



Avaya Solution & Interoperability Test Lab

Application Notes for ClearOne Converge Pro VH20 with Avaya Aura® Session Manager and Avaya Aura® Communication Manager - Issue 1.0

Abstract

These Application Notes describe the steps required to integrate the ClearOne Converge Pro VH20 Conferencing Solution with Avaya Aura® Session Manager and Avaya Aura® Communication Manager using a SIP interface. The Converge Pro VH20 links other Converge Pro products to create a complete audio conferencing system that is integrated with an Avaya SIP telephony network. In this compliance test, Converge Pro VH20 provided SIP connectivity for the Converge Pro 880T equipped with a speaker and microphone. The focus of these Application Notes is on the interoperability between Converge Pro VH20, Session Manager, and Communication 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 the steps required to integrate the ClearOne Converge Pro VH20 Conferencing Solution with Avaya Aura® Session Manager and Avaya Aura® Communication Manager using a SIP interface. The Converge Pro VH20 links other Converge Pro products to create a complete audio conferencing system that is integrated with an Avaya SIP telephony network. In this compliance test, Converge Pro VH20 provided SIP connectivity for the Converge Pro 880T equipped with a speaker and microphone. The focus of these Application Notes is on the interoperability between Converge Pro VH20, Session Manager, and Communication Manager.

2. General Test Approach and Test Results

To verify interoperability of ClearOne Converge Pro VH20, linking Converge Pro 880T, with Communication Manager and Session Manager, voice calls were made to Avaya IP telephones (SIP and H.323). All test cases were performed manually.

2.1 Interoperability Compliance Testing

Interoperability compliance testing covered the following features and functionality:

- Successful registration of Converge Pro VH20 with Session Manager.
- Voice calls between Converge Pro VH20 and Avaya IP telephones (SIP and H.323), including proper call disconnect.
- Long duration calls.
- G.711 and G.729 codec support and code negotiation.
- Audio mute on Converge Pro VH20 and Avaya endpoints.
- Converge Pro VH20 DTMF support.
- Proper handling of unsuccessful calls due to call abort, no answer, dialing invalid number, and called party busy.
- Proper system recovery after a restart of Converge Pro VH20 and loss of IP connectivity.

2.2 Test Results

All test cases passed. One observation is that the Communication Manager Preferred Minimum Session Refresh Interval setting in the SIP trunk group form and the Converge Pro VH20 Min-SE Timer have to match, or incoming calls to VH20 will fail with a SIP Status message indicating “Session Interval Too Small”.

2.3 Support

For technical support and information on Converge Pro VH20, contact ClearOne at:

- Phone: 800-283-5936 (toll free)
- Email: techsupport@clearone.com
- Website: <http://www.clearone.com/support>

3. Reference Configuration

Figure 1 illustrates a sample configuration with an Avaya SIP-based network that includes the following Avaya products:

- Avaya Aura® Communication Manager running on an Avaya S8800 Server with a G650 Media Gateway. Communication Manager was configured as an Evolution Server.
- Avaya Aura® Session Manager connected to Communication Manager via a SIP trunk and acting as a Registrar/Proxy for SIP telephones and video endpoints.
- Avaya Aura® System Manager used to configure Session Manager.

In addition, ClearOne Converge Pro VH20 registered as a SIP endpoint to Session Manager. Converge Pro VH20 then connected to Converge Pro 880T, which provided connectivity to a speaker and tabletop microphone. The Converge Console was used to configure the Converge Pro VH20. All SIP devices registered with Session Manager and were configured as Off-PBX Stations (OPS) on Communication Manager.

Note: The focus of these Application Notes is on the Converge Pro VH20.

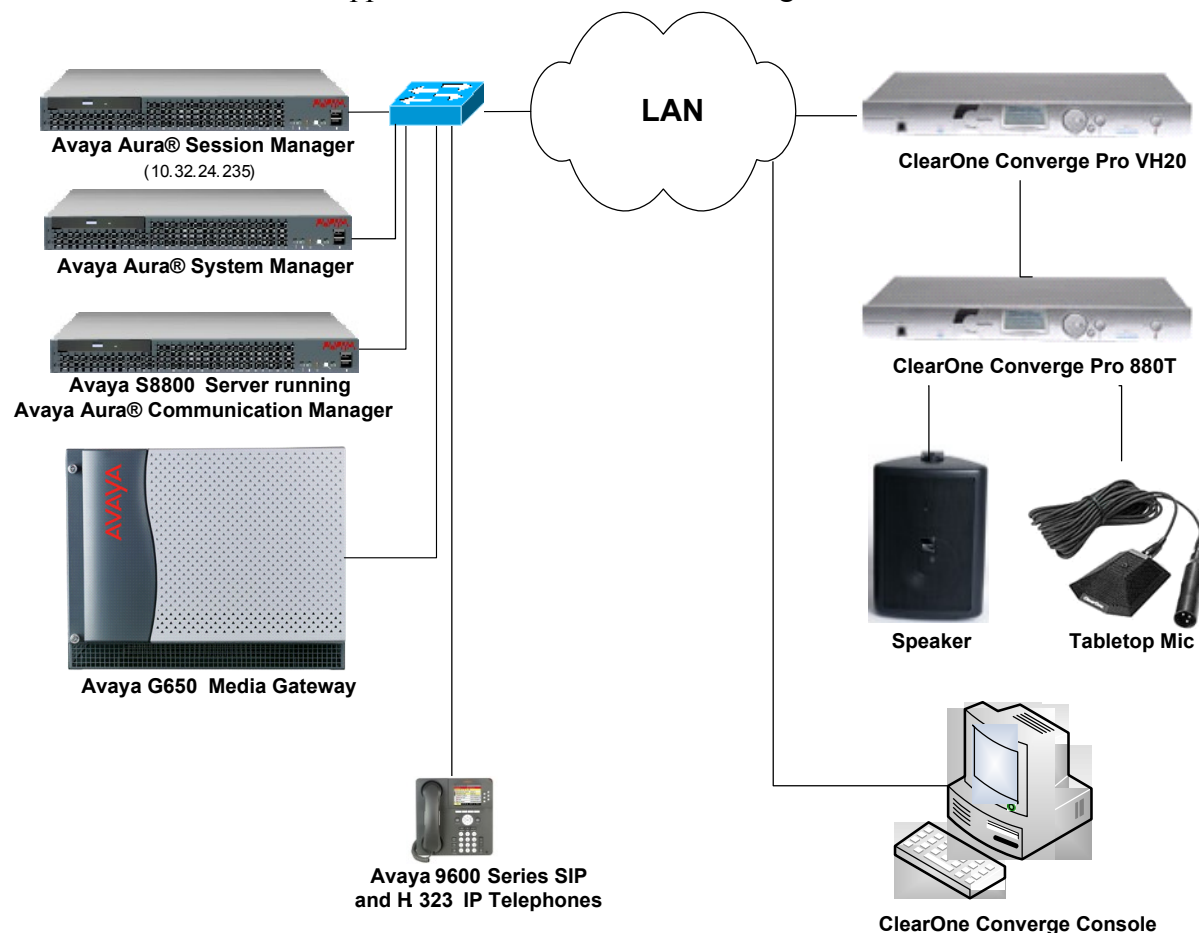


Figure 1: Avaya SIP Network with ClearOne Converge Pro VH20

4. Equipment and Software Validated

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

Hardware Component	Version
Avaya S8800 Servers and G650 Media Gateway	Avaya Aura® Communication Manager 6.0.1 SP 3
Avaya Aura® Session Manager	6.1 (6.1.2.0-612004)
Avaya Aura® System Manager	6.1.0 (6.1.0.4.5072-6.1.4.113)
Avaya 9600 Series IP Telephones	3.011b (H.323) 2.6 (SIP)
ClearOne Converge Pro VH20	3.0.6.15
ClearOne Converge Pro 880T	3.0.6.15
ClearOne Converge Console	3.0.5

5. Configure Communication Manager

This section provides the procedures for configuring Communication Manager. The procedures include the following areas:

- Verify Communication Manager license
- Configure Converge Pro VH20 as an Off-PBX Station (OPS)
- Configure a SIP trunk between Communication Manager and Session Manager

Use the System Access Terminal (SAT) to configure Communication Manager and log in with the appropriate credentials.

5.1 Verify OPS and SIP Trunk Capacity

Using the SAT, verify that the Off-PBX Telephones (OPS), video capable endpoints, and SIP Trunk options are enabled on the **system-parameters customer-options** form. The license file installed on the system controls these options. If a required feature is not enabled, contact an authorized Avaya sales representative.

On **Page 1**, verify that the number of OPS stations allowed in the system is sufficient for the number of SIP endpoints that will be deployed.

```
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 161
                                Maximum Stations: 41000 78
                                Maximum XMOBILE Stations: 41000 0
Maximum Off-PBX Telephones - EC500: 36000 0
Maximum Off-PBX Telephones - OPS: 41000 8
Maximum Off-PBX Telephones - PBFMC: 36000 0
Maximum Off-PBX Telephones - PVFMC: 36000 0
Maximum Off-PBX Telephones - SCCAN: 0 0
Maximum Survivable Processors: 313 0

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

On **Page 2** of the **system-parameters customer-options** form, verify that the number SIP trunks supported by the system is sufficient.

display system-parameters customer-options		Page 2 of 11
OPTIONAL FEATURES		
IP PORT CAPACITIES		USED
Maximum Administered H.323 Trunks:	12000	30
Maximum Concurrently Registered IP Stations:	18000	20
Maximum Administered Remote Office Trunks:	12000	0
Maximum Concurrently Registered Remote Office Stations:	18000	0
Maximum Concurrently Registered IP eCons:	414	0
Max Concur Registered Unauthenticated H.323 Stations:	100	0
Maximum Video Capable Stations:	18000	1
Maximum Video Capable IP Softphones:	18000	4
Maximum Administered SIP Trunks:	24000	30
Maximum Administered Ad-hoc Video Conferencing Ports:	24000	0
Maximum Number of DS1 Boards with Echo Cancellation:	522	0
Maximum TN2501 VAL Boards:	128	1
Maximum Media Gateway VAL Sources:	250	0
Maximum TN2602 Boards with 80 VoIP Channels:	128	0
Maximum TN2602 Boards with 320 VoIP Channels:	128	0
Maximum Number of Expanded Meet-me Conference Ports:	300	0
(NOTE: You must logoff & login to effect the permission changes.)		

5.2 Configure SIP Trunk

In the **IP Node Names** form, assign an IP address and host name for the C-LAN board in the G650 Media Gateway and the Session Manager SIP interface. The host names will be used throughout the other configuration screens of Communication Manager.

change node-names ip		Page 1 of 2
IP NODE NAMES		
Name	IP Address	
Gateway001	10.32.24.1	
ModMsg	192.50.10.45	
clancrm	10.32.24.20	
default	0.0.0.0	
devcon-asm	10.32.24.235	
medprocrm	10.32.24.21	
procr	10.32.24.10	
procr6	::	

(8 of 8 administered node-names were displayed)
Use 'list node-names' command to see all the administered node-names
Use 'change node-names ip xxx' to change a node-name 'xxx' or add a node-name

In the **IP Network Region** form, the **Authoritative Domain** field is configured to match the domain name configured on Session Manager. In this configuration, the domain name is *avaya.com*. By default, **IP-IP Direct Audio** (shuffling) is enabled to allow audio traffic to be sent directly between IP endpoints without using media resources in the Avaya G650 Media Gateway. The **IP Network Region** form also specifies the **IP Codec Set** to be used for calls routed over the SIP trunk to Session Manager. This codec set is used when its corresponding network region (i.e., IP Network Region '1') is specified in the SIP signaling group.

change ip-network-region 1		Page 1 of 20
IP NETWORK REGION		
Region: 1		
Location: 1	Authoritative Domain: avaya.com	
Name:		
MEDIA PARAMETERS	Intra-region IP-IP Direct Audio: yes	
Codec Set: 1	Inter-region IP-IP Direct Audio: yes	
UDP Port Min: 2048	IP Audio Hairpinning? y	
UDP Port Max: 65535		
DIFFSERV/TOS PARAMETERS		
Call Control PHB Value: 34		
Audio PHB Value: 46		
Video PHB Value: 26		
802.1P/Q PARAMETERS		
Call Control 802.1p Priority: 7		
Audio 802.1p Priority: 6		
Video 802.1p Priority: 5	AUDIO RESOURCE RESERVATION PARAMETERS	
H.323 IP ENDPOINTS	RSVP Enabled? n	
H.323 Link Bounce Recovery? y		
Idle Traffic Interval (sec): 20		
Keep-Alive Interval (sec): 5		
Keep-Alive Count: 5		

In the **IP Codec Set** form, select the audio codec type supported for calls routed over the SIP trunk to Converge Pro VH20. The form is accessed via the **change ip-codec-set 1** command. Note that IP codec set '1' was specified in IP Network Region '1' shown above. The default settings of the **IP Codec Set** form are shown below. Testing was also performed with the G.729B codec.

change ip-codec-set 1

Page 1 of 2

IP Codec Set

Codec Set: 1

	Audio Codec	Silence Suppression	Frames Per Pkt	Packet Size (ms)
1:	G.711MU	n	2	20
2:				
3:				
4:				
5:				
6:				
7:				

Prior to configuring a SIP trunk group for communication with Session Manager, a SIP signaling group must be configured. Configure the Signaling Group form as follows:

- Set the **Group Type** field to *sip*.
- Set the **IMS Enabled** field to *n*.
- Set the **Transport Method** field to *tcp*.
- Specify the C-LAN board and the Session Manager as the two ends of the signaling group in the **Near-end Node Name** field and the **Far-end Node Name** field, respectively. These field values were taken from the **IP Node Names** form.
- Ensure that the TCP port value of *5060* is configured in the **Near-end Listen Port** and the **Far-end Listen Port** fields.
- The preferred codec for the call will be selected from the IP codec set assigned to the IP network region specified in the **Far-end Network Region** field.
- Enter the domain name of Session Manager in the **Far-end Domain** field. In this configuration, the domain name is *avaya.com*.
- The **DTMF over IP** field should be set to the default value of *rtp-payload*. Communication Manager supports DTMF transmission using RFC 2833.
- The **Direct IP-IP Audio Connections** field was enabled on this form.
- The default values for the other fields may be used.

add signaling-group 50		Page 1 of 1
SIGNALING GROUP		
<div style="display: flex; justify-content: space-between;"> Group Number: 50 Group Type: sip </div> <div style="display: flex; justify-content: space-between;"> IMS Enabled? n Transport Method: tcp </div> <div style="display: flex; justify-content: space-between;"> Q-SIP? n SIP Enabled LSP? n </div> <div style="display: flex; justify-content: space-between;"> IP Video? n Enforce SIPS URI for SRTP? y </div> <div style="display: flex; justify-content: space-between;"> Peer Detection Enabled? y Peer Server: SM </div>		
<div style="display: flex; justify-content: space-between;"> Near-end Node Name: clancrm Far-end Node Name: devcon-asm </div> <div style="display: flex; justify-content: space-between;"> Near-end Listen Port: 5060 Far-end Listen Port: 5060 </div> <div style="display: flex; justify-content: space-between;"> Far-end Network Region: 1 Far-end Secondary Node Name: </div>		
<div style="display: flex; justify-content: space-between;"> Far-end Domain: avaya.com Bypass If IP Threshold Exceeded? n </div> <div style="display: flex; justify-content: space-between;"> Incoming Dialog Loopbacks: eliminate RFC 3389 Comfort Noise? n </div> <div style="display: flex; justify-content: space-between;"> DTMF over IP: rtp-payload Direct IP-IP Audio Connections? y </div> <div style="display: flex; justify-content: space-between;"> Session Establishment Timer(min): 3 IP Audio Hairpinning? n </div> <div style="display: flex; justify-content: space-between;"> Enable Layer 3 Test? n Initial IP-IP Direct Media? n </div> <div style="display: flex; justify-content: space-between;"> H.323 Station Outgoing Direct Media? n Alternate Route Timer(sec): 6 </div>		

Configure the **Trunk Group** form as shown below. This trunk group is used for calls to SIP endpoints. Set the **Group Type** field to *sip*, set the **Service Type** field to *tie*, specify the signaling group associated with this trunk group in the **Signaling Group** field, and specify the **Number of Members** supported by this SIP trunk group. Configure the other fields in bold and accept the default values for the remaining fields.

add trunk-group 50		Page 1 of 21	
TRUNK GROUP			
Group Number: 50	Group Type: sip	CDR Reports: y	
Group Name: To devcon-asm	COR: 1	TN: 1	TAC: 1050
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: 50	
		Number of Members: 10	

On Page 2, verify that the **Preferred Minimum Session Refresh Interval (sec)** field matches the configuration on Converge Pro VH20 as described in **Section 7**. In this compliance test, Converge Pro VH20 was configured to match the setting on Communication Manager. That is, the Min SE Timer on Converge Pro VH20 was set to 180 sec. Alternatively, this timer can be changed in the trunk group to match the setting on Converge Pro VH20.

add trunk-group 50		Page 2 of 21	
Group Type: sip			
TRUNK PARAMETERS			
Unicode Name: auto			
Redirect On OPTIM Failure: 5000			
SCCAN? n	Digital Loss Group: 18		
Preferred Minimum Session Refresh Interval(sec): 90			
Disconnect Supervision - In? y Out? y			
XOIP Treatment: auto		Delay Call Setup When Accessed Via IGAR? n	

5.3 Configure Station for ClearOne Converge Pro VH20

The **station** and **off-pbx-telephone station-mapping** configuration shown in this section was automatically performed after creating the **User** in Session Manager as described in **Section 6.7**. In this section, simply verify the settings. Note that the **User** has to be added in Session Manager first before it can be viewed on Communication Manager. Alternatively, this configuration could have also been performed manually.

Use the **display station** command to view the station created for Converge Pro VH20 and verify the settings in bold. Note that the **IP Video** field must be set to *y*.

add station 78305		Page 1 of 6
STATION		
Extension: 78401	Lock Messages? n	BCC: 0
Type: 9630SIP	Security Code:	TN: 1
Port: IP	Coverage Path 1:	COR: 1
Name: 78305, VH20	Coverage Path 2:	COS: 1
	Hunt-to Station:	
STATION OPTIONS		
	Time of Day Lock Table:	
Loss Group: 19		
	Message Lamp Ext: 78305	
Display Language: english	Button Modules: 0	
Survivable COR: internal		
Survivable Trunk Dest? y	IP SoftPhone? n	
	IP Video? n	

Use the **display off-pbx-telephone station-mapping** command to view the mapping of the Communication Manager extensions (e.g., 78305) to the same extension configured in System Manager. Verify the field values shown. For the sample configuration, the **Trunk Selection** field is set to *aar* so that AAR call routing is used to route calls to Session Manager. AAR call routing configuration is not shown in these Application Notes. The **Configuration Set** value can reference a set that has the default settings.

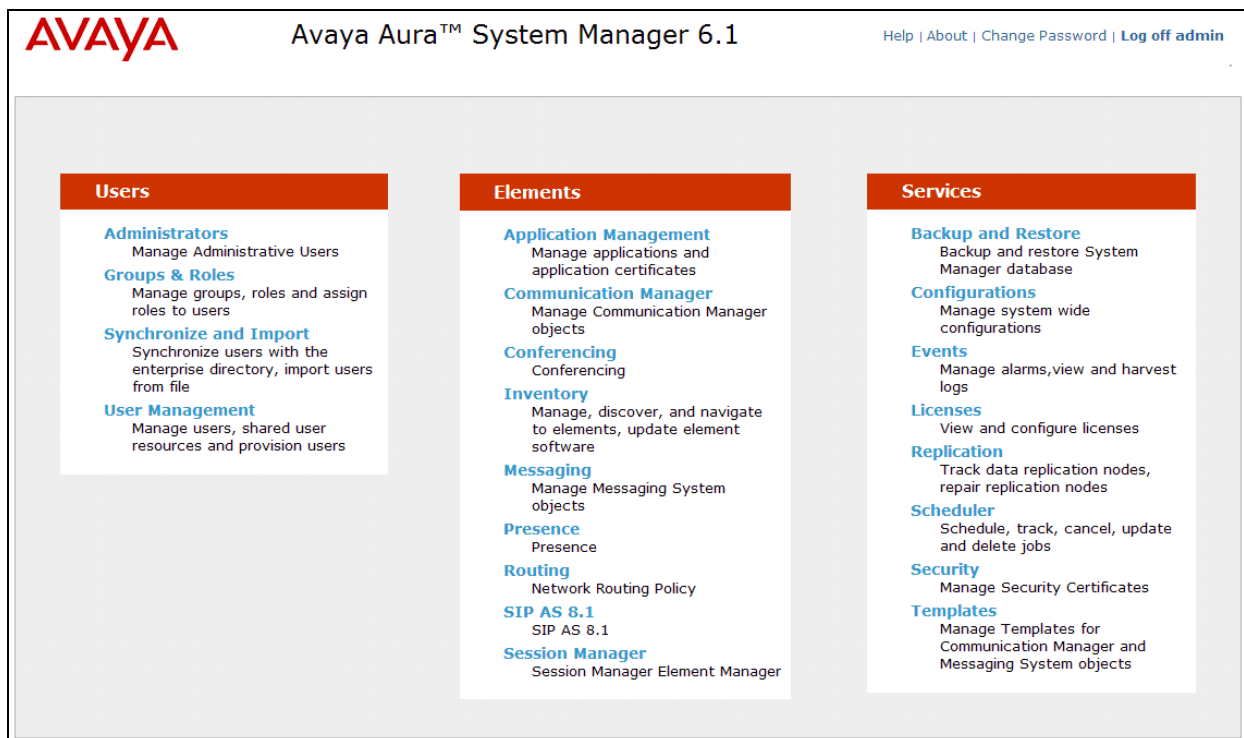
change off-pbx-telephone station-mapping 78305						Page	1	of	3
STATIONS WITH OFF-PBX TELEPHONE INTEGRATION									
Station Extension	Application	Dial Prefix	CC	Phone Number	Trunk Selection	Config Set	Dual Mode		
78305	OPS	-		78305	aar	1			

6. Configure Session Manager

This section provides the procedures for configuring Session Manager. The procedures include adding the following items:

- SIP domain
- Logical/physical Locations that can be occupied by SIP Entities
- SIP Entities corresponding to Session Manager and Communication Manager
- Entity Links, which define the SIP trunk parameters used by Session Manager when routing calls to/from SIP Entities
- Define Communication Manager as Administrable Entity (i.e., Managed Element)
- Application Sequence
- Session Manager, corresponding to the Session Manager Server to be managed by System Manager
- Add SIP User

Configuration is accomplished by accessing the browser-based GUI of System Manager using the URL “https://<ip-address>/SMGR”, where <ip-address> is the IP address of System Manager. Log in with the appropriate credentials. The initial screen is displayed as shown below. The configuration in this section will be performed under **Routing** and **Session Manager** listed within the **Elements** box.



6.1 Specify SIP Domain

Add the SIP domain for which the communications infrastructure will be authoritative. Do this by selecting **Domains** on the left and clicking the **New** button (not shown) on the right. The following screen will then be shown. Fill in the following:

- **Name:** The authoritative domain name (e.g., *avaya.com*)
- **Notes:** Descriptive text (optional).

Click **Commit**.

Since the sample configuration does not deal with any other domains, no additional domains need to be added.

The screenshot shows the Avaya Aura System Manager 6.1 interface. The top navigation bar includes the Avaya logo, the title "Avaya Aura™ System Manager 6.1", and links for "Help", "About", "Change Password", and "Log off admin". Below the navigation bar, there is a breadcrumb trail: "Home / Elements / Routing / Domains - Domain Management". The left sidebar contains a tree view with "Routing" expanded, showing sub-items: "Domains", "Locations", "Adaptations", "SIP Entities", "Entity Links", "Time Ranges", "Routing Policies", "Dial Patterns", "Regular Expressions", and "Defaults". The main content area is titled "Domain Management" and contains a table with one item. The table has columns: "Name", "Type", "Default", and "Notes". The row shows "avaya.com" as the Name, "sip" as the Type, an unchecked "Default" checkbox, and "Enterprise Domain" as the Notes. Below the table, there is a red asterisk and the text "Input Required". At the top right of the main content area, there are "Commit" and "Cancel" buttons. At the bottom right, there are also "Commit" and "Cancel" buttons. A "Filter: Enable" link is visible on the right side of the table.

Name	Type	Default	Notes
* avaya.com	sip	<input type="checkbox"/>	Enterprise Domain

6.2 Add Locations

Locations can be used to identify logical and/or physical locations where SIP Entities reside for purposes of bandwidth management. To add a location, select **Locations** on the left and click on the **New** button (not shown) on the right. The following screen will then be shown. Fill in the following:

Under *General*:

- **Name:** A descriptive name.
- **Notes:** Descriptive text (optional).

Under *Location Pattern*:

- **IP Address Pattern:** A pattern used to logically identify the location.
- **Notes:** Descriptive text (optional).

The screen below shows addition of the *BR-DevConnect* location, which includes the Communication Manager and Session Manager. Click **Commit** to save the Location definition.

AVAYA Avaya Aura™ System Manager 6.1 [Help](#) | [About](#) | [Change Password](#) | [Log off admin](#)

[Routing](#) [Home](#)

Routing [Home / Elements / Routing / Locations - Location Details](#)

Location Details [Help ?](#) [Commit](#) [Cancel](#)

Call Admission Control has been set to ignore SDP. All calls will be counted using the Default Audio Bandwidth.
See [Session Manager -> Session Manager Administration -> Global Setting](#)

General

* **Name:**

Notes:

Overall Managed Bandwidth

Managed Bandwidth Units:

Total Bandwidth:

Per-Call Bandwidth Parameters

* **Default Audio Bandwidth:**

Location Pattern

[Add](#) [Remove](#)

1 Item [Refresh](#) [Filter: Enable](#)

<input type="checkbox"/>	IP Address Pattern	Notes
<input type="checkbox"/>	* 10.32.24.*	<input type="text"/>

Select : [All](#), [None](#)

* Input Required [Commit](#) [Cancel](#)

6.3 Add SIP Entities

In the sample configuration, a SIP Entity is added for Session Manager and the C-LAN in the G650 Media Gateway.

6.3.1 Session Manager

A SIP Entity must be added for Session Manager. To add a SIP Entity, select **SIP Entities** on the left and click on the **New** button (not shown) on the right. The following screen is displayed. Fill in the following:

Under *General*:

- **Name:** A descriptive name.
- **FQDN or IP Address:** IP address of the signaling interface on Session Manager.
- **Type:** Select *Session Manager*.
- **Location:** Select the location defined previously.
- **Time Zone:** Time zone for this location.

Under *Port*, click **Add**, and then edit the fields in the resulting new row as shown below:

- **Port:** Port number on which the system listens for SIP requests.
- **Protocol:** Transport protocol to be used to send SIP requests.
- **Default Domain** The domain used for the enterprise (e.g., *avaya.com*).

Defaults can be used for the remaining fields. Click **Commit** to save each SIP Entity definition.

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

Home / Elements / Routing / SIP Entities - SIP Entity Details

[Help ?](#)

SIP Entity Details

[Commit](#) [Cancel](#)

General

* **Name:**

* **FQDN or IP Address:**

Type: ▼

Notes:

Location: ▼

Outbound Proxy: ▼

Time Zone: ▼

Credential name:

SIP Link Monitoring

SIP Link Monitoring: ▼

Entity Links

Entity Links can be modified after SIP Entity is committed.

Port

[Add](#) [Remove](#)

3 Items [Refresh](#)

Filter: [Enable](#)

<input type="checkbox"/>	Port	Protocol	Default Domain	Notes
<input type="checkbox"/>	<input type="text" value="5060"/>	<input type="text" value="UDP"/> ▼	<input type="text" value="avaya.com"/> ▼	<input type="text"/>
<input type="checkbox"/>	<input type="text" value="5060"/>	<input type="text" value="TCP"/> ▼	<input type="text" value="avaya.com"/> ▼	<input type="text"/>
<input type="checkbox"/>	<input type="text" value="5061"/>	<input type="text" value="TLS"/> ▼	<input type="text" value="avaya.com"/> ▼	<input type="text"/>

Select : All, None

* Input Required

[Commit](#) [Cancel](#)

6.3.2 Communication Manager

A SIP Entity must be added for the Communication Manager. To add a SIP Entity, select **SIP Entities** on the left and click on the **New** button (not shown) on the right. The following screen is displayed. Fill in the following:

Under *General*:

- **Name:** A descriptive name.
- **FQDN or IP Address:** IP address of the signaling interface (e.g., C-LAN board) on the telephony system.
- **Type:** Select *CM*.
- **Location:** Select the location defined previously.
- **Time Zone:** Time zone for this location.

Defaults may be used for the remaining fields. Click **Commit** to save the SIP Entity definition.

The screenshot displays the Avaya Aura System Manager 6.1 web interface. The top navigation bar includes the Avaya logo, the title "Avaya Aura™ System Manager 6.1", and links for "Help", "About", "Change Password", and "Log off admin". A breadcrumb trail shows "Home / Elements / Routing / SIP Entities - SIP Entity Details". On the left, a sidebar menu lists various configuration areas, with "SIP Entities" selected. The main content area is titled "SIP Entity Details" and features a "General" tab. The form contains several fields: "Name" (devcon13), "FQDN or IP Address" (10.32.24.20), "Type" (CM), "Notes", "Adaptation", "Location" (BR-DevConnect), "Time Zone" (America/New_York), "Override Port & Transport with DNS SRV" (unchecked), "SIP Timer B/F (in seconds)" (4), "Credential name", and "Call Detail Recording" (none). Below these is the "SIP Link Monitoring" section with a dropdown set to "Use Session Manager Configuration". At the bottom, a red message states "Entity Links can be modified after SIP Entity is committed." and a note indicates "* Input Required". "Commit" and "Cancel" buttons are present at the top right and bottom right of the form area.

6.4 Add Entity Link

The SIP trunk from Session Manager to Communication Manager is described by an Entity link. To add an Entity Link, select **Entity Links** on the left and click on the **New** button (not shown) on the right. Fill in the following fields in the new row that is displayed:

- **Name:** A descriptive name (e.g., *devcon13 Link*).
- **SIP Entity 1:** Select the Session Manager.
- **Protocol:** Select the appropriate protocol.
- **Port:** Port number to which the other system sends SIP requests.
- **SIP Entity 2:** Select the name of Communication Manager.
- **Port:** Port number on which the other system receives SIP requests.
- **Trusted:** Check this box. *Note: If this box is not checked, calls from the associated SIP Entity specified in **Section 6.3.2** will be denied.*

Click **Commit** to save the Entity Link definition.

Avaya Aura™ System Manager 6.1

Help | About | Change Password | Log off admin

Routing * Home

Home / Elements / Routing / Entity Links - Entity Links

Entity Links

Help ?

Commit Cancel

1 Item Refresh Filter: Enable

Name	SIP Entity 1	Protocol	Port	SIP Entity 2	Port	Trusted	Notes
* devcon13 Link	* devcon-asm	TCP	* 5060	* devcon13	* 5060	<input checked="" type="checkbox"/>	

* Input Required

Commit Cancel

6.5 Define Communication Manager as Managed Element

Before adding SIP users, Communication Manager must be added to System Manager as a managed element. This action allows System Manager to access Communication Manager over its administration interface. Using this administration interface, System Manager will notify Communication Manager when new SIP users are added.

To define Communication Manager as a managed element, select **Elements→Inventory→Manage Elements** on the left and click on the **New** button (not shown) on the right. In the **New Entities Instance** screen (not shown), select **CM** in the **Type** field can click **Commit**.

In the **New CM Instance** screen, fill in the following fields as follows:

In the *Application* tab:

- **Name:** Enter an identifier for Communication Manager.
- **Type:** Select **CM** from the drop-down field.
- **Node:** Enter the IP address of the administration interface for Communication Manager.

The screenshot shows the Avaya Aura System Manager 6.1 interface. The top navigation bar includes the Avaya logo, the title 'Avaya Aura™ System Manager 6.1', and links for 'Help | About | Change Password | Log off admin'. Below this is a breadcrumb trail: 'Home / Elements / Inventory / Manage Elements - New CM Instance'. The left sidebar shows a tree view with 'Inventory' expanded, containing 'Manage Elements', 'Discovered Inventory', 'Discovery Management', and 'Synchronization'. The main content area is titled 'New CM Instance' and contains a form with two tabs: 'Application' (selected) and 'Attributes'. The 'Application' tab has the following fields: 'Name' (text input with value 'devcon13-CM-ES'), 'Type' (dropdown menu with value 'CM' and a 'Reset' button), 'Description' (text area), and 'Node' (text input with value '10.32.24.10'). Below these fields are sections for 'Access Point' and 'Port', each with a dropdown arrow. At the bottom right of the form are 'Commit' and 'Cancel' buttons. A legend at the bottom left indicates that an asterisk (*) denotes a required field.

In the *Attributes* tab:

- **Login / Password:** Enter the login and password used for administration access.
- **Is SSH Connection:** Enable SSH access.
- **Port:** Enter the port number for SSH administration access (5022).

Defaults can be used for the remaining fields. Click **Commit** to save the settings.

The screenshot shows the Avaya Aura System Manager 6.1 interface. The top navigation bar includes the Avaya logo, the title 'Avaya Aura™ System Manager 6.1', and links for 'Help | About | Change Password | Log off admin'. Below this is a breadcrumb trail: 'Home / Elements / Inventory / Manage Elements - New CM Instance'. The left sidebar shows a tree view with 'Inventory' expanded, containing 'Manage Elements', 'Discovered Inventory', 'Discovery Management', and 'Synchronization'. The main content area is titled 'New CM Instance' and has 'Commit' and 'Cancel' buttons. It features two tabs: 'Application' and 'Attributes', with the 'Attributes' tab selected. Under the 'Attributes' tab, there is a section for 'SNMP Attributes' with a 'Version' field set to 'None' (radio buttons for None, V1, V3). Below this is a section for 'Attributes' containing several fields: 'Login' (masked with dots), 'Password' (masked with dots), 'Confirm Password' (masked with dots), 'Is SSH Connection' (checked checkbox), 'Port' (text field with '5022'), 'Alternate IP Address' (text field), 'RSA SSH Fingerprint (Primary IP)' (text field), 'RSA SSH Fingerprint (Alternate IP)' (text field), 'Is ASG Enabled' (unchecked checkbox), 'ASG Key' (text field), 'Confirm ASG Key' (text field), and 'Location' (text field). At the bottom left, there is a legend: '* Required'. At the bottom right, there are 'Commit' and 'Cancel' buttons.

6.6 Add Application Sequence

To define an application for Communication Manager, navigate to **Elements → Session Manager → Application Configuration → Applications** on the left and select **New** button (not shown) on the right. Fill in the following fields:

- **Name:** Enter name for application.
- **SIP Entity:** Select the Communication Manager SIP entity.
- **CM System for SIP Entity** Select the Communication Manager managed element.

Click **Commit** to save the Application definition.

The screenshot shows the Avaya Aura System Manager 6.1 web interface. The top header includes the Avaya logo, the product name "Avaya Aura™ System Manager 6.1", and links for "Help", "About", "Change Password", and "Log off admin". A breadcrumb trail reads "Home / Elements / Session Manager / Application Configuration / Applications - Applications". The left sidebar contains a navigation menu with items like "Session Manager", "Dashboard", "Session Manager Administration", "Communication Profile Editor", "Network Configuration", "Device and Location Configuration", "Application Configuration", "Applications", "Application Sequences", "Implicit Users", "NRS Proxy Users", "System Status", and "System Tools". The main content area is titled "Application Editor" and contains the following fields:

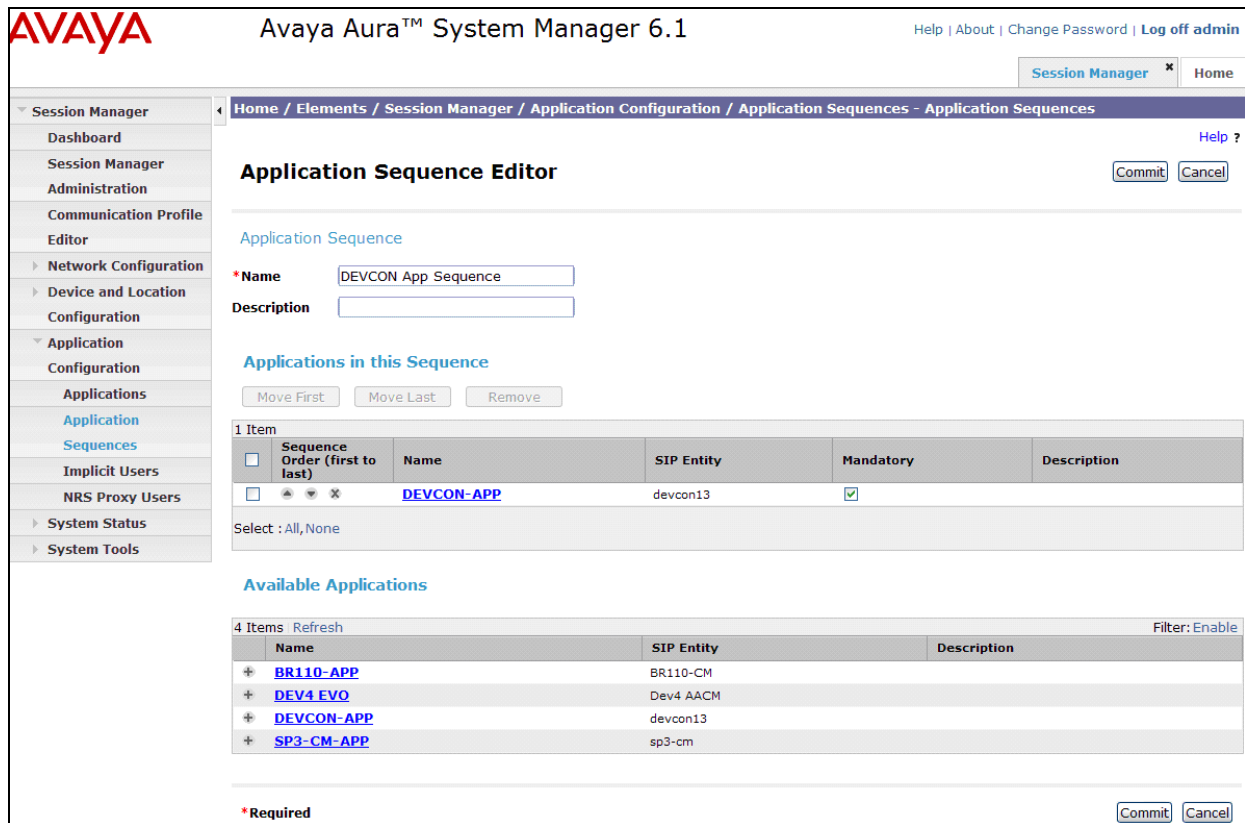
- Name:** A text input field containing "DEVCON-APP".
- SIP Entity:** A dropdown menu showing "devcon13".
- CM System for SIP Entity:** A dropdown menu showing "devcon13-CM-ES", with a "Refresh" button and a link "View/Add CM Systems".
- Description:** A text input field.
- Application Attributes (optional):** A table with two columns: "Name" and "Value". It contains two rows: "Application Handle" and "URI Parameters", each with an associated text input field.

At the bottom of the form, there is a legend indicating that fields marked with an asterisk (*) are required. "Commit" and "Cancel" buttons are located at the top right and bottom right of the form area.

Next, navigate to **Elements → Session Manager → Application Configuration → Application Sequences** to define the Application Sequence for Communication Manager as shown below. Provide a **Name** (e.g., *DEVCON App Sequence*) for the Application Sequence and under **Available Applications**, click on the plus (+) sign by *DEVCON-APP* to add it under the **Application in this sequence** section.

Verify a new entry is added to the **Applications in this Sequence** table and the **Mandatory** column is  as shown below.

Note: The Application Sequence defined for Communication Manager Evolution Server can only contain a single Application.



The screenshot shows the Avaya Aura™ System Manager 6.1 interface. The top navigation bar includes the Avaya logo, the title "Avaya Aura™ System Manager 6.1", and links for "Help | About | Change Password | Log off admin". Below this is a breadcrumb trail: "Home / Elements / Session Manager / Application Configuration / Application Sequences - Application Sequences". The left sidebar contains a menu with options like "Session Manager", "Dashboard", "Session Manager Administration", "Communication Profile Editor", "Network Configuration", "Device and Location Configuration", "Application Configuration", "Applications", "Application Sequences", "Implicit Users", "NRS Proxy Users", "System Status", and "System Tools". The main content area is titled "Application Sequence Editor" and includes "Commit" and "Cancel" buttons. It features a section for "Application Sequence" with input fields for "Name" (containing "DEVCON App Sequence") and "Description". Below this is a section for "Applications in this Sequence" with "Move First", "Move Last", and "Remove" buttons. A table lists the current applications in the sequence:

Sequence Order (first to last)	Name	SIP Entity	Mandatory	Description
1	DEVCON-APP	devcon13	<input checked="" type="checkbox"/>	

Below the table is a "Select : All, None" option. The "Available Applications" section shows a list of applications that can be added to the sequence:

Name	SIP Entity	Description
BR110-APP	BR110-CM	
DEV4.EVO	Dev4 AACM	
DEVCON-APP	devcon13	
SP3-CM-APP	sp3-cm	

At the bottom, there is a "*Required" label and "Commit" and "Cancel" buttons.

6.7 Add SIP User

Add a SIP user for Converge Pro VH20. The following configuration will automatically create the SIP station on Communication Manager Evolution Server.

To add new SIP users, navigate to **Users → User Management → Manage Users** from the left and select **New** button (not shown) on the right.

Enter values for the following required attributes for a new SIP user in the **Identity** tab of the new user form.

- **Last Name:** Enter the last name of the user.
- **First Name:** Enter the first name of the user.
- **Login Name:** Enter <extension>@<sip domain> of the user (e.g., 78305@avaya.com).
- **Authentication Type:** Select *Basic*.
- **Password:** Enter the password which will be used to log into System Manager
- **Confirm Password:** Re-enter the password from above.

The screen below shows the information when adding a new SIP user to the sample configuration.

AVAYA Avaya Aura® System Manager 6.1 [Help](#) | [About](#) | [Change Password](#) | [Log off admin](#)

[User Management](#) * [Home](#)

Home /Users / User Management / Manage Users- New User Profile [Help ?](#)

New User Profile [Commit](#) [Cancel](#)

Identity * **Communication Profile** * **Membership** **Contacts**

Identity ▾

* **Last Name:** 78305

* **First Name:** VH20

Middle Name:

Description:

* **Login Name:** 78305@avaya.com

* **Authentication Type:** Basic ▾

* **Password:** ●●●●●●●●

* **Confirm Password:** ●●●●●●●●

Localized Display Name:

Endpoint Display Name:

Honorific:

Language Preference: English ▾

Time Zone:

Enter values for the following required attributes for a new SIP user in the **Communication Profile** tab of the new user form.

- **Communication Profile Password:** Enter the password which will be used by Converge Pro VH20 to register with Session Manager.
- **Confirm Password:** Re-enter the password from above.

Scroll down to the **Communication Address** section and select **New** to define a **Communication Address** for the new SIP user. Enter values for the following required fields:

- **Type:** Select *Avaya SIP*.
- **Fully Qualified Address:** Enter extension number and select SIP domain.

The screen below shows the information when adding a new SIP user to the sample configuration. Click **Add**.

AVAYA Avaya Aura® System Manager 6.1 [Help](#) | [About](#) | [Change Password](#) | [Log off admin](#)

[User Management](#) × [Home](#)

Home / Users / User Management / Manage Users - New User Profile [Help ?](#)

New User Profile [Commit](#) [Cancel](#)

Communication Profile

Communication Profile Password:

Confirm Password:

[New](#) [Delete](#) [Done](#) [Cancel](#)

Name
Primary
Select : None

* Name:

Default : ☒

Communication Address

[New](#) [Edit](#) [Delete](#)

Type	Handle	Domain
No Records found		

Type:

* Fully Qualified Address: @

[Add](#) [Cancel](#)

In the *Session Manager Profile* section, specify the Session Manager entity from **Section 6.3.1** for **Primary Session Manager** and assign the **Application Sequence** defined in **Section 6.6** to the new SIP user as part of defining the **SIP Communication Profile**. The **Application Sequence** can be used for both the originating and terminating sequence. Set the **Home Location** field to the **Location** configured in **Section 6.2**.

☒ Session Manager Profile

* Primary Session Manager

devcon-asm

Secondary Session Manager

(None)

Origination Application Sequence

DEVCON App Sequence

Termination Application Sequence

DEVCON App Sequence

Survivability Server

(None)

* Home Location

BR-DevConnect

Primary	Secondary	Maximum
13	0	13

Primary	Secondary	Maximum

In the **Endpoint Profile** section, fill in the following fields:

- **System:** Select the managed element corresponding to Communication Manager.
- **Profile Type** Select *Endpoint*.
- **Use Existing Stations:** If field is not selected, the station will automatically be added in Communication Manager.
- **Extension:** Enter extension number of SIP user.
- **Template:** Select template for type of SIP phone.
- **Port:** Enter *IP*.
- **Delete Endpoint on Unassign of Endpoint:** Enable field to automatically delete station when **Endpoint Profile** is un-assigned from user.

The screenshot shows a web-based configuration form for an Endpoint Profile. At the top, there is a section header "Endpoint Profile" with a checkmark icon and a dropdown arrow. Below this, the form contains several fields and options:

- * System:** A dropdown menu with "devcon13-CM-ES" selected.
- * Profile Type:** A dropdown menu with "Endpoint" selected.
- Use Existing Endpoints:** An unchecked checkbox.
- * Extension:** A text input field containing "78305" and a magnifying glass icon. To its right is a button labeled "Endpoint Editor".
- * Template:** A dropdown menu with "DEFAULT_9630SIP_CM_6_0" selected.
- Set Type:** A text input field containing "9630SIP".
- Security Code:** An empty text input field.
- * Port:** A text input field containing "IP" and a magnifying glass icon.
- Voice Mail Number:** An empty text input field.
- Delete Endpoint on Unassign of Endpoint from User or on Delete User:** A checkbox that is checked.

6.8 Add Session Manager

To complete the configuration, adding the Session Manager will provide the linkage between System Manager and Session Manager. Expand the **Session Manager** menu on the left and select **Session Manager Administration**. Click **Add** (not shown), and fill in the fields as described below and shown in the following screen:

Under *Identity*:

- **SIP Entity Name:** Select the name of the SIP Entity added for Session Manager
- **Description:** Descriptive comment (optional)
- **Management Access Point Host Name/IP:** Enter the IP address of the Session Manager management interface.

Under *Security Module*:

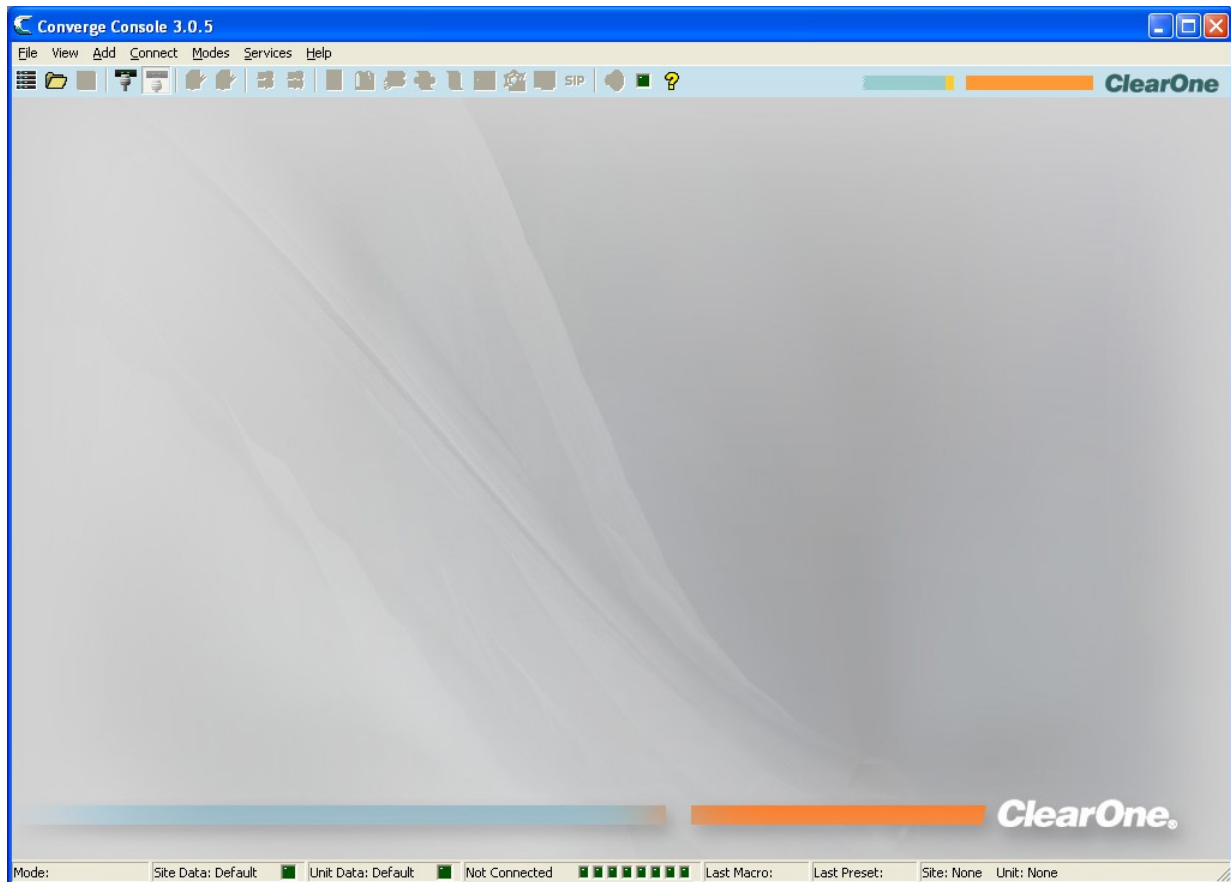
- **Network Mask:** Enter the network mask corresponding to the IP address of Session Manager
- **Default Gateway:** Enter the IP address of the default gateway for Session Manager

Use default values for the remaining fields. Click **Commit** to add this Session Manager.

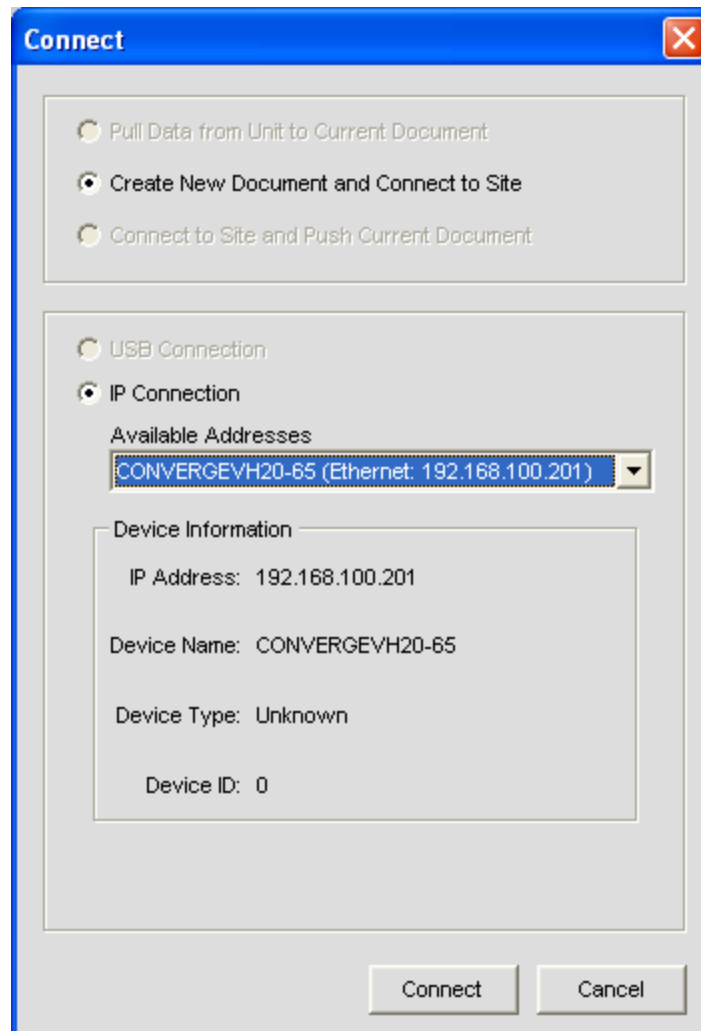
7. Configure ClearOne Converge Pro VH20

The configuration of Converge Pro VH20 was performed via the Converge Console. The Converge Pro VH20 used DHCP to obtain an IP address. Refer to [3] for additional information on configuring Converge Pro VH20.

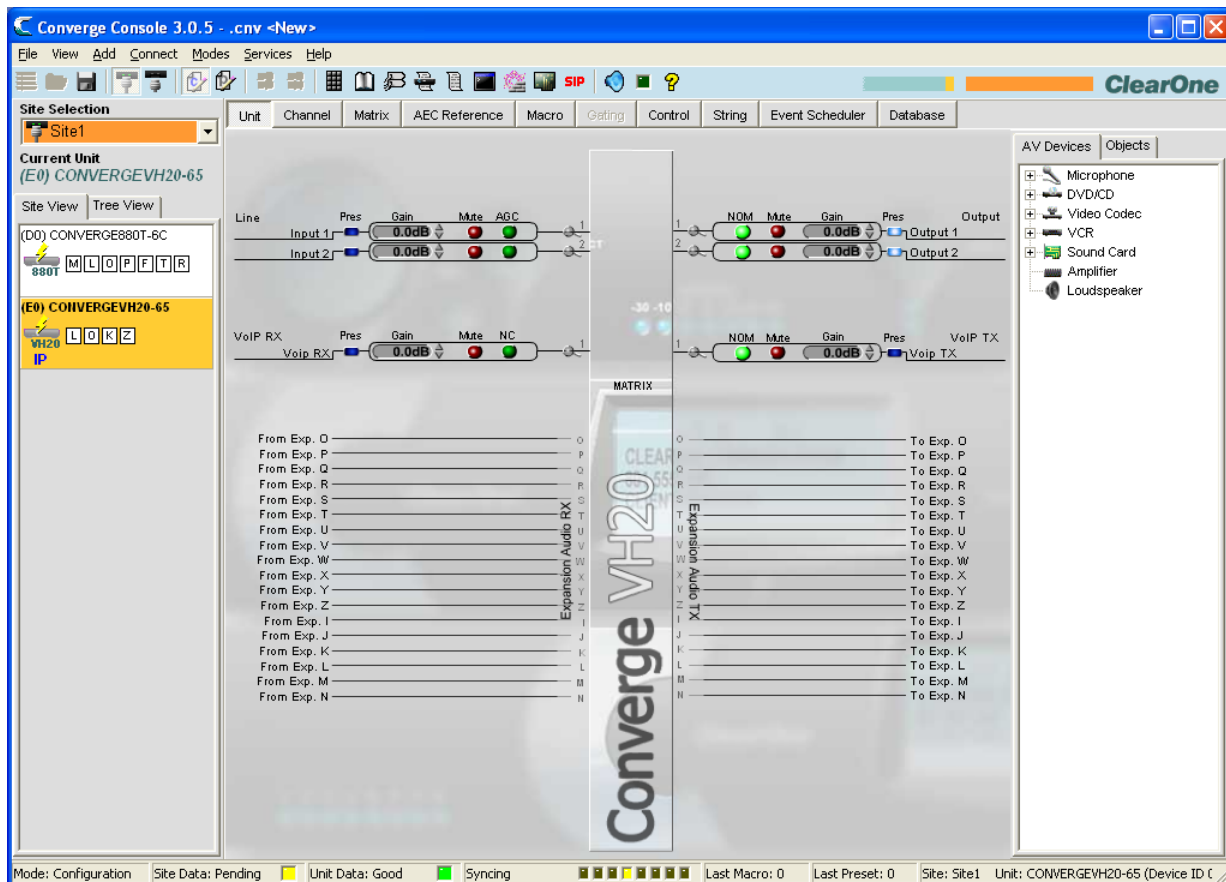
From a PC with the Converge Console installed, launch the application to display the window below.



From the **Converge Console**, select the **Connect** option in the menu bar to display the **Connect** window shown below. Select the **IP Connection** radio button. In the **Available Addresses** field, select the entry for Converge VH20 with the IP address obtained from DHCP. Click the **Connect** button.



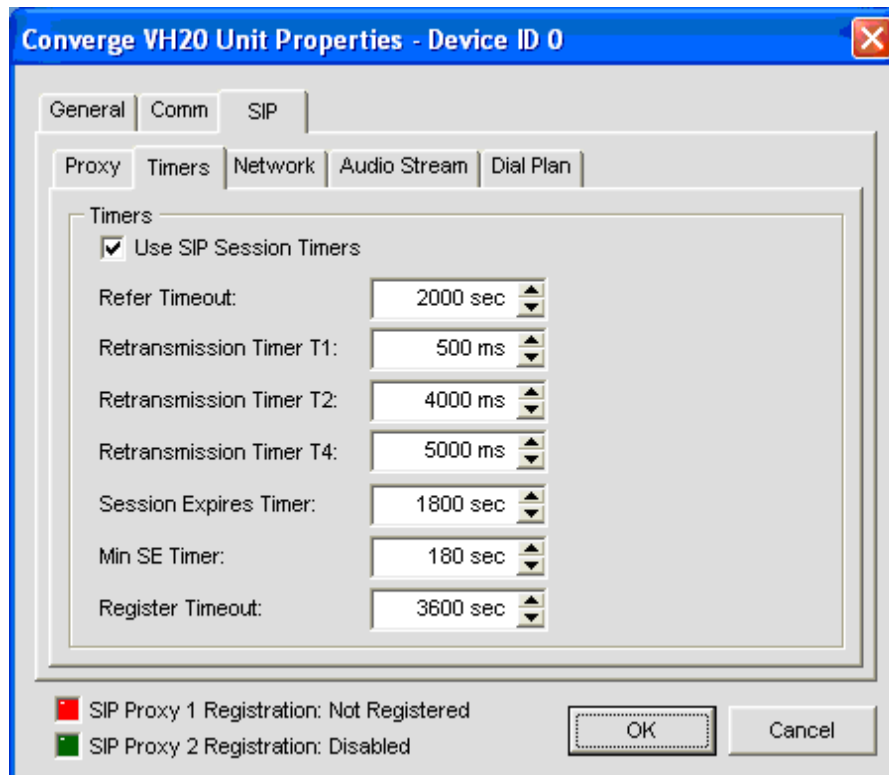
Once the Converge Console is connected to Converge Pro VH20, the following window is displayed. Select the Converge Pro VH20 in the left pane, and then click the **SIP** icon (in red) under the menu bar.



After selecting the SIP option, the **Converge VH20 Unit Properties** window is displayed as shown below. Select the **SIP** tab and configure the SIP parameters as shown below, including the VH20's extension number in the **Local Phone Number** and **Authorization User** fields and its **Authorization Password**. Next, configure the **SIP Domain**, the Proxy IP address/URL (i.e., Session Manager IP address), and the **Proxy Port**. Lastly, configure the **SIP Transport** method.

The screenshot shows the 'Converge VH20 Unit Properties - Device ID 0' window. The 'SIP' tab is selected. Under the 'Proxy' sub-tab, the 'Phone Number' section has 'Local Phone Number' set to 78305 and 'Display Name (Hostname)' set to CONVERGEVH20-65. The 'Proxy 1' section has 'SIP Authentication' checked, with 'Authorization User' set to 78305 and 'Authorization Password' set to 123456. 'SIP Proxy Registration' is also checked, with 'SIP Domain' set to avaya.com, 'Proxy IP Address/URL' set to 10.32.24.235, and 'Proxy Port' set to 5060. The 'Outbound Proxy' section is unchecked. The 'SIP Transport' section has 'UDP' selected with 'Listen Port' 5060, and 'TLS' is also shown with 'Listen Port' 5061. There are fields for 'Private Key', 'Local Cert', and 'CA Certs' with 'Browse...' buttons. An 'Export Certificates...' button is at the bottom. A status bar at the bottom shows 'SIP Proxy 1 Registration: Not Registered' (red square) and 'SIP Proxy 2 Registration: Disabled' (green square). 'OK' and 'Cancel' buttons are at the bottom right.

In the **Timers** tab, set the **Min SE Timer** to *180 sec*. This is required so that it matches the setting in the SIP trunk group in Communication Manager; otherwise, there will be a mismatch, and incoming calls to Converge Pro VH20 will with a status of Min-SE is too small. Alternatively, this timer can be changed in the Communication Manager SIP trunk group to match the setting on Converge Pro VH20.



In the Dial Plan tab, the Dial Plan Domain Name/IP Address was set to the Session Manager IP address and Extension Dialing was set to 5 since 5-digit extensions were being used. Any dialing prefixes can be entered here too.

Converge VH20 Unit Properties - Device ID 0

General Comm SIP

Proxy Timers Network Audio Stream **Dial Plan**

☐ Dial Plan
View... Browse...

☒ Manual Configuration

Dial Plan Domain Name/IP Address: 10.32.24.235

Manual Send Key: #

Total Dial Timer: 2 Minutes

Interdigit Timer: 30 Seconds

First Digit Timer: 30 Seconds

☒ Extension Dialing: 5

☒ Local Dialing Prefix: 9

☒ Long Distance Dialing Prefix: 91

☒ International Dialing Prefix: 9011

☒ Emergency Dialing: 911

☒ Operator Dialing: 0

Number of Digits

	Min:	Max:
Local Dialing Prefix	8	8
Long Distance Dialing Prefix	12	12
International Dialing Prefix	4	4

☒ SIP Proxy 1 Registration: Not Registered

☒ SIP Proxy 2 Registration: Disabled

OK Cancel

There is no configuration required in the **Audio Stream** tab; however, it is shown here to show the **Codec Priority** of Converge Pro VH20. Click **OK**.

The image shows a screenshot of the 'Converge VH20 Unit Properties - Device ID 0' dialog box, specifically the 'Audio Stream' tab. The dialog has a blue title bar with a close button. It contains several tabs: 'General', 'Comm', 'SIP', 'Proxy', 'Timers', 'Network', 'Audio Stream' (selected), and 'Dial Plan'. The 'Audio Stream' tab is divided into several sections: 'RTP/RTCP' with 'RTP Base Port' set to 50000 and 'RTCP Enable' checked; 'QoS' with 'Description/Precedence' set to 'Express Forwarding' and 'Custom/Current DSCP Value' set to 0x28; 'SRTP' with 'Cipher' set to 'AES CTR', 'MAC' set to 'HMAC SHA-1 80', 'KDR Offer' set to 24, and 'SRTCP' set to 'NEGOTIATE'; 'VAD' with 'VAD Noise Matching' set to 'Level'; 'DTMF Relay' with 'Payload' set to 97; and 'Codec Priority' with a list of codecs and up/down arrows. At the bottom, there are status indicators for 'SIP Proxy 1 Registration: Not Registered' and 'SIP Proxy 2 Registration: Disabled', along with 'OK' and 'Cancel' buttons.

Converge VH20 Unit Properties - Device ID 0

General Comm SIP

Proxy Timers Network **Audio Stream** Dial Plan

RTP/RTCP

RTP Base Port: 50000 ☒ RTCP Enable

QoS

Description/Precedence: Express Forwarding

Custom/Current DSCP Value: 0x28 (0x0 - 0x3F)

☐ SRTP

Cipher: AES CTR

MAC: HMAC SHA-1 80

KDR Offer: 24 (0 - 24)

SRTCP: NEGOTIATE

☒ VAD

VAD Noise Matching: ☐ None ☒ Level

☒ DTMF Relay

Payload: 97 (96 - 127)

Codec Priority

G.722 – 64 Kbps
G.722 – 56 Kbps
G.722 – 48 Kbps
G.711 uLaw
G.711 ALaw
G.729AB
G.723.1 6.3 Kbps
G.723.1 5.3 Kbps

Select a codec on the left and press the up/down arrow to change its priority

☒ SIP Proxy 1 Registration: Not Registered
☒ SIP Proxy 2 Registration: Disabled

OK Cancel

8. Verification Steps

This section provides the steps that may be performed to verify proper configuration of the ClearOne ConvergePro VH20 with Avaya Aura® Communication Manager and Avaya Aura® Session Manager.

1. Verify that the ClearOne ConvergePro VH20 has successfully registered with Session Manager. Under **SIP Properties**, verify that the **SIP Proxy 1 Registration** status is *Registered* as shown at the bottom of the screen.

The screenshot shows the 'Converge VH20 Unit Properties - Device ID 0' dialog box with the 'SIP' tab selected. The 'Proxy' sub-tab is also active. The 'Phone Number' section shows 'Local Phone Number' as 78305 and 'Display Name (Hostname)' as CONVERGEVH20-65. The 'Proxy 1' section has 'SIP Authentication' checked with 'Authorization User' 78305 and 'Authorization Password' 123456. 'SIP Proxy Registration' is also checked, with 'SIP Domain' set to 'Domain Name' and 'avaya.com', 'Proxy IP Address/URL' as 10.32.24.235, and 'Proxy Port' as 5060. The 'Outbound Proxy' section is unchecked. The 'SIP Transport' section shows 'UDP' selected with 'Listen Port' 5060, and 'TLS' with 'Listen Port' 5061. There are fields for 'Private Key', 'Local Cert', and 'CA Certs' with 'Browse...' buttons. An 'Export Certificates...' button is at the bottom. The status bar at the bottom shows 'SIP Proxy 1 Registration: Registered' with a green icon and 'SIP Proxy 2 Registration: Disabled' with a red icon. 'OK' and 'Cancel' buttons are at the bottom right.

Converge VH20 Unit Properties - Device ID 0

General Comm SIP

Proxy Timers Network Audio Stream Dial Plan

Phone Number

Local Phone Number: 78305

Display Name (Hostname): CONVERGEVH20-65

Proxy 1 Proxy 2

☒ SIP Authentication

Authorization User: 78305

Authorization Password: 123456

☒ SIP Proxy Registration

SIP Domain: Domain Name avaya.com

Proxy IP Address/URL: 10.32.24.235

Proxy Port: 5060

☐ Outbound Proxy

Proxy IP Address/URL:

Proxy Port: 5060

SIP Transport

☒ UDP Listen Port: 5060 ☐ TCP Listen Port: 5060

☐ TLS Listen Port: 5061

Private Key: Browse...

Local Cert: Browse...

CA Certs

Add... Del

Export Certificates...

SIP Proxy 1 Registration: Registered

SIP Proxy 2 Registration: Disabled

OK Cancel

2. Place an incoming call to the ConvergePro VH20 and verify two-way audio.
3. Place an outgoing voice call from the ConvergePro VH20 to an Avaya IP telephone and verify that the call completes with two-way audio.

9. Conclusion

These Application Notes have described the administration steps required to integrate the ClearOne Converge Pro VH20 with Avaya Aura® Communication Manager and Avaya Aura® Session Manager. ClearOne Converge Pro VH20 successfully registered with Session Manager and voice calls were established successfully. All test cases passed with observations noted in **Section 2.2**.

10. References

This section references the Avaya and ClearOne documentation relevant to these Application Notes. The Avaya product documentation is available at <http://support.avaya.com>.

- [1] *Administering Avaya Aura® Communication Manager*, August 2010, Release 6.0, Issue 6.0, Document Number 03-300509.
- [2] *Administering Avaya Aura® Session Manager*, August 2010, Issue 3, Release 6.0, Document Number 03-603324.
- [3] *ClearOne Converge Pro Installation & Operation Manual*, available at <http://www.clearone.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.