Abstract

These Application Notes describe the configuration steps required for IPC Alliance MX 15.03 to interoperate with Avaya Aura® Communication Manager 6.3 and 5.2.1, Avaya Aura® Session Manager 6.3 in a Centralized Messaging Environment using Avaya Modular Messaging 5.2.

IPC Alliance MX is a trading communication solution. In the compliance testing, IPC Alliance MX used E1 QSIG trunks to Avaya Aura® Communication Manager, for IPC turret users to obtain voice messaging services from Avaya Modular Messaging.

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 MX 15.03 to interoperate with Avaya Aura® Communication Manager 6.3 and 5.2.1, Avaya Aura® Session Manager 6.3 in a Centralized Messaging Environment using Avaya Modular Messaging 5.2.

IPC Alliance MX is a trading communication solution. In the compliance testing, IPC Alliance MX used E1 QSIG trunks to Avaya Aura® Communication Manager, for IPC turret users to obtain voice messaging services from Avaya Modular Messaging. E1 QSIG trunks were used from IPC Alliance MX to Avaya Aura® Communication Manager, and SIP trunks were used from Avaya Aura® Communication Manager to Avaya Aura® Session Manager to reach Avaya Modular Messaging. The Avaya Modular Messaging system in the Central site supported local subscribers from Avaya Aura® Communication Manager at the Central site, and from IPC turret users at the Remote site.

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 the Avaya Modular Messaging voicemail pilot to verify various call scenarios.

The serviceability test cases were performed manually by disconnecting and reconnecting the E1 connection to IPC.

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 testing included basic call, basic display, G.711/G.729, hold/reconnect, DTMF, call forwarding unconditional/ring-no-answer/busy, blind/attended transfer, and conference.

For Avaya Modular Messaging, the solution test verified only up to login, greeting, voice message, and message waiting indicator. The main features of Avaya Modular Messaging (ie, personal operator, auto attendant, find me, call me, call sender, and transfer) were not part of the test and not included during the compliance test.

The serviceability testing focused on verifying the ability of IPC Alliance MX to recover from adverse conditions, such as disconnecting/reconnecting the E1 connection to IPC Alliance MX.
2.2. Test Results
All test cases were executed and passed. The following were the observations from the compliance testing.

- IPC does not offer the Coverage feature, therefore coverage to voicemail for the turret users was accomplished by setting the Modular Messaging pilot number as the Call Forwarding destination for the users.

2.3. Support
Technical support on IPC Alliance MX can be obtained through the following:

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

As shown in Figure 1, IPC Alliance MX at the Remote Site consisted of the Alliance MX, System Center, and Turrets. E1 QSIG trunks were used from IPC Alliance MX to Communication Manager, and SIP trunks were used from Communication Manager to Session Manager to reach Avaya Modular Messaging. In the test configuration, QSIG allowed IPC turret users at the Remote Site to “cover” to Avaya Modular Messaging at the Central site for voice messaging services.

The configuration of Session Manager is performed via the web interface of System Manager. The detailed administration of basic connectivity among Communication Manager, Session Manager, and Avaya Modular Messaging is not the focus of these Application Notes and will not be described. These Application Notes will focus on the additional configuration required to support IPC turret users as local subscribers on Avaya Modular Messaging.

The detailed administration of E1 QSIG trunks between Communication Manager and IPC Alliance MX, to enable IPC turret users to reach users on Communication Manager and on the PSTN, is assumed to be in place with details described in [3] in Section 10.

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 user(s) at the Central site (Communication Manager 6.3 – 72xxx), Remote site (Communication Manager 5.2.1 – 22xxx), and IPC turret users at the Remote site (33xxx). The Avaya Modular Messaging pilot number was 7777.

The call path from an IPC turret is following:

[Alliance 15.03] ← (QSIG trunk) → [Avaya CM1 6.3] ← (H.323 trunks) → [Avaya CM2 5.2.1] ← (SIP trunk) → [Session-Manager 6.3] ← (SIP trunk) → [Modular Messaging 5.2]

Note: In this call path, Session Manager was used solely for a routing purpose.
Figure 1: Test Configuration of IPC Alliance with Avaya Aura® Communication Managers, Avaya Aura® Session Manager, and Avaya Modular Messaging
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 Aura® Communication Manager on Avaya S8300D Server</td>
<td>6.3 (R016x.03.0.124.0-20553)</td>
</tr>
<tr>
<td>Avaya G450 Media Gateway</td>
<td>33.13</td>
</tr>
<tr>
<td>Avaya Aura® Communication Manager on Avaya S8720 Server</td>
<td>5.2.1 (R015x.02.1.016.4-19880)</td>
</tr>
<tr>
<td>Avaya G650 Media Gateway</td>
<td></td>
</tr>
<tr>
<td>Avaya Aura® Session Manager</td>
<td>6.3 SP2</td>
</tr>
<tr>
<td>Avaya Aura® System Manager</td>
<td>6.3 SP2</td>
</tr>
<tr>
<td>Avaya Modular Messaging</td>
<td></td>
</tr>
<tr>
<td>• Messaging Storage Server</td>
<td>5.2 SP9</td>
</tr>
<tr>
<td>• Messaging Application Server</td>
<td>5.2 SP9</td>
</tr>
<tr>
<td>Avaya 96xx Series IP Telephones (H.323)</td>
<td>3.1</td>
</tr>
<tr>
<td>Avaya 96x1 Series IP Telephone (H.323)</td>
<td>6.22</td>
</tr>
<tr>
<td>Avaya DCP phone</td>
<td>-</td>
</tr>
<tr>
<td>IPC</td>
<td></td>
</tr>
<tr>
<td>• System Center</td>
<td>15.03.00.18c</td>
</tr>
<tr>
<td>• QSIG Line Card</td>
<td>15.03.00.17a</td>
</tr>
</tbody>
</table>
5. Configure Avaya Aura® Communication Manager

For a QSIG trunk configuration between Communication Manager and IPC Alliance, please refer to [3] in Section 10. Otherwise, there is no special configuration in Communication Manager.

This section describes the H.323 trunk configuration between Communication Manager 6.3 and Communication Manager 5.2.1. The following topics are discussed:

- Administer trunk group in Communication Manager 6.3.
- Administer hunt group in Communication Manager 6.3
- Administer hunt group in Communication Manager 5.2.1

Assumptions are made that routings (automatic alternate routing and route-pattern) in Communication Manager 6.3 and 5.2.1 are correctly set and working properly.

5.1. Administer a Trunk Group in Avaya Aura® Communication Manager 6.3 (CM1)

Administer an ISDN trunk group to interface with Communication Manager. Use the “add trunk-group n” command, where “n” is an available trunk group number. Enter the following values for the specified fields, and retain the default values for the remaining fields.

- Group Type: “isdn”
- Group Name: A descriptive name.
- TAC: An available trunk access code.
- Direction: “two-way”
- Carrier Medium: “H.323”
- Service Type: “tie”

```
change trunk-group 10
TRUNK GROUP
Group Number: 10                   Group Type: isdn          CDR Reports: y
Group Name: S8720-IP trunk              COR: 1        TN: 1        TAC: 1010
Direction: two-way        Outgoing Display? y         Carrier Medium: H.323
Dial Access? y              Busy Threshold: 255  Night Service:
Queue Length: 0
Service Type: tie
Auth Code? n
Member Assignment Method: auto
Signaling Group: 10
Number of Members: 10
```
Navigate to Page 2. For **Supplementary Service Protocol**, enter “b”. For **Digit Handling (in/out)**, enter “enbloc/enbloc”. Retain the default values for the remaining fields.

<table>
<thead>
<tr>
<th>TRUNK PARAMETERS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Codeset to Send Display: 6</td>
</tr>
<tr>
<td>Charge Advice: none</td>
</tr>
<tr>
<td><strong>Supplementary Service Protocol:</strong> b</td>
</tr>
<tr>
<td>Incoming Calling Number - Delete:</td>
</tr>
<tr>
<td>Disconnect Supervision - In? y Out? y</td>
</tr>
<tr>
<td>Digital Loss Group: 18</td>
</tr>
<tr>
<td>CONNECT Reliable When Call Leaves ISDN? n</td>
</tr>
<tr>
<td>CPN to Send for Redirected Calls: calling</td>
</tr>
</tbody>
</table>

Navigate to Page 3. Enable **Send Name** and **Send Calling Number**. For **Format**, enter “private”.

<table>
<thead>
<tr>
<th>TRUNK FEATURES</th>
</tr>
</thead>
<tbody>
<tr>
<td>ACA Assignment? n</td>
</tr>
<tr>
<td>Internal Alert? n</td>
</tr>
<tr>
<td>Data Restriction? n</td>
</tr>
<tr>
<td><strong>Send Name:</strong> y</td>
</tr>
<tr>
<td>Used for DCS? n</td>
</tr>
<tr>
<td>Suppress # Outpulsing? n</td>
</tr>
<tr>
<td>Format: private</td>
</tr>
<tr>
<td>UUI IE Treatment: shared</td>
</tr>
<tr>
<td>Maximum Size of UUI IE Contents: 128</td>
</tr>
<tr>
<td>Replace Restricted Numbers? n</td>
</tr>
<tr>
<td>Replace Unavailable Numbers? n</td>
</tr>
<tr>
<td>Send Connected Number: y</td>
</tr>
<tr>
<td>Hold/Unhold Notifications? y</td>
</tr>
<tr>
<td>Send UUI IE? y</td>
</tr>
<tr>
<td>Send UCID? y</td>
</tr>
<tr>
<td>Send Codeset 6/7 LAI IE? y</td>
</tr>
</tbody>
</table>

Note: **Communication Manager 5.2.1 (CM2) should have the same information in the trunk group form.**
5.2. Administer a hunt group in Avaya Aura® Communication Manager 6.3 (CM1)

To configure the hunt group, use the “add hunt-group n” command, where “n” is an available hunt-group number. On Page 2 of the hunt group form, enter the following values for the specified fields, and retain the default values for the remaining fields.

- **Message Center:** “qsig-mwi”
- **Voice Mail Number:** Enter the pilot number.
- **Routing Digits:** Enter the aar access code from the feature access code form.

![Hunt Group Configuration](image)

5.3. Administer a hunt group in Avaya Aura® Communication Manager 5.2.1 (CM2)

To configure the hunt group, use the “add hunt-group n” command, where “n” is an available hunt-group number. On Page 2 of the hunt group form, enter the following values for the specified fields, and retain the default values for the remaining fields.

- **Message Center:** “sip-adjunct”
- **Voice Mail Handle:** Enter the pilot number.
- **Routing Digits:** Enter the aar access code from the feature access code form.

![Hunt Group Configuration](image)
6. Configure Avaya Modular Messaging MSS

This section provides the procedures for configuring IPC turret users as local subscribers on Avaya Modular Messaging. 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** sub-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 33xxx 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. For the **Local Subscriber Mailbox Number** field toward the top of the screen, enter the first IPC turret user extension to add as a local subscriber, in this case “33309”. Click **Add or Edit**.

![Manage Subscribers Screen](image-url)
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**, **PBX Extension**, and **Email Handle** fields. Select the appropriate **Class Of Service**, and retain the default values in the remaining fields. Repeat this section to add all IPC subscribers.

### 7. Configure IPC Alliance MX

For the compliance test, no special configuration is needed for the IPC Alliance MX. For a QSIG trunk configuration between Communication Manager and IPC Alliance, please refer to [3] in **Section 10**.
8. Verification Steps

This section provides the tests that can be performed to verify proper configuration of Communication Manager, Avaya Modular Messaging, Session Manager, and IPC Alliance MX.

- Place a call from an IPC turret user, which is a subscriber in Modular Messaging, to the Modular Messaging pilot number. Verify that Modular Messaging recognizes the calling party as a local subscriber.
- Place calls from an IPC turret user to stations which are registered to Communication Manager 1. Verify there is two way audio.
- Place calls from an IPC turret user to stations which are registered to Communication Manager 2. Verify there is two way audio.

9. Conclusion

These Application Notes describe the configuration steps required for IPC Alliance MX 15.03 to successfully interoperate with Avaya Aura® Communication Manager 6.3, Avaya Aura® Communication Manager 5.2.1, Avaya Aura® Session Manager 6.3, and Avaya Modular Messaging 5.2 in a centralized messaging environment using QSIG trunks to Avaya Aura® Communication Manager 6.3. All feature and serviceability test cases were successfully completed with an observation noted in Section 2.2.

10. Additional References

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


