



Avaya Solution & Interoperability Test Lab

Application Notes for Phybridge UniPhyer with Avaya Aura® Communication Manager 6.3 and Avaya Aura® Session Manager 6.3 – Issue 1.0

Abstract

These Application Notes describe the configuration steps required for Phybridge UniPhyer to interoperate with Avaya Aura® Communication Manager 6.3 and Avaya Aura® Session Manager 6.3. In the compliance testing, the Phybridge UniPhyer leveraged the existing single-pair telephony wiring to provide dedicated Ethernet voice path and Power over Ethernet to Avaya H.323 IP telephones registered to Avaya Aura® Communication Manager and Avaya SIP IP telephones registered to Avaya Aura® Session Manager.

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 a compliance-tested configuration consisting of Phybridge UniPhyer, Phybridge PhyAdapters, Avaya Aura® Communication Manager, Avaya Aura® System Manager, Avaya Aura® Session Manager, Avaya H.323 and Avaya SIP IP telephones.

The Phybridge UniPhyer is a LAN appliance that leverages the existing single-pair telephony wiring to provide dedicated Ethernet and Power over Ethernet (PoE) to Avaya H.323 and SIP IP telephones.

2. General Test Approach and Test Results

The compliance testing focused on the interoperability between Phybridge UniPhyer and Avaya IP telephones to ensure that the phones work as expected. Serviceability testing was also performed.

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

Testing consisted of typical call scenarios involving Avaya endpoints connected to UniPhyer. External call scenarios were also tested with a PRI PSTN connection. All tests were performed manually and the focus was on verifying interoperability compliance.

Feature testing included: registration, audio codec, media shuffling, basic calls, hold/reconnect, conference, transfer, display, DTMF, and message waiting indicator (MWI) scenarios.

The serviceability testing focused on verifying the ability of Phybridge UniPhyer to recover from adverse conditions, such as disconnecting and reconnecting the Ethernet cables to the Phybridge UniPhyer and to the Avaya IP telephones. Reboots and power cycling of Phybridge UniPhyer were also tested.

2.2. Test Results

All applicable test cases were executed and passed with the following observations:

The Avaya B179 Conference Phone was powered with its local power supply and connected to the PhyAdapter with an Ethernet cable as per **Reference 5** in **Section 10**. This configuration was used because the B179 phone required more PoE power than could be supplied by UniPhyer. Other Class 3 endpoints may also require this configuration. UniPhyer Switches can power Class 1, Class 2 and some Class 3 IEEE 802.3af compliant IP devices.

The Phybridge PhyAdapters will reset if they receive Jumbo Ethernet Frames and it was found that Avaya one-X® Deskphone H.323 3.2.1 software would generate Jumbo Ethernet Frames in some situations causing loss of network connectivity. The latest version of Avaya one-X® Deskphone H.323 3.2.2 software fixes this issue.

2.3. Support

Technical support on the Phybridge UniPhyer can be obtained through the following:

- **Phone:** (888) 901-3633
- **Email:** Support@Phybridge.com

3. Reference Configuration

In the test configuration shown in **Figure 1**, Avaya IP telephones are connected to the network via the Phybridge UniPhyer leveraging the existing CAT3 cabling that was previously used for Analog and Digital phones. For each station user, one end of the CAT3 cable is changed to connect to the Phybridge UniPhyer instead of the Analog or Digital Line circuit pack on the Avaya G650. The other end of the CAT3 cable connects to a Phybridge PhyAdapter with an RJ11 connector. Each PhyAdapter is connected using a standard CAT5 Ethernet cable to an Avaya IP telephone.

In the sample configuration Avaya H.323 IP telephones register to Communication Manager and Avaya SIP IP telephones register to Session Manager.

The Phybridge UniPhyer provides power to the Avaya IP telephones, and is transparent to the telephones in terms of the telephones' network settings.

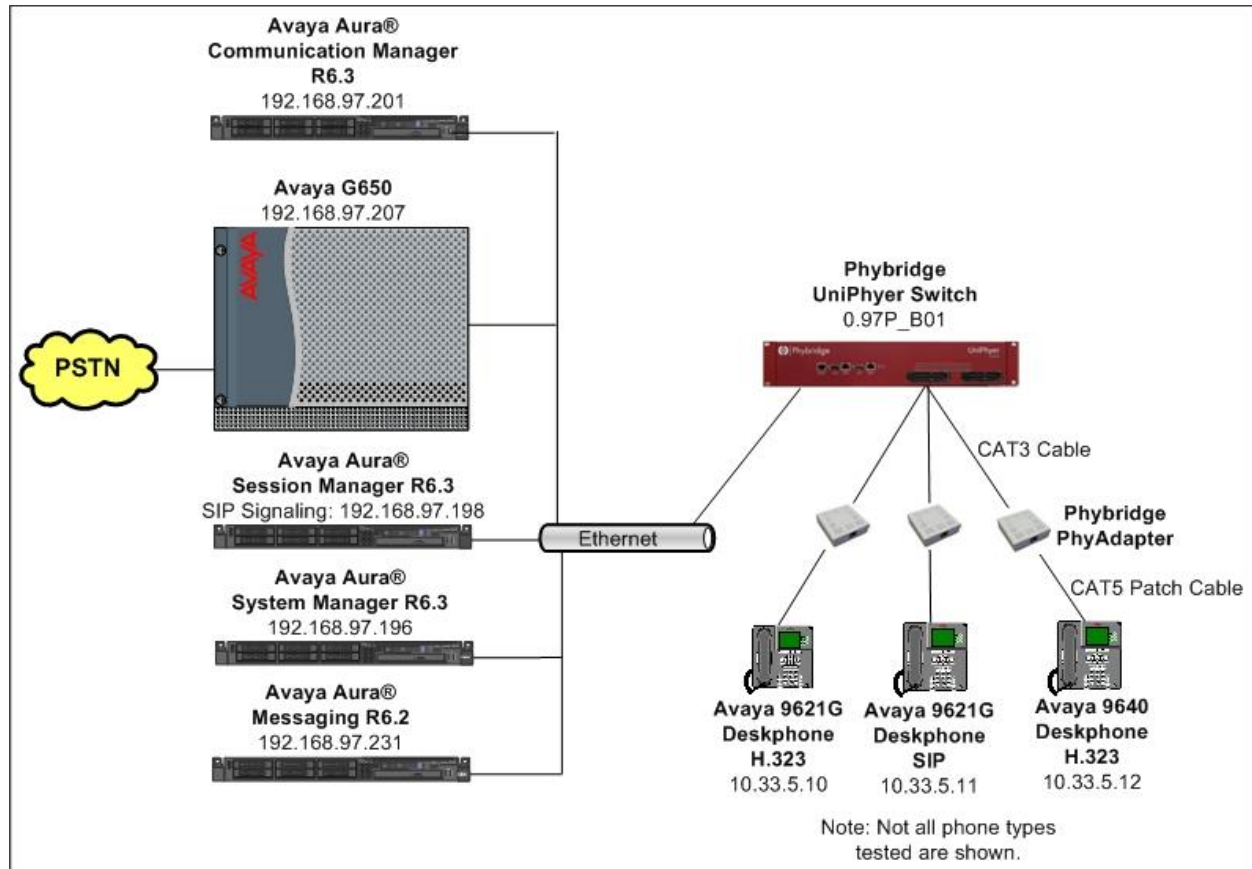


Figure 1: Phybridge UniPhyer with Avaya Aura® Communication Manager and Avaya Aura® Session Manager

4. Equipment and Software Validated

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

Equipment/Software	Release/Version
Avaya Aura® Session Manager running on S8800 Server	Release: 6.3.2.0.632023
Avaya Aura® System Manager running on S8800 Server	6.3.0 - FP2 Build No. - 6.3.0.8.5682-6.3.8.1627
Avaya Aura® Communication Manager running on Avaya S8800Server/G650 Media Gateway	R016x.03.0.124.0 patch 21172
Avaya Aura® Messaging	6.2
Avaya 1140E Deskphone (SIP)	04.04.10.00
1608 IP Deskphone (H.323)	1.3.4
Avaya 9621G IP Deskphone (H.323)	6.3.1.16
Avaya 9621G IP Deskphone (SIP)	6.3.0.73
Avaya 9640 IP Deskphone (H.323)	3.2.1
Avaya 9620L IP Deskphone (SIP)	2.6.11.4
Avaya B179 Conference Phone (SIP)	2.3.8
Phybridge PhyAdapters	LB-PA111
Phybridge UniPhyer Switch LB-UA2324	0.97P_B01

5. Configure Avaya H.323 Phones on Avaya Aura® Communication Manager

No special configuration is required for Avaya H.323 phones to interoperate with UniPhyer. For completeness, this section provides the procedures for configuring Avaya H.323 phones on Communication Manager. It is assumed that Communication Manager and Session Manager have already been installed and are functioning.

In a typical installation of Phybridge UniPhyer, analog and digital telephones using existing CAT3 cabling would be replaced with new IP telephones as described in **Section 3**. This section shows an example of modifying an existing station type to match the new Avaya H.323 IP telephone, and allows the user to retain the same extension number.

Change the station type of an existing analog or digital station by using the command **change station n**, where “n” is the existing extension number. For **Type**, enter the applicable IP station type, in this case “9640”, and the **Port** field will be populated automatically. Enter a desired **Security Code**.

change station 53044		Page 1 of 5
STATION		
Extension: 53044	Lock Messages? n	BCC: 0
Type: 9640	Security Code: 53044	TN: 1
Port: IP	Coverage Path 1:	COR: 1
Name: 9640	Coverage Path 2:	COS: 1
	Hunt-to Station:	Tests? y
STATION OPTIONS		
Time of Day Lock Table:		
Loss Group: 19	Personalized Ringing Pattern: 1	
	Message Lamp Ext: 53044	
Speakerphone: 2-way	Mute Button Enabled? y	
Display Language: english	Button Modules: 0	
Survivable GK Node Name:		
Survivable COR: internal	Media Complex Ext:	
Survivable Trunk Dest? y	IP SoftPhone? n	
	IP Video? n	
	Short/Prefixed Registration Allowed: default	
	Customizable Labels? y	

Repeat this section to modify the station type for all applicable analog and digital stations that are being replaced with H.323 Stations.

Use the **save translation** command to save these changes.

6. Configure Avaya SIP Phones

No special configuration is required for Avaya SIP phones to interoperate with UniPhyer. For completeness, this section provides information for configuring Avaya SIP phones with Session Manager and Communication Manager. It is assumed that Communication Manager and Session Manager have already been installed and are functioning. It is also assumed that dial plan routing has been configured on Session Manager and Communication Manager.

In a typical installation of Phybridge UniPhyer, analog and digital telephones using existing CAT3 cabling would be replaced with new IP telephones as described in **Section 3**. This section shows an example of modifying an existing station type to match the new Avaya SIP IP telephone, and allows the user to retain the same extension number.

6.1. SIP Phone Configuration on Avaya Aura® Communication Manager

This section provides the procedures for modifying a current station on Communication Manager to be a SIP station. The procedures fall into the following areas:

- Change Station Configuration
- Verify Off-PBX-Telephone Station-Mapping

6.1.1. Change Station Configuration

Change the station type of an existing analog or digital station by using the command **change station n**, where “n” is the existing extension number. For **Type**, enter the applicable IP station type, in this case “9621SIP”, and the **Port** field will be populated automatically. Enter a desired **Security Code**.

change station 53045		Page 1 of 6
STATION		
Extension: 53045	Lock Messages? n	BCC: 0
Type: 9621SIP	Security Code: 53045	TN: 1
Port: IP	Coverage Path 1:	COR: 1
Name: 53045	Coverage Path 2:	COS: 1
	Hunt-to Station:	
STATION OPTIONS		
Time of Day Lock Table:		
Loss Group: 19	Message Lamp Ext: 53045	
Display Language: english		
Survivable COR: internal		
Survivable Trunk Dest? y	IP SoftPhone? n	
IP Video? n		

Navigate to **Page 4**. Add the desired number of **call-appr** entries in the **BUTTON ASSIGNMENTS** section. This governs how many concurrent calls can be supported. In the sample configuration, three call appearances were configured to support transfer and conferencing scenarios.

change station 53045		Page 4 of 6
STATION		
SITE DATA		
Room:		Headset? n
Jack:		Speaker? n
Cable:		Mounting: d
Floor:		Cord Length: 0
Building:		Set Color:
ABBREVIATED DIALING		
List1:	List2:	List3:
BUTTON ASSIGNMENTS		
1: call-appr	5:	
2: call-appr	6:	
3: call-appr	7:	
4:	8:	

Navigate to **Page 6**. Enter **aar** for the **SIP Trunk** setting and use defaults for remaining fields.

change station 53045		Page 6 of 6
STATION		
SIP FEATURE OPTIONS		
Type of 3PCC Enabled: None		
SIP Trunk: aar		

6.1.2. Verify Off-PBX-Telephone Station-Mapping

Use the **change off-pbx-telephone station-mapping x** command where “x” is an extension assigned to a SIP Deskphone to verify an Off-PBX station mapping was automatically created for the SIP station.

On **Page 1**, verify the following fields were correctly populated.

- **Application:** Verify “**OPS**” is assigned.
- **Trunk Selection:** Verify “**aar**” is assigned.

change off-pbx-telephone station-mapping 53045							Page 1 of 3
STATIONS WITH OFF-PBX TELEPHONE INTEGRATION							
Station	Application	Dial	CC	Phone Number	Trunk	Config	Dual
Extension		Prefix			Selection	Set	Mode
53045	OPS	-		53045	aar	1	

On **Page 2**, verify the following fields were correctly populated.

- **Mapping Mode:** Verify “**both**” is assigned.
- **Calls Allowed:** Verify “**all**” is assigned.

change off-pbx-telephone station-mapping 53045							Page 2 of 3
STATIONS WITH OFF-PBX TELEPHONE INTEGRATION							
Station	Appl	Call	Mapping	Calls	Bridged	Location	
Extension	Name	Limit	Mode	Allowed	Calls		
53045	OPS	4	both	all	none		

Use the **save translation** command to save these changes.

6.2. SIP Phone Configuration on Avaya Aura® Session Manager

This section describes the procedure to configure a SIP IP phone on Session Manager. It is assumed that Application and Application Sequence have already been configured.

The procedures fall into the following areas:

- Add SIP User
- Synchronize Changes with Communication Manager

Access the browser-based GUI of System Manager, using the URL **http://<FQDN>/SMGR**, where “<FQDN>” is the fully qualified domain name of System Manager. Log in to System Manager with the appropriate credentials (not shown).

6.2.1. Add SIP User

Add a new SIP user for the SIP station defined in **Section 6.1**.

On the System Manager home screen under the **Users** column select **User Management** (not shown). Select **Manage Users** from the left navigation menu.

Step 1: Click **New** (not shown). Enter values for the following required attributes for a new SIP user in the **Identity** section and use default values for the remaining fields.

- **Last Name:** Enter last name of user.
- **First Name:** Enter first name of user.
- **Login Name:** Enter “**extension number@<domain>**” where “<domain>” matches the domain being used. In this example bvwddev.com was used.
- **Authentication Type:** Verify “**Basic**” is selected.
- **Password:** Enter password used to log into System Manager.
- **Confirm Password:** Repeat value entered above.
- **Localized Display Name:** Enter display name for user [Optional].

The screen below shows results from **Step 1** for a new SIP user.

The screenshot shows the 'New User Profile' form in the Avaya Aura Session Manager GUI. The form is divided into four tabs: Identity, Communication Profile, Membership, and Contacts. The 'Identity' tab is selected. The form contains the following fields and values:

- Last Name:** User
- First Name:** SIP
- Middle Name:** (empty)
- Description:** (empty)
- Login Name:** 53045@bvwddev.com
- Authentication Type:** Basic
- Password:** (masked with dots)
- Confirm Password:** (masked with dots)
- Localized Display Name:** (empty)
- Endpoint Display Name:** (empty)

At the top right of the form, there are three buttons: 'Commit & Continue', 'Commit', and 'Cancel'. The left navigation menu shows 'User Management' and 'Manage Users'.

Click **Commit & Continue** to save changes from **Step 1**.

Step 2: The **Communication Profile** tab should now be displayed. Click on **Edit** beside the **Communication Profile Password** text box (not shown). Enter the value the endpoint will use to register to Session Manager in the **Communication Profile Password** and **Confirm Password** fields. The **Communication Profile Password** should match the **Security Code** field defined in **Section 6.1.1**.

Verify there is a default entry identified as the Primary profile as shown below:

The screenshot shows a web interface for editing a user profile. The breadcrumb trail is "Home / Users / User Management / Manage Users". The page title is "User Profile Edit: 53045@bvwdev.com". There are buttons for "Commit & Continue", "Commit", and "Cancel". The "Communication Profile" tab is active, showing fields for "Communication Profile Password" and "Confirm Password". Below these fields are buttons for "New", "Delete", "Done", and "Cancel". A table lists communication profiles with one entry named "Primary" which is selected and marked as the default. The "Name" field is set to "Primary" and the "Default" checkbox is checked.

Name
Primary

Select : None

* Name: Primary

Default : ☒

If an entry does not exist, select **New** and enter values for the following required attributes:

- **Name:** Enter "**Primary**".
- **Default:** Verify that the check box is selected.

Step 3: Expand **Communication Address** sub-section and select **New** to define a **Communication Address** for the new user.

Enter values for the following required attributes:

- **Type:** Select “**Avaya SIP**” from drop-down menu.
- **Fully Qualified Address:** Enter the same extension number as used for **Login Name** in **Step 1** in the textbox.
- **Domain:** Select the value that matches the domain name defined in **Step 1**.

Click **Add** to save the Communication Address.

Communication Address ▼

<input type="checkbox"/>	Type	Handle	Domain
No Records found			

Type: ▼

*** Fully Qualified Address:** @ ▼

Step 4: Scroll down to the **Session Manager Profile** section and select the check box.

Enter the following values.

- **Primary Session Manager:** Select the appropriate Session Manager. In this example **DevSM** was used.
- **Origination Application Sequence:** Select an **Application Sequence**.
- **Termination Application Sequence:** Select an **Application Sequence**.
- **Conference Factory Set:** Retain the default value of “**(None)**”.
- **Survivability Server:** Select “**(None)**” from drop-down menu.
- **Home Location:** Select Location.

The remaining values were left at default for this sample configuration. The screen below shows results from **Step 4**.

☒ **Session Manager Profile**

SIP Registration

- * **Primary Session Manager** DevSM

Primary	Secondary	Maximum
38	0	38
- Secondary Session Manager** (None)
- Survivability Server** (None)
- Max. Simultaneous Devices** 1
- Block New Registration When Maximum Registrations Active?** ☐

Application Sequences

- Origination Sequence** DevCM-SEQ
- Termination Sequence** DevCM-SEQ

Call Routing Settings

- * **Home Location** Belleville
- Conference Factory Set** (None)

Step 5: Scroll down to the **CM Endpoint Profile** section and select the check box.

Enter the following values and use defaults for remaining fields.

- **System:** Select Managed Element defined for Communication Manager.
- **Profile Type:** Select “**Endpoint**”.
- **Use Existing Endpoints:** Select the check box to use the existing extension.
- **Extension:** Enter same extension number used for Login Name in **Step 1**.
- **Template:** Select template for type of SIP phone.
- **Security Code:** Enter numeric value used to register the SIP endpoint.
Note: this field should match the value entered for the Communication Profile Password field in **Step 2**.
- **Voice Mail Number:** Enter Pilot Number for Avaya Modular Messaging or Avaya Aura® Messaging if installed. Else, leave field blank.

The screen below shows the results from **Step 5** when adding a new SIP user in this sample configuration.

The screenshot shows a web-based configuration form for a 'CM Endpoint Profile'. At the top, there is a section header 'CM Endpoint Profile' with a dropdown arrow. Below this, the form contains several fields and checkboxes. The 'System' field is a dropdown menu with 'DevCM' selected. The 'Profile Type' field is a dropdown menu with 'Endpoint' selected. The 'Use Existing Endpoints' checkbox is checked. The 'Extension' field is a text input with '53045' and a magnifying glass icon, followed by an 'Endpoint Editor' button. The 'Template' field is a dropdown menu with '9621SIP_DEFAULT_CM_6_3' selected. The 'Set Type' field is a text input with '9621SIP'. The 'Security Code' field is a text input with six dots. The 'Port' field is a text input with 'IP'. The 'Voice Mail Number' field is a text input. The 'Preferred Handle' field is a dropdown menu with '(None)' selected. Below these fields, there are three checkboxes: 'Enhanced Callr-Info display for 1-line phones' (unchecked), 'Delete Endpoint on Unassign of Endpoint from User or on Delete User' (checked), and 'Override Endpoint Name' (checked).

☒ **CM Endpoint Profile**

* **System** DevCM

* **Profile Type** Endpoint

Use Existing Endpoints ☒

* **Extension** 53045 **Endpoint Editor**

Template 9621SIP_DEFAULT_CM_6_3

Set Type 9621SIP

Security Code ●●●●●●

Port IP

Voice Mail Number

Preferred Handle (None)

Enhanced Callr-Info display for 1-line phones ☐

Delete Endpoint on Unassign of Endpoint from User or on Delete User ☒

Override Endpoint Name ☒

Click **Commit** (not shown) to save the definition of the new user.

6.2.2. Synchronize Changes with Avaya Aura® Communication Manager

After completing these changes in System Manager, perform an on demand synchronization. From the System Manager Home page navigate to **Services → Inventory → Synchronization → Communication System**.

On the **Synchronize CM Data and Configure Options** page, select the row associated with Communication Manager as shown below.

Home / Services / Inventory / Synchronization / Communication System

Synchronize CM Data and Configure Options

Note: Please avoid any administration task on CM while synchronization or audit is in progress.

Synchronize CM Data/Launch Element Cut Through

4 Items Refresh Show ALL Filter: Enable

<input type="checkbox"/>	Element Name	FQDN/IP Address	Last Sync Time	Last Translation Time	Sync Type	Sync Status	Location	Software Version
<input checked="" type="checkbox"/>	DevCM	192.168.97.201	February 26, 2014 11:00:10 PM -05:00	10:00 pm WED FEB 26, 2014	Incremental	Completed		R016x.03.0.124.0
<input type="checkbox"/>	DevCM2	192.168.97.246	February 26, 2014 11:00:05 PM -05:00	10:00 pm WED FEB 26, 2014	Incremental	Completed		R016x.03.0.124.0
<input type="checkbox"/>	DevCM3_62	10.33.4.9	February 26, 2014 11:00:06 PM -05:00	10:00 pm WED FEB 26, 2014	Incremental	Completed		R016x.03.0.124.0
<input type="checkbox"/>	DevCMS	192.168.97.219	February 26, 2014 11:00:06 PM -05:00	10:00 pm WED FEB 26, 2014	Incremental	Completed		R015x.02.1.016.4

Select : All, None

☐ Initialize data for selected devices
☒ Incremental Sync data for selected devices
☐ Execute 'save trans all' for selected devices
☐ Audit

Now Schedule Launch Element Cut Through View Audit Report

Select the **Incremental Sync data for selected devices** option and click **Now** to start the synchronization.

Use the **Refresh** button in the table header to verify status of the synchronization. Verify synchronization successfully completes by verifying the status in the **Sync Status** column shows **“Completed”**.

Note: Depending on the number of administration changes made, synchronization might take several minutes to complete.

6.3. Avaya 9600 Series Deskphone (SIP) Configuration

This section describes the procedure to configure an Avaya 9600 Series Deskphone (SIP) so that it does not use Jumbo Ethernet Frames. This is required because the PhyAdapters will reset if they receive Jumbo Ethernet Frames causing the phone to lose network connectivity.

The **46xxsettings.txt** file can be used to configure 9600 Series SIP Deskphones to not use Jumbo Frames. In this sample configuration the setting **SET MTU_SIZE 1496** was used in the 46xxsettings.txt file to disable the use of Jumbo Frames.

The following is a section of the **46xxsettings.txt** file that is available for download at <http://support.avaya.com>.

```
## MTU_SIZE specifies the maximum transmission unit (MTU) size transmitted by the
phone.
## Valid values are 1496 or 1500.
## Use 1496 for older Ethernet switches.
SET MTU_SIZE 1496
##
```

Detailed information on using the 46xxsettings.txt file can be found in **Reference 3** in **Section 10**.

7. Configure Phybridge UniPhyer

This section provides the procedures for configuring UniPhyer. The procedures fall into the following areas:

- Launch web interface
- Administer Phybridge UniPhyer IP Address
- Save Running Configuration

All remaining configuration settings on UniPhyer were left as default in this sample configuration.

7.1. Launch Web Interface

Access the UniPhyer web interface by using the URL “**http://ip-address**” in an Internet browser window, where “ip-address” is a valid IP address of the UniPhyer switch. The default IP address of the UniPhyer management port is “**192.168.1.1**” and the default IP address of the UniPhyer GBE ports is “**192.168.100.1**”. In this example, the web interface of the UniPhyer switch was accessed by the management port. The **Web Interface Login** screen is displayed as shown below. Log in using the appropriate credentials.



7.2. Administer Phybridge UniPhyer IP Address

In the subsequent screen (not shown), select **System** → **Board IP Setup** from the left panel. In the **Board IP Setup** panel on the right, the IP address configuration of the UniPhyer switch can be changed as needed. Click **Save** when finished. The default values were used for the sample configuration of the UniPhyer switch as shown below.

The screenshot shows the 'Board IP Setup' configuration page for a Phybridge UniPhyer device. The left sidebar contains a menu with options: System (expanded), System Info, Board IP Setup, Ethernet Port Service, ADSL Port Service, CLI Setup, Cluster Setup, System Inventory, System Contact Info, SNMP, TACACS+ Setup, TACACS+ Privilege Mapping, IP Routes, Management ACL, User Administration, Duplicator, and Logout. Under 'System', there are sub-options: Bridge, ADSL, Traffic, SNMP, and Maintenance. The main content area is titled 'Board IP Setup' and contains a 'Save' button at the top left. Below it is the 'Address Management' section, which is divided into two columns: 'GBE (In Band)' and 'MGMT (Out Band)'. The 'GBE (In Band)' column shows IP Address 192.168.100.1 and Subnet Mask 255.255.255.0. The 'MGMT (Out Band)' column shows IP Address 192.168.1.1 and Subnet Mask 255.255.255.0. Below these are fields for 'NO Limit VID' (checked), 'Limit VID' (empty), 'Priority' (0), 'DHCP Client' (Disable DHCP Client), 'DHCP Timeout' (60), and 'DHCP Lease' (4294967295). At the bottom, there are fields for 'HTTP Port' (80), 'MGMT Speed' (Auto Negotiate), 'Remote IP' (192.168.1.2), and 'System Name' (UniPhyer). A red warning message at the bottom states: 'Modifying the configuration may cause a connection loss'.

Address Management			
GBE (In Band)		MGMT (Out Band)	
IP Address	192 . 168 . 100 . 1	IP Address	192 . 168 . 1 . 1
Subnet Mask	255 . 255 . 255 . 0	Subnet Mask	255 . 255 . 255 . 0
NO Limit VID	<input checked="" type="checkbox"/>	DHCP Client	Disable DHCP Client ▼
Limit VID		DHCP Timeout	60
Priority	0 ▼	DHCP Lease	4294967295
HTTP Port	80	MGMT Speed	Auto Negotiate
		Remote IP	192.168.1.2
		System Name	UniPhyer

[System Inventory]

Modifying the configuration may cause a connection loss

7.3. Save Running Configuration

Next, navigate to **Maintenance** → **Database** to save the running configuration to flash. In the **DB Config Select** field, select option **D** and click the **Write_Running** button.

The screenshot shows the 'Database Configuration' page for a Phybridge UniPhyer device. The left sidebar contains a menu with options: System, Bridge, ADSL, Traffic, SNMP, and Maintenance (expanded). Under 'Maintenance', there are sub-options: SYS Log Server, Database, Firmware Update, Boot Code Update, ATM Loopbacks, Fault Management, and Performance Monitoring. The main content area is titled 'Database Configuration' and contains a 'DB Config Select' dropdown menu with the option '(D)Save Running Config to Flash(System Config)' selected. To the right of the dropdown is a 'RESTART' button. Below the dropdown is a 'Write_Running' button.

DB Config Select: (D)Save Running Config to Flash(System Config) RESTART

Write_Running

8. Verification Steps

This section provides tests that can be performed to verify proper configuration of Communication Manager, Session Manager and UniPhyer.

8.1. Verify Avaya Aura® Communication Manager

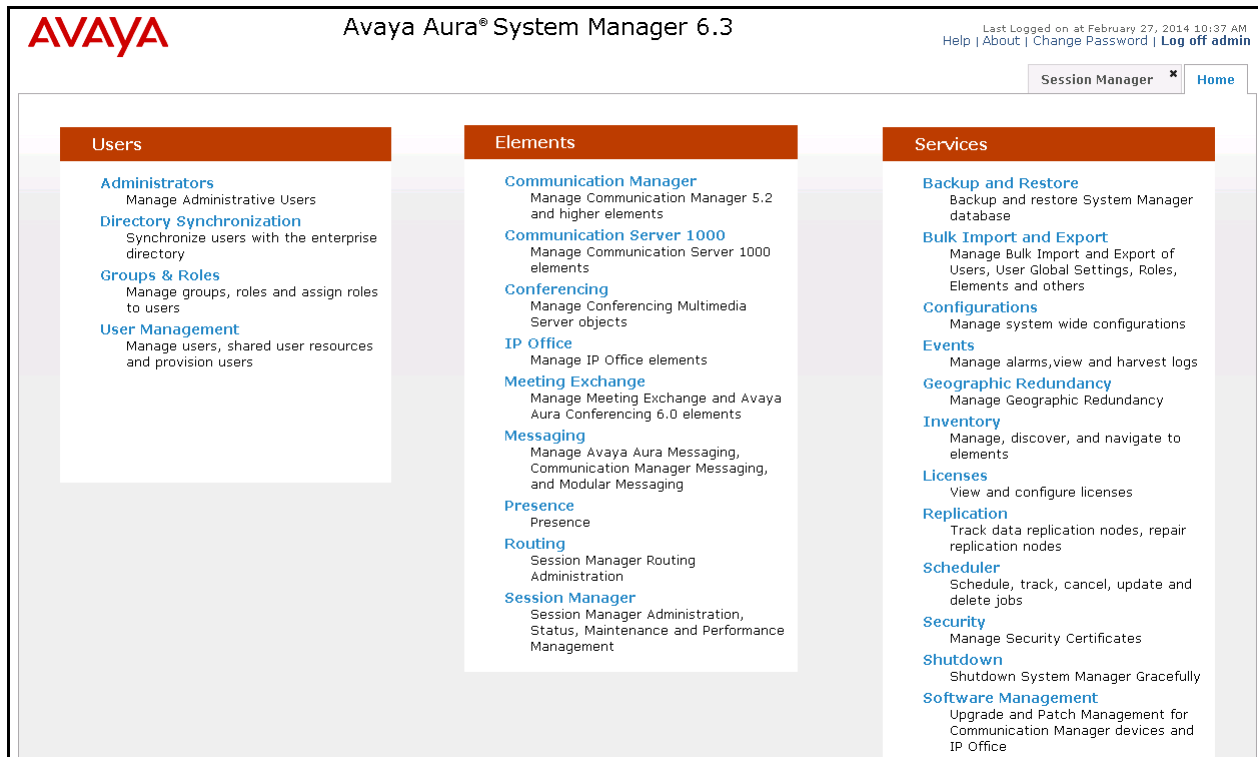
This section verifies the registration of H.323 IP phones on Communication Manager. Use the **list registered-ip-stations** command to verify that all H.323 IP stations connected via the UniPhyer registered successfully with Communication Manager, as shown below.

list registered-ip-stations					
REGISTERED IP STATIONS					
Station Ext or Orig Port	Set Type/ Net Rgn	Prod ID/ Release	TCP Skt	Station IP Address/ Gatekeeper IP Address	
53010	4625 1	IP_Phone 3.103S	y	10.33.5.178 192.168.97.201	
53011	4625 1	IP_Phone 6.2313	y	10.33.5.34 192.168.97.201	
53012	4625 1	IP_Phone 6.2313	y	10.33.5.26 192.168.97.201	
53013	9608 1	IP_Phone 6.2313	y	10.33.5.52 192.168.97.201	
53015	4620 1	IP_Phone 2.300	y	10.33.5.12 192.168.97.201	
53016	9620 1	IP_Phone 6.3116	y	192.168.98.50 192.168.97.201	
53044	9640 1	IP_Phone 3.210A	y	10.33.5.53 192.168.97.201	

8.2. Verify Avaya Aura® Session Manager

This section verifies the registration of SIP IP phones on Session Manager. Access the browser-based GUI of System Manager, using the URL <http://<FQDN>/SMGR>, where “<FQDN>” is the fully qualified domain name of System Manager. Log in to System Manager with the appropriate credentials (not shown).

From the main System Manager page click on the **Session Manager** link in the **Elements** column as shown in the following figure.



In the next screen that opens, expand **System Status** from the navigation tree on the left. Now select **User Registrations** under **System Status**. As shown below, a search was performed for user 53045@bvwdev.com that was used in this sample configuration. It is shown to be registered by the checkmark in the **Prim** column.

User Registrations

Select rows to send notifications to devices. Click on Details column for complete registration status.

View: Default Force Unregister AST Device Notifications: Reboot Reload Failback As of 2:46 PM

1 Item Found Refresh Show ALL Filter: Disable, Apply, Clear

Details	Address	First Name	Last Name	Actual Location	IP Address	Remote Office	Shared Control	Simult. Devices	AST Device	Registered		
										Prim	Sec	Surv
<input type="checkbox"/> Show	53045@bvwdev.com	SIP	User	---	192.168.98.51:5060	<input type="checkbox"/>	<input type="checkbox"/>	1/1	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/> (AC)	<input type="checkbox"/>	<input type="checkbox"/>

Select: All, None

8.3. Verify Phybridge UniPhyer

From the UniPhyer web interface, select **SYSTEM → ADSL Port Service** from the left panel. Verify the **Current Status** for ports that have physically connected IP Phones is **ON**, as shown below for port 1.

Phybridge UniPhyer

ADSL Port Service

Admin: ON Service Profile: 2 Spectrum Profile: 2 TCA Profile: 2 All ☐ Modify

The Service Profile range from 1 to 120
The Spectrum Profile range from 1 to 120
The TCA Profile range from 1 to 64

Port 01~12 Query

Select	Port	Admin Status	Current Status	Service Profile	Spectrum Profile	TCA Profile
<input checked="" type="radio"/>	1	ON	ON	2	2	2
<input type="radio"/>	2	ON	OFF	2	2	2
<input type="radio"/>	3	ON	OFF	2	2	2
<input type="radio"/>	4	ON	OFF	2	2	2
<input type="radio"/>	5	ON	OFF	2	2	2
<input type="radio"/>	6	ON	OFF	2	2	2
<input type="radio"/>	7	ON	OFF	2	2	2
<input type="radio"/>	8	ON	OFF	2	2	2
<input type="radio"/>	9	ON	OFF	2	2	2
<input type="radio"/>	10	ON	OFF	2	2	2
<input type="radio"/>	11	ON	OFF	2	2	2
<input type="radio"/>	12	ON	OFF	2	2	2

[SERVICE PROFILE | SPECTRUM PROFILE | TCA PROFILE]

9. Conclusion

These Application Notes describe the configuration steps required for Phybridge UniPhyer to interoperate with Avaya IP telephones (H.323) registered to Avaya Aura® Communication Manager and Avaya IP telephones (SIP) registered to Avaya Aura® Session Manager. All feature and serviceability test cases were completed and passed as per **Section 2** with observations explained in **Section 2.2**.

10. Additional References

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

Documentation for Avaya products may be found at <http://support.avaya.com>.

Avaya Aura® Communication Manager

[1] *Administering Avaya Aura® Communication Manager*, Release 6.3,
Document Number 03-300509, Issue 9, October 2013

[2] *Avaya Aura® Communication Manager Feature Description and Implementation*, Release 6.3, Document Number 555-245-205, Issue 11, October 2013

[3] *Avaya one-X™ Deskphone Edition for 9600 Series IP Telephones Administrator Guide Release 3.1*, Document Number 16-300698, Issue 7, November 2009

Documentation for Phybridge products may be found at <http://phybridge.com>.

Phybridge UniPhyer Switch

[4] *Phybridge – UniPhyer Web Configuration Tool Guide*, Part Number 8003-03, Issue 2, May 2009

[5] *NON POE devices on a PhyAdater or PhyLink*, document 009-011 TS – 017 Version 002, 27 December 2012

©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.