Avaya Solution & Interoperability Test Lab

Application Notes for Avaya Aura™ Communication Manager 5.2.1, Avaya Aura™ Session Manager 5.2, and Acme Packet Net-Net 3800 Integration with Skype Connect R1.3 – Issue 1.0

Abstract

These Application Notes describe the steps to configure the Avaya Aura™ SIP trunk solution with Skype Connect R1.3. The Avaya SIP trunk architecture consists of Avaya Aura™ Communication Manager (version 5.2.1), and Avaya Aura™ Session Manager (version 5.2).

The Skype Connect R1.3 service referenced within these Application Notes is designed for business customers with an Avaya SIP trunk solution. The service provides bi-directional 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.

Testing was conducted at the Avaya Solution & Interoperability Test Lab utilizing a traditional Internet T1 ISP circuit for accessing the Skype Connect 1.3 service directly over the Internet.

Table of Contents

1. Introduction

These Application Notes describe the steps to configure the Avaya SIP trunk solution with Skype Connect using an Internet-based connection. Skype Connect enables a business to use their Skype Connect certified hardware to take advantage of Skype's global calling rates to landline and mobile phones. Also, businesses may choose to purchase separately Skype's online numbers to receive calls. Access to a broadband Internet connection is required.

The Skype Connect service uses multiple session border controllers (also called service nodes) in the Skype network to deliver service redundancy. The Avaya SIP trunk architecture consists of Avaya Aura™ Communication Manager (version 5.2.1), Avaya Aura™ Session Manager (version 5.2), and Avaya Aura™ System Manager (version 5.2). Various Avaya H.323, digital, and analog stations are also included. While not the focus of this testing, a SIP-integrated Avaya Modular Messaging (version 5.2) system was used to provide enterprise voicemail call coverage for Avaya telephones. For an illustrative example of configuring Avaya Modular Messaging as a SIP-based centralized voicemail system see **Reference [1]**.

In the reference configuration **shown in Figure 1,** a single Acme Packet Net-Net 3800 was used as the edge device residing on the customer network and was used to interface to the Skype Connect service over a broadband Internet connection. In addition, the Acme Packet SBC provided SIP header manipulation and Avaya Customer Premise Equipment (CPE) topology hiding functionality.

Avaya Aura™ Session Manager serves 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 Skype Connect service 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 calls have dedicated inbound and outbound SIP trunks provisioned on Avaya Aura™ Communication Manager. This allows specific voice parameters to be provisioned (e.g. codec selection) as well as specific SIP trunk parameters to be set.

For more information on the Skype Connect service, see **Reference [7]**.

1.1. Skype Connect SBC Redundancy

A single Acme Packet Net-Net 3800 can be programmed to ensure that SIP trunk calls can be automatically rerouted to bypass SBC failures due to network or component outages. Redundancy for outbound calls from the Avaya CPE to the Skype Connect service was achieved by programming "sag-recursion" on the Acme Packet Net-Net 3800 and a "session-group" pointing to two different SBCs in Skype's network. For inbound calls from the Skype Connect service to the Avaya CPE, Skype Connect will automatically re-deliver the call to the Avaya CPE via Skype's secondary SBC. In the reference configuration, the Acme Packet Net-Net 3800 resides at the edge of the customer network.

1.2. Reference Configuration

Figure 1 illustrates the reference configuration located in the Solution and Interoperability Test Lab. All of the Avaya CPE is located on a private IP network. The “inside” interface of the Acme Packet SBC is also connected to this private network. The “outside” interface of the Acme Packet SBC is connected to a Juniper edge router that provides access to the Internet via a traditional T1 connection. This Internet connection is used for traditional Internet access as well as access to the Skype Connect service.

The Avaya CPE location simulates a customer site and uses private IP addressing. At the edge of the Avaya CPE location, the Acme Packet SBC provides NAT functionality that converts the private IP addressing to public addressing that is passed to the Skype Connect service, thus hiding the Avaya CPE network topology.

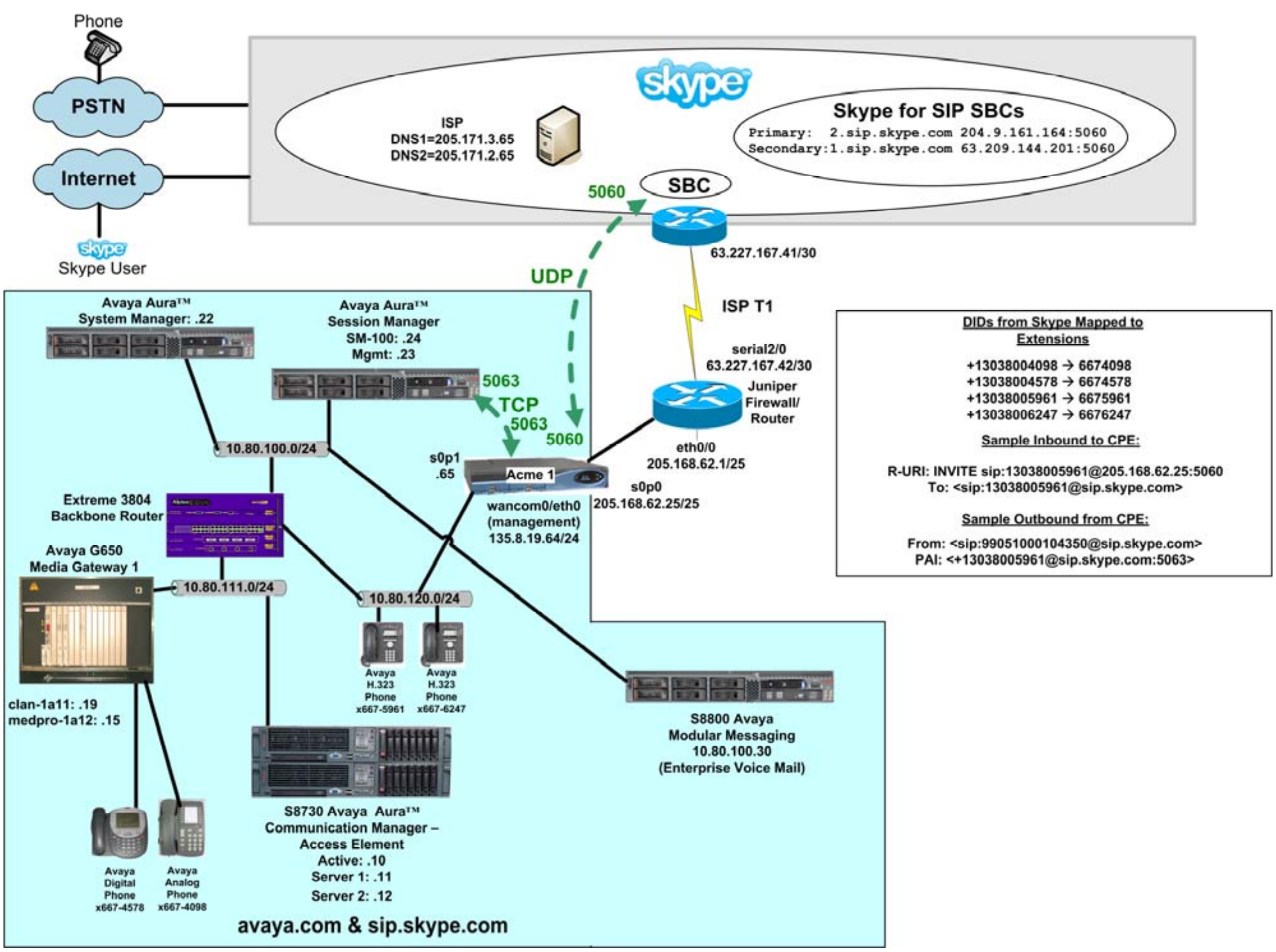

Figure 1: Reference Configuration

The installation and provisioning of the ISP T1 circuit is not part of the Skype Connect service.

For inbound calls, Skype online number were provisioned that provided Direct Inward Dial (DID) 11 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 Skype Connect service used a domain of *sip.skype.com.* The Avaya CPE environment was assigned a domain of *avaya.com*.

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

Note – The domains and IP addressing specified in these Application Notes apply only to the reference configuration shown in **Figure 1**. Skype Connect customers will use their own domains and IP addressing as required.

- Skype Connect domain
  - *sip.skype.com*
- Avaya CPE domain
  - *avaya.com*
- Acme Packet Net-Net 3800 SBC
- Avaya Aura™ Communication Manager
  - SIP trunk for inbound/outbound voice traffic
    - Voice
      - Signaling Group defined with Far-end Domain field specifying the Skype Connect domain
      - Signaling Group defined with Near-end Listen Port 5063
      - Trunk components assigned to IP Network Region 68
      - IP Network Region 68 specifies Skype Connect domain and IP Codec Set 5
      - IP Codec Set 5 specifies G.729
- Avaya Aura™ Session Manager
  - Route all inbound and outbound SIP calls based on request URI header information
  - Provide digit conversion functionality (converting Skype Connect 11 digit numbers to 7 digit Avaya Aura™ Communication Manager extensions and vice-versa) for inbound and outbound calls (see **Section 4.3.2**)
- Avaya Aura™ Communication Manager running on Avaya S8730 Servers with an Avaya G650 Media Gateway
- Avaya 9600 Series IP telephones using the H.323 software bundle
- Avaya 2420 Digital phones
- Analog phones

1.2.1 Audio Codec

A specific audio codec can be implemented for calls that utilize the Skype Connect service. This can be achieved on Avaya Aura™ Communication Manager by assigning an IP Codec Set to be used for inter-region communications between the IP Network Region assigned to Avaya CPE phones and the IP Network Region assigned to the Skype Connect service. In the reference configuration, G.729 was used for calls between the Avaya CPE and the Skype Connect service. G.711MU is also supported.

1.2.1.1 Inbound Calls to Avaya Aura™ Communication Manager

In order to accept calls from the Skype Connect domain (*sip.skype.com*), Avaya Aura™ Communication Manager will listen on port 5063 for these calls. The signaling group Near-end Listen Port is set to port 5063 and the Far-end Domain field is set to *sip.skype.com*. In addition, the Far-end Network Region associated with the Skype Connect service was set to an IP Network Region with an Authoritative Domain value of *sip.skype.com*.

1.2.1.2 Outbound Calls from Avaya Aura™ Communication Manager

Outbound voice calls are processed by Avaya Aura™ Communication Manager based on Automatic Route Selection (ARS) of the called number. The ARS table selects different route patterns based on the called number and the route pattern will direct the outbound call to the Skype Connect trunk.

1.2.2 Dialing Examples

The following are examples of outbound and inbound voice calls.

Given:

- Station 6675961
- Inbound/Outbound SIP trunk 68

Inbound

- Voice
    - PSTN dials Skype Connect online DID number (13038005961) and the Skype Connect service sends the call to the Acme Packet SBC at the Avaya CPE.
    - The Acme Packet passes the call to Avaya Aura™ Session Manager. Avaya Aura™ Session Manager performs digit conversion, changes the 11 digit DID number to the associated Avaya Aura™ Communication Manager extension (6675961), and sends the call to Avaya Aura™ Communication Manager C-LAN board to port 5063.
    - The call arrives on inbound/outbound trunk 68 and connects to station 6675961 using the G729 audio codec.

Outbound

- Voice
    - Avaya Aura™ Communication Manager voice stations first dial 9 followed by an 11 digit number (13035381762).
    - ARS sends the call to Route Pattern 68. Route Pattern 68 specifies trunk 68.

- The call will select trunk 68 and Avaya Aura™ Communication Manager sends the call via the C-LAN to Avaya Aura™ Session Manager specifying:
  - Port 5063
  - G729 audio codec
  - The Skype Connect domain
    - *sip.skype.com*
- Avaya Aura™ Session Manager performs digit manipulation as necessary and sends the call to the Acme SBC.
- The Acme SBC performs header manipulation on the From header in the SIP Invite as follows:
  - From: <sip:99051000104350@sip.skype.com>
    - The user part in the From header is the Skype-assigned user name. The user name consists of a 14 digit number.
    - The domain part in the From header must always be *sip.skype.com* in order to conform to the Skype Connect service requirements.
- The Acme SBC sends the call to the Skype Connect service node.

1.2.3 Local to Foreign Domain Conversion for Outbound Calls

As mentioned in **Section 1.2**, the Avaya CPE environment used a domain of *avaya.com*, and the Skype Connect service used a domain of *sip.skype.com.* For outbound calls, the Skype Connect service requires that the domain be *sip.skype.com* in the SIP request URI. In the reference configuration, this was accomplished in Avaya Aura™ Communication Manager by setting the Far-end Domain field of the outbound signaling group form to *sip.skype.com.* This setting will result in Avaya Aura™ Communication Manager sending a SIP request URI to Avaya Aura™ Session Manager with the format:

<called number>@ sip.skype.com

Avaya Aura™ Session Manager forwards this URI to the Acme SBC for transmission to the Skype Connect service.

1.3. Known Limitations

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

- Skype Connect is currently U.S. only. The service will be introduced in other regions at a later stage.
- Skype Connect does not support calls to the emergency service. Another PSTN trunk must be provisioned in Avaya Aura™ Communication Manager to route calls to the emergency service.
- Porting of existing PSTN numbers (DIDs) to Skype Connect is not supported.
- Access to a broadband internet connection is required.
- Maximum of 300 simultaneous calls per SIP Profile. A company may have multiple SIP Profiles.
- Maximum 99 Online Numbers per SIP Profile. Sequential number block (DID) purchases will be introduced at a later stage.
- Call processing tones are locally generated by the SIP User-Agent.
- Premium-rated numbers (1-900, 1-976) are blocked.
- DNS A records are supported for Skype Connect service node name resolution, while DNS SRV records will be introduced at a later stage.
- The SIP REFER request is not supported for call redirection/transfer.
- SIP 3xx Redirect Responses are not supported.
- SIP over TLS is not currently supported by Skype Connect .
- SRTP is not supported.
- T.38 fax is not supported.
- RTCP and RTCP XR are not supported.
- IP TOS or DiffServ QoS markings are neither set nor honored, therefore Skype Connect cannot guarantee the end-to-end voice quality. Service Level Agreements (SLAs) are not available.
- G.711A/mu-law, G.729 codecs are supported.
- E.164 International number format must be used for all calls.
- Skype Connect calls are limited to 4 hours.
- SIP Profile AOR expiry timer is set to 45 seconds for SIP User-Agents registering from behind a NAT router.
- SIP Profile AOR expiry timer is set to 300 seconds for SIP User-Agents registering directly with Skype Connect (without NAT).
- Only one AOR per SIP Profile is allowed.
- Skype Connect is not guaranteed to work with credit card machines, franking (stamping) machines and alarm systems or other services which use a regular phone line with a modem connection.
- Calls from Communication Manager extensions that activate Calling Party Number (CPN) Blocking will result in a caller id of 000-012-3456 or another bogus number.
- This solution does currently support outbound SIP calls to Skype names.
- A DTMF "tone leakage" interoperability issue was occasionally observed with Skype Connect. See **Appendix B** for more information.

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 S8730 Servers	-	-
Avaya Aura™ Communication Manager	-	R015x.02.1.016.4 with SP1 (17959)
Avaya G650 Media Gateway IPSI – TN2312BP CLAN – TN799DP MEDPRO – TN2302AP	 HW15 FW40 HW01 FW38 HW2 FW54	- - -
Avaya Aura™ Session Manager	-	5.2.1.1.521012 – 01-14-2010
Avaya Aura™ System Manager		5.2.0.8.27
Avaya 9620 and 9630 H.323 IP Telephones	-	3.110b (H.323)
Avaya 2420 Digital Phones	-	-
Analog Phones	-	-
Avaya Modular Messaging	-	5.2 (9.2.150.13)
Acme Packet Net-Net 3800	-	SCX6.2.0 MR-3 GA (Build 619)
Skype (for PC)	-	4.2.0.169

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 the Skype Connect service, in compliance with existing support agreements for Avaya Communication Manager release 5.2.1 and Avaya Aura™ Session Manager 5.2, and in conformance with the integration guidelines as specified in the body of this document.

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 Skype Connect service.

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 S8730 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 S8730 Servers. The Avaya CPE site also contained Avaya H.323, Avaya Digital and analog phones.

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.

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 Skype Connect service and any other SIP trunking applications. Be aware that for each call between a non-SIP endpoint at the Avaya CPE and the Skype Connect service one SIP trunk is used for the duration of the call.

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

IP PORT CAPACITIES                                              USED
                     Maximum Administered H.323 Trunks: 500   30
           Maximum Concurrently Registered IP Stations: 18000 6
             Maximum Administered Remote Office Trunks: 0     0
Maximum Concurrently Registered Remote Office Stations: 0     0
              Maximum Concurrently Registered IP eCons: 3     0
  Max Concur Registered Unauthenticated H.323 Stations: 100   0
                        Maximum Video Capable Stations: 10    0
                   Maximum Video Capable IP Softphones: 10    0
                       Maximum Administered SIP Trunks: 1000  56
  Maximum Administered Ad-hoc Video Conferencing Ports: 10    0
   Maximum Number of DS1 Boards with Echo Cancellation: 0     0
                             Maximum TN2501 VAL Boards: 128   1
                     Maximum Media Gateway VAL Sources: 10    0
           Maximum TN2602 Boards with 80 VoIP Channels: 128   0
          Maximum TN2602 Boards with 320 VoIP Channels: 128   2
   Maximum Number of Expanded Meet-me Conference Ports: 5     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  11
                                OPTIONAL FEATURES

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

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

3. On **Page 4** of the **System-Parameters Customer-Options** form, verify that the **IP Trunks** and **ISDN-PRI** features are enabled.

```
display system-parameters customer-options                      Page   4 of  11
                                OPTIONAL FEATURES

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

           IP Attendant Consoles? y
```

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

3.1.1 Dial Plan

In the reference configuration the Avaya CPE environment uses seven digit local extensions such as 667-5961. Trunk Access Codes (TAC) are 3 digits in length and begin with #. 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 **667**
     2. In the **Total Length** field enter **7**
     3. In the **Call Type** field enter **ext**
   - TAC codes:
     1. In the **Dialed String** field enter **#**
     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
     667          7    ext
     #            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.

- **ASM1** and **10.80.100.24** are the **Name** and **IP Address** of the Avaya Aura™ Session Manager SIP Routing Interface
- **clan-1a11** and **10.80.111.19** are the **Name** and **IP Address** of the C-LAN signaling processor in the G650 Media Gateway
- **medpro-1a12** and **10.80.111.15** are the **Name** and **IP Address** of the Media Processor in the G650 Media Gateway
- **gateway1** and **10.80.111.1** 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
ASM1                10.80.100.24
clan-1a11           10.80.111.19
medpro-1a12         10.80.111.15
gateway001          10.80.111.1
```

Figure 6: IP Node Names Form

3.1.3 IP-Network-Regions

Two IP Network Regions are defined in the reference configuration. Avaya Aura™ Communication Manager components that interface to the Skype Connect service via Avaya Aura™ Session Manager are assigned to IP Network Region **68**. Avaya telephones are assigned to IP Network Region **1**.

Avaya Component	IP_Network-Region
C-LAN	68
MedPro	68
SIP Trunk 68	68
Avaya Telephones	1

Table 2 – IP Network Regions

The SIP trunk IP Network Regions are defined in the SIP Signaling Group form Far-end Network Region parameter (see **Section 3.1.5**).

IP 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 MEDPRO 01A02 TN2602        XFire            /24   gateway1         1    n
                              10.80.111.13
 y C-LAN  01A03 TN799  D      CLAN-1           /24   gateway1         1    n
                              10.80.111.16
 y C-LAN  01A07 TN799  D      CLAN-2           /24   gateway1         1    n
                              10.80.111.17
 y VAL    01A08 TN2501        VAL              /24   gateway1              n
                              10.80.111.18
 y C-LAN  01A11 TN799  D      clan-1a11        /24   gateway1         68   n
                              10.80.111.19
 y MEDPRO 01A12 TN2602        medpro-1a12      /24   gateway1         68   n
                              10.80.111.15
```

Figure 7: IP Interface IP Network Region Assignments

The IP 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 1a11                                        Page   1 of   3
                                IP INTERFACES


                  Type: C-LAN
                  Slot: 01A11        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: 68                              Gatekeeper Priority: 5

                                IPV4 PARAMETERS
             Node Name: clan-1a11
           Subnet Mask: /24
     Gateway Node Name: gateway1

         Ethernet Link: 4
         Network uses 1's for Broadcast Addresses? y
```

Figure 8: IP Interface IP Network Region Assignment

The **IP Network Region** form specifies the parameters used by the Avaya Aura™ Communication Manager components and how components defined to different regions interact with each other. The following IP Network Region assignments are 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 IP Codec Set form configurations.

Inter Region Communication	IP Codec Set used
Region 1 to Region 1	Codec Set 1
Region 1 to Region 68	Codec Set 5
Region 68 to Region 68	Codec Set 5

Table 3: Inter Region Codec Assignments

Note – Avaya IP telephones inherit the IP Network Region of the C-LAN (or procr for Avaya Servers that have the procr interface enabled) through which they register. If an IP phone registers to a C-LAN that is assigned IP Network Region **1**, that phone will become part of IP Network Region **1**. If an IP phone needs to be defined to a different IP Network Region regardless of registration, this may be performed with the ***ip-network-map*** command. See **Reference [2]**

3.1.3.1 IP Network Region 1

IP Network Region 1 is defined for Avaya Aura™ Communication Manager telephones. The IP 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** for local Avaya telephones. In the reference configuration, the Authoritative Domain is ***avaya.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: avaya.com
    Name:
MEDIA PARAMETERS                Intra-region IP-IP Direct Audio: yes
      Codec Set: 1              Inter-region IP-IP Direct Audio: yes
   UDP Port Min: 2048                      IP Audio Hairpinning? n
   UDP Port Max: 65535
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 9: IP Network Region 1 – Page 1

2. On **Page 7** of the **IP Network Region** form:
    - Define the **Codec Set** used for inter-region communications. **Codec Set 5** is entered for communications with IP Network Region **68**.
    - 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 the reference configuration.

```
change ip-network-region 1                                      Page   7 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
 68   5     y    NoLimit                                             n
```

Figure 10: IP Network Region 1 – Page 7

3.1.3.2 IP Network Region 68

IP Network Region **68** is defined for SIP trunks. Provisioning is the same as for IP Network Region **1** except:

1. On **Page 1** of the **IP Network Region** form:
    - Configure the **Authoritative Domain** field to ***sip.skype.com***.
    - Set the **Codec Set** to **5** to be used for the corresponding calls within the IP Network Region.

```
change ip-network-region 68                                     Page   1 of  19
                               IP NETWORK REGION
  Region: 68
Location:         Authoritative Domain: sip.skype.com
    Name:
MEDIA PARAMETERS                Intra-region IP-IP Direct Audio: yes
      Codec Set: 5              Inter-region IP-IP Direct Audio: yes
   UDP Port Min: 2048                      IP Audio Hairpinning? n
   UDP Port Max: 65535
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 68 – Page 1

2. On **Page 3** of the **IP Network Region** form:

- Verify the **Codec Set** used for inter-region communications. Verify that for destination region **1** codec set **5** is entered for communications to/from IP Network Region **68**.

```
change ip-network-region 68                                 Page   3 of  19

 Source Region: 68    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    5     y    NoLimit                                             n
```

Figure 12: IP Network Region 68 – Page 3

3.1.4 IP Codec Sets

Two IP codec sets are defined in the reference configuration. One for local intra customer location calls (IP Codec Set **1**) and one for off network voice calls (IP Codec Set **5**). **Table 4** shows the audio codecs defined to each of these IP Codec Sets.

IP Codec Set	IP Network Region	Codecs Defined
1	1	G.711MU / G.729
5	68	G.729

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.729 is also specified as an option. Other codecs could be specified as well depending on local requirements. IP Codec Set **1** 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 set number.

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

```
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.729             n          2        20
```

Figure 15: IP Codec Set 1

3.1.4.2 Trunk Calls – IP Codec Set 5

G.729 was picked as the first option as it uses less bandwidth. G.711MU could be used but was not configured in the reference configuration. IP Codec Set **5** is associated with IP Network Region **68**.

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

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

```
change ip-codec-set 5                                          Page   1 of   2
                          IP Codec Set
    Codec Set: 5
    Audio        Silence      Frames   Packet
    Codec        Suppression  Per Pkt  Size(ms)
 1: G.729             n          2        20
```

Figure 15: IP Codec Set 5

2. On **Page 2** of the form:
    - Configure the **Fax** field to **off.** T.38 fax calls are not supported through the Skype Connect service.
    - Configure the **Fax Redundancy** field to **0.**
    - Other fields may be left at their default.

```
change ip-codec-set 5                                        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 5 – Page 2

3.1.5 SIP Trunk Groups

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

SIP Trunk Function	Avaya Aura^{TM} Communication Manager SIP Signaling Group/Trunk Group	Avaya Aura^{TM} Communication Manager SIP Signaling Group *Far-End Domain*	Avaya Aura^{TM} Communication Manager IP Network Region
Public Inbound/Outbound Voice	Trunk 68	*sip.skype.com*	68

Table 5: Avaya SIP Trunk Configuration

Note – In the SIP trunk configurations below (and in the Avaya Aura^{TM} 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 SIP Trunk

1. Using the ***add signaling-group 68*** command, configure the 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 Skype Connect service.
- Specify the C-LAN used for SIP signaling (node name **clan-1a11**) and Avaya Aura™ Session Manager (node name **ASM1**) 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 **5063** in the **Near-End** and **Far-end Listen Port** fields.
- Enter the value **68** into the **Far-end Network Region** field. This value is the **IP Network Region** defined in **Section 3.1.3.2**.
- Enter *sip.skype.com* in the **Far-end Domain** field.
- 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 Acme SBC.
- 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 68                                          Page   1 of   1
                                SIGNALING GROUP

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




   Near-end Node Name: clan-1a11             Far-end Node Name: ASM1
 Near-end Listen Port: 5063                Far-end Listen Port: 5063
                                        Far-end Network Region: 68
Far-end Domain: sip.skype.com

                                             Bypass If IP Threshold Exceeded? n
Incoming Dialog Loopbacks: eliminate                  RFC 3389 Comfort Noise? n
         DTMF over IP: rtp-payload            Direct IP-IP Audio Connections? y
Session Establishment Timer(min): 3                     IP Audio Hairpinning? n
         Enable Layer 3 Test? n                     Direct IP-IP Early Media? n
H.323 Station Outgoing Direct Media? n            Alternate Route Timer(sec): 30
```

Figure 19: Public SIP Trunk - Signaling Group 68

2. Using the ***add trunk-group 68*** command, add the SIP 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 **#68**.
      - Set the **Service Type** field to **public-ntwrk**.
      - Enter **68** as the **Signaling Group** number.
      - Specify the **Number of Members** used by this SIP trunk group (e.g. **6**). This number should correspond to the number of **Calling channels** assigned in the Skype Connect Profile Settings page as described in **Section 6.1**.

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

Group Number: 68                     Group Type: sip          CDR Reports: y
  Group Name: Skype Inbound/Outbound       COR: 1        TN: 1        TAC: #68
   Direction: two-way       Outgoing Display? n
 Dial Access? n                                   Night Service:
Queue Length: 0
Service Type: public-ntwrk          Auth Code? n

                                                       Signaling Group: 68
                                                     Number of Members: 6
```

Figure 20: Public SIP Trunk Group 68 – 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 68                                           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 SIP Trunk Group 68 – Page 3

c. On **Page 4** of the **Trunk Group** form:
  - Set the **Network Call Redirection** field to **n**. Skype Connect does not support SIP Refer which is controlled by this field.
  - Set the **Telephone Event Payload Type:** field to **101.**
  - Other values may be left at their default.

```
change trunk-group 68                                        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 SIP Trunk Group 68 – Page 4

3.1.6 Public Unknown Numbering – Basic Configuration

In the reference configuration, the extensions on Avaya Aura™ Communication Manager use a 7 digit dialing plan using extensions in the range 667xxxx. The **Numbering – Public/Unknown Format** form allows Avaya Aura™ Communication Manager to use these extensions as the calling party number for outbound calls. Otherwise, calls are sent without calling party number information and are delivered as *Anonymous* calls. 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. **6**).

- Set the **Ext Len** field to **7**.
- Set the **Ext Code** field to **667**.
- Set the **Trk Grp(s)** field to **68.**
- Set the **Total CPN Len** field to **7**. 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: 1
 7  667            68                       7          Maximum Entries: 9999
```

Figure 23: Numbering – Public/Unknown Format Form – Basic Configuration

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. This routing is also 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 a SIP trunk to the Avaya Aura™ Session Manager, which in turn completes the calls to the Skype Connect 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 **Numbering – Public/Unknown Format** 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: Dial Plan Analysis Table

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   9
                               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: *11
                       Answer Back Access Code:

      Auto Alternate Routing (AAR) Access Code: 8
    Auto Route Selection (ARS) - Access Code 1: 9     Access Code 2:
                 Automatic Callback Activation:        Deactivation:
Call Forwarding Activation Busy/DA: *22    All: *21    Deactivation: #21
   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:
            Conditional Call Extend Activation:        Deactivation:
                   Contact Closure   Open Code:          Close Code:
```

Figure 26: Feature Access Code 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:

    - 1303 (voice destination beginning with 1303)
    - 011 (international voice destination)

    For example, to specify how to route calls to dialed numbers beginning with 1303, enter the command ***change ars analysis 1303*** and enter the following values:
    - Set the **Dialed String** field to **1303**
    - Set the **Total Min** field to **11**
    - Set the **Total Max** field to **11**
    - Set the **Route Pattern** field to **68** (will direct the call to the SIP trunk)
    - Set the **Type** field to **fnpa**

Note – ARS will route based on the most complete match. For example, 13035381762 will match before 1303.

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
    1303                     11   11     68        fnpa         n
    011                      10   18     68        intl         n
```

Figure 27: ARS Digit Analysis Table

3.1.7.1.2 Route Patterns

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

1. Use the **change route-pattern** command to define the outbound SIP trunk group 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 ***68***.
     - Set the **FRL** field to ***0***.
     - All other values may be left at their default.

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

Figure 28: Route Pattern 68 – Outbound Calls

3.1.7.2 Incoming Calls

SIP trunk group 68 is also used for inbound voice calls. In the reference configuration, the Avaya Aura™ Session Manager is used to convert inbound Skype online 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 – If necessary, incoming called numbers may be changed to match a provisioned extension 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, 7 digit voice stations are provisioned with the extension format 667xxxx.

3.1.8.1 Voice Stations – Calling Party Number Block

Figure 30 shows an example of a voice extension (Avaya H.323 IP phone). Since the phone is an IP device, a virtual port **S00013** 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. 9630)
- Set the **Name** field to some value (e.g. Avaya H.323)

```
add station 6675961                                                Page   1 of   5
                                     STATION

Extension: 667-5961                      Lock Messages? n               BCC: 0
     Type: 9630                          Security Code: *                TN: 1
     Port: S00013                      Coverage Path 1: 3               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: 667-5961
            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

                                                         IP Video? n


                                              Customizable Labels? y
```

Figure 30: Station Extension – Avaya H.323 IP Phone – Page 1

On **Page 4** of the form:

- Select an empty button assignment and enter **cpn-blk.** This button will enable calling party number block on a per call basis on the phone. The user presses the cpn-blk button prior to dialing the called party number. This will result in an *Anonymous* call.
- Call appearances (**call-appr**) will appear automatically based on the station type.

```
change station 6675961                                          Page   4 of   5
                                     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: call-appr                          7:
 4: cpn-blk                            8:

    voice-mail Number: 6665000
```

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

3.1.9 Save Avaya Aura™ Communication Manager Provisioning

Enter the ***save translation*** command to save all programming.

4. Avaya Aura™ Session Manager Provisioning

This section provides the procedures for configuring Avaya Aura™ Session Manager as provisioned in the reference configuration. Avaya Aura™ Session Manager is comprised of two functional components: the Avaya Aura™ Session Manager server and the Avaya Aura™ System Manager management server. All SIP call provisioning and system programming 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 **References [4-5]**.

4.1. Network Interfaces

Avaya Aura™ Session Manager 5.2 is comprised of two main components, the server itself and the SM-100 card, which is embedded in the server. **Figure 36** shows the backplane of Avaya Aura™ Session Manager.

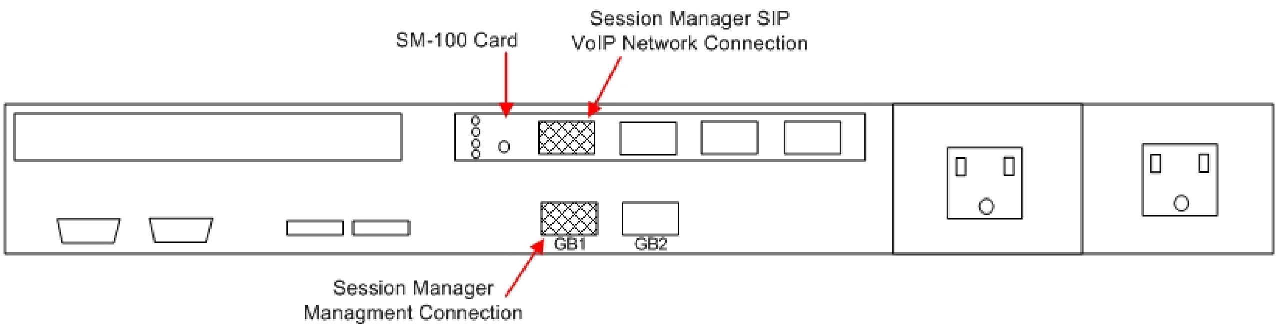

Figure 36 – Avaya Aura™ Session Manager Network Connections

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 may use a different network than the SM-100 connection.

4.2. System Manager

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

- **Network Routing Policy**
  - o **SIP Domains** - Define FQDNs that may send calls to Avaya Aura™ Session Manager.
  - o **Locations** – Logical/physical areas that may be occupied by SIP Entities.
  - o **SIP Entities** – Typically devices corresponding to the SIP telephony systems including Avaya Aura™ Session Manager and other devices such as SBCs.
  - o **Entity Links** – Connection information which define the SIP trunk parameters used by Avaya Aura™ Session Manager when routing calls to/from other SIP Entities.
  - o **Dial Patterns** – Matching digit patterns which govern to which SIP Entity a call is routed.
  - o **Routing Policies** - Policies that determine call routing between the SIP Entities based on applicable Dial Patterns.
  - o **Time Ranges** – Specified windows during which SIP call processing is permitted for 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 5.2, the URL to access the browser-based GUI of System Manager is ***https://<ip-address>/SMGR***. Log in with the appropriate credentials.

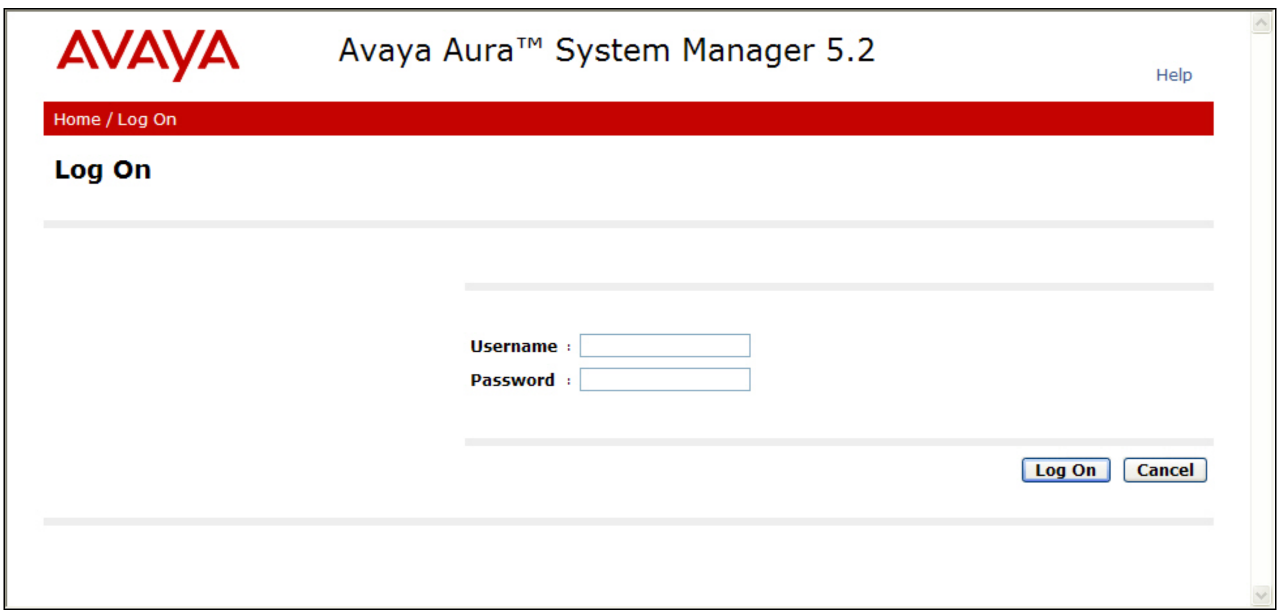

Figure 37: System Manager GUI Log On Screen

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.

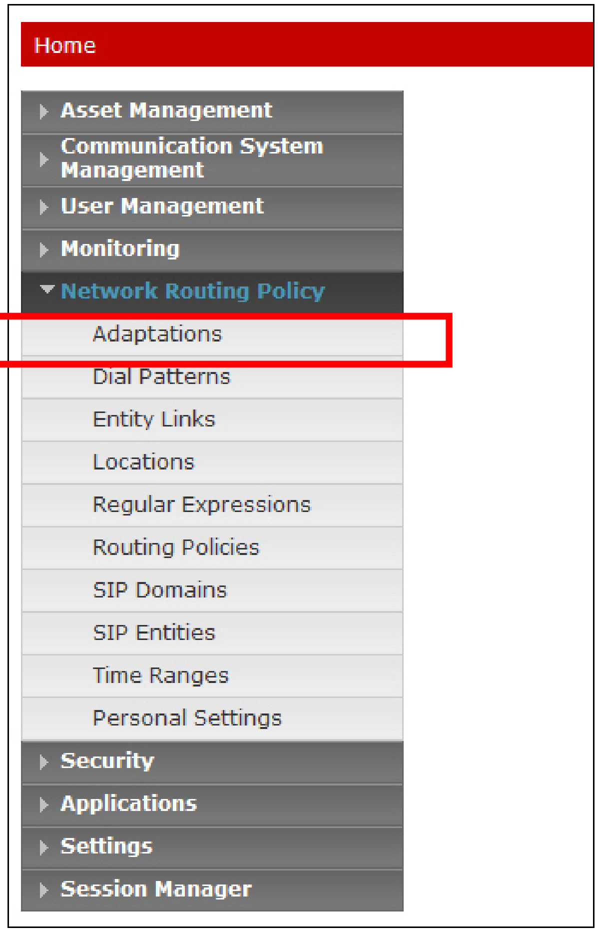

Figure 38: Network Routing Policy Menu

4.3.1 SIP Domains

In the reference configuration two SIP domains (FQDNs) are used. The Avaya CPE location is *avaya.com* and the Skype Connect service is *sip.skype.com*. The Skype Connect domain *sip.skype.com* is used for bi-directional calls between the Avaya CPE and the Skype Connect service. The Avaya CPE location uses *avaya.com for* calls internal to the Avaya CPE location. 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 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.

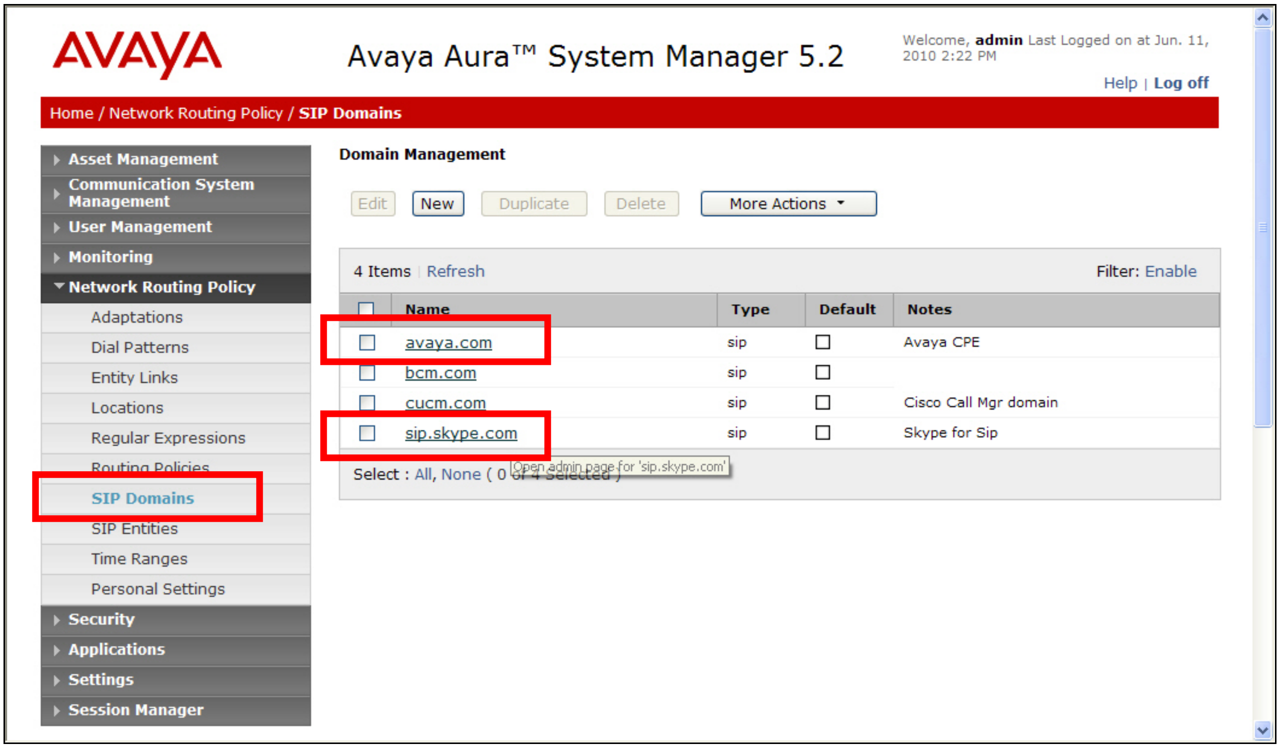

Figure 39: SIP Domain Menu

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. One of these adaptations is used in the reference configuration: DigitConversionAdapter.

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 (PAI) 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 Skype Connect, 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 SBC is outgoing.

1. Select **Adaptations** from the menu.
2. Select **New**.
3. Enter a descriptive name (e.g. **SkypeDigitConversionAdapter**).

4. Specify **DigitConversionAdapter** in the Module Name field.
5. Leave the **Module parameter** field blank.
6. Leave the **Egress URI Parameters** field blank (this is for adding additional parameters such as user=phone).
7. Enter a description in the **Notes** field if desired.

In the incoming example, Avaya Aura™ Communication Manager extension 6675961 will be converted to Skype Connect online number +13038005961 for calls going from Avaya Aura™ Communication Manager to Avaya Aura™ Session Manager.

8. In the **Digit Conversion for Incoming Calls to SM** section, click the **Add** button and enter:
   a. **Matching Pattern –** The digit string to match → **6675961**
   b. **Min –** The minimum number of digits → **7**
   c. **Max –** The maximum number of digits → **7**
   d. **Delete Digits –** The number of digits to delete → **3**
   e. **Insert Digits –** The digit to be inserted → **+1303800**
   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 to g for each incoming digit conversion.

In the outgoing example, Skype Connect online number 13038005961 will be converted to Avaya Aura™ Communication Manager extension 6675961 for calls going from Avaya Aura™ Session Manager to Avaya Aura™ Communication Manager.

9. In the **Digit Conversion for Outgoing Calls from SM** section, click the **Add** button and enter:
   a. **Matching Pattern –** The digit string to match → **+13038005961**
   b. **Min –** The minimum number of digits → **11**
   c. **Max –** The maximum number of digits → **11**
   d. **Delete Digits –** The number of digits to delete → **7**
   e. **Insert Digits –** The digit to be inserted → **667**
   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 steps a to g for each outgoing digit conversion.
10. When completed, the Adaptation Details window for SkypeDigitConversionAdapter will look like **Figure 40**.
11. Click on the **Commit** button.

In the reference configuration, Avaya Aura™ Communication Manager extensions were converted to Skype Connect online numbers and vice versa. Skype Connect uses the PAI to identify the caller ID that should be used for the outbound call from the Avaya CPE to the Skype Connect service.

Extension	Skype Online Number
6674098	+13038004098
6674578	+13038004578
6675961	+13038005961
6676247	+13038006247

Table 6: Extension/Skype Online Number assignments

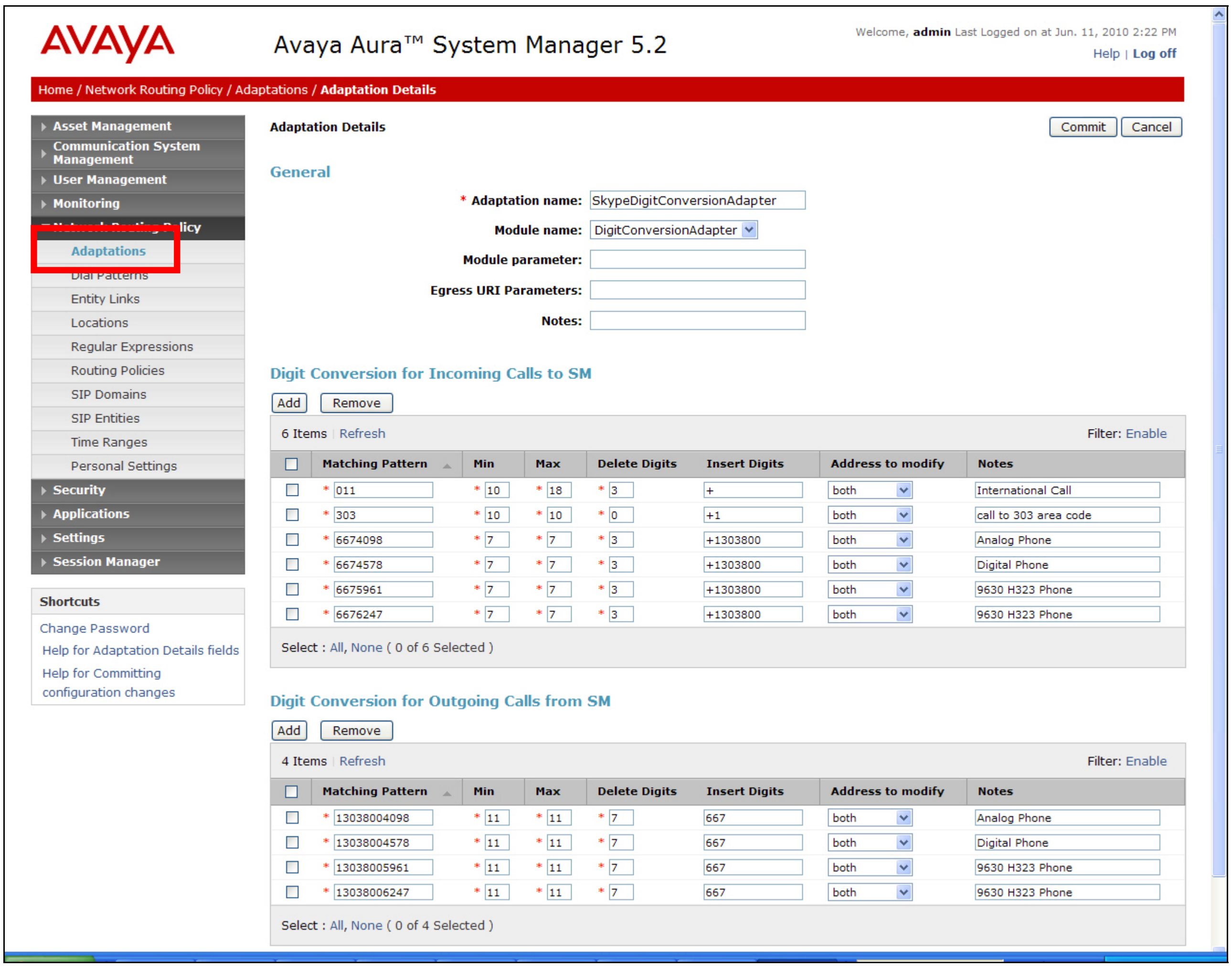

Figure 40: SkypeDigitConversionAdapter Adaptation Details

4.3.3 Locations

Locations are used to identify logical and/or physical locations where SIP Entities reside. Named locations are assigned with an IP Address Pattern. Locations may also be used for bandwidth management purposes for outbound calls from Avaya CPE to Skype, if required. In the reference configuration, multiple locations are defined for the Avaya CPE and one location is defined for the Acme SBC. However, the bandwidth management capability was not utilized.

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. AvayaCPE).
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. **10.80.111.***)
5. Enter a description in the **Notes** field if desired.
6. Repeat steps 3 to 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.

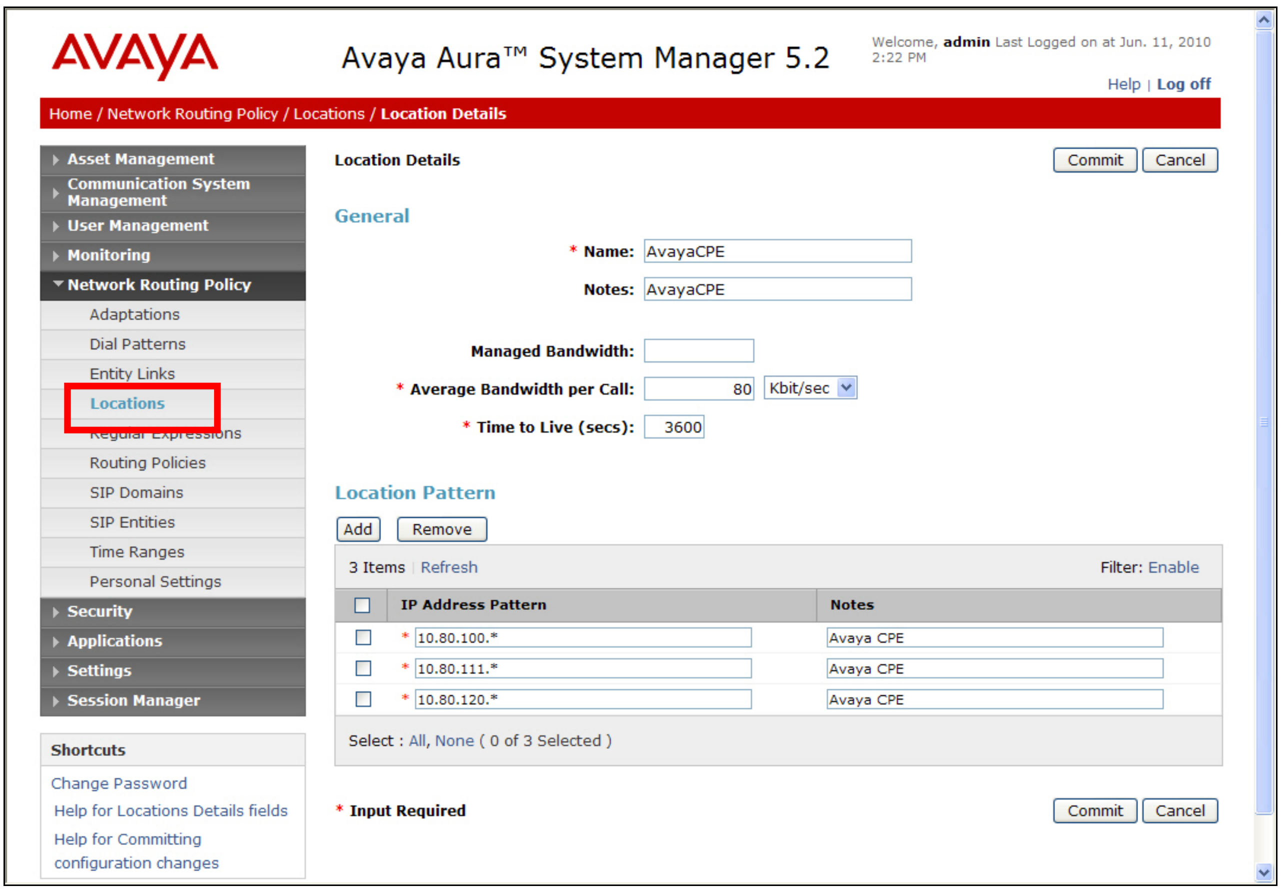

Figure 43: Location Details

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, SIP Entities are provisioned for:

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

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 name in the **Name** field.
   b. Enter the IP address for the SIP Entity (e.g. **10.80.111.19** 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 4.3.2**).
      i. For the C-LAN Entity in Avaya Aura™ Communication Manager, the **SkypeDigitConversionAdapter** adaptation is selected. This function is applied to the C-LAN Entity to convert Avaya extensions to Skype online numbers and vice versa depending on whether the call is inbound from Avaya Aura™ Communication Manager to Avaya Aura™ Session Manager or outbound from Avaya Aura™ Session Manager to Avaya Aura™ Communication Manager.
      ii. For Acme SBC Entity, no adaptation is defined in the reference configuration.
   f. From the Locations drop down menu select **AvayaCPE**.
   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

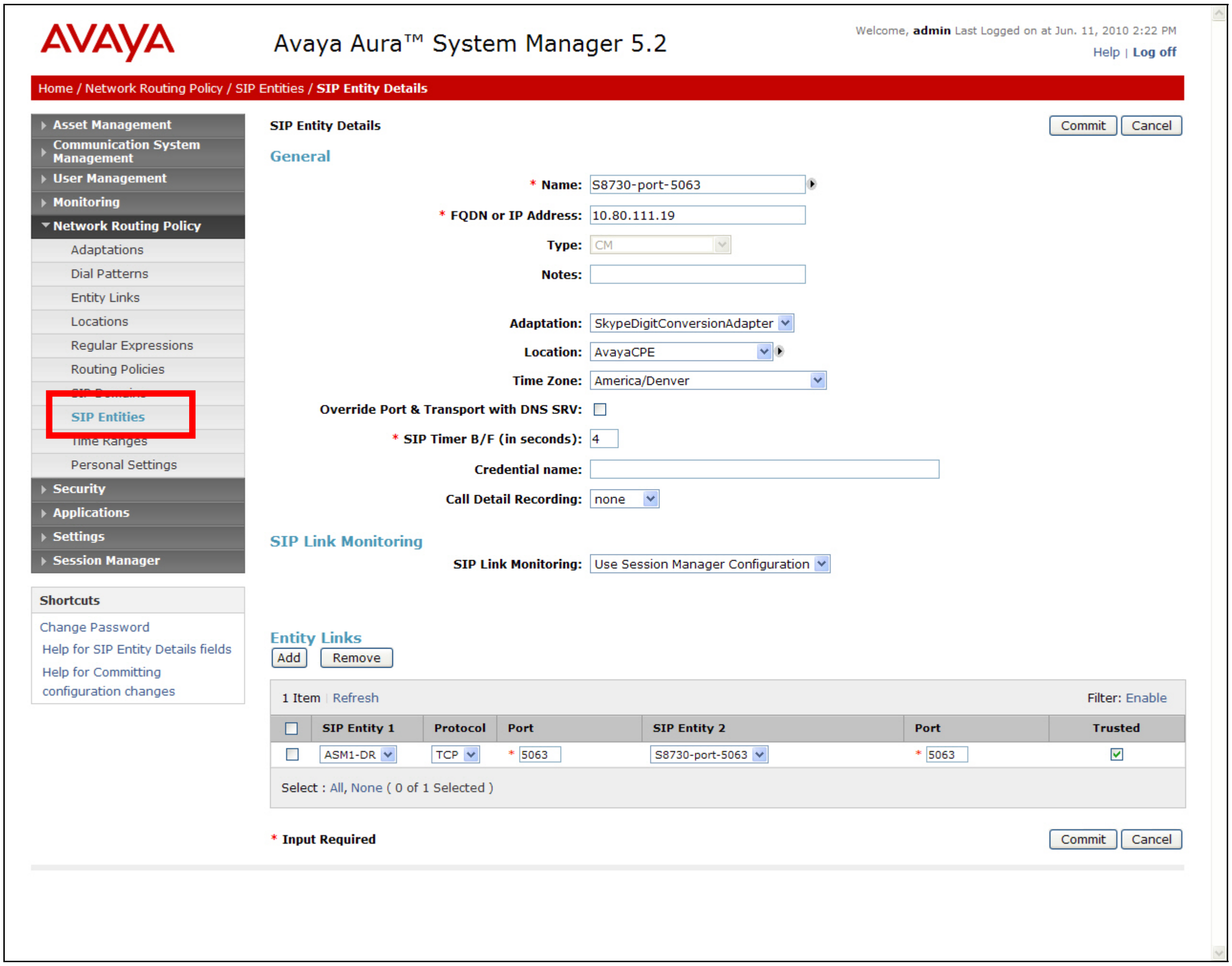

Figure 44: C-LAN SIP Entity Details

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 are 5063, TCP and the Skype Connect domain.

The following SIP Entity values are specified in the reference configuration. SIP Entity Type "Other" can be used for the Acme Packet SBC SIP Entity.

Name	IP Address	Type	Adaptation	Location	Port	Protocol	Domain
S8730-port-5063	10.80.111.19	CM	SkypeDigitConversionAdapter	AvayaCPE	5063	TCP	Skype Connect
ASM1-DR	10.80.100.24	Session Manager	-	AvayaCPE	5063	TCP	Skype Connect
ACME1	10.80.120.65	Other	-	AvayaCPE	5063	TCP	Skype Connect

Table 7: SIP Entity Provisioning

Figure 45 shows a complete SIP Entities list. The SIP Entities relevant to the reference configuration are listed in **Table 7.**

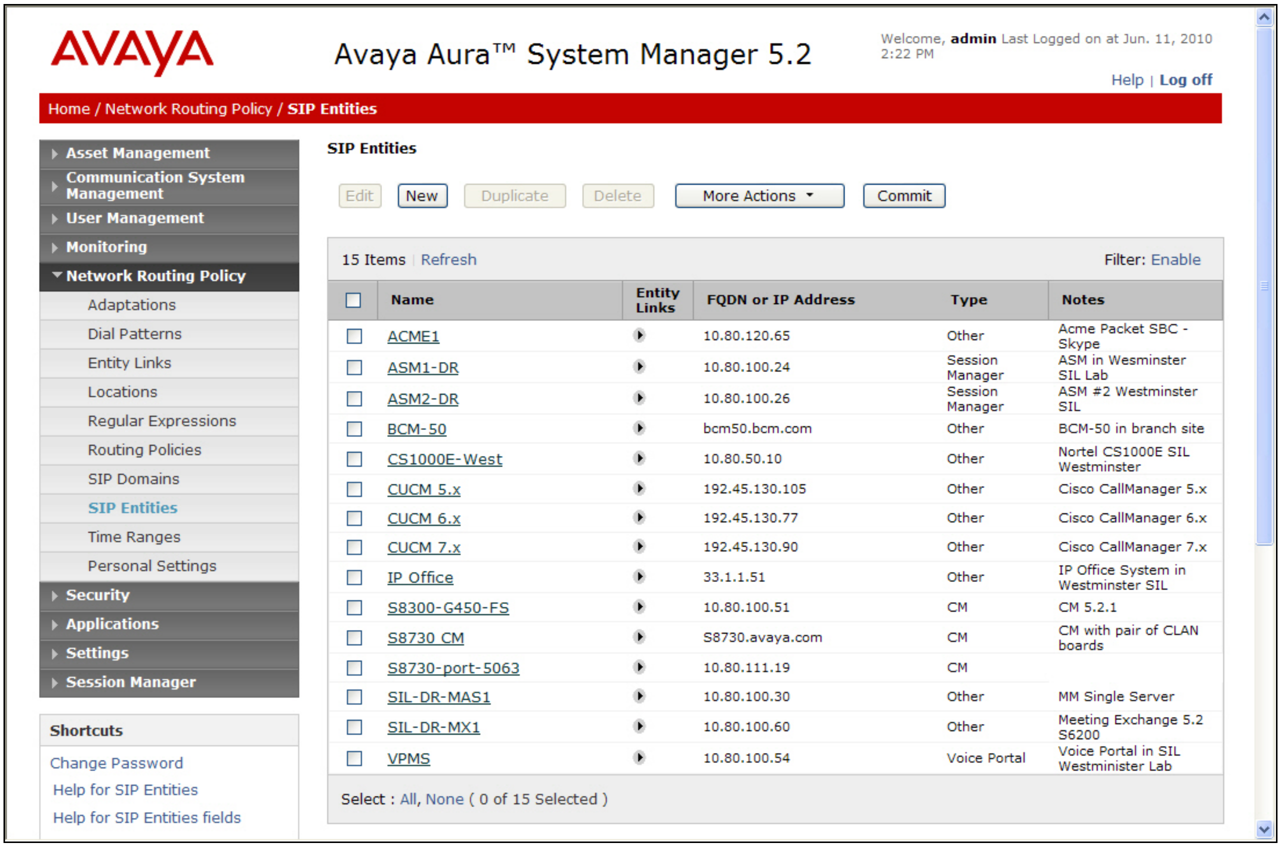

Figure 45: Completed SIP Entities Form

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 Acme Packet SBC (ACME1)
- The Avaya Aura™ Communication Manager C-LAN (S8730_port_5063)

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 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-DR**).
3. In the **Port** field enter **5063**.
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 **5063**.

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.

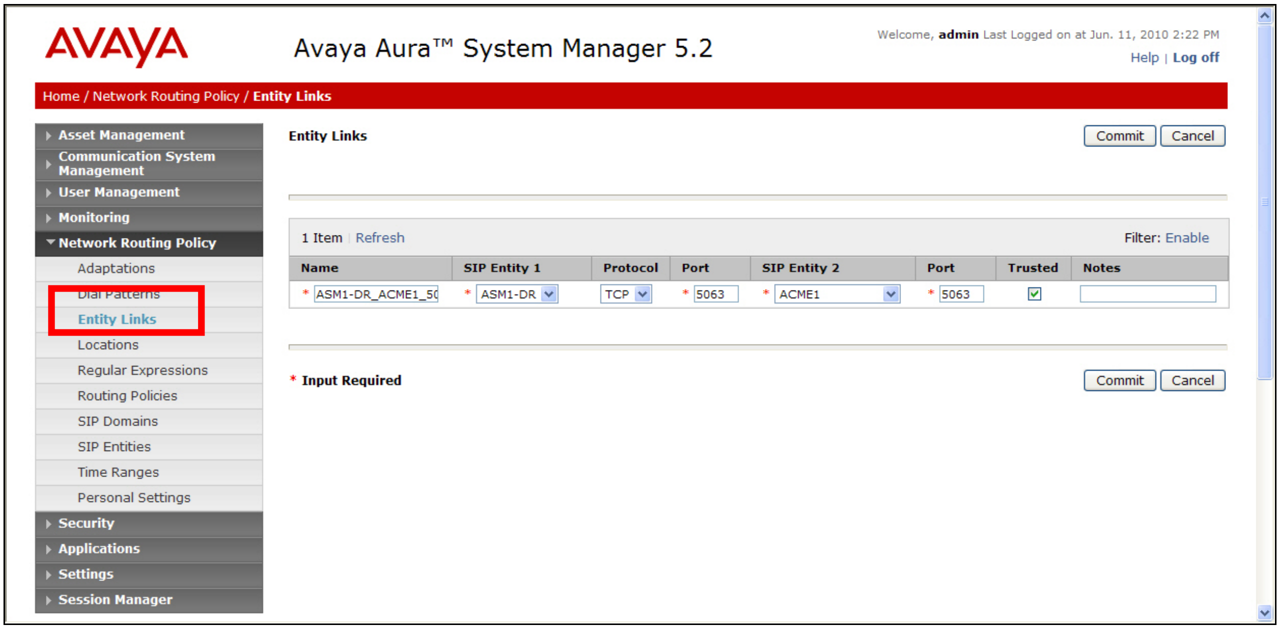

Figure 46: Entity Link – ACME1 SBC

10. Click on **New** and repeat steps 1 to 9 for the **C-LAN** Entity Link, specifying **S8730_port_5063** in the **SIP Entity 2** drop down menu. Note that port 5063 is used for the Entity Link between the Session Manager and the Communication Manager C-LAN.

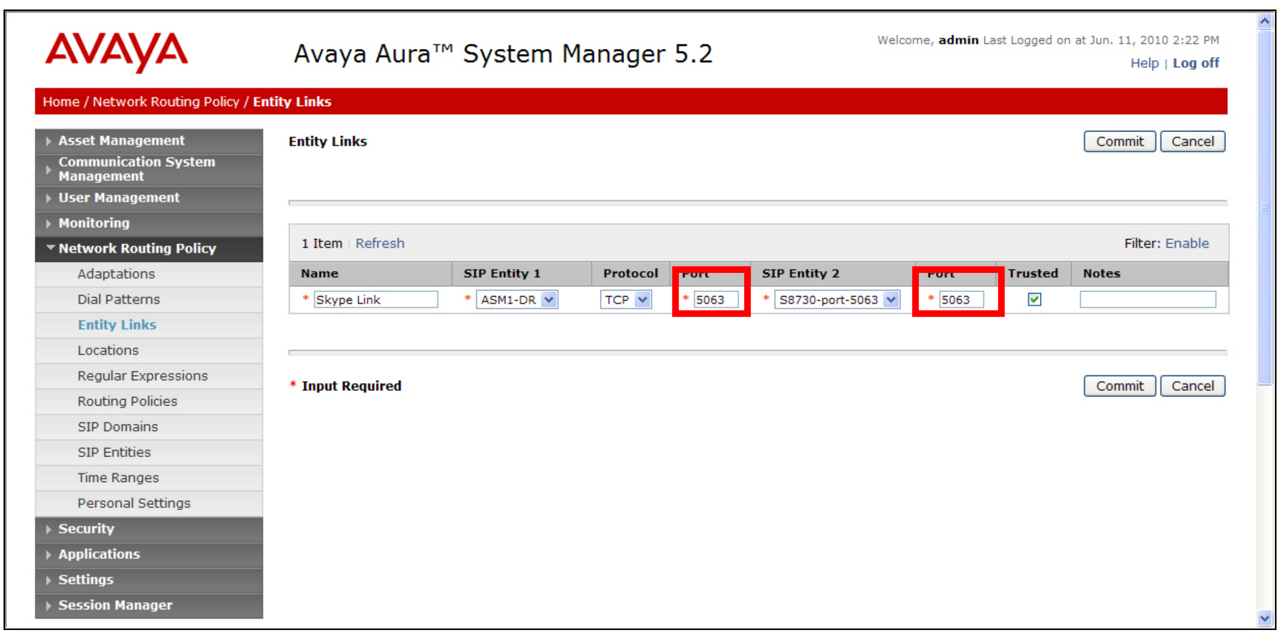

Figure 47: Entity Link – Communication Manager C-LAN

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

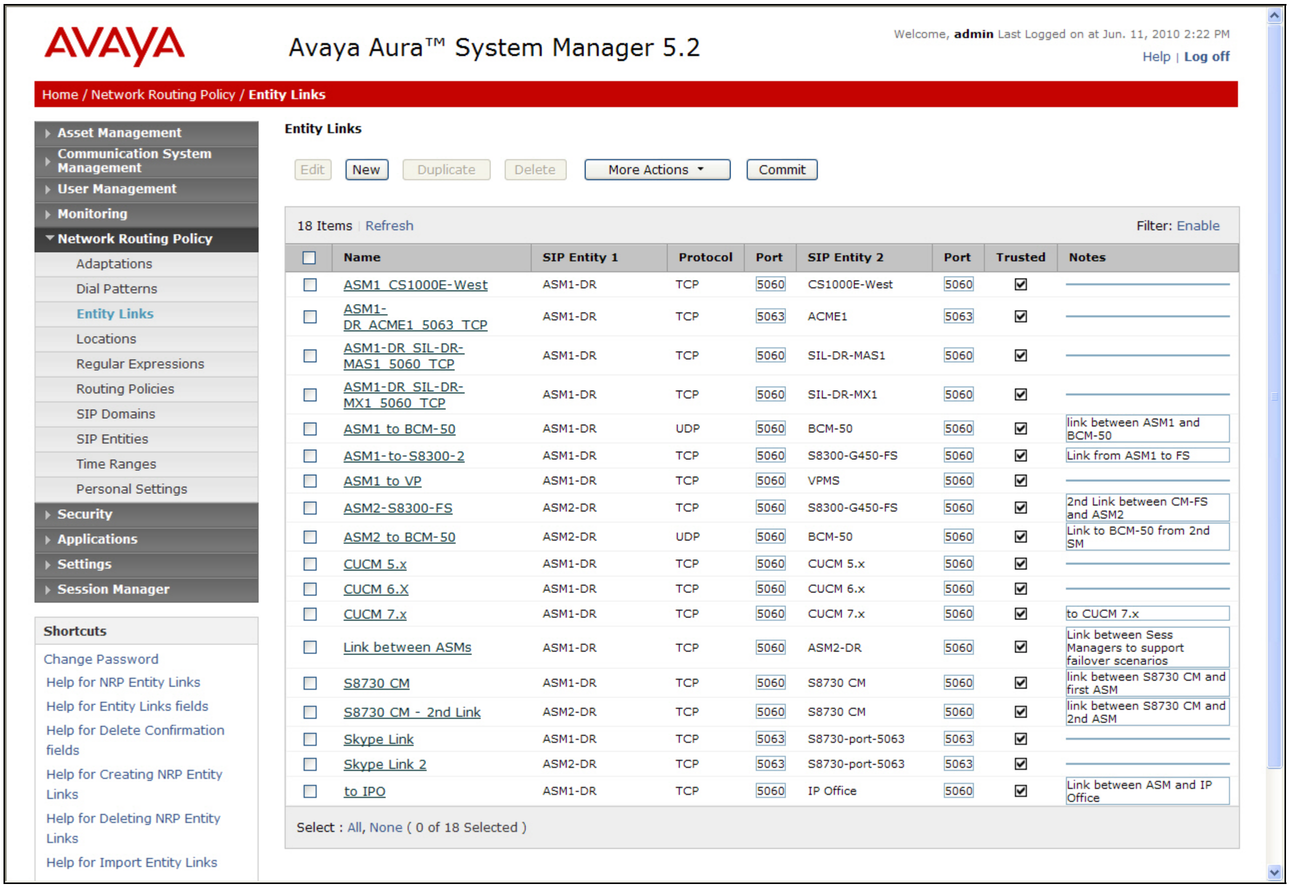

Figure 48: Completed Entity Links Form

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 name in the **Name** field (e.g. **24/7**).
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.

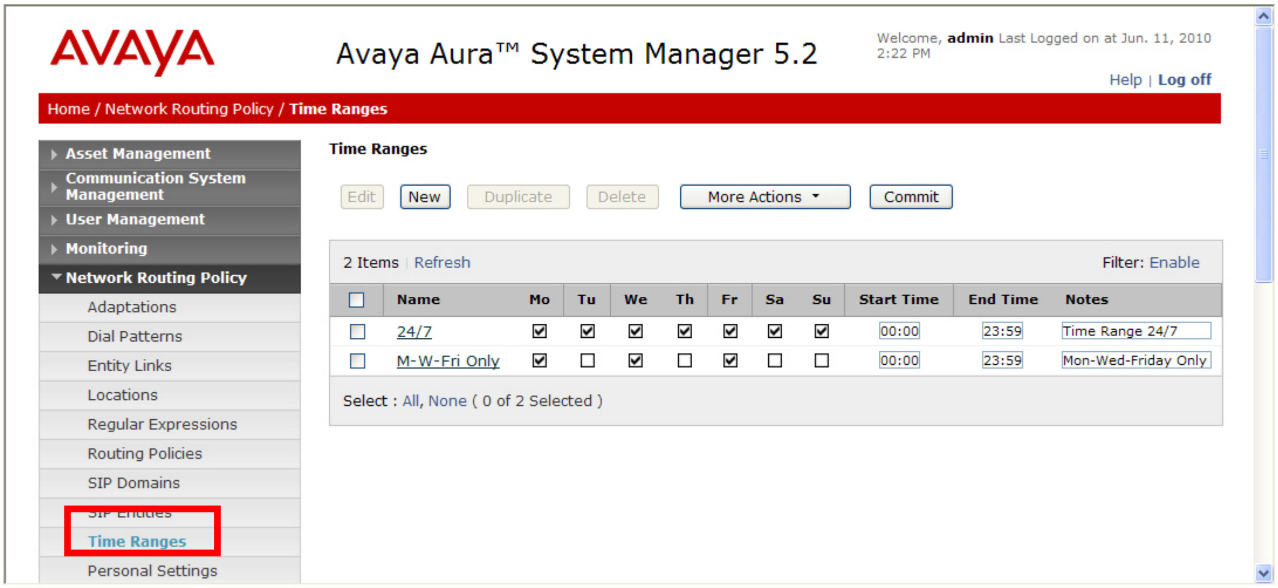

Figure 49: Time Ranges

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 voice calls (to Avaya Aura™ Communication Manager)
- Outbound calls to Acme1 (all outbound calls to Skype Connect)

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

Name	SIP Entity Destination	Time Of Day	Dial Pattern(s)	Notes
to_S8730_5063	S8730_port_5063	24/7	13038004098 13038004578 13038005961 13038006247	Any call to these dial patterns will route to Avaya Aura™ Communication Manager extensions (after digit conversion), and use port 5063.
to_SBC_for_Skype	ACME1	24/7	+	All matching dial patterns will route to ACME1 to be sent to Skype Connect.

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.

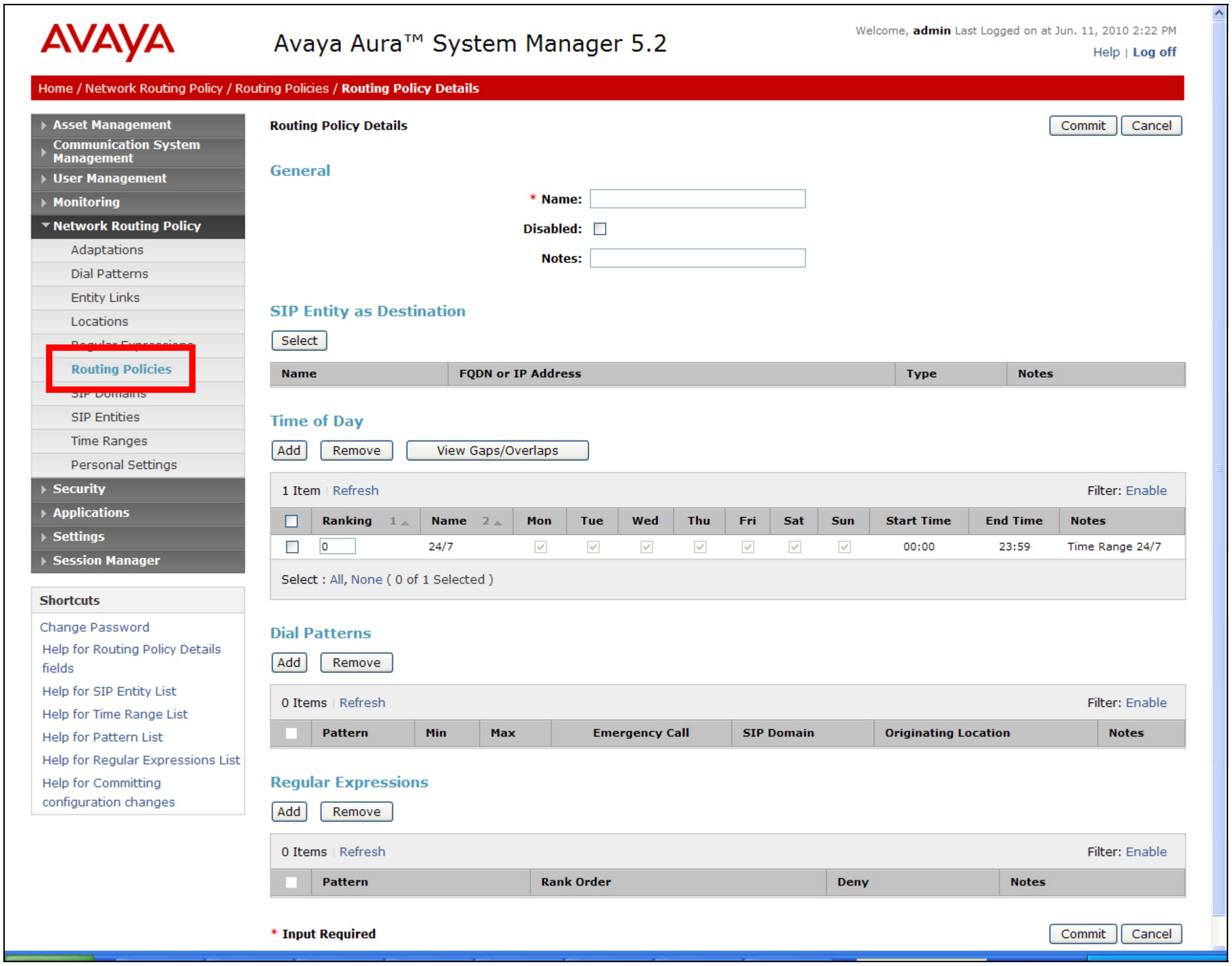

Figure 50: Routing Policy Details

1. **General** section
   a. Enter a descriptive name in the **Name** field (e.g. **to_S8730_5063**).
   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. **S8730_port_5063**)
   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**.

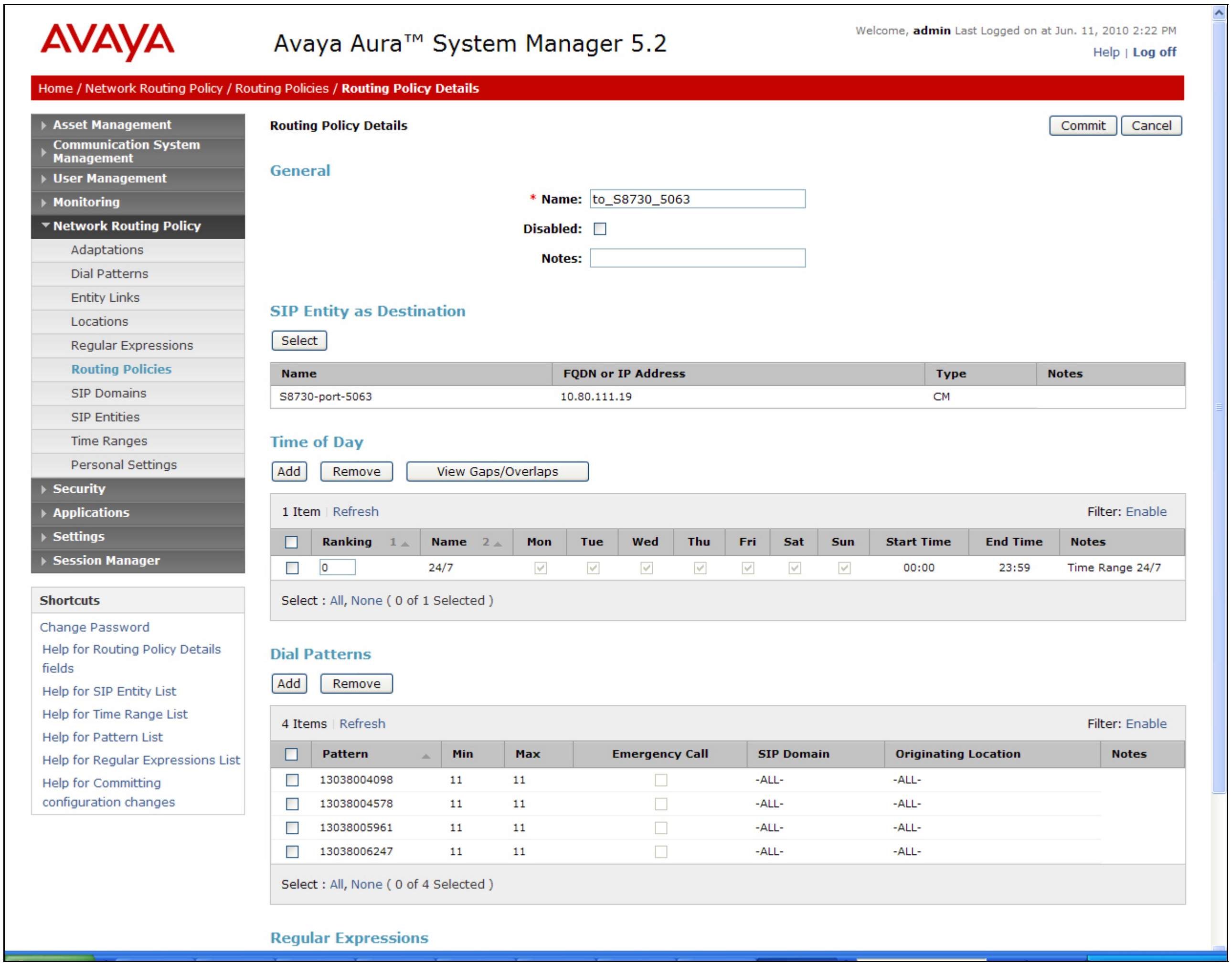

Figure 51: Routing Policy Details - Completed

5. Click the **Commit** button.
6. Repeat steps 1 to 5 for each Routing Policy. When completed the form will look like **Figure 52**. The routing policies relevant to the reference configuration are listed in **Table 8**.

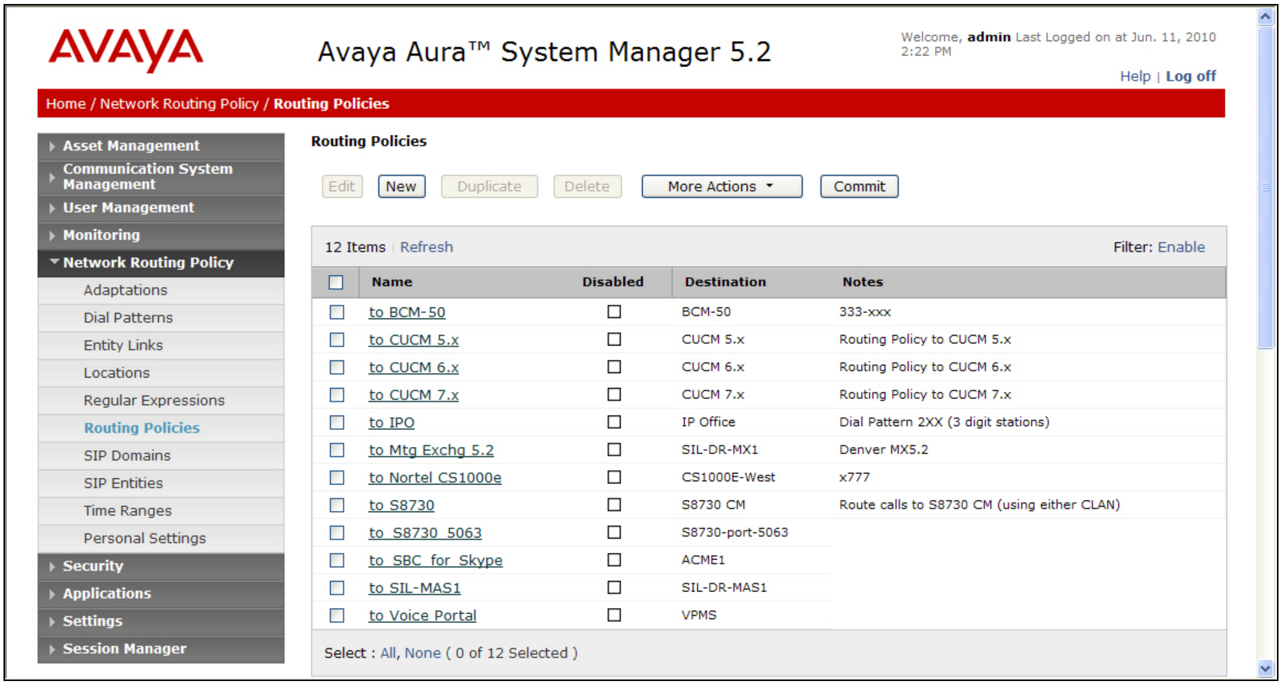

Figure 52: Routing Policies- Completed

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 7 digit string 667 is defined first in the list, and the 7 digit string 6675961 is defined last, a call for 6675961 will match on the 6675961 string.

The following Dial Patterns were provisioned in the reference configuration.

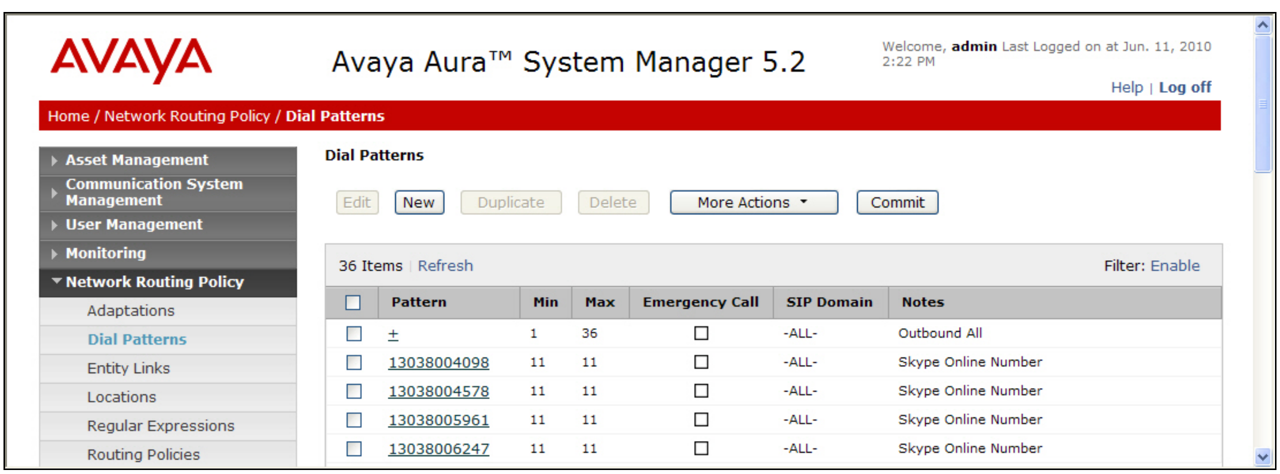

Figure 53: Completed Dial Patterns

Note – The DigitConversionAdapter adaptation is provisioned on the Avaya Aura™ Communication Manager C-LAN SIP Entity. This means that the conversion from Skype Connect online numbers 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 any number beginning with "+", and sent by *sip.skype.com* (this would be an outbound call from Avaya Aura™ Communication Manager to Avaya Aura™ Session Manager, destined for Skype Connect).

1. **General** Section
   a. Enter a unique pattern in the **Pattern** field (e.g. +).
   b. In the **Min** column enter the minimum number of digits (e.g. **1**).
   c. In the **Max** column enter the maximum number of digits (e.g. 36).
   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.

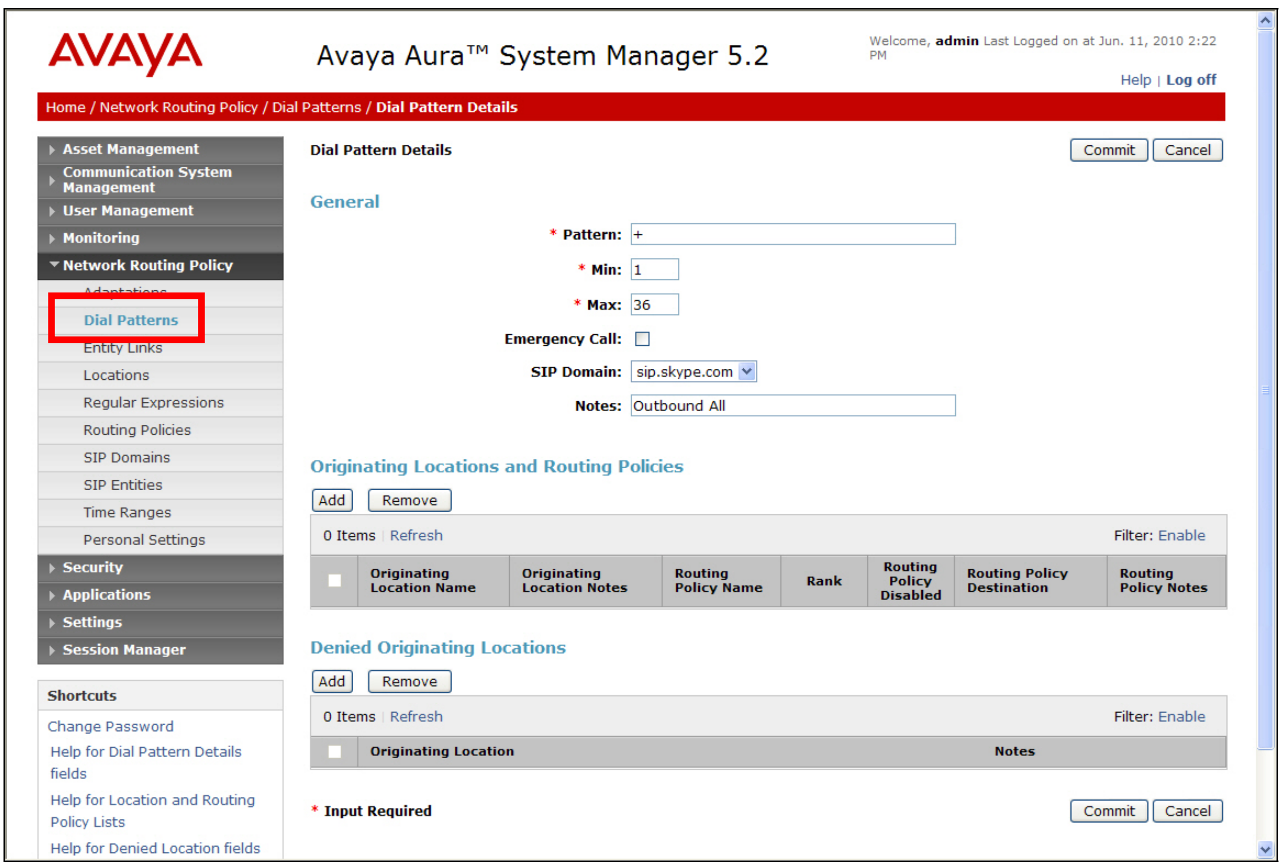

Figure 54: Dial Pattern Details - General

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 **AvayaCPE**
      ii. Routing Policy **to_SBC_for_Skype** (ACME1).
   c. Click on the **Select** button and return to the Dial Pattern window.

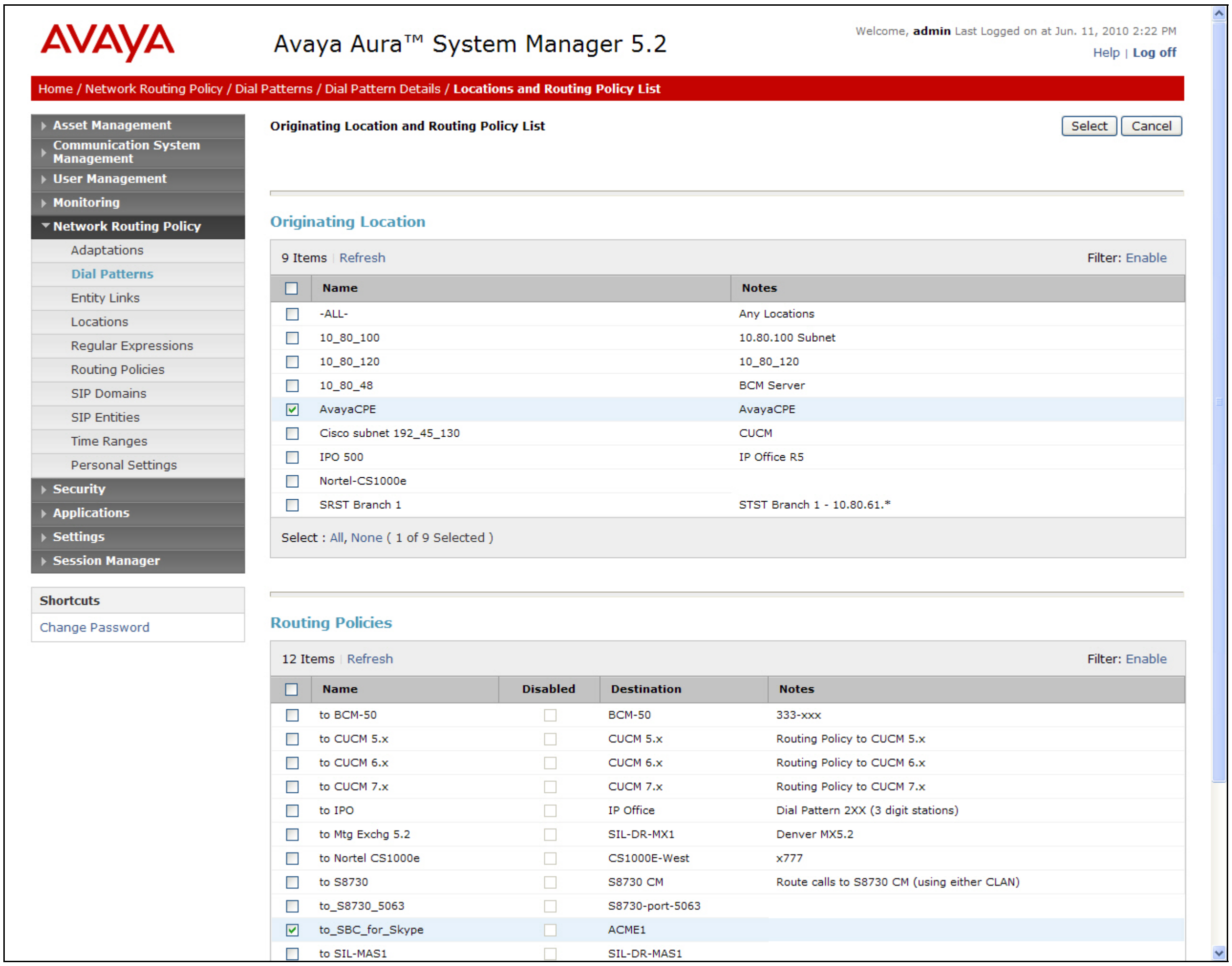

Figure 55: Dial Pattern Details – Originating Locations and Routing Policies

In the reference configuration, a request URI of *+1xxxxxxxxxx@sip.skype.com* would match and be sent to ACME1.

3. Click the **Commit** button
4. Repeat steps 1 to 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. Note that this step is part of standard product installation and provisioning and may have already been performed. To add an Avaya Aura™ Session Manager, select **Session Manager Administration** on the left **Session Manager** menu and click on the **New** button. The screen shown in **Figure 56** is part of the **Edit Session Manager** screen and contains the same fields as the **Add Session Manager** screen.

1. **General** section
   a. Select the **SIP Entity Name** field (e.g. **ASM1-DR**).
   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. **10.80.100.23**).
2. **Security Module** section
   a. Enter the **Network Mask** (e.g. **255.255.255.0**)
   b. Enter the **Default Gateway** (e.g. **10.80.100.1**)
   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 57** will be displayed.

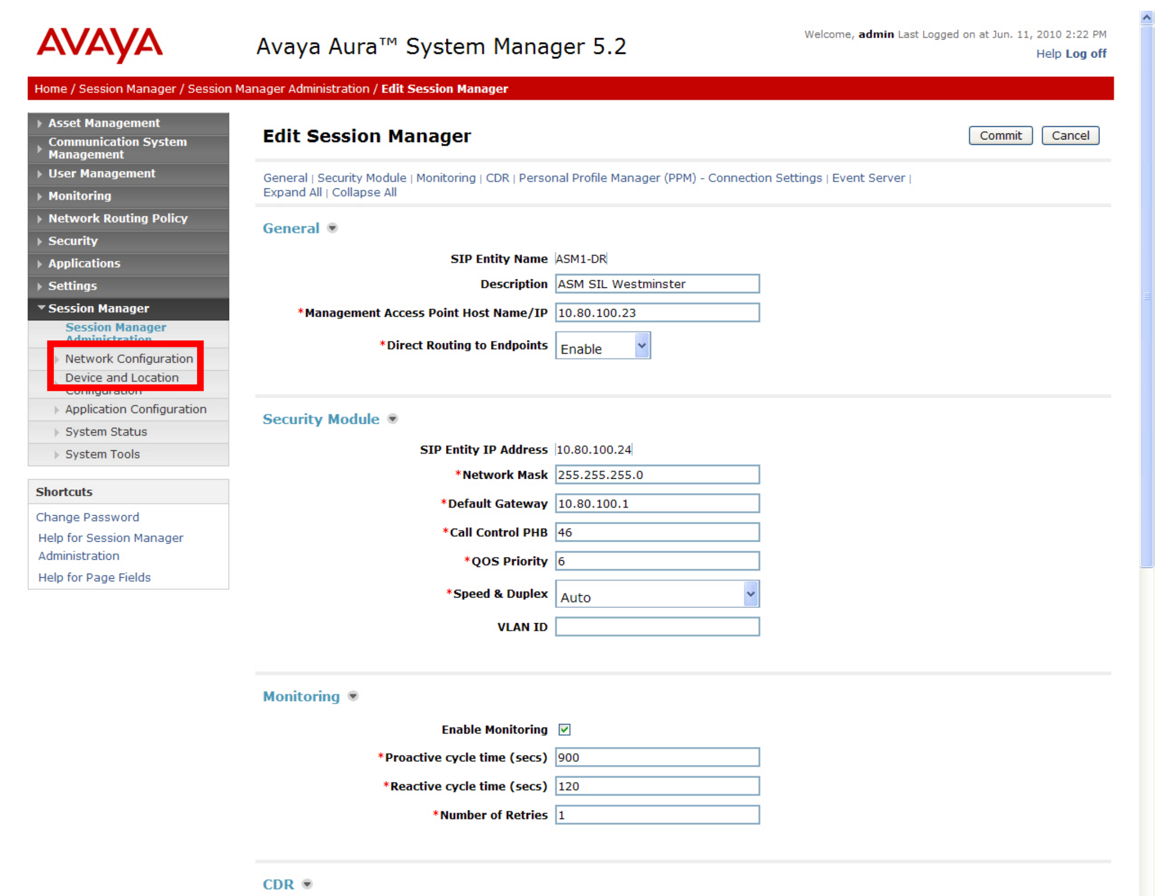

Figure 56: Edit Session Manager

Note – The SIP Entity IP address (under the Security Module heading) is automatically populated with the IP address defined for the Avaya Aura™ Session Manager SIP Entity (**ASM1-DR**) in **Section 4.3.4**.

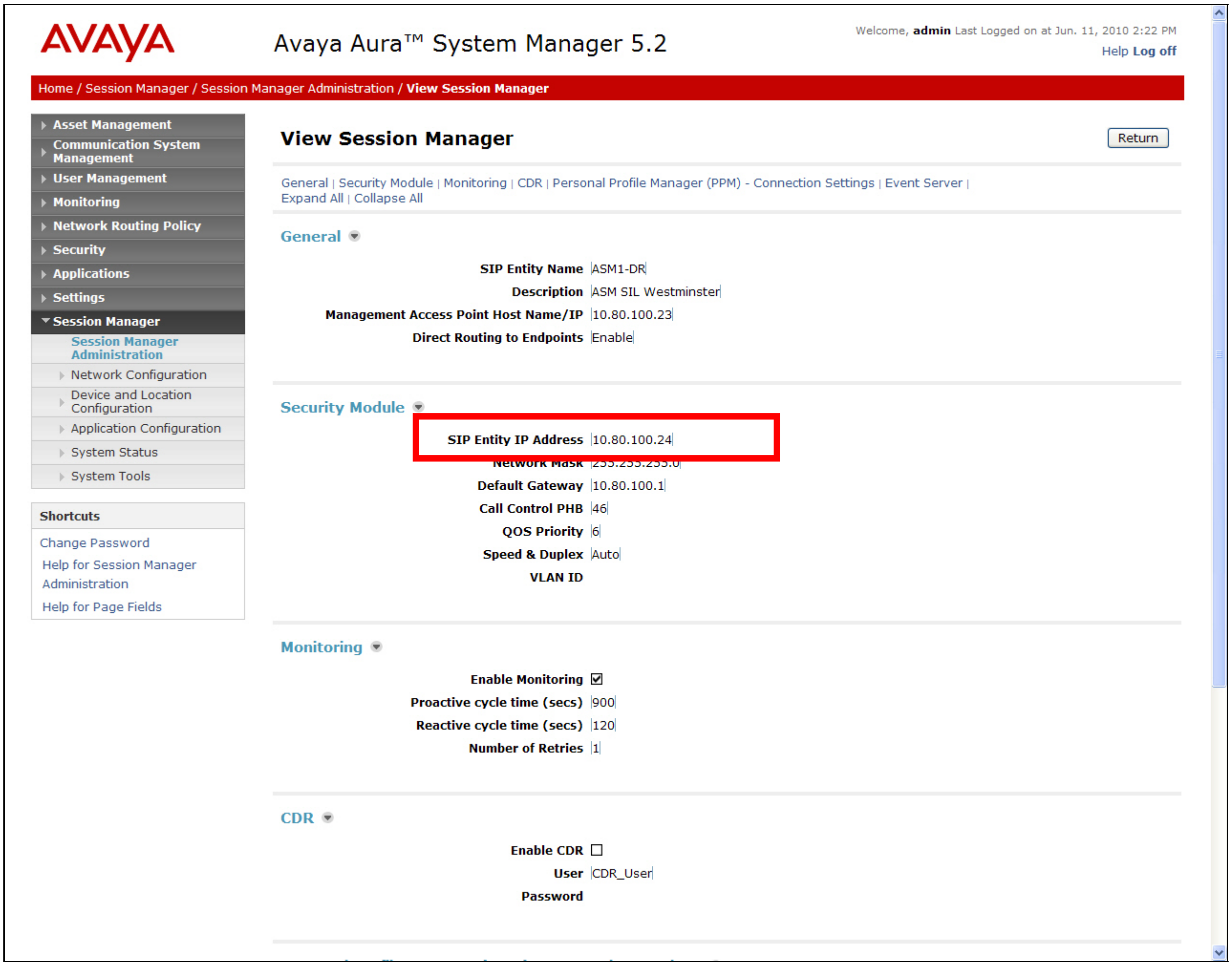

Figure 57: Completed Session Manager Form

5. Acme Packet Net-Net 3800

As described in **Section 1**, the Skype Connect service provides multiple SBCs for inbound and outbound call delivery. In the reference configuration, a single Acme Packet SBC is programmed to ensure the SIP trunk calls can be automatically rerouted to bypass SBC failures. For inbound calls from the Skype Connect service to the Avaya CPE, Skype Connect will automatically re-deliver the call to the Avaya CPE via Skype's secondary SBC.

Note – At this time, configurations involving Acme Packet high-availability on the Avaya CPE location are not supported by Skype Connect.

5.1. Acme Packet Service States

In the reference configuration, the Acme Packet SBC requests and provides service state 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 404 Not Found which is accepted by Session Manager as a valid “Up” Link Status response
- Acme/Skype Connect
  - Acme Packet to Skype Connect > OPTIONS messages are disabled.
  - Skype Connect does not send SIP OPTIONS messages.

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 “EXTERNAL” (to Skype Connect) and “INTERNAL” (to Avaya CPE) interfaces is described in **Sections 5.3.3 and 5.3.4**.

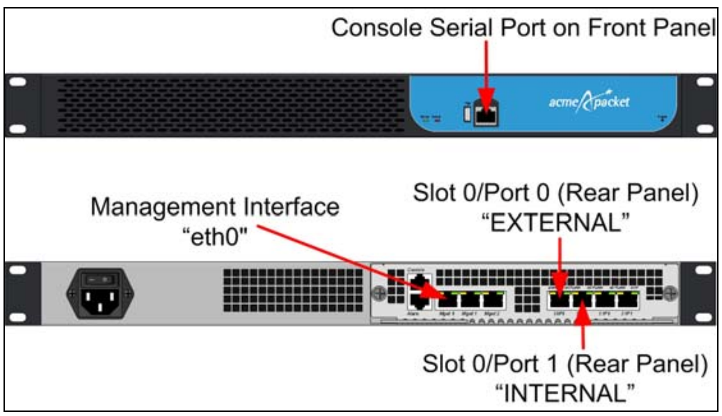

Figure 58: Acme Packet Network Interfaces

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 **References [8-9]**.

Note – The following Sections describe the provisioning of the Acme Packet SBC.

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 "eth0". In the reference configuration, the management IP address 172.16.253.230 is assigned.

From the *configure* prompt (steps 1 to 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 : eth0** 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. **135.8.19.64: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. **135.8.19.1**) 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

Local policies are defined to allow any SIP request from the **INTERNAL** realm to be routed to the SKYPE_GROUP Session Agent Group in the **EXTERNAL** realm (and vice-versa). In **Section 5.3.2.1**, the policy attribute with a **next-hop** value **0.0.0.0** and a **methods** value of **OPTIONS** terminates the Session Manager's SIP OPTIONS message at the SBC and prevents it from being sent to Skype. For these SIP OPTIONS messages, the SBC responds to the Session Manager with a 404 Not Found.

5.3.2.1 INTERNAL to EXTERNAL

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

1. Create a local-policy for the INTERNAL realm
   a. Enter **session-router → local-policy**
   b. Enter **from-address →** *
   c. Enter **to-address →** *
   d. Enter **source-realm → INTERNAL**
   e. Enter **state → enabled**
   f. Enter **policy-attributes**
   g. Enter **next-hop → SAG:SKYPE_GROUP**
   h. Enter **realm → EXTERNAL**
   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 **done**
   o. Enter **next-hop → 0.0.0.0**
   p. Enter **realm → EXTERNAL**
   q. Enter **start-time → 0000**
   r. Enter **end-time → 2400**
   s. Enter **days-of-week → U-S**
   t. Enter **app-protocol → SIP**
   u. Enter **state → enabled**
   v. Enter **methods → OPTIONS**
   w. Enter **done**
   x. Enter **exit**

y. Enter **exit**
z. Enter **exit**
aa. Enter **exit**

5.3.2.2 EXTERNAL to INTERNAL

1. Create a local-policy for the **EXTERNAL** realm. Procedures are the same as for the INTERNAL local-policy except:
   a. Enter **source-realm → EXTERNAL**
   b. Enter **policy-attributes**
   c. Enter **next-hop → 10.80.100.24**
   d. Enter **realm → INSIDE**

5.3.3 Network Interfaces

This section defines the network interfaces to the private (Avaya CPE) and public (Skype Connect) IP networks.

5.3.3.1 Public Interface

1. Create a network-interface to the public (Internet/Skype Connect) side of the Acme SBC.
   a. Enter **system → network-interface**
   b. Enter **name → s0p0**
   c. Enter **ip-address → 205.168.62.25**
   d. Enter **netmask → 255.255.255.128**
   e. Enter **gateway → 205.168.62.1**
   f. Enter **done**
   g. Enter **exit**

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 → s0p1**
   c. Enter **ip-address → 10.80.120.65**
   d. Enter **netmask → 255.255.255.0**
   e. Enter **gateway → 10.80.120.1**
   f. Enter **done**
   g. Enter **exit**

5.3.4 Physical Interfaces

This section defines the physical interfaces to the private (Avaya CPE) and public (Skype Connect) networks.

5.3.4.1 Public Interface

1. Create a network-interface to the public (Internet/Skype Connect) side of the Acme.
   a. Enter **system → phy-interface**
   b. Enter **name → s0p0**

c. Enter **operation-type → media**
d. Enter **port → 0**
e. Enter **slot → 0**
f. Enter **done**
g. Enter **exit**

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 → s0p1**
    c. Enter **operation-type → media**
    d. Enter **port → 1**
    e. Enter **slot → 0**
    f. Enter **done**
    g. Enter **exit**

5.3.5 Realms

Realms are used as a basis for determining egress and ingress associations between physical and network interfaces.

5.3.5.1 EXTERNAL Realm

1. Create a realm for the outside network.
    a. Enter **media-manager → realm-config**
    b. Enter **identifier → EXTERNAL**
    c. Enter **addr-prefix → 0.0.0.0**
    d. Enter **network-interfaces → s0p0:0**
    e. Enter **done**
    f. Enter **exit**

5.3.5.2 INTERNAL 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 → INTERNAL**
    c. Enter **addr-prefix → 0.0.0.0**
    d. Enter **network-interfaces → s0p1:0**
    e. Enter **done**
    f. Enter **exit**

5.3.6 Steering Pools

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

5.3.6.1 EXTERNAL Steering Pool

1. Create a steering pool for the external network.

a. Enter **media-manager → steering-pool**
b. Enter **ip-address → 205.168.62.25**
c. Enter **start-port → 49152**
d. Enter **end-port → 65535**
e. Enter **realm-id → EXTERNAL**
f. Enter **done**
g. Enter **exit**

5.3.6.2 INTERNAL Steering Pool

1. Create a steering pool for the inside network. Procedures are the same as for the external steering pool except:
   a. Enter **media-manager → steering-pool**
   b. Enter **ip-address → 10.80.120.65**
   c. Enter **start-port → 2048**
   d. Enter **end-port → 65535**
   e. Enter **realm-id → INTERNAL**
   f. Enter **done**
   g. Enter **exit**

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 is defined for the SIP for Skype service nodes (external) and the Avaya Aura™ Session Manager (internal).

5.3.7.1 EXTERNAL Session Agents

1. Create session agents for the Skype-assigned SBCs.
   a. Enter **session-router → session-agent**
   b. Enter **hostname → 2.sip.skype.com**
   c. Enter **port → 5060**
   d. Enter **state → enabled**
   e. Enter **app-protocol → SIP**
   f. Enter **transport-method → UDP**
   g. Enter **realm-id → EXTERNAL**
   h. Enter **description → Skype Connect SBC Primary**
   i. Enter **ping-interval → 0**
   j. Enter **done**
   k. Enter **exit**
   l. Repeat for the secondary Skype-assigned SBC.

5.3.7.2 INTERNAL 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 → 10.80.100.24**
   c. Enter **ip-address → 10.80.100.24**

d. Enter **state → enabled**
e. Enter **app-protocol → SIP**
f. Enter **port → 5063**
g. Enter **transport-method → staticTCP**
h. Enter **realm-id → INTERNAL**
i. Enter **description → Avaya Aura Session Manager**
j. Enter **allow-next-hop-lp → enabled**
k. Enter **ping-method → OPTIONS**
l. Enter **ping-interval → 300**
m. Enter **in-manipulationid → Avaya-incoming**
n. Enter **done**
o. Enter **exit**

5.3.8 Session Groups

A Session Agent Group (SAG) defines a single or multiple destinations that are referenced in provisioning session agents.

5.3.8.1 Skype Connect Session Group

1. Create a session group for the Skype Connect SBCs.
   a. Enter **session-router → session-group**
   b. Enter **groupname → SKYPE_GROUP**
   c. Enter **state → enabled**
   d. Enter **app-protocol → SIP**
   e. Enter **strategy → Hunt**
   f. Enter **dest →** (**2.sip.skype.com 1.sip.skype.com)**
   g. Enter **done**
   h. Enter **exit**

5.3.8.2 Avaya CPE Session Group

a. Since only one Session Manager is implemented in the reference configuration, a session group was not utilized for the Avaya CPE network. Note that, if multiple Session Managers are deployed then a session group could be utilized for the Avaya CPE.

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 → INTERNAL**
5. Enter **registrar-domain → *** (Note: this option is required when using Registration Method. See **Section 6.3.1**.)

6. Enter **registrar-host → *** (Note: this option is required when using Registration Method. See **Section 6.3.1**.)
7. Enter **done**
8. Enter **exit**

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 EXTERNAL SIP Interface

1. Create a sip-interface for the external network.
    a. Enter **session-router → sip-interface**
    b. Enter **state → enabled**
    c. Enter **realm-id → EXTERNAL**
    d. Enter **sip-port →**
        1. Enter **address → 205.168.62.25**
        2. Enter **port → 5060**
        3. Enter **transport-protocol → UDP**
        4. Enter **allow-anonymous → agents-only**
    e. Enter **exit**
    f. Enter **done**
    g. Enter **exit**

5.3.10.2 INTERNAL 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 → INTERNAL**
    c. Enter **sip-port →**
        1. Enter **address → 10.80.120.65**
        2. Enter **port → 5063**
        3. Enter **transport-protocol → TCP**
        4. Enter **allow-anonymous → agents-only**
    d. Enter **done**
    e. Enter **registration-caching → enabled** (Note: this option is required when using Registration Method. See **Section 6.3.1**.)
    f. Enter **route-to-registrar → enabled** (Note: this option is required when using Registration Method. See **Section 6.3.1**.)
    g. Enter **exit**
    h. 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 at the session agent associated with the Avaya Aura™ Session Manager. See **Section 5.3.7.2**.

- Insert Skype User Name in From Header for outbound calls from Avaya CPE to Skype Connect
- Insert Skype Connect domain in From Header for outbound calls from Avaya CPE to Skype Connect

1. Enter **session-router → sip-manipulation**
2. Enter **name → Avaya-incoming**
3. Enter **description → insert skype user name in From header required for Skype and also used to match surrogate user required for Proxy-Authentication**
4. Enter **header-rules**
5. Proceed to the following sections

5.3.11.1 From Header

1. Enter **session-router → sip-manipulation → header-rule**
2. Enter **name → skype From**
3. **Enter header-name → From**
4. Enter **action → manipulate**
5. Enter **comparison-type → case-sensitive**
6. Enter **msg-type → request**
7. Enter **element-rules →**
    a. Enter **name → skype From user**
    b. Enter **parameter-name → From**
    c. Enter **type → uri-user**
    d. Enter **action → replace**
    e. Enter **match-val-type → any**
    f. Enter **comparison-type → case-sensitive**
    g. Enter **new-value → 99051000104350**
8. Enter **exit**
9. Enter **element-rules →**
    a. Enter **name → skype From host**
    b. Enter **parameter-name → From**
    c. Enter **type → uri-host**
    d. Enter **action → replace**
    e. Enter **match-val-type → any**
    f. Enter **comparison-type → case-sensitive**
    g. Enter **new-value → sip.skype.com**
10. Enter **done**
11. Enter **exit**

5.3.12 Surrogate Registration

Surrogate registration allows the Acme SBC to perform trunk side registrations to the Skype Connect network. Programming of the surrogate registration capability is only necessary if **Registration Method** is selected on the Skype Connect profile as described in **Section 6.3.1.** Note that the values for **register-user**, **register-contact-user** and **password** are assigned by Skype and are displayed on the Authentication details page as shown in **Section 6.3.1.**

1. Enter **session-router → surrogate-agent**
2. Enter **register-host → sip.skype.com**
3. Enter **register-user → 99051000104350**
4. Enter **state → enabled**
5. Enter **realm-id → INTERNAL**
6. Enter **customer-next-hop → SAG:SKYPE_GROUP**
7. Enter **register-contact-host → 205.168.62.25**
8. Enter **register-contact-user → 99051000104350**
9. Enter **password → XXXXXXXXXXXXXX**
10. Enter **register-expires → 240**
11. Enter **options → auth-method="INVITE,CANCEL,ACK,BYE,UPDATE,PRACK,INFO,OPTIONS"**
12. Enter **done**
13. Enter **exit**
14. Enter **exit**
15. Enter **exit**

5.3.13 Other Acme Packet provisioning

5.3.13.1 Access-control

The Static Access Control List was not used in the reference configuration.

5.3.13.2 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 it is not enabled, proceed to steps 3 to 5.:
3. Enter **state → enabled**
4. Enter **done**
5. Enter **exit**

5.3.13.3 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 → 135.8.19.1**
4. Enter **done**
5. Enter **exit**

6. Skype Connect

Information regarding the Skype Connect service offer can be found at http://www.skype.com.

6.1. Skype Manager

The Skype Connect service provisioning is performed using Skype Manager, a self-service, web-based provisioning tool. The following elements are provisioned using Skype Manager and are discussed in more detail in subsequent sections.

- **Skype Connect Profile**
  - **Profile settings**
    - **Profile Name** - Define a name for the Profile.
    - **Calling channels –** Defines the number of available channels for inbound/outbound voice calls. This number should match the number of channels programmed on Avaya Aura™ Communication Manager in the trunk group form's **Number of Members** field as described in **Section 3.1.5.1**.
    - **Outgoing calls –** For billing purposes, define how payments will be handled.
    - **Caller ID –** Define what Caller ID should be used for outbound calls from Avaya CPE to Skype Connect.
    - **Incoming calls –** Skype online number and Skype business account definitions. This includes Skype business account to called party number/extension mapping.
  - **Authentication details**
    - **Registration**
    - **IP Authentication**
  - **Reports**
    - **Skype Credit usage reports**

To access the Skype Manager, navigate to http://manager.skype.com and log in with the appropriate credentials.

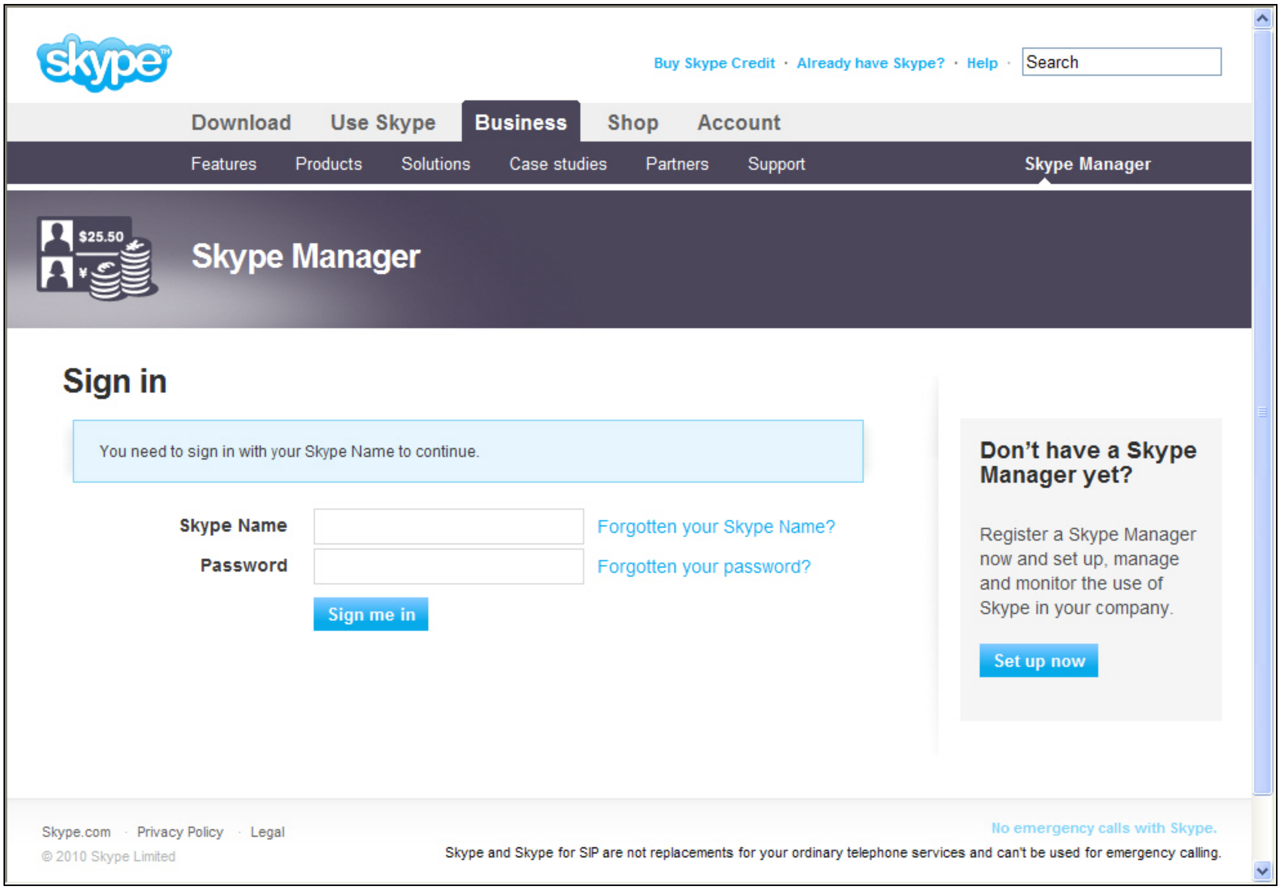

Figure 59: Skype Manager Sign In Screen

6.2. Skype Connect Profile

After logging in, the Dashboard screen is displayed as shown in **Figure 60**.

1. Click on **Skype for SIP.** See **Figure 60.**
2. Click on **Create a new profile**. See **Figure 61**.
3. Enter a name for the new profile (e.g. SIL Westminster SBC). See **Figure 62**.
4. **Section 6.3** provides details on how to setup **SIP Authentication**.

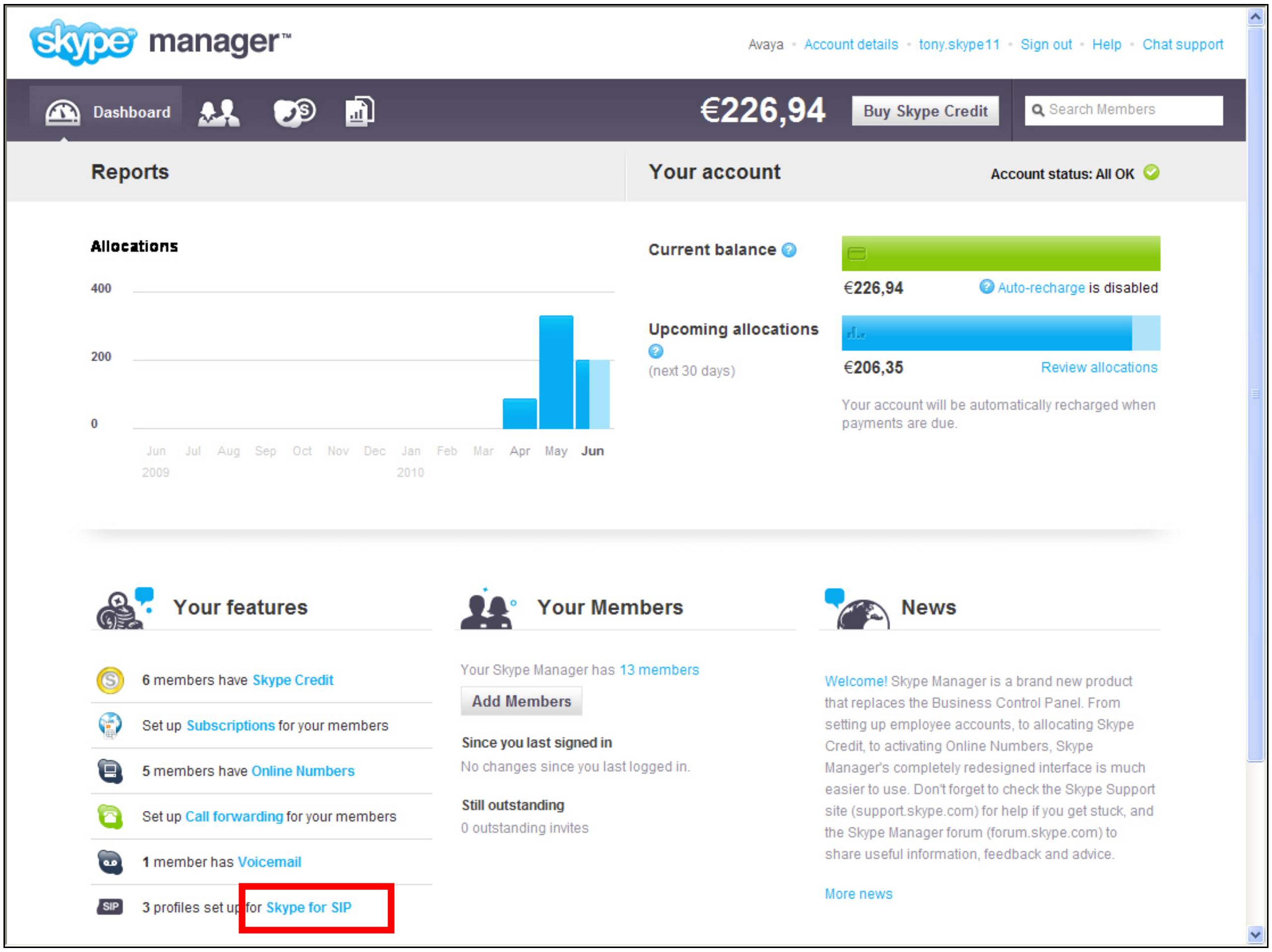

Figure 60: Skype Manager Dashboard Screen

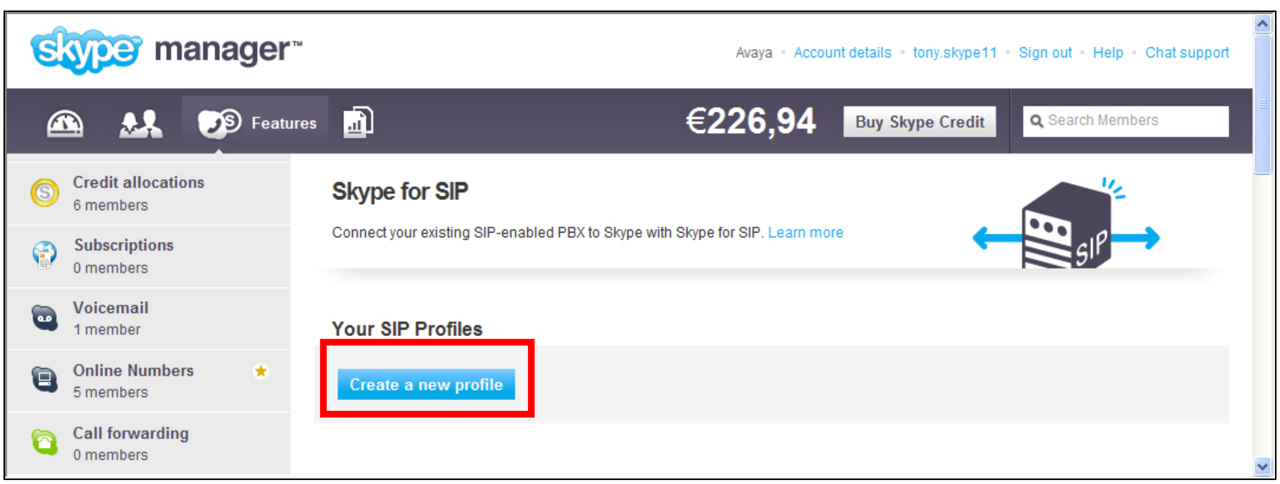

Figure 61: Create a new profile

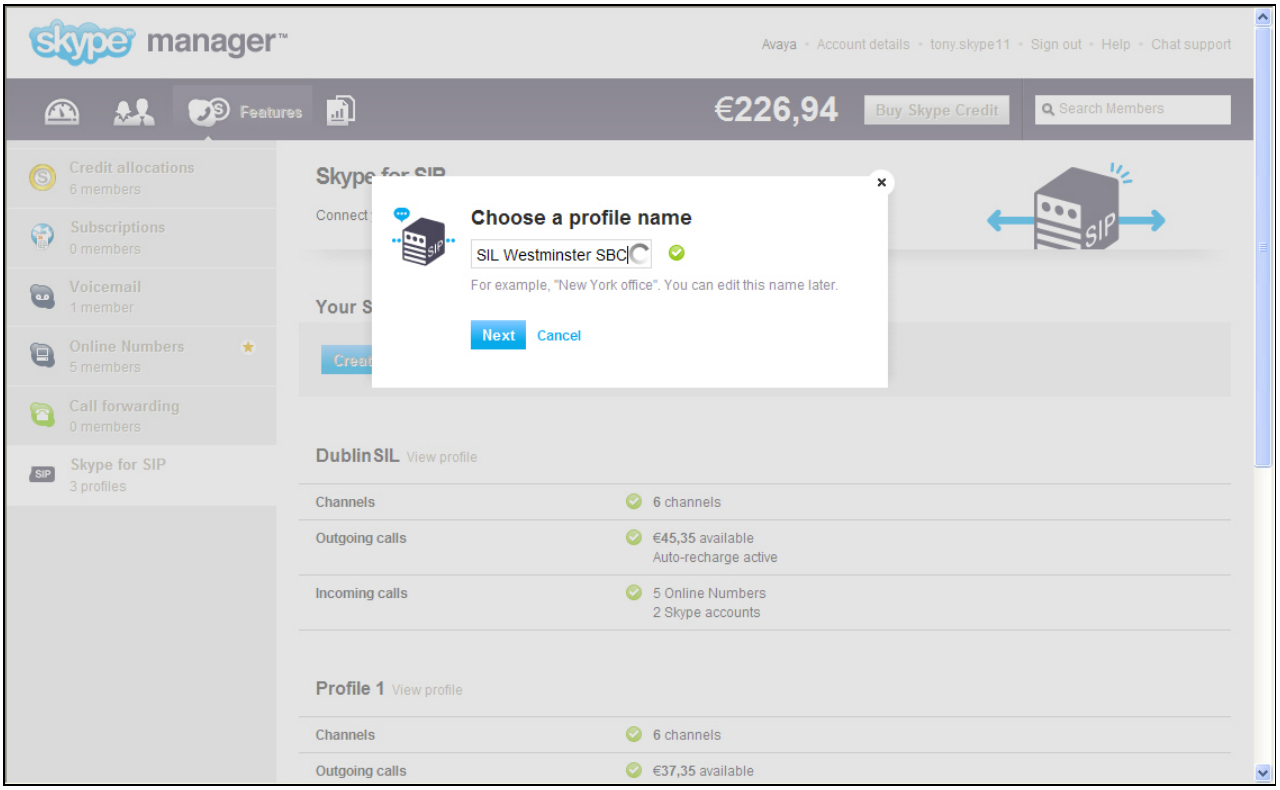

Figure 62: New Profile Name

6.3. Skype Connect Authentication Details

The Skype Connect service supports two methods of authentication: Registration or IP Authentication. Only one method may be selected per profile.

6.3.1 Registration Method

SIP DIGEST users are provided with a single Fully Qualified Domain Name (FQDN) to register too, which is "sip.skype.com" where the registrar contains the address of record (AoR) for each user. The AoR contains the SIP Username. Using this method requires that the Acme SBC at the Avaya CPE be programmed to perform trunk side registrations. The Acme SBC must be programmed with the Skype-assigned SIP User name and the Skype-assigned Password as shown in **Figure 63**. This is accomplished by enabling the Acme SBC's "surrogate-agent" capability as described in **Section 5.3.12.**

1. Click on **Registration**
2. Verify the green check mark next to **Registration**
3. Locate the following Skype-assigned information:
    a. SIP User information (**register-user** and **register-contact-user** in **Section 5.3.12**)
    b. Password (**password** in **Section 5.3.12**)
    c. Skype for SIP address (**register-host** in **Section 5.3.12**)
    d. UDP Port (**port** for **EXTERNAL Session Agents** in **Section 5.3.7.1**)

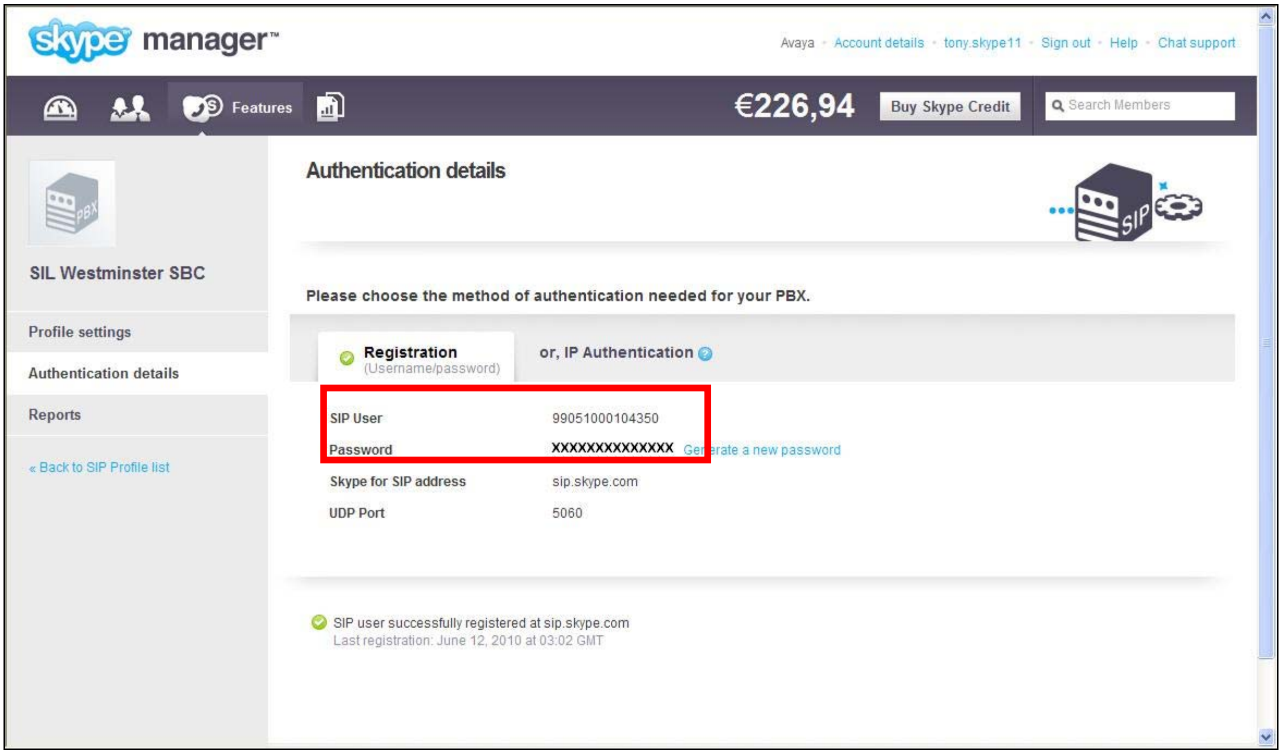

Figure 63: Registration Method

6.3.2 IP Authentication Method

The **IP Authentication** method shown in **Figure 64** can also be selected in cases where the **Registration** method is not supported by the CPE equipment or is not preferred for security reasons. Since SIP registrations are not utilized, during the IP Authentication method set up process, Skype creates a static AoR entry the Skype SIP registrar which enables Skype to locate and explicitly point traffic to the Acme SBC deployed at the Avaya CPE. Note that when using the **IP Authentication** method the Acme SBC's "surrogate-agent" capability described in **Section 6.3.1** should not be implemented.

1. Click on **IP Authentication**
2. Verify the green check mark next to **IP Authentication**
3. Enter the IP details of the Acme SBC:
    a. **Public IP address → 205.168.62.25**
    b. **UDP Port → 5060** (**port** for **EXTERNAL SIP Interface** in **Section 5.3.10.1**)

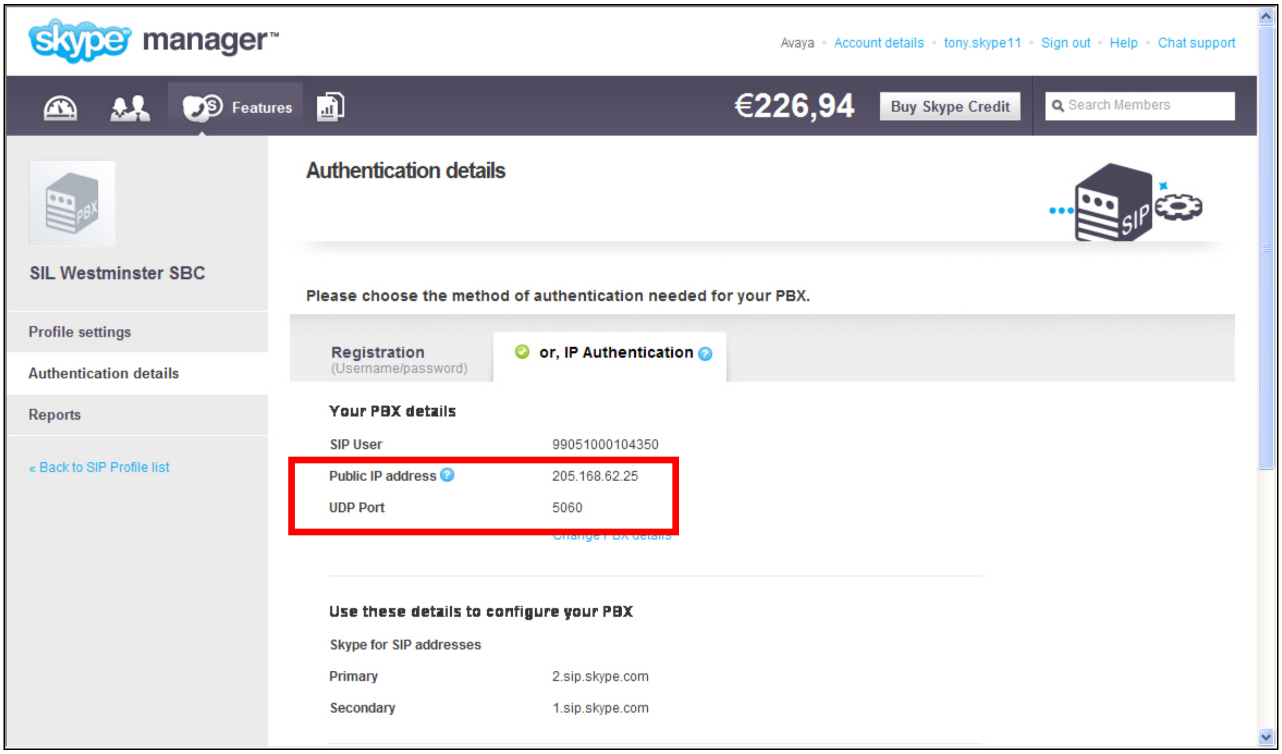

Figure 64: IP Authentication Method

6.4. Calling channels

As shown in **Figure 65**, the reference configuration utilized **6** Calling channels. The number of calling channels should match the number of channels programmed on Avaya Aura™ Communication Manager in the trunk group form's **Number of Members** field as described in **Section 3.1.5.1**. These calling channels are provided by Skype on a subscription basis.

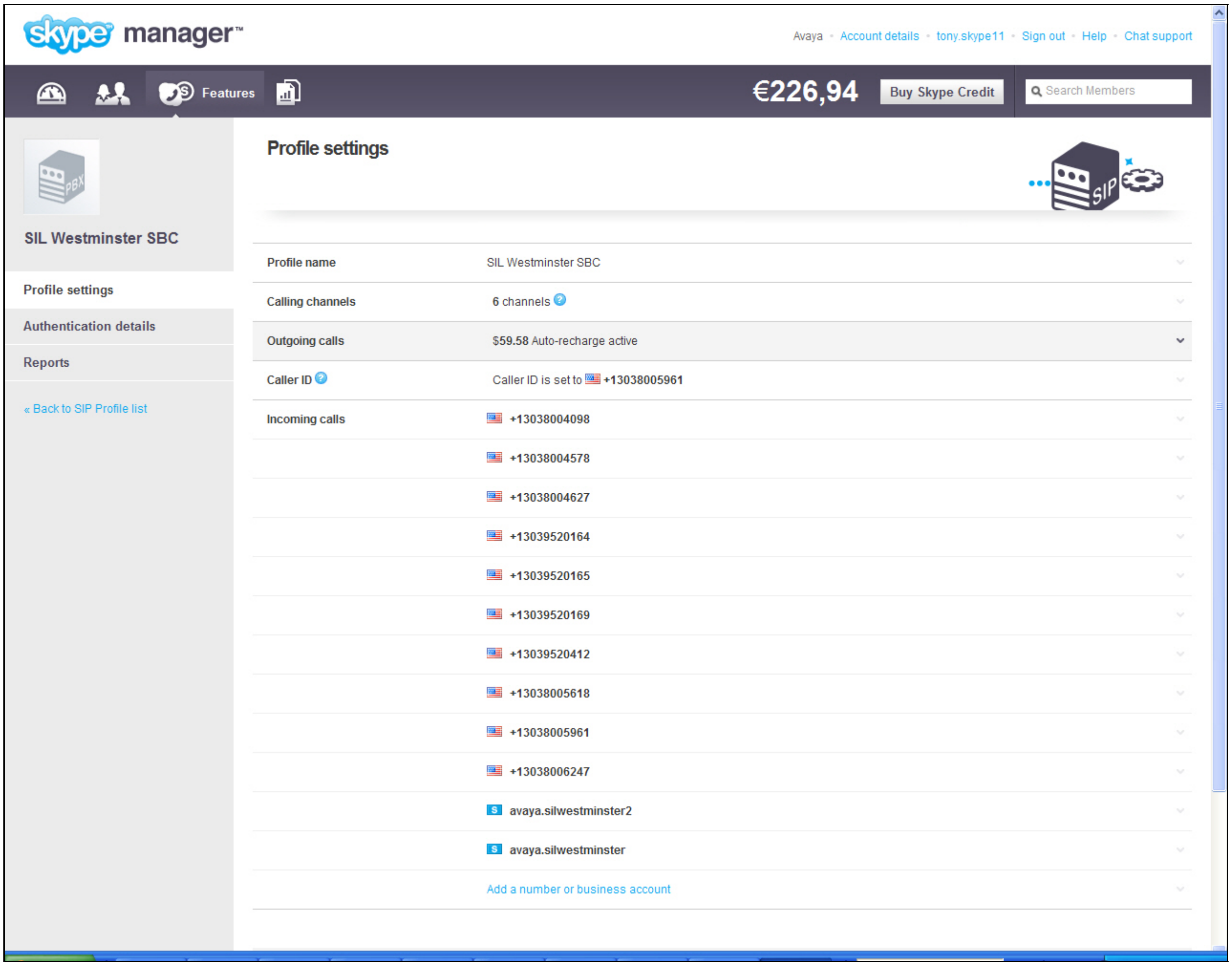

Figure 65: Profile Settings

6.5. Outgoing calls

As shown in **Figure 65**, outgoing calls from Avaya CPE to Skype Connect utilize Skype credit. Verify that sufficient Skype credit is allocated for outbound calls.

6.6. Caller ID

The SIP user options for outbound caller ID are:

1. Select any Online number associated to the SIP profile
2. Select any landline number that is registered with Skype
3. Any combination of the above

Skype Connect allows a business to register their landline telephone numbers via the Skype profile. When a business has been verified, any landline number that is registered is inserted into a virtual CLI database that also contains all Online numbers associated to the SIP profile. When the Avaya CPE uses the P-Asserted-ID header, Skype check's the content of the P-Asserted-ID header against the users CLI database. If the values match, Skype will then use the number in the P-Asserted-ID header as the outbound caller ID. If the values do not match, Skype will use the statically assigned caller ID. In the reference configuration, the statically assigned caller ID is set to "13038005961".

For Caller Line Identification restriction, Skype supports the following uses:

- Privacy: id
- P-Asserted-ID "anonymous@invalid.com"

Avaya Aura™ Communication Manager's Calling Party Number Block feature is compatible with Skype Connect. Note that calls from Communication Manager extensions that activate Calling Party Number (CPN) Blocking will result in a caller id of 000-012-3456. See **Section 3.1.8.1**.

Incoming PSTN calls from Skype that are forwarded to outbound PSTN destinations will receive the default caller ID associated with the Skype profile. Incoming PSTN calls from Skype that are transferred to outbound PSTN destinations will receive either the caller ID of the transferring party, per the requirements described above, or the default caller ID from the Skype profile.

6.7. Incoming calls

Skype online numbers can be purchased from Skype and assigned to the Skype Connect profile. When these online numbers are dialed from the PSTN, Skype will deliver the call to the Avaya CPE. These Skype online numbers are listed in the **Incoming calls** section of the Skype Connect profile. **Section 4.3.2.1** describes how Avaya Aura™ Session Manager routes calls from Skype Connect and converts the online numbers to Avaya Aura™ Communication Manager extensions.

6.7.1 Incoming calls – Skype Business Acount

Skype Connect enables a Business Account (Skype name) to be assigned to a SIP profile so other Skype users can make free calls to a SIP user's Skype name (Skype to Skype calls). Calls are routed from the Skype P2P network to the Skype Connect profile's User Agent. As shown in **Figure 66**, a Skype P2P call to "avaya.silwestminster" is mapped to extension 6675961[1], and 6675961 is the destination number delivered in the Request URI of the SIP Invite. These calls are delivered as inbound calls from Skype Connect to the Avaya CPE. For these types of calls that are directed at Avaya Aura™ Communication Manager extensions, digit conversion may not be required. However, additional Dial Patterns should be assigned to handle routing of these numbers by Avaya Aura™ Session Manager to Avaya Aura™ Communication Manager as described in **Section 4.3.8**.

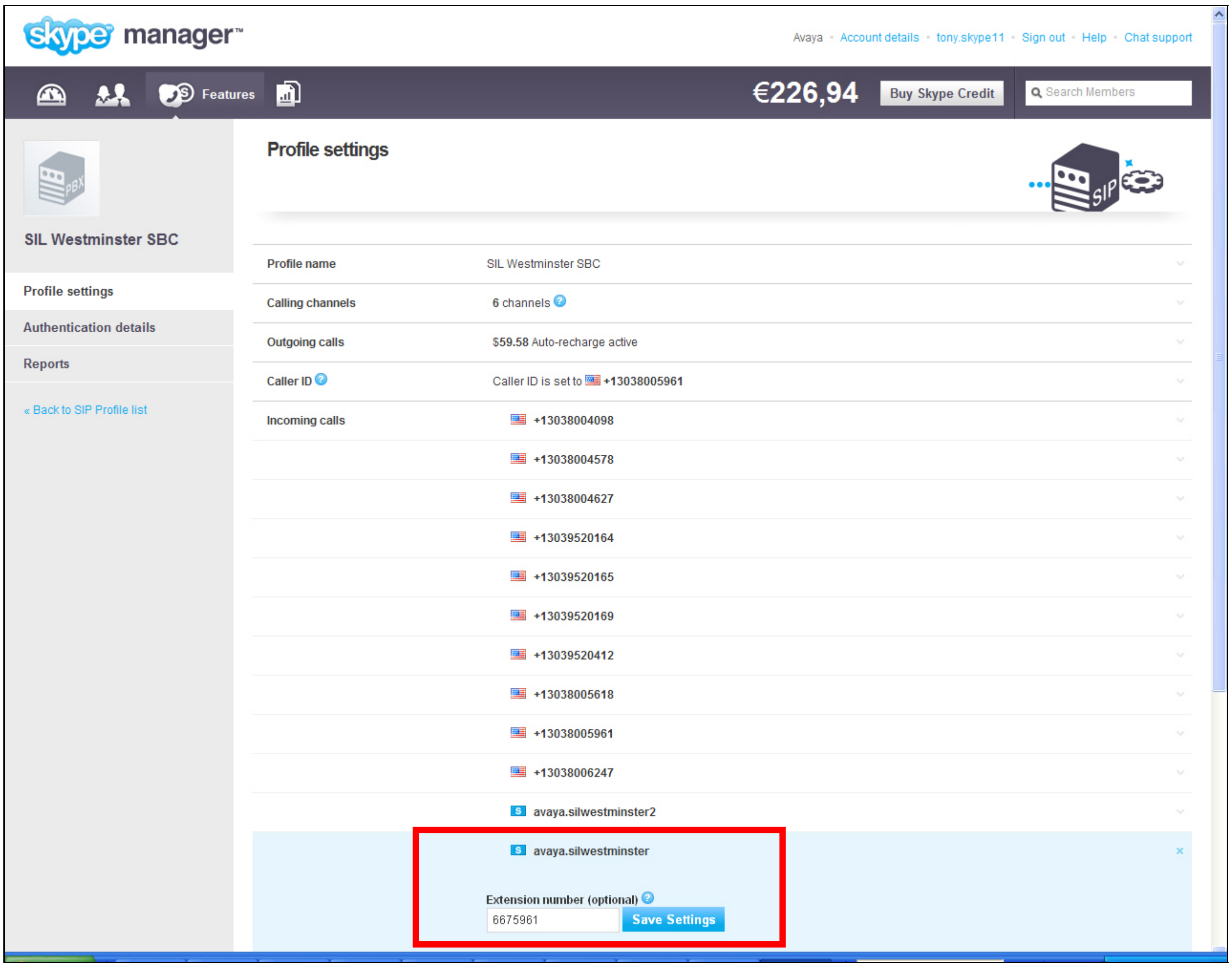

Figure 66: Skype Business Account to Extension Number Mapping

[1] When no extension number is specified, Skype delivers the Skype-assigned SIP User name in the Request URI of the SIP Invite. See **Figure 63**.

6.8. Skype Connect Reports

Usage reports can be viewed by accessing the **Profile settings** screen as shown in **Figure 65**. Then, select **Reports** as shown in **Figure 67**.

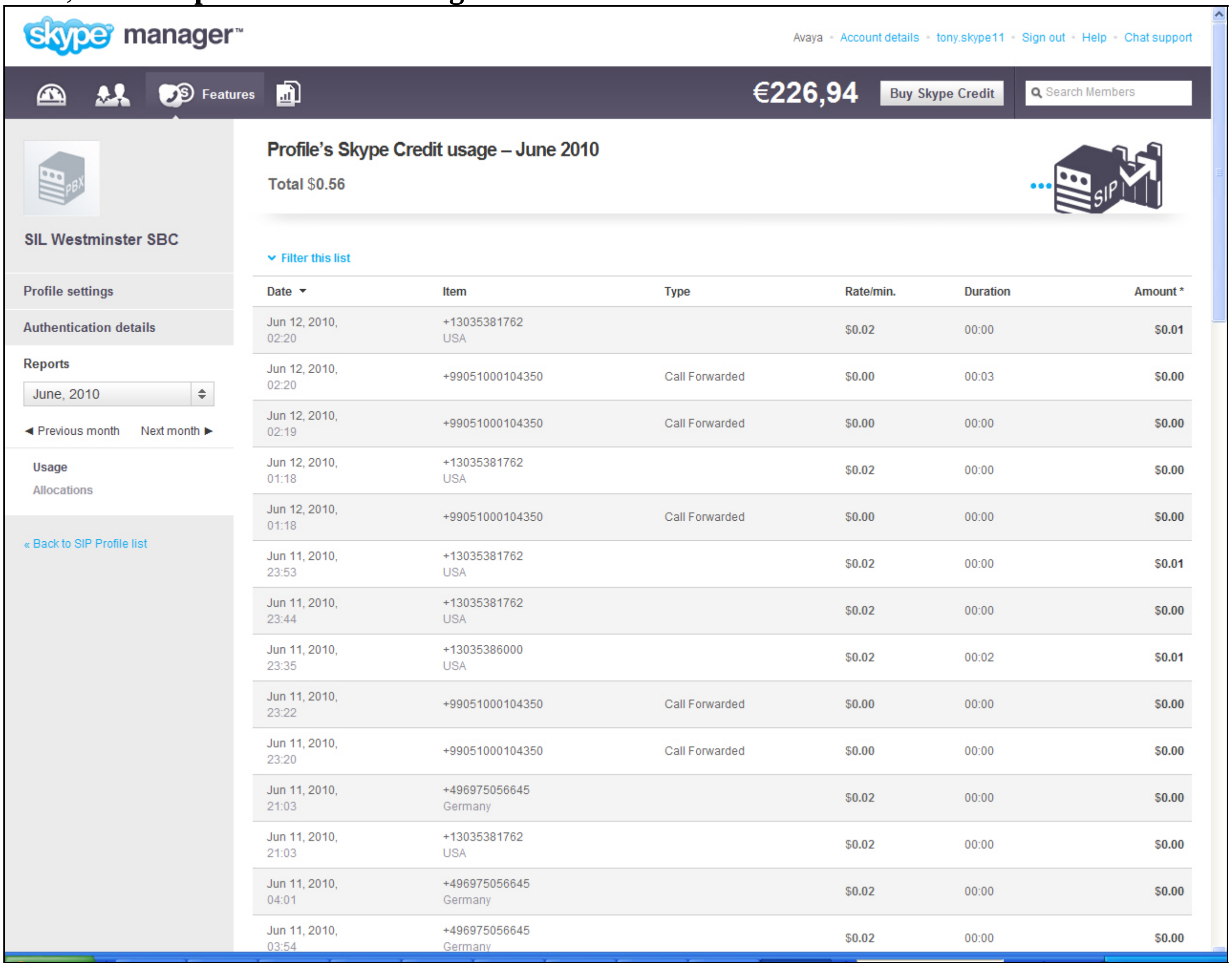

Figure 67: Skype Credit Usage Report

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 the Skype Connect 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 in **Figure 68**.

```
status trunk 68

                              TRUNK GROUP STATUS

Member   Port     Service State      Mtce Connected Ports
                                     Busy

0068/001 T00133   in-service/idle    no
0068/002 T00134   in-service/idle    no
0068/003 T00135   in-service/idle    no
0068/004 T00136   in-service/idle    no
0068/005 T00137   in-service/idle    no
0068/006 T00138   in-service/idle    no
```

Figure 68: 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 68
                          STATUS SIGNALING GROUP

        Group ID: 68                              Active NCA-TSC Count: 0
      Group Type: sip                              Active CA-TSC Count: 0
  Signaling Type: facility associated signaling
     Group State: in-service
```

Figure 69: Status Signaling Group

Make a call between an Avaya Aura™ Communication Manager H.323 station and the PSTN. Verify the status of the connected SIP trunk. Run the "***status trunk x***" command first, where "***x***" is the number of the outbound SIP trunk group, to determine which trunk member is active. Then, run 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 68/1                                           Page   1 of   3
                                TRUNK STATUS
  Trunk Group/Member: 0068/001             Service State: in-service/active
                Port: T00133            Maintenance Busy? no
  Signaling Group ID: 68
    IGAR Connection? no
     Connected Ports: S00013
```

Figure 70: Status Trunk – Active Call – Page 1

```
status trunk 68/1                                             Page   2 of   3
                                CALL CONTROL SIGNALING

Near-end Signaling Loc: 01A1117
  Signaling   IP Address                                 Port
   Near-end:  10.80.111.19                             : 5063
    Far-end:  10.80.100.24                             : 5063
 H.245 Near:
  H.245 Far:
   H.245 Signaling Loc:          H.245 Tunneled in Q.931? no

 Audio Connection Type: ip-direct     Authentication Type: None
    Near-end Audio Loc:                        Codec Type: G.729
   Audio      IP Address                                 Port
   Near-end:  10.80.120.101                            : 12182
    Far-end:  10.80.120.65                             : 2062

 Video Near:
  Video Far:
 Video Port:
  Video Near-end Codec:               Video Far-end Codec:
```

Figure 71: 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 assigned on Session Manager **ASM1-DR** are down (as indicated by **0/14** in **Figure 72)**, indicating that they are all reachable for call routing.

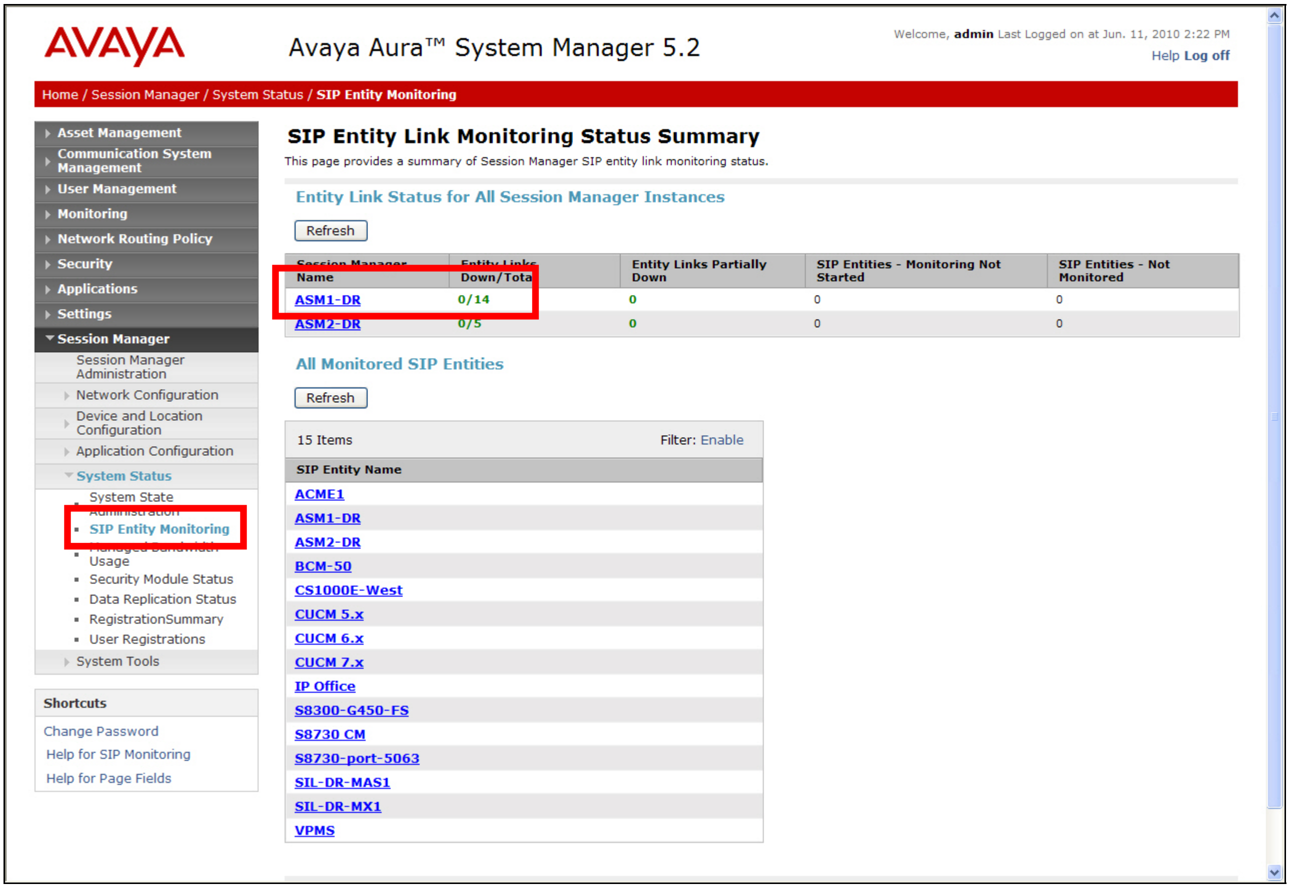

Figure 72: SIP Entity Link Monitoring - Summary

Selecting a monitored SIP Entity from the list will display its status (e.g. **S8730_port_5063**). **Figure 73** displays a **Conn. Status** of "Up" and a **Reason Code** of "200 OK" for SIP Entity S8730-port-5063. As pointed out in **Section 5.1**, the SIP Entity associated with the SBC (e.g. **ACME1**) will display a **Conn. Status** "Up" and a **Reason Code** of "404 Not Found".

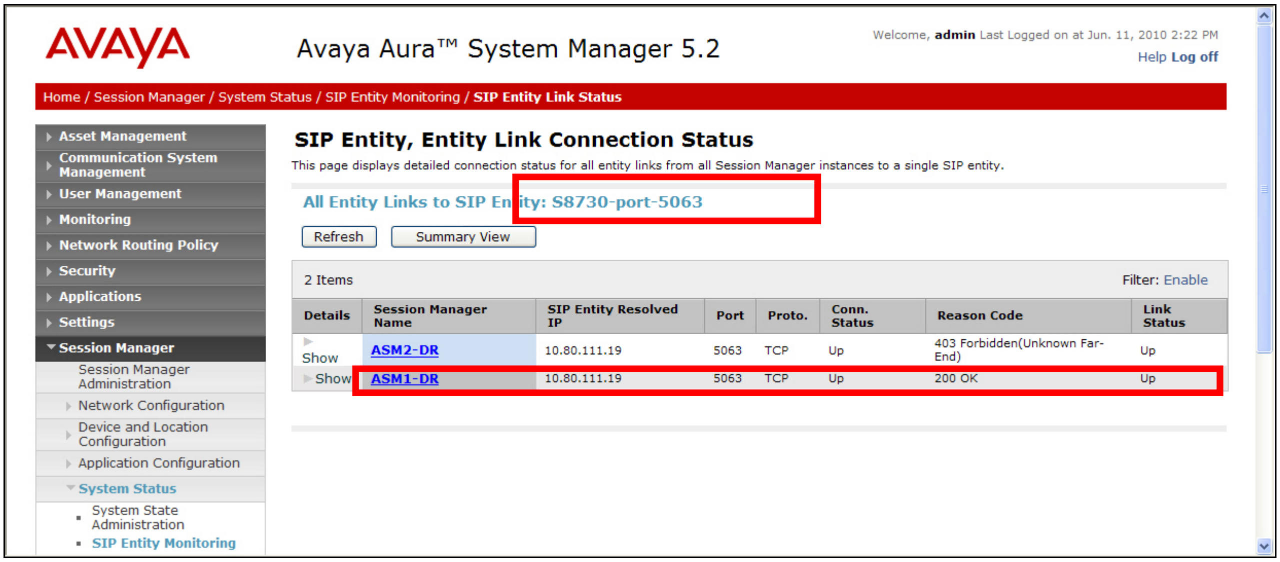

Figure 73: SIP Entity Link Connection Status

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.

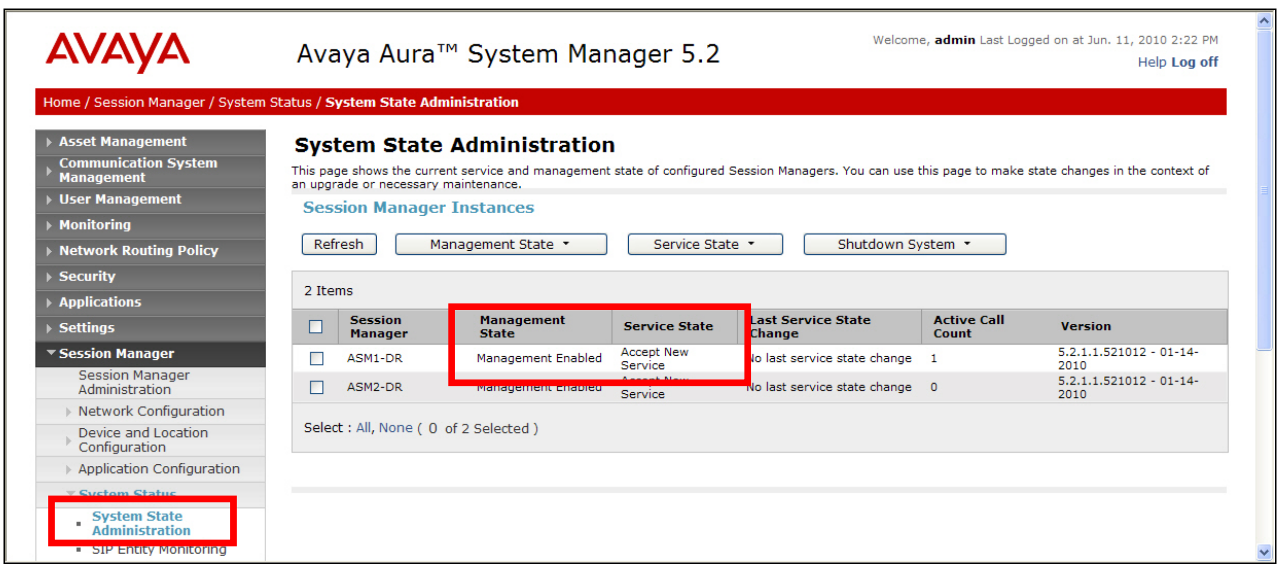

Figure 74: System State

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 6675961 to PSTN number 13035381762 is provisioned correctly.

Note - Since the DigitConversionAdapter is provisioned for the Avaya Aura™ Communication Manager Clan SIP Entity (e.g. S8730_port_5063), station 6675961 will be converted to its Skype Online Number (+13038005961) 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 – +1035381762@sip.skype.com** → This is the request URI sent by Avaya Aura™ Communication Manager to Avaya Aura™ Session Manager.
- **Calling Party URI – +13038005961@sip.skype.com** → This is the contents of the Avaya Aura™ Communication Manager From header.
- **Calling Party Address – 10.80.111.19** → This is the source IP address of the call (Avaya Aura™ Communication Manager C-LAN).
- **Session Manager Listening Port – 5063**→ 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-DR**).

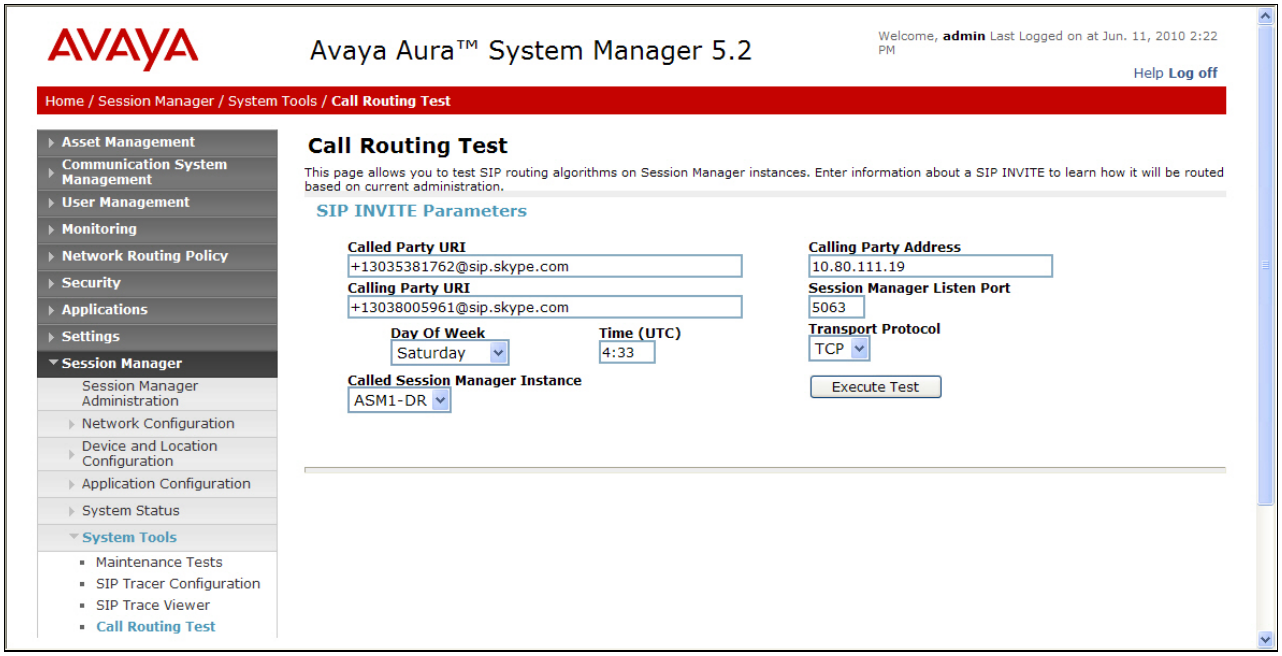

Figure 75: Call Routing Test

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 as shown in **Figure 76**. At the top of the list, the heading **Routing Decisions** shows the final result. In the example, the call will be sent to ACME1. The next heading Routing Decision Process shows all the routing algorithm calculations.

Routing Decision Process

Checking NRP to determine if this is a call to an emergency number.
Originating Location is AvayaCPE. Using digits < +13035381762 > and host < sip.skype.com > for routing.
NRP Dial Patterns: No matches for digits < +13035381762 > and domain < sip.skype.com >.
NRP Dial Patterns: No matches for digits < +13035381762 > and domain < skype.com >.
NRP Dial Patterns: No matches for digits < +13035381762 > and domain < null >.
NRP Dial Patterns: No matches found for AvayaCPE. Trying again using NRP Dial Patterns that specify -ALL- NRP Locations.
NRP Dial Patterns: Found a Dial Pattern match for pattern < + > Min/Max length 1/36 and domain < sip.skype.com >.
NRP Routing Policies: Ranked destination NRP Sip Entities: ACME1.
NRP Routing Policies: Removing disabled routes.
NRP Routing Policies: Ranked destination NRP Sip Entities: ACME1.
NRP Adaptations: SkypeDigitConversionAdapter applied.
NRP Adaptations: P-Asserted-Identity set to sip:+13038005961@sip.skype.com
NRP Sip Entities: Originating SIP Entity is S8730-port-5063.
Originating Location is AvayaCPE. Using digits < +13035381762 > and host < sip.skype.com > for routing.
NRP Dial Patterns: No matches for digits < +13035381762 > and domain < sip.skype.com >.
NRP Dial Patterns: No matches for digits < +13035381762 > and domain < skype.com >.
NRP Dial Patterns: No matches for digits < +13035381762 > and domain < null >.
NRP Dial Patterns: No matches found for AvayaCPE. Trying again using NRP Dial Patterns that specify -ALL- NRP Locations.
NRP Dial Patterns: Found a Dial Pattern match for pattern < + > Min/Max length 1/36 and domain < sip.skype.com >.
NRP Routing Policies: Ranked destination NRP Sip Entities: ACME1.
NRP Routing Policies: Removing disabled routes.
NRP Routing Policies: Ranked destination NRP Sip Entities: ACME1.
Adapting and proxying for SIP Entity ACME1.
NRP Entity Links: Found direct link to destination. Link uses TCP to port 5063.
NRP Adaptations: no Outgoing Adaptation administered.
Route < sip:+13035381762@sip.skype.com > to SIP Entity ACME1 (10.80.120.65). Terminating Location is null.

Figure 76: Call Routing Test - Results

7.3. Verify Acme Packet Net-Net 3800

7.3.1 Verify SIP Session Agents

Verify that all session agents defined in **Section 5.3.7** are "in-service". The status of the session agents can be displayed by using the "show sipd agents" command. Entering this command without any arguments lists all SIP session agents. The session agent states are defined as follows:

- I – in-service
- O – out-of-service
- S – transitioning from out-of-service to in-service
- D – disabled

```
acmesystem# show sipd agents
10:26:01-56 (recent)
                       ----- Inbound -----   ---- Outbound ----- -- Latency --   Max
Session Agent          Active  Rate  ConEx  Active  Rate  ConEx    Avg    Max Burst

1.sip.skype.com      I      0   0.0      0       0   0.0      0  0.000  0.000     0
10.80.100.24         I      0   0.0      0       0   0.0      0  0.000  0.000     1
2.sip.skype.com      I      0   0.0      0       0   0.0      0  0.000  0.000     1
```

Figure 77: Session Agent Status

7.3.2 Verify SIP Surrogate Registration

Verify that the surrogate registration defined in **Section 5.3.12** is “active”. The status of surrogate registration can be displayed by using the “show registration” command.

```
acmesystem# show registration
10:35:15-140
SIP Registrations          -- Period -- -------- Lifetime --------
                 Active    High   Total      Total  PerMax    High
User Entries          0       0       0          0       0       0
Local Contacts        1       1       0          1       1       1
Via Entries           0       0       0          0       0       0
AURI Entries          0       0       0          0       0       0
Free Map Ports        0       0       0          0       0       0
Used Map Ports        0       0       0          0       0       0
Forwards              -       -       0          0       0
Refreshes             -       -       0          0       0
Rejects               -       -       0          0       0
Timeouts              -       -       0          0       0
Fwd Postponed         -       -       0          0       0
Fwd Rejected          -       -       0          0       0
Refr Extension        0       0       0          0       0       0
Refresh Extended      -       -       0          0       0
Surrogate Regs        1       1       0          1       1       1
Surrogate Sent        -       -       1       5103       2
Surrogate Reject      -       -       0        176       1
Surrogate Timeout     -       -       0          0       0
HNT Entries           0       0       0          0       0       0
Non-HNT Entries       1       1       0          1       1       1
```

Figure 78: Surrogate Registration Status

The “show sipd endpoint-id” command displays registration information for a designated endpoint. Verify that there is output from the “show sipd endpoint-ip <i>” command, where <i> is the 14 digit value assigned to **register-user** in **Section 5.3.12 Step 3**.

```
acmesystem# show sipd endpoint-ip 99051000104350
User <sip:99051000104350@sip.skype.com>
  Contact exp=164
    UA-Contact: <sip:99051000104350@sip.skype.com> keep-acl
         realm=INTERNAL
    SD-Contact: <sip:99051000104350@205.168.62.25:5060> realm=EXTERNAL
    Call-ID: 9ff1826f925d04638aa640c4674416ca@10.80.120.65'
    SA=204.9.161.164
```

Figure 79: Registration Status by Endpoint

More detailed information regarding registration is available using the “show registration sipd by-user” command. Verify the output of the “show registration sipd by-user <i>” command, where <i> is the 14 digit value assigned to **register-user** in **Section 5.3.12 Step 3**. Verify that the **Registered at** section contains time and date information.

```
acmesystem# show registration sipd by-user 99051000104350 detailed

Registration Cache (Detailed View)    MON AUG 16 2010  10:49:18

User: sip:99051000104350@sip.skype.com
  Registered at: 2010-08-09-14:15:48     Surrogate User: true

  Contact Information:
    Contact:
      Name: sip:99051000104350@sip.skype.com
      Valid: true
      Challenged: false
      Registered at: 2010-08-09-14:15:48
      Last Registered at: 2010-08-16-10:48:20
      Expire: 182
      Local expire: 182
      Half: 62

      Registrar IP: 204.9.161.164
      Transport: none
      Secure: false
      Local IP:

      User Agent Info:
        Contact: sip:99051000104350@sip.skype.com
        Realm: INTERNAL
        IP:

      SD Info:
        Contact: sip:99051000104350@205.168.62.25:5060
        Realm: EXTERNAL

      Call-ID: 9ff1826f925d04638aa640c4674416ca@10.80.120.65
```

Figure 80: Detailed Registration Status

7.4. 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.729 codecs.
    - Avaya 9630 (H.323) as well as traditional analog and digital TDM phones.
    - Inbound call from Skype P2P user to Skype Business Account delivered to an Avaya 9630 telephone.
- Direct IP-to-IP Media (also known as “Shuffling”) when applicable.
- DTMF Tone Support.
- Skype Connect SBC Redundancy.

- Supplementary calling features were verified. The supplementary calling features verified are:
  - Hold, Call transfer, Conference.
  - Voicemail Coverage and Retrieval.
  - Calling Party Number Block

7.5. Conclusion

As illustrated in these Application Notes, Avaya Aura™ Communication Manager 5.2.1, Avaya Aura™ Session Manager 5.2, and Acme Packet Session Border Controllers can be configured to interoperate successfully with the Skype Connect service. This solution provides users of Avaya Aura™ Communication Manager the ability to support inbound and outbound calls over a Skype Connect trunk service connection.

8. Support

8.1. Avaya

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

8.2. Skype

For technical support on the Skype Connect service, visit their online support at http://www.skype.com/support

9. References

9.1. Avaya

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

[1] *Configuring Avaya Modular Messaging as a Centralized Messaging Solution for the Avaya CS1000E, Avaya Aura™ Session Manager and Avaya Aura™ Communication Manager - Feature Server & Access Element 5.2.1 – Issue 1.0*
[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] *Feature Description and Implementation for Avaya Communication Manager, 555-245-205, Issue 6, January 2008*

9.2. Skype Connect

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

[7] *Skype Connect product datasheet, Version 1.0,* Doc ID 555-245-206, May, 2009.

9.3. Acme Packet

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

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

10. Appendix A – Acme Packet Net-Net 3800 Configuration

This section contains a copy of the complete SBC configuration.

ANNOTATION: The host routes below specify IP routes to the Avaya Aura™ Session Manager and NTP servers. Default routes were used to access the Skype border elements.

```
host-routes
     dest-network                    10.80.100.24
     netmask                         255.255.255.255
     gateway                         10.80.120.1
     description
     last-modified-by                admin@135.8.19.107
     last-modified-date              2010-05-10 13:33:39
host-routes
     dest-network                    135.9.1.2
     netmask                         255.255.255.255
     gateway                         135.8.19.1
     description
     last-modified-by                admin@135.8.19.107
     last-modified-date              2010-06-28 13:46:34
```

ANNOTATION: The local policy below governs the routing of SIP messages from the Skype Connect service to Session Manager.

```
local-policy
      from-address
                                      *
      to-address
                                      *
      source-realm
                                      EXTERNAL
      description
      activate-time                   N/A
      deactivate-time                 N/A
      state                           enabled
      policy-priority                 none
      last-modified-by                admin@135.8.19.107
      last-modified-date              2010-06-11 18:58:53
      policy-attribute
            next-hop                        10.80.100.24
            realm                           INTERNAL
            action                          none
            terminate-recursion             disabled
            carrier
            start-time                      0000
            end-time                        2400
            days-of-week                    U-S
            cost                            0
            app-protocol                    SIP
            state                           enabled
            methods
            media-profiles
            lookup                          single
```

```
            next-key
            eloc-str-lkup                 disabled
            eloc-str-match
```

ANNOTATION: The local policy below governs the routing of SIP messages from elements on the network on which the Avaya elements, e.g., Communication Manager, etc., reside to the Skype Connect service. The Session Agent Group (SAG) is defined here, and further down, provisioned under the session group “SKYPE_GROUP”.

```
local-policy
     from-address
                              *
     to-address
                              *
     source-realm
                              INTERNAL
     description
     activate-time            N/A
     deactivate-time          N/A
     state                    enabled
     policy-priority          none
     last-modified-by         admin@135.8.19.107
     last-modified-date       2010-06-11 19:39:18
     policy-attribute
      next-hop                 SAG:SKYPE_GROUP
      realm                    EXTERNAL
      action                   none
      terminate-recursion      disabled
      carrier
      start-time               0000
      end-time                 2400
      days-of-week             U-S
      cost                     0
      app-protocol             SIP
      state                    enabled
      methods
      media-profiles
      lookup                   single
      next-key
      eloc-str-lkup            disabled
      eloc-str-match
```

ANNOTATION: The policy attribute below terminates SIP OPTIONS messages from Session Manager at the SBC. These are not forwarded to the Skype Connect service.

```
     policy-attribute
      next-hop                 0.0.0.0
      realm
      action                   none
      terminate-recursion      disabled
      carrier
      start-time               0000
      end-time                 2400
      days-of-week             U-S
```

```
        cost                            0
        app-protocol                    SIP
        state                           enabled
        methods                         OPTIONS
        media-profiles
        lookup                          single
        next-key
        eloc-str-lkup                   disabled
        eloc-str-match
```

ANNOTATION: Enable Media Manager state on the Acme Packet SBC.

```
media-manager
        state                           enabled
        latching                        enabled
        flow-time-limit                 86400
        initial-guard-timer             300
        subsq-guard-timer               300
        tcp-flow-time-limit             86400
        tcp-initial-guard-timer         300
        tcp-subsq-guard-timer           300
        tcp-number-of-ports-per-flow    2
        hnt-rtcp                        disabled
        algd-log-level                  NOTICE
        mbcd-log-level                  NOTICE
        red-flow-port                   1985
        red-mgcp-port                   1986
        red-max-trans                   10000
        red-sync-start-time             5000
        red-sync-comp-time              1000
        media-policing                  enabled
        max-signaling-bandwidth         10000000
        max-untrusted-signaling         100
        min-untrusted-signaling         30
        app-signaling-bandwidth         0
        tolerance-window                30
        rtcp-rate-limit                 0
        trap-on-demote-to-deny          enabled
        min-media-allocation            2000
        min-trusted-allocation          4000
        deny-allocation                 64000
        anonymous-sdp                   disabled
        arp-msg-bandwidth               32000
        fragment-msg-bandwidth          0
        rfc2833-timestamp               disabled
        default-2833-duration           100
        rfc2833-end-pkts-only-for-non-sig enabled
        translate-non-rfc2833-event     disabled
        media-supervision-traps         disabled
        dnsalg-server-failover          disabled
        last-modified-by                admin@135.8.19.107
        last-modified-date              2010-05-10 03:13:36
```

ANNOTATION: The network interface below defines the IP addresses on the interface connected to the network on which the Skype Connect service resides. External ISP DNS servers were configured to resolve the Skype Connect SIP domains.

```
network-interface
     name                           s0p0
     sub-port-id                    0
     description
     hostname
     ip-address                     205.168.62.25
     pri-utility-addr
     sec-utility-addr
     netmask                        255.255.255.128
     gateway                        205.168.62.1
     sec-gateway
     gw-heartbeat
      state                          disabled
      heartbeat                      0
      retry-count                    0
      retry-timeout                  1
      health-score                   0
     dns-ip-primary                 205.171.3.65
     dns-ip-backup1                 205.171.2.65
     dns-ip-backup2
     dns-domain                     sip.skype.com
     dns-timeout                    11
        hip-ip-list                    205.168.62.25
     ftp-address                    205.168.62.25
        icmp-address                   205.168.62.25
     snmp-address
     telnet-address
     ssh-address                    205.168.62.25
     last-modified-by               admin@135.8.19.107
     last-modified-date             2010-07-09 22:41:52
```

ANNOTATION: The network interface below defines the IP addresses on the interface connected to the network on which the Avaya elements reside.

```
network-interface
     name                           s0p1
     sub-port-id                    0
     description
     hostname
     ip-address                     10.80.120.65
     pri-utility-addr
     sec-utility-addr
     netmask                        255.255.255.0
     gateway                        10.80.120.1
     sec-gateway
     gw-heartbeat
      state                          disabled
      heartbeat                      0
      retry-count                    0
      retry-timeout                  1
```

```
 health-score                    0
dns-ip-primary
dns-ip-backup1
dns-ip-backup2
dns-domain
dns-timeout                     11
   hip-ip-list                     10.80.120.65
ftp-address
   icmp-address                    10.80.120.65
snmp-address
telnet-address
ssh-address
last-modified-by                admin@135.8.19.107
last-modified-date              2010-05-09 20:24:30
```

ANNOTATION: The NTP time server configuration for the SBC is shown below.

```
ntp-config
     server                          135.9.1.2
     last-modified-by                admin@135.8.19.107
     last-modified-date              2010-05-10 00:16:59
```

ANNOTATION: The physical interface configuration for the SBC is shown below.

```
phy-interface
     name                            s0p1
     operation-type                  Media
     port                            1
     slot                            0
     virtual-mac
     admin-state                     enabled
     auto-negotiation                enabled
     duplex-mode
     speed
     overload-protection             disabled
     last-modified-by                admin@10.80.120.1
     last-modified-date              2010-05-09 17:34:48

phy-interface
     name                            s0p0
     operation-type                  Media
     port                            0
     slot                            0
     virtual-mac
     admin-state                     enabled
     auto-negotiation                enabled
     duplex-mode                     FULL
     speed                           100
     overload-protection             disabled
     last-modified-by                admin@10.80.120.1
     last-modified-date              2010-05-09 17:34:13
```

ANNOTATION: The realm configuration “EXTERNAL” below represents the external network on which the Skype Connect service resides.

```
realm-config
     identifier                    EXTERNAL
     description
     addr-prefix                   0.0.0.0
     network-interfaces
                                   s0p0:0
     mm-in-realm                   disabled
     mm-in-network                 enabled
     mm-same-ip                    enabled
     mm-in-system                  enabled
     bw-cac-non-mm                 disabled
     msm-release                   disabled
     generate-UDP-checksum         disabled
     max-bandwidth                 0
     fallback-bandwidth            0
     max-priority-bandwidth        0
     max-latency                   0
     max-jitter                    0
     max-packet-loss               0
     observ-window-size            0
     parent-realm
     dns-realm
     media-policy
     media-sec-policy
     in-translationid
     out-translationid
     in-manipulationid
     out-manipulationid
     manipulation-string
     manipulation-pattern
     class-profile
     average-rate-limit            0
     access-control-trust-level    none
     invalid-signal-threshold      0
     maximum-signal-threshold      0
     untrusted-signal-threshold    0
     nat-trust-threshold           0
     deny-period                   30
     ext-policy-svr
     symmetric-latching            disabled
     pai-strip                     disabled
     trunk-context
     early-media-allow
     enforcement-profile
     additional-prefixes
     restricted-latching           none
     restriction-mask              32
     accounting-enable             enabled
     user-cac-mode                 none
     user-cac-bandwidth            0
     user-cac-sessions             0
     icmp-detect-multiplier        0
```

```
     icmp-advertisement-interval    0
     icmp-target-ip
     monthly-minutes                0
     net-management-control         disabled
     delay-media-update             disabled
     refer-call-transfer            disabled
     dyn-refer-term                 disabled
     codec-policy
     codec-manip-in-realm           disabled
     constraint-name
     call-recording-server-id
     xnq-state                      xnq-unknown
     hairpin-id                     0
     stun-enable                    disabled
     stun-server-ip                 0.0.0.0
     stun-server-port               3478
     stun-changed-ip                0.0.0.0
     stun-changed-port              3479
     match-media-profiles
     qos-constraint
     sip-profile
     sip-isup-profile
     block-rtcp                     disabled
     hide-egress-media-update       disabled
     last-modified-by               admin@135.8.19.107
     last-modified-date             2010-07-08 19:47:07
```

ANNOTATION: The realm configuration "INTERNAL" below represents the internal network on which the Avaya elements reside.

```
realm-config
     identifier                     INTERNAL
     description
     addr-prefix                    0.0.0.0
     network-interfaces
                                    s0p1:0
     mm-in-realm                    disabled
     mm-in-network                  enabled
     mm-same-ip                     enabled
     mm-in-system                   enabled
     bw-cac-non-mm                  disabled
     msm-release                    disabled
     generate-UDP-checksum          disabled
     max-bandwidth                  0
     fallback-bandwidth             0
     max-priority-bandwidth         0
     max-latency                    0
     max-jitter                     0
     max-packet-loss                0
     observ-window-size             0
     parent-realm
     dns-realm
     media-policy
     media-sec-policy
     in-translationid
     out-translationid
```

```
in-manipulationid
out-manipulationid
manipulation-string
manipulation-pattern
class-profile
average-rate-limit              0
access-control-trust-level      none
invalid-signal-threshold        0
maximum-signal-threshold        0
untrusted-signal-threshold      0
nat-trust-threshold             0
deny-period                     30
ext-policy-svr
symmetric-latching              disabled
pai-strip                       disabled
trunk-context
early-media-allow
enforcement-profile
additional-prefixes
restricted-latching             none
restriction-mask                32
accounting-enable               enabled
user-cac-mode                   none
user-cac-bandwidth              0
user-cac-sessions               0
icmp-detect-multiplier          0
icmp-advertisement-interval     0
icmp-target-ip
monthly-minutes                 0
net-management-control          disabled
delay-media-update              disabled
refer-call-transfer             disabled
dyn-refer-term                  disabled
codec-policy
codec-manip-in-realm            disabled
constraint-name
call-recording-server-id
xnq-state                       xnq-unknown
hairpin-id                      0
stun-enable                     disabled
stun-server-ip                  0.0.0.0
stun-server-port                3478
stun-changed-ip                 0.0.0.0
stun-changed-port               3479
match-media-profiles
qos-constraint
sip-profile
sip-isup-profile
block-rtcp                      disabled
hide-egress-media-update        disabled
last-modified-by                admin@135.8.19.107
last-modified-date              2010-06-11 20:06:07
```

ANNOTATION: The session agent below represents the Session Manager used in the reference configuration. Note that here a header manipulation rule named **Avaya-incoming** (defined below) is assigned.

```
session-agent
      hostname                      10.80.100.24
      ip-address                    10.80.100.24
      port                          5063
      state                         enabled
      app-protocol                  SIP
      app-type
      transport-method              StaticTCP
      realm-id                      INTERNAL
      egress-realm-id
      description                   Avaya Aura Session Manager
      carriers
      allow-next-hop-lp             enabled
      constraints                   disabled
      max-sessions                  0
      max-inbound-sessions          0
      max-outbound-sessions         0
      max-burst-rate                0
      max-inbound-burst-rate        0
      max-outbound-burst-rate       0
      max-sustain-rate              0
      max-inbound-sustain-rate      0
      max-outbound-sustain-rate     0
      min-seizures                  5
      min-asr                       0
      time-to-resume                0
      ttr-no-response               0
      in-service-period             0
      burst-rate-window             0
      sustain-rate-window           0
      req-uri-carrier-mode          None
      proxy-mode
      redirect-action
      loose-routing                 enabled
      send-media-session            enabled
      response-map
      ping-method                   OPTIONS
      ping-interval                 300
      ping-send-mode                keep-alive
      ping-all-addresses            disabled
      ping-in-service-response-codes
      out-service-response-codes
      media-profiles
      in-translationid
      out-translationid
      trust-me                      disabled
      request-uri-headers
      stop-recurse                  408,486
      local-response-map
      ping-to-user-part
      ping-from-user-part
```

```
li-trust-me                     disabled
in-manipulationid               Avaya-incoming
out-manipulationid
manipulation-string
manipulation-pattern
p-asserted-id
trunk-group
max-register-sustain-rate       0
early-media-allow
invalidate-registrations        disabled
rfc2833-mode                    none
rfc2833-payload                 0
codec-policy
enforcement-profile
refer-call-transfer             disabled
reuse-connections               NONE
tcp-keepalive                   none
tcp-reconn-interval             10
max-register-burst-rate         0
register-burst-window           0
sip-profile
sip-isup-profile
last-modified-by                admin@135.8.19.107
last-modified-date              2010-07-13 11:52:18
```

ANNOTATION: The **session agents** below represent the Skype Connect service border elements. The Acme Packet SBC will attempt to send calls to the Primary or Secondary border elements. Both Skype Connect service border elements are also specified in the **session-group** section. SAG recursion behavior can be modified using the **stop-recurse** parameter. As shown, SAG recursion is stopped if a SIP 408 Timeout or a SIP 486 User Busy message is received from the Skype Connect service.

```
session-agent
      hostname                  2.sip.skype.com
      ip-address
      port                      5060
      state                     enabled
      app-protocol              SIP
      app-type
      transport-method          UDP
      realm-id                  EXTERNAL
      egress-realm-id
      description               Skype for SIP SBC Primary
      carriers
      allow-next-hop-lp         enabled
      constraints               disabled
      max-sessions              0
      max-inbound-sessions      0
      max-outbound-sessions     0
      max-burst-rate            0
      max-inbound-burst-rate    0
      max-outbound-burst-rate   0
      max-sustain-rate          0
      max-inbound-sustain-rate  0
      max-outbound-sustain-rate 0
```

```
        min-seizures                    5
        min-asr                         0
        time-to-resume                  30
        ttr-no-response                 30
        in-service-period               30
        burst-rate-window               0
        sustain-rate-window             0
        req-uri-carrier-mode            None
        proxy-mode
        redirect-action
        loose-routing                   enabled
        send-media-session              enabled
        response-map
        ping-method
        ping-interval                   0
        ping-send-mode                  keep-alive
        ping-all-addresses              disabled
        ping-in-service-response-codes
        out-service-response-codes
        media-profiles
        in-translationid
        out-translationid
        trust-me                        disabled
        request-uri-headers
        stop-recurse                    408,486
        local-response-map
        ping-to-user-part
        ping-from-user-part
        li-trust-me                     disabled
        in-manipulationid
        out-manipulationid
        manipulation-string
        manipulation-pattern
        p-asserted-id
        trunk-group
        max-register-sustain-rate       0
        early-media-allow
        invalidate-registrations        disabled
        rfc2833-mode                    none
        rfc2833-payload                 0
        codec-policy
        enforcement-profile
        refer-call-transfer             disabled
        reuse-connections               NONE
        tcp-keepalive                   none
        tcp-reconn-interval             0
        max-register-burst-rate         0
        register-burst-window           0
        sip-profile
        sip-isup-profile
        last-modified-by                admin@135.8.19.107
        last-modified-date              2010-07-13 11:51:40

session-agent
        hostname                        1.sip.skype.com
        ip-address
        port                            5060
```

state	**enabled**
app-protocol	**SIP**
app-type	
transport-method	**UDP**
realm-id	**EXTERNAL**
egress-realm-id	
description	**Skype for SIP SBC Secondary**
carriers	
allow-next-hop-lp	**enabled**
constraints	disabled
max-sessions	0
max-inbound-sessions	0
max-outbound-sessions	0
max-burst-rate	0
max-inbound-burst-rate	0
max-outbound-burst-rate	0
max-sustain-rate	0
max-inbound-sustain-rate	0
max-outbound-sustain-rate	0
min-seizures	5
min-asr	0
time-to-resume	30
ttr-no-response	30
in-service-period	30
burst-rate-window	0
sustain-rate-window	0
req-uri-carrier-mode	None
proxy-mode	
redirect-action	
loose-routing	enabled
send-media-session	enabled
response-map	
ping-method	
ping-interval	**0**
ping-send-mode	keep-alive
ping-all-addresses	disabled
ping-in-service-response-codes	
out-service-response-codes	
media-profiles	
in-translationid	
out-translationid	
trust-me	disabled
request-uri-headers	
stop-recurse	**408,486**
local-response-map	
ping-to-user-part	
ping-from-user-part	
li-trust-me	disabled
in-manipulationid	
out-manipulationid	
manipulation-string	
manipulation-pattern	
p-asserted-id	
trunk-group	
max-register-sustain-rate	0
early-media-allow	
invalidate-registrations	disabled

```
rfc2833-mode                   none
rfc2833-payload                0
codec-policy
enforcement-profile
refer-call-transfer            disabled
reuse-connections              NONE
tcp-keepalive                  none
tcp-reconn-interval            0
max-register-burst-rate        0
register-burst-window          0
sip-profile
sip-isup-profile
last-modified-by               admin@216.41.24.2
last-modified-date             2010-07-09 14:31:44
```

ANNOTATION: The **session group** below specifies the Skype Connect service border elements (see **session agents** above). Also a **strategy** of "Hunt" is defined. This means the SBC will only use the secondary BE if access to the Primary fails. This session group is also specified in the local-policy source-realm "INTERNAL". SAG recursion behavior can be modified using the **stop-recurse** parameter. As shown, SAG recursion is stopped if a SIP 408 Timeout or a SIP 486 User Busy message is received from the Skype Connect service.

```
session-group
      group-name                     SKYPE_GROUP
      description
      state                          enabled
      app-protocol                   SIP
      strategy                       Hunt
      dest
                                     2.sip.skype.com
                                     1.sip.skype.com
      trunk-group
      sag-recursion                  enabled
      stop-sag-recurse               408,486
      last-modified-by               admin@135.8.19.107
      last-modified-date             2010-07-13 11:38:11
```

ANNOTATION: The sip-config defines global sip-parameters, including SIP timers, SIP options, which realm to send requests to if not specified elsewhere, and enabling the SBC to collect statistics on requests other than REGISTERs and INVITEs.

```
sip-config
      state                          enabled
      operation-mode                 dialog
      dialog-transparency            enabled
      home-realm-id                  INTERNAL
      egress-realm-id
      nat-mode                       None
      registrar-domain               *
      registrar-host                 *
      registrar-port                 0
      register-service-route         always
      init-timer                     500
      max-timer                      4000
```

```
    trans-expire                    32
    invite-expire                   180
    inactive-dynamic-conn           32
    enforcement-profile
    pac-method
    pac-interval                    10
    pac-strategy                    PropDist
    pac-load-weight                 1
    pac-session-weight              1
    pac-route-weight                1
    pac-callid-lifetime             600
    pac-user-lifetime               3600
    red-sip-port                    1988
    red-max-trans                   10000
    red-sync-start-time             5000
    red-sync-comp-time              1000
    add-reason-header               disabled
    sip-message-len                 4096
    enum-sag-match                  disabled
    extra-method-stats              enabled
    registration-cache-limit        0
    register-use-to-for-lp          disabled
    options                         max-udp-length=0
    refer-src-routing               disabled
    add-ucid-header                 disabled
    proxy-sub-events
    pass-gruu-contact               disabled
    sag-lookup-on-redirect          disabled
    last-modified-by                admin@console
    last-modified-date              2010-07-10 13:27:05
```

ANNOTATION: The SIP interface below is used to communicate with the Avaya Aura™ Session Manager.

```
sip-interface
     state                          enabled
     realm-id                       INTERNAL
     description
     sip-port
      address                        10.80.120.65
      port                           5063
      transport-protocol             TCP
      tls-profile
      allow-anonymous                agents-only
      ims-aka-profile
     carriers
     trans-expire                   0
     invite-expire                  0
     max-redirect-contacts          0
     proxy-mode
     redirect-action
     contact-mode                   none
     nat-traversal                  none
     nat-interval                   30
     tcp-nat-interval               90
     registration-caching           enabled
```

```
     min-reg-expire                    300
     registration-interval             3600
     route-to-registrar                enabled
     secured-network                   disabled
     teluri-scheme                     disabled
     uri-fqdn-domain
     trust-mode                        all
     max-nat-interval                  3600
     nat-int-increment                 10
     nat-test-increment                30
     sip-dynamic-hnt                   disabled
     stop-recurse                      401,407
     port-map-start                    0
     port-map-end                      0
     in-manipulationid
     out-manipulationid
     manipulation-string
     manipulation-pattern
     sip-ims-feature                   disabled
     operator-identifier
     anonymous-priority                none
     max-incoming-conns                0
     per-src-ip-max-incoming-conns     0
     inactive-conn-timeout             0
     untrusted-conn-timeout            0
     network-id
     ext-policy-server
     default-location-string
     charging-vector-mode              pass
     charging-function-address-mode pass
     ccf-address
     ecf-address
     term-tgrp-mode                    none
     implicit-service-route            disabled
     rfc2833-payload                   101
     rfc2833-mode                      transparent
     constraint-name
     response-map
     local-response-map
     ims-aka-feature                   disabled
     enforcement-profile
     route-unauthorized-calls
     tcp-keepalive                     none
     add-sdp-invite                    disabled
     add-sdp-profiles
     sip-profile
     sip-isup-profile
     last-modified-by                  admin@console
     last-modified-date                2010-07-10 13:22:14
```

ANNOTATION: The SIP interface below is used to communicate with the Skype Connect service.

```
sip-interface
     state                             enabled
     realm-id                          EXTERNAL
```

```
description
sip-port
 address                       205.168.62.25
 port                          5060
 transport-protocol            UDP
 tls-profile
 allow-anonymous               agents-only
 ims-aka-profile
carriers
trans-expire                   0
invite-expire                  0
max-redirect-contacts          0
proxy-mode
redirect-action
contact-mode                   none
nat-traversal                  none
nat-interval                   30
tcp-nat-interval               90
registration-caching           disabled
min-reg-expire                 300
registration-interval          3600
route-to-registrar             disabled
secured-network                disabled
teluri-scheme                  disabled
uri-fqdn-domain
trust-mode                     all
max-nat-interval               3600
nat-int-increment              10
nat-test-increment             30
sip-dynamic-hnt                disabled
stop-recurse                   401,407
port-map-start                 0
port-map-end                   0
in-manipulationid
out-manipulationid
manipulation-string
manipulation-pattern
sip-ims-feature                disabled
operator-identifier
anonymous-priority             none
max-incoming-conns             0
per-src-ip-max-incoming-conns  0
inactive-conn-timeout          0
untrusted-conn-timeout         0
network-id
ext-policy-server
default-location-string
charging-vector-mode           pass
charging-function-address-mode pass
ccf-address
ecf-address
term-tgrp-mode                 none
implicit-service-route         disabled
rfc2833-payload                101
rfc2833-mode                   transparent
constraint-name
response-map
```

```
    local-response-map
    ims-aka-feature               disabled
    enforcement-profile
    route-unauthorized-calls
    tcp-keepalive                 none
    add-sdp-invite                disabled
    add-sdp-profiles
    sip-profile
    sip-isup-profile
    last-modified-by              admin@135.8.19.107
    last-modified-date            2010-07-09 22:42:15
```

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

1) Insert Skype Connect User Name in From Header for outbound calls from Avaya CPE to Skype Connect
2) Insert Skype Connect domain in From Header for outbound calls from Avaya CPE to Skype Connect

```
sip-manipulation
      name                          Avaya-incoming
      description                   insert skype user name in From header
required for Skype and also used to match surrogate user required for Proxy-
Authentication
      split-headers
      join-headers
      header-rule
            name                          skype_From
            header-name                   From
            action                        manipulate
            comparison-type               case-sensitive
            msg-type                      request
            methods
            match-value
            new-value
            element-rule
                  name                          skype_From_user
                  parameter-name                From
                  type                          uri-user
                  action                        replace
                  match-val-type                any
                  comparison-type               case-sensitive
                  match-value
                  new-value                     99051000104350
            element-rule
                  name                          skype_From_host
                  parameter-name                From
                  type                          uri-host
                  action                        replace
                  match-val-type                any
                  comparison-type               case-sensitive
                  match-value
                  new-value                     sip.skype.com
      last-modified-by              admin@135.8.19.107
```

```
      last-modified-date            2010-07-09 15:18:48
```

ANNOTATION: The steering pools below define the RTP port range on the respective realms.

```
steering-pool
      ip-address                    205.168.62.25
      start-port                    49152
      end-port                      65535
      realm-id                      EXTERNAL
      network-interface
      last-modified-by              admin@135.8.19.107
      last-modified-date            2010-05-11 22:19:24

steering-pool
      ip-address                    10.80.120.65
      start-port                    2048
      end-port                      65535
      realm-id                      INTERNAL
      network-interface
      last-modified-by              admin@135.8.19.107
      last-modified-date            2010-06-11 19:10:24
```

ANNOTATION: Surrogate registration allows the Acme Packet SBC to perform trunk side registrations to the Skype Connect network on behalf of the Avaya CPE. Programming of the surrogate registration capability is only necessary if **Registration Method** is selected on the Skype Connect profile as described in **Section 6.3.1.** Note that the values for **register-user**, **register-contact-user** and **password** are assigned by Skype and are displayed on the Authentication details page as shown in **Section 6.3.1**.

```
surrogate-agent
      register-host                 sip.skype.com
      register-user                 99051000104350
      state                         enabled
      realm-id                      INTERNAL
      description
      customer-host
      customer-next-hop             SAG:SKYPE_GROUP
      register-contact-host         205.168.62.25
      register-contact-user         99051000104350
      password                      XXXXXXXXXXXXXX
      register-expires              240
      replace-contact               disabled
      options                       auth-
method="INVITE,CANCEL,ACK,BYE,UPDATE,PRACK,INFO,OPTIONS"
      route-to-registrar            enabled
      aor-count                     1
      auth-user
      max-register-attempts         3
      register-retry-time           300
      count-start                   1
      last-modified-by              admin@135.8.19.107
      last-modified-date            2010-07-10 13:45:40
```

ANNOTATION: The “system-config” section below describes the system configuration used during testing.

```
system-config
      hostname                       acmesbc
      description
      location
      mib-system-contact
      mib-system-name
      mib-system-location
      snmp-enabled                   enabled
      enable-snmp-auth-traps         disabled
      enable-snmp-syslog-notify      disabled
      enable-snmp-monitor-traps      disabled
      enable-env-monitor-traps       disabled
      snmp-syslog-his-table-length   1
      snmp-syslog-level              WARNING
      system-log-level               WARNING
      process-log-level              DEBUG
      process-log-ip-address         0.0.0.0
      process-log-port               0
      collect
            sample-interval                5
            push-interval                  15
            boot-state                     disabled
            start-time                     now
            end-time                       never
            red-collect-state              disabled
            red-max-trans                  1000
            red-sync-start-time            5000
            red-sync-comp-time             1000
            push-success-trap-state        disabled
      call-trace                     enabled
      internal-trace                 enabled
      log-filter                     all
      default-gateway                205.168.62.1
      restart                        enabled
      exceptions
      telnet-timeout                 0
      console-timeout                0
      remote-control                 enabled
      cli-audit-trail                enabled
      link-redundancy-state          disabled
      source-routing                 disabled
      cli-more                       disabled
      terminal-height                24
      debug-timeout                  0
      trap-event-lifetime            0
      default-v6-gateway             ::
      ipv6-support                   disabled
      cleanup-time-of-day            00:00
      last-modified-by               admin@135.8.19.107
      last-modified-date             2010-07-08 21:37:04
capture-receiver
      state                          disabled
      address
```

```
network-interface              :0
last-modified-by               admin@135.8.19.107
last-modified-date             2010-05-10 15:16:31
```

11. Appendix B – DTMF Tone Leakage

A DTMF "tone leakage" interoperability issue was occasionally observed with Skype Connect. The scenario involves an inbound call from Skype Connect to the Avaya CPE in which the call is processed by call vectoring on Communication Manager and call prompting is involved to collect DTMF digits. DTMF digits were being detected twice. When the issue occurs, the RTP stream that Skype sends not only contains DTMF RTP payload event packets as specified in the RFC, but also has audible tones embedded in the audio stream.

The issue was reported to Skype and is under investigation. If this issue appears in the field, the workaround described below can been implemented to strip off any DTMF signal from the RTP stream.

G430/G450 Media Gateways:
VoIP parameter 60 will try to strip out the tone from the received RTP stream. The G4xx Media Gateway commands to activate it (via telnet or SSH) are:

G450-001(super)# **voip-parameters**
Warning:
The values chosen for non-default voip parameters can significantly affect
the quality of service that users experience. Avaya recommends seeking
technical assistance from Avaya before making any modifications to the voip
parameter defaults.
G450-001(super-voip-parameters)# **set id 60 value 1**
Done!
G450-001(super-voip-parameters)# **exit**
G450-001(super)# **copy run start**
Warning! It is a recommended policy to override default configuration
master key with user defined secret - for details see user reference.
Otherwise device saves configuration secrets using Avaya default secret.
Beginning copy operation .... Done!
G450-001(super)#

TN2602 Circuit Pack:
VoIP parameter 60 will try to strip out the tone from the received RTP stream. The "TN2602" commands to activate it (via telnet or SSH) are:

setVoipParam 60, 1
sendVoipParams
saveVoipParams
reset

Please e-mail any questions or comments pertaining to these Application Notes along with the full title name and filename, located in the lower right corner, directly to the Avaya Solution & Interoperability Test Lab at interoplabnotes@list.avaya.com