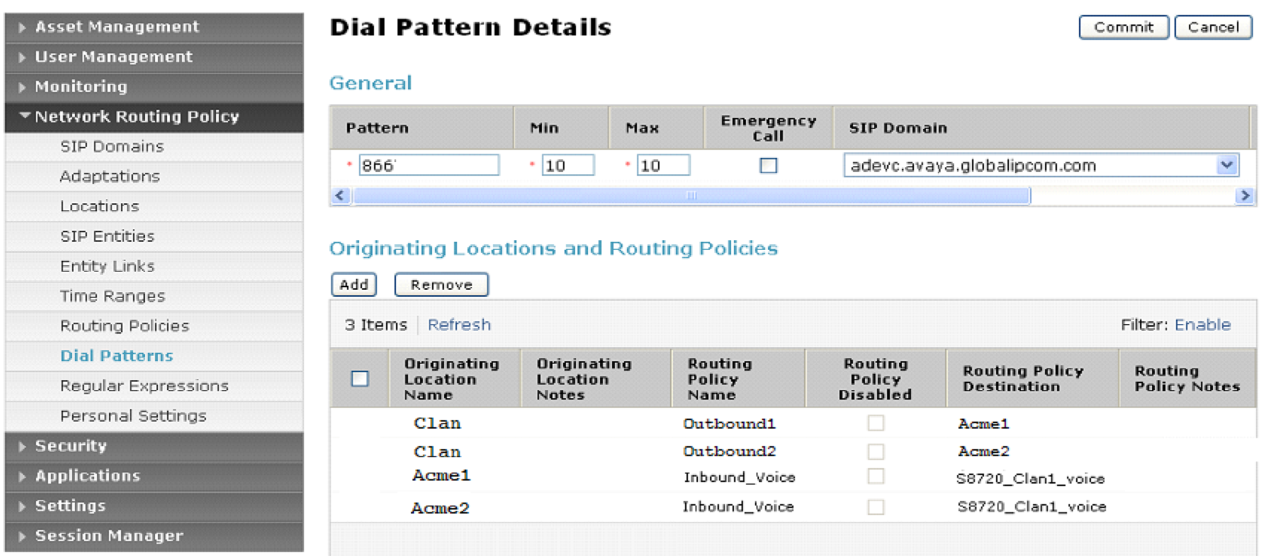


Figure 71: Completed Dial Pattern Form

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 IP Trunk service 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] *Avaya Aura™ Session Manager Overview, Doc ID 03-603323.*

[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] *Application Notes for Configuring the Avaya SIP Trunk Architecture with the Verizon Business IP Trunk service offer in a SIP Trunk Redundant (2-CPE) Environment. – Issue1.0*

[7] *Feature Description and Implementation for Avaya Communication Manager, 555-245-205, Issue 6, January 2008*

10.2. Verizon Business

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

[8] *Verizon Business Product Integration requirement Avaya IP-PBX 5.1 SIP TRUNK Interoperability Testing, Date:10/10/08, Rev 1.1*

[9] *Retail VoIP Interoperability Test Plan version 1.8*

[10] *Network Interface Specification Retail VoIP Trunk Interface (for non-registering devices) Document Version: 3, 2008-08-28*

[11] *Additional information regarding Verizon Business IP Trunk service 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/

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

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

11. Addendum 2 – Supplemental Information for DNS, DSCP, Processor Ethernet, and Alternate Routing

Unless otherwise noted in this addendum, the configuration documented in the main body of these Application Notes remains valid. This addendum is provided as a supplement with expanded coverage of the following topics:

- Use of the Acme Packet Net-Net Session Director to determine the IP Address and Port of the Verizon SIP signaling entities using DNS. See Section 11.3.
- Marking the Differentiated Services Code Point (DSCP) for SIP Signaling messages. See Section 11.4.
- Use of Avaya Aura™ Communication Manager "Processor Ethernet" for SIP signaling from the active Avaya S8720 Server to Avaya Aura™ Session Manager. The "Processor Ethernet" of the Avaya server running Communication Manager may be used for SIP signaling, as an alternative or supplement to the TN799DP C-LAN SIP signaling configuration described in Section 3.1.5 of these Application Notes. Similarly, the addendum illustrates use of an Avaya G450 Media Gateway, as an alternative or supplement to the Avaya G650 Media Gateway configuration. See Section 11.5.
- Expanded coverage of alternate routing considerations for outbound calls, including the use of Communication Manager Look-Ahead Routing. See Section 11.6.

11.1. Updated Software Versions Applicable to Addendum 2

As indicated in the Note below **Table 1** in Section 2, the configuration documented in the main body of these Application Notes remains valid for Avaya Aura™ Communication Manager 5.2.1 and Avaya Aura™ Session Manager 5.2. The following equipment and software were used for the supplemental configuration illustrated in this addendum.

Equipment	Software
Avaya S8720 Servers (Communication Manager)	Avaya Aura™ Communication Manager Release 5.2.1 (016.4) with SP0
Avaya S8300 Server (Communication Manager LSP) in an Avaya G450 Media Gateway	Avaya Aura™ Communication Manager Release 5.2.1 (016.4) with SP0
Avaya S8510 Server (System Manager)	Avaya Aura™ System Manager Release 5.2 (Load 5.2.0.0.520008) with System Platform VSP Patch 1.1.0.4.8
Avaya S8510 Server (Session Manager)	Avaya Aura™ Session Manager Release 5.2 (Load 5.2.0.0.520011)
Avaya 9600-Series Telephones (H.323)	Release 3.1 – H.323
Acme Packet Net-Net 4250 Session Director	nnSC610m2p5.gz

Table 10: Equipment and Software Used in Supplemental Addendum 2 Configuration

11.2. Updated Network Diagram Applicable to Addendum 2

Figure 72 depicts a network similar to the network shown in **Figure 1** and described in Section 2.1.1. Compared to **Figure 1**, **Figure 72** highlights the addition of SIP Signaling using the Avaya S8720 Server "Processor Ethernet" (PE), and the use of an Avaya G450 Media Gateway.

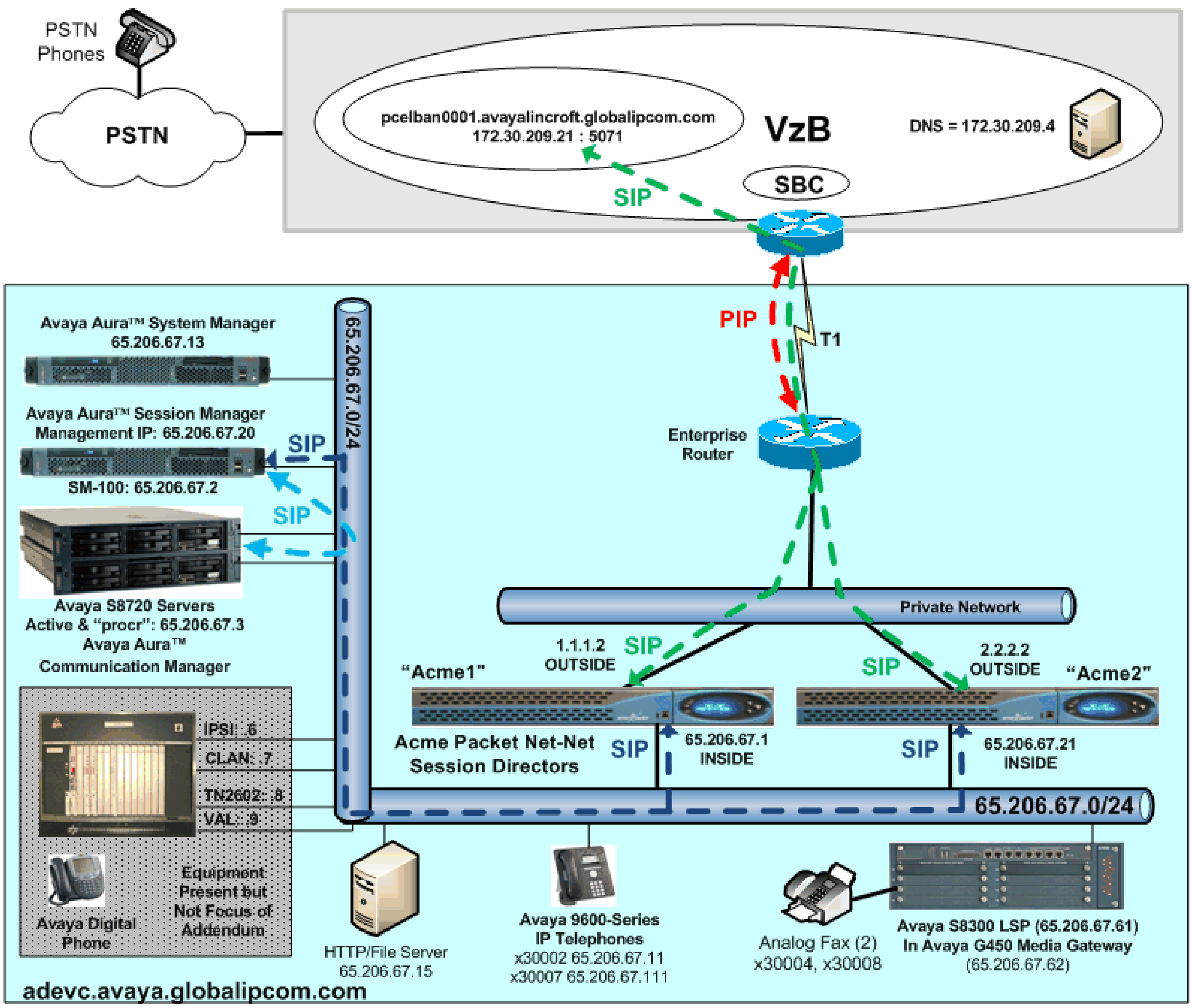


Figure 72: Addendum 2 Configuration using Processor Ethernet and G450 Media Gateway

The color-coded dashed lines with arrows indicate SIP signaling paths. The green dashed line is the SIP signaling path interfacing with Verizon, flowing from the "outside" (i.e., public-facing) interface of the two Acme Packet Net-Net Session Directors to the SIP Service Provider network. The dark blue dashed lines logically connect the "inside" (i.e., private-facing) interfaces of the Acme Packet Session Directors to Avaya Aura™ Session Manager. All inbound and outbound SIP PSTN calls make use of both the green and dark blue paths, and these signaling paths are common between the network shown in **Figure 1** and the network shown in **Figure 72**. In this addendum, inbound and outbound SIP PSTN calls can flow between Communication Manager and

Session Manager along the light blue dashed line using the S8720 PE. Although a mix of C-LAN based SIP trunks and PE SIP trunks are present and can co-exist in a configuration, this addendum focuses on the use of the Avaya S8720 Server PE with Avaya G450 Media Gateway. The Avaya G650 Media Gateway remains physically present in the network, as shown in the grayed-out box in the lower left, but the G650 Media Gateway components, documented in the main body of these Application Notes, are not the topic of this addendum. In many configurations, the use of H.248 Gateways (such as the Avaya G450 Media Gateway or Avaya G430 Media Gateway) with PE can obviate the need for Avaya G650 Media Gateways and the associated IPSI, C-LAN, Media Processor, and Announcement cards.

In the sample configuration, both Acme Packet Net-Net Session Directors signal to the same instance of Session Manager. In production, it may be desirable to have each Session Director signal to a different instance of Session Manager (which in turn could signal to different SIP signaling entities of Communication Manager).

11.3. DNS Procedures with Verizon DNS Server

The Acme Packet Net-Net Session Director can use DNS procedures to look up the Verizon SIP signaling elements and SIP signaling ports. DNS can be used as an alternative to static provisioning of the Verizon IP Address and SIP signaling port in the session agent configuration. Potential benefits of using DNS include:

- Simplified and standardized initial provisioning of the session agent parameters
- Opportunity for automated discovery of new SIP signaling IP Address and port parameters should the service provider make changes or perform maintenance in the network.

If static IP Address and SIP port configuration is initially in place, as documented in Section 5 of these Application Notes, the following approach can be used to enable DNS:

- Add the Verizon-provided DNS Server information to the existing Acme Packet Session Director “OUTSIDE” network interface (i.e., facing Verizon)
- Add a host-route for the Verizon-provided DNS IP Address (e.g., “172.30.209.4”) to route to the proper gateway IP Address
- Edit the existing session-agent to remove the previously configured IP Address and SIP port. In Section 5.3.8.1, the “dest” for the session agent group named “SERV_PROVIDER” is configured with “pcelban0001.avayalincroft.globalipcom.com”. No change is required to the SERV_PROVIDER session agent group. In Section 5.3.7.1, the session agent with this hostname is statically configured with “ip-address” 172.30.209.21 and “port” 5071. This is the session agent that will be modified.

The detailed configuration steps implementing this approach for Acme1 are as follows. Although not detailed below, similar configuration can be performed on Acme2.

1. Configure the Verizon DNS IP Address on the “OUTSIDE” network interface. From the *configure* prompt (steps 1 thru 3 in **Section 5.3**):
   a. Enter **system**
   b. Enter **network-interface**
   c. Enter **select**

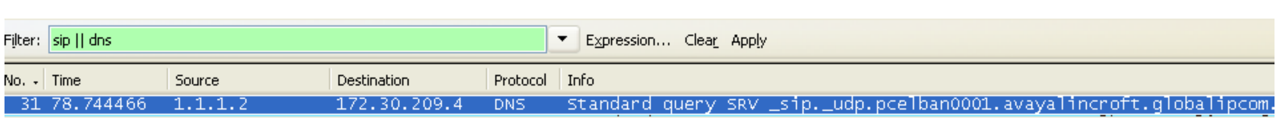
d. Enter **return** at the prompt to make the list appear
e. From the list of network interfaces, select the number of the network interface facing Verizon. In the example configuration, it is M00:0 with IP-address 1.1.1.2
f. Enter **dns-ip-primary 172.30.209.4** /** Verizon DNS Server IP Address **/
g. Enter **dns-domain globalipcom.com**
h. Enter **done**
i. Enter **exit** /** return to system level **/
j. Enter **exit** /** exit configure terminal, save if desired **/

2. Configure a host route for the Verizon DNS IP Address. From the *configure* prompt (steps 1 thru 3 in **Section 5.3**):
k. Enter **system**
l. Enter **host-route**
m. Enter **dest-network 172.30.209.4** /** Verizon DNS Server IP Address **/
n. Enter **netmask 255.255.255.255**
o. Enter **gateway 1.1.1.1** /** Gateway IP for OUTSIDE interface **/
p. Enter **done**
q. Enter **exit** /** return to system level **/
r. Enter **exit** /** exit configure terminal, save if desired **/

3. Remove the IP Address and port from the session agent. From the *configure* prompt (steps 1 thru 3 in **Section 5.3**):
s. Enter **session-router**
t. Enter **session-agent**
u. Enter **select**
v. Enter **return** at the hostname prompt
w. From the list of session agents, select the number of the session agent with hostname "pcelban0001.avayalincroft.globalipcom.com" on the OUTSIDE realm, as configured in Section 5.3.7.1.
x. Enter **ip-address ""** /** double quotes removes the IP Address **/
y. Enter **port 0** /** port 0 removes the port configuration **/
z. Enter **done** /** observe changed session-agent **/
aa. Enter **exit** /** return to session-router level **/
bb. Enter **exit** /** exit configure terminal **/
cc. Enter **save**

Once these configuration changes are activated (e.g., "reboot activate"), the Acme Packet Session Director will use DNS to learn the IP Address and SIP signaling port of the session agent corresponding to the Verizon network.

For example, the following portion of a Wireshark trace shows an example DNS Service Location (SRV) query sourced by the Session Director (1.1.1.2) toward the Verizon DNS server (172.30.209.4).



The following shows details of this DNS SRV query. The Verizon domain "pcelban0001.avayalincroft.globalipcom.com" can be observed in the query.

```
    Source: 1.1.1.2 (1.1.1.2)
    Destination: 172.30.209.4 (172.30.209.4)
⊟ User Datagram Protocol, Src Port: socks (1080), Dst Port: domain (53)
    Source port: socks (1080)
    Destination port: domain (53)
    Length: 77
  ⊟ Checksum: 0xc5ed [validation disabled]
      [Good Checksum: False]
      [Bad Checksum: False]
⊟ Domain Name System (query)
    [Response In: 34]
    Transaction ID: 0x0001
  ⊞ Flags: 0x0100 (Standard query)
    Questions: 1
    Answer RRs: 0
    Authority RRs: 0
    Additional RRs: 0
  ⊟ Queries
    ⊟ _sip._udp.pcelban0001.avayalincroft.globalipcom.com: type SRV, class IN
        Name: _sip._udp.pcelban0001.avayalincroft.globalipcom.com
        Type: SRV (Service location)
        Class: IN (0x0001)
```

The following portion of a Wireshark trace highlights a Verizon response to the DNS SRV query.

Filter: sip || dns   Expression... Clear Apply

No.	Time	Source	Destination	Protocol	Info
31	78.744466	1.1.1.2	172.30.209.4	DNS	Standard query SRV _sip._udp.pcelban0001.avayalincroft.globalipcom.
32	78.862161	172.30.209.4	1.1.1.2	DNS	Standard query response SRV 100 50 5071 pc-n0001-elba.avayalincroft

The following shows details of the Verizon DNS SRV response. Observe that the "answer" includes port 5071, and the Target "pc-n0001-elba.avayalincroft.globalipcom.com".

```
⊟ Queries
  ⊟ _sip._udp.pcelban0001.avayalincroft.globalipcom.com: type SRV, class IN
      Name: _sip._udp.pcelban0001.avayalincroft.globalipcom.com
      Type: SRV (Service location)
      Class: IN (0x0001)
⊟ Answers
  ⊟ _sip._udp.pcelban0001.avayalincroft.globalipcom.com: type SRV, class IN, priority 100, weight 50, port 5071, targ
      Name: _sip._udp.pcelban0001.avayalincroft.globalipcom.com
      Type: SRV (Service location)
      Class: IN (0x0001)
      Time to live: 6 hours
      Data length: 22
      Priority: 100
      Weight: 50
      Port: 5071
      Target: pc-n0001-elba.avayalincroft.globalipcom.com
```

After the DNS SRV response is received, the Acme Packet Session Director will send a DNS A query to determine the IP Address of the "Target" supplied in the DNS SRV response. The following portion of a Wireshark trace shows both the DNS A query (highlighted) and the Verizon response.

Filter: sip || dns   Expression... Clear Apply

No.	Time	Source	Destination	Protocol	Info
35	79.849301	1.1.1.2	172.30.209.4	DNS	Standard query A pc-n0001-elba.avayalincroft.globalipcom.com
36	79.964301	172.30.209.4	1.1.1.2	DNS	Standard query response A 172.30.209.21

The following shows details of the Session Director DNS A query. Observe that the query contains the "Target" supplied by Verizon in the DNS SRV response.

```
⊟ Queries
  ⊟ pc-n0001-elba.avayalincroft.globalipcom.com: type A, class IN
      Name: pc-n0001-elba.avayalincroft.globalipcom.com
      Type: A (Host address)
      Class: IN (0x0001)
```

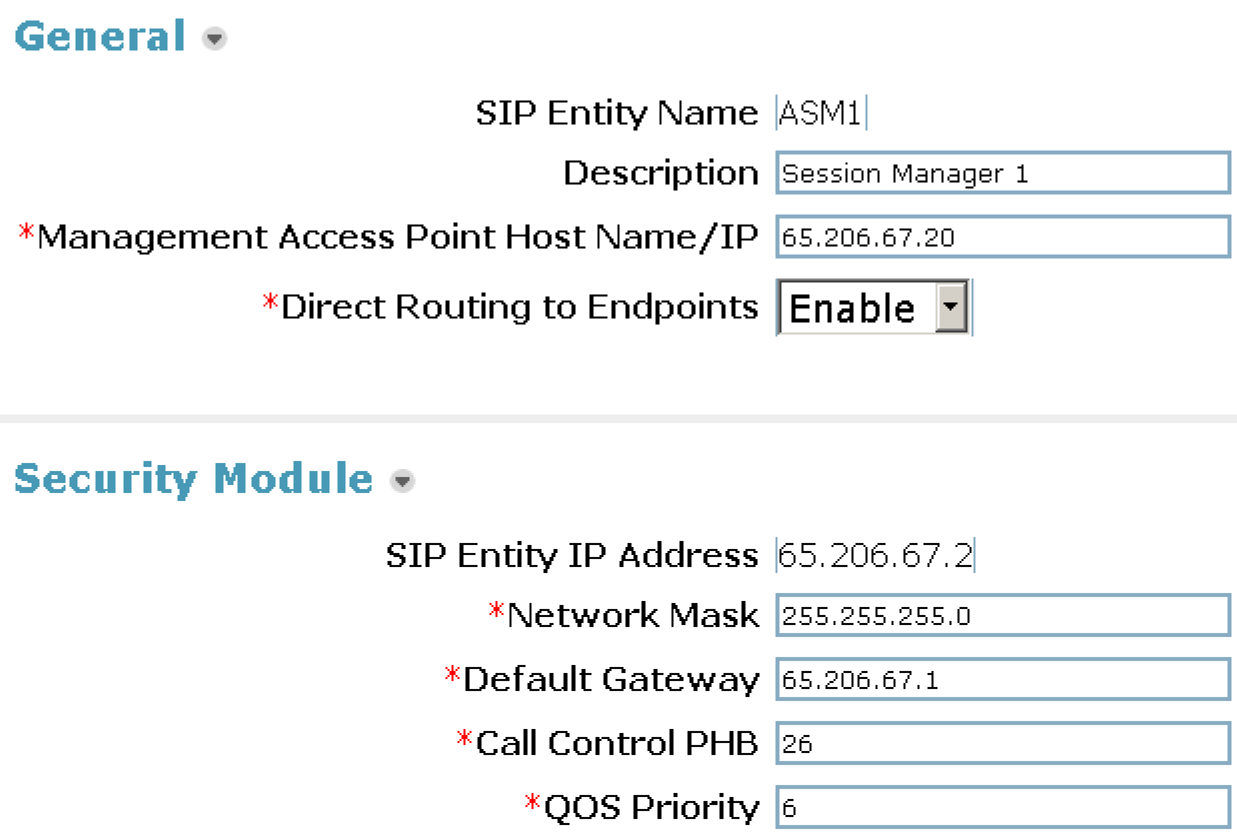
The following shows details of the Verizon DNS A query response. Observe that the answer contains the IP Address 172.30.209.21.

```
⊟ Queries
  ⊟ pc-n0001-elba.avayalincroft.globalipcom.com: type A, class IN
      Name: pc-n0001-elba.avayalincroft.globalipcom.com
      Type: A (Host address)
      Class: IN (0x0001)
⊟ Answers
  ⊟ pc-n0001-elba.avayalincroft.globalipcom.com: type A, class IN, addr 172.30.209.21
      Name: pc-n0001-elba.avayalincroft.globalipcom.com
      Type: A (Host address)
      Class: IN (0x0001)
      Time to live: 6 hours
      Data length: 4
      Addr: 172.30.209.21
```

In sum, the Acme Packet DNS configuration has enabled the Session Director to look up the Verizon IP Address and SIP signaling port. Use of DNS is an alternative to the static provisioning of IP Address and SIP signaling port for the session agent.

11.4. Quality of Service for SIP Signaling

In the enterprise network, all SIP signaling from Avaya Aura™ Session Manager to other SIP entities such as the Acme Packet Net-Net Session Director will be re-marked by Session Manager to a configurable value. To view or change this value, log in to System Manager. The overview provided in Section 4.2 applies, except that the URL to access the browser-based GUI of System Manager is now ***https://<ip-address>/SMGR***, where "<ip-address>" is the IP address of System Manager. Log in with the appropriate credentials. Navigate to **Session Manager → Session Manager Administration.** After selecting the appropriate instance of Session Manager to view or edit, scroll down to the area of the screen with parameters for the Security Module. The parameter "Call Control PHB" (evident in the screen capture below) determines the value of the Differentiated Services Code Point (DSCP) for SIP signaling re-marked by Session Manager.



In the enterprise network, SIP signaling from Avaya Aura™ Communication Manager to the far-end of a SIP signaling group is determined by the "Call Control PHB Value" for the network region of the near-end of the signaling group. For example, for a SIP signaling group whose near-end is a C-LAN in network region 1 (such as signaling group 4 shown in **Figure 19**), the Call Control PHB Value shown for IP Network Region 1 (shown in **Figure 9** in Section 3.1.3.1) will apply. Since all traffic to and from Verizon passes through Session Manager, and Session Manager re-marks all SIP signaling, the DSCP applied to SIP signaling packets by Communication Manager is only relevant to the QoS policies in the enterprise network between Communication Manager and Session Manager.

The approach to marking SIP signaling towards Verizon need not be the same as the approach used in the enterprise network. If desired, the Acme Packet Net-Net Session Director can be configured to mark all SIP signaling towards the Verizon network with a specific Differentiated Services Code Point (DSCP), which may be the same or different from the DSCP used for SIP signaling within the enterprise.

The following approach may be used if a specific DSCP should appear in all SIP signaling towards Verizon:

- Create a named "media-policy" (e.g., "marksip") that will mark all SIP messages with a specific "tos-value"
- Create a named class policy "profile-name" (e.g., "marksip-profile") that applies to the newly created media policy (e.g., "marksip)
- Apply the new "marksip-profile" as the **class-profile** to the realm facing Verizon (e.g., the "OUTSIDE" realm)

The detailed configuration steps implementing this approach for Acme1 are as follows. Although not shown, similar configuration can be performed on Acme2 as well.

1. Create a named "media-policy" called "marksip". From the *configure* prompt (steps 1 thru 3 in **Section 5.3**):
   a. Enter **media-manager**
   b. Enter **media-policy**
   c. Enter **name marksip** /** or desired name **/
   d. Enter **tos-settings**
   e. Enter **media-type message**
   f. Enter **media-sub-type sip**
   g. Enter **tos-value 0x68** /** or desired tos-value **/
   h. Enter **done** /** tos-settings are summarized **/
   i. Enter **exit** /** return to media-policy level **/
   j. Enter **done** /** media-policy named marksip is summarized **/
   k. Enter **exit** /** return to media-manager level **/
   l. Enter **exit** /** exit configure terminal, save if desired **/

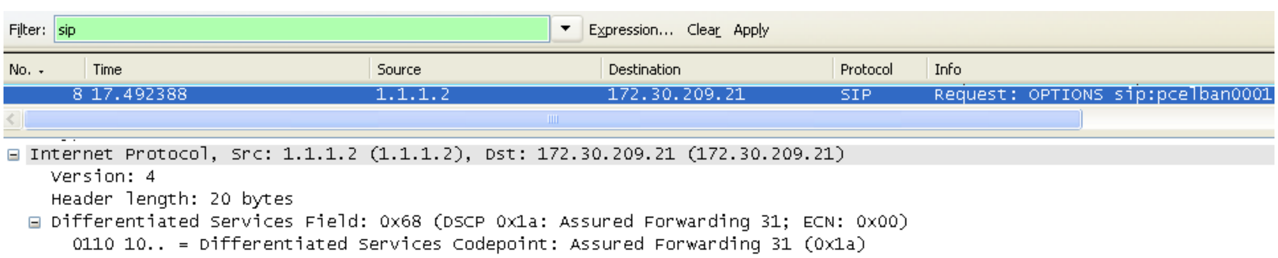
2. Create a named class policy "profile-name" (e.g., "marksip-profile") that applies the media policy named in step 1c above. From the *configure* prompt (steps 1 thru 3 in **Section 5.3**):
   m. Enter **session-router**
   n. Enter **class-profile**
   o. Enter **policy**
   p. Enter **profile-name marksip-profile** /** or desired name **/
   q. Enter **to-address *** /** or more granular if needed **/
   r. Enter **media-policy marksip** /** name configured in Step 1c **/
   s. Enter **done** /** class-policy profile-name marksip-profile is summarized **/
   t. Enter **done**

u. Enter **exit** /** return to class-profile level **/
v. Enter **exit** /** return to session-router level **/
w. Enter **exit** /** exit configure terminal, save if desired **/

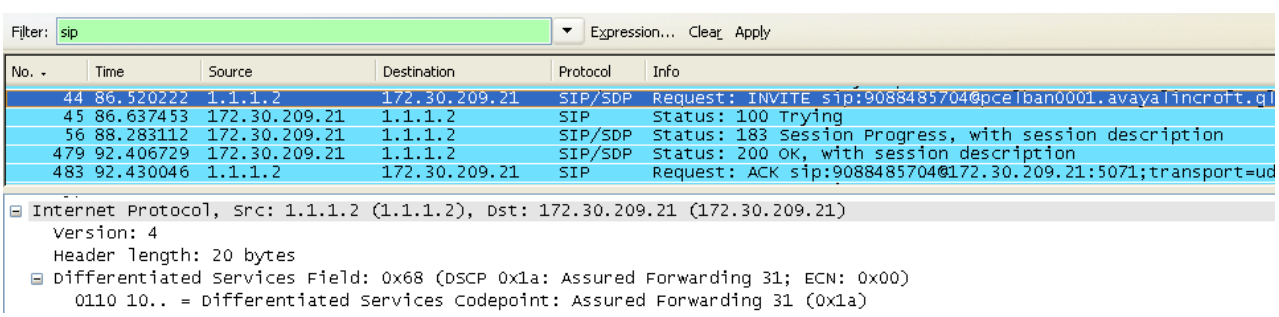
3. Apply the profile named in Step 2p above (e.g., "marksip-profile") as the **class-profile** to the realm facing Verizon (e.g., the "OUTSIDE" realm). From the *configure* prompt (steps 1 thru 3 in **Section 5.3**):
   x. Enter **media-manager**
   y. Enter **realm-config**
   z. Enter **select** and return, then select the number of the OUTSIDE realm
   aa. Enter **class-profile marksip-profile** /** name configured in Step 2p **/
   bb. Enter **done** /** realm-config for OUTSIDE realm is summarized **/
   cc. Enter **exit** **/** return to media-manager level **/**
   dd. Enter **exit** **/** exit configure terminal **/**
   ee. Enter **save**

Once this configuration is activated ("activate-config"), all SIP signaling towards Verizon will be marked with the "tos-value" specified in step 1g above. The configure "tos-value" 0x68 corresponds to DSCP decimal value 26 (0x1a), which would be decoded by Wireshark as "Assured Forwarding 31".

For example, the following portion of a Wireshark trace shows an example SIP OPTIONS sourced by the Session Director, once this configuration has been activated:



As another example, the following portion of a Wireshark trace shows an example outbound call where the SIP INVITE sent to Verizon is expanded to show this same configured DSCP.



If desired, this same approach can be used to re-mark all SIP signaling packets toward Session Manager on the INSIDE realm.

11.5. Using S8720 Server Processor Ethernet and G450 Media Gateway

This section illustrates an example configuration allowing SIP signaling via the "Processor Ethernet" of the Avaya S8720 Servers to Session Manager. This section is not intended to be procedural or prescriptive.

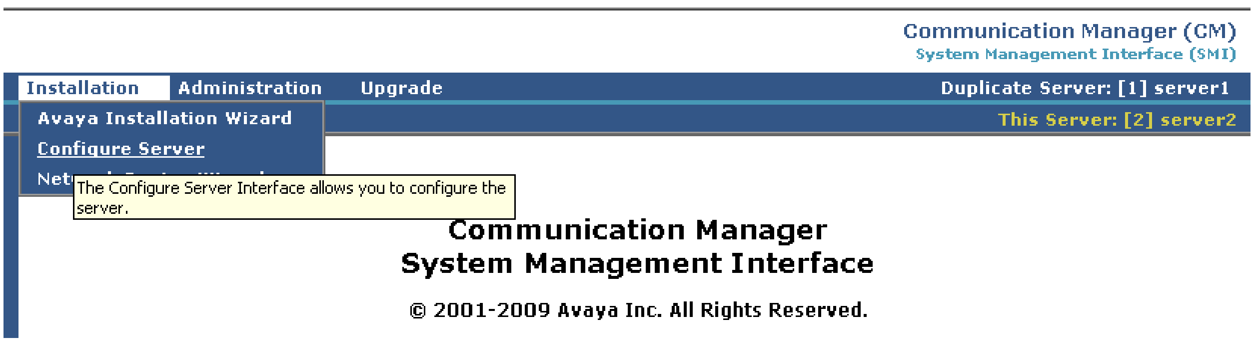
11.5.1 Communication Manager Configuration

Except for the web configuration shown in Section 11.5.1.1, all remaining configuration is performed via the Communication Manager SAT interface of the active Avaya S8720 Server. Screens are abridged for brevity in presentation.

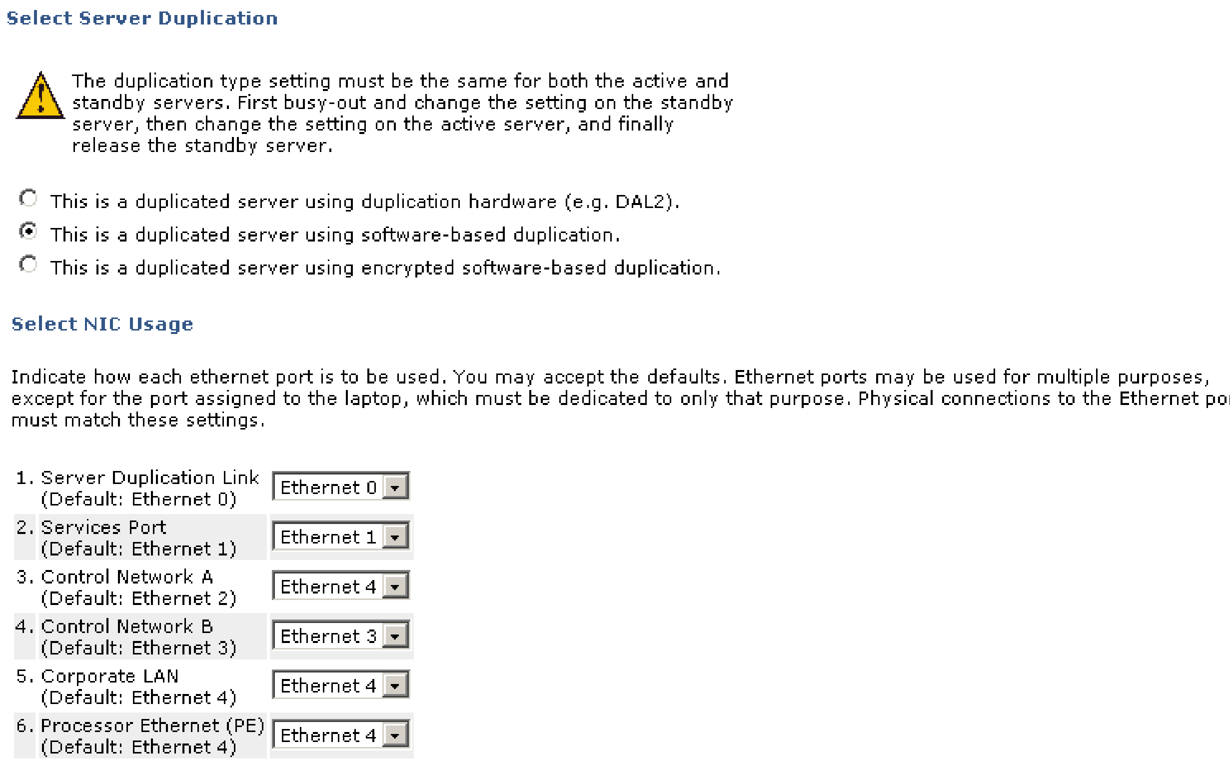
11.5.1.1 Processor Ethernet Configuration on S8720 Servers

The Processor Ethernet must be configured via the "Configure Server" Web pages on both S8720 servers. The screens in this section illustrate a previously completed configuration on only one of the servers. Consult product documentation for further procedural guidance (e.g., performing changes on the standby server to mitigate service disruptions). Reference [PE] also contains a procedural example for adding Processor Ethernet.

The S8720 Server can be accessed via a web interface in an internet browser. To add Processor Ethernet to an existing configuration, select **Configure Server** under **Installation**, as shown.



Navigate to **Set Identities**. The following screen shows a portion of the **Set Identities** screen. Note that the **Processor Ethernet (PE)** is assigned to the same interface as the Corporate LAN.



Select the **Continue** button to proceed. The screen below shows a portion of the resulting screen, with the IP Addresses from the sample configuration populated in the mandatory fields, indicated by a red star. The "active server" IP Address is 65.206.67.3. This is the IP Address that will be associated with the Processor Ethernet (PE) or "procr" of the active S8720 Server. Avaya Aura™ Session Manager will have a SIP Entity and SIP Entity Link for 65.206.67.3.

Ethernet 4: Control Network A, Processor Ethernet (PE), Corporate LAN Interface

IP address server1 (server1)	65.206.67.4 *
IP address server2 (server2)	65.206.67.5 *
Alias IP address, active server (server)	65.206.67.3 *
Gateway	65.206.67.1 *
Subnet mask	255.255.255.0 *
Speed *(Current speed : AUTO SENSE)*	AUTO SENSE *

☐ Enable VLAN 802.1q priority tagging

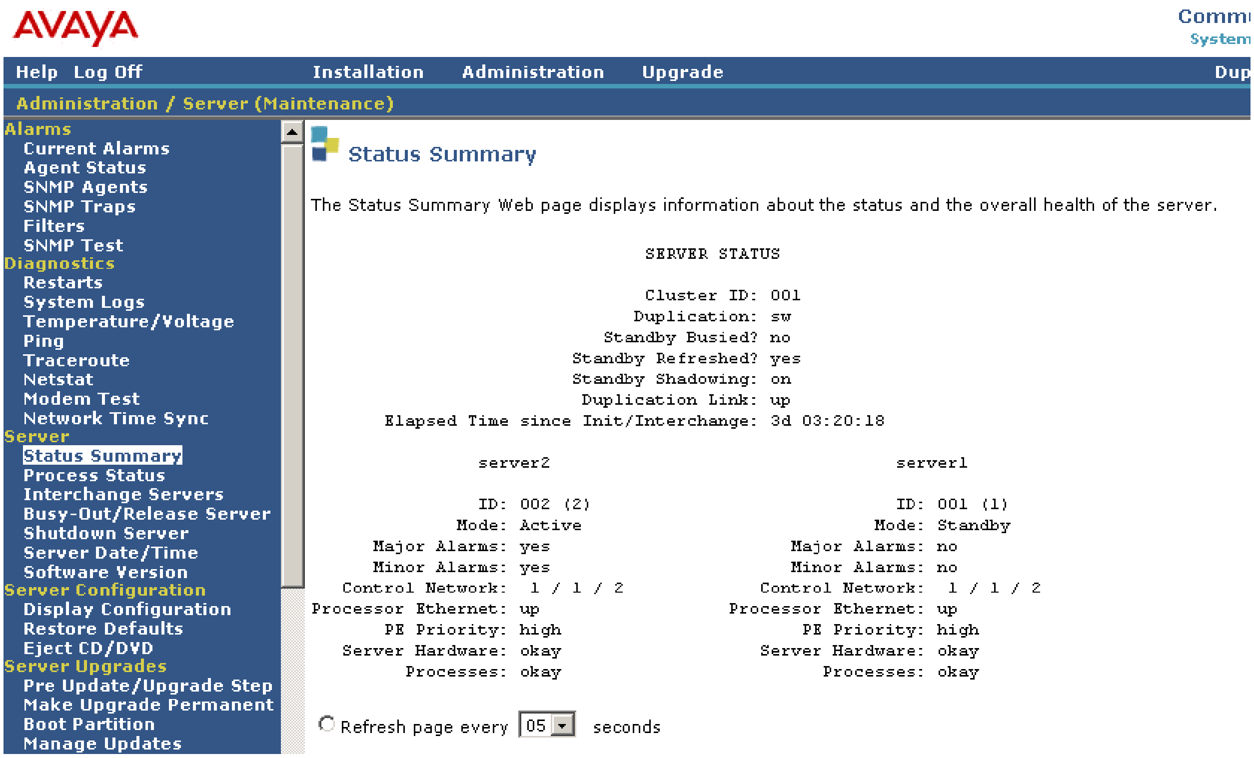
Processor Ethernet (PE) Parameters:

PE Interchange Priority:	◉ HIGH ○ EQUAL ○ LOW ○ IGNORE
IP address for PE Health Check:	65.206.67.1 *

Click **Change** to change values.

Change | Close Window | Help

The **Status Summary** page from the Maintenance web interface may be used to check the Processor Ethernet status, as shown below with the status “up”.



11.5.1.2 Node Names

Node names are mappings of names to IP Addresses that can be used in various screens. The following abridged list output (from the active S8720 Server) shows some of the relevant node-names in the sample configuration. As shown in bold, the node name for Avaya Aura™ Session Manager is “ASM” with IP Address 65.206.67.2, and other node names are also identical to **Figure 6** in the main body of these Application Notes. The node name and IP Address for the Processor Ethernet “procr” appears automatically due to the web configuration in Section 11.5.1.

```
list node-names all
                        NODE NAMES
Type      Name              IP Address
IP        ASM               65.206.67.2
IP        GW1-CLAN1         65.206.67.7
IP        GW1-MEDPRO1       65.206.67.8
IP        Gateway001        65.206.67.1
IP        S8300-LSP         65.206.67.61
IP        VAL               65.206.67.9
IP        procr             65.206.67.3
```

11.5.1.3 IP Interface for procr

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

```
change ip-interface procr                                            Page   1 of   1
                                  IP INTERFACES
                  Type: PROCR
                                                       Target socket load: 19200
      Enable Interface? y                          Allow H.323 Endpoints? y
                                                    Allow H.248 Gateways? y
        Network Region: 1                            Gatekeeper Priority: 1
                                 IPV4 PARAMETERS
             Node Name: procr
           Subnet Mask: /24
```

The following screen lists the IP interfaces, which now includes the bold "procr" at the end of the list.

```
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
 y VAL    01A06 TN2501        VAL              /24   Gateway001            n
                              65.206.67.9
 y PROCR                      65.206.67.3      /24   65.206.67.1      1
```

11.5.1.4 Network Regions for Gateway, Telephones

Network regions provide a means to logically group resources. In the example in this addendum, the Avaya G450 Media Gateway is in region 4, and other resources are located in other regions. For example, as per the main body of these Application Notes, there is a G650 Media Gateway whose resources are in network region 1.

Non-IP telephones (e.g., analog, digital) derive network region and location configuration from the Avaya gateway to which the device is connected. The following display command shows that media gateway 2 is an Avaya G450 Media Gateway configured for network region 4.   It can also be observed that the "Controller IP Address" is the Avaya S8720 processor Ethernet (65.206.67.3). This field is not configured, but rather simply displays the current controller for the gateway.

```
change media-gateway 2                                          Page   1 of   1
                              MEDIA GATEWAY
         Number: 2                           Registered?  y
           Type: g450              FW Version/HW Vintage: 30 .10 .3  /1
           Name: G450-BR1                 MGP IP Address: 65 .206.67 .62
      Serial No: 08IS35173859      Controller IP Address: 65 .206.67 .3
   Encrypt Link? y                           MAC Address: 00:1b:4f:03:42:d8
 Network Region: 4    Location: 2             Enable CF? n
                                               Site Data:
  Recovery Rule: none

Slot   Module Type            Name                   DSP Type  FW/HW version
 V1:   S8300                  ICC MM                 MP80      29   3
 V2:   MM712                  DCP MM
 V3:   MM710                  DS1 MM
 V4:   MM711                  ANA MM
 V5:
 V6:
 V7:
 V8:   MM710                  DS1 MM               Max Survivable IP Ext: 8
 V9:   gateway-announcements  ANN VMM
```

IP telephones can be assigned a network region based on an IP address mapping. The network region can also associate the IP telephone to a location for location-based routing decisions. The following screen illustrates a subset of the IP network map configuration used to verify this addendum. If the IP address of a registering IP Telephone does not appear in the ip-network-map, the phone is assigned the network region of the "gatekeeper" (e.g., CLAN or PE) to which it registers. When the IP address of a registering IP telephone is in the ip-network-map, the phone is assigned the network region assigned by the form shown below. In the sample configuration, Avaya IP Telephones logically associated with the Avaya G450 Media Gateway site are mapped to network region 4, the same region as the G450 gateway. For example, the specific IP address 65.206.67.11 is mapped to network region 4. In production environments, different sites will typically be on different networks, and ranges of IP Addresses assigned by the DHCP scope serving the site can be entered as one entry in the network map, to assign all telephones in a range to a specific network region.

```
change ip-network-map                                           Page   1 of  63
                               IP ADDRESS MAPPING
                                                Subnet Network     Emergency
 IP Address                                     Bits   Region VLAN Location Ext
 ---------------------------------------------- ------ ------ ---- -------------
 FROM: 65.206.67.11                             /32    4      n
   TO: 65.206.67.11
 FROM: 65.206.67.111                            /32    4      n
   TO: 65.206.67.111
```

The following screen shows IP Network Region 4 configuration. Network region 4 is used in this addendum, to avoid any conflict with the network regions described in the main body of these Application Notes. In this example, codec set 4 will be used for calls within region 4. Location 2 has been assigned to region 4. If desired, IP Telephones in region 4 that make ARS calls can optionally consult the ARS location-specific tables for location 2 before the ARS "all locations" table, if location-based routing is to be performed by Communication Manager. The "Authoritative Domain" is set to the SIP domain shown in **Figure 1**, coordinated among Communication Manager, Session Manager, and Verizon.

```
change ip-network-region 4                                        Page   1 of  19
                               IP NETWORK REGION
  Region: 4
Location: 2       Authoritative Domain: adevc.avaya.globalipcom.com
    Name: Branch-x-LSP
MEDIA PARAMETERS                Intra-region IP-IP Direct Audio: yes
      Codec Set: 4              Inter-region IP-IP Direct Audio: yes
   UDP Port Min: 2048                      IP Audio Hairpinning? n
   UDP Port Max: 3329
DIFFSERV/TOS PARAMETERS                  RTCP Reporting Enabled? y
 Call Control PHB Value: 46      RTCP MONITOR SERVER PARAMETERS
        Audio PHB Value: 46       Use Default Server Parameters? y
        Video PHB Value: 26
802.1P/Q PARAMETERS
 Call Control 802.1p Priority: 6
        Audio 802.1p Priority: 6
        Video 802.1p Priority: 5      AUDIO RESOURCE RESERVATION PARAMETERS
H.323 IP ENDPOINTS                                        RSVP Enabled? n
  H.323 Link Bounce Recovery? y
 Idle Traffic Interval (sec): 20
   Keep-Alive Interval (sec): 5
            Keep-Alive Count: 5
```

The following screen shows the inter-network region connection configuration for region 4. The bold row shows that network region 4 is directly connected to network region 1, and that codec set 4 will also be used for any connections between region 4 and region 1. In configurations where a central site has gateway resources in region 1, it may be desirable to use the central resources (e.g., during ring-back phase, or for announcements before a specific site is selected for the call). For configurations where multiple remote gateways are used, each gateway will typically be configured for a different region, and this screen can be used to specify unique codec or call admission control parameters for the pairs of regions. If a different codec should be used for inter-region connectivity than for intra-region connectivity, a different codec set can be entered in the codec set field for the appropriate row in the screen shown below. Once submitted, the configuration becomes symmetric, meaning that network region 1, Page 3 will also show codec set 4 for region 4 to region 1 connectivity.

```
change ip-network-region 4                                        Page   3 of  19

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

11.5.1.5 Locations

The “change locations” screen allows other location-specific parameters to be defined in a multi-location system, if needed. In this addendum, the Avaya G450 Media Gateway was assigned to location 2. The Avaya G650 Media Gateway, retained from the main body of these Application Notes, is assigned location 1.

```
change locations                                              Page   1 of  16
                                   LOCATIONS
               ARS Prefix 1 Required For 10-Digit NANP Calls? y

 Loc  Name            Timezone Rule  NPA  ARS  Atd      Disp   Prefix   Proxy Sel
 No                    Offset              FAC  FAC      Parm              Rte Pat
 1:  Main            + 00:00   0                          1                  3
 2:  branch-x        + 00:00   0                          1
 3:                      :
```

11.5.1.6 IP Codec Sets

The following screen shows the configuration for codec set 4. Codec set 4 is used in this addendum, to avoid any conflict with the codec sets described in the main body of these Application Notes. In general, an IP codec set is a list of allowable codecs in priority order. In the example screen below, all calls to and from the PSTN via the SIP trunks would use G.711MU. Other calls using this same codec set that are between devices capable of the G.722-64K codec (e.g., Avaya 9600-Series IP Telephone) can use G.722.

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

    Audio         Silence      Frames   Packet
    Codec         Suppression  Per Pkt  Size(ms)
 1: G.722-64K                    2        20
 2: G.711MU            n         2        20
 3:
 4:
 5:
 6:
 7:
```

11.5.1.7 SIP Signaling Groups Using Processor Ethernet

This section illustrates the configuration of the SIP Signaling Groups that use the Processor Ethernet. Each signaling group has a “Group Type” of “sip”, and a “Near-end Node Name” of “procr”. In the example screens, the “Transport Method” for all signaling groups is “tcp” using port 5060. In production, TLS transport between Avaya Aura™ Communication Manager and Avaya Aura™ Session Manager can be used. The “Enable Layer 3 Test” field is enabled to allow Communication Manager to maintain the signaling group using the SIP OPTIONS method. Other fields can be left at default values, including “DTMF over IP” set to “rtp-payload”, which corresponds to RFC 2833.

The following screen shows signaling group 7. The “Near-end Node Name” is “procr” and the “Far-end Node Name” is “ASM”, the node name of the Session Manager. The “Far-end Network Region” is configured to region 4, the region of the Avaya G450 Media Gateway. Signaling group 7 can be used for processing incoming PSTN calls from Session Manager.

```
change signaling-group 7                                        Page   1 of   1

 Group Number: 7             Group Type: sip
                       Transport Method: tcp
  IMS Enabled? n

   Near-end Node Name: procr                 Far-end Node Name: ASM
 Near-end Listen Port: 5060                Far-end Listen Port: 5060
                                        Far-end Network Region: 4
Far-end Domain:
                                             Bypass If IP Threshold Exceeded? n
Incoming Dialog Loopbacks: eliminate                  RFC 3389 Comfort Noise? n
         DTMF over IP: rtp-payload             Direct IP-IP Audio Connections? y
Session Establishment Timer(min): 3                     IP Audio Hairpinning? n
         Enable Layer 3 Test? y                       Direct IP-IP Early Media? n
H.323 Station Outgoing Direct Media? n              Alternate Route Timer(sec): 6
```

The following screen shows signaling group 8. The "Near-end Node Name" is "procr" and the "Far-end Node Name" is "ASM", the node name of the Session Manager. The "Far-end Network Region" is 4. Signaling group 8 can be used for processing outgoing calls to Session Manager destined for the PSTN. Note that the "Alternate Route Timer" that defaults to 6 seconds impacts fail-over timing for outbound calls. If Communication Manager does not get an expected response, Look-Ahead Routing (LAR) can be triggered, after the expiration of the Alternate Route Timer. Detailed examples of the use of LAR can be found in reference [PE], reference [LAR], and Section 11.6.

```
change signaling-group 8                                        Page   1 of   1

 Group Number: 8             Group Type: sip
                       Transport Method: tcp
  IMS Enabled? n

   Near-end Node Name: procr                 Far-end Node Name: ASM
 Near-end Listen Port: 5060                Far-end Listen Port: 5060
                                        Far-end Network Region: 4
Far-end Domain:
                                             Bypass If IP Threshold Exceeded? n
Incoming Dialog Loopbacks: eliminate                  RFC 3389 Comfort Noise? n
         DTMF over IP: rtp-payload             Direct IP-IP Audio Connections? y
Session Establishment Timer(min): 3                     IP Audio Hairpinning? n
         Enable Layer 3 Test? y                       Direct IP-IP Early Media? n
H.323 Station Outgoing Direct Media? n              Alternate Route Timer(sec): 6
```

11.5.1.8 SIP Trunk Groups Using Processor Ethernet

This section illustrates the configuration of two SIP Trunks Groups, corresponding to the two SIP signaling groups using Processor Ethernet. Each trunk group has a "Group Type" of "sip", and a "Service Type" of "public-ntwrk".

The following shows page 1 for trunk group 7. The "Number of Members" field defines how many simultaneous calls are permitted for the trunk group. Although not strictly necessary, the "Direction" has been configured to "incoming" to emphasize that trunk group 7 is used for incoming calls from Session Manager in the sample configuration.

```
change trunk-group 7                                            Page   1 of  21
                                TRUNK GROUP
Group Number: 7                    Group Type: sip           CDR Reports: y
  Group Name: Inbound-Procr               COR: 1        TN: 1        TAC: 107
   Direction: incoming       Outgoing Display? n
 Dial Access? n                                 Night Service:

Service Type: public-ntwrk          Auth Code? n
                                                     Signaling Group: 7
                                                   Number of Members: 10
```

The following shows Page 2 for trunk group 7. All parameters shown are default values, except for the "Preferred Minimum Session Refresh Interval", which has been changed from 600 to 900. Although not strictly necessary, some SIP products prefer a higher session refresh interval than the Avaya Aura™ Communication Manager default value, which can result in unnecessary SIP messages to re-establish a higher refresh interval for each call.

```
change trunk-group 7                                            Page   2 of  21
      Group Type: sip

TRUNK PARAMETERS
     Unicode Name: auto
                                            Redirect On OPTIM Failure: 5000
            SCCAN? n                               Digital Loss Group: 18
                      Preferred Minimum Session Refresh Interval(sec): 900
```

The following shows Page 3 for trunk group 7. All parameters except those in bold are default values. Optionally, replacement text strings can be configured using the "system-parameters features" screen, such that incoming "private" calls can display an Avaya-configured text string on called party telephones.

```
change trunk-group 7                                            Page   3 of  21
TRUNK FEATURES
          ACA Assignment? n            Measured: none
                                                       Maintenance Tests? y
                     Numbering Format: public
                                                UUI Treatment: service-provider
                                                 Replace Restricted Numbers? y
                                                Replace Unavailable Numbers? y
```

The following shows Page 4 for trunk group 7. The considerations for these parameters for the trunk groups associated with the processor Ethernet SIP Trunks are the same as the considerations associated with the C-LAN SIP Trunk groups, as discussed in Section 3.1.5.1.

```
change trunk-group 7                                            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? y
             Telephone Event Payload Type: 101
```

The following shows Page 1 for trunk group 8. The "Number of Members" field defines how many simultaneous calls are permitted for the trunk group. Although not strictly necessary, the "Direction" has been configured to "outgoing" to emphasize that trunk group 8 is used for outgoing calls to Session Manager. The remaining pages for trunk group 8 match trunk group 7 and therefore will not be illustrated here.

```
change trunk-group 8                                            Page   1 of  21
                                TRUNK GROUP
Group Number: 8                    Group Type: sip           CDR Reports: y
  Group Name: Outbound-procr             COR: 1        TN: 1        TAC: 108
   Direction: outgoing       Outgoing Display? n
 Dial Access? n
Queue Length: 0
Service Type: public-ntwrk
                                                       Signaling Group: 8
                                                     Number of Members: 10
```

11.5.1.9 Route Pattern Directing Calls to Processor Ethernet SIP Trunk

Route pattern 19 will be used for calls destined for the PSTN via the SIP trunks to Session Manager. Digit manipulation can be performed on the number, if needed. In the sample configuration, the leading digit (i.e., the 1) is deleted and a 10 digit number is sent to Session Manager. The following screen shows route pattern 19, containing trunk group 8.

If desired, Look-Ahead Routing (LAR) can be set to "next", and one or more alternate Communication Manager trunks can be listed in the route pattern. Examples are provided in references [PE], [LAR], and in Section 11.6 of this addendum.

```
change route-pattern 19                                         Page   1 of   3
                    Pattern Number: 19  Pattern Name: To-VZ-via-SM
                             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: 8    0                    1                                        n   user
 2:                                                                    n   user
 3:                                                                    n   user
 4:                                                                    n   user
 5:                                                                    n   user
 6:                                                                    n   user

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

11.5.1.10 Public Numbering

The "change public-unknown-numbering" command may be used to define the format of the calling party number to be sent for the newly defined trunk groups. The considerations for the processor Ethernet based SIP Trunks are identical to the considerations for C-LAN based trunks, as detailed in Section 3.1.6. In the bolded row shown in the example abridged output below, a specific Communication Manager extension is mapped to a PSTN number that is known to Verizon, when the call uses SIP Trunk group 7 or 8.

```
change public-unknown-numbering 0                              Page   1 of   2
                      NUMBERING - PUBLIC/UNKNOWN FORMAT
                                           Total
Ext Ext           Trk       CPN             CPN
Len Code          Grp(s)    Prefix          Len
 5  30001         7-8       7329450228      10
 5  30002         7-8       7329450231      10
```

11.5.1.11 ARS Routing For Outbound Calls

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

The following screen shows a sample ARS configuration. If a user dials the ARS access code followed by 1-908-848-57xx, the call will select route pattern 19.

```
change ars analysis 1908                                       Page   1 of   2
                             ARS DIGIT ANALYSIS TABLE
                                   Location:  all          Percent Full:    1
          Dialed           Total     Route    Call   Node  ANI
          String          Min  Max  Pattern   Type   Num   Reqd
    190884857             11   11    19       natl         n
```

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

```
list ars route-chosen 19088485704
                           ARS ROUTE CHOSEN REPORT

     Location:  1                     Partitioned Group Number:  1

      Dialed            Total         Route    Call      Node
      String          Min    Max    Pattern   Type     Number    Location

 190884857            11    11       19       natl                 all

   Actual Outpulsed Digits by Preference (leading 35 of maximum 42 digit)

 1: 9088485704                         9:
 2:                                   10:
 3:                                   11:
 4:                                   12:
 5:                                   13:
 6:                                   14:
 7:                                   15:
 8:                                   16:
```

11.5.1.12 Incoming Call Handling Treatment for Incoming Calls

In general, the "incoming call handling treatment" for a trunk group can be used to manipulate the digits received for an incoming call. In the sample configuration, since Avaya Aura™ Session Manager is present, Session Manager is used to perform digit conversion, as described in Section 4.3.2.1. To see examples of using the Communication Manager incoming call handling table, in cases where another entity such as Session Manager is not normalizing the dial plan, consult references [PE] and [CLAN].

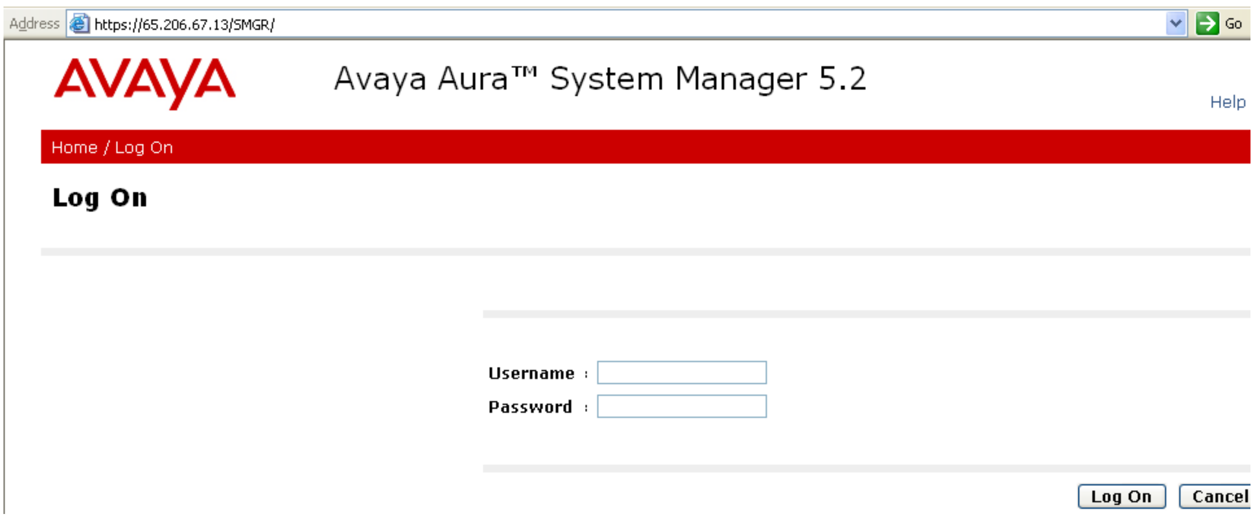
11.5.1.13 Saving Communication Manager Configuration Changes

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

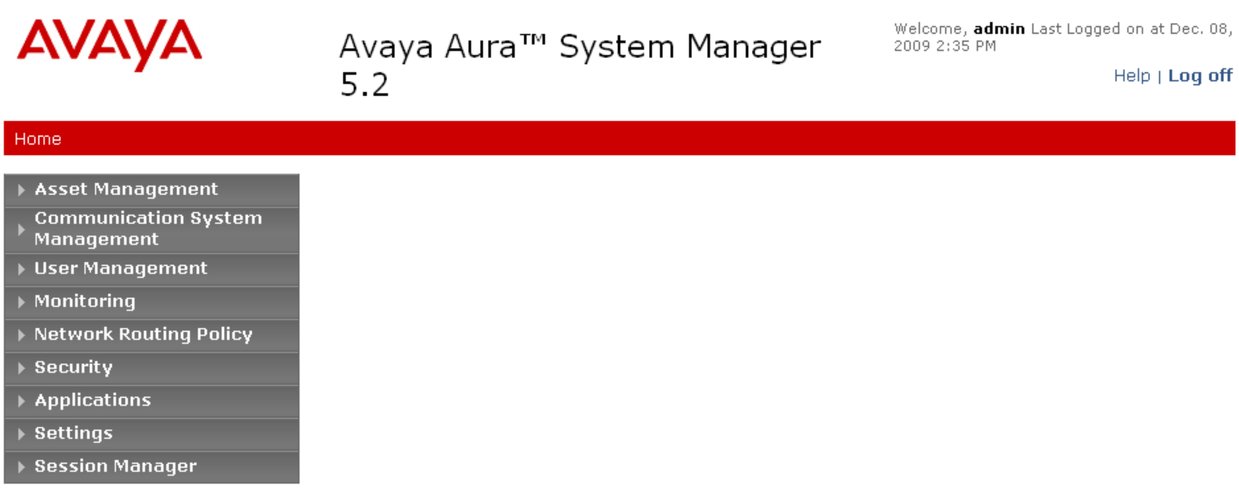
11.5.2 Session Manager Configuration

This section illustrates relevant aspects of the Avaya Aura™ Session Manager configuration used in the verification of this addendum. Since the version of Session Manager used in the addendum is updated compared with the version used in the main body of these Application Notes, example screens are presented for reference.

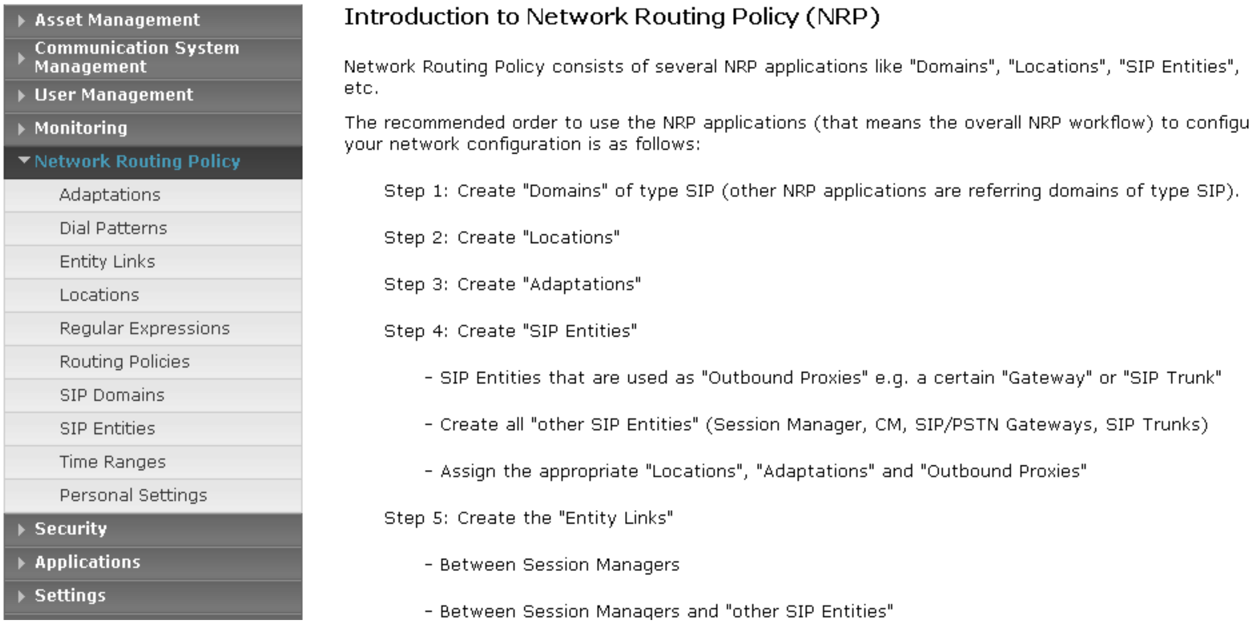
Session Manager is managed via Avaya Aura™ System Manager. Using a web browser, access "https://<ip-addr of System Manager>/SMGR" and log in via the screen presented below. Note that this log-in link address has changed for release 5.2.



Once logged in, a screen such as the following is displayed.



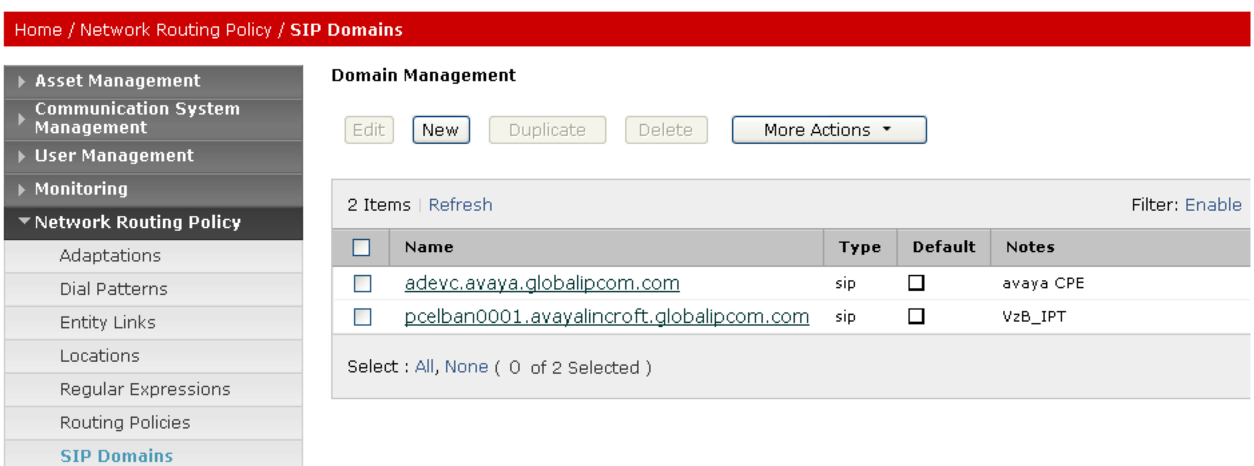
Select **Network Routing Policy**. The screen shown below shows the various sub-headings, as well as a step-by-step summary in the right pane. Although this addendum does not intend to be prescriptive, the sub-sections below are in the same order as the steps outlined under **Introduction to Network Routing Policy (NRP)** in the screen below.



11.5.2.1 Domains

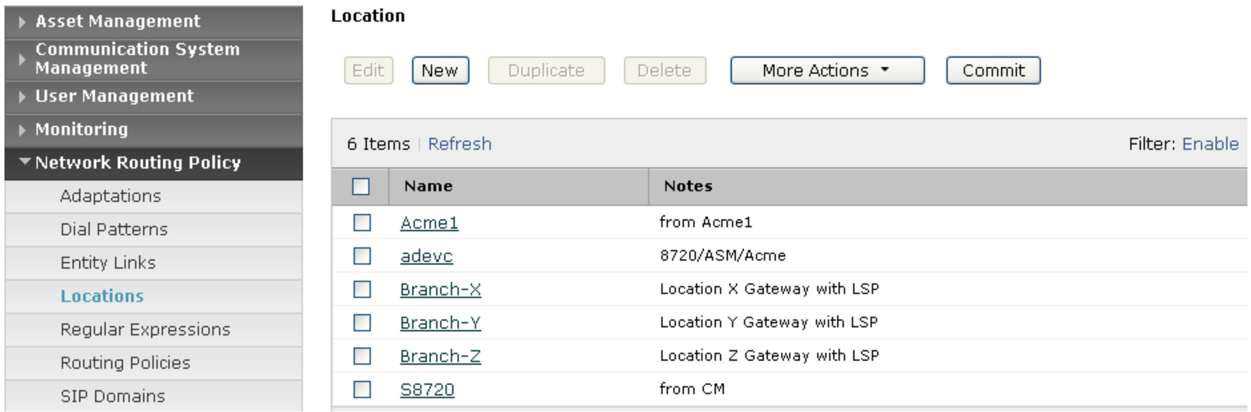
To view or change SIP domains, select **Network Routing Policy → SIP Domains**. Click on the checkbox next to the name of the SIP domain and **Edit** to edit an existing SIP domain, or the **New** button to add a SIP domain.

The following screen shows the list of previously configured SIP domains. As in Section 4.3.1, the domain "adevc.avaya.globalipcom.com" is associated with the enterprise SIP domain. The domain "pcelban0001.avayalincroft.globalipcom.com" is associated with Verizon.



11.5.2.2 Locations

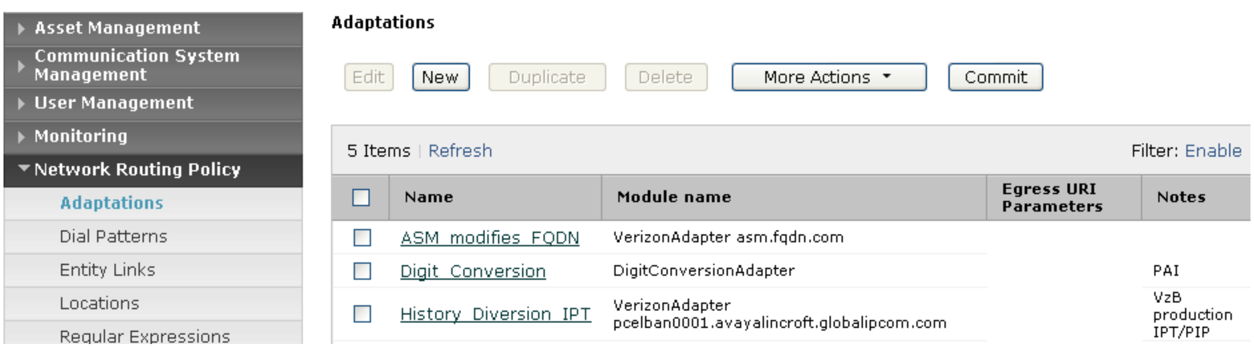
To view or change locations, select **Network Routing Policy → Locations**. The following screen shows an example list of configured locations. Click on the checkbox corresponding to the name of a location and **Edit** to edit an existing location, or the **New** button to add a location. Assigning unique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



Later, the Avaya S8720 Server PE will be assigned to the location named “adevc” evident in the locations list screen.

11.5.2.3 Adaptations / Digit Conversion Adapter

To view or change adaptations, select **Network Routing Policy → Adaptations**. Click on the checkbox corresponding to the name of an adaptation and **Edit** to edit an existing adaptation, or the **New** button to add an adaptation. The following screen shows a portion of the list of adaptations in the sample configuration.



The following screen shows a portion of the Digit Conversion adapter settings for “incoming calls to SM”, which correspond with outgoing calls from Avaya Aura™ Communication Manager. Digit conversion such as this, that converts a Communication Manager extension to a corresponding LDN or DID number known to the PSTN, can be performed in Communication Manager (e.g., using “public unknown numbering”) or in Session Manager.

Digit Conversion for Incoming Calls to SM

Add | Remove

5 Items | Refresh   Filter: Enable

☐	Matching Pattern	Min	Max	Delete Digits	Insert Digits	Address to modify	Notes
☐	* 30001	* 5	* 5	* 5	7329450228	both	Digital
☐	* 30002	* 5	* 5	* 5	7329450231	both	9620 H323

The following screen shows a portion of the Digit Conversion adapter settings for "outgoing calls from SM", which correspond to incoming calls to Avaya Aura™ Communication Manager. As an example, if a user on the PSTN dials 732-945-0231, Session Manager will convert the number to 30002 before sending the SIP INVITE to Communication Manager. In this case, the mapping of PSTN DID numbers to Communication Manager extensions is done in Session Manager. As an alternative, it is also possible to perform mappings in Communication Manager using the incoming call handling treatment of the receiving trunk group. In these sample screens, only the PSTN number 732-945-0231 corresponding to Communication Manager extension 30002 is relevant; other entries shown in the screens can be ignored.

Digit Conversion for Outgoing Calls from SM

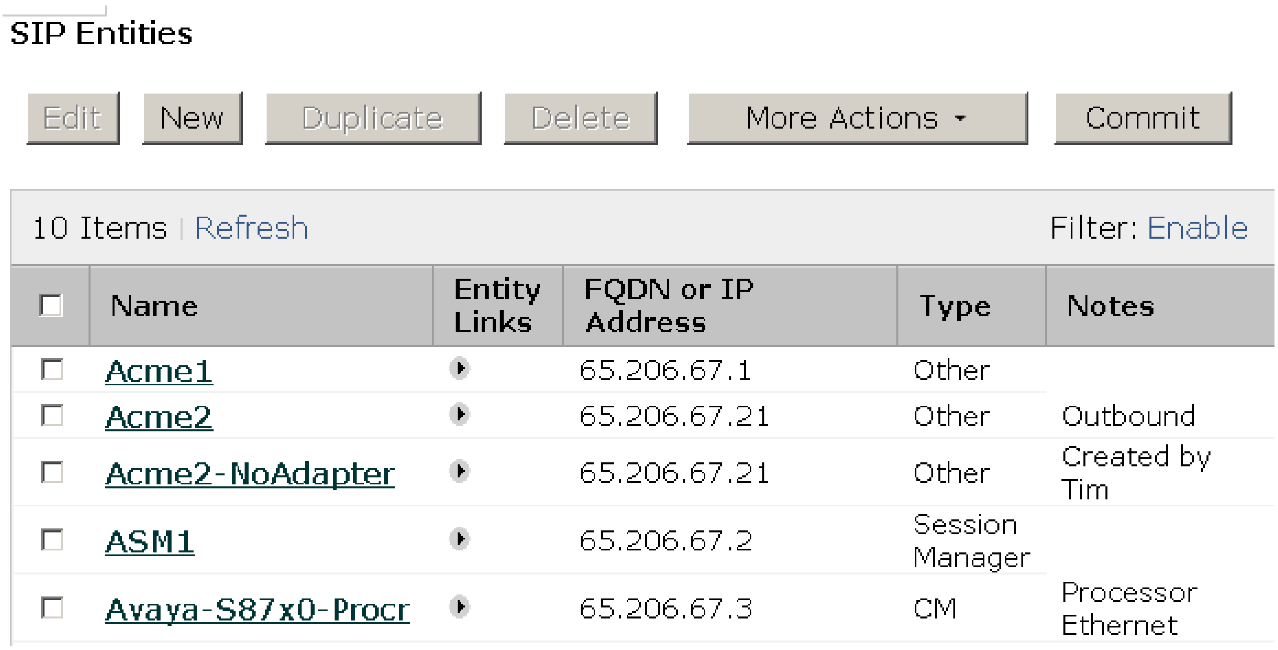
Add | Remove

14 Items | Refresh   Filter: Enab

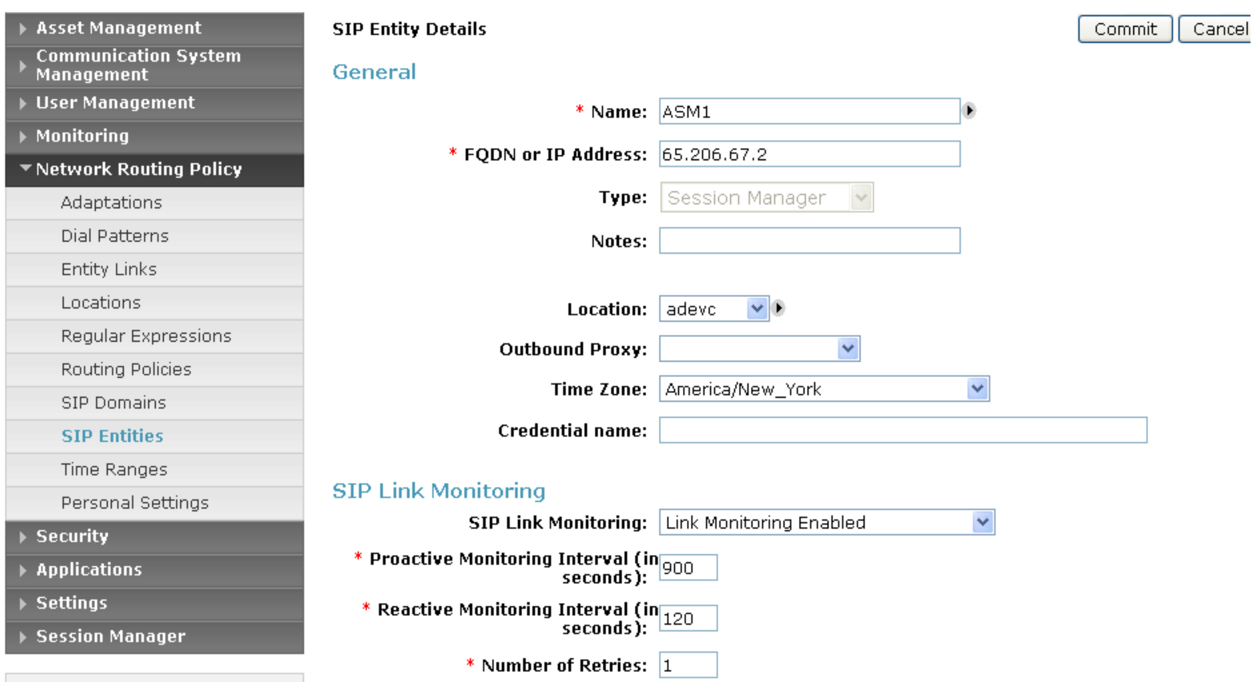
☐	Matching Pattern	Min	Max	Delete Digits	Insert Digits	Addres modify
☐	* 7329450228	* 10	* 10	* 10	30003	both
☐	* 7329450229	* 10	* 10	* 10	30001	both
☐	* 7329450230	* 10	* 10	* 10	30004	both
☐	* 7329450231	* 10	* 10	* 10	30002	both

11.5.2.4 SIP Entities

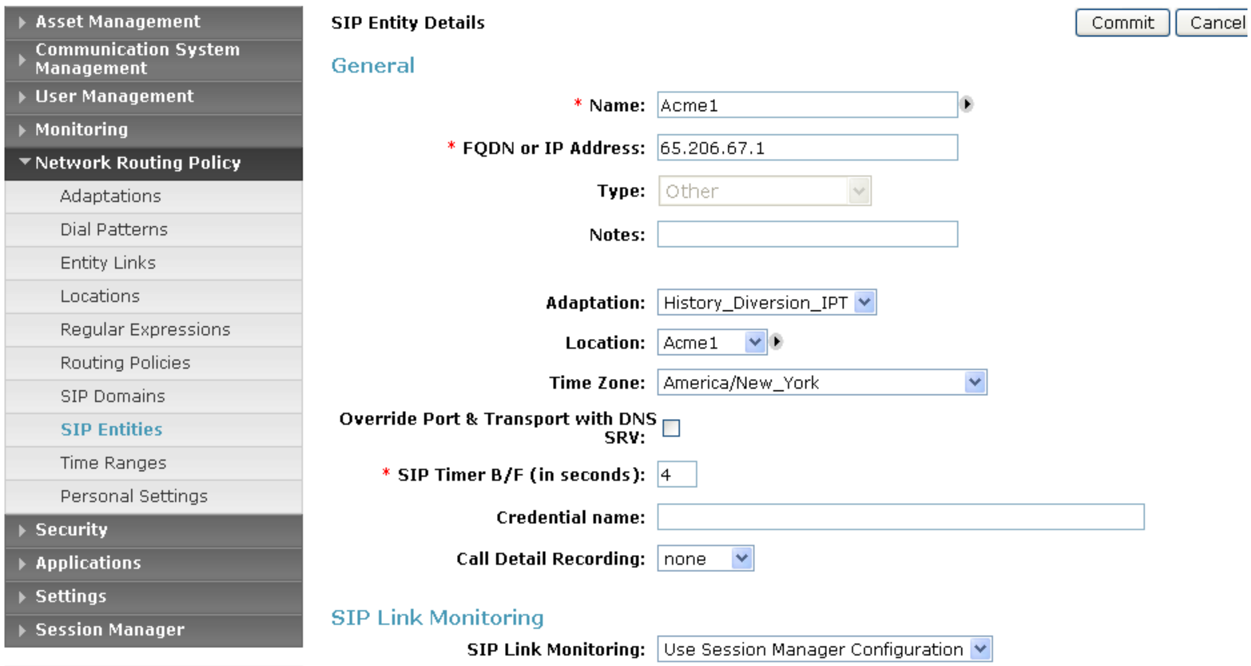
To view or change SIP entities, select **Network Routing Policy → SIP Entities**. Click the checkbox corresponding to the name of an entity and **Edit** to edit an existing entity, or the **New** button to add an entity. The following screen shows a portion of the list of configured SIP entities. The entities named "ASM1", "Acme1", and "Avaya-S87x0-Procr" are most relevant to this addendum.



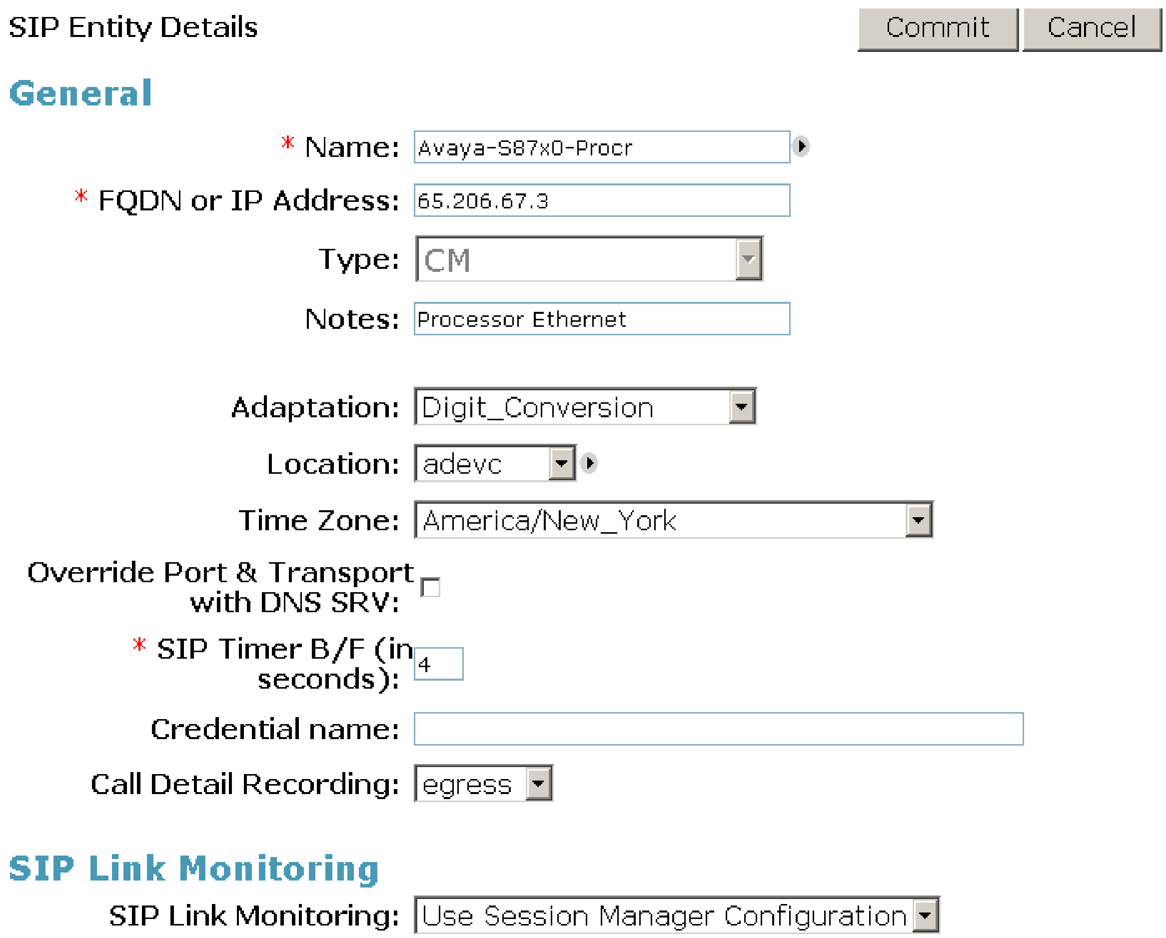
The following screen shows the **SIP Entity Details** corresponding to "ASM1", which uses the Avaya Aura™ Session Manager Security Module IP Address (65.206.67.2). The default **SIP Link Monitoring** parameters can be observed. Unless changed elsewhere, entity links from other SIP entities to this instance of Session Manager will use the default SIP Link Monitoring timers shown below.



The following screen shows the **SIP Entity Details** corresponding to “Acme1”, the Acme Packet Net-Net Session Director inside IP Address (65.206.67.1). Observe that the Acme Packet Session Director has been assigned to location “Acme1”, and the History_Diversion_IPT adapter is applied. This adaptation uses the “VerizonAdapter”, as described in Section 4.3.2.1.

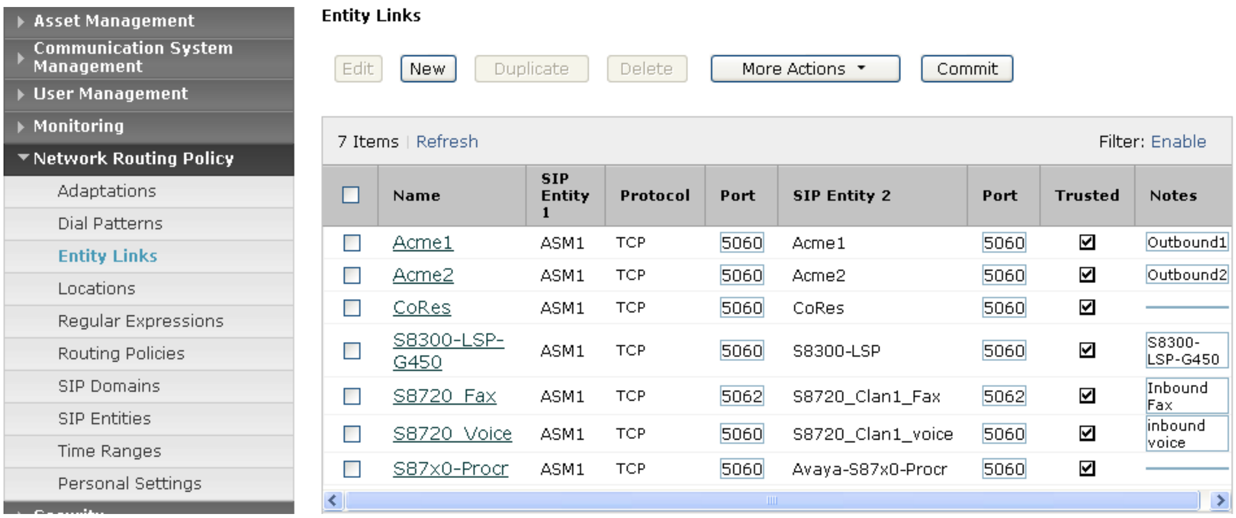


The following screen shows the **SIP Entity Details** corresponding to the S8720 PE (65.206.67.3). Note the similarity of this configuration to **Figure 44** in Section 4.3.4, which creates the SIP Entity corresponding to the Avaya C-LAN.



11.5.2.5 Entity Links

To view or change Entity Links, select **Network Routing Policy → Entity Links**. Click on the checkbox corresponding to the name of an entity link and **Edit** to edit an existing link, or the **New** button to add a link. The following screen shows the list of configured entity links. The SIP Entity Links defined in Section 4.3.5 can be observed, and the procedures described in Section 4.3.5 can be used to configure a new entity link named "S87x0-Procr". This new SIP Entity Link is defined between the Avaya Aura™ Session Manager instance "ASM1" as **SIP Entity 1** and the **SIP Entity 2** name corresponding to the Avaya S8720 PE, "Avaya-S87x0-Procr".



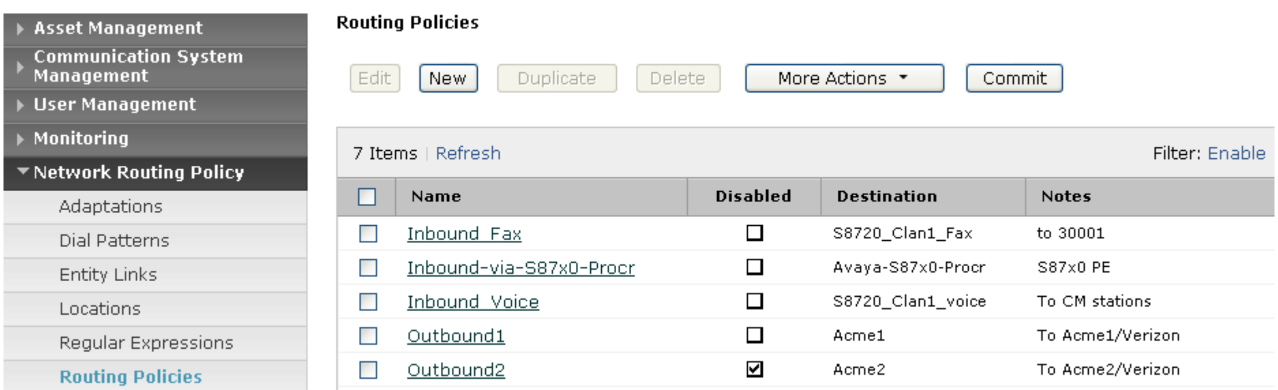
Name	SIP Entity 1	Protocol	Port	SIP Entity 2	Port	Trusted	Notes
Acme1	ASM1	TCP	5060	Acme1	5060	☑	Outbound1
Acme2	ASM1	TCP	5060	Acme2	5060	☑	Outbound2
CoRes	ASM1	TCP	5060	CoRes	5060	☑	
S8300-LSP-G450	ASM1	TCP	5060	S8300-LSP	5060	☑	S8300-LSP-G450
S8720_Fax	ASM1	TCP	5062	S8720_Clan1_Fax	5062	☑	Inbound Fax
S8720_Voice	ASM1	TCP	5060	S8720_Clan1_voice	5060	☑	inbound voice
S87x0-Procr	ASM1	TCP	5060	Avaya-S87x0-Procr	5060	☑	

11.5.2.6 Time Ranges

To view or change Time Ranges, select **Network Routing Policy → Time Ranges**. The time range shown in Section 4.3.6 can be retained for the addendum.

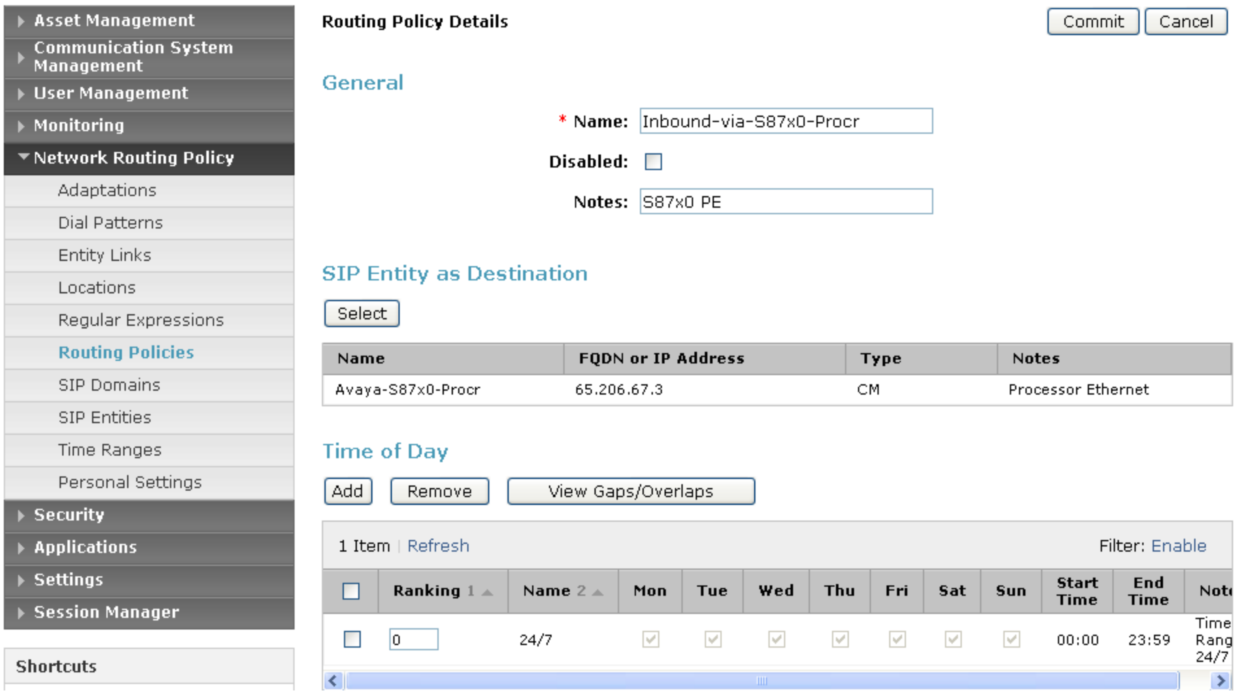
11.5.2.7 Routing Policies

To view or change routing policies, select **Network Routing Policy → Routing Policies**. Click on the checkbox corresponding to the name of a policy and **Edit** to edit an existing policy, or **New** to add a policy. The following screen shows an example list of configured policies.



Name	Disabled	Destination	Notes
Inbound_Fax	☐	S8720_Clan1_Fax	to 30001
Inbound-via-S87x0-Procr	☐	Avaya-S87x0-Procr	S87x0 PE
Inbound_Voice	☐	S8720_Clan1_voice	To CM stations
Outbound1	☐	Acme1	To Acme1/Verizon
Outbound2	☑	Acme2	To Acme2/Verizon

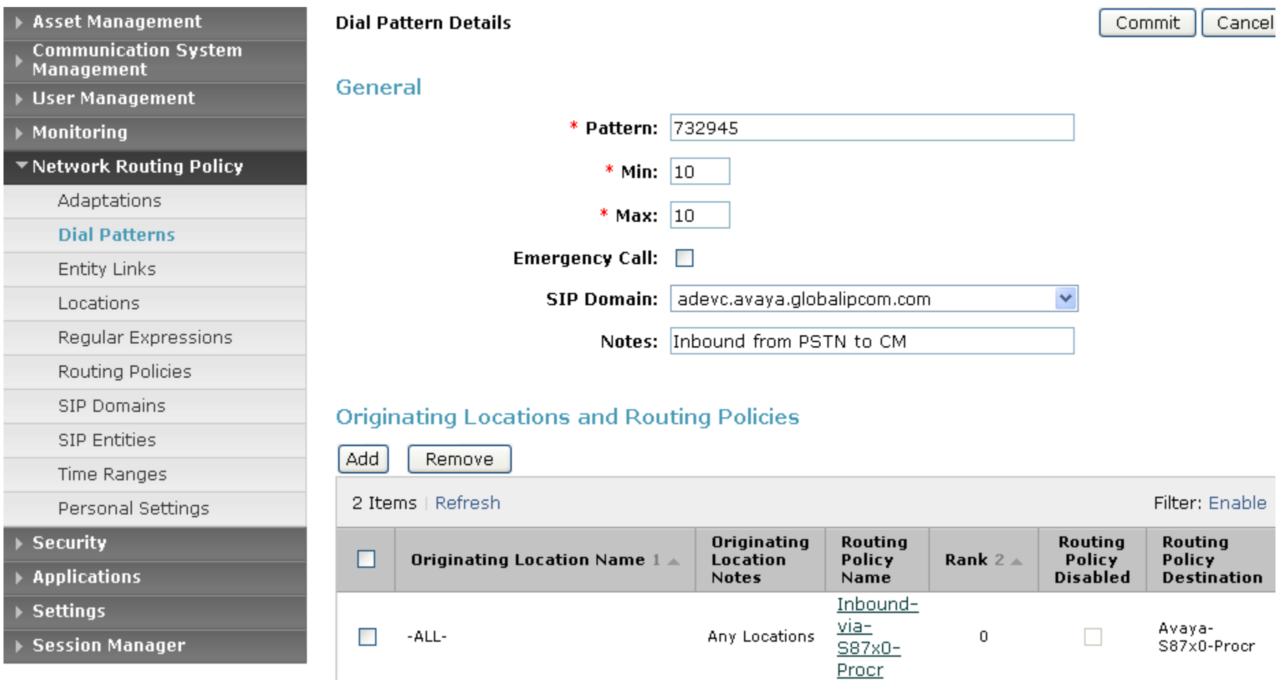
The following screen shows the **Routing Policy Details** for the policy named "Inbound-via-S87x0-Procr" associated with incoming calls from Verizon to Communication Manager, using the Avaya S8720 PE. Observe the **SIP Entity as Destination** is the entity named "Avaya-S87x0-Procr".



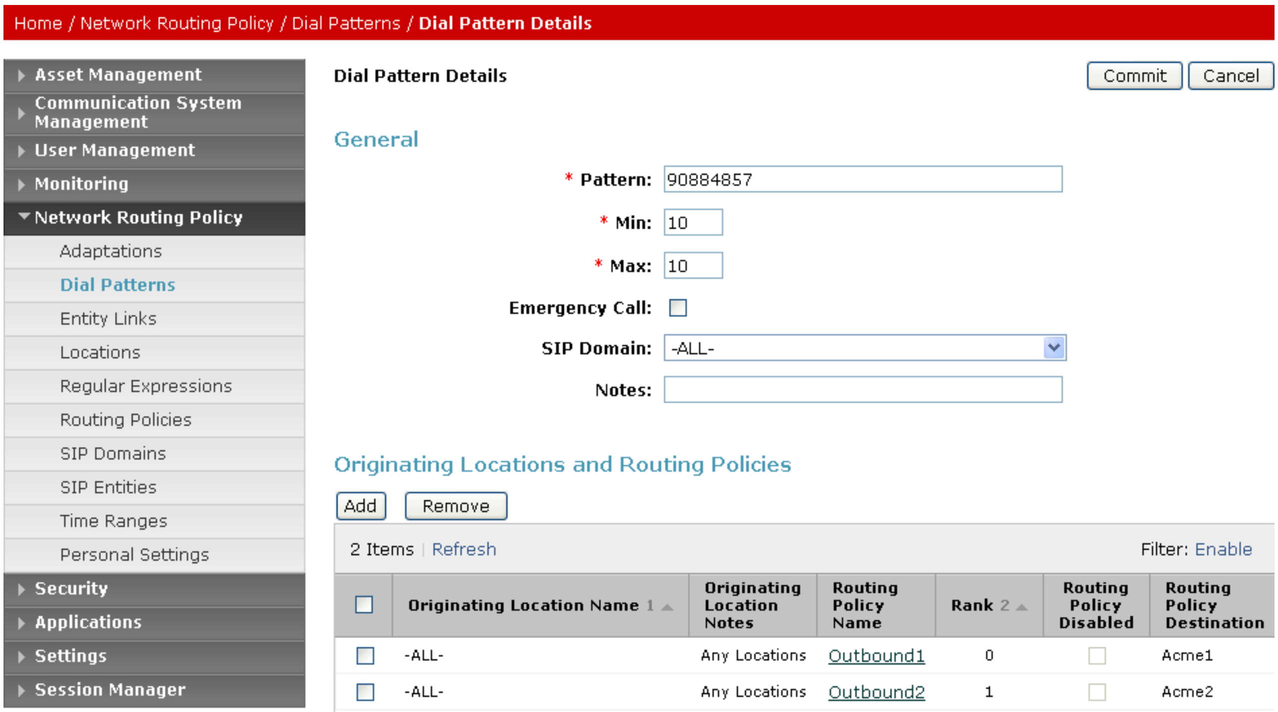
11.5.2.8 Dial Patterns

To view or change dial patterns, select **Network Routing Policy → Dial Patterns**. Click on the checkbox corresponding to the name of a pattern and **Edit** to edit an existing pattern, or **New** to add a pattern.

The following screen illustrates an example dial pattern used to verify inbound PSTN calls to the enterprise via the Avaya S8720 Processor Ethernet. When a user on the PSTN dials a number such as 732-945-0231, Verizon delivers the 732-945-xxxx number to the enterprise, and the Acme Packet Session Director sends the call to Session Manager. The pattern below matches on these 732-945-xxxx numbers, and the first routing policy is configured to send calls to the S8720 PE.



The following screen illustrates an example dial pattern used to verify outbound calls from the enterprise to the PSTN. When a Communication Manager user dials a PSTN number such as 9-1-908-848-5704, Communication Manager sends 908-848-5704 to Session Manager, via the S8720 PE. Session Manager will match the dial pattern shown below and send the call to the Acme Packet Session Director via the **Routing Policy Name** "Outbound1". If the call can not be routed via "Outbound1", the call can automatically re-route via **Routing Policy Name** "Outbound2". For more information on Session Manager routing, see Section 11.6.



11.5.3 Example Incoming Call via SIP Trunk to Avaya S8720 PE

Incoming PSTN calls arrive from Verizon at an Acme Packet Session Director, which sends the call to Avaya Aura™ Session Manager. In this addendum, Session Manager sends the call to Avaya Aura™ Communication Manager via the entity link corresponding to the Avaya S8720 PE. On Communication Manager, the incoming call arrives via signaling group 7 and trunk group 7.

The following Communication Manager "list trace" trace output shows a call incoming on trunk group 7. The PSTN telephone dialed 732-945-0231. Session Manager mapped the number received from Verizon to the extension of a Communication Manager telephone (x30002). Extension 30002 is an IP Telephone with IP Address 65.206.67.11 in Region 4. Initially, the G450 Media Gateway in region 4 (65.206.67.62) is used, but as can be seen in the final trace output, once the call is answered, the final RTP media path is "ip-direct" from the IP Telephone (65.206.67.11) to the "inside" of the Acme Packet Session Director (65.206.67.1). Note that although the list trace output indicates "no calling party number", the calling party number is indeed received and displayed on the called Avaya telephone.

```
list trace tac 107                                                  Page   1
                                LIST TRACE
time            data
09:17:41     Calling party trunk-group 7 member 1  cid 0x31
09:17:41     Calling Number & Name NO-CPNumber NO-CPName
09:17:41     active trunk-group 7 member 1  cid 0x31
09:17:41     dial 30002
09:17:41     ring station    30002 cid 0x31
09:17:41     G711MU ss:off ps:20
             rgn:4 [65.206.67.1]:49300
             rgn:4 [65.206.67.62]:2052
09:17:41     xoip options: fax:off modem:off tty:US  uid:0x5002e
             xoip ip: [65.206.67.62]:2052
09:17:41     G711MU ss:off ps:20
             rgn:4 [65.206.67.11]:2174
             rgn:4 [65.206.67.62]:2050
09:17:47     active station    30002 cid 0x31
09:17:48     G711MU ss:off ps:20
             rgn:4 [65.206.67.1]:49300
             rgn:4 [65.206.67.11]:2174
09:17:48     G711MU ss:off ps:20
             rgn:4 [65.206.67.11]:2174
             rgn:4 [65.206.67.1]:49300
```

The following portion of a filtered Wireshark trace shows an incoming PSTN call using the S8720 PE. In frame 673, the Acme Packet Session Director sends the INVITE to Session Manager. In frame 677, Session Manager sends the INVITE to the S8720 PE. The call proceeds as usual using the S8720 PE with 100 Trying, 180 Ringing, and 200 OK upon answer. In frame 745, Communication Manager sends the INVITE to begin the process of shuffling the media paths to "ip-direct", which concludes with the ACKs in frames 765-766.

Filter: sip && ip.addr == 65.206.67.3 or ip.addr == 65.206.67.1 Expression... Clear Apply

No.	Time	Source	Destination	Protocol	Info
673	71.779240	65.206.67.1	65.206.67.2	SIP/SDP	Request: INVITE sip:7329450231@65.206.67.2:5060;transport=tc
674	71.785178	65.206.67.2	65.206.67.1	SIP	Status: 100 Trying
677	71.795275	65.206.67.2	65.206.67.3	SIP/SDP	Request: INVITE sip:30002@adevc.avaya.globalipcom.com:5060;t
679	71.797216	65.206.67.3	65.206.67.2	SIP	Status: 100 Trying
682	71.803045	65.206.67.3	65.206.67.2	SIP/SDP	Status: 180 Ringing, with session description
686	71.824152	65.206.67.2	65.206.67.1	SIP/SDP	Status: 180 Ringing, with session description
737	78.458588	65.206.67.3	65.206.67.2	SIP/SDP	Status: 200 OK, with session description
740	78.467205	65.206.67.2	65.206.67.1	SIP/SDP	Status: 200 OK, with session description
743	78.625119	65.206.67.1	65.206.67.2	SIP	Request: ACK sip:7329450231@65.206.67.3;transport=tcp
744	78.631917	65.206.67.2	65.206.67.3	SIP	Request: ACK sip:7329450231@65.206.67.3;transport=tcp
745	78.634802	65.206.67.3	65.206.67.2	SIP	Request: INVITE sip:9088485704@65.206.67.1:5060;transport=tc
747	78.668968	65.206.67.2	65.206.67.3	SIP	Status: 100 Trying
749	78.671262	65.206.67.2	65.206.67.1	SIP	Request: INVITE sip:9088485704@65.206.67.1:5060;transport=tc
751	78.674266	65.206.67.1	65.206.67.2	SIP	Status: 100 Trying
761	78.866827	65.206.67.1	65.206.67.2	SIP/SDP	Status: 200 OK, with session description
763	78.870740	65.206.67.2	65.206.67.3	SIP/SDP	Status: 200 OK, with session description
765	78.877161	65.206.67.3	65.206.67.2	SIP/SDP	Request: ACK sip:9088485704@65.206.67.1:5060;transport=tcp,
766	78.882688	65.206.67.2	65.206.67.1	SIP/SDP	Request: ACK sip:9088485704@65.206.67.1:5060;transport=tcp,

11.5.4 Example Outgoing Call to PSTN via Avaya S8720 PE

The following trace shows an outbound ARS call from IP Telephone x30002 to the PSTN number 9-1-908-848-5704. The call is routed to route pattern 19 and trunk group 8. The call initially uses the gateway media processor in region 4 (65.206.67.62), but after the call is answered, the call is "shuffled" to become an "ip-direct" connection between the IP Telephone (65.206.67.11) and the "inside" of the Acme Packet Session Director (65.206.67.1).

```
list trace tac 108                                                      Page   1
                                LIST TRACE
time             data
09:28:58     dial 919088485704 route:ARS
09:28:58     route-pattern  19 preference 1  cid 0x33
09:28:58     seize trunk-group 8 member 5  cid 0x33
09:28:58     Calling Number & Name 30002 adevc_9620_H3
09:28:58     Setup digits 9088485704
09:28:58     Calling Number & Name 7329450231 adevc_9620_H3
09:28:58     Proceed trunk-group 8 member 5  cid 0x33
09:29:00     G711MU ss:off ps:20
             rgn:4 [65.206.67.1]:49304
             rgn:4 [65.206.67.62]:2052
09:29:00     xoip options: fax:off modem:off tty:US  uid:0x5003c
             xoip ip: [65.206.67.62]:2052
09:29:09     active trunk-group 8 member 5  cid 0x33
09:29:10     G711MU ss:off ps:20
             rgn:4 [65.206.67.11]:2174
             rgn:4 [65.206.67.1]:49304
09:29:10     G711MU ss:off ps:20
             rgn:4 [65.206.67.1]:49304
             rgn:4 [65.206.67.11]:2174
```

The following portion of a filtered Wireshark trace shows an outgoing call using the S8720 PE. In frame 51, Communication Manager uses the S8720 PE to send an INVITE to Session Manager. In frame 56, Session Manager sends the INVITE to the Acme Packet Session Director “Acme1”. The call proceeds with 100 Trying, 183 Session Progress, and 200 OK upon answer by the PSTN phone. In frame 117, Communication Manager sends an INVITE to begin the shuffling process, which concludes with the ACKs in frames 129-130.

Filter: sip && ip.addr == 65.206.67.3 or ip.addr == 65.206.67.1 Expression... Clear Apply

No.	Time	Source	Destination	Protocol	Info
51	6.947123	65.206.67.3	65.206.67.2	SIP/SDP	Request: INVITE sip:9088485704@65.206.67.2, with session descript
53	6.953307	65.206.67.2	65.206.67.3	SIP	Status: 100 Trying
56	6.965059	65.206.67.2	65.206.67.1	SIP/SDP	Request: INVITE sip:9088485704@pcelban0001.avayalincroft.globalip
57	6.968413	65.206.67.1	65.206.67.2	SIP	Status: 100 Trying
83	9.123342	65.206.67.1	65.206.67.2	SIP/SDP	Status: 183 Session Progress, with session description
85	9.128816	65.206.67.2	65.206.67.3	SIP/SDP	Status: 183 Session Progress, with session description
108	11.057794	65.206.67.1	65.206.67.2	SIP/SDP	Status: 200 OK, with session description
110	11.065439	65.206.67.2	65.206.67.3	SIP/SDP	Status: 200 OK, with session description
112	11.068508	65.206.67.3	65.206.67.2	SIP	Request: ACK sip:9088485704@65.206.67.1:5060;transport=tcp
113	11.074960	65.206.67.2	65.206.67.1	SIP	Request: ACK sip:9088485704@65.206.67.1:5060;transport=tcp
117	11.159231	65.206.67.3	65.206.67.2	SIP	Request: INVITE sip:9088485704@65.206.67.1:5060;transport=tcp
119	11.164847	65.206.67.2	65.206.67.3	SIP	Status: 100 Trying
120	11.165923	65.206.67.2	65.206.67.1	SIP	Request: INVITE sip:9088485704@65.206.67.1:5060;transport=tcp
121	11.168643	65.206.67.1	65.206.67.2	SIP	Status: 100 Trying
125	11.547023	65.206.67.1	65.206.67.2	SIP/SDP	Status: 200 OK, with session description
127	11.551123	65.206.67.2	65.206.67.3	SIP/SDP	Status: 200 OK, with session description
129	11.555702	65.206.67.3	65.206.67.2	SIP/SDP	Request: ACK sip:9088485704@65.206.67.1:5060;transport=tcp, with
130	11.561848	65.206.67.2	65.206.67.1	SIP/SDP	Request: ACK sip:9088485704@65.206.67.1:5060;transport=tcp, with

11.6. Alternate Routing for Outbound Calls to the PSTN

This section summarizes considerations for alternate routing of outbound calls to the PSTN. Both Communication Manager and Session Manager have alternate routing capabilities that can allow calls to complete automatically, despite transient or persistent network problems along preferred paths.

11.6.1 Alternate Routing by Session Manager

In the sample configuration, when a Communication Manager user makes an outbound call destined for the PSTN, the call is preferentially routed to Session Manager. Session Manager can route the call to Verizon via either of two Acme Packet Net-Net Session Directors, Acme1 or

Acme2. As shown in Section 11.5.2.8, the Routing Policies "Outbound1" and "Outbound2" are assigned to outbound PSTN dial patterns to achieve this Session Manager alternate routing. If the primary path (Acme1) is unavailable to complete the call, Session Manager will automatically re-route the call to the secondary path (Acme2), transparent to Communication Manager (from a SIP signaling perspective). Session Manager could re-route for a variety of reasons, including transient or persistent network connectivity loss along the primary path, configurable bandwidth restrictions applicable to the location assigned to entities along the primary path, or SIP error responses received from Verizon. As an example, the following Communication Manager trace of an outbound PSTN call from station 30002 to PSTN number 908-848-5704 was captured while the Acme1 outside interface to Verizon was out of service. From the point of view of Communication Manager, the trunk group to Session Manager is in-service. Therefore, Communication Manager sends the call to Session Manager via the PE using trunk group 8 as illustrated previously. Session Manager completes the call via the secondary route to Acme2. As can be observed in the bold rows below, once the call is answered and the media path shuffles to "ip-direct", the final media path is between the calling telephone (65.206.67.11) and Acme2 (65.206.67.21).

```
list trace station 30002                                            Page   1
                                 LIST TRACE
time            data
08:32:06     active station    30002 cid 0x20f
08:32:06     G711MU ss:off ps:20
             rgn:4 [65.206.67.11]:3126
             rgn:4 [65.206.67.62]:2054
08:32:10     dial 9190884857 route:ARS
08:32:10     term trunk-group 8    cid 0x20f
08:32:10     dial 919088485704 route:ARS
08:32:10     route-pattern  19 preference 1  cid 0x20f
08:32:10     seize trunk-group 8 member 7  cid 0x20f
08:32:10     Calling Number & Name NO-CPNumber NO-CPName
08:32:10     Setup digits 9088485704
08:32:10     Calling Number & Name 7329450231 adevc_9620_H3
08:32:10     Proceed trunk-group 8 member 7  cid 0x20f
08:32:12     G711MU ss:off ps:20
             rgn:4 [65.206.67.21]:49190
             rgn:4 [65.206.67.62]:2058
08:32:12     xoip options: fax:Relay modem:off tty:US  uid:0x5003e
             xoip ip: [65.206.67.62]:2058
08:32:14     active trunk-group 8 member 7  cid 0x20f
08:32:14     G711MU ss:off ps:20
             rgn:4 [65.206.67.11]:3126
             rgn:4 [65.206.67.21]:49190
08:32:14     G711MU ss:off ps:20
             rgn:4 [65.206.67.21]:49190
             rgn:4 [65.206.67.11]:3126
```

11.6.2 Alternate Routing by Communication Manager

If Session Manager exhausts its alternate routing policies for a given dial pattern, the call will be rejected back to Communication Manager. Communication Manager can use Look-Ahead Routing, configured via the route-pattern, to automatically complete the call.

In the following example route-pattern, trunk group 8, the PE SIP Trunk to Session Manager remains the preferred route. For this preference, the field "LAR" has been set to "next", as shown in bold. If Communication Manager encounters an error (e.g., a timeout to the SIP INVITE, or an explicit SIP message capable of triggering LAR) after routing a call to this first preference, the call will attempt to use the second preference, trunk group 80. Trunk group 80 is a traditional ISDN-PRI trunk in the Avaya G450 Media Gateway that offers alternate access to the PSTN.

```
change route-pattern 19                                         Page   1 of   3
                    Pattern Number: 19  Pattern Name: To-VZ-via-SM
                             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: 8    0                    1                                       n   user
 2: 80   0                                                            n   user
 3:                                                                   n   user
 4:                                                                   n   user
 5:                                                                   n   user
 6:                                                                   n   user

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

Although not intended to be prescriptive, the configuration of trunk group 80 is summarized in the screens that follow. On page 1, observe that the trunk group type is ISDN.

```
change trunk-group 80                                           Page   1 of  21
                                TRUNK GROUP

Group Number: 80                  Group Type: isdn          CDR Reports: y
  Group Name: PSTN-ISDN                  COR: 1        TN: 1        TAC: 180
   Direction: two-way        Outgoing Display? n        Carrier Medium: PRI/BRI
 Dial Access? n              Busy Threshold: 255  Night Service:
Queue Length: 0
Service Type: public-ntwrk          Auth Code? n            TestCall ITC: rest
```

On page 5, observe that the trunk group members use the MM710 in slot 2V8 of the G450 Media Gateway shown in Section 11.5.1.4. The corresponding signaling group is signaling group 80.

```
change trunk-group 80                                           Page   5 of  21
                                 TRUNK GROUP
                                      Administered Members (min/max):   1/23
GROUP MEMBER ASSIGNMENTS                  Total Administered Members:  23

       Port    Code Sfx Name        Night           Sig Grp
  1: 002V801  MM710                                   80
  2: 002V802  MM710                                   80
  3: 002V803  MM710                                   80
  4: 002V804  MM710                                   80
  5: 002V805  MM710                                   80
  6: 002V806  MM710                                   80
```

Signaling group 80 uses port 24 of the MM710 in slot 2V8 of the G450 Media Gateway in a standard ISDN-PRI with facility associated signaling.

```
change signaling-group 80                                       Page   1 of   5
                                SIGNALING GROUP

 Group Number: 80             Group Type: isdn-pri
                    Associated Signaling? y          Max number of NCA TSC: 0
                       Primary D-Channel: 002V824     Max number of CA TSC: 0
                                                   Trunk Group for NCA TSC:
       Trunk Group for Channel Selection: 80
      TSC Supplementary Service Protocol: a          Network Call Transfer? n
```

Consider an example where the SIP trunk between Communication Manager and Session Manager is in-service and operational, but the end-end SIP Trunk path is not available to complete the call. For example, assume the end-end primary path is down (e.g., either the inside or the outside interfaces of Acme1 are out of service), and the secondary path has reached the configured maximum bandwidth for the location assigned to Acme2. Under these conditions, a new call attempt will be rejected by Session Manager with a SIP "606 Not Acceptable" message. For cases such as this, Communication Manager Look-Ahead Routing can automatically redirect the call to a traditional trunk such as an ISDN-PRI trunk in an Avaya gateway.

As another example, the following Communication Manager trace of an outbound PSTN call from station 30002 to PSTN number 908-848-5704 was captured while the Acme1 and Acme2 outside interfaces to Verizon were out of service. From the point of view of Communication Manager, the trunk group to Session Manager is in-service. Therefore, Communication Manager sends the call to Session Manager via the PE using trunk group 8 as illustrated previously. Session Manager exhausts its configured alternate routes, and rejects the call back to Communication Manager. Communication Manager uses LAR to "route-advance" to the next trunk in the route pattern, and completes the call using trunk group 80, a traditional ISDN-PRI trunk.

```
list trace station 30002                                          Page   1
                                LIST TRACE
time            data
08:38:33     active station    30002 cid 0x212
08:38:33     G711MU ss:off ps:20
             rgn:4 [65.206.67.11]:3126
             rgn:4 [65.206.67.62]:2060
08:38:38     dial 9190884857 route:ARS
08:38:38     term trunk-group 8    cid 0x212
08:38:38     dial 919088485704 route:ARS
08:38:38     route-pattern  19 preference 1  cid 0x212
08:38:38     seize trunk-group 8 member 9  cid 0x212
08:38:38     Calling Number & Name NO-CPNumber NO-CPName
08:38:38     Setup digits 9088485704
08:38:38     Calling Number & Name 7329450231 adevc_9620_H3
08:38:38     Proceed trunk-group 8 member 9  cid 0x212
08:38:39     denial event 1192: Temporary failure D1=0x8c9f D2=0x29
08:38:39     route-pattern  19 preference 1 unavailable cid 0x212
08:38:39     dial 919088485704 route:ARS
08:38:39     term trunk-group 80    cid 0x212
08:38:39     dial 919088485704 route:ARS
08:38:39     route-pattern  19 preference 2  cid 0x212
08:38:39     seize trunk-group 80 member 5  cid 0x212
08:38:39     Setup digits 19088485704
08:38:39     Calling Number & Name 7329450231 adevc_9620_H3
08:38:39     Proceed trunk-group 80 member 5  cid 0x212
08:38:39     Alert trunk-group 80 member 5  cid 0x212
             VOIP data from: [65.206.67.62]:2060
08:38:44     Jitter:0 0 0 0 0 0 0 0 0 0: Buff:13 WC:8 Avg:0
08:38:44     Pkloss:0 0 0 0 0 0 0 0 0 0: Oofo:0 WC:0 Avg:0
08:38:45     active trunk-group 80 member 5  cid 0x212
```

If multiple locations are used (e.g., multiple branch gateways that each have local trunking), Communication Manager location-based routing can be used so that different route patterns are chosen based on the location of the call originator. Each pattern could contain the SIP trunk to Session Manager as the preferred route, plus the appropriate local trunk that could serve the call originator should the Session Manager route be unusable.

11.7. References Applicable to Addendum 2

This section references documentation relevant to the addendum. Avaya product documentation is available at http://support.avaya.com. Acme Packet product documentation is available at http://www.acmepacket.com. A support account may be required to access the Acme Packet documentation.

Reference [PE] documents a configuration with verification results using Processor Ethernet on a main Communication Manager and an ESS for survivable SIP Trunking. The verifications in this document illustrate additional survivability considerations.

[PE] Sample Configuration Illustrating Avaya Aura™ Communication Manager SIP Trunking Using Processor Ethernet and Acme Packet Net-Net 4500 Session Director –
Issue 1.0
https://devconnect.avaya.com/public/flink.do?f=/public/download/interop/CM-PE-NN4500.pdf

Reference [CLAN] documents a similar configuration to [PE] using survivable SIP Trunks signaled from C-LAN interfaces rather than processor Ethernet.

[CLAN] Sample Configuration Illustrating Avaya Aura™ Communication Manager SIP Trunk Survivability with Enterprise Survivable Server and Acme Packet Net-Net 4500 Session Director, Issue 1.0
https://devconnect.avaya.com/public/flink.do?f=/public/download/interop/CM-ESS-NN4500.pdf

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

[SM1] *Administering Avaya Aura™ Session Manager*, Document Number 03-603324, Release 5.2, November 2009.
http://support.avaya.com/css/P8/documents/100068081