



Avaya Solution & Interoperability Test Lab

Application Notes for Avaya Aura® Communication Manager 6.3, Avaya Aura® Session Manager 6.3, and Avaya Session Border Controller for Enterprise 6.2 with Verizon Business IP Trunk SIP Trunk Service – Issue 1.2

Abstract

These Application Notes illustrate a sample configuration using Avaya Aura® Session Manager Release 6.3, Avaya Aura® Communication Manager Release 6.3, and Avaya Session Border Controller for Enterprise Release 6.2 with the Verizon Business Private IP (PIP) IP Trunk service. These Application Notes update previously published Application Notes with newer versions of Communication Manager and Session Manager.

The Verizon Business IP Trunk service offer referenced within these Application Notes is designed for business customers with an Avaya SIP trunk solution. The service provides local and/or long distance PSTN calling via standards-based SIP trunks directly, without the need for additional TDM enterprise gateways or TDM cards and the associated maintenance costs.

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, utilizing a Verizon Business Private IP (PIP) circuit connection to the production Verizon Business IP Trunking service.

Table of Contents

1.	Introduction.....	4
2.	General Test Approach and Test Results.....	4
2.1.	Interoperability Compliance Testing	4
2.2.	Test Results.....	5
2.3.	History Info and Diversion Headers	6
2.4.	The SIP Trunk Redundant (2-CPE) Architecture Option	6
2.5.	Support.....	6
3.	Reference Configuration.....	7
3.1.	Remote Workers	9
4.	Equipment and Software Validated	10
5.	Configure Avaya Aura® Communication Manager Release 6.3	11
5.1.	Verify Licensed Features	11
5.2.	Dial Plan.....	13
5.3.	Node Names.....	14
5.4.	Processor Ethernet Configuration on HP Common Server.....	14
5.5.	Network Regions for Gateway, Telephones	15
5.6.	IP Codec Sets	18
5.7.	SIP Signaling Group	19
5.8.	SIP Trunk Group.....	21
5.9.	Route Pattern Directing Outbound Calls to Verizon	24
5.10.	Route Pattern for Internal Calls via Session Manager	25
5.11.	Private Numbering.....	25
5.12.	ARS Routing For Outbound Calls	26
5.13.	Avaya Aura® Communication Manager Stations	26
5.14.	EC500 Configuration for Diversion Header Testing.....	27
5.15.	Saving Communication Manager Configuration Changes	27
6.	Configure Avaya Aura® Session Manager Release 6.3.....	28
6.1.	Domains	30
6.2.	Locations.....	30
6.3.	Adaptations	33
6.4.	SIP Entities.....	37
6.5.	Entity Links.....	42
6.6.	Time Ranges	43
6.7.	Routing Policies	43
6.8.	Dial Patterns.....	45
6.9.	Fax Users	47
7.	Configure Avaya Session Border Controller for Enterprise Release 6.2.....	49
7.1.	Network Management.....	51
7.2.	Routing Profile.....	52
7.3.	Topology Hiding Profile.....	53
7.4.	Server Interworking Profile	55
7.4.1	Server Interworking– Avaya.....	56
7.4.2	Server Interworking – Verizon IP Trunk	58
7.5.	Signaling Manipulation.....	61
7.6.	Server Configuration.....	62

7.6.1	Server Configuration for Session Manager.....	63
7.6.2	Server Configuration for Verizon IP Trunk.....	65
7.7.	Media Rule.....	66
7.8.	Signaling Rule.....	68
7.9.	Application Rule.....	71
7.10.	Endpoint Policy Group	71
7.11.	Media Interface	73
7.12.	Signaling Interface	73
7.13.	End Point Flows - Server Flow	74
8.	AudioCodes MP-114	77
8.1.	Fax Configuration Settings	77
8.2.	SIP Endpoint Registration and Proxy Settings	80
8.3.	Routing.....	82
9.	Verizon Business IP Trunk Services Suite Configuration.....	85
9.1.	Service Access Information	85
10.	Verification Steps.....	86
10.1.	Avaya Aura® Communication Manager Verifications	86
10.1.1	Example Incoming Call from PSTN via Verizon SIP Trunk	86
10.1.2	Example Outgoing Calls to PSTN via Verizon IP Trunk	88
10.2.	Avaya Aura® System Manager and Avaya Aura® Session Manager Verifications.....	89
10.2.1	Verify SIP Entity Link Status	89
10.2.2	Call Routing Test	91
10.3.	Avaya Session Border Controller for Enterprise Verification.....	93
10.3.1	Welcome Screen	93
10.3.2	Alarms.....	93
10.3.3	Incidents	94
10.3.4	Diagnostics.....	95
10.3.5	Tracing	96
11.	Conclusion	97
12.	Additional References.....	98
12.1.	Avaya	98
12.2.	Verizon Business	98
12.3.	AudioCodes.....	98
Appendix A	99

1. Introduction

These Application Notes illustrate a sample configuration using Avaya Aura® Session Manager Release 6.3, Avaya Aura® Communication Manager Release 6.3, and Avaya Session Border Controller for Enterprise Release 6.2 with the Verizon Business Private IP (PIP) IP Trunk service. The Verizon Business IP Trunk service provides local and/or long-distance calls (with PSTN endpoints) via standards-based SIP trunks.

2. General Test Approach and Test Results

The test approach was manual testing of inbound and outbound calls using the Verizon IP Trunk SIP Trunk Service on a production Verizon PIP access circuit, as shown in **Figure 1**.

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

Compliance testing scenarios for the configuration described in these Application Notes included the following:

- Inbound and outbound voice calls between telephones controlled by Communication Manager and the PSTN can be made using G.711MU or G.729A codecs.
- Direct IP-to-IP Media (also known as “Shuffling”) when applicable.
- DTMF using RFC 2833
 - Outbound call to PSTN application requiring post-answer DTMF (e.g., an IVR or voice mail system)
 - Inbound call from PSTN to Avaya CPE application requiring post-answer DTMF (e.g., Communication Manager Messaging, Avaya vector digit collection steps)
- Additional PSTN numbering plans (e.g., International, operator assist, 411)
- Hold / Retrieve with music on hold
- Call transfer using two approaches
 - REFER approach (Communication Manager Network Call Redirection flag on trunk group form set to “y”)
 - INVITE approach (Communication Manager Network Call Redirection flag on trunk group form set to “n”)
- Conference calls
- SIP Diversion Header for call redirection
 - Call Forwarding
 - EC500
- Long hold time calls

2.2. Test Results

Interoperability testing of Verizon Business IP Trunk SIP Trunk Service was completed with successful results for all test cases. The following limitations are noted for the sample configuration described in these Application Notes.

- Verizon provisioned T.38 Fax on the production circuit used to verify these Application Notes. Verizon Business IP Trunk service requires all fax calls to start off with G.711 as the first codec choice, and relies on the CPE to send a re-Invite to T.38 when placing or receiving a fax call. If the **FAX Mode** field on the Communication Manager ip-codec-set form page 2 is set to “t.38-standard” (see **Section 5.6**), Communication Manager will send the proper re-Invite to T.38, but will not fallback to G.711 should the Verizon network reject the Communication Manager attempt to transition to T.38 by sending a 488 Not Acceptable message. Communication Manager Release 6.3 introduces the T.38 Fax with Fallback to G.711 Pass-Through feature. This provides the functionality for Communication Manager to interoperate with Verizon networks by re-Inviting to G.711 after receiving a 488 Not Acceptable message. If the **FAX Mode** is set to the new “t.38-G711-fallback” setting¹, Communication Manager will send a re-Invite to T.38 for inbound fax calls only and relies on the far end to send a re-Invite to T.38 for outbound calls. Communication Manager assumes T.38 fax is not supported for an outbound fax call unless an Invite for T.38 is received. The result is an outbound fax sent using G.711, even though the circuit is provisioned for T.38. Inbound fax calls negotiate properly to T.38. With the limitations of T.38 on Verizon’s network and Verizon’s requirement for fax calls to start off with G.711 as the first codec choice, it is recommended to use an AudioCodes MP-114 or MP-124 Gateway between Session Manager and the fax device when fax is used with Verizon IP Trunk service.
- When the **Initial IP-IP Direct Media** field on the Communication Manager signaling group form page 1 is set to ‘y’, Communication Manager sends a “183 Session Progress” without SDP during an inbound PSTN call that is forwarded to another PSTN call just before a 183 is sent with SDP information to the far end. This is undesirable to Verizon and results in no audio. The recommendation in **Section 5.7** is to leave the **Initial IP-IP Direct Media** field to “n”. As a safeguard, an Avaya SBCE Server Interworking Profile in **Section 7.4.2** includes a parameter to insure Verizon always receives “183 Session Progress” with SDP.
- Emergency 911/E911 Services Limitations and Restrictions - Although Verizon provides 911/E911 calling capabilities, 911 capabilities were not tested; therefore, it is the customer’s responsibility to ensure proper operation with its equipment/software vendor.
- Verizon Business IP Trunking service does not support G.711a codec for domestic service (EMEA only).
- Verizon Business IP Trunking service does not support G.729B codec.

¹ The “T.38 Fax with Fallback to G.711 Pass-Through” feature requires G430 or G450 Media Gateways with release 33.13 or higher.

Note - These Application Notes describe the provisioning used for the sample configuration shown in **Figure 1**. Other configurations may require modifications to the provisioning described in this document.

2.3. History Info and Diversion Headers

The Verizon Business IP Trunk service does not support SIP History Info Headers. Instead, the Verizon Business IP Trunk service requires that the SIP Diversion Header be sent for redirected calls. The Communication Manager SIP trunk group form provides the options for specifying whether History Info Headers or Diversion Headers are sent.

If Communication Manager sends the History Info Header, Session Manager can convert the History Info header into the Diversion Header. This is performed by specifying the “*VerizonAdapter*” adaptation in Session Manager.

The Communication Manager Call Forwarding or Extension to Cellular (EC500) features may be used for the call scenarios testing the Diversion Header.

2.4. The SIP Trunk Redundant (2-CPE) Architecture Option

Verizon Business and Avaya developed the SIP Trunk Redundant (2-CPE) architecture to ensure that SIP trunk calls can be automatically rerouted to bypass SIP trunk failures due to network or component outages. The 2-CPE architecture described is based on a customer location having two Avaya Session Border Controllers for Enterprise. One Avaya SBCE is designated as Primary and one as Secondary. The Avaya SBCEs reside at the edge of the customer network.

Avaya Aura® Session Manager is provisioned to attempt outbound calls to the Primary Avaya SBCE first. If that attempt fails, the Secondary Avaya SBCE is used. Similarly, the Verizon Business Private IP Trunk service node will send inbound calls to the Primary Avaya SBCE. If there is no response then the call will be sent to the Secondary Avaya SBCE. For more information on how to configure 2-CPE see [MO-VZIPT-SM62].

2.5. Support

For technical support on the Avaya products described in these Application Notes visit <http://support.avaya.com>

For technical support on Verizon Business IP Trunk service offer, visit online support at <http://www.verizonbusiness.com/us/customer/>

3. Reference Configuration

Figure 1 illustrates the sample configuration used for the testing. The Avaya CPE location simulates a customer site. The PIP service defines a secure MPLS connection between the Avaya CPE T1 connection and the Verizon service node.

The Avaya SBCE receives traffic from the Verizon Business IP Trunk service on port 5060 and sends traffic to the Verizon Business IP trunk service on port 5071, using UDP protocol for network transport (required by the Verizon Business IP Trunk service). The Verizon Business IP Trunk service provided Direct Inward Dial (DID) 10 digit numbers. These DID numbers can be mapped by Avaya Aura® Session Manager or Avaya Aura® Communication Manager to Avaya telephone extensions.

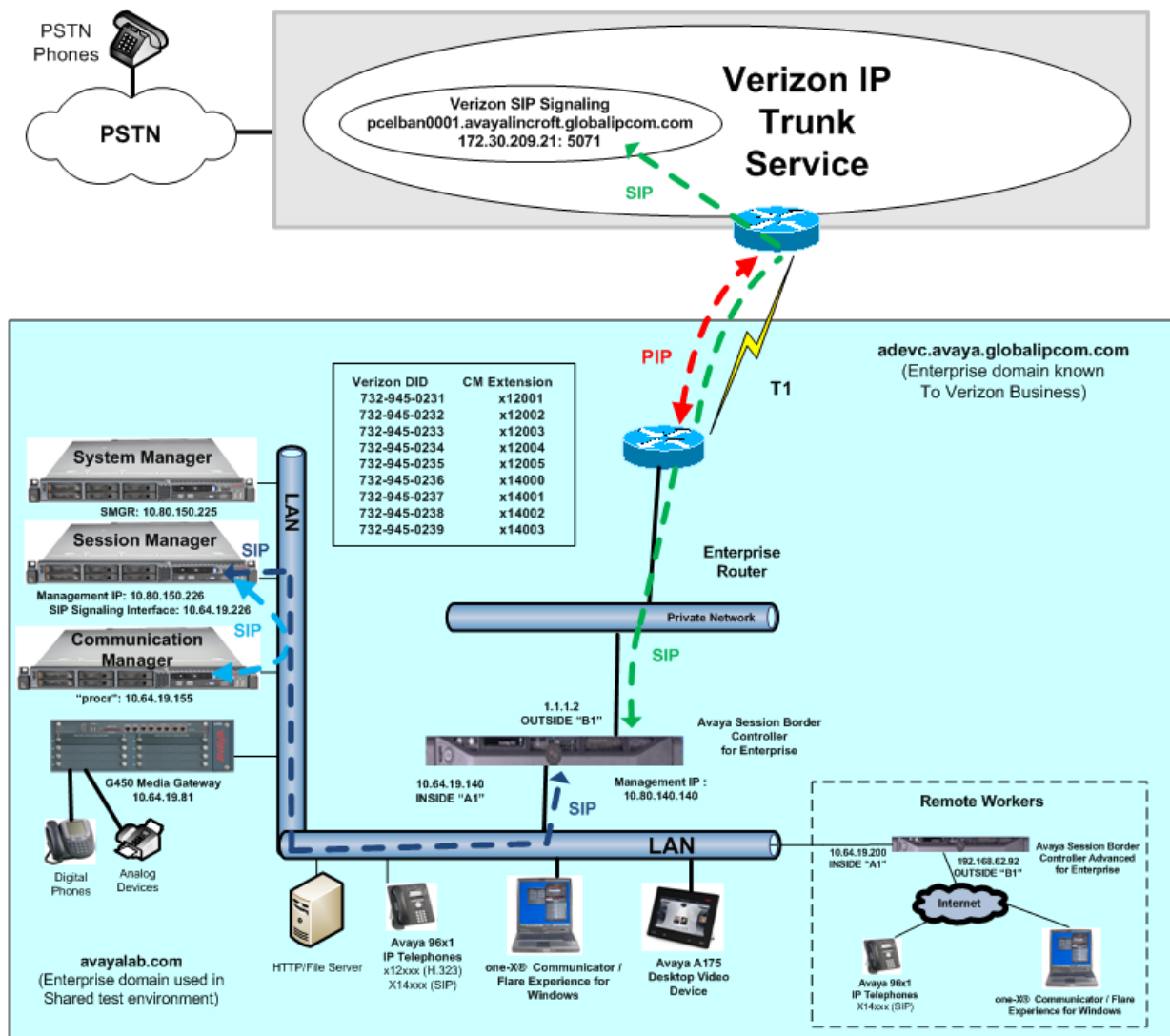


Figure 1: Avaya Interoperability Test Lab Configuration

The Verizon Business IP Trunk service used FQDN *pcelban0001.avayalincroft.globalipcom.com*. The Avaya CPE environment was known to Verizon Business IP Trunk service as FQDN *adevc.avaya.globalipcom.com*. Access to the Verizon Business IP Trunk service was added to a configuration that already used domain “avayalab.com” at the enterprise. As such, the Avaya SBCE is used to adapt the “avayalab.com” domain to the domain known to Verizon. These Application Notes indicate a configuration that would not be required in cases where the CPE domain in Communication Manager and Session Manager match the CPE domain known to the Verizon Business IP Trunk service.

Note – The Fully Qualified Domain Names and IP addressing specified in these Application Notes apply only to the reference configuration shown in **Figure 1**. Verizon Business customers will use their own FQDNs and IP addressing as required.

In summary, the following components were used in the reference configuration.

- Verizon Business IP Trunk network Fully Qualified Domain Name (FQDN)
 - *pcelban0001.avayalincroft.globalipcom.com*
- Avaya CPE Fully Qualified Domain Name (FQDN) known to Verizon
 - *adevc.avaya.globalipcom.com*
- Avaya Session Border Controllers for Enterprise Release 6.2
- Avaya Aura® Communication Manager Release 6.3
- Avaya Aura® Session Manager Release 6.3
- Avaya 96X1 Series IP telephones using the SIP and H.323 software bundle
- Avaya 96X0 Series IP telephones using the H.323 software bundle
- Avaya Digital Phones
- Remote Workers
 - Avaya Session Border Controller Advanced for Enterprise Release 6.2
 - Avaya 96X1 Series IP telephones using the SIP software bundle
 - Avaya Flare® Experience for Windows

3.1. Remote Workers

In the sample configuration, remote Avaya SIP endpoints connected through Avaya SBCE with Advanced Services licensing were used along with local Avaya endpoints in the verification of these Application Notes. The figure below illustrates a detailed view of the Remote Workers section previously shown in **Figure 1**. Although not the primary focus of these Application Notes, relevant configuration parameters of the Avaya SBCE for use with Remote Worker are illustrated in **Appendix A**.

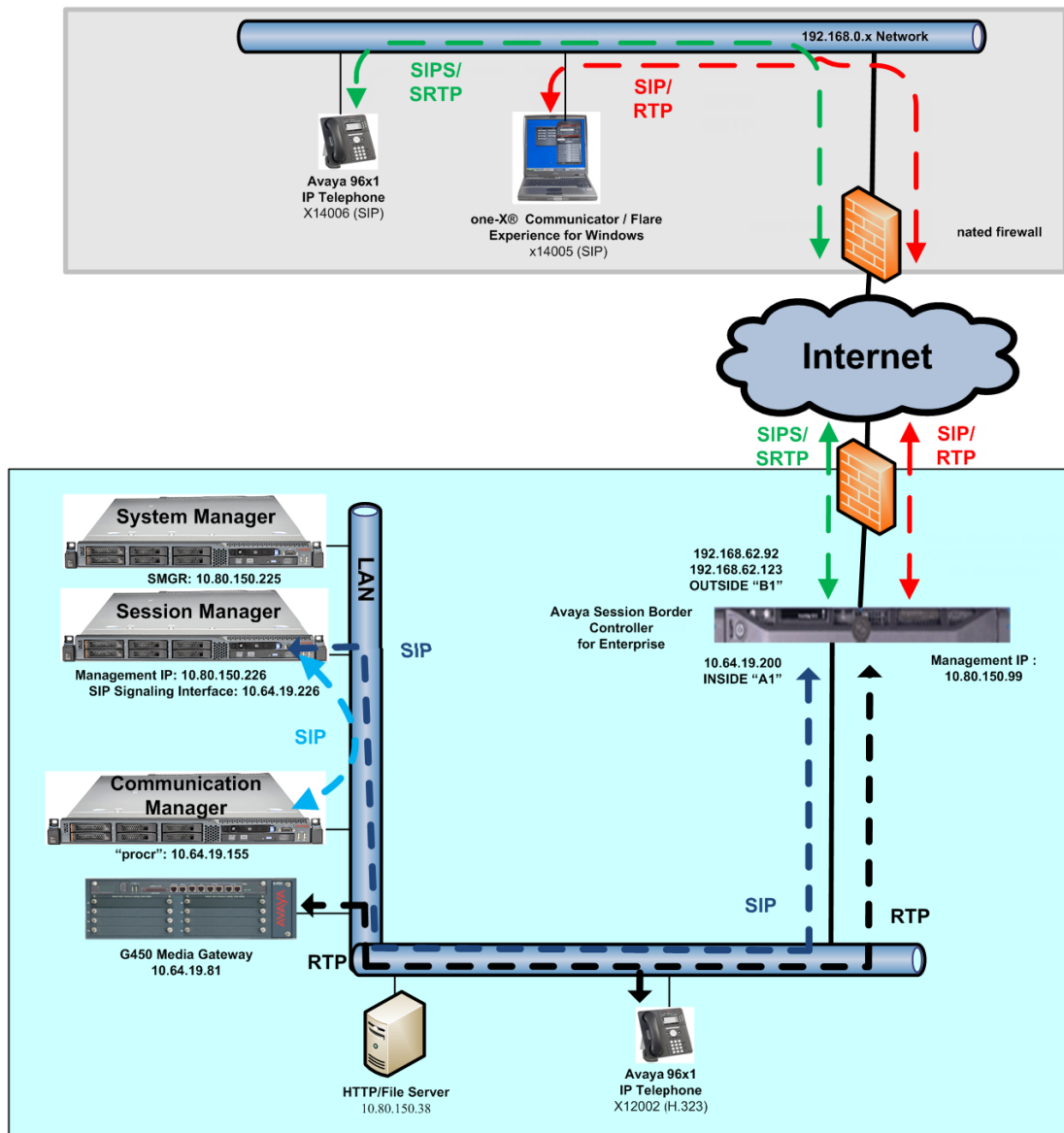


Figure 2: Remote Worker Lab Configuration

4. Equipment and Software Validated

The following equipment and software were used in the sample configuration.

Equipment:	Software:
HP ProLiant DL360 G7	Avaya Aura® Communication Manager Release 6.3 SP0
HP ProLiant DL360 G7	Avaya Aura® System Manager 6.3 SP2
HP ProLiant DL360 G7	Avaya Aura® Session Manager 6.3 SP2
G450 Gateway	33.13.0
DELL 210 RII	Avaya Session Border Controller for Enterprise Version 6.2 Q36
Avaya 96X0-Series Telephones (H.323)	R 3.2
Avaya 96X1- Series Telephones (SIP)	R6.2.2.17
Avaya 96X1- Series Telephones (H323)	R6.2313
Avaya One-X Communicator (H.323)	6.1.8.06-SP8-40314
Avaya Flare® Experience for Windows	1.1.2.11
Avaya Desktop Video Device	Flare 1.1.3
Avaya 2400-Series and 6400-Series Digital Telephones	N/A
AudioCodes MP-114	6.20A.035.001
Okidata Analog Fax	N/A

Table 1: Equipment and Software Used in the Sample Configuration

5. Configure Avaya Aura® Communication Manager Release 6.3

This section illustrates an example configuration allowing SIP signaling via the “Processor Ethernet” of the Avaya HP Server to Session Manager. In configurations that use an Avaya G650 Media Gateway, it is also possible to use an Avaya C-LAN in the Avaya G650 Media Gateway for SIP signaling to Session Manager.

Note - The initial installation, configuration, and licensing of the Avaya servers and media gateways for Communication Manager are assumed to have been previously completed and are not discussed in these Application Notes.

5.1. Verify Licensed Features

Communication Manager license file controls customer capabilities. Contact an authorized Avaya representative for assistance if a required feature needs to be enabled.

On **Page 2** of the *display system-parameters customer-options* form, verify that the **Maximum Administered SIP Trunks** is sufficient for the combination of trunks to the Verizon Business IP Trunk service offer and any other SIP applications. Each call from a non-SIP endpoint to the Verizon Business IP Trunk service uses one SIP trunk for the duration of the call. Each call from a SIP endpoint to the Verizon Business IP Trunk service uses two SIP trunks for the duration of the call.

display system-parameters customer-options		Page	2 of 11
OPTIONAL FEATURES			
IP PORT CAPACITIES		USED	
Maximum Administered H.323 Trunks:		12000	0
Maximum Concurrently Registered IP Stations:		18000	3
Maximum Administered Remote Office Trunks:		12000	0
Maximum Concurrently Registered Remote Office Stations:		18000	0
Maximum Concurrently Registered IP eCons:		128	0
Max Concur Registered Unauthenticated H.323 Stations:		100	0
Maximum Video Capable Stations:		36000	3
Maximum Video Capable IP Softphones:		18000	1
Maximum Administered SIP Trunks:		12000	40
Maximum Administered Ad-hoc Video Conferencing Ports:		12000	0
Maximum Number of DS1 Boards with Echo Cancellation:		522	0
Maximum TN2501 VAL Boards:		10	0
Maximum Media Gateway VAL Sources:		250	2
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

On **Page 3** of the *display system-parameters customer-options* form, verify that **ARS** is enabled.

display system-parameters customer-options		Page 3 of 11
OPTIONAL FEATURES		
Abbreviated Dialing Enhanced List? y	Audible Message Waiting? y	
Access Security Gateway (ASG)? n	Authorization Codes? y	
Analog Trunk Incoming Call ID? y	CAS Branch? n	
A/D Grp/Sys List Dialing Start at 01? y	CAS Main? n	
Answer Supervision by Call Classifier? y	Change COR by FAC? n	
ARS? y	Computer Telephony Adjunct Links? y	
ARS/AAR Partitioning? y	Cvg Of Calls Redirected Off-net? y	
ARS/AAR Dialing without FAC? n	DCS (Basic)? y	
ASAI Link Core Capabilities? n	DCS Call Coverage? y	
ASAI Link Plus Capabilities? n	DCS with Rerouting? y	
Async. Transfer Mode (ATM) PNC? n	Digital Loss Plan Modification? y	
Async. Transfer Mode (ATM) Trunking? n	DS1 MSP? y	
ATM WAN Spare Processor? n	DS1 Echo Cancellation? y	
ATMS? y		
Attendant Vectoring? y		

On **Page 4** of the *display system-parameters customer-options* form, verify that the **Enhanced EC500**, **IP Trunks**, **IP Stations**, and **ISDN-PRI** features are enabled. If the use of SIP REFER messaging or send-only SDP attributes will be required verify that the **ISDN/SIP Network Call Redirection** feature is enabled.

display system-parameters customer-options		Page 4 of 11
OPTIONAL FEATURES		
Emergency Access to Attendant? y	IP Stations? y	
Enable 'dadmin' Login? y		
Enhanced Conferencing? y	ISDN Feature Plus? n	
Enhanced EC500? y	ISDN/SIP Network Call Redirection? y	
Enterprise Survivable Server? n	ISDN-BRI Trunks? y	
Enterprise Wide Licensing? n	ISDN-PRI? y	
ESS Administration? y	Local Survivable Processor? n	
Extended Cvg/Fwd Admin? y	Malicious Call Trace? y	
External Device Alarm Admin? y	Media Encryption Over IP? n	
Five Port Networks Max Per MCC? n	Mode Code for Centralized Voice Mail? n	
Flexible Billing? n		
Forced Entry of Account Codes? y	Multifrequency Signaling? y	
Global Call Classification? y	Multimedia Call Handling (Basic)? y	
Hospitality (Basic)? y	Multimedia Call Handling (Enhanced)? y	
Hospitality (G3V3 Enhancements)? y	Multimedia IP SIP Trunking? y	
IP Trunks? y		
IP Attendant Consoles? y		

On **Page 5** of the *display system-parameters customer-options* form, verify that the **Private Networking** and **Processor Ethernet** features are enabled.

display system-parameters customer-options		Page 5 of 11
OPTIONAL FEATURES		
Multinational Locations? n	Station and Trunk MSP? y	
Multiple Level Precedence & Preemption? n	Station as Virtual Extension? y	
Multiple Locations? n		
Personal Station Access (PSA)? y	System Management Data Transfer? n	
PNC Duplication? n	Tenant Partitioning? y	
Port Network Support? y	Terminal Trans. Init. (TTI)? y	
Posted Messages? y	Time of Day Routing? y	
	TN2501 VAL Maximum Capacity? y	
	Uniform Dialing Plan? y	
Private Networking? y	Usage Allocation Enhancements? y	
Processor and System MSP? y		
Processor Ethernet? y	Wideband Switching? y	
	Wireless? n	
Remote Office? y		
Restrict Call Forward Off Net? y		
Secondary Data Module? y		

5.2. Dial Plan

In the reference configuration, the Avaya CPE environment uses five digit local extensions such as 12xxx, 14xxx or 20xxx. Trunk Access Codes (TAC) are 3 digits in length and begin with *. The Feature Access Code (FAC) to access ARS is the single digit 9. The Feature Access Code (FAC) to access AAR is the single digit 8. The dial plan illustrated here is not intended to be prescriptive; any valid dial plan may be used.

The dial plan is modified with the *change dialplan analysis* command as shown below.

change dialplan analysis						Page 1 of 12		
DIAL PLAN ANALYSIS TABLE								
Location: all						Percent Full: 1		
Dialed String	Total Length	Call Type	Dialed String	Total Length	Call Type	Dialed String	Total Length	Call Type
1	5	ext						
2	5	ext						
8	1	fac						
9	1	fac						
*	3	dac						
#	3	dac						

5.3. Node Names

Node names are mappings of names to IP addresses that can be used in various screens. The following *change node-names ip* output shows relevant node-names in the sample configuration. As shown in bold, the node name for Session Manager is “SM63” with IP address “10.64.19.226”. The node name and IP address for the Processor Ethernet “procr” is “10.64.19.155”.

change node-names ip		Page 1 of 2
IP NODE NAMES		
Name	IP Address	
SM63	10.64.19.226	
default	0.0.0.0	
procr	10.64.19.155	
procr6	::	

5.4. Processor Ethernet Configuration on HP Common Server

The *add ip-interface procr* or *change ip-interface procr* command can be used to configure the Processor Ethernet (PE) parameters. The following screen shows the parameters used in the sample configuration. While the focus here is the use of the PE for SIP Trunk Signaling, observe that the Processor Ethernet will also be used for registrations from H.323 IP Telephones and H.248 gateways in the sample configuration.

change ip-interface procr		Page 1 of 2
IP INTERFACES		
Type: PROCR		
Target socket load: 1700		
Enable Interface? y	Allow H.323 Endpoints? y	
	Allow H.248 Gateways? y	
Network Region: 1	Gatekeeper Priority: 5	
IPV4 PARAMETERS		
Node Name: procr	IP Address: 10.64.19.155	
Subnet Mask: /24		

5.5. Network Regions for Gateway, Telephones

Network regions provide a means to logically group resources. In the shared Communication Manager configuration used for the testing, the Avaya G450 Media Gateway is in region 1. To provide testing flexibility, network region 2 was associated with other components used specifically for the Verizon testing.

Non-IP telephones (e.g., analog, digital) derive network region and location configuration from the Avaya gateway to which the device is connected. The following display command shows that **Media Gateway 1** is an Avaya G450 Media Gateway configured for network region 1. It can also be observed that the **Controller IP Address** is the Avaya Processor Ethernet (10.64.19.155), and that the gateway IP address is 10.64.19.81. These fields are not configured in this screen, but just display the current information for the Media Gateway.

```
change media-gateway 1                                     Page 1 of 2
                                                           MEDIA GATEWAY 1

Type: g450
Name: G450-1
Serial No: 08IS38199678
Encrypt Link? y                                           Enable CF? n
Network Region: 1                                         Location: 1
                                                           Site Data:

Recovery Rule: 1

Registered? y
FW Version/HW Vintage: 33 .13 .0 /1
MGP IPV4 Address: 10.64.19.81
MGP IPV6 Address:
Controller IP Address: 10.64.19.155
MAC Address: 00:1b:4f:03:52:18
```

The following screen shows **Page 2** for **Media Gateway 1**. The gateway has an **S8300** in slot V1 (unused), an **MM712** media module supporting Avaya digital phones in slot V2, an **MM711** supporting analog devices in slot V3, and the capability to provide announcements and music on hold via “gateway-announcements” in logical slot V9.

```
change media-gateway 1                                     Page 2 of 2
                                                           MEDIA GATEWAY 1

Type: g450

Slot  Module Type      Name      DSP Type  FW/HW version
V1:    S8300           ICC MM    MP80      110 3
V2:    MM712           DCP MM
V3:    MM711           ANA MM
V4:
V5:
V6:
V7:
V8:
V9:    gateway-announcements ANN VMM

Max Survivable IP Ext: 8
```

IP telephones can be assigned a network region based on an IP address mapping. The network region can also associate the IP telephone to a location for location-based routing decisions. The following screen illustrates a subset of the IP network map configuration used to verify these Application Notes. If the IP address of a registering IP Telephone does not appear in the ip-network-map, the phone is assigned the network region of the “gatekeeper” (e.g., CLAN or PE) to which it registers. When the IP address of a registering IP telephone is in the ip-network-map, the phone is assigned the network region assigned by the form shown below. For example, the IP address 10.64.19.109 would be mapped to network region 1, based on the configuration in bold below. In production environments, different sites will typically be on different networks, and ranges of IP addresses assigned by the DHCP scope serving the site can be entered as one entry in the network map, to assign all telephones in a range to a specific network region.

change ip-network-map

Page 1 of 63

IP ADDRESS MAPPING

IP Address	Subnet Bits	Network Region VLAN	Emergency Location Ext
FROM: 10.64.19.100	/	1	n
TO: 10.64.19.120			

The following screen shows IP Network Region 2 configuration. In the shared test environment, network region 2 is used to allow unique behaviors for the Verizon test environment. In this example, codec set 2 will be used for calls within region 2. The shared Avaya Interoperability Lab test environment uses the domain “avayalab.com” (i.e., for network region 1 including the region of the Processor Ethernet “procr”). Session Manager also uses this domain to determined routes for calls based on the domain information of the calls and for SIP phone registration. Avaya SBCE will adapt “avayalab.com” to “adevc.avaya.globalipcom.com” for the From, PAI and Diversion headers.

change ip-network-region 2		Page 1 of 20
IP NETWORK REGION		
Region: 2		
Location: 1	Authoritative Domain: avayalab.com	
Name: Session Manager	Stub Network Region: n	
MEDIA PARAMETERS		
Codec Set: 2	Intra-region IP-IP Direct Audio: yes	
	Inter-region IP-IP Direct Audio: yes	
	IP Audio Hairpinning? n	
UDP Port Min: 2048		
UDP Port Max: 3329		
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		
H.323 IP ENDPOINTS		AUDIO RESOURCE RESERVATION PARAMETERS
		RSVP Enabled? n
H.323 Link Bounce Recovery? y		
Idle Traffic Interval (sec): 20		
Keep-Alive Interval (sec): 5		
Keep-Alive Count: 5		

The following screen shows the inter-network region connection configuration for region 2. The first bold row shows that network region 2 is directly connected to network region 1, and that codec set 2 will also be used for any connections between region 2 and region 1. For configurations where multiple remote gateways are used, each gateway will typically be configured for a different region, and this screen can be used to specify unique codec or call admission control parameters for the pairs of regions. If a different codec should be used for inter-region connectivity than for intra-region connectivity, a different codec set can be entered in the **codec set** column for the appropriate row in the screen shown below. Once submitted, the configuration becomes symmetric, meaning that network region 1, **Page 4** will also show codec set 2 for region 2 to region 1 connectivity.

change ip-network-region 2										Page	4 of 20
Source Region: 2										Inter Network Region Connection Management	
										I	M
										G	A
dst	codec	direct	WAN-BW-limits	Video	Intervening					Dyn	A
rgn	set	WAN	Units	Total Norm	Prio Shr	Regions				CAC	R
1	2	y	NoLimit							n	L
2	2										e
3											t
4										all	

The following screen shows IP Network Region 1 configuration. In this example, codec set 1 will be used for calls within region 1 due to the **Codec Set** parameter on **Page 1**, but codec set 2 will be used for connections between region 1 and region 2 as noted previously.

change ip-network-region 1										Page	1 of 20
										IP NETWORK REGION	
Region: 1											
Location: 1										Authoritative Domain: avayalab.com	
Name: Enterprise										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: 2048										IP Audio Hairpinning? n	
UDP Port Max: 3329											
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											
H.323 IP ENDPOINTS										AUDIO RESOURCE RESERVATION PARAMETERS	
H.323 Link Bounce Recovery? y										RSVP Enabled? n	
Idle Traffic Interval (sec): 20											
Keep-Alive Interval (sec): 5											
Keep-Alive Count: 5											

The following screen shows the inter-network region connection configuration for region 1. The bold row shows that network region 1 is directly connected to network region 2, and that codec set 2 will be used for any connections between region 2 and region 1.

change ip-network-region 1										Page	4 of	20					
Source Region: 1										Inter Network Region Connection Management				I	M		
										G	A	t					
dst codec direct										WAN-BW-limits	Video	Intervening	Dyn	A	G	c	
rgn set										WAN Units	Total Norm	Prio Shr	Regions	CAC	R	L	e
1										1							all
2										2	y	NoLimit			n		t

5.6. IP Codec Sets

The following screen shows the configuration for codec set 2, the codec set configured to be used for calls within region 2 and for calls between region 1 and region 2. In general, an IP codec set is a list of allowable codecs in priority order. Using the example configuration shown below, calls to and from the PSTN via the SIP trunks between devices capable of the G.722-64K codec (e.g., Avaya 9600-Series IP Telephone) can use G.722. While all other calls would use G.729A, since G.729A is the next preferred codec by both Verizon and the Avaya ip-codec-set. Include G.711MU in the ip-codec-set if fax will be used.

change ip-codec-set 2

Page 1 of 2

IP Codec Set

Codec Set: 2

	Audio	Silence	Frames	Packet
	Codec	Suppression	Per Pkt	Size(ms)
1:	G.722-64K		2	20
2:	G.729A	n	2	20
3:	G.711MU	n	2	20
4:				

The following screen shows **Page 2** of the form. Configure the **Fax Mode** field to “off” and set the **Fax Redundancy** field to “0”. See **Section 2.2** for more details regarding fax and the recommendation to use an AudioCodes MP-1xx for fax.

change ip-codec-set 2

Page 2 of 2

IP Codec Set

Allow Direct-IP Multimedia? n

	Mode	Redundancy
FAX	off	0
Modem	off	0
TDD/TTY	US	3
Clear-channel	n	0

The following screen shows the configuration for codec set 1. This configuration for codec set 1 is used for analog, digital, H.323, SIP phones and other connections within region 1.

change ip-codec-set 1				Page 1 of 2
IP Codec Set				
Codec Set: 1				
Audio	Silence	Frames	Packet	
Codec	Suppression	Per Pkt	Size (ms)	
1: G.722-64K		2	20	
2: G.711MU	n	2	20	
3:				
4:				

5.7. SIP Signaling Group

This section illustrates the configuration of the SIP Signaling Groups. Each signaling group has a **Group Type** of “sip”, a **Near-end Node Name** of “procr”, and a **Far-end Node Name** of “SM63”. In the example screens, the **Transport Method** for all signaling groups is “tls”. The **Peer Detection Enabled** field is set to “y” and a peer Session Manager has been previously detected. The **Far-end Domain** is set to “avayalab.com” matching the configuration in place prior to adding the Verizon IP SIP Trunking configuration. The **Enable Layer 3 Test** field is enabled on each of the signaling groups to allow Communication Manager to maintain the signaling group using the SIP OPTIONS method. Fields that are not referenced in the text below can be left at default values, including **DTMF over IP** set to “rtp-payload”, which corresponds to RFC 2833.

The following screen shows signaling group 1. Signaling group 1 will be used for processing PSTN calls to / from Verizon via Session Manager. The **Far-end Network Region** is configured to region 2. Port 5081 has been configured as both the **Near-end Listen Port** and **Far-end Listen Port**. Session Manager will be configured to direct calls arriving from the PSTN with Verizon DID numbers to a route policy that uses a SIP entity link to Communication Manager specifying port 5081. The use of different ports is one means to allow Communication Manager to distinguish different types of calls arriving from the same Session Manager. The **Initial IP-IP Direct Media?** is set to “n”. Other parameters may be left at default values.

The **Alternate Route Timer** that defaults to 6 seconds impacts fail-over timing for outbound calls. If Communication Manager does not get an expected response, Look-Ahead Routing (LAR) can be triggered, after the expiration of the Alternate Route Timer.

```

change signaling-group 1                                     Page 1 of 2
                                SIGNALING GROUP

Group Number: 1                      Group Type: sip
IMS Enabled? n                      Transport Method: tls
    Q-SIP? n
    IP Video? n                      Enforce SIPS URI for SRTP? y
Peer Detection Enabled? y Peer Server: SM
Prepend '+' to Outgoing Calling/Alerting/Diverting/Connected Public Numbers? y
Remove '+' from Incoming Called/Calling/Alerting/Diverting/Connected Numbers? n

Near-end Node Name: procr                Far-end Node Name: SM63
Near-end Listen Port: 5081                Far-end Listen Port: 5081
                                           Far-end Network Region: 2

Far-end Domain: avayalab.com

Incoming Dialog Loopbacks: eliminate      Bypass If IP Threshold Exceeded? n
                                           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? n
H.323 Station Outgoing Direct Media? n    Alternate Route Timer(sec): 6

```

The following screen shows signaling group 3, the signaling group to Session Manager that was in place prior to adding the Verizon IP Trunk configuration to the shared Avaya Solutions and Interoperability Test Lab configuration. This signaling group reflects configuration not specifically related to Verizon IP Trunk but will be used to enable SIP phones to register to Session Manager and to use features from Communication Manager. Again, the **Near-end Node Name** is “procr” and the **Far-end Node Name** is “SM63”, the node name of the Session Manager. Unlike the signaling group used for the Verizon IP Trunk signaling, the **Far-end Network Region** is “1”. The **Peer Detection Enabled** field is set to “y” and a peer Session Manager has been previously detected.

```

change signaling-group 3                                     Page 1 of 2
                                SIGNALING GROUP

Group Number: 3                      Group Type: sip
IMS Enabled? n                      Transport Method: tls
    Q-SIP? n
    IP Video? n                      Enforce SIPS URI for SRTP? y
Peer Detection Enabled? y Peer Server: SM
Prepend '+' to Outgoing Calling/Alerting/Diverting/Connected Public Numbers? y
Remove '+' from Incoming Called/Calling/Alerting/Diverting/Connected Numbers? n

Near-end Node Name: procr                Far-end Node Name: SM63
Near-end Listen Port: 5061                Far-end Listen Port: 5061
                                           Far-end Network Region: 1

Far-end Domain: avayalab.com

Incoming Dialog Loopbacks: eliminate      Bypass If IP Threshold Exceeded? n
                                           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? n
H.323 Station Outgoing Direct Media? n    Alternate Route Timer(sec): 6

```

5.8. SIP Trunk Group

This section illustrates the configuration of the SIP Trunk Groups corresponding to the SIP signaling group from the previous section.

The following shows **Page 1** for trunk group 1, which will be used for incoming and outgoing PSTN calls from Verizon. The **Number of Members** field defines how many simultaneous calls are permitted for the trunk group. The **Service Type** field is set to “public-ntwrk” for the trunks that will handle calls with Verizon. The **Direction** has been configured to “two-way” to allow incoming and outgoing calls in the sample configuration.

change trunk-group 1		Page 1 of 21	
TRUNK GROUP			
Group Number: 1	Group Type: sip	CDR Reports: y	
Group Name: OUTSIDE CALL	COR: 1	TN: 1	TAC: *01
Direction: two-way	Outgoing Display? n		
Dial Access? n	Night Service:		
Queue Length: 0			
Service Type: public-ntwrk	Auth Code? n	Member Assignment Method: auto	
		Signaling Group: 1	
		Number of Members: 10	

The following screen shows **Page 2** for trunk group 1. All parameters shown are default values, except for the **Preferred Minimum Session Refresh Interval**, which has been changed from the default 600 to 900. Although not strictly necessary, some SIP products prefer a higher session refresh interval than the Communication Manager default value, which can result in unnecessary SIP messages to re-establish a higher refresh interval for each call.

change trunk-group 1		Page 2 of 21	
Group Type: sip			
TRUNK PARAMETERS			
Unicode Name: auto		Redirect On OPTIM Failure: 5000	
SCCAN? n	Digital Loss Group: 18		
Preferred Minimum Session Refresh Interval(sec): 900			
Disconnect Supervision - In? y Out? y			
XOIP Treatment: auto		Delay Call Setup When Accessed Via IGAR? n	

The following screen shows **Page 3** for trunk group 1. All parameters except those in bold are default values. The **Numbering Format** will use “private” numbering, meaning that the private numbering table would be consulted for any mappings of Communication Manager extensions to alternate numbers to be sent to Session Manager.

change trunk-group 1		Page 3 of 21
TRUNK FEATURES		
ACA Assignment? n	Measured: none	Maintenance Tests? y
Numbering Format: private		
UI Treatment: service-provider		
Replace Restricted Numbers? n		
Replace Unavailable Numbers? n		
Modify Tandem Calling Number: no		
Show ANSWERED BY on Display? y		

The following screen shows **Page 4** for trunk group 1. The bold fields have non-default values. The **Convert 180 to 183 for Early Media** field was new in Communication Manager Release 6. Verizon recommends that inbound calls to the enterprise result in a 183 with SDP rather than a 180 with SDP, and setting this field to “y” for the trunk group handling inbound calls from Verizon produces this result. Although not strictly necessary, the **Telephone Event Payload Type** has been set to 101 to match Verizon configuration. Setting the **Network Call Redirection** flag to “y” enables advanced services associated with the use of the REFER message, while also implicitly enabling Communication Manager to signal “send-only” media conditions for calls placed on hold at the enterprise site. If neither REFER signaling nor “send-only” media signaling is required, this field may be left at the default “n” value. In the testing associated with these Application Notes, transfer testing using REFER was successfully completed with the **Network Call Redirection** flag set to “y”, and transfer testing using INVITE was successfully completed with the **Network Call Redirection** flag set to “n”.

For redirected calls, Verizon supports the Diversion header, but not the History-Info header. Communication Manager can send the Diversion header by marking **Send Diversion Header** to “y”. Alternatively, Communication can send the History-Info header by setting **Support Request History** to “y”, and Session Manager can adapt the History-Info header to the Diversion header using the “VerizonAdapter”. In the testing associated with these Application Notes, call redirection testing with Communication Manager sending History-Info and Session Manager adapting to Diversion Header was completed successfully.

change trunk-group 1	Page 4 of 21
PROTOCOL VARIATIONS	
Mark Users as Phone? n Prepend '+' to Calling/Alerting/Diverting/Connected Number? n Send Transferring Party Information? n Network Call Redirection? y Build Refer-To URI of REFER From Contact For NCR? n Send Diversion Header? n Support Request History? y Telephone Event Payload Type: 101	
Convert 180 to 183 for Early Media? y Always Use re-INVITE for Display Updates? n Identity for Calling Party Display: P-Asserted-Identity Block Sending Calling Party Location in INVITE? n Accept Redirect to Blank User Destination? n Enable Q-SIP? n	

The following screen shows **Page 1** for trunk group 3, the bi-directional “tie” trunk group to Session Manager that existed before adding the Verizon SIP Trunk configuration to the shared Avaya Interoperability Lab network. Recall that this trunk is used to enable SIP phones to use features from Communication Manager and to communicate with other Avaya applications, such as Avaya Aura® Messaging, and does not reflect any unique Verizon configuration.

change trunk-group 3	Page 1 of 21		
TRUNK GROUP			
Group Number: 3	Group Type: sip	CDR Reports: y	
Group Name: To SM Enterprise	COR: 1	TN: 1	TAC: *03
Direction: two-way	Outgoing Display? n	Night Service:	
Dial Access? n			
Queue Length: 0			
Service Type: tie	Auth Code? n		
Member Assignment Method: auto			
Signaling Group: 3			
Number of Members: 20			

The following shows **Page 3** for trunk group 3. Note that this tie trunk group uses a “private” **Numbering Format**.

change trunk-group 3	Page 3 of 21	
TRUNK FEATURES		
ACA Assignment? n	Measured: none	
	Maintenance Tests? y	
Numbering Format: private	UII Treatment: service-provider	
	Replace Restricted Numbers? n	
	Replace Unavailable Numbers? n	
Modify Tandem Calling Number: no		

The following screen shows **Page 4** for trunk group 3. Note that unlike the trunks associated with Verizon calls that have non-default “protocol variations”, this trunk group maintains all default

values. **Support Request History** must remain set to the default “y” to support proper subscriber mailbox identification by Communication Manager Messaging.

change trunk-group 3	Page 4 of 21
PROTOCOL VARIATIONS <div> Mark Users as Phone? n Prepend '+' to Calling/Alerting/Diverting/Connected Number? n Send Transferring Party Information? n Network Call Redirection? n Send Diversion Header? n Support Request History? y Telephone Event Payload Type: 120 Convert 180 to 183 for Early Media? y Always Use re-INVITE for Display Updates? n Identity for Calling Party Display: P-Asserted-Identity Block Sending Calling Party Location in INVITE? n Accept Redirect to Blank User Destination? n Enable Q-SIP? n </div>	

5.9. Route Pattern Directing Outbound Calls to Verizon

Route pattern 1 will be used for calls destined for the PSTN via the Verizon IP Trunk service. Set the Facility Restriction Level (**FRL**) field to a level that allows access to this trunk for all users that require it. The value of “0” is the least restrictive level. The **Numbering Format** “unk-unk” means no special numbering format will be included.

If desired, one or more alternate Communication Manager trunks can be listed in the route pattern so that the Look-Ahead Routing (**LAR**) “next” setting can route-advance to attempt to complete the call using alternate trunks should there be no response or an error response from the far-end.

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

5.10. Route Pattern for Internal Calls via Session Manager

Route pattern 3 contains trunk group 3, the “private” tie trunk group to Session Manager. The **Numbering Format** “lev0-pvt” insures proper numbering format for internal local calls to Session Manager.

change route-pattern 3												Page 1 of 3	
Pattern Number: 3												Pattern Name: ToSM Enterprise	
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:	3	0										n	user
2:											n	user	
3:											n	user	
4:											n	user	
5:											n	user	
6:											n	user	
BCC VALUE				TSC	CA-TSC	ITC BCIE				Service/Feature	PARM	No. Numbering	LAR
0	1	2	M	4	W	Request				Dgts Format			
										Subaddress			
1:	y	y	y	y	y	y	n	bothept				lev0-pvt	none
2:	y	y	y	y	y	n	n	rest					none
3:	y	y	y	y	y	n	n	rest					none
4:	y	y	y	y	y	n	n	rest					none
5:	y	y	y	y	y	n	n	rest					none
6:	y	y	y	y	y	n	n	rest					none

5.11. Private Numbering

The *change private-unknown-numbering* command may be used to define the format of numbers sent to Verizon in SIP headers such as the “From” and “PAI” headers. In general, the mappings of internal extensions to Verizon DID numbers may be done in Communication Manager (via private-numbering form for outbound calls, and incoming call handling treatment form for the inbound trunk group).

In the example abridged output below, a specific Communication Manager extension (x12001) is mapped to a DID number that is known to Verizon for this SIP Trunk connection (7329450231), when the call uses trunk group 1. Alternatively, Communication Manager can send the five digit extension to Session Manager, and Session Manager can adapt the number to the Verizon DID. Both methods were tested successfully.

change private-numbering 0					Page 1 of 2	
NUMBERING - PRIVATE FORMAT						
Ext	Ext	Trk	Private	Total		
Len	Code	Grp(s)	Prefix	Len		
5	10			5	Total Administered: 5	
5	12			5	Maximum Entries: 540	
5	14			5		
5	20			5		
5	12001	1	7329450231	10		

5.12. ARS Routing For Outbound Calls

Although not illustrated in these Application Notes, location-based routing may be configured so that users at different locations that dial the same telephone number can have calls choose different route-patterns. In these Application Notes, the ARS “all locations” table directs ARS calls to specific SIP Trunks to Session Manager.

The following screen shows a specific ARS configuration as an example. If a user dials the ARS access code followed by 13035387024, the call will select route pattern 1. Of course, matching of the dialed string need not be this specific. The ARS configuration shown here is not intended to be prescriptive.

change ars analysis 13035387022							Page 1 of 2
ARS DIGIT ANALYSIS TABLE							
Location: all				Percent Full: 1			
Dialed String	Total Min	Total Max	Route Pattern	Call Type	Node Num	ANI Reqd	
13035387024	11	11	1	fnpa		n	

The *list ars route-chosen* command can be used on a target dialed number to check whether routing will behave as intended. An example is shown below.

list ars route-chosen 13035387024						
ARS ROUTE CHOSEN REPORT						
Location: 1		Partitioned Group Number: 1				
Dialed String	Total Min	Total Max	Route Pattern	Call Type	Node Number	Location
13035387024	11	11	1	fnpa		all
Actual Outpulsed Digits by Preference (leading 35 of maximum 42 digit)						
1: 13035387024						

5.13. Avaya Aura® Communication Manager Stations

In the sample configuration, five digit station extensions were used with the format 12xxx, and 14xxx. The following abbreviated screen shows an example extension for an Avaya H.323 IP telephone.

change station 12002		Page	1 of	5
STATION				
Extension: 12002	Lock Messages? n	BCC:	0	
Type: 9621	Security Code: *	TN:	1	
Port: S00025	Coverage Path 1:	COR:	1	
Name: test IP	Coverage Path 2:	COS:	1	
	Hunt-to Station:	Tests?	y	
STATION OPTIONS				
	Time of Day Lock Table:			
Loss Group: 19	Personalized Ringing Pattern: 1			
	Message Lamp Ext: 12002			
Speakerphone: 2-way	Mute Button Enabled? y			
Display Language: english				
Survivable GK Node Name:				

5.14. EC500 Configuration for Diversion Header Testing

When EC500 is enabled for a Communication Manager station, a call to that station will generate a new outbound call from Communication Manager to the configured EC500 destination, typically a mobile phone. The following screen shows an example EC500 configuration for the user with station extension 12005. Use the command *change off-pbx-telephone station mapping x* where *x* is Communication Manager station (e.g. 12002).

- **Station Extension** – This field will automatically populate
- **Application** – Enter “EC500”
- **Dial Prefix** – Enter a prefix (e.g., 1) if required by the routing configuration
- **Phone Number** – Enter the phone that will also be called (e.g., 3035387024)
- **Trunk Selection** – Enter “ars”. This means ARS will be used to determine how Communication Manager will route to the **Phone Number** destination.
- **Config Set** – Enter “1”
- Other parameters can retain default values

change off-pbx-telephone station-mapping 12002							Page	1 of	3
STATIONS WITH OFF-PBX TELEPHONE INTEGRATION									
Station	Application	Dial	CC	Phone Number	Trunk	Config	Dual		
Extension		Prefix			Selection	Set	Mode		
12002	EC500	-	1	3035387024	ars	1			

5.15. Saving Communication Manager Configuration Changes

The command *save translation all* can be used to save the configuration.

save translation all	
SAVE TRANSLATION	
Command Completion Status	Error Code
Success	0

6. Configure Avaya Aura® Session Manager Release 6.3

This section illustrates relevant aspects of the Session Manager configuration used in the verification of these Application Notes.

Note – The following sections assume that Session Manager and System Manager have been installed and that network connectivity exists between System Manager and Session Manager.

Session Manager is managed via System Manager. Using a web browser, access “https://<ip-addr of System Manager>/SMGR”. In the **Log On** screen, enter appropriate **User ID** and **Password** and press the **Log On** button (not shown).

AVAYA Avaya Aura® System Manager 6.3

Home / Log On

Log On

Recommended access to System Manager is via FQDN.
[Go to central login for Single Sign-On](#)

If IP address access is your only option, then note that authentication will fail in the following cases:

- First time login with "admin"

User ID:

Password:

Once logged in, a **Home Screen** is displayed. An abridged **Home Screen** is shown below.

Users

- [Administrators](#)
Manage Administrative Users
- [Directory Synchronization](#)
Synchronize users with the enterprise directory
- [Groups & Roles](#)
Manage groups, roles and assign roles to users
- [User Management](#)
Manage users, shared user resources and provision users

Elements

- [B5800 Branch Gateway](#)
Manage B5800 Branch Gateway 6.2 elements
- [Communication Manager](#)
Manage Communication Manager 5.0 and higher elements
- [Communication Server 1000](#)
Manage Communication Server 1000 elements
- [Conferencing](#)
Manage Conferencing Multimedia Server objects
- [Inventory](#)
Manage, discover, and navigate to elements, update element software
- [Meeting Exchange](#)
Manage Meeting Exchange and Avaya Aura Conferencing 6.0 elements
- [Messaging](#)
Manage Avaya Aura Messaging, Communication Manager Messaging, and Modular Messaging
- [Presence](#)
Presence
- [Routing](#)
Session Manager Routing Administration
- [Session Manager](#)
Session Manager Administration, Status, Maintenance and Performance Management

Services

- [Backup and Restore](#)
Backup and restore System Manager database
- [Bulk Import and Export](#)
Manage Bulk Import and Export of Users, User Global Settings, Roles, Elements and others
- [Configurations](#)
Manage system wide configurations
- [Events](#)
Manage alarms, view and harvest logs
- [Geographic Redundancy](#)
Manage Geographic Redundancy
- [Licenses](#)
View and configure licenses
- [Replication](#)
Track data replication nodes, repair replication nodes
- [Scheduler](#)
Schedule, track, cancel, update and delete jobs
- [Security](#)
Manage Security Certificates
- [Shutdown](#)
Shutdown System Manager Gracefully
- [Templates](#)
Manage Templates for Messaging System objects

Under the heading “Elements” in the center, select **Routing**. The right side of the screen, illustrated below, outlines a series of steps. The sub-sections that follow are in the same order as the steps outlined under **Introduction to Network Routing Policy** in the abridged screen shown below.

Introduction to Network Routing Policy

Network Routing Policy consists of several routing applications like "Domains", "Locations", "SIP Entities", etc.

The recommended order to use the routing applications (that means the overall routing workflow) to configure your network configuration is as follows:

Step 1: Create "Domains" of type SIP (other routing applications are referring domains of type SIP).

Step 2: Create "Locations"

Step 3: Create "Adaptations"

Step 4: Create "SIP Entities"

- SIP Entities that are used as "Outbound Proxies" e.g. a certain "Gateway" or "SIP Trunk"
- Create all "other SIP Entities" (Session Manager, CM, SIP/PSTN Gateways, SIP Trunks)
- Assign the appropriate "Locations", "Adaptations" and "Outbound Proxies"

Step 5: Create the "Entity Links"

- Between Session Managers
- Between Session Managers and "other SIP Entities"

Step 6: Create "Time Ranges"

- Align with the tariff information received from the Service Providers

Step 7: Create "Routing Policies"

- Assign the appropriate "Routing Destination" and "Time Of Day"
- (Time Of Day = assign the appropriate "Time Range" and define the "Ranking")

Step 8: Create "Dial Patterns"

- Assign the appropriate "Locations" and "Routing Policies" to the "Dial Patterns"

Step 9: Create "Regular Expressions"

- Assign the appropriate "Routing Policies" to the "Regular Expressions"

Scroll down to review additional information as shown below. In these Application Notes, all steps are illustrated with the exception of Step 9, since “Regular Expressions” were not used.

Each "Routing Policy" defines the "Routing Destination" (which is a "SIP Entity") as well as the "Time of Day" and its associated "Ranking".

IMPORTANT: the appropriate dial patterns are defined and assigned afterwards with the help of the routing application "Dial patterns". That's why this overall routing workflow can be interpreted as

"Dial Pattern driven approach to define Routing Policies"

That means (with regard to steps listed above):

Step 7: "Routing Policies" are defined

Step 8: "Dial Patterns" are defined and assigned to "Routing Policies" and "Locations" (one step)

Step 9: "Regular Expressions" are defined and assigned to "Routing Policies" (one step)

6.1. Domains

To view or change SIP domains, select **Routing → Domains**. Click on the checkbox next to the name of the SIP domain and **Edit** to edit an existing domain, or the **New** button to add a domain. Click the **Commit** button after changes are completed.

The following screen shows a list of configured SIP domains. The Session Manager used in the verification of these Application Notes was shared among other Avaya interoperability test efforts. The domain “avayalab.com” was used for communication with Avaya SIP Telephones and other Avaya systems and applications. The domain “avayalab.com” is not known to the Verizon production service.

The domain “adevc.avaya.globalipcom.com” is the domain known to Verizon as the enterprise SIP domain. For example, for calls from the enterprise site to Verizon, this domain can appear in the From and P-Asserted-Identity headers in the INVITE message sent to Verizon.

The screenshot shows the 'Domain Management' interface. At the top, there is a breadcrumb trail: 'Home / Elements / Routing / Domains'. Below this, there are buttons for 'New', 'Edit', 'Delete', 'Duplicate', and 'More Actions'. A table lists 2 items with columns for 'Name', 'Type', and 'Notes'. The first item is 'adevc.avaya.globalipcom.com' with type 'sip' and note 'CPE Domain known by Verizon'. The second item is 'avayalab.com' with type 'sip' and note 'Avaya SIL Domain'. There is a 'Filter: Enable' option and a 'Select: All, None' option at the bottom.

<input type="checkbox"/>	Name	Type	Notes
<input type="checkbox"/>	adevc.avaya.globalipcom.com	sip	CPE Domain known by Verizon
<input type="checkbox"/>	avayalab.com	sip	Avaya SIL Domain

6.2. Locations

To view or change locations, select **Routing → Locations**. The following screen shows an abridged list of configured locations. Click on the checkbox corresponding to the name of a location and **Edit** to edit an existing location, or the **New** button to add a location. Click the **Commit** button (not shown) after changes are completed. Assigning unique locations can allow Session Manager to perform location-based routing, bandwidth management, and call admission control.

The screenshot shows the 'Location' management interface. At the top, there is a breadcrumb trail: 'Home / Elements / Routing / Locations'. Below this, there are buttons for 'New', 'Edit', 'Delete', 'Duplicate', and 'More Actions'. A table lists 3 items with columns for 'Name' and 'Notes'. The first item is 'Loc19-CM' with note 'Location 19 CM'. The second item is 'SM-Denver' with note 'Session Manager'. The third item is 'Vz-ASBCE' with note 'SBC to Verizon'. There is a 'Filter: Enable' option and a 'Select: All, None' option at the bottom.

<input type="checkbox"/>	Name	Notes
<input type="checkbox"/>	Loc19-CM	Location 19 CM
<input type="checkbox"/>	SM-Denver	Session Manager
<input type="checkbox"/>	Vz-ASBCE	SBC to Verizon

The following screen shows the location details for the location named “Vz-ASBCE”, corresponding to the Avaya SBCE relevant to these Application Notes. Later, the location with name “Vz-ASBCE” will be assigned to the corresponding Avaya SBCE SIP Entity.

The **Location Pattern** is used to identify call routing based on IP address. Session Manager matches the IP address of SIP Entities against the patterns defined in this section. If a call is from a SIP Entity that does not match the IP address pattern then Session Manager uses the Location administered in the SIP Entity form. In this sample configuration Locations are added to SIP Entities in **Section 6.4**, so it is not necessary to add a pattern.

Home / Elements / Routing / Locations

Help ?

Commit Cancel

Location Details

General

* Name:

Vz-ASBCE

Notes:

SBC to Verizon

Overall Managed Bandwidth

Managed Bandwidth Units:

Kbit/sec

Total Bandwidth:

Multimedia Bandwidth:

Audio Calls Can Take Multimedia Bandwidth:

☒

Per-Call Bandwidth Parameters

Maximum Multimedia Bandwidth (Intra-Location):

1000

Kbit/Sec

Maximum Multimedia Bandwidth (Inter-Location):

1000

Kbit/Sec

* Minimum Multimedia Bandwidth:

64

Kbit/Sec

* Default Audio Bandwidth:

80

Kbit/sec

Alarm Threshold

Overall Alarm Threshold:

80

%

Multimedia Alarm Threshold:

80

%

* Latency before Overall Alarm Trigger:

5

Minutes

* Latency before Multimedia Alarm Trigger:

5

Minutes

Location Pattern

Add

Remove

0 Items | Refresh

Filter: Enable

	IP Address Pattern	Notes
--	--------------------	-------

The following screen shows the location details for the location named “Loc19-CM”, corresponding to Communication Manager. Later, the location with name “Loc19-CM” will be assigned to the corresponding Communication Manager SIP Entity. In the sample configuration, other location parameters (not shown) retained the default values.

The screenshot shows a web interface for configuring a location. At the top, a breadcrumb trail reads 'Home / Elements / Routing / Locations'. Below this, the title 'Location Details' is displayed on the left, and 'Commit' and 'Cancel' buttons are on the right, along with a 'Help ?' link. The 'General' tab is selected. The 'Name' field is labeled with a red asterisk and contains the text 'Loc19-CM'. The 'Notes' field contains the text 'Location 19 CM'.

The following screen shows the location details for the location named “SM-Denver”, corresponding to Session Manager. This location was created during the installation of Session Manager and was assigned to the Session Manager SIP Entity. In the sample configuration, other location parameters (not shown) retained the default values.

The screenshot shows a web interface for configuring a location. At the top, a breadcrumb trail reads 'Home / Elements / Routing / Locations'. Below this, the title 'Location Details' is displayed on the left, and 'Commit' and 'Cancel' buttons are on the right, along with a 'Help ?' link. The 'General' tab is selected. The 'Name' field is labeled with a red asterisk and contains the text 'SM-Denver'. The 'Notes' field contains the text 'Session Manager'.

6.3. Adaptations

To view or change adaptations, select **Routing → Adaptations**. Click on the checkbox corresponding to the name of an adaptation and **Edit** to edit an existing adaptation, or the **New** button to add an adaptation. Click the **Commit** button after changes are completed (not shown).

Home / Elements / Routing / Adaptations				
Adaptations				
New Edit Delete Duplicate More Actions				
7 Items Refresh Filter: Enable				
<input type="checkbox"/>	Name	Module name	Egress URI Parameters	Notes
<input type="checkbox"/>	AuraMsg	DigitConversionAdapter fromto=true		7 digit mailbox conversion
<input type="checkbox"/>	CM63-TG1-IPT-IDA	DigitConversionAdapter fromto=true osrcd=avayalab.com		CM - Verizon IPT - IDA
<input type="checkbox"/>	CM63-TG1-VzIPT	DigitConversionAdapter fromto=true osrcd=avayalab.com		CM - Verizon IPT
<input type="checkbox"/>	CM63-TG2-VzIPCC	DigitConversionAdapter fromto=true osrcd=avayalab.com		CM - Verizon IPCC
<input type="checkbox"/>	VerizonIPCC-SBC	VerizonAdapter fromto=true osrcd=adevc.avaya.globalipcc.com odstcd=199.173.94.16		SBC - Verizon IPCC
<input type="checkbox"/>	VerizonIPT-IDA to Avaya	VerizonAdapter fromto=true osrcd=icrcn1n0002.customer08.tsengr.com		SBC - Verizon IPT-IDA
<input type="checkbox"/>	VerizonIPT-SBC	VerizonAdapter fromto=true		SBC - Verizon IPT
Select : All, None				

The adapter named “VerizonIPT-SBC” shown below will later be assigned to the SIP Entity for the Avaya SBCE, specifying that all communication from Session Manager to the Avaya SBCEs will use this adapter.

This adaptation uses the “VerizonAdapter” module and specifies the “fromto=true” parameter. This parameter adapts the From and To headers along with the Request-Line and PAI headers.

Home / Elements / Routing / Adaptations		Help ?
Adaptation Details		Commit Cancel
General		
* Adaptation name:	<input type="text" value="VerizonIPT-SBC"/>	
Module name:	<input type="text" value="VerizonAdapter"/>	
Module parameter:	<input type="text" value="fromto=true"/>	
Egress URI Parameters:	<input type="text"/>	
Notes:	<input type="text" value="SBC - Verizon IPT"/>	

Scrolling down to the **Digit Conversion for Incoming Calls to SM** section, the following screen shows the addition of the 10 digit DID numbers assigned by Verizon intended for fax calls converted to the extension numbers used by the AudioCodes gateway.

Digit Conversion for Incoming Calls to SM

Add Remove

1 Item Refresh Filter: Enable

<input type="checkbox"/>	Matching Pattern	Min	Max	Phone Context	Delete Digits	Insert Digits	Address to modify	Adaptation Data	Notes
<input type="checkbox"/>	* 7329450231	* 10	* 10		* 10	17555	both		

Select : All, None

Scrolling down to the **Digit Conversion for Outgoing Calls from SM** section, the following screen shows an example configuration for Verizon’s Unscreened ANI feature. This optional configuration allows customers to send an “unscreened” ANI to Verizon’s network which is then displayed to the called party as Caller ID. An “unscreened” ANI can be any telephone number that the customer passes through Verizon’s network for Caller ID display purposes only. If this feature is enabled on the Verizon IP Trunk services, Verizon will designate one of the assigned telephone numbers as a “Screened Telephone Number” for each unique location. Verizon will use this Screened Telephone Number to determine call origination for billing, call routing, and E911.

The Screened Telephone Number (STN) provided by Verizon for this test is 732-945-0821. Typically, customers would have one or more STN; one for every location. A central Session Manager could be used to pass multiple STNs to Verizon based on a **Matching Pattern** (i.e., a user’s Calling Line Identification). The STN would then be entered in the **Adaptation Data** field as shown below.

Digit Conversion for Outgoing Calls from SM

Add Remove

1 Item Refresh Filter: Enable

<input type="checkbox"/>	Matching Pattern	Min	Max	Phone Context	Delete Digits	Insert Digits	Address to modify	Adaptation Data	Notes
<input type="checkbox"/>	* 408990883x	* 10	* 10		* 0		origination	7329450821	Unscreened ANI - Diversion

Select : All, None

The following screen shows the addition of extension numbers used on Communication Manager that are being converted to the 10 digit DID numbers assigned by Verizon. Since this adapter will be assigned to the SIP Entity sending calls to Avaya SBCE for routing to the PSTN, the settings for **Digit Conversion for Outgoing Calls from SM** correspond with outgoing calls from Communication Manager to the PSTN using the Verizon IP Trunk service. In general, digit conversion such as this, that converts a Communication Manager extension (e.g., 12xxx) to a corresponding LDN or DID number known to the PSTN (e.g., 73294502xx), can be performed in Session Manager as shown below. For example, if extension 12001 dials the PSTN, and if Communication Manager sends the extension 12001 to Session manager as the calling number, Session Manager would convert the calling number to 7329450231.

Digit Conversion for Outgoing Calls from SM

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

6 Items | [Refresh](#) Filter: [Enable](#)

<input type="checkbox"/>	Matching Pattern ^	Min	Max	Phone Context	Delete Digits	Insert Digits	Address to modify	Adaptation Data	Notes
<input type="checkbox"/>	* 10000	* 5	* 5		* 5	7329450243	origination		
<input type="checkbox"/>	* 12000	* 5	* 5		* 5	7329450241	origination		
<input type="checkbox"/>	* 12001	* 5	* 5		* 5	7329450231	origination		
<input type="checkbox"/>	* 12002	* 5	* 5		* 5	7329450232	origination		
<input type="checkbox"/>	* 12003	* 5	* 5		* 5	7329450233	origination		
<input type="checkbox"/>	* 408990883x	* 10	* 10		* 10		origination	7329450821	Unscreened ANI - Diversic

Select : All, None

The adapter named “CM63-TG1-VzIPT” shown in the following screen will later be assigned to the SIP Entity linking Session Manager to Communication Manager for calls involving Verizon Business IP Trunk service. This adaptation uses the “DigitConversionAdapter” and specifies the following parameters:

- “fromto=true”. This adapts the From and To headers along with the Request-Line and PAI headers.
- “osrcd=avayalab.com”. This enables the source domain to be overwritten with “avayalab.com”. For example, for inbound PSTN calls from Verizon to Communication Manager, the PAI header will contain “avayalab.com”.

Depending on the Communication Manager configuration, it may not be necessary for Session Manager to adapt the domain in this fashion.

Home / Elements / Routing / Adaptations [Help ?](#)

Adaptation Details [Commit](#) [Cancel](#)

General

* Adaptation name:

Module name:

Module parameter:

Egress URI Parameters:

Notes:

Scrolling down, the following screen shows a portion of the “CM63-TG1-VzIPT” adapter that can be used to convert 10 digit DID numbers assigned by Verizon to the extension number used on Communication Manager. Since this adapter will be assigned to the SIP Entity sending calls to Communication Manager from the PSTN, the settings for **Digit Conversion for Outgoing Calls from SM** correspond to incoming calls from the PSTN to Communication Manager. In the example shown below, if a user on the PSTN dials 732-945-0231, Session Manager will convert the number to 12001 before sending the SIP INVITE to Communication Manager. In this case, digit conversion is done after the routing decision has been made based upon the user part of the SIP URI. As such, it would not be necessary to use the incoming call handling table of the

receiving Communication Manager trunk group to convert the DID number to its corresponding extension.

Digit Conversion for Outgoing Calls from SM

Add
Remove

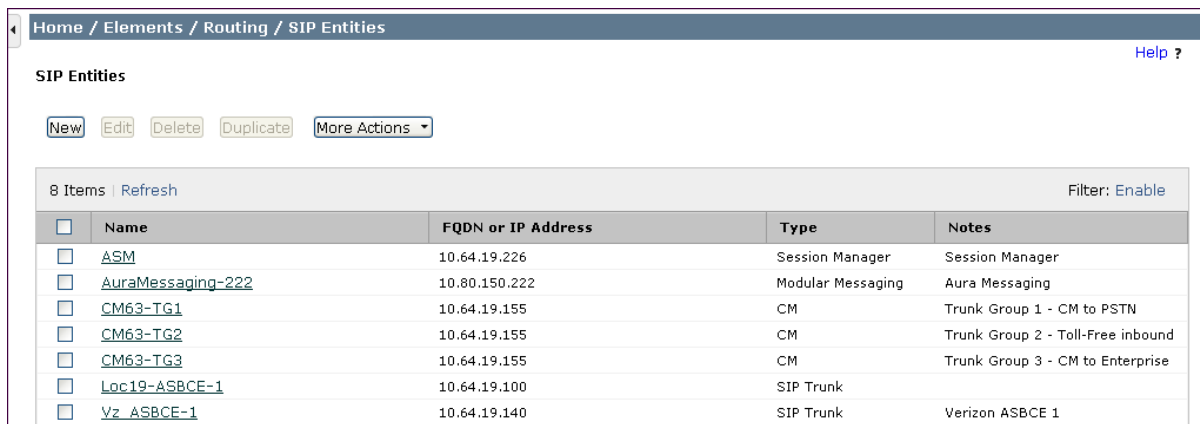
13 Items
Refresh
Filter: Enable

	Matching Pattern	Min	Max	Phone Context	Delete Digits	Insert Digits	Address to modify	Adaptation Data	Notes
<input type="checkbox"/>	* 7329450243	* 10	* 10		* 10	10000	destination		
<input type="checkbox"/>	* 7329450241	* 10	* 10		* 10	12000	destination		
<input type="checkbox"/>	* 7329450231	* 10	* 10		* 10	12001	destination		
<input type="checkbox"/>	* 7329450232	* 10	* 10		* 10	12002	destination		
<input type="checkbox"/>	* 7329450233	* 10	* 10		* 10	12003	destination		

6.4. SIP Entities

To view or change SIP entities, select **Routing → SIP Entities**. Click the checkbox corresponding to the name of an entity and **Edit** to edit an existing entity, or the **New** button to add an entity. Click the **Commit** button after changes are completed.

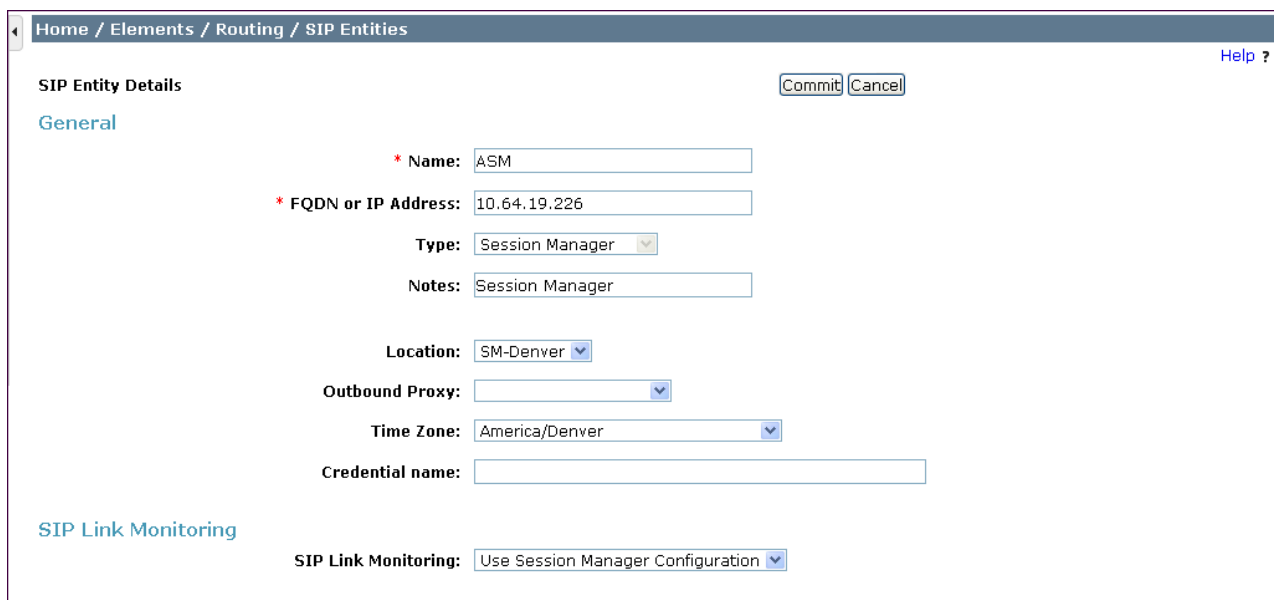
The following screen shows the list of configured SIP entities in the shared test environment.



The screenshot shows the 'SIP Entities' page with a breadcrumb trail 'Home / Elements / Routing / SIP Entities'. Below the title are buttons for 'New', 'Edit', 'Delete', 'Duplicate', and a 'More Actions' dropdown. A table lists 8 items with columns for Name, FQDN or IP Address, Type, and Notes. The entities listed are ASM, AuraMessaging-222, CM63-TG1, CM63-TG2, CM63-TG3, Loc19-ASBCE-1, and Vz_ASBCE-1.

<input type="checkbox"/>	Name	FQDN or IP Address	Type	Notes
<input type="checkbox"/>	ASM	10.64.19.226	Session Manager	Session Manager
<input type="checkbox"/>	AuraMessaging-222	10.80.150.222	Modular Messaging	Aura Messaging
<input type="checkbox"/>	CM63-TG1	10.64.19.155	CM	Trunk Group 1 - CM to PSTN
<input type="checkbox"/>	CM63-TG2	10.64.19.155	CM	Trunk Group 2 - Toll-Free inbound
<input type="checkbox"/>	CM63-TG3	10.64.19.155	CM	Trunk Group 3 - CM to Enterprise
<input type="checkbox"/>	Loc19-ASBCE-1	10.64.19.100	SIP Trunk	
<input type="checkbox"/>	Vz_ASBCE-1	10.64.19.140	SIP Trunk	Verizon ASBCE 1

The following screen shows the upper portion of the **SIP Entity Details** corresponding to “ASM”. The **FQDN or IP Address** field for “ASM” is the Session Manager Security Module IP Address (10.64.19.226), which is used for SIP signaling with other networked SIP entities. The **Type** for this SIP entity is “Session Manager”. Select an appropriate location for the Session Manager from the **Location** drop-down menu. In the shared test environment, the Session Manager used location “SM-Denver”. The default **SIP Link Monitoring** parameters may be used. Unless changed elsewhere, links from other SIP entities to this instance of Session Manager will use the default SIP Link Monitoring timers, configurable at the Session Manager level. If desired, these timers may be customized for each entity.



The screenshot shows the 'SIP Entity Details' page for the 'ASM' entity. It includes a 'General' section with fields for Name, FQDN or IP Address, Type, Notes, Location, Outbound Proxy, Time Zone, and Credential name. There is also a 'SIP Link Monitoring' section with a dropdown for 'SIP Link Monitoring'.

SIP Entity Details [Commit] [Cancel]

General

* Name: ASM

* FQDN or IP Address: 10.64.19.226

Type: Session Manager

Notes: Session Manager

Location: SM-Denver

Outbound Proxy:

Time Zone: America/Denver

Credential name:

SIP Link Monitoring

SIP Link Monitoring: Use Session Manager Configuration

Scrolling down, the following screen shows the middle portion of the **SIP Entity Details**, a listing of the **Entity Links** previously configured for “ASM”. The links relevant to these Application Notes are described in the subsequent section.

Entity Links

Add Remove

7 Items Refresh Filter: Enable

<input type="checkbox"/>	SIP Entity 1	Protocol	Port	SIP Entity 2	Port	Connection Policy	Deny New Service
<input type="checkbox"/>	ASM	TLS	* 5061	AuraMessaging-222	* 5061	trusted	<input type="checkbox"/>
<input type="checkbox"/>	ASM	TLS	* 5081	CM63-TG1	* 5081	trusted	<input type="checkbox"/>
<input type="checkbox"/>	ASM	TLS	* 5071	CM63-TG2	* 5071	trusted	<input type="checkbox"/>
<input type="checkbox"/>	ASM	TLS	* 5061	CM63-TG3	* 5061	trusted	<input type="checkbox"/>
<input type="checkbox"/>	ASM	TCP	* 5060	Vz_ASBCE-1	* 5060	trusted	<input type="checkbox"/>

Select : All, None < Previous Page 1 of 2 Next >

Scrolling down, the following screen shows the lower portion of the **SIP Entity Details**, illustrating the configured ports for “ASM”. This section is only present for Session Manager SIP entities. This section defines a default set of ports that Session Manager will use to listen for SIP requests, typically from registered SIP endpoints. Session Manager can also listen on additional ports defined elsewhere such as the ports specified in the SIP Entity Link definition in **Section 6.5**.

Port

TCP Failover port:

TLS Failover port:

Add Remove

5 Items Refresh Filter: Enable

<input type="checkbox"/>	Port	Protocol	Default Domain	Notes
<input type="checkbox"/>	5060	TCP	avayalab.com	<input type="text"/>
<input type="checkbox"/>	5060	UDP	avayalab.com	<input type="text"/>
<input type="checkbox"/>	5061	TLS	avayalab.com	<input type="text"/>
<input type="checkbox"/>	5071	TLS	avayalab.com	<input type="text"/>
<input type="checkbox"/>	5081	TLS	avayalab.com	<input type="text"/>

The following screen shows the upper portion of the **SIP Entity Details** corresponding to “Vz_ASBC-1”. The **FQDN or IP Address** field is configured with the Avaya SBCE inside IP Address (10.64.19.140). “SIP Trunk” is selected from the **Type** drop-down menu for Avaya SBCE SIP Entities. This Avaya SBCE has been assigned to **Location** “Vz-ASBC”, and the “VerizonIPT-SBC” adapter is applied. Other parameters (not shown) retain default values.

The screenshot displays the 'SIP Entity Details' configuration page for 'Vz_ASBC-1'. The page has a breadcrumb trail 'Home / Elements / Routing / SIP Entities' and a 'Help ?' link. A 'Hide navigation tree' button is in the top left, and 'Commit' and 'Cancel' buttons are in the top right. The 'General' section contains the following fields: 'Name' (Vz_ASBC-1), 'FQDN or IP Address' (10.64.19.140), 'Type' (SIP Trunk), 'Notes' (Verizon ASBC 1), 'Adaptation' (VerizonIPT-SBC), 'Location' (Vz-ASBC), 'Time Zone' (America/Denver), 'Override Port & Transport with DNS SRV' (unchecked), 'SIP Timer B/F (in seconds)' (4), 'Credential name' (empty), and 'Call Detail Recording' (egress). The 'Loop Detection' section has 'Loop Detection Mode' set to 'Off'. The 'SIP Link Monitoring' section has 'SIP Link Monitoring' set to 'Link Monitoring Enabled', 'Proactive Monitoring Interval (in seconds)' (900), 'Reactive Monitoring Interval (in seconds)' (120), and 'Number of Retries' (1).

Home / Elements / Routing / SIP Entities [Help ?](#)

Hide navigation tree tails [Commit](#) [Cancel](#)

General

* Name: Vz_ASBC-1

* FQDN or IP Address: 10.64.19.140

Type: SIP Trunk

Notes: Verizon ASBC 1

Adaptation: VerizonIPT-SBC

Location: Vz-ASBC

Time Zone: America/Denver

Override Port & Transport with DNS SRV: ☐

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

Credential name:

Call Detail Recording: egress

Loop Detection

Loop Detection Mode: Off

SIP Link Monitoring

SIP Link Monitoring: Link Monitoring Enabled

* Proactive Monitoring Interval (in seconds): 900

* Reactive Monitoring Interval (in seconds): 120

* Number of Retries: 1

The following screen shows a portion of the **SIP Entity Details** corresponding to a Communication Manager SIP Entity named “CM63-TG3”. This is the SIP Entity that was already in place in the shared Avaya Interoperability Test Lab environment, prior to adding the Verizon IP Trunk configuration. The **FQDN or IP Address** field contains the IP Address of the “processor Ethernet” (10.64.19.155). In systems with Avaya G650 Media Gateways containing C-LAN cards, C-LAN cards may also be used as SIP entities, instead of, or in addition to, the “processor Ethernet”. “CM” is selected from the **Type** drop-down menu and “Loc19-CM” is selected for the **Location**.

The screenshot displays the 'SIP Entity Details' configuration page for the entity 'CM63-TG3'. The page has a breadcrumb trail 'Home / Elements / Routing / SIP Entities' and a 'Help ?' link. The 'General' tab is active. Fields include: 'Name' (CM63-TG3), 'FQDN or IP Address' (10.64.19.155), 'Type' (CM), 'Notes' (Trunk Group 3 - CM to Enterprise), 'Adaptation' (empty), 'Location' (Loc19-CM), 'Time Zone' (America/Denver), 'Override Port & Transport with DNS SRV' (unchecked), 'SIP Timer B/F (in seconds)' (4), 'Credential name' (empty), 'Call Detail Recording' (none), 'Loop Detection Mode' (Off), and 'SIP Link Monitoring' (Use Session Manager Configuration). 'Commit' and 'Cancel' buttons are at the top right.

SIP Entity Details	
Commit Cancel	
General	
* Name:	CM63-TG3
* FQDN or IP Address:	10.64.19.155
Type:	CM
Notes:	Trunk Group 3 - CM to Enterprise
Adaptation:	
Location:	Loc19-CM
Time Zone:	America/Denver
Override Port & Transport with DNS SRV:	<input type="checkbox"/>
* SIP Timer B/F (in seconds):	4
Credential name:	
Call Detail Recording:	none
Loop Detection	
Loop Detection Mode:	Off
SIP Link Monitoring	
SIP Link Monitoring:	Use Session Manager Configuration

The following screen shows the **SIP Entity Details** for an entity named “CM63-TG1”. This entity uses the same **FQDN or IP Address** (10.64.19.155) as the prior entity with name “CM63-TG3”; both correspond to Communication Manager Processor Ethernet IP Address. Later, a unique port, 5081, will be used for the Entity Link to “CM63-TG1”. Using a different port is one approach that will allow Communication Manager to distinguish traffic originally from Verizon IP Trunk from other SIP traffic arriving from the same IP Address of the Session Manager, such as SIP traffic associated with SIP Telephones or other SIP-integrated applications. “CM” is selected from the **Type** drop-down menu, and “Loc19-CM” is selected for the **Location**.

The screenshot displays the 'SIP Entity Details' configuration page for an entity named 'CM63-TG1'. The page has a breadcrumb trail at the top: 'Home / Elements / Routing / SIP Entities'. On the right side of the header, there is a 'Help ?' link. Below the breadcrumb, the title 'SIP Entity Details' is shown, followed by 'Commit' and 'Cancel' buttons. The 'General' section is active, showing the following fields: 'Name' (CM63-TG1), 'FQDN or IP Address' (10.64.19.155), 'Type' (CM), 'Notes' (Trunk Group 1 - CM to PSTN), 'Adaptation' (CM63-TG1-VzIPT), 'Location' (Loc19-CM), and 'Time Zone' (America/Denver). There is an unchecked checkbox for 'Override Port & Transport with DNS SRV:'. The 'SIP Timer B/F (in seconds):' is set to 4. The 'Credential name:' field is empty. 'Call Detail Recording' is set to 'none'. The 'Loop Detection' section shows 'Loop Detection Mode' set to 'Off'. The 'SIP Link Monitoring' section shows 'SIP Link Monitoring' set to 'Use Session Manager Configuration'.

Home / Elements / Routing / SIP Entities [Help ?](#)

SIP Entity Details [Commit](#) [Cancel](#)

General

* Name: CM63-TG1

* FQDN or IP Address: 10.64.19.155

Type: CM

Notes: Trunk Group 1 - CM to PSTN

Adaptation: CM63-TG1-VzIPT

Location: Loc19-CM

Time Zone: America/Denver

Override Port & Transport with DNS SRV: ☐

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

Credential name:

Call Detail Recording: none

Loop Detection

Loop Detection Mode: Off

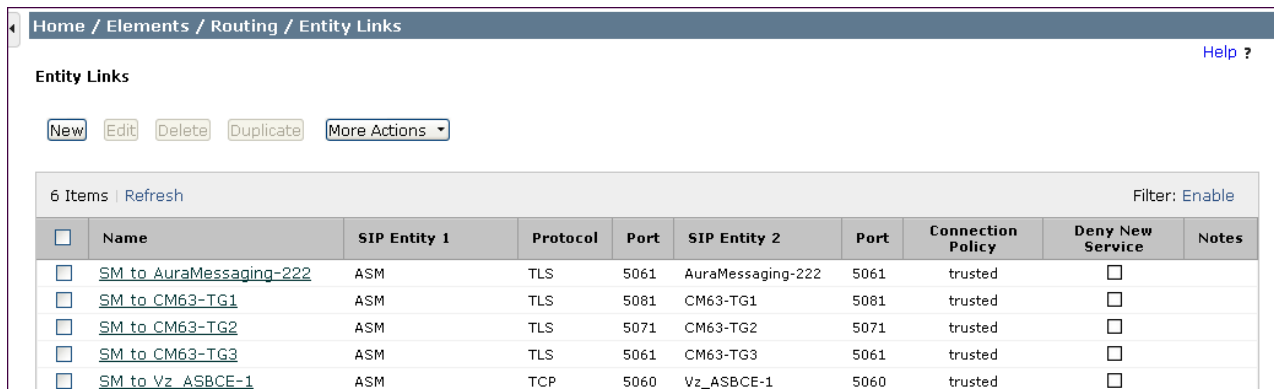
SIP Link Monitoring

SIP Link Monitoring: Use Session Manager Configuration

6.5. Entity Links

To view or change Entity Links, select **Routing → Entity Links**. Click on the checkbox corresponding to the name of a link and **Edit** to edit an existing link, or the **New** button to add a link. Click the **Commit** button after changes are completed.

The following screen shows a list of configured links. In the screen below, the links named “SM to Vz_ASBCE-1” and “SM to CM63-TG1” are most relevant to these Application Notes. Each link uses the entity named “ASM” as **SIP Entity 1**, and the appropriate entity, such as “Vz_ASBCE-1”, for **SIP Entity 2**.



Entity Links									
6 Items Refresh									
Filter: Enable									
<input type="checkbox"/>	Name	SIP Entity 1	Protocol	Port	SIP Entity 2	Port	Connection Policy	Deny New Service	Notes
<input type="checkbox"/>	SM to AuraMessaging-222	ASM	TLS	5061	AuraMessaging-222	5061	trusted	<input type="checkbox"/>	
<input type="checkbox"/>	SM to CM63-TG1	ASM	TLS	5081	CM63-TG1	5081	trusted	<input type="checkbox"/>	
<input type="checkbox"/>	SM to CM63-TG2	ASM	TLS	5071	CM63-TG2	5071	trusted	<input type="checkbox"/>	
<input type="checkbox"/>	SM to CM63-TG3	ASM	TLS	5061	CM63-TG3	5061	trusted	<input type="checkbox"/>	
<input type="checkbox"/>	SM to Vz_ASBCE-1	ASM	TCP	5060	Vz_ASBCE-1	5060	trusted	<input type="checkbox"/>	

The link named “SM to CM63-TG3” links Session Manager “ASM” with Communication Manager processor Ethernet. This link existed in the configuration prior to adding the Verizon IP Trunk related configuration. This link, using port 5061, can carry traffic between Session Manager and Communication Manager that is not necessarily related to calls with Verizon, such as traffic related to SIP Telephones registered to Session Manager.

The link named “SM to CM63-TG1” also links Session Manager “ASM” with Communication Manager processor Ethernet. However, this link uses port 5081 for both entities in the link. This link was created to allow Communication Manager to distinguish calls from Verizon IP Trunk from other calls that arrive from the same Session Manager. Other methods of distinguishing traffic could be used, if desired.

6.6. Time Ranges

To view or change Time Ranges, select **Routing → Time Ranges**. The Routing Policies shown subsequently will use the “24/7” range since time-based routing was not the focus of these Application Notes. Click the **Commit** button (not shown) after changes are completed.

The screenshot shows the 'Time Ranges' configuration page. At the top, there is a breadcrumb trail: 'Home / Elements / Routing / Time Ranges'. Below this, there are buttons for 'New', 'Edit', 'Delete', 'Duplicate', and a 'More Actions' dropdown. A 'Filter: Enable' link is also present. The main content area shows '1 Item' and a 'Refresh' button. Below this is a table with columns: 'Name', 'Mo', 'Tu', 'We', 'Th', 'Fr', 'Sa', 'Su', 'Start Time', 'End Time', and 'Notes'. The table contains one row with the name '24/7', all days of the week checked, and a time range from '00:00' to '23:59'. The notes for this row are 'Time Range 24/7'. At the bottom, there is a 'Select : All, None' option.

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

6.7. Routing Policies

To view or change routing policies, select **Routing → Policies**. Click on the checkbox corresponding to the name of a policy and **Edit** to edit an existing policy, or **New** to add a policy. Click the **Commit** button after changes are completed (not shown).

The following screen shows the **Routing Policy Details** for the policy named “To-CM63-TG1” associated with incoming PSTN calls from Verizon to Communication Manager. Observe the **SIP Entity as Destination** is the entity named “CM63-TG1”.

The screenshot shows the 'Routing Policy Details' page for the policy 'To-CM63-TG1'. At the top, there is a breadcrumb trail: 'Home / Elements / Routing / Routing Policies'. Below this, there are buttons for 'Commit' and 'Cancel'. The main content area is divided into sections: 'General', 'SIP Entity as Destination', and 'Time of Day'. The 'General' section contains fields for 'Name' (To-CM63-TG1), 'Disabled' (checkbox), 'Retries' (0), and 'Notes' (Trunk Group 1 to PSTN). The 'SIP Entity as Destination' section has a 'Select' button and a table with columns: 'Name', 'FQDN or IP Address', 'Type', and 'Notes'. The table contains one row with the name 'CM63-TG1', FQDN '10.64.19.155', Type 'CM', and Notes 'Trunk Group 1 - CM to PSTN'. The 'Time of Day' section has buttons for 'Add', 'Remove', and 'View Gaps/Overlaps'. Below this is a table with columns: 'Ranking', 'Name', 'Mon', 'Tue', 'Wed', 'Thu', 'Fri', 'Sat', 'Sun', 'Start Time', 'End Time', and 'Notes'. The table contains one row with Ranking '0', Name '24/7', all days of the week checked, and a time range from '00:00' to '23:59'. The notes for this row are 'Time Range 24/7'.

Name	FQDN or IP Address	Type	Notes
CM63-TG1	10.64.19.155	CM	Trunk Group 1 - CM to PSTN

Ranking	Name	Mon	Tue	Wed	Thu	Fri	Sat	Sun	Start Time	End Time	Notes
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

The following screen shows the **Routing Policy Details** for the policy named “To Vz-ASBCE-1” associated with outgoing calls from Communication Manager to the PSTN via Verizon through Avaya SBCE. Observe the **SIP Entity as Destination** as the entity named “Vz_ASBCE-1” that was created in **Section 6.4**.

Home / Elements / Routing / Routing Policies

Hide navigation tree
Help ?

Routing Policy Details
Commit Cancel

General

* Name: To Vz-ASBCE-1

Disabled: ☐

* Retries: 0

Notes: To Verizon ASBCE-1

SIP Entity as Destination

Select

Name	FQDN or IP Address	Type	Notes
Vz_ASBCE-1	10.64.19.140	SIP Trunk	Verizon ASBCE 1

Time of Day

Add Remove View Gaps/Overlaps

1 Item | Refresh
Filter: Enable

<input type="checkbox"/>	Ranking	Name	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

6.8. Dial Patterns

To view or change dial patterns, select **Routing → Dial Patterns**. Click on the checkbox corresponding to the name of a pattern and **Edit** to edit an existing pattern, or **New** to add a pattern. Click the **Commit** button after changes are completed.

The following screen illustrates an example dial pattern used to verify inbound PSTN calls to the enterprise. When a user on the PSTN dials a number assigned to the Verizon IP Trunk service, such as 732-945-0231, Verizon delivers the number to the enterprise, and the Avaya SBCE sends the call to Session Manager. The pattern below matches on 732-945-0231 specifically. Dial patterns can alternatively match on ranges of number (e.g., a DID block). Under **Originating Locations and Routing Policies**, the routing policy named “To-CM63-TG1” is chosen when the call originates from **Originating Location Name** “Vz-ASBCE”. This sends the call to Communication Manager using port 5081 as described previously.

Home / Elements / Routing / Dial Patterns

Help ?

Dial Pattern Details

CommitCancel

General

* Pattern:

7329450231

* Min:

10

* Max:

10

Emergency Call:

☐

Emergency Priority:

1

Emergency Type:

SIP Domain:

-ALL-

Notes:

Verizon DID number to CM6.3

Originating Locations and Routing Policies

AddRemove

1 Item | Refresh

Filter: Enable

<input type="checkbox"/>	Originating Location Name ▲	Originating Location Notes	Routing Policy Name	Rank	Routing Policy Disabled	Routing Policy Destination	Routing Policy Notes
<input type="checkbox"/>	Vz-ASBCE	SBC to Verizon	To-CM63-TG1		<input type="checkbox"/>	CM63-TG1	Trunk Group 1 to PSTN

The following screen illustrates an example dial pattern used to verify outbound calls from the enterprise to the PSTN. When a Communication Manager user dials a PSTN number such as 9-1303-XXX-XXX, Communication Manager sends the call to Session Manager. Session Manager will match the dial pattern shown below and send the call to the Avaya SBCE via the **Routing Policy Name** “To Vz-ASBCE-1”.

Home / Elements / Routing / Dial Patterns
[Help ?](#)

Dial Pattern Details
Commit Cancel

General

* Pattern: 1303

* Min: 11

* Max: 11

Emergency Call: ☐

Emergency Priority: 1

Emergency Type:

SIP Domain: -ALL-

Notes:

Originating Locations and Routing Policies
Add Remove

1 Item | Refresh
Filter: Enable

<input type="checkbox"/>	Originating Location Name ▲	Originating Location Notes	Routing Policy Name	Rank	Routing Policy Disabled	Routing Policy Destination	Routing Policy Notes
<input type="checkbox"/>	Loc19-CM	Location 19 CM	To Vz-ASBCE-1		<input type="checkbox"/>	Vz_ASBCE-1	To Verizon ASBCE-1

6.9. Fax Users

The following is an example SIP user created on System Manager to register an AudioCodes MP-114 port with Session Manager. On the Home screen, under the heading “Users”, select **User Management**. On the left side, select **Manager Users** and click **New** as shown below.



The following screen shows the **Identity** tab of a sample SIP user created for fax calls.

A screenshot of the 'New User Profile' form in the 'Identity' tab. The breadcrumb trail is 'Home / Users / User Management / Manage Users'. The form has tabs for 'Identity', 'Communication Profile', 'Membership', and 'Contacts'. The 'Identity' tab is active. Fields include: 'Last Name' (17555), 'First Name' (Fax2), 'Middle Name' (empty), 'Description' (empty), 'Login Name' (17555@avayalab.com), 'Authentication Type' (Basic), 'Password' (masked), 'Confirm Password' (masked), 'Localized Display Name' (empty), 'Endpoint Display Name' (empty), 'Title' (empty), 'Language Preference' (dropdown), 'Time Zone' (dropdown), 'Employee ID' (empty), 'Department' (empty), and 'Company' (empty). Action buttons 'Commit & Continue', 'Commit', and 'Cancel' are at the top right.

The following screen shows the **Communication Profile** tab of the sample user. The **Communication Profile Password** is the password used by the SIP device to register with Session Manager, and should match the password set on the AudioCodes MP-114 in **Section 8.2**. The **Application Sequences** section is set to “(None)”, and the **CM Endpoint Profile** is unchecked. This allows for fax calls to be sent to the AudioCodes MP-114, without involving Communication Manager in the call setup. As stated in **Section 2.2**, Verizon requires fax calls to start off with G.711 as the first codec choice, and if all other voice calls prefer G.729 as the first codec, a separate Communication Manager trunk group dedicated for fax calls using an ip-codec-

set with G.711 as the first codec choice would be required. Having the **Application Sequence** section set to “(None)” prevents the need for a separate fax dedicated trunk group on Communication Manager. As a result, fewer SIP re-Invites messages are sent during the beginning of a fax call, and voice calls to and from Communication Manager can use other preferred codecs. However, any functionality that would normally be controlled by Communication Manager, such as codec negotiation, calling restrictions, dial patterns, etc., will be controlled by the AudioCodes device, and therefore will need to be configured directly on the AudioCodes device. See **Section 8** and **Section 12.3** for information on AudioCodes MP-114 configuration.

Communication Profile

Communication Profile Password:
Edit

New Delete Done Cancel

Name

Primary

Select : None

* Name: Primary

Default : ☒

Communication Address

New Edit Delete

Type	Handle	Domain
Avaya SIP	17555	avayalab.com

Select : All, None

☒ Session Manager Profile

SIP Registration

* Primary Session Manager
ASM

Secondary Session Manager
(None)

Survivability Server
(None)

Max. Simultaneous Devices
1

Block New Registration When Maximum Registrations Active?
☐

Application Sequences

Origination Sequence
(None)

Termination Sequence
(None)

Call Routing Settings

* Home Location
Loc19

Conference Factory Set
(None)


☐ Collaboration Environment Profile

☐ CM Endpoint Profile

7. Configure Avaya Session Border Controller for Enterprise Release 6.2

These Application Notes assume that the installation of the Avaya SBCE and the assignment of all IP addresses have already been completed, including the management IP address.

In the sample configuration, the management IP is 10.80.140.140. Access the web management interface by entering `https://<ip-address>` where `<ip-address>` is the management IP address assigned during installation. Log in with the appropriate credentials. Click **Log In**.



Session Border Controller for Enterprise

Log In

Username:

Password:

This system is restricted solely to authorized users for legitimate business purposes only. The actual or attempted unauthorized access, use or modifications of this system is strictly prohibited. Unauthorized users are subject to company disciplinary procedures and or criminal and civil penalties under state, federal or other applicable domestic and foreign laws.

The use of this system may be monitored and recorded for administrative and security reasons. Anyone accessing this system expressly consents to such monitoring and recording, and is advised that if it reveals possible evidence of criminal activity, the evidence of such activity may be provided to law enforcement officials.


All users must comply with all corporate instructions regarding the protection of information assets.

© 2011 - 2013 Avaya Inc. All rights reserved.

The main page of the Avaya SBCE will appear.

AlarmsIncidentsStatisticsLogsDiagnosticsUsersSettingsHelpLog Out

Session Border Controller for Enterprise



Dashboard

- Administration
- Backup/Restore
- System Management
 - Global Parameters
 - Global Profiles
 - SIP Cluster
 - Domain Policies
 - TLS Management
 - Device Specific Settings

Dashboard

Information		
System Time	11:47:08 AM GMT	Refresh
Version	6.2.0.Q36	
Build Date	Thu Feb 14 23:25:50 UTC 2013	

Alarms (past 24 hours)	
None found.	

Installed Devices	
EMS	
VZ_1	

Incidents (past 24 hours)	
VZ_1: Method Prohibited Out-of-Dialog	
VZ_1: Method Prohibited Out-of-Dialog	
VZ_1: Method Prohibited Out-of-Dialog	
VZ_1: Method Prohibited Out-of-Dialog	
VZ 1: Method Prohibited Out-of-Dialog	

To view system information that was configured during installation, navigate to **System Management**. A list of installed devices is shown in the right pane. In the case of the sample configuration, a single device named “VZ_1” is shown. To view the configuration of this device, click **View** as highlighted below.

The screenshot shows the Avaya Session Border Controller for Enterprise web interface. The top navigation bar includes Alarms, Incidents, Statistics, Logs, Diagnostics, Users, Settings, Help, and Log Out. The main header displays 'Session Border Controller for Enterprise' and the Avaya logo. On the left, a sidebar menu lists various management options, with 'System Management' currently selected. The main content area is titled 'System Management' and contains four tabs: Devices, Updates, SSL VPN, and Licensing. The 'Devices' tab is active, displaying a table of installed devices. The table has columns for Device Name (Serial Number), Management IP, Version, Status, and a set of action buttons. One device, 'VZ_1 (IPCS31030013)', is listed with a Management IP of 10.80.140.140 and version 6.2.0.Q36. The 'View' button for this device is highlighted with a red rectangle.

Device Name (Serial Number)	Management IP	Version	Status				
VZ_1 (IPCS31030013)	10.80.140.140	6.2.0.Q36	Commissioned	Reboot	Shutdown	Restart Application	View

The **System Information** screen shows the **Network Settings**, **DNS Configuration**, and **Management IP** information provided during installation and corresponds to **Figure 1**. The **Box Type** was set to “SIP” and the **Deployment Mode** was set to “Proxy”. Default values were used for all other fields. Note that the **Management IP** must be on a separate subnet from the IP interfaces designated for SIP traffic.

The screenshot shows the 'System Information: VZ_1' configuration window. It contains several sections with configuration details:

- General Configuration:**
 - Appliance Name: VZ_1
 - Box Type: SIP
 - Deployment Mode: Proxy
- Device Configuration:**
 - HA Mode: No
 - Two Bypass Mode: No
- Network Configuration:**

IP	Public IP	Netmask	Gateway	Interface
10.64.19.140	10.64.19.140	255.255.255.0	10.64.19.1	A1
1.1.1.2	1.1.1.2	255.255.255.0	1.1.1.1	B1
- DNS Configuration:**
 - Primary DNS: 10.80.150.201
 - Secondary DNS:
 - DNS Location: DMZ
 - DNS Client IP: 10.64.19.140
- Management IP(s):**
 - IP: 10.80.140.140

7.1. Network Management

The Network Management screen is where the network interface settings are configured and enabled. During the installation process, certain network-specific information is defined such as device IP address(es), public IP address(es), netmask, gateway, etc., to interface the device to the network. It is this information that populates the various Network Management tab displays, which can be edited as needed to optimize device performance and network efficiency. Navigate to **Device Specific Settings → Network Management** and verify the IP addresses assigned to the interfaces and that the interfaces are enabled. The following screen shows the internal interface is assigned to **A1** and the external interface is assigned to **B1**.

The screenshot shows the 'Session Border Controller for Enterprise' interface. The left sidebar lists navigation options, with 'Network Management' highlighted. The main content area is titled 'Network Management: VZ_1' and has two tabs: 'Network Configuration' (active) and 'Interface Configuration'. A warning message states: 'Modifications or deletions of an IP address or its associated data require an application restart before taking effect. Application restarts can be issued from System Management.' Below this, there are input fields for 'A1 Netmask' (255.255.255.0), 'A2 Netmask', 'B1 Netmask' (255.255.255.0), and 'B2 Netmask'. An 'Add' button is present. Below these fields is a table with columns: IP Address, Public IP, Gateway, and Interface. The table contains two rows: one for interface A1 with IP 10.64.19.140 and gateway 10.64.19.1, and another for interface B1 with IP 1.1.1.2 and gateway 1.1.1.1. Each row has a 'Delete' button next to the interface name.

IP Address	Public IP	Gateway	Interface	
10.64.19.140		10.64.19.1	A1	Delete
1.1.1.2		1.1.1.1	B1	Delete

The following screen shows interface **A1** and **B1** are **Enabled**. To enable an interface click the corresponding **Toggle State** button.

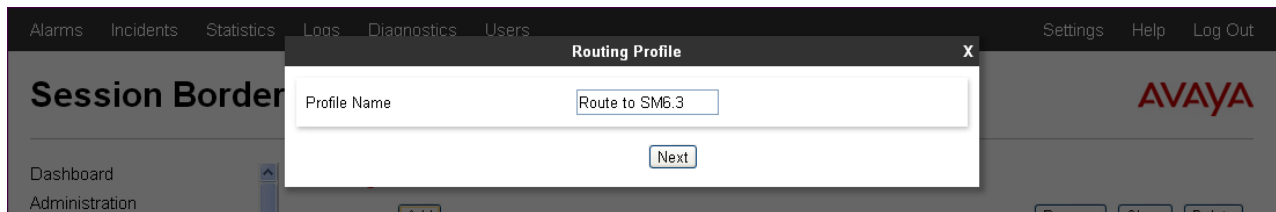
The screenshot shows the same 'Session Border Controller for Enterprise' interface, but with the 'Interface Configuration' tab selected. It displays a table with columns 'Name' and 'Administrative Status'. The table lists four interfaces: A1 (Enabled), A2 (Disabled), B1 (Enabled), and B2 (Disabled). Each row has a 'Toggle' button next to the status.

Name	Administrative Status	
A1	Enabled	Toggle
A2	Disabled	Toggle
B1	Enabled	Toggle
B2	Disabled	Toggle

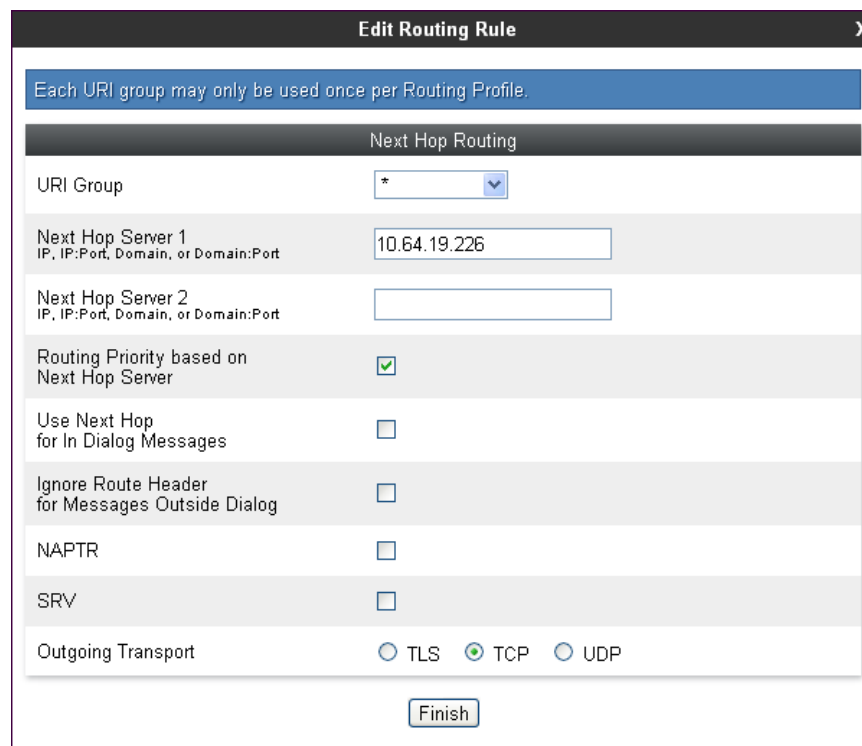
7.2. Routing Profile

Routing profiles define a specific set of packet routing criteria that are used in conjunction with other types of domain policies to identify a particular call flow and thereby ascertain which security features will be applied to those packets. Parameters defined by Routing Profiles include packet transport settings, name server addresses and resolution methods, next hop routing information, and packet transport types.

Create a Routing Profile for Session Manager and Verizon IP Trunk service. To add a routing profile, navigate to **Global Profiles → Routing** and select **Add**. Enter a **Profile Name** and click **Next** to continue.



In the shared test environment the following screen shows Routing Profile “Route to SM6.3” created for Session Manager. The **Next Hop Server 1** IP address must match the IP address of Session Manager Entity created in **Section 6.4**. The **Outgoing Transport** is set to **TCP** and matched the **Protocol** set in the Session Manager Entity Link for Avaya SBCE in **Section 6.5**.



The following screen shows Routing Profile “Route To Vz_IPT” created for Verizon. Enter the IP address and port of the Verizon SIP signaling interface as **Next Hop Server 1**, as shown below. It is only necessary to include the port after the IP address when it is not the default SIP port. Choose **UDP** for **Outgoing Transport**, and click **Finish**.

7.3. Topology Hiding Profile

The Topology Hiding profile manages how various source, destination and routing information in SIP and SDP message headers are substituted or changed to maintain the integrity of the network. It hides the topology of the enterprise network from external networks.

Click the **Add** button (not shown) to add a new profile, or select an existing topology hiding profile to edit. If adding a profile, a screen such as the following is displayed. Enter a **Profile Name** such as “Avaya” shown below. Click **Next**.

In the resultant screen, click the **Add Header** button in the upper right multiple times to reveal additional headers.

Topology Hiding Profile

X

Add Header

Header	Criteria	Replace Action	Overwrite Value	
Request-Line	IP/Domain	Auto		Delete

In the **Replace Action** column an action of “Auto” will replace the header field with the IP address of the Avaya SBCE interface and the “Overwrite” will use the value in the **Overwrite Value**. In the example shown, this profile will later be applied in the direction of the Session Manager and “Overwrite” has been selected for the To/From and Request-Line headers and the shared interop lab domain of “avayalab.com” has been inserted. Click **Finish**.

Edit Topology Hiding Profile

X

Header	Criteria	Replace Action	Overwrite Value	
To	IP/Domain	Overwrite	avayalab.com	Delete
Request-Line	IP/Domain	Overwrite	avayalab.com	Delete
Via	IP/Domain	Auto		Delete
SDP	IP/Domain	Auto		Delete
From	IP/Domain	Overwrite	avayalab.com	Delete
Record-Route	IP/Domain	Auto		Delete

Finish

After configuration is completed, the Topology Hiding for profile “Avaya” will appear as follows. This profile will later be applied to the Server Flow for Avaya.

Topology Hiding			
Header	Criteria	Replace Action	Overwrite Value
To	IP/Domain	Overwrite	avayalab.com
Request-Line	IP/Domain	Overwrite	avayalab.com
Via	IP/Domain	Auto	---
SDP	IP/Domain	Auto	---
From	IP/Domain	Overwrite	avayalab.com
Record-Route	IP/Domain	Auto	---

[Edit](#)

Similarly, create a Topology Hiding profile for Verizon. The following screen shows Topology Hiding profile “VzIPT-TopoHiding” created for Verizon. This profile will later be applied to the Server Flow for Verizon.

Topology Hiding Profiles: VzIPT-TopoHiding																															
<div> Add </div> <div> Rename Clone Delete </div>																															
<div> <div> <div>Topology Hiding Profiles</div> <div> <div>default</div> <div>cisco_th_profile</div> <div>Avaya</div> <div>IPCC_Topology_Hiding</div> <div>VzIPT-TopoHiding</div> </div> </div> <div> <div>Click here to add a description.</div> <div> <div>Topology Hiding</div> <table> <tr> <th>Header</th><th>Criteria</th><th>Replace Action</th><th>Overwrite Value</th></tr> <tr> <td>SDP</td><td>IP/Domain</td><td>Auto</td><td>---</td></tr> <tr> <td>To</td><td>IP/Domain</td><td>Overwrite</td><td>pcelban0001.avayalincroft.globalipcom.com</td></tr> <tr> <td>Record-Route</td><td>IP/Domain</td><td>Auto</td><td>---</td></tr> <tr> <td>From</td><td>IP/Domain</td><td>Overwrite</td><td>adevc.avaya.globalipcom.com</td></tr> <tr> <td>Via</td><td>IP/Domain</td><td>Auto</td><td>---</td></tr> <tr> <td>Request-Line</td><td>IP/Domain</td><td>Overwrite</td><td>pcelban0001.avayalincroft.globalipcom.com</td></tr> </table> <div>Edit</div> </div> </div> </div>				Header	Criteria	Replace Action	Overwrite Value	SDP	IP/Domain	Auto	---	To	IP/Domain	Overwrite	pcelban0001.avayalincroft.globalipcom.com	Record-Route	IP/Domain	Auto	---	From	IP/Domain	Overwrite	adevc.avaya.globalipcom.com	Via	IP/Domain	Auto	---	Request-Line	IP/Domain	Overwrite	pcelban0001.avayalincroft.globalipcom.com
Header	Criteria	Replace Action	Overwrite Value																												
SDP	IP/Domain	Auto	---																												
To	IP/Domain	Overwrite	pcelban0001.avayalincroft.globalipcom.com																												
Record-Route	IP/Domain	Auto	---																												
From	IP/Domain	Overwrite	adevc.avaya.globalipcom.com																												
Via	IP/Domain	Auto	---																												
Request-Line	IP/Domain	Overwrite	pcelban0001.avayalincroft.globalipcom.com																												


7.4. Server Interworking Profile

The Server Interworking profile includes parameters to make the Avaya SBCE function in an enterprise VoIP network using different implementations of the SIP protocol. There are default profiles available that may be used as is, or modified, or new profiles can be configured as described below.

In the sample configuration, separate Server Interworking Profiles were created for Avaya and Verizon IP Trunk.

7.4.1 Server Interworking– Avaya

Navigate to **Global Profiles** → **Server Interworking** and click the **Add Profile** button (not shown) to add a new profile or select an existing interworking profile. If adding a profile, a screen such as the following is displayed. Enter an appropriate **Profile Name** such as “Avaya” shown below. Click **Next**.

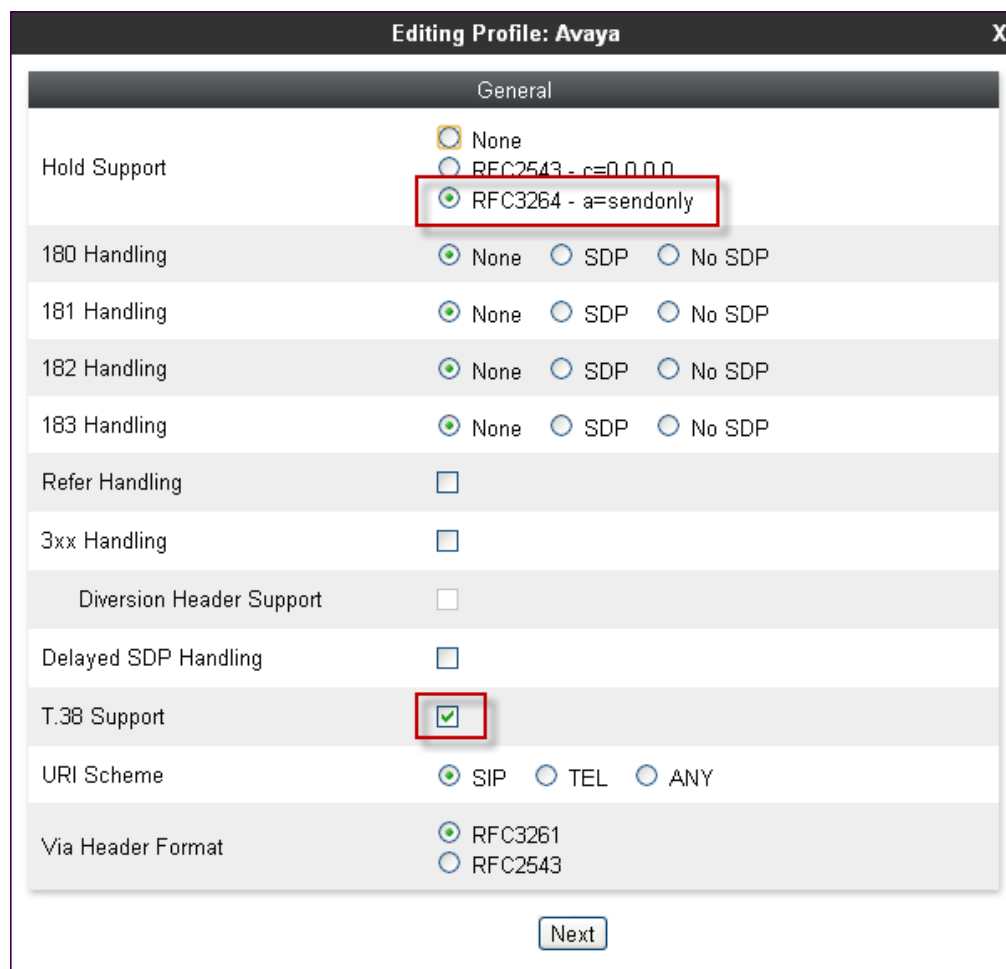


Interworking Profile

Profile Name: Avaya

Next

The following screens illustrate the “General” parameters used in the sample configuration for the Interworking Profile named “Avaya”. Most parameters retain default values. In the sample configuration, **RFC3264 – a=sendonly** is selected and **T.38 support** is checked.



Editing Profile: Avaya

General

Hold Support: ☐ None ☐ RFC2543 - c=0.0.0.0 ☒ RFC3264 - a=sendonly

180 Handling: ☒ None ☐ SDP ☐ No SDP

181 Handling: ☒ None ☐ SDP ☐ No SDP

182 Handling: ☒ None ☐ SDP ☐ No SDP

183 Handling: ☒ None ☐ SDP ☐ No SDP

Refer Handling: ☐

3xx Handling: ☐

Diversion Header Support: ☐

Delayed SDP Handling: ☐

T.38 Support: ☒

URI Scheme: ☒ SIP ☐ TEL ☐ ANY

Via Header Format: ☒ RFC3261 ☐ RFC2543

Next

Click **Next** to advance to through both the Privacy / DTMF parameters screen, and the SIP / Transport Timers parameters screen, which may retain default values.

Interworking Profile

X

Privacy

Privacy Enabled

☐

User Name

P-Asserted-Identity

☐

P-Preferred-Identity

☐

Privacy Header

DTMF

DTMF Support

☒ None

☐ SIP NOTIFY

☐ SIP INFO

Back

Next

Interworking Profile

X

All fields are optional.

SIP Timers

Min-SE

seconds, [90 - 86400]

Init Timer

milliseconds, [50 - 1000]

Max Timer

milliseconds, [200 - 8000]

Trans Expire

seconds, [1 - 64]

Invite Expire

seconds, [180 - 300]

Transport Timers

TCP Connection Inactive Timer

seconds, [600 - 3600]

Back

Next

The following screen illustrates the **Advanced Settings** configuration. The **Topology Hiding: Change Call-ID** is unchecked and the **AVAYA Extensions** is checked. All other parameters shown are default values. Note that the default configuration will result in Record-Route headers in SIP messages.

The screenshot shows the 'Interworking Profile' configuration window. It contains the following settings:

- Record Routes: ☐ None, ☐ Single Side, ☒ Both Sides
- Topology Hiding: Change Call-ID: ☐ (highlighted with a red box)
- Call-Info NAT: ☐
- Change Max Forwards: ☒
- Include End Point IP for Context Lookup: ☐
- OCS Extensions: ☐
- AVAYA Extensions: ☒ (highlighted with a red box)
- NORTEL Extensions: ☐
- Diversion Manipulation: ☐
- Diversion Header URI:
- Metaswitch Extensions: ☐
- Reset on Talk Spurt: ☐
- Reset SRTP Context on Session Refresh: ☐
- Has Remote SBC: ☒
- Route Response on Via Port: ☐
- Cisco Extensions: ☐

At the bottom, there are 'Back' and 'Finish' buttons.

7.4.2 Server Interworking – Verizon IP Trunk

Click the **Add** button (not shown) to add a new profile or select an existing interworking profile. If adding a profile, a screen such as the following is displayed. Enter an appropriate **Profile Name** such as “Verizon_IPT” shown below. Click **Next**.

The screenshot shows the 'Interworking Profile' configuration window. It contains the following settings:

- Profile Name:

At the bottom, there is a 'Next' button.

The following screens illustrate the **General** parameters used in the sample configuration for the Interworking Profile named “Verizon_IPT”. Most parameters retain default values. In the sample configuration, **183 Handling** is set to “SDP” to make sure all “183 Session Progress” messages include SDP. Verizon requires SDP to be included for all “183 Session Progress” messages. **T.38 support** is set to “Yes”, **Hold Support** is set for RFC3264, and all other fields retained default values.

Interworking Profiles: Verizon_IPT

Add

Interworking Profiles

cs2100
avaya-ru
OCS-Edge-Server
cisco-ccm
cups
Sipera-Halo
OCS-FrontEnd-Server
Avaya
Verizon-IPCC
Verizon_IPT

Rename
Clone
Delete

Click here to add a description.

GeneralTimersURI ManipulationHeader ManipulationAdvanced

General

Hold Support	RFC3264
180 Handling	None
181 Handling	None
182 Handling	None
183 Handling	SDP
Refer Handling	No
3xx Handling	No
Diversion Header Support	No
Delayed SDP Handling	No
T.38 Support	Yes
URI Scheme	SIP
Via Header Format	RFC3261

Privacy

Privacy Enabled	No
User Name	
P-Asserted-Identity	No
P-Preferred-Identity	No
Privacy Header	

DTMF

DTMF Support	None
--------------	------

On the Timers tab, select 6 seconds for the **Trans Expire** timer as shown below.

General	Timers	URI Manipulation	Header Manipulation	Advanced
SIP Timers				
Min-SE	---			
Init Timer	---			
Max Timer	---			
Trans Expire	6 seconds			
Invite Expire	---			
Transport Timers				
TCP Connection Inactive Timer	---			
Edit				

The following screen illustrates the **Advanced Settings** configuration. The **Topology Hiding: Change Call-ID** and **Change Max Forwards** defaults were changed to “No”. All other parameters shown are default values. Note that the default configuration will result in Record-Route headers in SIP messages.

General	Timers	URI Manipulation	Header Manipulation	Advanced
Record Routes	Both			
Topology Hiding: Change Call-ID	No			
Call-Info NAT	No			
Change Max Forwards	No			
Include End Point IP for Context Lookup	No			
OCS Extensions	No			
AVAYA Extensions	No			
NORTEL Extensions	No			
Diversion Manipulation	No			
Metaswitch Extensions	No			
Reset on Talk Spurt	No			
Reset SRTP Context on Session Refresh	No			
Has Remote SBC	Yes			
Route Response on Via Port	No			
Cisco Extensions	No			
Edit				

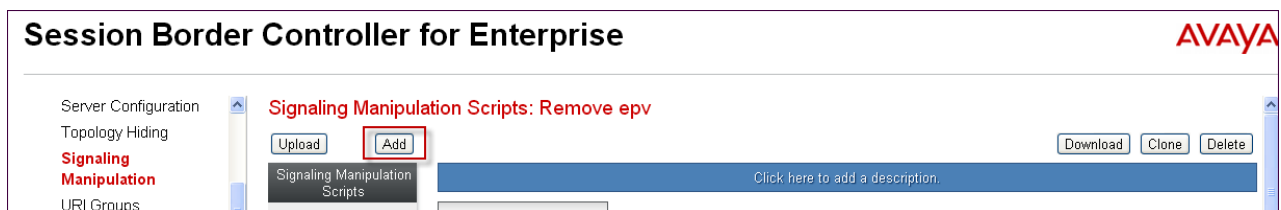
7.5. Signaling Manipulation

The Signaling Manipulation feature allows the ability to add, change and delete any of the headers in a SIP message. This feature will add the ability to configure such manipulation in a highly flexible manner using a proprietary scripting language called SigMa.

The SigMa scripting language is designed to express any of the SIP header manipulation operations to be done by the Avaya SBCE. Using this language, a script can be written and tied to a given flow through the Avaya SBCE web interface. The Avaya SBCE appliance then interprets this script at the given entry point or “hook point”.

These Application Notes will not discuss the full feature of Signaling Manipulation but will show an example of a script created during compliance testing. The sample script is used to remove the “epv” parameter Session Manager places in the Contact header. This parameter contains Endpoint-View information, including the internal domain. Removing this parameter helps mask the internal topology of the enterprise. The Endpoint-View header and other proprietary headers are removed using a Signaling Rule as illustrated in **Section 7.8**. This configuration is optional, in that the “epv” parameter does not cause any user-perceivable problems if presented to Verizon.

To create a new Signaling Manipulation, navigate to **Global Profiles → Signaling Manipulation** and click on **Add**. A new blank SigMa Editor window will pop up.



The following screen illustrates the “Remove epv” script.

```
within session "ALL"
{
  act on message where %DIRECTION="OUTBOUND" and %ENTRY_POINT="POST_ROUTING"
  {
    //OPTIONAL- Remove epv parameter from CONTACT header to hide internal domain
    remove (%HEADERS["Contact"][1].URI.PARAMS["epv"]);
  }
}
```

In the Signaling Manipulation script above, the statement **act on message where %DIRECTION="OUTBOUND" and %ENTRY_POINT="POST_ROUTING"** specifies the portion of the script that will take effect on all outbound SIP messages and the manipulation will be done after routing. The manipulation will be according to the rules contained in this statement.

The following screen shows the finished Signaling Manipulation Script “Remove epv” used during compliance testing. This script will later be applied to the Verizon Server Configuration in **Section 7.6.2**.

The screenshot displays the 'Signaling Manipulation Scripts: Remove epv' interface. On the left, a sidebar lists various scripts: 'Signaling Manipulation Scripts' (selected), 'Example', 'CS1K_Combined', 'Example22', 'Example_for_IPCC', 'IPCC Test', and 'Remove epv' (highlighted in red). The main area shows the script content for 'Remove epv' under the 'Signaling Manipulation' tab. The script is as follows:

```
within session "ALL"
{
  act on message where %DIRECTION="OUTBOUND" and %ENTRY_POINT="POST_ROUTING"
  {
    //OPTIONAL- Remove epv parameter from CONTACT header to hide internal domain
    remove(%HEADERS["Contact"][1].URI.PARAMS["epv"]);
  }
}
```

Buttons for 'Upload', 'Add', 'Download', 'Clone', and 'Delete' are visible at the top. A blue bar with the text 'Click here to add a description.' is also present. An 'Edit' button is located at the bottom right of the script area.

7.6. Server Configuration

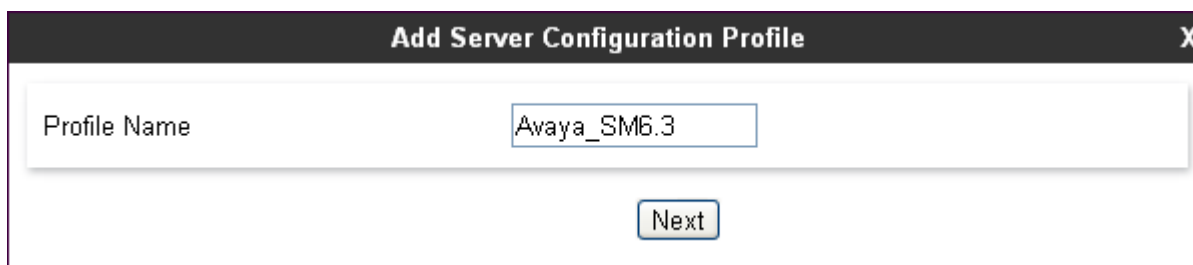
The **Server Configuration** screen contains four tabs: **General**, **Authentication**, **Heartbeat**, and **Advanced**. Together, these tabs configure and manage various SIP call server-specific parameters such as TCP and UDP port assignments, heartbeat signaling parameters, DoS security statistics, and trusted domains.

Select **Server Configuration** from the left-side menu as shown below.

The screenshot shows a vertical list of menu items. The items are: 'Dashboard', 'Administration', 'Backup/Restore', 'System Management', 'Global Parameters' (with a right-pointing triangle), 'Global Profiles' (with a left-pointing triangle), 'Domain DoS', 'Fingerprint', 'Server Interworking', 'Phone Interworking', 'Media Forking', 'Routing', 'Server Configuration' (highlighted in red), 'Topology Hiding', 'Signaling Manipulation', and 'URI Groups'.

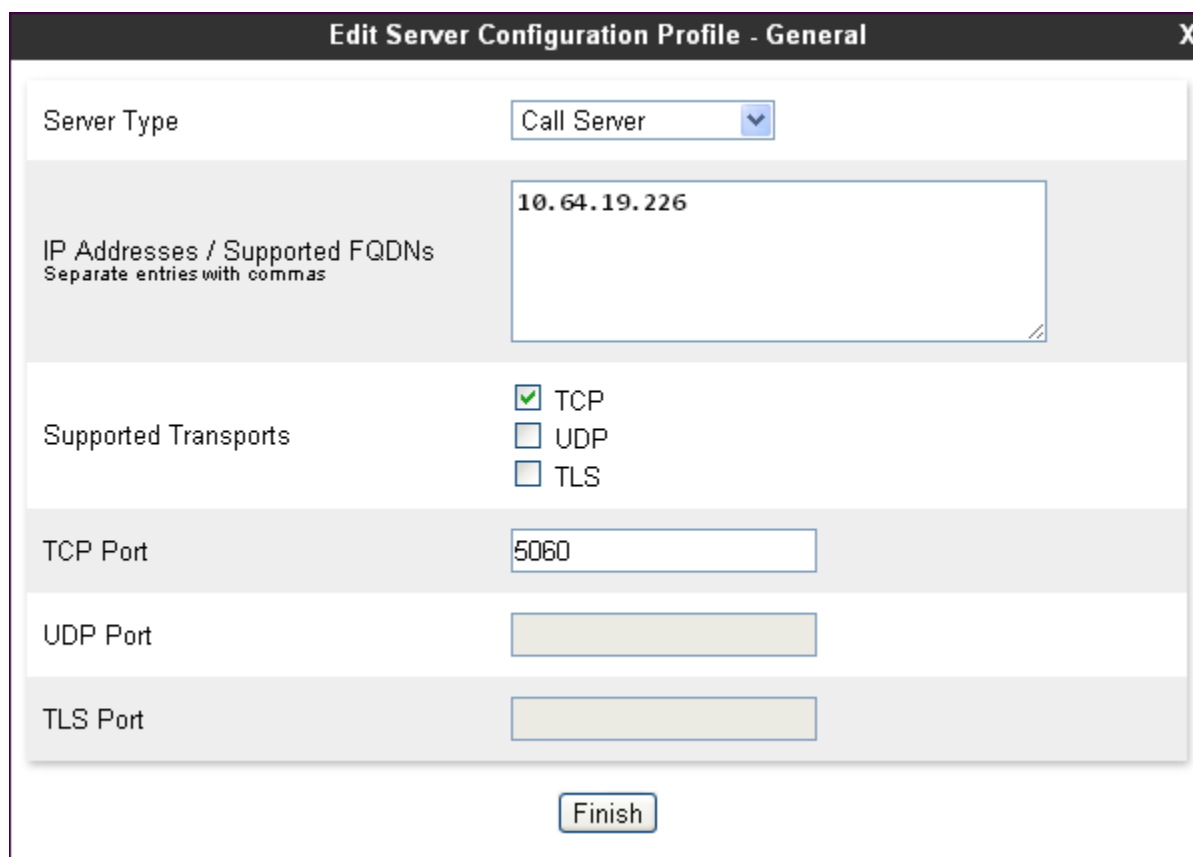
7.6.1 Server Configuration for Session Manager

Click the **Add** button (not shown) to add a new profile, or select an existing profile to edit. If adding a profile, a screen such as the following is displayed. Enter an appropriate **Profile Name** such as “Avaya_SM6.3” shown below. Click **Next**.



The dialog box titled "Add Server Configuration Profile" has a close button (X) in the top right corner. It contains a text input field labeled "Profile Name" with the value "Avaya_SM6.3" entered. Below the input field is a "Next" button.

The following screens illustrate the Server Configuration for the Profile name “Avaya_SM6.3”. On the **General** tab, select “Call Server” from the **Server Type** drop-down menu. In the **IP Addresses / Supported FQDNs** area, the IP Address of the Session Manager SIP signaling interface in the sample configuration is entered. This IP Address is 10.64.19.226. In the **Supported Transports** area, **TCP** is selected, and the **TCP Port** is set to 5060. This configuration corresponds with the Session Manager entity link configuration for the entity link to the Avaya SBCE created in **Section 6.4**. If adding a new profile, click **Next** (not shown). If editing an existing profile, click **Finish**.



The dialog box titled "Edit Server Configuration Profile - General" has a close button (X) in the top right corner. It contains the following fields and controls:

- Server Type**: A drop-down menu with "Call Server" selected.
- IP Addresses / Supported FQDNs**: A text area with the value "10.64.19.226" entered. Below the text area is the label "Separate entries with commas".
- Supported Transports**: Three checkboxes: ☒ TCP, ☐ UDP, and ☐ TLS.
- TCP Port**: A text input field with the value "5060" entered.
- UDP Port**: An empty text input field.
- TLS Port**: An empty text input field.

At the bottom of the dialog box is a "Finish" button.

If adding the profile, click **Next** to accept default parameters for the **Authentication** tab (not shown), and advance to the **Heartbeat** area. If editing an existing profile, select the **Heartbeat** tab and click **Edit** (not shown).

Avaya SBCE can be configured to source “heartbeats” in the form of SIP OPTIONS. In the sample configuration, with one Session Manager, this configuration is optional. If Avaya SBCE-sourced OPTIONS messages are desired, check the **Enable Heartbeat** box. Select “OPTIONS” from the **Method** drop-down menu. Select the desired frequency that the Avaya SBCE will source OPTIONS to this server. The **From URI** and **To URI** may be filled in to configure easily identifiable URIs to appear in SIP OPTIONS sourced by the Avaya SBCE towards Session Manager. If adding a new profile, click **Next** (not shown). If editing an existing profile, click **Finish** (not shown).

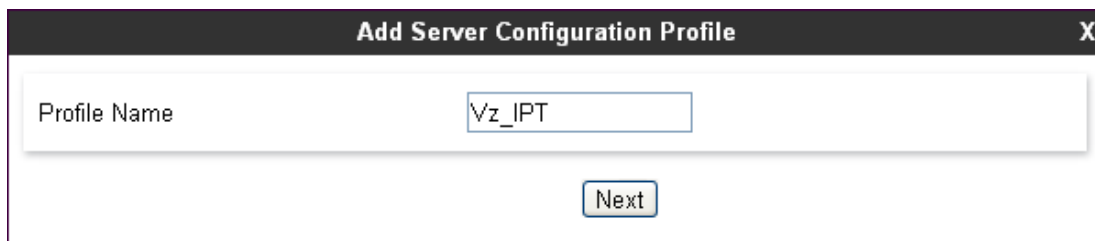
General	Authentication	Heartbeat	Advanced
Enable Heartbeat <input checked="" type="checkbox"/>			
Method OPTIONS			
Frequency 60 seconds			
From URI PING@avayalab.com			
To URI PING@avayalab.com			
Edit			

If adding a profile, click **Next** to continue to the “Advanced” settings (not shown). If editing an existing profile, select the **Advanced** tab and **Edit** (not shown). In the resultant screen, select **Enable Grooming** to allow the same TCP connection to be used for all SIP messages from this device. Select the **Interworking Profile** “Avaya” created previously. Click **Finish**.

General	Authentication	Heartbeat	Advanced
Enable DoS Protection <input type="checkbox"/>			
Enable Grooming <input checked="" type="checkbox"/>			
Interworking Profile Avaya			
Signaling Manipulation Script None			
TCP Connection Type SUBID			
Edit			

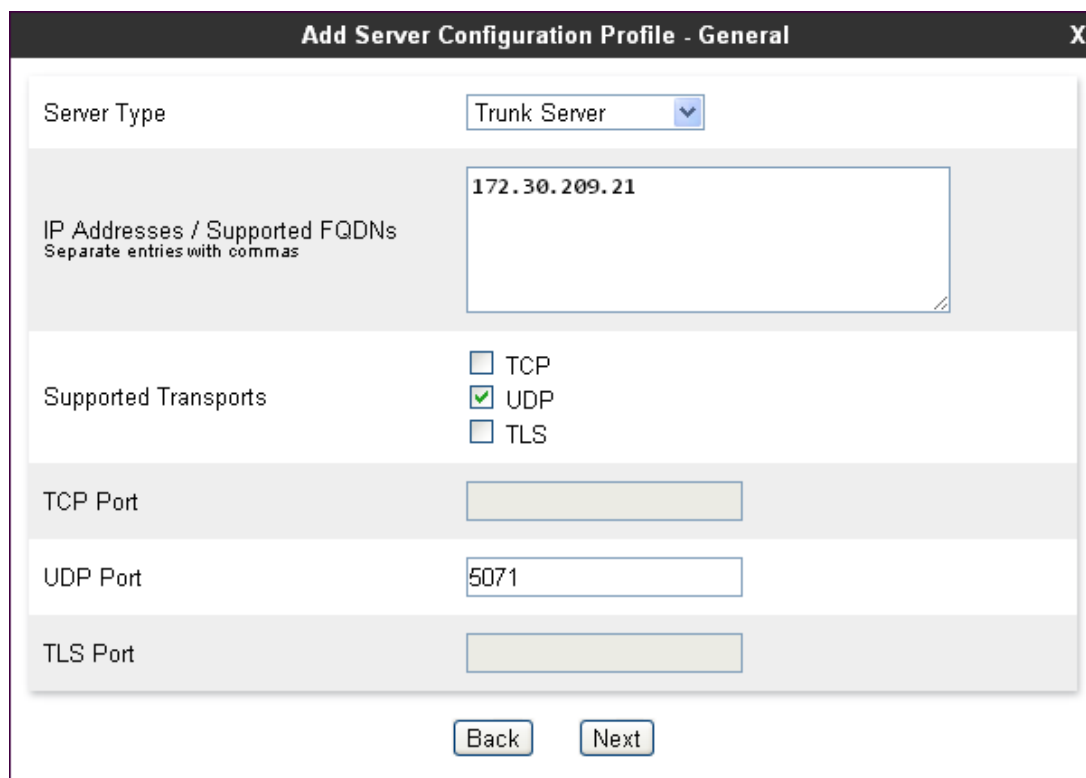
7.6.2 Server Configuration for Verizon IP Trunk

Click the **Add** button (not shown) to add a new profile, or select an existing profile to edit. If adding a profile, a screen such as the following is displayed. Enter an appropriate **Profile Name** such as “Vz_IPT” shown below. Click **Next**.



The screenshot shows a dialog box titled "Add Server Configuration Profile" with a close button (X) in the top right corner. Inside the dialog, there is a text input field labeled "Profile Name" containing the text "Vz_IPT". Below the input field, there is a "Next" button.

The following screens illustrate the Server Configuration with Profile name “Vz_IPT”. In the “General” parameters, select “Trunk Server” from the **Server Type** drop-down menu. In the **IP Addresses / Supported FQDNs** area, the Verizon-provided IP Trunk IP Address is entered. This IP Address is 172.30.209.21. In the **Supported Transports** area, UDP is selected, and the **UDP Port** is set to 5071. Click **Next** to proceed to the **Authentication** tab.



The screenshot shows a dialog box titled "Add Server Configuration Profile - General" with a close button (X) in the top right corner. The dialog contains several configuration fields: "Server Type" is a dropdown menu set to "Trunk Server"; "IP Addresses / Supported FQDNs" is a text area containing "172.30.209.21" with a note "Separate entries with commas"; "Supported Transports" has three checkboxes: "TCP" (unchecked), "UDP" (checked), and "TLS" (unchecked); "TCP Port" is an empty text field; "UDP Port" is a text field containing "5071"; and "TLS Port" is an empty text field. At the bottom, there are "Back" and "Next" buttons.

If adding the profile, click **Next** to accept default parameters for the **Authentication** tab (not shown), and advance to the Heartbeat area. If editing an existing profile, select the **Heartbeat** tab and click **Edit** (not shown).

The ASBCE can be configured to source “heartbeats” in the form of SIP OPTIONS towards Verizon. This configuration is optional. Independent of whether the ASBCE is configured to source SIP OPTIONS towards Verizon, Verizon will receive OPTIONS from the enterprise site as a result of the SIP Entity Monitoring configured for Session Manager. When Session Manager sends SIP OPTIONS to the inside private IP Address of the Avaya SBCE, the Avaya SBCE will send SIP OPTIONS to Verizon. When Verizon responds, the Avaya SBCE will pass the response to Session Manager.

Select “OPTIONS” from the **Method** drop-down menu. Select the desired frequency that the SBCE will source OPTIONS. The **From URI** and **To URI** may be filled in to configure easily identifiable URIs to appear in SIP OPTIONS sourced by the Avaya SBCE. If adding a new profile, click **Next** to continuing to the “Advanced” settings. If editing an existing profile, click Finish (not shown).

The screenshot shows the 'Heartbeat' configuration tab. It includes a table with the following settings:

Property	Value
Enable Heartbeat	<input checked="" type="checkbox"/>
Method	OPTIONS
Frequency	60 seconds
From URI	ping@adevc.avaya.globalipcom.com
To URI	ping@pcelban0001.avayalincroft.globalipcom.com

Below the table is an 'Edit' button.

If editing an existing profile, highlight the desired profile and select the **Advanced** tab and then click the **Edit button**. In the resultant screen, **Enable Grooming** is not used for UDP connections and left unchecked. Select the **Interworking Profile** “Verizon_IPT” created previously, and **Signaling Manipulation Script** will be the script shown in the previous section titled “Remove epv”. Click **Finish**.

The screenshot shows the 'Advanced' configuration tab. It includes a table with the following settings:

Property	Value
Enable DoS Protection	<input type="checkbox"/>
Enable Grooming	<input type="checkbox"/>
Interworking Profile	Verizon_IPT
Signaling Manipulation Script	Remove epv
UDP Connection Type	SUBID

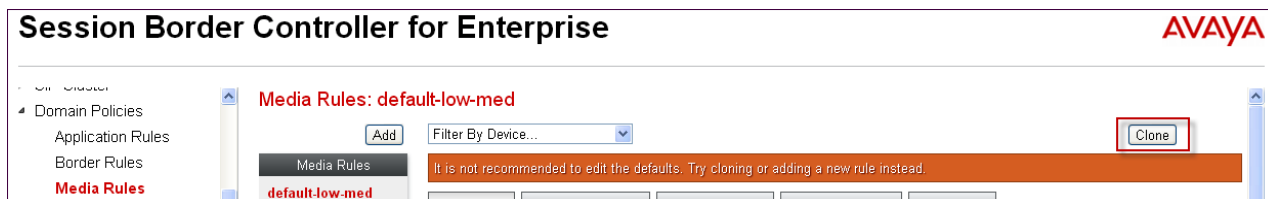
Below the table is an 'Edit' button.

7.7. Media Rule

Media Rules define RTP media packet parameters such as prioritizing encryption techniques and packet encryption techniques. Together these media-related parameters define a strict profile that is

associated with other SIP-specific policies to determine how media packets matching these criteria will be handled by the Avaya SBCE security product.

In the sample configuration, a single media rule is created by cloning the default rule called “default-low-med”. Select the default-low-med rule and click the **Clone** button.



Enter a name in the **Clone Name** field, such as “def-low-media-QoS” as shown below. Click **Finish**.

Clone Rule	
Rule Name	default-low-med
Clone Name	def-low-media-QoS
Finish	

Select the newly created rule, select the **Media QoS** tab and click the **Edit** button (not shown). In the resulting screen below, check the **Media QoS Marking Enabled** checkbox. Select **DSCP** and select “EF” for expedited forwarding as shown below. Click **Finish**.

Media QoS		
Media QoS Reporting		
RTCP Enabled	<input type="checkbox"/>	
Media QoS Marking		
Enabled	<input checked="" type="checkbox"/>	
ToS		
Audio Precedence	Routine	000
Audio ToS	Minimize Delay	1000
Video Precedence	Routine	000
Video ToS	Minimize Delay	1000
DSCP		
Audio	EF	101110
Video	EF	101110
Finish		

When configuration is complete, the “default-low-media-QoS” media rule **Media QoS** tab appears as follows.

The screenshot shows the 'Media Rules: def-low-media-QoS' configuration page. On the left is a sidebar with a list of media rules: 'default-low-med', 'default-low-med-enc', 'default-high', 'default-high-enc', 'avaya-low-med-enc', and 'def-low-media-QoS' (highlighted in red). The main area has tabs for 'Media NAT', 'Media Encryption', 'Media Anomaly', 'Media Silencing', and 'Media QoS' (selected). Below the tabs are sections for 'Media QoS Reporting' (RTCP Enabled checkbox), 'Media QoS Marking' (Enabled checkbox, QoS Type dropdown set to DSCP), 'Audio QoS' (Audio DSCP dropdown set to EF), and 'Video QoS' (Video DSCP dropdown set to EF). Buttons for 'Add', 'Filter By Device...', 'Rename', 'Clone', 'Delete', and 'Edit' are visible.

7.8. Signaling Rule

Signaling Rules define the action to be taken (Allow, Block, Block with Response, etc.) for each type of SIP-specific signaling request and response message. When SIP signaling packets are received by Avaya SBCE, they are parsed and “pattern-matched” against the particular signaling criteria defined by these rules. Packets matching the criteria defined by the Signaling Rules are tagged for further policy matching.

To add a signaling rule, navigate to **Domain Policies → Signaling Rules**. Click the **Add** button to add a new signaling rule.

The screenshot shows the 'Session Border Controller for Enterprise' interface with the 'Signaling Rules: default' page. The left sidebar lists 'Media Rules', 'Security Rules', 'Signaling Rules' (highlighted in red), 'Time of Day Rules', and 'End Point Policy'. The main area shows the 'Add' button highlighted with a red box. Below the 'Add' button is a message: 'It is not recommended to edit the defaults. Try cloning or adding a new rule instead.' There are also 'Filter By Device...' and 'Clone' buttons.

In the **Rule Name** field, enter an appropriate name, such as “Block_Hdr_Remark” and click **Next**.

The screenshot shows a 'Signaling Rule' dialog box. It has a title bar with 'Signaling Rule' and a close button 'X'. Inside, there is a 'Rule Name' label and a text input field containing 'Block_Hdr_Remark'. Below the input field is a 'Next' button.

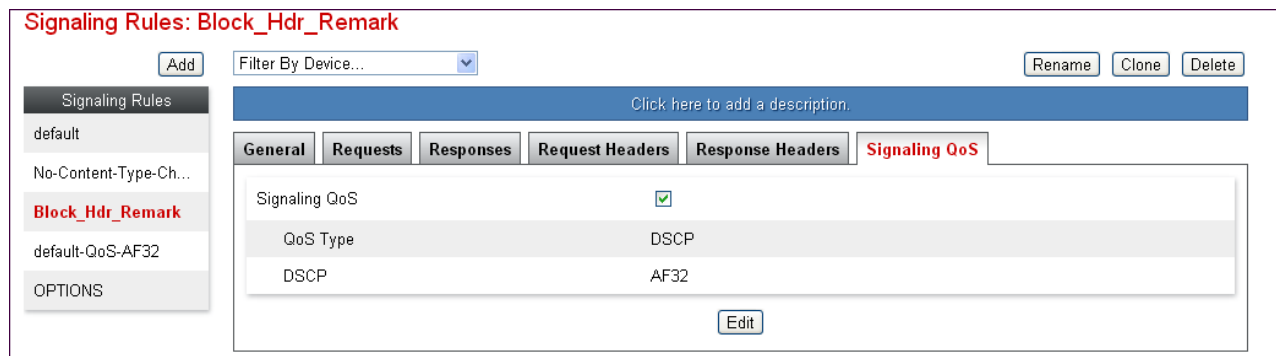
In the subsequent screen (not shown), click **Next** to accept defaults. In the **Signaling QoS** screen below, select **DSCP** and select the desired **Value** for Signaling QoS from the drop-down box. In the sample configuration, “AF32” is selected for Assured Forwarding 32. Click **Finish**.



The image shows a configuration window titled "Signaling QoS" with a close button (X) in the top right corner. The window contains the following settings:

- Enabled:** A checkbox that is checked with a green checkmark.
- ToS:** A radio button that is unselected.
- Precedence:** A dropdown menu set to "Routine" and a text box containing "000".
- ToS:** A dropdown menu set to "Minimize Delay" and a text box containing "1000".
- DSCP:** A radio button that is selected with a green dot.
- Value:** A dropdown menu set to "AF32" and a text box containing "011100".
- Finish:** A button at the bottom center of the window.

After this configuration, the new “Block_Hdr_Remark” will appear as follows.



The image shows a configuration window titled "Signaling Rules: Block_Hdr_Remark" with a close button (X) in the top right corner. The window contains the following settings:

- Signaling Rules:** A list on the left side with items: "default", "No-Content-Type-Ch...", "Block_Hdr_Remark" (highlighted in red), "default-QoS-AF32", and "OPTIONS".
- Filter By Device...:** A dropdown menu.
- Buttons:** "Add", "Rename", "Clone", and "Delete" buttons.
- Click here to add a description.** A blue bar with a link.
- Tabs:** "General", "Requests", "Responses", "Request Headers", "Response Headers", and "Signaling QoS" (selected and highlighted in red).
- Signaling QoS:** A checkbox that is checked with a green checkmark.
- QoS Type:** A dropdown menu set to "DSCP".
- DSCP:** A dropdown menu set to "AF32".
- Edit:** A button at the bottom center of the window.

Select this rule in the center pane, then select the **Request Headers** tab to view the manipulations performed on the request messages such as the initial INVITE or UPDATE message. The following screen shows the “Alert-Info”, “Endpoint-View”, “P-Location” and other proprietary headers removed during the compliance test. This configuration is optional in that these headers do not cause any user-perceivable problems if presented to Verizon.

Signaling Rules: Block_Hdr_Remark

Click here to add a description.

Row	Header Name	Method Name	Header Criteria	Action	Proprietary	Direction		
1	AV-Global-Session-ID	ALL	Forbidden	Remove Header	Yes	IN	Edit	Delete
2	Alert-Info	ALL	Forbidden	Remove Header	No	IN	Edit	Delete
3	Endpoint-View	ALL	Forbidden	Remove Header	Yes	IN	Edit	Delete
4	P-AV-Message-Id	ALL	Forbidden	Remove Header	Yes	IN	Edit	Delete
5	P-Location	ALL	Forbidden	Remove Header	Yes	IN	Edit	Delete

Similarly, manipulations can be performed on the SIP response messages. These can be viewed by selecting the **Response Headers** tab as shown below.

Signaling Rules: Block_Hdr_Remark

Click here to add a description.

Row	Header Name	Response Code	Method Name	Header Criteria	Action	Proprietary	Direction		
1	AV-Global-Session-ID	1XX	ALL	Forbidden	Remove Header	Yes	IN	Edit	Delete
2	AV-Global-Session-ID	2XX	ALL	Forbidden	Remove Header	Yes	IN	Edit	Delete
3	Endpoint-View	1XX	ALL	Forbidden	Remove Header	Yes	IN	Edit	Delete
4	Endpoint-View	2XX	ALL	Forbidden	Remove Header	Yes	IN	Edit	Delete
5	P-AV-Message-Id	1XX	ALL	Forbidden	Remove Header	Yes	IN	Edit	Delete
6	P-AV-Message-Id	2XX	ALL	Forbidden	Remove Header	Yes	IN	Edit	Delete
7	P-Location	1XX	ALL	Forbidden	Remove Header	Yes	IN	Edit	Delete
8	P-Location	2XX	ALL	Forbidden	Remove Header	Yes	IN	Edit	Delete

7.9. Application Rule

Application Rules define which types of SIP-based Unified Communications (UC) applications the Avaya SBCE security device will protect: voice, video, and/or Instant Messaging (IM). In addition, user can determine the maximum number of concurrent voice and video sessions the network will process in order to prevent resource exhaustion.

Select **Domain Policies** → **Application Rules** from the left-side menu as shown below. In the sample configuration, a single default application rule “default-trunk” is used and will be applied to the Endpoint Policy Group in the next section.

Session Border Controller for Enterprise AVAYA

Dashboard
Administration
Backup/Restore
System Management
‣ Global Parameters
‣ Global Profiles
‣ SIP Cluster
‣ Domain Policies
  Application Rules
  Border Rules
  Media Rules
  Security Rules
  Signaling Rules
  Time of Day Rules
  End Point Policy Groups
  Session Policies

Application Rules: default-trunk

Add Filter By Device... **Clone**

It is not recommended to edit the defaults. Try cloning or adding a new rule instead.

Application Rule

Application Type	In	Out	Maximum Concurrent Sessions	Maximum Sessions Per Endpoint
Voice	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	2000	2000
Video	<input type="checkbox"/>	<input type="checkbox"/>		
IM	<input type="checkbox"/>	<input type="checkbox"/>		

Miscellaneous

CDR Support	None
RTCP Keep-Alive	No

Edit

7.10. Endpoint Policy Group

The rules created within the Domain Policy section are assigned to an Endpoint Policy Group. The Endpoint Policy Group is then applied to a Server Flow in **Section 7.13**. Create a separate Endpoint Policy Group for the enterprise and the Verizon IP Trunk. To create a new policy group, navigate to **Domain Policies** → **Endpoint Policy Groups**. Select the **Add** button.

Session Border Controller for Enterprise AVAYA

Signaling Rules
Time of Day Rules
End Point Policy Groups
Session Policies

Policy Groups: default-low

Add Filter By Device... **Clone**

It is not recommended to edit the defaults. Try adding a new group instead.

Policy Group

Name	Description	Action
default-low		

Miscellaneous

CDR Support	None
RTCP Keep-Alive	No

Edit

Enter a name in the **Group Name** field, such as “def_low_remark” as shown below. Click **Next**.

Policy Group X

Group Name def_low_remark

Next

In the sample configuration, defaults were selected for all fields, with the exception of the **Application Rule** which is set to “default-trunk”, **Media Rule** which is set to “default-low-media-QoS”, and the **Signaling Rule**, which is set to “Block_Hdr_Remark” as shown below. The selected non-default media rule and signaling rule chosen were created in previous sections. Click **Finish**.

Rule Type	Value
Application Rule	default-trunk
Border Rule	default
Media Rule	def-low-media-QoS
Security Rule	default-low
Signaling Rule	Block_Hdr_Remark
Time of Day Rule	default

Finish

Once configuration is completed, the “default-low-remark” policy group will appear as follows.

Policy Groups: def_low_remark

Buttons: Add, Filter By Device..., Rename, Delete

Policy Groups List:

- default-low
- default-low-enc
- default-med
- default-med-enc
- default-high
- default-high-enc
- OCS-default-high
- avaya-def-low-enc
- def_low_remark**

Policy Group Table:

Order	Application	Border	Media	Security	Signaling	Time of Day	
1	default-trunk	default	def-low-media-QoS	default-low	Block_Hdr_Remark	default	Edit Clone

7.11. Media Interface

The Media Interface screen is where the SIP media ports are defined. Avaya SBCE will send SIP media on the defined ports. Create a SIP Media Interface for both the inside and outside IP interfaces.

To create a new Signaling Interface, navigate to **Device Specific Settings → Media Interface** and click **Add Media Interface**. The following screen shows the media interfaces created in the sample configuration for the inside and outside IP interfaces.

The screenshot shows the 'Session Border Controller for Enterprise' web interface. The left sidebar lists navigation options: SIP Cluster, Domain Policies, TLS Management, Device Specific Settings (selected), Network Management, Media Interface (selected), Signaling Interface, Signaling Forking, End Point Flows, Session Flows, and Relay Services. The main content area is titled 'Media Interface: VZ_1'. It features a 'Media Interface' tab and a table of configured interfaces. A warning message states: 'Modifying or deleting an existing media interface will require an application restart before taking effect. Application restarts can be issued from System Management.' The table has columns for Name, Media IP, and Port Range, with 'Edit' and 'Delete' links for each row.

Name	Media IP	Port Range	Edit	Delete
Int_Media_to_CPE	10.64.19.140	35000 - 40000	Edit	Delete
Ext_Media_to_Vz	1.1.1.2	35000 - 40000	Edit	Delete

7.12. Signaling Interface

The Signaling Interface screen is where the SIP signaling ports are defined. Avaya SBCE will listen for SIP requests on the defined ports. Create a Signaling Interface for both the inside and outside IP interfaces.

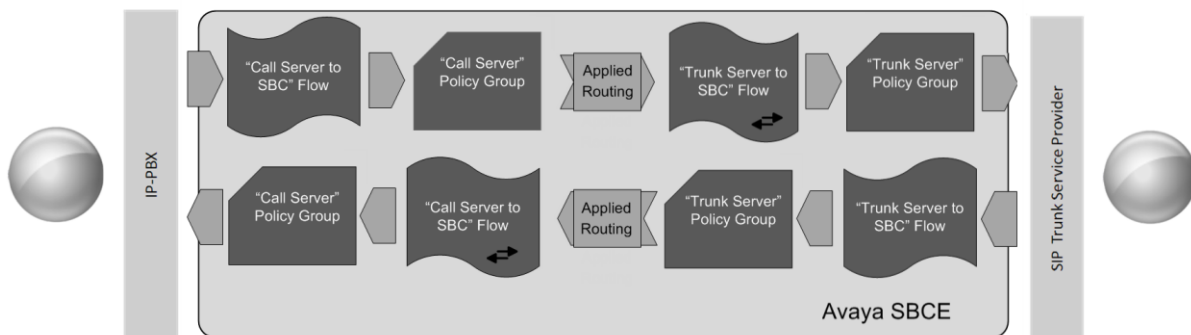
To create a new Signaling Interface, navigate to **Device Specific Settings → Signaling Interface** and click **Add Signaling Interface**. The following screen shows the signaling interfaces created in the sample configuration for the inside and outside IP interfaces.

The screenshot shows the 'Session Border Controller for Enterprise' web interface. The left sidebar lists navigation options: Device Specific Settings (selected), Network Management, Media Interface, Signaling Interface (selected), Signaling Forking, End Point Flows, Session Flows, and Relay Services. The main content area is titled 'Signaling Interface: VZ_1'. It features a 'Signaling Interface' tab and a table of configured interfaces. The table has columns for Name, Signaling IP, TCP Port, UDP Port, TLS Port, and TLS Profile, with 'Edit' and 'Delete' links for each row.

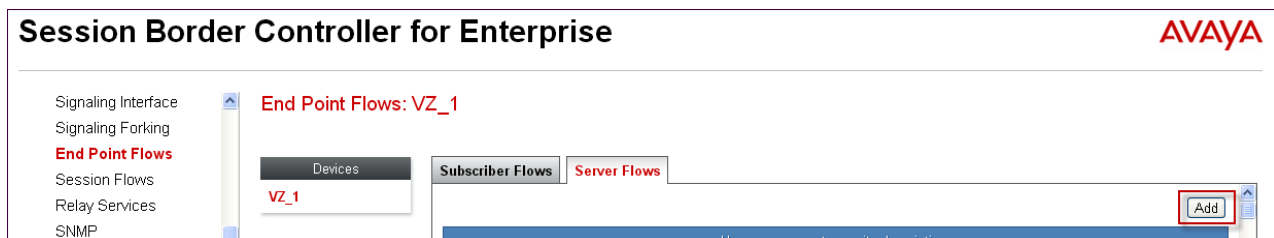
Name	Signaling IP	TCP Port	UDP Port	TLS Port	TLS Profile	Edit	Delete
Sig_Inside_to_CPE	10.64.19.140	5060	---	---	None	Edit	Delete
Sig_Outside_to_Vz	1.1.1.2	---	5060	---	None	Edit	Delete

7.13. End Point Flows - Server Flow

When a packet is received by Avaya SBCE, the content of the packet (IP addresses, URIs, etc.) is used to determine which flow it matches. Once the flow is determined, the flow points to a policy which contains several rules concerning processing, privileges, authentication, routing, etc. Once routing is applied and the destination endpoint is determined, the policies for this destination endpoint are applied. The context is maintained, so as to be applied to future packets in the same flow. The following screen illustrates the flow through the Avaya SBCE to secure a SIP Trunk call.



Create a Server Flow for Session Manager and the Verizon IP Trunk. To create a Server Flow, navigate to **Device Specific Settings** → **End Point Flows**. Select the **Server Flows** tab and click **Add Flow** as shown in below.



The following screen shows the flow named “Avaya SM6.3 Flow” used in the sample configuration. This flow uses the interfaces, policies, and profiles defined in previous sections. Click **Finish**.

Edit Flow: Avaya SM6.3 FlowX

Flow Name	Avaya SM6.3 Flow
Server Configuration	Avaya_SM6.3
URI Group	*
Transport	*
Remote Subnet	*
Received Interface	Sig_Outside_to_Vz
Signaling Interface	Sig_Inside_to_CPE
Media Interface	Int_Media_to_CPE
End Point Policy Group	def_low_remark
Routing Profile	Route to Vz_IPT
Topology Hiding Profile	Avaya
File Transfer Profile	None

Finish

The following screen shows the flow named “Vz-IPT-Flow” used in the sample configuration. This flow uses the interfaces, policies, and profiles defined in previous sections. Click **Finish**.

Add FlowX

Flow Name	Vz-IPT-Flow
Server Configuration	Vz_IPT
URI Group	*
Transport	*
Remote Subnet	*
Received Interface	Sig_Inside_to_CPE
Signaling Interface	Sig_Outside_to_Vz
Media Interface	Ext_Media_to_Vz
End Point Policy Group	def_low_remark
Routing Profile	Route to SM6.3
Topology Hiding Profile	VzIPT-TopoHiding
File Transfer Profile	None

Finish

8. AudioCodes MP-114

During the verification these Application Notes, an AudioCodes MP-114 was used for fax calls to and from the PSTN. This section will show the necessary settings to incorporate fax calls with Verizon IP Trunk service and to register the MP-114 with Session Manager. These Application Notes assume that the installation of the AudioCodes MP-114 and the assignment of an IP address have already been completed. See **Section 12.3** for information regarding the installation of the AudioCodes MP-114.

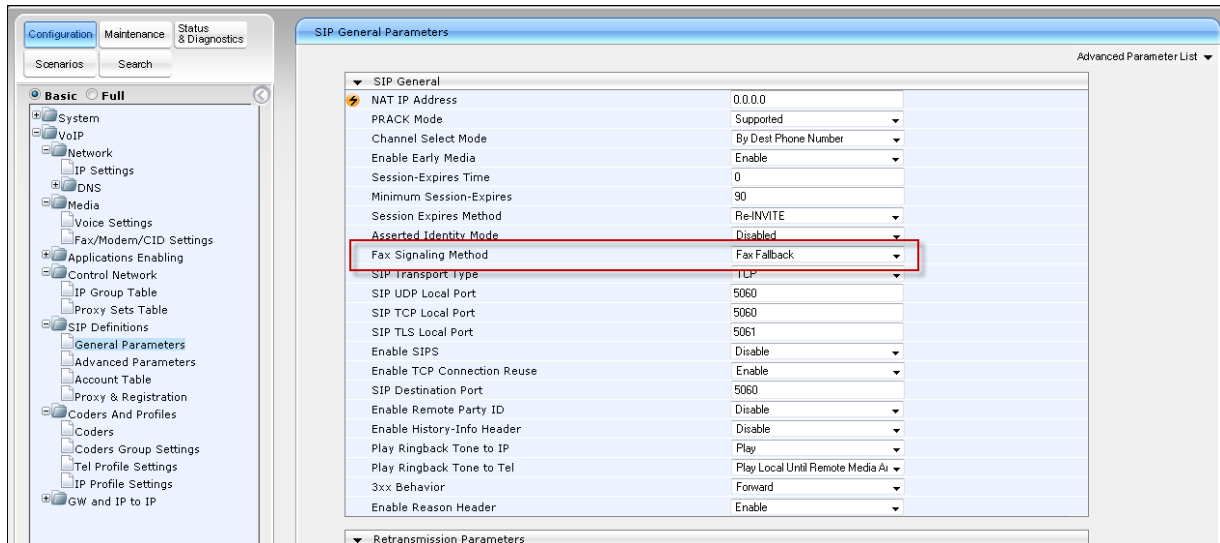
Note - Although the MP-114 is described in these Application Notes, other AudioCodes Telephone Adapters such as the MP-202 or MP-124 may be used.

8.1. Fax Configuration Settings

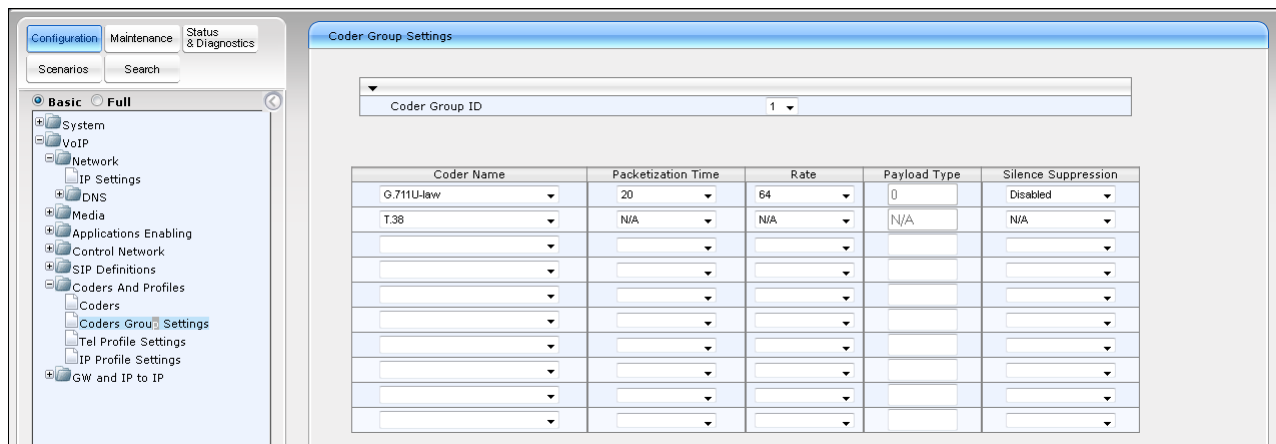
Select **Configuration** menu on the top left of the screen, and navigate to **VoIP→Media→Fax/Modem/CID Settings**. Set the **Fax Transport Mode** to “RelayEnable” and set the **Fax Relay Settings** as highlighted below.

Fax/Modem/CID Settings	
General Settings	
Fax Transport Mode	RelayEnable
Caller ID Transport Type	Mute
Caller ID Type	Standard Bellcore
V.21 Modem Transport Type	Enable Bypass
V.22 Modem Transport Type	Enable Bypass
V.23 Modem Transport Type	Enable Bypass
V.32 Modem Transport Type	Enable Bypass
V.34 Modem Transport Type	Enable Bypass
Fax CNG Mode	Enable
CNG Detector Mode	Disable
Fax Relay Settings	
Fax Relay Redundancy Depth	2
Fax Relay Enhanced Redundancy Depth	2
Fax Relay ECM Enable	Disable
Fax Relay Max Rate (bps)	14400bps
Bypass Settings	
Fax/Modem Bypass Coder Type	G711Mulaw
Fax/Modem Bypass Packing Factor	1
Fax Bypass Output Gain	0
Modem Bypass Output Gain	0

Navigate to **VoIP→SIP Definitions→General Parameters**. Set the **Fax Signaling Method** to “Fax Fallback”.



Navigate to **VoIP→Coders and Profiles→Coders Group Settings**. Select **Coder Group ID “1”** and under the **Coder Name** column, select “G.711U-Law” as the first choice and “T.38” as the second choice as shown below. This will allow calls to and from the fax to begin with G.711 as the first codec choice and re-Invite to T.38 when fax tones are detected.



Navigate to **VoIP→Coders and Profiles→Tel Profile Settings**. Select **Profile ID “1”** and set **Fax Signaling Method** to “Fax Fallback”. Select “Coder Group 1” for the **Coder Group**.

Tel Profile Settings

Profile ID: 1
Profile Name:

Profile Parameters

Profile Preference	1
Fax Signaling Method	Fax Fallback
Enable Polarity Reversal	Enable
Enable Current Disconnect	Enable
MWI Analog Lamp	Disable
MWI Display	Disable
Echo Canceled	Enable
Flash Hook Period	700
Enable Early Media	Enable
Progress Indicator to IP	Not Configured
Dialing Mode	One Stage
Disconnect Call on Detection of Busy Tone	Enable
Time For Reorder Tone [sec]	255
Enable 911 PSAP	Disable
Swap Tel To IP Phone Numbers	Disable

Coder Group

Coder Group	Coder Group 1
-------------	---------------

Navigate to **VoIP→Coders and Profiles→IP Profile Settings**. Select **Profile ID “1”** and set **Fax Signaling Method** to “Fax Fallback”.

IP Profile Settings

Profile ID: 1
Profile Name:

Common Parameters

Disconnect on Broken Connection	Yes
Echo Canceled(*)	Enable

Gateway Parameters

Fax Signaling Method	Fax Fallback
Play Ringback Tone to IP	Don't Play
Enable Early Media	Enable
Copy Destination Number to Redirect Number	Disable
Modems Transport Type	Enable Bypass
Number of Calls Limit	-1
Progress Indicator to IP	Not Configured
Profile Preference	1
Coder Group	Default Coder Group
Enable Hold	Enable

8.2. SIP Endpoint Registration and Proxy Settings

Navigate to **VoIP→Analog Gateway→Authentication**. Set the **User Name** and **Password** for each FXS port used for fax. The **User Name** corresponds to the **Avaya SIP Handle** of the SIP User created in System Manager and the **Password** corresponds to the **Communication Profile Password** as shown in **Section 6.9**.

Gateway Port	User Name	Password
Port 1 FXS	17555	*****
Port 2 FXS	17556	*****
Port 3 FXO		
Port 4 FXO		

Navigate to **VoIP→Control Network→Proxy Sets Table**. Set the **Proxy Address** to the IP address and port used by Session Manager to listen for SIP REGISTER requests. In the sample configuration, this is “10.64.19.226:5060”. Set the **Transport Type** to “TCP”.

Proxy Set ID	Proxy Address	Transport Type
1	10.64.19.226:5060	TCP
2		
3		
4		
5		

Enable Proxy Keep Alive	Using Options
Proxy Keep Alive Time	60
Proxy Load Balancing Method	Disable
Is Proxy Hot Swap	Yes
Proxy Redundancy Mode	Not Configured
SRD Index	0
Classification Input	IP only

Navigate to **VoIP→SIP Definitions→Proxy & Registration**. Set the **Registrar Name** and **Gateway Name** to the domain name used by Session Manager as set in **Section 6.1**. Set the **Registrar IP Address** to Session Manager Security Module IP Address (10.64.19.226). Set the **Subscription Mode** and **Registration Mode** to “Per Endpoint” and verify the **Cnonce** setting. Click **Submit** and then **Register** on the bottom of the screen.

Proxy & Registration	
Use Default Proxy	Yes
Proxy Set Table	[icon]
Proxy Name	
Redundancy Mode	Homing
Proxy IP List Refresh Time	60
Enable Fallback to Routing Table	Disable
Prefer Routing Table	No
Use Routing Table for Host Names and Profiles	Disable
Always Use Proxy	Enable
Enable Registration	Enable
Registrar Name	avayalab.com
Registrar IP Address	10.64.19.226
Registrar Transport Type	TCP
Registration Time	3600
Re-registration Timing [%]	50
Registration Retry Time	30
Registration Time Threshold	0
Re-register On INVITE Failure	Disable
ReRegister On Connection Failure	Disable
Gateway Name	avayalab.com
Gateway Registration Name	
Subscription Mode	Per Endpoint
User Name	
Password	Default_Passwd
Cnonce	0a123bcbf
Registration Mode	Per Endpoint

Register Un-Register
Submit

Select the **Status & Diagnostics** menu, and navigate to **VoIP Status→Registration Status**. At this point, the the **Gateway Port(s)** used for fax should show a **Status** of “REGISTERED”.

Registration Status			
Registered Per Gateway: NO			
Ports Registration Status			
Gateway Port	Status		
Port 1: FXS	REGISTERED		
Port 2: FXS	REGISTERED		
Port 3: FXO	NOT REGISTERED		
Port 4: FXO	NOT REGISTERED		
Accounts Registration Status			
Index	Group Type	Group Name	Status

8.3. Routing

Select **Configuration** menu again on the top left of the screen, and navigate to **VoIP→GW and IP to IP→Hunt Group→EndPoint Phone Number**. Configure a Channel for each FXS port used for fax as shown below. Set the **Hunt Group ID** to “1”. Set the **Tel Profile ID** to the ID modified in **Section 8.1**.

The screenshot shows the 'Endpoint Phone Number Table' configuration screen. On the left is a navigation tree with 'Basic' and 'Full' tabs. The 'Basic' tab is selected, and the tree is expanded to 'Hunt Group > EndPoint Phone Number'. The main area contains a table with 5 columns: Index, Channel(s), Phone Number, Hunt Group ID, and Tel Profile ID. The table has 4 rows of data.

	Channel(s)	Phone Number	Hunt Group ID	Tel Profile ID
1	1	17555	1	1
2	2	17556	1	1
3				
4				

Navigate to **VoIP→GW and IP to IP→Hunt Group→Hunt Group Settings**. Configure **Hunt Group ID** “1” with **Channel Select Mode** set to “By Dest Phone Number” and **Registration Mode** set to “Per Endpoint”.

The screenshot shows the 'Hunt Group Settings' configuration screen. On the left is a navigation tree with 'Basic' and 'Full' tabs. The 'Basic' tab is selected, and the tree is expanded to 'Hunt Group > Hunt Group Settings'. The main area shows a table with 4 columns: Index, Hunt Group ID, Channel Select Mode, and Registration Mode. The table has 8 rows of data. The first row is pre-filled with values.

	Hunt Group ID	Channel Select Mode	Registration Mode
1	1	By Dest Phone Number	Per Endpoint
2			
3			
4			
5			
6			
7			
8			

Navigate to **VoIP→GW and IP to IP→Routing→Tel to IP Routing**. Set the **Src. Trunk Group ID**, **Dest. Phone Prefix**, and **Source Phone Prefix** to “*”. Set the **Dest. IP Address** to the Session Manager Security Module IP Address (10.64.19.226).

Tel to IP Routing

Routing Index: 1-10
Tel To IP Routing Mode: Route calls before manipulation

	Src. Trunk Group ID	Dest. Phone Prefix	Source Phone Prefix	->	Dest. IP Address	Port	Transport Type	Dest. IPGroup ID	Dest. SRD	IP Profile ID
1	*	*	*		10.64.19.226		TCP	-1	-1	1
2							Not Configured	-1		
3							Not Configured	-1		
4							Not Configured	-1		
5							Not Configured	-1		
6							Not Configured	-1		
7							Not Configured	-1		
8							Not Configured	-1		
9							Not Configured	-1		
10							Not Configured	-1		

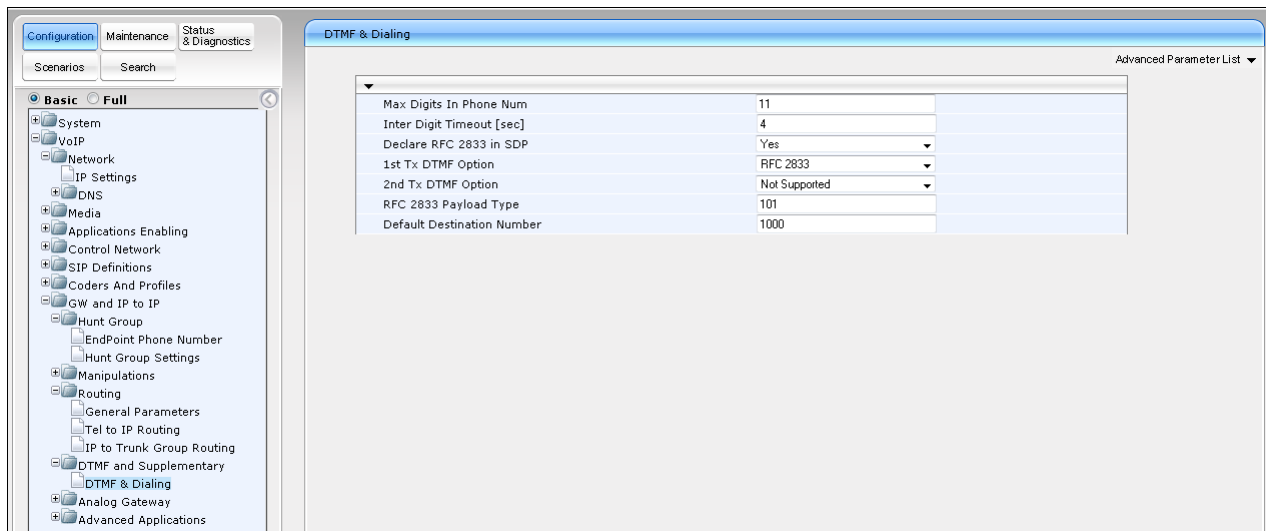
Navigate to **VoIP→GW and IP to IP→Routing→IP to Trunk Group Routing**. Set the **Dest. Phone Prefix** for each FXS port used for fax with the appropriate extension number as shown below. Set the **Source Phone Prefix** and **Source IP Address** to “*”. Set the **Hunt Group ID** to “1” and **IP Profile ID** to “1” for each extension number.

IP To Hunt Group Routing Table

Routing Index: 1-12
IP To Tel Routing Mode: Route calls after manipulation

	Dest. Phone Prefix	Source Phone Prefix	Source IP Address	->	Hunt Group ID	IP Profile ID
1	17555	*	*		1	1
2	17556	*	*		1	1
3						
4						
5						
6						
7						
8						
9						
10						
11						
12						

Navigate to **VoIP→GW and IP to IP→DTMF and Supplementary→DTMF & Dialing**. Set the **Max Digits In Phone Num** to the maximum amount of digits the fax machine will use to dial a PSTN fax machine.



9. Verizon Business IP Trunk Services Suite Configuration

Information regarding the Verizon Business IP Trunk Services suite offer can be found at <http://www.verizonbusiness.com/Products/communications/ip-telephony/> or by contacting a Verizon Business sales representative.

The reference configuration described in these Application Notes is located in the Avaya Solutions and Interoperability Test Lab. Access to the Verizon Business IP Trunk Services suite was via a Verizon Private IP (PIP) T1 connection. Verizon Business provided all of the necessary service provisioning.

9.1. Service Access Information

The following service access information (FQDN, ports, DID numbers) was provided by Verizon for the sample configuration.

CPE (Avaya)	Verizon Network
<i>adevc.avaya.globalipcom.com</i> <i>UDP port 5060</i>	<i>pcelban0001.avayalincroft.globalipcom.com</i> <i>UDP Port 5071</i>

IP DID Numbers
732-945-0231
732-945-0232
732-945-0233
732-945-0234
732-945-0235
732-945-0236
732-945-0237
732-945-0238
732-945-0239

10. Verification Steps

This section provides example verifications of the Avaya configuration with Verizon Business Private IP (PIP) Trunk service.

10.1. Avaya Aura® Communication Manager Verifications

This section illustrates verifications from Communication Manager.

10.1.1 Example Incoming Call from PSTN via Verizon SIP Trunk

Incoming PSTN calls arrive from Verizon at Avaya SBCE, which sends the call to Session Manager. Session Manager sends the call to Communication Manager. On Communication Manager, the incoming call arrives via signaling group 1 and trunk group 1.

The following edited Communication Manager *list trace tac* trace output shows a call incoming on trunk group 1. The PSTN telephone dialed 732-945-0232. Session Manager mapped the number received from Verizon to the extension of a Communication Manager telephone (x12002). Extension 12002 is an IP Telephone with IP address 10.64.19.109 in Region 1. The RTP media path is “ip-direct” from the IP Telephone (10.64.19.109) to the “inside” of the Avaya SBCE (10.64.19.140) in Region 2.

list trace tac *01		Page 1
LIST TRACE		
time	data	
14:30:19	TRACE STARTED 03/26/2013 CM Release String cold-02.0.823.0-20396	
14:30:26	SIP<INVITE sip:12002@avayalab.com SIP/2.0	
14:30:26	Call-ID: BW203026076260313-1913181969@65.211.120.226	
14:30:26	active trunk-group 1 member 249 cid 0x32d	
14:30:26	SIP>SIP/2.0 180 Ringing	
14:30:26	Call-ID: BW203026076260313-1913181969@65.211.120.226	
14:30:26	dial 12002	
14:30:26	ring station 12002 cid 0x32d	
14:30:28	SIP>SIP/2.0 200 OK	
14:30:28	Call-ID: BW203026076260313-1913181969@65.211.120.226	
14:30:28	active station 12002 cid 0x32d	
14:30:28	G729A ss:off ps:20	
	rgn:1 [10.64.19.109]:3132	
	rgn:2 [10.64.19.140]:35022	
14:30:28	G729A ss:off ps:20	
	rgn:2 [10.64.19.140]:35022	
	rgn:1 [10.64.19.109]:3132	
14:30:28	SIP<ACK sip:12002@10.64.19.155:5061;transport=tls SIP/2.0	
14:30:28	Call-ID: BW203026076260313-1913181969@65.211.120.226	
14:30:35	SIP>BYE sip:3035387006@10.64.19.140:5060;transport=tcp;gsid	
14:30:35	SIP>=fded8570-9653-11e2-b83f-9c8e992b0a68 SIP/2.0	
14:30:35	Call-ID: BW203026076260313-1913181969@65.211.120.226	
14:30:35	idle station 12002 cid 0x32d	

The following screen shows **Page 2** of the output of the *status trunk* command pertaining to this same call. Note the signaling using port 5061 between Communication Manager and Session Manager. Note the media is “ip-direct” from the IP Telephone (10.64.19.109) to the inside IP address of Avaya SBCE (10.64.19.140) using codec G.729a.

```

status trunk 1/249                                     Page 2 of 3
                                CALL CONTROL SIGNALING

Near-end Signaling Loc: PROCR
  Signaling   IP Address                               Port
  Near-end:   10.64.19.155                             : 5061
  Far-end:    10.64.19.226                             : 5061
H.245 Near:
H.245 Far:
  H.245 Signaling Loc:                               H.245 Tunneler in Q.931? no

Audio Connection Type: ip-direct      Authentication Type: None
  Near-end Audio Loc:                               Codec Type: G.729A
  Audio       IP Address                           Port
  Near-end:   10.64.19.109                         : 3132
  Far-end:    10.64.19.140                         : 35024

Video Near:
Video Far:
Video Port:
Video Near-end Codec:                  Video Far-end Codec:

```

The following screen shows **Page 3** of the output of the *status trunk* command pertaining to this same call. Here it can be observed that G.729a codec is used.

```

status trunk 1/249                                     Page 3 of 3
                                SRC PORT TO DEST PORT TALKPATH

src port: T00249
T00249:TX:10.64.19.140:35024/g729a/20ms
S00025:RX:10.64.19.109:3132/g729a/20ms

```

10.1.2 Example Outgoing Calls to PSTN via Verizon IP Trunk

The following edited trace shows an outbound ARS call from IP Telephone x12002 to the PSTN number 9-1-303-538-7024. The call is routed to route pattern 1 and trunk group 1. The call initially uses the G450 gateway (10.64.19.81), but after the call is answered, the call is “shuffled” to become an “ip-direct” connection between the IP Telephone (10.64.19.109) and the “inside” of the Avaya SBCE (10.64.19.140).

```
list trace tac *01                                     Page 1
LIST TRACE
time          data
14:40:29 TRACE STARTED 03/26/2013 CM Release String cold-02.0.823.0-20396
14:40:34      dial 913035387024 route:PREFIX|FNPA|ARS
14:40:34      route-pattern 1 preference 1 location 1/ALL cid 0x330
14:40:34      seize trunk-group 1 member 20 cid 0x330
14:40:34      Calling Number & Name 12002 test IP
14:40:34 SIP>INVITE sip:3035387024@avayalab.com SIP/2.0
14:40:34      Call-ID: 070bf25995e2188225156b4a00
14:40:34      Setup digits 13035387024
14:40:34      Calling Number & Name 12002 test IP
14:40:34 SIP<SIP/2.0 100 Trying
14:40:34      Call-ID: 070bf25995e2188225156b4a00
14:40:34      Proceed trunk-group 1 member 20 cid 0x330
14:40:37 SIP<SIP/2.0 183 Session Progress
14:40:37      Call-ID: 070bf25995e2188225156b4a00
14:40:37      G729 ss:off ps:20
14:40:37      rgn:2 [10.64.19.140]:35026
14:40:37      rgn:1 [10.64.19.81]:2052
14:40:37      xoip options: fax:T38 modem:off tty:US uid:0x5000c
14:40:37      xoip ip: [10.64.19.81]:2052
14:40:39 SIP<SIP/2.0 200 OK
14:40:39      Call-ID: 070bf25995e2188225156b4a00
14:40:39 SIP>ACK sip:3035387024@10.64.19.140:5060;transport=tcp;gsi
14:40:39 SIP>d=68c5b470-9655-11e2-b83f-9c8e992b0a68 SIP/2.0
14:40:39      Call-ID: 070bf25995e2188225156b4a00
14:40:39      active trunk-group 1 member 20 cid 0x330
14:40:39 SIP>INVITE sip:13035387024@10.64.19.140:5060;transport=tcp;
14:40:39 SIP>gsid=68c5b470-9655-11e2-b83f-9c8e992b0a68 SIP/2.0
14:40:39      Call-ID: 070bf25995e2188225156b4a00
14:40:39 SIP<SIP/2.0 100 Trying
14:40:39      Call-ID: 070bf25995e2188225156b4a00
14:40:39 SIP<SIP/2.0 200 OK
14:40:39      Call-ID: 070bf25995e2188225156b4a00
14:40:39      G729 ss:off ps:20
14:40:39      rgn:1 [10.64.19.109]:3132
14:40:39      rgn:2 [10.64.19.140]:35026
14:40:39 SIP>ACK sip:3035387024@10.64.19.140:5060;transport=tcp;gsi
14:40:39 SIP>d=68c5b470-9655-11e2-b83f-9c8e992b0a68 SIP/2.0
14:40:39      Call-ID: 070bf25995e2188225156b4a00
14:40:39      G729A ss:off ps:20
14:40:39      rgn:2 [10.64.19.140]:35026
14:40:39      rgn:1 [10.64.19.109]:3132
14:41:16 SIP<BYE sip:12002@10.64.19.155:5061;transport=tls SIP/2.0
14:41:16      Call-ID: 070bf25995e2188225156b4a00
14:41:16 SIP>SIP/2.0 200 OK
14:41:16      Call-ID: 070bf25995e2188225156b4a00
14:41:16      idle trunk-group 1 member 20 cid 0x330
```


10.2. Avaya Aura® System Manager and Avaya Aura® Session Manager Verifications

This section contains verification steps that may be performed using System Manager for Session Manager.

10.2.1 Verify SIP Entity Link Status

Log in to System Manager. Expand **Elements** → **Session Manager** → **System Status** → **SIP Entity Monitoring**, as shown below.

▼ Session Manager
Dashboard
Session Manager
Administration
Communication Profile Editor
▶ Network Configuration
▶ Device and Location Configuration
▶ Application Configuration
▼ System Status
System State
Administration
SIP Entity Monitoring

Home / Elements / Session Manager / System Status / SIP Entity Monitoring
[Help ?](#)

SIP Entity Link Monitoring Status Summary

This page provides a summary of Session Manager SIP entity link monitoring status.

SIP Entities Status for All Monitoring Session Manager Instances

Run Monitor

1 Items | Refresh
Filter: Enable

<input type="checkbox"/>	Session Manager	Type	Monitored Entities					
			Down	Partially Up	Up	Not Monitored	Deny	Total
<input type="checkbox"/>	ASM	Core	0	0	5	0	0	5

All Monitored SIP Entities

Run Monitor

5 Items (1 Selected) | Refresh
Filter: Enable

<input type="checkbox"/>	SIP Entity Name
<input type="checkbox"/>	Loc19-CM-TG1
<input type="checkbox"/>	Loc19-CM Messaging
<input type="checkbox"/>	CS1K
<input checked="" type="checkbox"/>	Vz_ASBCE-1
<input type="checkbox"/>	Vz_ASBCE-2

From the list of monitored entities, select an entity of interest, such as “Vz_ASBCE-1”. Under normal operating conditions, the **Link Status** should be “UP” as shown in the example screen below.

All Entity Links to SIP Entity: Vz_ASBCE-1

Summary View

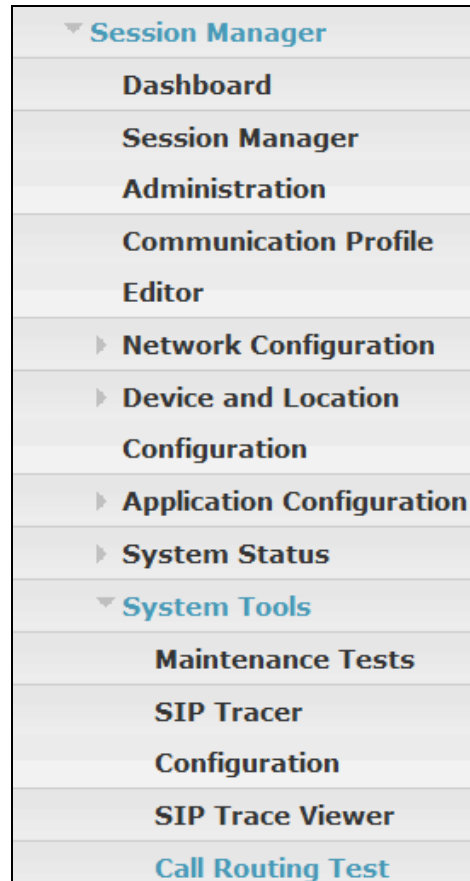
Status Details for the selected Session Manager:

1 Items | Refresh
Filter: Enable

	Session Manager Na	SIP Entity Resolved IP	Port	Proto.	Deny	Conn. Status	Reason Code	Link Status
<input type="radio"/>	ASM	10.64.19.140	5060	TCP	FALSE	UP	200 OK	UP

10.2.2 Call Routing Test

The **Call Routing Test** verifies the routing for a particular source and destination. To run the routing test, expand **Elements** → **Session Manager** → **System Tools** → **Call Routing Test**, as shown below.



A screen such as the following is displayed.

[Home](#) / [Elements](#) / [Session Manager](#) / [System Tools](#) / [Call Routing Test](#)[Help ?](#)

Call Routing Test

This page allows you to test SIP routing algorithms on Session Manager instances. Enter information about a SIP INVITE to learn how it will be routed based on current administration.

SIP INVITE Parameters

Called Party URI	Calling Party Address
<input type="text"/>	<input type="text"/>
Calling Party URI	Session Manager Listen Port
<input type="text"/>	<input type="text" value="5060"/>
Day Of Week	Transport Protocol
<input type="text" value="Wednesday"/>	<input type="text" value="TCP"/>
Time (UTC)	
<input type="text" value="15:32"/>	
Called Session Manager Instance	
<input type="text" value="Select Target..."/>	<input type="button" value="Execute Test"/>

Populate the fields for the call parameters of interest. For example, the following screen shows an example call routing test for an outbound call to the PSTN via Verizon. Under **Routing Decisions**, observe that the call will route via an Avaya SBCE on the path to Verizon. Scroll down to inspect the details of the **Routing Decision Process** if desired (not shown).

Home / Elements / Session Manager / System Tools / Call Routing Test

Call Routing Test

This page allows you to test SIP routing algorithms on Session Manager instances. Enter information about a SIP INVITE to learn how it will be routed based on current administration.

SIP INVITE Parameters

Called Party URI <input type="text" value="3035387024@avayalab.com"/>	Calling Party Address <input type="text" value="10.64.19.205"/>
Calling Party URI <input type="text" value="12002@avayalab.com"/>	Session Manager Listen Port <input type="text" value="5061"/>
Day Of Week Time (UTC) Wednesday 15:28	Transport Protocol TLS
Called Session Manager Instance ASM	<input type="button" value="Execute Test"/>

Routing Decisions

Route < sip:3035387024@avayalab.com > to SIP Entity Vz_ASBCE-1 (10.64.19.140). Terminating Location is Vz-ASBCE.
Route < sip:3035387024@avayalab.com > to SIP Entity Vz_ASBCE-2 (10.64.19.141). Terminating Location is Vz-ASBCE.

Another example shows an inbound call to one of Verizon assigned DID numbers. Observe that the DID number 732-945-0232 has been converted to Communication Manager extension 12002 under **Routing Decisions** and will be routed to Communication Manager.

Home / Elements / Session Manager / System Tools / Call Routing Test

Call Routing Test

This page allows you to test SIP routing algorithms on Session Manager instances. Enter information about a SIP INVITE to learn how it will be routed based on current administration.

SIP INVITE Parameters

Called Party URI <input type="text" value="7329450232@avayalab.com"/>	Calling Party Address <input type="text" value="10.64.19.140"/>
Calling Party URI <input type="text" value="3035551234@avayalab.com"/>	Session Manager Listen Port <input type="text" value="5060"/>
Day Of Week Time (UTC) Wednesday 20:14	Transport Protocol TCP
Called Session Manager Instance ASM	<input type="button" value="Execute Test"/>

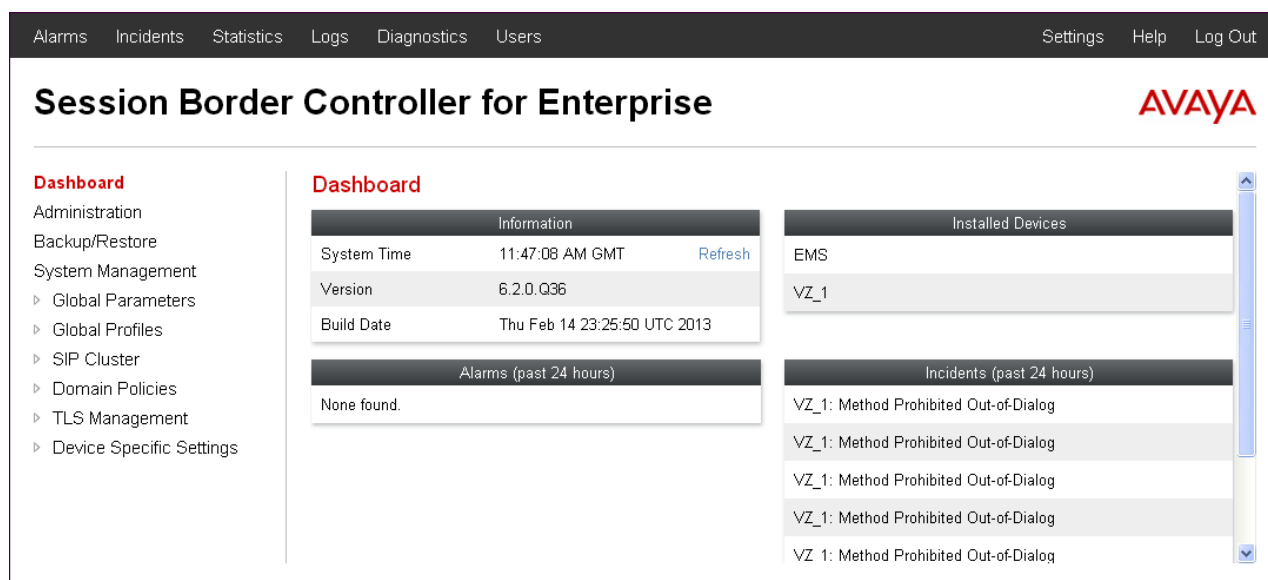
Routing Decisions

Route < sip:12002@avayalab.com > to SIP Entity Loc19-CM-TG1 (10.64.19.205). Terminating Location is Loc19-CM.

10.3. Avaya Session Border Controller for Enterprise Verification

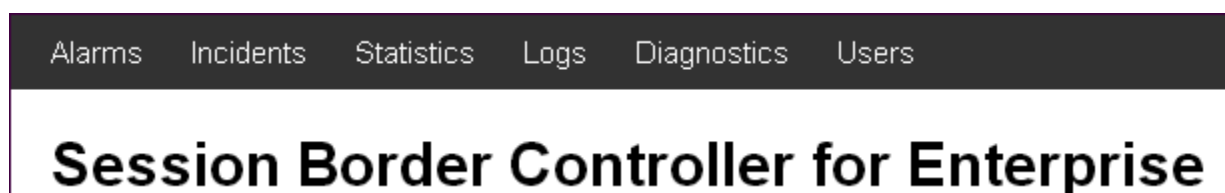
10.3.1 Welcome Screen

The welcome screen shows alarms, incidents, and the status of all managed Avaya SBCs at a glance.

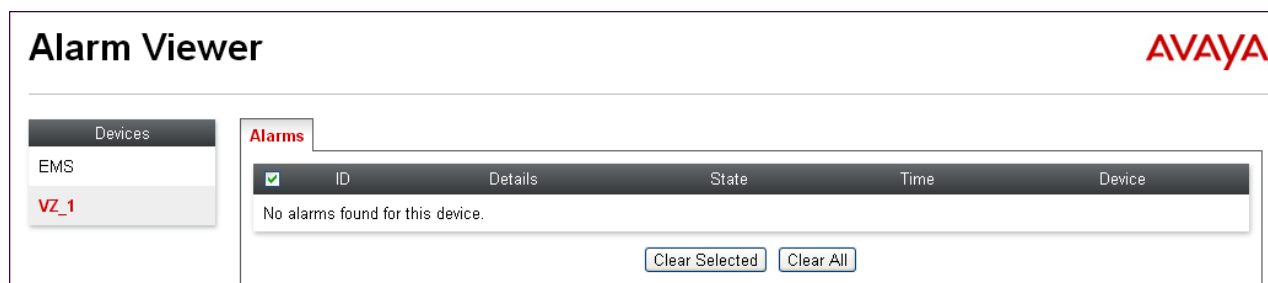


10.3.2 Alarms

A list of the most recent alarms can be found under the **Alarms** tab on the top left bar.



Alarm Viewer.




10.3.3 Incidents

A list of all recent incidents can be found under the **Incidents** tab at the top left next to the Alarms.

Incident Viewer:

Incident Viewer



Device All Category All Clear Refresh Generate Report

Displaying results 61 to 75 out of 2000.

Type	ID	Date	Time	Category	Device	Cause
Message Dropped	684874147805223	5/28/13	1:38 PM	Policy	VZ_1	No Server Flow Matched for Incoming Message
Message Dropped	684874147803744	5/28/13	1:38 PM	Policy	VZ_1	No Server Flow Matched for Incoming Message
Message Dropped	684874147557151	5/28/13	1:38 PM	Policy	VZ_1	No Server Flow Matched for Incoming Message
Message Dropped	684874147554881	5/28/13	1:38 PM	Policy	VZ_1	No Server Flow Matched for Incoming Message
Server Heartbeat	684874143447079	5/28/13	1:38 PM	Policy	VZ_1	Heartbeat Failed, Server is Down
Server Heartbeat	684874140446076	5/28/13	1:38 PM	Policy	VZ_1	Heartbeat Failed, Server is Down
Server Heartbeat	684873948921126	5/28/13	1:31 PM	Policy	VZ_1	Heartbeat Failed, Server is Down
Server Heartbeat	684873942136097	5/28/13	1:31 PM	Policy	VZ_1	Heartbeat Failed, Server is Down
Message Dropped	684873910362024	5/28/13	1:30 PM	Policy	VZ_1	Method Prohibited Out-of-Dialog
Message Dropped	684873880366952	5/28/13	1:29 PM	Policy	VZ_1	Method Prohibited Out-of-Dialog
Message Dropped	684873850371848	5/28/13	1:28 PM	Policy	VZ_1	Method Prohibited Out-of-Dialog
Message Dropped	684873820376800	5/28/13	1:27 PM	Policy	VZ_1	Method Prohibited Out-of-Dialog
Message Dropped	684873790381735	5/28/13	1:26 PM	Policy	VZ_1	Method Prohibited Out-of-Dialog
Message Dropped	684873760386666	5/28/13	1:25 PM	Policy	VZ_1	Method Prohibited Out-of-Dialog
Message Dropped	684873730391513	5/28/13	1:24 PM	Policy	VZ_1	Method Prohibited Out-of-Dialog

<< < 1 2 3 4 5 6 7 8 9 > >>

Further Information can be obtained by clicking on an incident in the incident viewer.

Incident Information			
General Information			
Incident Type	Server Heartbeat	Category	Policy
Timestamp	May 28, 2013 1:31:37 PM GMT	Device	VZ_1
Cause	Heartbeat Failed, Server is Down		
Message Data			
Response Code	408	Transport	UDP
Call ID	44e850483e6b6b28cdb9371b10a5f17cshiepaertab	From	sip:Ping@adevc.avaya.globalipcom.com
To	sip:Ping@pcelban0001.avayalincroft.globalipcom.com	Source IP	172.30.209.21
Destination IP	1.1.1.2		
Server Configuration	Vz_IPT		

10.3.4 Diagnostics

The full diagnostics check that can be run can run line checks in both directions.

Click on **Diagnostics** on the top bar, select the Avaya SBCE from the list of devices and then click “Start Diagnostics”.

Full Diagnostic

Ping Test

Application

Protocol

Start Diagnostic

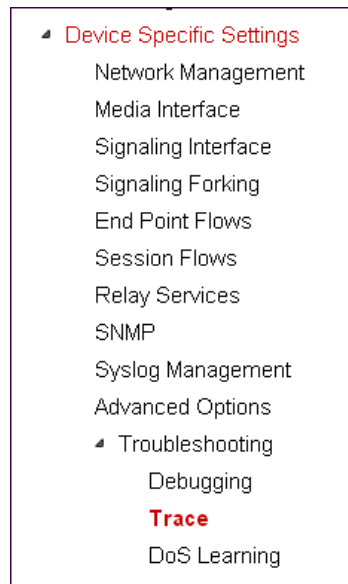
	Task Description	Status
⊖	EMS Link Check	
⊖	UC-Sec Link Check: A1	
⊖	UC-Sec Link Check: B1	
⊖	Ping: UC-Sec (10.80.140.141) to Gateway (10.80.140.1)	
⊖	Ping: UC-Sec (10.80.140.141) to Primary DNS (172.30.209.4)	
⊖	Ping: UC-Sec (2.2.2.2) to Gateway (2.2.2.1)	
⊖	Ping: UC-Sec (2.2.2.2) to Primary DNS (172.30.209.4)	

A green check mark or a red x will indicate success or failure.

Full Diagnostic		Ping Test	Application	Protocol		
					Start Diagnostic	
	Task Description			Status		
✓	EMS Link Check			eth5 is operating within normal parameters with a - duplex connection at 10Mb/s.		
✓	UC-Sec Link Check: A1			eth3 is operating within normal parameters with a - duplex connection at 10Mb/s.		
✓	UC-Sec Link Check: B1			eth1 is operating within normal parameters with a - duplex connection at 10Mb/s.		
✓	Ping: UC-Sec (10.80.140.141) to Gateway (10.80.140.1)			Average ping from 10.80.140.141 to 10.80.140.1 is 1.232ms.		
✗	Ping: UC-Sec (10.80.140.141) to Primary DNS (172.30.209.4)			Error: Unable to reach 172.30.209.4 from 10.80.140.141.		
✓	Ping: UC-Sec (2.2.2.2) to Gateway (2.2.2.1)			Average ping from 2.2.2.2 to 2.2.2.1 is 1.809ms.		
✗	Ping: UC-Sec (2.2.2.2) to Primary DNS (172.30.209.4)			Error: Unable to reach 172.30.209.4 from 2.2.2.2.		

10.3.5 Tracing

To take a call trace, Select **Device Specific Settings** → **Troubleshooting** → **Tracing** from the left-side menu as shown below.



Select the **Packet Capture** tab and set the desired configuration for a call trace and click **Start Capture**.

Trace: VZ_1

Devices

VZ_1

Call Trace **Packet Capture** Captures

Packet Capture Configuration

Status	Ready
Interface	B1
Local Address IP[:Port]	All :
Remote Address *, *:Port, IP, IP:Port	*
Protocol	All
Maximum Number of Packets to Capture	9990
Capture Filename Using the name of an existing capture will overwrite it.	Test-Trace.pcap

Start Capture Clear

When tracing has reached the desired number of packets the trace will stop automatically, or alternatively, click the **Stop Capture** button at the bottom.

Trace: VZ_1

Devices
VZ_1

Call Trace
Packet Capture
Captures

A packet capture is currently in progress. This page will automatically refresh until the capture completes.

Packet Capture Configuration

Status: In Progress

Interface: B1

Local Address IP:Port: All :

Remote Address *,*,Port, IP, IP:Port: *

Protocol: All

Maximum Number of Packets to Capture: 9990

Capture Filename Using the name of an existing capture will overwrite it. Test-Trace.pcap

Stop Capture

Select the **Captures** tab at the top and the capture will be listed; select the **File Name** and choose to open it with an application like Wireshark.

Trace: VZ_1

Devices
VZ_1

Call Trace
Packet Capture
Captures

Last Modified Descending Sort Reset Refresh

File Name	File Size (bytes)	Last Modified	
Test-Trace_20130613110845.pcap	90,112	June 13, 2013 11:09:54 AM GMT	Delete

11. Conclusion

As illustrated in these Application Notes, Avaya Aura® Communication Manager 6.3, Avaya Aura® Session Manager 6.3, and Avaya Session Border Controller for Enterprise can be configured to interoperate successfully with Verizon Business IP Trunk service. This solution allows Avaya Aura® Communication Manager and Avaya Aura® Session Manager users access to the PSTN using a Verizon Business IP Trunk public SIP trunk service connection.

12. Additional References

12.1. Avaya

Avaya product documentation, including the following, is available at <http://support.avaya.com>

- [1] *Implementing Avaya Aura® Communication Manager*, Doc ID 03-603558, Release 6.3
- [2] *Administering Avaya Aura® Communication Manager*, Doc ID 03-300509, Release 6.3
- [3] *Implementing Avaya Aura® Session Manager*, Release 6.3
- [4] *Installing Service Packs for Avaya Aura® Session Manager*, Release 6.3
- [5] *Upgrading Avaya Aura® Session Manager*, Release 6.3
- [6] *Maintaining and Troubleshooting Avaya Aura® Session Manager*, Release 6.3
- [7] *Implementing Avaya Aura® System Manager*, Release 6.3
- [8] *Installing Avaya Session Border Controller for Enterprise*, Release 6.2
- [9] *Administering Avaya Session Border Controller for Enterprise*, Release 6.2

Avaya Application Notes, including the following, are also available at <http://support.avaya.com>

The following Application Notes cover Session Manager 6.2 with Verizon IP SIP Trunk Service using the Avaya Session Border Controller for Enterprise.

[MO-VZIPT-SM62] Application Notes for Avaya Aura® Communication Manager 6.2, Avaya Aura® Session Manager 6.2, and Avaya Session Border Controller for Enterprise with Verizon Business IP Trunk SIP Trunk Service – Issue 1.0

<http://downloads.avaya.com/css/P8/documents/100162132>

The following Application Notes cover Session Manager 6.1 with Verizon IP SIP Trunk Service using the Avaya Session Border Controller for Enterprise.

[MO-VZIPT-SM61] Application Notes for Avaya Aura® Communication Manager 6.0.1, Avaya Aura® Session Manager 6.1, and Avaya Session Border Controller for Enterprise with Verizon Business IP Trunk SIP Trunk Service – Issue 1.0

<http://downloads.avaya.com/css/P8/documents/100164354>

12.2. Verizon Business

The following documents may be obtained by contacting a Verizon Business Account Representative.

- *Retail VoIP Interoperability Test Plan*
- *Network Interface Specification Retail VoIP Trunk Interface (for non-registering devices)*

12.3. AudioCodes

The following document is available at <http://audiocodes.com>

- *Verizon T.38 FAX Configuration Guide for AudioCodes MP-11x*

Appendix A

This section covers the configuration settings of Avaya SBCE, Session Manager, and a sample endpoint as used for Remote Workers during compliance testing. In the test environment, a dedicated Avaya SBCE with private IP addresses was used to access the Verizon Business Private IP (PIP) IP Trunk service. To allow remote SIP endpoints access to the test environment through a public network, a separate Avaya SBCE with public IP addresses was utilized. The settings presented here simply illustrate the sample configuration used during compliance testing with Verizon IP Trunk service, and are not intended to be prescriptive. Other routing criteria and policies may be appropriate based on different customer needs.

Standard and Advanced Session Licenses are required for Remote Worker. Contact an authorized Avaya representative for assistance if additional licensing is required.

The following screen shows the **Network Management** screen of the Avaya SBCE. The internal interface is assigned to **A1** and the external interfaces are assigned to **B1**. Avaya SIP endpoints registered to IP address “192.168.62.92” and retrieved firmware and configuration data from IP address “192.168.63.123”. For security reasons, any actual public IP addresses used in the configuration have been replaced with private IP addresses.

Note – A SIP Entity in Session Manager was *not* configured for the Avaya SBCE’s internal IP address used for Remote Worker. This keeps the interface untrusted in Session Manager, thereby allowing Session Manager to properly challenge user registration requests.

The screenshot shows the Avaya Session Border Controller for Enterprise (SBCE) Network Management interface. The top navigation bar includes Alarms, Incidents, Statistics, Logs, Diagnostics, Users, Settings, Help, and Log Out. The main header displays "Session Border Controller for Enterprise" and the Avaya logo. A left sidebar lists various management sections, with "Network Management" highlighted. The main content area is titled "Network Management: ASBCE" and contains two tabs: "Network Configuration" and "Interface Configuration". A warning message states: "Modifications or deletions of an IP address or its associated data require an application restart before taking effect. Application restarts can be issued from System Management." Below this, there are input fields for A1 Netmask (255.255.255.0), A2 Netmask, B1 Netmask (255.255.255.128), and B2 Netmask, with "Add", "Save", and "Clear" buttons. A table lists configured interfaces with columns for IP Address, Public IP, Gateway, and Interface. The table contains three entries: 192.168.62.92 (Public IP blank, Gateway 192.168.62.1, Interface B1), 10.64.19.200 (Public IP blank, Gateway 10.64.19.1, Interface A1), and 192.168.62.123 (Public IP blank, Gateway 192.168.62.1, Interface B1). Each entry has a "Delete" button.

IP Address	Public IP	Gateway	Interface	
192.168.62.92		192.168.62.1	B1	Delete
10.64.19.200		10.64.19.1	A1	Delete
192.168.62.123		192.168.62.1	B1	Delete

It is possible to deploy Remote Worker using the same Avaya SBCE as the one used for SIP trunking. However, separate IP addresses are needed for each function. This allows the Avaya SBCE to enforce proper security policies as if it were two different Avaya SBCEs. Only two network interfaces on the Avaya SBCE may be active at one time, so this requires all external IP addresses to be on the same subnet so they may be applied to the same network interface. Similarly, additional internal IP addresses must be on the same internal subnet.

Interfaces **A1** and **B1** were both set to **Enabled**.

The screenshot shows the 'Session Border Controller for Enterprise' web interface. The left sidebar contains a navigation menu with 'Network Management' highlighted. The main content area is titled 'Network Management: ASBCE' and has two tabs: 'Network Configuration' and 'Interface Configuration'. The 'Interface Configuration' tab is active, displaying a table of interfaces.

Name	Administrative Status	
A1	Enabled	Toggle
A2	Disabled	Toggle
B1	Enabled	Toggle
B2	Disabled	Toggle

The following screen shows the **Media Interface** settings. Media interfaces were created for the inside and outside IP interfaces used for Remote Worker SIP traffic.

The screenshot shows the 'Session Border Controller for Enterprise' web interface. The left sidebar has 'Media Interface' selected under 'Device Specific Settings'. The main content area is titled 'Media Interface: ASBCE' and has a 'Media Interface' tab. A warning message states: 'Modifying or deleting an existing media interface will require an application restart before taking effect. Application restarts can be issued from System Management.' Below this is a table of media interfaces.

Name	Media IP	Port Range	
Media_Outside_92	192.168.62.92	8000 - 8999	Edit Delete
Media_Inside_200	10.64.19.200	2048 - 5059	Edit Delete

The following screen shows the **Signaling Interface** settings. Signaling interfaces were also created for the inside and outside IP interfaces used for Remote Worker SIP traffic. The interface named “Sig_Outside_92” supports TCP and TLS, while the interface named “Sig_Inside_200” supports TLS only.

The screenshot shows the 'Session Border Controller for Enterprise' web interface. The left sidebar has 'Signaling Interface' selected under 'Device Specific Settings'. The main content area is titled 'Signaling Interface: ASBCE' and has a 'Signaling Interface' tab. A table of signaling interfaces is displayed.

Name	Signaling IP	TCP Port	UDP Port	TLS Port	TLS Profile	
Sig_Outside_92	192.168.62.92	5060	---	5061	AvayaSBCServer	Edit Delete
Sig_Inside_200	10.64.19.200	---	---	5061	AvayaSBCServer	Edit Delete

Routing Profile “SessionMgr-TLS” was created for Session Manager as shown in the following screens.

The screenshot shows the 'Session Border Controller for Enterprise' web interface. The top navigation bar includes 'Alarms', 'Incidents', 'Statistics', 'Logs', 'Diagnostics', 'Users', 'Settings', 'Help', and 'Log Out'. The main header displays 'Session Border Controller for Enterprise' and the 'AVAYA' logo. On the left, a sidebar menu lists 'Global Parameters', 'Global Profiles', and 'Routing Profiles'. Under 'Routing Profiles', 'SessionMgr-TLS' is selected. The main content area is titled 'Routing Profiles: SessionMgr-TLS' and includes buttons for 'Add', 'Rename', 'Clone', and 'Delete'. A description field is present with the text 'Click here to add a description.' Below this, a table lists the routing profiles. The table has columns for 'Priority', 'URI Group', 'Next Hop Server 1', and 'Next Hop Server 2'. A single entry is shown with Priority '1', URI Group '*', Next Hop Server 1 '10.64.19.226', and Next Hop Server 2 '--'. The table includes 'View' and 'Edit' links for each entry.

Priority	URI Group	Next Hop Server 1	Next Hop Server 2
1	*	10.64.19.226	--

The screenshot shows the 'Edit Routing Rule' dialog box. It features a blue header bar with the text 'Each URI group may only be used once per Routing Profile.' Below this, the 'Next Hop Routing' section is displayed. The 'URI Group' is set to '*'. The 'Next Hop Server 1' is set to '10.64.19.226'. The 'Next Hop Server 2' is empty. The 'Routing Priority based on Next Hop Server' checkbox is checked. The 'Use Next Hop for In Dialog Messages' checkbox is unchecked. The 'Ignore Route Header for Messages Outside Dialog' checkbox is unchecked. The 'NAPTR' checkbox is unchecked. The 'SRV' checkbox is unchecked. The 'Outgoing Transport' is set to 'TLS'. The 'Finish' button is at the bottom.

Next Hop Routing
URI Group: *
Next Hop Server 1: 10.64.19.226
Next Hop Server 2:
Routing Priority based on Next Hop Server: <input checked="" type="checkbox"/>
Use Next Hop for In Dialog Messages: <input type="checkbox"/>
Ignore Route Header for Messages Outside Dialog: <input type="checkbox"/>
NAPTR: <input type="checkbox"/>
SRV: <input type="checkbox"/>
Outgoing Transport: <input checked="" type="radio"/> TLS <input type="radio"/> TCP <input type="radio"/> UDP

The following screens illustrate the **Server Configuration** for the Profile named “SM6.3” created for Session Manager. The **Authentication** and **Heartbeat** tabs were kept at the default disabled setting.

The screenshot shows the Avaya Session Border Controller for Enterprise web interface. The top navigation bar includes Alarms, Incidents, Statistics, Logs, Diagnostics, Users, Settings, Help, and Log Out. The main header displays "Session Border Controller for Enterprise" and the Avaya logo. On the left, a sidebar lists various configuration categories, with "Server Configuration" highlighted in red. The main content area is titled "Server Configuration: SM6.3" and includes an "Add" button and "Rename", "Clone", and "Delete" buttons. Below the title, there are four tabs: "General", "Authentication", "Heartbeat", and "Advanced". The "General" tab is active, showing a table with the following configuration details:

Server Type	Call Server
IP Addresses / FQDNs	10.64.19.226
Supported Transports	TLS
TLS Port	5061

An "Edit" button is located at the bottom right of the configuration table.

On the **Advanced** tab, default profiles were specified that applies to traffic between the Avaya SBCE and Session Manager as shown below.

The screenshot shows the Avaya Session Border Controller for Enterprise web interface, specifically the "Advanced" tab of the "Server Configuration: SM6.3" profile. The top navigation bar and sidebar are consistent with the previous screenshot. The "Advanced" tab is active, displaying a table with the following configuration details:

Enable DoS Protection	<input type="checkbox"/>
Enable Grooming	<input checked="" type="checkbox"/>
Interworking Profile	avaya-ru
TLS Client Profile	AvayaSBCClient
Signaling Manipulation Script	None
TLS Connection Type	SUBID

An "Edit" button is located at the bottom right of the configuration table.

User Agents were created for each type of endpoint tested. This allows for different policies to be applied based on the type of device. For example, Avaya one-X Deskphones will use TLS and SRTP, while one-X® Communicator and Avaya Flare® will use TCP and RTP.

The screenshot shows the 'User Agents' configuration page in the Session Border Controller for Enterprise. The page has a sidebar with navigation links: Dashboard, Administration, Backup/Restore, System Management, Global Parameters (selected), RADIUS, DoS / DDoS, Scrubber, User Agents (highlighted), Global Profiles, and SIP Cluster. The main content area is titled 'User Agents' and contains a table with the following data:

Name	Regular Expression	Edit	Delete
one-X Communicator	Avaya one-X Communicator.*	Edit	Delete
Flare	Avaya Flare.*	Edit	Delete
one-X Deskphone	Avaya one-X Deskphone.*	Edit	Delete

The following abridged output of Session Manager’s traceSM command shows the details of an INVITE message from an Avaya one-X Deskphone. The **User-Agent** shown in this trace will match “one-X Deskphone” shown above with a **Regular Expression** of “Avaya one-X Deskphone.*”. In this expression, “.*” will match any software version listed after the user agent name.

```
INVITE sip:12002@avayalab.com SIP/2.0
From: <sip:14006@avayalab.com>;tag=-76557dff51bb3900-5c89896d_F1400610.80.150.111
To: <sip:12002@avayalab.com>
CSeq: 357 INVITE
Call-ID: 161_51bb3900-2ff0c2ff-5c898dda_I@10.80.150.111
Contact: <sip:14006@10.64.19.200:5061;transport=tls;subid_ipcs=448140782>;+avaya-cm-line=1
Record-Route: <sip:10.64.19.200:5061;ipcs-line=930;lr;transport=tls>
Record-Route: <sips:205.168.62.92:5061;ipcs-line=930;lr;transport=tls>
Allow:
INVITE,ACK,BYE,CANCEL,SUBSCRIBE,NOTIFY,MESSAGE,REFER,INFO,PRACK,PUBLISH,UPDATE
Supported: 100rel,eventlist,feature-ref,replaces
User-Agent: Avaya one-X Deskphone 6.2.2.17 (40235)
Max-Forwards: 69
Via: SIP/2.0/TLS 10.64.19.200:5061;branch=z9hG4bK-s1632-001744755540-1--s1632-
Via: SIP/2.0/TLS 10.80.150.111:5061;branch=z9hG4bK165_51bb39027017c28d-5c899bb5_I14006
Accept-Language: en
Content-Type: application/sdp
Content-Length: 416
```

Relay Services are used to define how firmware updates and configuration data are routed for remote endpoints. The following screen shows the **Application Relay** tab with the two application relays created for the sample configuration. This allows for both HTTP and HTTPS traffic to be routed to the appropriate internal file server. The **Remote IP:Port** was set to the IP address and port of the internal file server used to provide the firmware updates and configuration data for the remote endpoints. The **Listen IP:Port** was set to the IP address and port of the Avaya SBCE's external IP address designated for file transfers. The **Connected IP** was set to the internal IP address of the Avaya SBCE.

The screenshot shows the 'Session Border Controller for Enterprise' web interface. The left sidebar lists navigation options: Alarms, Incidents, Statistics, Logs, Diagnostics, Users, Settings, Help, and Log Out. The main content area is titled 'Relay Services: ASBCE'. Under the 'Application Relay' tab, there is a table with two entries:

Remote Domain	Remote IP:Port	Remote Transport	Published Domain	Listen IP:Port	Listen Transport	Connect IP	Whitelist Flows	
avayalab.com	10.80.150.38:80	TCP	avayalab.com	192.168.62.123:80	TCP	10.64.19.200	<input type="checkbox"/>	Edit Delete
avayalab.com	10.80.150.38:443	TCP	avayalab.com	192.168.62.123:443	TCP	10.64.19.200	<input type="checkbox"/>	Edit Delete

A **Cluster Proxy** is used for Personal Profile Manager (PPM) data and Presence services. The following screen shows the cluster proxy "remotephones" created in the sample configuration. A Presence Services server was not part of the sample configuration. Therefore, configuration of the cluster proxy for use with Presence is not shown and only configuration related to PPM data is present.

The screenshot shows the 'Session Border Controller for Enterprise' web interface. The left sidebar lists navigation options: Dashboard, Administration, Backup/Restore, System Management, Global Parameters, Global Profiles, SIP Cluster, Cluster Proxy, Domain Policies, TLS Management, and Device Specific Settings. The main content area is titled 'Cluster Proxy: remotephones'. Under the 'General' tab, there is a form with the following information:

Cluster Information	
Call Server Type	Avaya
Security Information	
Secure Mode	Disabled
Miscellaneous Information	
Domain Name	avayalab.com
Configuration Update Interval	15 minute(s)

On the **Primary** tab, PPM traffic received on **Device IP** “192.168.62.92” will be routed to the **Configuration Server Client Address** “10.64.19.200”. The **Real IP** field is not used for PPM, so any IP address can be entered, e.g., “1.2.3.4”. This enables the remote Avaya SIP endpoints to send and receive PPM information to and from Session Manager via the Avaya SBCE.

Alarms
Incidents
Statistics
Logs
Diagnostics
Users
Settings
Help
Log Out

Session Border Controller for Enterprise

Dashboard
Administration
Backup/Restore
System Management
Global Parameters
Global Profiles
SIP Cluster
Cluster Proxy
Domain Policies
TLS Management
Device Specific Settings

Cluster Proxy: remotephones
Add
Delete

General
Primary
Secondary
Tertiary

Device Information

Device Name	ASBCE
Device IP	192.168.62.123
Configuration Server Client Address	10.64.19.200

Edit

Configuration Servers
Add

Type	Real Type	Port	Real IP	Real Port	Relay Mode	Rewrite URL	Server TLS Profile	
HTTPS	HTTP	443	1.2.3.4	80	---	---	AvayaSBCServer	Edit Delete
HTTP Server	HTTP	80	1.2.3.4	80	Yes	---	---	Edit Delete

Signaling Servers

Server Configuration Profile	End Point Signaling Interface	Session Policy Group	
SM6.3	Sig_Outside_92	default	Edit

The following screens show the **Application Rules** “MaxVoiceSession” and “remotephones” used in the sample configuration. In an actual customer installation, set the **Maximum Concurrent Sessions** for the **Voice** application to a value slightly larger than the licensed sessions. For example, if licensed for 300 session set the values to “500”. For the “MaxVoiceSession” rule, the **Maximum Session Per Endpoint** matches the **Maximum Concurrent Sessions**. For the application rule applied to the Remote Workers subscriber flows, a value of “10” is recommended for the **Maximum Session Per Endpoint**.

The screenshot displays the Avaya Session Border Controller for Enterprise web interface. The top navigation bar includes links for Alarms, Incidents, Statistics, Logs, Diagnostics, Users, Settings, Help, and Log Out. The main header shows the product name and the Avaya logo. On the left, a sidebar menu lists various configuration areas, with 'Application Rules' highlighted under 'Domain Policies'. The main content area is titled 'Application Rules: MaxVoiceSession'. It features a list of application rules on the left, with 'MaxVoiceSession' selected. The right pane shows the configuration for this rule, including a table for application types and a miscellaneous section.

Application Type	In	Out	Maximum Concurrent Sessions	Maximum Sessions Per Endpoint
Voice	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	2000	2000
Video	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	100	100
IM	<input type="checkbox"/>	<input type="checkbox"/>		

Miscellaneous:

CDR Support	None
RTCP Keep-Alive	No

The screenshot displays the Avaya Session Border Controller for Enterprise web interface, showing the configuration for the 'remotephones' application rule. The layout is similar to the previous screenshot, but the selected rule is 'remotephones'. The table for application types shows different values for 'Maximum Concurrent Sessions' and 'Maximum Sessions Per Endpoint'.

Application Type	In	Out	Maximum Concurrent Sessions	Maximum Sessions Per Endpoint
Voice	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	2000	10
Video	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	100	10
IM	<input type="checkbox"/>	<input type="checkbox"/>		

Miscellaneous:

CDR Support	None
RTCP Keep-Alive	No

The following screens show **Media Rules** “New-Avaya-Enc” and “default-low-med” that will later be assigned to the End Point Policy Groups. Note that both rules have **Interworking** checked. Based on how calls are routed through Avaya SBCE, this will convert SRTP media to RTP and vice versa. In the sample configuration, Avaya SBCE will convert the SRTP media stream from remote Avaya 96x1 SIP Telephones to RTP towards the enterprise and also towards remote endpoints using TCP. Avaya SBCE will also convert RTP media from calls originating from Session Manager to SRTP towards Avaya 96x1 SIP Telephones using TLS through the external IP interface. The “New-Avaya-Enc” policy was cloned from the existing “default-low-med” policy. The parameters on the other tabs not shown retained their default values.

The screenshot shows the Avaya Session Border Controller for Enterprise web interface. The left sidebar contains a navigation menu with categories like Dashboard, Administration, Backup/Restore, System Management, and Domain Policies. The 'Media Rules' section is highlighted under Domain Policies. The main content area is titled 'Media Rules: New-Avaya-Enc'. It features a list of media rules on the left, including 'default-low-med', 'default-low-med-enc', 'default-high', 'default-high-enc', 'avaya-low-med-enc', 'Int-AllowShuffle', 'New-Low-Med', 'New-Avaya-Enc' (highlighted), and 'New-Avaya-Unknown'. The main configuration area for 'New-Avaya-Enc' has tabs for 'Media NAT', 'Media Encryption' (selected), 'Media Anomaly', 'Media Silencing', and 'Media QoS'. Under 'Media Encryption', there are sections for 'Audio Encryption' and 'Video Encryption'. 'Audio Encryption' shows 'Preferred Formats' as 'SRTP_AES_CM_128_HMAC_SHA1_80' and 'Interworking' checked. 'Video Encryption' shows 'Preferred Formats' as 'RTP' and 'Interworking' checked. There is also a 'Miscellaneous' section with 'Capability Negotiation' unchecked. Buttons for 'Add', 'Filter By Device...', 'Rename', 'Clone', 'Delete', and 'Edit' are visible.

The screenshot shows the Avaya Session Border Controller for Enterprise web interface. The left sidebar is the same as the previous screenshot. The main content area is titled 'Media Rules: default-low-med'. It features a list of media rules on the left, including 'default-low-med' (highlighted), 'default-low-med-enc', 'default-high', 'default-high-enc', 'avaya-low-med-enc', 'Int-AllowShuffle', 'New-Low-Med', 'New-Avaya-Enc', and 'New-Avaya-Unknown'. The main configuration area for 'default-low-med' has tabs for 'Media NAT', 'Media Encryption' (selected), 'Media Anomaly', 'Media Silencing', and 'Media QoS'. Under 'Media Encryption', there are sections for 'Audio Encryption' and 'Video Encryption'. 'Audio Encryption' shows 'Preferred Formats' as 'RTP' and 'Interworking' checked. 'Video Encryption' shows 'Preferred Formats' as 'RTP' and 'Interworking' checked. There is also a 'Miscellaneous' section with 'Capability Negotiation' unchecked. A warning message at the top states: 'It is not recommended to edit the defaults. Try cloning or adding a new rule instead.' Buttons for 'Add', 'Filter By Device...', 'Clone', and 'Edit' are visible.

The following **End Point Policy Groups** will later be assigned to the subscriber and server flows. The “Remote_User_SRTP” policy uses the “remotephones” **Application** rule and the “New-Avaya-Enc” **Media** rule.

The screenshot shows the Avaya Session Border Controller for Enterprise web interface. The left sidebar contains a navigation menu with categories like System Management, Domain Policies, and Session Policies. The 'End Point Policy Groups' link is highlighted in red. The main content area is titled 'Policy Groups: Remote_User_SRTP'. It features a list of policy groups on the left, including 'default-low', 'default-low-enc', 'default-med', 'default-med-enc', 'default-high', 'default-high-enc', 'OCS-default-high', 'avaya-def-low-enc', 'Remote_User_SRTP' (highlighted in red), 'Remote_User', and 'SM'. The 'Remote_User_SRTP' group is selected, and its configuration is displayed in a table. The table has columns for Order, Application, Border, Media, Security, Signaling, and Time of Day. A single row is shown with Order 1, Application 'remotephones', Border 'default', Media 'New-Avaya-Enc', Security 'default-low', Signaling 'default', and Time of Day 'default'. There are 'Edit' and 'Clone' buttons for this row. Above the table, there are buttons for 'Add', 'Filter By Device...', 'Rename', and 'Delete'. There are also links to 'Click here to add a description' and 'Click here to add a row description'.

The “Remote_User” policy uses the “remotephones” **Application** rule and the “default-low-med” **Media** rule.

The screenshot shows the Avaya Session Border Controller for Enterprise web interface. The left sidebar contains a navigation menu with categories like System Management, Domain Policies, and Session Policies. The 'End Point Policy Groups' link is highlighted in red. The main content area is titled 'Policy Groups: Remote_User'. It features a list of policy groups on the left, including 'default-low', 'default-low-enc', 'default-med', 'default-med-enc', 'default-high', 'default-high-enc', 'OCS-default-high', 'avaya-def-low-enc', 'Remote_User_SRTP', 'Remote_User' (highlighted in red), and 'SM'. The 'Remote_User' group is selected, and its configuration is displayed in a table. The table has columns for Order, Application, Border, Media, Security, Signaling, and Time of Day. A single row is shown with Order 1, Application 'remotephones', Border 'default', Media 'default-low-med', Security 'default-med', Signaling 'default', and Time of Day 'default'. There are 'Edit' and 'Clone' buttons for this row. Above the table, there are buttons for 'Add', 'Filter By Device...', 'Rename', and 'Delete'. There are also links to 'Click here to add a description' and 'Hover over a row to see its description'.

The “SM” policy uses the “MaxVoiceSession” **Application** rule and the “default-low-med” **Media** rule.

The screenshot shows the Avaya Session Border Controller for Enterprise web interface. The left sidebar contains a navigation menu with categories like System Management, Global Profiles, SIP Cluster, Domain Policies, and Session Policies. The 'End Point Policy Groups' link is highlighted in red. The main content area displays a list of Policy Groups. A table shows the configuration for the 'SM' policy group.

Order	Application	Border	Media	Security	Signaling	Time of Day	
1	MaxVoiceSession	default	default-low-med	default-low	default	default	Edit Clone

Three **Subscriber Flows** were created for Remote Workers. One for each **User Agent** previously created.

The screenshot shows the Avaya Session Border Controller for Enterprise web interface, specifically the 'End Point Flows: ASBCE' configuration page. The left sidebar shows the 'Device Specific Settings' menu with 'End Point Flows' highlighted in red. The main content area displays a table of Subscriber Flows.

Priority	Flow Name	URI Group	Source Subnet	User Agent	End Point Policy Group	
1	Remote-User-96x1	*	*	one-X Deskphone	Remote_User_S RTP	View Clone Edit Delete
2	Remote-User-one-X	*	*	one-X Communicator	Remote_User	View Clone Edit Delete
3	Remote-User-Flare	*	*	Flare	Remote_User	View Clone Edit Delete

The following screen shows the details of the flow named “Remote-User-96x1” used in the sample configuration. This flow will match traffic from remote Avaya 96x1 Series IP Telephones set to use TLS. Note that the **User Agent** was set to “one-X Deskphone” and that the **End Point Policy Group** was set to “Remote_User_SRTP”.

View Flow: Remote-User-96x1		View Flow: Remote-User-one-X																											
Criteria <table border="1"> <tr><td>Flow Name</td><td>Remote-User-96x1</td></tr> <tr><td>URI Group</td><td>*</td></tr> <tr><td>User Agent</td><td>one-X Deskphone</td></tr> <tr><td>Source Subnet</td><td>*</td></tr> <tr><td>Via Host</td><td>*</td></tr> <tr><td>Contact Host</td><td>*</td></tr> <tr><td>Signaling Interface</td><td>Sig_Outside_92</td></tr> </table>		Flow Name	Remote-User-96x1	URI Group	*	User Agent	one-X Deskphone	Source Subnet	*	Via Host	*	Contact Host	*	Signaling Interface	Sig_Outside_92	Optional Settings <table border="1"> <tr><td>Topology Hiding Profile</td><td>None</td></tr> <tr><td>Phone Interworking Profile</td><td>Avaya-Ru</td></tr> <tr><td>TLS Client Profile</td><td>AvayaSBCClient</td></tr> <tr><td>RADIUS Profile</td><td>None</td></tr> <tr><td>File Transfer Profile</td><td>None</td></tr> <tr><td>Signaling Manipulation Script</td><td>None</td></tr> </table>		Topology Hiding Profile	None	Phone Interworking Profile	Avaya-Ru	TLS Client Profile	AvayaSBCClient	RADIUS Profile	None	File Transfer Profile	None	Signaling Manipulation Script	None
Flow Name	Remote-User-96x1																												
URI Group	*																												
User Agent	one-X Deskphone																												
Source Subnet	*																												
Via Host	*																												
Contact Host	*																												
Signaling Interface	Sig_Outside_92																												
Topology Hiding Profile	None																												
Phone Interworking Profile	Avaya-Ru																												
TLS Client Profile	AvayaSBCClient																												
RADIUS Profile	None																												
File Transfer Profile	None																												
Signaling Manipulation Script	None																												
Profile <table border="1"> <tr><td>Source</td><td>Subscriber</td></tr> <tr><td colspan="2">Methods Allowed Before REGISTER</td></tr> <tr><td>User Agent</td><td>one-X Deskphone</td></tr> <tr><td>Media Interface</td><td>Media_Outside_92</td></tr> <tr><td>End Point Policy Group</td><td>Remote_User_SRTP</td></tr> <tr><td>Routing Profile</td><td>SessionMgr-TLS</td></tr> </table>				Source	Subscriber	Methods Allowed Before REGISTER		User Agent	one-X Deskphone	Media Interface	Media_Outside_92	End Point Policy Group	Remote_User_SRTP	Routing Profile	SessionMgr-TLS														
Source	Subscriber																												
Methods Allowed Before REGISTER																													
User Agent	one-X Deskphone																												
Media Interface	Media_Outside_92																												
End Point Policy Group	Remote_User_SRTP																												
Routing Profile	SessionMgr-TLS																												

The “Remote-User-one-X” flow will match traffic from remote one-X® Communicator devices set to use TCP. Note that the **User Agent** was set to “one-X Communicator” and that the **End Point Policy Group** was set to “Remote_User”.

View Flow: Remote-User-one-X		View Flow: Remote-User-one-X																											
Criteria <table border="1"> <tr><td>Flow Name</td><td>Remote-User-one-X</td></tr> <tr><td>URI Group</td><td>*</td></tr> <tr><td>User Agent</td><td>one-X Communicator</td></tr> <tr><td>Source Subnet</td><td>*</td></tr> <tr><td>Via Host</td><td>*</td></tr> <tr><td>Contact Host</td><td>*</td></tr> <tr><td>Signaling Interface</td><td>Sig_Outside_92</td></tr> </table>		Flow Name	Remote-User-one-X	URI Group	*	User Agent	one-X Communicator	Source Subnet	*	Via Host	*	Contact Host	*	Signaling Interface	Sig_Outside_92	Optional Settings <table border="1"> <tr><td>Topology Hiding Profile</td><td>None</td></tr> <tr><td>Phone Interworking Profile</td><td>Avaya-Ru</td></tr> <tr><td>TLS Client Profile</td><td>None</td></tr> <tr><td>RADIUS Profile</td><td>None</td></tr> <tr><td>File Transfer Profile</td><td>None</td></tr> <tr><td>Signaling Manipulation Script</td><td>None</td></tr> </table>		Topology Hiding Profile	None	Phone Interworking Profile	Avaya-Ru	TLS Client Profile	None	RADIUS Profile	None	File Transfer Profile	None	Signaling Manipulation Script	None
Flow Name	Remote-User-one-X																												
URI Group	*																												
User Agent	one-X Communicator																												
Source Subnet	*																												
Via Host	*																												
Contact Host	*																												
Signaling Interface	Sig_Outside_92																												
Topology Hiding Profile	None																												
Phone Interworking Profile	Avaya-Ru																												
TLS Client Profile	None																												
RADIUS Profile	None																												
File Transfer Profile	None																												
Signaling Manipulation Script	None																												
Profile <table border="1"> <tr><td>Source</td><td>Subscriber</td></tr> <tr><td colspan="2">Methods Allowed Before REGISTER</td></tr> <tr><td>User Agent</td><td>one-X Communicator</td></tr> <tr><td>Media Interface</td><td>Media_Outside_92</td></tr> <tr><td>End Point Policy Group</td><td>Remote_User</td></tr> <tr><td>Routing Profile</td><td>SessionMgr-TLS</td></tr> </table>				Source	Subscriber	Methods Allowed Before REGISTER		User Agent	one-X Communicator	Media Interface	Media_Outside_92	End Point Policy Group	Remote_User	Routing Profile	SessionMgr-TLS														
Source	Subscriber																												
Methods Allowed Before REGISTER																													
User Agent	one-X Communicator																												
Media Interface	Media_Outside_92																												
End Point Policy Group	Remote_User																												
Routing Profile	SessionMgr-TLS																												

The “Remote-User-Flare” flow will match traffic from remote Avaya Flare® devices set to use TCP. Note that the **User Agent** was set to “Flare” and that the **End Point Policy Group** was set to “Remote_User”.

View Flow: Remote-User-FlareX

Criteria

Flow Name	Remote-User-Flare
URI Group	*
User Agent	Flare
Source Subnet	*
Via Host	*
Contact Host	*
Signaling Interface	Sig_Outside_92

Optional Settings

Topology Hiding Profile	None
Phone Interworking Profile	Avaya-Ru
TLS Client Profile	None
RADIUS Profile	None
File Transfer Profile	None
Signaling Manipulation Script	None

Profile

Source	Subscriber
Methods Allowed Before REGISTER	
User Agent	Flare
Media Interface	Media_Outside_92
End Point Policy Group	Remote_User
Routing Profile	SessionMgr-TLS

The following screens show the **Server Flows** settings for Session Manager.

The screenshot shows the 'Session Border Controller for Enterprise' web interface. The top navigation bar includes 'Alarms', 'Incidents', 'Statistics', 'Logs', 'Diagnostics', 'Users', 'Settings', 'Help', and 'Log Out'. The main header displays 'Session Border Controller for Enterprise' and the 'AVAYA' logo. On the left, a sidebar menu lists various settings, with 'End Point Flows' highlighted in red. The main content area is titled 'End Point Flows: ASBCE' and features a tabbed interface with 'Subscriber Flows' and 'Server Flows'. The 'Server Flows' tab is active, showing a table of server configurations. A tooltip 'Hover over a row to see its description.' is visible. The table has columns for Priority, Flow Name, URI Group, Received Interface, Signaling Interface, End Point Policy Group, and Routing Profile. One row is listed with Priority 1, Flow Name 'SM6.3-Remote-Worker', URI Group '*', Received Interface 'Sig_Outside_92', Signaling Interface 'Sig_Inside_200', End Point Policy Group 'SM', and Routing Profile 'default'. Action links 'View', 'Clone', 'Edit', and 'Delete' are provided for each row. An 'Add' button is located in the top right corner of the table area.

Priority	Flow Name	URI Group	Received Interface	Signaling Interface	End Point Policy Group	Routing Profile
1	SM6.3-Remote-Worker	*	Sig_Outside_92	Sig_Inside_200	SM	default

The screenshot shows the 'Edit Flow: SM6.3-Remote-Worker' configuration window. It contains the following fields and values:

- Flow Name: SM6.3-Remote-Worker
- Server Configuration: SM6.3
- URI Group: *
- Transport: *
- Remote Subnet: *
- Received Interface: Sig_Outside_92
- Signaling Interface: Sig_Inside_200
- Media Interface: Media_Inside_200
- End Point Policy Group: SM
- Routing Profile: default
- Topology Hiding Profile: None
- File Transfer Profile: None

A 'Finish' button is located at the bottom of the window.

In the sample configuration, the internal IP address of the Avaya SBCE used for Remote Worker was added to Session Manager's SIP Firewall Whitelist and PPM limiting was disabled.

To add an IP address to the Whitelist, log into System Manager and navigate to **Session Manager → Network Configuration → SIP Firewall**. Select the Session Manager listed in the top section and click **Edit SM Default**. Select the **Whitelist** tab towards the bottom of the screen and click **New**. Enter the internal IP address of Avaya SBCE used for Remote Workers in the **Value** field and "255.255.255.255" in the **Mask** field. Click **Apply As Current** to save the configuration.

Home / Elements / Session Manager / Network Configuration / SIP Firewall

Firewall Configuration

Load default or selected configuration into editor. Then apply editor as current or backup configuration on selected SM(s)

[Edit SM Default](#)
[Edit BSM Default](#)
[Edit Current](#)
[Edit Backup](#)
[Apply As Backup](#)
[Apply As Current](#)

1 Item | Refresh Filter: Enable

Name	Type	Description
ASM	SM	Session Manager

Select : All, None

Editing: ASM Current

[Rules](#)
[Blacklist](#)
[Whitelist](#)

Enabled: ☐

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

Key	Value	Mask
Remote IP Address	10.64.19.200	255.255.255.255

Select : All, None

To disable PPM limiting, navigate to **Session Manager → Session Manager Administration** in the left-hand navigation pane and click **View** (not shown). A screen such as the following is displayed.

AVAYA Avaya Aura® System Manager 6.3

Last Logged on at June 13, 2013 8:42 AM
[Help](#) | [About](#) | [Change Password](#) | [Log off admin](#)

Session Manager x Home

Home / Elements / Session Manager / Session Manager Administration

Edit Session Manager [Commit](#) [Cancel](#)

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

General

SIP Entity Name ASM

Description Session Manager

*Management Access Point Host Name/IP 10.80.150.226

*Direct Routing to Endpoints Enable

VMware Virtual Machine ☐

Scroll down to the **Personal Profile manager (PPM) – Connection Settings**. Uncheck **Limited PPM Client Connections** and **PPM Packet Rate Limiting**.

Personal Profile Manager (PPM) - Connection Settings

Limited PPM Client Connection ☐

*Maximum Connection per PPM Client

PPM Packet Rate Limiting ☐

*PPM Packet Rate Limiting Threshold

The following screens show an Avaya one-X® Deskphone SIP Emulator illustrating the administration settings of a SIP endpoint used for Remote Worker. Note that the **HTTPS File Server** is set to the external IP address of the Avaya SBCE designated for firmware and configuration file transfers. Under **SIP Global Settings**, the **SIP Domain** is set to “avayalab.com”. The domain expected by Session Manager.

1:41pm 6/10/13

Address Procedures

Obtain network settings automatically

Use DHCP Yes

Phone: 192.168.0.101

Router: 192.168.0.1

Mask: 255.255.255.0

HTTPS File Server: 192.168.62.123

HTTP File Server:

Save Change Cancel

4:39pm 6/11/13

SIP Global Settings

Use <|> to change setting.

SIP Mode: Proxied

SIP Domain: avayalab.com

Avaya Environment: Auto

Reg. Policy alternate

Failback Policy auto

Avaya Config Server:

Save Change Cancel

Under **SIP Proxy Settings**, the **SIP Proxy Server** is set to the external IP address of Avaya SBCE designated for Remote Worker SIP traffic. The Transport Type and SIP Port should be set according to device type. For example, “TLS” and “5061” for one-X® Deskphones, and “TCP” and “5060” for one-X® Communicator and Flare® Experience.

1:42pm 6/10/13

SIP Proxy Settings

UDP or TCP or TLS.

SIP Proxy Server: 192.168.62.92

Transport Type: TLS

SIP Port: 5061

Save Change Cancel

©2014 Avaya Inc. All Rights Reserved.

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

Please e-mail any questions or comments pertaining to these Application Notes along with the full title name and filename, located in the lower right corner, directly to the Avaya DevConnect Program at devconnect@avaya.com.