



Avaya Solution & Interoperability Test Lab

Application Notes for IPC System Interconnect 15.03 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 15.03 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 turrent 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 15.03 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.

DevConnect Compliance Testing is conducted jointly by Avaya and DevConnect members. The jointly-defined test plan focuses on exercising APIs and/or standards-based interfaces pertinent to the interoperability of the tested products and their functionalities. DevConnect Compliance Testing is not intended to substitute full product performance or feature testing performed by DevConnect members, nor is it to be construed as an endorsement by Avaya of the suitability or completeness of a DevConnect member's solution.

2.2. Test Results

All test cases were executed and verified.

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 “avaya.com” domain was used for Avaya site, and “ipc.com” was used on IPC site.

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 (20xxx), and IPC turret users at the Remote site (332xx).

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.

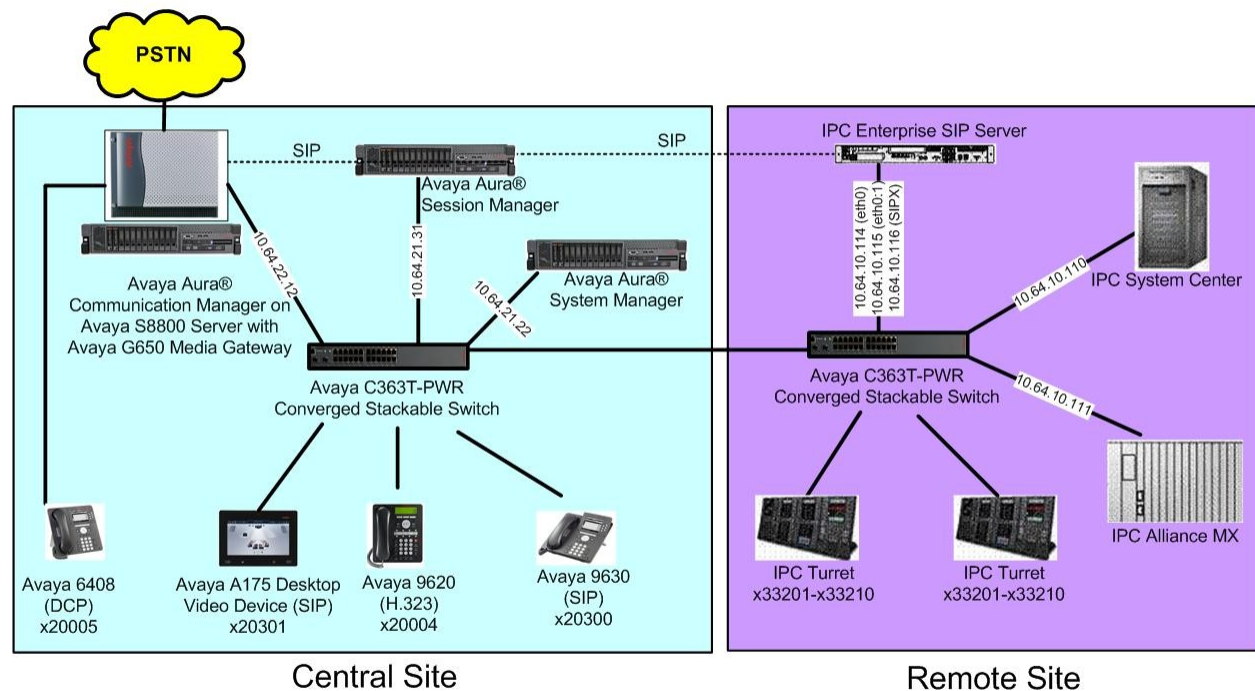


Figure 1: Test Configuration of IPC Alliance

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(R016x.00.1.510.1) with special patch 19823
Avaya G650 Media Gateway <ul style="list-style-type: none">• TN799DP C-LAN Circuit Pack• TN2302AP IP Media Processor• TN464F	HW01 FW038 HW20 FW122 000010
Avaya Aura® Session Manager	6.1.5
Avaya Aura® System Manager	6.1.5
Avaya 9620 IP Telephone (H.323)	3.1
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 MX• System Center<ul style="list-style-type: none">○ SIPX Line Card• Turrets• Enterprise SIP Server	15.03.00.07a 15.03.00.07a 15.03.00.07a 15.03.00.07a 15.03.00.07a 2.01.00-01

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.

display system-parameters customer-options		Page 2 of 11
OPTIONAL FEATURES		
IP PORT CAPACITIES	USED	
Maximum Administered H.323 Trunks: 12000	98	
Maximum Concurrently Registered IP Stations: 18000	1	
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	376	
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 Attended/Transferred Calls: transferred
      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 “8”.

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 8                                           Page 1 of 21
      TRUNK GROUP

      Group Number: 8      Group Type: sip      CDR Reports: y
      Group Name: PN1 to SM_21_31      COR: 1      TN: 1      TAC: *008
      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: 8
      Number of Members: 10
```

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

change trunk-group 8	Page 3 of 21
TRUNK FEATURES	
ACA Assignment? n	Measured: none
	Maintenance Tests? y
Numbering Format: private	
	UI 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 8	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 purpose, also note the values of **Near-end Listen Port** and **Far-end Listen Port**, which will be used later.

change signaling-group 8	Page 1 of 1
SIGNALING GROUP	
Group Number: 8	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: CLAN1A	Far-end Node Name: SM 21 31
Near-end Listen Port: 5060	Far-end Listen Port: 5060
	Far-end Network Region: 1
Far-end Domain: avaya.com	
Incoming Dialog Loopbacks: eliminate	Bypass If IP Threshold Exceeded? n
DTMF over IP: rtp-payload	RFC 3389 Comfort Noise? n
Session Establishment Timer(min): 120	Direct IP-IP Audio Connections? y
Enable Layer 3 Test? y	IP Audio Hairpinning? y
H.323 Station Outgoing Direct Media? n	Initial IP-IP 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:                               Authoritative Domain: avaya.com
Name: PN1
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
Call Control PHB Value: 46
Audio PHB Value: 46
Video PHB Value: 26
```

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. 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                                         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:
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 “8”. For **Pattern Name**, update as desired to reflect the same route pattern used to reach Session Manager and IPC.

change route-pattern 8													Page	1 of	3					
Pattern Number: 8													Pattern Name: toSM61							
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:	8	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 2 and routed to trunk group 8 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	2	8				5		Total Administered: 4				
5	2	12				5		Maximum Entries: 540				

5.9. Administer Uniform Dial Plan

This section provides a sample AAR routing used for routing calls with dialed digits 332xx 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 332xx, 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
332	5	0		aar n	
333	5	0		aar n	

5.10. Administer AAR Analysis

Use the “change aar analysis 0” command, and add an entry to route calls to 332xx. In the example shown below, calls with digits 332xx will be routed using route pattern “8”. Set the **Call Type** to “unku”, to prevent “+” being added as a prefix.

change aar analysis 3						Page 1 of 2	
AAR DIGIT ANALYSIS TABLE							
Location: all				Percent Full: 1			
Dialed String	Total Min Max		Route Pattern	Call Type	Node Num	ANI Req'd	
332	5	5	8	unku	n		
333	5	5	9	aar	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 “99”. 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. By enabling this feature, the calling party number will be sent to PSTN when call is coming from IPC side via a SIP trunk.

change trunk-group 99			Page 3 of 21	
TRUNK FEATURES				
ACA Assignment? n		Measured: none	Wideband Support? 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				

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 3 and routed to trunk group 99 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	3	99	all	3035381202	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, a box contains the text: "Recommended access to System Manager is via FQDN." followed by a link "Go to central login for Single Sign-On". Below this, it states: "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, there are two input fields labeled "User ID:" and "Password:". Below these fields are two buttons: "Log On" and "Cancel". At the bottom right, there is a link "Change Password".

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 Commit Cancel

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

General

* Name: D4H30

Notes:

Overall Managed Bandwidth

Managed Bandwidth Units: Kbit/sec

Total Bandwidth: 2048

Per-Call Bandwidth Parameters

* Default Audio Bandwidth: 80 Kbit/sec

Location Pattern

Add Remove

2 Items Refresh Filter: Enable

<input type="checkbox"/>	IP Address Pattern	Notes
<input type="checkbox"/>	* 10.64.10.*	
<input type="checkbox"/>	* 10.64.22.*	

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 “iodstd=avaya.com odst=ipc.com“, where “avaya.com” is the Avaya side domain, and “ipc.com” is IPC side domain. This will set the source and destination domains for all incoming and outgoing calls for IPC.

The screenshot displays the Avaya Aura System Manager 6.1 web interface. The top header includes the Avaya logo, the product name 'Avaya Aura® System Manager 6.1', and links for 'Help', 'About', 'Change Password', and 'Log off admin'. A breadcrumb trail shows 'Home / Elements / Routing / Adaptations - Adaptation Details'. The left-hand navigation pane lists various configuration categories, with 'Routing' expanded and 'Adaptations' highlighted. The main content area is titled 'Adaptation Details' and features a 'General' sub-section. Within this section, there are several input fields: 'Adaptation name' (containing 'Alliance conversion'), 'Module name' (a dropdown menu set to 'DigitConversionAdapter'), 'Module parameter' (containing 'fromto=true iodstd=avaya.com odst=ipc.com'), 'Egress URI Parameters', and 'Notes'. At the top right of the form area, there are 'Commit' and 'Cancel' buttons, along with a 'Help ?' link.

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](#) × [Session Manager](#) × [Application Management](#) × [Home](#)

[Home](#) / [Elements](#) / [Routing](#) / [SIP Entities - SIP Entity Details](#)

SIP Entity Details [Help ?](#) [Commit](#) [Cancel](#)

General

* **Name:** Alliance

* **FQDN or IP Address:** 10.64.10.114

Type: Other

Notes: IPC ESS

Adaptation: Alliance conversion

Location: D4H30

Time Zone: America/Denver

Override Port & Transport with DNS SRV: ☐

* **SIP Timer B/F (in seconds):** 4

Credential name:

Call Detail Recording: none

SIP Link Monitoring

SIP Link Monitoring: Use Session Manager Configuration

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.
- **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**.
- **Connection Policy:** Leave it as Trusted

The screenshot shows the Avaya Aura System Manager 6.1 interface. The left navigation pane has 'Entity Links' selected under the 'Routing' category. The main content area is titled 'Entity Links' and contains a table with one entry. The table has columns for Name, SIP Entity 1, Protocol, Port, SIP Entity 2, Port, and Connection Policy. The entry is 'Alliance-SM-TCP' with SIP Entity 1 'SM_21_31', Protocol 'TCP', Port '5060', SIP Entity 2 'Alliance', Port '5060', and Connection Policy 'Trusted'. There are 'Commit' and 'Cancel' buttons at the bottom right. A 'Help ?' link is also present.

Name	SIP Entity 1	Protocol	Port	SIP Entity 2	Port	Connection Policy
* Alliance-SM-TCP	* SM_21_31	TCP	* 5060	* Alliance	* 5060	Trusted

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 [Help ?](#)

Routing Policy Details [Commit](#) [Cancel](#)

General

* **Name:**

Disabled: ☐

Notes:

SIP Entity as Destination

[Select](#)

Name	FQDN or IP Address	Type	Notes
Alliance	10.64.10.114	Other	IPC ESS

Time of Day

[Add](#) [Remove](#) [View Gaps/Overlaps](#)

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

<input type="checkbox"/>	Ranking	Name	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

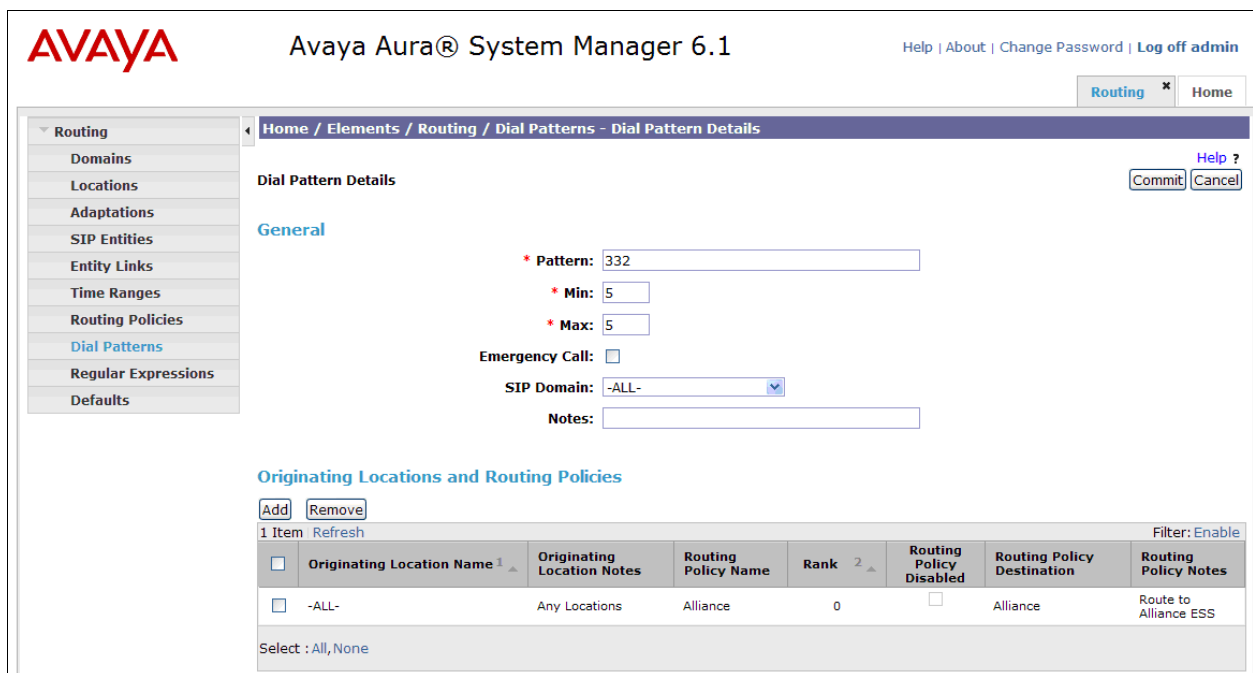
6.7. Administer Dial Patterns

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:** During the compliance test, “all” was selected for the sip domain.
- **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 [Help ?](#)

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

General

* **Pattern:**

* **Min:**

* **Max:**

Emergency Call: ☐

SIP Domain:

Notes:

Originating Locations and Routing Policies

[Add](#) [Remove](#) [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	Alliance	0	<input type="checkbox"/>	Alliance	Route to Alliance ESS

Select : All, None

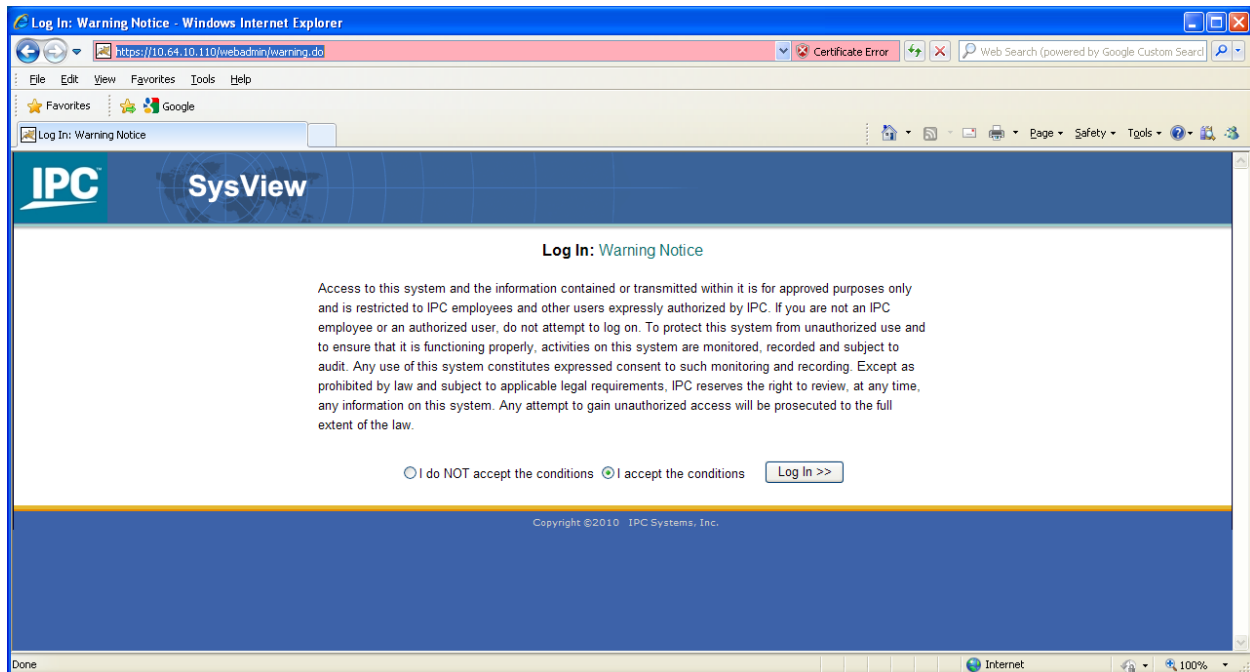
7. Configure IPC System Interconnect

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

- Configure Route Plan
- Configure SIP Proxy
- Administer Trusted Host
- Configure SIP Trunk

7.1. Configure Route Plan

Access the **IPC System Center** web interface by using the URL <https://ip-address/webadmin> in an Internet browser window, where “ip-address” is the IP address of the System Center. Select **I accept the condition**, and log in using the appropriate credentials.



On the **SysView** page, navigate to **SIP → Routing Plan → View Routing Plan** to view what is used during the compliance test.

The entry with **Sequence No. 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 “group35.com”. The entry with **Sequence No. 3** 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**.

To create a new routing plan, redirect the path to **SIP → Routing Plan → Add Routing Plan**.

Site Name: CURLY ICM Site 00
Address:
Current User: ipcinstall
iView: active

Enterprise Site ID: 0
Release: 15
Users: 1

Home | Trader Config | Line Config | Groups | SIP | Reports | Tools | Admin | Soft Turret | Help | Logoff

View Routing Plan: View

From: To: Sort by: Sequence No Results per page: 50 Search >>

Sequence No.	Action	From	To	Destination
1	Forward	sip:*	sip:3035*	sip:{user}@group35.com
2	Forward	sip:*	sip:332\$\$@*	sip:{user}@group35.com
3	Forward	sip:*	sip:*	sip:{user}@10.64.21.31;transport=TCP

Results 1 - 3 of 3

Back

7.2. Configure SIP Proxy

On the SysView page, navigate to **SIP → SIP Server → Configuration** to create a new server configuration. Enter a domain that will be used on the IPC side. Provide SIP ports for TCP/UDP and TLS. During the test TCP was used.

The screenshot shows the 'Edit Configuration: Enter Details' page for a Proxy Server in the IPC SysView interface. The page has a blue header with the IPC logo and SysView text. On the right, it displays site information: Site Name: CURLY ICM Site 00, Address: ipcinstall, View: active, Enterprise Site ID: 0, Release: 15, and Users: 1. Below the header is a navigation bar with links: Home, Trader Config, Line Config, Groups, SIP, Reports, Tools, Admin, Soft Turret, Help, and Logoff. The main content area is titled 'Edit Configuration: Enter Details' and contains a 'Proxy Server' section with the following fields:

Domains List:	ipc.com
SIP Ports:	TCP/UDP Port: 5060
	TLS Port: 5061
Security Parameters:	Domain: sip:ipc.com
	Realm: ipc.com
TLS Certificate:	Certificate File: /usr/local/SipProxy/config/localhost.key-cert.pem
	Trusted CA File: /usr/local/SipProxy/config/SipStackCACert.pem
License Server: (IP or FQDN)	10.64.10.110

7.3. 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 10.64.21.31 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=10.64.21.31

[root@esshost SipProxy]# ./trusted_hosts.pl -view
ip_address      last_modified
10.64.21.31     2012-06-04 15:38:35
```

7.4. Configure SIP Trunk

On the **SysView** page, navigate to **SIP → SIP Trunk Parameters** and select the **Edit SIP Config** button.

IPC SysView

Site Name: CURLY ICM Site 00 Enterprise Site ID: 0
Address: Release: 15
Current User: ipcinstall Users: 1
iView: active

Home Trader Config Line Config Groups SIP Reports Tools Admin Soft Turret Help Logoff

Edit SIP Config: Enter Details

1. Enter Search Criteria
DDI Groups: -- All --

2. Choose Display Format
Sort by: DDI Group ID Display 50 results per page

Back Reset Edit SIP Config >>

On the **Select SIP Config to Edit** page, select the relevant SIP **DDI Group ID**, in this case “35” and click on the “Edit Selected” button.

IPC SysView

Site Name: CURLY ICM Site 00 Enterprise Site ID: 0
Address: Release: 15
Current User: ipcinstall Users: 1
iView: active

Home Trader Config Line Config Groups SIP Reports Tools Admin Soft Turret Help Logoff

Edit SIP Config: Select SIP Config to Edit

<< Change Search

Search Results for: --All-- Results 1 - 1 of 1

Select	DDI Group ID	Outbound URI	Transport Type	User Name
<input checked="" type="radio"/>	35	avaya.com	TCP	ipc

Back Edit Selected >>

On the **Edit SIP Config Details** page, provide **Outbound URI**.

IPC SysView

Site Name: CURLY ICM Site 00 Enterprise Site ID: 0
Address: Release: 15
Current User: ipcinstall Users: 1
iView: active

Home Trader Config Line Config Groups SIP Reports Tools Admin Soft Turret Help Logoff

Edit SIP Config: Edit SIP Config Details

<< Back to Search Results

Advanced...

1. Enter Details

DDI Group ID: 35
Outbound URI: avaya.com
User Name: ipc
Password: ***
Confirm Password: ***

Back Reset Save Edits >>

8. Configure IPC Alliance MX

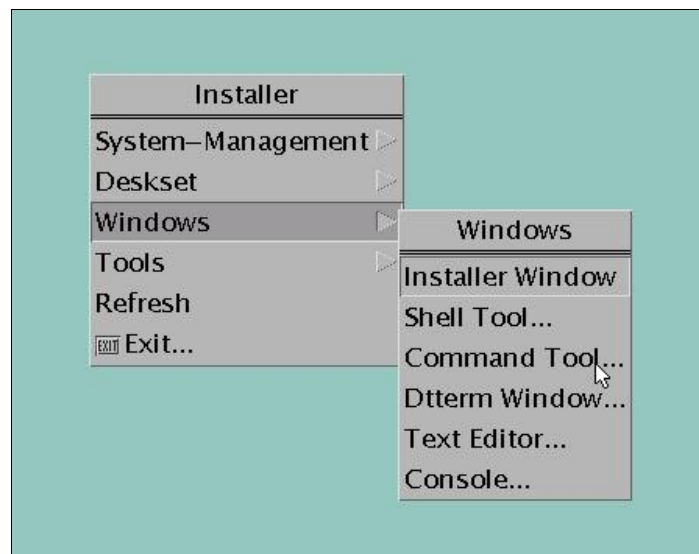
This section provides the procedures for configuring IPC Alliance MX. The procedures include the following areas:

- Launch Iview
- Administer wire groups

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

8.1. Launch Iview

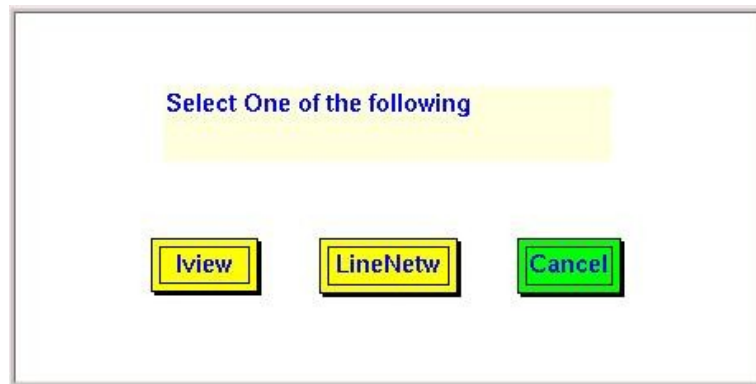
From the Alliance MX console (or System Center console), right-click and select **Windows** → **Command Tool** from the pop-up boxes.



The **cmdtool** screen is displayed. Enter “**iview &**”, as shown below.

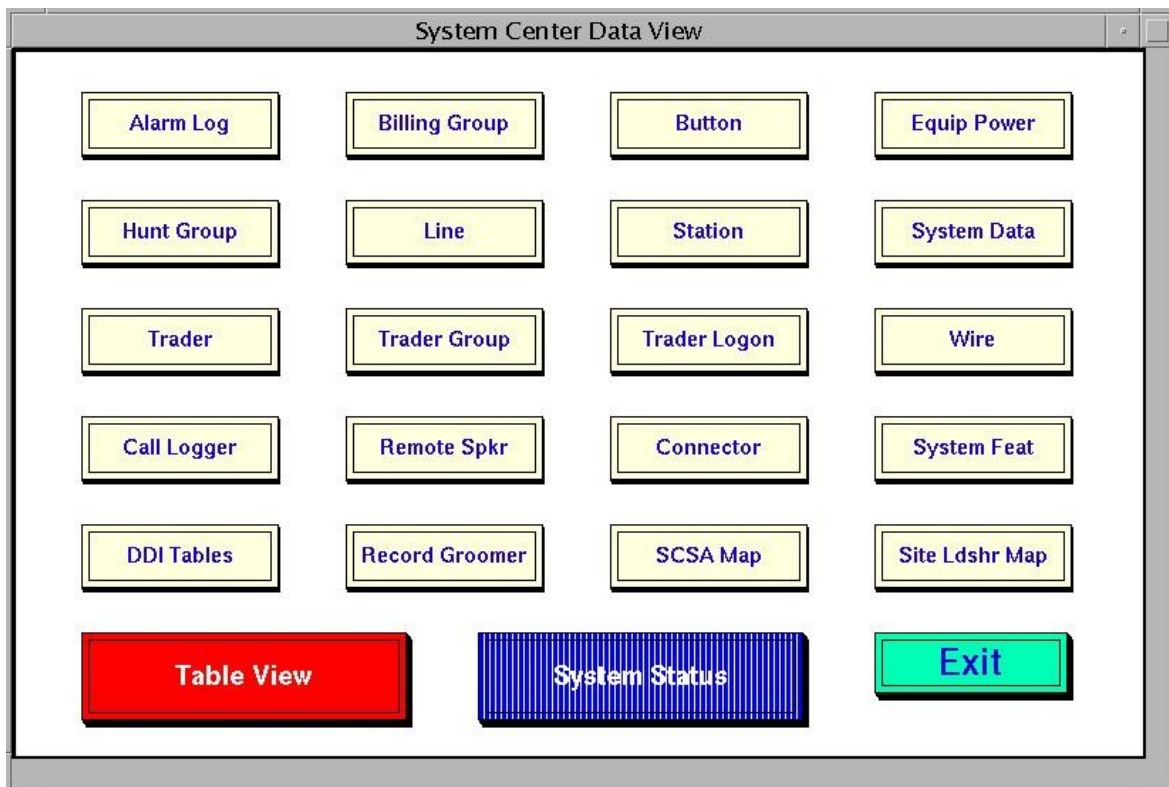


In the pop-up box shown below, click **Iview**.

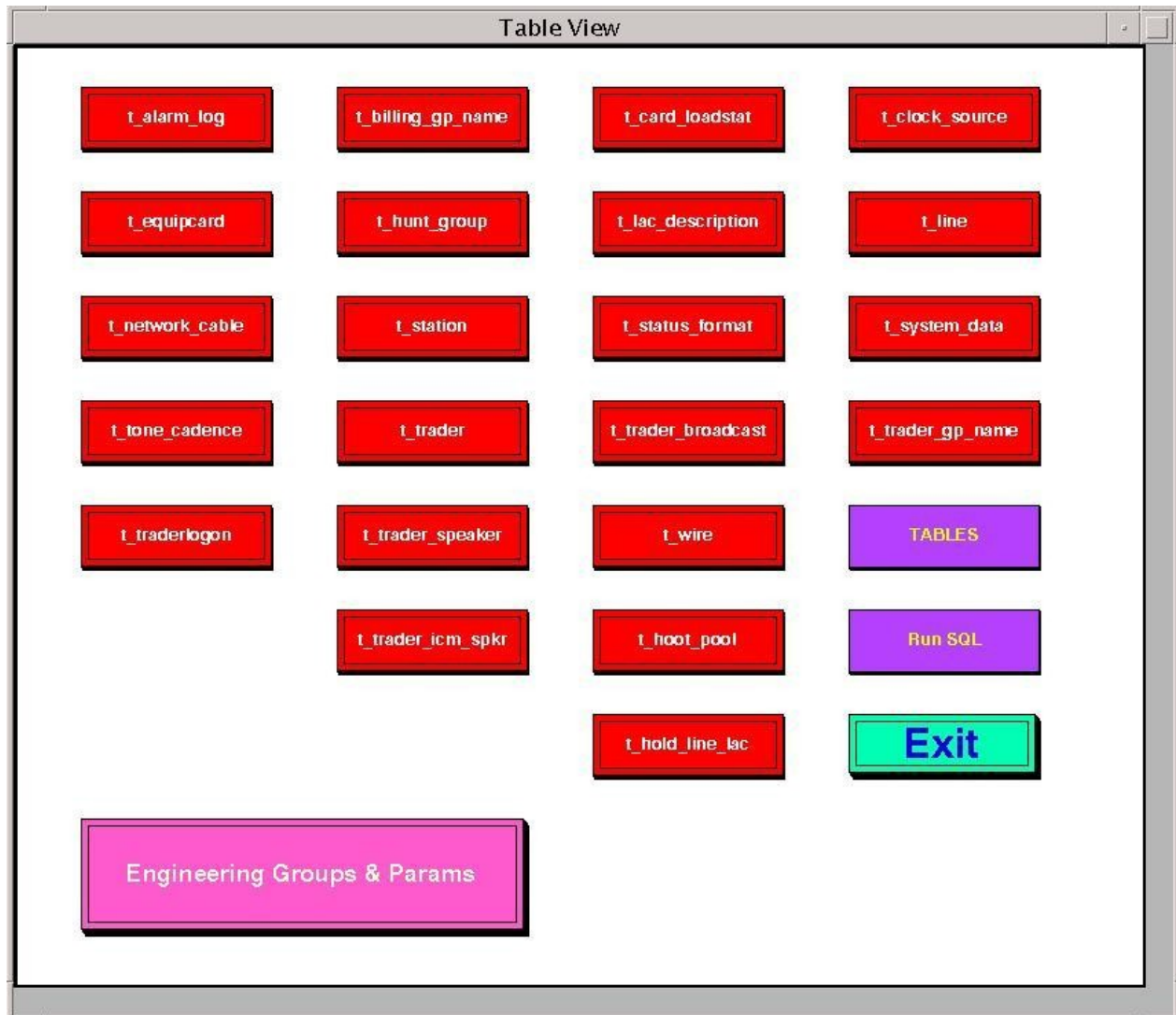


8.2. Administer Wire Groups

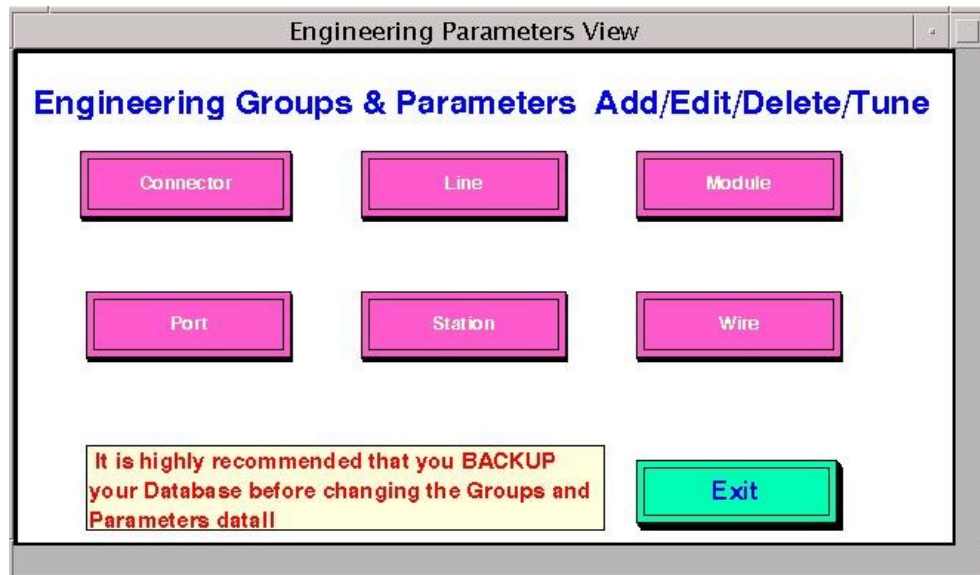
The **System Center Data View** screen is displayed. Click **Table View**.



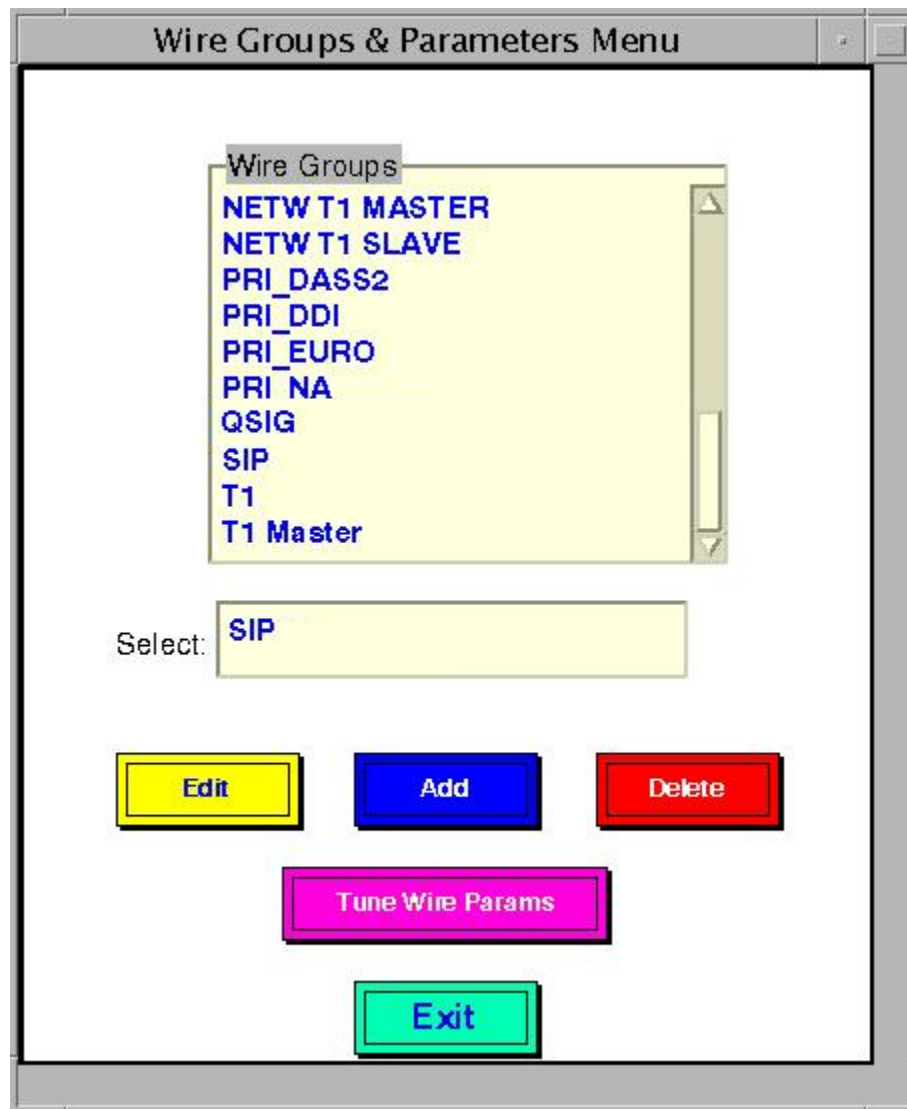
The **Table View** screen is displayed. Click **Engineering Groups & Params**.



The **Engineering Parameters View** screen is displayed next. Click **Wire**.



The **Wire Groups & Parameters Menu** screen is displayed. In the **Wire Groups** sub-section, scroll down and select “SIP”. Click **Edit**.



The **p_Wire Edit Group** screen is displayed next. Scroll down the screen as necessary to locate the entry with **Param ID** of “365”. Click on the corresponding **New Param Value** field, and enter “2” to denote Avaya as the PBX provider.

Locate the entry with **Param ID** of “370”. Click on the corresponding **New Param Value** field, and enter “4” to enable Forward Switching. Scroll down the screen as necessary to locate the entry with **Param ID** of “661”. Click on the corresponding **New Param Value** field, and enter “1” to activate detection for G729. Locate the entry with **Param ID** of “666”. Click on the corresponding **New Param Value** field, and enter “1” to enable SIP Provisional Acknowledgement (PRACK). Locate the entry with **Param ID** of “668”. Click on the corresponding **New Param Value** field, and enter “0” to disable SIP Remote Party ID (RPI).

After the configuration changes, reboot the SIP trunk card or perform a system load.

73	SIP Line Card	32767	1	32767	DSP_TERM_ATTEN	DSP TERM threshold	number	141
74	SIP Line Card	0	-5	5	TERM_SHIFT	gain/loss into ipc network	number	362
75	SIP Line Card	0	-5	5	PERIPH_SHIFT	gain/loss into public network	number	363
76	SIP Line Card	6	0	32	INTERDIGIT_TO	interdigit timeout for enbloc signaling	number	364
77	SIP Line Card	2	1	7	PBX_PROVIDER	7,DEF,AVYA,NRTL,ERISN,MITL,SMNS,CS21	enum	365
78	SIP Line Card	6	1	15	MAX_DIVERTS	Max Number of Diverts per Call	number	369
79	SIP Line Card	4	0	4	FS_ENABLE	0-4/Off, Imm&Busy, RNA, All, Always FS	number	370
80	SIP Line Card	200	200	10000	FS_DELAY	Time(msec) to Wait B4 Forward Switching	number	371
81	SIP Line Card	1	1	5	LN_RECORDS	1-5/NONE,MX_PBX,MWI,DISC,All	number	375
82	SIP Line Card	16	-32767	32767	VPKT_CONTROL	Voice Pkt Control	number	642
83	SIP Line Card	10	-32767	32767	VPKT_PERIOD	Voice Pkt Period in samples	number	643
84	SIP Line Card	12825	-32767	32767	VPKT_JITTERDEPTH	Voice Pkt Jitter Depth in samples	number	644
85	SIP Line Card	0	-32767	32767	VPKT_JITTERCTRL	Voice Pkt Jitter Control	number	645
86	SIP Line Card	0	-32767	32767	VPKT_SPARE1	Voice Pkt spare1	number	646
87	SIP Line Card	1400	0	3000	INTRUSION_FREQ	Intrusion frequency, Hz	number	647
88	SIP Line Card	350	0	3000	DIALTONELO_FREQ	Dialtone LO frequency, Hz	number	648
89	SIP Line Card	440	0	3000	DIALTONEHI_FREQ	Dialtone HI frequency, Hz	number	649
90	SIP Line Card	480	0	3000	BUSYTONELO_FREQ	Busytone LO frequency, Hz	number	650
91	SIP Line Card	620	0	3000	BUSYTONEHI_FREQ	Busytone HI frequency, Hz	number	651
92	SIP Line Card	440	0	3000	RINGBACKLO_FREQ	Ringback LO frequency, Hz	number	652
93	SIP Line Card	480	0	3000	RINGBACKHI_FREQ	Ringback HI frequency, Hz	number	653
94	SIP Line Card	480	0	3000	ERRTONELO_FREQ	Error tone LO frequency, Hz	number	654
95	SIP Line Card	620	0	3000	ERRTONEHI_FREQ	Error tone HI frequency, Hz	number	655
96	SIP Line Card	1209	0	3000	SPLSHTONELO_FREQ	Splash tone LO frequency, Hz	number	656
97	SIP Line Card	1477	0	3000	SPLSHTONEHI_FREQ	Splash tone HI frequency, Hz	number	657
98	SIP Line Card	1400	0	3000	RECWARNTONE_FREQ	Record warning frequency, Hz	number	658
99	SIP Line Card	0	0	10000	MRD_Ringback_Ton	Ringback Tone Duration (msec)	number	659
100	SIP Line Card	1	0	1	VAD	Voice Activity Detection	number	661
101	SIP Line Card	0	0	1	MWI_Subscribe	Send MWI Subscribe, Off = 0, On = 1	number	663
102	SIP Line Card	0	0	1	SIP_Divert	HistoryInfo = 0, CCDiversion = 1	number	664
103	SIP Line Card	1	0	1	SIP_PRACK	Enable SIP Provisional ACK	number	666
104	SIP Line Card	1	0	1	SIP_PA1	Enable SIP P-Asserted Identity	number	667
105	SIP Line Card	0	0	1	SIP_RPID	Enable SIP Remote Party ID	number	668
106	SIP Line Card	0	0	1	AEC_Enable	Enable AEC Control Filter	number	669
107	SIP Line Card	0	-3	3	AEC_Control	AEC Aggression level	number	670
108	SIP Line Card	0	0	1	AEC_NR_Filter	Enable AEC Noise Reduction	number	671
109	SIP Line Card	1	0	1	VoIP_Stat_Log	Enable VoIP Statistics Logging	number	672
110	SIP Line Card	1	0	1	SIP_3264_Hold	Enable SIP 3264 Call Hold/Resume	number	673
111	SIP Line Card	1	0	1	SIP_Conn_Party_U	Enable SIP connected party update messag	number	674
112	SIP Line Card	15	0	15	FRF11_Idle_Signa	FRF11 Idle bit pattern	number	675
113	SIP Line Card	10	0	15	FRF11_Seize_Sign	FRF11 Seize bit pattern	number	676
114								

9. Verification Steps

This section provides the tests that can be performed to verify proper configuration of Avaya Aura® Session Manager and IPC Alliance MX.

9.1. 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 2 items. The table has columns for Session Manager Name, Entity Links Down/Total, Entity Links Partially Down, SIP Entities - Monitoring Not Started, and SIP Entities - Not Monitored. The data rows are SM_21_31 and SM_10_62. Below the table is a 'Select' dropdown set to 'All, None'. Further down, there is a section for 'All Monitored SIP Entities' with another 'Run Monitor' button and a list of 19 items. The list includes SIP Entity Name, AAM_21_72, and Alliance (highlighted with a red box).

Session Manager Name	Entity Links Down/Total	Entity Links Partially Down	SIP Entities - Monitoring Not Started	SIP Entities - Not Monitored
SM_21_31	3/22	1	0	7
SM_10_62	0/5	0	0	1

SIP Entity Name
AAM_21_72
Alliance

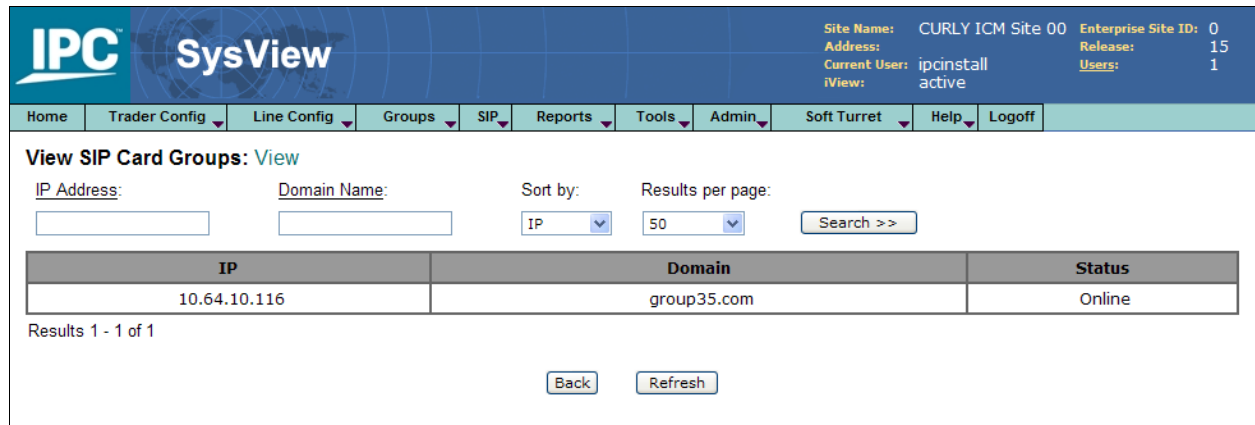
The **SIP Entity, Entity Link Connection Status** screen is displayed. Verify that **Conn. Status** and **Link Status** are “Up”, as shown below.

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 2 items. The table has columns for Session Manager Name, SIP Entity Resolved IP, Port, Proto, Conn. Status, Reason Code, and Link Status. The data rows are SM_21_31 and SM_21_31. The 'Conn. Status' and 'Link Status' columns show 'Up' for both rows.

Details	Session Manager Name	SIP Entity Resolved IP	Port	Proto.	Conn. Status	Reason Code	Link Status
Show	SM_21_31	10.64.10.114	5060	UDP	Up	200 OK	Up
Show	SM_21_31	10.64.10.114	5060	TCP	Up	200 OK	Up

9.2. Verify IPC System Interconnect

From the SysView web interface, select **SIP → Update ESS with SIP Trunk Info → View SIP Cards Groups**. Verify that there is an entry that corresponds to SIP card number. Verify that the **Status** is “Online”, as shown below.



The screenshot shows the IPC SysView web interface. The top navigation bar includes tabs for Home, Trader Config, Line Config, Groups, SIP, Reports, Tools, Admin, Soft Turret, Help, and Logoff. The right side of the header displays system information: Site Name: CURLY ICM Site 00, Address: , Current User: ipcinstall, iView: active, Enterprise Site ID: 0, Release: 15, and Users: 1. The main content area is titled 'View SIP Card Groups: View'. It features search filters for IP Address, Domain Name, Sort by (set to IP), and Results per page (set to 50). A 'Search >>' button is present. Below the filters is a table with the following data:

IP	Domain	Status
10.64.10.116	group35.com	Online

Below the table, it indicates 'Results 1 - 1 of 1' and provides 'Back' and 'Refresh' buttons.

10. Conclusion

These Application Notes describe the configuration steps required for IPC Alliance MX 15.03 to successfully interoperate with Avaya Aura® Communication Manager 6.0.1 and Avaya Aura® Session Manager 6.1 using SIP trunks to Avaya Aura® Session Manager. All feature and serviceability test cases were completed.

11. Additional References

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

- *Administering Avaya AuraTM Communication Manager*, Document 03-300509, Issue 6.0, Release 6.0, June 2010, available at <http://support.avaya.com>.
- *IPC PATCH 15.03.00.07a Intall Guide*, Revision Number 7, April 2011, available upon request to IPC Support.
- *Nexus Suite 2.0 SP1 Patch11 or Higher Deployment Guide*, Part Number B02200161, Revision Number 01, available 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.