Abstract

These Application Notes describe the configuration steps required for IPC Alliance 16 to interoperate with Avaya Modular Messaging 5.2 via Avaya Aura® Session Manager 6.3 using SIP trunks.

IPC Alliance 16 is a trading communication solution. In the compliance test, IPC Alliance 16 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 Alliance 16 to interoperate with Avaya Modular Messaging 5.2 via Avaya Aura® Session Manager 6.3 using SIP trunks.

The IPC Alliance system is a trading communication solution. In the compliance test, the IPC Alliance system used SIP trunks to Avaya Aura® Session Manager, for turret users on IPC to reach users on Avaya Aura® Communication Manager, and Avaya Modular Messaging (hereon refers to as MM) pilot number.

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, PSTN users, and/or MM pilot number. 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.

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.

2.1. Interoperability Compliance Testing

The interoperability compliance test included feature and serviceability testing.

The feature test cases were performed manually. Calls were manually established among IPC turret users with Avaya SIP, Avaya H.323, PSTN users, and/or MM voicemail pilot to verify various call scenarios. The Avaya Modular Messaging Web Subscriber Options web-based interface was used to configure subscriber features such as Call Me, Find Me, and Call Sender. During the DevConnect solution test, the following features were performed:

- Login
- Ring No Answer Greeting
- Calling Party Verification
- Message Waiting Indicator (MWI)
- Multiple Call Forwarding
- Receptionist/Personal Operator
- Live Attendant
- Find Me
- Call Me
- Call Sender
The serviceability testing focused on verifying the ability of IPC Alliance 16 to recover from adverse conditions, such as disconnecting/reconnecting the LAN connection to IPC Alliance 16.

### 2.2. Test Results

All test cases were executed and verified, with following observations.

- During the Personal Operator test case, Communication Manager sends “SIP / 2.0 481 Call Transaction does not exist” in Notify message after “202 Accepted” message. Also heard “That extension does not answer” on the calling party endpoint. This happens because Communication Manager does not know the destination extension (Personal Operator). – For remedy, see Section 5.1.
- During the Personal Operator test case, no RTP between calling party and personal operator was observed. – For remedy, see Section 5.2.

### 2.3. Support

Technical support on IPC Alliance 16 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 Alliance 16 at the Remote Site consists of the Enterprise SIP Server (ESS), System Center, and Turrets. SIP trunks are used from Alliance 16 to Session Manager, to reach users on Communication Manager, MM, 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 Communication Manager Users at the Central site (720xx), and IPC turret users at the Remote site (332xx). Following were the subscribers used during the compliance test:

- Avaya H323 – 72001, 72002, 72003
- Avaya SIP – 72021, 72022, 72023
- IPC turret Users – 33201, 33210

The configuration of Session Manager is performed via the web interface of System Manager. The detailed administration of basic connectivity between Communication Manager and 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:

<table>
<thead>
<tr>
<th>Equipment</th>
<th>Software</th>
</tr>
</thead>
<tbody>
<tr>
<td>Avaya Modular Messaging</td>
<td>5.2 with SP 16 (9.2.737.16002)</td>
</tr>
<tr>
<td>Avaya Aura® Communication Manager on Avaya S8300D Server</td>
<td>6.3 (R016x.03.0.124.0-22147)</td>
</tr>
<tr>
<td>Avaya G450 Media Gateway</td>
<td>36.12</td>
</tr>
<tr>
<td>Avaya Aura® Session Manager</td>
<td>6.3.13.0.631304</td>
</tr>
<tr>
<td>Avaya Aura® System Manager</td>
<td>6.3.13</td>
</tr>
<tr>
<td>Avaya 9600 Series IP Telephone (H.323)</td>
<td>3.2.2/3.2.3</td>
</tr>
<tr>
<td>Avaya 96x1 Series IP Telephone (H.323)</td>
<td>6.2.3</td>
</tr>
<tr>
<td>Avaya 9600 Series IP Telephone (SIP)</td>
<td>2.6.12</td>
</tr>
<tr>
<td>Avaya 96x1 Series IP Telephone (SIP)</td>
<td>6.4.1</td>
</tr>
<tr>
<td>IPC Alliance 16</td>
<td></td>
</tr>
<tr>
<td>• One Management System (Ones)</td>
<td>16.02.01.09</td>
</tr>
</tbody>
</table>

Figure 1: Test Configuration of IPC Alliance 16 with Avaya Modular Messaging
5. Configure Avaya Aura® Communication Manager

This section provides the procedures for configuring Communication Manager. The basic configurations, including signaling group, trunk group, and all routings, are not included in these App Notes. However, the procedures include the following areas:

- Administer locations
- Administer trunk group (Page 4)

Note: for detailed configuration on Communication Manager for the Alliance system, please refer to [4].

5.1. Administer Locations

During the Personal Operator test case, Communication Manager sends “SIP / 2.0 481 Call Transaction does not exist” in Notify message after “202 Accepted” message. Also heard “That extension does not answer” on the calling party endpoint. This happens because Communication Manager does not know the destination extension (Personal Operator).

The remedy to the issue is: sending all unknown destination extensions to Session Manager via the SIP trunk.

Use the “change locations” command to send all unknown destination extension to Session Manager. In the Locations form, enter the trunk group number so that all unknown extensions will be sent to Session Manager from Communication Manager. In this case, it was 92.

<table>
<thead>
<tr>
<th>Loc No</th>
<th>Name</th>
<th>Timezone</th>
<th>DST</th>
<th>City/Area</th>
<th>Proxy Sel</th>
<th>Rte Pat</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Main</td>
<td>+00:00</td>
<td>0</td>
<td></td>
<td></td>
<td>92</td>
</tr>
</tbody>
</table>
5.2. Administer Trunk Group (Page 4)
During the Personal Operator test case, no RTP between calling party and personal operator was observed.

To remedy the issue, navigate to Page 4 of the trunk group (between Communication Manager and Session Manager). Enabled the Build Refer-To URI of REFER from Contact For NCR field by selecting “y”.

<table>
<thead>
<tr>
<th>change trunk-group 92</th>
<th></th>
<th>Page 4 of 21</th>
</tr>
</thead>
<tbody>
<tr>
<td>PROTOCOL VARIATIONS</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Mark Users as Phone?</td>
<td>n</td>
<td></td>
</tr>
<tr>
<td>Prepend '+' to</td>
<td>n</td>
<td></td>
</tr>
<tr>
<td>Calling/Alerting/</td>
<td>n</td>
<td></td>
</tr>
<tr>
<td>Diverting/Connected</td>
<td>y</td>
<td></td>
</tr>
<tr>
<td>Number?</td>
<td>y</td>
<td></td>
</tr>
<tr>
<td>Build Refer-To URI of</td>
<td>y</td>
<td></td>
</tr>
<tr>
<td>REFER From Contact For</td>
<td></td>
<td></td>
</tr>
<tr>
<td>NCR?</td>
<td>n</td>
<td></td>
</tr>
<tr>
<td>Send Diversion Header</td>
<td>n</td>
<td></td>
</tr>
<tr>
<td>Support Request History</td>
<td>y</td>
<td></td>
</tr>
<tr>
<td>Telephone Event Payload Type:</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Convert 180 to 183 for Early Media?</td>
<td>n</td>
<td></td>
</tr>
<tr>
<td>Always Use re-INVITE for Display Updates?</td>
<td>n</td>
<td></td>
</tr>
<tr>
<td>Identity for Calling Party Display: P-Asserted-Identity</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Block Sending Calling Party Location in INVITE?</td>
<td>n</td>
<td></td>
</tr>
<tr>
<td>Accept Redirect to Blank User Destination?</td>
<td>n</td>
<td></td>
</tr>
<tr>
<td>Enable Q-SIP?</td>
<td>n</td>
<td></td>
</tr>
<tr>
<td>Interworking of ISDN Clearing with In-Band Tones: keep-channel-active</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
6. Configure Avaya Modular Messaging MSS

This section provides the procedures for configuring IPC turret users as local and remote subscribers on MM. The subscriber management is configured on the Messaging Storage Server (MSS) component. The configuration procedures include the following areas:

- Launch messaging administration
- Administer subscriber extension ranges
- Administer subscribers

6.1. Launch Messaging Administration

Access the MSS web interface by using the URL http://<ip-address> in an Internet browser window, where “ip-address” is the IP address of the MSS server. The Logon screen is displayed. Log in using a valid user name and password. The Password field will appear after a value is entered into the Username field.

The Messaging Administration screen appears, as shown below.
6.2. Administer Subscriber Extension Ranges

Select **Messaging Administration → Networked Machines** from the left pane, to display the **Manage Networked Machines** screen. Select the MSS server from the table listing, and click **Edit the Selected Networked Machine** toward the bottom right of the screen.
The **Edit Networked Machine** screen is displayed. Under the **MAILBOX NUMBER RANGES** section, locate an available entry line and enter the desired starting and ending mailbox numbers to be used for the IPC subscribers as necessary. In the compliance testing, the existing entry covered the 332xx extensions used by the IPC turret users.
6.3. Administer Subscribers

Select **Messaging Administration → Subscriber Management** from the left pane, to display the **Manage Subscribers** screen. There are two ways to add a subscriber. For the **Local Subscriber Mailbox Number** field toward the top of the screen, enter the first IPC turret user (or any subscriber) extension to add as a local subscriber, in this case “33201”. Click **Add or Edit**.

Or Click the **Manage** button on Local Subscribers field. On the Manage Local Subscribers screen, click the **Add a New Subscriber** button.
The **Add Local Subscriber** screen is displayed next. Enter the desired string into the **Last Name**, **First Name**, and **Password** fields.

In the compliance testing, the same telephone extensions for the IPC subscribers were used for the **Mailbox Number**, **Numeric Address**, and **PBX Extension** fields. Select the appropriate **Class Of Service**, and retain the default values in the remaining fields.

Scroll down to the bottom of the screen and click **Save** (not shown). Repeat this section to add all IPC subscribers.
7. Configure Avaya Modular Messaging MAS

This section provides the procedures for configuring the Avaya Messaging Application Server (MAS) servers. A change is needed on each MAS server, to set the way Modular Messaging reads the SIP History Information records for proper integration with IPC. Note that enabling this setting has an impact on the proper identification of calling party number for Vectoring call scenarios.

From the first MAS server, navigate to the C:\Avaya_Support\Registry_Keys directory, and double-click on CalledPartyAlgorithm-Orig.

Select Start → Settings → Control Panel → Administrative Tools → Services, to display the Services screen. Navigate to the MM Messaging Application Server entry, right-click on the entry and select Restart. Repeat these procedures on all MAS servers, if more than one MAS is utilized.
8. Configure Avaya Aura® Session Manager

This section provides the procedures for configuring Session Manager for IPC Alliance 16 and MM. An assumption is made that the SIP trunk between Communication manager and Session Manager is already configured and working. The procedures include the following areas:

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

8.1. Launch System Manager

Access the System Manager web interface by using the URL http://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 system manager main page is displayed. Navigate to **Elements → Routing.**
8.2. Administer Locations

In 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.

The Location Details screen is displayed. In the General sub-section, enter a descriptive Name and optional Notes. Retain the default values in the remaining fields.

Repeat the previous steps to add the locations for MM.
The following screen shows the **Locations** page after the locations for Alliance and MM are added.
8.3. 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”
- **Location:** Select the IPC location name from Section 8.2.
- **Time Zone:** Select the applicable time zone.

![SIP Entity Details Screen](image_url)
The following screen shows the SIP Entities page for MM. 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 MAS server.
- **Type:** “Modular Messaging”
- **Location:** Select the MM location name from **Section 8.2**.
- **Time Zone:** Select the applicable time zone.

![SIP Entities page](image1)

The following screen shows the SIP Entities page after the entities for Alliance 16 and MM are added.

![SIP Entities page](image2)
8.4. 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 and MM.

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:** Enter the Session Manager entity name.
- **Protocol:** Enter a signaling group transport method.
- **Port:** Enter a signaling group listen port number.
- **SIP Entity 2:** The IPC entity name from Section 8.3.
- **Port:** Enter a signaling group listen port number.
- **Connection Policy:** Select “trusted”.

During the compliance test, Alliance 16 utilized two SIP trunks (TCP and UDP). The following shows UDP protocol.
The following screen shows the entity link for MM. Enter the following values for the specified fields, and retain the default values for the remaining fields.

- **Name:** A descriptive name.
- **SIP Entity 1:** Enter the Session Manager entity name.
- **Protocol:** Enter a signaling group transport method.
- **Port:** Enter a signaling group listen port number.
- **SIP Entity 2:** The MM entity name from Section 8.3.
- **Port:** Enter a signaling group listen port number.
- **Connection Policy:** Select “trusted”.

The following screen shows the **Entity Links** page after the entity links for Alliance and MM are added.
8.5. 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 and MM.

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**.

![Routing Policy Details Screen](image-url)
On the **SIP Entities** screen, Select the IPC entity name from **Section 8.3** in the listing, and click the **Select** button.

When returns to the **Routing Policy Details** page, retain the default value and click **Commit**.
Repeat the above steps to configure a routing policy for MM. The following shows the routing policy details page for MM.

The following screen shows the Routing Policies page after the routing policies for Alliance and MM are added.
8.6. 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.
Under the **Originating Location** submenu, check the **Apply The Selected Routing Policies to All Originating Locations** checkbox.

Under the **Routing Policies** submenu, select a routing policy created in **Section 8.5**.

Retain the default values in the remaining fields and click **Select**.
When return to **Dial Pattern Details** page, click **Commit**.
Repeat the above steps to configure a pilot number to send calls to MM. The following screen shows the dial pattern for x7777, which is the pilot number on MM.

The following screen shows the **Dial Patterns** page after the dial pattern for Alliance and MM are added.
9. Configure IPC Alliance 16
Prior to the compliance test, installation and basic configuration were accomplished by an IPC engineer. This section will only describe the areas relevant to the compliance test.

The procedures include the following areas:
- Configure System Settings
- Configure Route Plan
- Configure SIP Proxy
- Configure SIP Trunk
- Administer Trusted Host
- Administer Wire Group

9.1. Configure System Settings
Access the IPC System Center web interface by using the URL https://ip-address/oneview in an Internet browser window, where “ip-address” is the IP address of the System Center. Check the ”I agree to the terms and conditions” checkbox, and log in using the appropriate credentials.
The License Login page is displayed. Provide an appropriate license password. Click Login.

Click Continue>> on the Login Information page.
On the **OneView Main Menu** page, navigate to **SYSTEM SETTINGS → System Feature** to view and modify what is used during the compliance test.

Search for **Transfer Group** in the **Select column** field, and click the **Go** button. The following screen shows the transfer group, which is set to “15”. The value “15” in the transfer group indicates the SIP trunk. Thus, all transfer calls will go out through the SIP trunk.
Above **Transfer Group** value comes from the **Load Share Group Data View** page, which is shown below. To view the **Load Share Group Data View** page, navigate to LINE CONFIG → DDI → **Load Share Group Data View**. In this screen, the **Load Share Group Id “1”** indicates QSIG, and the **Load Share Group Id “15”** indicates SIP.
9.2. Configure Route Plan

On the One View Main Menu page, navigate to NEXUS→Routing Plan→View/Edit/Delete Routing Plan to view what is used during the compliance test.

On the View/Edit/Delete Routing Plan page, click Submit.

The entry with Sequence Number 1 was used for routing 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 Number 2 was used for routing 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 8.4.

To create a new routing plan, redirect the path to NEXUS→Routing Plan→Add Routing Plan.
9.3. Configure SIP Proxy

On the **One View Main Menu** page, navigate to **NEXUS → SIP Servers → Configuration** to view what SIP proxy is used during the compliance test.

On the **Configuration** page, enter a domain that will be used on the IPC side. Provide SIP ports for TCP/UDP or TLS.

![Configuration Table](image)
9.4. Configure SIP Trunk

On the One View Main Menu page, navigate to NEXUS ➔ SIP Trunk Parameters ➔ Update ESS with SIP Trunk Info ➔ View/Delete SIP Cards to Trunks to view what SIP trunk is used during the compliance test.

On the View/Delete SIP Cards to Trunks page, click Search.

Verify the Domain (DDI Group ID) and IP Address of the SIP card is correct, and Status is “Online”
9.5. 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 10.64.41.42 is the IP address of the signaling interface for Session Manager, and 10.64.10.110 is the IP address of the OneView server (System Center in Figure 1).

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

```
[ipaadmin@esshost SipProxy]$ ./trusted_hosts.pl -add 10.64.41.42
[ip_address] last_modified
10.64.41.42 2014-08-13 06:00:27
10.64.10.110 2014-08-13 06:28:59
```

9.6. Administer Wire Groups

From the OneView Main Menu page, navigate to GROUPS → Engineering Groups → Wire Group.

Provide the following information:

- **Select Wire Group** “Avaya SIP” using a drop-down menu.
- **Select Operation** “Edit” using a drop-down menu.

Click Submit.
The **Edit Wire Groups** screen is displayed next. Scroll down the screen as necessary to locate the entry with **Param ID** of “365”. 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”. 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.

```
<table>
<thead>
<tr>
<th>Group Name</th>
<th>Group Class</th>
<th>Group</th>
<th>Param Value</th>
<th>Param Min</th>
<th>Param Max</th>
<th>Param</th>
<th>Param Value</th>
<th>Param Type</th>
<th>Param ID</th>
</tr>
</thead>
<tbody>
<tr>
<td>Avaya SIP</td>
<td>SIP</td>
<td>Avaya SIP</td>
<td>2</td>
<td>1</td>
<td>7</td>
<td>PBX_PROVIDER</td>
<td>1-7/DEF,AVYA... num</td>
<td>365</td>
<td></td>
</tr>
<tr>
<td>Avaya SIP</td>
<td>SIP</td>
<td>Avaya SIP</td>
<td>6</td>
<td>1</td>
<td>15</td>
<td>MAX_DIVERTS</td>
<td>Max Number of... number</td>
<td>369</td>
<td></td>
</tr>
<tr>
<td>Avaya SIP</td>
<td>SIP</td>
<td>Avaya SIP</td>
<td>4</td>
<td>0</td>
<td>4</td>
<td>FS_ENABLE</td>
<td>0-4/0V, Imm... number</td>
<td>370</td>
<td></td>
</tr>
<tr>
<td>Avaya SIP</td>
<td>SIP</td>
<td>Avaya SIP</td>
<td>200</td>
<td>200</td>
<td>10000</td>
<td>FS_DELAY</td>
<td>Time(msec) To... number</td>
<td>371</td>
<td></td>
</tr>
<tr>
<td>Avaya SIP</td>
<td>SIP</td>
<td>Avaya SIP</td>
<td>1</td>
<td>1</td>
<td>5</td>
<td>LN_RECORDS</td>
<td>1-5/NONE,MX... number</td>
<td>373</td>
<td></td>
</tr>
<tr>
<td>Avaya SIP</td>
<td>SIP</td>
<td>Avaya SIP</td>
<td>16</td>
<td>-32767</td>
<td>32767</td>
<td>VPRT.CONTROL</td>
<td>Voice Pkt Cont... number</td>
<td>642</td>
<td></td>
</tr>
<tr>
<td>Avaya SIP</td>
<td>SIP</td>
<td>Avaya SIP</td>
<td>10</td>
<td>-32767</td>
<td>32767</td>
<td>VPRT.PERIOD</td>
<td>Voice Pkt Peri... number</td>
<td>643</td>
<td></td>
</tr>
<tr>
<td>Avaya SIP</td>
<td>SIP</td>
<td>Avaya SIP</td>
<td>12325</td>
<td>-32767</td>
<td>32767</td>
<td>VPRT.JITTERL</td>
<td>Voice Pkt Jitter... number</td>
<td>644</td>
<td></td>
</tr>
<tr>
<td>Avaya SIP</td>
<td>SIP</td>
<td>Avaya SIP</td>
<td>0</td>
<td>-32767</td>
<td>32767</td>
<td>VPRT.JITTERL</td>
<td>Voice Pkt Jitter... number</td>
<td>645</td>
<td></td>
</tr>
<tr>
<td>Avaya SIP</td>
<td>SIP</td>
<td>Avaya SIP</td>
<td>1400</td>
<td>0</td>
<td>3000</td>
<td>INTRUSION_F.</td>
<td>Intrusion freq... number</td>
<td>647</td>
<td></td>
</tr>
<tr>
<td>Avaya SIP</td>
<td>SIP</td>
<td>Avaya SIP</td>
<td>350</td>
<td>0</td>
<td>3000</td>
<td>DEALTONELO._</td>
<td>Dialtone LO freq... number</td>
<td>648</td>
<td></td>
</tr>
<tr>
<td>Avaya SIP</td>
<td>SIP</td>
<td>Avaya SIP</td>
<td>440</td>
<td>0</td>
<td>3000</td>
<td>DEALTONEHI._</td>
<td>Dialtone HI freq... number</td>
<td>649</td>
<td></td>
</tr>
<tr>
<td>Avaya SIP</td>
<td>SIP</td>
<td>Avaya SIP</td>
<td>480</td>
<td>0</td>
<td>3000</td>
<td>BUSYTONEL._</td>
<td>Busytone LO freq... number</td>
<td>659</td>
<td></td>
</tr>
<tr>
<td>Avaya SIP</td>
<td>SIP</td>
<td>Avaya SIP</td>
<td>620</td>
<td>0</td>
<td>3000</td>
<td>BUSYTONEH._</td>
<td>Busytone HI freq... number</td>
<td>651</td>
<td></td>
</tr>
<tr>
<td>Avaya SIP</td>
<td>SIP</td>
<td>Avaya SIP</td>
<td>440</td>
<td>0</td>
<td>3000</td>
<td>RINGBACKLO._</td>
<td>Ringback LO freq... number</td>
<td>652</td>
<td></td>
</tr>
<tr>
<td>Avaya SIP</td>
<td>SIP</td>
<td>Avaya SIP</td>
<td>480</td>
<td>0</td>
<td>3000</td>
<td>RINGBACKHI._</td>
<td>Ringback HI freq... number</td>
<td>653</td>
<td></td>
</tr>
<tr>
<td>Avaya SIP</td>
<td>SIP</td>
<td>Avaya SIP</td>
<td>480</td>
<td>0</td>
<td>3000</td>
<td>ERRTONELO._</td>
<td>Error tone LO freq... number</td>
<td>654</td>
<td></td>
</tr>
<tr>
<td>Avaya SIP</td>
<td>SIP</td>
<td>Avaya SIP</td>
<td>620</td>
<td>0</td>
<td>3000</td>
<td>ERRTONEHI._</td>
<td>Error tone HI freq... number</td>
<td>655</td>
<td></td>
</tr>
<tr>
<td>Avaya SIP</td>
<td>SIP</td>
<td>Avaya SIP</td>
<td>1208</td>
<td>0</td>
<td>3000</td>
<td>SPLASHTONELO._</td>
<td>Splash tone LO... number</td>
<td>656</td>
<td></td>
</tr>
<tr>
<td>Avaya SIP</td>
<td>SIP</td>
<td>Avaya SIP</td>
<td>1477</td>
<td>0</td>
<td>3000</td>
<td>SPLASHTONEHI._</td>
<td>Splash tone HI... number</td>
<td>657</td>
<td></td>
</tr>
<tr>
<td>Avaya SIP</td>
<td>SIP</td>
<td>Avaya SIP</td>
<td>1400</td>
<td>0</td>
<td>3000</td>
<td>RECWARNLO._</td>
<td>Record warning... number</td>
<td>658</td>
<td></td>
</tr>
<tr>
<td>Avaya SIP</td>
<td>SIP</td>
<td>Avaya SIP</td>
<td>0</td>
<td>0</td>
<td>10000</td>
<td>MBR Ringback._</td>
<td>Ringback Tone... number</td>
<td>659</td>
<td></td>
</tr>
<tr>
<td>Avaya SIP</td>
<td>SIP</td>
<td>Avaya SIP</td>
<td>1</td>
<td>0</td>
<td>1</td>
<td>VAD</td>
<td>Voice Activity... number</td>
<td>661</td>
<td></td>
</tr>
<tr>
<td>Avaya SIP</td>
<td>SIP</td>
<td>Avaya SIP</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>MM52_SUBS_.</td>
<td>MMT Subscribe</td>
<td>Send MMT Sub... number</td>
<td>663</td>
</tr>
<tr>
<td>Avaya SIP</td>
<td>SIP</td>
<td>Avaya SIP</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>SIP Divert.</td>
<td>HistoryInfo =... number</td>
<td>664</td>
<td></td>
</tr>
<tr>
<td>Avaya SIP</td>
<td>SIP</td>
<td>Avaya SIP</td>
<td>1</td>
<td>0</td>
<td>1</td>
<td>SIP.PRACK</td>
<td>Enable SIP Pr... number</td>
<td>666</td>
<td></td>
</tr>
<tr>
<td>Avaya SIP</td>
<td>SIP</td>
<td>Avaya SIP</td>
<td>1</td>
<td>0</td>
<td>1</td>
<td>SIP.PAI</td>
<td>Enable SIP P... number</td>
<td>667</td>
<td></td>
</tr>
<tr>
<td>Avaya SIP</td>
<td>SIP</td>
<td>Avaya SIP</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>SIP.WFD</td>
<td>Enable SIP Re... number</td>
<td>668</td>
<td></td>
</tr>
</tbody>
</table>
```
10. Verification Steps
This section provides the tests that can be performed to verify proper configuration of Session Manager and IPC Alliance 16 and MM.

10.1. Verify Avaya Aura® Session Manager
From the System Manager home page (not shown), select Elements → Session Manager to display the Session Manager Dashboard screen.

![Session Manager Dashboard](image)
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 Session Manager name, SM63, to see all entity links from Session Manager.
The **SIP Entity, Entity Link Connection Status** screen is displayed. Verify that **Conn. Status** and **Link Status** are “Up” for Alliance and MM, as shown below.
11. Conclusion
These Application Notes describe the configuration steps required for IPC Alliance 16 to successfully interoperate with Avaya Modular Messaging 5.2 via Avaya Aura® Session Manager, using SIP trunks. All feature and serviceability test cases were completed successfully with observations noted in Section 2.2.

12. Additional References
This section references the product documentation relevant to these Application Notes.
[3] IPC PATCH 15.03.00.18 Install Guide, Revision Number 19, February 2013, available upon request to IPC Support.
©2015 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.