Avaya Solution & Interoperability Test Lab

Application Notes for Avaya Aura™ Communication Manager 6.0 and Acme Packet Net-Net Session Director 6.2.0 SIP Trunk Integration with Skype Connect – Issue 1.1

Abstract

These Application Notes describe the steps to configure Avaya Aura™ Communication Manager (version 6.0) and Acme Packet Net-Net Session Director (version 6.2.0) to connect to the Skype Connect service via a SIP trunk.

The Skype Connect service referenced in these Application Notes is designed for business customers with an Avaya SIP trunk solution. The service provides bi-directional 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 broadband data circuit for accessing the Skype Connect service directly over the Internet.

Table of Contents

1. Introduction

These Application Notes describe the steps to configure Avaya Aura™ Communication Manager (version 6.0) and Acme Packet Net-Net Session Director (version 6.2.0) to connect to the Skype Connect service via a SIP trunk. 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 depicted in these Application Notes consists of Avaya Aura™ Communication Manager (version 6.0). 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 see **Reference [1]**.

In the reference configuration, a single Acme Packet 3800 Net-Net Session Director 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 CPE topology hiding functionality.

The Skype Connect service described in these Application Notes is designed for business customers using Avaya Aura™ Communication Manager and an Acme Packet Net-Net Session Director SBC. 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 [4]**.

1.1. Skype Connect SBC Redundancy

A single Acme Packet 3800 Net-Net Session Director 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 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 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 an edge router that provides access to the Internet via a traditional T1 data broadband 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.

The installation and provisioning of the broadband ISP circuit is not part of the Skype Connect service and is outside of the scope of these Application Notes.

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™ Communication Manager to their associated Avaya Aura™ Communication Manager extensions.

The Skype Connect service uses a domain of *sip.skype.com.* The Avaya CPE environment was assigned a domain of *avaya.com*; however any other enterprise SIP domain can be used in a production environment.

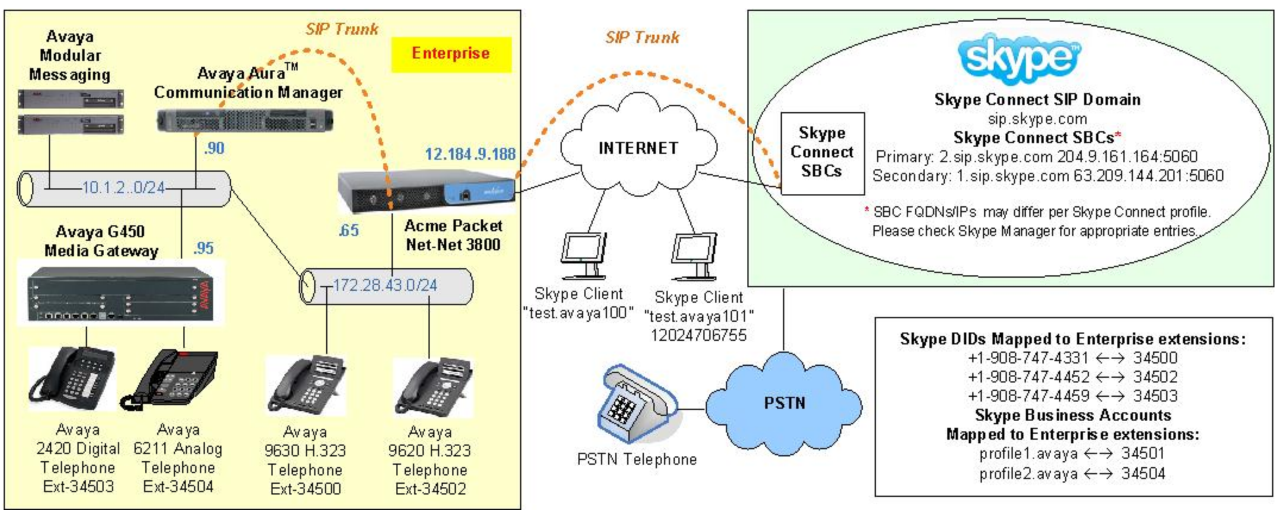

Figure 1: Reference Configuration

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 for SIP 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 for SIP domain
      - Signaling Group defined with Near-end Listen Port 5063
      - Trunk components assigned to IP Network Region 68
      - IP Network Region 68 specifies Skype for SIP domain and IP Codec Set 5
      - IP Codec Set 5 specifies G.729
  - Provide digit conversion functionality (converting Skype for SIP 11 digit numbers to 5 digit Avaya Aura™ Communication Manager extensions and vice-versa)
  - Avaya Aura™ Communication Manager running on Avaya S8800 Server with an Avaya G450 Media Gateway
- Avaya 9600 Series IP telephones using the H.323 software bundle
- Avaya 2420 Digital phone

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 and G.711A are 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 was configured in these Application Notes to listen on port 5063 for these calls; however another port could have been used. 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 outbound and inbound call examples were implemented in the sample configuration depicted in these Application Notes.

Given:

- Station 34500
- Inbound/Outbound SIP trunk 68

Inbound

- Voice
  - PSTN dials Skype Connect online DID number (19087474459) and the Skype Connect service sends the call to the Acme Packet Net-Net 3800 SBC at the Avaya CPE.
  - The Acme Packet SBC passes the call to Avaya Aura™ Communication Manager via trunk 68. Avaya Aura™ Communications Manager performs digit conversion, changes the 11 digit DID number to the associated extension (34500), and sends the call to Avaya Aura™ Communication Manager processor ethernet board port 5063.

Outbound

- Voice
  - Avaya Aura™ Communication Manager voice stations first dial 9 followed by an 11 digit number (19088485705).
  - 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, performs digit manipulation and sends the call via the S8800 processor Ethernet board to the Acme Packet SBC:
    - Port 5063
    - G729 audio codec
    - The Skype Connect domain
      - *sip.skype.com*
  - The Acme Packet SBC performs header manipulation on the From header in the SIP Invite as follows:
    - From: <sip:99051000003759@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 Packet 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 uses a domain of *avaya.com*, and the Skype Connect service uses 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 the Acme Packet SBC with the format:

<called number>@ sip.skype.com

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 Avaya Aura™ Communication Manager.
- 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.
- For outbound calls (local, national and international) via Skype Connect the E.164 or International numbering format (00 + <country code>) must be used.
- For inbound calls Skype Connect delivers the called/calling number in E.164 format
- 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.
- This solution does currently support outbound SIP calls to Skype names.
- 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.
- On outbound calls from Avaya Communication Manager to the PSTN, the called party phone sometimes displays the following calling name: “sip_profile:990”. The calling party number is displayed correctly.
- Occasionally on calls from the PSTN to the Avaya CPE, post dial delays bigger than 7 seconds were observed before a SIP INVITE message comes in from Skype Connect.
- Avaya Aura™ Communication Manager does not terminate a call properly if it gets a “408 Request Timeout” message from Skype Connect. When the message is received by the PBX, the PSTN called party is disconnected, however the Avaya telephone continues ringing. The issue is being investigated.

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	Software
Avaya S8800 Server	-
Avaya Aura™ Communication Manager	R016x.00.0.345.0
Avaya G450 Media Gateway	30.13.2
Avaya 9620 and 9630 H.323 IP Telephones	3.110b (H.323)
Avaya 2420 Digital Telephones	-
Avaya 6211 Analog Telephones	-
Avaya Modular Messaging	5.2
Acme Packet 3800 Net-Net Session Director	SCX6.2.0 MR-3 GA (Build 619)
Skype Connect	1.4
Skype Clients	4.2.32.169

Table 1: Equipment and Software Used in the Reference Configuration

3. Configure Avaya Aura™ Communication Manager for SIP Trunking

This section describes the steps for configuring Avaya Aura™ Communication Manager with the necessary signaling and media characteristics for the SIP trunk connection with the 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 an Avaya S8800 server with an Avaya G450 Media Gateway. 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 to access 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 for SIP 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: 12000 100
           Maximum Concurrently Registered IP Stations: 18000 7
             Maximum Administered Remote Office Trunks: 12000 0
Maximum Concurrently Registered Remote Office Stations: 18000 0
              Maximum Concurrently Registered IP eCons: 414   0
  Max Concur Registered Unauthenticated H.323 Stations: 100   0
                       Maximum Video Capable Stations: 18000 0
                  Maximum Video Capable IP Softphones: 18000 0
                       Maximum Administered SIP Trunks: 24000 162
  Maximum Administered Ad-hoc Video Conferencing Ports: 24000 0
   Maximum Number of DS1 Boards with Echo Cancellation: 522   0
                             Maximum TN2501 VAL Boards: 128   0
                     Maximum Media Gateway VAL Sources: 250   1
           Maximum TN2602 Boards with 80 VoIP Channels: 128   0
          Maximum TN2602 Boards with 320 VoIP Channels: 128   0
   Maximum Number of Expanded Meet-me Conference Ports: 300   0
```

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

Note – If any changes are made to the **system-parameters customer-options** form, please 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? y
        Access Security Gateway (ASG)? n              Authorization Codes? y
        Analog Trunk Incoming Call ID? y                       CAS Branch? n
 A/D Grp/Sys List Dialing Start at 01? y                         CAS Main? n
Answer Supervision by Call Classifier? y                Change COR by FAC? n
                                 ARS? y  Computer Telephony Adjunct Links? y
                ARS/AAR Partitioning? y   Cvg Of Calls Redirected Off-net? y
          ARS/AAR Dialing without FAC? n                     DCS (Basic)? y
          ASAI Link Core Capabilities? n                DCS Call Coverage? y
          ASAI Link Plus Capabilities? n               DCS with Rerouting? y
       Async. Transfer Mode (ATM) PNC? n
  Async. Transfer Mode (ATM) Trunking? n    Digital Loss Plan Modification? y
              ATM WAN Spare Processor? n                          DS1 MSP? y
                                ATMS? y           DS1 Echo Cancellation? y
                  Attendant Vectoring? y
```

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

           IP Attendant Consoles? y
```

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

3.2. Dial Plan

In the reference configuration, the Avaya CPE environment uses five digit local extensions such as 14303. 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 **345**
     2. In the **Total Length** field enter **5**
     3. In the **Call Type** field enter **ext**
   - TAC codes:
     1. In the **Dialed String** field enter **#**
     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
     345         5    ext
     #           3    dac
     9           1    fac
```

Figure 5: Change Dialplan Analysis Form – Page 1

3.3. Node Names

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

- **SBC** and **172.28.43.65** are the **Name** and **IP Address** of the Acme SBC
- **procr** and **10.1.2.90** are the **Name** and **IP Address** of the S8800 server processor

```
display node-names ip
                                  IP NODE NAMES
    Name                  IP Address
SBC                   172.28.43.65
default               0.0.0.0
msgserver             10.1.2.14
procr                 10.1.2.90
procr6                ::
```

Figure 6: IP Node Names Form

3.4. IP-Network-Regions

Two IP Network Regions are defined in the reference configuration. The Avaya Aura™ Communication Manager SIP trunk that interfaces to the Skype Connect service via the Acme SBC is assigned to IP Network Region **68**. The Avaya S8800 server and Avaya telephones are assigned to IP Network Region **1**.

Avaya Component	IP-Network-Region
S8800 processor ethernet	1
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 3.6**).

IP Network Region assignments for signaling 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                         Rgn   VLAN
                              IP-Address/
                              Gateway Node
-- ------ ----- --------      ---------------  ----                         ---   ----
 y PROCR                      procr            /24                          1
                              10.1.2.90
                              10.1.2.1
 n PROCR                      procr6           /64                          1
                              ::
                              ::
```

Figure 7: IP Interface IP Network Region Assignments

IP Network Region assignments for the media gateway may be verified with the ***list media-gateway*** command.

```
list media-gateway

                              MEDIA-GATEWAY REPORT

Num Name                     Serial No/       IP Address/       Type    NetRgn Reg?
                             FW Ver/HW Vint   Cntrl IP Addr             RecRule

1   G450                     08IS43202588     10.1 .2 .95      g450      1       y
                             30 .13 .2  /0    10.1 .2 .90                none
```

Figure 7a: Media Gateway 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 name of the S8800 board processor ethernet interface "procr" (or the location of the C-LAN board in a G650 Media Gateway).

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


                  Type: PROCR
                                                        Target socket load: 1700

      Enable Interface? y                             Allow H.323 Endpoints? y
                                                       Allow H.248 Gateways? y
        Network Region: 1                               Gatekeeper Priority: 5


                                 IPV4 PARAMETERS
             Node Name: procr                       IP Address: 10.1.2.90


           Subnet Mask: /24
```

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 3.5** 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 S8800 "procr" IP interface (or C-LAN for Avaya G650 Media Gateways) through which they register. If an IP phone registers to a "procr" 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]**

3.4.1 IP Network Region 1

IP Network Region 1 is defined for the Avaya Aura™ Communication Manager S8800 server and IP 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 the local Avaya server and 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  20
                               IP NETWORK REGION
  Region: 1
Location:         Authoritative Domain: avaya.com
    Name: Avaya devices
MEDIA PARAMETERS                Intra-region IP-IP Direct Audio: yes
      Codec Set: 1              Inter-region IP-IP Direct Audio: yes
   UDP Port Min: 2048                      IP Audio Hairpinning? y
   UDP Port Max: 65535
DIFFSERV/TOS PARAMETERS
 Call Control PHB Value: 46
        Audio PHB Value: 46
        Video PHB Value: 26
802.1P/Q PARAMETERS
 Call Control 802.1p Priority: 6
        Audio 802.1p Priority: 6
        Video 802.1p Priority: 5      AUDIO RESOURCE RESERVATION PARAMETERS
H.323 IP ENDPOINTS                                        RSVP Enabled? n
  H.323 Link Bounce Recovery? y
```

```
 Idle Traffic Interval (sec): 20
   Keep-Alive Interval (sec): 5
            Keep-Alive Count: 5
```

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  20

 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       t
```

Figure 10: IP Network Region 1 – Page 7

3.4.2 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  20
                               IP NETWORK REGION
  Region: 68
Location: 1       Authoritative Domain: sip.skype.com
    Name: Skype Far End Region
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? y
   UDP Port Max: 3329
DIFFSERV/TOS PARAMETERS                  RTCP Reporting Enabled? y
 Call Control PHB Value: 46      RTCP MONITOR SERVER PARAMETERS
        Audio PHB Value: 46       Use Default Server Parameters? y
        Video PHB Value: 26
802.1P/Q PARAMETERS
 Call Control 802.1p Priority: 6
        Audio 802.1p Priority: 6
        Video 802.1p Priority: 5      AUDIO RESOURCE RESERVATION PARAMETERS
H.323 IP ENDPOINTS                                     RSVP Enabled? n
  H.323 Link Bounce Recovery? y
 Idle Traffic Interval (sec): 20
```

```
  Keep-Alive Interval (sec): 5
           Keep-Alive Count: 5
```

Figure 11: IP Network Region 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  20

 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       t
```

Figure 12: IP Network Region 68 – Page 3

3.5. 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
5	68	G.729/G.711MU

Table 4: Codec Form Codec Assignments

3.5.1 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**

```
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
```

Figure 15: IP Codec Set 1

3.5.2 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.**
   - Configure the **Audio Codec** field 2 to **G.711MU.**

```
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
 2: G.711MU           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

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

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

Table 5: Avaya SIP Trunk Configuration

3.6.1 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 the Acme SBC, not the transport method used to the Skype Connect service.
- Specify the S8800 processor IP interface used for SIP signaling (node name **procr**) and the Acme SBC (node name **SBC**) 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 3.2.**
- 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 3.4.2**.
- 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 **Enable Layer 3 Test** field should be set to **y** to allow SIP OPTIONS messages to be sent to the Acme Packet SBC.
- 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
  IMS Enabled? n        Transport Method: tcp
        Q-SIP? n                                               SIP Enabled LSP? n
     IP Video? n                                     Enforce SIPS URI for SRTP? y
  Peer Detection Enabled? y  Peer Server: Others



   Near-end Node Name: procr                  Far-end Node Name: SBC
 Near-end Listen Port: 5063                 Far-end Listen Port: 5060
                                         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? y                    Initial IP-IP Direct Media? n
H.323 Station Outgoing Direct Media? n             Alternate Route Timer(sec): 6
```

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 shown in **Section 5.2**.

```
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
                                              Member Assignment Method: auto
                                                       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


                                Modify Tandem Calling Number: no


 Show ANSWERED BY on Display? y
```

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.

```
add 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


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

Figure 22: Public SIP Trunk Group 68 – Page 4

3.7. Public Unknown Numbering – Basic Configuration

In the reference configuration, the extensions on Avaya Aura™ Communication Manager use a 5 digit dialing plan using extensions in the range 345xx. The **Numbering – Public/Unknown Format** form allows Avaya Aura™ Communication Manager to assign DIDs to local extensions 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. **345**).

- Set the **Ext Len** field to **5**.
- Set the **Ext Code** field to a specific telephone extension number.
- Set the **Trk Grp(s)** field to **68.**
- Set the **CPN Prefix** field to a DID assigned to the telephone extension.
- Set the **Total CPN Len** field to **11**. This is the total number of digits in the extension.
- Repeat previous steps for each DID.

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: 7
```

```
 5  345            99                         5         Maximum Entries: 240
 5  34500          68         19087474331     11
 5  34502          68         19087474452     11
 5  34503          68         19087474459     11
```

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

3.8. Call Routing

3.8.1 Outbound Calls

The following Sections describe Avaya Aura™ Communication Manager provisioning required for outbound dialing. Avaya Aura™ Communication Manager uses ARS to direct outbound calls to the Acme SBC. This routing is also used to determine the codec type used for these calls (see **Section 3.1.3**).

3.8.1.1 ARS

The Automatic Route Selection feature is used to route calls via a SIP trunk to the Acme Packet SBC, 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 3.7**).
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  10
                               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: *10
                       Answer Back Access Code:
                         Attendant Access Code: 2
      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: *20    All: *21    Deactivation: #20
   Call Forwarding Enhanced Status:        Act:        Deactivation:
                         Call Park Access Code: *22
                       Call Pickup Access Code: *23
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:

   - 1xxxxxxxxxx (voice destination beginning with 1, where xxxxxxxxxx represents any 10 digit number)
   - 011 (international voice destination)

   For example, to specify how to route calls to dialed numbers beginning with 1xxxxxxxxxx, enter the command ***change ars analysis 1xxxxxxxxxx*** and enter the following values:
   - Set the **Dialed String** field to **1xxxxxxxxxx**
   - 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 **natl**

Note – ARS will route based on the most complete match. For example, 19085555555 will match before 1xxxxxxxxxx.

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
    1xxxxxxxxxx            11   11     68       natl         n
    011                    10   18     69       intl         n
```

Figure 27: ARS Digit Analysis Table

3.8.1.2 Route Patterns

Route patterns are used to route calls to specific trunk groups. In addition, route patterns may also be used to add or delete digits prior to sending them out the specified trunk(s).

1. Use the **change route-pattern** command to define the outbound SIP trunk group included in the route pattern that ARS selects for North American calls.
   - **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: Skype Natl
                             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 – North American Outbound Calls

2. Use the **change route-pattern** command to define the outbound SIP trunk group included in the route pattern that ARS selects for international calls.
   - **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***.
     - Set the **No. Del Dgts** field to **3**. This field delete the "011" prefix. Skype Connect requires the called number to be in E.164 number format.
     - All other values may be left at their default.

```
change route-pattern 69                                           Page   1 of   3
                    Pattern Number: 69  Pattern Name: Skype Int
                             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                    3                                            n   user
```

Figure 28a: Route Pattern 68 – North American Outbound Calls

3.8.2 Incoming Calls

SIP trunk group 68 is also used for inbound voice calls. In the reference configuration, the Avaya Aura™ Communication Manager is used to convert inbound Skype online DID numbers to Avaya Aura™ Communication Manager extensions using the *change inc-call-handling-trmt trunk-group x* command, where **x** is the receiving trunk.

```
change inc-call-handling-trmt trunk-group 68                  Page   1 of   3
                     INCOMING CALL HANDLING TREATMENT
 Service/      Number   Number      Del Insert
 Feature        Len      Digits
 public-ntwrk    11 19087474331      11  34500
 public-ntwrk    11 19087474452      11  34502
 public-ntwrk    11 19087474459      11  34503
```

Figure 29: Route Pattern 68 – North American Outbound Calls

3.9. Avaya Aura™ Communication Manager Stations

In the reference configuration, 5 digit voice stations are provisioned with the extension format 143xx.

3.9.1 Voice Stations

Figure 30 shows an example of a voice extension (Avaya H.323 IP phone). Since the phone is an IP device, a virtual port (**S00001**) 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 34500                                              Page   1 of   5
                                     STATION

Extension: 34500                        Lock Messages? n             BCC: 0
     Type: 9630                         Security Code: ******         TN: 1
     Port: S00001                     Coverage Path 1: 1             COR: 1
     Name: Avaya H.323                Coverage Path 2:               COS: 1
                                      Hunt-to Station:
STATION OPTIONS
                                          Time of Day Lock Table:
              Loss Group: 19       Personalized Ringing Pattern: 1
                                                Message Lamp Ext: 34500
            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:

- Call appearances (**call-appr**) will appear automatically based on the station type.
- Select an empty button assignment and enter **cpn-blk** if you would like to test 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.

```
change station 34500                                            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: 14399
```

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

3.10. Save Avaya Aura™ Communication Manager Configuration

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

4. Acme Packet Net-Net Session Director

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, CPE high availability is not supported by Skype Connect.

4.1. 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™ Communication Manager
  - Acme Packet sends OPTIONS → Avaya Aura™ Communication Manager responds with 200 OK.
  - Avaya Aura™ Communication Manager sends OPTIONS → Acme Packet responds with 404 Not Found which is accepted by Avaya Aura™ Communication Manager as a valid "Up" Link Status response.
- Acme/SkypeConnect
  - Acme Packet to Skype Connect > OPTIONS messages are disabled.
  - Skype Connect does not send SIP OPTIONS messages.

4.2. 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 4.3.3 and 4.3.4**.

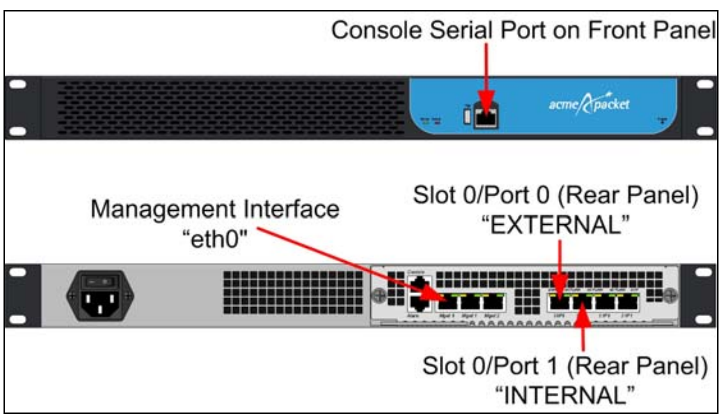

Figure 58: Acme Packet Network Interfaces

4.3. Acme Packet Provisioning

These Application Notes assume that basic Acme Packet SBC administration has already been performed. The Acme Packet SBC configuration used in the reference configuration is provided below as a reference. The notable settings are highlighted in bold and brief annotations are provided on the pertinent settings. Consult with Acme Packet Support [5-6] for further details and explanations on the configuration below.

ANNOTATION: The host routes below specify IP routes to the Skype Connect border elements and external DNS servers.

```
host-routes
      dest-network                   204.9.161.0
      netmask                        255.255.255.0
      gateway                        12.184.9.129
      description
      last-modified-by               admin@console
      last-modified-date             2010-06-17 02:59:49
host-routes
      dest-network                   63.209.144.0
      netmask                        255.255.255.0
      gateway                        12.184.9.129
      description
      last-modified-by               admin@console
      last-modified-date             2010-06-17 03:00:24
host-routes
      dest-network                   12.127.16.0
      netmask                        255.255.255.0
      gateway                        12.184.9.129
      description
      last-modified-by               admin@console
      last-modified-date             2010-06-17 11:23:58
host-routes
      dest-network                   10.1.2.0
      netmask                        255.255.255.0
      gateway                        172.28.43.1
      description
      last-modified-by               admin@console
      last-modified-date             2010-06-17 03:59:49
```

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@console
last-modified-date             2010-06-26 10:38:28
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 blocks SIP OPTIONS messages to be forwarded from Communication Manager 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: The local policy below governs the routing of SIP messages from the Skype Connect service to Communication 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@console
    last-modified-date          2010-06-16 05:33:05
    policy-attribute
          next-hop                    10.1.2.90
          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: 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@console
        last-modified-date              2010-06-16 05:40:01
```

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                      12.184.9.188
        pri-utility-addr
        sec-utility-addr
        netmask                         255.255.255.128
        gateway                         12.184.9.129
        sec-gateway
        gw-heartbeat
              state                           disabled
              heartbeat                       0
              retry-count                     0
              retry-timeout                   1
              health-score                    0
        dns-ip-primary                  12.127.16.67
        dns-ip-backup1                  12.127.16.68
        dns-ip-backup2
        dns-domain                      sip.skype.com
        dns-timeout                     11
          hip-ip-list                     12.184.9.188
        ftp-address
          icmp-address                    12.184.9.188
        snmp-address
        telnet-address
        ssh-address
        last-modified-by                admin@console
        last-modified-date              2010-06-16 05:36:44
```

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                      172.28.43.65
        pri-utility-addr
        sec-utility-addr
        netmask                         255.255.255.0
        gateway                         172.28.43.1
        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                     172.28.43.65
        ftp-address
          icmp-address                    172.28.43.65
        snmp-address
        telnet-address
        ssh-address
        last-modified-by                admin@console
        last-modified-date              2010-06-16 05:37:28
```

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

```
  phy-interface
        name                            s0p0
        operation-type                  Media
        port                            0
        slot                            0
        virtual-mac
        admin-state                     enabled
        auto-negotiation                enabled
        duplex-mode
        speed
        overload-protection             disabled
        last-modified-by                admin@console
        last-modified-date              2010-06-16 15:32:55

  phy-interface
        name                            s0p1
        operation-type                  Media
        port                            1
        slot                            0
        virtual-mac
        admin-state                     enabled
        auto-negotiation                enabled
        duplex-mode                     FULL
        speed                           100
```

```
      overload-protection             disabled
      last-modified-by                admin@console
      last-modified-date              2010-06-16 15:37:35
```

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@console
      last-modified-date            2010-06-17 17:58:39
```

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@console
last-modified-date              2010-06-17 17:59:04
```

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 below.

Note: The Skype Connect SBC FQDNs/IPs may differ per Skype Connect profile. Please check Skype Manager for appropriate entries (See section 5.3.2).

```
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 Connect Primary Border Element
      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
```

```
      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@console
      last-modified-date             2010-06-22 18:28:02
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 Connect Secondary Border Element
      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
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@console
last-modified-date             2010-06-22 18:43:49
```

ANNOTATION: The session agent below represents the Communication Manager used in the reference configuration and applies the incoming SIP manipulation "Avaya-incoming".

```
session-agent
      hostname                 10.1.2.90
      ip-address               10.1.2.90
      port                     5063
      state                    enabled
      app-protocol             SIP
```

```
app-type
transport-method               StaticTCP
realm-id                       INTERNAL
egress-realm-id
description                    Avaya_Aura_CM6
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                  30
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
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@console
last-modified-date             2010-06-17 12:56:31
```

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".

Note: The Skype Connect SBC FQDNs/IPs may differ per Skype Connect profile. Please check Skype Manager for appropriate entries (See section 5.3.2).

```
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               401,407,486
      last-modified-by               admin@console
      last-modified-date             2010-06-22 18:46:46
```

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 SD 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                       Public
      registrar-domain               *
      registrar-host                 *
      registrar-port                 5060
      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             2010-06-25 18:44:36
```

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                        12.184.9.188
            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@console
        last-modified-date            2010-06-22 18:48:04
```

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

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

```
description
sip-port
      address                        172.28.43.65
      port                           5060
      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             2010-06-17 02:37:42
```

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

1) Insert Skype Connect User Name in From Header for outbound calls from Avaya CPE to Skype Connect. Also used to match surrogate user required for Proxy-authentication.
2) Insert Skype Connect domain in From Header for outbound calls from Avaya CPE to Skype Connect. Also used to match surrogate user required for Proxy-authentication.

```
sip-manipulation
      name                           Avaya-incoming
      description                    Insert Skype username 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                      99051000003759
            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@console
            last-modified-date          2010-07-09 19:14:18
```

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

```
steering-pool
      ip-address                    12.184.9.188
      start-port                    49152
      end-port                      65535
      realm-id                      EXTERNAL
      network-interface
      last-modified-by              admin@console
      last-modified-date            2010-06-16 15:58:07
steering-pool
      ip-address                    172.28.43.65
      start-port                    2048
      end-port                      65535
      realm-id                      INTERNAL
      network-interface
      last-modified-by              admin@console
      last-modified-date            2010-06-16 15:59:20
```

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 5.3.1.** Note that the values for **register-user**, **register-contact-user**, **auth-user**, and **password** are assigned by Skype and are displayed on the Authentication details page as shown in **Section 5.3.1.**

```
surrogate-agent
        register-host                 sip.skype.com
        register-user                 99051000003759
        state                         enabled
        realm-id                      INTERNAL
        description                   Skype Connect registration
        customer-host
        customer-next-hop             SAG:SKYPE_GROUP
        register-contact-host         12.184.9.188
        register-contact-user         99051000003759
        password                      ***************
        register-expires              240
        replace-contact               disabled
        route-to-registrar            enabled
        aor-count                     1
        auth-user                     99051000003759
        max-register-attempts         3
        register-retry-time           300
        count-start                   1
        last-modified-by              admin@console
        last-modified-date            2010-06-28 14:16:57
```

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

```
system-config
      hostname
      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               NOTICE
      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                      disabled
      internal-trace                  disabled
      log-filter                      all
      default-gateway                 0.0.0.0
      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@console
      last-modified-date              2010-06-21 17:16:25
```

5. Skype Connect

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

Note: While the Skype Manager screenshots in these Application Notes show the name of the SIP trunking service as "Skype for SIP", Skype will be updating the name to "Skype Connect".

5.1. 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 3.6.1**.
    - **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.

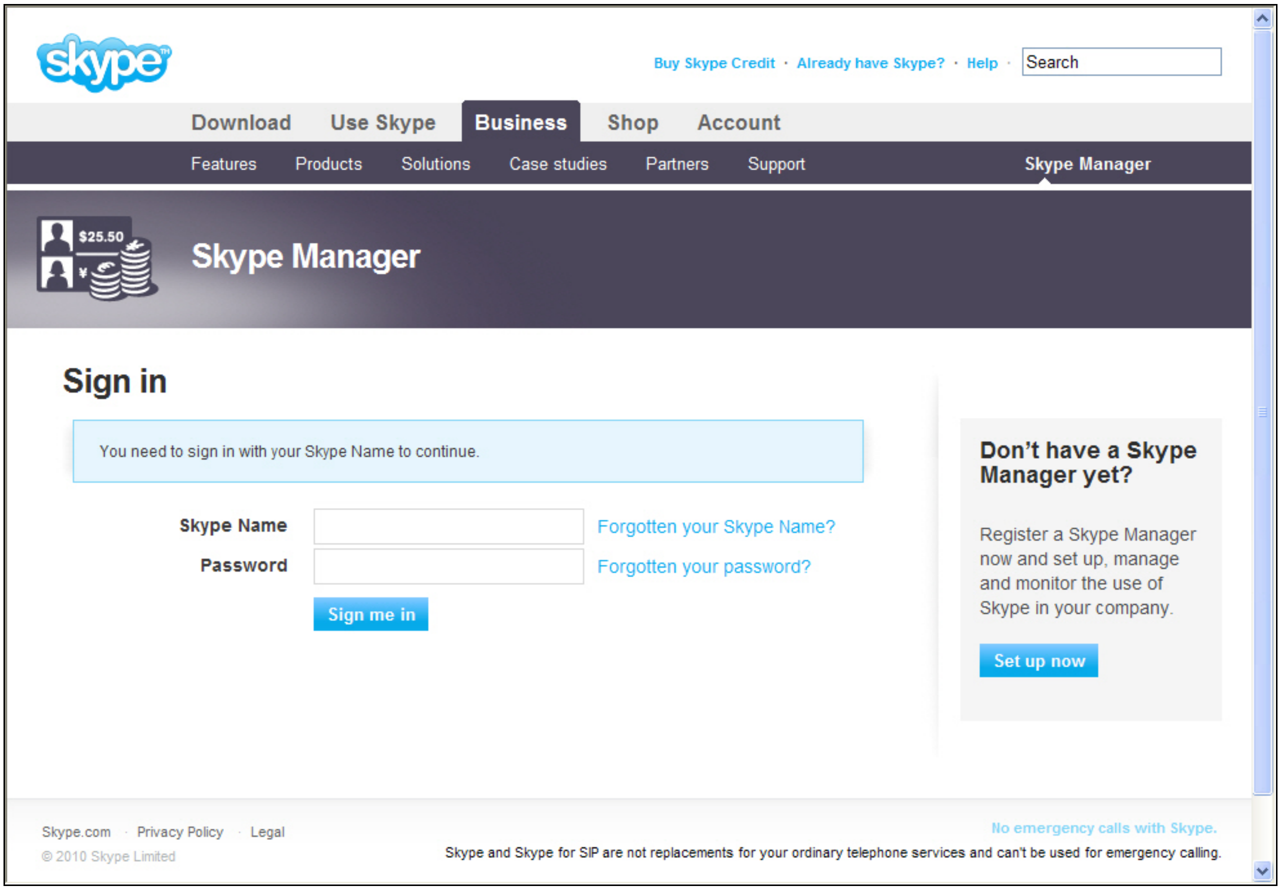

Figure 59: Skype Manager Sign In Screen

5.2. 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. Profile 1). See **Figure 62**.
4. **Section 5.3** provides details on how to setup **SIP Authentication**.

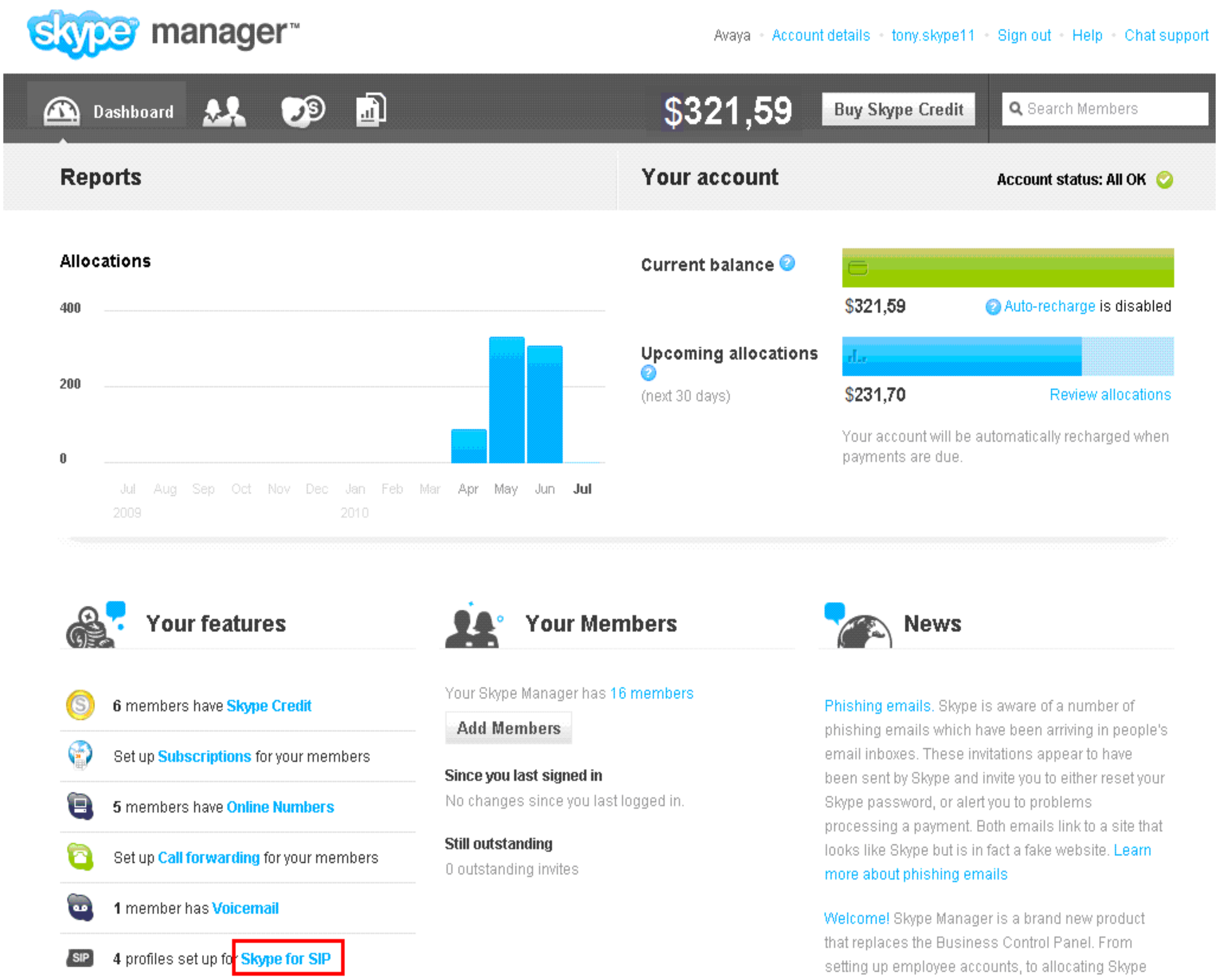

Figure 60: Skype Manager Dashboard Screen

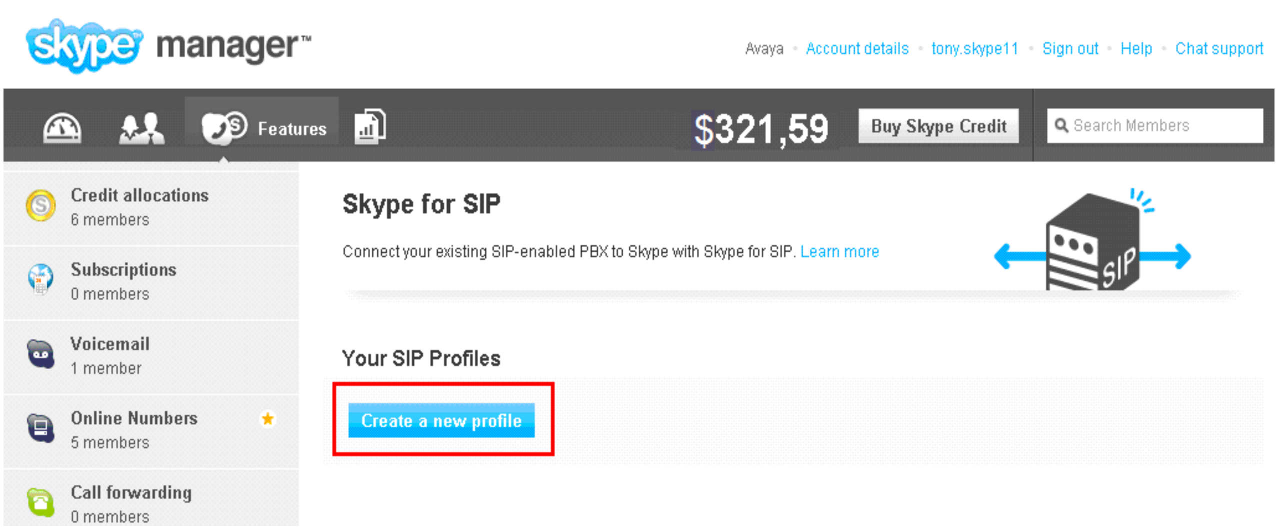

Figure 61: Create a new profile

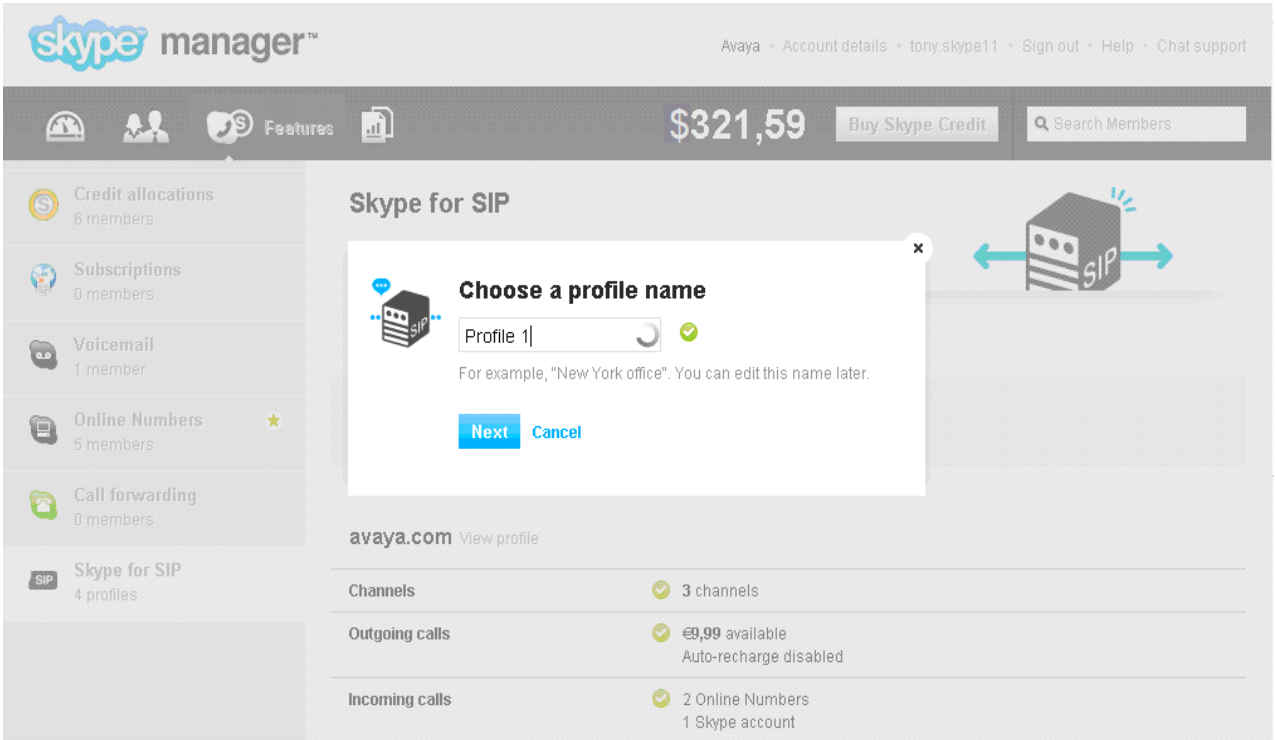

Figure 62: New Profile Name

5.3. Skype Connect Authentication Details

The Skype Connect "formerly known as Skype for SIP" service supports two methods of authentication: Registration or IP Authentication. Only one method may be selected per profile.

5.3.1 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 4.3.**

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 4.3 – Surrogate Registration section**)
    b. Password (**password** in **Section 4.3 – Surrogate Registration section**)
    c. Skype for SIP address (**register-host** in **Section 4.3 – Surrogate Registration section**)
    d. UDP Port (**port** for **EXTERNAL Session-Agents** in **Section 4.3**)

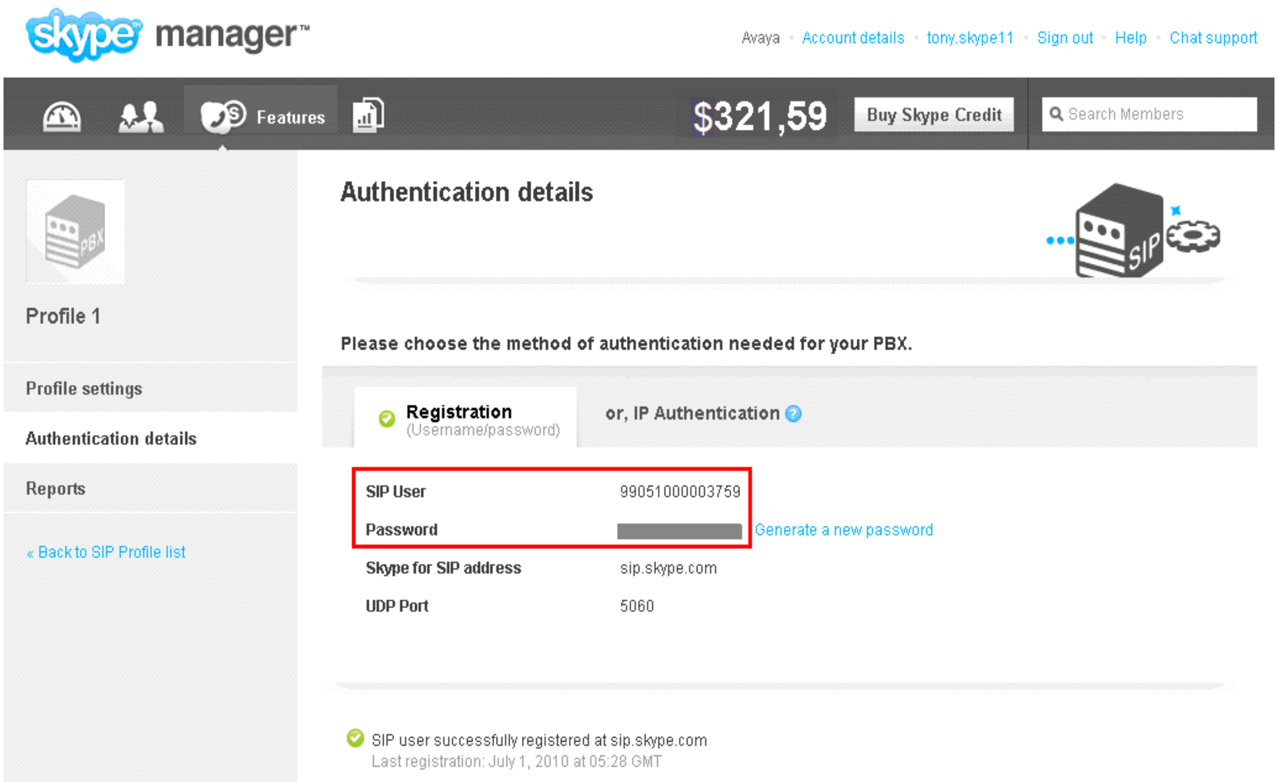

Figure 63: Registration Method

5.3.2 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 4.3** 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 → 12.184.9.188**
    b. **UDP Port → 5060** (**port** for **EXTERNAL SIP Interface** in **Section 4.3**)

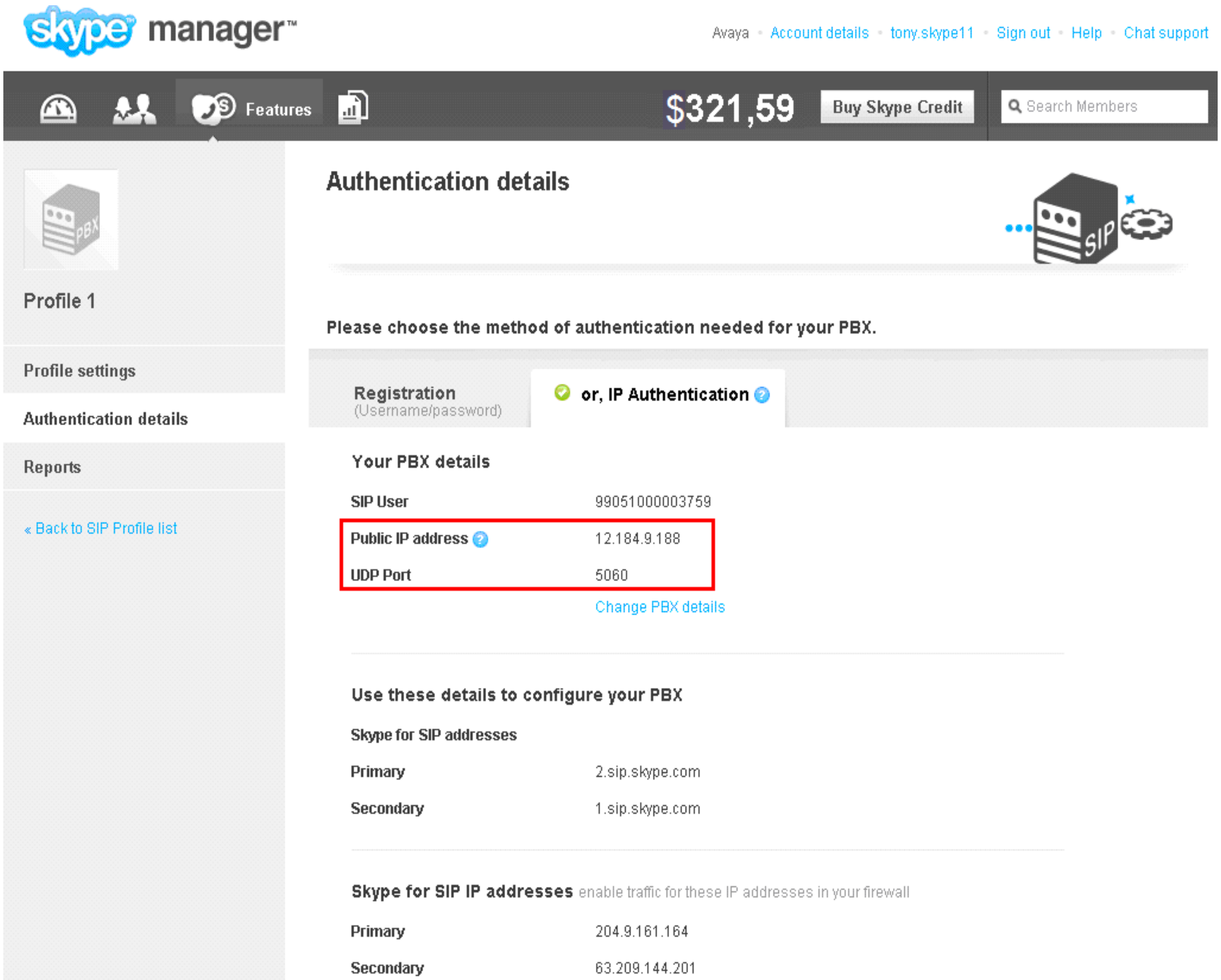

Figure 64: IP Authentication Method

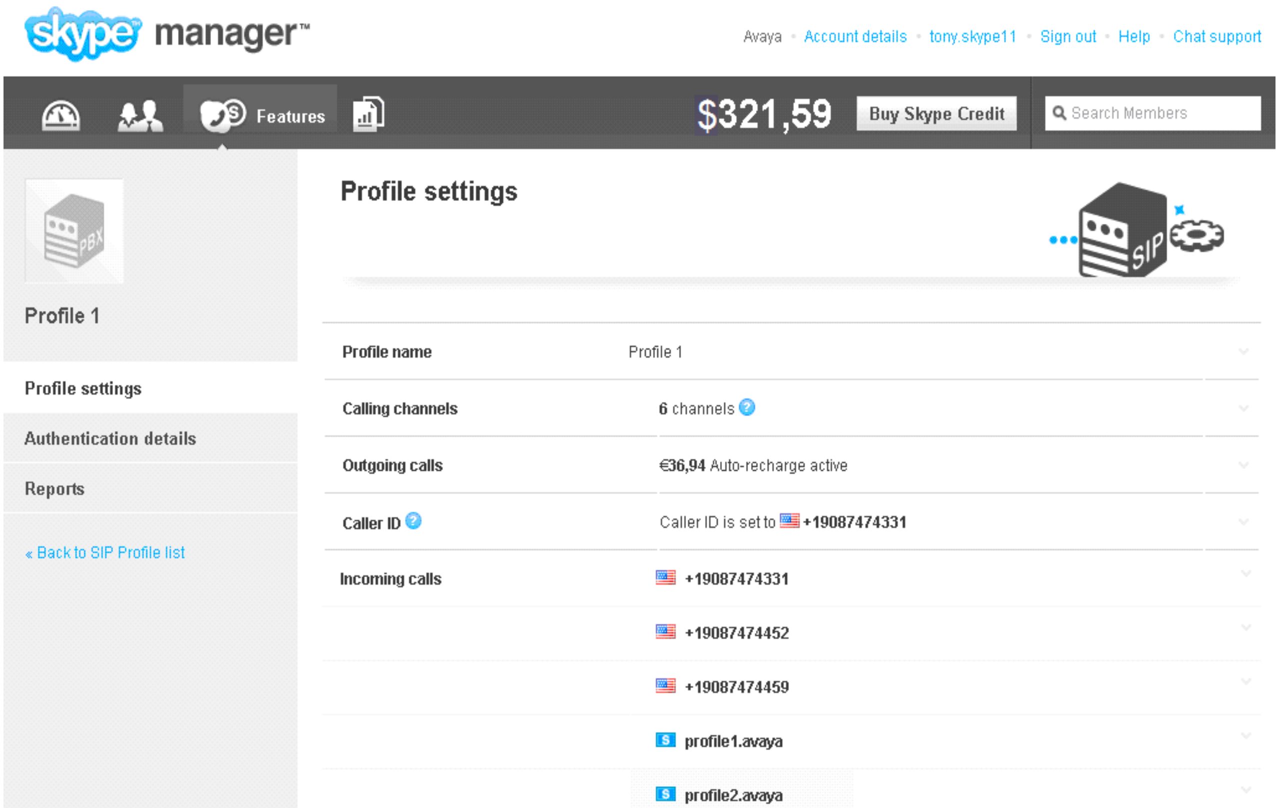

Figure 65: Profile Settings

5.4. 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.

5.5. 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.

5.6. 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 "19087474331".

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. See **Section 3.9.1**.

Notes: During testing, an incoming PSTN call to an Avaya Aura™ Communication Manager extension configured to forward calls off-net to another PSTN number displayed the Skype Connect profile default caller ID on the forwarded-to telephone. The display on the calling party PSTN phone did not get updated after the call-forward was complete.

Likewise, an Incoming PSTN call to an Avaya Aura™ Communication Manager extension that is transferred off-net to another PSTN number displayed the originally dialed Skype Connect online number on the transferred-to telephone. The display on the calling party PSTN phone did not get updated after the transfer was complete.

5.7. 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 3.8.2** describes how Avaya Aura™ Communication Manager routes calls from Skype Connect and converts the online numbers to Avaya Aura™ Communication Manager extensions.

5.7.1 Incoming calls – Skype Business Account

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 "formerly know as Skype for SIP" profile's User Agent. As shown in **Figure 66**, a Skype P2P call to "profile2.avaya" is mapped to extension 34504, and 34504 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.

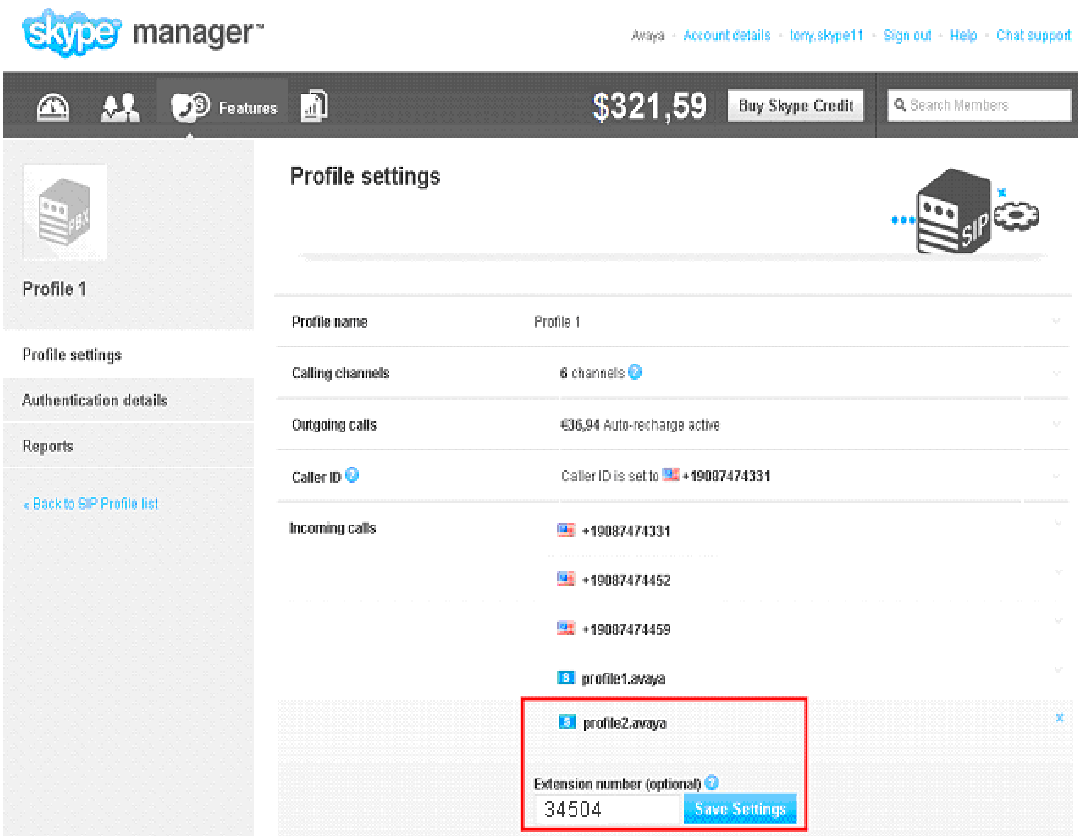

Figure 66: Skype Business Account to Extension Number Mapping

5.8. 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**.

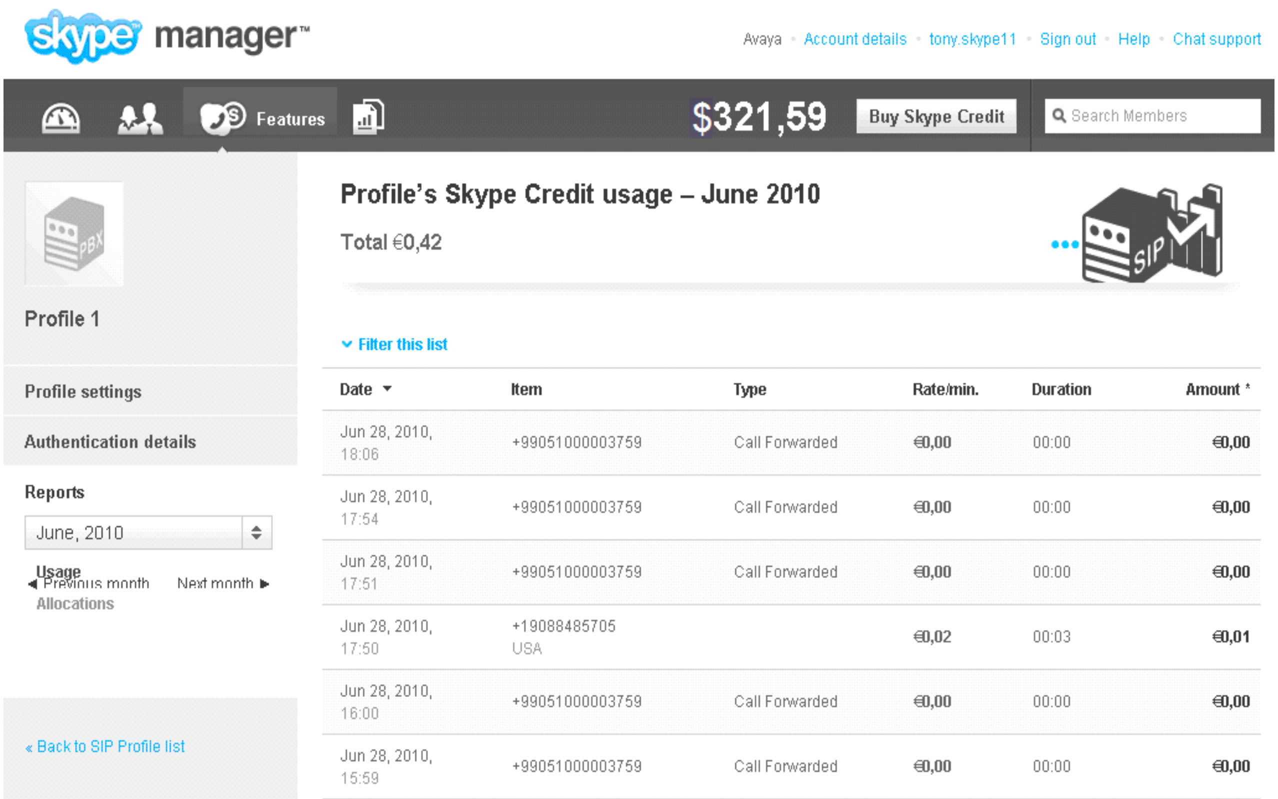

Figure 67: Skype Credit Usage Report

6. 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.

6.1. Verify Acme Packet Net-Net Session Director SBC

Verify the status of the session agents "SIP trunks" to Avaya Aura™ Communication Manager and the Skype Connect service using the "show sipd agents" command. Verify that all session agents are in the "I" state as shown below. The letter "I" indicates the session agents are in service.

```
3800-AV# show sipd agents
01:48:55-39 (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
10.1.2.90         I     0   0.0      0       0   0.0      0  0.003  0.003     0
2.sip.skype.com   I     0   0.0      0       0   0.0      0  0.000  0.000     0
```

Figure 68: Session Agent Status

6.2. Verify Avaya Aura™ Communication Manager

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 3.6.1**. Verify that all trunks are in the "in-service/idle" state as shown below.

```
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 69: 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 3.6.1**. 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 70: 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 S8800 server IP interface and Acme Packet SBC 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: T00085             Maintenance Busy? no
  Signaling Group ID: 68

    IGAR Connection? no

     Connected Ports: S00001
```

Figure 71: Status Trunk – Active Call – Page 1

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

Near-end Signaling Loc: 01A0017
  Signaling   IP Address                                   Port
   Near-end:  10.1.2.90                                  : 5063
    Far-end:  172.28.43.65                               : 5060
 H.245 Near:
  H.245 Far:
   H.245 Signaling Loc:           H.245 Tunneled in Q.931? no

 Audio Connection Type: ip-direct     Authentication Type: None
    Near-end Audio Loc:                        Codec Type: G.729
   Audio      IP Address                                   Port
   Near-end:  172.28.43.105                              : 2112
    Far-end:  172.28.43.65                               : 2060

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

Figure 72: Status Trunk – Active Call – Page 2

6.3. Verification Call Scenarios

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

- Inbound and outbound basic voice calls between various telephones on the Avaya Aura™ Communication Manager and PSTN can be made in both directions using G.711MU and/or G.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 IP 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

6.4. Conclusion

As illustrated in these Application Notes, Avaya Aura™ Communication Manager 6.0 and Acme Packet Net-Net Session Director 6.2.0 Session Border Controllers can be configured to interoperate successfully with the Skype Connect service via a SIP trunk.

7. Technical Support

Avaya

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

Skype

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

8. References

8.1. 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, June 2010.

[3] *Feature Description and Implementation for Avaya Communication Manager*, *555-245-205, Release 6.0, Issue 8.0, June 2010*

8.2. Skype Connect

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

[4] *Skype Connect Product Datasheet, Version 9.7*

8.3. Acme Packet

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

[5] *Net-Net® 4000, ACLI Reference Guide, Release Version S-C6.2.0*

[6] *Net-Net® 4000 ACLI, Configuration Guide, Release Version S-C6.2.0*

9. APPENDIX A – Inbound INVITE – From Skype to Avaya

```
INVITE sip:19087474452@12.184.9.188:5060;transport=udp SIP/2.0
From: <sip:19088485705@sip.skype.com>;tag=a4a109cc-13c4-4c2ca4fc-5890d55-
5882cec8
To: <sip:19087474452@sip.skype.com>
Call-ID: CXC-57-65ec20f0-a4a109cc-13c4-4c2ca4fc-5890d55-51cd48ba
CSeq: 1 INVITE
Via: SIP/2.0/UDP 204.9.161.164:5060;branch=z9hG4bK-5ebb-4c2ca4fc-5890d55-
41632b61
Max-Forwards: 30
User-Agent: sipgw-1.0
Allow: INVITE,ACK,CANCEL,OPTIONS,BYE
Contact: <sip:19088485705@204.9.161.164:5060;transport=udp>
Content-Type: application/sdp
Content-Length: 265

v=0
o=19088485705 1277994236 1277994236 IN IP4 204.9.161.164
s=Skype call
c=IN IP4 204.9.161.164
t=0 0
m=audio 29820 RTP/AVP 18 0 8 101
a=rtpmap:18 G729/8000
a=rtpmap:0 PCMU/8000
a=rtpmap:8 PCMA/8000
a=rtpmap:101 telephone-event/8000
a=fmtp:18 annexb=no
```

10. APPENDIX B – Outbound INVITE with Proxy-Authorization Header (Registration) – From Avaya to Skype

```
INVITE sip: 19088485705@sip.skype.com SIP/2.0
Via: SIP/2.0/UDP 12.184.9.188:5060;branch=z9hG4bK46o55020dgj04h81f4d0
From: "Digital John"
<sip:99051000003759@sip.skype.com>;tag=8056ee9df49cdf1deb4c285b3a00
To: <sip:19088485705@sip.skype.com>
Call-ID: 8056ee9df49cdf1dfb4c285b3a00
CSeq: 2 INVITE
Max-Forwards: 70
Supported: 100rel,histinfo,join,replaces,sdp-anat,timer
Allow: INVITE,ACK,OPTIONS,BYE,CANCEL,SUBSCRIBE,NOTIFY,REFER,INFO,PRACK,PUBLISH
User-Agent: Avaya CM/R016x.00.0.345.0
Contact: <sip:99051000003759@sip.skype.com;transport=udp>
Accept-Language: en
Alert-Info: <cid:internal@sip.skype.com>;avaya-cm-alert-type=internal
History-Info: <sip:19088485705@sip.skype.com>;index=1
History-Info: "19088485705" <sip:19088485705@sip.skype.com>;index=1.1
Min-SE: 1200
P-Asserted-Identity: "Digital John" <sip:19087474452@avaya.com>
Session-Expires: 1200;refresher=uac
Content-Type: application/sdp
Content-Length: 199
Route: <sip:19088485705@2.sip.skype.com:5060;lr>
Proxy-Authorization: Digest username="99051000003759", realm="sip.skype.com",
nonce="4c37e71e00016d846c41fd74060f1ed86cc519a61ee59c3c",uri="sip:19088485705@s
ip.skype.com", response="cb66fb5b5432f9c021fcd07d05d09cc1", algorithm=MD5,auth-
params=sha1-credential

v=0
o=- 1 1 IN IP4 12.184.9.188
s=-
c=IN IP4 12.184.9.188
b=AS:64
t=0 0
m=audio 49168 RTP/AVP 18 0 101
a=rtpmap:18 G729/8000
a=fmtp:18 annexb=no
a=rtpmap:0 PCMU/8000
a=rtpmap:101 telephone-event/8000
```

11. APPENDIX C – Outbound INVITE without Proxy-Authorization Header – From Avaya to Skype

```
INVITE sip: 19088485705@sip.skype.com SIP/2.0
Via: SIP/2.0/UDP 12.184.9.188:5060;branch=z9hG4bK46o55020dgj04h81f4d0
From: "Digital John"
<sip:99051000003759@sip.skype.com>;tag=8056ee9df49cdf1deb4c285b3a00
To: <sip:19088485705@sip.skype.com>
Call-ID: 8056ee9df49cdf1dfb4c285b3a00
CSeq: 2 INVITE
Max-Forwards: 70
Supported: 100rel,histinfo,join,replaces,sdp-anat,timer
Allow: INVITE,ACK,OPTIONS,BYE,CANCEL,SUBSCRIBE,NOTIFY,REFER,INFO,PRACK,PUBLISH
User-Agent: Avaya CM/R016x.00.0.345.0
Contact: <sip:99051000003759@sip.skype.com;transport=udp>
Accept-Language: en
Alert-Info: <cid:internal@sip.skype.com>;avaya-cm-alert-type=internal
History-Info: <sip:19088485705@sip.skype.com>;index=1
History-Info: "19088485705" <sip:19088485705@sip.skype.com>;index=1.1
Min-SE: 1200
P-Asserted-Identity: "Digital John" <sip:19087474452@avaya.com>
Session-Expires: 1200;refresher=uac
Content-Type: application/sdp
Content-Length: 199
Route: <sip:19088485705@2.sip.skype.com:5060;lr>

v=0
o=- 1 1 IN IP4 12.184.9.188
s=-
c=IN IP4 12.184.9.188
b=AS:64
t=0 0
m=audio 49168 RTP/AVP 18 0 101
a=rtpmap:18 G729/8000
a=fmtp:18 annexb=no
a=rtpmap:0 PCMU/8000
a=rtpmap:101 telephone-event/8000
```

12. APPENDIX D: 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