



Avaya Solution & Interoperability Test Lab

Application Notes for Empirix Hammer IP with Avaya Aura® Communication Manager and Avaya Aura® Session Manager using SIP Trunk Emulation – Issue 1.0

Abstract

These Application Notes describe the configuration steps required to integrate the Empirix Hammer IP with Avaya Aura® Communication Manager and Avaya Aura® Session Manager using SIP trunk emulation. Empirix Hammer IP is a test solution for understanding how IP-based systems will behave in the real world. Empirix Hammer IP can be used to assess and monitor network performance, reliability and quality of VoIP services in an Avaya IP telephony network. In this configuration, Empirix Hammer IP emulates SIP trunks that interface to Avaya Aura® Session Manager and originates and terminates calls through Avaya SIP telephony network. While the call is active, Empirix Hammer IP can send DTMF tones and voice media, and provide voice quality metrics. Call progress can also be monitored, and at the completion of the test, test reports can be generated. The Hammer IP provides a collection of applications used to configure the system; create, schedule, and monitor tests; and create reports.

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

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

1 Introduction

These Application Notes describe the configuration steps required to integrate the Empirix Hammer IP with Avaya Aura® Communication Manager and Avaya Aura® Session Manager using SIP trunk emulation. Empirix Hammer IP is a test solution for understanding how IP-based systems will behave in the real world. Empirix Hammer IP can be used to assess and monitor network performance, reliability and quality of VoIP services in an Avaya IP telephony network. In this configuration, Empirix Hammer IP emulates SIP trunks that interface to Avaya Aura® Session Manager and originates and terminates calls through Avaya SIP telephony network. While the call is active, Empirix Hammer IP can send DTMF tones and voice media, and provide voice quality metrics. Call progress can also be monitored, and at the completion of the test, test reports can be generated. Empirix Hammer IP provides a collection of applications used to configure the system; create, schedule, and monitor tests; and create reports.

The following set of Hammer IP applications were used during the compliance testing:

- **Hammer Configurator** used to configure and manage the system.
- **Hammer TestBuilder** used to create and run test scripts.
- **Hammer System Monitor** used to monitor SIP registration status and call progress.
- **Hammer Call Summary Monitor** used to monitor call completion and to create reports.

Below is a list of related Application Notes that describes terminating calls to SIP endpoints, H.323 endpoints, and H.323 trunks.

- *Application Notes for Empirix Hammer IP with Avaya Aura® Communication Manager and Avaya Aura® Session Manager using SIP Endpoint Emulation [3]*
- *Application Notes for Empirix Hammer IP with Avaya Aura® Communication Manager using H.323 Endpoint Emulation [4]*
- *Application Notes for Empirix Hammer IP with Avaya Aura® Communication Manager using H.323 Trunk Emulation [5]*

2 General Test Approach and Test Results

Interoperability compliance testing covered feature and serviceability testing. The feature testing was conducted by originating and terminating calls using SIP trunk channels on Hammer IP and establishing the calls through the Avaya SIP telephony network. The compliance test also covered monitoring various reports on the Hammer IP during and after the test runs, and checking the status of various SIP resources on Communication Manager. The serviceability testing focused on verifying the ability of the Hammer IP to recover from adverse conditions, such as disconnecting the Ethernet cable and rebooting the server.

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.

Avaya recommends our customers implement Avaya solutions using appropriate security and encryption capabilities enabled by our products. The testing referenced in this DevConnect Application Note included the enablement of supported encryption capabilities in the Avaya products. Readers should consult the appropriate Avaya product documentation for further information regarding security and encryption capabilities supported by those Avaya products.

Support for these security and encryption capabilities in any non-Avaya solution component is the responsibility of each individual vendor. Readers should consult the appropriate vendor-supplied product documentation for more information regarding those products.

For the testing associated with this Application Note, the interface between Avaya systems and Empirix Hammer IP did not include use of any specific encryption features as requested by Empirix.

2.1 Interoperability Compliance Testing

The interoperability compliance testing focused on verifying that the Hammer IP can establish a SIP trunk to Session Manager, establish calls, send voice media, and provide voice quality metrics. The following features and functionality were covered:

- Establishing SIP trunks to Session Manager and verifying the exchange of SIP Options messages.
- Originating and terminating calls through Avaya SIP telephony network.
- Support of G.711 mu-law and G.729 codecs.
- Support of direct IP-to-IP media (also known as “Shuffling” which allows IP endpoints to send audio RTP packets directly to each other without using media resources on the Avaya Media Gateway).
- Calls with IP Audio Hairpinning enabled.
- Generating voice quality metrics with Shuffling disabled.
- DTMF support.
- Originating calls from SIP trunks and terminating calls on SIP trunks, SIP endpoints, H.323 endpoints, and H.323 trunks.

Note: Performance and load testing was not the focus of the compliance test.

2.2 Test Results

All test cases passed. Hammer IP was successful in originating calls using SIP trunk emulation and terminating calls on channels emulating SIP trunks, SIP endpoints, H.323 trunks, and H.323 endpoints. The compliance test was completed with the following observations:

- Direct IP-to-IP Media (i.e., Shuffling) using H.323 trunks between Communication Manager and Hammer IP is not supported. However, Shuffling with H.323 endpoints and SIP endpoints/trunks is supported.

- IP Audio Hairpinning with H.323 trunks is not supported. However, IP Audio Hairpinning with H.323 endpoints and SIP endpoints/trunks is supported.
- When a call scenario originates from a H.323 trunk and terminates on a SIP endpoint/trunk, and uses the Media Server for media processing, the SDP payload type must match between Communication Manager and Hammer IP. The payload type may be configured in the SIP trunk group on Communication Manager or the Media Profile on Hammer IP.
- Communication Manager does not shuffle calls between a SIP trunk and a H.323 trunk. This is per design. If the originating endpoint on the Hammer IP is a SIP endpoint, note that the call arrives on Communication Manager via a SIP trunk. Therefore, a call from a SIP endpoint to a H.323 trunk is essentially a call from a SIP trunk to a H.323 trunk and the call is not shuffled.

Important Note: The purpose of this compliance test was to verify interoperability between Hammer IP and Communication Manager and Session Manager using SIP trunk emulation. That is, the goal was to verify that Hammer IP establish a SIP trunk to Session Manager and establish calls. This was successfully verified. If a Hammer test encounters failed calls, there are various items to consider, including:

- The **Guard Time** and **Stagger** parameters may be set too aggressively (e.g., Hammer IP may be initiating too many calls too quickly) and the configuration under test may not be able to handle the load generated by Hammer IP. These parameters should be considered carefully for each test. It may be necessary to slow down the test to a rate that can be reasonably handled by the test configuration.
- Resources may be getting exhausted in the Avaya Media Gateway. These resources may include media processing resources, touch-tone receivers (TTRs), network trunks, and TDM bus resources.
- The pause duration in a test script may need to be adjusted to synchronize the A and B sides.

Generally speaking, call failures encountered in Hammer IP are usually a result of one of the issues mentioned above.

2.3 Support

Technical support on the Empirix Hammer IP can be obtained via phone, website, or email.

- **Phone:** (978) 313-7002
- **Web:** <https://www.empirix.com/support/maintenance/>
- **Email:** supportcontract@empirix.com

3 Reference Configuration

The network diagram below illustrates the test configuration. In this configuration, Session Manager receives calls from the Hammer IP, which emulates SIP trunks. The call is routed through the Avaya SIP telephony network. The call is eventually routed back to the Hammer IP where it is terminated. While the call is established, the Hammer IP sends voice media (i.e., RTP traffic) using an audio recording. This allows voice quality metrics to be provided at the end of each call. The Hammer IP applications running on the Hammer IP server were used to configure the system, create and monitor the tests, and view the test reports.

Note: When testing IP Audio Hairpinning, an Avaya G650 Media Gateway with a Media Processor (TN2302AP) was required, but not shown in the diagram below.

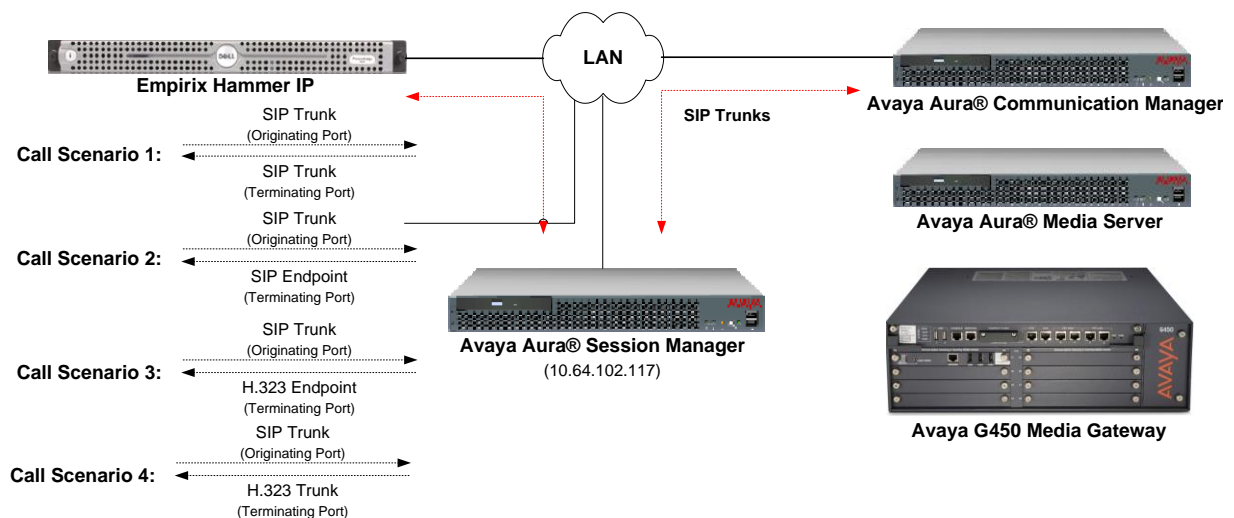


Figure 1: Empirix Hammer IP with Avaya SIP Telephony Network

4 Equipment and Software Validated

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

Equipment	Software
Avaya Aura® Communication Manager	7.1.3 FP3 (R017x.01.0.532.0 with Patch 24515)
Avaya G450 Media Gateway	FW 38.21.1
Avaya G650 Media Gateway with <ul style="list-style-type: none">Media Processor TN2302APCLAN TN799DP	HW12 FW121 HW01 FW044
Avaya Aura® Media Server	v.7.8.0.393
Avaya Aura® Session Manager	7.1.3.0.713014
Avaya Aura® System Manager	7.1.3 Build No. – 7.1.0.0.1125193 Software Update Revision No: 7.1.3.0.037763 Feature Pack 3
Empirix Hammer IP running on Microsoft Windows Server 2012 R2 Standard with 2.93 GHz (4 processors) Intel Xeon CPU and 4.0 GB of RAM on VMware	7.1.0.37

5 Configure Avaya Aura® Communication Manager

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

- Administer IP Node Names
- Administer IP Codec Set
- Administer IP Network Region
- Administer SIP Trunk Group to Session Manager
- Administer AAR Call Routing

Communication Manager is configured through the System Access Terminal (SAT).

5.1 Administer IP Node Names

In the **IP Node Names** form, assign an IP address and host name for Communication Manager (*procr*) and Session Manager (*devcon-sm*). The host names will be used in other configuration screens of Communication Manager.

change node-names ip		Page 1 of 2
		IP NODE NAMES
Name	IP Address	
HammerIP-Orig	10.64.102.171	
HammerIP-Term	10.64.102.181	
default	0.0.0.0	
devcon-aes	10.64.102.119	
devcon-ams	10.64.102.118	
devcon-sm	10.64.102.117	
procr	10.64.102.115	
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		

5.2 Administer IP Codec Set

In the **IP Codec Set** form, specify the audio codec(s) required by the test that will be run on the Hammer IP. The form is accessed via the **change ip-codec-set 1** command. Note the codec set number since it will be used in the IP Network Region covered in the next section. For the compliance test, G.711 mu-law, G.729AB, and G.729A codecs were used. In the **IP Codec Set** form, specify the appropriate codec being used by the Hammer test. Below is the IP codec set configured for G.711mu-law.

```
change ip-codec-set 1                                     Page 1 of 2

                                IP Codec Set

Codec Set: 1

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

5.3 Administer IP Network Region

In the **IP Network Region** form, specify the codec set to be used for Hammer calls and specify whether **IP-IP Direct Audio** (Shuffling) is required for the test. Shuffling allows audio traffic to be sent directly between IP endpoints without using media resources in the Avaya G450 Media Gateway or Media Server. Note that if Shuffling is enabled, audio traffic does not egress the Hammer IP since the calls would be shuffled. The **Authoritative Domain** for this configuration is *avaya.com*.

```
change ip-network-region 1                               Page 1 of 20

                                IP NETWORK REGION

Region: 1      NR Group: 1
Location: 1    Authoritative Domain: avaya.com
Name:          Stub Network Region: n
MEDIA PARAMETERS      Intra-region IP-IP Direct Audio: no
                      Inter-region IP-IP Direct Audio: no
                      IP Audio Hairpinning? n
Codec Set: 1
UDP Port Min: 2048
UDP Port Max: 50999
DIFFSERV/TOS PARAMETERS
Call Control PHB Value: 46
Audio PHB Value: 46
Video PHB Value: 26
802.1P/Q PARAMETERS
Call Control 802.1p Priority: 6
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
```


5.4 Administer SIP Trunk to Session Manager

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*.
- The **Transport Method** field was set to *tls*.
- Specify the Communication Manager (*procr*) 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 are taken from the **IP Node Names** form.
- Ensure that the TLS port value of *5061* 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 **Direct IP-IP Audio Connections** field was enabled on this form.
- The **DTMF over IP** field should be set to the default value of *rtp-payload*.
- Enable **IP Audio Hairpinning**, if required.
- Disable **Initial IP-IP Direct Media**.

Communication Manager supports DTMF transmission using RFC 2833. The default values for the other fields may be used.

add signaling-group 10		Page 1 of 2
SIGNALING GROUP		
Group Number: 10	Group Type: sip	
IMS Enabled? n	Transport Method: tls	
Q-SIP? n		
IP Video? n	Enforce SIPS URI for SRTP? n	
Peer Detection Enabled? y	Peer Server: SM	
Prepend '+' to Outgoing Calling/Alerting/Diverting/Connected Public Numbers? y		
Remove '+' from Incoming Called/Calling/Alerting/Diverting/Connected Numbers? n		
Alert Incoming SIP Crisis Calls? n		
Near-end Node Name: procr		Far-end Node Name: devcon-sm
Near-end Listen Port: 5061		Far-end Listen Port: 5061
		Far-end Network Region: 1
Far-end Domain: avaya.com		
Incoming Dialog Loopbacks: eliminate		Bypass If IP Threshold Exceeded? n
DTMF over IP: rtp-payload		RFC 3389 Comfort Noise? n
Session Establishment Timer(min): 3		Direct IP-IP Audio Connections? y
Enable Layer 3 Test? y		IP Audio Hairpinning? n
H.323 Station Outgoing Direct Media? n		Initial IP-IP Direct Media? n
		Alternate Route Timer(sec): 6

Configure the **Trunk Group** form as shown below. This trunk group is used for SIP calls to Hammer IP. 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 10		Page 1 of 22	
TRUNK GROUP			
Group Number: 10	Group Type: sip	CDR Reports: y	
Group Name: To devcon-sm	COR: 1	TN: 1	TAC: 1010
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: 10		
	Number of Members: 40		

5.5 AAR Call Routing

SIP calls to Session Manager are routed over a SIP trunk via AAR call routing. Configure the AAR analysis form and enter add an entry that routes digits beginning with “78” to route pattern 10 as shown below. Note that the digits arriving from Hammer IP for incoming call requests will start with ‘8’, the AAR feature access code. The AAR feature access code will steer the call to AAR routing.

change aar analysis 78							Page 1 of 2
AAR DIGIT ANALYSIS TABLE							
Location: all							Percent Full: 1
Dialed String	Total Min	Total Max	Route Pattern	Call Type	Node Num	ANI Reqd	
78	5	5	10	lev0		n	

Configure a preference in Route Pattern 10 to route calls over SIP trunk group 10 as shown below.

change route-pattern 10										Page 1 of 3		
Pattern Number: 10										Pattern Name: To devcon-sm		
SCCAN? n		Secure SIP? n		Used for SIP stations? n								
Grp No	FRL	NPA	Pfx	Hop	Toll	No.	Inserted	DCS/	IXC			
			Mrk	Lmt	List	Del	Digits	QSIG				
							Dgts	Intw				
1:	10	0						n	user			
2:								n	user			
3:								n	user			
4:								n	user			
5:								n	user			
6:								n	user			
	BCC VALUE		TSC	CA-TSC		ITC BCIE		Service/Feature	PARM	Sub	Numbering	LAR
	0	1	2	M	4	W	Request			Dgts	Format	
1:	y	y	y	y	y	n	n	rest			unk-unk	none
2:	y	y	y	y	y	n	n	rest				none
3:	y	y	y	y	y	n	n	rest				none
4:	y	y	y	y	y	n	n	rest				none
5:	y	y	y	y	y	n	n	rest				none

6 Configure Avaya Aura® 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
- Routing Policies
- Dial Patterns
- Session Manager, corresponding to the Session Manager Server to be managed by System Manager

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.

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 on the right (not shown). The following screen will then be shown. Fill in the following:

- **Name:** The authoritative domain name (e.g., *avaya.com*).
- **Type:** Set to *sip*.
- **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 7.1 web interface. The top navigation bar includes the Avaya logo, the text 'Aura System Manager 7.1', and a user status area showing 'Last Logged on at July 23, 2018 11:05 AM' with a 'Log off admin' link. The main content area is titled 'Domain Management' and features a left-hand sidebar with a tree view containing 'Routing', 'Domains', 'Locations', 'Adaptations', 'SIP Entities', 'Entity Links', 'Time Ranges', 'Routing Policies', 'Dial Patterns', 'Regular Expressions', and 'Defaults'. The 'Domains' item is selected. The main panel displays a table with one item, 'avaya.com', with a type of 'sip'. The table has columns for 'Name', 'Type', and 'Notes'. At the bottom of the panel are 'Commit' and 'Cancel' buttons. A 'Filter: Enable' link is also visible.

Name	Type	Notes
* avaya.com	sip	

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).

The screen below shows addition of the *Thornton* location, which includes Communication Manager and Session Manager.

AVAYA
Aura® System Manager 7.1

Last Logged on at July 23, 2018 11:05 AM
Go... Log off admin

Home Routing

Home / Elements / Routing / Locations

Location Details Commit Cancel

Help ?

General

* Name: Thornton

Notes:

Dial Plan Transparency in Survivable Mode

Enabled: ☐

Listed Directory Number:

Associated CM SIP Entity:

Under *Location Pattern*:

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

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

Location Pattern

Add Remove

1 Item Filter: Enable

IP Address Pattern	Notes
<input type="checkbox"/> * 10.64.102.*	

Select : All, None

Commit Cancel

6.3 Add SIP Entities

In the sample configuration, a SIP Entity is added for Session Manager, Communication Manager, and Hammer IP.

6.3.1 Avaya Aura® 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 one of the locations defined previously.
- **Time Zone:** Time zone for this location.

The screenshot displays the Avaya Aura System Manager 7.1 web interface. The top header shows the Avaya logo and 'Aura System Manager 7.1'. The right side of the header indicates 'Last Logged on at July 23, 2018 11:05 AM' and includes a 'Log off admin' button. The main navigation menu on the left lists various configuration areas: Routing, Domains, Locations, Adaptations, SIP Entities (highlighted), Entity Links, Time Ranges, Routing Policies, Dial Patterns, Regular Expressions, and Defaults. The breadcrumb trail at the top of the content area reads 'Home / Elements / Routing / SIP Entities'. The main content area is titled 'SIP Entity Details' and includes 'Commit' and 'Cancel' buttons. Under the 'General' tab, the form contains the following fields: 'Name' (text input with value 'devcon-sm'), 'FQDN or IP Address' (text input with value '10.64.102.117'), 'Type' (dropdown menu with 'Session Manager' selected), 'Notes' (text area), 'Location' (dropdown menu with 'Thornton' selected), 'Outbound Proxy' (dropdown menu), 'Time Zone' (dropdown menu with 'America/New_York' selected), 'Minimum TLS Version' (dropdown menu with 'Use Global Setting' selected), and 'Credential name' (text input).

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

- **Listen Ports:** 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** (not shown) to save the SIP Entity definition.

Listen Ports

Add Remove

3 Items Filter: Enable

<input type="checkbox"/>	Listen Ports	Protocol	Default Domain	Endpoint	Notes
<input type="checkbox"/>	5060	TCP	avaya.com	<input checked="" type="checkbox"/>	
<input type="checkbox"/>	5060	UDP	avaya.com	<input checked="" type="checkbox"/>	
<input type="checkbox"/>	5061	TLS	avaya.com	<input checked="" type="checkbox"/>	

Select : All, None

6.3.2 Avaya Aura® 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 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., Communication Manager (*procr*)) on the telephony system.
- **Type:** Select *CM*.
- **Location:** Select one of the locations defined previously.
- **Time Zone:** Time zone for this location.

Under *Loop Detection*:

- **Loop Detection Mode:** Disable this option or set the *Loop Count Threshold* to the number of simultaneous calls being established by Hammer IP, when enabled.

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

The screenshot shows the Avaya Aura System Manager 7.1 interface. The top header displays the Avaya logo and 'Aura® System Manager 7.1'. The right header shows 'Last Logged on at July 27, 2018 11:24 AM' and a 'Log off admin' button. The main navigation pane on the left includes 'Home', 'Routing', 'Domains', 'Locations', 'Adaptations', 'SIP Entities' (selected), 'Entity Links', 'Time Ranges', 'Routing Policies', 'Dial Patterns', 'Regular Expressions', and 'Defaults'. The breadcrumb trail is 'Home / Elements / Routing / SIP Entities'. The main content area is titled 'SIP Entity Details' and contains two tabs: 'General' and 'Loop Detection'. The 'General' tab is active, showing the following fields: 'Name' (devcon-cm), 'FQDN or IP Address' (10.64.102.115), 'Type' (CM), 'Notes' (empty), 'Adaptation' (empty), 'Location' (Thornton), 'Time Zone' (America/New_York), 'SIP Timer B/F (in seconds)' (4), 'Minimum TLS Version' (Use Global Setting), 'Credential name' (empty), 'Securable' (checkbox), and 'Call Detail Recording' (none). The 'Loop Detection' tab is also visible, showing 'Loop Detection Mode' (Off). At the top right of the form are 'Commit' and 'Cancel' buttons, and a 'Help ?' link.

6.3.3 Empirix Hammer IP

Two SIP Entities must be added for Hammer IP, one for originating calls and another one for terminating calls. 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., *HammerIP-Orig*) of the originating channel on Hammer IP.
- **Type:** Select *SIP Trunk*.
- **Location:** Select the location defined previously.
- **Time Zone:** Time zone for this location.

Under *Loop Detection*:

- **Loop Detection Mode:** Disable this option or set the *Loop Count Threshold* to the number of simultaneous calls being established by Hammer IP, when enabled.

The following SIP Entity is for originating call requests from Hammer IP.

The screenshot displays the Avaya Aura System Manager 7.1 web interface. The left sidebar shows a navigation menu with 'SIP Entities' selected. The main content area is titled 'SIP Entity Details' and shows the 'General' tab. The form contains the following fields and values:

- Name:** HammerIP-Orig
- FQDN or IP Address:** 10.64.102.171
- Type:** SIP Trunk
- Notes:** (empty)
- Adaptation:** (empty)
- Location:** Thornton
- Time Zone:** America/New_York
- SIP Timer B/F (in seconds):** 4
- Minimum TLS Version:** Use Global Setting
- Credential name:** (empty)
- Securable:** ☐
- Call Detail Recording:** egress
- Loop Detection Mode:** Off

Buttons for 'Commit' and 'Cancel' are visible at the top right of the form area. A 'Help ?' link is also present.

The following SIP Entity is for terminating calls on Hammer IP.

The screenshot displays the Avaya Aura System Manager 7.1 web interface. The top header shows the Avaya logo and 'Aura System Manager 7.1'. The user is logged in as 'admin' and the session expires at 'Last Logged on at July 26, 2018 11:22 AM'. The breadcrumb trail is 'Home / Elements / Routing / SIP Entities'. The left sidebar contains a navigation menu with 'Routing' expanded, showing sub-items: Domains, Locations, Adaptations, SIP Entities (selected), Entity Links, Time Ranges, Routing Policies, Dial Patterns, Regular Expressions, and Defaults. The main content area is titled 'SIP Entity Details' with 'Commit' and 'Cancel' buttons. The 'General' tab is active, showing the following fields: Name (HammerIP-Term), FQDN or IP Address (10.64.102.181), Type (SIP Trunk), Notes (empty), Adaptation (empty), Location (Thornton), Time Zone (America/New_York), SIP Timer B/F (in seconds) (4), Minimum TLS Version (Use Global Setting), Credential name (empty), Securable (unchecked), Call Detail Recording (egress), and Loop Detection Mode (Off).

AVAYA
Aura System Manager 7.1

Last Logged on at July 26, 2018 11:22 AM
GO... Log off admin

Home Routing

Home / Elements / Routing / SIP Entities

SIP Entity Details Commit Cancel

Help ?

General

* Name: HammerIP-Term

* FQDN or IP Address: 10.64.102.181

Type: SIP Trunk

Notes:

Adaptation:

Location: Thornton

Time Zone: America/New_York

* SIP Timer B/F (in seconds): 4

Minimum TLS Version: Use Global Setting

Credential name:

Securable: ☐

Call Detail Recording: egress

Loop Detection

Loop Detection Mode: Off

6.4 Add Entity Links

This section covers the configuration of Entity Links for Communication Manager and Hammer IP.

6.4.1 Communication Manager 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., *devcon-cm 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.
- **Connection Policy:** Select *trusted*. *Note: If trusted is not selected, calls from the associated SIP Entity specified in Section 6.3.2 will be denied.*

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

The following Entity Link is between Session Manager and Communication Manager.

The screenshot shows the Avaya Aura System Manager 7.1 interface. The left sidebar contains a navigation menu with options: Home, Routing, Domains, Locations, Adaptations, SIP Entities, Entity Links, Time Ranges, Routing Policies, Dial Patterns, Regular Expressions, and Defaults. The main content area is titled 'Entity Links' and shows a table with 6 items. The table has columns: Name, SIP Entity 1, Protocol, Port, SIP Entity 2, Port, DNS Override, Connection Policy, Deny New Service, and Notes. The row for 'devcon-cm link' is highlighted with a red box. The 'devcon-cm link' row shows SIP Entity 1 as 'devcon-sm', Protocol as 'TLS', Port as '5061', SIP Entity 2 as 'devcon-cm', Port as '5061', DNS Override as 'No', Connection Policy as 'trusted', and Deny New Service as 'No'.

Name	SIP Entity 1	Protocol	Port	SIP Entity 2	Port	DNS Override	Connection Policy	Deny New Service	Notes
devcon-aam Link	devcon-sm	TLS	5061	devcon-aam	5061	<input type="checkbox"/>	trusted	<input type="checkbox"/>	
devcon-cm link	devcon-sm	TLS	5061	devcon-cm	5061	<input type="checkbox"/>	trusted	<input type="checkbox"/>	
devcon-ipose Link	devcon-sm	UDP	5060	devcon-ipose	5060	<input type="checkbox"/>	trusted	<input type="checkbox"/>	
HammerIP-Orig	devcon-sm	UDP	5060	HammerIP-Orig	5060	<input type="checkbox"/>	trusted	<input type="checkbox"/>	
HammerIP-Term	devcon-sm	UDP	5060	HammerIP-Term	5060	<input type="checkbox"/>	trusted	<input type="checkbox"/>	

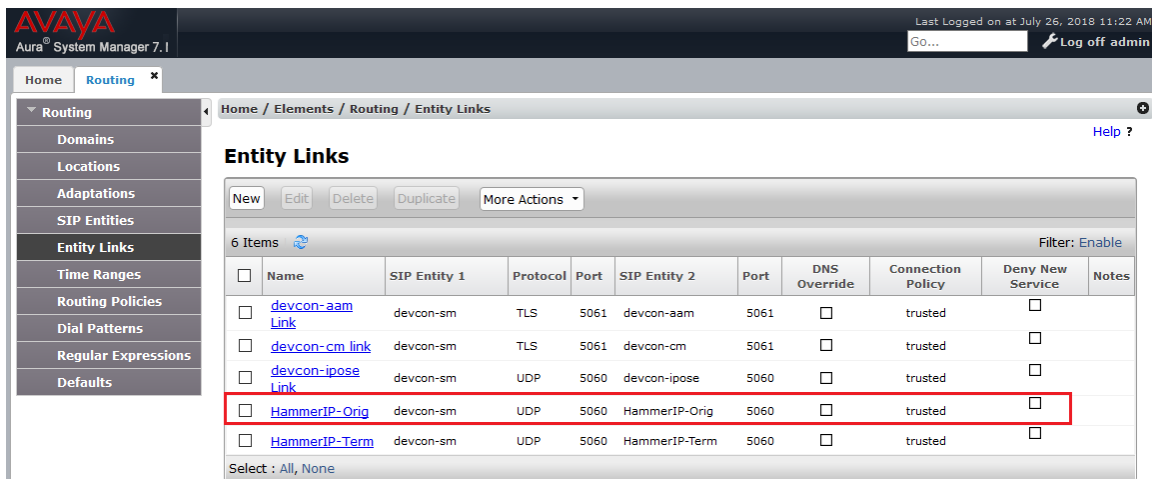
6.4.2 Hammer IP Entity Links

The SIP trunk from Session Manager to Hammer IP is described by an Entity link. Two entity links are required for Hammer IP, one for originating calls on Hammer IP and another one for terminating calls on Hammer IP. 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., *HammerIP-Orig* or *HammerIP-Term*).
- **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 *HammerIP-Orig* or *HammerIP-Term* SIP entity.
- **Port:** Port number on which the other system receives SIP requests.
- **Connection Policy:** Selected *trusted*. *Note: If the link is not trusted, calls from the associated SIP Entity specified in Section 6.3.3 will be denied.*

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

The following Entity Link is between Session Manager and the SIP Entity that handles call origination from Hammer IP (i.e., *HammerIP-Orig*).



The screenshot shows the Avaya Aura System Manager 7.1 interface. The left sidebar contains a navigation menu with options: Home, Routing, Domains, Locations, Adaptations, SIP Entities, Entity Links (selected), Time Ranges, Routing Policies, Dial Patterns, Regular Expressions, and Defaults. The main content area is titled 'Entity Links' and shows a table with 6 items. The table has columns: Name, SIP Entity 1, Protocol, Port, SIP Entity 2, Port, DNS Override, Connection Policy, Deny New Service, and Notes. The 'HammerIP-Orig' link is highlighted with a red box.

	Name	SIP Entity 1	Protocol	Port	SIP Entity 2	Port	DNS Override	Connection Policy	Deny New Service	Notes
<input type="checkbox"/>	devcon-aam Link	devcon-sm	TLS	5061	devcon-aam	5061	<input type="checkbox"/>	trusted	<input type="checkbox"/>	
<input type="checkbox"/>	devcon-cm link	devcon-sm	TLS	5061	devcon-cm	5061	<input type="checkbox"/>	trusted	<input type="checkbox"/>	
<input type="checkbox"/>	devcon-ipose Link	devcon-sm	UDP	5060	devcon-ipose	5060	<input type="checkbox"/>	trusted	<input type="checkbox"/>	
<input type="checkbox"/>	HammerIP-Orig	devcon-sm	UDP	5060	HammerIP-Orig	5060	<input type="checkbox"/>	trusted	<input type="checkbox"/>	
<input type="checkbox"/>	HammerIP-Term	devcon-sm	UDP	5060	HammerIP-Term	5060	<input type="checkbox"/>	trusted	<input type="checkbox"/>	

Select : All, None

The following Entity Link is between Session Manager and the SIP Entity that handles call termination on Hammer IP (i.e., *HammerIP-Term*).

The screenshot shows the Avaya Aura System Manager 7.1 interface. The left sidebar contains a navigation menu with the following items: Home, Routing, Domains, Locations, Adaptations, SIP Entities, Entity Links (selected), Time Ranges, Routing Policies, Dial Patterns, Regular Expressions, and Defaults. The main content area is titled 'Entity Links' and shows a table of 6 items. The table has the following columns: Name, SIP Entity 1, Protocol, Port, SIP Entity 2, Port, DNS Override, Connection Policy, Deny New Service, and Notes. The 'HammerIP-Term' link is highlighted in red.

	Name	SIP Entity 1	Protocol	Port	SIP Entity 2	Port	DNS Override	Connection Policy	Deny New Service	Notes
<input type="checkbox"/>	devcon-aam Link	devcon-sm	TLS	5061	devcon-aam	5061	<input type="checkbox"/>	trusted	<input type="checkbox"/>	
<input type="checkbox"/>	devcon-cm link	devcon-sm	TLS	5061	devcon-cm	5061	<input type="checkbox"/>	trusted	<input type="checkbox"/>	
<input type="checkbox"/>	devcon-ipose Link	devcon-sm	UDP	5060	devcon-ipose	5060	<input type="checkbox"/>	trusted	<input type="checkbox"/>	
<input type="checkbox"/>	HammerIP-Orig	devcon-sm	UDP	5060	HammerIP-Orig	5060	<input type="checkbox"/>	trusted	<input type="checkbox"/>	
<input type="checkbox"/>	HammerIP-Term	devcon-sm	UDP	5060	HammerIP-Term	5060	<input type="checkbox"/>	trusted	<input type="checkbox"/>	

Select : All, None

6.5 Add Routing Policies

Routing policies describe the conditions under which calls will be routed to the SIP Entities specified in **Section 6.3**. Two routing policies were added – one for Communication Manager and one for Hammer IP. To add a routing policy, select **Routing Policies** 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*:

Enter a descriptive name in **Name**.

Under *SIP Entity as Destination*:

Click **Select**, and then select the appropriate SIP entity to which this routing policy applies.

Defaults can be used for the remaining fields. Click **Commit** to save each Routing Policy definition. The following screen shows the Routing Policy for Communication Manager.

The screenshot shows the Avaya Aura System Manager 7.1 interface. The left sidebar contains a navigation menu with the following items: Routing, Domains, Locations, Adaptations, SIP Entities, Entity Links, Time Ranges, Routing Policies (highlighted), Dial Patterns, Regular Expressions, and Defaults. The main content area is titled 'Routing Policy Details' and includes a breadcrumb trail: 'Home / Elements / Routing / Routing Policies'. There are 'Commit' and 'Cancel' buttons in the top right corner of the main area. The 'General' tab is active, showing the following fields: 'Name' (devcon-cm Policy), 'Disabled' (checkbox), 'Retries' (0), and 'Notes' (empty). Below the 'General' tab is the 'SIP Entity as Destination' section, which includes a 'Select' button and a table with the following data:

Name	FQDN or IP Address	Type	Notes
devcon-cm	10.64.102.115	CM	

The following screen shows the Routing Policy for Hammer IP.

The screenshot displays the Avaya Aura System Manager 7.1 web interface. The top header shows the Avaya logo and 'Aura System Manager 7.1'. The right side of the header indicates 'Last Logged on at July 26, 2018 11:22 AM' and includes a 'Log off admin' button. The left sidebar contains a navigation menu with options: Home, Routing, Domains, Locations, Adaptations, SIP Entities, Entity Links, Time Ranges, Routing Policies (selected), Dial Patterns, Regular Expressions, and Defaults. The main content area is titled 'Routing Policy Details' and includes 'Commit' and 'Cancel' buttons. The 'General' tab is active, showing fields for 'Name' (Hammer IP Policy), 'Disabled' (checkbox), 'Retries' (0), and 'Notes'. Below this is the 'SIP Entity as Destination' section, which includes a 'Select' button and a table with the following data:

Name	FQDN or IP Address	Type	Notes
HammerIP-Term	10.64.102.181	SIP Trunk	

6.6 Add Dial Patterns

Dial patterns must be defined to direct calls to the appropriate SIP Entity. In the sample configuration, a 6-digit number beginning with '8' followed by "78600" will be routed to Communication Manager. The '8' is the AAR access code and "78600" are the digits routed to the Hammer IP, which will terminate on a SIP trunk. To add a dial pattern, select **Dial Patterns** on the left and click on the **New** button (not shown) on the right. Fill in the following:

Under *General*:

- **Pattern:** Dialed number or prefix.
- **Min** Minimum length of dialed number.
- **Max** Maximum length of dialed number.
- **SIP Domain** SIP domain of dial pattern.
- **Notes** Comment on purpose of dial pattern (optional).

Under *Originating Locations and Routing Policies*:

Click **Add**, and then select the appropriate location and routing policy from the list.

Default values can be used for the remaining fields. Click **Commit** to save this dial pattern. The following screen shows the dial pattern definition for Communication Manager. Based on these digits, Communication Manager will route the call to Hammer IP via a SIP trunk.

Avaya Aura System Manager 7.1

Home / Elements / Routing / Dial Patterns

Dial Pattern Details

Commit Cancel

Help ?

General

* Pattern: 878600

* Min: 6

* Max: 6

Emergency Call: ☐

Emergency Priority: 1

Emergency Type:

SIP Domain: -ALL-

Notes: CM to Hammer IP SIP Trk

Originating Locations and Routing Policies

Add Remove

1 Item

<input type="checkbox"/>	Originating Location Name	Originating Location Notes	Routing Policy Name	Rank	Routing Policy Disabled	Routing Policy Destination	Routing Policy Notes
<input type="checkbox"/>	Thornton		devcon-cm Policy	0	<input type="checkbox"/>	devcon-cm	

Select : All, None

The following screen shows the dial pattern definition for Hammer IP. The extension, 78600, will be routed to Hammer IP. Note that “78600” does not have to match any configuration on Hammer IP. Hammer IP will answer any calls routed to it regardless of the digits.

Avaya Aura System Manager 7.1

Last Logged on at July 26, 2018 11:22 AM

Home / Elements / Routing / Dial Patterns

Dial Pattern Details [Commit] [Cancel] [Help ?]

General

* Pattern: 78600

* Min: 5

* Max: 5

Emergency Call: ☐

Emergency Priority: 1

Emergency Type:

SIP Domain: -ALL-

Notes: Hammer IP

Originating Locations and Routing Policies

[Add] [Remove]

1 Item [Filter: Enable]

	Originating Location Name	Originating Location Notes	Routing Policy Name	Rank	Routing Policy Disabled	Routing Policy Destination	Routing Policy Notes
<input type="checkbox"/>	Thornton		Hammer IP Policy	0	<input type="checkbox"/>	HammerIP-Term	

Select : All, None

6.7 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**. Then 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.

AVAYA
Aura® System Manager 7.1

Last Logged on at July 26, 2018 11:22 AM
Go... Log off admin

Home Session Manager

Home / Elements / Session Manager / Session Manager Administration

Edit Session Manager [Commit] [Cancel]

General | Security Module | Monitoring | CDR | Personal Profile Manager (PPM) - Connection Settings | Event Server |
Expand All | Collapse All

General

SIP Entity Name devcon-sm

Description

*Management Access Point Host Name/IP 10.64.102.116

*Direct Routing to Endpoints Enable

Data Center None

Avaya Aura Device Services Server Pairing None

Maintenance Mode ☐

Security Module

SIP Entity IP Address 10.64.102.117

*Network Mask 255.255.255.0

*Default Gateway 10.64.102.1

*Call Control PHB 46

*SIP Firewall Configuration SM 6.3.8.0

The following screen shows the **Monitoring** section, which determines how frequently Session Manager sends SIP Options messages to Hammer IP. Use default values for the remaining fields. Click **Commit** to add this Session Manager. In the following configuration, Session Manager sends a SIP Options message every 900 secs. If there is no response, Session Manager will send a SIP Options message every 120 secs.

Monitoring ▾

Enable Monitoring ☒

*Proactive cycle time (secs)

900

*Reactive cycle time (secs)

120

*Number of Retries

1

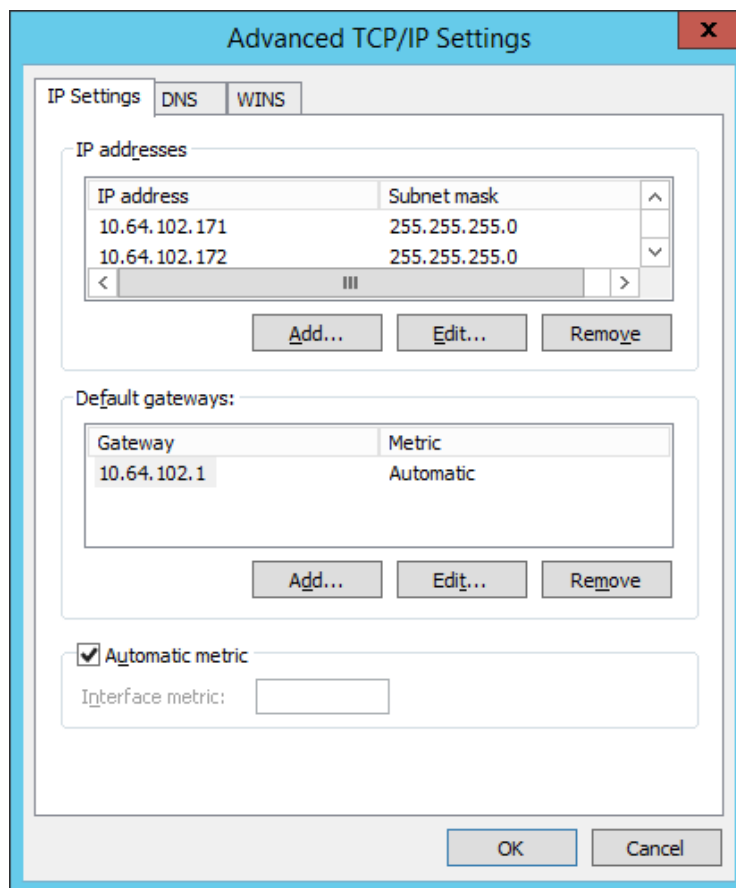
7 Configure Empirix Hammer IP

This section provides the procedures for configuring the Empirix Hammer IP. The procedures fall into the following areas:

- Assign IP addresses to each Hammer IP channel.
- Configure the system, including the originating and terminating channels and the phone book, using the **Hammer Configurator**.
- Save and apply the Hammer configuration and start the Hammer server.
- Create and run the test script using the **Hammer TestBuilder**.

7.1 Configure IP Addresses on Hammer IP Server

The Hammer IP server needs to be configured with IP addresses for each channel. During the compliance test, 20 SIP trunk channels were used. 10 channels were used to originate calls and 10 channels were used to terminate calls. This requires two IP addresses, one for the originating channels and one for the terminating channels. The two IP addresses used were 10.64.102.171 and 10.64.102.181. These IP addresses are configured in the **Advanced TCP/IP Settings** under Network Connections in Windows Server 2012.



7.2 Configure System

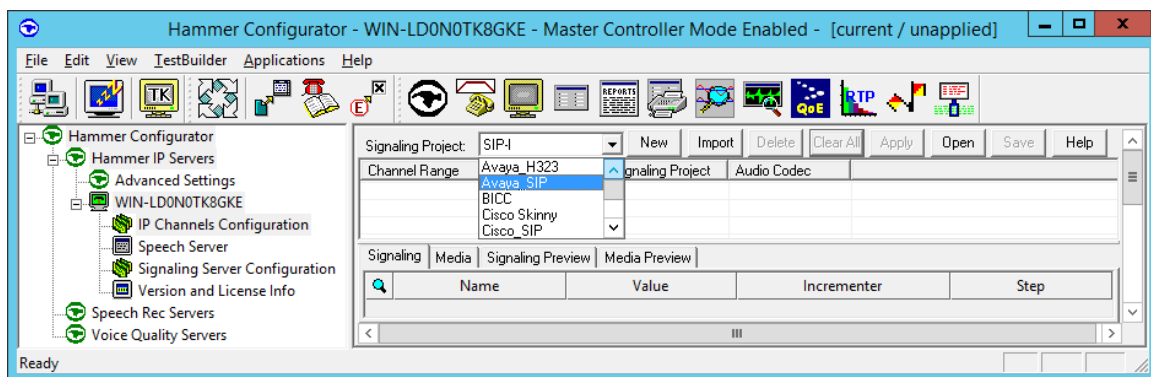
This section covers the configuration of originating and terminating channels. In this configuration, the originating channels emulate SIP trunks (described in **Section 7.2.1**). The terminating channels can emulate SIP trunks, H.323 trunks, SIP endpoints or H.323 endpoints. These Application Notes will explicitly describe the configuration for terminating calls to SIP trunks in **Section 7.2.2.1**. In addition, references are provided to other Application Notes for configuring terminating channels as SIP endpoints, H.323 endpoints, and H.323 trunks in **Sections 7.2.2.2, 7.2.2.3, and 7.2.2.4**, respectively. Only one of those sections needs to be followed depending on the configuration desired.

7.2.1 Configure Originating Channels – SIP Trunks

Hammer IP is configured through the **Hammer Configurator**, a graphical user interface, residing on the Hammer IP server. From the Hammer IP server, run the **Hammer Configurator**. The following screen is displayed.

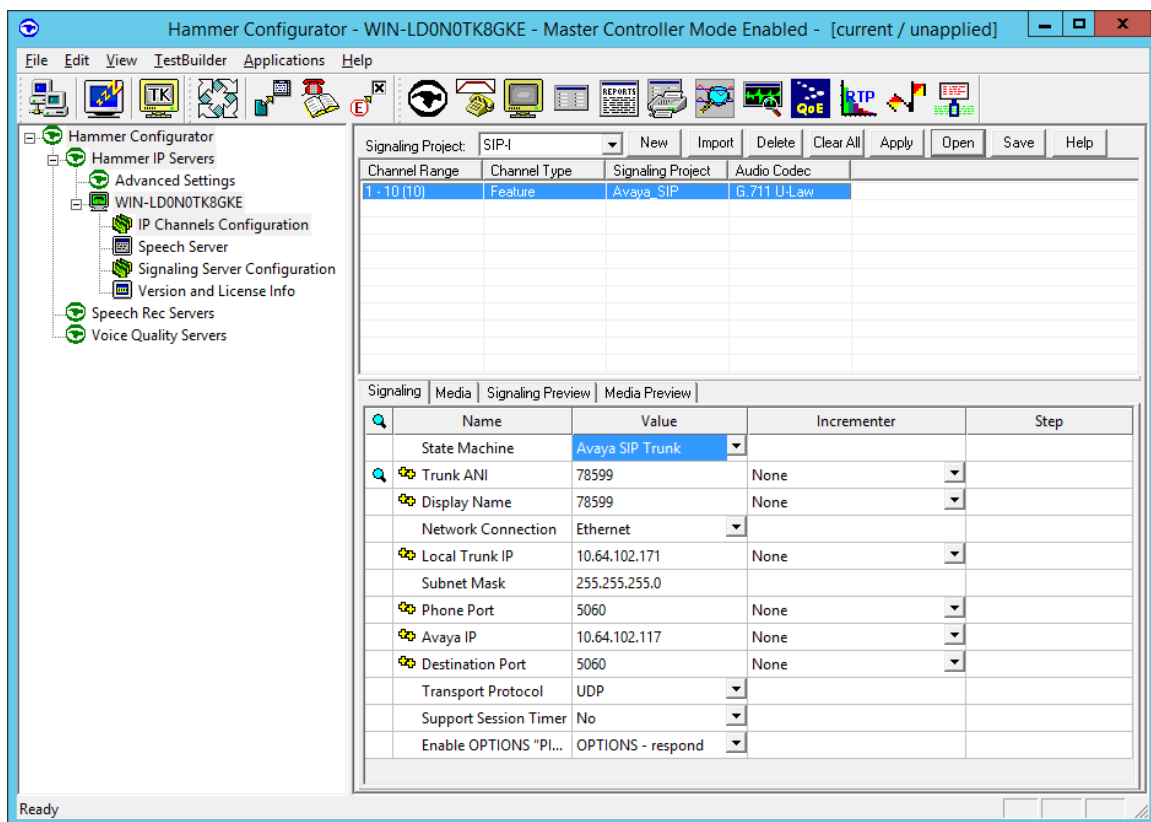
Note: It is assumed that Hammer IP is already in **Master Controller Mode**. To verify, check that the title bar of the **Hammer Configurator** indicates *Master Controller Mode Enabled* as shown below. It is also assumed that a system was already added to the configuration. In this configuration, the system name is *WIN-LD0N0TK8GKE*, which corresponds to the server name.

In the **Hammer Configurator**, the server name will appear in the left pane of the **Hammer Configurator**. Expand the server name (e.g., *WIN-LD0N0TK8GKE*) in the left pane and click on **IP Channels Configuration**. The following window will be displayed. Select *Avaya_SIP* for the **Signaling Project** and then click **New**.



The first line in the grid that is highlighted in the figure below corresponds to the 10 originating channels. To set the number of channels in the group, click on the **Channel Range** cell in the grid and enter the number *10*. The following fields in the **Signaling** tab should be set as follows:

- **State Machine** should be set to *Avaya SIP Trunk*.
- **Trunk ANI** may be any extension.
- **Display Name** may be any extension.
- **Network Connection** should be set to the appropriate network interface.
- **Local Trunk IP** should be set to a unique IP address (e.g., *10.64.102.171*) and should match the IP address configured on Communication Manager in **Section 5.1**. This IP address will be used for the group of originating channels.
- **Subnet Mask** should be set to the network mask (e.g., *255.255.255.0*).
- **Avaya IP** should be set to the Session Manager SIP interface (e.g., *10.64.102.117*).
- **Destination Port** should be set to the SIP listen port (e.g., *5061*).
- **Transport Protocol** should be set to *UDP*.
- **Enable OPTIONS “PING”** should be set to *OPTIONS - respond*.
- The default values for other fields may be used as shown.



In the **Media** tab of the 10 originating channels, configure the fields as follows:

- **Audio Codec** should be set to the appropriate codec for the test. G711 U-Law, G729AB, and G.729A were used during the compliance testing.
- **Frequency [ms]** should be set to the appropriate value for the specified codec. It should match the Packet Size [ms] field in the **IP Codec Set** form on Communication Manager for the specified codec.
- **Network Connection** should specify the appropriate network interface.
- **Source IP Address** should be set to the IP address of the channel group (e.g., 10.64.102.171).
- **Media Profile** should be set to one that specifies the codec configured in the **Audio Codec** field. The default values for the remaining fields may be used as shown.

Hammer Configurator - WIN-LD0N0TK8GKE - Master Controller Mode Enabled - [current / unapplied]

File Edit View TestBuilder Applications Help

Signaling Project: SIP-I New Import Delete Clear All Apply Open Save Help

Channel Range	Channel Type	Signaling Project	Audio Codec
1 - 10 (10)	Feature	Avaya_SIP	G.711 U-Law

Signaling Media Signaling Preview Media Preview

Name	Value	Incrementer	Step
Audio Codec	G.711 U-Law		
Frequency [ms]	20 [ms]		
Network Connection	Ethernet		
Source IP Address	10.64.102.171	None	
Audio Port	10000	++++++	2
DTMF Type	In Band		
Silence Type	Audio		
Jitter Buffer	8 x Frequency [ms]		
Subnet Mask	255.255.255.0		
Media Profile	G711U.s...		
RTCP	Enabled		
TestBuilder Configur...	None		
SRTP Encryption	Disabled		

Ready

7.2.2 Configure Terminating Channels

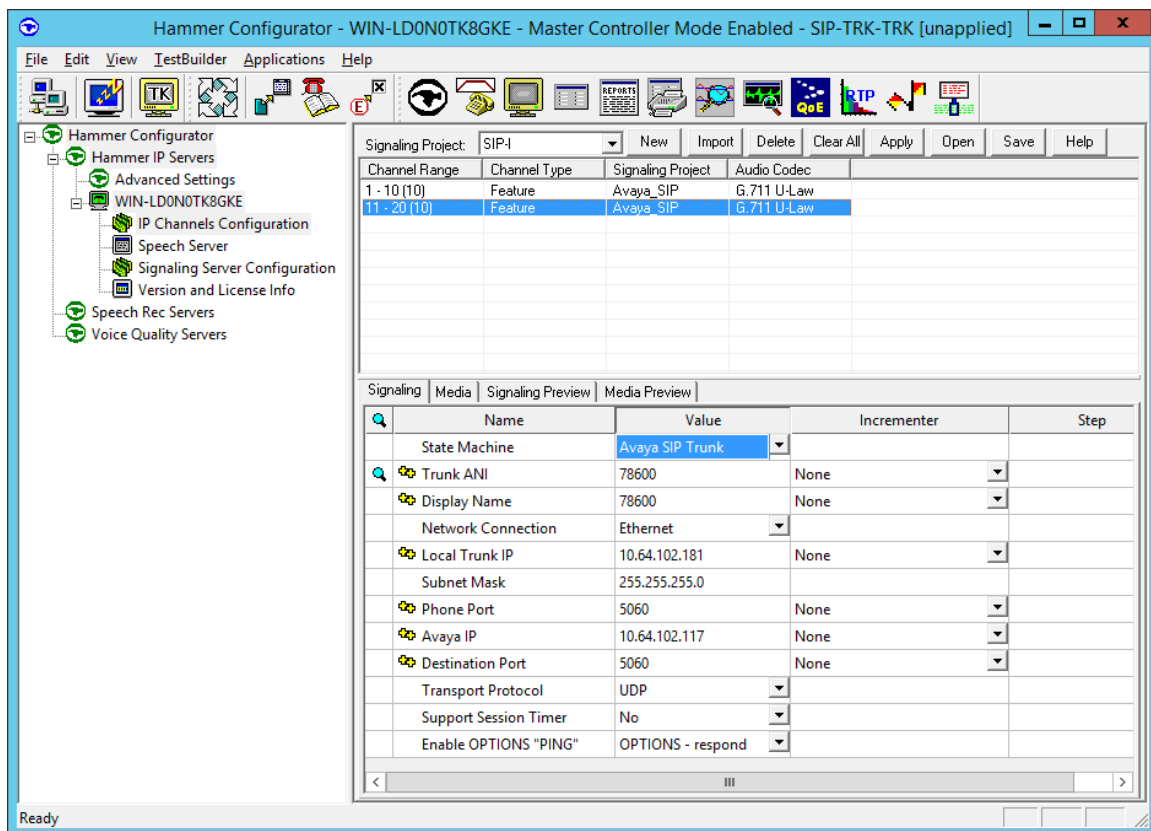
During the compliance test, the originating channels emulated SIP endpoints with the calls terminating on SIP endpoints, SIP trunks, or H.323 endpoints. Select one of the following subsections depending on the configuration desired.

- **Section 7.2.2.1** for terminating calls on SIP trunks.
- **Section 7.2.2.2** for terminating calls on SIP endpoints.
- **Section 7.2.2.3** for terminating calls on H.323 endpoints.
- **Section 7.2.2.4** for terminating calls on H.323 trunks.

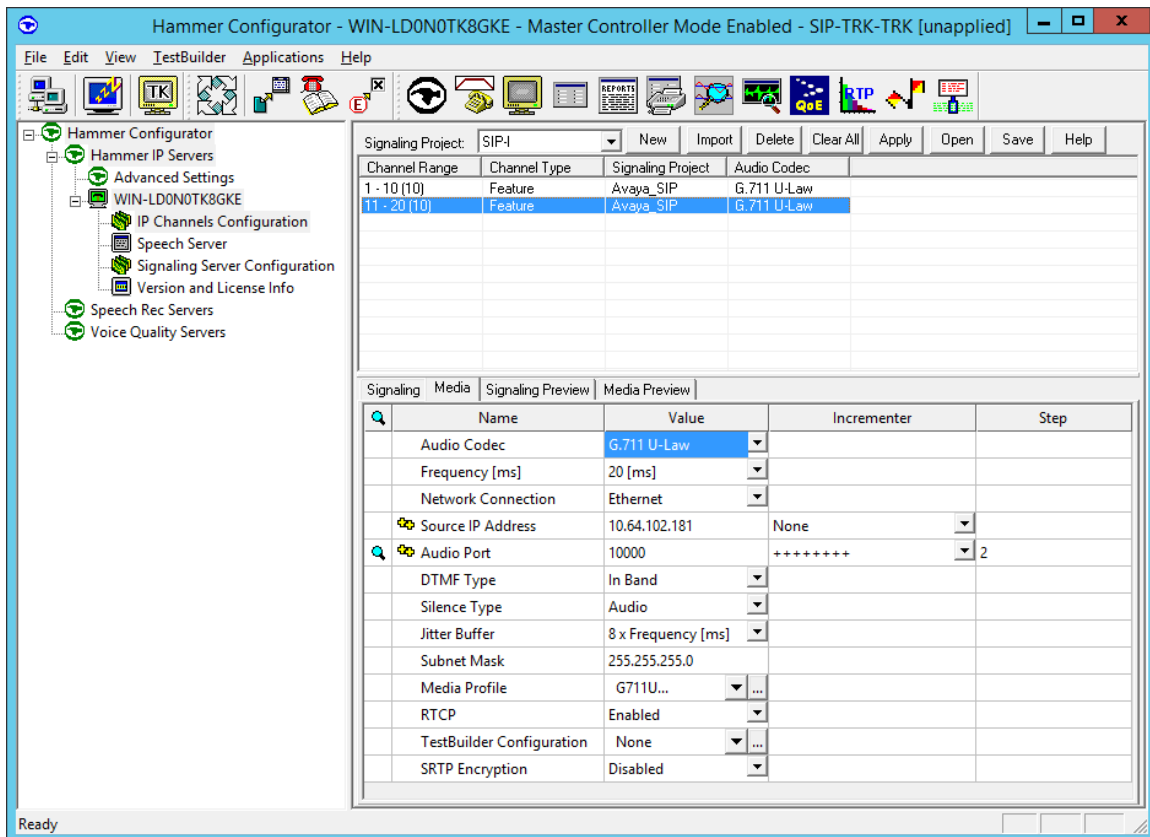
Note: Ensure that the originating and terminating channels are assigned unique IP addresses.

7.2.2.1 Configure Terminating Channels – SIP Trunks

The second line in the grid that is highlighted in the figure below corresponds to the second group of channels that will terminate calls. Set the **Channel Range** cell to the number of channels in this group. The configuration of the **Signaling** tab is similar to the one for the group of originating channels in **Section 7.2.1** with the exception that the **Trunk ANI**, **Display Name**, and **Local Trunk IP** fields will be different. This group of channels will be assigned IP address *10.64.102.181*.



The **Media** tab for the group of terminating channels is shown below. The configuration is similar to the one for the group of originating channels except for the **Source IP Address** field.



7.2.2.2 Configure Terminating Channels – SIP Endpoints

To terminate the calls to SIP endpoints follow the instructions described in [3], specifically:

- **Section 5** describes how to configure SIP stations and call routing on Communication Manager.
- **Section 6** describes how to configure SIP endpoints on Session Manager.
- **Section 7.2.2.1** describes how to configure terminating SIP endpoints on Hammer IP.
- **Section 7.2.3** describes how to configure the PhoneBook.
- **Section 7.4** describes how to disable the **Do Connect Latency** option (required) and how to specify the dialed digits when running a test script.

The configuration described in all the aforementioned sections of [3] must be completed for terminating calls to SIP endpoints.

7.2.2.3 Configure Terminating Channels – H.323 Endpoints

To terminate the calls to H.323 endpoints follow the instructions described in [4], specifically:

- **Section 5** describes how to configure H.323 endpoints for the terminating channels on Communication Manager.
- **Section 6.2.2.1** describes how to configure terminating H.323 endpoints on Hammer IP.
- **Section 6.2.3** describes how to configure the PhoneBook.
- **Section 6.4** describes how to specify the dialed digits when running a test script.

The configuration described in all the aforementioned sections of [4] must be completed for terminating calls to H.323 endpoints.

7.2.2.4 Configure Terminating Channels – H.323 Trunks

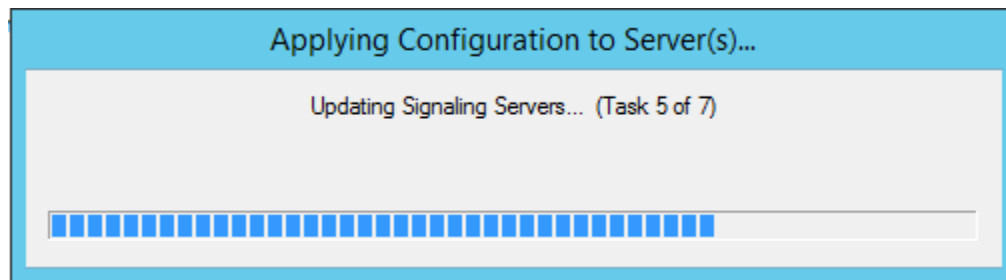
To terminate the calls to H.323 trunks follow the instructions described in [5], specifically:

- **Section 5** describes how to configure H.323 trunks and call routing on Communication Manager.
- **Section 6.2.2.1** describes how to configure terminating H.323 trunks on Hammer IP.
- **Section 6.4** describes how to specify the dialed digits when running a test script.

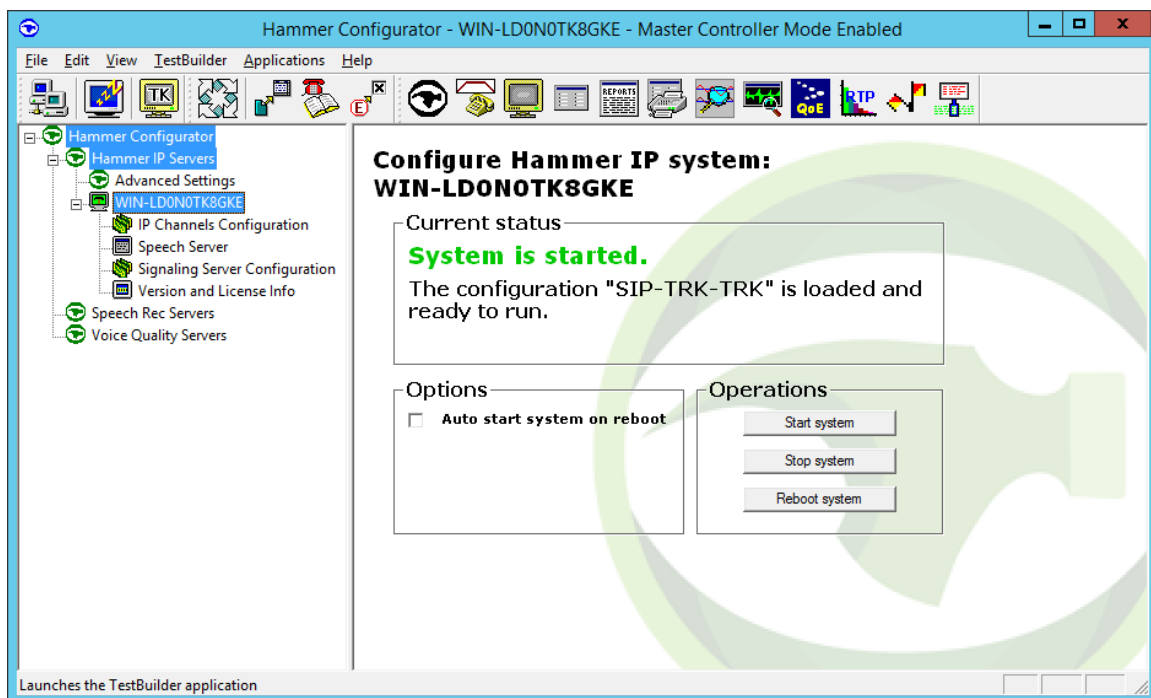
The configuration described in all the aforementioned sections of [5] must be completed for terminating calls to H.323 trunks.

7.3 Applying the Hammer IP Configuration

This completes the configuration of Hammer IP. This configuration should be saved by clicking the **Save** button on the **Hammer Configurator** window. The configuration needs to be applied to the server for the changes to take effect. Click on the **Apply** button in the **Hammer Configurator** window. The following window is displayed as the configuration is being applied to the server.



Check that the system has been started by clicking on the server name (e.g., *WIN-LD0N0TK8GKE*) in the left pane of the **Hammer Configurator**. If the current status is *System Is Stopped*, click the **Start system** button to start the system. When the system is started, it should appear as shown below and should also specify which configuration has been applied. The configuration performed above was saved as *SIP-TRK-TRK*.

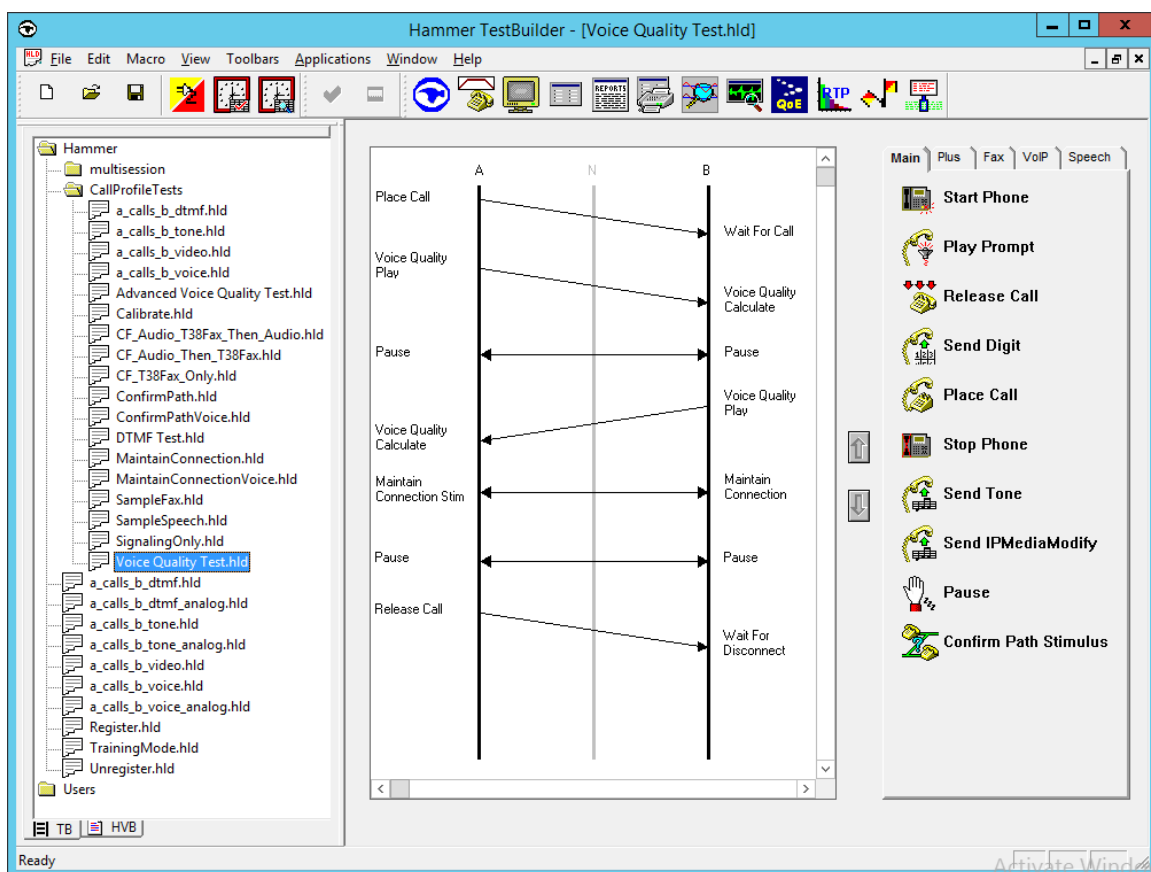


7.4 Configure and Run the Test Script

For the compliance test, two default test scripts were used:

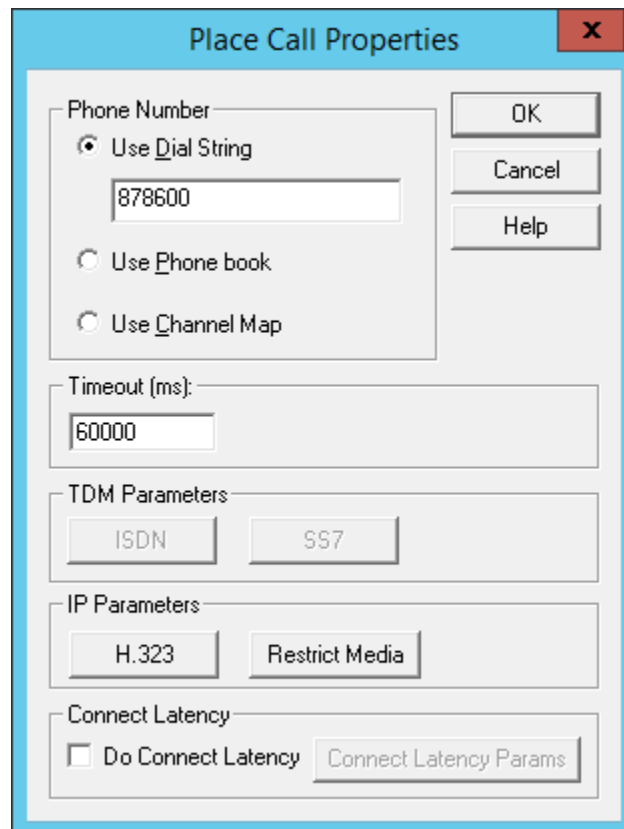
- `a_calls_b_dtmf.hld` to verify DTMF
- `Voice Quality Test.hld` to verify voice quality

The sample test script, `Voice Quality Test.hld`, establishes a VoIP call between two SIP trunks on Hammer IP, followed by the originating side playing an audio prompt to the far-end so that voice quality metrics (e.g., PESQ score) can be obtained. The test script is configured with the **Hammer TestBuilder** application and can be displayed in a ladder diagram as shown below by double-clicking on the test script name.



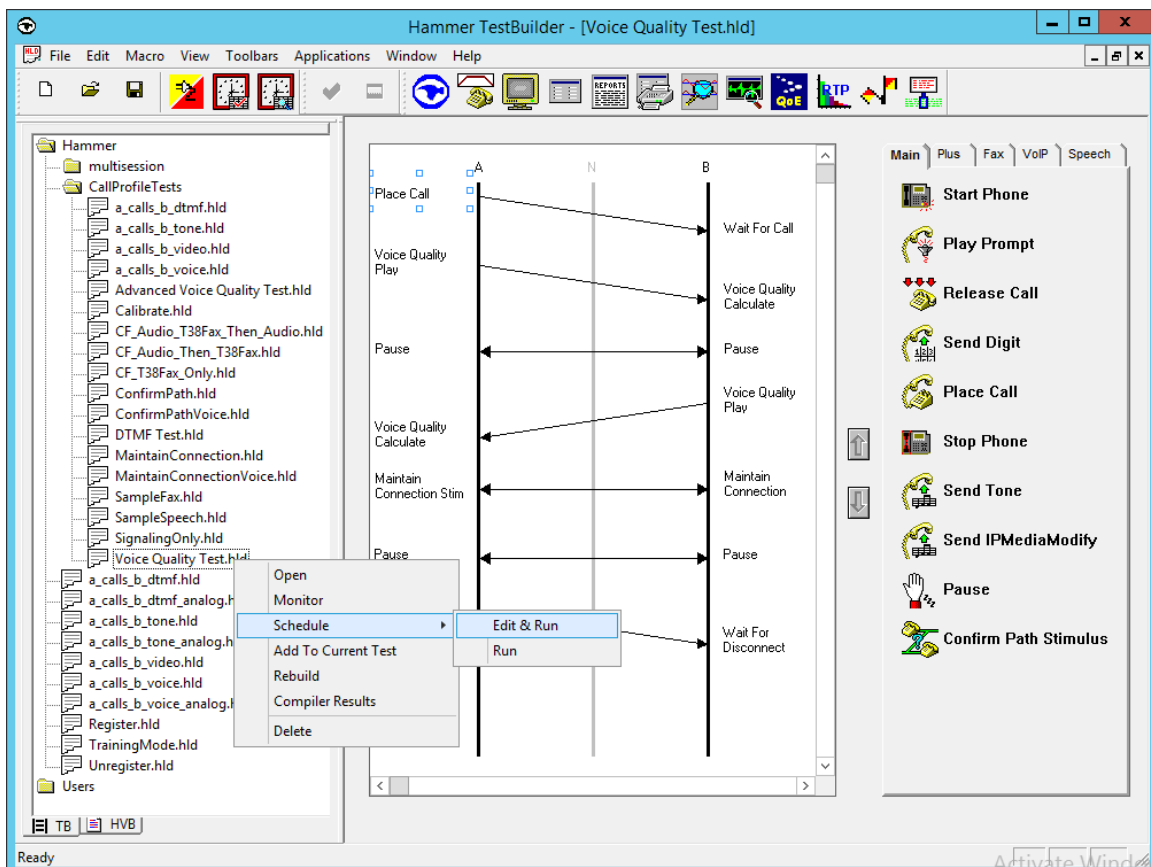
In the sample test script configured above, the A-side (originating SIP trunk) places a call to the B-side (terminating SIP trunk) using the **Place Call** action. The **Place Call** properties can be configured by double-clicking on the action in the ladder diagram. The **Place Call Properties** is configured to dial the same digits for every call. In this example, the Hammer IP dials the AAR access code '8' followed by "78600".

Note: Disable the **Do Connect Latency** option in the **Place Call Properties** window.



The image shows a 'Place Call Properties' dialog box with a blue title bar and a red close button. The dialog is divided into several sections. The 'Phone Number' section has three radio buttons: 'Use Dial String' (selected), 'Use Phone book', and 'Use Channel Map'. Below 'Use Dial String' is a text field containing '878600'. To the right of this section are 'OK', 'Cancel', and 'Help' buttons. The 'Timeout (ms):' section has a text field containing '60000'. The 'TDM Parameters' section has two buttons: 'ISDN' and 'SS7'. The 'IP Parameters' section has two buttons: 'H.323' and 'Restrict Media'. The 'Connect Latency' section has a checkbox labeled 'Do Connect Latency' which is unchecked, and a button labeled 'Connect Latency Params'.

To run the test, right-click on the test script in the left pane of the **Hammer TestBuilder** window and navigate to **Schedule→Edit & Run**. To re-run the test, the user can simply select **Schedule→Run**, if no changes are required.



In the **Properties** window, click on the ellipses button (...) in the **Channels** section and assign channels to the **A-Side** and **B-Side**. Set the **Loop Count** to the appropriate value to control the number of iterations the test should run. Setting this field to **-1** will allow the test to run forever. Setting this field to a specific number will run the test for the many iterations and then stop. The **Guard Time (ms)** field specifies how long to wait before the test is run again on the same channel. The minimum setting should be **3500**. The **Stagger** section allows the user to specify how long to wait before the test is run on the next channel.

Important Note: The **Guard Time** and **Stagger** parameters should be carefully considered for every test. A test script could fail because the configuration under test cannot handle the load generated by the Hammer IP. These parameters can slow down the test to a rate that can be reasonably handled by the test configuration.

The screenshot shows the 'Properties' dialog box for the 'TB Scheduler' tab. The 'Channels' section is expanded, showing 'A-Side' and 'B-Side' fields. The 'Stagger' section is also expanded, showing 'User Defined' selected with a value of 50 ms. The 'Guard Time (ms)' field is set to 3500. The 'Loop Count' field is set to -1. The 'Max Active Connections' field is set to 0. The 'Max Test Time' fields are set to 0 hours and 0 minutes. The 'Action if a Channel is busy' dropdown is set to 'Wait'. The 'PhoneBook' dropdown is set to 'Default-phonebook'. The 'Start Time' is set to 12:27:26 PM on 7/27/2018. The 'File' field shows the path '...ary\Hammer\CallProfileTests\Voice Quality Test.hld'. The 'OK', 'Cancel', 'Apply', and 'Help' buttons are at the bottom.

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 Empirix Hammer IP.

8.1 Verify Avaya Aura® Communication Manager

When the Hammer IP is running a test script, the **status trunk** command may be used to view the active call status. The trunk that is being monitored here is the trunk to Session Manager. This command should specify the trunk group and trunk member used for the call be specified.

status trunk 10/1	Page 1 of 4
TRUNK STATUS	
Trunk Group/Member: 0010/001	Service State: in-service/active
Port: T00001	Maintenance Busy? no
Signaling Group ID:	
IGAR Connection? no	
Connected Ports: T00079	

Page 2 of the **status trunk** command indicates the codec being used for the call and whether the call is shuffled. If the call is shuffled, the **Audio Connection Type** field would be set to *ip-direct*, if the call is hairpinned, the field would be set to *ip-hairpin*; otherwise, the field would be set to *ip-tdm* as shown below.

status trunk 10/1	Page 2 of 4
CALL CONTROL SIGNALING	
Near-end Signaling Loc: PROCR	
Signaling	IP Address Port
Near-end:	10.64.102.115 : 5061
Far-end:	10.64.102.117 : 5061
H.245 Near:	
H.245 Far:	
H.245 Signaling Loc:	H.245 Tunneled in Q.931? no
Audio Connection Type: ip-tdm	Authentication Type: None
Near-end Audio Loc: MG1	Codec Type: G.711MU
Audio	IP Address Port
Near-end:	10.64.50.55 : 2074
Far-end:	10.64.102.172 : 10002
Video Near:	
Video Far:	
Video Port:	
Video Near-end Codec:	Video Far-end Codec:

8.2 Verify Avaya Aura® Session Manager

Verify that the Hammer SIP trunks are up by navigating to **Home→Elements→Session Manager→System Status→SIP Entity Monitoring** and clicking on the appropriate SIP entities. Below is the status of the SIP trunks used for incoming/outgoing calls from/to Hammer IP.

The screenshot shows the Avaya Aura System Manager 7.1 web interface. The left sidebar contains a navigation menu with options like Session Manager, Dashboard, Session Manager Administration, Global Settings, Communication Profile Editor, Network Configuration, Device and Location Configuration, Application Configuration, System Status, SIP Entity Monitoring, Managed Bandwidth Usage, and Security Module Status. The main content area is titled 'Session Manager Entity Link Connection Status' and displays a table of entity links for the selected Session Manager 'devcon-sm'.

Session Manager Entity Link Connection Status
This page displays detailed connection status for all entity links from a Session Manager.

Status Details for the selected Session Manager:

All Entity Links for Session Manager: devcon-sm

Summary View

6 Items Filter: Enable

	SIP Entity Name	IP Address Family	SIP Entity Resolved IP	Port	Proto.	Deny	Conn. Status	Reason Code	Link Status
<input type="radio"/>	devcon-cm	IPv4	10.64.102.115	5061	TLS	FALSE	UP	200 OK	UP
<input type="radio"/>	devcon-aam	IPv4	10.64.102.101	5061	TLS	FALSE	UP	200 OK	UP
<input type="radio"/>	devcon-ipose	IPv4	10.64.102.90	5060	UDP	FALSE	UP	200 OK	UP
<input type="radio"/>	HammerIP-Orig	IPv4	10.64.102.171	5060	UDP	FALSE	UP	200 OK	UP
<input type="radio"/>	HammerIP-Term	IPv4	10.64.102.181	5060	UDP	FALSE	UP	200 OK	UP

Select : None

8.3 Verify Empirix Hammer IP

Call progress can be monitored in the **Hammer System Monitor**. The call log for an originating channel may be logged to the left window and the call log for a terminating channel may be logged to the right window.

The screenshot shows the Hammer System Monitor application window. It has a menu bar (File, View, Channel, Options, Applications, Help) and a toolbar with various icons. The main area is divided into three panes. The left pane shows a list of channels under 'Hammers' with a 'Calls' tab selected, displaying a grid of call status indicators. The middle pane shows a log for 'Script: Voice Quality Test_A.sbx' on 'Server: WIN-LD0N0TK8GKE' for 'Group: 0' and 'Channel: 1'. The right pane shows a log for 'Script: Voice Quality Test_B.sbx' on 'Server: WIN-LD0N0TK8GKE' for 'Group: 1' and 'Channel: 11'. Both logs show a sequence of events including call initialization, protocol completion, signaling transport protocol setup, audio local port configuration, and recording prompts.

Hammer System Monitor

File View Channel Options Applications Help

Hammers

WIN-LD0N0TK8GKE

Calls Registration

CC 0 1

1 2 3 4 5 6 7 8 9 10

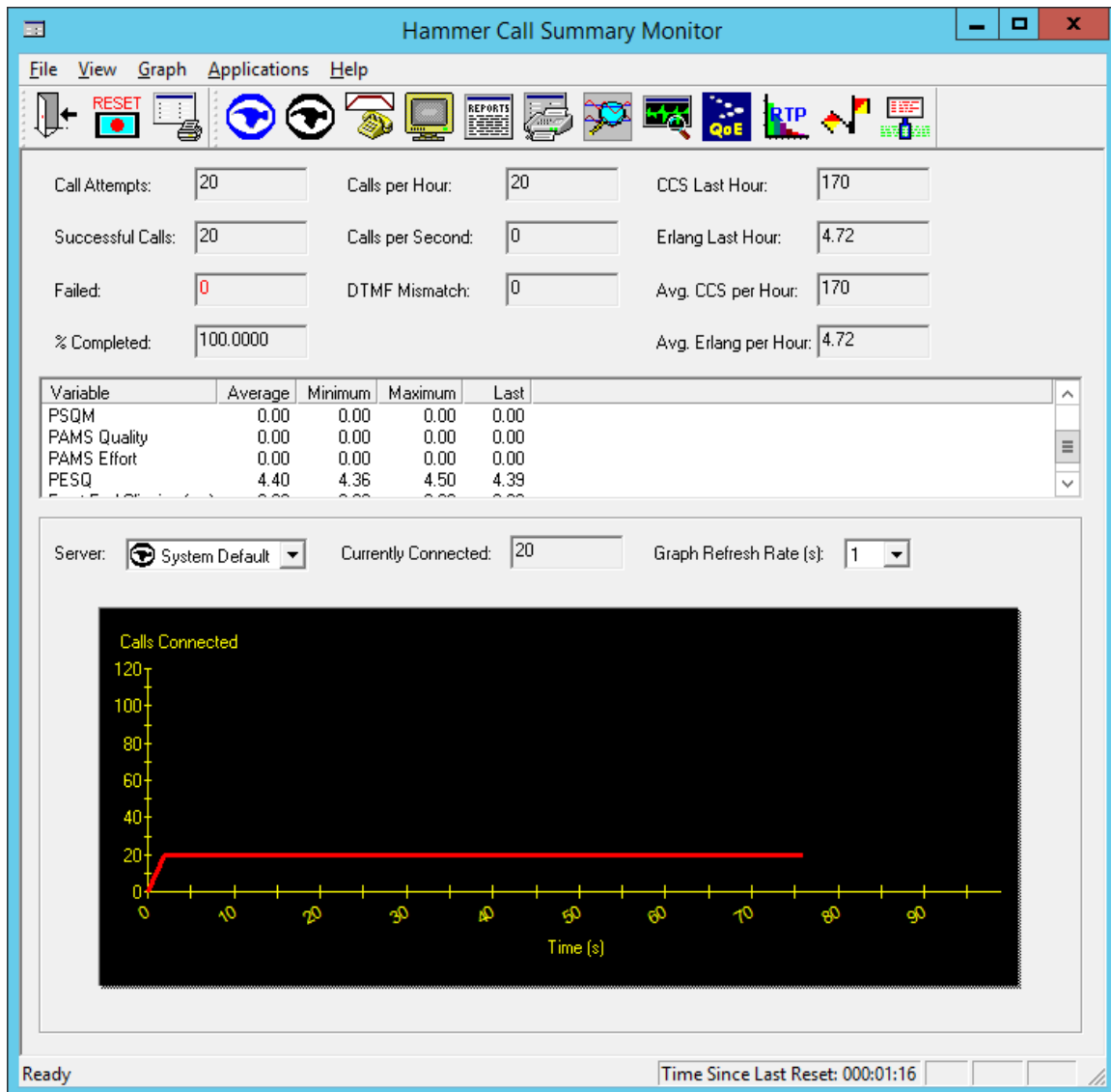
Script: Voice Quality Test_A.sbx
Server: WIN-LD0N0TK8GKE Group: 0 Channel: 1

12:28:41.557 Voice Quality Test : is now initializing...
12:28:41.557 Start protocol completed
12:28:51.589 ***** PlaceCall *****
12:28:51.604 > Placing call to 878600
12:28:51.614 The signaling transport protocol is UDP
12:28:51.669 > Audio local port: 10.64.102.171:10000; remote destination
12:28:51.700 > Call is answered
12:28:52.700 ***** Begin Simple VQ Play *****
12:28:52.700 => SQpromptName = WIN-LD0N0TK8GKE#Voice Quality T
12:29.22.701 > Done Playing
12:29.22.701 ***** Pausing for 7 seconds. *****
12:29.23.701 ***** Begin Simple VQ Calculate *****
12:29.23.701 > Recording Prompt: voip14Mboy1p1.pcm
12:29.53.702 > Done Recording
12:29.53.702 ***** MaintainConnectionStimulus*****
12:29.53.702 Clear digits completed

Script: Voice Quality Test_B.sbx
Server: WIN-LD0N0TK8GKE Group: 1 Channel: 11

12:28:41.525 Voice Quality Test : is now initializing...
12:28:41.525 Start protocol completed
12:28:41.525 ***** WaitForCall *****
12:28:41.552 The signaling transport protocol is UDP
12:28:51.900 > Audio local port: 10.64.102.181:10000; remote destination 10.64.5
12:28:51.931 > Answering call in 1 rings
12:28:52.931 ***** Begin Simple VQ Calculate *****
12:28:52.931 > Recording Prompt: voip14Mboy1p1.pcm
12:29.22.932 > Done Recording
12:29.22.932 ***** Pausing for 5 seconds. *****
12:29.27.932 ***** Begin Simple VQ Play *****
12:29.27.932 => SQpromptName = WIN-LD0N0TK8GKE#Voice Quality Test#11#
12:29.57.933 > Done Playing
12:29.57.933 ***** MaintainConnectionResponse*****
12:29.57.933 Clear digits completed

The **Hammer Call Summary Monitor** may be used to get a test status overview, including the number of call attempts, number of failed calls, PESQ scores, amongst other useful metrics.



9 Conclusion

These Application Notes describe the configuration steps required to integrate the Empirix Hammer IP with an Avaya SIP telephony network using SIP trunk emulation. The Hammer IP was able to establish a SIP trunk with Avaya Aura® Session Manager, exchange SIP Options messages, successfully establish calls through the Avaya SIP telephony network, generate voice quality metrics, monitor the calls, and generate reports. All feature and serviceability test cases were completed with observations noted in **Section 2.2**.

10 References

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

- [1] *Administering Avaya Aura® Communication Manager*, Release 7.1.3, Issue 7, May 2018, available at <http://www.avaya.com>.
- [2] *Administering Avaya Aura® Session Manager*, Release 7, Issue 5, July 2018, available at <http://www.avaya.com>.
- [3] *Application Notes for Empirix Hammer IP with Avaya Aura® Communication Manager Avaya Aura® Session Manager using SIP Endpoint Emulation*, Issue 1.0, available at <http://www.avaya.com>.
- [4] *Application Notes for Empirix Hammer IP with Avaya Aura® Communication Manager using H.323 Endpoint Emulation*, Issue 1.0, available at <http://www.avaya.com>.
- [5] *Application Notes for Empirix Hammer IP with Avaya Aura® Communication Manager using H.323 Trunk Emulation*, Issue 1.0, available at <http://www.avaya.com>.

©2018 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.