



Avaya Solution & Interoperability Test Lab

Application Notes for configuring Aculab's ApplianX IP Gateway to interoperate with Avaya Aura® Communication Manager R6.3 and Avaya Aura® Session Manager R6.3 using SIP Trunks - Issue 1.0

Abstract

These Application Notes describe the configuration steps for provisioning an Aculab ApplianX IP Gateway to permit Avaya Aura® Communication Manager using a SIP Trunk via Avaya Aura® Session Manager to communicate with a third party Private Branch Exchange via a QSIG Trunk.

Readers should pay attention to section 2, in particular the scope of testing as outlined in Section 2.1 as well as the observations noted in Section 2.2, to ensure that their own use cases are adequately covered by this scope and results.

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

The ApplianX IP Gateway can be used in a variety of TDM and VoIP migration strategies, whether it is connecting a TDM-based Private Branch Exchange (PBX) to a new IP network, or IP PBX, or providing a PSTN front end to SIP-based solutions. The ApplianX IP Gateway is a 'plug & play' gateway. On the PSTN side, the ApplianX IP Gateway provides one, two or four universal T1/E1 (USA, Japan, Europe, worldwide) interfaces, with a wide range of signalling protocols, including, SIP, PRI/ISDN types, T1 robbed bit and E1 CAS, R1, R2 and DTMF, plus PBX protocols, such as QSIG and DPNSS. A different protocol can be selected for each trunk.

2. General Test Approach and Test results

The general test approach was to configure a SIP trunk and an E1 QSIG trunk on the Aculab ApplianX IP Gateway (ApplianX). The SIP trunk connected to the VoIP port on the ApplianX then converted the signalling to QSIG and vice versa. A SIP Entity and Entity Link were configured on Session Manager so as to route calls to and from the ApplianX. Testing focused on verifying that SIP and QSIG signals were converted correctly.

Note: During compliance testing Communication Manager was connected to the VoIP port on the ApplianX was known as the SIP PBX and the Communication Manager connected to the E1/T1 port on the ApplianX was known as the QSIG PBX.

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 testing included:

- Verification of connectivity between Communication Manager (SIP PBX) and Communication Manager (QSIG PBX) via the ApplianX IP Gateway
- Basic call tests: Calls from SIP PBX to QSIG PBX and vice versa
- Calls On Hold/Release
- Transfers and Conferences
- Call Waiting
- DTMF
- Route Optimisation (Path Replacement)
- Call Diverts

2.2. Test Results

Tests were performed to insure full interoperability of an Aculab ApplianX IP Gateway when configured for SIP (using Session Manager) and QSIG. The tests were all functional in nature and performance testing was not included. All the test cases passed successfully with the following observations:

- Music on Hold is not a supported feature on the ApplianX IP Gateway in this solution.
- Message Waiting Indication is not supported on this version of ApplianX IP Gateway software.

Note: Although during testing a Communication Manager and Media Gateway was configured with QSIG trunks, an ApplianX IP Gateway will function with any PBX supporting QSIG.

2.3. Support

Technical support can be obtained for Aculab products as follows:

- E-mail: support@aculab.com
- Phone: +44(0)1908 273805

Note: An Aculab support contract is required to gain access to Aculab support services.

3. Reference Configuration

Figure 1 illustrates the network configuration used during compliance testing. Communication Manager was configured to use SIP to connect to the VoIP port on the ApplianX via the Session Manager. An E1/T1 port on the ApplianX was configured for QSIG and connected directly to the E1/T1 port on the G430. Avaya 9608 (H.323), 9641G (H.323) and Avaya 2420 digital telephones were used to make and receive calls via the ApplianX. System Manager was used to manage the Communication Manager.

Note: Communication Manager, Session Manager, and System Manager were run on a virtual environment. During compliance testing the PBX hosting the QSIG trunk was a Communication Manager and G430 media gateway.

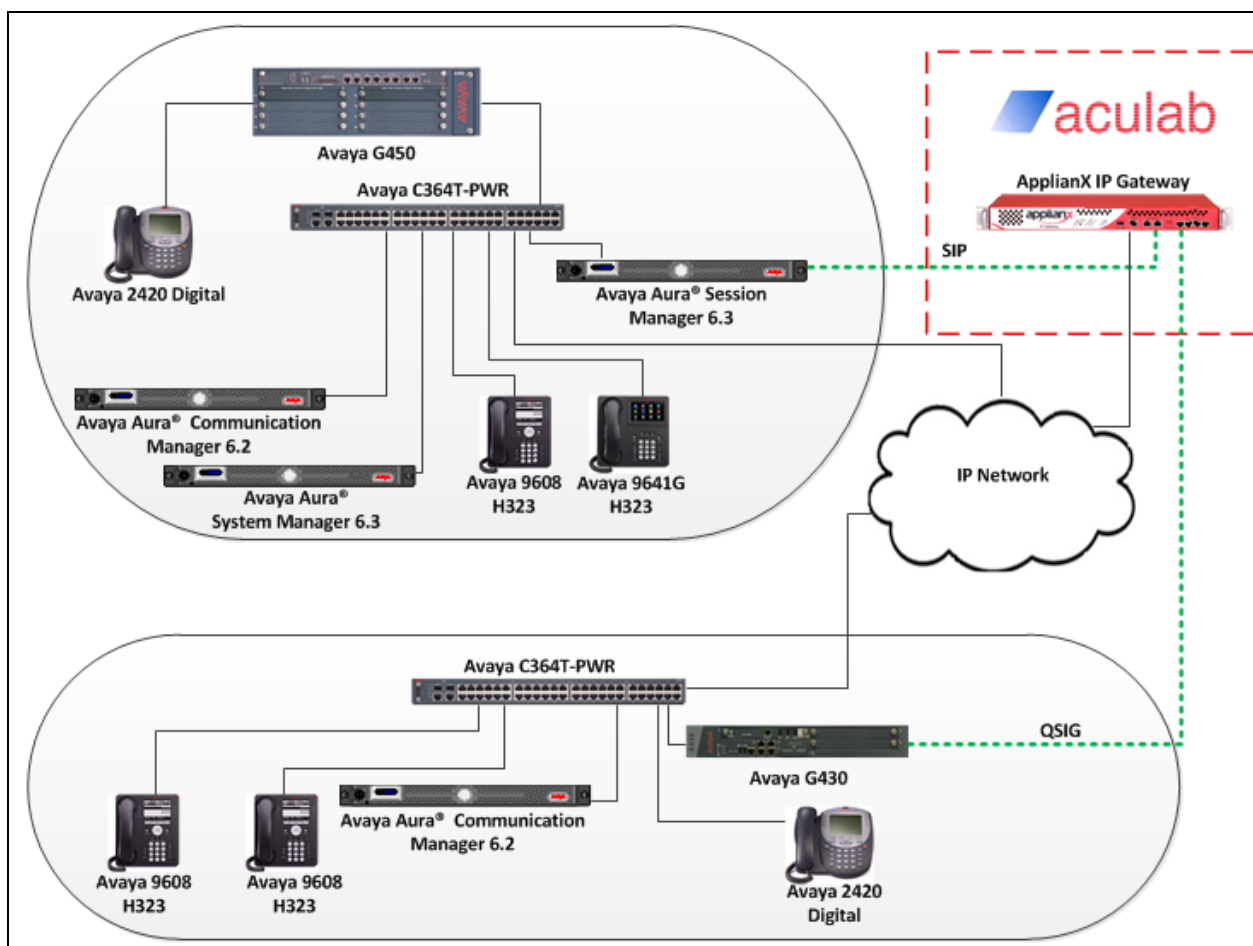


Figure 1: Avaya Aura® Communication Manager/Avaya Aura® Session Manager and Aculab ApplianX IP Gateway Reference Configuration

4. Equipment and Software Validated

The hardware and associated software used in the compliance testing is listed below.

Avaya Equipment	Software Version
Avaya Aura® Communication Manager	Avaya Aura® Communication Manager R6.2 Build R016x.02.0.832.0
Avaya Aura® Session Manager	R6.3 Build 6.3.0.8.5682-6.3.8.2826 Update 6.3.5.52017
Avaya Aura® System Manager	R6.3 Build 6.3.5.0.635005
Avaya 9608 IP phone	S9608_11HALBR6_2_4_08_V452
Avaya 9641G IP Phone	S9621_11HALBR6_2_4_08_V452
Avaya 2420 Digital phone	Rel 6.0, FWV 6
Aculab Equipment	Software Version
ApplianX IP Gateway	Version 2.3.1 release 792
Gateway Engine	Version 1.5.2-208

Table 1: Hardware and Software Version Numbers

Note: The 3rd –Party QSIG PBX was an Avaya Aura® Communication Manager 6.3 and Avaya G430 Gateway

5. Configure Avaya Aura® Communication Manager

Configuration and verification operations on Communication Manager illustrated in this section were all performed using Avaya Site Administrator. The information provided in this section describes the configuration of Communication Manager for this solution. It is implied that a working system is already in place. For all other provisioning information, such as initial installation and configuration, please refer to the product documentation in **Section 10**. The configuration operations described in this section can be summarized as follows: (**Note:** during compliance testing all inputs not highlighted in bold were left as default)

- Configure Session Manager Node
- Configure Signaling-Group
- Configure Trunk Group

Note: The configuration of the QSIG PBX is outside of the scope of these Application Notes. The ApplianX will interoperate with a wide range of PBXs supporting QSIG trunks.

5.1. Configure Session Manager Node

For Communication Manager to communicate with Session Manager a node must be configured on Communication Manager. Use the **change node-name ip** command and configure the following:

- **Name** Enter an informative for the Session manager node (i.e. **sm62vmmc-sig**)
- **IP Address** Enter the IP address of the Session Manager (10.10.60.14)

change node-names ip		Page 1 of 2	
		IP NODE NAMES	
Name	IP Address		
aes62vmmc	10.10.60.10		
default	0.0.0.0		
procr	10.10.60.11		
procr6	::		
sm62vmmc-sig	10.10.60.14		

5.2. Configure Signaling Group

A signaling group is required before a trunk-group can be configured. Use the **add signaling-group** command followed by next available signaling group number to configure the following:

- **Group Type:** Enter **SIP**
- **Transport Method** Enter **tcp**
- **Near-end Node Name:** Enter **procr**
- **Far-end Node Name:** Enter **sm62vmmc-sig** (Session Manager Node as configured in **Section 5.1**)
- **Far-end Network Region:** Enter the appropriate Network region (i.e. 1)
- **Far End Domain:** Enter the appropriate Domain (note: during compliance testing no Domain was used)
- **Initial IP-IP Direct Media:** Enter **y**
- **H323 Station Outgoing Direct Media:** Enter **y**

```

add signaling-group 1                                     Page 1 of 2
                                SIGNALING GROUP

Group Number: 1                      Group Type: sip
IMS Enabled? n                      Transport Method: tcp
    Q-SIP? n
    IP Video? n                      Enforce SIPS URI for SRTP? y
Peer Detection Enabled? y Peer Server: SM

Near-end Node Name: procr              Far-end Node Name: sm62vmcmc-sig
Near-end Listen Port: 5060            Far-end Listen Port: 5060
                                Far-end Network Region: 1

Far-end Domain:

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

```

5.3. Configure Trunk Group

This section describes the trunk group configuration used during compliance. Use the **add trunk-group** command followed by next available group number to configure the following:

- **Group Type:** Enter **sip**
- **Group Name:** Enter an informative name for the trunk (i.e. **To SM62VMC**)
- **TAC** Enter a TAC number i.e. **701**
- **Service Type:** Enter **tie**
- **Signaling Group:** Enter the Signaling Group number as configured in **Section 5.2**
- **Number of Members:** Enter the number of channels require to connect to the Session Manger (during compliance testing 15 channels were used)

```
add trunk-group 1                                     Page 1 of 21
TRUNK GROUP
Group Number: 1                                     Group Type: sip          CDR Reports: y
Group Name: To SM62VMC                             COR: 1                 TN: 1          TAC: 701
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: 1
                                                Number of Members: 15
```

Go to **Page 3** and enter the following:

- **Numbering format:** Enter **private**

```
add trunk-group 1                                     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
Modify Tandem Calling Number: no
Show ANSWERED BY on Display? y
```


Go to **Page 4** and enter the following:

- **Send Transferring Party Information?:** Enter y
- **Network Call Redirection?:** Enter y
- **Always Use re-INVITE for Display Updates?:** Enter y

add trunk-group 1	Page 4 of 21
PROTOCOL VARIATIONS	
Mark Users as Phone? n	
Prepend '+' to Calling Number? n	
Send Transferring Party Information? y	
Network Call Redirection? y	
Send Diversion Header? n	
Support Request History? n	
Telephone Event Payload Type:	
Convert 180 to 183 for Early Media? n	
Always Use re-INVITE for Display Updates? y	
Identity for Calling Party Display: P-Asserted-Identity	
Enable Q-SIP? n	

The screen shot below shows the trunk group members used during compliance testing.

add trunk-group 1	Page 5 of 21
TRUNK GROUP	
Administered Members (min/max): 1/15	
Total Administered Members: 15	
GROUP MEMBER ASSIGNMENTS	
Port	Name
1: T00001	To SM62VMM
2: T00002	To SM62VMM
3: T00003	To SM62VMM
4: T00004	To SM62VMM
5: T00005	To SM62VMM
6: T00006	To SM62VMM
7: T00007	To SM62VMM
8: T00008	To SM62VMM
9: T00009	To SM62VMM
10: T00010	To SM62VMM
11: T00011	To SM62VMM
12: T00012	To SM62VMM
13: T00013	To SM62VMM
14: T00014	To SM62VMM
15: T00015	To SM62VMM

6. Configuring Avaya Aura® Session Manager

A number of configurations are required to enable Session Manager to route calls between Communication Manager and ApplianX. All configurations of Session Manager are performed using System Manager. The configuration operations described in this section can be summarized as follows:

- Logging on to Avaya Aura® System Manager
- Administer SIP Domain
- Administer Locations
- Create ApplianX as a SIP Entity
- Create an Entity Link for ApplianX
- Create a Routing Policy for ApplianX
- Create a Dial Pattern for ApplianX

Note: It is implied a working system is already in place, including a Location, a SIP Entity an Entity Link, a Routing Policy and a Dial Pattern to route calls to Communication Manager, which are outside the scope of these Application Notes.

6.1. Logging on to Avaya Aura® System Manager

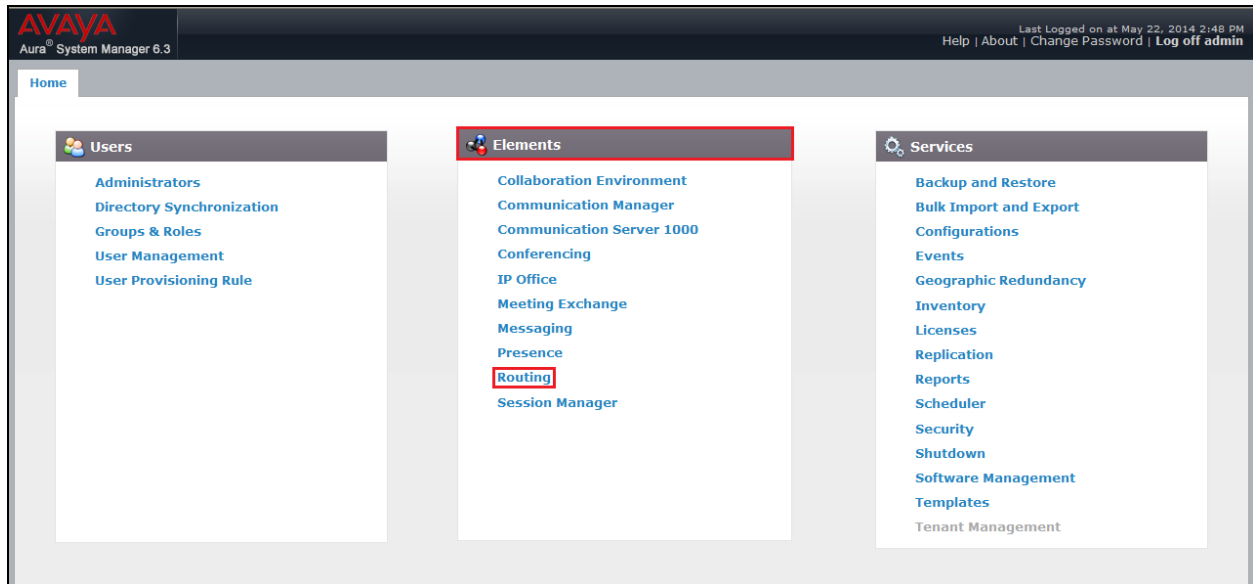
Log on by accessing the browser-based GUI of System Manager, using the URL “http://<fqdn>/SMGR” or “http://<ip-address>/SMGR”, where:

“<fqdn> is the fully qualified domain name of System Manager or the “<ip-address>” is the IP address of System Manager.

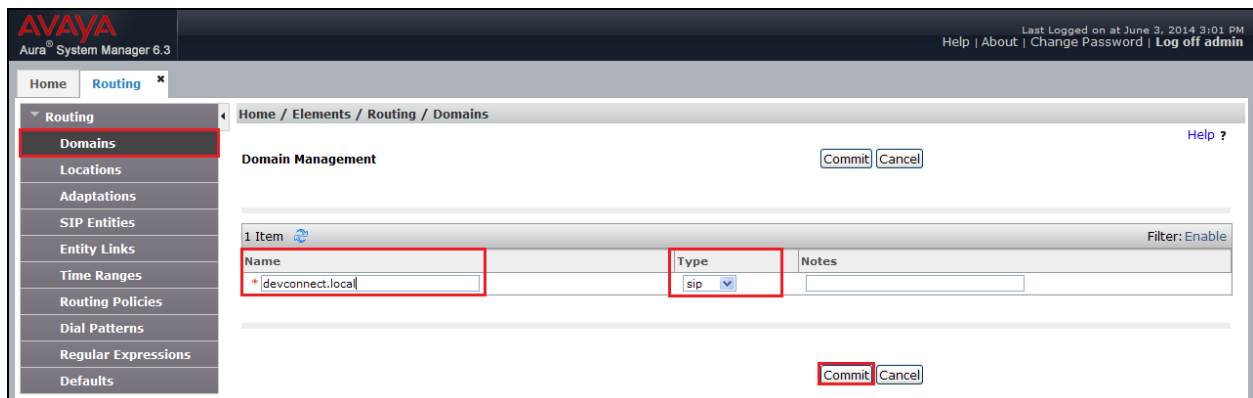
Once the System Manager Web page opens, log in with the appropriate credentials and click on the **Log On** button.

6.2. Administer SIP Domain

Once logged in, select **Routing** from under the **Elements** column.

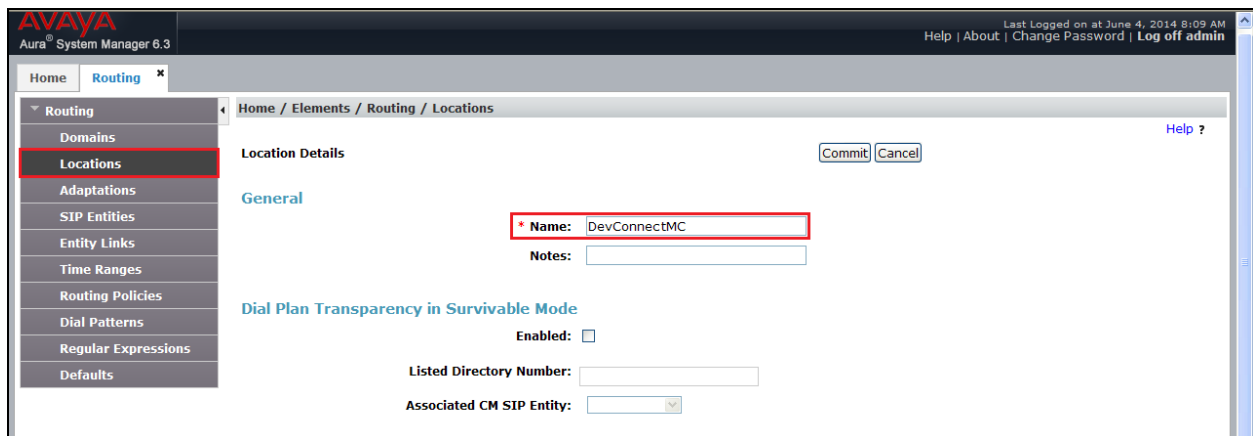


Select **Domains** on the left panel menu and then click on the **New** button (not shown). In the **Name** field enter the domain of the enterprise (i.e., devconnect.local) and select **sip** from the dropdown box. Click **Commit** to save changes.



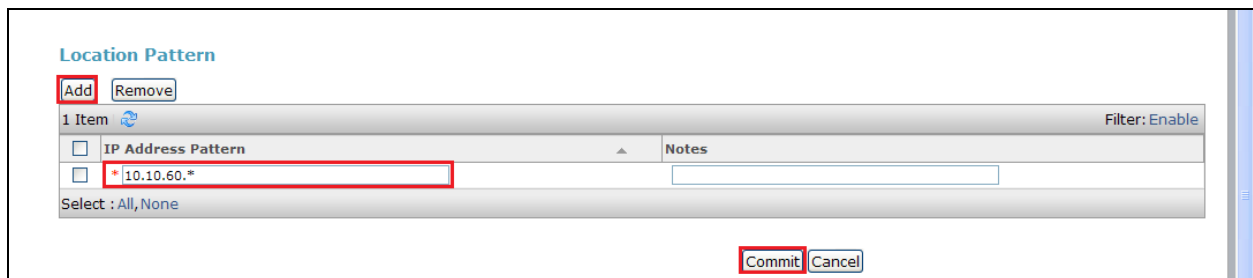
6.3. Administer Locations

Locations can be used to identify logical and/or physical locations where SIP Entities reside for the purposes of bandwidth management. One location is added to the sample configuration for all of the enterprise SIP entities. Select **Locations** on the left panel menu and then click on the **New** button (not shown). In the **Name** field enter an informative name for the location (i.e., DevconnectMC). During compliance testing, all other fields were left at default values.



The screenshot shows the Avaya Aura System Manager 6.3 interface. The left sidebar has a menu with 'Locations' highlighted. The main content area is titled 'Home / Elements / Routing / Locations'. It shows 'Location Details' with a 'Name' field containing 'DevConnectMC'. There are 'Commit' and 'Cancel' buttons. Below the 'Name' field is a 'Notes' field. Further down, there is a section 'Dial Plan Transparency in Survivable Mode' with an 'Enabled' checkbox. At the bottom, there are fields for 'Listed Directory Number' and 'Associated CM SIP Entity'.

Scroll to the bottom of the page and under **Location Pattern**, click **Add**, and enter an **IP Address Pattern** in the resulting new row. The * is used to specify any number of allowed characters at the end of the string. Below is the location configuration used during compliance testing.



The screenshot shows the 'Location Pattern' configuration page. It has an 'Add' button highlighted. Below it is a table with one row. The table has two columns: 'IP Address Pattern' and 'Notes'. The first row contains '*10.10.60.*' in the 'IP Address Pattern' column. At the bottom right, there are 'Commit' and 'Cancel' buttons.

IP Address Pattern	Notes
10.10.60.	

6.4. Create ApplianX as a SIP Entity

A SIP Entity must be added for the ApplianX. To add a SIP Entity, select **SIP Entities** on the left panel menu and then click on the **New** button (not shown).

Note: A SIP Entity was already configured for Communication Manager and was called **CM63**.

Enter the following for the ApplianX SIP Entity:

Under **General** enter the following:

- **Name** Enter an informative name (e.g., **applianx**)
- **FQDN or IP Address** Enter the IP address of the signalling interface of the ApplianX
- **Type** Select **SIP Trunk** from the dropdown box
- **Location** Select the location from the dropdown box that was configured in **Section 6.3**
- **Time Zone** Select Time zone for this location from the dropdown box
- **SIP Timer** Enter **4**

Once the correct information is entered click the **Commit** Button.

Note: During compliance testing **Adaptation** was left blank.

The screenshot shows the Avaya Aura System Manager 6.3 web interface. The left sidebar has a menu with 'SIP Entities' highlighted. The main content area is titled 'SIP Entity Details' and 'General'. The form contains the following fields:

- Name:** Applianx
- FQDN or IP Address:** 10.10.60.40
- Type:** SIP Trunk (dropdown)
- Notes:** SIP Trunk to ApplianX
- Adaptation:** (empty dropdown)
- Location:** DevConnectMC (dropdown)
- Time Zone:** Europe/Dublin (dropdown)
- SIP Timer B/F (in seconds):** 4
- Credential name:** (empty text field)
- Call Detail Recording:** egress (dropdown)

At the top right of the form are 'Commit' and 'Cancel' buttons. The breadcrumb trail at the top reads 'Home / Elements / Routing / SIP Entities'.

6.5. Create an Entity Link for ApplianX

The SIP trunk between Session Manager and the ApplianX requires an Entity Link.

To add an Entity Link, select **Entity Links** on the left panel menu and click on the **New** button, (not shown), enter the following:

- **Name** An informative name, (e.g. **Applianx_5060_TCP**)
- **SIP Entity 1** Select **Session Manager 1** from the **SIP Entity 1** dropdown box
- **Protocol** Select **TCP** from the Protocol drop down box
- **Port** Enter **5060**
- **SIP Entity 2** Select **applianx** from the **SIP Entity 2** dropdown box (configured in **Section 6.4**)
- **Port** Enter **5060** as the Port
- **Connection Policy** Check the **Trusted** check box

Click **Commit** to save changes. The following screen shows the Entity Links used.

AVAYA
Aura® System Manager 6.3

Last Logged on at May 22, 2014 2:48 PM
Help | About | Change Password | Log off admin

Home Routing

Routing
Domains
Locations
Adaptations
SIP Entities
Entity Links
Time Ranges
Routing Policies
Dial Patterns
Regular Expressions
Defaults

Home / Elements / Routing / Entity Links

Entity Links

Commit Cancel

1 Item

	Name	SIP Entity 1	Protocol	Port	SIP Entity 2	DNS Override	Port	Connection Policy	Deny New Service	Notes
<input type="checkbox"/>	*Applianx_5060_TCP	*Session Manager 1	TCP	*5060	*Applianx	<input type="checkbox"/>	*5060	trusted	<input type="checkbox"/>	

Select : All, None

6.6. Create a Routing Policy for ApplianX

Create routing policies to direct calls to the ApplianX via Session Manager. To add a routing policy, select **Routing Policies** on the left panel menu and then click on the **New** button (not shown). In **Routing Policy Details** enter an informative name in the **Name** field, (example **To applianx**), and enter **0** in the **Retries** field. At **SIP Entity as Destination**, click the **Select** button. A Routing Policy was also configured to direct calls to Communication Manager, but is outside the scope of these Application Notes.

AVAYA
Aura® System Manager 6.3

Last Logged on at May 22, 2014 2:48 PM
Help | About | Change Password | Log off admin

Home Routing

Home / Elements / Routing / Routing Policies

Routing Policy Details

Commit Cancel

General

* Name: To applianx

Disabled: ☐

* Retries: 0

Notes: Calls to applianx

SIP Entity as Destination

Select

Once the **SIP Entity** list screen opens, check the **applianx** radio button. Click on the **Select** button to confirm the chosen options and then return to the Routing Policies Details screen and select the **Commit** button (not shown) to save.

AVAYA
Aura® System Manager 6.3

Last Logged on at May 22, 2014 2:48 PM
Help | About | Change Password | Log off admin

Home Routing

Home / Elements / Routing / Routing Policies

SIP Entities

Select Cancel

SIP Entities

4 Items Filter: Enable

Name	FQDN or IP Address	Type	Notes
6.3 CM	10.10.16.211	CM	Richards CM6.3
Applianx	10.10.60.40	SIP Trunk	SIP Trunk to ApplianX
CM62VMC	10.10.60.11	CM	
Session Manager 1	10.10.60.14	Session Manager	

Select : None

6.7. Create a Dial Pattern for ApplianX

A dial pattern must be created on Session Manager to route calls to and from the ApplianX. During compliance testing a number of patterns were used. The example below shows 4. To configure the Dial Pattern to route calls to the ApplianX, select **Dial Patterns** on the left panel menu and then click on the **New** button (not shown). A Dial Pattern was also configured to route calls to Communication Manager, but is outside the scope of these Application Notes. Under **General** enter out the following:

- **Pattern** Enter 4
- **Min** Enter 4 as the minimum length of dialed number
- **Max** Enter 4 as the maximum length of dialed number
- **SIP Domain** Select **All** from the drop down box

Click the **Add** button in **Originating Locations and Routing Policies**.

The screenshot shows the Avaya Aura System Manager 6.3 interface. The top navigation bar includes 'Home' and 'Routing' tabs. The left sidebar lists various configuration options: Domains, Locations, Adaptations, SIP Entities, Entity Links, Time Ranges, Routing Policies, Dial Patterns, Regular Expressions, and Defaults. The main content area is titled 'Dial Pattern Details' and contains a 'General' tab. The 'Pattern' field is set to '4', 'Min' is '4', and 'Max' is '4'. The 'SIP Domain' dropdown is set to '-ALL-'. The 'Emergency Call' checkbox is unchecked, 'Emergency Priority' is '1', and 'Emergency Type' is empty. The 'Notes' field is empty. At the bottom, the 'Originating Locations and Routing Policies' section has an 'Add' button highlighted with a red box. The top right corner shows the user is logged in as 'admin' and the last login time is 'May 22, 2014 2:48 PM'.

In **Originating Location** check the **DevConnectMC** check box. Under **Routing Policies** check the **To applanx** check box. Click on the **Select** button to confirm the chosen options and then be returned to the Dial Pattern screen (shown previously), select **Commit** button to save (not shown).

AVAYA
Aura® System Manager 6.3

Last Logged on at May 22, 2014 2:48 PM
Help | About | Change Password | Log off admin

Home Routing

Home / Elements / Routing / Dial Patterns

Originating Location Select Cancel

Originating Location

☐ Apply The Selected Routing Policies to All Originating Locations

1 Item Filter: Enable

<input checked="" type="checkbox"/>	Name	Notes
<input checked="" type="checkbox"/>	DevConnectMC	

Select : All, None

Routing Policies

2 Items Filter: Enable

<input type="checkbox"/>	Name	Disabled	Destination	Notes
<input type="checkbox"/>	CM1	<input type="checkbox"/>	CM62VMC	Call to CM1 (6.2)
<input checked="" type="checkbox"/>	To applanx	<input type="checkbox"/>	Applanx	Calls to applanX

Select : All, None

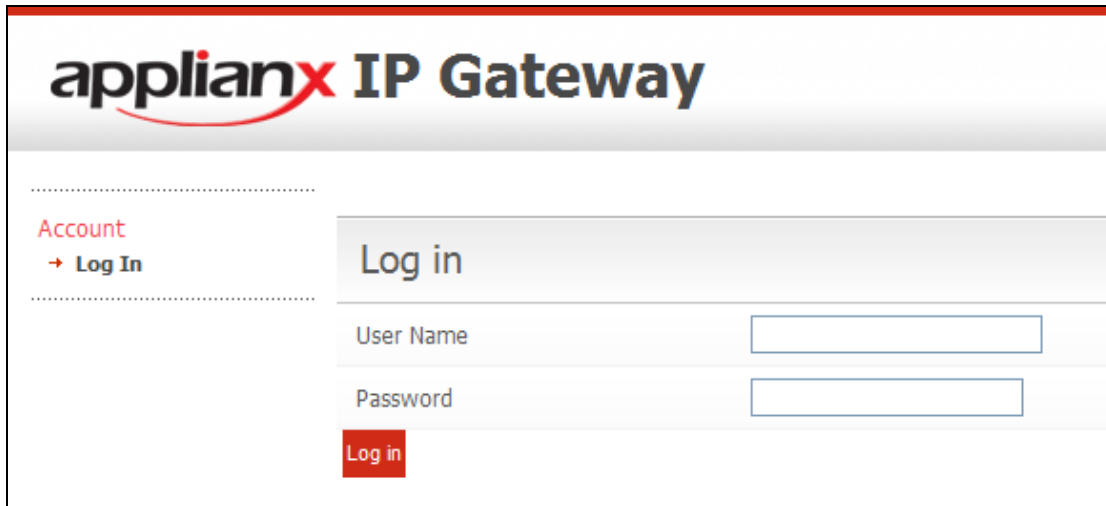
7. Configure Aculab ApplianX IP Gateway

A number of steps are required to configure the Aculab ApplianX IP Gateway, the initial assigning of the administration IP address, administration user name and password are assumed to be completed. The configuration operations described in this section can be summarized as follows:

- Login to ApplianX IP Gateway
- Run the Setup Wizard
- Configure QSIG Trunk
- Configure SIP Trunk
- Configure Endpoints
- Configure Groups
- Configure Routes
- Configure SIP
- Configure Codecs
- Save configuration
- Use configuration

7.1. Login to ApplianX IP Gateway

Login by accessing the browser-based GUI, using the URL *http://<ip-address>* assigned to the ApplianX. Once the ApplianX IP Gateway web page opens, log in with the appropriate credentials and click on the **Log in** button.



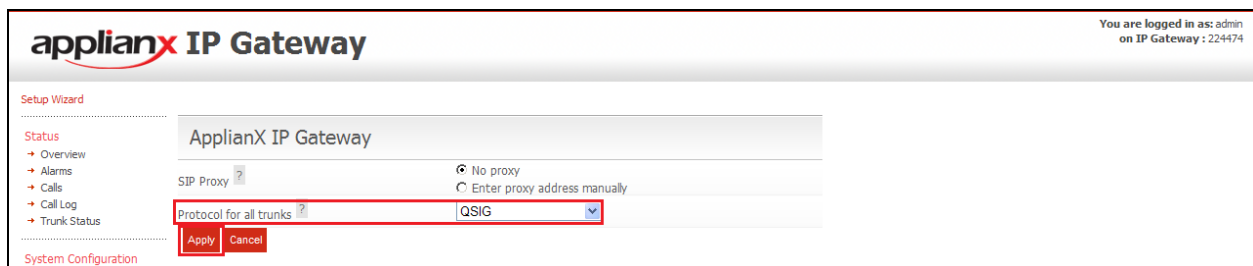
The screenshot shows the login interface for the ApplianX IP Gateway. At the top, the logo 'applianx IP Gateway' is displayed. Below the logo, there is a 'Log in' section. On the left side of this section, there is a link labeled 'Account' with a red arrow pointing to 'Log In'. The 'Log in' section contains two input fields: 'User Name' and 'Password'. Below these fields is a red button labeled 'Log in'.

7.2. Run the Setup Wizard

After the main web page opens, select **Setup Wizard** from System Configuration section.



Once the **Setup Wizard** page opens, select **QSIG** from the **Protocol for all trunks**, drop-down box, and click on the **Apply** button.



After clicking the **Apply** button in the previous step, the **Edit Configurations** page opens. Click on the **Edit** button for **My Configuration**.

applianceX IP Gateway You are logged in as: admin
on IP Gateway : 224474

Edit Configurations

Status

- Overview
- Alarms
- Calls
- Call Log
- Trunk Status

System Configuration

- Global Configuration
- Networking
- Setup Wizard
- SIP Credentials

Gateway Configuration

- Alias Registrar
- DDI Barring
- Edit Configurations**

Edit Configurations

Active configuration

Name	Description	Last updated		
Change with Bridge media Qsig - DG		2013-12-06 06:14:08	Running	View Copy

Available configurations

Name	Description	Last updated		
My configuration		2014-02-05 08:51:34	Edit	Delete Copy Use

[Delete Multiple Configurations](#)

In the **General** tab, give a descriptive name to the configuration. During compliance testing, **Avaya SIP-QSIG Test** was used.

applianceX IP Gateway You are logged in as: admin
on IP Gateway : 224474

Edit Configurations > Gateway Configuration

Status

- Overview
- Alarms
- Calls
- Call Log
- Trunk Status

System Configuration

- Global Configuration
- Networking
- Setup Wizard

Editing: Avaya SIP-QSIG Test

General **Trunks** **Endpoints** **Groups** **Routes** **Clocking** **SIP** **Codecs** **Survivability** **Test**

General Configuration Information

Configuration name:

Configuration description:

7.3. Configure QSIG Trunk

Click on the **Trunks** Tab followed by the **Trunk 1 Edit** button. This trunk was configured for QSIG. A cable was connected between the E1/T1 Trunk 1 port on the front of the ApplianX and the T1/E1 port on the G430 Gateway of the Communication Manager. Please note that the configurations of the QSIG trunk are dependent on the configuration of the QSIG gateway of connecting PBX, pay special attention to the Master/Slave configuration. The screenshots in this section relate to the configuration used during compliance testing of this solution.

The screenshot displays the 'applianx IP Gateway' web interface. The top right corner indicates the user is logged in as 'admin' on 'IP Gateway : 224474'. The left sidebar contains a navigation menu with sections: Status (Overview, Alarms, Calls, Call Log, Trunk Status), System Configuration (Global Configuration, Networking, Setup Wizard, SIP Credentials), Gateway Configuration (Alias Registrar, DDI Barring, Edit Configurations, Interoperability, Cause Mappings), and Diagnostics (Remote Logging, Network Diagnostics, Watchdog Status). The main content area is titled 'Editing: Avaya SIP-QSIP Test' and features a tabbed interface with 'General', 'Trunks', 'Endpoints', 'Groups', 'Routes', 'Clocking', 'SIP', 'Codecs', 'Survivability', and 'Test'. The 'Trunks' tab is active, showing two sections: 'SIP trunks' and 'TDM trunks'. The 'SIP trunks' section contains a table with one entry, 'Trunk 5', which is of type 'SIP' and belongs to the 'No group'. The 'TDM trunks' section contains a table with four entries: 'Trunk 1', 'Trunk 2', 'Trunk 3', and 'Trunk 4', all of type 'TDM' and belonging to the 'TDM trunks' group. Each entry in the 'TDM trunks' table has an 'Edit' button. At the bottom of the 'TDM trunks' table, there are three buttons: 'Save Changes', 'Save and Return', and 'Cancel Changes'.

Name	Description	Type	Group	
Trunk 5		SIP	No group	Edit

Name	Description	Type	Group	
Trunk 1		TDM	TDM trunks	Edit
Trunk 2		TDM	TDM trunks	Edit
Trunk 3		TDM	TDM trunks	Edit
Trunk 4		TDM	TDM trunks	Edit

In the **Trunk Name** field (i.e., Avaya QSIG Trunk) and in the **Trunk description** field enter a description (i.e., Trunk to Avaya G430). Configure the remaining fields as shown in the following screen shot. Click on the **Change** button in the **Protocol configuration** section.

applanix IP Gateway You are logged in as: admin on IP Gateway : 224474

Edit Configurations > Trunk Overview > Edit Trunk

Status

- Overview
- Alarms
- Calls
- Call Log
- Trunk Status

System Configuration

- Global Configuration
- Networking
- Setup Wizard
- SIP Credentials

Gateway Configuration

- Alias Registrar
- DDI Barring
- Edit Configurations**
- Interoperability
- Cause Mappings

Diagnostics

- Remote Logging
- Network Diagnostics
- Watchdog Status
- Restart
- Diagnostic Log
- Endpoint Status
- About
- Hardware

Account

- Log Out
- Change Password

Editing: Avaya SIP-QSIG Test

Apply Cancel

General settings

Trunk name: Avaya QSIG Trunk

Trunk description: Trunk to Avaya G430

Open inward speech path before answer: ☒

Routing group: TDM trunks

Block trunk from call activity: No

Outgoing timeslot allocation strategy: Lowest available

Minimum digit count: 0

Interdigit timeout (milliseconds): 3000

Interdigit timeout for virtual calls (milliseconds): 1000

Send sending complete on outgoing calls: ☒

Send overlap digits on outgoing calls: ☒

Response to unroutable incoming calls: Release

SNMP configuration

Enable SNMP traps: ☒

Protocol configuration

Protocol: QSIG Edit Change

Click on the **Select** button for **QSIG**.

applanix IP Gateway You are logged in as: admin on IP Gateway : 224474

Select a protocol

Status

- Overview
- Alarms
- Calls
- Call Log
- Trunk Status

System Configuration

- Global Configuration
- Networking
- Setup Wizard
- SIP Credentials

Gateway Configuration

- Alias Registrar
- DDI Barring
- Edit Configurations**
- Interoperability
- Cause Mappings

Diagnostics

- Remote Logging
- Network Diagnostics
- Watchdog Status
- Restart
- Diagnostic Log
- Endpoint Status
- About

Select a protocol

DPNSS	DPNSS Enhanced. Conforming to BTNR-188.	Select
QSIG	QSIG, also known as PSS1. Conforming to ECMA-143.	Select
ETS300	EuroISDN. Conforming to ETS300-102.	Select
INS1500	T1 Q.931 variant conforming to the INS-Net Interface and Services specification published by the NTT.	Select
DASS	DASS2 conforming to BTNR 190	Select
AT&T	T1 Q.931 variant conforming to AT&T TR 41459. Sometimes called 5ESS.	Select
DMS100	T1 Q.931 variant conforming to the Nortel NIS-A211-1 Primary Rate User-Network Interface Specification.	Select
NI2	T1 Q.931 variant conforming to National ISDN 2 (Belcore).	Select
E1LS	'E1 Linese' as implemented by AT&T Definity and Nortel Meridian switches. E&M Immediate Start, Delay Dial and Wink Start, Loopstart User (LSU) and Loopstart Network (LSN), Feature Group B (FGB), and Feature Group D (FGD) configuration options available. MFR1, DTMF or Decadic Register signalling available. (A-Law)	Select
T1RB	A highly configurable implementation of T1 Robbed Bit. E&M Immediate Start, Delay Dial and Wink Start, Loopstart User (LSU) and Loopstart Network (LSN), Feature Group B (FGB), and Feature Group D (FGD) configuration options available. MFR1, DTMF or Decadic Register signalling available. (U-Law)	Select
R2T1	A highly configurable implementation of R2 based on the CCITT Blue Book, a collection of Ericsson specifications, and a multitude of National signalling specifications. MFCR2 DTMF or Decadic Register signalling available. (A-Law)	Select
IEM	Indonesian E&M protocol. Also known as discontinuous line signalling. MFCR2 Register signalling. (A-Law)	Select
T1HK	T1 Robbed Bit for Hong Kong. MFR1, DTMF or Decadic Register signalling available. (U-Law)	Select

Cancel

Configure all as is shown in the following screen shots.

applianx IP Gateway

You are logged in as: admin
on IP Gateway : 224474

Protocol Options

Status

- Overview
- Alarms
- Calls
- Call Log
- Trunk Status

System Configuration

- Global Configuration
- Networking
- Setup Wizard
- SIP Credentials

Gateway Configuration

- Alias Registrar
- DDI Barring
- Edit Configurations
- Interoperability
- Cause Mappings

Diagnostics

- Remote Logging
- Network Diagnostics
- Watchdog Status
- Restart
- Diagnostic Log
- Endpoint Status
- About
- Hardware

Account

- Log Out
- Change Password

QSIG

General settings

Trunk modeE1

Impedence120 Ohms (default)

CRC enabled?☒

Master/Slave configurationMaster, Priority B

Basic features

Display direction?

Send and receive

Loop avoidance mapping?

☐ Disabled

☒ Transparent

☐ Transit

Global transit limit?

25

Insert loop avoidance in outgoing calls?☐

Do-not-disturb mapping?☒

Party Category Mode?

Send using ANF-CMN (default)

Send progress indicators?☒

Allow incoming data calls?☒

Use 3.1KHz Audio bearer for speech?☐

Hold method?

None (default)

Call Offer Enabled?☒

Call Transfer Enabled?☒

Call Diversion Supplementary Service Support

MC, Reviewed:
SPOC 10/15/2014

Solution & Interoperability Test Lab Application Notes
2014 Avaya Inc. All Rights Reserved

Page 23 of 38
AX_SIP_QSIG

Continuation....

Call Diversion Supplementary Service Support	
Call Diversion Enabled ?	<input checked="" type="checkbox"/>
Divert as proxy ?	<input type="checkbox"/>
Divert unmatched to outgoing group ?	<input checked="" type="checkbox"/>
Send Diverted Address ?	<input checked="" type="checkbox"/>
Automatic Diversion Validation ?	<input type="checkbox"/>
Basic Service Type ?	Speech
Subscription Option Type ?	Notify With Number
'divertingLegInformation3.inv' Send Mode ?	Presentation Allowed
Default Party Number Type ?	Unknown
Include pSS1InfoElement Progress Indicator ?	<input checked="" type="checkbox"/>
CBWF/CBWN (CC) Supplementary Service Support	
CBWF/CBWN (CC) Enabled ?	<input checked="" type="checkbox"/>
Retain Signalling Connection ?	<input type="checkbox"/>
Message Waiting Supplementary Service Support	
Message Waiting Method ?	Facility (default)
Path Replacement Additional Network Feature	
Path Replacement Enabled ?	<input checked="" type="checkbox"/>
Dummy QSIG call identity ?	9999
Operate as originating end if other side cannot ?	<input checked="" type="checkbox"/>
Operate as terminating end if other side cannot ?	<input checked="" type="checkbox"/>
Allow Path Replacement proposal by terminating end also ?	<input type="checkbox"/>
Accept Path Replacement proposal when originating end ?	<input checked="" type="checkbox"/>
Delay in seconds after transfer before a Route Optimisation/Path Replacement proposal can be sent	30
Delay in seconds after a Route Optimisation/Path Replacement rejection before a new proposal can be sent	30

Enter the remaining values and click on the **Apply** button.

QSIG Protocol Compatibility	
Length of invoke ids (in bytes) ?	2
Facility protocol profile ?	0x9F - ISO (default)
Send NFE and Interpretation APDUs ?	<input checked="" type="checkbox"/>
Use global IDs in Facility ?	<input type="checkbox"/>
Raw configuration options	
Options ?	
Apply Cancel	

After returning to the **Editing** page, click on the **Apply** button.

aplianx IP Gateway You are logged in as: admin
on IP Gateway : 224474

Edit Configurations > Trunk Overview > Edit Trunk

Status

- Overview
- Alarms
- Calls
- Call Log
- Trunk Status

System Configuration

- Global Configuration
- Networking
- Setup Wizard
- SIP Credentials

Gateway Configuration

- Alias Registrar
- DDI Barring
- Edit Configurations**
- Interoperability
- Cause Mappings

Diagnostics

- Remote Logging
- Network Diagnostics
- Watchdog Status
- Restart
- Diagnostic Log
- Endpoint Status
- About
- Hardware

Account

- Log Out
- Change Password

Editing: Avaya SIP-QSIG TEST

Apply **Cancel**

General settings

Trunk name	Avaya QSIG Trunk
Trunk description	Trunk to Avaya G430
Open inward speech path before answer ?	<input checked="" type="checkbox"/>
Routing group	TDM trunks
Block trunk from call activity ?	No
Outgoing timeslot allocation strategy ?	Lowest available
Minimum digit count ?	0
Interdigit timeout (milliseconds) ?	3000
Interdigit timeout for virtual calls (milliseconds) ?	1000
Send sending complete on outgoing calls ?	<input checked="" type="checkbox"/>
Send overlap digits on outgoing calls ?	<input checked="" type="checkbox"/>
Response to unroutable incoming calls ?	Release

SNMP configuration

Enable SNMP traps	<input checked="" type="checkbox"/>
-------------------	-------------------------------------

Protocol configuration

Protocol	QSIG	Edit Change
----------	------	---------------------------

7.4. Configure SIP Trunk

To configure the SIP trunk, click on the **Trunk 5 Edit** button.

aplianx IP Gateway You are logged in as: admin
on IP Gateway : 224474

Edit Configurations > Trunk Overview

Status

- Overview
- Alarms
- Calls
- Call Log
- Trunk Status

System Configuration

- Global Configuration
- Networking
- Setup Wizard
- SIP Credentials

Gateway Configuration

- Alias Registrar
- DDI Barring
- Edit Configurations**
- Interoperability
- Cause Mappings

Diagnostics

- Remote Logging
- Network Diagnostics
- Watchdog Status

Editing: Avaya SIP-QSIG TEST

General **Trunks** **Endpoints** **Groups** **Routes** **Clocking** **SIP** **Codecs** **Survivability** **Test**

SIP trunks

Name	Description	Type	Group	
Trunk 5		SIP	No group	Edit

TDM trunks

Name	Description	Type	Group	
Avaya QSIG Trunk	Trunk to Avaya G430	TDM	TDM trunks	Edit
Trunk 2		TDM	TDM trunks	Edit
Trunk 3		TDM	TDM trunks	Edit
Trunk 4		TDM	TDM trunks	Edit

Save Changes **Save and Return** **Cancel Changes**

Enter a descriptive name in the **Trunk Name** field (i.e., Avaya SIP Trunk) and in the **Trunk description** field enter a description (i.e., SIP Trunk to Avaya SM). Configure the remaining fields as shown in the following screen shot. Click on the **Apply** button to save the changes.

The screenshot shows the 'applanx IP Gateway' interface. The top right corner indicates 'You are logged in as: admin on IP Gateway : 224474'. The breadcrumb trail is 'Edit Configurations > Trunk Overview > Edit Trunk'. The left sidebar contains a navigation menu with sections: Status (Overview, Alarms, Calls, Call Log, Trunk Status), System Configuration (Global Configuration, Networking, Setup Wizard, SIP Credentials), Gateway Configuration (Alias Registrar, DDI Barring, Edit Configurations, Interoperability, Cause Mappings), and Diagnostics (Remote Logging, Network Diagnostics, Watchdog Status, Restart, Diagnostic Log, Endpoint Status, About, Hardware). The main content area is titled 'Editing: Avaya SIP-QSIG TEST'. It features an 'Apply' button and a 'Cancel' button. Below these are three sections: 'General settings' with fields for 'Trunk name' (Avaya SIP Trunk) and 'Trunk description' (SIP Trunk to Avaya SM), and checkboxes for 'Open inward speech path before answer' (checked) and 'Response to unroutable incoming calls' (Release); 'SNMP configuration' with a checked 'Enable SNMP traps'; and 'For use under supervision of Aculab Technical Support' with a 'WARNING: Setting this value too high may result in system performance issues.' and a field for 'SIP Trunk Capacity' (120). At the bottom are buttons for 'Save Changes', 'Save and Return', and 'Cancel Changes'.

7.5. Configure Endpoints

The ApplanX requires information relating to Session Manager so as to communicate with Communication Manager. After clicking on the **Endpoints** tab, click on the icon for **Proxy** as shown in the screen shot below.

The screenshot shows the 'applanx IP Gateway' interface. The top right corner indicates 'You are logged in as: admin on IP Gateway : 224474'. The breadcrumb trail is 'Edit Configurations > SIP Endpoint Overview'. The left sidebar is identical to the previous screenshot. The main content area is titled 'Editing: Avaya SIP-QSIG TEST'. It features a tabbed interface with tabs: General, Trunks, Endpoints, Groups, Routes, Clocking, SIP, Codecs, Survivability, and Test. The 'Endpoints' tab is selected. Below the tabs are four rows of endpoint configuration: 'Default SIP Endpoint' (Default endpoint to match incoming SIP calls that don't match any other endpoint.), 'ApplanX IP Gateway self' (Certain supplementary services can result in the ApplanX IP Gateway being asked to call itself. This endpoint matches those calls and allows them to be routed correctly.), 'ApplanX IP Gateway registered users' (Destination for calls to registered users.), and 'Proxy' (A SIP proxy). The 'Proxy' row is highlighted with a red box. To the right of each row is a document icon. Below the 'Proxy' row is a red 'X' icon. At the bottom are buttons for 'Save Changes', 'Save and Return', and 'Cancel Changes'.

Enter a descriptive name in the **Name** field (i.e., Avaya Session Manager) and in the **Description** field enter a description (i.e., Avaya Session Manager Proxy). Configure the following in the remaining fields:

- **Routing Group** Select **Proxy group** from the dropdown box
- **Endpoint address** Enter the IP address of the Session Manager (this is the same IP address as configured in **Section 5.1**)
- **UDP port** Enter **5060**
- **TCP port** Enter **5060**

Configure the remaining fields as shown in the following screen shot.

The screenshot shows the 'applianceX IP Gateway' web interface. The top right corner indicates the user is logged in as 'admin' on IP Gateway : 224474. The breadcrumb trail is 'Edit Configurations > SIP Endpoint Overview > Edit SIP Endpoint'. The left sidebar contains navigation menus for Status, System Configuration, Gateway Configuration, Diagnostics, and Account. The main content area is titled 'Editing: Avaya SIP-QSIG TEST' and features 'Apply' and 'Cancel' buttons. The configuration is organized into sections: General, Endpoint Options, Registration, and T.38 Fax Gateway Configuration. In the General section, the Name is 'Avaya Session Manager' and the Description is 'Session Manager Proxy'. The Routing group is set to 'Proxy group'. In the Endpoint Options section, the Endpoint address is '10.10.60.14', the UDP port is '5060', and the TCP port is '5060'. Several checkboxes are checked, including 'Monitor this endpoint', 'Trust this endpoint', and options for sending 'INVITE' and 'REFER' with replaces during call transfers. The 'Register a user name with this endpoint' checkbox is unchecked. The 'T.38 Fax Gateway Configuration' section is currently collapsed.

Continuation....

After configuring the remaining fields, click on the **Apply** button on the top of the screen (not shown) to save the changes.

T.38 Fax Gateway Configuration	
Allow T.38 on this endpoint ?	<input checked="" type="checkbox"/>
Allow ECM negotiation for this endpoint ?	<input checked="" type="checkbox"/>
Allow V.17 Modem to be negotiated for this endpoint ?	<input checked="" type="checkbox"/>
Redundancy level ?	<input type="text" value="2"/>
Re-INVITE delay ?	<input type="text" value="500"/>

7.6. Configure Groups

During compliance testing no group configuration was required as only one TDM trunk was configured. If multiple TDM trunks are required please refer to the Aculab documentation (see **Section 10**).

7.7. Configure Routes

To configure the QSIG Route, click on the **Routes** tab and uncheck **Use the same rules for all groups** the check box.

aplianx IP GatewayYou are logged in as: admin on IP Gateway : 224474

Edit Configurations > Manage Routing

Status

- Overview
- Alarms
- Calls
- Call Log
- Trunk Status

System Configuration

- Global Configuration
- Networking
- Setup Wizard
- SIP Credentials

Gateway Configuration

- Alias Registrar
- DDI Barring
- Edit Configurations**
- Interoperability
- Cause Mappings

Diagnostics

- Remote Logging
- Network Diagnostics
- Watchdog Status
- Restart
- Firewall Log

Editing: Avaya SIP-QSIG TEST

General Trunks Endpoints Groups **Routes** Clocking SIP Codecs Survivability Test

Routing Options

Use the same rules for all groups ? ☐

Allow calls from unknown endpoints ? ☐

Routing Rules

Select the group for which you want to configure the routing

Name ? DDI/DID criteria ? DDI/DID man. ? CLI/ANI criteria ? CLI/ANI man. ? Destination ?

Registrar look % % % % Registrar

Add new rule

Use these rules for all groups

Save Changes

Save and Return

Cancel Changes

7.7.1. Configure QSIG Route

- Select **TDM trunks** from the **Select the group for which you want to configure the routing** dropdown box
- **Name** Enter a descriptive name (i.e. QSIG to SIP)
- **Destination** Select **Proxy group** from the dropdown box

Click on the **Save Changes** button.

The screenshot shows the 'appliance IP Gateway' web interface. The top right corner indicates the user is logged in as 'admin' on 'IP Gateway : 224474'. The left sidebar contains navigation menus for 'Status', 'System Configuration', 'Gateway Configuration', and 'Diagnostics'. The main content area is titled 'Editing: Avaya SIP-QSIG TEST' and features a tabbed interface with 'General', 'Trunks', 'Endpoints', 'Groups', 'Routes', 'Clocking', 'SIP', 'Codecs', 'Survivability', and 'Test'. The 'Routes' tab is active, showing 'Routing Options' and 'Routing Rules'. Under 'Routing Rules', a dropdown menu is set to 'TDM trunks'. Below this, a table-like structure shows a rule named 'QSIG to SIP' with a 'Destination' dropdown set to 'Proxy group'. At the bottom, there are buttons for 'Add new rule', 'Use these rules for all groups', 'Save Changes', 'Save and Return', and 'Cancel Changes'.

7.7.2. Configure SIP Route

- Select **Proxy group** from the **Select the group for which you want to configure the routing** dropdown box
- Click on the **Add new rule** button
- **Name** Enter a descriptive name (i.e. SIP to QSIG)
- **Destination** Select **TDM trunks** from the dropdown box

Click on the **Save Changes** button.

The screenshot shows the 'applanx IP Gateway' web interface. The top right corner indicates the user is logged in as 'admin' on 'IP Gateway : 224474'. The left sidebar contains navigation menus for 'Status', 'System Configuration', 'Gateway Configuration', and 'Diagnostics'. The main content area is titled 'Editing: Avaya SIP-QSIG TEST' and has tabs for 'General', 'Trunks', 'Endpoints', 'Groups', 'Routes', 'Clocking', 'SIP', 'Codecs', 'Survivability', and 'Test'. The 'Routing Rules' section is active, showing a table with columns: 'Name', 'DDI/DID criteria', 'DDI/DID man.', 'CLI/ANI criteria', 'CLI/ANI man.', and 'Destination'. A new rule is being added with the name 'SIP to QSIG' and destination 'TDM trunks'. The 'Proxy group' is selected in the dropdown for 'Select the group for which you want to configure the routing'. At the bottom, there are buttons for 'Add new rule', 'Use these rules for all groups', 'Save Changes', 'Save and Return', and 'Cancel Changes'.

applanx IP Gateway

You are logged in as: admin
on IP Gateway : 224474

Edit: Configurations > Manage Routing

Status

- Overview
- Alarms
- Calls
- Call Log
- Trunk Status

System Configuration

- Global Configuration
- Networking
- Setup Wizard
- SIP Credentials

Gateway Configuration

- Alias Registrar
- DDI Barring
- Edit Configurations
- Interoperability
- Cause Mappings

Diagnostics

- Remote Logging
- Network Diagnostics
- Watchdog Status
- Restart

Editing: Avaya SIP-QSIG TEST

General Trunks Endpoints Groups Routes Clocking SIP Codecs Survivability Test

Routing Options

Use the same rules for all groups ? ☐

Allow calls from unknown endpoints ? ☐

Routing Rules

Select the group for which you want to configure the routing Proxy group

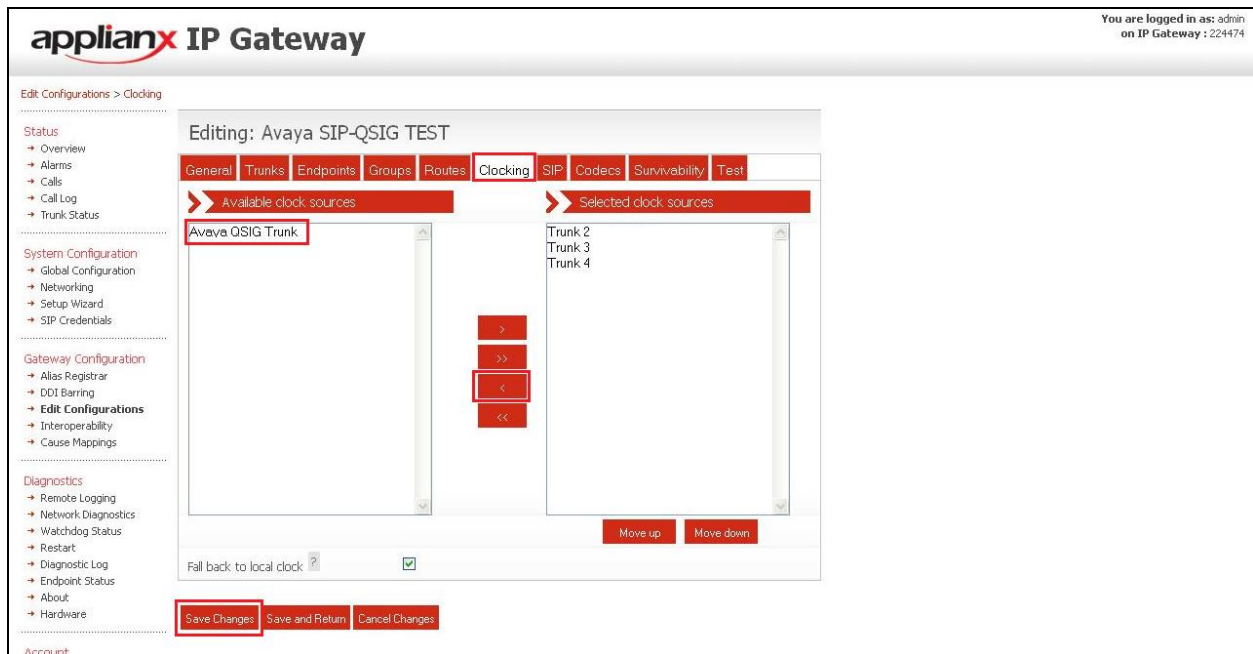
Name ?	DDI/DID criteria ?	DDI/DID man. ?	CLI/ANI criteria ?	CLI/ANI man. ?	Destination ?
SIP to QSIG	%	%	%	%	TDM trunks

Add new rule Use these rules for all groups

Save Changes Save and Return Cancel Changes

7.8. Configure Clocking

During compliance testing clocking was provided by the Avaya QSIG trunk. To configure clocking, click on the **Clocking** tab and highlight the **QSIG Trunk** from the **Selected clock sources** frame and click on the left icon button . Click on the **Save Changes** button.



7.9. Configure SIP

To configure the SIP settings click on the **SIP** tab and enter all the information as shown in the screen shot below.

The screenshot displays the 'aplianx IP Gateway' web interface. The top right corner indicates the user is logged in as 'admin' on 'IP Gateway : 224474'. The main navigation menu on the left includes sections for Status, System Configuration, Gateway Configuration, Diagnostics, and Account. The 'Edit Configurations > SIP Configuration' breadcrumb is visible. The main content area is titled 'Editing: Avaya SIP-QSIG TEST' and features a tabbed interface with 'SIP' selected. The configuration is organized into sections: 'Transport for outgoing calls' (with a dropdown for 'TCP'), 'Media options' (containing settings for DTMF over IP, tone and interdigit durations, and checkboxes for comfort noise, 183 for ringing, DTX, PLC, and RTCP), and 'Jitter Buffer'.

Section	Parameter	Value
Transport for outgoing calls	Transport protocol	TCP
	DTMF over IP send method	RFC2833 encoded RTP
Media options	Tone duration of regenerated DTMF	250
	Interdigit duration of regenerated DTMF	250
	Enable comfort noise	<input checked="" type="checkbox"/>
	Send 183 for Ringing	<input checked="" type="checkbox"/>
	Enable Discontinuous Transmission (DTX)	<input checked="" type="checkbox"/>
	Enable Packet Loss Concealment (PLC)	<input checked="" type="checkbox"/>
	Enable RTCP	<input type="checkbox"/>
	Use 'sendonly' for Hold	<input type="radio"/>
Jitter Buffer	Use 'inactive' for Hold	<input type="radio"/>
	Use 'recvonly' for Hold	<input type="radio"/>
	Bridge media streams	<input type="checkbox"/>

Continuation....

After configuring the remaining fields, click on the **Save Changes** button to save the changes.

The screenshot shows the configuration page for an Avaya SIP Gateway. The page is titled "Change Password" at the top left. The main content area is divided into several sections, each with a red header and a right-pointing arrow. The sections are: "Jitter Buffer" (with a sub-section "Manual jitter buffer configuration" and a checkbox), "Listening ports" (with "UDP listen port (0 to disable)" and "TCP listen port (0 to disable)" both set to 5060), "Endpoint monitoring" (with "Polling interval" set to 60), "Message Waiting Supplementary Service Support" (with "Accept unsolicited message summary" and "Send unsolicited message summary" both checked), "Call Diversion Supplementary Service Support" (with "Call Diversion Enabled", "History-Info Method Preferred", "Divert as proxy", "Divert unmatched to outgoing group", and "Send Diverted Address" all checked), and "Custom messages conveying non-SIP features" (with "Exchange transfer information", "Exchange Route Optimisation/Path Replacement information", and "CBWF/CBWNJ Enabled" all checked). At the bottom of the page are three buttons: "Save Changes", "Save and Return", and "Cancel Changes".

7.10. Configure Codecs

During compliance testing the codec settings were left as default. The screen shot below shows the configured codecs.

The screenshot shows the "Editing: Avaya SIP-QSIG TEST" window in the Avaya SIP Gateway configuration interface. The window has a tabbed interface with tabs for "General", "Trunks", "Endpoints", "Groups", "Routes", "Clocking", "SIP", "Codecs", "Survivability", and "Test". The "Codecs" tab is selected. The "Available codecs" list on the left contains "G729". The "Configured codecs" list on the right contains "G711_Alaw" and "G711_Mulaw". Between the two lists are four buttons: ">", ">>", "<<", and "<". At the bottom of the window are two buttons: "Move Up" and "Move Down". At the bottom of the page are three buttons: "Save Changes", "Save and Return", and "Cancel Changes". The top right of the page shows the user is logged in as "admin" on "IP Gateway : 224474".

7.11. Save Configuration

Once all the configuration changes have been made, click on the **Save and Return** button.

applianceX IP Gateway

You are logged in as: admin
on IP Gateway : 224474

Edit Configurations > Codec Configuration

Status

- Overview
- Alarms
- Calls
- Call Log
- Trunk Status

System Configuration

- Global Configuration
- Networking
- Setup Wizard
- SIP Credentials

Gateway Configuration

- Alias Registrar
- DDI Barring
- Edit Configurations**
- Interoperability
- Cause Mappings

Diagnostics

- Remote Logging
- Network Diagnostics
- Watchdog Status
- Restart
- Diagnostic Log
- Endpoint Status
- About

Editing: Avaya SIP-QSIG TEST

General Trunks Endpoints Groups Routes Clocking SIP Codecs Survivability Test

Available codecs

G729

Configured codecs

G711_Alaw
G711_Mulaw

Move Up Move Down

Save Changes Save and Return Cancel Changes

7.12. Use Configuration

Once all the configurations have been made and saved, click on the **Use** button for this configuration (Avaya SIP-QSIG Test) to apply them to the ApplianceX.

applianceX IP Gateway

You are logged in as: admin
on IP Gateway : 224474

Edit Configurations

Changes saved

Edit Configurations

Active configuration

Name	Description	Last updated	
Change with Bridge media Qsig - DG		2013-12-06 06:14:08	Running View Copy

Available configurations

Name	Description	Last updated	
Avaya DQ Test Setup		2013-06-11 22:22:50	Edit Delete Copy Use
Avaya SIP-QSIG TEST		2014-02-14 03:33:21	Edit Delete Copy Use
Avaya test config (1byte invokeid)		2013-03-28 19:40:18	Edit Delete Copy Use

Delete Multiple Configurations

Click on the **Yes** button to confirm.

aplianx IP Gateway

You are logged in as: admin
on IP Gateway : 224474

Status

- Overview
- Alarms
- Calls
- Call Log
- Trunk Status

System Configuration

- Global Configuration
- Networking

Question

Are you sure you want to use the configuration Avaya SIP-QSIG TEST?

Yes

No

Once the configuration is active, the web page should update to something similar to the screen below.

aplianx IP Gateway

You are logged in as: admin
on IP Gateway : 224474

Edit Configurations

Status

- Overview
- Alarms
- Calls
- Call Log
- Trunk Status

System Configuration

Edit Configurations

>> Active configuration

Name	Description	Last updated	
Avaya SIP-QSIG TEST		2014-02-14 03:33:21	Running <div><div>View</div><div>Copy</div></div>

8. Verification Steps

This section provides the tests that can be performed to verify correct configuration of the Avaya and Aculab solution.

8.1. Verify the SIP Entity Link status for the ApplianX IP Gateway

From System Manager select **Session Manager** from under the **Elements** column (not shown). When the **Session Manager** tab opens select **System Status** followed by **SIP Entity Monitoring**, then click on **Session Manager**.

AVAYA
Aura® System Manager 6.3

Last Logged on at June 4, 2014 8:09 AM
Help | About | Change Password | Log off admin

Home / Elements / Session Manager / System Status / SIP Entity Monitoring

SIP Entity Link Monitoring Status Summary

This page provides a summary of Session Manager SIP entity link monitoring status.

SIP Entities Status for All Monitoring Session Manager Instances

Run Monitor

1 Items | Refresh Filter: Enable

Session Manager	Type	Monitored Entities						Total
		Down	Partially Up	Up	Not Monitored	Deny		
<input type="checkbox"/> Session Manager								
<input type="checkbox"/> Session Manager 1	Core	0	0	3	0	0	3	

When the **Session Manager Entity Link Connection Status** window opens, observe the **Conn Status** and **Link Status** and ensure that they are both showing as **up** for the **Applianx** SIP Entity.

AVAYA
Aura® System Manager 6.3

Last Logged on at June 4, 2014 8:09 AM
Help | About | Change Password | Log off admin

Home / Elements / Session Manager / System Status / SIP Entity Monitoring

Session Manager Entity Link Connection Status

This page displays detailed connection status for all entity links from a Session Manager.

All Entity Links for Session Manager: Session Manager 1

Summary View

Status Details for the selected Session Manager:

3 Items | Refresh Filter: Enable

	SIP Entity Name	SIP Entity Resolved IP	Port	Proto.	Deny	Conn. Status	Reason Code	Link Status
<input type="radio"/>	6.3 CM	10.10.16.211	5061	TLS	FALSE	UP	200 OK	UP
<input type="radio"/>	Applianx	10.10.60.40	5060	TCP	FALSE	UP	200 OK	UP
<input type="radio"/>	CM62VMMC	10.10.60.11	5060	TCP	FALSE	UP	200 OK	UP

8.2. Verify calls via the ApplianX IP Gateway

1. Make a call to the SIP PBX from the QSIG PBX. Ensure the call is connected and there is a two way speech path.
2. Make a call to the QSIG PBX from the SIP PBX. Ensure the call is connected and there is a two way speech path.

9. Conclusion

These Application Notes describe the configuration steps required for an Aculab ApplianX IP Gateway to interoperate with an Avaya Aura® Communication Manager 6.2 using a SIP trunk to interoperate with a QSIG trunk. All test cases have passed and met the objectives with two observations outlined in **Section 2.2**.

10. Additional References

This section references the Avaya and Aculab documentation that is relevant to these Application Notes. Product documentation for Avaya products may be found at:

<http://support.avaya.com>

[1] Avaya Aura® Communication Manager Feature Description and Implementation, Release 6.2, Issue 9.0, February 2012, Document Number 555-245-205.

[2] Administering Avaya Aura® Communication Manager, Release 6.2, Issue 7.0, February 2012, Document Number 03-300509.

[3] Administering Avaya Aura® Session Manager, Release 6.3, Issue 3 October 2013

[4] Administering Avaya Aura® System Manager, Release 6.3, Issue 3, October, 2013

Product Documentation for ApplianX IP Gateway can be at the following location:

<http://www.aculab.com/documents/>

©2014 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.