Avaya Solution & Interoperability Test Lab

Application Notes for Avaya Aura™ Communication Manager 5.2.1 and Avaya Aura™ SIP Enablement Services 5.2.1 Integration with Skype Connect 2.0 – Issue 1.0

Abstract

These Application Notes describe the steps to configure the Avaya Aura™ SIP trunk solution with Skype Connect 2.0. The Avaya SIP trunk architecture consists of Avaya Aura™ Communication Manager 5.2.1, and Avaya Aura™ SIP Enablement Services 5.2.1.

The Skype Connect 2.0 service referenced within these Application Notes is designed for business customers with an Avaya SIP trunk solution. The service provides bi-directional local and/or long distance PSTN calling via standards-based SIP trunks directly, without the need for additional TDM enterprise gateways or TDM cards and the associated maintenance costs.

Testing was conducted at the Avaya Solution & Interoperability Test Lab utilizing a traditional Internet T1 ISP circuit for accessing the Skype Connect 2.0 service directly over the Internet.

Table of Contents

1. Introduction

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

The Skype Connect service uses multiple session border controllers (also called service nodes) in the Skype network to deliver service redundancy. The Avaya SIP trunk architecture referenced in these Application Notes consists of Avaya Aura™ Communication Manager 5.2.1, and Avaya Aura™ SIP Enablement Services 5.2.1. Various Avaya H.323, Avaya SIP, digital, and analog stations are also included. While not the focus of this testing, Avaya Aura™ Communication Manager Messaging was enabled on the S8300 Server and used to provide enterprise voicemail call coverage for Avaya telephones.

In the reference configuration shown in **Figure 1,** traditional Internet access equipment are used to interface to the Skype Connect service over a broadband Internet connection. In addition, the Avaya Customer Premise Equipment (CPE) equipment is configured with public Internet IP addresses.

SIP Enablement Services is used to process all inbound and outbound SIP traffic and is implemented as a co-resident application with Communication Manager. Communication Manager SIP trunks were provisioned to terminate on SIP Enablement Services.

The Skype Connect service described in these Application Notes is designed for business customers using Avaya Aura™ Communication Manager and Avaya Aura™ SIP Enablement Services. 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 [8]**.

1.1. SIP Call Routing

For outbound calls from Avaya CPE to Skype, Domain Based Routing was configured on the SIP Enablement Services server per **Reference [1]**. Domain Based Routing relies on the SIP Enablement Services server to issue Domain Name Service (DNS) queries to a DNS server. In the reference configuration, DNS servers located on the Internet Service Provider network are used to provide a name to IP address resolution for the "sip.skype.com" domain[1]. Responses to these queries provide the call routing information (typically an IP address) for outbound call attempts.

---

[1] As of this writing, Skype Connect supports type "A" address resource records.

For inbound calls from the Skype Connect service to the Avaya CPE, Skype Connect will deliver the call to the Avaya CPE via Skype's primary or secondary SBC.

1.2. Reference Configuration

Figure 1 illustrates the reference configuration located in the Solution and Interoperability Test Lab. All of the Avaya CPE is connected to a Juniper edge router[2] that provides access to the Internet via a traditional T1 connection. This Internet connection is used for traditional Internet access as well as access to the Skype Connect service.

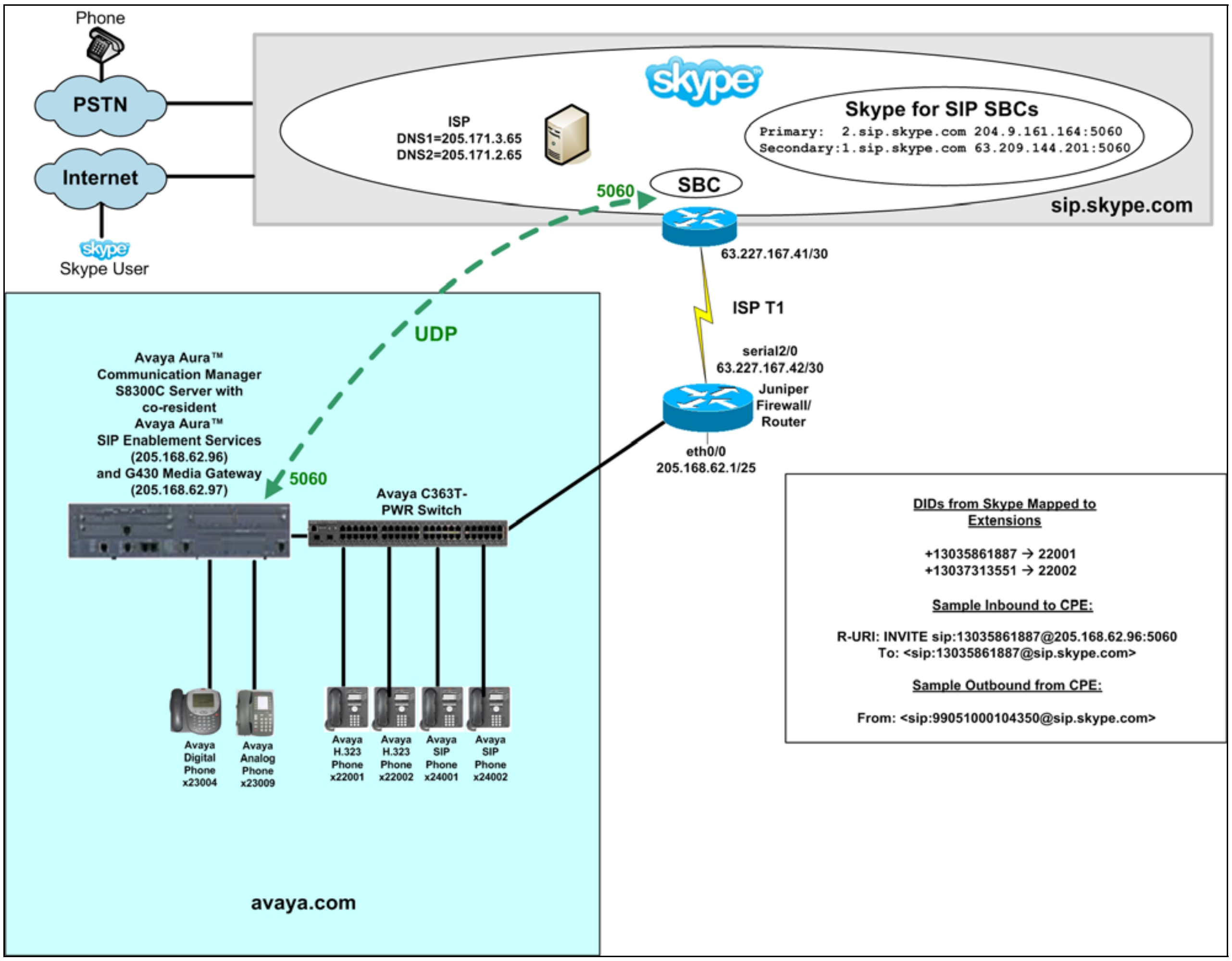

Figure 1: Reference Configuration

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

For inbound calls, Skype Online Numbers were provisioned that provided Direct Inward Dial (DID) 11 digit numbers for use during the testing. These DIDs were programmed in host maps on the SIP Enablement Services server. These host maps were used to route inbound SIP calls to Communication Manager. Communication Manager mapped the DID numbers to their associated extensions.

---

[2] The Juniper edge router also incorporates a firewall.

The Skype Connect service used a domain of *sip.skype.com.* The Avaya CPE environment was assigned a domain of *avaya.com*.

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

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

- Skype Connect domain
  - *sip.skype.com*
- Avaya CPE domain
  - *avaya.com*
- Avaya Aura™ Communication Manager
  - SIP trunk for inbound/outbound voice traffic
    - Voice
      - Signaling Group defined with Far-end Domain field specifying the Skype Connect domain
      - Signaling Group defined with Near-end Listen Port 6001
      - Trunk components assigned to IP Network Region 68
      - IP Network Region 68 specifies Skype Connect domain and IP Codec Set 5
      - IP Codec Set 5 specifies G.729
- Avaya Aura™ SIP Enablement Services
  - Route all inbound and outbound SIP calls based on SIP Request URI header information
  - Provide Domain Based Routing for outbound calls and host map based routing for inbound calls. See **Section 4.2.6.1**.
- Avaya Aura™ Communication Manager running on Avaya S8300 Server with an Avaya G430 Media Gateway
- Avaya 9600 Series IP telephones using the H.323 software bundle
- Avaya 9600 Series IP telephones using the SIP software bundle
- Avaya 2420 Digital telephones
- Analog telephones

1.2.1 Audio Codec

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

1.2.1.1 Inbound Calls to Avaya Aura™ Communication Manager

In order to accept calls from the Skype Connect domain (*sip.skype.com*), Avaya Aura™ Communication Manager will listen on port 5061 for these calls. The signaling group Near-end Listen Port is set to port 6001 and the Far-end Domain field is set to *sip.skype.com*. In addition, the Far-end Network Region associated with the Skype Connect service was set to an IP Network Region with an Authoritative Domain value of *sip.skype.com*.

1.2.1.2 Outbound Calls from Avaya Aura™ Communication Manager

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

1.2.2 Dialing Examples

The following are examples of outbound and inbound voice calls.

Given:

- Station 22001
- Inbound/Outbound SIP trunk 68

Inbound

- Voice
  - PSTN dials Skype Connect online DID number (13035861887) and the Skype Connect service sends the call to the Avaya Aura™ SIP Enablement Services server which is co-resident with Communication Manager at the Avaya CPE.
  - The SIP Enablement Services uses host maps to determine when to route the call to Avaya Aura™ Communication Manager and sends the call to Communication Manager processor (procr) Ethernet interface. Communication Manager performs digit manipulation via the INCOMING CALL HANDLING TREATMENT table associated with the incoming trunk group and changes the 11 digit DID number to the associated Communication Manager extension (22001).
  - The call arrives on inbound/outbound trunk 68 and connects to station 22001 using the G729 audio codec.

Outbound

- Voice
  - Avaya Aura™ Communication Manager voice stations first dial 9 followed by an 11 digit number (13035381762).

- ARS sends the call to Route Pattern 68. Route Pattern 68 performs digit manipulation as necessary and specifies trunk 68.
- The call will select trunk 68 and Avaya Aura™ Communication Manager sends the call via the processor Ethernet interface to Avaya Aura™ SIP Enablement Services specifying:
  - Port 5061
  - G729 audio codec
  - The Skype Connect domain
    - *sip.skype.com*
  - Skype-assigned user name as the calling party number
- SIP Enablement Services sends the call to the Skype Connect service node.

1.2.3 Local to Foreign Domain Conversion for Outbound Calls

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

<*called number*>*@ sip.skype.com*

Avaya Aura™ SIP Enablement Services forwards this URI to the Skype Connect service.

1.3. Known Limitations

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

- Skype Connect 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.
- When an Avaya telephone activates the CPN-BLK (calling party number block) feature, Communication Manager sends <sip:anonymous@anonymous.invalid> in the From: header which does not meet Skype requirements. Skype sends back 407 Proxy Authentication required and the call is blocked.
- Call-by-Call Caller ID is not supported. Outbound PSTN destinations will receive the statically assigned caller ID from the Skype profile or other Skype default caller ID (e.g. 000-123-456).
- For unanswered outbound calls from Avaya CPE to Skype, SIP Enablement Services sends a SIP CANCEL message at 30 seconds, which drops the call. See **Appendix C** for more information.
- An inbound call from Skype to Avaya CPE that routes to a telephone that has Call Forwarding active to the PSTN via Skype will not forward to the PSTN but rather go to enterprise voice mail coverage on Communication Manager, assuming that enterprise voice mail coverage has been assigned to the called telephone.

- An inbound call from Skype to Avaya CPE that is forwarded off-network from Communication Manager to the PSTN via Skype is not supported. This includes calls to a telephone that has EC500 activated and the EC500 destination is an off-network PSTN destination accessed via a Skype trunk. This also includes calls to a Vector Directory Number that are then routed to an off-network destination via a Skype trunk using the *route-to* command that is part of Communication Manager's Call Vectoring feature described in **Reference [7]**.
- Inbound anonymous calls from Skype to Avaya CPE may arrive with an IP address in the domain part of the P-Asserted-Identity header (instead of *sip.skype.com*) necessitating a separate signaling group and incoming trunk group with a blank **Far-End Domain** field on Communication Manager. This issue has been reported to Skype and is currently under investigation.
- Skype Connect is currently U.S. only. The service will be introduced in other regions at a later stage.
- Porting of existing PSTN numbers (DIDs) to Skype Connect is not supported.
- Access to a broadband Internet connection is required.
- Maximum of 300 simultaneous calls per SIP Profile. A company may have multiple SIP Profiles.
- Maximum 99 Online Numbers per SIP Profile. Sequential number block (DID) purchases will be introduced at a later stage.
- Call processing tones are locally generated by the SIP User-Agent.
- Premium-rated numbers (1-900, 1-976) are blocked.
- DNS A records are supported for Skype Connect service node name resolution, while support for DNS SRV records will be introduced by Skype Connect at a later stage.
- The SIP REFER request is not supported for call redirection/transfer.
- SIP 3xx Redirect Responses are not supported.
- SIP over TLS is not currently supported by Skype Connect.
- SRTP is not supported.
- T.38 fax is not supported.
- RTCP and RTCP XR are not supported.
- IP TOS or DiffServ QoS markings are neither set nor honored, therefore Skype Connect cannot guarantee the end-to-end voice quality. Service Level Agreements (SLAs) are not available.
- G.711A/mu-law, G.729 codecs are supported.
- E.164 International number format must be used for all calls.
- SIP Profile Address of Record (AOR) expiry timer is set to 45 seconds for SIP User-Agents registering from behind a NAT router. This capability is not part of the reference configuration in these Application Notes.
- SIP Profile AOR expiry timer is set to 300 seconds for SIP User-Agents registering directly with Skype Connect (without NAT). This capability is not part of the reference configuration in these Application Notes.
- 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 not currently support outbound SIP calls to Skype names.
- A DTMF “tone leakage” interoperability issue was occasionally observed with Skype Connect. See **Appendix A** for more information.

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

2. Equipment and Software Validated

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

Equipment	Firmware	Software
Avaya S8300 Server	-	-
Avaya Aura™ Communication Manager	-	R015x.02.1.016.4 with Service Pack 4.01 (18433)
Avaya G430 Media Gateway	FW 30.14.0 HW 1	- - -
Avaya Aura™ SIP Enablement Services	-	5.2.1 with SP3 (SES-02.1.016.4-SP3b)
Avaya Aura™ Communication Manager Messaging		N5.2.1-13.0
Avaya 9620 and 9630 H.323 Telephones	3.1.1	
Avaya 9620 and 9630 SIP Telephones	2.6 SP1	
Avaya 2420 Digital Telephones	-	-
Analog Telephones	-	-
Skype (for PC)	-	4.2.0.169
Skype Connect		2.0

Table 1: Equipment and Software Used in the Reference Configuration

Note - The solution integration validated in these Application Notes should be considered valid for deployment with Avaya Aura™ Communication Manager 5.2.1 and Avaya Aura™ SIP Enablement Services 5.2.1. Avaya agrees to provide service and support for the integration of Avaya Aura™ Communication Manager 5.2.1 and Avaya Aura™ SIP Enablement Services 5.2.1 with the Skype Connect service, in compliance with existing support agreements for Avaya Communication Manager 5.2.1 and Avaya Aura™ SIP Enablement Services 5.2.1, and in conformance with the integration guidelines as specified in the body of this document.

3. Configure Avaya Aura™ Communication Manager for SIP Trunking

This section describes the steps for configuring Avaya Aura™ Communication Manager with the necessary signaling and media characteristics for the SIP trunk connection with the Skype Connect service.

Note - The initial installation, configuration, and provisioning of the Avaya server 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 S8300 Server. Collocated with this server is an Avaya G430 Media Gateway containing DSP media processing resources. The Avaya CPE site also contained Avaya H.323, Avaya SIP, Avaya Digital and analog telephones.

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

3.1. Verify System Capacity and Features

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

1. On **Page 2** of the ***display system-parameters customer-options*** form, verify that the **Maximum Administered SIP Trunks** is sufficient for the combination of trunks to the Skype Connect service and any other SIP trunking applications. Be aware that for each call between a non-SIP endpoint at the Avaya CPE and the Skype Connect service one SIP trunk is used for the duration of the call. An Avaya SIP endpoint uses two SIP trunks 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: 100   12
           Maximum Concurrently Registered IP Stations: 450   2
             Maximum Administered Remote Office Trunks: 0     0
Maximum Concurrently Registered Remote Office Stations: 0     0
              Maximum Concurrently Registered IP eCons: 0     0
  Max Concur Registered Unauthenticated H.323 Stations: 0     0
                  Maximum Video Capable H.323 Stations: 0     0
                   Maximum Video Capable IP Softphones: 0     0
                       Maximum Administered SIP Trunks: 450   14
  Maximum Administered Ad-hoc Video Conferencing Ports: 0     0
   Maximum Number of DS1 Boards with Echo Cancellation: 0     0
                             Maximum TN2501 VAL Boards: 0     0
                     Maximum Media Gateway VAL Sources: 1     1
           Maximum TN2602 Boards with 80 VoIP Channels: 0     0
          Maximum TN2602 Boards with 320 VoIP Channels: 0     0
   Maximum Number of Expanded Meet-me Conference Ports: 0     0

        (NOTE: You must logoff & login to effect the permission changes.)
```

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

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

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

```
display system-parameters customer-options                      Page   3 of  11
                                OPTIONAL FEATURES

    Abbreviated Dialing Enhanced List? y          Audible Message Waiting? n
        Access Security Gateway (ASG)? n              Authorization Codes? n
        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? n   Cvg Of Calls Redirected Off-net? y
          ARS/AAR Dialing without FAC? y                     DCS (Basic)? n
          ASAI Link Core Capabilities? y                DCS Call Coverage? n
          ASAI Link Plus Capabilities? y               DCS with Rerouting? n
       Async. Transfer Mode (ATM) PNC? n
  Async. Transfer Mode (ATM) Trunking? n    Digital Loss Plan Modification? n
              ATM WAN Spare Processor? n                          DS1 MSP? n
                                ATMS? n            DS1 Echo Cancellation? y
                  Attendant Vectoring? n
```

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

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

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

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

           IP Attendant Consoles? n
```

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

3.1.1 Dial Plan

In the reference configuration the Avaya CPE environment uses five digit local extensions such as 22001. 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 **2**
     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
     2            5    ext
     #            3    dac
     9            1    fac
```

Figure 5: Change Dialplan Analysis Form – Page 1

3.1.2 Node Names

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

- **co-res-ses** and **205.168.62.96** are the **Name** and **IP Address** of the Avaya Aura™ SIP Enablement Services SIP signaling interface
- All other values are default

```
change node-names ip                                          Page   1 of   2
                                  IP NODE NAMES
    Name              IP Address
co-res-ses          205.168.62.96
procr               205.168.62.96
```

Figure 6: IP Node Names Form

3.1.3 IP-Network-Regions

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

Avaya Component	IP_Network-Region
Communication Manager "procr" interface	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 3.1.5**).

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

```
list ip-interface all

                                IP INTERFACES

                                                                 Net
ON Type   Slot  Code/Sfx      Node Name/       Mask  Gateway Node    Rgn  VLAN
                              IP-Address
-- ------ ----- --------      ---------------  ----  --------------- ---  ----
 y PROCR                      205.168.62.96    /25   205.168.62.1    1
```

Figure 7: IP Interface IP Network Region Assignments

The IP Network Region for an IP interface may be modified with the ***change ip-interface x*** command where **x** is the board location or procr (the procr interface is shown in the example below).

```
change ip-interface procr                                    Page   1 of   1
                                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
           Subnet Mask: /24
```

Figure 8: IP Interface IP Network Region Assignment

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

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

Table 3: Inter Region Codec Assignments

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

3.1.3.1 IP Network Region 1

IP Network Region 1 is defined for Avaya Aura™ Communication Manager telephones. The IP Network Regions are modified with the ***change ip-network-region x*** command, where x is the network region number (**Figure 9**).

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

```
change ip-network-region 1                                      Page   1 of  19
                               IP NETWORK REGION
  Region: 1
Location: 1       Authoritative Domain: avaya.com
    Name: Location 1
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: 3029
DIFFSERV/TOS PARAMETERS                  RTCP Reporting Enabled? y
 Call Control PHB Value: 46      RTCP MONITOR SERVER PARAMETERS
        Audio PHB Value: 46       Use Default Server Parameters? y
        Video PHB Value: 26
802.1P/Q PARAMETERS
 Call Control 802.1p Priority: 6
        Audio 802.1p Priority: 6
        Video 802.1p Priority: 5      AUDIO RESOURCE RESERVATION PARAMETERS
H.323 IP ENDPOINTS                                        RSVP Enabled? n
  H.323 Link Bounce Recovery? y
 Idle Traffic Interval (sec): 20
   Keep-Alive Interval (sec): 5
            Keep-Alive Count: 5
```

Figure 9: IP Network Region 1 – Page 1

2. On **Page 7** of the **IP Network Region** form:
    - Define the **Codec Set** used for inter-region communications. **Codec Set 5** is entered for communications with IP Network Region **68**.
    - Set the **direct WAN** field to **y**, indicating that devices in each region can directly communicate with each other.
    - Set the **WAN-BW-Limits** fields to **NoLimit,** indicating that the Inter Network Region Connections are not constrained by bandwidth limits.
    - Set the **IGAR** (Inter-Gateway-Alternate-Routing) field to **n** because this field is not used in the reference configuration.

```
change ip-network-region 1                                      Page   7 of  19

 Source Region: 1     Inter Network Region Connection Management     I        M
                                                                     G  A     e
 dst codec direct   WAN-BW-limits   Video      Intervening      Dyn  A  G     a
 rgn  set   WAN  Units    Total Norm  Prio Shr Regions          CAC  R  L     s
 68   5     y    NoLimit                                             n
```

Figure 10: IP Network Region 1 – Page 7

3.1.3.2 IP Network Region 68

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

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

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

 Source Region: 68    Inter Network Region Connection Management     I       M
                                                                     G  A    e
 dst codec direct   WAN-BW-limits   Video      Intervening      Dyn  A  G    a
 rgn  set   WAN  Units    Total Norm  Prio Shr Regions          CAC  R  L    s
 1    5     y    NoLimit                                             n
```

Figure 12: IP Network Region 68 – Page 3

3.1.4 IP Codec Sets

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

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

Table 4: Codec Form Codec Assignments

3.1.4.1 Intra Customer Location IP Codec Set 1

G.711MU is typically used within the same location and is often specified first. G.729 is also specified as an option. Other codecs could be specified as well depending on local requirements. IP Codec Set **1** is associated with IP Network Region **1**.

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

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

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

Figure 13: IP Codec Set 1

3.1.4.2 Trunk Calls – IP Codec Set 5

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

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

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

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

Figure 14: 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 15: IP Codec Set 5 – Page 2

3.1.5 SIP Trunk Groups

SIP trunks are defined for off network voice calls to the Skype Connect service. **Table 5** lists the SIP trunks used in the reference configuration. A SIP trunk is created in Avaya Aura™ 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

Note – In the SIP trunk configurations below (and in the Avaya Aura™ SIP Enablement Services configuration, **Section 4.2.3**), TLS was selected as the transport protocol between Communication Manager and SIP Enablement Services. UDP was used between SIP Enablement Services and Skype Connect.

3.1.5.1 Configure SIP Trunk

1. Using the ***add signaling-group 68*** command, configure the signaling group as follows:

   - Set the **Group Type** field to **sip**.
   - Set the **Transport Method** field to **tls**. Note that this specifies the transport method used between Avaya Aura™ Communication Manager and Avaya Aura™ SIP Enablement Services, not the transport method used to the Skype Connect service.
   - Specify the procr interface used for SIP signaling (node name **procr**) and Avaya Aura™ SIP Enablement Services (node name **co-res-ses**) as the two ends of the signaling group in the **Near-end Node Name** and **Far-end Node Name** fields, respectively. These field values are taken from the **IP Node Names** form shown in **Section 3.1.2**.
   - Specify **6001** and **5061** in the **Near-End** and **Far-end Listen Port** fields, respectively. Note that these values specify the TCP ports used between Avaya Aura™ Communication Manager and Avaya Aura™ SIP Enablement Services, not the ports used to the Skype Connect service.
   - Enter the value **68** into the **Far-end Network Region** field. This value is the **IP Network Region** defined in **Section 3.1.3.2**.
   - Enter *sip.skype.com* in the **Far-end Domain** field.
   - The **Direct IP-IP Audio Connections** field should be set to **y** to allow RTP voice paths to be established directly between IP telephones and the Skype border element.
   - The **DTMF over IP** field should remain set to the default value of **rtp-payload**. This value enables Avaya Aura™ Communication Manager to send DTMF tones using RFC 2833.
   - The default values for the other fields may be used.

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

 Group Number: 68             Group Type: sip
                        Transport Method: tls
  IMS Enabled? n         Co-Resident SES? y





   Near-end Node Name: procr                    Far-end Node Name: co-res-ses
 Near-end Listen Port: 6001                   Far-end Listen Port: 5061
                                           Far-end Network Region: 68
Far-end Domain: sip.skype.com

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

Figure 16: 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 **Direction:** field to **two-way**.
      - 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. **2**). This number should correspond to the number of **Calling channels** assigned in the Skype Connect Profile Settings page as described in **Section 5.4**.

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

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

                                                     Signaling Group: 68
                                                   Number of Members: 2
```

Figure 17: Public SIP Trunk Group 68 – Page 1

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

```
add trunk-group 68                                          Page   3 of  21
TRUNK FEATURES
          ACA Assignment? n            Measured: none
                                                          Maintenance Tests? y
                     Numbering Format: public
                                                UUI Treatment: service-provider
                                                 Replace Restricted Numbers? n
                                                Replace Unavailable Numbers? n
```

Figure 18: Public SIP Trunk Group 68 – Page 3

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

```
change trunk-group 68                                            Page   4 of  21
                              PROTOCOL VARIATIONS

                          Mark Users as Phone? n
                Prepend '+' to Calling Number? n
          Send Transferring Party Information? n
                     Network Call Redirection? n
                        Send Diversion Header? n
                      Support Request History? y
                 Telephone Event Payload Type: 101
```

Figure 19: Public SIP Trunk Group 68 – Page 4

3.1.6 Public Unknown Numbering – Basic Configuration

All outbound calls from Avaya CPE to Skype must have the Skype-assigned SIP User name in the From: header of the outgoing SIP INVITE. To meet this requirement, the **Numbering – Public/Unknown Format** table on Avaya Aura™ Communication Manager was used to insert the Skype-assigned SIP User name as the Calling Party Number (CPN). This CPN is used in the From: header for outbound calls[3]. 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. **2**).

- Set the **Ext Len** field to **5**.
- Set the **Ext Code** field to **2**. This is the leading digit of the extension range.
- Set the **Trk Grp(s)** field to **68.** This is the Skype trunk group number.
- Set the **CPN Prefix** field to the 14 digit Skype-assigned SIP user name**.** See **Section 5.3.2**.
- Set the **Total CPN Len** field to **14**. This is the total number of digits to be sent as the CPN.

[3] Outbound calls that do not have the Skype-assigned SIP User name in the From: header are blocked by Skype. Such would be the case if the CPN-BLK (calling party number block) feature is activated in an attempt to make an *Anonymous* outbound call.

All provisioned public-unknown-numbering entries can be displayed by entering the command ***display public-unknown-numbering 0*** as shown in **Figure 20**.

```
display public-unknown-numbering 0                             Page   1 of   2
                      NUMBERING - PUBLIC/UNKNOWN FORMAT
                                           Total
Ext Ext            Trk       CPN            CPN
Len Code           Grp(s)    Prefix         Len
                                                     Total Administered: 1
 5  2              68        99051000115591  14         Maximum Entries: 240
```

Figure 20: Numbering – Public/Unknown Format Form – Basic Configuration

3.1.7 Call Routing

3.1.7.1 Outbound Calls

The following sections describe Avaya Aura™ Communication Manager provisioning required for outbound dialing. Although Avaya Aura™ SIP Enablement Services routes all inbound and outbound SIP trunk calls, Avaya Aura™ Communication Manager uses ARS to direct outbound calls to Avaya Aura™ SIP Enablement Services. This routing is also used to determine the codec type used for these calls (see **Section 3.1.4**).

3.1.7.1.1 ARS

The Automatic Route Selection feature is used to route calls via a SIP trunk to Avaya Aura™ SIP Enablement Services, 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. Use the ***change dialplan analysis*** command to add **9** as a feature access code (**fac**).
   - Set **Dialed String** to **9**.
   - Set **Total Length** to **1**.
   - Set **Call Type** to **fac**.

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

Figure 21: Dial Plan Analysis Table

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

```
change feature-access-codes                                     Page   1 of   9
                               FEATURE ACCESS CODE (FAC)
         Abbreviated Dialing List1 Access Code:
         Abbreviated Dialing List2 Access Code:
         Abbreviated Dialing List3 Access Code:
Abbreviated Dial - Prgm Group List Access Code:
                      Announcement Access Code: *40
                       Answer Back Access Code: #16
                         Attendant Access Code:
      Auto Alternate Routing (AAR) Access Code: 8
    Auto Route Selection (ARS) - Access Code 1: 9     Access Code 2:
                 Automatic Callback Activation:        Deactivation:
Call Forwarding Activation Busy/DA: *13    All: *14    Deactivation: *15
   Call Forwarding Enhanced Status:        Act:        Deactivation:
                         Call Park Access Code: *16
                       Call Pickup Access Code:
CAS Remote Hold/Answer Hold-Unhold Access Code:
                   CDR Account Code Access Code:
                        Change COR Access Code:
                   Change Coverage Access Code:
            Conditional Call Extend Activation:        Deactivation:
                   Contact Closure   Open Code:          Close Code:
```

Figure 22: Feature Access Code Form – Page 1

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

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

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

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

Using the same procedure, specify the other called number patterns in the ARS table. **Figure 23** shows the completed ARS table.

```
display ars analysis 0                                      Page   1 of   2
                             ARS DIGIT ANALYSIS TABLE
                                   Location:  all          Percent Full:    0
          Dialed             Total     Route     Call   Node  ANI
          String            Min  Max  Pattern    Type   Num   Reqd
    1303                    11   11    68        fnpa         n
    011                     3    28    69        intl         n
```

Figure 23: ARS Digit Analysis Table

3.1.7.1.2 Route Patterns

Note - Route patterns may also be used to add or delete digits prior to sending them out the specified trunk(s). This feature was used to insert a "+1" for domestic U.S.-based outbound called party numbers or "+" for outbound international called party numbers.

1. Use the **change route-pattern** command to define the outbound SIP trunk group and digit manipulation used for U.S.-based called party numbers.
   - **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 **Inserted Digits** field to ***p1***.
     - All other values may be left at their default.

```
change route-pattern 68                                     Page   1 of   3
                  Pattern Number: 68  Pattern Name:
                          SCCAN? n     Secure SIP? n
   Grp FRL NPA Pfx Hop Toll No.  Inserted                          DCS/ IXC
   No          Mrk Lmt List Del  Digits                            QSIG
                          Dgts                                     Intw
 1: 68   0                     p1                                   n   user
```

Figure 24: Route Pattern 68 – U.S. Called Party Numbers

2. Use the **change route-pattern** command to define the outbound SIP trunk group and digit manipulation used for international called party numbers.
   - **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 entry deletes the "011" digits dialed by the user.
     - Set the **Inserted Digits** field to ***p***.
     - All other values may be left at their default.

```
change route-pattern 69                                        Page   1 of   3
                    Pattern Number: 69  Pattern Name:
                             SCCAN? n     Secure SIP? n
    Grp FRL NPA Pfx Hop Toll No.  Inserted                            DCS/ IXC
    No          Mrk Lmt List Del  Digits                              QSIG
                             Dgts                                     Intw
 1: 69   0                    3   p                                    n   user
```

Figure 25: Route Pattern 69 – International Called Party Numbers

3.1.7.2 Incoming Calls

SIP trunk group 68 is also used for inbound voice calls. In the reference configuration, the Avaya Aura™ SIP Enablement Services is used to match inbound Skype Online Numbers, also known as Direct Inward Dial (DID) numbers, and route the calls to Avaya Aura™ Communication Manager (see **Section 4.2.6.2.1**). Incoming called numbers were changed to match provisioned extensions using the Avaya Aura™ Communication Manager *change inc-call-handling-trmt trunk-group x* command, where **x** is the receiving trunk.

1. Use the **change inc-call-handling-trmt trunk-group x** command to change incoming called numbers and match them to provisioned extensions.
   - Set the **Number Len** field to ***11***.
   - Set the **Number Digits** field to a Skype Online Number. See **Section 5.7**.
   - Set the **Del** field to **11**.
   - Set the **Inserted Digits** field to an extension number, such as **22001**. Note that an entry should exist here for each Skype Online Number.
   - All other values may be left at their default.

```
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    14 99051000115591   14  22001
 public-ntwrk    11 13035861887      11  22001
 public-ntwrk    11 13037313551      11  22002
```

Figure 26: Route Pattern 68 – U.S. Called Party Numbers

3.1.8 Save Avaya Aura™ Communication Manager Provisioning

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

4. Avaya Aura™ SIP Enablement Services Provisioning

This section provides the procedures for configuring Avaya Aura™ SIP Enablement Services as provisioned in the reference configuration. In this configuration, Avaya Aura™ SIP Enablement Services runs co-resident with Avaya Aura™ Communication Manager on an Avaya S8300 Server. The Avaya S8300 Server, in turn, is inserted in an Avaya G430 Media Gateway[4]. All SIP call provisioning and system programming for SIP Enablement Services is performed via the web-based System Management Interface.

Note – The following sections assume that Avaya Aura™ Communication Manager and Avaya Aura™ SIP Enablement Services have been installed and configured for basic operations. For more information on Avaya Aura™ SIP Enablement Services see **References [5-6]**.

4.1. Network Interfaces

The Avaya S8300 Server is inserted into slot 1 of the Avaya G430 Media Gateway. **Figure 27** shows the front panel of the Avaya G430 Media Gateway.

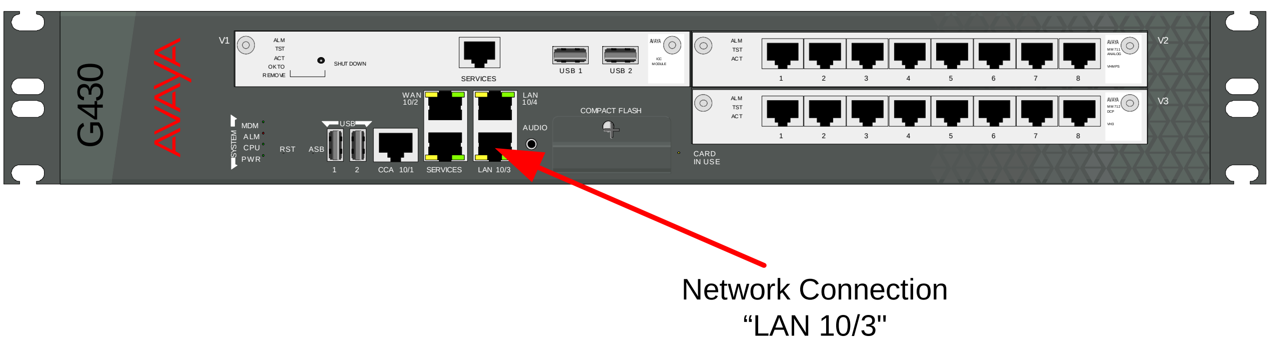

Figure 27: Avaya G430 Media Gateway Front Panel Network Connection

The Avaya G430 has multiple network interface ports. In the reference configuration, the network interface labeled “LAN 10/3” is used to connection to the SIP VoIP network. This interface is used for all inbound and outbound SIP signaling and must have network connectivity to the public Internet. This same interface also provides network connectivity for the embedded Avaya S8300 Server and the Avaya G430 Media Gateway’s internal VoIP[5] module.

4.2. SIP Enablement Services

The following provisioning is performed via SIP Enablement Services to enable SIP trunking:

- **System Properties**
  - **Host Type –** Verify host type.

---

[4] This solution is extensible to the Avaya G450 Media Gateway and other Avaya Servers using the Avaya G650 Media Gateway with a TN2602 Media Resource circuit pack. Note that co-resident SIP Enablement Services may not be supported on all Avaya Servers. In these cases, a stand-alone SIP Enablement Services server may be deployed.

[5] The IP address assigned to the G430 Media Gateway during installation is used to send and receive RTP audio streams and is separate from the IP address assigned to the S8300 Server. Both IP addresses must have access to Skype’s border element IP addresses on the public Internet.

  - **SIP Domain** - Define the SIP Domain of the SIP Enablement Services server.
- **SIP Enablement Services Host Information**
- **Communication Manager Server**
  - **Map** - Define Communication Manager Server Address Maps.
  - **Contact** – Define a destination for calls that match the associated address map.
- **Trusted Hosts**
- **Call Routing**
- **DNS Information**

4.2.1 Log in to SIP Enablement Services

With co-resident SIP Enablement Services Release 5.2.1, the URL to access the browser-based management GUI is ***https://<ip-address of Avaya S8300 Server>***. Log in with the appropriate credentials.

Figure 28: SIP Enablement Services GUI Log On Screen

After entering the appropriate credentials the window shown in **Figure 29** will open. From the **Administration** menu, select **SIP Enablement Services**.

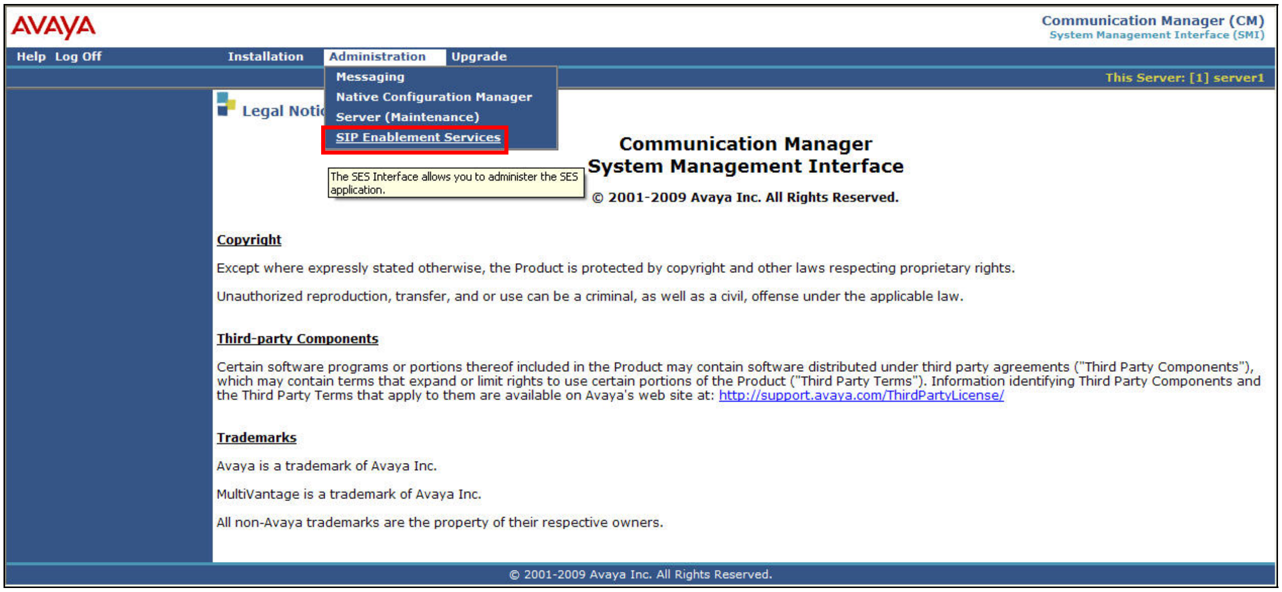

Figure 29: System Management Interface (SMI) Main Page

4.2.2 Verify System Properties

From the left pane of the **Top SIP Server Management** page, select the **Server Configuration** option and then select **System Properties**.

Figure 30: SIP Server Management Top Page

The **View System Properties** page (**Figure 31**) displays the SES Version and other system properties.

In the **View System Properties Page**:

1. Verify the SES Host Type information in the **View System Properties** page. In the reference configuration, the **Host Type** is **SES combined home-edge** (defined during installation).
2. Enter the **SIP Domain**. In the reference configuration, *avaya.com* is used.
3. Select **Update**.

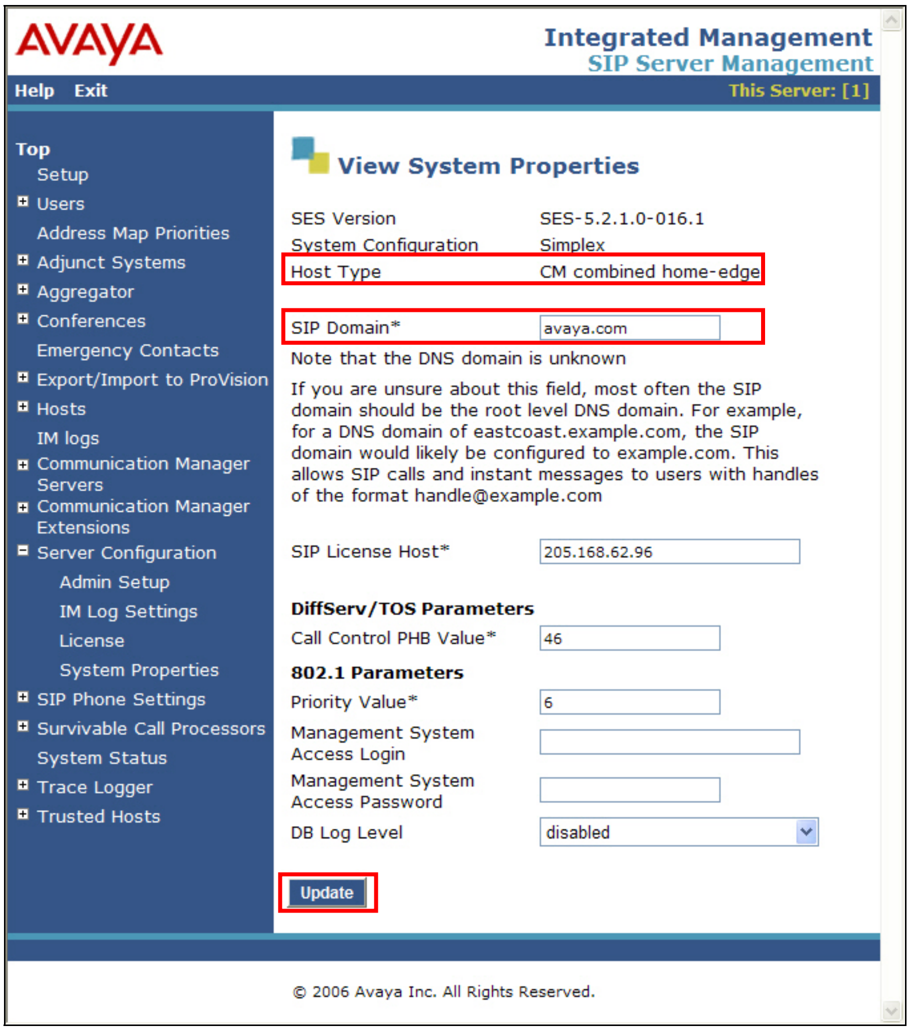

Figure 31: View System Properties

4.2.3 Verify SIP Enablement Services Host Information

Display the **Edit Host** page by following the **Hosts** link in the left navigation pane and then clicking on the **Edit** option under the **Commands** section of the **List Hosts** screen (**Figure 32**).

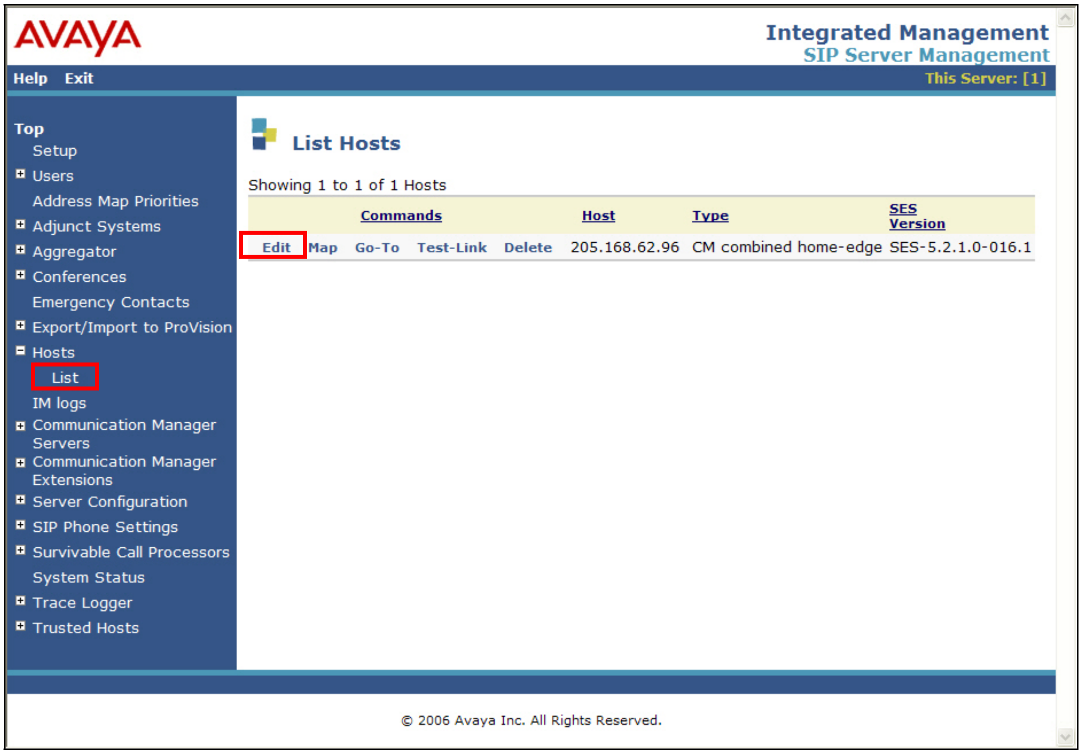

Figure 32: List Hosts

On the **Edit Host** screen (**Figure 33**):

- Verify that the IP address of this combined SES Home/Edge server is in the **Host IP Address** field (e.g, **205.168.62.96**).
- Do not modify the **Profile Service Password** fields.
- Verify that the **UDP**, **TCP** and **TLS** checkboxes are enabled as **Listen Protocols** (TCP is enabled by default).
- Verify that **TLS** is selected as the **Link Protocol**.
- Verify that the **Outbound Routing Allowed** options **Internal** and **External** are checked.
- Leave the **Outbound Proxy** and **Outbound Direct Domains** fields blank.
- Default values for the remaining fields may be used.
- Click the **Update** button only if changes are necessary. Otherwise, exit the **Edit Host** page by selecting the **Top** link on the left navigation bar.

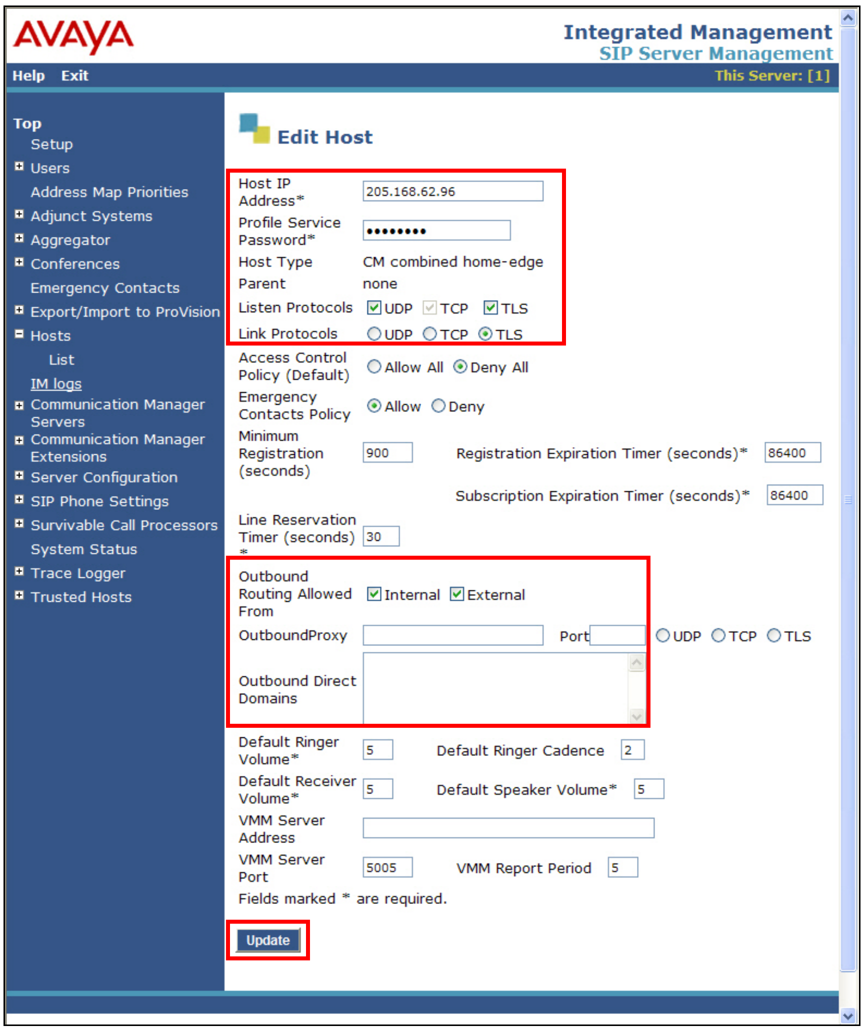

Figure 33: Edit Host

4.2.4 Communication Manager Servers

Expand the **Communication Manager Servers** option within any **SIP Server Management** page, and select **List** to display or edit the existing **Communication Manager Server** configuration (**Figure 34**).

Figure 34: List Communication Manager Servers

Figure 35 shows the **Communication Manager Server Interface** configuration, which matches the Signaling Group **68** configuration (Skype SIP trunk) on Communication Manager (see **Section 3.1.5.1**).

On the **Edit Communication Manager Server Interface** screen:

- Verify the **Communication Manager Server Interface Name**. Note that for co-resident SIP Enablement Services the name will be the IP address of Communication Manager followed by "CM".
- Verify the **Host** and **SIP Trunk IP Address** fields are set to the IP address of Communication Manager.
- Verify the **SIP Trunk Port** field is set to **6001**. This is the port number specified in the **Near-end Listen Port** specified in the Communication Manager Signaling Group form for the associated SIP Trunk.
- Click the **Update** button only if changes are necessary. Otherwise, exit the **Edit Communication Manager Server Interface** page by selecting the **Top** link on the left navigation bar.

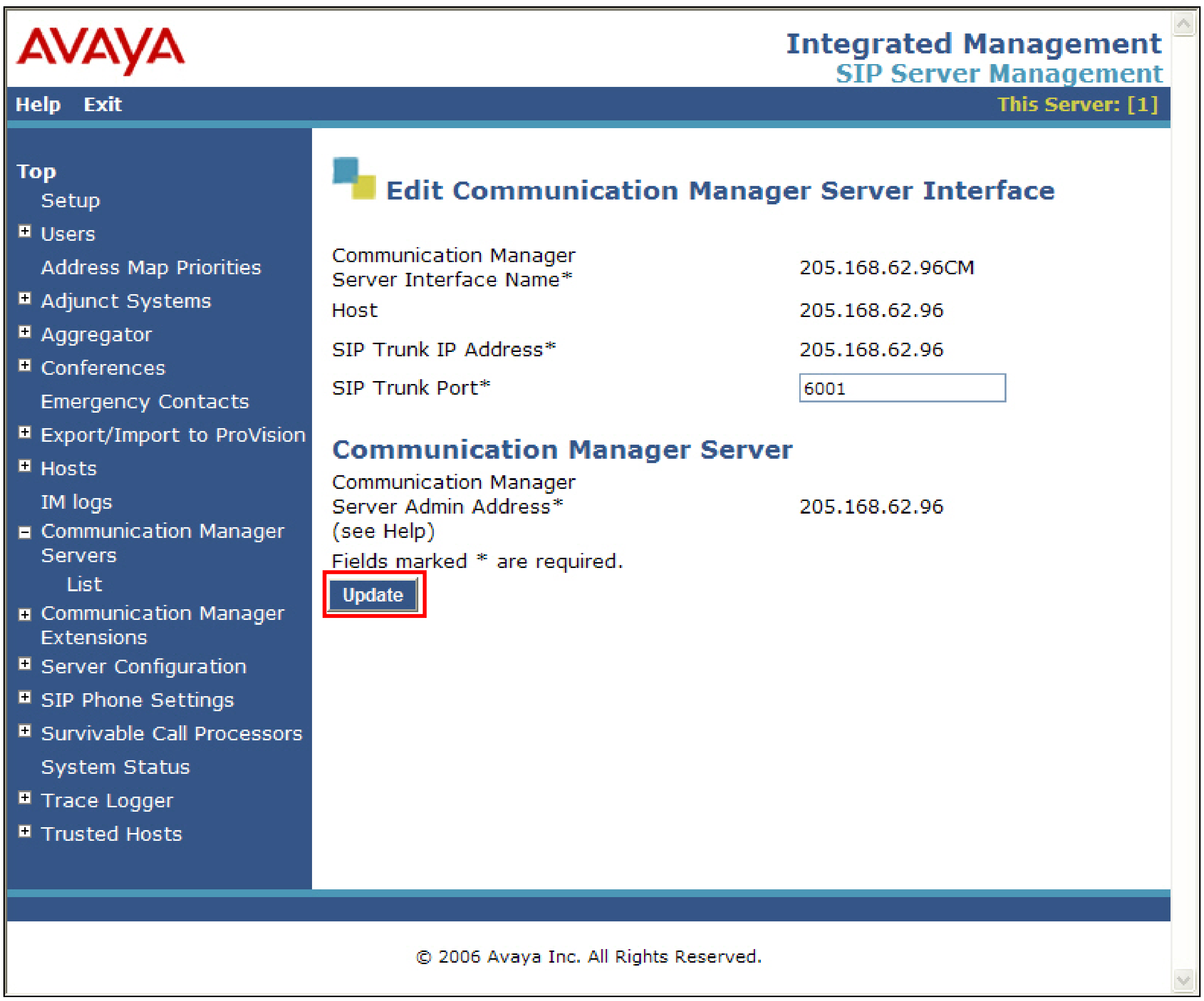

Figure 35: Communication Manager Server Interface

4.2.5 Configure Trusted Hosts

SIP Enablement Services will deny inbound calls from unknown foreign nodes. Therefore the Skype service nodes must be specified as Trusted Hosts in SIP Enablement Services.

Expand the **Trusted Hosts** option and select **Add** to add a new **Trusted Host** or select **List** to display or edit an existing **Trusted Host** configuration (**Figure 36**).

From the Avaya SIP Enablement Services "**Top**" web page, select **Trusted Hosts**.

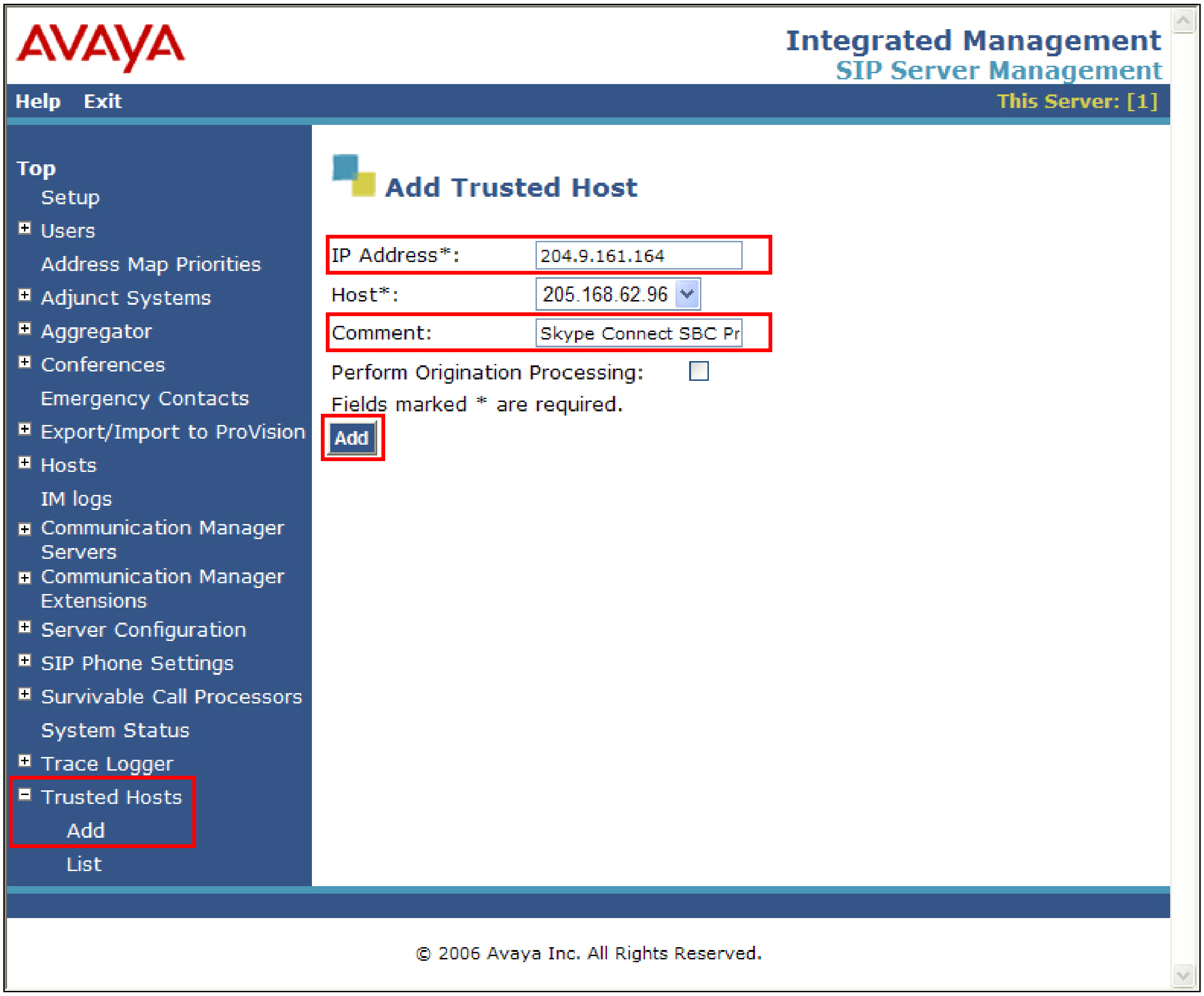

Figure 36: Add Trusted Host

On the **Add Trusted Host** screen:

- In the **IP Address** field, specify the IP address of the **Trusted Host** (e.g, **204.9.161.164**).
- In the **Comment** field, specify a description of the **Trusted Host** entry (e.g, **Skype Connect SBC Primary**).
- Verify that **Perform Origination Processing** is not checked.
- Select **Add** to save changes.
- Add another **Trusted Host** for the secondary Skype service node.

Note – A Trusted Host must be entered for each Skype service node that may send SIP messages to or receive SIP messages from the SIP Enablement Services server.

4.2.6 Configure Call Routing

The SIP Enablement Services server functions as a SIP proxy server for the SIP trunk connections to the Skype Connect service. In this role, for outbound calls the SIP Enablement Services server must direct SIP messages originating from Communication Manager to the Skype service nodes. In a similar manner for incoming DID calls, the SIP Enablement Services server must route messages received from the Skype SIP network to Communication Manager.

4.2.6.1 Domain Based Routing – Outbound Calls

Domain Based Routing is used to send outbound calls from Communication Manager to SIP Enablement Services.

Note – Domain Based Routing requires that a DNS server IP address be configured within Communication Manager. See **Section 4.2.6.3** for steps to configure the DNS server within Communication Manager. The DNS IP address used in the reference configuration points to a standard DNS server on the public Internet. In addition, the foreign Fully Qualified Domain Name (FQDN) used by Skype Connect is "sip.skype.com".

In the reference configuration Communication Manager specifies the FQDN of the Skype service nodes (***sip.skype.com***) in the **Far-End Domain** field of the outbound SIP Trunk Signaling Group (Trunk 68 in the reference configuration, see **Section 3.1.5.1**). The SIP Enablement Services server receives an INVITE from Communication Manager with the destination URL of ***<callednumber>@sip.skype.com,*** and with no Outbound Proxy specified in the SIP Enablement Services server **Edit Host** Page (see **Figure 33**), the SIP Enablement Services server will issue a DNS record query for the foreign domain. The DNS server will then return the appropriate destination IP address. The SIP Enablement Services server will then send the INVITE to the IP address provided in the DNS response.

This method of call routing for outbound calls provides increased call routing flexibility since network changes within the Skype Connect service do not require any modification to Avaya provisioning.

Note – SIP Enablement Services will use UDP port 5060 for outbound calls.

4.2.6.2 Inbound Calls

The SIP message routing for inbound calls uses **Address Maps** that examine some or all of the *called number* (matching on a defined pattern) and route to a specific predetermined destination (called a **Contact**).

The *called number* is contained within the *user* part of the Uniform Resource Identifier (URI) of an incoming SIP INVITE message. The URI usually takes the form of *sip:user@destination*, where *destination* can be the CPE (SES) FQDN or IP address. The *user* part of the URI will only contain digits in these Application Notes[6].

The **Address Map Patterns** are specified using Linux regular expression syntax. Patterns are generally designed to match a collection of *called numbers* that require identical SIP message routing. However, each Pattern must also be specific enough to direct each unique *called number* to the proper signaling Contact**.** The Address Map Patterns must also be mutually exclusive (non-overlapping) from all other Address Map Patterns used in the SIP Enablement Services server to ensure proper operation.

Appendix B provides a detailed description of the Linux regular expression syntax used within the address map patterns.

Note – Address Map provisioning is very flexible, with possibilities for either broad or narrow routing constraints. The following provisioning should be viewed as reference examples.

[6] SIP does permit mnemonic addressing such as "sip:john.doe@customer.com". However, this convention is not used for SIP trunks in these Application Notes. Further discussion of this topic is beyond the scope of this document.

4.2.6.2.1 Inbound Call Routing

Inbound calls that arrive from Skype will typically contain a Skype Online Number or possibly the Skype-assigned 14 digit SIP user name. In the reference configuration, Address Maps are provisioned for each Online Number and also for the 14 digit SIP user name. Since all inbound calls should route to the Communication Manager trunk, all Address Maps use the same Contact.

To configure the **Communication Manager Server Address Maps**:

- Expand the **Communication Manager Servers** link in the left navigation menu of any **SIP Server Management** page. Select **List** to display the **List Communication Manager Servers** page as shown in **Figure 37.**
- Click on the **Map** link to display the **List Communication Manager Server Address Map** page.

Figure 37: List Communication Manager Servers

Figure 38 shows address maps for two Skype Online Numbers and one for the Skype SIP user name.

1. **Skype Online Number Map provisioning.**
    - Click on the ***Edit*** button next to the **SKYPE13035861887** name.

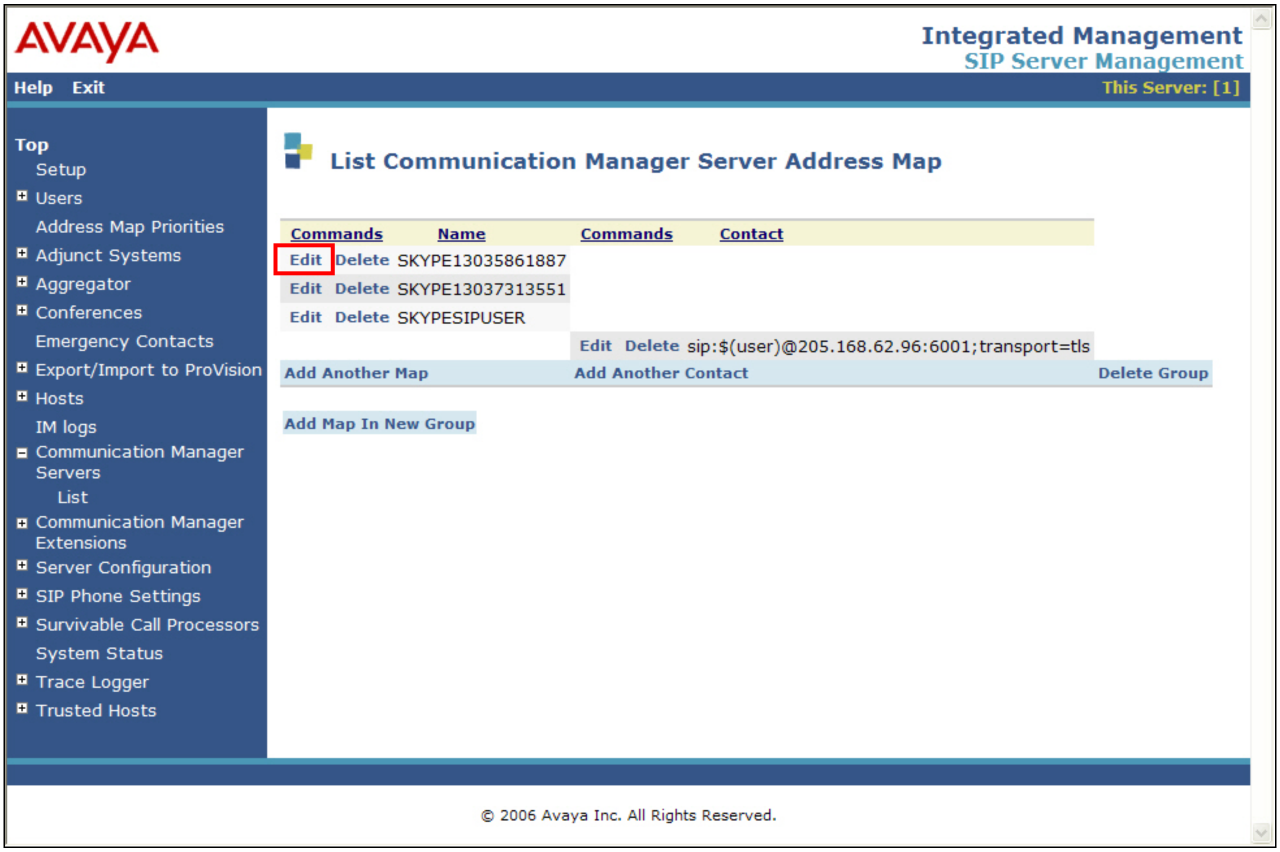

Figure 38: List Communication Manager Server Address Map

The **Edit Communication Manager Map Entry** window will open (**Figure 39**).

- Enter a name for the map. (e.g, ***SKYPE13035861887***)
- Enter the **Address Map Pattern** for incoming calls to this Skype Online Number into the **Pattern** field.
- A Map entry must be created for each Skype Online Number that can generate an inbound SIP INVITE. The entry *^sip:13035861887* means match exactly the digits 13035381887.
- Click the **Update** button once the form is completed. Then, click the **Continue** button (not shown).

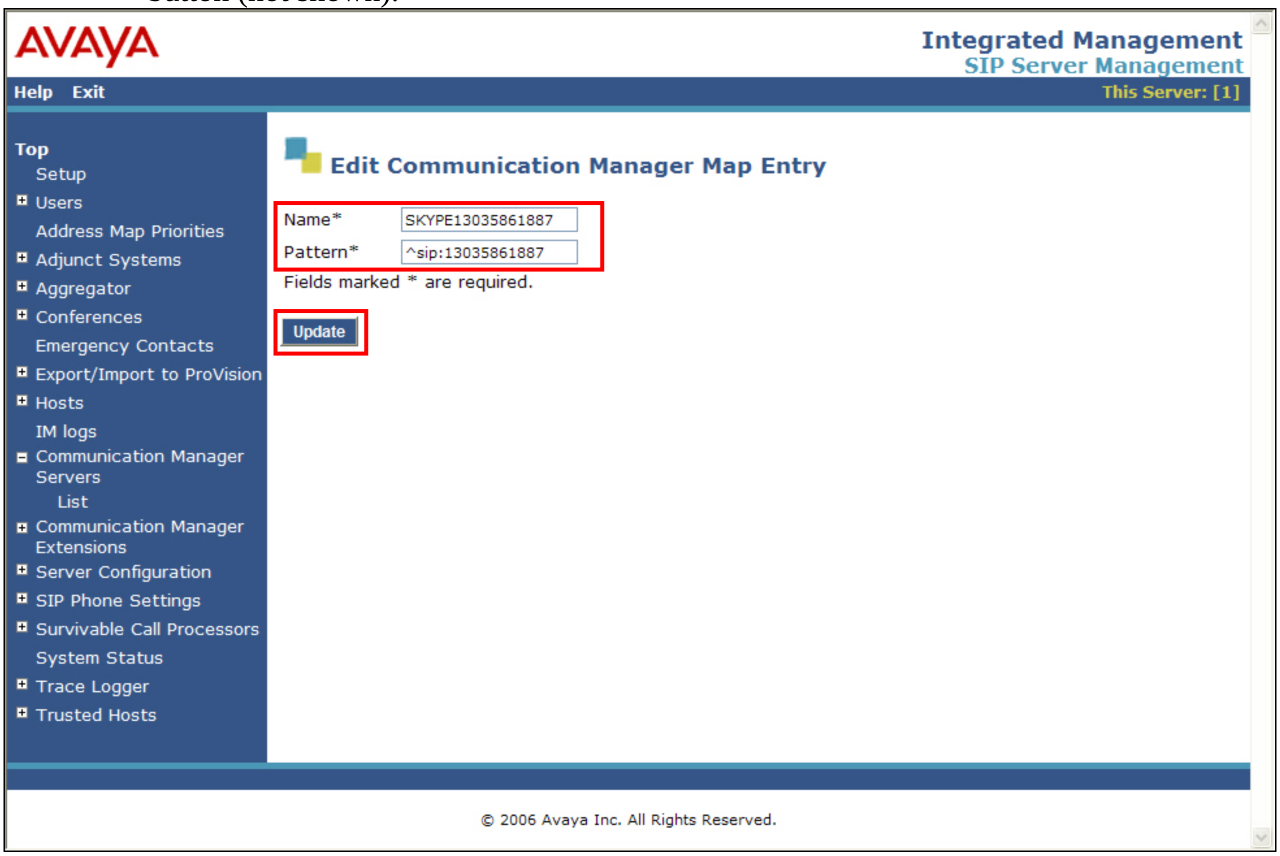

Figure 39: Skype Online Number Address Map

2. **Skype SIP User Name provisioning.**
Go back to the **List Communication Manager Server Address Map** (**Figure 37**) and click on the *Edit* button next to the **SKYPESIPUSER** name and the **Edit Communication Manager Map Entry** page will open (**Figure 40**).
    - Enter a name for the map. (e.g, ***SKYPESIPUSER***)
    - Enter the **Address Map Pattern** for incoming calls that use the Skype SIP User Name into the **Pattern** field.
    - A Map entry should be created for the Skype SIP User name. See **Section 5.7.1** for a case where Skype may deliver the Skype-assigned SIP User Name in the Request URI of the SIP INVITE. The entry ^*sip:99051000115591* means match exactly the digits 99051000115591.
    - Click the **Update** button once the form is completed. Then, click the **Continue** button (not shown).

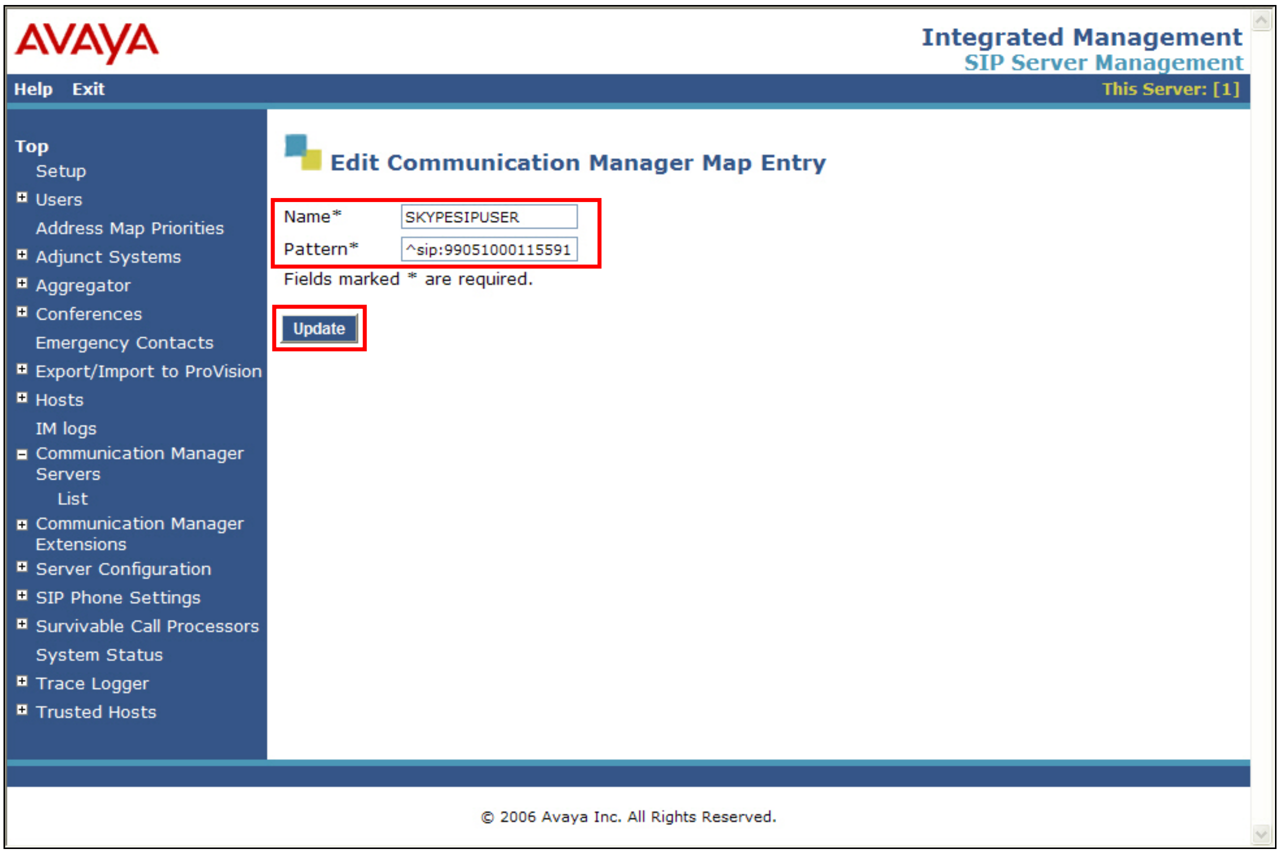

Figure 40: Skype SIP User Name Address Map

As shown in **Figure 41**, after the first **Communication Manager Address Map** is created, a corresponding media server **Contact** entry is created automatically.

sip:$(user)@205.168.62.96:6001;transport=tls

This **Contact** entry contains the IP address of the Communication Manager (procr address), the port (***6001*** is the port for TLS) and the transport protocol (***tls***) to be used. The incoming digits sent in the ***user*** part of the original request URI will replace the $(user) string when the message is sent to the **Contact**.

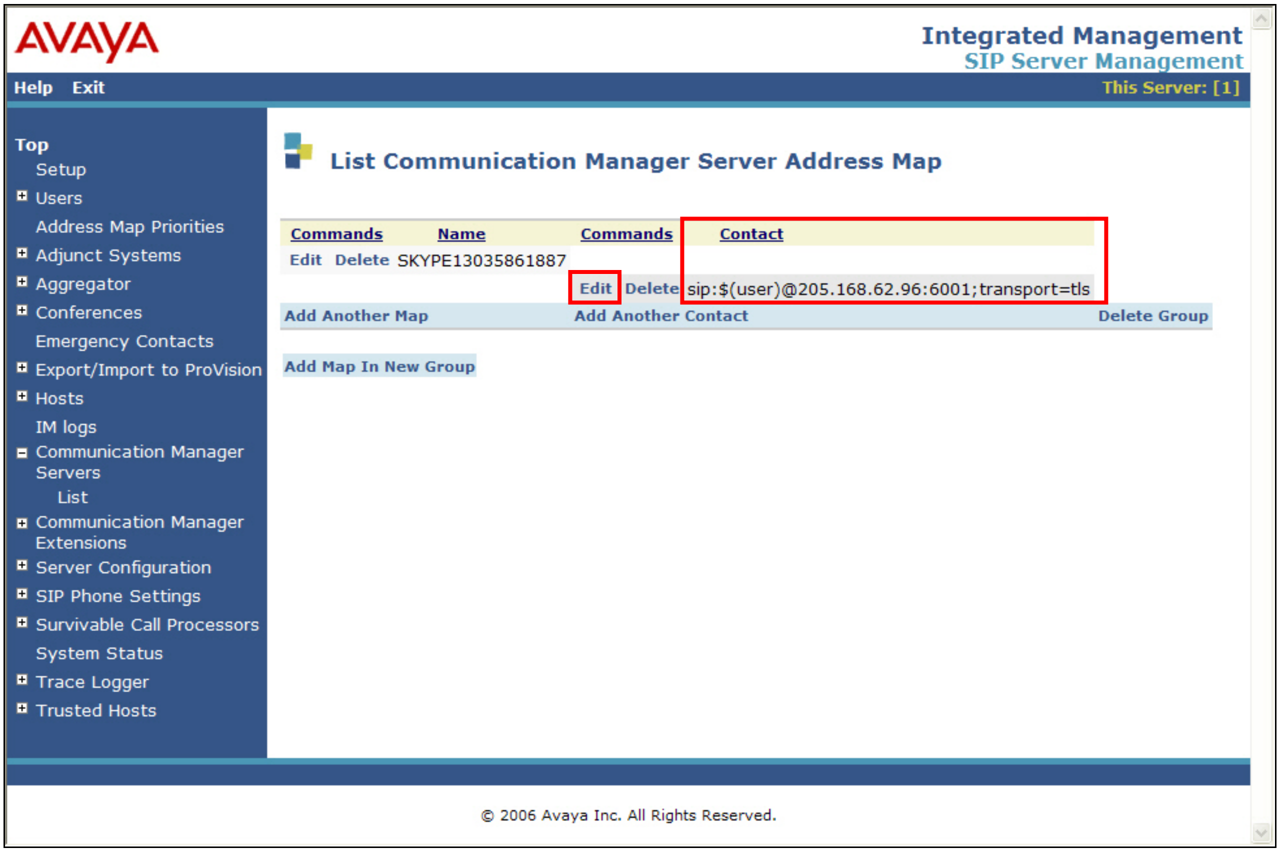

Figure 41: Communication Manager Contact

If necessary, the Contact information can be modified by clicking on the ***Edit*** button. The Edit **Communication Manager Contact** window will open (see **Figure 42**). Click the **Submit** button to submit the changes.

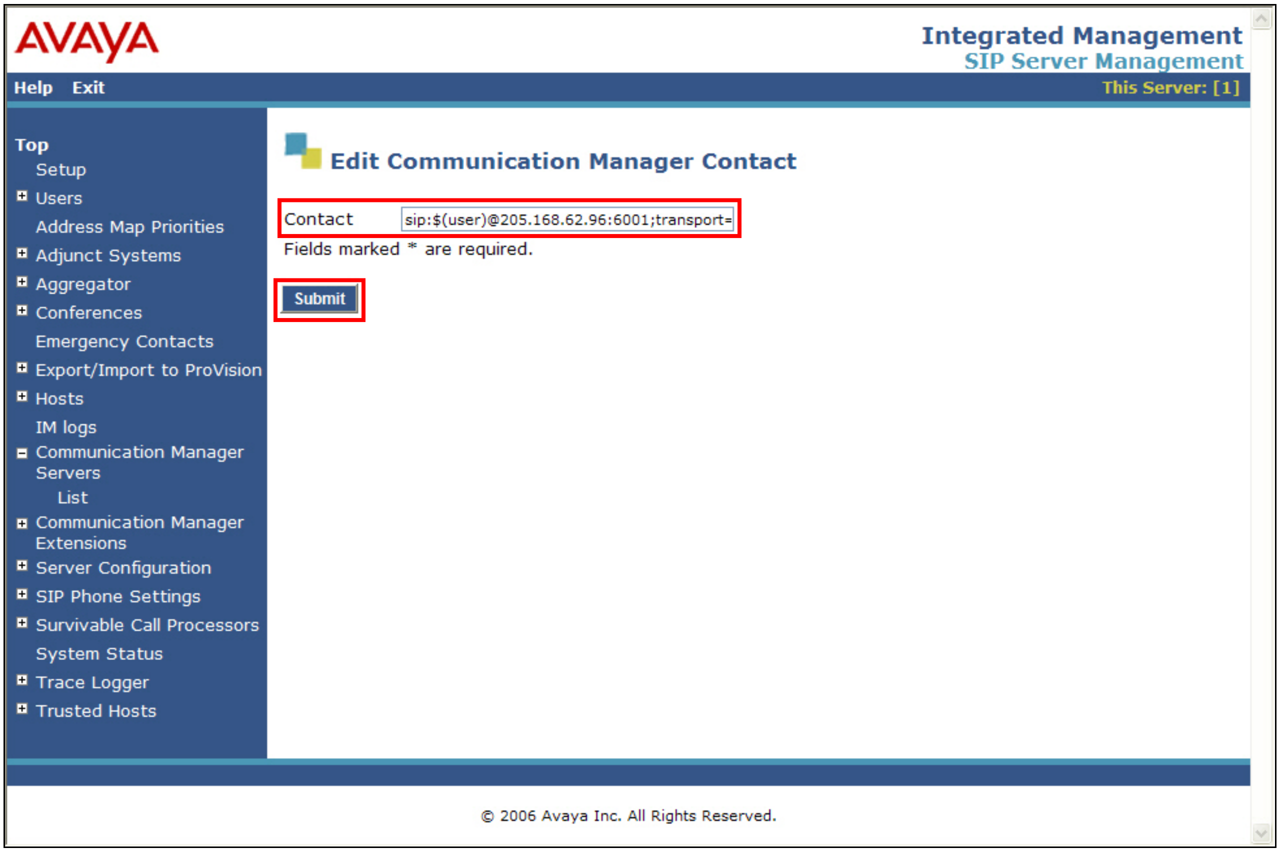

Figure 42: Edit Communication Manager Contact

4.2.6.3 Verifying/Configuring DNS Information

In the reference configuration, Communication Manager and SIP Enablement Services are co-resident on the same platform. The Communication Manager Management web interface is used to modify the DNS entry used by SIP Enablement Services.

As shown in **Section 4.2.1**, the URL to access the browser-based management GUI is ***https://<ip-address of Avaya S8300 Server>***. Log in with the appropriate credentials.

- After entering the appropriate credentials, the window shown in **Figure 43** will open. From the **Installation** menu, select **Configure Server**.

Figure 43: System Management Interface (SMI) Main Page

- After selecting **Configure Server**, a separate window will open to the **Configure Server** page (not shown). Select **Continue**.
- The **Back Up Data** page appears and provides instructions to back up current data, if necessary. Select **Continue** (not shown).
- As shown in **Figure 44**, select **Configure individual services**, and then select **Continue**.

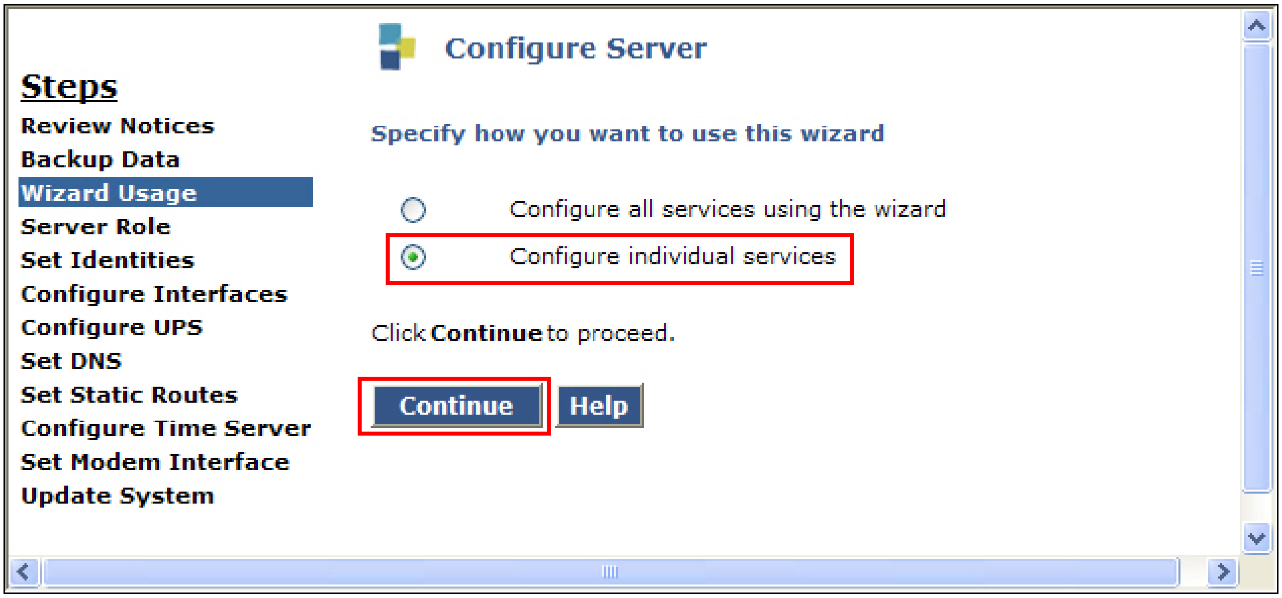

Figure 44: Configure Server

The **Configure Server Notice!** Page is presented as shown in **Figure 45**.

- Click on **Set DNS.**

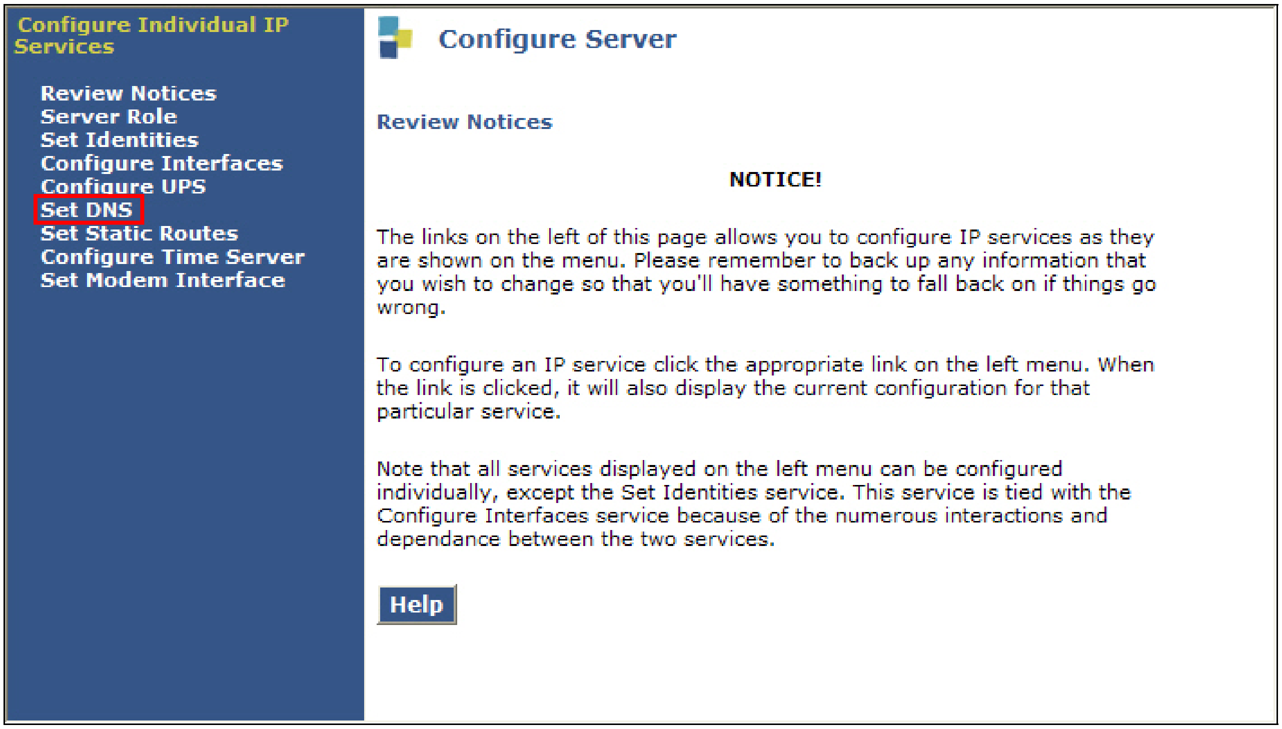

Figure 45: Configure Individual IP Services

The **Set DNS** Page is presented as shown in **Figure 46**.

- Configure the **Name Servers** fields as provided by your Internet Service Provider (ISP). In the reference configuration, two DNS servers located on the ISP network are used to provide a name to IP address resolution for the “sip.skype.com” domain.
- Select the **Change** button to save the configuration change.

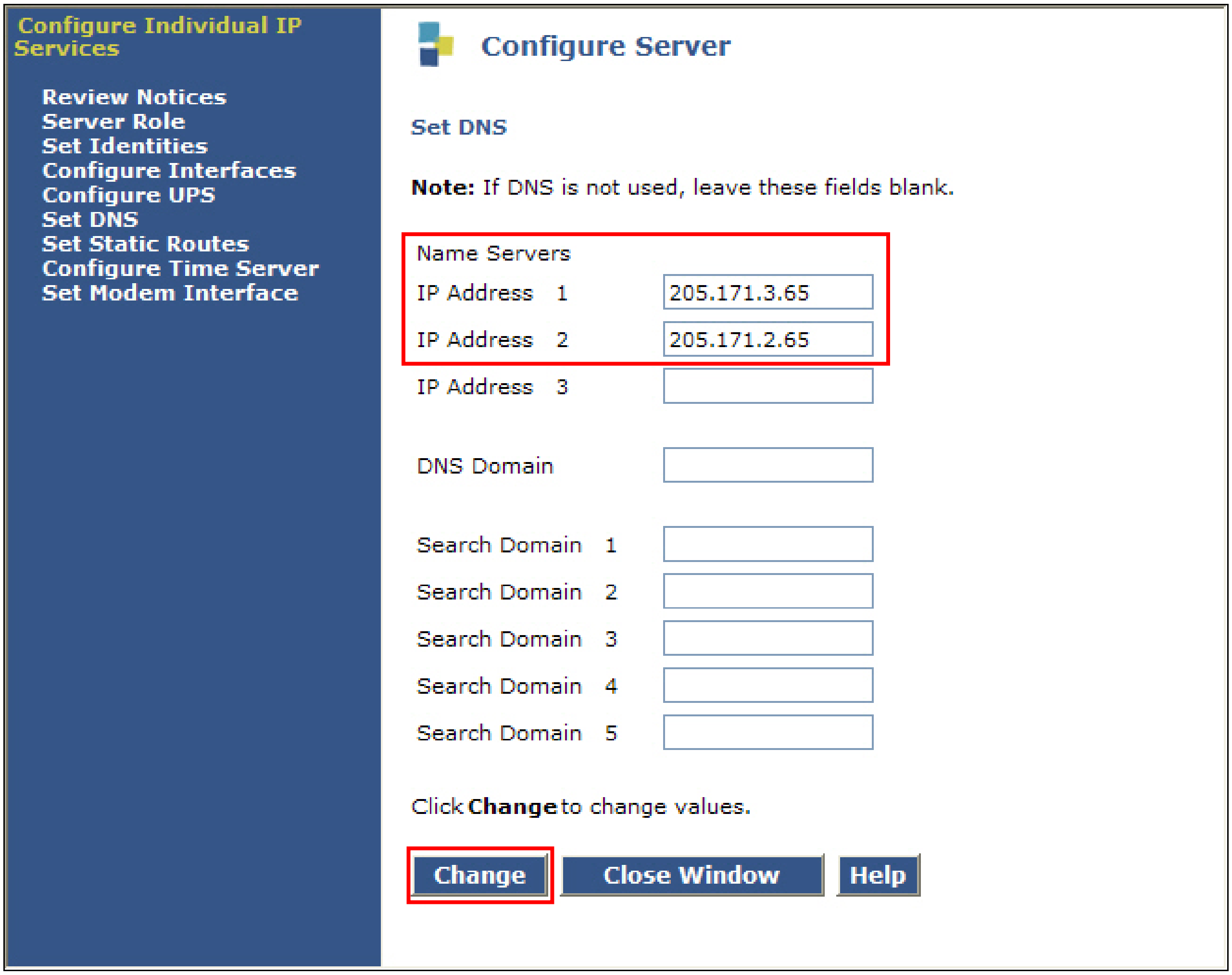

Figure 46: Set DNS

- When the changes are accepted successfully, the window shown in **Figure 47** will appear. Select the **Close Window** button. Then exit the browser session.

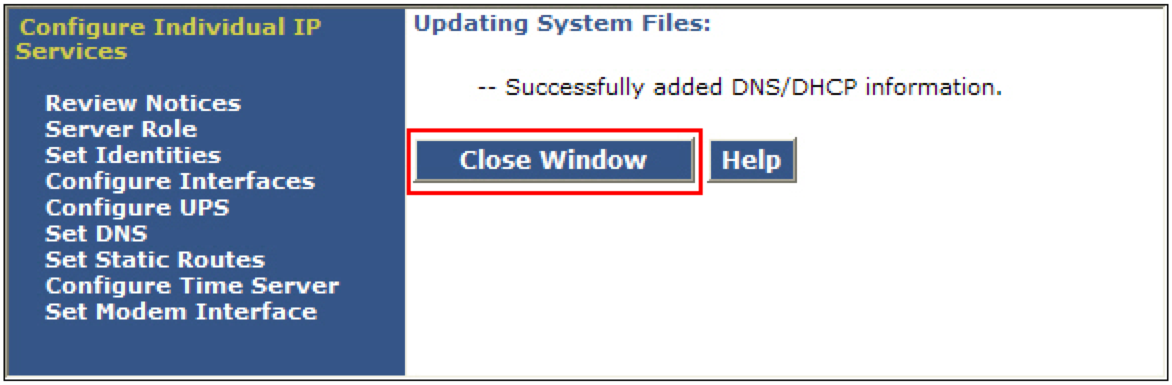

Figure 47: DNS Server Successful Update

5. Skype Connect

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

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 3.1.5.1**.
    - **Outgoing calls** – For billing purposes, define how payments will be handled.
    - **Caller ID** – Define what Caller ID should be used for outbound calls from Avaya CPE to Skype Connect.
    - **Incoming calls** – Skype Online Number and Skype Business Account definitions. This includes Skype Business Account to called party number/extension mapping.
  - **Authentication details**
    - **Registration**[7]
    - **IP Authentication**
  - **Reports**
    - **Skype Credit usage reports**

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

[7] The Registration Authentication method is not supported in the reference configuration documented in these Application Notes.

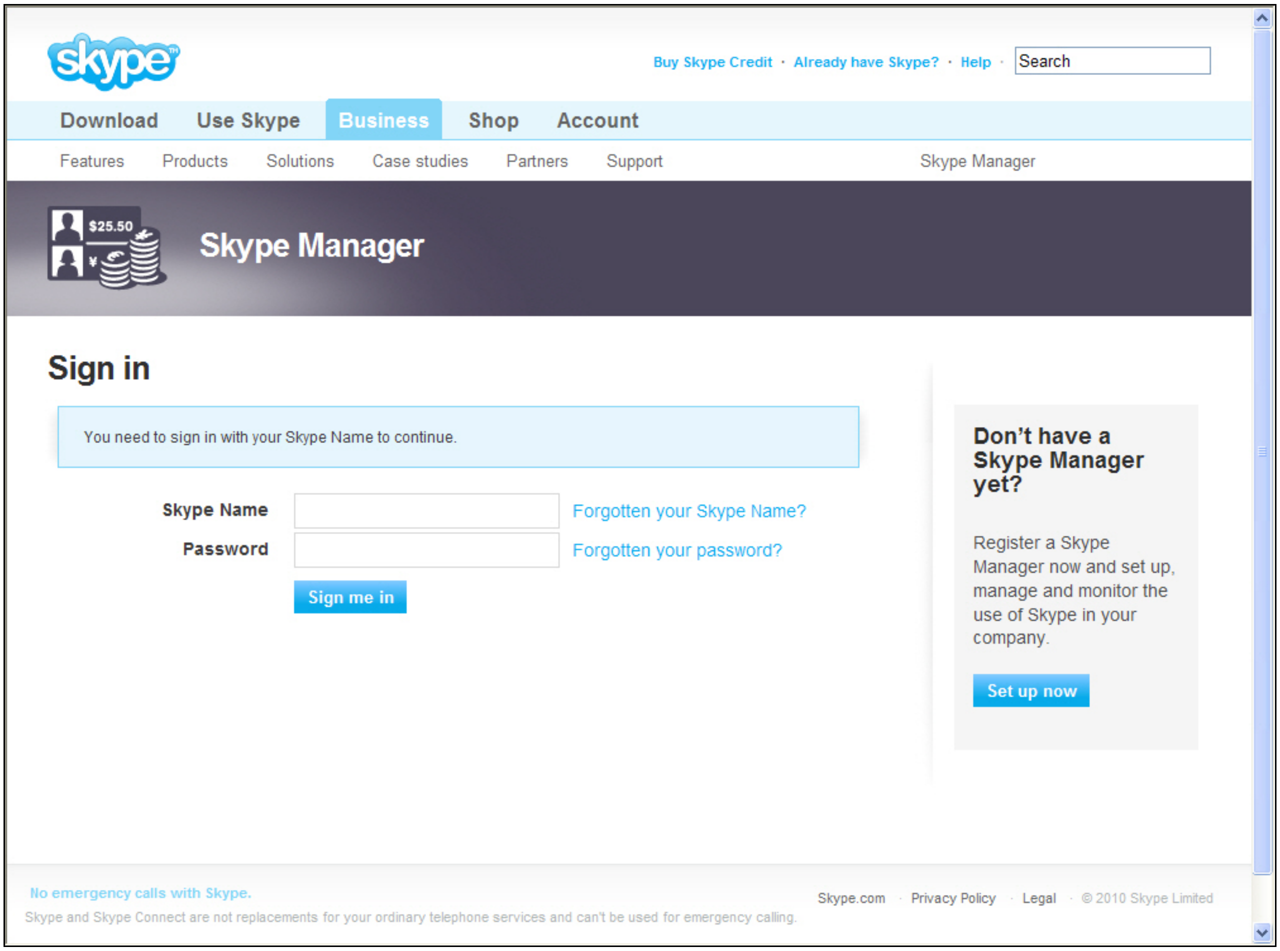

Figure 48: Skype Manager Sign In Screen

5.2. Skype Connect Profile

After logging in, the Dashboard screen is displayed as shown in **Figure 49**.

1. Click on **Skype Connect.** See **Figure 49.**
2. Click on **Create a new profile**. See **Figure 50**.
3. Enter a name for the new profile (e.g. SIL Westminster Co-RES). See **Figure 51**.
4. **Section 5.3.2** provides details on how to setup **SIP Authentication**.

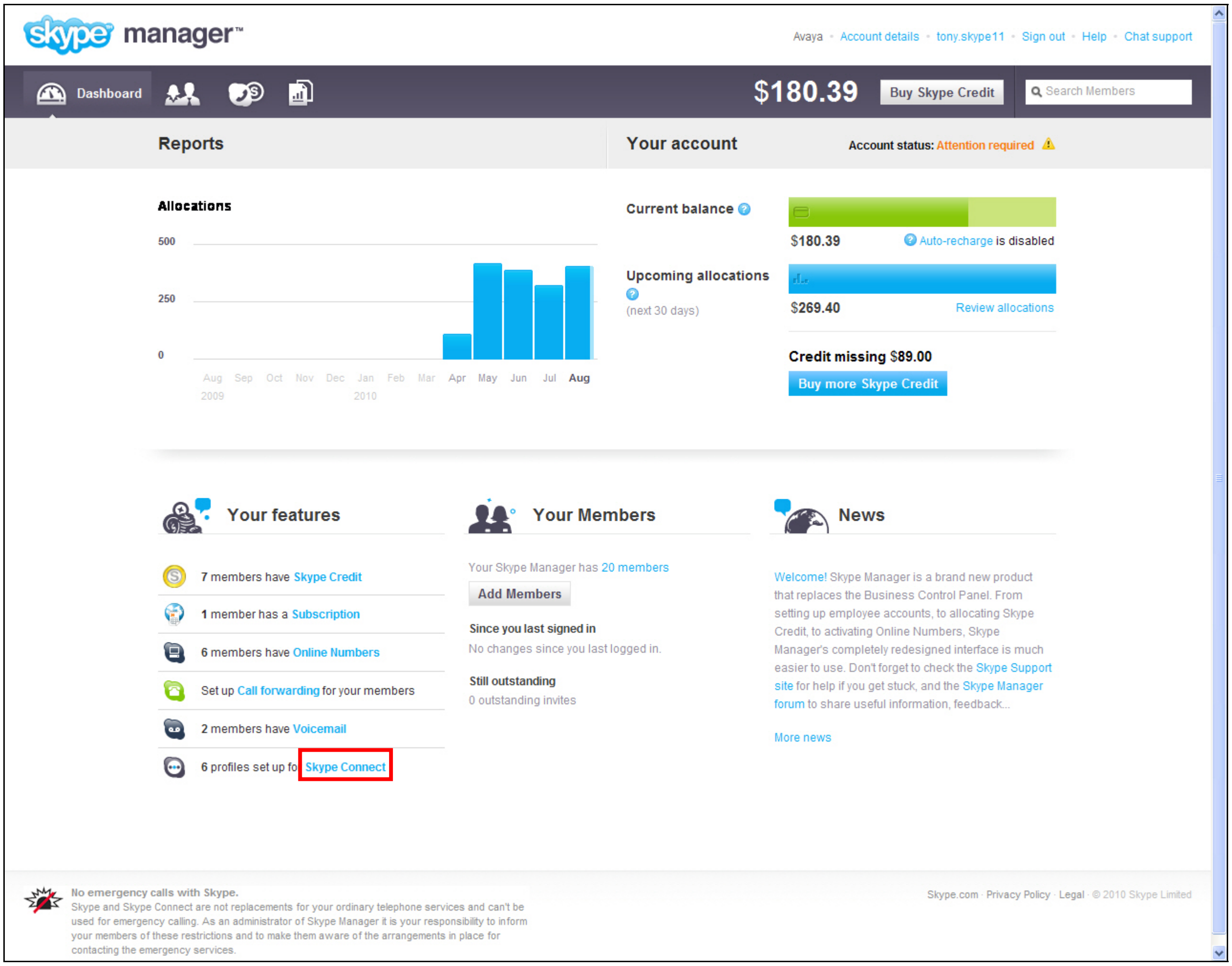

Figure 49: Skype Manager Dashboard Screen

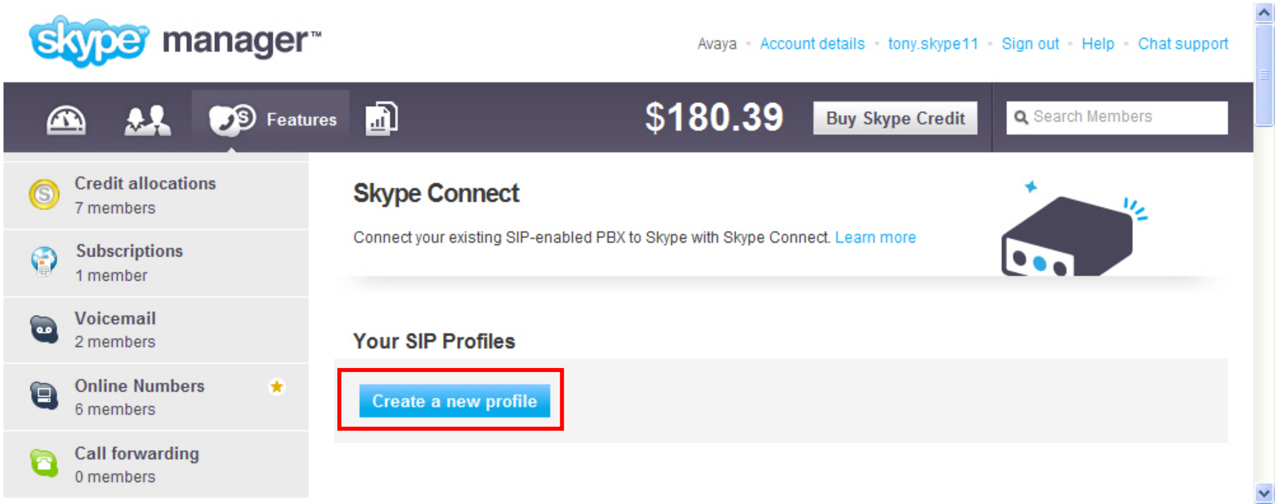

Figure 50: Create a new profile

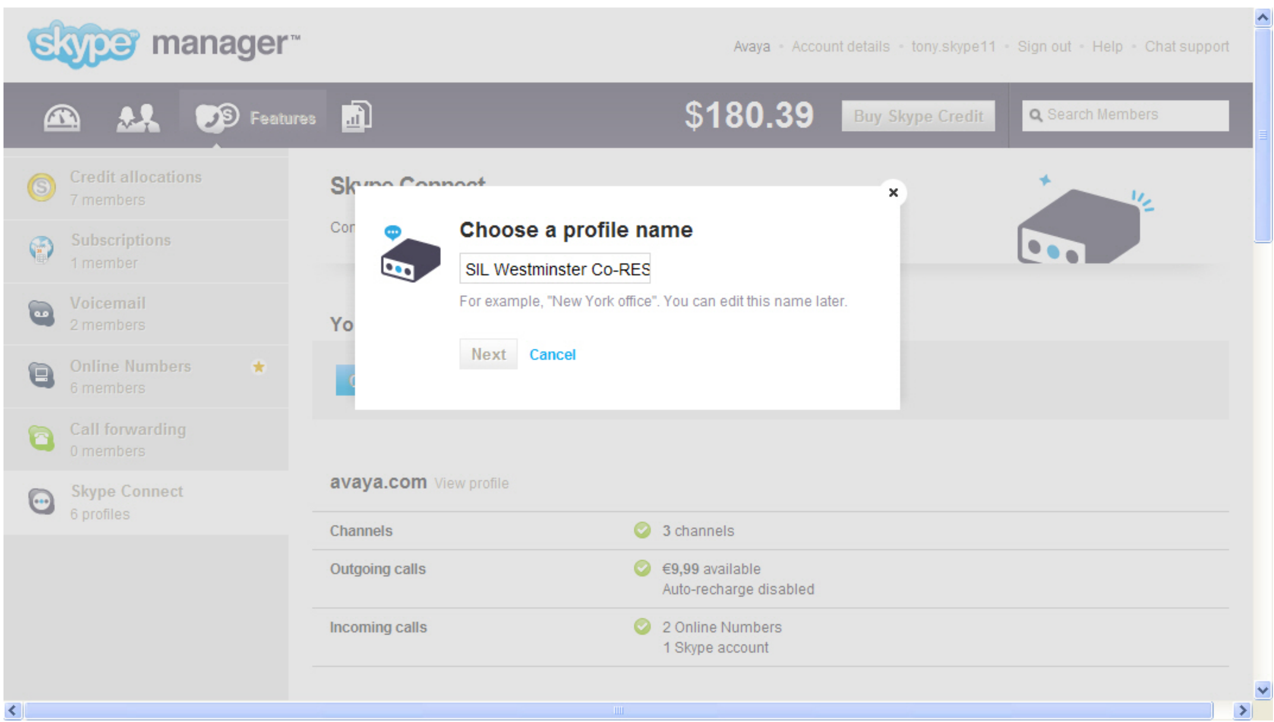

Figure 51: Choose a Profile Name

5.3. Skype Connect Authentication Details

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

5.3.1 Registration Authentication Method

The Registration Authentication method is not supported in the reference configuration documented in these Application Notes.

5.3.2 IP Authentication Method

The **IP Authentication** method shown in **Figure 52** is 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 in the Skype SIP registrar which enables Skype to locate and explicitly point traffic to the SIP Enablement Services server deployed at the Avaya CPE.

1. Click on **IP Authentication**
2. Verify the green check mark next to **IP Authentication**
3. Enter the IP details of the SIP Enablement Services server:
   a. **Public IP address → 205.168.62.96**
   b. **UDP Port → 5060**

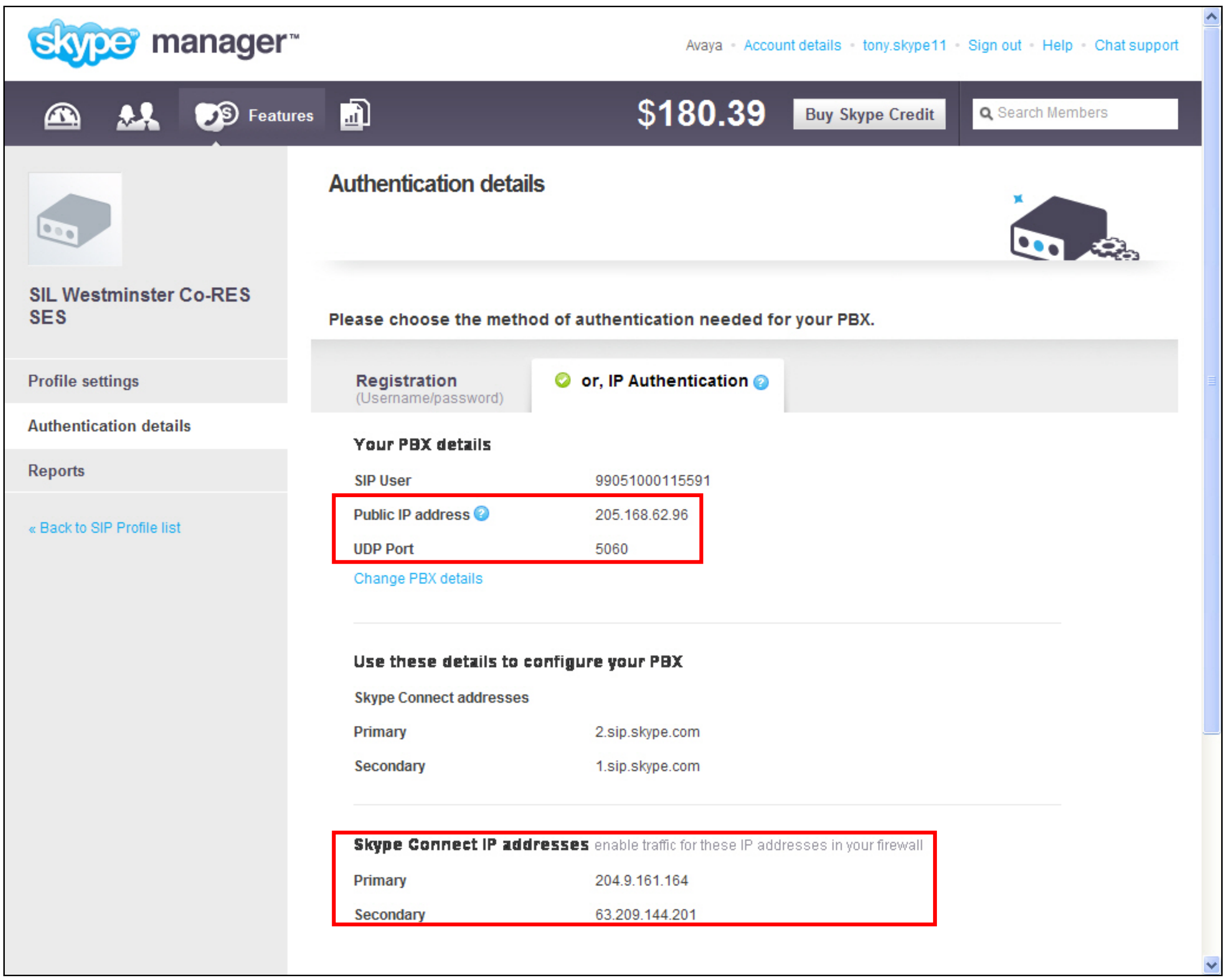

Figure 52: IP Authentication Method

The **IP Authentication** tab also contains pertinent details regarding the Skype Connect service nodes. The IP addresses of Skype's Primary and Secondary service nodes are displayed. Existing firewall devices deployed at the Avaya CPE should be programmed to enable traffic for these addresses. In addition, these IP addresses should be configured as Trusted Hosts in the SIP Enablement Services server. See **Section 4.2.5**.

5.4. Calling channels

As shown in **Figure 53**, the reference configuration utilized 2 **Calling channels**. The number of **Calling channels** should match the number of channels programmed on Avaya Aura™ Communication Manager in the trunk group form's **Number of Members** field as described in **Section 3.1.5.1**. These calling channels are provided by Skype on a subscription basis.

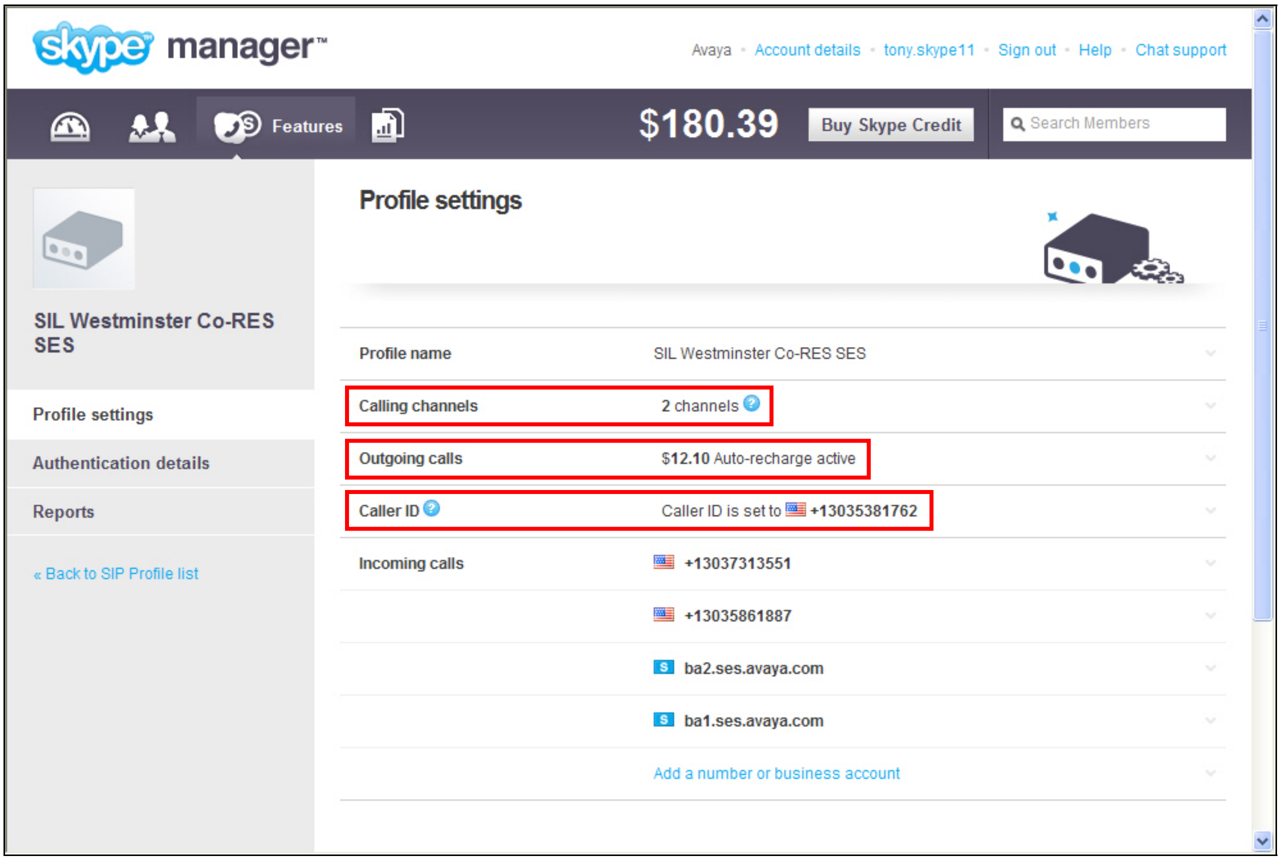

Figure 53: Profile Settings

5.5. Outgoing Calls

As shown in **Figure 53**, 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 Skype Online Numbers associated to the SIP profile. In the reference configuration, outbound PSTN destinations will receive the statically assigned caller ID from the Skype profile or other Skype default caller ID (e.g. 000-123-456).

As pointed out in **Section 1.3**, Call-by-Call Caller ID is not supported. The reference configuration described in these Application Notes generates the Skype User Name in the P-Asserted-ID header of the outgoing SIP INVITE. When Skype checks the content of the P-Asserted-ID header against the users CLI database, the values will not match and Skype will use the statically assigned caller ID. In the reference configuration, the statically assigned caller ID is set to “13035381762” as shown in **Figure 53**.

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

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

In the reference configuration documented in these Application Notes, Avaya Aura™ Communication Manager’s Calling Party Number Block feature is not compatible with Skype Connect. Note that calls from Communication Manager endpoints that activate Calling Party Number (CPN) Blocking will be blocked.

Incoming PSTN calls from Skype that are transferred to outbound PSTN destinations will receive the statically programmed caller ID from the Skype profile or other default caller ID (e.g. 000-123-456).

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 4.2.6.2.1** describes how Avaya Aura™ SIP Enablement Services routes calls from Skype Connect to Avaya Aura™ Communication Manager.

5.7.1 Incoming calls – Skype Business Acount

Skype Connect enables a Business Account (Skype name) to be assigned to a SIP profile so other Skype users can make free calls to a SIP user's Skype name (Skype-to-Skype calls). Calls are routed from the Skype Peer-to-Peer (P2P) network to the Skype Connect profile's User Agent. As shown in **Figure 54**, a Skype P2P call to "ba1.ses.avaya.com" is mapped to extension 22001[8], and 22001 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, additional Address Maps will be required to handle the routing of extension numbers by Avaya Aura™ SIP Enablement Services to Communication Manager as described in **Section 4.2.6.2.1**. However, since these calls exactly match an extension number on Communication Manager, additional entries are not required in the INCOMING CALL HANDLING TREATMENT form described in **Section 3.1.7.2**.

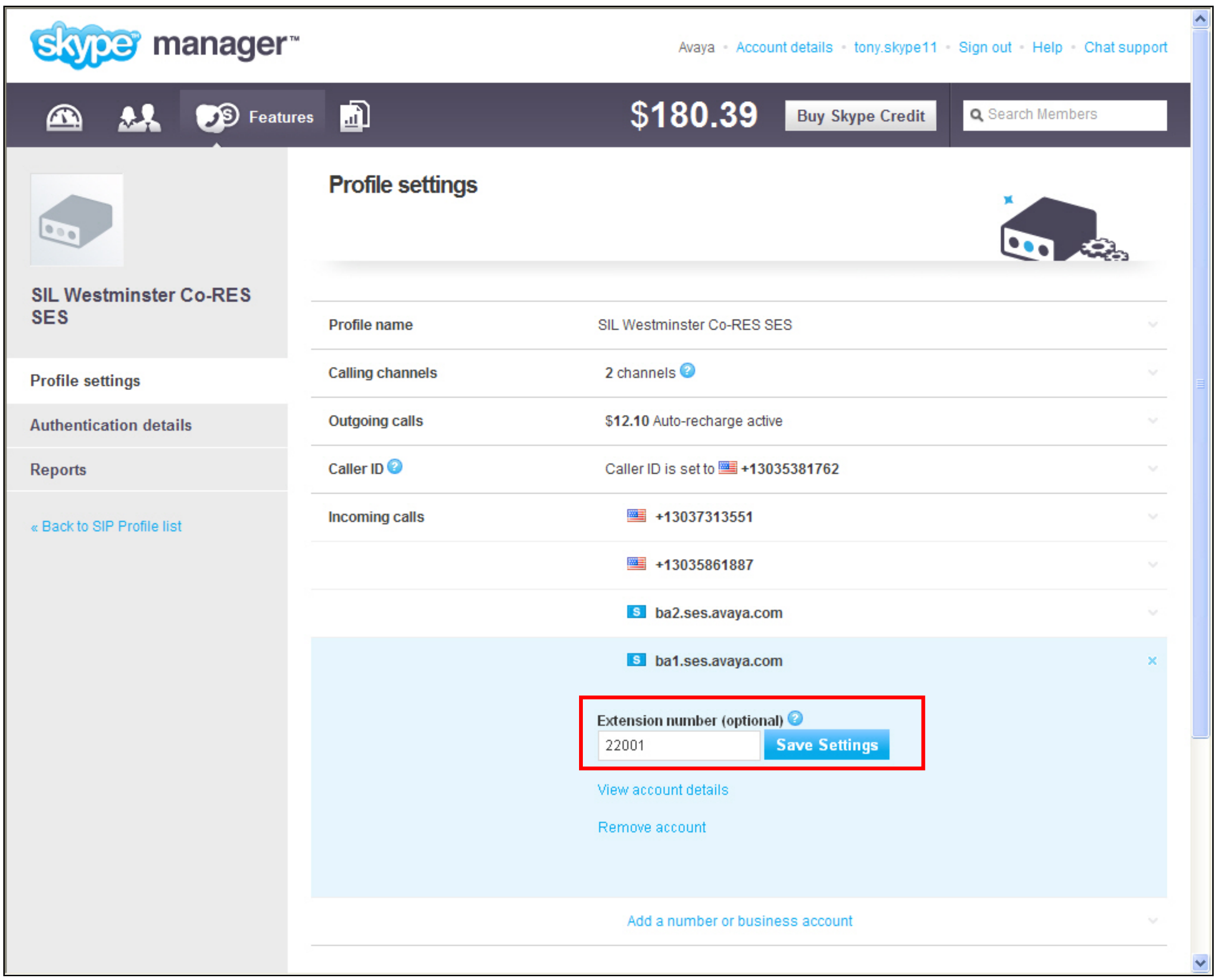

Figure 54: Skype Business Account to Extension Number Mapping

[8] When no extension number is specified, Skype delivers the Skype-assigned SIP User name (shown in **Figure 52)** in the Request URI of the SIP Invite. In this case, additional Address Maps will be required to handle the Skype SIP User Name per **Section 4.2.6.2.1** and additional entries will be required per **Section 3.1.7.2**.

5.8. Skype Connect Reports

Usage reports can be viewed by accessing the **Profile settings** screen as shown in **Figure 53**. Then, select **Reports** as shown in **Figure 55**.

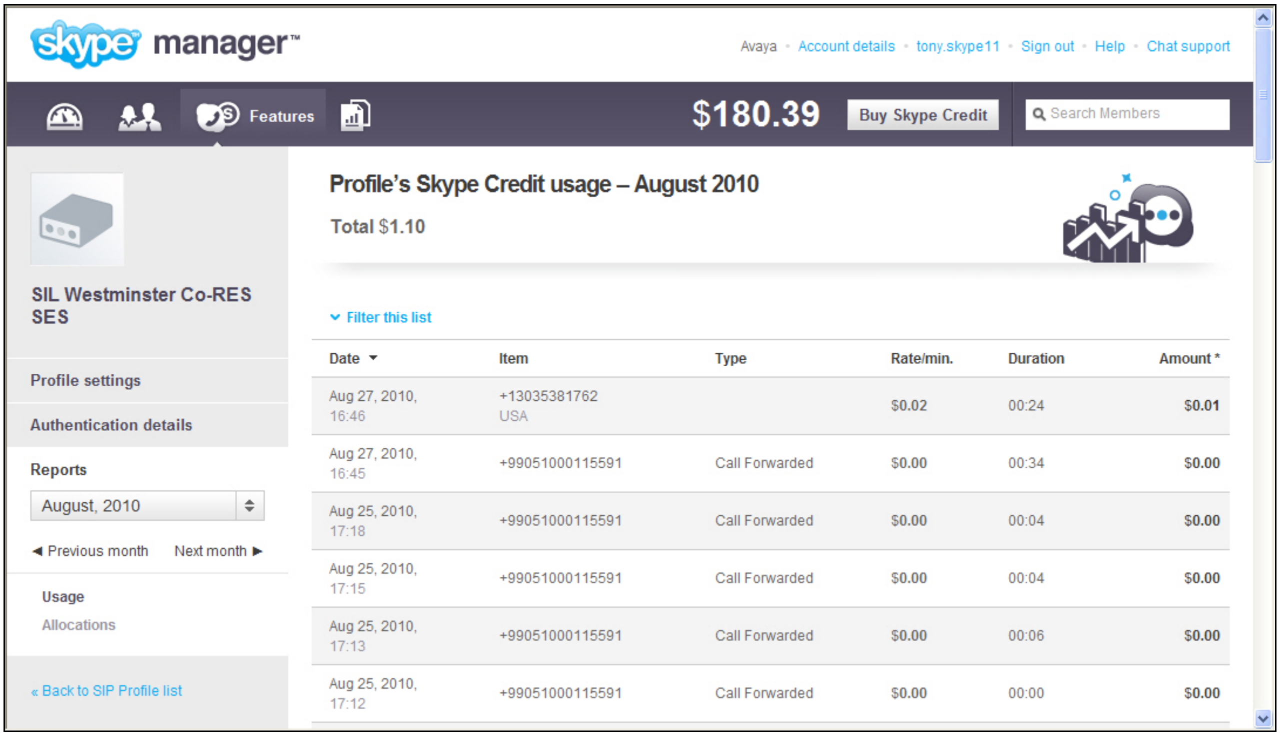

Figure 55: Skype Credit Usage Report

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. 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 & SIP) as well as traditional analog and digital TDM phones.
  - Inbound call from Skype P2P user to Skype Business Account delivered to an Avaya 9630 telephone.
- Direct IP-to-IP Media (also known as "Shuffling") when applicable.
- DTMF Tone Support.
- Supplementary calling features were verified. The supplementary calling features verified are:
  - Hold, Call transfer, Conference.
  - Voicemail Coverage and Retrieval.

6.2. Troubleshooting

6.2.1 Avaya Aura™ Communication Manager

- Use the SAT ***list trace station xxx*** command, where xxx is a station extension, to monitor station call progress.
- Use the SAT ***status station xxx*** command, where xxx is a station extension, to view station call states.
- Use the SAT ***list trace tac xxx*** command, where xxx is the tac code defined on the trunk group form, to monitor trunk activity.

Verify the status of the SIP trunk group by using the "status trunk n" command, where "n" is the trunk group number administered in **Section 3.1.5**. Verify that all trunks are in the "in-service/idle" state as shown in **Figure 56**.

```
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
```

Figure 56: Status Trunk

Verify the status of the SIP signaling groups by using the "status signaling-group n" command, where "n" is the signaling group number administered in **Section 3.1.5.1**. 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 57: 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 Communication Manager "procr" interface and SIP Enablement Services server are shown in the **Signaling** section. In addition, the **Audio** section shows that the G.729 codec is used, the IP address of the Avaya H.323 endpoint in the **Near-end** field, the IP address of the Skype Connect service node in the **Far-end** field, as well as the UDP ports used for the audio connection. The **Audio Connection Type** displays "**ip-direct**", indicating direct media between the two endpoints.

```
status trunk 68/2                                                Page   1 of   3
                              TRUNK STATUS

 Trunk Group/Member: 0068/002              Service State: in-service/active
              Port: T00114             Maintenance Busy? no
 Signaling Group ID: 68

   IGAR Connection? no

    Connected Ports: S00003
```

Figure 58: Status Trunk – Active Call – Page 1

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

Near-end Signaling Loc: 01A0017
  Signaling   IP Address                                     Port
   Near-end:  205.168.62.96                                : 6001
    Far-end:  205.168.62.96                                : 5061
 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:  205.168.62.99                                : 2932
    Far-end:  63.209.144.201                               : 23192

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

Figure 59: Status Trunk – Active Call – Page 2

6.2.2 Avaya Aura™ SIP Enablement Services

- SIP Enablement Services Trace Logger – The trace logger is accessed via the browser-based management GUI.
  1. Access the browser-based management GUI as described in **Section 4.2.1** and **Figure 29**.
  2. As shown in **Figure 60**, the "Top" window is displayed. Expand the **Trace Logger** section and select **Configure Filters**.

Figure 60: Sip Server Management Top Page

3. The **Filter Configuration** window will open (**Figure 61**). Select **Add New Rule to Filter**.

Figure 61: Filter Configuration

4. Create a filter to capture all traffic as shown in **Figure 62**.
    - Filter Label → Enter a name for the filter.
    - Message Type → Select **any**.
    - From → Enter .*
    - Other fields may be left at their default values.
    - Select **Add** to save the filter. Then, select **OK** when prompted. Then, select **Continue**.

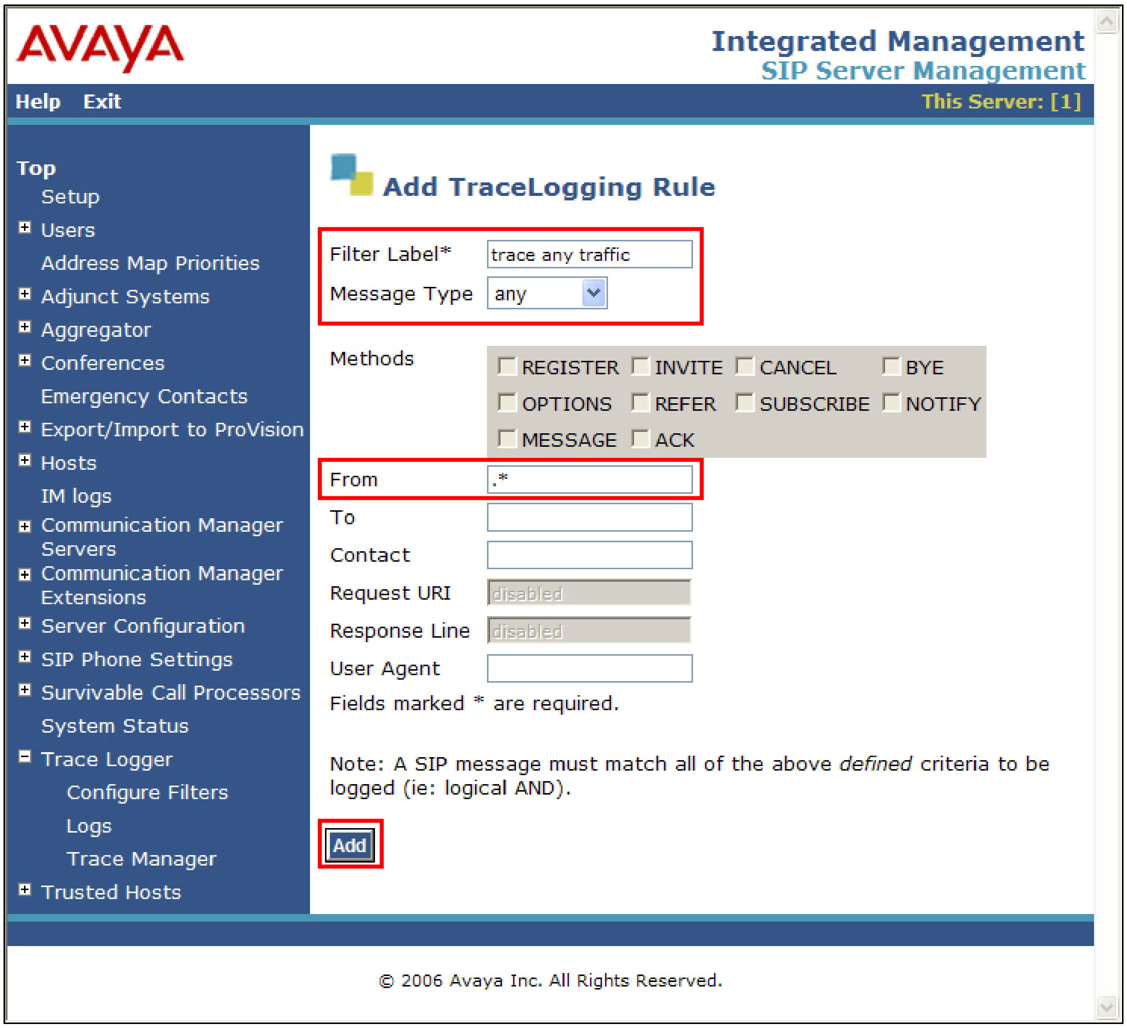

Figure 62: Filter to Capture All Traffic

5. The new filter rule will be displayed as shown in **Figure 63**.

Figure 63: Filter Rule

6. Select **Trace Manager** and the **Trace Manager** window is displayed as shown in **Figure 64**. Select **Start Tracing** (the screen will update to display **Tracing is on** and **Stop Tracing**). Run the test. When the test is completed select **Stop Tracing**.

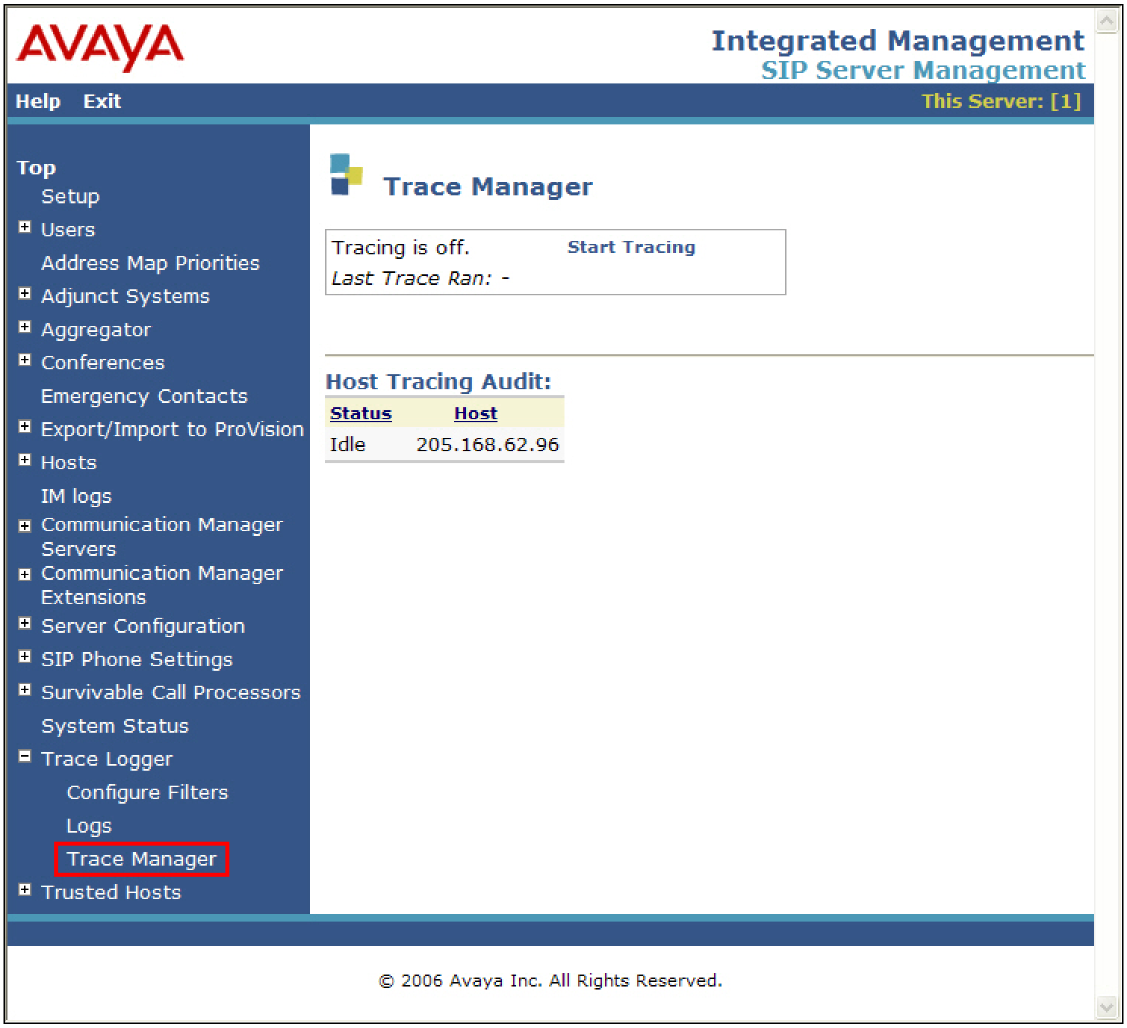

Figure 64: Trace Manager

7. When tracing is complete select **Logs** and the **TraceLogs File Download** window will open displaying details of the captured trace (**Figure 65**). Select **Download** and then **OK** when prompted. A dialog box will be presented prompting the user to save the file. Once the file is saved it may be viewed with any text editor.

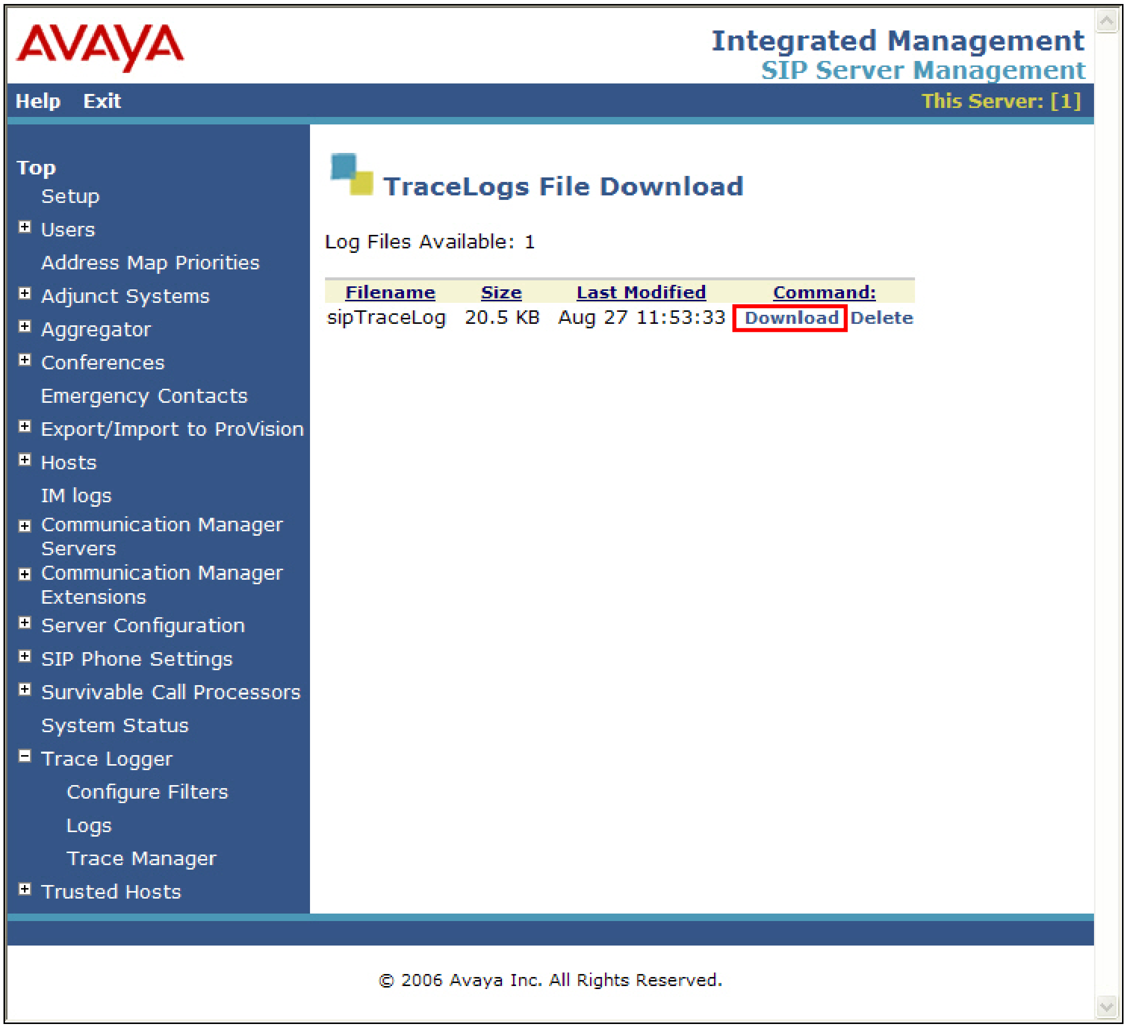

Figure 65: TraceLogs File Download

8. **Figure 66** shows sample output from the captured trace log file.

```
Aug 27 11:52:50 2010 start remote trace session on server1-pe:
      Using the following filters:
      Field<from> Value<.*>

-----------------------------------------------------------------
Aug 27 11:52:59 2010 matching filter label <trace any traffic>: server1-pe:
[Recv Request  ]
{connection: host=204.9.161.164 port=5060 protocol=UDP}
INVITE sip:13035861887@205.168.62.96:5060;transport=udp SIP/2.0
From: <sip:13035381779@sip.skype.com>;tag=a4a109cc-13c4-4c77fb95-2bcf955c-
3e18229d
To: <sip:13035861887@sip.skype.com:5060>
Call-ID: CXC-376-6807aad0-a4a109cc-13c4-4c77fb95-2bcf955c-41085147
CSeq: 1 INVITE
Via: SIP/2.0/UDP 204.9.161.164:5060;branch=z9hG4bK-3b46b-4c77fb95-2bcf955c-
6d40c312
Max-Forwards: 30
User-Agent: SipGW 0.3.19
Allow: INVITE,ACK,CANCEL,OPTIONS,BYE
Contact: <sip:13035381779@204.9.161.164:5060;transport=udp>
Content-Type: application/sdp
Content-Length: 265

v=0
o=13035381779 1282931605 1282931605 IN IP4 204.9.161.164
s=Skype call
c=IN IP4 204.9.161.164
t=0 0
m=audio 28854 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

-----------------------------------------------------------------
Aug 27 11:52:59 2010 matching filter label <trace any traffic>: server1-pe:
[Send Response ]
{connection: host=204.9.161.164 port=5060 protocol=UDP}
SIP/2.0 100 Trying
From: <sip:13035381779@sip.skype.com>;tag=a4a109cc-13c4-4c77fb95-2bcf955c-
3e18229d
To: <sip:13035861887@sip.skype.com:5060>
Call-ID: CXC-376-6807aad0-a4a109cc-13c4-4c77fb95-2bcf955c-41085147
CSeq: 1 INVITE
Via: SIP/2.0/UDP 204.9.161.164:5060;received=204.9.161.164;branch=z9hG4bK-
3b46b-4c77fb95-2bcf955c-6d40c312
Content-Length: 0
Organization: avaya.com
Server: Avaya SIP Enablement Services
```

Figure 66: Sample Trace Log

6.3. Conclusion

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

7. Support

7.1. Avaya

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

7.2. Skype

For technical support on the Skype Connect 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] *Application Notes for Configuring Alternate Methods of Domain Based Routing for Outbound SIP Calls with the Avaya SIP Trunk Architecture – Issue 1.0*

[2] *Administering Avaya Aura™ Communication Manager*, Doc ID 03-300509, May 2009.

[3] *Avaya Aura™ Communication Manager Feature Description and Implementation, 555-245-205, Issue 7, May 2009*

[4] *SIP Support in Avaya Aura™ Communication Manager Running on the Avaya S8xxx Servers, Doc ID 555-245-206, May 2009.*

[5] *Administering Avaya Aura™ SIP Enablement Services on the Avaya S8300 Server, Doc ID 03-602508, May 2009.*

[6] *Installing, Administering, Maintaining, and Troubleshooting Avaya Aura™ SIP Enablement Services, Doc ID 03-600768, November 2009.*

[7] *Avaya Aura™ Call Center 5.2 Call Vectoring and Expert Agent Selection (EAS) Reference, Doc ID 07-600780, Release 5.2, April 2009.*

8.2. Skype Connect

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

[8] *Skype Connect Product Datasheet, Version 3.0*

9. Appendix A – 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

10. Appendix B – Specifying Pattern Strings in Address Maps

The syntax for the pattern matching used within the Avaya Aura™ SIP Enablement Services is a Linux regular expression used to match against the URI string found in the SIP INVITE message.

Regular expressions are a way to describe text through pattern matching. The regular expression is a string containing a combination of normal text characters, which match themselves, and special *metacharacters*, which may represent items like quantity, location or types of character(s).

In the pattern matching string used in SIP Enablement Services:

- Normal text characters and numbers match themselves.
- Common metacharacters used are:
  - A period **.** matches any character once (and only once).
  - An asterisk ***** matches zero or more of the preceding characters.
  - Square brackets enclose a list of any character to be matched. Ranges are designated by using a hyphen. Thus the expression **[12345]** or **[1-5]** both describe a pattern that will match any single digit between 1 and 5.
  - Curly brackets containing an integer 'n' indicate that the preceding character must be matched exactly 'n' times. Thus **5{3}** matches '555' and **[0-9]{10}** indicates any 10 digit number.
  - The circumflex character **^** as the first character in the pattern indicates that the string must begin with the character following the circumflex.

Putting these constructs together as used in this document, the pattern to match the SIP INVITE string for any valid 1+ 10 digit number in the North American dial plan would be:

^sip:1[0-9]{10}

This reads as: "Strings that begin with exactly **sip:1** and having any 10 digits following will match.

A typical INVITE request below uses the shaded portion to illustrate the matching pattern.

INVITE sip:13035551212@20.1.1.54:5060;transport=udp SIP/2.0

11. Appendix C – Deactivation of Per Contact Timer

In the software version of Avaya Aura™ SIP Enablement Services referenced in these Application Notes, the following behavior was observed: For unanswered outbound calls from Avaya CPE to Skype, SIP Enablement Services sends a SIP CANCEL message at 30 seconds, which drops the call. This behavior is controlled by a software timer called **PerContactWaitTime4DnsRoute** and the default value for this timer is 30 seconds. If this behavior is observed in the field, the workaround described below can been implemented to deactivate this timer and allow unanswered outbound calls to ring for longer than 30 seconds.

On the SIP Enablement Services, the appropriate level of access must be used and the following command must be executed:

```
# setSipTimers4DnsRouting per_contact 0
TRACE(set-ccsconf-name-value): replace /usr/impress/sip-server/etc/ccs.conf now
14783
```

The following command can be used to verify the change to the timer value:

```
# setSipTimers4DnsRouting status
/usr/impress/sip-server/bin/setSipTimers4DnsRouting: timerb= ms
/usr/impress/sip-server/bin/setSipTimers4DnsRouting: per_contact=0 seconds
/usr/impress/sip-server/bin/setSipTimers4DnsRouting: location_set= seconds
```

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