Avaya Solution & Interoperability Test Lab

Application Notes for IPC System Interconnect with Avaya Aura^{TM} Communication Manager Using Avaya Aura^{TM} SIP Enablement Services – Issue 1.0

Abstract

These Application Notes describe the configuration steps required for IPC System Interconnect 16.1 to interoperate with Avaya Aura^{TM} Communication Manager 5.2.1 using Avaya Aura^{TM} SIP Enablement Services 5.2.1.

IPC System Interconnect is a trading communication solution. In the compliance testing, IPC System Interconnect used SIP trunks to Avaya Aura^{TM} SIP Enablement Services, for turret users on IPC to reach users on Avaya Aura^{TM} Communication Manager and on the PSTN.

Information in these Application Notes has been obtained through DevConnect compliance testing and additional technical discussions. Testing was conducted via the DevConnect Program at the Avaya Solution and Interoperability Test Lab.

1. Introduction

These Application Notes describe the configuration steps required for IPC System Interconnect 16.1 to interoperate with Avaya Aura™ Communication Manager 5.2.1 using Avaya Aura™ SIP Enablement Services (SES) 5.2.1.

IPC System Interconnect is a trading communication solution. In the compliance testing, IPC System Interconnect used SIP trunks to Avaya Aura™ SES, for turret users on IPC to reach users on Avaya Aura™ Communication Manager and on the PSTN.

1.1. Interoperability Compliance Testing

The interoperability compliance test included feature and serviceability testing.

The feature testing included basic call, display, G.711MU, G.729AB, codec negotiation, media shuffling, hold/reconnect, DTMF, call forwarding unconditional/ring-no-answer/busy, blind/attended transfer, and attended conference.

The serviceability testing focused on verifying the ability of IPC System Interconnect to recover from adverse conditions, such as disconnecting/reconnecting the Ethernet cables to IPC System Interconnect.

1.2. Support

Technical support on IPC System Interconnect can be obtained through the following:

- **Phone:** (800) NEEDIPC, (203) 339-7800
- **Email:** systems.support@ipc.com

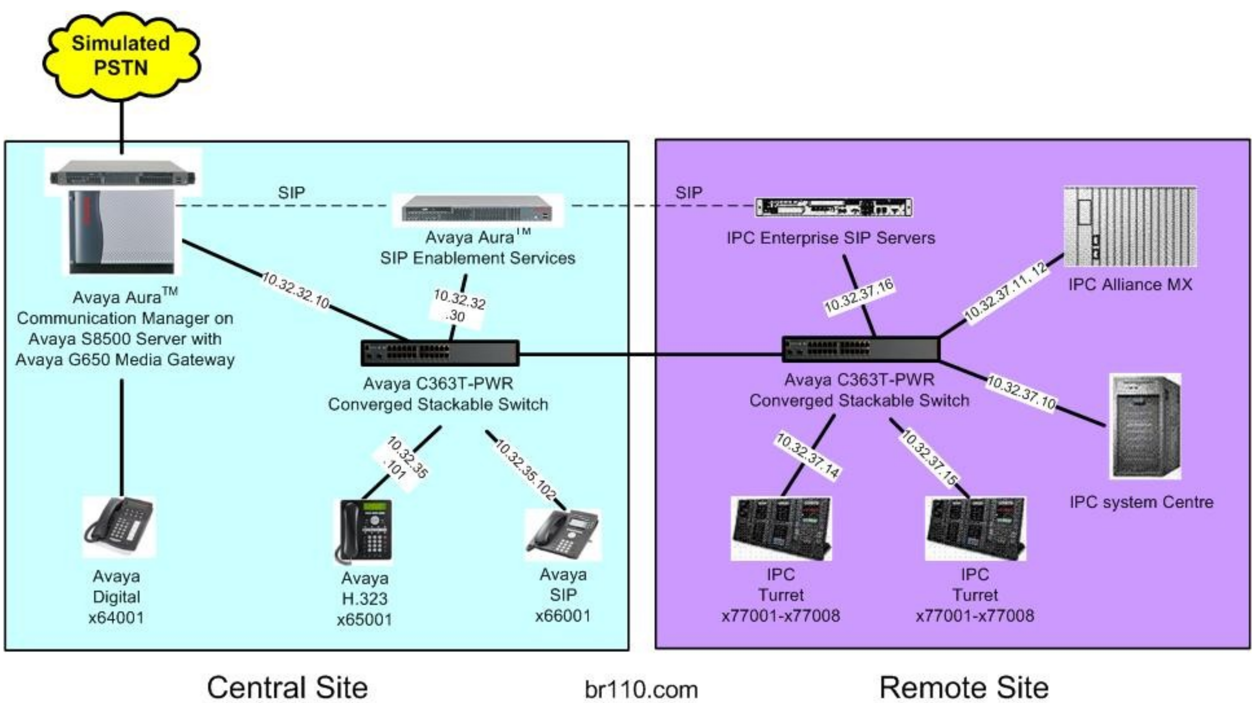
2. Reference Configuration

As shown in the test configuration below, IPC System Interconnect at the Remote Site consists of the Enterprise SIP Server (ESS), Alliance MX, System Center, and Turrets. SIP trunks are used from System Interconnect to Avaya Aura™ SES, to reach users on Avaya Aura™ Communication Manager and on the PSTN.

IPC System Interconnect supports only one SIP domain, which will be used in both the SIP "From" and "To" headers. Therefore, the same domain must be used for the two sites. In the compliance testing, the "br110.com" domain was used for all users on both sites.

A five digit Uniform Dial Plan (UDP) was used to facilitate dialing between the Central and Remote sites. Unique extension ranges were associated with Avaya Aura™ Communication Manager users at the Central site (6xxxx), and IPC turret users at the Remote site (7xxxx).

The detailed administration of basic connectivity between Avaya Aura™ Communication Manager and Avaya Aura™ SIP Enablement Services is not the focus of these Application Notes and will not be described.



3. Equipment and Software Validated

The following equipment and software were used for the sample configuration provided:

Equipment	Software
Avaya Aura™ Communication Manager on Avaya S8500 Server	5.2.1 (R015x.02.1.016.4-18433)
Avaya G650 Media Gateway • TN799DP C-LAN Circuit Pack • TN2302AP IP Media Processor	 HW01 FW038 HW20 FW121
Avaya Aura™ SIP Enablement Services	5.2.1 (SES-5.2.1.0-016.4)
Avaya 1608 IP Telephone (H.323)	1.3
Avaya 9630 IP Telephone (H.323)	3.1
Avaya 9630 IP Telephone (SIP)	2.6.2
IPC System Interconnect • Alliance MX • Enterprise SIP Server • System Center o SIPX Line Card • Turrets	SipProxy-2.00.01-13 16.01.01.03.0007 16.01.01.03.0007 16.01.01.03.0007 16.01.01.03.0007 16.01.01.03.0007

4. Configure Avaya Aura^{TM} Communication Manager

This section provides the procedures for configuring Avaya Aura^{TM} Communication Manager. The procedures include the following areas:

- Verify Communication Manager license
- Administer system parameters features
- Administer SIP trunk group
- Administer SIP signaling group
- Administer IP network region
- Administer IP codec set
- Administer route pattern
- Administer public unknown numbering
- Administer uniform dial plan
- Administer AAR analysis
- Administer ISDN trunk group
- Administer tandem calling party number

In the compliance testing, the same set of codec set, network region, trunk group, and signaling group were used for the Avaya SIP and IPC turret users, which enabled IPC turret users to use the same digits dialing as Avaya SIP users, to reach other users on Communication Manager and on the PSTN.

4.1. Verify Communication Manager License

Log into the System Access Terminal (SAT) to verify that the Communication Manager license has proper permissions for features illustrated in these Application Notes. Use the "display system-parameters customer-options" command. Navigate to **Page 2**, and verify that there is sufficient remaining capacity for SIP trunks by comparing the **Maximum Administered SIP Trunks** field value with the corresponding value in the **USED** column.

The license file installed on the system controls the maximum permitted. If there is insufficient capacity, contact an authorized Avaya sales representative to make the appropriate changes.

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

IP PORT CAPACITIES                                                USED
                     Maximum Administered H.323 Trunks: 100   6
           Maximum Concurrently Registered IP Stations: 18000 4
             Maximum Administered Remote Office Trunks: 8000  0
Maximum Concurrently Registered Remote Office Stations: 18000 0
              Maximum Concurrently Registered IP eCons: 10    0
  Max Concur Registered Unauthenticated H.323 Stations: 10    0
                  Maximum Video Capable H.323 Stations: 100   0
                   Maximum Video Capable IP Softphones: 100   0
                       Maximum Administered SIP Trunks: 100   10
  Maximum Administered Ad-hoc Video Conferencing Ports: 0     0
   Maximum Number of DS1 Boards with Echo Cancellation: 0     0
```

4.2. Administer System Parameters Features

Use the “change system-parameters features” command to allow for trunk-to-trunk transfers.

This feature is needed to be able to transfer an incoming call from IPC back out to IPC (incoming trunk to outgoing trunk), and to transfer an outgoing call to IPC to another outgoing call to IPC (outgoing trunk to outgoing trunk). For ease of interoperability testing, the **Trunk-to-Trunk Transfer** field was set to “all” to enable all trunk-to-trunk transfers on a system wide basis. Note that this feature poses significant security risk, and must be used with caution. For alternatives, the trunk-to-trunk feature can be implemented on the Class Of Restriction or Class Of Service levels. Refer to [1] for more details.

```
change system-parameters features                              Page   1 of  18
                            FEATURE-RELATED SYSTEM PARAMETERS
                               Self Station Display Enabled? y
                                    Trunk-to-Trunk Transfer: all
               Automatic Callback with Called Party Queuing? n
    Automatic Callback - No Answer Timeout Interval (rings): 3
                       Call Park Timeout Interval (minutes): 10
        Off-Premises Tone Detect Timeout Interval (seconds): 20
                                 AAR/ARS Dial Tone Required? y

              Music (or Silence) on Transferred Trunk Calls? no
                       DID/Tie/ISDN/SIP Intercept Treatment: attd
    Internal Auto-Answer of Attd-Extended/Transferred Calls: none
                  Automatic Circuit Assurance (ACA) Enabled? n




             Abbreviated Dial Programming by Assigned Lists? n
       Auto Abbreviated/Delayed Transition Interval (rings): 2
                    Protocol for Caller ID Analog Terminals: Bellcore
    Display Calling Number for Room to Room Caller ID Calls? n
```

4.3. Administer SIP Trunk Group

Use the “change trunk-group n” command, where “n” is the existing SIP trunk group number used to reach Avaya SES, in this case “5”.

For **Group Name**, update as desired to reflect the same trunk group used to reach SES and IPC. For **Number of Members**, enter sufficient number for simultaneous calls to Avaya SIP and IPC users. Note that a call between an Avaya SIP user and an IPC user uses two SIP trunks, whereas a call between an Avaya non-SIP user and an IPC user uses one SIP trunk. Make a note of the **Signaling Group** number.

```
change trunk-group 5                                            Page   1 of  21
                                TRUNK GROUP

Group Number: 5                    Group Type: sip          CDR Reports: y
  Group Name: SIP Trunk to SES/IPC        COR: 1        TN: 1        TAC: 1005
   Direction: two-way        Outgoing Display? n
 Dial Access? n                                   Night Service:
Queue Length: 0
Service Type: tie                   Auth Code? n

                                                       Signaling Group: 5
                                                     Number of Members: 10
```

Navigate to **Page 3**, and enter “public” for **Numbering Format**.

```
change trunk-group 5                                            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
```

Navigate to **Page 4**, and enter “101” for **Telephone Event Payload Type**, as shown below.

```
change trunk-group 5                                            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
```

4.4. Administer SIP Signaling Group

Use the "change signaling-group n" command, where "n" is the existing SIP signaling group number used by the SIP trunk group from **Section 4.3**.

For **DTMF over IP**, enter "rtp-payload". For **Direct IP-IP Audio Connections**, enter "y". Make a note of the **Far-end Network Region** number.

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

 Group Number: 5              Group Type: sip
                        Transport Method: tls
  IMS Enabled? n


   Near-end Node Name: Clan-1                 Far-end Node Name: SES
 Near-end Listen Port: 5061                 Far-end Listen Port: 5061
                                        Far-end Network Region: 1
Far-end Domain: br110.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): 6
```

4.5. Administer IP Network Region

Use the "change ip-network-region n" command, where "n" is the existing far-end network region number used by the SIP signaling group from **Section 4.4**.

For **Name**, update as desired to reflect the same network region used to reach SES and IPC. Enter "yes" for **Intra-region IP-IP Direct Audio** and **Inter-region IP-IP Direct Audio**, as shown below. In the compliance testing, the same network region was used for all Avaya users. Make a note of the **Codec Set** number. Also make a note of the **Authoritative Domain**, which should match the SIP domain name of the SES server, and will be used later to configure IPC.

```
change ip-network-region 1                                     Page   1 of  19
                               IP NETWORK REGION
  Region: 1
Location:          Authoritative Domain: br110.com
    Name: SES/IPC Region
MEDIA PARAMETERS                Intra-region IP-IP Direct Audio: yes
      Codec Set: 1              Inter-region IP-IP Direct Audio: yes
   UDP Port Min: 2048                      IP Audio Hairpinning? n
   UDP Port Max: 3329
DIFFSERV/TOS PARAMETERS                  RTCP Reporting Enabled? y
 Call Control PHB Value: 46      RTCP MONITOR SERVER PARAMETERS
        Audio PHB Value: 46       Use Default Server Parameters? y
        Video PHB Value: 26
```

4.6. Administer IP Codec Set

Use the “change ip-codec-set n” command, where “n” is the existing codec set number used by the IP network region from **Section 4.5**. Update the audio codec types in the **Audio Codec** fields as necessary. Note that IPC System Interconnect supports the G.711 and G.729 codec variants. For **Media Encryption**, make certain “none” is specified.

In the compliance testing, the same codec set was used for all Avaya users.

```
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.729AB           n         2        20
 3:
 4:
 5:
 6:
 7:


     Media Encryption
 1: none
 2:
```

4.7. Administer Route Pattern

Use the “change route-pattern n” command, where “n” is the existing route pattern number to reach SES, in this case “5”. For **Pattern Name**, update as desired to reflect the same route pattern used to reach SES and IPC. For **Secure SIP**, make certain the value is “n”.

```
change route-pattern 5                                          Page   1 of   3
                    Pattern Number: 5   Pattern Name: To SES/IPC
                             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: 5    0                                                           n   user
 2:                                                                  n   user
 3:                                                                  n   user
 4:                                                                  n   user
 5:                                                                  n   user
 6:                                                                  n   user

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

4.8. Administer Public Unknown Numbering

Use the "change public-unknown-numbering 0" command, to define the calling party number to send to IPC. Add an entry for the trunk group defined in **Section 4.3**. In the example shown below, all calls originating from a 5-digit extension beginning with 6 and routed to trunk group 5 will result in a 5-digit calling number. The calling party number will be in the SIP "From" header.

```
change public-unknown-numbering 0                              Page   1 of   2
                      NUMBERING - PUBLIC/UNKNOWN FORMAT
                                           Total
Ext Ext           Trk       CPN             CPN
Len Code          Grp(s)    Prefix          Len
                                                     Total Administered: 3
 5  6             5                         5           Maximum Entries: 9999
```

4.9. Administer Uniform Dial Plan

This section provides a sample AAR routing used for routing calls with dialed digits 7xxxx to IPC. Note that other methods of routing may be used. Use the "change uniform-dialplan 0" command, and add an entry to specify the use of AAR for routing digits 7xxxx, as shown below.

```
change uniform-dialplan 0                                       Page   1 of   2
                       UNIFORM DIAL PLAN TABLE
                                                              Percent Full: 0

  Matching                   Insert              Node
  Pattern       Len Del      Digits      Net Conv Num

 7               5   0                   aar  n
```

4.10. Administer AAR Analysis

Use the "change aar analysis 0" command, and add an entry to specify how to route calls to 7xxxx. In the example shown below, calls with digits 7xxxx will be routed as an AAR call using route pattern "5" from **Section 4.7**.

```
change aar analysis 0                                           Page   1 of   2
                             AAR DIGIT ANALYSIS TABLE
                                   Location:  all          Percent Full:    2

          Dialed          Total     Route    Call   Node  ANI
          String         Min  Max  Pattern   Type   Num   Reqd
    7                    5    5     5        aar          n
```

4.11. Administer ISDN Trunk Group

Use the "change trunk-group n" command, where "n" is the existing ISDN trunk group number used to reach the PSTN, in this case "500".

For **Modify Tandem Calling Number**, enter "y" to allow for the calling party number from IPC to be modified.

```
change trunk-group 500                                          Page   3 of  21
TRUNK FEATURES
          ACA Assignment? n            Measured: none      Wideband Support? n
                                 Internal Alert? n       Maintenance Tests? y
                               Data Restriction? n     NCA-TSC Trunk Member:
                                      Send Name: n      Send Calling Number: y
            Used for DCS? n                            Send EMU Visitor CPN? y
   Suppress # Outpulsing? n    Format: public
 Outgoing Channel ID Encoding: preferred     UUI IE Treatment: service-provider

                                                 Replace Restricted Numbers? n
                                                Replace Unavailable Numbers? n
                                                      Send Connected Number: y
Network Call Redirection: none                    Hold/Unhold Notifications? n
             Send UUI IE? y                     Modify Tandem Calling Number? y
               Send UCID? n
 Send Codeset 6/7 LAI IE? y                           Ds1 Echo Cancellation? n

    Apply Local Ringback? n              US NI Delayed Calling Name Update? n
 Show ANSWERED BY on Display? y
                             Network (Japan) Needs Connect Before Disconnect? n
```

4.12. Administer Tandem Calling Party Number

Use the "change tandem-calling-party-num" command, to define the calling party number to send to the PSTN for tandem calls from IPC turret users.

In the example shown below, all calls originating from a 5-digit extension beginning with 7 and routed to trunk group 500 will result in a 10-digit calling number. For **Number Format**, use an applicable format, in this case "pub-unk".

```
change tandem-calling-party-num                                 Page   1 of   8
                  CALLING PARTY NUMBER CONVERSION
                          FOR TANDEM CALLS
     CPN              Trk                               Number
 Len Prefix           Grp(s)     Delete  Insert         Format

 5   7                500                90884          pub-unk
```

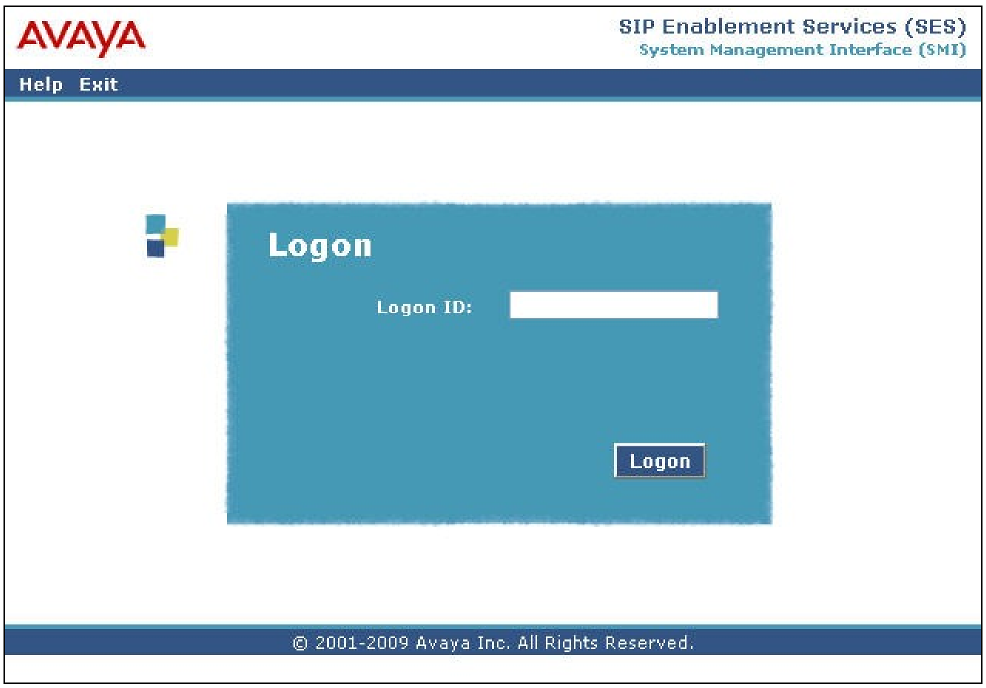
5. Configure Avaya Aura™ SIP Enablement Services

This section provides the procedures for configuring Avaya Aura™ SES. The procedures include the following areas:

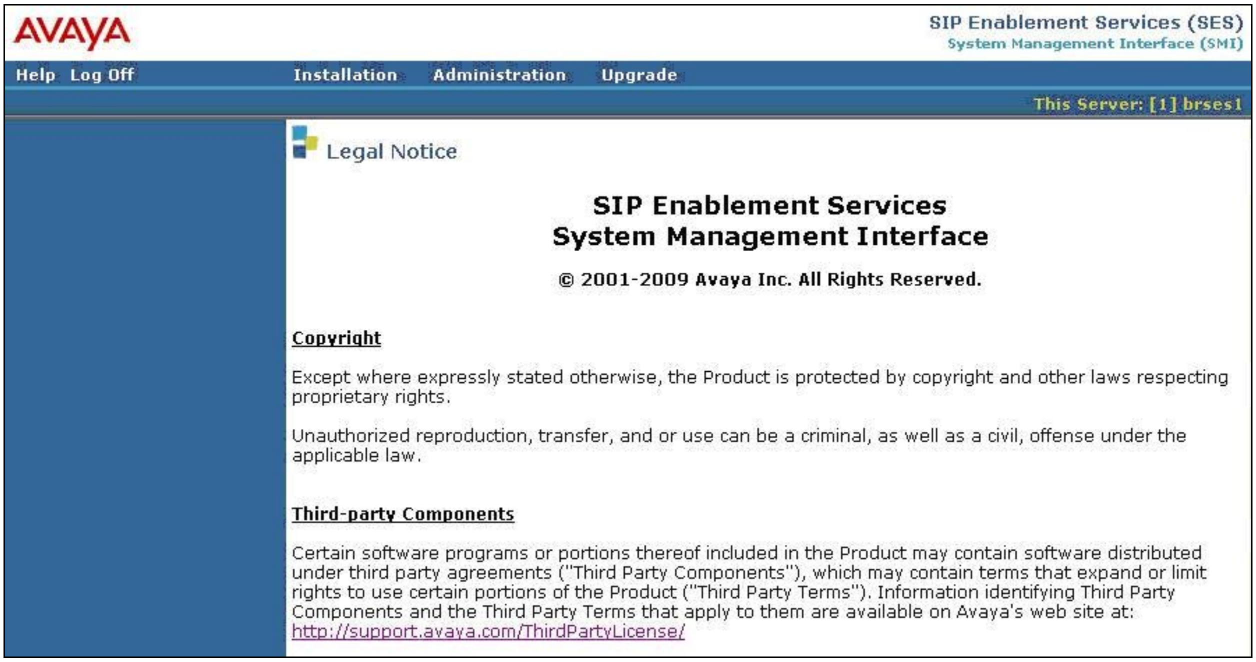
- Launch SES administration
- Administer host address map
- Administer host contact
- Administer trusted host

5.1. Launch SES Administration

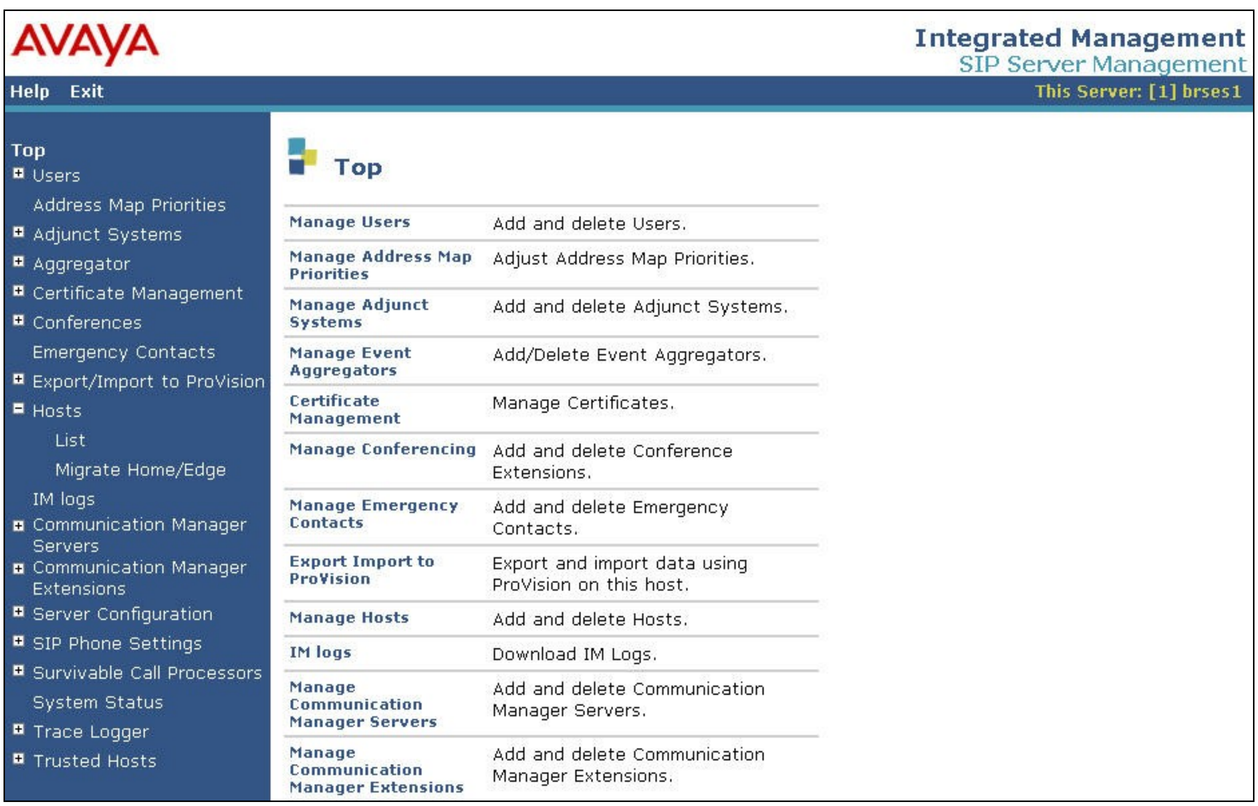
Access the SES web interface by using the URL "http://ip-address/admin" in an Internet browser window, where "ip-address" is the IP address of the SES server. Log in using the appropriate credentials.



In the subsequent screen, select **Administration > SIP Enablement Services** from the top menu.

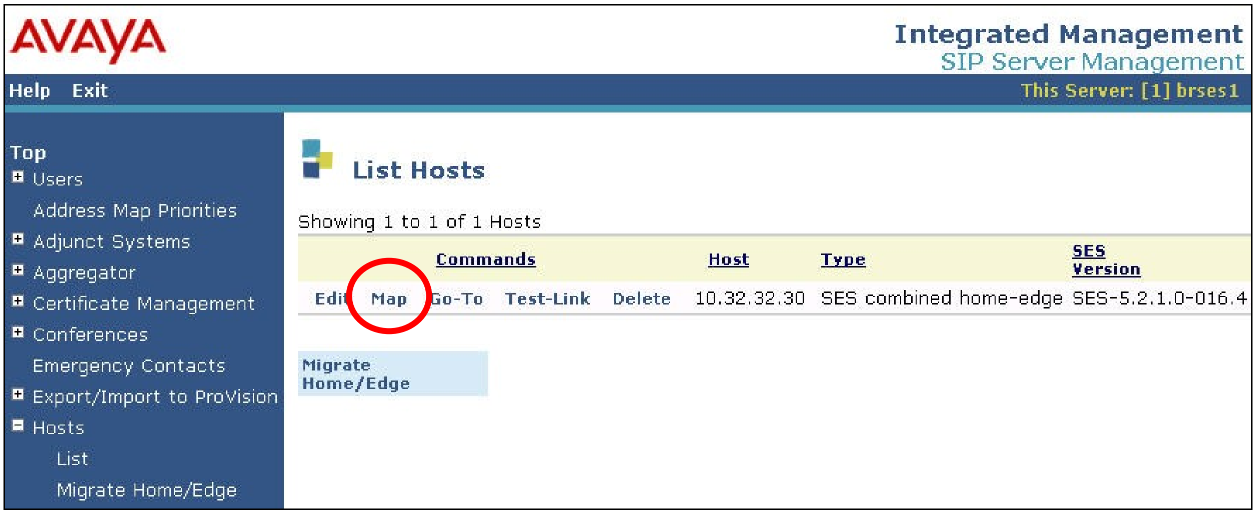


The **Top** screen is displayed next.

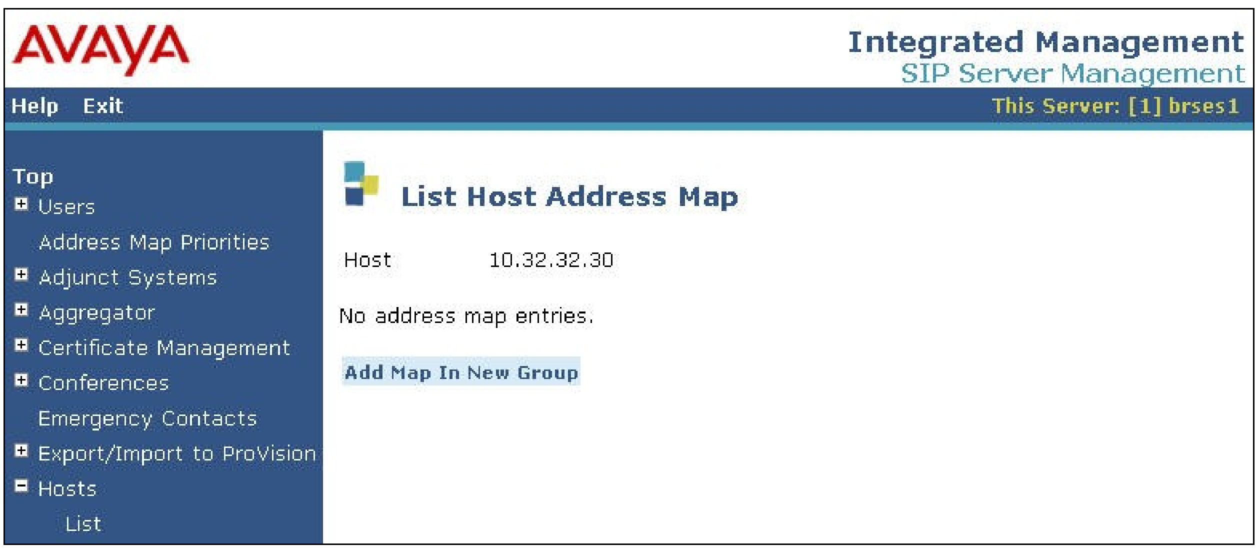


5.2. Administer Host Address Map

Select **Hosts** > **List** from the left pane. The **List Hosts** screen is displayed. Click on the **Map** link.



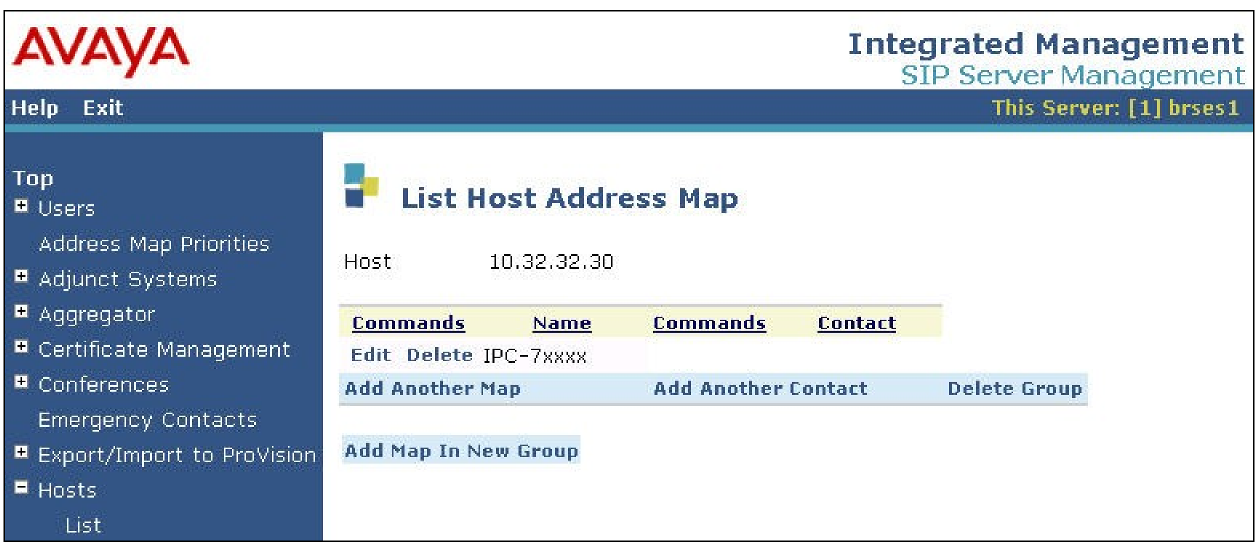
In the **List Host Address Map** screen below, click **Add Map In New Group** in the right pane.



The **Add Host Address Map** screen is displayed next. This screen is used to specify which calls are to be routed to IPC. For **Name**, enter a descriptive name to denote the routing. For **Pattern**, enter an appropriate syntax for address mapping. For the compliance testing, a pattern of "^sip:7[0-9]{4}" is used to match to any IPC turret user extensions of 7xxxx. Maintain the check in **Replace URI**.

5.3. Administer Host Contact

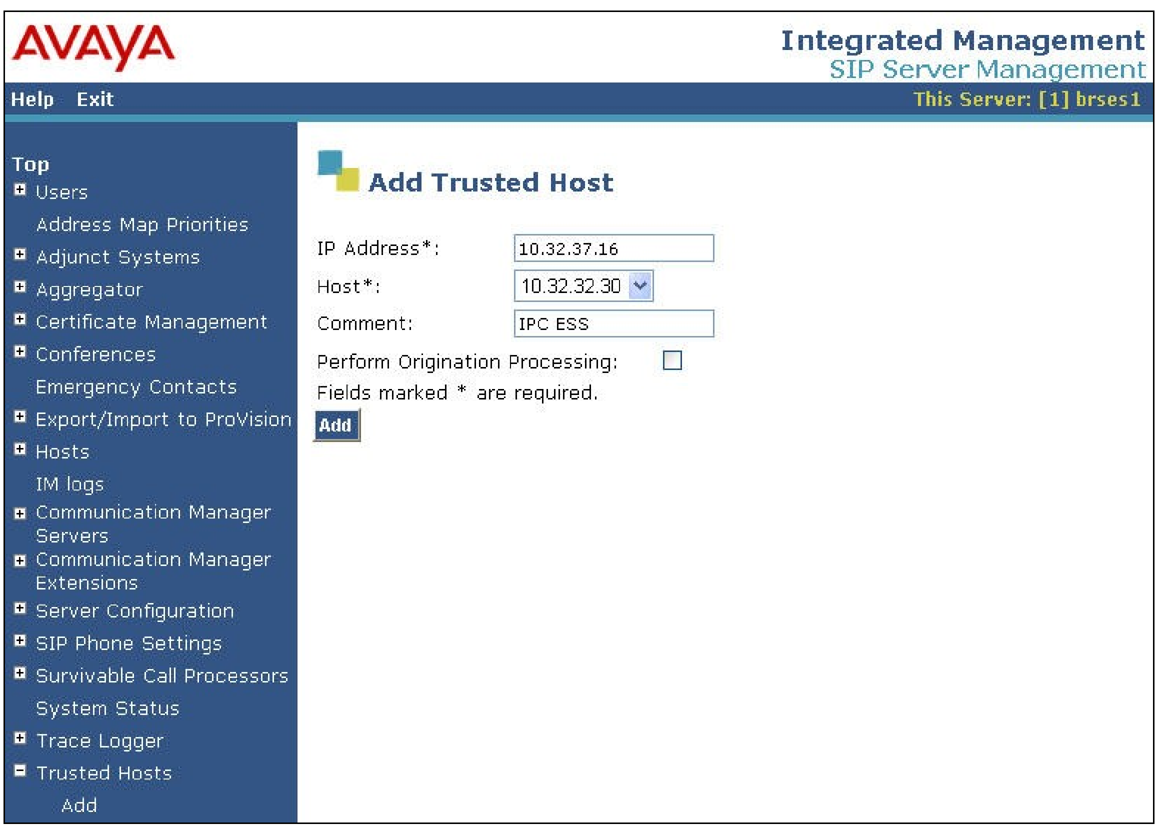
The **List Host Address Map** screen is displayed again, and updated with the newly created address map. Click **Add Another Contact** in the right pane.



In the **Add Host Contact** screen, enter the contact "sip:$(user)@<destination-IP-address> :5060;transport=tcp", where the <destination-IP-address> is the IP address of the IPC ESS server. Avaya SES will substitute "$(user)" with the user portion of the request URI before sending the message.

5.4. Administer Trusted Host

Select **Trusted Hosts > Add** from the left pane. The **Add Trusted Host** screen is displayed. For the **IP Address** field, enter the IP address of the IPC ESS server from **Section 5.3**. Enter a desired description for **Comment**.



6. Configure IPC System Interconnect

This section provides the procedures for configuring IPC System Interconnect. The procedures include the following areas:

- Launch One Management System
- Administer SIP configuration
- Administer routing plan
- Administer wire groups
- Administer trusted host

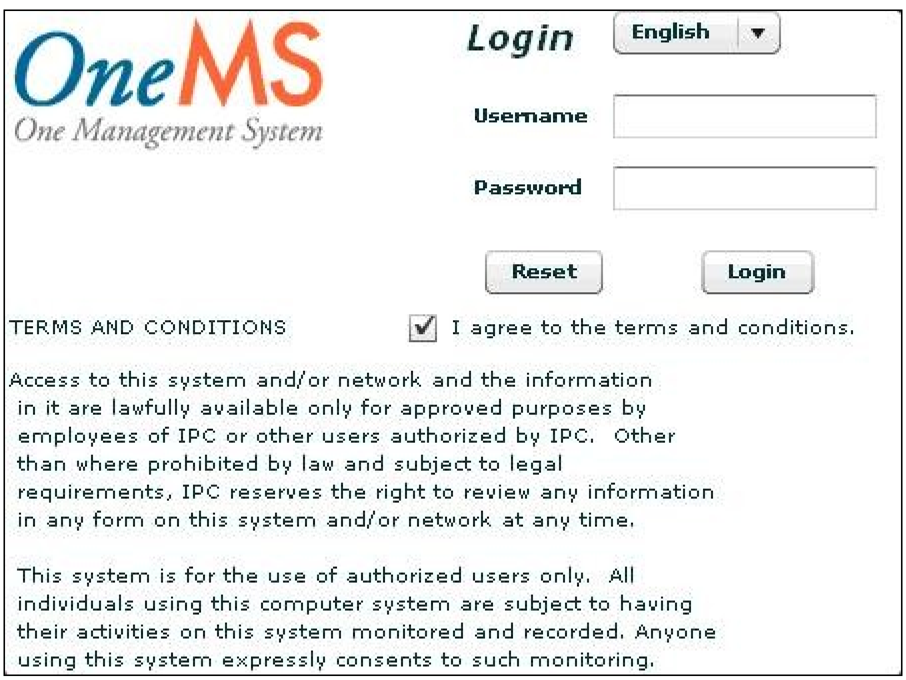
The configuration of System Interconnect is typically performed by IPC installation technicians. The procedural steps are presented in these Application Notes for informational purposes.

6.1. Launch One Management System

Access the One Management System web interface by using the URL "http://ip-address/oneview" in an Internet browser window, where "ip-address" is the IP address of IPC System Center. Log in using the appropriate credentials.

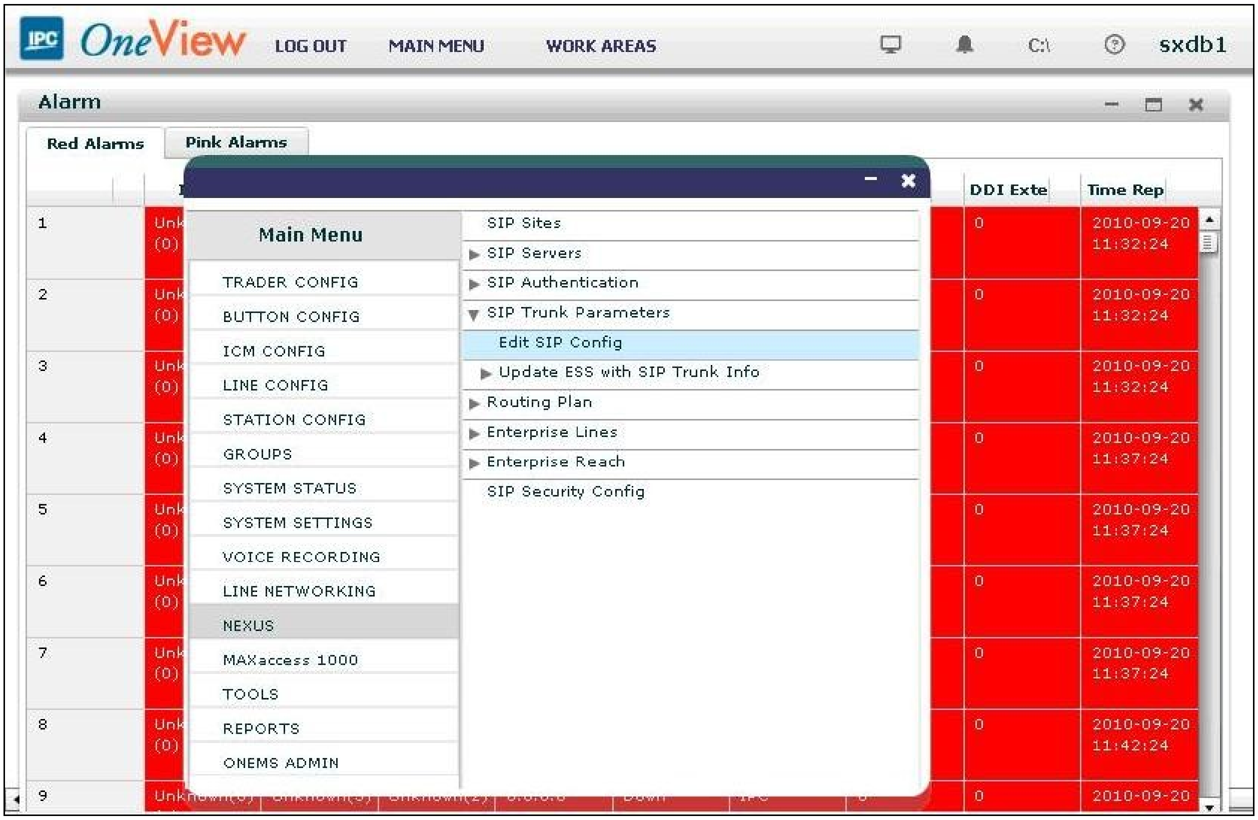
The **Login** screen is displayed. Enter the appropriate credentials. Check **I agree to the terms and conditions**, and click **Login**.

The **License Login** screen is displayed next (not shown). Enter the appropriate password and click **Login**. In the subsequent **Login Information** screen (not shown), click **Continue**.



6.2. Administer SIP Configuration

The screen below is displayed next, with the **Main Menu** screen in the forefront. Select **NEXUS > SIP Trunk Parameters > Edit SIP Config**, as shown below.

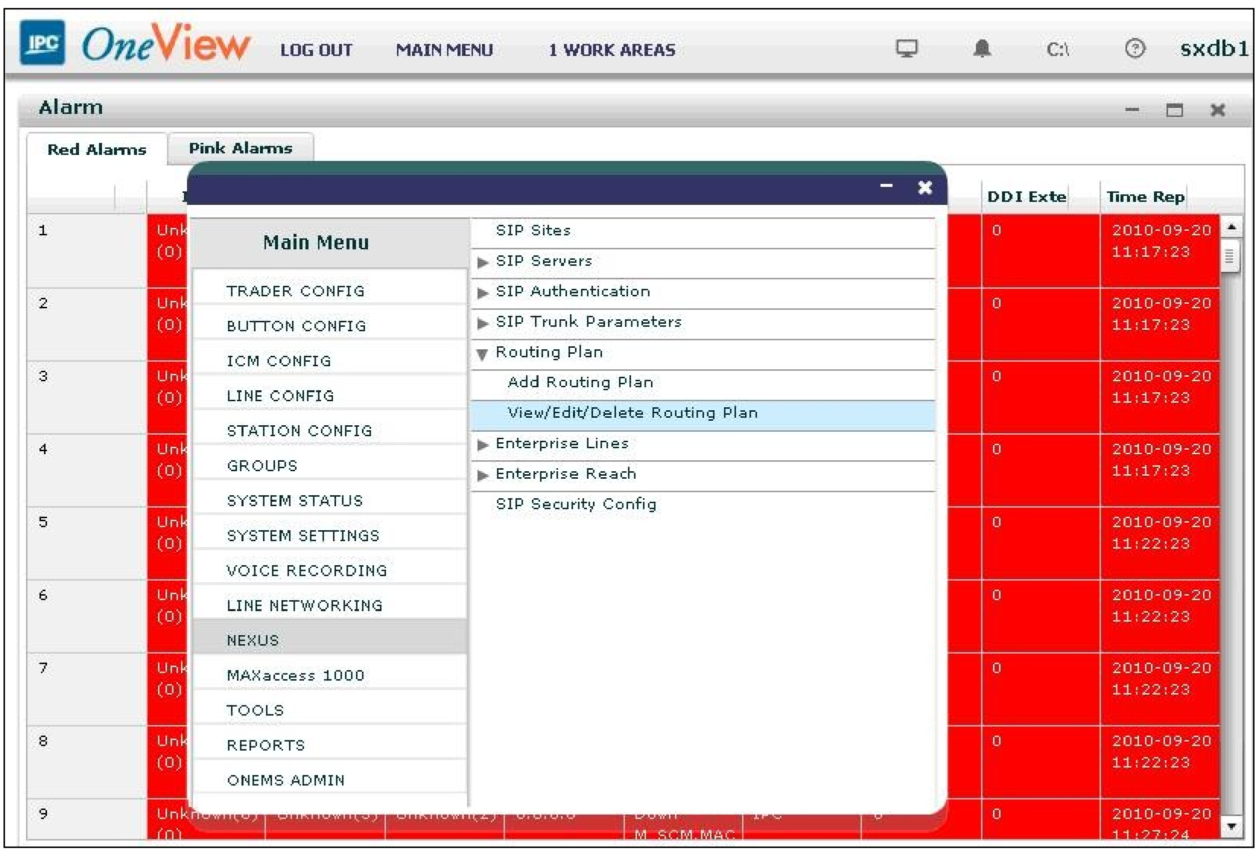


The **Edit SIP Config** screen is displayed. For **DDI Group ID/ DDI Group Name**, select the relevant SIP trunk card number from the drop-down list, in this case “5”. Click **Submit**.

The **Edit SIP Config** screen is updated with the located **DDI Group ID** entry. Double click on the **Outbound URL** field corresponding to the located entry, and enter the SIP domain from **Section 4.5**. IPC will use this SIP domain in the SIP "From" and "To" headers.

6.3. Administer Routing Plan

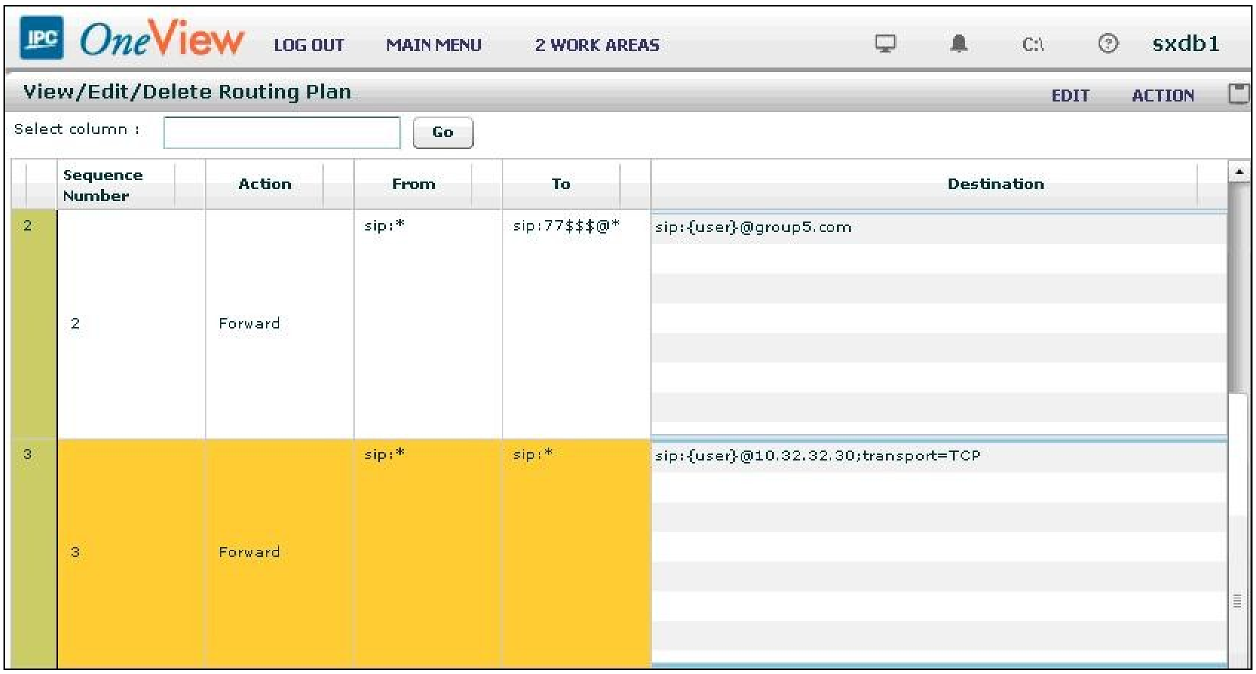
Select **MAIN MENU** from the top menu to display the **Main Menu** screen. Select **NEXUS > Routing Plan > View/Edit/Delete Routing Plan**, as shown below. Click **Submit** in the subsequent screen (not shown) to search for all routing plans.



The **View/Edit/Delete Routing Plan** screen is displayed. Follow [3] to add two routing entries shown below.

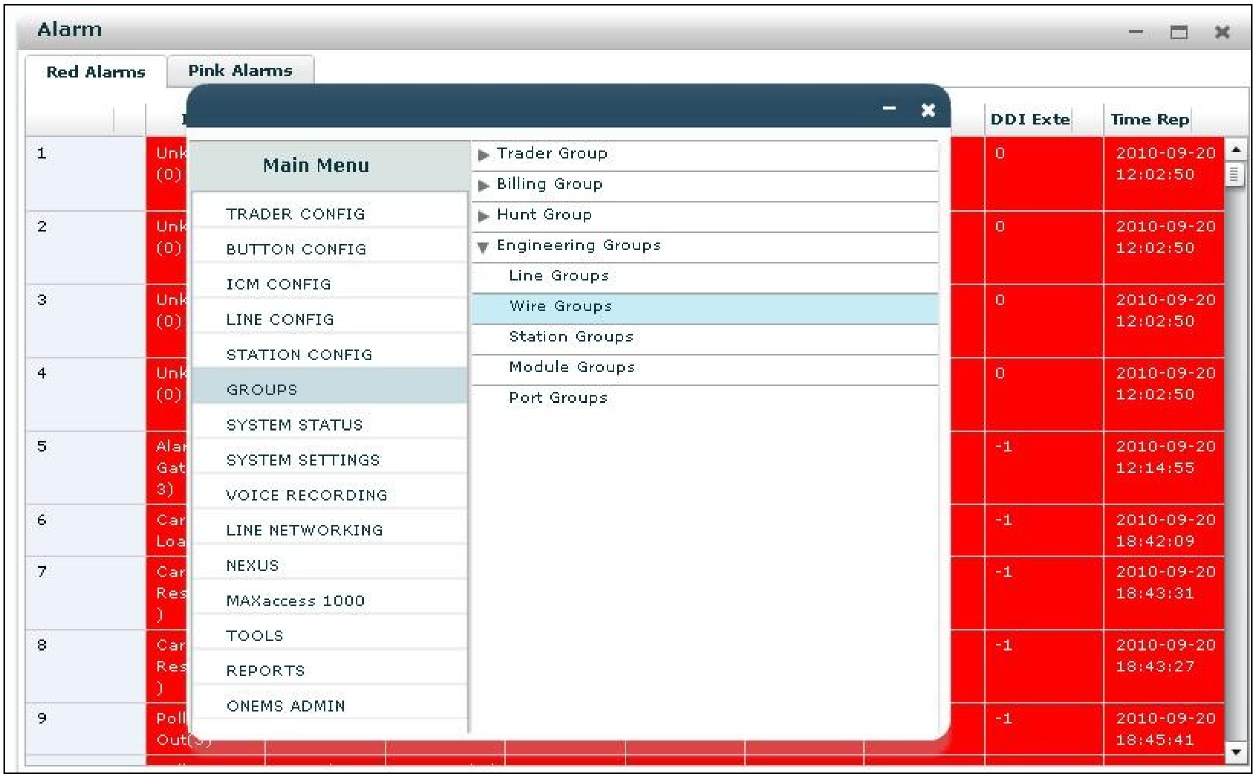
The entry with **Sequence Number 2** was used for routing of inbound calls to IPC. Note that the **Destination** URL contains the internal default value for the SIP trunk card, in this case “group5.com”.

The entry with **Sequence Number 3** was used for routing of outbound calls to Avaya SES. Note the **Destination** URL includes the IP address of Avaya SES, and the transport method from **Section 5.3**.

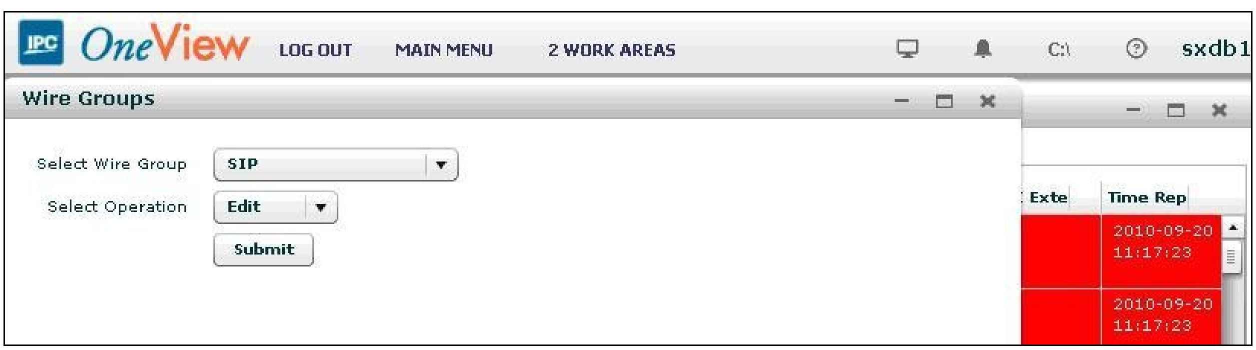


6.4. Administer Wire Groups

Select **MAIN MENU** from the top menu to display the **Main Menu** screen. Select **GROUPS > Engineering Groups > Wire Groups**, as shown below.

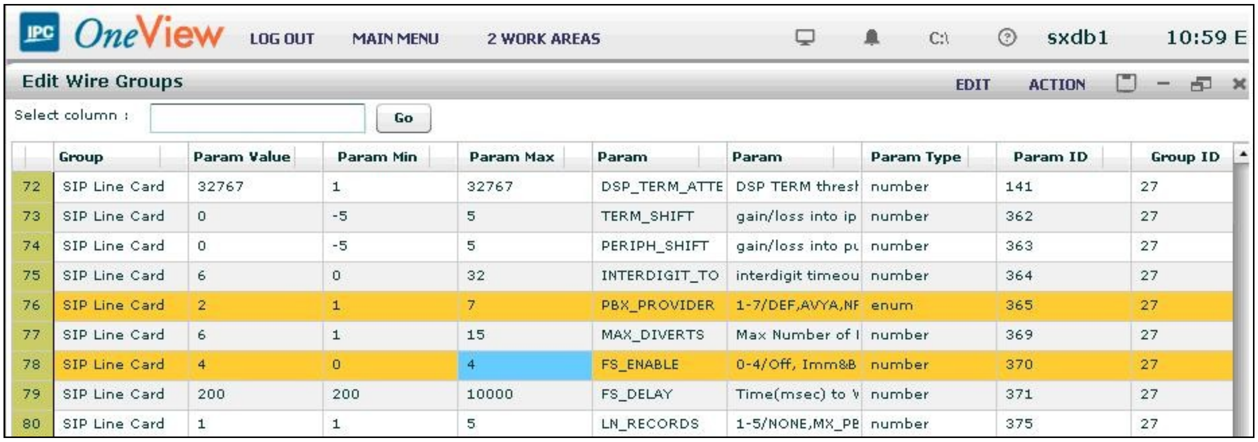


The **Wire Groups** screen is displayed next. Select "SIP" from the **Select Wire Group** drop-down list, and "Edit" from the **Select Operation** drop-down list, as shown below.



The **Edit Wire Groups** screen is displayed. Scroll down the screen as necessary to locate the entry with **Param ID** of “365”. Double click on the corresponding **Param Value** field, and enter “2” to denote Avaya as the PBX provider.

Locate the entry with **Param ID** of “370”. Double click on the corresponding **Param Value** field, and enter “4” to enable Forward Switching.



	Group	Param Value	Param Min	Param Max	Param	Param	Param Type	Param ID	Group ID
72	SIP Line Card	32767	1	32767	DSP_TERM_ATTE	DSP TERM thresh	number	141	27
73	SIP Line Card	0	-5	5	TERM_SHIFT	gain/loss into ip	number	362	27
74	SIP Line Card	0	-5	5	PERIPH_SHIFT	gain/loss into pu	number	363	27
75	SIP Line Card	6	0	32	INTERDIGIT_TO	interdigit timeou	number	364	27
76	SIP Line Card	2	1	7	PBX_PROVIDER	1-7/DEF,AVYA,NF	enum	365	27
77	SIP Line Card	6	1	15	MAX_DIVERTS	Max Number of I	number	369	27
78	SIP Line Card	4	0	4	FS_ENABLE	0-4/Off, Imm&B	number	370	27
79	SIP Line Card	200	200	10000	FS_DELAY	Time(msec) to V	number	371	27
80	SIP Line Card	1	1	5	LN_RECORDS	1-5/NONE,MX_PE	number	375	27

Scroll down the screen as necessary to locate the entry with **Param ID** of “661”. Double click on the corresponding **Param Value** field, and enter “1” to activate detection for G729.

Locate the entry with **Param ID** of “666”. Double click on the corresponding **Param Value** field, and enter “1” to enable SIP Provisional Acknowledgement (PRACK).

Locate the entry with **Param ID** of “668”. Double click on the corresponding **Param Value** field, and enter “0” to disable SIP Remote Party ID (RPI).

Follow [3] to reboot the SIP trunk card.

	Group	Param Value	Param Min	Param Max	Param	Param	Param Type	Param ID	Group ID
95	SIP Line Card	1209	0	3000	SPLSHTONELO_F	Splash tone LO f	number	656	27
96	SIP Line Card	1477	0	3000	SPLSHTONEHI_FI	Splash tone HI f	number	657	27
97	SIP Line Card	1400	0	3000	RECWARNTONE_	Record warning f	number	658	27
98	SIP Line Card	0	0	10000	MRD Ringback T	Ringback Tone D	number	659	27
99	SIP Line Card	1	0	1	VAD	Voice Activity De	number	661	27
100	SIP Line Card	0	0	1	MWI Subscribe	Send MWI Subsc	number	663	27
101	SIP Line Card	0	0	1	SIP Divert	HistoryInfo = 0,	number	664	27
102	SIP Line Card	1	0	1	SIP PRACK	Enable SIP Provi	number	666	27
103	SIP Line Card	1	0	1	SIP PAI	Enable SIP P-As:	number	667	27
104	SIP Line Card	0	0	1	SIP RPID	Enable SIP Rem	number	668	27
105	SIP Line Card	0	0	1	AEC_Enable	Enable AEC Cont	number	669	27
106	SIP Line Card	0	-3	3	AEC_Control	AEC Aggression	number	670	27

6.5. Administer Trusted Host

From the Linux shell of the ESS server, navigate to the **/usr/local/SipProxy**/ directory, and issue the command shown below with the "-add" option to add Avaya SES as a trusted host. Note that 10.32.32.30 is the IP address of Avaya SES.

The same command can be used with the "-view" option to make certain Avaya SES is displayed as a trusted host.

```
[root@esshost ~]# cd /usr/local/SipProxy/
[root@esshost SipProxy]# ./trusted_hosts.pl -add=10.32.32.30

[root@esshost SipProxy]# ./trusted_hosts.pl -view
ip_address      last_modified
10.32.32.30     2010-09-21 16:48:09
```

7. General Test Approach and Test Results

The feature test cases were performed manually. Calls were manually established among IPC turret users with Avaya SIP, Avaya H.323, Avaya Digital, and/or PSTN users. Call controls were performed from the various users to verify the call scenarios.

The serviceability test cases were performed manually by disconnecting and reconnecting the LAN cables to the IPC ESS and IPC System Center servers.

All test cases were executed and passed.

8. Verification Steps

This section provides the tests that can be performed to verify proper configuration of Avaya Aura™ Communication Manager, Avaya Aura™ SIP Enablement Services, and IPC System Interconnect.

8.1. Verify Avaya Aura™ Communication Manager

From the SAT interface, verify the status of the SIP trunk groups by using the "status trunk n" command, where "n" is the trunk group number administered in **Section 4.3**. Verify that all trunks are in the "in-service/idle" state as shown below.

```
status trunk 5

                             TRUNK GROUP STATUS

Member   Port     Service State      Mtce Connected Ports
                                     Busy

0005/001 T00083   in-service/idle    no
0005/002 T00084   in-service/idle    no
0005/003 T00085   in-service/idle    no
0005/004 T00086   in-service/idle    no
0005/005 T00087   in-service/idle    no
0005/006 T00082   in-service/idle    no
0005/007 T00088   in-service/idle    no
0005/008 T00089   in-service/idle    no
0005/009 T00090   in-service/idle    no
0005/010 T00091   in-service/idle    no
```

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 4.4**. Verify that the signaling group is "in-service" as indicated in the **Group State** field shown below.

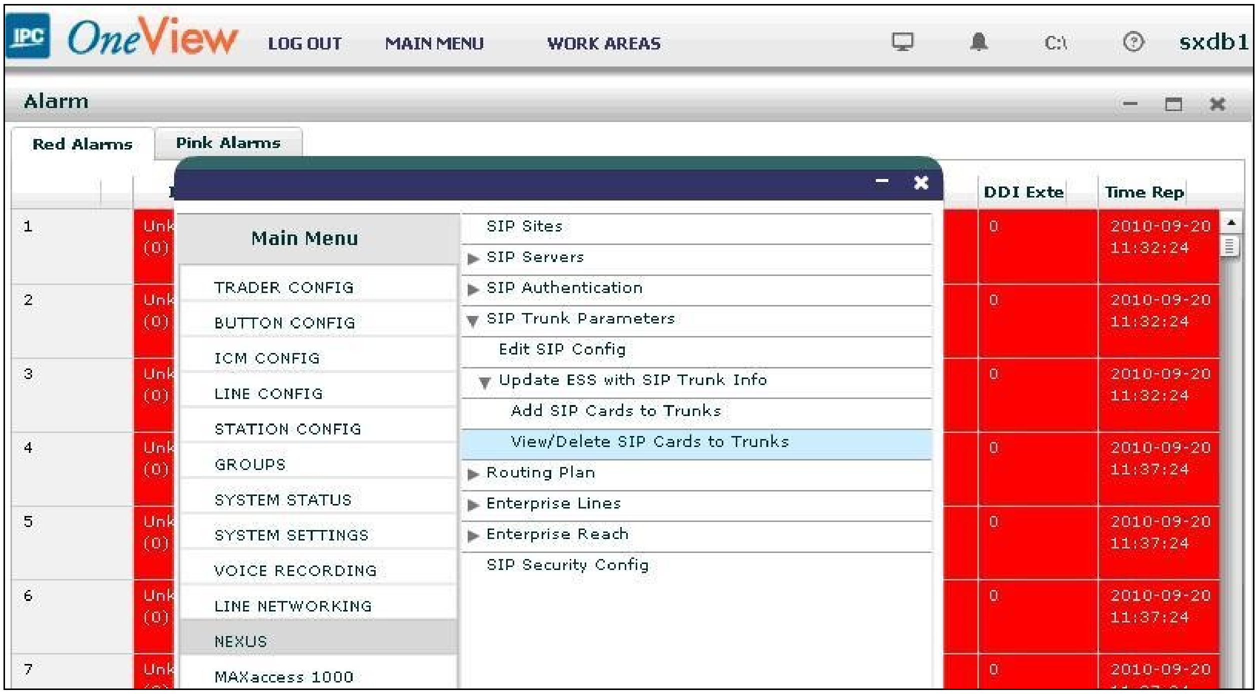
```
status signaling-group 5
                         STATUS SIGNALING GROUP

        Group ID: 5                             Active NCA-TSC Count: 0
      Group Type: sip                            Active CA-TSC Count: 0
  Signaling Type: facility associated signaling
     Group State: in-service
```

8.2. Verify Avaya Aura^{TM} SIP Enablement Services

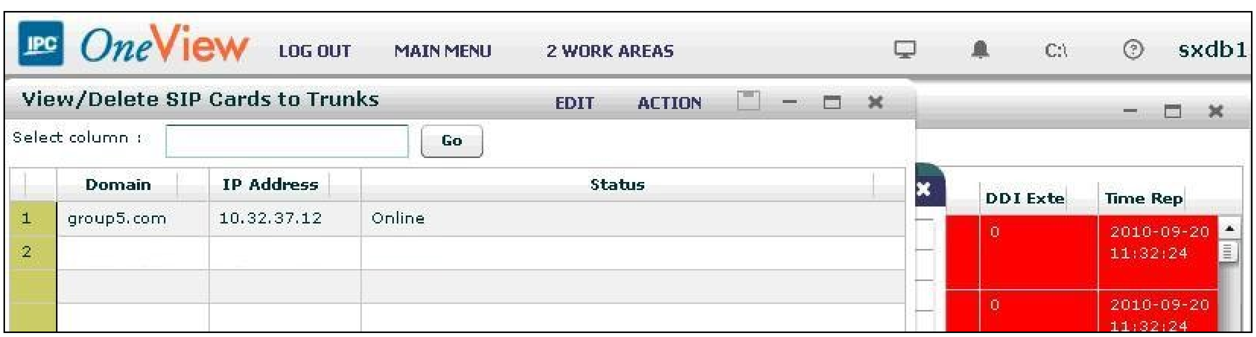
From the SES web interface, select **Trusted Hosts > List** from the left pane, to display the **List Trusted Hosts** screen. Verify that IPC ESS is listed as a trusted host.

8.3. Verify IPC System Interconnect

From the One Management System web interface, select **MAIN MENU** from the top menu to display the **Main Menu** screen. Select **NEXUS > SIP Trunk Parameters > Update ESS with SIP Trunk Info > View/Delete SIP Cards to Trunks**, as shown below.



The **View/Delete SIP Cards to Trunks** screen is displayed. Verify that there is an entry that corresponds to SIP card number 5. Verify that the **Status** is "Online", as shown below.



9. Conclusion

These Application Notes describe the configuration steps required for IPC System Interconnect 16.1 to successfully interoperate with Avaya Aura™ Communication Manager 5.2.1 using Avaya Aura™ SIP Enablement Services 5.2.1. All feature and serviceability test cases were completed.

10. Additional References

This section references the product documentation relevant to these Application Notes.

1. *Administrator Guide for Avaya Aura™ Communication Manager*, Document 03-300509, Issue 8.0, Release 5.2, May 2009, available at http://support.avaya.com.

2. *Installing, Administering, Maintaining, and Troubleshooting Avaya Aura™ SIP Enablement Services*, Document ID 03-600768, Issue 8.0, November 2009, available at http://support.avaya.com.

3. *Nexus Suite 2.0 SP1 Patch11 or Higher Deployment Guide*, Part Number B02200161, Revision Number 01, upon request to IPC Support.

Please e-mail any questions or comments pertaining to these Application Notes along with the full title name and filename, located in the lower right corner, directly to the Avaya DevConnect Program at devconnect@avaya.com.