



## **Configuring SIP Trunks Among Avaya Aura® Communication Manager 6.0.1, Avaya Aura® Session Manager 6.1, and Avaya Aura® Session Border Controller 6.0 – Issue 1.0**

### **Abstract**

These Application Notes describe the steps required to configure SIP trunks between Avaya Aura® Session Border Controller 6.0, Avaya Aura® Communication Manager Evolution Server 6.0.1 and Avaya Aura® Session Manager 6.1.

The main function of Avaya Aura® Session Border controller is to protect private network from outside intrusion by topology hiding. It does NAT translations for SIP and Media traffic for inbound and outbound calls. It supports SIP traffic on UDP, TCP and TLS protocols.

<b>1.</b>	<b>INTRODUCTION.....</b>	<b>4</b>
<b>2.</b>	<b>REFERENCE CONFIGURATION .....</b>	<b>4</b>
<b>3.</b>	<b>EQUIPMENT AND SOFTWARE VALIDATED.....</b>	<b>5</b>
<b>4.</b>	<b>CONFIGURE AVAYA AURA® COMMUNICATION MANAGER EVOLUTION SERVER.....</b>	<b>6</b>
4.1.	VERIFY COMMUNICATION MANAGER LICENSE.....	7
4.2.	CONFIGURE IP NODE NAMES.....	7
4.3.	CONFIGURE IP CODEC SETS .....	8
4.4.	CONFIGURE IP NETWORK REGION .....	8
4.5.	VERIFY IP INTERFACE.....	9
4.6.	ADD SIP SIGNALING GROUP .....	9
4.7.	CONFIGURE A SIP TRUNK GROUP .....	10
4.8.	CONFIGURE ROUTE PATTERN .....	11
4.9.	VIEW CONFIGURED DIAL PLAN .....	11
4.10.	CONFIGURE PUBLIC UNKNOWN NUMBERING .....	12
4.11.	ADMINISTER AAR ANALYSIS .....	12
4.12.	VIEW FEATURE ACCESS CODE .....	13
4.13.	SAVE TRANSLATIONS .....	13
<b>5.</b>	<b>CONFIGURE AVAYA AURA® SESSION MANAGER .....</b>	<b>14</b>
5.1.	SPECIFY SIP DOMAIN .....	16
5.2.	ADD LOCATIONS.....	17
5.3.	ADD SIP ENTITIES.....	19
5.4.	ADD ENTITY LINKS .....	22
5.5.	ADD TIME RANGES .....	24
5.6.	ADD ROUTING POLICIES.....	24
5.7.	ADD DIAL PATTERNS .....	27
<b>6.</b>	<b>CONFIGURE AVAYA AURA® SESSION BORDER CONTROLLER.....</b>	<b>29</b>
6.1.	ACCESSING AVAYA AURA® SESSION BORDER CONTROLLER .....	29
6.2.	CONFIGURING THE ETHERNET INTERFACE .....	32
6.2.1.	<i>Configuring Private Ethernet Interface 0 .....</i>	<i>32</i>
6.2.2.	<i>Administer SIP TCP Configuration On Eth0 .....</i>	<i>33</i>
6.2.3.	<i>Configuring Public Ethernet Interface 2 .....</i>	<i>34</i>
6.2.4.	<i>Administer SIP TCP Configuration On Eth2 .....</i>	<i>35</i>
6.2.5.	<i>Administer Kernel Filter .....</i>	<i>36</i>
6.3.	ADMINISTER ENTERPRISE PBX SERVER .....	38
6.3.1.	<i>Administer SIP TCP Configuration On PBX Server .....</i>	<i>39</i>
6.4.	ADMINISTER ENTERPRISE TELCO SERVER .....	40
6.4.1.	<i>Administer SIP TCP Configuration On TELCO Server .....</i>	<i>41</i>
6.5.	SAVE AND UPDATE CONFIGURATION .....	41
<b>7.</b>	<b>CONFIGURE SERVICE PROVIDER .....</b>	<b>42</b>
<b>8.</b>	<b>VERIFICATION STEPS .....</b>	<b>43</b>
8.1.	VERIFY LINK STATUS ON COMMUNICATION MANAGER .....	43
8.2.	VERIFY LINK STATUS ON SESSION MANAGER.....	44
8.3.	VERIFY PRIVATE AND PUBLIC LINK STATUS ON SESSION BORDER CONTROLLER.....	46
8.4.	MAKE A BASIC TCP CALL .....	46

8.5.	VERIFY CALL LOGS ON SESSION BORDER CONTROLLER.....	47
8.6.	TROUBLESHOOTING POST CONFIGURATION ISSUES.....	49
<b>9.</b>	<b>CONCLUSION .....</b>	<b>52</b>
<b>10.</b>	<b>ADDITIONAL REFERENCES .....</b>	<b>52</b>

# 1. Introduction

Avaya Aura® Session Border Controller secures the IP border for the real time interactive communications that flow from outside to internal network and is a standard element of Avaya's Communication Architecture. The main features are secure SIP voice, and SIP signaling elements against security threats and overloads.

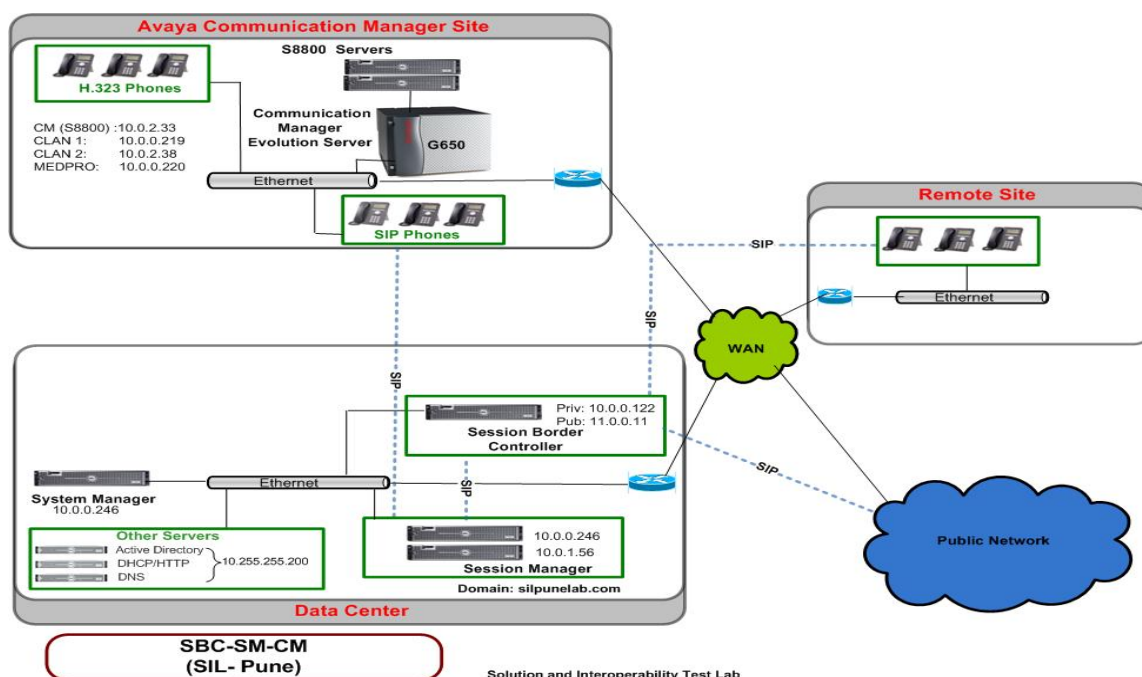
These Application Notes present a sample configuration for a network that connects Avaya Aura® Communication Manager 6.0.1 and Avaya Aura® Session Manager 6.1 with Avaya Aura® Session Border Controller using SIP trunks.

## 2. Reference Configuration

In the sample configuration, Avaya Aura® Communication Manager 6.0.1 runs on an Avaya S8800 Server with Avaya G650 Media Gateway, Avaya Aura® Session Manager 6.1, Avaya Aura® System Manager and Avaya Aura® Session Border Controller 6.0 all runs on an Avaya S8800 Server platform. The sample configuration is shown in **Figure 1**.

The test configuration below shows Communication Manager Site and Data Center as part of private enterprise network. Session Border Controller is located on the edge of private network and controls SIP traffic to and from public network. For the sample configuration, Communication Manager was connected via SIP trunk over the enterprise WAN to simulate a SIP Service Provider.

The current configuration shows Communication Manager and Session Manager connected to Session Border Controller via SIP trunk. On public side Session Border Controller has SIP trunk configured to Communication Manager in simulated public network.



**Figure 1: Test configuration**

### 3. Equipment and Software Validated

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

Hardware Component	Software/Firmware Version
S8800 Media Server	Avaya Aura® Session Manager 6.1.1.0.611023
	Avaya Aura® System Manager 6.1.0 (Build No. - 6.1.0.0.7345-6.1.5.7)
S8800 Server	Avaya Aura® Session Border Controller Release 6.0.0.1.5 (GA build)
S8800 Server with G450 Media Gateway	Avaya Aura® Communication Manager 6.0.1 acting as an Evolution Server. Release: R016x.00.1.510.1
Avaya 9600 Series IP Deskphone.	SIP version 2.6.4 & H.323 version FW3.110b

## 4. Configure Avaya Aura® Communication Manager Evolution Server

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

- Verify Communication Manager license
- Configure IP node names
- Verify IP interfaces
- Configure Codec Set
- Configure Network Region
- Administer a SIP Trunk to Session Manager
- Configure Route Pattern Configure Location and Public Unknown Numbering
- View configured Dial Plan analysis
- Administer AAR Analysis
- Add station(s)
- Save Translations

Throughout this section the administration of Communication Manager is performed using a System Access Terminal (SAT). The following commands are entered on the system with the appropriate administrative permissions. Some administration screens have been abbreviated for clarity.

These instructions assume that the Communication Manager has been installed, configured, licensed and provided with a functional dial plan. Refer to the appropriate documentation as described in references for more details.

## 4.1. Verify Communication Manager License

Use the **display system-parameters customer-options** command. Navigate to **Page 2** and verify that there is sufficient remaining capacity for SIP trunks by comparing the **Maximum Administered SIP Trunks** field value with the corresponding value in the **USED** column. The difference between the two values needs to be greater than or equal to the desired number of simultaneous SIP trunk connections. Verify the highlighted value, as shown below.

display system-parameters customer-options		Page	2 of 11
OPTIONAL FEATURES			
IP PORT CAPACITIES		USED	
Maximum Administered H.323 Trunks:		12000	1129
Maximum Concurrently Registered IP Stations:		18000	14
Maximum Administered Remote Office Trunks:		12000	0
Maximum Concurrently Registered Remote Office Stations:		18000	0
Maximum Concurrently Registered IP eCons:		414	0
Max Concur Registered Unauthenticated H.323 Stations:		100	0
Maximum Video Capable Stations:		18000	5
Maximum Video Capable IP Softphones:		18000	415
<b>Maximum Administered SIP Trunks:</b>		<b>24000</b>	<b>2953</b>
Maximum Administered Ad-hoc Video Conferencing Ports:		24000	18
Maximum Number of DS1 Boards with Echo Cancellation:		522	0
Maximum TN2501 VAL Boards:		128	0
Maximum Media Gateway VAL Sources:		250	0
Maximum TN2602 Boards with 80 VoIP Channels:		128	0
Maximum TN2602 Boards with 320 VoIP Channels:		128	4
Maximum Number of Expanded Meet-me Conference Ports:		300	0

If there is insufficient capacity of SIP Trunks or a required feature is not enabled, contact an authorized Avaya sales representative to make the appropriate changes.

## 4.2. Configure IP Node Names

All SIP signaling with Session Manager is carried through an IP-interface. When configuring a SIP Trunk in Communication Manager, use the IP-address of the Session Manager's SIP Entity interface.

Use the **change node-names ip** command to add the **Name** and **IP Address** for the Session Manager. In the sample configuration, **ASMC** and **10.0.0.246** were used.

change node-names ip		Page	1 of 2
		IP NODE NAMES	
Name	IP Address		
ASMA	10.0.0.247		
<b>ASMC</b>	<b>10.0.0.246</b>		
CLAN_1a04	10.0.0.219		
Clan_1a09	10.0.2.38		
Clan_3a04	10.0.2.126		

### 4.3. Configure IP Codec Sets

Use the command **change ip-codec-set n** command where **n** is the codec set used in the configuration. Enter the following values:

- **Audio Codec** Set for **G.711MU/ G.711A**.
- **Silence Suppression:** Retain the default value **n**.
- **Frames Per Pkt:** Enter **2**.
- **Packet Size (ms):** Enter **20**.

Retain the default values for the remaining fields, and submit these changes.

change ip-codec-set 1				Page	1 of	2
IP Codec Set						
Codec Set: 1						
Audio Codec	Silence Suppression	Frames Per Pkt	Packet Size(ms)			
1: G.711MU	n	2	20			
2: G.711A	n	2	20			

### 4.4. Configure IP Network Region

Use the **change ip-network-region n** command, where **n** is the number of the network region used and set the **Intra-region IP-IP Direct Audio**, and **Inter-region IP-IP Direct Audio** fields to **yes**. For the **Codec Set** enter the corresponding audio codec set configured in previous section. Set the **Authoritative Domain** to the SIP domain. Retain the default values for the remaining fields, and submit these changes.

**Note:** In the test configuration, **network region 1** was used. When creating a new network region or modifying another one, ensure to configure it with the correct parameters.

change ip-network-region 1		Page	1 of	20
IP NETWORK REGION				
Region: 1				
Location: 1		Authoritative Domain: <b>silpunelab.com</b>		
Name: <b>default</b>				
MEDIA PARAMETERS		Intra-region IP-IP Direct Audio: yes		
Codec Set: 1		Inter-region IP-IP Direct Audio: yes		
UDP Port Min: 2048		IP Audio Hairpinning? y		
UDP Port Max: 65535				
DIFFSERV/TOS PARAMETERS				
Call Control PHB Value: 46				
Audio PHB Value: 46				
Video PHB Value: 26				



## 4.5. Verify IP Interface

Use the **change ip-interface procr** command to verify procr interface on Communication Manager to communicate with Session Manager.

change ip-interface procr		Page 1 of 2
IP INTERFACES		
Type: PROCR		
Enable Interface? y		Target socket load: 19660
Network Region: 1		Allow H.323 Endpoints? y
		Allow H.248 Gateways? y
		Gatekeeper Priority: 5
IPV4 PARAMETERS		
Node Name: procr		IP Address:
Subnet Mask: /24		

## 4.6. Add SIP Signaling Group

Use the **add signaling-group n** command, where **n** is an available signaling group number, for one of the SIP trunks to Session Manager, and fill in the indicated fields. Default values can be used for the remaining fields:

- **Group Type:** sip
- **Transport Method:** tcp
- **Peer Detection Enabled?:** y
- **Peer Server:** SM
- **Near-end Node Name:** procr
- **Far-end Node Name:** Session Manager node name from **section 4.2**.
- **Near-end Listen Port:** 5060
- **Far-end Listen Port:** 5060
- **Far-end Network Region:** 1
- **Far-end Domain:** silpunelab.com
- **IMS Enabled?:** n

IMS Enabled? n

add signaling-group 1

Page 1 of 1

SIGNALING GROUP

Group Number: 1

Group Type: sip

IMS Enabled? n

Transport Method: tcp

Q-SIP? n

SIP Enabled LSP? n

IP Video? y

Priority Video? y

Enforce SIPS URI for SRTP? n

Peer Detection Enabled? y

Peer Server: SM

Near-end Node Name: procr

Far-end Node Name: ASMC

Near-end Listen Port: 5060

Far-end Listen Port: 5060

Far-end Network Region: 1

Far-end Secondary Node Name:

Far-end Domain: silpunelab.com

Bypass If IP Threshold Exceeded? n

Incoming Dialog Loopbacks: eliminate

RFC 3389 Comfort Noise? n

DTMF over IP: rtp-payload

Direct IP-IP Audio Connections? y

Session Establishment Timer(min): 3

IP Audio Hairpinning? n

Enable Layer 3 Test? y

Initial IP-IP Direct Media? y

H.323 Station Outgoing Direct Media? n

Alternate Route Timer(sec): 6

## 4.7. Configure a SIP Trunk Group

Add the corresponding trunk group controlled by this signaling group via the **add trunk-group n** command, where **n** is an available trunk group number and fill in the indicated fields.

- **Group Type:** sip
- **Group Name:** A descriptive name
- **TAC:** An available trunk access code i.e., **#01**
- **Service Type:** tie
- **Signaling Group:** signaling group number added in **section 4.6** i.e., **1**
- **Number of Members:** The number of SIP trunks to be allocated to calls routed to Session Manager (must be within the limits of the total trunks available from licensed verified in **section 4.1** )

**Note:** the number of members determines how many simultaneous calls can be processed by the trunk through Session Manager.

add trunk-group 1		Page 1 of 21	
TRUNK GROUP			
Group Number: 1	Group Type: <b>sip</b>	CDR Reports: y	
Group Name: <b>To ASMC</b>	COR: 1	TN: 1	TAC: <b>#01</b>
Direction: two-way	Outgoing Display? n	Night Service:	
Dial Access? n			
Queue Length: 0			
Service Type: <b>tie</b>	Auth Code? n		
Member Assignment Method: auto			
Signaling Group: 1			
Number of Members: 50			

Navigate to **page 3** and change **Numbering Format** to **public**. Use default values for all other fields. Submit these changes.

add trunk-group 1		Page 3 of 21	
TRUNK FEATURES			
ACA Assignment? n	Measured: none		
		Maintenance Tests? y	
<b>Numbering Format: public</b>			
UII Treatment: service-provider			

## 4.8. Configure Route Pattern

Configure a route pattern to correspond to the newly added SIP trunk group. Use **change route pattern n** command, where **n** is an available route pattern. Enter the following values for the specified fields, and retain the default values for the remaining fields. Submit these changes.

- **Pattern Name:** A descriptive name i.e., **to asmc**
- **Grp No:** The trunk group number from **section 4.7**.
- **FLR:** Enter a level that allows access to this trunk, with **0** being least restrictive.

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

## 4.9. View Configured Dial Plan

The system was configured with a 5-digit dialplan. As shown below, dialed strings that begin with 62 with a total length of 4 are assigned to extension numbers. Dialed strings that begin with 61 with a total length of 5 will be routed to Session Border Controller using AAR tables.

Dialplan can be verified with the **display dialplan analysis** command. Note extensions used are in the range 6200-6299 and set 61000-61999 to AAR.

display dialplan analysis										Page	1 of	12
DIAL PLAN ANALYSIS TABLE												
Location: all										Percent Full: 4		
Dialed	Total	Call			Dialed	Total	Call			Dialed	Total	Call
String	Length	Type			String	Length	Type			String	Length	Type
4	4	ext										
61	5	aar										
62	4	ext										
8	1	fac										
9	1	fac										
*	3	fac										
#	3	dac										

## 4.10. Configure Public Unknown Numbering

Use the **change public-unknown-numbering 1** command, to define the calling party number to be sent to Session Border Controller. Add an entry for the trunk group defined in **section 4.7**. In the example shown below, all calls originating from a 4-digit extension beginning with “62” and routed to trunk group 1 will result in a 5-digit calling number. The calling party number will be in the SIP “From” header. Submit these changes.

For Communication Manager:

- **Ext Len:** Number of digits for extension. i.e., **4**
- **Trk Grp:** Trunk group number. i.e., **1**
- **Ext Code:** Enter range for CM extensions. i.e., **62**

change public-unknown-numbering 1					Page	1 of	2
NUMBERING - PUBLIC/UNKNOWN FORMAT							
					Total		
Ext	Ext	Trk	CPN	CPN			
Len	Code	Grp(s)	Prefix	Len			
					Total Administered: 2		
5	62	1		5	Maximum Entries: 9999		

## 4.11. Administer AAR Analysis

This section provides sample Automatic Alternate Routing (AAR) used for routing calls with dialed digits 61xxx to SBC via SM. Note that other methods of routing may be used.

Use the **change aar analysis 0** command and add an entry to specify how to route the calls. Enter the following values for the specified fields and retain the default values for the remaining fields. Submit these changes.

- **Dialed String:** Dialed prefix digits to match on, in this case **61**
- **Total Min:** Minimum number of digits, in this case **5**
- **Total Max:** Maximum number of digits, in this case **5**
- **Route Pattern:** The route pattern number from **section 4.8**. i.e., **1**
- **Call Type:** aar

change aar analysis 6							Page	1 of	2
AAR DIGIT ANALYSIS TABLE									
Location: all							Percent Full: 1		
Dialed		Total		Route		Call		Node	
String		Min Max		Pattern		Type		Num	
61		5 5		1		aar		ANI	
								Reqd	
								n	

## 4.12. View Feature Access Code

To view the Feature-access-code configuration, execute **display feature-access-codes** command note “8” is used as AAR the feature-access-code.

display feature-access-codes	Page 1 of 11
FEATURE ACCESS CODE (FAC)	
Abbreviated Dialing List1 Access Code:	
Abbreviated Dialing List2 Access Code:	
Abbreviated Dialing List3 Access Code:	
Abbreviated Dial - Prgm Group List Access Code:	
Announcement Access Code:	
Answer Back Access Code:	#35
Attendant Access Code:	
<b>Auto Alternate Routing (AAR) Access Code: 8</b>	
Auto Route Selection (ARS) - Access Code 1:	9
Access Code 2:	
Automatic Callback Activation:	*64
Deactivation:	*36
Call Forwarding Activation Busy/DA:	*91 All: *90
Deactivation:	#90
Call Forwarding Enhanced Status:	Act:
Deactivation:	
Call Park Access Code:	#30
Call Pickup Access Code:	*37
CAS Remote Hold/Answer Hold-Unhold Access Code:	
CDR Account Code Access Code:	
Change COR Access Code:	*77
Change Coverage Access Code:	
Conditional Call Extend Activation:	Deactivation:
Contact Closure Open Code:	Close Code:

## 4.13. Save Translations

Configuration of Communication Manager is complete. Use the **save translation** command to save these changes.

save translation	SAVE TRANSLATION
Command Completion Status	Error Code
	Success

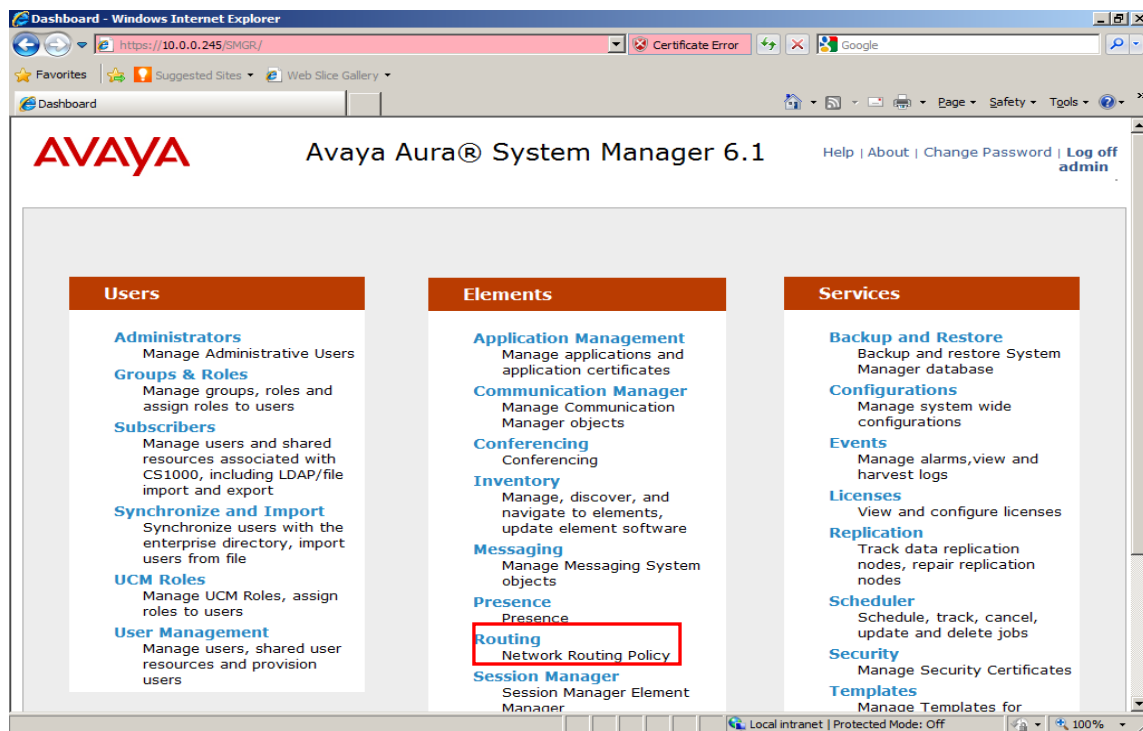
## 5. Configure Avaya Aura® Session Manager

This section provides the procedures for configuring Session Manager, assuming it has been installed and licensed as described in the references. The following steps describe configuration of Session Manager for:

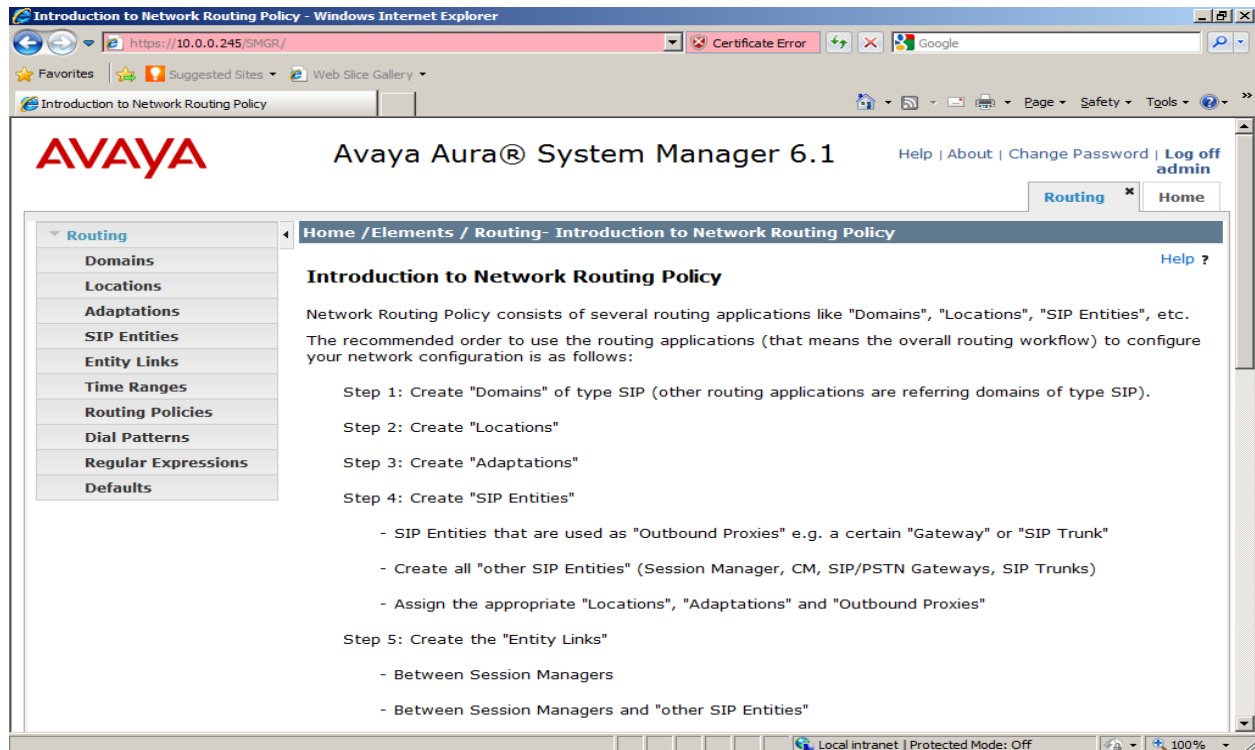
- Access Avaya Aura® Session Manager.
- Add SIP Domain.
- Add Location.
- Administer Avaya Aura® Session Manager SIP Entity.
- Administer Avaya Aura® Communication Manager Evolution Server SIP Entity.
- Administer Avaya Aura® Session Border Controller Entity.
- Administer SIP Entity Link.
- Administer Time ranges.
- Administer Route Policies.
- Administer Dial Pattern.

Configuration is accomplished by accessing the browser-based GUI of System Manager, using the URL **http://<ip-address>/SMGR** where **<ip-address>** is the IP address of System Manager. Log in to the system with valid credentials. The menu shown below is displayed. Click on the **Routing** link as shown in snapshot below. The sub-menus displayed in the left column below will be used to configure all but the last of the above items

Log in to the system with valid credentials. The menu shown below is displayed. Select the **Routing** link in the **Elements** section as shown.



The sub-menus displayed in the left column below will be used to configure call routing for Session Manager.



## 5.1. Specify SIP Domain

Add the SIP domain for which the communications infrastructure will be authoritative. Select **Domains** on the left and clicking the **New** button on the right. The following screens will then be shown. Fill in the following fields and click **Commit**.

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

The first screenshot shows the 'Domain Management' page with a list of 7 existing domains. The 'New' button is highlighted with a red box. The second screenshot shows the 'Add New Domain' form with the 'Name' field containing 'sbc.silpunelab.com' and the 'Type' set to 'sip'. The 'Commit' button is highlighted with a red box.

**Avaya Aura® System Manager 6.1**

Help | About | Change Password | Log off admin

Routing \* Home

Home / Elements / Routing / Domains- Domain Management

**Domain Management**

Edit New Duplicate Delete More Actions

7 Items Refresh Filter: Enable

Name	Type	Default	Notes
<a href="#">cmm.silpunelab.com</a>	sip	<input type="checkbox"/>	Domain for CMM configuration
<a href="#">examplee.com</a>	sip	<input type="checkbox"/>	examplee.com
<a href="#">pune.mango.com</a>	sip	<input type="checkbox"/>	
<a href="#">pune.silpunelab.com</a>	sip	<input type="checkbox"/>	MM-ASM Integration
<a href="#">silpunelab3.com</a>	sip	<input type="checkbox"/>	silpunelab3.com
<a href="#">silpunelab4.com</a>	sip	<input type="checkbox"/>	
<a href="#">silpunelab.com</a>	sip	<input type="checkbox"/>	silpunelab.com

Select : All, None

Local intranet | Protected Mode: Off

**Avaya Aura® System Manager 6.1**

Help | About | Change Password | Log off admin

Routing \* Home

Home / Elements / Routing / Domains- Domain Management

**Domain Management**

Commit Cancel

1 Item Refresh Filter: Enable

Name	Type	Default	Notes
<input type="text" value="sbc.silpunelab.com"/>	sip	<input type="checkbox"/>	<input type="text"/>

\* Input Required

Commit Cancel



## 5.2. Add Locations

Locations can be used to identify logical and/or physical locations where SIP Entities reside, for purposes of bandwidth management. Location is added to the configuration for Communication Manager and Session Border Controller. 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 for Session Border Controller.
- **Notes:** Descriptive text (optional).
- **Managed Bandwidth:** Use the default value.

Under **Location Pattern**:

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

After entering the location details for Session Border Controller, click **Commit** button to save.

The screenshot shows the 'Add Location' configuration page for a Session Border Controller. The page is divided into several sections:

- General:** Contains fields for **Name** (highlighted with a red box, containing 'SBC'), **Notes**, and **Managed Bandwidth** (set to 'Kbit/sec').
- Overall Managed Bandwidth:** Contains fields for **Total Bandwidth**, **Multimedia Bandwidth**, and a checkbox for **Audio Calls Can Take Multimedia Bandwidth** (checked).
- Per-Call Bandwidth Parameters:** Contains fields for **Maximum Multimedia Bandwidth (Intra-Location)** (1000 Kbit/Sec), **Maximum Multimedia Bandwidth (Inter-Location)** (1000 Kbit/Sec), **Minimum Multimedia Bandwidth** (64 Kbit/Sec), and **Default Audio Bandwidth** (80 Kbit/Sec).
- Location Pattern:** Contains a table with one item, **IP Address Pattern** (highlighted with a red box, containing '10.0.0.122').

At the bottom right, there are **Commit** and **Cancel** buttons. A red asterisk indicates that input is required for the highlighted fields.

Add Location for Communication Manager.

Under **General**:

- **Name:** A descriptive name for Communication Manager.
- **Notes:** Descriptive text (optional).
- **Managed Bandwidth:** Use the default value.

Under **Location Pattern**:

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

The screenshot displays the configuration interface for a Communication Manager location. On the left is a sidebar with navigation links: Entity Links, Time Ranges, Routing Policies, Dial Patterns, Regular Expressions, and Defaults. The main content area is divided into two sections: General and Location Pattern.

**General Section:**

- Name:** A text field containing "IBCM", highlighted with a red box.
- Notes:** An empty text field.
- Overall Managed Bandwidth:**
  - Managed Bandwidth Units:** A dropdown menu set to "Kbit/sec".
  - Total Bandwidth:** A text field containing "1000000".
  - Multimedia Bandwidth:** A text field containing "1000000".
  - Audio Calls Can Take Multimedia Bandwidth:** A checkbox that is checked.
- Per-Call Bandwidth Parameters:**
  - Maximum Multimedia Bandwidth (Intra-Location):** A text field containing "1000" Kbit/Sec.
  - Maximum Multimedia Bandwidth (Inter-Location):** A text field containing "1000" Kbit/Sec.
  - Minimum Multimedia Bandwidth:** A text field containing "64" Kbit/Sec.
  - \* Default Audio Bandwidth:** A dropdown menu set to "80" Kbit/sec.

**Location Pattern Section:**

- Add** and **Remove** buttons.
- A table with 1 item, showing the **IP Address Pattern** and **Notes**. The first row has a checkbox, a text field containing "\* 10.0.2.33" (highlighted with a red box), and an empty notes field.
- A "Filter: Enable" link.
- A "Select : All, None" dropdown.
- \* Input Required** label.
- Commit** and **Cancel** buttons.

Verify the Location for Session Manager. Note this configuration is done during installation of Session Manager.

The screenshot shows the Session Manager configuration interface. On the left is a sidebar with links: Entity Links, Time Ranges, Routing Policies, Dial Patterns, Regular Expressions, and Defaults. The main area is titled 'Overall Managed Bandwidth' and contains the following settings:

- Name:** ASMC (highlighted with a red box)
- Notes:** asmc
- Managed Bandwidth Units:** Mbit/sec
- Total Bandwidth:** 100000
- Multimedia Bandwidth:** 4098
- Audio Calls Can Take Multimedia Bandwidth:** ☒

Below this is the 'Per-Call Bandwidth Parameters' section:

- Maximum Multimedia Bandwidth (Intra-Location):** 80 Kbit/Sec
- Maximum Multimedia Bandwidth (Inter-Location):** 90 Kbit/Sec
- Minimum Multimedia Bandwidth:** 64 Kbit/Sec
- \* Default Audio Bandwidth:** 80 Kbit/sec

At the bottom is the 'Location Pattern' section, which includes an 'Add' button, a 'Remove' button, and a table with 6 items. The table has columns for 'IP Address Pattern' and 'Notes'. The last row, with IP address '10.0.0.246', is highlighted with a red box.

IP Address Pattern	Notes
* 15.0.0.15	IPO
* 10.0.*	stations
* 10.0.0.191	cmfs
* 10.0.0.219	ibcm
* 10.0.0.166	vpss
* 10.0.0.246	asmc

### 5.3. Add SIP Entities

A SIP Entity must be added for Session Manager and for each SIP-based telephony system communicating with it using SIP trunks. In the sample configuration, the following SIP entities were added:

- Communication Manager (**IBCM**), and
- Session Border Controller (**SBC**).

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 for Communication Manager.
- **FQDN or IP Address:** IP address of the signaling interface
- **Type:** **CM** for Communication Manager
- **Location:** Select one of the locations defined previously. i.e., **IBCM**
- **Time Zone:** Time zone for this location.

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

The following screen shows the addition of Communication Manager. The IP address used is that of the “procr” as configured in **section 4.5**. Keep **Adaptation** as blank. **Location** is IBCM for Communication Manager

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

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

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

**SIP Entity Details** [Help ?](#) [Commit](#) [Cancel](#)

**General**

\* Name: IBCM

\* FQDN or IP Address: 10.0.0.219

Type: CM

Notes:

Adaptation:

Location: IBCM

Time Zone: Asia/Kolkata

Override Port & Transport with DNS SRV: ☐

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

Credential name:

Call Detail Recording: none

**SIP Link Monitoring**

SIP Link Monitoring: Use Session Manager Configuration

**Entity Links**

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

Done Local intranet | Protected Mode: Off 100%

Note the screen shot below shows configuration of Session Manager. The IP address used is that of the SIP Entity Interface configured on the Session Manager.

The screenshot shows the Avaya Aura System Manager 6.1 interface. The left sidebar contains a navigation menu with options: Routing, Domains, Locations, Adaptations, SIP Entities (highlighted), Entity Links, Time Ranges, Routing Policies, Dial Patterns, Regular Expressions, and Defaults. The main content area is titled 'SIP Entity Details' and includes a breadcrumb trail: Home / Elements / Routing / SIP Entities- SIP Entity Details. Below this, the 'General' tab is active, showing configuration fields for a SIP entity named 'avaya-asmc'. The fields are: Name (avaya-asmc), FQDN or IP Address (10.0.0.246), Type (Session Manager), Notes (empty), Location (ALL), Outbound Proxy (empty), Time Zone (Asia/Kolkata), and Credential name (empty). Below the General tab is the 'SIP Link Monitoring' section with a dropdown set to 'Use Session Manager Configuration'. At the bottom, the 'Entity Links' section shows a table with 24 items, filtered to 'Enable'. The table has columns: SIP Entity 1, Protocol, Port, SIP Entity 2, Port, and Trusted. The first row shows 'avaya-asmc' connected to 'ABG' via TCP on port 5060, marked as trusted.

For Session Manager, there is additional Port configuration as shown below.

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

The screenshot shows a detailed view of the Port configuration table. The table has columns: Port, Protocol, Default Domain, and Notes. There are two items listed: one for port 5060 using TCP with default domain 'silpunelab.com', and another for port 5061 using TLS with the same default domain. Below the table, there are 'Add' and 'Remove' buttons, and a 'Select: All, None' option. The table is filtered to 'Enable'.

Port	Protocol	Default Domain	Notes
5060	TCP	silpunelab.com	
5061	TLS	silpunelab.com	

The following screen shows the addition of Session Border Controller.

- **Name:** A descriptive name for Session Border Controller.
- **FQDN or IP Address:** IP address of the signaling interface
- **Type:** SIP Trunk
- **Location:** Select one of the locations defined previously. i.e., **SBC**
- **Time Zone:** Time zone for this location.

The screenshot displays the Avaya Aura System Manager 6.1 web interface. The top navigation bar includes the Avaya logo, the product name 'Avaya Aura® System Manager 6.1', and links for 'Help', 'About', 'Change Password', and 'Log off admin'. A breadcrumb trail shows 'Home / Elements / Routing / SIP Entities- SIP Entity Details'. On the left, a sidebar menu lists various configuration areas: Routing, Domains, Locations, Adaptations, SIP Entities (highlighted), Entity Links, Time Ranges, Routing Policies, Dial Patterns, Regular Expressions, and Defaults. The main content area is titled 'SIP Entity Details' and has a 'General' tab selected. It contains several input fields: 'Name' (set to 'SBC'), 'FQDN or IP Address' (set to '10.0.0.122'), 'Type' (set to 'SIP Trunk'), 'Notes' (empty), 'Adaptation' (empty), 'Location' (set to 'ALL'), and 'Time Zone' (set to 'Asia/Kolkata'). There is an unchecked checkbox for 'Override Port & Transport with DNS SRV:'. Below this, 'SIP Timer B/F (in seconds)' is set to '4', 'Credential name' is empty, and 'Call Detail Recording' is set to 'egress'. A 'SIP Link Monitoring' section has a dropdown set to 'Use Session Manager Configuration'. At the bottom, there is an 'Entity Links' section with 'Add' and 'Remove' buttons. The bottom status bar shows 'Done', 'Local intranet | Protected Mode: Off', and a zoom level of '100%'.

## 5.4. Add Entity Links

A SIP trunk between Session Manager and a telephony system 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.
- **SIP Entity 1:** Select the Session Manager entity.
- **Port:** Port number to which the other system sends SIP requests
- **SIP Entity 2:** Select the name of the other system.
- **Port:** Port number on which the other system receives SIP requests. These ports should match SIP signaling ports.

- **Trusted:** Check this box. **Note:** If this box is not checked, calls from the associated SIP Entity will be denied.
- **Protocol:** Select the transport protocol among **UDP/TCP/TLS**. Check these are aligned with the definition on the other end of the link. In the example, **TCP** is used.

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

The following screen illustrates adding the Entity Link for Communication Manager.

The screenshot shows the Avaya Aura System Manager 6.1 interface. The left sidebar contains a navigation menu with options: 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 'Home / Elements / Routing / Entity Links- Entity Links'. It features a 'Commit' button and a 'Cancel' button. Below this is a table with the following columns: Name, SIP Entity 1, Protocol, Port, SIP Entity 2, Port, and Trust. The table contains one item: 'avaya-asmc\_IBCM\_S', 'avaya-asmc', 'TCP', '5060', 'IBCM', '5060', and a checked 'Trust' box. A red box highlights the entire row. Below the table, there is a '\* Input Required' message and another 'Commit' and 'Cancel' button.

Name	SIP Entity 1	Protocol	Port	SIP Entity 2	Port	Trust
avaya-asmc_IBCM_S	avaya-asmc	TCP	5060	IBCM	5060	<input checked="" type="checkbox"/>

Below is illustrated adding the Entity Link for Session Border Controller.

The screenshot shows the Avaya Aura System Manager 6.1 interface. The left sidebar contains a navigation menu with options: 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 'Home / Elements / Routing / Entity Links- Entity Links'. It features a 'Commit' button and a 'Cancel' button. Below this is a table with the following columns: Name, SIP Entity 1, Protocol, Port, SIP Entity 2, Port, and Trust. The table contains one item: 'avaya-asmc\_ASMC\_S', 'avaya-asmc', 'TCP', '5060', 'SBC', '5060', and a checked 'Trust' box. A red box highlights the entire row. Below the table, there is a '\* Input Required' message and another 'Commit' and 'Cancel' button.

Name	SIP Entity 1	Protocol	Port	SIP Entity 2	Port	Trust
avaya-asmc_ASMC_S	avaya-asmc	TCP	5060	SBC	5060	<input checked="" type="checkbox"/>

## 5.5. Add Time Ranges

Before adding routing policies (see next section), time ranges must be defined during which the policies will be active. In the sample configuration, one policy was defined that would allow routing to occur at anytime. To add this time range, select **Time Ranges** on the center of the Time Ranges page under the heading, click on the **New** button (not shown). Fill in the following:

- **Name:** A descriptive name (e.g., 24/7).
- **Mo through Su** Check the box under each of these headings
- **Start Time** Enter **00:00**.
- **End Time** Enter **23:59**

Click **Commit** to save this time range.

AVAYA Avaya Aura® System Manager 6.1 Help | About | Change Password | Log off admin

Routing x Home

Home / Elements / Routing / Time Ranges- Time Ranges

Time Ranges

Commit Cancel

1 Item Refresh Filter: Enable

Name	Mo	Tu	We	Th	Fr	Sa	Su	Start Time	End Time	Notes
24/7	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	* 00:00	* 23:59	Time Range 24/7

\* Input Required

Commit Cancel

## 5.6. Add Routing Policies

Routing policies describe the conditions under which calls will be routed to the SIP Entities specified in **section 5.3**. Two routing policies must be added – first for Communication Manager and second for Session Border Controller.

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**:

- **Name:** Enter a descriptive name for the Communication Manager policy.

Under **SIP Entity as Destination**:

- Click **Select**, and then select the appropriate SIP entity created for Communication Manager.

Under **Time of Day**:

- Click **Add**, and select the time range configured in the previous section.



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

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

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

**Home / Elements / Routing / Routing Policies- Routing Policy Details**

**Routing Policy Details** [Help ?](#) [Commit](#) [Cancel](#)

**General**

\* Name:

Disabled: ☐

Notes:

**SIP Entity as Destination**

[Select](#)

Name	FQDN or IP Address	Type	Notes
To IBCM	10.0.0.219	CM	

**Time of Day**

[Add](#) [Remove](#) [View Gaps/Overlaps](#)

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

<input type="checkbox"/>	Ranking 1 ▲	Name 2 ▲	Mon	Tue	Wed	Thu	Fri	Sat	Sun	Start Time	End Time	Notes
<input type="checkbox"/>	0	24/7	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	00:00	23:59	Time Range 24/7

Select : All, None

**Dial Patterns**

Under **General**:

- **Name**: Enter a descriptive name for Session Border Controller policy.

Under **SIP Entity as Destination**:

- Click **Select**, and then select the appropriate SIP entity created for Session Border Controller.

Under **Time of Day**:

- Click **Add**, and select the time range configured in the previous section.

Defaults can be used for the remaining fields. Click **Commit** to save the Routing Policy definition. Below is illustrated the Routing Policy for Session Border Controller, configured in these sample application notes.

The screenshot shows the Avaya Aura System Manager 6.1 interface. The left sidebar contains a navigation menu with options: 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 'Home / Elements / Routing / Routing Policies- Routing Policy Details'. It includes a 'Routing Policy Details' section with a 'General' tab. The 'Name' field is set to 'To SBC', 'Disabled' is unchecked, and 'Notes' is 'route to SBC'. Below this is the 'SIP Entity as Destination' section with a 'Select' button and a table listing SIP entities. The table has columns: Name, FQDN or IP Address, Type, and Notes. One entry is 'SBC' with FQDN '10.0.0.122' and Type 'SIP Trunk'. The 'Time of Day' section includes 'Add', 'Remove', and 'View Gaps/Overlaps' buttons. It shows a table with 1 item, a 'Filter: Enable' dropdown, and columns for Ranking, Name, and days of the week. The 'Name' field is set to '24/7'. The 'Dial Patterns' section is visible at the bottom.

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

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

Home / Elements / Routing / Routing Policies- Routing Policy Details [Help ?](#)

**Routing Policy Details** [Commit](#) [Cancel](#)

**General**

\* Name:

Disabled: ☐

Notes:

**SIP Entity as Destination**

[Select](#)

Name	FQDN or IP Address	Type	Notes
SBC	10.0.0.122	SIP Trunk	

**Time of Day**

[Add](#) [Remove](#) [View Gaps/Overlaps](#)

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

<input type="checkbox"/>	Ranking 1	Name 2	Mon	Tue	Wed	Thu	Fri	Sat	Sun	Start Time	End Time	Notes
<input type="checkbox"/>	0	24/7	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	00:00	23:59	Time Range 24/7

Select : All, None

**Dial Patterns**

Done Local intranet | Protected Mode: Off 100%

## 5.7. Add Dial Patterns

Dial patterns must be defined that will direct calls to the appropriate SIP Entity. In the sample configuration, 4-digit extensions beginning with **62** reside on Communication Manager and 5-digit starting with **61** will be routed to Session Border Controller. 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, as shown in the screen below, which corresponds to the dial pattern for routing calls to Communication Manager:

Under **General**:

- **Pattern:** Dialed number or prefix.
- **Min:** Minimum length of dialed number.
- **Max:** Maximum length of dialed number.
- **Notes:** Comment on purpose of dial pattern.

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 definitions for Communication Manager.

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

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

[Home / Elements / Routing / Dial Patterns- Dial Pattern Details](#)

**Dial Pattern Details** [Help ?](#) [Commit](#) [Cancel](#)

**General**

\* Pattern:

\* Min:

\* Max:

Emergency Call: ☐

SIP Domain:

Notes:

**Originating Locations and Routing Policies**

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

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

<input type="checkbox"/>	Originating Location Name 1 ▲	Originating Location Notes	Routing Policy Name	Rank 2 ▲	Routing Policy Disabled	Routing Policy Destination	Routing Policy Notes
<input type="checkbox"/>	ALL	ALL	To IBCM	0	<input type="checkbox"/>	IBCM	

Select : All, None

**Denied Originating Locations**

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

The following screen shows the dial pattern definitions for Session Border Controller.

- **Pattern:** 61
- **Min** 5
- **Max** 5
- **Notes** optional descriptive text.

The screenshot displays the Avaya Aura System Manager 6.1 interface. The left sidebar shows a navigation menu with 'Routing' selected. The main content area is titled 'Dial Pattern Details' and includes a 'General' section with the following fields: 'Pattern' (61), 'Min' (5), 'Max' (5), 'Emergency Call' (unchecked), 'SIP Domain' (-ALL-), and 'Notes' (To SBC). Below this is a table titled 'Originating Locations and Routing Policies' with one item: 'ALL' with 'ALL' as the location, 'To SBC' as the policy, and 'route to SBC' as the notes. The table also includes columns for 'Rank' (0), 'Routing Policy Disabled' (unchecked), and 'Routing Policy Destination' (SBC). The bottom section is titled 'Denied Originating Locations' and is currently empty.

**Avaya Aura® System Manager 6.1**

Help | About | Change Password | Log off admin

Routing x Home

Home / Elements / Routing / Dial Patterns- Dial Pattern Details

**Dial Pattern Details**

Commit Cancel Help ?

**General**

\* Pattern: 61

\* Min: 5

\* Max: 5

Emergency Call: ☐

SIP Domain: -ALL-

Notes: To SBC

**Originating Locations and Routing Policies**

Add Remove

1 Item Refresh Filter: Enable

<input type="checkbox"/>	Originating Location Name 1 ▲	Originating Location Notes	Routing Policy Name	Rank 2 ▲	Routing Policy Disabled	Routing Policy Destination	Routing Policy Notes
<input type="checkbox"/>	ALL	ALL	To SBC	0	<input type="checkbox"/>	SBC	route to SBC

Select : All, None

**Denied Originating Locations**

Add Remove

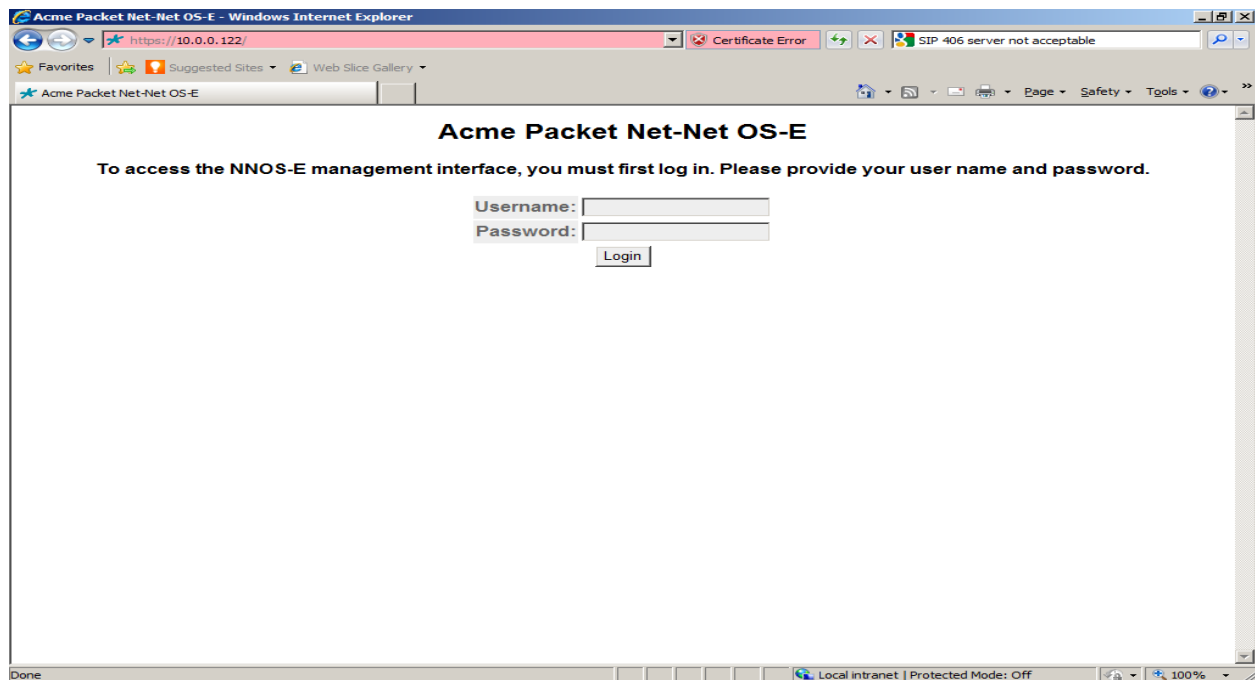
## 6. Configure Avaya Aura® Session Border Controller

This section provides the procedures for configuring Session Border Controller, assuming it has been installed and licensed as described in the references. The following steps describe configuration of Session Border Controller for:

- Access Avaya Aura® Session Border Controller
- Administer Ethernet Interfaces
  - Administer Ethernet private interface on eth0
  - Administer SIP TCP configuration on eth0
  - Administer public interface on eth2
  - Administer SIP TCP configuration on eth2
- Administer Enterprise PBX server
  - Administer SIP TCP configuration on PBX server
- Administer Enterprise TELCO server
  - Administer SIP TCP configuration on TELCO server

### 6.1. Accessing Avaya Aura® Session Border Controller

To access the Session Border Controller configuration use the browser-based GUI using the URL `http://<ip-address>` where `<ip-address>` is the IP-address of Session Border Controller configured on eth0 interface. Log in to the system with valid credentials.



The Home page for Session Border Controller configuration is shown below.

AVAYA aura acme packet powered

Logout admin

Home Configuration Status Call Logs Event Logs Actions Services Keys Access Tools

Get summary for: **Box 1** Refresh Help

<b>box-identifier</b>	0175-8833-83ce-b34c	
<b>box-status</b>	IPAddress State build-version build-number	LocalBox (10.0.0.122) Connected E362P1 47121
<b>master-services</b>	database	
<b>up-time</b>	time timezone uptime	16:31:32 Mon 2011-02-14 IST 5 days 20:40:38
<b>system-info</b>	cpu-usage-one-second	0%
<b>call-info</b>	active-calls	0
<b>location-info</b>	total-cache-entries location-bindings	0 0
<b>registration-info</b>	total-nonlocal-registrations total-terminated total-declined	0 0 7

Done Local intranet | Protected Mode: Off 100%

To access the configuration, click on **Configuration** tab. The web page shows two main nodes **cluster** and **vsp** as shown in left frame. By default cluster has single box configured on it. To view box configuration click on it.

**Note:** To update and save configuration for all the menus, click on **set** button after making changes.

AVAYA aura acme packet powered

Status Summary Logout admin

Home Configuration Status Call Logs Event Logs Actions Services Keys Access Tools

**Configuration: all**

Configuration Setup View

- cluster
  - box:punesbc.silpunelab.com
- vsp

**Configuration Loaded**

The configuration has been successfully loaded.

The box configuration is shown below has two Ethernet interfaces configured.

**Configuration: all**

Configuration | Setup | View

cluster  
box:punesbc.silpunelab.com

**Configure cluster\box:punesbc.silpunelab.com** Show advanced Help Index

Set Reset Back Copy Delete

\* number 1 (from 1 to 16)

admin enabled (Resource is active)

hostname punesbc.silpunelab.com (host name or n.n.n.n)

timezone enter Asia/Kolkata or select from Alaska (See Status tab System timezones for complete list)

name punesbc.silpunelab.com

description Acme Packet Net-Net OS

contact

location

identifier 00:CA:FE:64:92:34

interface	admin	mtu	arp	speed	duplex	autoneg	ip	vlan
<a href="#">Edit</a> <a href="#">Delete</a> interface_eth0	enabled	1500	enabled	1Gb	full	enabled	<a href="#">Edit</a> <a href="#">Configure</a>	
<a href="#">Edit</a> <a href="#">Delete</a> interface_eth2	enabled	1500	enabled	1Gb	full	enabled	<a href="#">Edit</a> <a href="#">Configure</a>	

[Add interface](#)

bootp-client [Configure](#)

ntp-client [Configure](#)

**Note:** The hostname, timezone and the Ethernet interfaces are configured during installation of the system.

## 6.2. Configuring the Ethernet Interface

Session Border Controller sits on the edge of enterprise network. The main functionality is similar to NAT and firewall is to protect private network from intrusion from public network. It has two Ethernet interfaces one configured in private network and other in public network. Session Border Controller performs the network address translation for SIP messages and media translations going from private to public or vice-versa.

### 6.2.1. Configuring Private Ethernet Interface 0

The private Ethernet interface has an IP-address in the range of addresses in the private network. Verify the IP-address and net-mask assigned to the interface.

The screenshot displays the Avaya Aura Configuration web interface. On the left, a navigation tree under 'Configuration: all' shows the path: cluster > box:punesbc.silpunelab.com > interface eth0. The main panel is titled 'Configure cluster:box:punesbc.silpunelab.com/interface eth0'. It contains several configuration fields: 'name' (eth0), 'admin' (enabled), 'mtu' (1500), 'arp' (enabled), 'speed' (1Gb), 'duplex' (full), and 'autoneg' (enabled). Below these is a table for IP addresses. The first row is highlighted with a red box, showing 'ip inside' with a static IP of 10.0.0.122/22. The table has columns for ip, admin, ip-address, geolocation, security-domain, address-scope, filter-intf, media-ports, metric, and class tag. At the bottom, there are links for 'Add ip' and 'Add vlan'. The interface also includes a status bar at the bottom showing 'Local intranet | Protected Mode: Off'.

ip	admin	ip-address	geolocation	security-domain	address-scope	filter-intf	media-ports	metric	class tag
ip inside	enabled	static 10.0.0.122/22	0			disabled	20000 5000 enabled	1	

Click on **ip inside** node and configure ICMP protocol. Select ICMP link as shown in snapshot below. Verify the IP-address for private interface is pingable from private network after completing entire configuration for Session Border Controller.



Make following changes to ICMP configuration.

- **admin:** enabled
- **rate:** 10

The screenshot shows the AVAYA aura Configuration page. The left sidebar shows a tree view of the configuration hierarchy: cluster > box:punesbc.silpunelab.com > interface eth0 > ip inside > icmp. The 'icmp' item is highlighted with a red box. The main content area shows the configuration for 'Configure clusterbox:punesbc.silpunelab.com/interface eth0/ip inside/icmp'. The 'admin' dropdown is set to 'enabled' (highlighted with a red box) and the 'rate' is set to '10' (also highlighted with a red box). The 'limit' section is expanded, showing 'rate' as '10 per second(from 1 to 10,000)'. Buttons for 'Set', 'Reset', 'Back', and 'Delete' are visible.

## 6.2.2. Administer SIP TCP Configuration On Eth0

To configure TCP SIP trunk for private interface, click on interface eth0 from left frame and then click on SIP link. Click on add TCP port.

The screenshot shows the AVAYA aura Configuration page. The left sidebar shows a tree view of the configuration hierarchy: cluster > box:punesbc.silpunelab.com > interface eth0 > ip inside > sip. The 'sip' item is highlighted with a red box. The main content area shows the configuration for 'Configure clusterbox:punesbc.silpunelab.com/interface eth0/ip inside/sip'. The 'admin' dropdown is set to 'enabled'. The 'nat-translation' dropdown is set to 'disabled'. The 'nat-add-received-from' dropdown is set to 'disabled'. The 'nat-add-X-Remote-Info' dropdown is set to 'enabled'. The 'load-balance-head-end' dropdown is set to 'false'. The 'udp-port' section shows a table with columns: udp-port, from-server, to-server, transport, remote-port, and certificate. The 'tcp-port' section shows a table with columns: tcp-port, from-server, to-server, transport, remote-port, and certificate. The 'Add tcp-port' link is highlighted with a red box. The 'tls-port' section shows a table with columns: tls-port, from-server, to-server, transport, remote-port, and certificate. The 'Add tls-port' link is visible at the bottom.

Make following changes to the configuration and click on set to save configuration.

- **Port:** 5060
- **Transport:** TCP

**Configuration: all**

Configuration Setup View

cluster

- box:punesbc.silpunelab.com
  - interface eth0
    - ip inside
      - ssh
      - snmp
      - web
      - web-service
      - sip
      - icmp
      - media-ports
    - routing
    - interface eth2
      - cli
- vsp
  - default-session-config
  - tls
  - policies
  - session-config-pool
  - dial-plan
  - registration-plan

**Configure clusterbox:punesbc.silpunelab.com\interface eth0\ip inside\sip\tcp-port 5060** [Help](#) [Index](#)

Set Reset Back Copy Delete

\* port 5060 (at minimum 1,default=5060)

from-server

to-server

transport TCP (Transmission Control Protocol)

remote-port 0 (from 0 to 65,535)

certificate

Set Reset Back Copy

[Help](#) [Index](#)

### 6.2.3. Configuring Public Ethernet Interface 2

The public Ethernet interface eth2 has an IP-address in the range of addresses in the public network. Verify the IP-address and net-mask assigned to the interface.

**Configuration: all**

Configuration Setup View

cluster

- box:punesbc.silpunelab.com
  - interface eth0
    - ip inside
      - ssh
      - snmp
      - web
      - web-service
      - sip
      - icmp
      - media-ports
    - routing
    - interface eth2
      - ip outside
        - sip
        - icmp
        - media-ports
      - routing
        - route Default
        - route external
        - route cm-outs
        - proxy tcp 80
        - proxy tcp 443
      - kernel-filter
        - allow-rule allo
        - deny-rule den
    - cli
  - vsp
    - default-session-config
    - tls
    - policies
    - session-config-pool
    - dial-plan
    - registration-plan
    - enterrise

**Configure clusterbox:punesbc.silpunelab.com\interface eth2** [Help](#) [Index](#)

Set Reset Back Delete

\* name eth2 (ethernet interface 2)

admin enabled (Resource is active)

mtu 1500 (from 100 to 1,500,default=1500)

arp enabled (Resource is active)

speed 1Gb

duplex full (Full duplex)

autoneg enabled (Resource is active)

	ip	admin	ip-address	geolocation	security-domain	address-scope	filter-intf	media-ports	metric	clas tag
Edit Delete	ip outside	enabled	static	0			disabled	enabled	1	
			11.0.0.11/24					20000		
								5000		
								enabled		
								Edit		

[Add ip](#)

[vlan](#) [Add vlan](#)

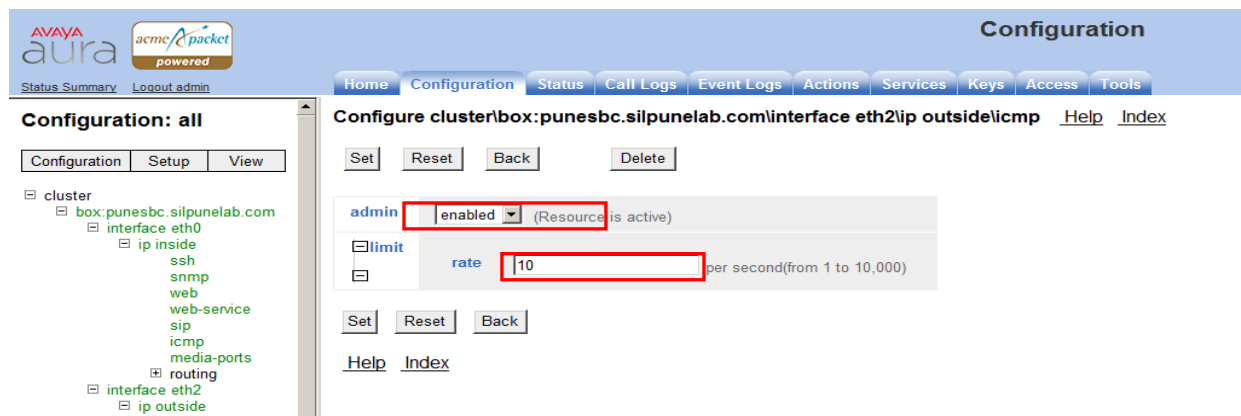
Set Reset Back

Done Local intranet | Protected Mode: Off 100%

Click on **ip outside** node and configure ICMP protocol as shown in snapshot below. Verify the IP-address for public interface is pingable from public network. Note the public and private network are configured in different subnets.

Make following changes to ICMP configuration.

- **admin:** enabled
- **rate:** 10

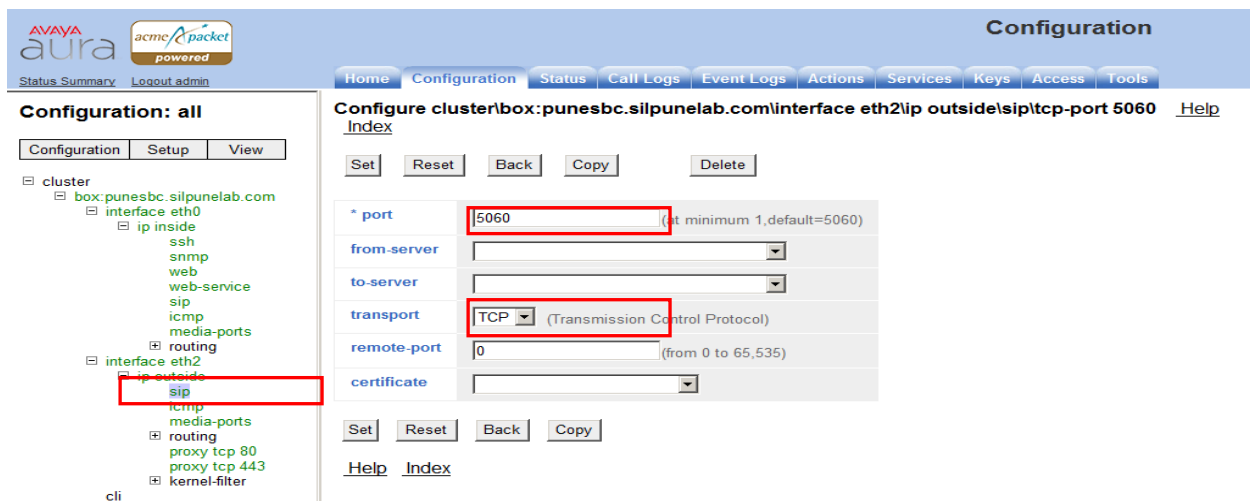


## 6.2.4. Administer SIP TCP Configuration On Eth2

To configure TCP SIP trunk for public interface, click on interface eth0 from left frame and then click on SIP link. Click on add TCP port.

Make following changes to the configuration and click on set to save configuration.

- **Port:** 5060
- **Transport:** TCP



## 6.2.5. Administer Kernel Filter

Kernel filtering is by default enabled on the outside network to restrict the traffic from the public network entering Session Border Controller. This is similar to Linux kernel firewall **iptables**, which allow or restrict traffic to and from Session Border Controller to public network. There are two types of rules defined in filter Allow and Deny.

Allow rule allows specific type of traffic to enter Session Border Controller based on protocol and port selection. And Deny rule restricts generically all other or specific type of traffic to enter Session Border Controller based on protocol and port selection.

Select kernel-filter node under ip outside and make following changes to Allow rule.

- **Protocol:** This is to make sure all SIP TCP traffic is allowed.
- **Port:** The port configured on Eth2 interface for Telco sip Trunk.
- **Source-address/mask:** Specify the public network range.

The screenshot displays the Avaya Aura Configuration web interface. On the left, a tree view shows the configuration hierarchy: cluster > box:punesbc.silpunelab.com > interface eth0 > ip inside > routing > media-ports > interface eth2 > ip outside > routing > proxy tcp 80 > proxy tcp 443 > kernel-filter. The main panel is titled 'Configure cluster:box:punesbc.silpunelab.com/interface eth2/ip outside/kernel-filter/allow-rule allow-sip-tcp-from-peer-1'. It contains a form with the following fields: 'name' (allow-sip-tcp-from-peer-1), 'admin' (enabled), 'destination-port' (5060), 'source-address/mask' (11.0.0.0/24), 'source-port' (0), and 'protocol' (tcp). Each of these fields is highlighted with a red rectangle. At the bottom of the form, there are buttons for 'Set', 'Reset', 'Back', and 'Copy', along with links for 'Help' and 'Index'.

Make following changes to **Deny** rule to restrict any other traffic from entering Session Border Controller from public network.

The screenshot shows the Avaya Aura Configuration web interface. The browser address bar indicates the URL is `https://10.0.0.122/config?type=system`. The page title is "Configure clusterbox:punesbc.silpunelab.cominterface eth2lip outsidekernel-filterdeny-rule deny-all-sip". The left sidebar shows a tree view of the configuration hierarchy, with "deny-rule deny" selected. The main content area displays the configuration for the "deny-all-sip" rule. The configuration fields are as follows:

Field	Value
* name	deny-all-sip
admin	enabled (Resource is active)
destination-port	5060 (from 0 to 65,535)
* source-address/mask	0.0.0.0/0 (n.n.n.n/n)
source-port	0 (from 0 to 65,535)
protocol	all (All protocol types)

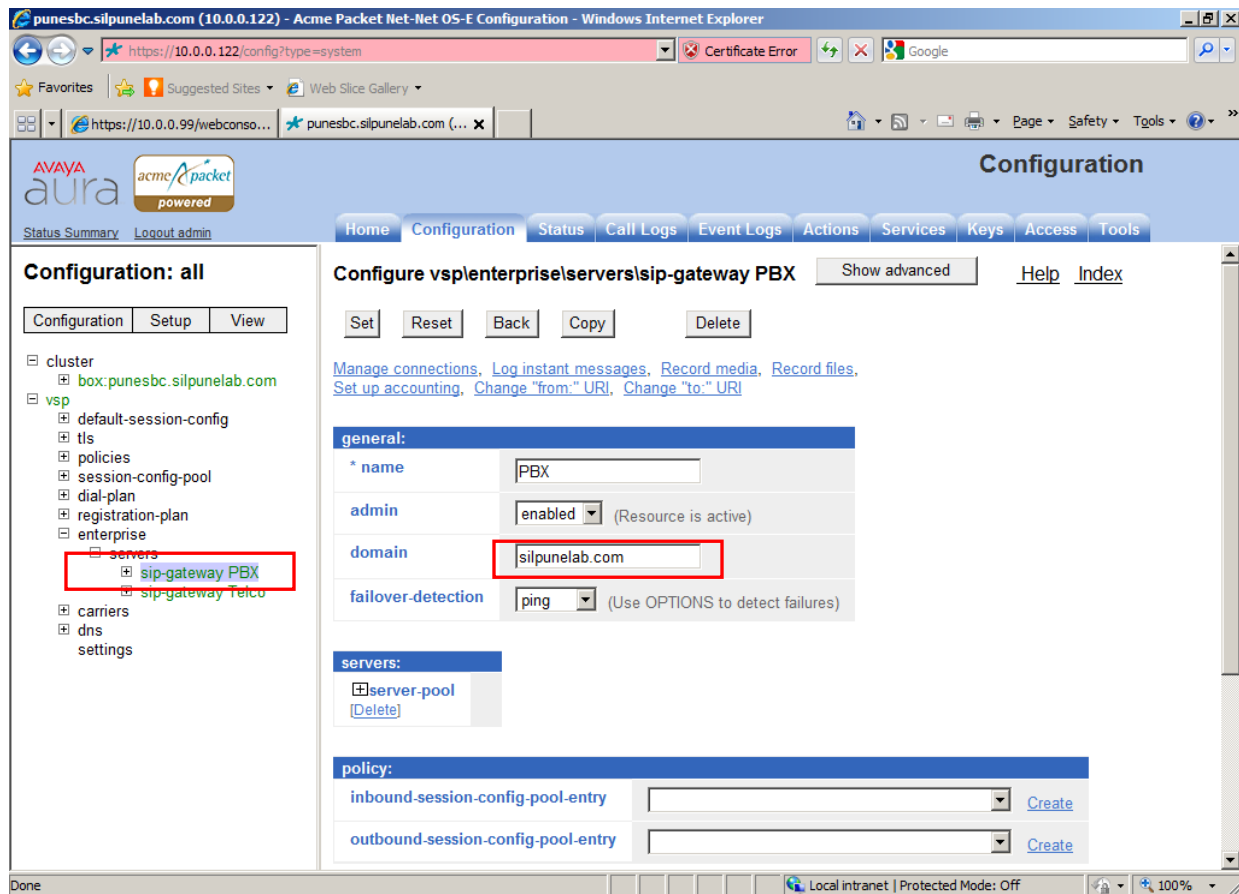
Buttons for "Set", "Reset", "Back", "Copy", and "Delete" are visible above and below the configuration fields. The "Help" and "Index" links are at the bottom of the configuration area.

### 6.3. Administer Enterprise PBX Server

PBX enterprise server configuration is required to create link to Session Manager. Go to **vsp** node and click on Enterprise. Select sip-gateway PBX to update configuration.

Enter following details:

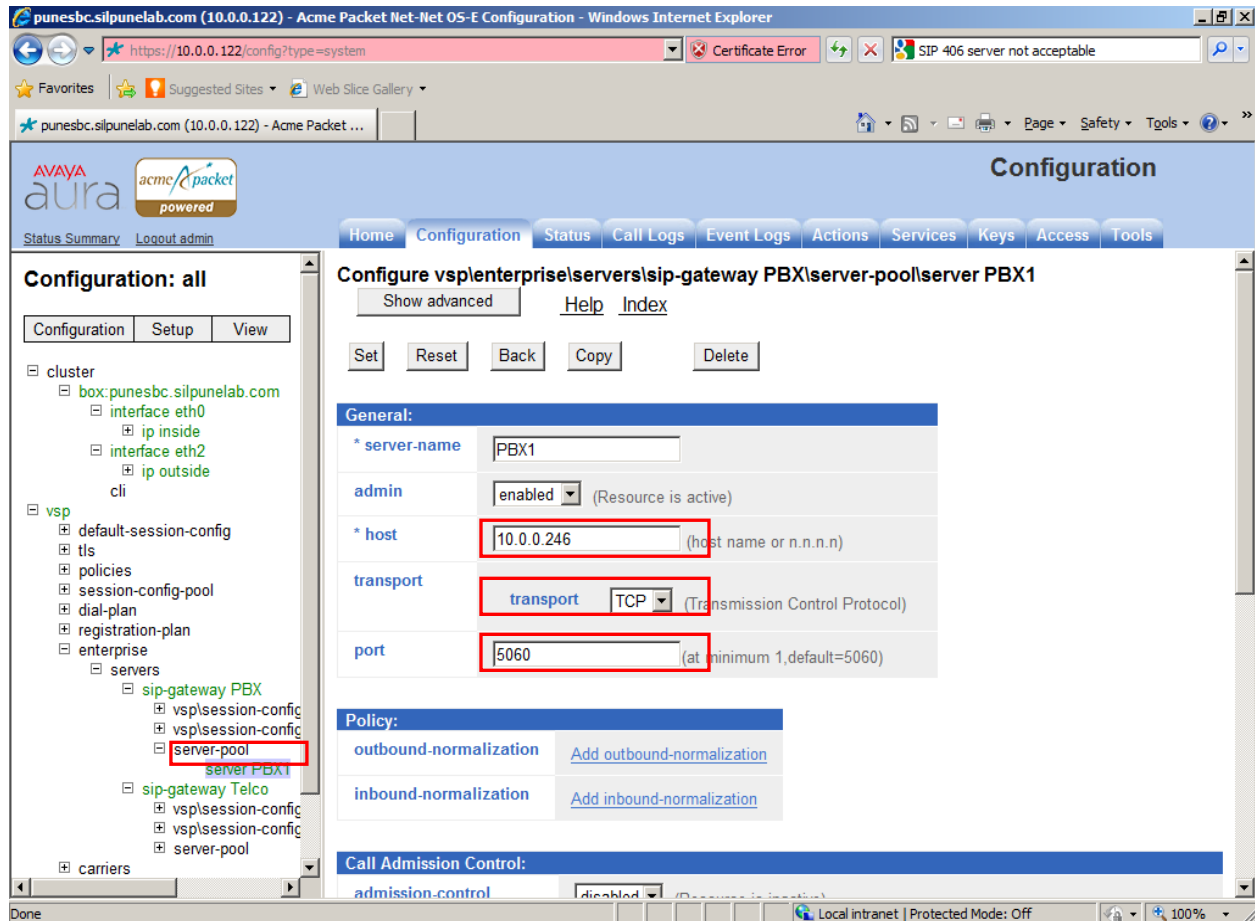
- **Domain:** Enter domain name as configured in Session Manager.



### 6.3.1. Administer SIP TCP Configuration On PBX Server

To administer PBX configuration click on server pool and select server **PBX1**. Make the following changes to the configuration. Click on set button after configuration to update it.

- **Host:** Set the value to Session Manager IP-address.
- **Transport:** TCP
- **Port:** 5060

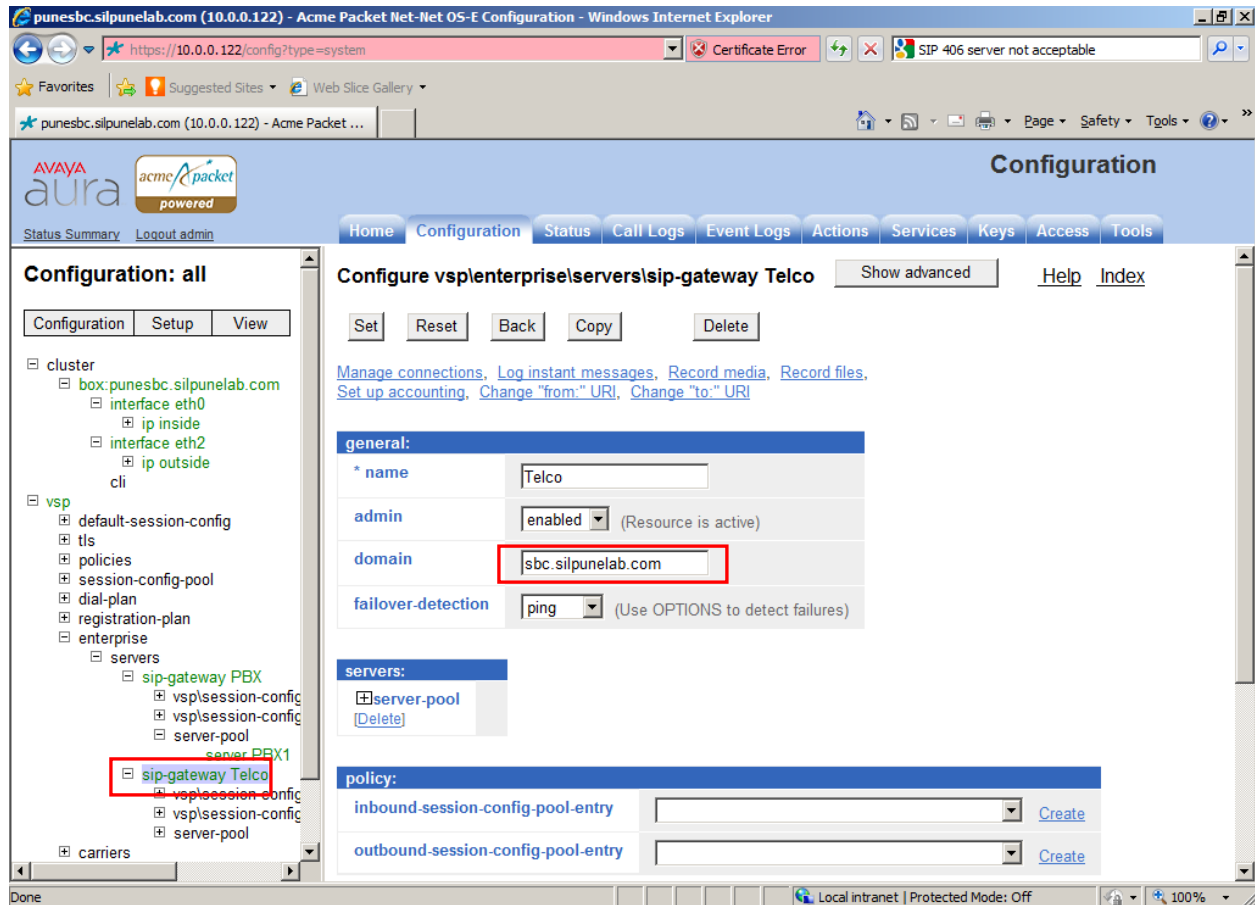


## 6.4. Administer Enterprise TELCO Server

Telco server configuration is required to create link to service provider in public network. Go to VSP node and click on **Enterprise**. Select **sip-gateway Telco** to update configuration.

Enter following details:

- **Domain:** Enter domain name for service provider network.

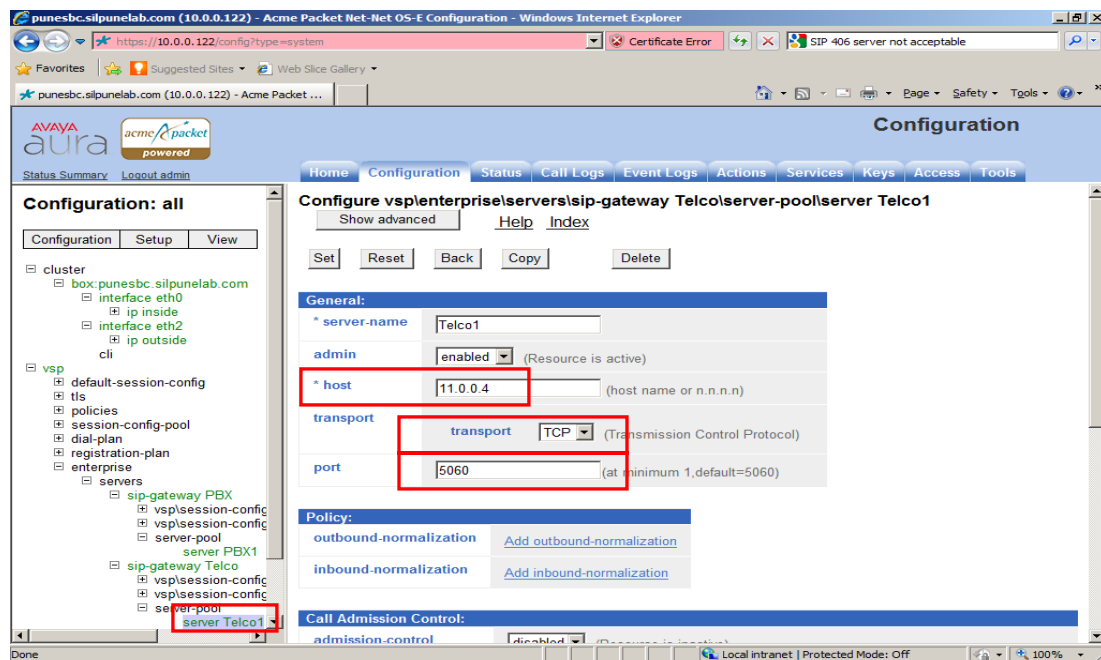




### 6.4.1. Administer SIP TCP Configuration On TELCO Server

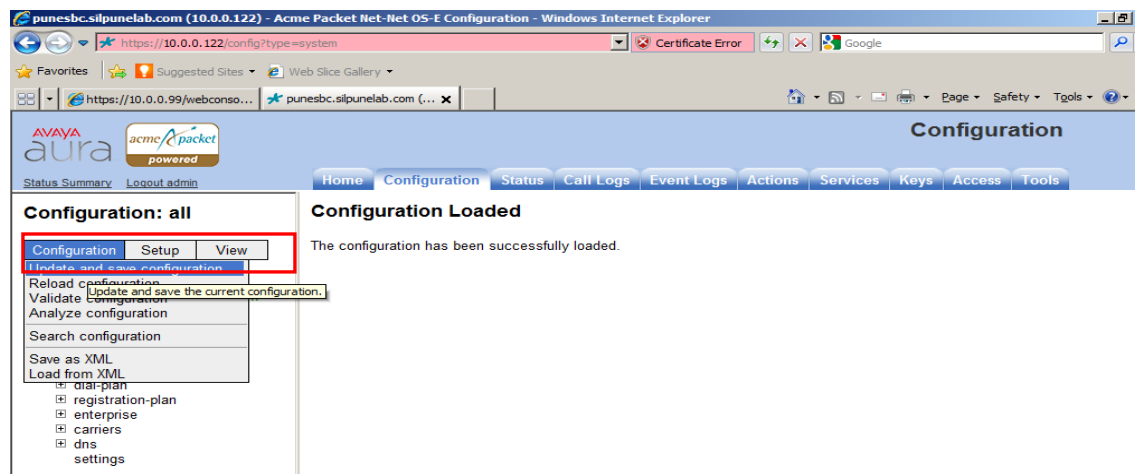
To administer Telco configuration click on server pool and select **server Telco1**. Make the following changes to the configuration. Click on the **set** button after configuration to update it.

- **Host:** Set the value to Server Provider IP-address.
- **Transport:** TCP
- **Port:** 5060



### 6.5. Save and Update Configuration

After completing configuration on the Session Border Controller, user is required to apply the changes to the current running configuration. Click on Configuration drop down menu button in left frame and select **Update and Save configuration**.



## 7. Configure Service Provider

This section provides the information for configuring Service provider in public network. In a customer deployment scenario, a user will configure a SIP trunk with parameters such as IP address and port received from the service provider.

In this lab deployment scenario Avaya Aura® Communication Manager Evolution Server 6.0.1 has been configured in public network to terminate calls to public network. The configuration on Communication Manager is similar to configuration described in **section 4**. Session Border controller is configured as a peer for the SIP trunk with Communication Manager. Avaya endpoints configured with this Communication Manager will act as public users to make and receive calls from private network.

## 8. Verification Steps

### 8.1. Verify Link Status On Communication Manager

To check status of the signaling link on Communication Manager, execute status signaling-group command.

```
status signaling-group 1
                        STATUS SIGNALING GROUP

      Group ID: 1
      Group Type: sip

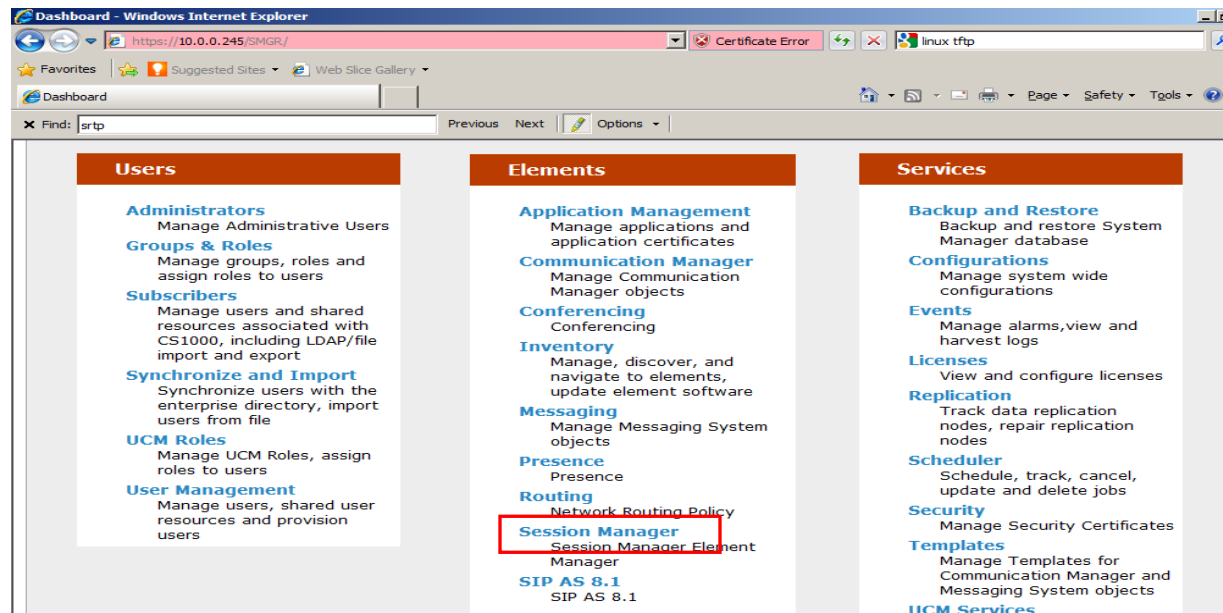
      Group State: in-service
```

To check the status of trunk group on Communication Manager, execute status trunk command.

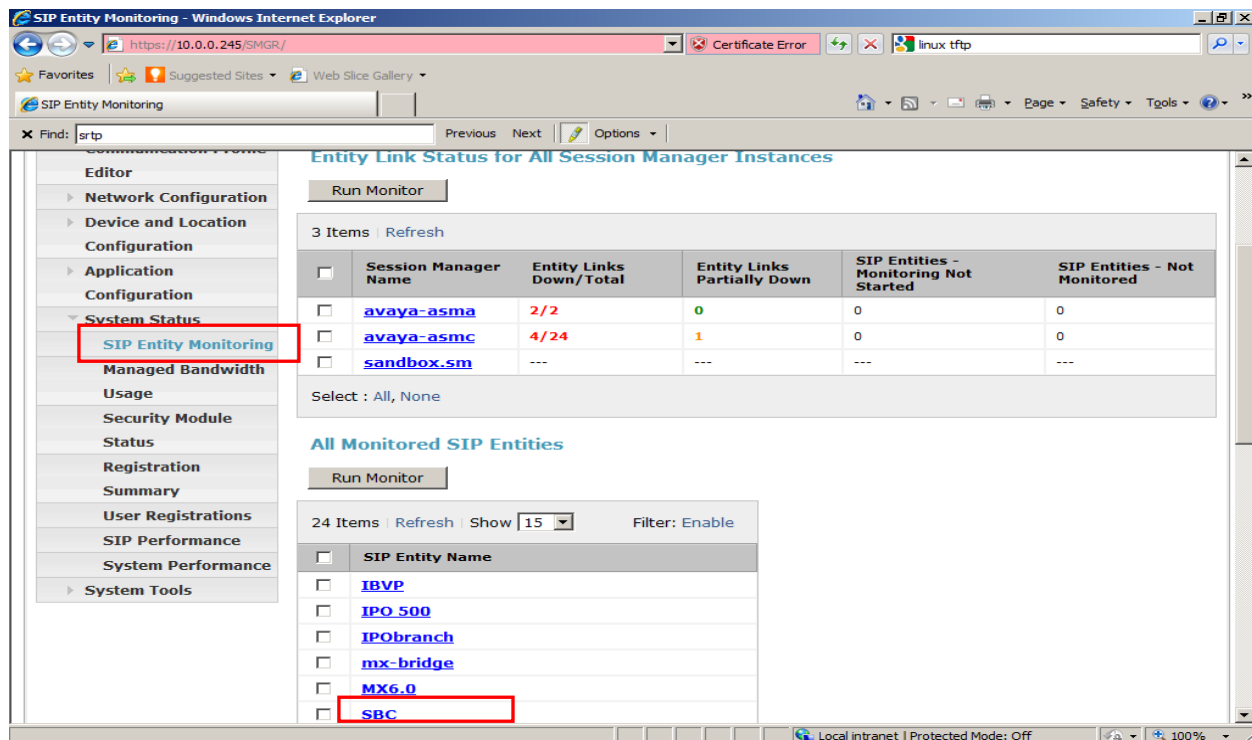
```
status trunk 1
                        TRUNK GROUP STATUS
Member  Port  Service State  Mtce Connected Ports
Busy
0001/001 T00001  in-service/idle  no
0001/002 T00002  in-service/idle  no
0001/003 T00003  in-service/idle  no
0001/004 T00004  in-service/idle  no
0001/005 T00005  in-service/idle  no
0001/006 T00006  in-service/idle  no
0001/007 T00007  in-service/idle  no
0001/008 T00008  in-service/idle  no
0001/009 T00009  in-service/idle  no
0001/010 T00010  in-service/idle  no
0001/011 T00011  in-service/idle  no
0001/012 T00012  in-service/idle  no
```

## 8.2. Verify Link Status on Session Manager

To verify the status on Session Manager go to the System Manager home page and click on **Session Manager** link in Elements column.



Go to **System Status** and select **SIP Entity Monitoring** from the menu. This shows the entities configured on Session Manager. Click on **Session Border Controller** entity to view its status.



Check the status for the link configured with **avaya-asmc** in Session Manager. The connection status and link status is UP.

The screenshot shows the 'SIP Entity Monitoring' web interface in Internet Explorer. The left sidebar contains a navigation menu with 'Session Manager' expanded. The main content area is titled 'SIP Entity, Entity Link Connection Status' and includes a red error message box stating: 'The following errors have occurred: Unable to access SIP monitoring data from Session Manager, sandbox.sm - cannot connect to server.' Below this, the section 'All Entity Links to SIP Entity: SBC' is displayed. A 'Summary View' button is present. A table shows 1 item with the following details:

Details	Session Manager Name	SIP Entity Resolved IP	Port	Proto.	Conn. Status	Reason Code	Link Status
► Show	avaya-asmc	10.0.0.122	5060	TCP	Up	200 OK	Up

Similarly check the status for SIP link with Communication Manager. Go back to SIP Entity Monitoring and click on **IBCM** link to view its status. Check the status for the link configured with avaya-asmc Session Manager. As shown below, the connection status and link status is UP.

The screenshot shows the 'SIP Entity Monitoring' web interface in Internet Explorer. The left sidebar contains a navigation menu with 'Session Manager' expanded. The main content area is titled 'SIP Entity, Entity Link Connection Status' and includes a red error message box stating: 'The following errors have occurred: Unable to access SIP monitoring data from Session Manager, sandbox.sm - cannot connect to server.' Below this, the section 'All Entity Links to SIP Entity: IBCM' is displayed. A 'Summary View' button is present. A table shows 2 items with the following details:

Details	Session Manager Name	SIP Entity Resolved IP	Port	Proto.	Conn. Status	Reason Code	Link Status
► Show	avaya-asma	10.0.0.219	5060	TCP	DOWN	500 Server Internal Error: Destination Unreachable	DOWN
► Show	avaya-asmc	10.0.0.219	5060	TCP	Up	200 OK	Up

### 8.3. Verify Private and Public Link Status on Session Border Controller

To verify the status on Session Border Controller go to the home page and click on **Status** tab. Go to the SIP node in the left frame and click on **sip-connections**. The webpage shows statistics for the connections. Check the status of connections to PBX and Telco server.

The screenshot shows the Avaya Aura SBC Status page. The left sidebar contains a tree view with the following items: MX, Media, Memory, Messaging, Netfilter, Policy, Presence, Profiling, RADIUS, Registration, SIP, active-association, active-call-peers, active-call-summary, active-calls, active-session, audit-trail, call-admission-control, cluster-session-statistics, load-balance, registration-admission, sip-authentication, sip-authentication-delegation, sip-b2b-status, sip-connections (highlighted), sip-data-structures, sip-dialog-status, sip-domain, sip-invite-responses, sip-invite-responses, sip-local-endpoints, and sip-message-activities. The main content area is titled 'sip-connections - SIP transport connection statistics'. It includes a 'View' dropdown set to 'Basic', a 'Search' button, and a 'Refresh' button. Below this is a table with the following data:

TPT	remote-endpoint	local-endpoint	if-index	box	in	out	call	connection-peer
TCP	11.0.0.4:11214	11.0.0.11:5060	3	local	21	21	0	default
TCP	11.0.0.14:1230	11.0.0.11:5060	3	local	0	0	0	default
TCP	11.0.0.20:41532	11.0.0.11:5060	3	local	0	0	0	default
TCP	10.0.2.135:3317	11.0.0.11:5060	3	local	0	0	0	default
TCP	10.0.0.246:5060	10.0.0.122:2941	1	local	755	755	0	PBX
TCP	10.0.0.246:55824	10.0.0.122:5060	1	local	2	2	0	default
TLS	11.0.0.4:5061	11.0.0.11:4021	3	local	1463	1463	0	Telco
TLS	10.0.0.246:17445	10.0.0.122:5061	1	local	443	432	0	default

Page 1 of 1 showing 25 items

Taken Feb 21, 2011 4:27:48 PM XML

About NNOS-E (c) 2005-2010 Acme Packet, Inc. All rights reserved.

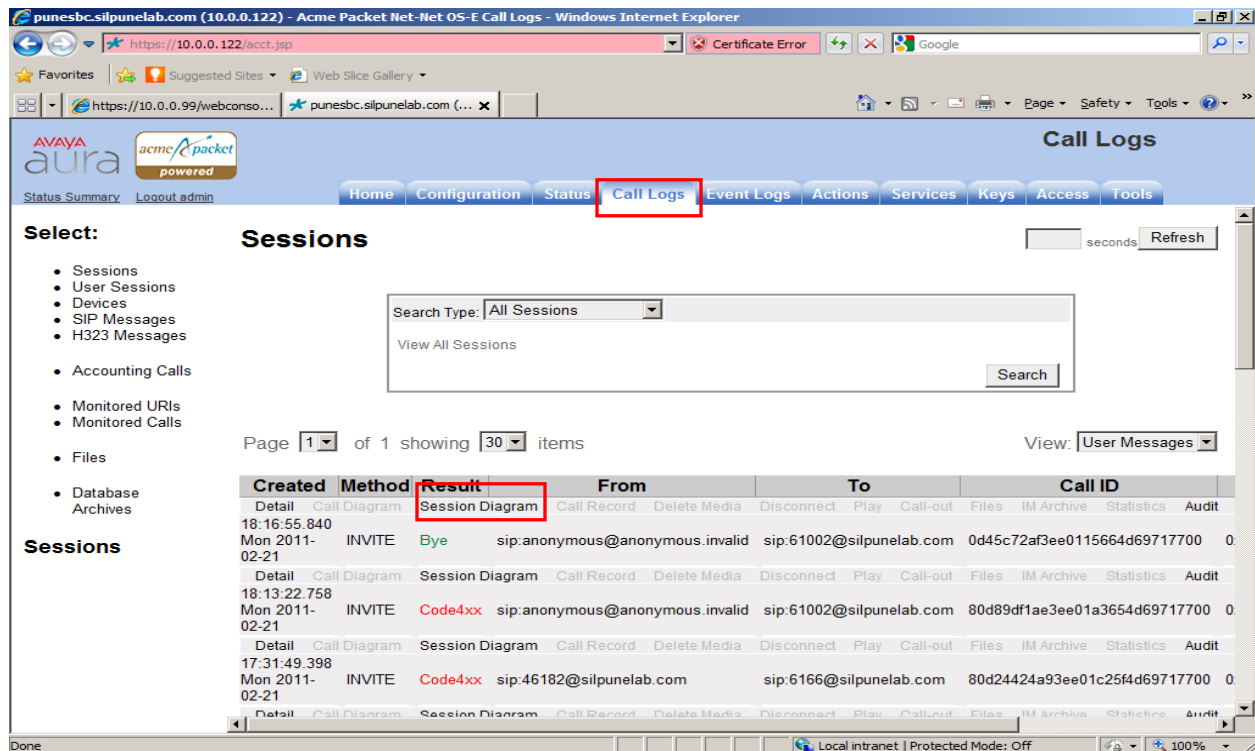
### 8.4. Make a Basic TCP Call

Station 6201 is configured on Communication Manager in the private network and Station 61002 is station on the Communication Manager serving as a simulated Telco server in public network. To make call to public network follow the steps below.

1. User dials 61002 from station 6201.
2. Call is routed to Session Border Controller by Session Manager.
3. Session Border Controller acts as proxy and routes the call to Telco Server.
4. The station registered to Telco Server rings and User answers the call.
5. Verify both party can talk to each other.
6. Called party terminates call. Verify the call logs on Session Border Controller.
7. Also make call from 61002 station to the private extension 6201. To verify public to private calling.

## 8.5. Verify Call Logs On Session Border Controller

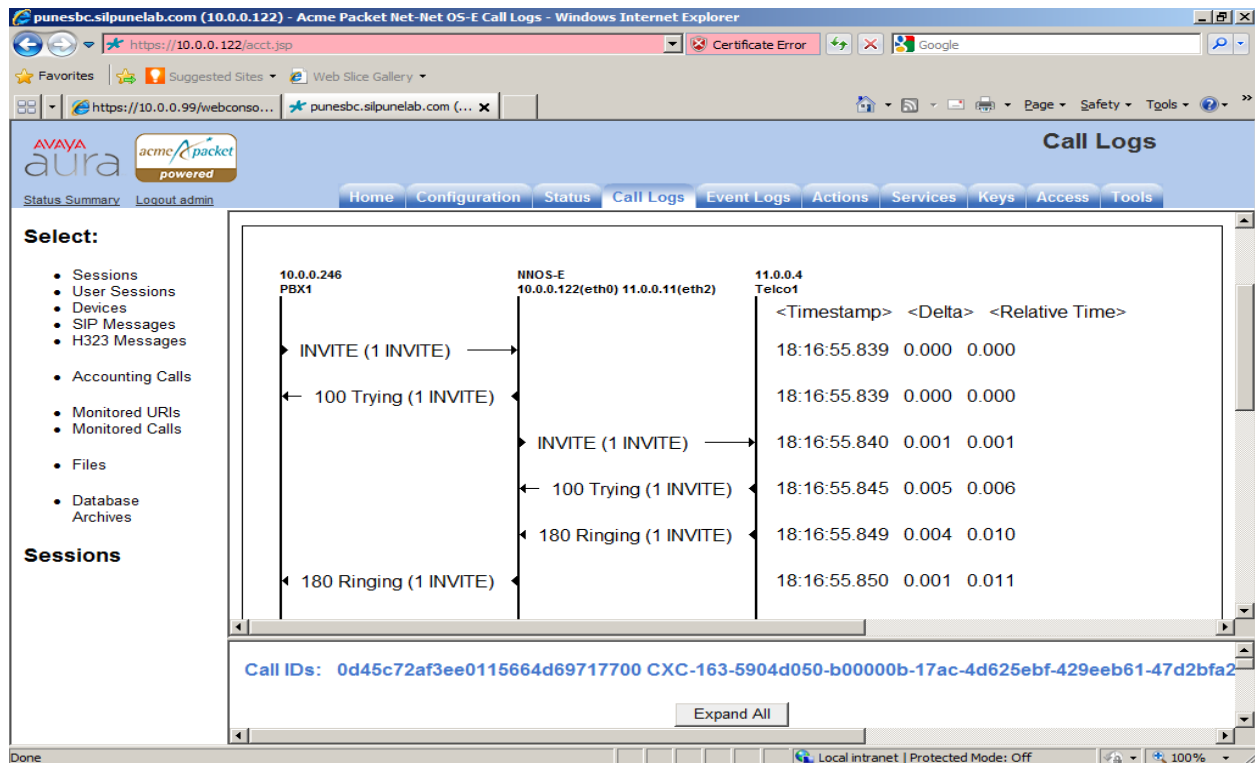
To view the call logs on Session Border Controller go to home page and click on **Call logs** tab and view the first entry in the logs which displays latest session.



The screenshot shows the Avaya Aura SBC Call Logs interface. The 'Call Logs' tab is selected in the top navigation bar. The 'Sessions' section displays a list of call logs. The first entry is selected, and the 'Session Diagram' link is highlighted in the 'Result' column.

Created	Method	Result	From	To	Call ID
18:16:55.840 Mon 2011-02-21	INVITE	Eye	sip:anonymous@anonymous.invalid	sip:61002@silpunelab.com	0d45c72af3ee0115664d69717700 0
18:13:22.758 Mon 2011-02-21	INVITE	Code4xx	sip:anonymous@anonymous.invalid	sip:61002@silpunelab.com	80d89df1ae3ee01a3654d69717700 0
17:31:49.398 Mon 2011-02-21	INVITE	Code4xx	sip:46182@silpunelab.com	sip:6166@silpunelab.com	80d24424a93ee01c25f4d69717700 0

Click on **Session Diagram** link, this shows the call flow for the session as shown above.



The following are different customer scenarios and call flows verified on the setup:

- Verify basic call flow from public station to private station on Communication Manager over TCP protocols.
- Verify basic call flow from private station to public station using different codec supported by Communication Manager.
- Verify call scenario where user performs call Hold/Un-Hold feature.
- Verify call scenario where user in private network performs Attended and Un-Attended transfers from one public user to another public station.
- Verify call scenario where user in private network conferences to other stations in public network via Session Border Controller.
- Verify that Call forward feature enabled on Communication Manager on private extension forwards call from public station.
- Verify that basic and call features can be tested using different Avaya Endpoints such as Avaya one-X® Communicator, Avaya one-X® Agent and 9600 Series IP Deskphone.



## 8.6. Troubleshooting Post Configuration Issues

After completing configuration for Session Border Controller the call failure may occur due different reasons. Following are some of the common failure scenarios and how to troubleshoot.

**Scenario1:** Session Border Controller receives no response from Telco server. Telco server is down.

The screenshot shows the Avaya Aura Call Logs interface in a Windows Internet Explorer browser. The browser address bar shows the URL <https://10.0.0.122/acct.jsp>. The interface has a navigation bar with tabs: Home, Configuration, Status, Call Logs, Event Logs, Actions, Services, Keys, Access, and Tools. The 'Call Logs' tab is selected. On the left, there is a 'Select:' menu with options: Sessions, User Sessions, Devices, SIP Messages (highlighted with a red box), H323 Messages, Accounting Calls, Monitored URIs, Monitored Calls, Files, and Database Archives. The main content area displays a sequence of SIP messages between two endpoints: 10.0.0.246 PBX1 and NNOS-E 10.0.0.122(eth0). The messages are as follows:

Direction	Message	Timestamp	Delta	Relative Time
TX	INVITE (1 INVITE)	17:20:32.383	0.000	0.000
RX	100 Trying (1 INVITE)	17:20:32.383	0.000	0.000
RX	502 Server Telco1 is down. (1 INVITE)	17:20:32.385	0.002	0.002
TX	ACK (1 ACK)	17:20:32.391	0.006	0.008

Below the message list, there is a 'Sessions' section with 'Call IDs: 8028c1bb703fe01e5a94d69717700' and 'Session ID: 0x04C2C4038052AC74'. An 'Expand All' button is present. A table below shows the message details:

Timestamp	Direction	Remote IP/Port	Local IP/Port	Transport
17:20:32.383 2011-02-22	RX	10.0.0.246:55824	10.0.0.122(eth0):5060	TCP
Message: More				
17:20:32.383 2011-02-22	TX	10.0.0.246:5060	10.0.0.122(eth0):5060	TCP

The browser status bar at the bottom shows 'Done' and 'Local intranet | Protected Mode: Off'.

### Troubleshooting steps:

1. Check the status of the SIP trunk from Telco server to Session Border Controller. Go to Call Logs tab and select SIP Messages link.
2. See snapshot below. Enter 40 to see last SIP messages. And check if 200 OK is received for OPTIONS message from Telco IP-address. If 200 OK is not received TELCO server is down.
3. Check the Telco server is reachable and SIP enabled.
4. If the Telco Server is reachable, then check the IP-address and ports are correctly configured on Telco server. The incorrect configuration of IP-address or port may be the reason for Telco server not reachable from Session Border Controller.
5. Also check Kernel-filter configuration in **section 6.2.5**, and verify allow rule is set correctly for **transport** and **network**, to accept SIP traffic from public network.

punesbc.silpunelab.com (10.0.0.122) - Acme Packet Net-Net 05-F Call Logs - Windows Internet Explorer

https://10.0.0.122/acct.jsp

Call Logs

Home Configuration Status **Call Logs** Event Logs Actions Services Keys Access Tools

Select: **Past 40 SIP messages**

- Sessions
- User Sessions
- Devices
- SIP Messages**
- H323 Messages
- Accounting Calls
- Monitored URIs
- Monitored Calls
- Files
- Database Archives

SIP Messages: Simple Search Advanced Search

☒ Show the last 40 messages

☐ Show messages from the past:

☐ Show messages for call ID:

Search

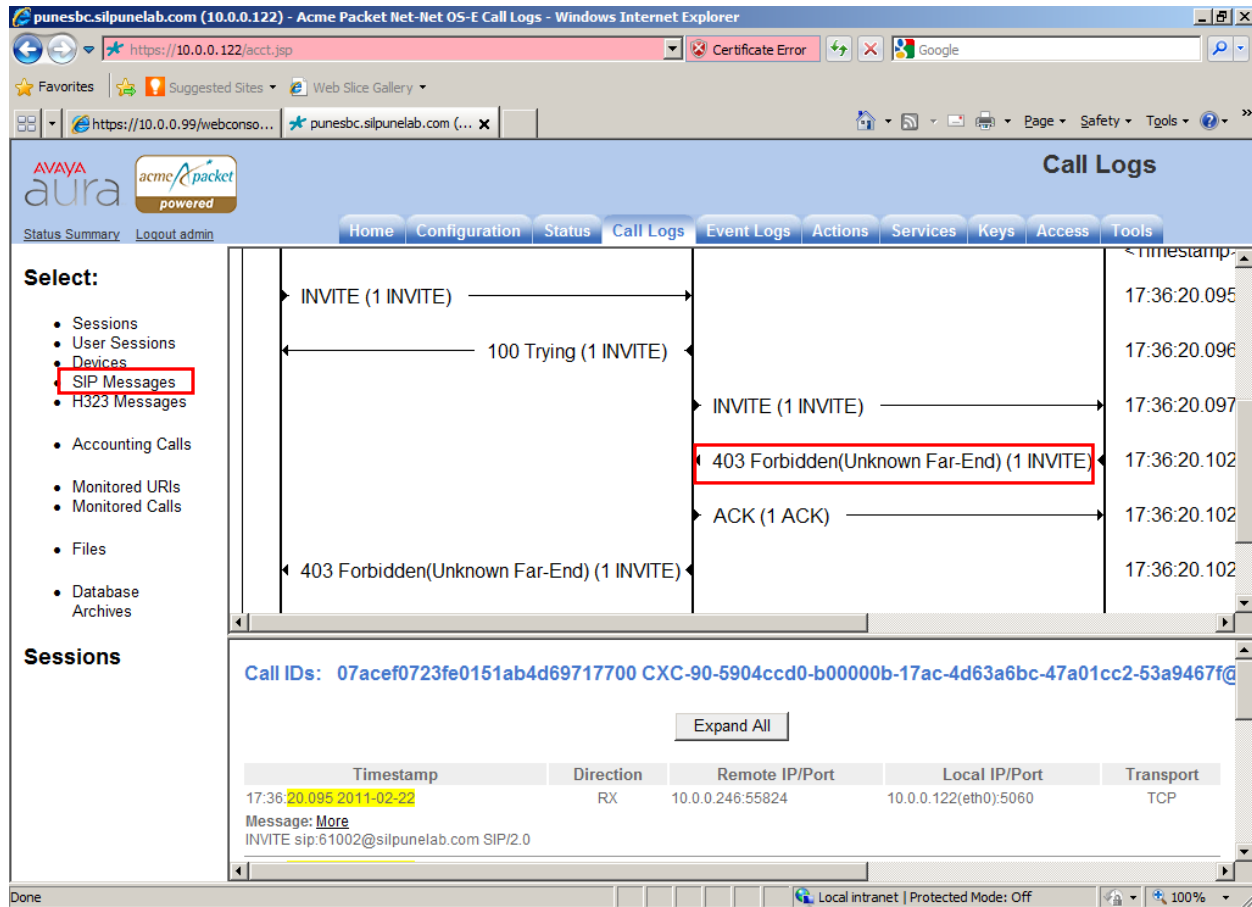
Show: most recent messages first Page 1 of 2 showing 20 items Expand All Collapse All Download as text

Timestamp	Direction	Remote IP/Port	Local IP/Port	Transport
17:28:29.244 2011-02-22	RX	11.0.0.17:4877	11.0.0.11(eth2):5060	TCP
17:28:29.044 2011-02-22	RX	11.0.0.20:51761	11.0.0.11(eth2):5060	TCP
17:28:27.644 2011-02-22	RX	11.0.0.14:2976	11.0.0.11(eth2):5060	TCP
17:28:26.649 2011-02-22	RX	10.0.0.246:5060	10.0.0.122(eth0):2941	TCP
Message: More SIP/2.0 200 OK				
17:28:24.143 2011-02-22	RX	11.0.0.17:4876	11.0.0.11(eth2):5060	TCP

Clear SIP messages

Local intranet | Protected Mode: Off

## Scenario2: Telco server rejects INVITE from Session Border Controller (Forbidden).



### Troubleshooting steps:

1. Check the status of the Telco server trunk to Session Border Controller. Go to Call Logs tab and select SIP Messages link
2. Enter 40 to see last SIP messages. And check if 200 OK is received for OPTIONS message from Telco IP-address.
3. If the Telco Server is reachable, then check configuration on the Session Border Controller for Telco server, Ethernet ETH2 have same transport type (in current configuration TCP). If the Telco server is TLS or UDP i.e., Transport type is mismatch then Telco server rejects call with 403 Forbidden. Update the configuration to correct transport type.

## 9. Conclusion

As illustrated in these Application Notes, Avaya Aura® Session Border Controller can be successfully configured with Avaya Aura® Session Manager 6.0 and Avaya Aura® Communication Manager. Avaya Aura® Session Border Controller allows enterprise network to be connected to public network and provides protection from intrusion and external attacks. The tests calls were made with SIP on TCP and media over RTP. However, for security reasons, it is preferable that SIP with TLS and media over SRTP be used.

## 10. Additional References

Avaya references, available at <http://support.avaya.com>

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

### Avaya Aura® Session Border Controller

- 1) Installing and configuring Avaya Aura® Session Border Controller.
- 2) Avaya Aura® Session Border Controller Release 6.0 Release Notes.
- 3) Avaya Aura(tm) Session Border Controller System Administration.
- 4) Avaya Aura(tm) Session Border Controller Objects and Properties Reference.
- 5) Avaya Aura(tm) Session Border Controller Session Services Guide.

### Avaya Aura® Session Manager

- 6) Avaya Aura™ Session Manager Overview, Doc ID 03-603323.
- 7) Installing and Upgrading Avaya Aura™ Session Manager 6.0, Doc ID 03-603324.
- 8) Installing and Upgrading Avaya Aura™ System Manager 6.0.
- 9) Maintaining and Troubleshooting Avaya Aura™ Session Manager 6.0, Doc ID 03-603325.

### Avaya Aura® Communication Manager

- 10) Installing and Configuring Avaya Aura™ Communication Manager, Doc ID 03-603558
- 11) Upgrading to Avaya Aura® Communication Manager Release 6.0.1, Doc ID 03-603560.
- 12) Administering Avaya Aura™ Communication Manager Doc ID 03-300509

---

**©2011 Avaya Inc. All Rights Reserved.**

Avaya and the Avaya Logo are trademarks of Avaya Inc. All trademarks identified by ® and ™ are registered trademarks or trademarks, respectively, of Avaya Inc. All other trademarks are the property of their respective owners. The information provided in these Application Notes is subject to change without notice. The configurations, technical data, and recommendations provided in these Application Notes are believed to be accurate and dependable, but are presented without express or implied warranty. Users are responsible for their application of any products specified in these Application Notes.

Please e-mail any questions or comments pertaining to these Application Notes along with the full title name and filename, located in the lower right corner, directly to the Avaya Solution & Interoperability Test Lab at [interoplabinotes@list.avaya.com](mailto:interoplabinotes@list.avaya.com)