



Avaya Solution & Interoperability Test Lab

Application Notes for IPC System Interconnect 16.01 with Avaya Aura® Communication Manager 6.0.1 and Avaya Aura® Session Manager 6.1 using SIP Trunks – Issue 1.0

Abstract

These Application Notes describe the configuration steps required for IPC System Interconnect 16.01 to interoperate with Avaya Aura® Communication Manager 6.0.1 and Avaya Aura® Session Manager 6.1 using SIP trunks.

IPC System Interconnect is a trading communication solution. In the compliance testing, IPC System Interconnect used SIP trunks to Avaya Aura® Session Manager, for turret users on IPC to reach users on Avaya Aura® 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 16.01 to interoperate with Avaya Aura® Communication Manager 6.0.1 and Avaya Aura® Session Manager 6.1 using SIP trunks.

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

2. 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, 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 connection to the IPC ESS server.

2.1. Interoperability Compliance Testing

The interoperability compliance test included feature and serviceability testing.

The feature testing included basic call, display, G.711, G.729, 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 LAN connection to IPC System Interconnect.

2.2. Test Results

All test cases were executed and verified. The one observation from the compliance testing is that IPC does not support interpretation of DMTF digits from Avaya endpoints, so the DTMF tests only covered the Avaya interpretation of DMTF digits from the IPC turrets.

2.3. Support

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

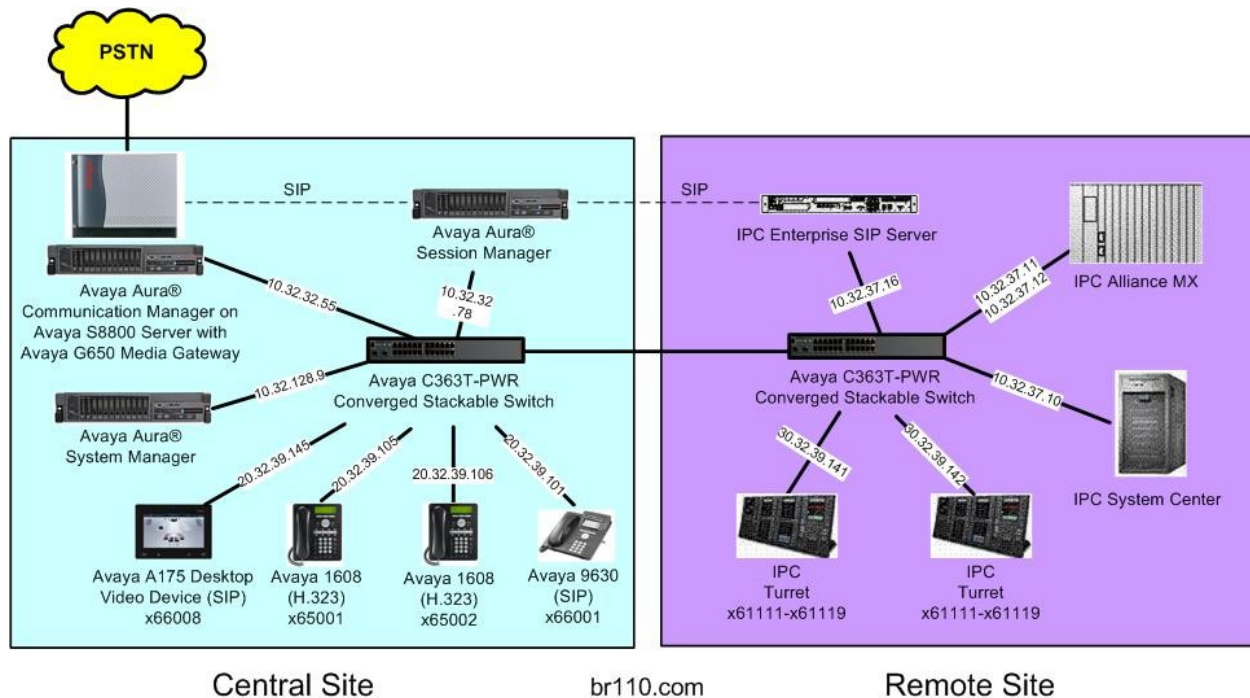
- **Phone:** (800) NEEDIPC, (203) 339-7800
- **Email:** systems.support@ipc.com

3. 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® Session Manager, to reach users on Avaya Aura® Communication Manager and on the PSTN. 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 (65xxx-66xxx), and IPC turret users at the Remote site (61xxx).

The configuration of Avaya Aura® Session Manager is performed via the web interface of Avaya Aura® System Manager. The detailed administration of basic connectivity between Avaya Aura® Communication Manager, Avaya Aura® System Manager, and Avaya Aura® Session Manager is not the focus of these Application Notes and will not be described.



4. Equipment and Software Validated

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

Equipment	Software
Avaya Aura® Communication Manager on Avaya S8800 Server	6.0.1 SP2 with special patch 18993 (R016x.00.1.510.1-18993)
Avaya G650 Media Gateway <ul style="list-style-type: none">TN799DP C-LAN Circuit PackTN2302AP IP Media Processor	HW01 FW038 HW20 FW122
Avaya Aura® Session Manager	6.1 SP2
Avaya Aura® System Manager	6.1 SP2
Avaya 1608 IP Telephone (H.323)	1.3
Avaya 9630 IP Telephone (SIP)	2.6.4
Avaya A175 Desktop Video Device (SIP)	1.0.2
IPC System Interconnect <ul style="list-style-type: none">Alliance MXEnterprise SIP ServerSystem Center<ul style="list-style-type: none">SIPX Line CardTurrets	SipProxy-2.00.01-13 16.01.01.04.0005 16.01.01.04.0005 16.01.01.04.0005 16.01.01.04.0005 16.01.01.04.0005

5. Configure Avaya Aura® Communication Manager

This section provides the procedures for configuring 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 private 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.

5.1. 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:	12000		6
	Maximum Concurrently Registered IP Stations:	18000		0
	Maximum Administered Remote Office Trunks:	12000		0
	Maximum Concurrently Registered Remote Office Stations:	18000		0
	Maximum Concurrently Registered IP eCons:	414		0
	Max Concur Registered Unauthenticated H.323 Stations:	100		0
	Maximum Video Capable Stations:	18000		1
	Maximum Video Capable IP Softphones:	18000		0
	Maximum Administered SIP Trunks:	24000		10
	Maximum Administered Ad-hoc Video Conferencing Ports:	24000		0
	Maximum Number of DS1 Boards with Echo Cancellation:	522		0

5.2. 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 19
      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
```

5.3. Administer SIP Trunk Group

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

For **Group Name**, update as desired to reflect the same trunk group used to reach Session Manager 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 SM/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
                                   Member Assignment Method: auto
                                   Signaling Group: 5
                                   Number of Members: 10
```

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

```
change trunk-group 5                                     Page 3 of 21
TRUNK FEATURES
    ACA Assignment? n                Measured: none
                                   Maintenance Tests? y

                                   Numbering Format: private
                                   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 required by IPC.

```
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
```

5.4. 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 5.3**.

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, and the **Far-end Domain** value. Note that **Transport Method** is set to “tcp” for troubleshooting purposes, also note the values of **Near-end Listen Port** and **Far-end Listen Port**, which will be used later.

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

Group Number: 5                      Group Type: sip
IMS Enabled? n                      Transport Method: tcp
Q-SIP? n                                SIP Enabled LSP? n
IP Video? n                          Enforce SIPS URI for SRTP? y
Peer Detection Enabled? y Peer Server: SM

Near-end Node Name: Clan-1           Far-end Node Name: S8800-SM-SIG
Near-end Listen Port: 5060           Far-end Listen Port: 5060
                                     Far-end Network Region: 1
                                     Far-end Secondary Node Name:
Far-end Domain: br110.com

Incoming Dialog Loopbacks: eliminate Bypass If IP Threshold Exceeded? n
DTMF over IP: rtp-payload           RFC 3389 Comfort Noise? n
Direct IP-IP Audio Connections? y
Session Establishment Timer(min): 3   IP Audio Hairpinning? n
Enable Layer 3 Test? y               Initial IP-IP Direct Media? n
H.323 Station Outgoing Direct Media? n Alternate Route Timer(sec): 6
```

5.5. 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 5.4**.

For **Name**, update as desired to reflect the same network region used to reach 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.

```
change ip-network-region 1                                     Page 1 of 20
                                     IP NETWORK REGION

Region: 1
Location: 1      Authoritative Domain: br110.com
Name: Main/IPC
MEDIA PARAMETERS      Intra-region IP-IP Direct Audio: yes
Codec Set: 1          Inter-region IP-IP Direct Audio: yes
UDP Port Min: 2048    IP Audio Hairpinning? n
UDP Port Max: 65535
DIFFSERV/TOS PARAMETERS
Call Control PHB Value: 46
Audio PHB Value: 46
```


5.6. 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 5.5**. 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 (not shown).

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

change ip-codec-set 1

Page1 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
3:			
4:			
5:			
6:			
7:			

5.7. Administer Route Pattern

Use the “change route-pattern n” command, where “n” is the existing route pattern number to reach Session Manager, in this case “5”. For **Pattern Name**, update as desired to reflect the same route pattern used to reach Session Manager 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 SM/IPC	
SCCAN? n												Secure SIP? n	
Grp	FRL	NPA	Pfx	Hop	Toll	No.	Inserted					DCS/	IXC
No			Mrk	Lmt	List	Del	Digits					QSIG	
												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	

5.8. Administer Private Numbering

Use the “change private-numbering 0” command, to define the calling party number to send to IPC. Add an entry for the trunk group defined in **Section 5.3**. 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 private-numbering 0					Page 1 of 2
NUMBERING - PRIVATE FORMAT					
Ext	Ext	Trk	Private	Total	
Len	Code	Grp(s)	Prefix	Len	
5	6	5		5	Total Administered: 1
					Maximum Entries: 540

5.9. Administer Uniform Dial Plan

This section provides a sample AAR routing used for routing calls with dialed digits 61xxx 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 61xxx, 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	
61	5	0		aar n	

5.10. Administer AAR Analysis

Use the “change aar analysis 0” command, and add an entry to route calls to 61xxx. In the example shown below, calls with digits 61xxx will be routed using route pattern “5” from **Section 5.7**. Set the **Call Type** to “unku”, to prevent “+” being added as a prefix.

change aar analysis 0					Page 1 of 2
AAR DIGIT ANALYSIS TABLE					
Location: all					Percent Full: 2
	Dialed	Total	Route	Call	Node
	String	Min Max	Pattern	Type	Num
61		5 5	5	unku	
					ANI
					Reqd
					n

5.11. 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 “10”. Navigate to **Page 3**.

For **Modify Tandem Calling Number**, enter “tandem-cpn-form” to allow for the calling party number from IPC to be modified.

change trunk-group 10		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: y	Send Calling Number: y	
Used for DCS? n		Send EMU Visitor CPN? n	
Suppress # Outpulsing? n	Format: public		
Outgoing Channel ID Encoding: preferred	UII IE Treatment: service-provider		
		Replace Restricted Numbers? n	
		Replace Unavailable Numbers? n	
		Send Connected Number: n	
Network Call Redirection: none		Hold/Unhold Notifications? n	
Send UII IE? y	Modify Tandem Calling Number: tandem-cpn-form		
Send UCID? n			
Send Codeset 6/7 LAI IE? y		Dsl 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		
DSN Term? n			

5.12. 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 6 and routed to trunk group 10 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	6	10		90884	pub-unk		

6. Configure Avaya Aura® Session Manager

This section provides the procedures for configuring Avaya Aura® Session Manager. The procedures include the following areas:

- Launch System Manager
- Administer locations
- Administer adaptations
- Administer SIP entities
- Administer entity links
- Administer routing policies
- Administer dial patterns

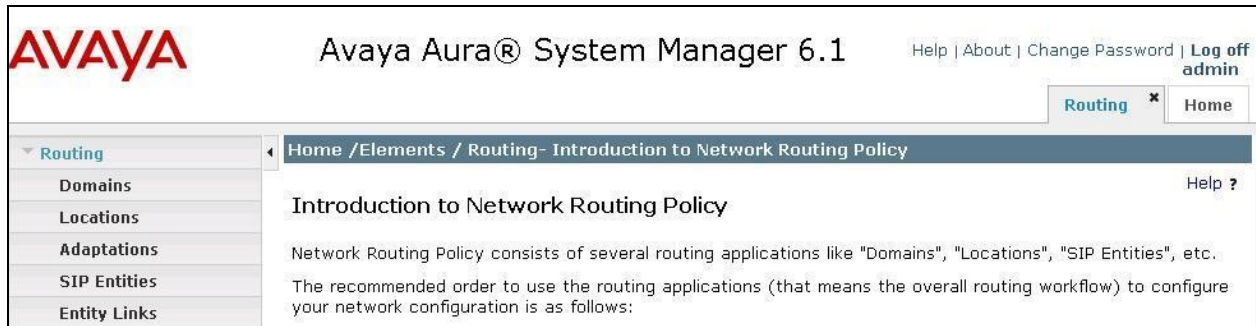
6.1. Launch System Manager

Access the System Manager web interface by using the URL “https://ip-address” in an Internet browser window, where “ip-address” is the IP address of the System Manager server. Log in using the appropriate credentials.

The screenshot shows the Avaya Aura® System Manager 6.1 login interface. At the top, the Avaya logo is on the left and the title "Avaya Aura® System Manager 6.1" is on the right. Below the title bar is a red navigation bar with the text "Home / Log On". The main heading is "Log On". On the left side, there is a box containing the following text: "Recommended access to System Manager is via FQDN." followed by a link "Go to central login for Single Sign-On". Below this, it says "If IP address access is your only option, then note that authentication will fail in the following cases:" followed by a bulleted list: "• First time login with 'admin' account" and "• Expired/Reset passwords". On the right side, there are two input fields: "User ID:" and "Password:". At the bottom right, there are two buttons: "Log On" and "Cancel". A link "Change Password" is located at the bottom right of the page.

6.2. Administer Locations

In the subsequent screen (not shown), select **Elements > Routing** to display the **Introduction to Network Routing Policy** screen below. Select **Routing > Locations** from the left pane, and click **New** in the subsequent screen (not shown) to add a new location for IPC.



AVAYA Avaya Aura® System Manager 6.1 Help | About | Change Password | Log off admin

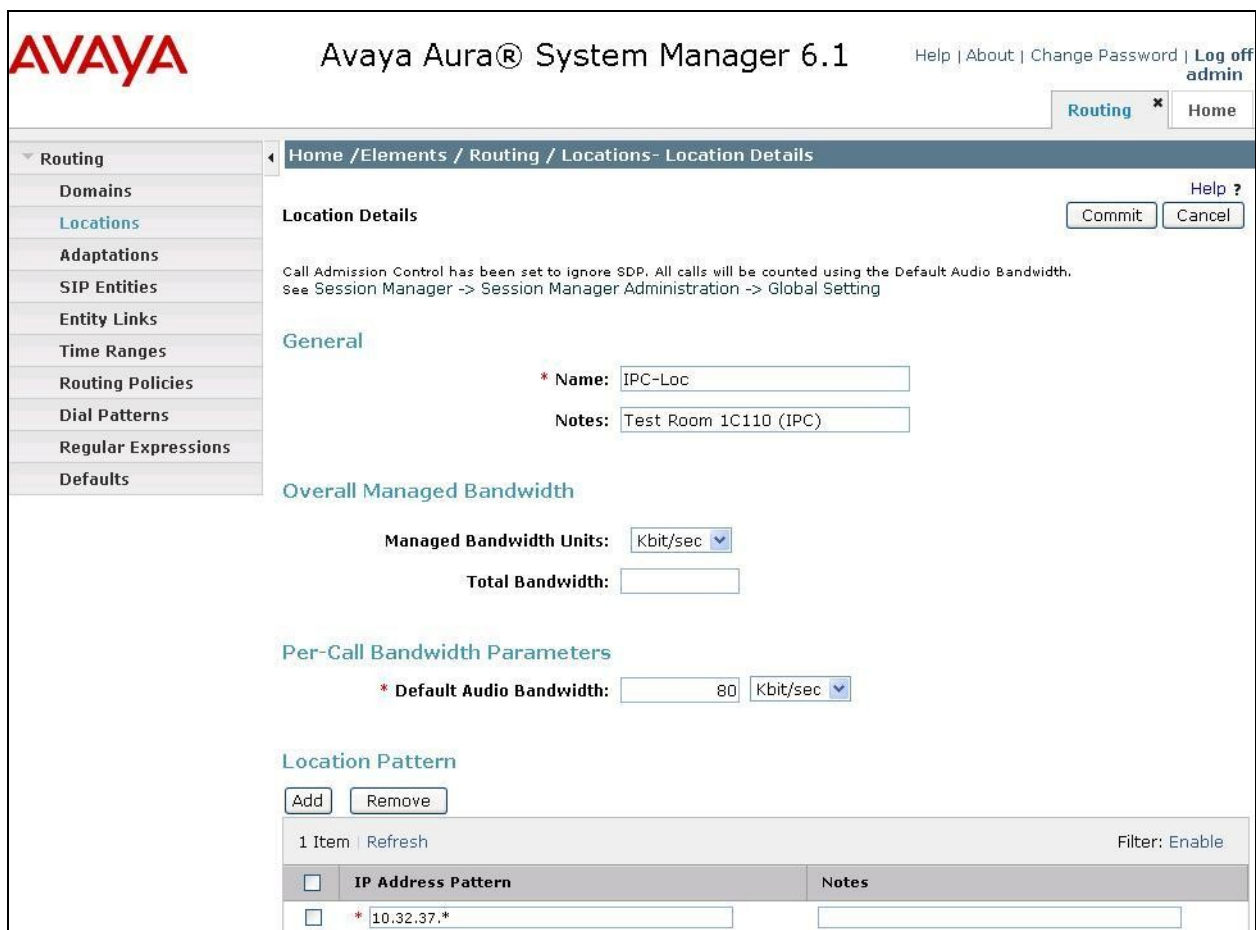
Routing x Home

Home /Elements / Routing- Introduction to Network Routing Policy Help ?

Introduction to Network Routing Policy

Network Routing Policy consists of several routing applications like "Domains", "Locations", "SIP Entities", etc.
The recommended order to use the routing applications (that means the overall routing workflow) to configure your network configuration is as follows:

The **Location Details** screen is displayed. In the **General** sub-section, enter a descriptive **Name** and optional **Notes**. In the **Location Pattern** sub-section, click **Add** and enter the applicable **IP Address Pattern**, as shown below. Retain the default values in the remaining fields.



AVAYA Avaya Aura® System Manager 6.1 Help | About | Change Password | Log off admin

Routing x Home

Home /Elements / Routing / Locations- Location Details Help ?

Location Details

Call Admission Control has been set to ignore SDP. All calls will be counted using the Default Audio Bandwidth.
See Session Manager -> Session Manager Administration -> Global Setting

Commit Cancel

General

* Name: IPC-Loc
Notes: Test Room 1C110 (IPC)

Overall Managed Bandwidth

Managed Bandwidth Units: Kbit/sec
Total Bandwidth:

Per-Call Bandwidth Parameters

* Default Audio Bandwidth: 80 Kbit/sec

Location Pattern

Add Remove

1 Item Refresh Filter: Enable

<input type="checkbox"/>	IP Address Pattern	Notes
<input type="checkbox"/>	* 10.32.37.*	

6.3. Administer Adaptations

Select **Routing > Adaptations** from the left pane, and click **New** in the subsequent screen (not shown) to add a new adaptation for IPC.

The **Adaptation Details** screen is displayed. In the **General** sub-section, enter a descriptive **Adaptation name**. For **Module name**, select “DigitConversionAdapter”.

For **Module parameter**, enter “osrcd=br110.com odstcd=br110.com iosrcd=br110.com iodstd=br110.com”, where “br110.com” is the applicable domain. This will set the source and destination domains for all incoming and outgoing calls for IPC.

AVAYA Avaya Aura® System Manager 6.1 [Help](#) | [About](#) | [Change Password](#) | [Log off admin](#)

[Routing](#) [Home](#)

Home / Elements / Routing / Adaptations - Adaptation Details

Adaptation Details [Help ?](#) [Commit](#) [Cancel](#)

General

* **Adaptation name:**

Module name:

Module parameter:

Egress URI Parameters:

Notes:

Digit Conversion for Incoming Calls to SM

[Add](#) [Remove](#)

0 Items | [Refresh](#) [Filter: Enable](#)

<input type="checkbox"/>	Matching Pattern	Min	Max	Phone Context	Delete Digits	Insert Digits	Address to modify	Notes
--------------------------	------------------	-----	-----	---------------	---------------	---------------	-------------------	-------

Digit Conversion for Outgoing Calls from SM

[Add](#) [Remove](#)

0 Items | [Refresh](#) [Filter: Enable](#)

<input type="checkbox"/>	Matching Pattern	Min	Max	Phone Context	Delete Digits	Insert Digits	Address to modify	Notes
--------------------------	------------------	-----	-----	---------------	---------------	---------------	-------------------	-------

6.4. Administer SIP Entities

Select **Routing > SIP Entities** from the left pane, and click **New** in the subsequent screen (not shown) to add a new SIP entity for IPC.

The **SIP Entity Details** screen is displayed. Enter the following values for the specified fields, and retain the default values for the remaining fields.

- **Name:** A descriptive name.
- **FQDN or IP Address:** The IP address of the IPC ESS server.
- **Type:** “Other”
- **Adaptation:** Select the IPC adaptation name from **Section 6.3**.
- **Location:** Select the IPC location name from **Section 6.2**.
- **Time Zone:** Select the applicable time zone.

AVAYA Avaya Aura® System Manager 6.1 [Help](#) | [About](#) | [Change Password](#) | [Log off admin](#)

[Routing](#) × [Home](#)

Home / Elements / Routing / SIP Entities - SIP Entity Details

SIP Entity Details [Help ?](#)

[Commit](#) [Cancel](#)

General

* **Name:**

* **FQDN or IP Address:**

Type:

Notes:

Adaptation:

Location:

Time Zone:

Override Port & Transport with DNS SRV: ☐

* **SIP Timer B/F (in seconds):**

Credential name:

Call Detail Recording:

SIP Link Monitoring

SIP Link Monitoring:

6.5. Administer Entity Links

Select **Routing > Entity Links** from the left pane, and click **New** in the subsequent screen (not shown) to add a new entity link for IPC.

The **Entity Links** screen is displayed. Enter the following values for the specified fields, and retain the default values for the remaining fields.

- **Name:** A descriptive name.
- **SIP Entity 1:** The Session Manager entity name, in this case “BR110-SM”.
- **Protocol:** The signaling group transport method from **Section 5.4**.
- **Port:** The signaling group listen port number from **Section 5.4**.
- **SIP Entity 2:** The IPC entity name from **Section 6.4**.
- **Port:** The signaling group listen port number from **Section 5.4**.
- **Trusted:** Retain the check.

The screenshot shows the Avaya Aura® System Manager 6.1 interface. The left navigation pane is expanded to 'Routing', and 'Entity Links' is selected. The main content area shows the 'Entity Links' configuration screen. At the top, there is a breadcrumb trail: 'Home / Elements / Routing / Entity Links - Entity Links'. Below this, there are 'Commit' and 'Cancel' buttons, and a 'Help ?' link. The main area contains a table with one item. The table has columns: Name, SIP Entity 1, Protocol, Port, SIP Entity 2, Port, and Trusted. The values in the table are: Name: BR110-SM2IPC, SIP Entity 1: BR110-SM, Protocol: TCP, Port: 5060, SIP Entity 2: IPC-ESS, Port: 5060, and Trusted: checked. Below the table, there is a 'Filter: Enable' link and a 'Refresh' link. At the bottom, there is a '* Input Required' message and 'Commit' and 'Cancel' buttons.

Name	SIP Entity 1	Protocol	Port	SIP Entity 2	Port	Trusted
* BR110-SM2IPC	* BR110-SM	TCP	* 5060	* IPC-ESS	* 5060	<input checked="" type="checkbox"/>

6.6. Administer Routing Policies

Select **Routing > Routing Policies** from the left pane, and click **New** in the subsequent screen (not shown) to add a new routing policy for IPC.

The **Routing Policy Details** screen is displayed. In the **General** sub-section, enter a descriptive **Name**.

In the **SIP Entity as Destination** sub-section, click **Select** and select the IPC entity name from **Section 6.4** in the listing (not shown).

Retain the default values in the remaining fields.

AVAYA Avaya Aura® System Manager 6.1 Help | About | Change Password | Log off admin

Routing * Home

Home / Elements / Routing / Routing Policies - Routing Policy Details

Routing Policy Details

General

* Name:

Disabled: ☐

Notes:

SIP Entity as Destination

Select

Name	FQDN or IP Address	Type	Notes
IPC-ESS	10.32.37.16	Other	

Time of Day

Add Remove View Gaps/Overlaps

1 Item | Refresh Filter: Enable

<input type="checkbox"/>	Ranking 1 ▲	Name 2 ▲	Mon	Tue	Wed	Thu	Fri	Sat	Sun	Start Time	End Time	Notes
<input type="checkbox"/>	0	24/7	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	00:00	23:59	Time Range 24/7

Select : All, None

6.7. Administer Dial Patterns

Select **Routing > Dial Patterns** from the left pane, and click **New** in the subsequent screen (not shown) to add a new dial pattern to reach IPC turret users.

The **Dial Pattern Details** screen is displayed. In the **General** sub-section, enter the following values for the specified fields, and retain the default values for the remaining fields.

- **Pattern:** A dial pattern to match.
- **Min:** The minimum number of digits to be matched.
- **Max:** The maximum number of digits to be matched.
- **SIP Domain:** The signaling group domain name from **Section 5.4**.
- **Notes:** Any desired description.

In the **Originating Locations and Routing Policies** sub-section, click **Add** and create a new policy for reaching IPC turret users. In the compliance testing, the policy allowed for call origination from all locations, as shown below. Retain the default values in the remaining fields.

AVAYA Avaya Aura® System Manager 6.1 [Help](#) | [About](#) | [Change Password](#) | [Log off admin](#)

[Routing](#) * [Home](#)

Home / Elements / Routing / Dial Patterns - Dial Pattern Details

Dial Pattern Details [Help ?](#) [Commit](#) [Cancel](#)

General

* **Pattern:**

* **Min:**

* **Max:**

Emergency Call: ☐

SIP Domain: [v](#)

Notes:

Originating Locations and Routing Policies

[Add](#) [Remove](#)

1 Item [Refresh](#) [Filter: Enable](#)

<input type="checkbox"/>	Originating Location Name 1 ▲	Originating Location Notes	Routing Policy Name	Rank 2 ▲	Routing Policy Disabled	Routing Policy Destination	Routing Policy Notes
<input type="checkbox"/>	-ALL-	Any Locations	To-IPC	0	<input type="checkbox"/>	IPC-ESS	

[<](#) [>](#)

Select : All, None

Denied Originating Locations

7. 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.

7.1. 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**.

OneMS
One Management System

Login English ▼

Username

Password

Reset Login

TERMS AND CONDITIONS ☒ I agree to the terms and conditions.

Access to this system and/or network and the information in it are lawfully available only for approved purposes by employees of IPC or other users authorized by IPC. Other than where prohibited by law and subject to legal requirements, IPC reserves the right to review any information in any form on this system and/or network at any time.

This system is for the use of authorized users only. All individuals using this computer system are subject to having their activities on this system monitored and recorded. Anyone using this system expressly consents to such monitoring.

7.2. 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 screenshot shows the IPC OneView interface. At the top, there is a navigation bar with 'LOG OUT', 'MAIN MENU', and '1 WORK AREAS'. Below this, a window titled 'Alarm' is open, displaying a list of alarms. A 'Main Menu' dialog box is overlaid on the alarm list, showing a tree structure of configuration options. The 'NEXUS' option is highlighted, and the 'Edit SIP Config' option is selected. The background alarm list is partially visible, showing columns for 'DDI Ext', 'Time Rep', and 'Time Rep'.

DDI Ext	Time Rep
-1	2011-06-10 09:21:30
-1	2011-06-10 09:21:34
-1	2011-06-10 09:21:34
-1	2011-06-10 09:21:35
-1	2011-06-10 09:21:35
-1	2011-06-10 09:21:35
-1	2011-06-10 09:21:46
-1	2011-06-10 09:22:11
-1	2011-06-10 09:22:13
-1	2011-06-10 09:22:14
-1	2011-06-10 09:22:14

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 screenshot shows the 'Edit SIP Config' screen. It features a label 'DDI Group ID/ DDI Group Name' followed by a dropdown menu showing '5 [?]'. Below the dropdown is a 'Submit' button.

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 5.4**. IPC will use this SIP domain in the SIP “From” and “To” headers.

	DDI Group ID	Outbound URL	Username	Password	Confirm Password	DNS1 IP Address
1	5	br110.com	avaya	*****	*****	

7.3. 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.

	DDI Ext	Time Rep
1	-1	2011-06-10 09:21:30
2	-1	2011-06-10 09:21:34
3	-1	2011-06-10 09:21:34
4	-1	2011-06-10 09:21:35
5	-1	2011-06-10 09:21:35
6	-1	2011-06-10 09:21:35
7	-1	2011-06-10 09:21:46
8	-1	2011-06-10 09:22:11
9	-1	2011-06-10 09:22:13
10	-1	2011-06-10 09:22:14
11	-1	2011-06-10

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

The entry with **Sequence Number 3** 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 4** was used for routing of outbound calls to Session Manager. Note the **Destination** URL includes the IP address of the signaling interface for Session Manager, and the transport method from **Section 5.4**.

Sequence Number	Action	From	To	Destination
3	Forward	sip:*	sip:611\$\$\$@*	sip:{user}@group5.com
4	Forward	sip:*	sip:*	sip:{user}@10.32.32.78;transport=TCP

1-4 of 4 Select page: 1 Count: 100

*Unsaved changes will be lost between page selections.

7.4. 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.

DDI Ext	Time Rep
-1	2011-06-10 09:21:30
-1	2011-06-10 09:21:34
-1	2011-06-10 09:21:34
-1	2011-06-10 09:21:35
-1	2011-06-10 09:21:35
-1	2011-06-10 09:21:46
-1	2011-06-10 09:22:11
-1	2011-06-10 09:22:13
-1	2011-06-10 09:22:14

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.

DDI Ext	Time Rep
-1	2011-06-10 09:21:30
-1	2011-06-10 09:21:34

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
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 l	number	369	27
78	SIP Line Card	4	0	4	FS_ENABLE	0-4/Off, Imm8B	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_PB	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
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 L	number	659	27
99	SIP Line Card	1	0	1	VAD	Voice Activity De	number	661	27
100	SIP Line Card	1	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
107	SIP Line Card	0	0	1	AEC_NR_Filter	Enable AEC Nois	number	671	27

7.5. 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 Session Manager as a trusted host. Note that 10.32.32.78 is the IP address of the signaling interface for Session Manager.

The same command can be used with the “-view” option to make certain Session Manager is displayed as a trusted host.

```
[root@esshost ~]# cd /usr/local/SipProxy/
[root@esshost SipProxy]# ./trusted_hosts.pl -add=10.32.32.78

[root@esshost SipProxy]# ./trusted_hosts.pl -view
ip_address      last_modified
10.32.32.78      2011-06-13 10:13:04
```

8. Verification Steps

This section provides the tests that can be performed to verify proper configuration of Avaya Aura® Communication Manager, Avaya Aura® Session Manager, 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 5.3**. 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 T00045      in-service/idle      no
0005/007 T00046      in-service/idle      no
0005/008 T00047      in-service/idle      no
0005/009 T00048      in-service/idle      no
0005/010 T00049      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 5.4**. 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
      Group Type: sip

      Group State: in-service
```

8.2. Verify Avaya Aura® Session Manager

From the System Manager home page (not shown), select **Elements > Session Manager** to display the **Session Manager Dashboard** screen (not shown). Select **Session Manager > System Status > SIP Entity Monitoring** from the left pane to display the **SIP Entity Link Monitoring Status Summary** screen. Click on the IPC entity name from **Section 6.4**.

The screenshot shows the Avaya Aura® System Manager 6.1 interface. The left navigation pane is expanded to 'System Status' > 'SIP Entity Monitoring'. The main content area displays the 'SIP Entity Link Monitoring Status Summary' page. It includes a 'Run Monitor' button and a table with 3 items. The table has columns: Session Manager Name, Entity Links Down/Total, Entity Links Partially Down, SIP Entities - Monitoring Not Started, and SIP Entities - Not Monitored. The rows are BR110-SM and Dev4 SM. Below the table is a 'Select: All, None' dropdown. Further down, there is a section for 'All Monitored SIP Entities' with another 'Run Monitor' button and a list of 15 items. The list includes SIP Entity Name, BR110-CM, IPC-ESS (circled in red), and mange.

Session Manager Name	Entity Links Down/Total	Entity Links Partially Down	SIP Entities - Monitoring Not Started	SIP Entities - Not Monitored
BR110-SM	1/3	0	0	0
Dev4 SM	1/3	0	0	0

SIP Entity Name
BR110-CM
IPC-ESS
mange

The **SIP Entity, Entity Link Connection Status** screen is displayed. Verify that **Conn. Status** and **Link Status** are “Up”, as shown below.

The screenshot shows the Avaya Aura® System Manager 6.1 interface. The left navigation pane is expanded to 'System Status' > 'SIP Entity Monitoring'. The main content area displays the 'SIP Entity, Entity Link Connection Status' page. It includes a 'Summary View' button and a table with 1 item. The table has columns: Details, Session Manager Name, SIP Entity Resolved IP, Port, Proto., Conn. Status, Reason Code, and Link Status. The row shows details for BR110-SM with a resolved IP of 10.32.37.16, port 5060, TCP protocol, 'Up' connection status, and 'Up' link status.

Details	Session Manager Name	SIP Entity Resolved IP	Port	Proto.	Conn. Status	Reason Code	Link Status
Show	BR110-SM	10.32.37.16	5060	TCP	Up	200 Options received from a non-SIPX UAC	Up

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. Click **Search** in the subsequent screen (not shown) to search for all SIP cards.

The screenshot shows the IPC OneView web interface. The top navigation bar includes "LOG OUT", "MAIN MENU", and "1 WORK AREAS". The "Alarm" section is active, showing "Red Alarms" and "Pink Alarms". A "Main Menu" dropdown is open, displaying options like "SIP Sites", "SIP Servers", "SIP Authentication", "SIP Trunk Parameters", "Edit SIP Config", "Update ESS with SIP Trunk Info", "Add SIP Cards to Trunks", "View/Delete SIP Cards to Trunks", "Routing Plan", "Enterprise Lines", "Enterprise Reach", and "SIP Security Config". The "View/Delete SIP Cards to Trunks" option is highlighted. Below the menu, a table lists SIP cards with columns for "DDI Ext", "Time Rep", and "Status". The table contains 11 rows of data, with the first row showing "1", "Layer2 Link", "Critical", "Attended", "1,2,5,4091", "IPC", "-1", "-1", and "2011-06-10 09:21:30".

	DDI Ext	Time Rep
1	-1	2011-06-10 09:21:30
2	-1	2011-06-10 09:21:34
3	-1	2011-06-10 09:21:34
4	-1	2011-06-10 09:21:35
5	-1	2011-06-10 09:21:35
6	-1	2011-06-10 09:21:35
7	-1	2011-06-10 09:21:46
8	-1	2011-06-10 09:22:11
9	-1	2011-06-10 09:22:13
10	-1	2011-06-10 09:22:14
11	-1	2011-06-10 09:22:14

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.

The screenshot shows the "View/Delete SIP Cards to Trunks" screen. The top navigation bar includes "LOG OUT", "MAIN MENU", and "2 WORK AREAS". The "View/Delete SIP Cards to Trunks" section is active, showing "EDIT" and "ACTION" buttons. A "Select column" dropdown is open, showing "Domain", "IP Address", and "Status". The "Status" column is selected. Below the dropdown, a table lists SIP cards with columns for "Domain", "IP Address", and "Status". The table contains 2 rows of data, with the first row showing "1", "group5.com", "10.32.37.12", and "Online".

	Domain	IP Address	Status
1	group5.com	10.32.37.12	Online
2			

9. Conclusion

These Application Notes describe the configuration steps required for IPC System Interconnect 16.01 to successfully interoperate with Avaya Aura® Communication Manager 6.0.1 and Avaya Aura® Session Manager 6.1 using SIP trunks. All feature and serviceability test cases were completed with an observation noted in **Section 2.2**.

10. Additional References

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

1. *Administering Avaya AuraTM Communication Manager*, Document 03-300509, Issue 6.0, Release 6.0, June 2010, available at <http://support.avaya.com>.
2. *Administering Avaya AuraTM Session Manager*, Document Number 03-603324, Issue 3, Release 6.0, August 2010, 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.

©2012 Avaya Inc. All Rights Reserved.

Avaya and the Avaya Logo are trademarks of Avaya Inc. All trademarks identified by ® and ™ are registered trademarks or trademarks, respectively, of Avaya Inc. All other trademarks are the property of their respective owners. The information provided in these Application Notes is subject to change without notice. The configurations, technical data, and recommendations provided in these Application Notes are believed to be accurate and dependable, but are presented without express or implied warranty. Users are responsible for their application of any products specified in these Application Notes.

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.