



Avaya Solution & Interoperability Test Lab

Application Notes for Valcom PagePro IP with Avaya Aura® Communication Manager and Avaya Aura® Session Manager – Issue 1.0

Abstract

These Application Notes describe the configuration steps required for Valcom PagePro IP to successfully interoperate with Avaya Aura® Communication Manager and Avaya Aura® Session Manager. The Valcom PagePro IP is a SIP-based paging device that integrates with Avaya Aura® Communication Manager and Avaya Aura® Session Manager as SIP endpoints.

Information in these Application Notes has been obtained through DevConnect compliance testing and additional technical discussions. Testing was conducted via the DevConnect Program at the Avaya Solution and Interoperability Test Lab.

1. Introduction

These Application Notes describe the configuration steps required for the Valcom PagePro IP to successfully interoperate with Avaya Aura® Communication Manager and Avaya Aura® Session Manager. The Valcom PagePro IP is a SIP-based paging device that integrates with Avaya Aura® Communication Manager and Avaya Aura® Session Manager as SIP endpoints.

1.1. Interoperability Compliance Testing

The interoperability compliance test plan included feature and serviceability test cases.

The feature testing covered SIP registration, basic calls, simultaneous calls, display verification, media shuffling, and audio codec negotiation. Various SIP access numbers for the Valcom PagePro IP device were dialed to test connection to the proper speaker groups.

The serviceability testing focused on verifying the ability of the Valcom PagePro IP to recover from adverse conditions, such as disconnecting and reconnecting the Ethernet cable to the device, rebooting Communication Manager, and rebooting Session Manager.

1.2. Support

Technical support for Valcom can be obtained through the following:

- **Phone:** (800) VALCOM1
- **Email:** support@valcom.com

2. Reference Configuration

The Valcom PagePro IP can register with Avaya Aura® Session Manager as eight separate SIP endpoints (access numbers), providing up to eight zones of SIP-based paging. When a call is placed to one of the access numbers, the device answers the call and automatically establishes a one-way communication path with a preconfigured group of IP speakers, and/or analog speakers/gateways associated with the access number. During compliance testing, the following Valcom Talkback IP Speakers were used as the preconfigured destinations for the access numbers:

- VIP-148L
- VIP-160
- VIP-172L
- VIP-422
- VIP-431-DS

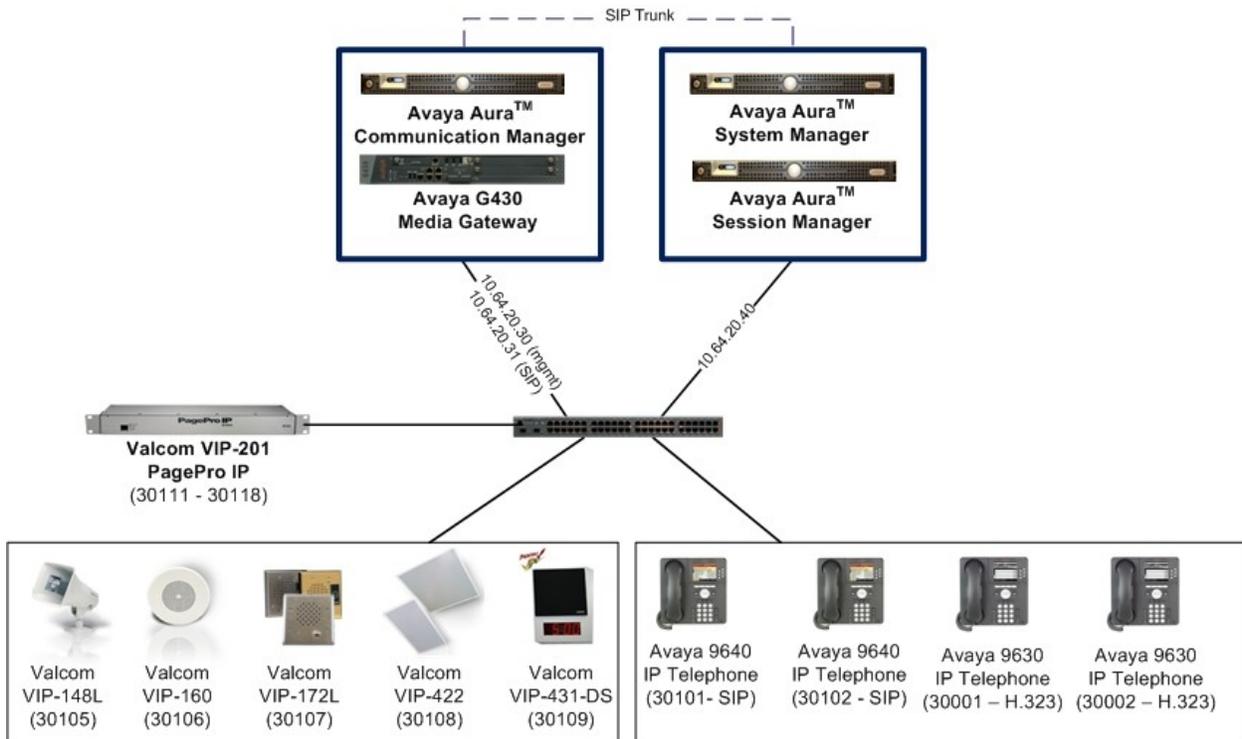


Figure 1: Valcom PagePro IP with Avaya Aura® Communication Manager and Avaya Aura® Session Manager

3. Equipment and Software Validated

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

Equipment	Software
Avaya S8800 Server with a Avaya G430 Media Gateway	Avaya Aura® Communication Manager 6.0, R016x.00.0.345.0, Update 18444 (Avaya Aura® System Platform: 6.0.1.0.5)
Avaya S8800 Server	Avaya Aura® System Platform: 6.0.1.0.5 Avaya Aura® System Manager: 6.0.7.0
Avaya S8800 Server	Avaya Aura® System Platform: 6.0.1.0.5 Avaya Aura® Session Manager 6.0.0.0.600020
Avaya 9600 Series IP Telephones <ul style="list-style-type: none">• H.323• SIP	3.1.1 2.6.2
Valcom PagePro IP <ul style="list-style-type: none">• VIP-201	2.17
Valcom Talkback IP Speakers <ul style="list-style-type: none">• VIP-148L• VIP-160• VIP-172L• VIP-422• VIP-431-DS	2.17

4. Configure Avaya Aura Communication Manager

The detailed administration of basic connectivity between Avaya Aura® Communication Manager and Avaya Aura® Session Manager is not the focus of these Application Notes and will not be described. For administration of basic connectivity between Avaya Aura® Communication Manager and Avaya Aura® Session Manager, refer to the appropriate documentation listed in **Section 10**. Note coded G.711MU was configured on Avaya Aura® Communication Manager. This section provides the procedures for the following:

- Verify Avaya Aura® Communication Manager License

4.1. Verify Communication Manager License

Log into the System Access Terminal (SAT) to verify that the Communication Manager license has proper permissions for features illustrated in these Application Notes. Use the “display system-parameters customer-options” command to verify that there is sufficient capacity for SIP stations by comparing the **Maximum Off-PBX Telephones - OPS** field value with the corresponding value in the **USED** column. The difference between the two values needs to be greater than or equal to the number of access numbers required for the Valcom PagePro IP device.

```
display system-parameters customer-options                               Page 1 of 11
                                OPTIONAL FEATURES

G3 Version: V16                                                         Software Package: Enterprise
Location: 2                                                             System ID (SID): 1
Platform: 28                                                            Module ID (MID): 1

                                USED
Platform Maximum Ports: 65000 90
Maximum Stations: 41000 24
Maximum XMOBILE Stations: 41000 0
Maximum Off-PBX Telephones - EC500: 41000 0
Maximum Off-PBX Telephones - OPS: 41000 18
Maximum Off-PBX Telephones - PBFMC: 41000 0
Maximum Off-PBX Telephones - PVFMC: 41000 0
Maximum Off-PBX Telephones - SCCAN: 0 0
Maximum Survivable Processors: 313 1

(NOTE: You must logoff & login to effect the permission changes.)
```

5. Configure Avaya Aura® Session Manager

This section provides the procedures for configuring Avaya Aura® Session Manager. The procedures include the following areas:

- Launch Session Manager administration interface
- Administer endpoints
- Administer users

5.1. Launch Session Manager Administration Interface

Configuration of Session Manager is accomplished by accessing the browser-based GUI of Avaya Aura™ System Manager, using the URL “https://<ip-address>/SMGR”, where “<ip-address>” is the IP address of System Manager. Log in using the appropriate credentials. The screen shown below is displayed.

Action	Description	Help
Elements	Interface to manage the application instances and contains the element managers for the different managed elements in the deployment.	Help for managing elements
Events	Interface to view and administer logs and alarms.	Help for managing logs and alarms
Groups & Roles	Interface to manage groups, resources and roles.	Help for managing groups and roles
Licenses	Interface to manage licenses for individual applications of Avaya Aura (TM) Unified Communication Solution.	Help for managing licenses
Routing	Interface to manage routing policies, adaptations, dial patterns, SIP elements.	Help for managing routing policies
Security	Interface to manage certificates .Certificates help enable setting up secure communication between different elements in the Avaya Aura (TM) Unified Communication Solution.	Help for managing certificates
System Manager Data	Interface to backup and restore System Manager data, manage data retention rules, list extension pack information, manage replication nodes, manage scheduled jobs and System Manager configuration.	Help for managing System Manager data and configuration
Users	Interface to administer users, contact lists, shared addresses and Access Control Lists (ACLs).	Help for managing users

5.2. Administer Endpoints

From the menu in the left pane, navigate to **Elements** → **Endpoints** → **Manage Endpoints** as shown below. Select the **New** button from the right pane.

The screenshot displays the Avaya Aura System Manager 6.0 interface. The top left features the Avaya logo. The top right shows a welcome message for user 'admin' and a 'Log off' button. A red navigation bar contains the breadcrumb 'Home / Elements / Endpoints / Manage Endpoints'. On the left, a sidebar menu lists various system management options, with 'Manage Endpoints' highlighted. The main content area is titled 'Endpoints' and includes a link to 'Select Device(s) from Communication Manager List'. Below this is an 'Endpoint List' section with buttons for 'View', 'Edit', 'New', 'Delete', and 'More Actions'. A table lists 25 items, with the first two rows visible. The table has columns for Name, Extension, Port, Set Type, COS, COR, User, and System.

Avaya Aura™ System Manager 6.0

Welcome, **admin** Last Logged on at October 27, 2010 11:09 AM
Help | About | Change Password | **Log off**

Home / Elements / Endpoints / Manage Endpoints

Endpoints

Select Device(s) from Communication Manager List ▶

Show List

Endpoint List

View Edit **New** Delete More Actions ▶ Advanced Search ▶

25 Items Refresh Show 15 Filter: Enable

<input type="checkbox"/>	Name	Extension	Port	Set Type	COS	COR	User	System
<input type="checkbox"/>	30101-ED	30101	S00000	9640SIP	1	1	30101@avaya.com	demoCMapp
<input type="checkbox"/>	30102-ED	30102	S00001	9640SIP	1	1	30102@avaya.com	demoCMapp

The Valcom endpoints were defined using the template for the Avaya 9620 SIP phone during compliance testing. Enter the following values for the specified fields, and retain the default values in the remaining fields.

- **Template** Enter “DEFAULT_9620SIP_CM_6_0”.
- **Name** Enter a descriptive name.
- **Extension** Enter a valid available extension for this endpoint.
- **Security Code** Enter the desired security code for this endpoint.

AVAYA Avaya Aura™ System Manager 6.0

Welcome, **admin** Last Logged on at October 27, 2010 11:09 AM
[Help](#) | [About](#) | [Change Password](#) | [Log off](#)

Home / Elements / Endpoints / Manage Endpoints / Add Endpoint

Add Endpoint [Commit](#) [Schedule](#) [Clear](#) [Cancel](#)

[\[Save As Template\]](#)

System demoCMapp **Extension** 30111

Template DEFAULT_9620SIP_CM_6_0 **Set Type** 9620SIP

Port IP **Security Code** *****

Name 30111

General Options | Feature Options | Site Data | Abbreviated Call Dialing | Enhanced Call Fwd | Button Assignment | Group Membership | Expand All | Collapse All

General Options

Class of Restriction (COR) 1 **Class Of Service (COS)** 1

Emergency Location Ext 30111 **Message Lamp Ext.** 30111

Tenant Number 1 **SIP Trunk** aar

Type of 3PCC Enabled None **Native Name**

Coverage Path 1

Lock Message

Coverage Path 2

Feature Options

Active Station Ringing single **Auto Answer** none

Click **Commit**. Repeat this procedure for each of the Valcom PagePro IP access numbers.

5.3. Administer Users

Users must be added to Session Manager that correspond to the SIP endpoints added in Section 5.2. From the menu in the left pane, navigate to **Users** → **Manage Users**. Select the **New** button from the right pane.

AVAYA Avaya Aura™ System Manager 6.0

Welcome, **admin** Last Logged on at October 13, 2010 6:55 PM
[Help](#) | [About](#) | [Change Password](#) | [Log off](#)

Home / Users / Manage Users

User Management

Users

[View](#) [Edit](#) [New](#) [Duplicate](#) [Delete](#) [More Actions](#) [Advanced Search](#)

21 Items Refresh Show 15 Filter: Enable

<input type="checkbox"/>	Status	Name	Login Name	E164 Handle	Last Login
<input type="checkbox"/>		30101-LD	30101@avaya.com	30101	
<input type="checkbox"/>		30102-LD	30102@avaya.com	30102	

Enter the following values for the specified fields, and retain the default values in the remaining fields.

Under *General*:

- **Last**
- **First**

Enter the last name of the user.

Enter the first name of the user.

General ▼

* Last Name:	<input type="text" value="201"/>
* First Name:	<input type="text" value="Valcom"/>
Middle Name:	<input type="text"/>
Description:	<input type="text"/>

Under *Identity*:

- **Login Name:** Using the extension from **Section 5.2**, enter the unique system login given to the user. It takes of form of *username@domain* (e.g. “30111@avaya.com”) and it is used to create the user’s primary handle.
- **Authentication Type:** Select “Basic” to have the user’s login authenticated by an Avaya Authentication Server.
- **SMGR Login Password:** Enter the password used to log into System Manger.
- **Shared Communication Profile Password:** Enter the password used to log into the Valcom endpoint (the Security Code from **Section 5.2**).
- **Localized Display Name:** Enter the localized display name of the user.
- **Endpoint Display Name:** Enter the full text name of the user represented in ASCII to support displays that cannot handle localized text.
- **Language Preference:** Select the user’s preferred written or spoken language
- **Time Zone:** Select the preferred time zone of the user.

Identity ▾

* **Login Name:**

* **Authentication Type:**

SMGR Login Password:

* **Password:**

* **Confirm Password:**

Shared Communication Profile Password:

Confirm Password:

Localized Display Name:

Endpoint Display Name:

Honorific:

Language Preference:

Time Zone:

Under *Communication Profile* → *Communication Address*:

- **Type:** Select “Avaya SIP”.
- **Fully Qualified Address:** Enter the extension and select the appropriate domain for the user.

Click the **Add** button.

Communication Profile ▼

New Delete Done Cancel

Name
Primary
Select : None

* Name: Primary

Default :

Communication Address ▼

New Edit Delete

Type	Handle	Domain
No Records found		

Type: Avaya SIP

* Fully Qualified Address: 30111 @ avaya.com

Add Cancel

Under *Communication Profile* → *Session Manager*:

- **Primary Session Manager** Select the Session Manager instance that should be used as the home server for the currently displayed Communication Profile.
- **Origination Application Sequence** Select an Application Sequence that will be invoked when calls are routed *from* this user.
- **Termination Application Sequence** Select an Application Sequence that will be invoked when calls are routed *to* this user.
- **Home Location** Select the Home Location of this user.

Session Manager Profile ▼

* Primary Session Manager	demoSM ▼	Primary	Secondary	Maximum
		20	0	20

Secondary Session Manager	(None) ▼	Primary	Secondary	Maximum

Origination Application Sequence demoCMseq ▼

Termination Application Sequence demoCMseq ▼

Survivability Server (None) ▼

* **Home Location** .20 Subnet ▼

Under *Communication Profile* → *Endpoint Profile*:

- **System:** Select the Communication Manager on which the endpoint exists.
- **Use Existing Endpoints** Check this box to use an endpoint administered in **Section 5.2**.
- **Extension:** Enter the extension of the endpoint from **Section 5.2** that you want to associate with this user.
- **Template:** Select an appropriate template matching the template configured in **Section 5.2**.
- **Security Code:** Enter the security code to be used by the Valcom endpoint when registering to the Session Manager, as administered in **Section 5.2**.
- **Port:** The Port field is automatically filled in.

Endpoint Profile ▼

* **System** demoCMapp ▼

Use Existing Endpoints

* **Extension** 30111

Template DEFAULT_9620SIP_CM_6_0 ▼

Set Type 9620SIP

Security Code ●●●●●●

* **Port** S00016

Voice Mail Number

Delete Endpoint on Unassign of Endpoint from User

Click the **Commit** button. Repeat the procedures in this section to add a user for each endpoint administered in **Section 5.2**.

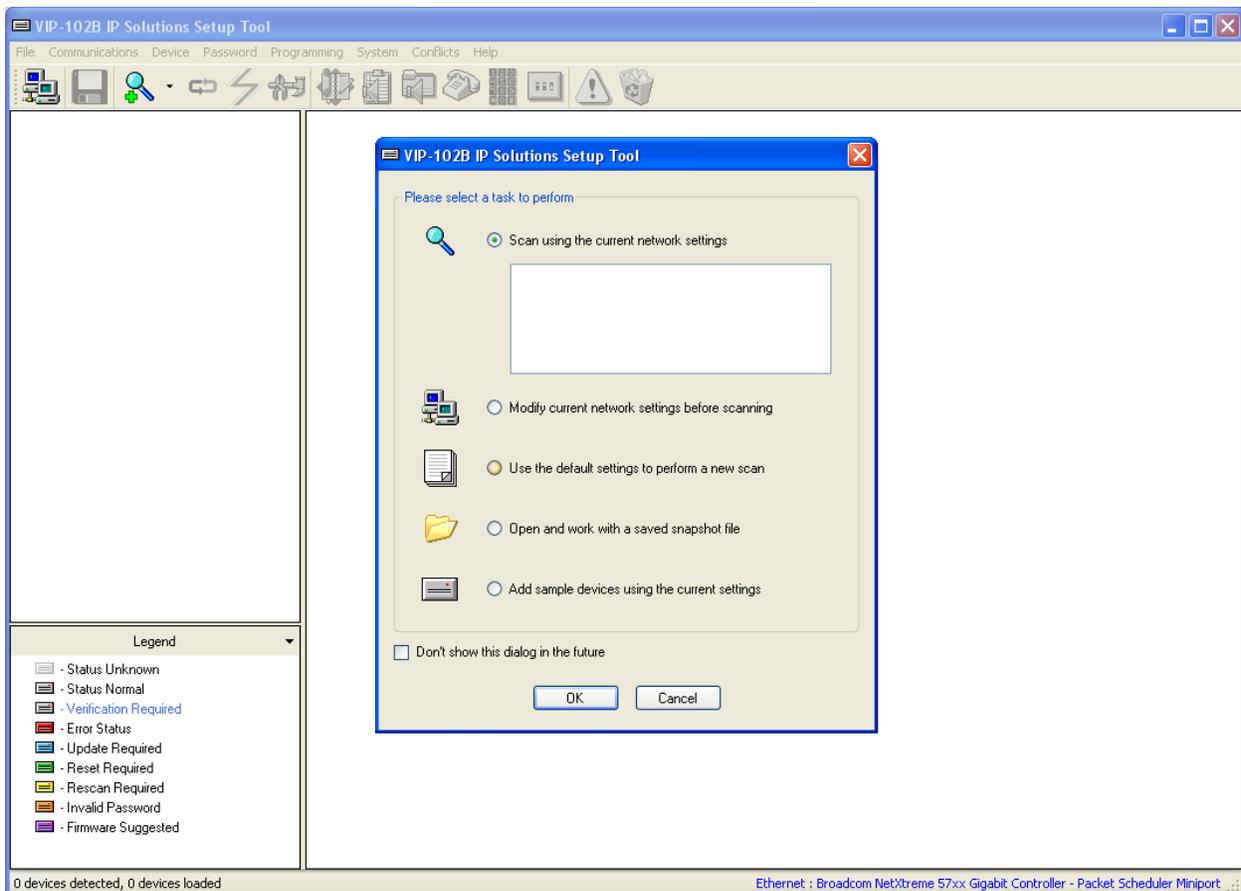
6. Configure Valcom PagePro IP

This section provides the procedures for configuring Valcom PagePro IP. The information shown is the minimum for configuring the Valcom device. Complete configuration details may be found in the Valcom documentation listed in **Section 10**. The procedures include the following areas:

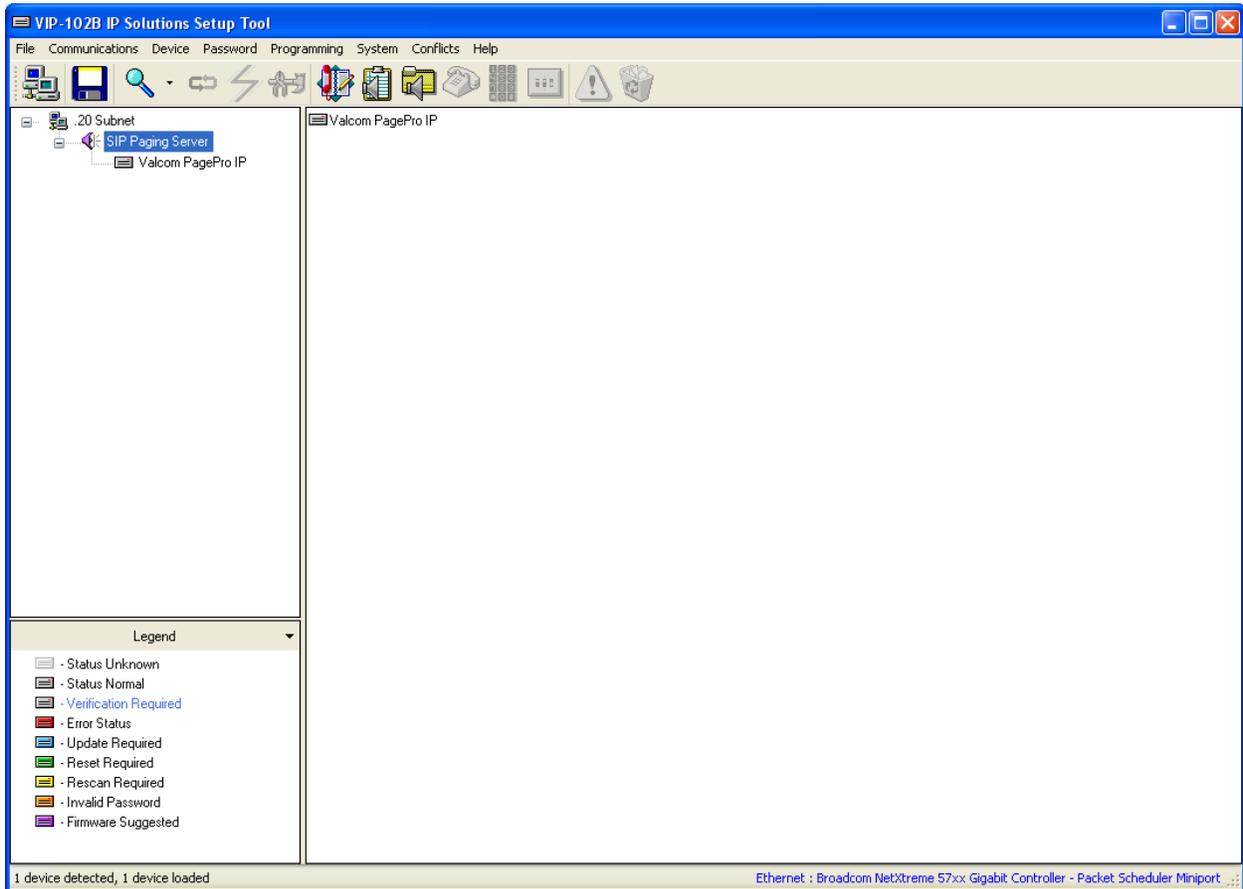
- Launch setup tool
- Administer properties
- Administer network
- Administer group membership
- Administer SIP

6.1. Launch Setup Tool

From a PC running the Valcom VIP-102B IP Solutions Setup Tool application, select **Start** → **All Programs** → **Valcom IP Solutions** → **VIP-102B IP Solutions Setup Tool**. The **VIP-102B IP Solutions Setup Tool** screen is displayed. Retain the default values and click **OK** to scan for Valcom devices.

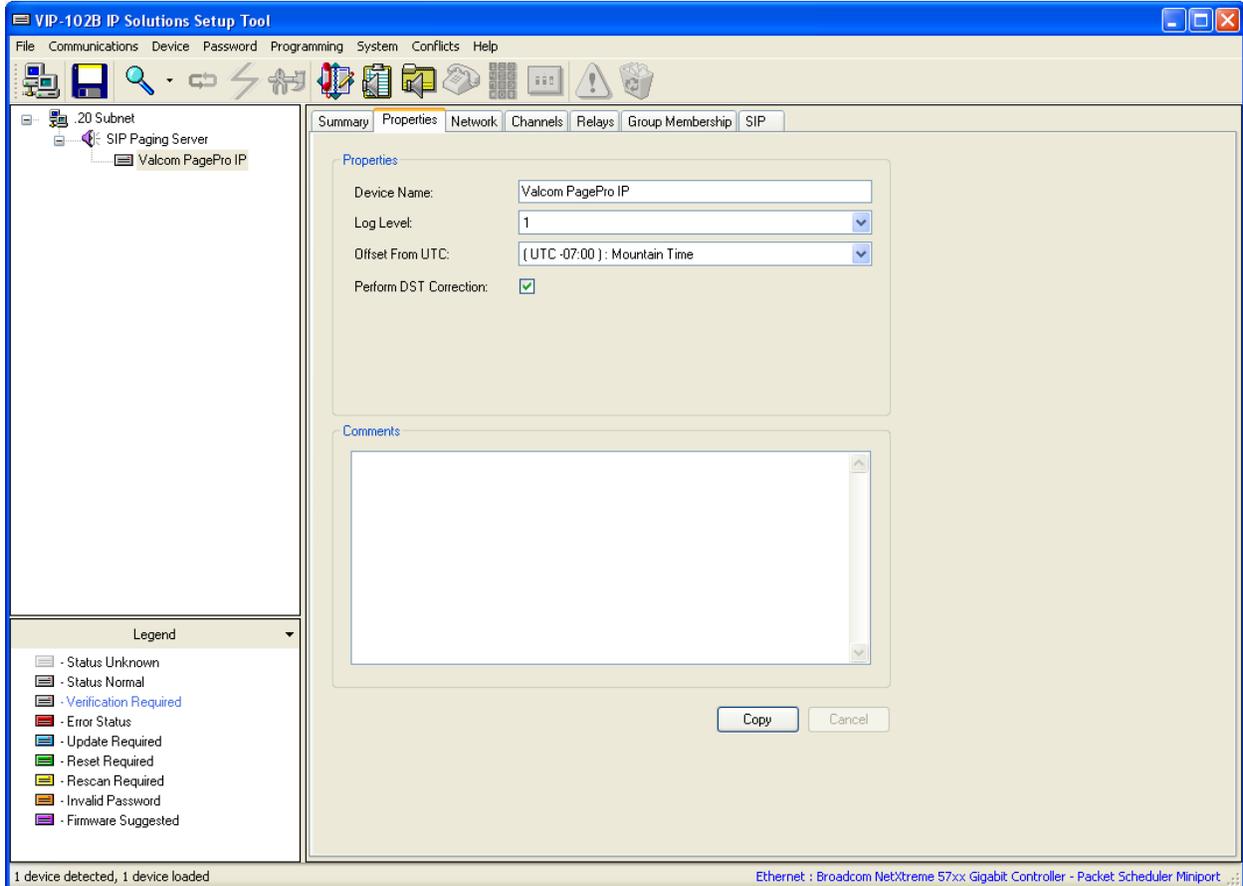


At the conclusion of the scan, the **VIP-102B IP Solutions Setup Tool** screen is updated with the discovered Valcom PagePro IP as shown below.



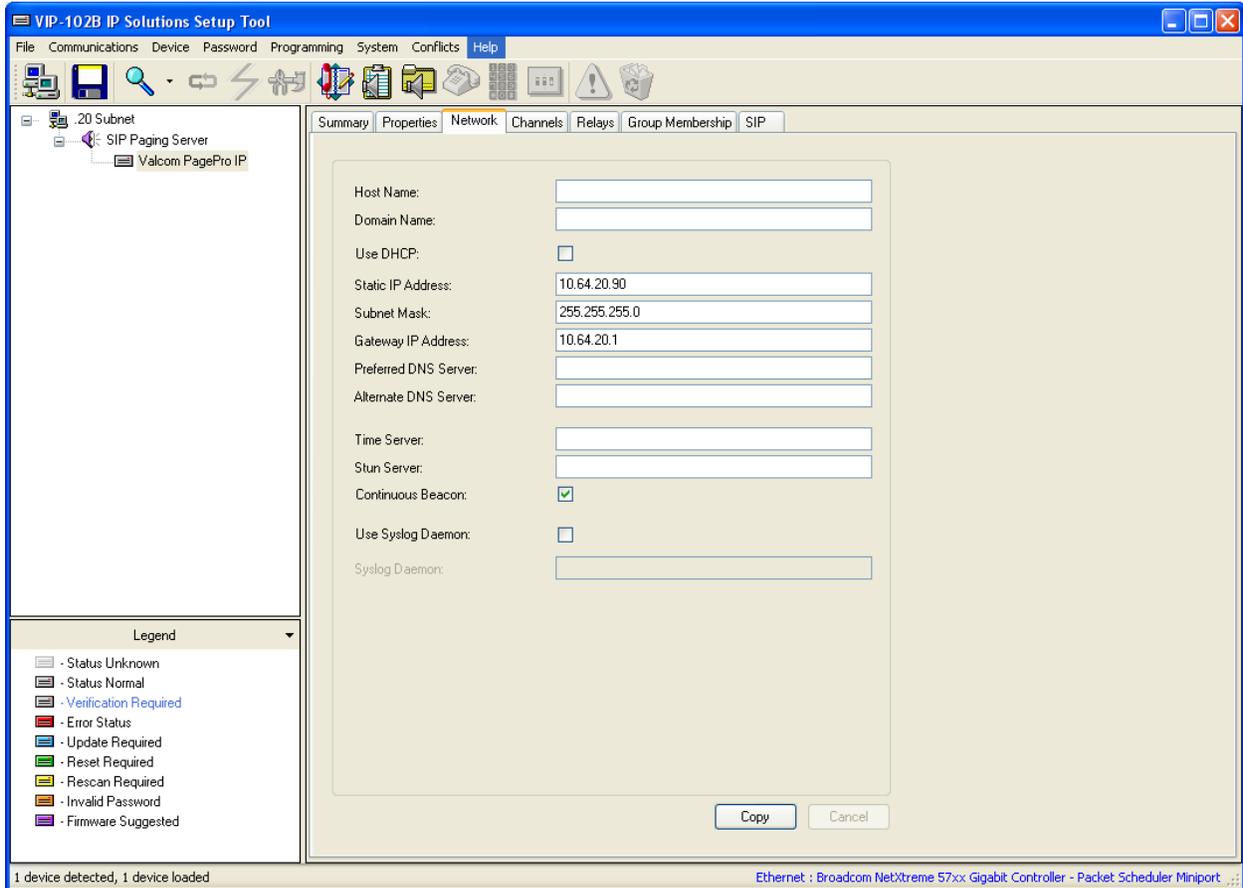
6.2. Administer Properties

Select the Valcom PagePro IP from the left pane to display the configuration tabs in the right pane. Select the **Properties** tab, and enter a descriptive **Device Name**. Select the appropriate time zone in the **Offset From UTC** field, and enter any desired **Comments**.



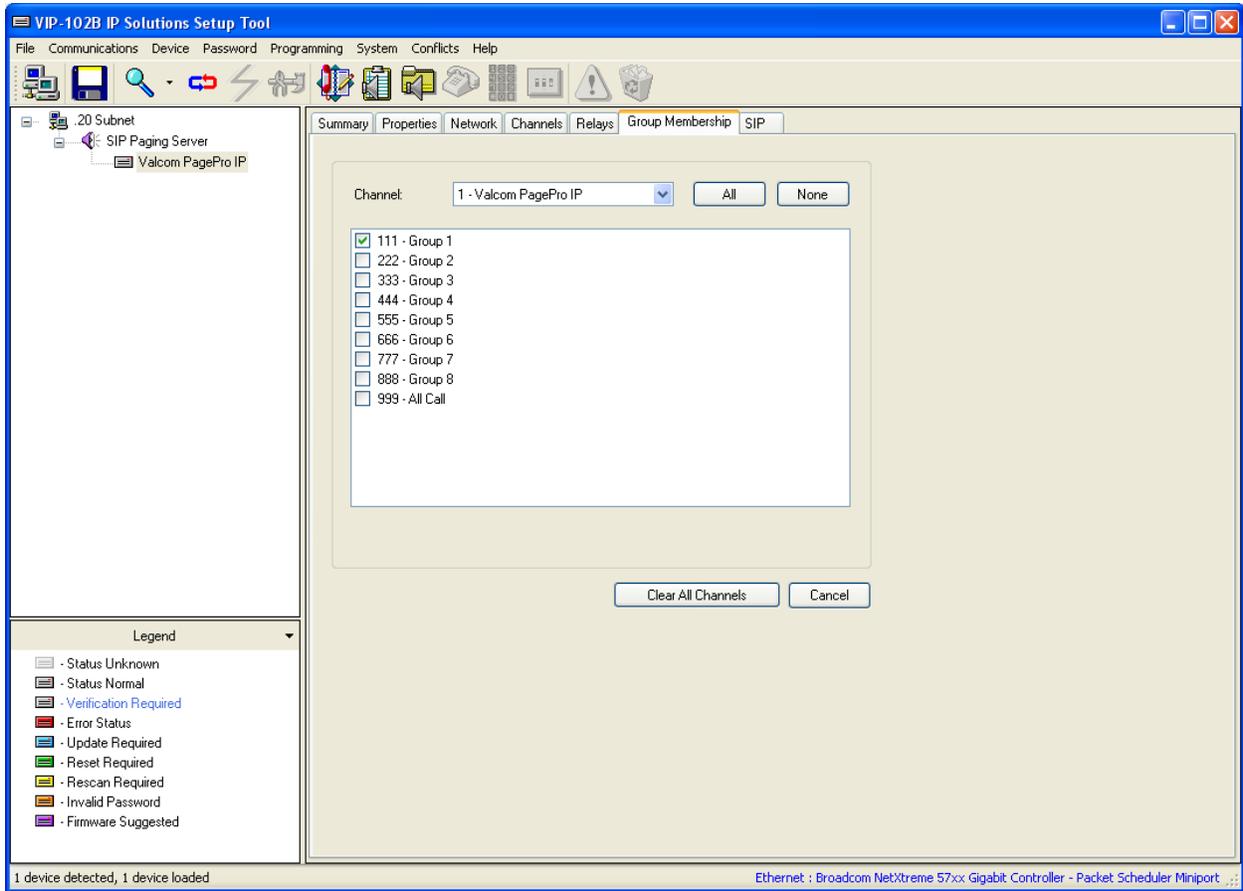
6.3. Administer Network

Select the **Network** tab and enter the appropriate values. During compliance testing, a **Static IP Address**, **Subnet Mask**, and **Gateway IP Address** were populated for the network configuration. The default values in the remaining fields may be retained.



6.4. Administer Group Membership

Select the **Group Membership** tab. Follow the appropriate documentation in **Section 10** to create the applicable speaker groups.

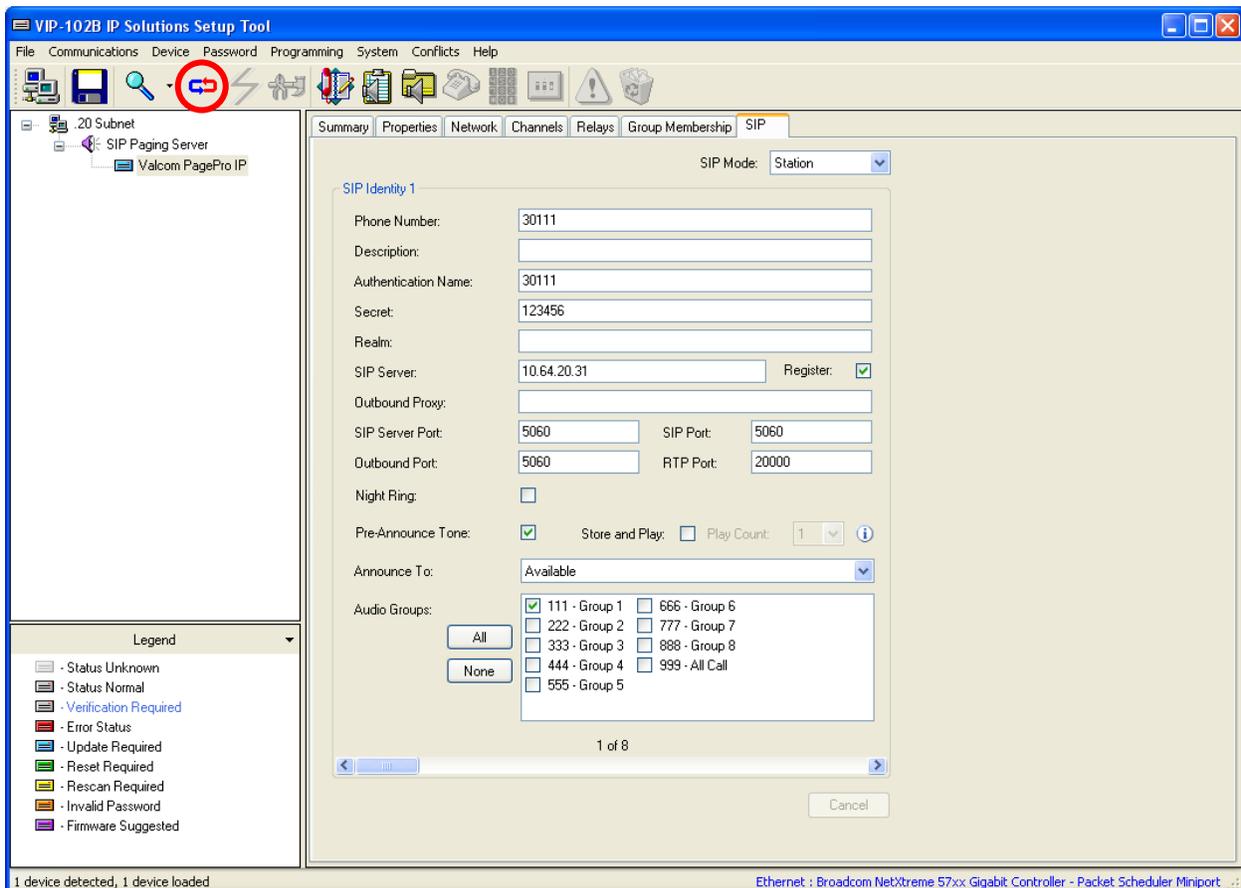


6.5. Administer SIP

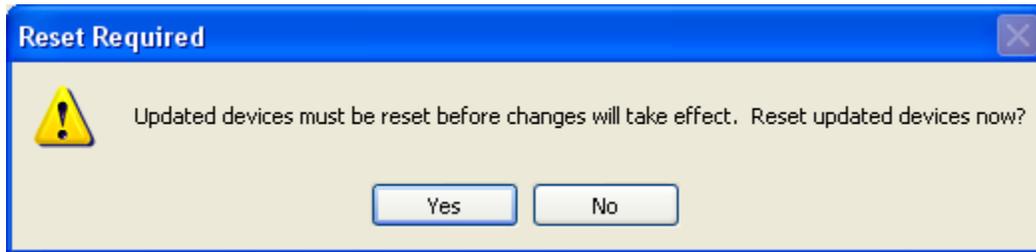
Select the **SIP** tab. Enter the following values for the specified fields, and retain the default values for the remaining fields.

- **Phone Number:** Enter the user extension from **Section 5.3**.
- **Authentication Name:** Enter the user handle from **Section 5.3**.
- **Secret:** Enter the user Security Code from **Section 5.3**.
- **SIP Server:** Enter the IP address of Session Manager.
- **Register:** Check this field.
- **Store and Play:** Check this field if desired (shown below as unchecked).
- **Audio Groups:** Select the desired group(s) of speakers to connect.

Move the slide toward the bottom of the screen to the right to administer **SIP Identity 2** (not shown), and use the credentials for the second SIP user from **Section 5.3**. Repeat this section to administer all eight SIP identities.



Click on the **Update Changed Devices** icon circled above. The **Reset Required** dialog box will appear as shown below. Click **Yes** to reset the updated devices.



7. General Test Approach and Test Results

The interoperability compliance test included feature and serviceability testing.

The feature testing covered SIP registration, basic calls, simultaneous calls, display verification, media shuffling, and audio codec negotiation. The feature test cases were performed manually. Various access numbers for the Valcom PagePro IP device were dialed to test connection to the proper speaker groups.

The serviceability testing focused on verifying the ability of the Valcom PagePro IP device to recover from adverse conditions, such as disconnecting and reconnecting the LAN cable to the Valcom PagePro IP. Additionally, the Communication Manager and Session Manager servers were each individually rebooted to verify the Valcom PagePro IP device was able to properly register and function normally after each server recovered.

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

- When shuffling (Direct IP-IP Audio) was enabled on Communication Manager, calls involving the Valcom devices did not shuffle.

8. Verification Steps

This section provides the tests that can be performed to verify proper configuration of Avaya Aura® Communication Manager, Avaya Aura® Session Manager, and the Valcom PagePro IP.

8.1. Verify User Registrations

On Session Manager, verify the registration status of the Valcom PagePro IP device by navigating to **Elements** → **Session Manager** → **System Status** → **User Registrations**. Verify that all the users administered in **Section 5.3** are listed as registered users.

8.2. Verify Valcom PagePro IP

Make a call to one of the access numbers for the Valcom PagePro IP device. Verify that the caller hears a pre-announce tone, and is connected to the appropriate speaker group from **Section 6.5** with a one-way talk path.

9. Conclusion

These Application Notes describe the configuration steps required for Valcom PagePro IP to successfully interoperate with Avaya Aura® Communication Manager and Avaya Aura® Session Manager.

All feature and serviceability test cases were completed with observations listed in **Section 7**.

10. Additional References

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

1. *Administering Avaya Aura™ Communication Manager*, Document 03-300509, Issue 6.0, Release 6.0, August 2010, available at <http://support.avaya.com>
2. *Administering Avaya Aura™ Communication Manager Server Options*, Document 03-603479, Issue 2, Release 6.0, June 2010, available at <http://support.avaya.com>
3. *Administering Avaya Aura™ Session Manager*, Document 03-603324, Issue 3, Release 6.0, August 2010, available at <http://support.avaya.com>
4. PagePro IP SIP Based Paging Server documentation is available at <http://www.valcom.com>
5. Valcom Talkback IP Speaker documentation is available at <http://www.valcom.com>
6. Valcom VIP-102B IP Solutions Setup Tool Reference Manual is available at <http://www.valcom.com>

©2011 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.