

Avaya Solution & Interoperability Test Lab

### Application Notes for Biamp Tesira SVC-2 with Avaya Aura<sup>®</sup> Communication Manager R6.3 and Avaya Aura<sup>®</sup> Session Manager R6.3 – Issue 1.0

#### Abstract

These Application Notes describe the procedures for configuring Biamp Tesira SVC-2 which was compliance tested with Avaya Aura<sup>®</sup> Communication Manager R6.3 and Avaya Aura<sup>®</sup> Session Manager R6.3.

The overall objective of the interoperability compliance testing is to verify Biamp Tesira SVC-2 functionalities in an environment comprised of Avaya Aura<sup>®</sup> Communication Manager, Avaya Aura<sup>®</sup> Session Manager and various Avaya H.323 and SIP IP Telephones.

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 procedures for configuring Biamp Tesira SVC-2 which was compliance tested with Avaya Aura<sup>®</sup> Communication Manager and Avaya Aura<sup>®</sup> Session Manager.

The Tesira SVC-2 enables conferencing over VoIP directly from Tesira SERVER-IO, with two channels of VoIP interface per card. Tesira SVC-2 allows Tesira SERVER-IO to connect directly to IP-based phone systems and eliminate the need for VoIP adapters. Used in conjunction with SEC-4 4-Channel Wideband Acoustic Echo Cancellation Input Cards and STC-2 Dual-Channel Telephone Interface Cards, the Tesira SVC-2 makes Tesira SERVER-IO a powerful, flexible, and affordable telephone conferencing product. Combined with the STC-2 Card, the Tesira SVC-2 makes it possible to create redundancies within a conferencing system for multi-point conferences and/or back-up to VoIP lines. Up to 6 Tesira SVC-2 can be installed into a single Tesira SERVER-IO unit.

For further details on Tesira SVC-2 configuration steps not covered in this document, consult **Section 10 [4]**.

### 2. General Test Approach and Test Results

All test cases were performed manually. The general test approach was to verify the Biamp Tesira SVC-2 registration and place various types of calls to and from Biamp Tesira SVC-2. Biamp Tesira SVC-2 operations such as inbound calls, outbound calls, hold/resume, DTMF, audio codecs (G.711Mu, G.729, G.722), and Biamp Tesira SVC-2 interactions with Session Manager, Communication Manager, and Avaya SIP and H.323 telephones were verified. For serviceability testing, failures such as cable pulls and resets were applied.

DevConnect Compliance Testing is conducted jointly by Avaya and DevConnect members. The jointly-defined test plan focuses on exercising APIs and/or standards-based interfaces pertinent to the interoperability of the tested products and their functionalities. DevConnect Compliance Testing is not intended to substitute full product performance or feature testing performed by DevConnect members, nor is it to be construed as an endorsement by Avaya of the suitability or completeness of a DevConnect member's solution.

### 2.1. Interoperability Compliance Testing

The interoperability compliance test included feature and serviceability testing. The feature testing evaluated the interoperability between Biamp Tesira SVC-2, Session Manager, and Communication Manager. The serviceability testing introduced failure scenarios to see if Biamp Tesira SVC-2 could resume after failure.

### 2.2. Test Results

All test cases passed.

#### 2.3. Support

Technical support for Biamp Tesira SVC-2 solution can be obtained by contacting Biamp at:

- <u>http://www.biamp.com/support/index.aspx</u>
- (800)-826-1457

### 3. Reference Configuration

**Figure 1** illustrates a sample configuration consisting of an Avaya S8300D Server, an Avaya G450 Media Gateway, Session Manager and Biamp Tesira SVC-2. The solution described herein is also extensible to other Avaya Servers and Media Gateways. For completeness, Avaya 9600 Series H.323 IP Telephones, Avaya 9600 Series SIP IP Telephones, and Avaya 6400 Series Digital Telephones, are included in Figure 1 to demonstrate calls between the Biamp Tesira SVC-2 and Avaya SIP, H.323, and digital telephones.



Figure 1: Test Configuration of Biamp Tesira SVC-2

### 4. Equipment and Software Validated

The following equipment and software were used for the test configuration.

Equipment/Software		Release/Version
Avaya Aura® Commun	ication Manager	R016x.03.0.124.0 w/ patch 03.0.124.0-
running on Avaya S830	0D Server with Avaya	21172
G450 Media Gateway		
Avaya Aura® System N	Ianager on Avaya	6.3.5.5.2017
S8800 Server		
Avaya Aura® Session M	Manager on Dell R610	6.3.0.0.18002
Avaya 9600 Series IP T	elephones	
	9620 (H.323)	3.1
	9630 (H.323)	3.1
	9650 (H.323)	3.1
Avaya 9600 Series SIP	Telephones	
	9620 (H.323)	2.6.4
	9630 (H.323)	2.6.4
9650 (H.323)		2.6.4
Avaya 6408D+ Digital Telephone		-
Biamp Tesira SVC-2		1.2.1
Biamp Tesira Server-IO		2.0.0
Biamp Linux		3.2.48-BIAMP

# 5. Configure Avaya Aura<sup>®</sup> Communication Manager

This section describes the procedure for setting up a SIP trunk between Communication Manager and Session Manager. The steps include setting up an IP codec set, an IP network region, IP node name, a signaling group, a trunk group, and a SIP station. Before a trunk can be configured, it is necessary to verify if there is enough capacity to setup an additional trunk. The highlights in the following screens indicate the values used during the compliance test. Default values may be used for all other fields.

These steps are performed from the Communication Manager System Access Terminal (SAT) interface. Biamp Tesira SVC-2 and other SIP telephones are configured as off-PBX telephones in Communication Manager.

#### 5.1. Capacity Verification

Enter the **display system-parameters customer-options** command. Verify that there are sufficient Maximum Off-PBX Telephones – OPS licenses. If not, contact an authorized Avaya account representative to obtain additional licenses



On **Page 2** of the form, verify that the number of SIP trunks supported by the system is sufficient for the number of SIP trunks needed. If not, contact an authorized Avaya account representative to obtain additional licenses.

display system-parameters customer-options		Page	2 of	11	
OPTIONAL FEATURES		2			
IP PORT CAPACITIES		USED			
Maximum Administered H.323 Trunks:	4000	27			
Maximum Concurrently Registered IP Stations:	2400	2			
Maximum Administered Remote Office Trunks:	4000	0			
Maximum Concurrently Registered Remote Office Stations:	2400	0			
Maximum Concurrently Registered IP eCons:	68	0			
Max Concur Registered Unauthenticated H.323 Stations:	100	0			
Maximum Video Capable Stations:	2400	2			
Maximum Video Capable IP Softphones:	2400	2			
Maximum Administered SIP Trunks:	4000	65			
Maximum Administered Ad-hoc Video Conferencing Ports:	4000	0			
Maximum Number of DS1 Boards with Echo Cancellation:	80	0			
Maximum TN2501 VAL Boards:	10	0			
Maximum Media Gateway VAL Sources:	50	1			
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			

#### 5.2. IP Codec Set

This section describes the steps for administering a codec set in Communication Manager. This codec set is used in the IP network region for communications between Communication Manager and Session Manager. Enter the **change ip-codec-set** <**c**> command, where **c** is a number between **1** and **7**, inclusive. IP codec sets are used in **Section 5.3** when configuring an IP network region to specify which codec sets may be used within and between network regions.

cha	change ip-codec-set 1						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:	G.729	n	2	20					
3:									

#### 5.3. Configure IP Network Region

This section describes the steps for administering an IP network region in Communication Manager for communication between Communication Manager and Session Manager. Enter the **change ip-network-region** <**n**> command, where **n** is a number between **1** and **250** inclusive, and configure the following:

- Authoritative Domain Enter the appropriate name for the Authoritative Domain. Set to the appropriate domain. During the compliance test, the authoritative domain is set to **avaya.com**. This should match the SIP Domain value on Session Manager.
- Intra-region IP-IP Direct Audio Set to yes to allow direct IP-to-IP audio connectivity between endpoints registered to Communication Manager or Session Manager in the same IP network region. The default value for this field is yes.
- Codec Set Set the codec set number as provisioned in Section 5.2.
- Inter-region IP-IP Direct Audio Set to yes to allow direct IP-to-IP audio connectivity between endpoints registered to Communication Manager or Session Manager in different IP network regions. The default value for this field is yes.

change ip-network-region 1	Page 1 of 20
I	P NETWORK REGION
Region: 1	
Location: 1 Authoritative	Domain: avaya.com
Name:	Stub Network Region: n
MEDIA PARAMETERS	Intra-region IP-IP Direct Audio: yes
Codec Set: 1	Inter-region IP-IP Direct Audio: yes
UDP Port Min: 16390	IP Audio Hairpinning? n
UDP Port Max: 16999	
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
Keep-Alive Count: 5	

#### 5.4. Configure IP Node Name

This section describes the steps for setting IP node name for Session Manager in Communication Manager. Enter the **change node-names ip** command, and add a node name for Session Manager along with its IP address.

change node-names	ip			Page	1 of	2
		IP NODE	NAMES			
Name	IP Address					
CLAN	10.64.40.24					
IPOffice	10.64.44.21					
SES	10.64.40.41					
SM-1	10.64.41.42					
SM-2	10.64.21.31					
default	0.0.0.0					
procr	10.64.41.21					
procr6	::					

#### 5.5. Configure SIP Signaling

This section describes the steps for administering a signaling group in Communication Manager for signaling between Communication Manager and Session Manager. Enter the **add signaling-group** <s> command, where s is an available signaling group and configure the following:

- **Group Type** Set to **sip.**
- Transport Method Set to tls
- Near-end Node Name Set to procr as displayed in Section 5.4.
- Far-end Node Name Set to the Session Manager name configured in Section 5.4.
- Far-end Network Region Set to the region configured in Section 5.3.

change signaling-group 92	Page 1 of 2
STENALING GIOUP 52	
SIGNALING GI	(001
Group Number: 92 Group Type: s:	1p
IMS Enabled? n Transport Method: t	ls
Q-SIP? n	
IP Video? v Priority Video? v	Enforce SIPS URI for SRTP? y
Peer Detection Enabled? v Peer Server: SN	1
Prepend '+' to Outgoing Calling/Alerting/Di	verting/Connected Public Numbers? v
Remove '+' from Incoming Called/Calling/Alex	cting/Diverting/Connected Numbers? n
Remove , from theoming carried, carring, hier	tering, biverering, connected Nambers. In
Maan and Mada Manay ana an	Ten and Made News, CM 1
Near-end Node Name: procr	Far-end Node Name: SM-1
Near-end Listen Port: 5061	Far-end Listen Port: 5061
Far-	-end Network Region: 1
Far-end S	Secondary Node Name:
Far-end Domain:	
	Bypass If IP Threshold Exceeded? n
Incoming Dialog Loopbacks: eliminate	RFC 3389 Comfort Noise? n
DTMF over IP: rtp-pavload	Direct IP-IP Audio Connections? v
Session Establishment Timer(min) · 3	IP Audio Hairpinning? n
Enable Laver 3 Test2 V	Initial ID-ID Diroct Modia? n
Thable Layer 5 lest: y	Alternata Denta Timen(sea).
H.323 Station Outgoing Direct Media? n	Alternate Route Timer(sec): 6

#### 5.6. Configure SIP Trunk

This section describes the steps for administering a trunk group in Communication Manager for trunking between Communication Manager and Session Manager. Enter the **add trunk-group** <**t**> command, where **t** is an unallocated trunk group and configure the following:

- **Group Type** Set the Group Type field to **sip**.
- **Group Name** Enter a descriptive name.
- TAC (Trunk Access Code) Set to any available trunk access code.
- Signaling Group Set to the Group Number field value configured in Section 5.5.
- Number of Members Allowed value is between 0 and 255. Set to a value large enough to accommodate the number of SIP telephone extensions being used.

add trunk-group 92	Page 1 of 21 TRUNK GROUP
Group Number: 92 Group Name: SM 41 Direction: two-w	Group Type: sip CDR Reports: y 42 COR: 1 TN: 1 TAC: 1092 ay Outgoing Display? y
Dial Access? n Queue Length: O	Night Service:
Service Type: tie	Auth Code? n
	Member Assignment Method: auto Signaling Group: 92 Number of Members: 10

#### 5.7. Configure SIP Endpoint

The following screen displays a SIP extension created from System Manager.

```
display station 72032
                                                               Page 1 of
                                                                             6
                                    STATION
                                                                      BCC: 0
Extension: 72032
                                        Lock Messages? n
    Type: 9630SIP
                                        Security Code: *
                                                                       TN: 1
                                      Coverage Path 1: 99
    Port: S00107
                                                                      COR: 1
                                      Coverage Path 2:
                                                                      COS: 1
    Name: Biamp-2
                                      Hunt-to Station:
STATION OPTIONS
                                          Time of Day Lock Table:
             Loss Group: 19
                                                Message Lamp Ext: 72032
       Display Language: english
                                                  Button Modules: 0
         Survivable COR: internal
   Survivable Trunk Dest? y
                                                    IP SoftPhone? n
                                                        IP Video? n
```

# 6. Configure Avaya Aura<sup>®</sup> Session Manager

This section provides the procedures for configuring Session Manager. Session Manager is comprised of two functional components: The Session Manager server and the System Manager server. All SIP call provisioning for Session Manager is performed through the System Manager Web interface and is then downloaded into Session Manager.

This section assumes that Session Manager and System Manager have been installed, and network connectivity exists between the two platforms.

The following will be covered in this section for configuring Session Manager.

- User Management
- TLS certificate between 3<sup>rd</sup> party endpoint and Session Manager

#### 6.1. Configure a SIP User

When adding new SIP user, use the option to automatically generate the SIP station in Communication Manager, after adding a new SIP user.

To add new SIP users, Navigate to Home  $\rightarrow$  Users  $\rightarrow$  User Management  $\rightarrow$  Manage Users. Click New and provide the following information:

- <u>Identity section</u>
  - Last Name Enter last name of user.
  - **First Name** Enter first name of user.
  - Login Name Enter extension number@sip domain. The sip domain is defined as Authoritative Domain in Section 5.3.
  - Authentication Type Verify Basic is selected.
  - **Password** Enter password to be used to log into System Manager.
  - **Confirm Password** Repeat value entered above.

AVAVA						Last Logged on at F	ebruary 13,	2014 12:39 PM
Aura <sup>®</sup> System Manager 6.3						Help   About   Ch	hange Pass	word   Log off admin
Home User Management *								
▼ User Management ◀	Home / Users / L	Jser Management / Mai	nage Us	sers				
Manage Users								Help ?
Public Contacts	New User Profile Commit & Continue Commit Cancel							Cancel
Shared Addresses								
System Presence ACLs	Identity *	Communication Pro	ofile	Membership	Contacts			
Communication Profile								
Password Policy	User Prov	Isioning Rule 🖷						
		User Provisioning Rule:			×			_
	Identity 🖷	)						
		* Last Name:	72032	2				
	Last N	ame (Latin Translation):						
		* First Name:	72032	2				
	First N	ame (Latin Translation):	72032					
		Middle Name:						
		Description:						
		* Login Name:	72032	@avaya.com				
		* Authentication Type:	Basic		~			
		Password:	••••					
		Confirm Password:	••••					
		Localized Display Name:	Biamp	-2				
		Endpoint Display Name:	Biamp	-2				
		Title:						
		Language Preference:	Enalis	h (United States)	*			
		Time Zone:	(-7:0	)Mountain Time (l	JS & C; 🎽			
		Emplovee ID:						

CRK; Reviewed: SPOC 5/9/2014

- <u>Communication Profile section</u>
  - **Communication Profile Password** Type Communication profile password in this field
  - **Confirm Password** Repeat value entered above.

Identity *	Communication Profile	Membership	Contacts
Communio	ation Profile 💿		
Communi	cation Profile Password: ••••	••	]
	Confirm Password:	••	
ONew (	Delete EDone Cance	ł	
Name			
OPrimar	Ŷ		
Select : None			
	* Name: Prima Default :	iry	

- <u>Communication Address sub-section</u>
  - Select "Avaya SIP" for the **Type** field.
  - **Fully Qualified Address** Enter the extension of the user and select the relevant domain name.
  - Click **Add** button

Communication Address 💌					
💿 New 🥖 Edit 💿 Dele	ete				
Туре	Handle	Domain			
No Records found					
Ту	pe: Avaya SIP	~			
* Fully Qualified Addre	ess: 72032 @	avaya.com 💌			
		Add Cancel			

- <u>Session Manager Profile section</u>
  - **Primary Session Manager** Select one of the Session Managers.
  - Secondary Session Manager Select (None) from the drop-down menu.
  - Survivability Server Select (None) from the drop-down menu.
  - **Origination Sequence** Select Application Sequence defined for Communication Manager.
  - **Termination Sequence** Select Application Sequence for Communication Manager.
  - **Home Location** Select Location.

Session Manager Profile 💌		
SIP Registration		
* Primary Session Manager	CM62	Primary Seconda
	SMUS	14 0
Secondary Session Manager	(None)	
Survivability Server	(None)	
Max. Simultaneous Devices	1 💌	
Block New Registration When Maximum Registrations Active?		
Application Sequences		
Origination Sequence	AppSeq-S8300D	
Termination Sequence	AppSeq-S8300D	
Call Routing Settings		
* Home Location	41-subnet 💌	
Conference Factory Set	(None)	

- Endpoint Profile section
  - System Select Managed Element defined in System Manager.
  - **Profile Type** Select **Endpoint**.
  - Use Existing Endpoints Leave unchecked to automatically create new endpoint when new user is created. Or else, check the box if endpoint is already defined in Communication Manager.
  - Extension Enter same extension number used in this section.
  - **Template** Select template for type of SIP phone
  - Security Code Enter numeric value used to logon to SIP telephone. (Note: this field must match the value entered for the Shared Communication Profile Password field).
  - **Port** Select **IP** from drop down menu
  - **Delete Station on Unassign of Endpoint** Check the box to automatically delete station when Endpoint Profile is un-assigned from user.

CM Endpoint Profile 💌	
* System	Element-S8300D
* Profile Type	Endpoint
Use Existing Endpoints	
* Extension	Q 72032 Endpoint Editor
Template	Select/Reset
Set Type	9630SIP
Security Code	•••••
Port	Q,IP
Voice Mail Number	
Preferred Handle	(None)
Enhanced Callr-Info display for 1-line phones	
Delete Endpoint on Unassign of Endpoint from User or on Delete User.	
Override Endpoint Name and Localized Name	

#### 6.2. Configure Biamp Tesira SVC-2 for TLS

In System Manager, Navigate to Home  $\rightarrow$  Elements  $\rightarrow$  Session Manager  $\rightarrow$  Dashboard. Select a Session Manager.

AVAVA Last Logged on at February 18, 2014 11:57 AM Help   About   Change Password   Log off admin					
Home Session Manager					
▼ Session Manager	Session Manager ( Home / Elements / Session Manager / Dashboard				
Dashboard	Dashboard Help ?				
Session Manager	Session Manager Dashboard				
Administration	This page provides the overall status and health summary of each administered Session Manager.				
Communication Profile	Session Manager Instances				
Editor	Session manager instances				
Network Configuration	Service State   Shutdown System  As of 12:22 PM				
Device and Location	> Device and Location 1 Item 🖑 Show ALL 🕙 Filter: Enable				
Configuration Application	Session Manager         Type         Tests Pass         Alarms         Security Module         Service State         Entity Monitoring         Active Call Count         Registrations         Data Replication				
Configuration <ul> <li>System Status</li> </ul>	SM63         Core         ✔         0/0/0         Up         Accept New Service         2/9         0         6/6         ✔         6.3.5.0.6350	005			
▶ System Tools	Select : All, None				

• From the Session Manager Administration page, verify that the Enable TLS Endpoint Certificate Validation field is not checked. By not checking, Session Manager does not request a certificate from the 3<sup>rd</sup> party endpoint.

AVAYA		Last Logged on at February 18, 2014 11:57 AM Help   About   Change Password   <b>Log off</b>
Aura System Manager 6.3		admin
Home Session Manager	د	
Session Manager	Home / Elements / Session Manager / Session Manager Administration	
Dashboard		Help ?
Session Manager	Session Manager Administration	
Administration	This page allows you to administer Session Manager instances and configure their global settings.	
Communication Profile	Global Settings	
Editor		
Network Configuration	Save	
Device and Location	Allow Unauthenticated Emergency Calls	
Configuration		
▶ Application		
Configuration	Failback Policy Auto	
▶ System Status	ELIN SIP Entity None 💌	
▹ System Tools	Better Matching Dial Pattern or Range in Location 🔽 ALL Overrides Match in Originator's Location	
Performance	Ignore SDP for Call Admission Control 📃	
	Disable Call Admission Control Threshold Alarms 📃	
	Disable Loop Detection Alarms	
	*Loop Detection Alarms Threshold (hours) 24	
	Enable TLS Endpoint Certificate Validation	
	Enable Dial Plan Ranges 📃	

## 7. Configure Biamp Tesira SVC-2

Biamp installs, configures, and customizes the Tesira SVC-2 application for their end customers. This section only provides steps to configure Biamp Tesira SVC-2 to interface with Session Manager. Select the Tesira icon from Desktop to start Tesira software and design a VoIP system. How to configure a Tesira system is out of the scope of this application note.

• Highlight the VoIPControl/Status block, as shown below.



• Click right mouse button and select **Properties**, and the Properties menu will display on the right



• Navigate the **Protocol SIP→Transport** to configure transport to be used. The default is UDP. During the compliance test, UDP was utilized. When TLS is selected, please refer to Tesira Operational Manual for additional configuration.

rop	perties		٩	<b>ب</b>
Vo	IPControlStatus1	•	1:	
		DSP Properties		
	Primary DNS	0.0.0		4
	Secondary DNS	0.0.0		
	Network Time		v	
	Time Synchronization	SNTP		
	Synchronized Time			
	SNTP Address			
	Daylight Savings Time	Disabled		
	Time Synchronization	64		
	Time Zone	(GMT-08:00) Pacific	Т	
	Network Provisioning	Server	•	
	TFTP Server Mode	None		
	TFTP Server Address			
	DHCP Custom Option	150		
	Network Ethernet		•	
	Ethernet Speed	Auto		
	Duplex	Full		
	Pad Short Frame	Yes		
	Accept Short Frame	Yes		
	QoS		•	
	Mode	DiffServ		
	L2 Other User Priority			
	L3 Other Precedence	0		
	L3 Other Min Delay	NO 		
	L3 Other Max Throug	Yes		
	L3 Other Max Reliabil	NO No		
	L3 Other Min Cost	110 CE0		
	Diversel STD	1.50	-	
	Trapport		-	
	Protocol SIDS		Ť	
	Certificate Droforena	ТСР		
	Root Certificate File N	TLS		
	Customized Certificat			
	Certificate File Name			
	Private Key File Name			
				$\nabla$

• Select Line Properties under the General section

Þ

rop	erties		₹ >
Vo	IPControlStatus1		
	ianlass Duan aution	DCD Duese subine	
	Isplay Properties	DSP Properties	
	Configuration	•	
	Allocated to unit	1	
	Fixed in unit	False	
	Instance Tag	VoIPControlStatus1	
	General	•	
	Country	USA	
	Line Properties		
	Network General	•	
	VLAN	Disabled	
	VLAN Id		
	DHCP	Disabled	
	Domain		
	IP Address	10.64.40.238	
	Netmask	255.255.255.0	
	Gateway	10.64.40.1	
	Primary DNS	0.0.0	
	Secondary DNS	0.0.0	
	Network Time	V	
	Time Synchronization Mode	SNTP	
	Synchronized Time		
	SNTP Address		
	Daylight Savings Time	Disabled	
	Time Synchronization Inter	64	
	Time Zone	(GMT-08:00) Pacific Time (	
	Network Provisioning Serv	ver 🔻	
	TFTP Server Mode	None	
	TFTP Server Address		
	DHCP Custom Option	150	
	Network Ethernet	•	
	Ethernet Speed	Auto	
	Duplex	Full	
	Pad Short Frame	Yes	
	Accept Short Frame	Yes	
	QoS	V	
	Mode	DiffServ	
	1.2 Other Hear Driority		

• From the Line Properties page, click the **Protocol** tab.

VoIP Line Properties		
Line 1 Line 2		
General Protocol Quality of Service NAT		
Tones		
DTMF Transmit Level -6.0		
Call Features		
Auto Answer Enabled		
Caller Id Enabled		
Use One Audio Format Enable		
	OK Cancel	

- From the Protocol page, provide the following information:
  - **SIP User Name** Enter a user created in **Section 6.1**.
  - Authentication User Name Enter a user created in Section 6.1.
  - Authentication Password Enter the password for the user in Section 6.1
  - Proxy Vendor Select Avaya SM
  - **Proxy Address** Enter the IP address of Session Manager.
  - **Proxy Port** Enter either 5060 or 5061.
  - Click on the **OK** button. Default values may be used for all other fields.

Note: Biamp Tesira SVC-2 can provide two inbound extensions (L1 and L2).

VoIP Line Properties			×	
Line 1 Line 2				
Constal - Ousity of Service NAT				
SIP				
SIP User Name	72032	Registration Expiration	3600 seconds	
SIP Display Name	72032,SM	Signaling Port	5060	
SIP Domain Name		T1 Timer	500 ms	
Authentication User Nam	e 72032	Retransmit Timeout	32000 ms	
Authentication Password	•••••	Session Timer	Enabled	
Proxy Vendor	Avaya SM 🔹 🔻	Session Refresher	Auto 🔻	
Proxy Address	10.64.41.42	Session Expiration	1800 seconds	
Proxy Port	5060	Minimum Session Expiration	90 seconds	
Outbound Proxy Address		Prack	None 🔻	
Outbound Proxy Port	5060			
Local Dial Plan	[2-9]11 0T 011xxx.T [0-1][2-9]xxxxx	0xxxx [2-9]xx0xxxxxxxxx [2-9]xx	хT	
		стре		
KTP/SKTP		5122		
Port Start	10000	Keyword		
Port End	14999			
Static RTP Port	Enable			
SRTP	*			
G. 723 Encoding Rate	5.3 🔻 kops			
			OKCancel	

### 8. Verification Steps

The following steps may be used to verify the configuration:

- Verify that Biamp Tesira SVC-2 successfully registers with the Session Manager server by navigating to Home → Elements → Session Manager → System Status → User Registrations System Manager.
- Place calls to and from Biamp Tesira SVC-2 and verify that the calls are successfully established with two-way talk path.

# 9. Conclusion

Biamp Tesira SVC-2 was compliance tested with Avaya Aura® Communication Manager R6.3 and Avaya Aura® Session Manager R6.3. Compliance testing between Biamp and Avaya Aura® Session Manager and Avaya Aura® Communication Manager was successful as per the tests outlined in **Section 2**.

## 10. Additional References

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

- [1] Administering Avaya Aura® Communication Manager, Release 6.3, October 2013, Issue 9,Document Number 03-300509
- [2] Administering Avaya Aura® Session Manager, Release 6.3, October 2013, Issue 3, Document Number03-603324
- [3] Administering Avaya Aura® System Manager, Release 6.3, October 2013, Issue 3

The following document was provided by Biamp.

[4] Tesira Operation Manual, Document.

#### ©2014 Avaya Inc. All Rights Reserved.

Avaya and the Avaya Logo are trademarks of Avaya Inc. All trademarks identified by  $\mathbb{R}$  and  $^{TM}$  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.