



Avaya Solution & Interoperability Test Lab

Application Notes for Configuring SIP Trunking between 911 Enable's SIP Trunking Service with an Avaya IP Telephony Solution – Issue 1.1

Abstract

These Application Notes describe the steps to configure Session Initiation Protocol (SIP) Trunking between the 911 Enable SIP Trunking service and an Avaya IP Telephony solution. The Avaya solution consists of Avaya SIP Enablement Services, Avaya Communication Manager, and various Avaya SIP, H.323, digital and analog endpoints.

911 Enable offers an E911 call routing and location provisioning solution for enterprises using both legacy and IP phone deployments. The solution supports advanced IP-PBX features that impact E911 service such as shared line appearance, extension mobility, and off campus users. To support these features on Avaya equipment, calls are delivered using standard VoIP protocols such as SIP and RTP. The SIP interface between 911 Enable and the enterprise is based on the NENA i2 standard for VoIP emergency call routing. This standard provides strict guidelines for the routing of IP based 9-1-1 calls to Public Safety Answering Points (PSAPs).

911 Enable is a member of the Avaya Developer*Connection* Service Provider program. Information in these Application Notes has been obtained through Developer*Connection* compliance testing and additional technical discussions. Testing was conducted via the Developer*Connection* Program at the Avaya Solution and Interoperability Test Lab.

1. Introduction

These Application Notes describe the steps for configuring SIP (Session Initiation Protocol) trunking between the 911 Enable's SIP Trunking service and an Avaya IP telephony solution consisting of Avaya SIP Enablement Services, Avaya Communication Manager and various Avaya telephony endpoints. These endpoints included Avaya IP telephones (using SIP and H.323 protocols), traditional Avaya analog and digital Phones and Avaya IP softphone running on a Microsoft Windows PC.

By configuring the Avaya equipment for use with the 911 Enable service, enterprises can adopt a cost effective solution that will act as a PS-ALI replacement for their existing deployment of IP, digital and analog phones. Connectivity is provided through a direct SIP trunk to 911 Enable, and there is no need to maintain traditional hardwired 9-1-1 trunk lines (T1, ISDN).

When 9-1-1 is dialed, the call is routed to 911 Enable via a secure SIP trunk, and the precise location and callback number are provided directly on the PSAP dispatcher's screen. When 9-1-1 is dialed from phones without a direct number, 911 Enable temporarily binds a DID to the extension for a period of 48 hours using its patented Extension Bind™ technology. This allows a PSAP to call back the extension directly, bypassing the IVR or receptionist, in the event of a dropped 911 call.

On campus IP phones can be automatically tracked by 3rd party network asset management tools that upload phone locations to the 911 Enable databases.

Remote users with an Avaya softphone can update their locations from a webpage hosted on the corporate intranet. The corporate intranet page can be programmed to use SOAP/XML to update end user locations in real-time in the 911 Enable database.

911 Enable's Service offers the following capabilities:

- Outbound 9-1-1 emergency calling to the local PSAP with Extension-Bind™
- Incoming PSAP Call Back to the originating 9-1-1 endpoint with Extension-Bind™
- Delivery of location information to the PSAP for both enterprise and remote users

Figure 1 illustrates an example Avaya IP telephony solution connected to 911 Enable's SIP Trunking service. This is the configuration used during *DeveloperConnection* compliance testing process.

The Avaya IP telephony solution used to create a simulated customer site contained:

- Avaya S8710 Server with an Avaya G650 Media Gateway. The Avaya S8710 Server served as the host processor for Avaya Communication Manager.
- Avaya SIP Enablement Services (SES) software operating on an Avaya S8500B server platform.
- Avaya 4620 IP Telephone (configured to use either the SIP or H.323 protocol).
- Avaya 6416 Digital and Avaya 6210 Analog Telephones.

- Avaya 9640 One –X Deskphone IP Telephone (H.323 protocol only)

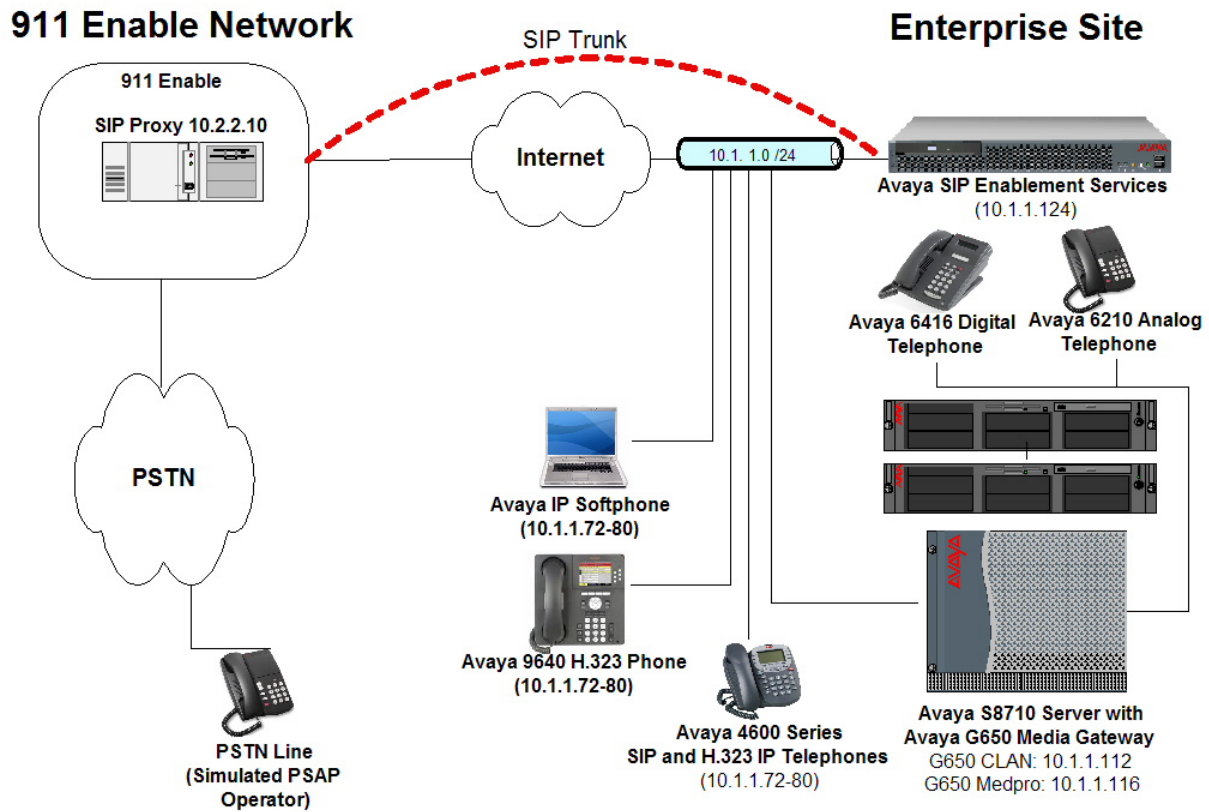


Figure 1: Avaya IP Telephony Network using 911 Enable SIP Trunking Service

1.1 Call Flows

To better understand how calls are routed using SIP trunks between the PSTN and the enterprise site shown in **Figure 1**, two call flows are described in this section. The first call scenario in **Figure 2** illustrates how 911 calls are routed from Avaya endpoints (SIP, IP, analog or digital) to the PSAP through 911 Enable.

1. An Avaya H.323, analog or digital telephone served by Avaya Communication Manager originates a 9-1-1.

- or -

1a. An Avaya SIP telephone originates a call that is routed via Avaya SES (as shown by the 1a arrow) to Avaya Communication Manager.

2. The call request is handled by Avaya Communication Manager where origination treatment such as class of service restrictions and automatic route selection is performed. Avaya Communication Manager selects the SIP trunk and sends the SIP signaling messages to Avaya SIP Enablement Services.

3. Avaya SIP Enablement Services routes the call to 911 Enable.

4. 911 Enable binds a DID to the incoming local extension number of the calling party and uses this DID for the Calling Party Number (CPN) to complete the call to the PSAP. This method is called Extension-Bind™ and it allows the PSAP operator to perform a callback in case the 9-1-1 call is dropped.

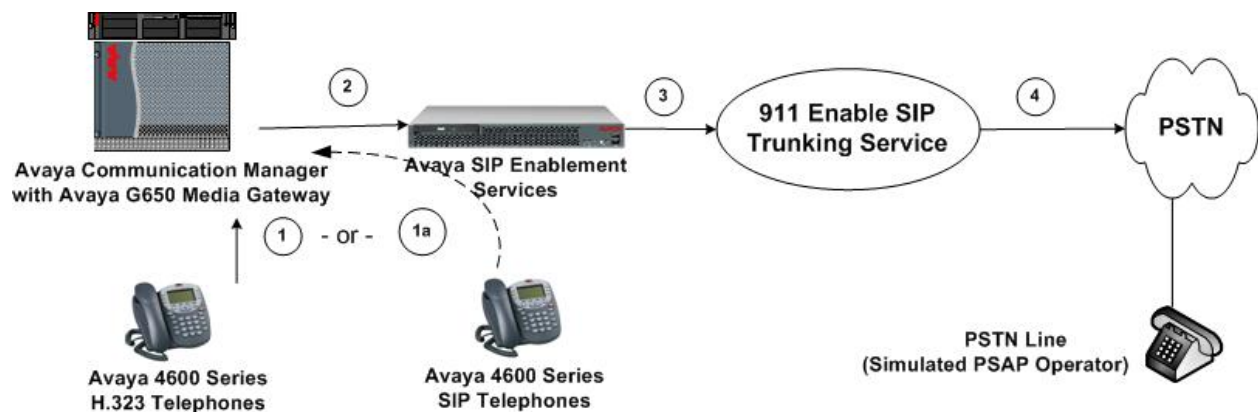


Figure 2: Outgoing 911 Call to local PSAP

Appendix A illustrates an example of a SIP INVITE message sent by 911 Enable for an incoming DID call.

The second call scenario illustrated in **Figure 3** is a PSAP call to the enterprise site terminating on a typical analog telephone supported by Avaya Communication Manager.

1. PSAP dispatcher initiates a callback by dialing the Callback Number (CBN) displayed on their screen. In this case the CBN is a direct inward dial (DID) number assigned by the 911 Enable Call Server, using Extension Bind, when the Avaya endpoint dialed 9-1-1. The call reaches 911 Enable, as the local provider, and is routed to the 911 Enable Call Server via a PSTN gateway.

2. Based on the extension number, 911 Enable routes the call to Avaya SES using SIP signaling messages sent over the converged access facility. Note that the assignment of the DID number and the local extension was previously created using Extension-Bind when the original 911 call was placed. In addition, the address of the Avaya SES server was previously established during the ordering and provisioning of the service.

3. Avaya SES routes the call to the Avaya S8710 Server running Avaya Communication Manager over a SIP trunk.

4. Avaya Communication Manager terminates the call to the directly connected analog phone as shown in step 4.

The same process occurs for calls to Avaya digital and H.323 IP phones.

- or -

4a. Inbound calls destined for a SIP extension at the enterprise are routed to Avaya Communication Manager which then transmits the appropriate SIP signaling via Avaya SES to the SIP telephone (as shown by the 4a arrow.)

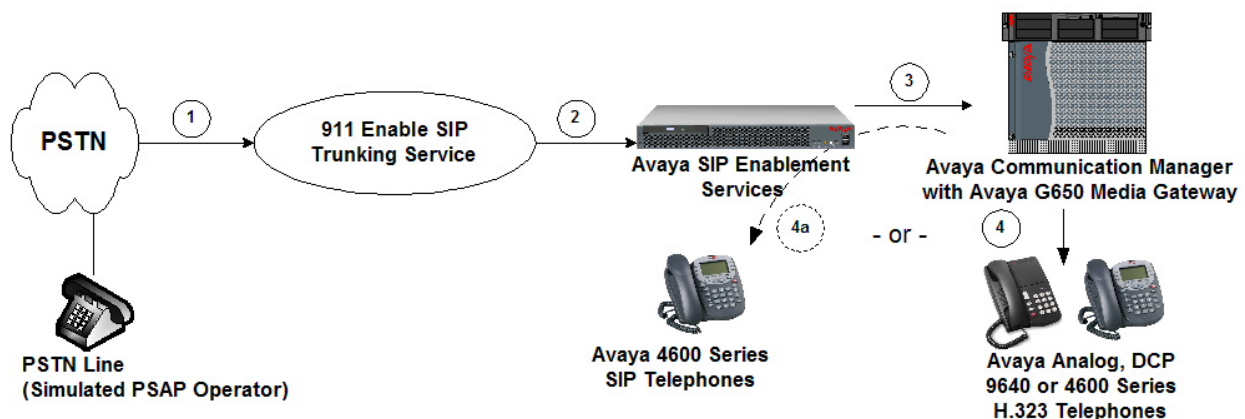


Figure 3: Incoming “Call Back” from local PSAP operator to local end point

2. Equipment and Software Validated

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

Avaya IP Telephony Solution Components	
Avaya S8710 Server with an Avaya G650 Media Gateway	Communication Manager 4.0 R014x.00.0.730.5 Update: 00.0.730.5 - 13566
Avaya SIP Enablement Services	SES-3.1.2.0-309.0
Avaya 4620 IP Telephone	R2.2.2 – SIP – s10d0b2.2.2.bin
Avaya 4610 IP Telephone	R2.8 – H.323 – a10d01b2_8.bin
Avaya 9640 IP Telephone	R S1.5 – ha96xxual_50.bin
Avaya IP Softphone	R6.0 Build 54
Avaya 6416 Digital Telephone	n/a
Avaya 6210 Analog Telephone	n/a
911 Enable SIP Trunking Service Components	
911 Enable	Sansay VSX V8.1.4

Table 1: Equipment and Software Tested

This solution is compatible with all other Avaya Server and Media Gateway platforms running similar versions of Avaya Communication Manager and Avaya SIP Enablement Services.

3. Configure Avaya Communication Manager

This section describes the steps for configuring a SIP trunk on Avaya Communication Manager. The SIP trunk is established between Avaya Communication Manager and Avaya SIP Enablement Services (SES) server. This trunk will carry the SIP signaling sent to 911 Enable's SIP Trunking service.

This SIP trunk also provides the trunking for SIP endpoint devices such as Avaya 4620 SIP telephone using Avaya Communication Manager in the recommended off-PBX stations (OPS) configuration. Avaya SIP telephones are configured as OPS stations on Avaya Communication Manager. OPS SIP stations register with Avaya SES but have calling privileges and features managed by Avaya Communication Manager. Avaya Communication Manager acts as a back-to-back SIP user agent when a SIP phone places or receives a call over a SIP trunk to a service provider.

Note the use of SIP endpoints is optional. The steps discussed in Sections 3.2 and 4.3 describing SIP endpoint administration may be omitted if SIP endpoints are not used. In the Avaya SIP architecture, the Avaya SES acts as a SIP proxy through which all incoming and outgoing SIP messages flow to 911 Enable. There is no direct SIP signaling path between 911 Enable and Avaya Communication Manager or Avaya SIP endpoints.

For incoming calls, the Avaya SES uses media server routing maps to direct the incoming SIP messages to the appropriate Avaya Communication Manager. Once the message arrives at the Avaya Communication Manager further incoming call treatment, such as incoming digit translations, class of service restrictions, etc. may be performed.

All outgoing calls to the 911 Enable network are processed within Avaya Communication Manager and may be first subject to outbound features such as automatic route selection, digit manipulation and class of service restrictions. Once Avaya Communication Manager selects a SIP trunk, the SIP signaling is routed to the Avaya SES. Within the Avaya SES, host address maps direct the outbound SIP messages to the 911 Enable SIP Proxy.

911 Enable is strictly a 911 Emergency Service Provider. Therefore, the dial plan for non-emergency calls such as 10-digit dialing for local and long-distance calls over the PSTN, Directory Assistance calls (411) and International calls (011+Country Code) are beyond the scope of this solution's configuration. Note: Avaya Communication Manager routes all emergency calls using Automatic Route Selection (ARS).

Avaya Communication Manager configuration was performed using the System Access Terminal (SAT). The general installation of the Avaya S8710 Server, Avaya G650 Media Gateway and circuit packs such as the C-LAN is presumed to have been previously completed and is not discussed here.

3.1 Sip Trunk Configuration

Step 1: Confirm Necessary Optional Features

Log into the Avaya Communication Manager's SAT interface and confirm that sufficient SIP trunk and Off PBX Telephone capacities are enabled. Use the **display system-parameters customer-options** command to determine the OFF-PBX Telephone capacities as shown in **Figure 4**. The license file installed on the system controls the maximum values for these attributes. If a required feature is not enabled or there is insufficient capacity, contact an authorized Avaya sales representative to add additional capacity.

display system-parameters customer-options		Page 1 of 10
OPTIONAL FEATURES		
G3 Version: V14		
Location: 1	RFA System ID (SID): 1	
Platform: 8	RFA Module ID (MID): 1	
		USED
	Platform Maximum Ports: 44000	229
	Maximum Stations: 36000	53
	Maximum XMOBILE Stations: 0	0
	Maximum Off-PBX Telephones - EC500: 10	0
	Maximum Off-PBX Telephones - OPS: 36000	23
	Maximum Off-PBX Telephones - SCCAN: 0	0
(NOTE: You must logoff & login to effect the permission changes.)		

Figure 4: System-Parameters Customer-Options Form – Page 1

On Page 2, verify that the number of **Maximum Administered SIP Trunks** supported by the system is sufficient for the combination of trunks to the 911 Enable network, SIP endpoints and any other SIP trunks used. Note that each SIP OPS telephone on a call with a SIP Service Provider uses two SIP trunks for the duration of the call.

display system-parameters customer-options		Page 2 of 10
OPTIONAL FEATURES		
IP PORT CAPACITIES		USED
Maximum Administered H.323 Trunks:	100	20
Maximum Concurrently Registered IP Stations:	100	1
Maximum Administered Remote Office Trunks:	0	0
Maximum Concurrently Registered Remote Office Stations:	0	0
Maximum Concurrently Registered IP eCons:	0	0
Max Concur Registered Unauthenticated H.323 Stations:	5	0
Maximum Video Capable H.323 Stations:	10	0
Maximum Video Capable IP Softphones:	10	0
Maximum Administered SIP Trunks:	200	156
Maximum Number of DS1 Boards with Echo Cancellation:	1	0
Maximum TN2501 VAL Boards:	1	1
Maximum G250/G350/G700 VAL Sources:	50	0
Maximum TN2602 Boards with 80 VoIP Channels:	2	1
Maximum TN2602 Boards with 320 VoIP Channels:	2	0
Maximum Number of Expanded Meet-me Conference Ports:	0	0
(NOTE: You must logoff & login to effect the permission changes.)		

Figure 5: System-Parameters Customer-Options Form – Page 2

Step 2: Assign Node Names

In the **IP Node Names** form, assign the node name and IP address for the Avaya SIP Enablement Server at the enterprise site as shown in **Figure 6**. In this case “SES” and “10.1.1.124” are being used, respectively. The SES node name will be used throughout the other configuration screens of Avaya Communication Manager.

In this example “CLAN” and “10.1.1.112” are the name and IP address assigned to the TN799DP Control-Lan card. The C-LAN entry was previously created during the installation of the system. Note, in smaller media gateways such as an Avaya G350, the Avaya Server S8300 processor address (procr) is used as the SIP signaling interface instead of the C-LAN interface.

change node-names ip		IP NODE NAMES		Page 1 of 1
Name	IP Address	Name	IP Address	
CLAN	10 .1 .1 .112		.	.
default	0 .0 .0 .0		.	.
ipsi	10 .1 .1 .109		.	.
medpro-hw11	10 .1 .1 .116		.	.
procr	10 .1 .1 .104		.	.
SES	10 .1 .1 .124		.	.
val1-tn250lap	10 .1 .1 .122		.	.
windowPC	10 .1 .1 .101		.	.
	.		.	.
	.		.	.
(8 of 8 administered node-names were displayed)				
Use 'list node-names' command to see all the administered node-names				
Use 'change node-names ip xxx' to change a node-name 'xxx' or add a node-name				

Figure 6: IP Nodes Names Form

Step 3: Define IP Network Region

The **IP Network Region** form specifies the parameters used by the SIP trunk group serving the Avaya SES server (used to reach 911 Enable and any optional SIP endpoints). Note that these parameters also apply to any other elements (such as H.323 phones, MedPro cards, etc.) also assigned to this region. Use the **change ip-network-region** form command to set the following values:

- The **Authoritative Domain** field is configured to match the domain name configured on the Avaya SES. In this configuration, the domain name is *east.devcon.com*. This field is required for endpoints to call the public network.
- By default, **IP-IP Direct Audio** (both **Intra** and **Inter Region**) is enabled to allow audio traffic to be sent directly between endpoints without using media resources such as the TN2302AP IP Media Processor (MedPro) card. In the case of 911 Enable, it is recommended that **IP-IP Direct Audio** be disabled for emergency calling. This feature can be supported by special request to 911 Enable. However, it is desirable for non-emergency calls to use the **IP-IP Direct Audio** feature and therefore the feature is enabled in the **IP Network Region** form by setting the field to **yes**. In order to prevent use of this feature for emergency calls, a dedicated signaling group will be used for emergency calls and the **IP-IP Direct Audio** feature will be disabled at this signaling group. This is documented in **Step 5** of this section.
- The **Codec Set** is set to the number of the IP codec set to be used for calls within the IP

network region. In this configuration, this codec set will apply to calls with 911 Enable as well as any IP telephone (H.323 or SIP) within the enterprise.

In this case, the SIP trunk is assigned to the same IP network region as the Avaya G650 Media Gateway, C-LAN and MedPro cards. If multiple network regions are used, Page 3 of each **IP Network Region** form must be used to specify the codec set for inter-region communications.

Note also that the **IP Network Region** form is used to set the QoS packet parameters that provides priority treatment for signaling and audio packets over other data traffic on 911 Enable's SIP Trunking service. These parameters may need to be aligned with the specific values provided by 911 Enable.

change ip-network-region 1		Page 1 of 19
IP NETWORK REGION		
Region: 1		
Location: 1	Authoritative Domain: east.devcon.com	
Name: Default System All		
MEDIA PARAMETERS		
Codec Set: 1	Intra-region IP-IP Direct Audio: yes	
UDP Port Min: 2048	Inter-region IP-IP Direct Audio: yes	
UDP Port Max: 3029	IP Audio Hairpinning? y	
DIFFSERV/TOS PARAMETERS		
Call Control PHB Value: 46	RTCP Reporting Enabled? y	
Audio PHB Value: 46	RTCP MONITOR SERVER PARAMETERS	
Video PHB Value: 26	Use Default Server Parameters? n	
802.1P/Q PARAMETERS		
Call Control 802.1p Priority: 6	Server IP Address: 10 .1 .1 .112	
Audio 802.1p Priority: 6	Server Port: 5005	
Video 802.1p Priority: 5	RTCP Report Period(secs): 5	
H.323 IP ENDPOINTS		
H.323 Link Bounce Recovery? y	AUDIO RESOURCE RESERVATION PARAMETERS	
Idle Traffic Interval (sec): 20	RSVP Enabled? n	
Keep-Alive Interval (sec): 5		
Keep-Alive Count: 5		

Figure 7: IP Network Region Form

Step 4: Define IP Codecs

Open the **IP Codec Set** form using the ip-codec value specified in the **IP Network Region** form (**Figure 7**) and enter the audio codec type to be used for calls routed over the SIP trunk. The settings of the **IP Codec Set** form are shown in **Figure 8**. Note that the **IP Codec Set** form may include multiple codecs listed in priority order to allow the codec for the call to be negotiated during call establishment. 911 Enable supports the G.711MU or G.711A codec only.

change ip-codec-set 1

Page1 of 2

IP Codec Set

Codec Set: 1

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

Figure 8: IP Codec Set Form

Step 5: Configure the Signaling Group

For interoperability with 911 Enable via SIP trunks, two signaling groups and corresponding trunk groups must be configured in order to handle both SIP and H.323 Avaya telephones as well as to ensure that the **Direct IP-IP Audio feature** is disabled for emergency calling. One signaling group will be dedicated to handle outbound and inbound emergency calls between 911 Enable's SIP trunking service and Avaya telephony end points. Avaya Digital, Analog and H.323 telephony end points will only need this first signaling group. Avaya SIP telephony end points will need this same signaling group plus a second additional signaling group. This is because Avaya SIP end points are configured as off-PBX stations (OPS). OPS stations register with Avaya SIP Enablement Services (SES) rather than with Avaya Communication Manager. Because of this, SIP end points need an additional signaling group that requires the **Far-end Domain** field to be set to the SIP domain of the SES. Therefore, the second signaling group will be used by Avaya SIP phones for OPS communication with the Avaya SES. The configuration steps below show how to configure this signaling group. Note: Additional signaling and trunk groups will need to be configured to handle non-emergency calls.

Configure the E911 **Signaling Group** form shown in **Figure 9** as follows using the **add signaling group** command:

- Set the **Group Type** field to *sip*.
- The **Transport Method** field will default to *tls* (Transport Layer Security). TLS is the only link protocol that is supported for SIP trunking with Avaya SIP Enablement Services
- **Near-end Node Name** Specify the Avaya Control-Lan card (node name "CLAN"). This field value is taken from the **IP Node Names** form shown in **Figure 6**. For smaller Server platforms, the near (local) end of the SIP signaling group may be the Avaya S8300 Server processor (procr) rather than the C-LAN.
- **Far-end Node Name** Specify the Avaya SIP Enablement Services (node name "SES"). This field value is taken from the **IP Node Names** form shown in **Figure 6**.
- Ensure that the recommended TLS port value of *5061* is configured in the **Near-end Listen Port** and the **Far-end Listen Port** fields.
- Enter the IP Network Region value assigned in the IP Network Region form (**Figure 7**). Note that if the **Far-end Network Region** field is different from the near-end network region, the preferred codec will be selected from the IP codec set assigned for the interregional connectivity for the pair of network regions. In this case, the same ip network region (Network Region 1) was used for local and emergency calls; however, different network regions can be used in the field.
- Enter the IP address of the 911 Enable SIP proxy server in the **Far-end Domain** field. In this configuration, the IP address is 10.2.2.10. This address is specified in the Uniform Resource Identifier (URI) of the SIP "To" address in the INVITE message for outbound calls. When handling inbound calls, it is also used by the Avaya SES to determine which SIP trunk to send a call over to Avaya Communication Manager. For example, if a 911 operator needs to call back an Avaya end point after the original emergency call was dropped, a SIP INVITE message will be passed to the Avaya SES with a "From" field URI address of 10.2.2.10. The SES will then look for a SIP signaling group that has the **Far-end Domain** field set to this address and then pass the

call over this trunk. This allows us to direct the call to a specific signaling group which has specific call settings, (such as **Direct IP-IP Audio** disabled in this case), required when the call is coming from a specific server. Mis-configuring this field may prevent calls from being successfully established to other SIP endpoints or to the local PSAP.

- The **Direct IP-IP Audio Connections** field is set to 'n' in this configuration. Because this signaling group will only be used for emergency calls to and from 911 Enable's service, this will disable the feature for calls using this signaling group only.
- The **DTMF over IP** field should remain set to the default value of *rtp-payload*. This value enables Avaya Communication Manager to send DTMF transmissions using RFC 2833. [8]
- The default values for the other fields may be used.

add signaling-group 1		Page 1 of 1
SIGNALING GROUP		
Group Number: 1	Group Type: sip Transport Method: tls	
Near-end Node Name: CLAN	Far-end Node Name: SES	
Near-end Listen Port: 5061	Far-end Listen Port: 5061	
	Far-end Network Region: 1	
Far-end Domain: 10.2.2.10		
	Bypass If IP Threshold Exceeded? n	
DTMF over IP: rtp-payload	Direct IP-IP Audio Connections? n	
	IP Audio Hairpinning? n	
Session Establishment Timer(min): 120		

Figure 9: E911 Signaling Group Form

Configure the OPS **Signaling Group**, (used by the SIP end points for OPS communication with the SES), following the same steps used above with two exceptions, enter the domain name used on the Avaya SES into the **Far-end Domain** field and set the **Direct IP-IP Audio Connections** field to “y” as shown in **Figure 10**. This will allow internal calls between Avaya SIP telephony end points as well as non-emergency calls to use this feature:

add signaling-group 2		Page 1 of 1
SIGNALING GROUP		
Group Number: 2	Group Type: sip Transport Method: tls	
Near-end Node Name: CLAN	Far-end Node Name: SES	
Near-end Listen Port: 5061	Far-end Listen Port: 5061	
	Far-end Network Region: 1	
Far-end Domain: east.devcon.com		
Bypass If IP Threshold Exceeded? n		
DTMF over IP: rtp-payload	Direct IP-IP Audio Connections? y	
	IP Audio Hairpinning? n	
Session Establishment Timer(min): 120		

Figure 10: OPS Signaling Group Form

Step 6: Configure the Trunk Groups

As described in **Step 5**, two trunks must also be configured. One trunk will be paired with the primary signaling group and the other with the secondary SIP end point signaling group.

Configure the E911 **Trunk Group** form as shown in **Figure 11** using the **add trunk-group** command. In this case the trunk group number chosen is 1. On Page 1 of this form:

- Set the **Group Type** field to *sip*.
- Choose a mnemonic **Group Name**.
- Specify an available trunk access code (TAC).
- Set the **Service Type** field to *tie*.
- Specify the signaling group associated with this trunk group in the **Signaling Group** field as previously specified in **Figure 9**.
- Specify the **Number of Members** supported by this SIP trunk group.

add trunk-group 1		Page 1 of 21	
TRUNK GROUP			
Group Number: 1	Group Type: sip	CDR Reports: y	
Group Name: E911 SIP	COR: 1	TN: 1	TAC: 101
Direction: two-way	Outgoing Display? n		
Dial Access? n		Night Service:	
Queue Length: 0			
Service Type: tie	Auth Code? n		
Signaling Group: 1			
Number of Members: 10			

Figure 11: Trunk Group Form (E911) – Page 1

On Page 3 of the **Trunk Group** form:

- set the **Numbering Format** field to *public*. This field specifies the format of the calling party number sent to the far-end.

change trunk-group 1		Page 3 of 21	
TRUNK FEATURES			
ACA Assignment? n	Measured: none	Maintenance Tests? y	
Numbering Format: public			
Prepend '+' to Calling Number? n			
Replace Unavailable Numbers? n			

Figure 12: Trunk Group Form (E911) – Page 3

Configure the OPS **Trunk Group** form as shown in **Figure 13** using the **add trunk-group** command. In this case the trunk group number chosen is 2. On Page 1 of this form:

- Set the **Group Type** field to *sip*.

- Choose a mnemonic **Group Name**.
- Specify an available trunk access code (**TAC**).
- Set the **Service Type** field to *tie*.
- Specify the *inbound* signaling group associated with this trunk group in the **Signaling Group** field as previously specified in **Figure 10**.
- Specify the **Number of Members** supported by this SIP trunk group.

add trunk-group 2		Page 1 of 21
TRUNK GROUP		
Group Number: 1	Group Type: sip	CDR Reports: y
Group Name: OPS SIP	COR: 1 TN: 1	TAC: 102
Direction: two-way	Outgoing Display? n	
Dial Access? n		Night Service:
Queue Length: 0		
Service Type: tie	Auth Code? n	
		Signaling Group: 2
		Number of Members: 10

Figure 13: Trunk Group Form (OPS) – Page 1

On Page 3 of the **Trunk Group** form:

- Set the **Numbering Format** field to *public*. This field specifies the format of the calling party number sent to the far-end.

change trunk-group 2		Page 3 of 21
TRUNK FEATURES		
ACA Assignment? n	Measured: none	Maintenance Tests? y
Numbering Format: public	Prepend '+' to Calling Number? n	
Replace Unavailable Numbers? n		

Figure 14: Trunk Group Form (OPS) – Page 3

Step 7: Configure Calling Party Number Information

Use the **change public-unknown-numbering** command to configure Avaya Communication Manager to send the calling party number, (CPN), to the far-end.

For 911 Enable's solution, there will be two calling party number formats used depending on the type of phone that is placing the emergency call. This solution supports Avaya analog, digital, IP hard phones (both H.323 and SIP), as well as Avaya IP Softphone.

For Avaya IP softphones, the CPN will consist of a prefix of "111" plus the 5 digit softphone station extension of the form 63xxx where x=[0-9]. In this test environment, all Avaya IP softphones use the extension space of 63xxx. This "111" prefix allows 911 Enable to immediately identify whether the station originating the emergency call is a softphone or a hard phone. In order to do this, the CPN will be set locally at the Avaya IP softphone emergency settings configuration interface as described in **Section 3.3.2**. In addition, it is important that no entry be made on the **public unknown numbering** form for any Avaya IP softphone using the dedicated emergency trunk. By leaving the form blank for the Avaya IP softphone, the CPN/Emergency Location Extension configured at the Avaya IP softphone interface will be allowed through. Please see **Section 6.2.2** for a detailed explanation.

For all Avaya analog, digital and IP hard phones, (both H.323 and SIP), the station's 5 digit extension will be used. In this case, entries on the public unknown numbering form are required. In this solution, all analog, digital and IP hard phones use the extension space of 60xxx, 61xxx or 62xxx. Therefore, all stations in this address space will send the calling party number 60xxx 61xxx or 62xxx when an outbound call uses SIP trunk group #1 (*this is the outbound trunk group specified in Step 6*). This calling party number will be sent to the far-end in the SIP "From" header.

Figure 15 shows the use of the **change public-unknown-numbering** command to implement this rule.

change public-unknown-numbering 0										Page	1	of	2
NUMBERING - PUBLIC/UNKNOWN FORMAT													
Total										Total			
Ext	Ext	Trk	CPN				CPN	Ext	Ext	Trk	CPN		
Len	Code	Grp(s)	Prefix	Len	Len	Code	Grp(s)	Prefix	Len	CPN			
5	60	1		5									
5	61	1		5									
5	62	1		5									

Figure 15: Numbering Public/Unknown Format Form

Step 8: Automatic Route Selection for Outbound Calls

In these Application Notes, the Automatic Route Selection (ARS) feature will be used to route outbound calls via the SIP trunk to the 911 Enable SIP Trunking service to a PSAP destination.

Use the **change dialplan analysis** command to add **9** as a feature access code (**fac**).

change dialplan analysis								
DIAL PLAN ANALYSIS TABLE								
Percent Full: 3								
Dialed	Total	Call	Dialed	Total	Call	Dialed	Total	Call
String	Length	Type	String	Length	Type	String	Length	Type
1	3	dac						
7	4	ext						
8	4	ext						
9	1	fac						
*	3	fac						
#	3	fac						

Figure 16: Change Dialplan Analysis Form

Use the **change feature-access-codes** command to specify **9** as the access code for outside dialing.

change feature-access-codes		Page 1 of 7
FEATURE ACCESS CODE (FAC)		
Abbreviated Dialing List1 Access Code:		
Abbreviated Dialing List2 Access Code:		
Abbreviated Dialing List3 Access Code:		
Abbreviated Dial - Prgm Group List Access Code:		
Announcement Access Code: *03		
Answer Back Access Code:		
Attendant Access Code:		
Auto Alternate Routing (AAR) Access Code:		
Auto Route Selection (ARS) - Access Code 1: 9		Access Code 2:
Automatic Callback Activation:		Deactivation:
Call Forwarding Activation Busy/DA: *10 All: *11		Deactivation: #10
Call Park Access Code:		
Call Pickup Access Code:		
CAS Remote Hold/Answer Hold-Unhold Access Code:		
CDR Account Code Access Code:		
Change COR Access Code:		
Change Coverage Access Code:		
Contact Closure Open Code:		Close Code:
Contact Closure Pulse Code:		

Figure 17: Feature Access Codes Form

Use the **change ars analysis** command to configure the route pattern selection rule based upon the number dialed following the dialed digit “9”. In this sample configuration, the emergency number dialed is in the form “911”. Since “9” activates ARS, we only need to add an entry for **11** in the ARS Digit Analysis Table and classify the Call Type as **emer** (emergency). The call is to be routed to a route pattern which re-appends the digit “9” back onto the “11” string and sends the call to the SIP trunk groups used for 911 Enable. An Entry for “9911” can also be added to handle the case where a user aware of the ARS FAC code of “9” dials the additional “9”. Note that further administration of ARS is beyond the scope of these Application Notes but discussed in References [1] and [2].

change ars analysis 173						Page 1 of 2		
ARS DIGIT ANALYSIS TABLE								
Location: all					Percent Full: 3			
Dialed		Total		Route		Call	Node	ANI
String		Min	Max	Pattern	Type	Num	Reqd	
11		2	2	1	emer		n	

Figure 18: ARS Analysis Form

Use the **change route-pattern** command to define the SIP trunk group included in the route pattern that ARS selects. In this configuration, route pattern 1 will be used to route calls to trunk group 1 (the SIP trunk created in **Step 6, Figure 11**). Set the following parameters:

- **Grp No:** The Trunk Group created in **Step 6, Figure 11**
- **Inserted Digits:** Enter the digit “9” to add it back to the dialed string after it had been removed by ARS. This ensures that string “911” is sent to 911 Enable.

change route-pattern 1												
Pattern Number: 1 Pattern Name: To PSTN												
SCCAN? n Secure SIP? n												
Grp			FRL	NPA	Pfx	Hop	Toll	No.	Inserted		DCS/	IXC
No					Mrk	Lmt	List	Del	Digits		QSIG	
									Dgts		Intw	
1:			1	0		.			9		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 3 4 W		Request					Dgts Format		
							Subaddress					
1:			y y y y y n	n		rest					none	
2:			y y y y y n	n		rest					none	
3:			y y y y y n	n		rest					none	
4:			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	

Figure 19: Route Pattern Form

Step 9: Configure Incoming Digit Translation

This step configures the settings necessary to map incoming Emergency calls from a 911 operator who needs to call back an extension that had previously placed an emergency call.

With 911 Enable's Extension Bind feature, local telephones without a direct number placing a 911 call have a DID assigned to them before they are passed to the local PSAP. This allows the local PSAP to use this DID in case the call drops and they need to call the telephone back. When a 911 operator calls back the originating telephone, the DID is then stripped by 911 Enable and replaced with the local station extension.

In this test environment, Avaya analog, digital and IP hard phones pass their local extension as the CPN to 911 Enable. When a call is placed back from a 911 operator, that same CPN/extension is passed back in the INVITE message from 911 Enable. Therefore, no digit manipulation is necessary in order to route calls to the appropriate extension and no entry is needed in the **Incoming Call Handling Treatment** form.

However, as stated in step **Step 7: Configure Calling Party Number Information**, Avaya IP softphones are using a special prefix of "111" plus the local extension as the CPN when placing emergency calls. This same CPN will be passed back in the INVITE message from 911 Enable. The "111" prefix must be stripped in order to route the call back to the proper local extension on Avaya Communication Manager.

The incoming CPN for IP softphones is [11163xxx] where x=[0-9]. These do not have a direct correlation to the internal extensions assigned to Avaya IP softphones within Avaya Communication Manager. Thus, the "111" prefix is deleted from the incoming CPN digits leaving the local assigned extension number.

To remove "111" from the extension number for incoming CPN's of the form **11163xxx**, configure as shown in **Figure 20**:

- Open the **Incoming Call Handling Treatment** form for the *E911* SIP trunk group configured in **Step6 Figure 11**, in this case Trunk Group 1.
- Enter **8** into the **Called Len** field and **3** into the **Del** field. Enter **11163** into the **Called Number** field. Note that the Called Number entry in this case represents the common matching portion applicable to all incoming Avaya IP softphone numbers. Leave the **Insert** field blank so that the remaining 5 digit local extension is used to route the call.

change inc-call-handling-trmt		trunk-group 1		Page 1 of 30	
INCOMING CALL HANDLING TREATMENT					
Service/ Feature tie	Called Len 8	Called Number 11163	Del 3	Insert	

Figure 20: Incoming Call Handling Treatment – Extension Mapping

Step 10: Save Avaya Communication Manager Changes

Enter “save translation” to make the changes permanent.

3.2 SIP Endpoint Configuration

This section describes the administration of SIP telephones and requires the preceding SIP Trunk configuration to have been completed. SIP telephones are optional and not required to use the 911 Enable SIP Trunking Service.

Step 1: Assign a Station

The first step in adding an off-PBX station (OPS) for Avaya SIP telephones registered with Avaya SIP Enablement Services is to assign a station as shown in **Figure 21**.

Using the **add station** command from the SAT:

- Leave the station **Type** at the default “6408D+” value. (Note this is the Avaya recommended best practice that will prevent an alarm warning that occurs when 4600 series phone models are entered).
- Enter “X” in the **Port** field to indicate station administration without port hardware.
- Enter a **Name** for the station that will be displayed.
- The **Security Code** is left blank for SIP OPS extensions.

The remaining fields are configured per normal station administration that is beyond the scope of these Application Notes. Note that the Class of Restrictions (**COR**) and Class of Service (**COS**) will govern the features and call restrictions that apply to this station.

add station 60000		Page 1 of 4
STATION		
Extension: 60000	Lock Messages? n	BCC: 0
Type: 6408D+	Security Code:	TN: 1
Port: X	Coverage Path 1:	COR: 1
Name: SipCM Phone60000	Coverage Path 2:	COS: 1
	Hunt-to Station:	
STATION OPTIONS		
Loss Group: 2	Personalized Ringing Pattern: 1	
Data Module? n	Message Lamp Ext: 60000	
Speakerphone: 2-way	Mute Button Enabled? y	
Display Language: english		
	Media Complex Ext:	
	IP SoftPhone? n	

Figure 21: Station Administration – Page 1

On Page 2 of the **Station** form,

- Set the **Restrict Last Appearance** value to 'n' on phones that have 3 or fewer call appearances to maintain proper SIP conference and transfer operation. Setting the **Restrict Last Appearance** value to 'y' reserves the last call appearance for outbound calls. Certain SIP conference and transfer features will not function properly if a third appearance is not available for incoming calls.

add station 60000		Page 2 of 4
STATION		
FEATURE OPTIONS		
LWC Reception: spe	Auto Select Any Idle Appearance? n	
LWC Activation? y	Coverage Msg Retrieval? y	
LWC Log External Calls? n	Auto Answer: none	
CDR Privacy? n	Data Restriction? n	
Redirect Notification? y	Idle Appearance Preference? n	
Per Button Ring Control? n	Bridged Idle Line Preference? n	
Bridged Call Alerting? n	Restrict Last Appearance? n	
Active Station Ringing: single	Conf/Trans on Primary Appearance? n	
H.320 Conversion? n	Per Station CPN - Send Calling Number? y	
Service Link Mode: as-needed		
Multimedia Mode: basic		
AUDIX Name:	Display Client Redirection? n	
	Select Last Used Appearance? n	
	Coverage After Forwarding? s	
	Multimedia Early Answer? n	
	Direct IP-IP Audio Connections? y	
Emergency Location Ext: 60000	IP Audio Hairpinning? n	

Figure 22: Station Administration – Page 2

On Page 3 of the **Station** form, configure at least 3 call appearances under the Button Assignments section for the SIP telephone as shown in **Figure 23**.

add station 60000		Page 3 of 4	
STATION			
SITE DATA			
Room:		Headset?	n
Jack:		Speaker?	n
Cable:		Mounting:	d
Floor:		Cord Length:	0
Building:		Set Color:	
ABBREVIATED DIALING			
List1:	List2:	List3:	
BUTTON ASSIGNMENTS			
1: call-appr	5:		
2: call-appr	6:		
3: call-appr	7:		
4:	8:		

Figure 23: Station Administration – Page 3

A similar number of call appearances should be configured on the SIP Telephone which is beyond the scope of these Application Notes. The parameters to administer call appearances (and many other settings) are described in Reference [6].

Step 2: Configure Off-PBX Station Mapping

Configure the **Off-PBX Telephone** form so that calls destined for a SIP telephone at the enterprise site are routed to Avaya SIP Enablement Services, which will then route the call to the SIP telephone.

On the **Off-PBX-Telephone Station-Mapping** form shown in **Figure 24**:

- Specify the **Station Extension** of the SIP endpoint.
- Set the **Application** field to *OPS*.
- Set the **Phone Number** field to the digits to be sent over the SIP trunk. In this case, the SIP telephone extensions configured on Avaya SIP Enablement Services also match the extensions of the corresponding AWOH (Administration Without Hardware) stations on Avaya Communication Manager. However, this is not a requirement.
- Set the **Trunk Selection** field to 2, which is the number assigned to the *inbound* SIP trunk group used to route the call to the SIP station. This trunk group number was previously defined in **Step 6 Figure 13**.
- Set the **Configuration Set** value. In these Application Notes, Configuration Set 1 uses the default values of the Configuration Set form.

change off-pbx-telephone station-mapping 60000					Page 1 of 2
STATIONS WITH OFF-PBX TELEPHONE INTEGRATION					
Station Extension	Application	Dial Prefix	Phone Number	Trunk Selection	Configuration Set
60000	OPS	-	60000	2	1

Figure 24: Stations with Off-PBX Telephone Integration – Page 1

On Page 2, set the **Call Limit** field to the maximum number of calls that may be active simultaneously at the station. In this example, the call limit is set to '3', which corresponds to the number of call appearances configured on the station form. Accept the default values for the other fields.

change off-pbx-telephone station-mapping 60000					Page 2 of 2
STATIONS WITH OFF-PBX TELEPHONE INTEGRATION					
Station Extension	Call Limit	Mapping Mode	Calls Allowed	Bridged Calls	
60000	3	both	all	both	

Figure 25: Stations with Off-PBX Telephone Integration – Page 2

Step 3: Repeat for each SIP Phone

Repeat Steps 1 and 2 for each SIP phone to be added.

Step 4: Save Avaya Communication Manager Changes

Enter "save translation" to make the changes permanent.

3.3 Emergency Location Extension Configuration

This section covers the configuration necessary to set the Emergency Location Extension for the 911 Enable solution. The Emergency Location Extension is the CPN used when an emergency call is placed from that station. The system default for this parameter is the local station extension. As discussed previously, this solution requires that:

- Avaya Analog, Digital and IP hard phones send their local 5 digit extension as the Emergency Location Extension i.e. the default setting
- Avaya IP softphones send a prefix of “111” plus their local 5 digit extension as the Emergency Location Extension

3.3.1 Avaya Analog, Digital and Hard IP Phone

For new and or existing Avaya analog and digital stations, confirm on page 2 of the **station** form that the **Emergency Location Extension** field is equal to the station’s extension as shown in **Figure 26**.

change station 62000		Page 2 of 4
STATION		
FEATURE OPTIONS		
LWC Reception: spe		Coverage Msg Retrieval? y
LWC Activation? y		Auto Answer: none
LWC Log External Calls? n		Data Restriction? n
CDR Privacy? n		Call Waiting Indication: y
Redirect Notification? y		Att. Call Waiting Indication: y
Per Button Ring Control? n		Distinctive Audible Alert? y
Bridged Call Alerting? n		Adjunct Supervision? y
Switchhook Flash? y		
Ignore Rotary Digits? n		
H.320 Conversion? n	Per Station CPN - Send Calling Number?	
Service Link Mode: as-needed		
Multimedia Mode: basic		
AUDIX Name:		Coverage After Forwarding? s
		Multimedia Early Answer? n
		Direct IP-IP Audio Connections? y
		IP Audio Hairpinning? n
Emergency Location Ext: 62000		

Figure 26: Analog Station form Emergency Location Extension

For Avaya IP hard phones, confirm on page 2 of the **station** form that the **Emergency Location Extension** field is equal to the station's extension. In addition, set the **Always Use** field to **y** so that the Emergency Location Extension cannot be overridden by the **IP Network Map** form as shown in **Figure 27**.

change station 60001		Page 2 of 5	
FEATURE OPTIONS		STATION	
LWC Reception: spe		Auto Select Any Idle Appearance? n	
LWC Activation? y		Coverage Msg Retrieval? y	
LWC Log External Calls? n		Auto Answer: none	
CDR Privacy? n		Data Restriction? n	
Redirect Notification? y		Idle Appearance Preference? n	
Per Button Ring Control? n		Bridged Idle Line Preference? n	
Bridged Call Alerting? n		Restrict Last Appearance? n	
Active Station Ringing: single			
		EMU Login Allowed? n	
H.320 Conversion? n		Per Station CPN - Send Calling Number? n	
Service Link Mode: as-needed			
Multimedia Mode: enhanced			
AUDIX Name:		Display Client Redirection? n	
		Select Last Used Appearance? n	
		Coverage After Forwarding? s	
		Multimedia Early Answer? n	
		Direct IP-IP Audio Connections? y	
Emergency Location Ext: 60001		Always Use? y	IP Audio Hairpinning? n

Figure 27: IP Hard Phone Station form Emergency Location Extension

3.3.2 Avaya IP Softphone

As described in **Section 3.1 step 7**, the Emergency Location Extension is set at the Avaya IP softphone interface. In order for the softphone to set this parameter, the station form of Avaya Communication Manager for the softphone must be set properly to allow this to work.

Step 1: Configure the Softphone Station Form on Avaya Communication Manager

On the station form for the softphone, there is an additional field on page 2 called **Remote Softphone Emergency Calls**. (Note: This field appears when the **IP Softphone** field is set to **y** on page 1 of the station form.) Set this field to **CESID, (Caller's Emergency Service Identification)**, as shown in **Figure 28** below. This setting allows the softphone to tell Avaya Communication what number to use as the Emergency Location Extension. Also make sure that the **Always Use** field is set to **n**.

change station 63005		Page 2 of 5
STATION		
FEATURE OPTIONS		
LWC Reception: spe	Auto Select Any Idle Appearance? n	
LWC Activation? y	Coverage Msg Retrieval? y	
LWC Log External Calls? n	Auto Answer: none	
CDR Privacy? n	Data Restriction? n	
Redirect Notification? y	Idle Appearance Preference? n	
Per Button Ring Control? n	Bridged Idle Line Preference? n	
Bridged Call Alerting? n	Restrict Last Appearance? y	
Active Station Ringing: single		
H.320 Conversion? n	Per Station CPN - Send Calling Number?	
Service Link Mode: as-needed		
Multimedia Mode: enhanced		
AUDIX Name:	Display Client Redirection? n	
	Select Last Used Appearance? n	
	Coverage After Forwarding? s	
	Multimedia Early Answer? n	
Remote Softphone Emergency Calls: cesid	Direct IP-IP Audio Connections? y	
Emergency Location Ext: 63005	Always Use? n IP Audio Hairpinning? n	

Figure 28: Avaya IP Softphone Station Form

Step 2: Configure the Emergency Location Extension at the IP Softphone Interface

Start the Avaya IP Softphone application and open the **Login Settings** window from the **Settings** menu as shown in **Figure 29**.

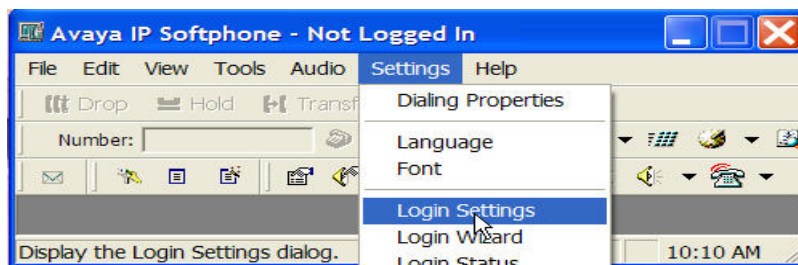


Figure 29: Opening the Login Settings Window

In the **Login Settings** window, go to the **Emergency** tab shown in **Figure 30** below. In the **Emergency** tab, enable the **Enable Emergency Call Handling** feature. Select the **Telephone**

number button and enter the prefix **111** followed by the IP Softphone station extension, in this example the full entry is **11163005**.

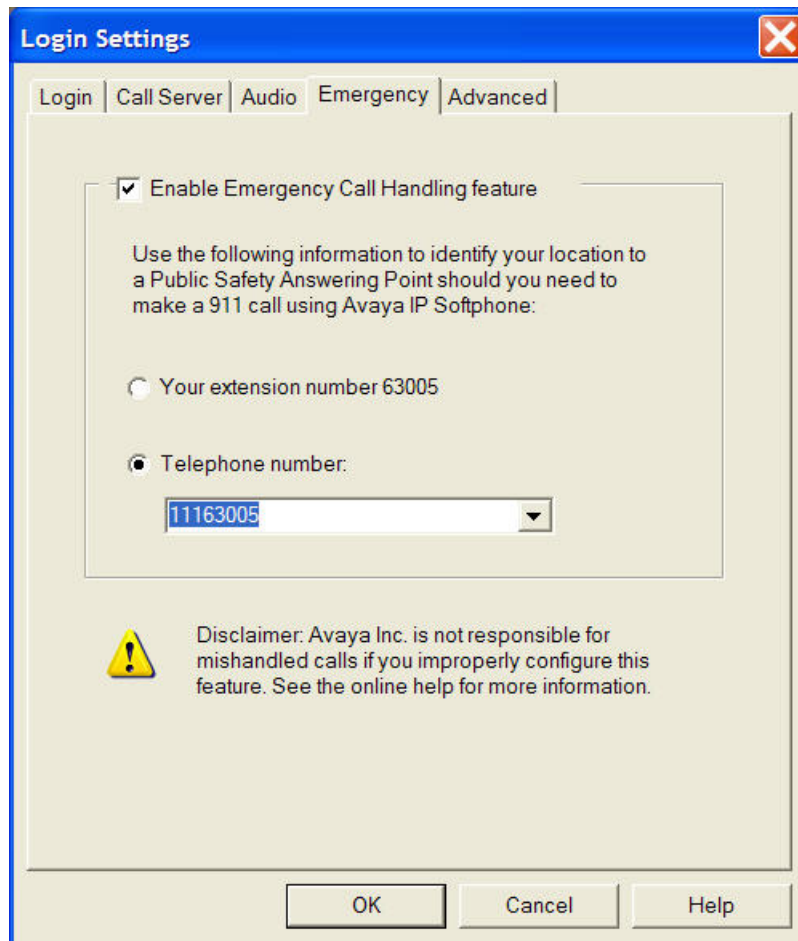


Figure 30: Avaya IP Softphone Emergency Tab

4. Configure Avaya SIP Enablement Services

This section covers the administration of Avaya SIP Enablement Services (SES). Avaya SES is configured via an internet browser using the Administration web interface. It is assumed that Avaya SES software and the license file have already been installed on the Avaya SES. During the software installation, the **initial_setup** script is run on the Linux shell of the server to specify the IP network properties of the server along with other parameters. For additional information on these installation tasks, refer to [4].

This section is divided into two parts: **Section 4.1** provides the steps necessary to configure a SIP trunk to 911 Enable's SIP Trunking service. **Section 4.2** provides the steps necessary to complete the administration for optional SIP endpoints.

4.1 SIP Trunking to 911 Enable

Step 1: Log into Avaya SIP Enablement Services

Access the SES Administration web interface, by entering **http://<ip-addr>/admin** as the URL in an Internet browser, where *<ip-addr>* is the IP address of Avaya SES server.

Log in with the appropriate credentials and then select the *Launch Administration Web Interface* link from the main screen as shown in **Figure 31**.

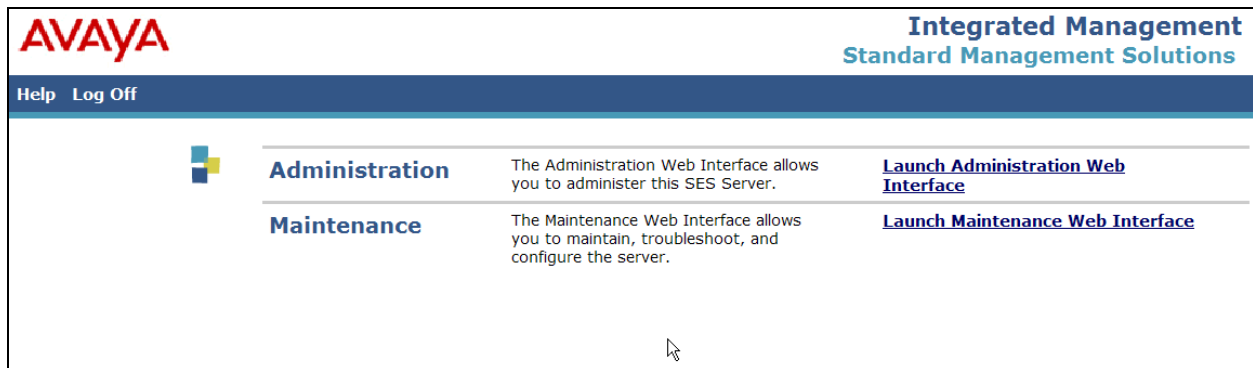


Figure 31 - Avaya SES Main Screen

The Avaya SES administration home screen shown in **Figure 32** will be displayed.

AVAYA Integrated Management SIP Server Management

Help Exit Server: 10.1.1.124

Top

- Users
- Conferences
- Media Server Extensions
- Emergency Contacts
- Hosts
- Media Servers
- Adjunct Systems
- Services
- Server Configuration
- Web Certificate Management
- IM Logs
- Trace Logger
- Export/Import to ProVision

Top	
Manage Users	Add and delete Users.
Manage Conferencing	Add and delete Conference Extensions.
Manage Media Server Extensions	Add and delete Media Server Extensions.
Manage Emergency Contacts	Add and delete Emergency Contacts.
Manage Hosts	Add and delete Hosts.
Manage Media Servers	Add and delete Media Servers.
Manage Adjunct Systems	Add and delete Adjunct Systems.
Manage Services	Start and stop server processes on this host.
Server Configuration	Edit Properties of the system.
Certificate Management	Manage Web Certificate.
IM Logs	Download IM Logs.
Trace Logger	Manage SIP Trace Logs.
Export Import to ProVision	Export and import data using ProVision on this host.

© 2006 Avaya Inc. All Rights Reserved.

Figure 32: Avaya SES Administration Home Page

Step 2: Verify System Properties

From the left pane of the Administration web interface, expand the **Server Configuration** option and select **System Properties**. This screen displays the Avaya SES version and the network properties entered via the **initial_setup** script during the installation process.

In the **System Properties** screen:

- Verify the **SIP Domain** name assigned to Avaya SES.
- Verify the **License Host** field. This is the host name, the fully qualified domain name, or the IP address of the Avaya SES that is running the WebLM application and has the associated license file installed. This entry should be set to **localhost** unless the WebLM server is not co-resident with this server.
- If changes were necessary in the **System Properties** screen, click the **Update** button.

The screenshot shows the 'Edit System Properties' interface. On the left is a navigation tree with 'Server Configuration' expanded to 'System Properties'. The main area contains the following fields:

SES Version	SES-3.1.0.0-018.0
System Configuration	simplex
Host Type	home/edge
SIP Domain*	<input type="text" value="east.devcon.com"/>

Note that the DNS domain is: east.devcon.com

If you are unsure about this field, most often the SIP domain should be the root level DNS domain. For example, for a DNS domain of eastcoast.example.com, the SIP domain would likely be configured to example.com. This allows SIP calls and instant messages to users with handles of the format handle@example.com

License Host*	<input type="text" value="localhost"/>
---------------	--

Network Properties

Local IP	10.1.1.124
Local Name	ses_eh.east.devcon.com
Logical IP	10.1.1.124
Logical Name	ses_eh.east.devcon.com
Gateway IP Address	10.1.1.97

Redundant Properties

Management Device	SAMP
-------------------	------

Fields marked * are required.

Update

Figure 33: System Properties

Step 3: Verify the Avaya SES Host Information

Verify the Avaya SES Host information using the **Edit Host** page. In these Application Notes the Avaya SES **Host Type** is a combined *home/edge*. This means that both the 911 Enable SIP Trunking Service and Avaya Communication Manager are contacting the same SES.

Display the **Edit Host** page (**Figure 34**) by following the **Hosts** link in the left navigation pane and then clicking on the **Edit** option under the **Commands** section of the **List Hosts** screen.

On the **Edit Host** screen:

- Verify that the IP address of this combined SES Home/Edge server is in the **Host IP Address** field.
- Do not modify the **DB Password** or **Profile Service Password** fields. If these fields are changed, exit the form without using the **Update** button. These values must match the values entered during the SES installation; incorrect changes may disable the SES.
- Verify that the **UDP**, **TCP** and **TLS** checkboxes are enabled as **Listen Protocols**.
- Verify that **TLS** is selected as the **Link Protocol**.
- Default values for the remaining fields may be used.
- Click the **Update** button only if changes are necessary. Otherwise exit the **Edit Host** page by selecting the **Top** link on the left navigation bar.

AVAYA

Integrated Management
SIP Server Management

Help Exit

Server: 10.1.1.124

Top

Users

Conferences

Media Server Extensions

Emergency Contacts

Hosts

List

Migrate Home/Edge

Media Servers

Adjunct Systems

Services

Server Configuration

System Properties

Admin Accounts

License

IM Log Settings

SNMP Configuration

Web Certificate Management

IM Logs

Trace Logger

Export/Import to ProVision

Edit Host

Host IP Address*

10.1.1.124

DB Password

.....

Profile Service Password

.....

Host Type

home/edge

Parent

none

Listen Protocols

☒UDP
☒TCP
☒TLS

Link Protocols

☐UDP
☐TCP
☒TLS

Presence

☐Allow All
☒Deny All

Access Policy (Default)

☒Allow
☐Deny

Emergency Contacts Policy

☒Allow
☐Deny

Minimum Registration (seconds)

300

Registration Expiration Timer (seconds)*

86400

Line Reservation Timer (seconds)*

30

Outbound Routing

☒Internal
☒External

Allowed From

OutboundProxy

Port

☐UDP
☐TCP
☐TLS

Outbound Direct Domains

Default Ringer Volume*

5

Default Ringer Cadence*

2

Default Receiver Volume*

5

Default Speaker Volume*

5

VMM Server Address

VMM Server Port

5005

VMM Report Period

5

Fields marked * are required.

Update

© 2006 Avaya Inc. All Rights Reserved.

Figure 34: Edit Host

Step 4: Add Avaya Communication Manager as Media Server

Under the **Media Servers** option in the Administration web interface, select **Add** to add the Avaya Media Server in the enterprise site. This will create the Avaya SES side of the SIP trunk previously created in Avaya Communication Manager.

In the **Add Media Server** screen, enter the following information:

- A descriptive name in the **Media Server Interface** field (e.g., S8710-SignalGroup1). Select IP address of the home SES server in the **Host** field as specified in **Step 3 Figure 34**.
- Select *TLS* (Transport Link Security) for the **Link Type**. TLS provides encryption at the transport layer. TLS is the only link protocol that is supported for SIP trunking with Avaya Communication Manager.
- Enter the IP address of the C-LAN board in the **SIP Trunk IP Address** field. (Note: This may be the IP address of the media server processor in smaller Avaya Communication Manager configurations such as an Avaya S8300 Server using an Avaya G350 Media Gateway.)
- After completing the **Add Media Server** screen, click on the **Add** button.

The screenshot displays the Avaya Integrated Management SIP Server Management web interface. The top header shows the Avaya logo and the title 'Integrated Management SIP Server Management' with a server IP of 10.1.1.124. A left-hand navigation menu lists various system management options. The main content area is titled 'Add Media Server Interface' and contains the following fields and options:

- Media Server Interface Name***: Text input field containing 'SP8710-SignalGroup1'.
- Host**: Dropdown menu showing '10.1.1.124'.
- SIP Trunk** section:
 - SIP Trunk Link Type**: Radio buttons for TCP and TLS, with TLS selected.
 - SIP Trunk IP Address***: Text input field containing '10.1.1.112'.
- Media Server** section:
 - Media Server Admin Address** (see Help): Text input field.
 - Media Server Admin Login**: Text input field.
 - Media Server Admin Password**: Text input field.
 - Media Server Admin Password Confirm**: Text input field.

Below these fields, a note states 'Fields marked * are required.' and an **Add** button is located at the bottom left of the form area. The **Add** button is circled in red in the original image.

© 2006 Avaya Inc. All Rights Reserved.

Figure 35: Add Media Server

Step 5: Specify Address Maps to Media Servers

Incoming calls arriving at Avaya SES are routed to the appropriate Avaya Communication Manager for termination services. This routing is specified in a Media Server Address Map configured on Avaya SES.

This routing compares the Uniform Resource Identifier (URI) of an incoming INVITE message to the pattern configured in the Media Server Address Map, and if there is a match, the call is routed to the designated Avaya Communication Manager. The URI usually takes the form of *sip:user@domain*, where *domain* can be a domain name or an IP address. Patterns must be specific enough to uniquely route incoming calls to the proper destination if there are multiple Avaya Communication Manager systems supported by the Avaya SES server.

In these Application Notes, only incoming emergency calls from the local PSAP require a media server address map entry. Calls originated by Avaya SIP telephones configured as OPS are automatically routed to the proper Avaya Communication Manager by the assignment of an Avaya Server extension to that phone. Address map definitions for SIP endpoints not assigned a media server extension and connections to multiple service providers are beyond the scope of these Application Notes.

For the 911 Enable SIP Trunking service, the *user* portion of the SIP URI will contain either the 5 digit local extension value of an analog, digital or IP hard phone station or an 8 digit value beginning with the prefix “111” representing an Avaya IP Softphone. An example of a SIP URI in an INVITE message received from 911 Enable would be:

Analog, Digital or IP Hard Phone:

sip:**61004**@10.1.1.124;user=phone;npdi=yes

Avaya IP Softphone:

sip:**11163005**@10.1.1.124;user=phone;npdi=yes

Note: The *npdi=yes* field refers to the Number Portability Dip Indicator and simply implies that a dip was made into the number portability database upstream.

The user portion in this case is the 5 digit extension number “61004” or the 8 digit prefix+extension number for the softphone example “11163005”. Each of these will require a separate **Media Server Address Map**. The Avaya SES will forward the messages with matching patterns to the appropriate C-LAN interface. To configure a **Media Server Address Map**:

- Select **Media Servers** in the left pane of the Administration web interface. This will display the **List Media Servers** screen.
- Click on the **Map** link associated with the appropriate media server to display the **List Media Server Address Map** screen.
- Click on the **Add Map In New Group** link. The screen shown in **Figure 36** is displayed. The **Host** field displays the name of the media server that this map applies to.
- Enter a descriptive name in the **Name** field

- Enter the regular expression to be used for the pattern matching in the **Pattern** field. In this configuration, there are two possible user part formats that will each require a separate address map.

The first pattern match in **Figure 36** is the pattern for the analog, digital or IP hard phone extension of the form “^sip:6[0-9]{4}”. This means that URIs beginning with “sip:6” followed by any combination of 4 digits should be sent to SP8710-SignalGroup1.

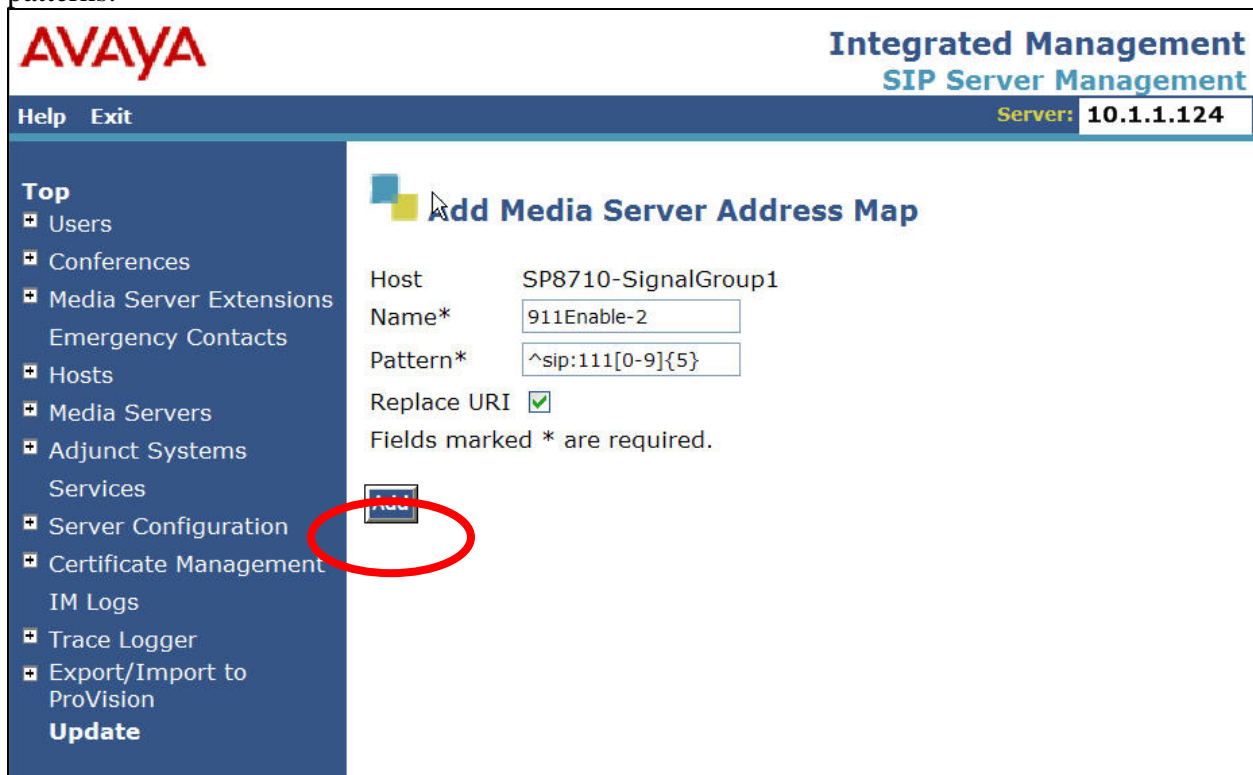
The screenshot shows the Avaya Integrated Management SIP Server Management interface. The top header includes the Avaya logo and the title 'Integrated Management SIP Server Management'. Below the header, there is a navigation menu on the left with options like 'Top', 'Users', 'Conferences', 'Media Server Extensions', 'Emergency Contacts', 'Hosts', 'Media Servers', 'Adjunct Systems', 'Services', 'Server Configuration', 'Certificate Management', 'IM Logs', 'Trace Logger', 'Export/Import to ProVision', and 'Update'. The main content area is titled 'Add Media Server Address Map'. It contains the following fields: 'Host' (SP8710-SignalGroup1), 'Name*' (911Enable), 'Pattern*' (^sip:6[0-9]{4}), and 'Replace URI' (checked). A note at the bottom states 'Fields marked * are required.' The 'Add' button is circled in red.

Figure 36: Media Server Address Map for Analog, Digital and IP Hard Phones

The second pattern match in **Figure 37** is the pattern for the IP softphone of the form “^sip:111[0-9]{5}”. This means that URIs beginning with “sip:111” followed by any combination of 5 digits should be sent to SP8710-SignalGroup1.

- Click the **Add** button once the form is completed.

Appendix B provides a detailed description of the syntax for address map patterns.



The screenshot displays the Avaya Integrated Management SIP Server Management web interface. The top header features the Avaya logo on the left and the title 'Integrated Management SIP Server Management' on the right, with a server IP address of 10.1.1.124. A navigation menu on the left lists various system components, with 'Server Configuration' highlighted and circled in red. The main content area is titled 'Add Media Server Address Map' and contains a form with the following fields: 'Host' (SP8710-SignalGroup1), 'Name*' (911Enable-2), and 'Pattern*' (^sip:111[0-9]{5}). The 'Replace URI' checkbox is checked. A note at the bottom of the form states 'Fields marked * are required.'.

Figure 37: Media Server Address Map for Avaya IP Softphone

After configuring the media server address map, the **List Media Server Address Map** screen appears as shown in **Figure 38**.

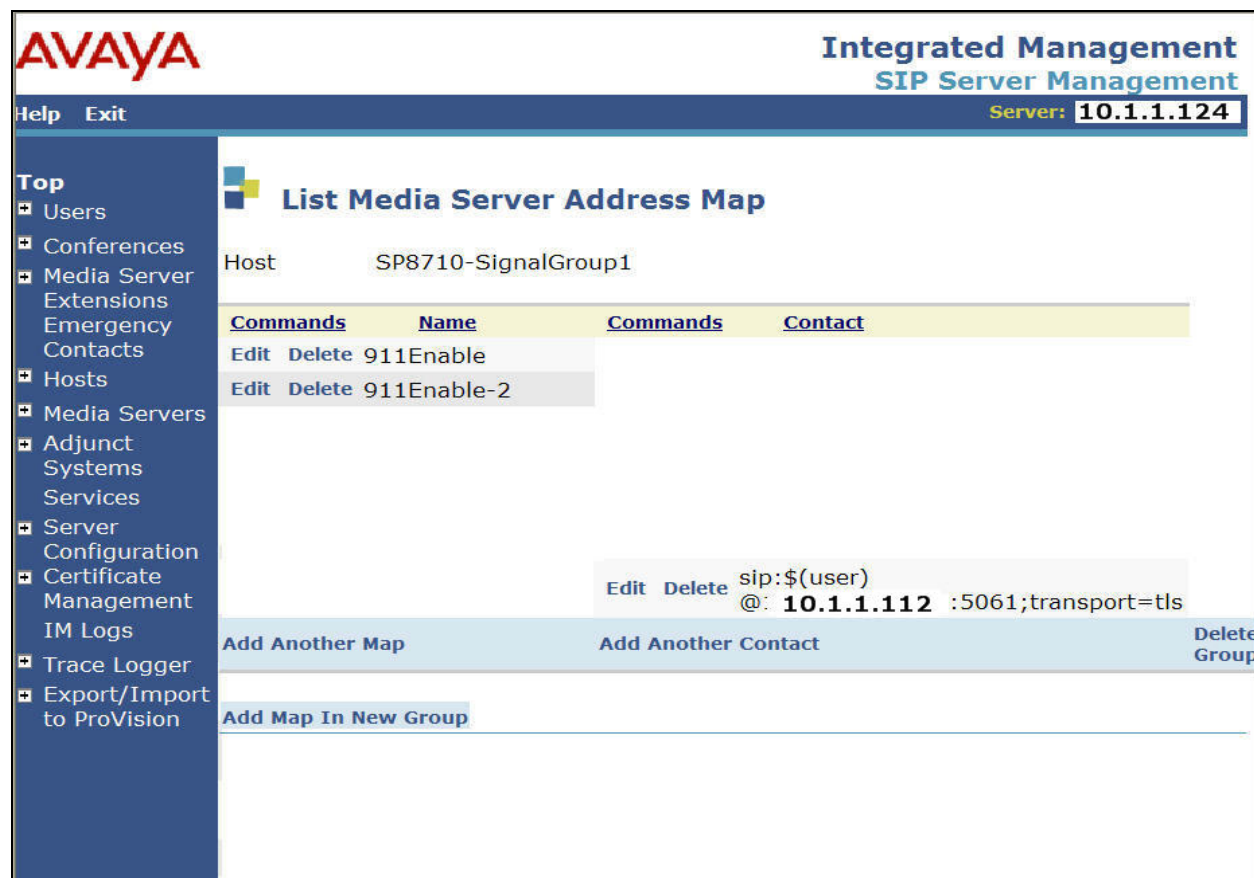


Figure 38: List Media Server Address Map

Note that after the first **Media Server Address Map** is added, the **Media Server Contact** is created automatically. For the **Media Server Address Map** added in **Figure 36** and **37**, the following contact was created:

sip:\$(user)@10.1.1.112:5061;transport=tls

The contact specifies the IP address of the CLAN and the transport protocol used to send SIP signaling messages. The incoming digits sent in the user part of the original request URI is substituted for \$(user).

Step 6: Specify Address Maps to 911 Enable

Outbound PSTN calls are directed by Avaya Communication Manager automatic route selection (ARS) according to the customer's network design guidelines. These guidelines determine what types of outgoing calls should be sent to 911 Enable SIP Trunking service. The ARS routing decisions (for trunk group selection) will be customer specific and are beyond the scope of these notes.

SIP signaling messages for outbound calls sent to the SIP trunk are then routed to the 911 Enable SIP proxy using Host Address Maps within Avaya SES. As with the inbound media server address maps, these Host Address Maps use pattern matching on the SIP URI to direct messages to the corresponding contact address (e.g., the 911 Enable SIP Proxy). In this configuration, the Avaya SES routing rule for the SIP trunk group will be to send all outbound 911 emergency call traffic to 911 Enable's SIP Trunking service. To perform this, one dialing pattern will be created in the Avaya SES.

- The 911 emergency call will be recognized using the pattern “^sip:911”.

Note: A user dialed access code (such as 9 to place the emergency call) has been previously deleted (by ARS) prior to seizing the outbound SIP trunk. Therefore, the route pattern is used to re-append the “9” to the “11” string before it is passed to the SES and 911 Enable as described in **Section 3.1, Step 8 and Figure 19**.

The configuration of the host address map for all 911 calls is shown in **Figure 39**.

- Access the **Add Host Address Map** screen by selecting the **Hosts** link in the left pane of the Administration web interface and then clicking on the **Map** link associated with the appropriate host. The **List Host Address Map** screen is displayed.
- From this screen, click the **Add Map In New Group** link to display the **Add Host Address Map** screen shown in **Figure 38**. Enter a descriptive name for the map, such as “Emergency911”.
- Specify an appropriate pattern for the call type. In this example, the pattern used for Emergency calls is “^sip:911”.
- Leave the **Replace URI** checkbox selected.
- Click the **Add** button

The screenshot displays the Avaya Integrated Management SIP Server Management web interface. The top header includes the Avaya logo, the title 'Integrated Management SIP Server Management', and the server IP '10.1.1.124'. A left-hand navigation menu lists various system components, with 'Hosts' currently selected. The main content area is titled 'Add Host Address Map' and contains the following fields and controls:

- Host:** 10.1.1.124
- Name*:** Emergency911
- Pattern*:** ^sip:911
- Replace URI:** ☒
- Fields marked * are required.**
- Add** button

Figure 39: Add Host Address Map

Step 7: Specify the 911 Enable Proxy Information

The next step is to enter the contact address for the 911 Enable SIP gateway. In this example, a IP Address is used to identify 911 Enable's SIP proxy. This customer specific information is provided by 911 Enable. To enter the 911 Enable SIP proxy information:

- As described in **Step 6**, display the **List Host Address Map** screen.
- Click on the **Add Another Contact** link associated with the address map added in **Figure 39** to open the **Add Host Contact** screen. In this screen, the **Contact** field specifies the destination for the call and it is entered as:

sip:\$(user)@10.2.2.10:5060;transport=udp

The user part in the original request URI is inserted in place of the “\$(user)” string before the message is sent to 911 Enable. .

- Click the **Add** button when completed.

After configuring the host address maps and contact information, the **List Host Address Map** screen will appear as shown in **Figure 40**.

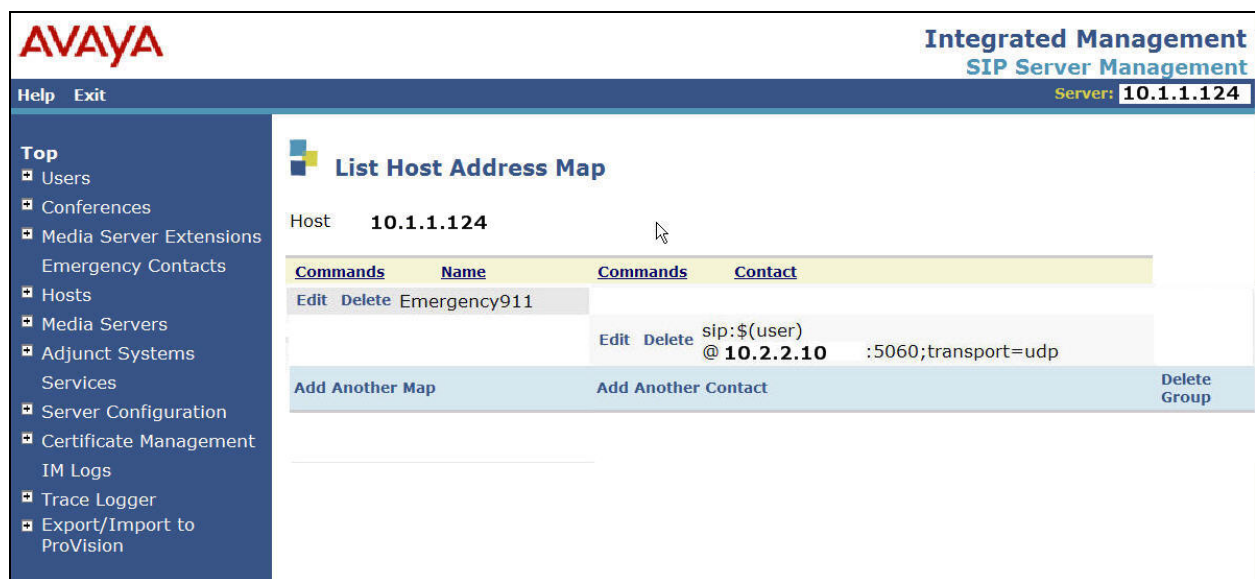


Figure 40: List Host Address Map

Step 8: Save the Changes

After making changes within Avaya SES, it is necessary to commit the database changes using the **Update** link that appears when changes are pending. Perform this step by clicking on the **Update** link found in the bottom of the blue navigation bar on the left side of any of the SES Administration screens as shown in **Figure 41**.

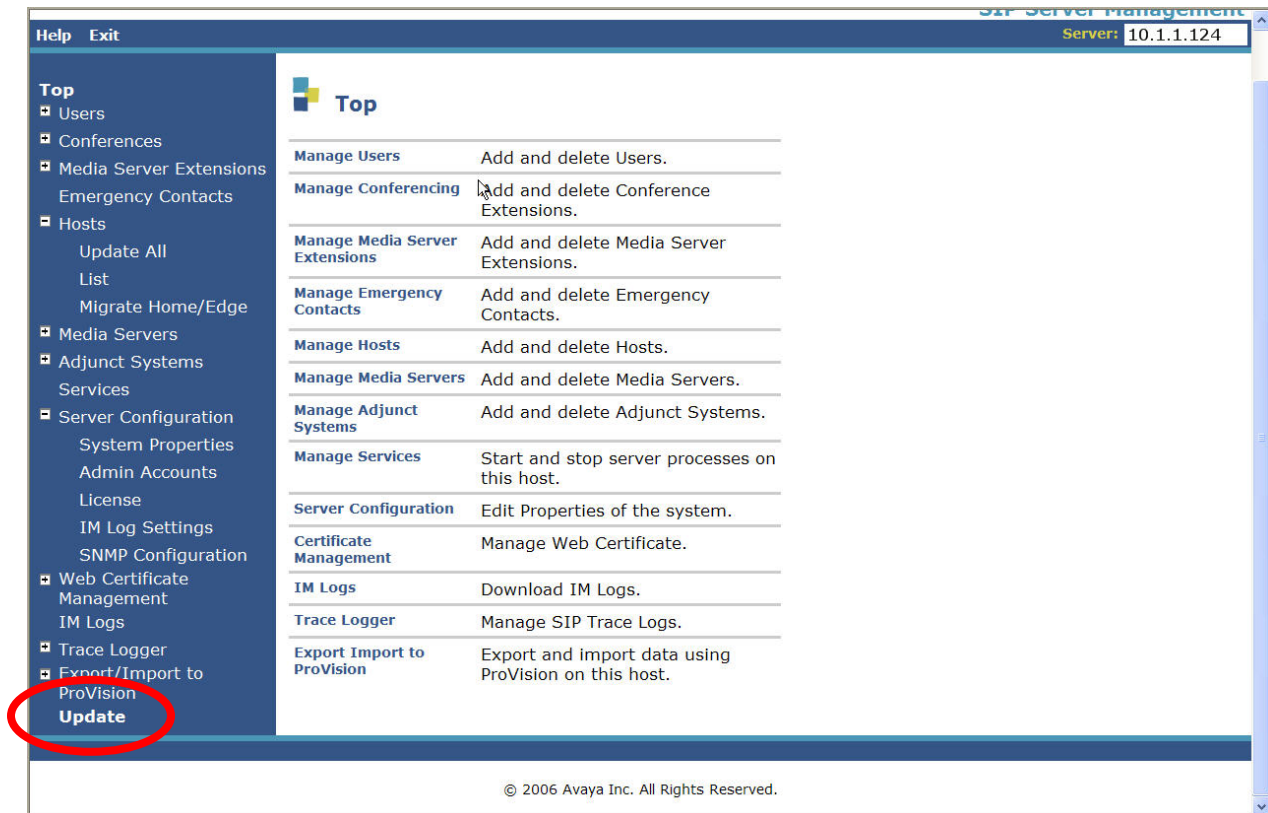


Figure 41: Update Following SES Administrative Changes

Step 9: Specify the 911 Enable SIP Proxy as a Trusted Host

The final step to complete the SIP trunk administration on Avaya SES is to designate the IP address of the 911 Enable SIP Gateway as a trusted host. As a trusted host, Avaya SES will not issue SIP authentication challenges for incoming requests from the designated IP address.¹ If multiple SIP proxies are used, the IP address of each SIP proxy must be added as a trusted host.

To configure a trusted host:

- Telnet or SSH to the Avaya SES Linux shell using the administrative login and password.
- Enter the following trustedhost command at the Linux shell prompt:

```
trustedhost -a 10.2.2.10 -n 10.1.1.124 -c 911 Enable
```

The `-a` argument specifies the address to be trusted; `-n` specifies the SES host name; `-c` adds a comment.

- Use the following trustedhost command to verify the entry is correct:
`trustedhost -L`

Figure 42 illustrates the results of the trustedhost commands.²

- Complete the trusted host configuration by returning to the main Avaya SES Administration web page and again clicking on the **Update** link as shown in **Figure 41**. If the **Update** link is not visible, refresh the page by selecting **Top** from the left hand menu. Note this step is required even though the trusted host was configured via the Linux shell.

```
admin@ses_eh> trustedhost -L
Third party trusted hosts.
```

Trusted Host	CCS Host Name	Comment
10.2.2.10	10.1 .1 .124	911 Enable

```
admin@ses_eh>
```

Figure 42: Configuring a Trusted Host

¹ Note, if the trusted host step is not done, authentication challenges to incoming SIP messages (such as INVITEs and BYEs) will be issued by the Avaya SES. This may cause call setup to fail, active calls to be disconnected after timeout periods, and/or SIP protocol errors.

² For completeness, the `-d` argument allows the trust relationship to be deleted. For example, `trustedhost -d 10.2.2.10 -n 10.1.1.124` removes the trust relationship added above.

4.3 Configuration for SIP Telephones

This section provides very basic instructions for completing the administration necessary to support the optional Avaya 46xx SIP telephones. Additional features such as the use of mnemonic addressing and instant messaging are also supported by Avaya SES but are beyond the scope of these Application Notes.

Step 1: Add a SIP User

Create the SIP user record as follows:

- In Avaya SES administration, expand the **Users** link in the left side blue navigation bar and click on the **Add** link.
- In the **Add User** screen, enter the extension of the SIP endpoint in the **Primary Handle** field.
- Enter a user password in the **Password** and **Confirm Password** fields. This password will be used when logging into the user's SIP telephone.
- In the **Host** field, select the Avaya SES server hosting the domain (10.1.1.124) for this user. Enter the **First Name** and **Last Name** of the user.
- To associate a media server extension with this user, select the **Add Media Server Extension** checkbox. Calls from this user will always be routed through Avaya Communication Manager over the SIP trunk for origination services.
- Press the **Add** button. This will cause a confirmation screen to appear.
- Press **Continue** on the confirmation screen.

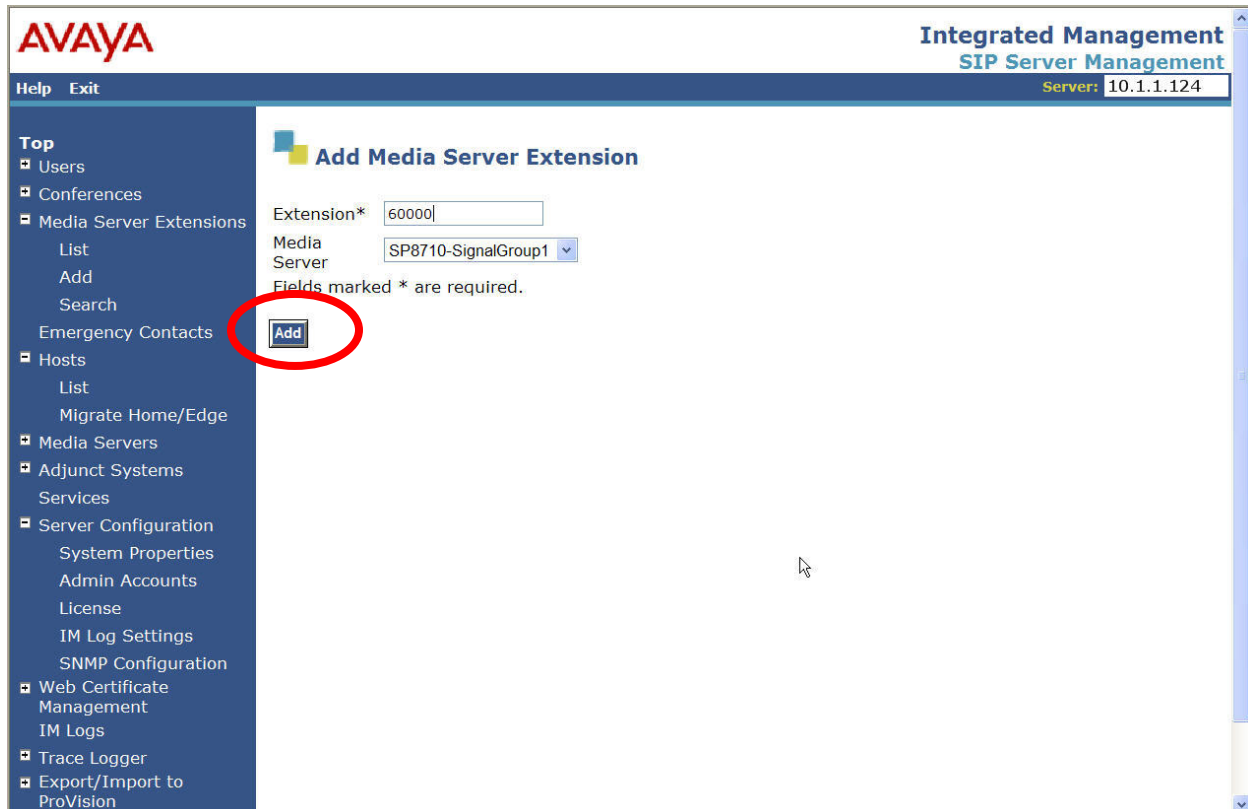
The screenshot shows the 'Add User' form in the Avaya Integrated Management SIP Server Management interface. The top header includes the Avaya logo, 'Integrated Management SIP Server Management', and the server IP '10.1.1.124'. A left-hand navigation menu lists various system components. The main form area contains fields for user creation: Primary Handle* (60000), User ID, Password* (masked with dots), Confirm Password* (masked with dots), Host* (10.1.1.124), First Name* (SIP), Last Name* (60000), Address 1, Address 2, Office, City, State, Country, and Zip. There is also an 'Add Media Server Extension' checkbox which is checked. A note at the bottom states 'Fields marked * are required.' and an 'Add' button is at the bottom left of the form area.

Figure 43: Add User

Step 2: Specify Corresponding Avaya Communication Manager Extension

The SIP phone handle must now be associated with the corresponding extension on Avaya Communication Manager.

- In the **Add Media Server Extension** screen, enter the **Extension** configured on the media server, shown in **Figure 22**, for the OPS extension on Avaya Communication Manager previously defined in **Section 3.2**. Usually, the media server extension and the user extension are the same (recommended) but it is not required.
- Select the **Media Server** assigned to this extension.
- Click on the **Add** button.



The screenshot displays the Avaya Integrated Management SIP Server Management web interface. The top header includes the Avaya logo, the title 'Integrated Management SIP Server Management', and the server IP '10.1.1.124'. A left-hand navigation menu lists various system management options. The main content area is titled 'Add Media Server Extension' and contains a form with the following fields: 'Extension*' with the value '60000', and 'Media Server' with a dropdown menu showing 'SP8710-SignalGroup1'. A note below the fields states 'Fields marked * are required.' The 'Add' button at the bottom of the form is circled in red.

Figure 44: Add Media Server Extension

Step 3: Repeat for Each SIP User

Repeat Steps 1 and 2 for each SIP user.

5. 911 Enable Trunking Services Configuration

In order to use the 911 Enable service, a customer request must be made by following the 911 Enable sales process. The process can be started by one of two ways:

- Fill out the Contact Us form: <http://www.911enable.com/signup.php>. After submitting the form, the customer is contacted via email by a 911 Enable sales representative for the purpose of scheduling a telephone follow up.
- Contact the Toll Free telephone number **1-877-862-2835**

911 Enable has established a 6 step project integration plan. This process ensures that Avaya equipment has been adequately configured and tested for the 911 Enable service, and that the necessary data has been gathered to configure Emergency Response Locations and provision Avaya endpoints.

Preparation:

This phase introduces team members and establishes the objectives, project tasks and timelines. 911 Enable will also discuss the specifics of the Avaya deployment to determine if 911 Enable will be required to perform an on-site assessment.

ERL assessment:

This assessment allows 911 Enable to determine Emergency Response Location (ERL) parameters while gathering switch and port information. 911 Enable can then assign switch and port data to the appropriate ERLs as necessary, in accordance with local ordinances governing emergency 9-1-1 call handling.

Connectivity testing:

911 Enable provides a configuration worksheet which requests information regarding the customer network, (i.e. the soft switch and media gateway models, the IP address of the SIP proxy, and IP address of the media gateway for RTP etc.). The testing phase itself is performed in the lab environment and ensures that all components will work together during live deployment. 911 Enable performs a series of test cases which have been designed to ensure that 9-1-1 calls are directed to the correct PSAP. 9-1-1 calls are made using a PSAP simulator and data pertaining to these calls is logged and reviewed. Once each test case has passed successfully, 911 Enable and the enterprise can sign off on the testing period.

Provisioning Integration:

This stage includes integration work with the enterprise's existing databases and provisioning processes. The enterprise consults with 911 Enable in order to complete the intranet provisioning service using the SOAP/XML interface to 911 Enable, and to prepare the network for switch crawling technology such as Locate 911. If Locate 911 is used, an itinerary of switch and port information and phone data must be compiled for upload to the appliance. Enterprises that use a network asset management tool other than Locate 911 must consult with 911 Enable to determine systems compatibility.

First Office Application (FOA):

In the First Office Application, an enterprise site is selected that will undergo initial switchover to the 911 Enable service. Rigorous testing ensures that the system is properly configured and is able to support every potential fallback scenario. The FOA is capped off by a period monitoring before the final signoff.

Rollout:

A rollout plan is established, and each site is put into service using the same work flow as the FOA. After every site is fully operative, 911 Enable and the customer can sign off on project rollout.

6. Interoperability Compliance Testing

This section describes the interoperability compliance testing used to verify SIP trunking interoperability between 911 Enable's SIP Trunking Service and an Avaya IP Telephony Solution.

6.1. General Test Approach

A simulated enterprise site consisting of an Avaya IP telephony solution supporting SIP trunking was connected to the public Internet using a dedicated broadband connection. The enterprise site was configured to use the commercially available 911 Enable service allowing the enterprise site to use SIP trunking for emergency calling.

The following features and functionality were covered during the SIP trunking interoperability compliance test:

- Outgoing emergency calls from the enterprise site were completed via 911 Enable to the local simulated PSAP destination.
- Incoming calls to the enterprise site from the simulated 911 operator in the event of a dropped call.
- Calls using SIP, H.323, digital and analog endpoints supported by the Avaya IP telephony solution.
- Calls using G.711mu codec and G.711a codec.
- The telephone "hold" feature. This feature was tested to simulate the possibility of a user needing to go on hold in an emergency situation.
- Direct IP-to-IP media. This feature, also known as "Shuffling," allows SIP endpoints to send audio (RTP) packets directly to each other without using media resources on the Avaya Media Gateway. **Note This feature is only available upon special request. 911 Enable recommends against using this feature for emergency calls.**
- Proper configuration of the Emergency Location Extension on different Avaya telephony end points. This setting determines the Calling Party Number (CPN) sent to the 911 Enable service.

6.2. Test Results

Interoperability testing of the sample configuration was completed with successful results.

The following observations were noted.

6.2.1 Emergency Calling From a Bridged Call Appearance

When an emergency call is placed from a bridged call appearance that traverses a SIP Trunk, the Calling Party Number sent is that of the principal's and not that of the physical set the call was placed from.

Discussion/Workaround

This behavior may change in a future release.

6.2.2 Public Unknown Numbering Form and Emergency Location Extension Configuration

When using SIP trunks for emergency calls, if the following is true:

- A station's Emergency Location Extension is different than the actual station's main extension.
- The **Public Unknown Numbering** form in Avaya Communication Manager has an entry for the station's main extension.

Then the station's main extension is sent as the CPN instead of the Emergency Location Extension.

Discussion/Workaround

Use a dedicated SIP trunk group for emergency calling only and do not make an entry for the station's main extension on the **Public Unknown Numbering** form in Avaya Communication Manager.

7. Verification Steps

This section provides verification steps that may be performed to verify that the SIP, H.323, digital and analog endpoints can place outbound and receive inbound emergency calls through 911 Enable. This testing must be done in conjunction with a 911 Enable technician so that the test calls are not passed into the real emergency network.

1. Verify that endpoints at the enterprise site can place emergency calls to 911 Enable's network and that call remains active for more than 35 seconds. This time period is included to verify that proper routing of the SIP messaging has satisfied SIP protocol timers.
2. Verify that endpoints at the enterprise site can receive calls from the 911 Enable network and that the call can remain active for more than 35 seconds.
3. Verify that the user on the 911 Enable network can terminate an active call by hanging up.
4. Verify that an endpoint at the enterprise site can terminate an active call by hanging up.

8. Support

For 911 Enable technical support, contact 911 Enable Customer Service at 1-888-908-4167 or submit support requests at <http://support.connexon.com/main/users/main.php>

9. Conclusion

These Application Notes describe the configuration steps required to connect customers using an Avaya Communication Manager and Avaya SIP Enablement Services Telephony solution to 911 Enable.

911 Enable offers a reliable, future proof 911 solution that has been fully tested by technical teams as part of the Avaya Developer*Connection* Service Provider program. Enterprises with an Avaya deployment can integrate 911 Enable as their 911 solution provider by configuring the Avaya equipment to route 911 calls over a secure SIP trunk.

10. References

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

- [1] *Administrator Guide for Avaya Communication Manager*, February 2007, Issue 3.1, Document Number 03-300509.
- [2] *Feature Description and Implementation for Avaya Communication Manager*, Issue 4, Document Number 555-245-205
- [3] *Avaya Extension to Cellular and Off-PBX Station (OPS) Installation and Administration Guide Release 3.1*, Feb 2006, Issue 9, Document Number 210-100-700.
- [4] *Installing and Administering SIP Enablement Services R3.1*, February 2006, Issue 1.5, Document Number 03-600768
- [5] *SIP Support in Release 3.1 of Avaya Communication Manager Running on the Avaya S8300, S8500, S8500B, S8700, and S8710 Media Server*, February 2006, Issue 6, Document Number 555-245-206.
- [6] *4600 Series IP Telephone R2.8 LAN Administrator Guide*, February 2007, Issue 6, Document Number 555-233-507

Non Avaya Documentation:

- [7] RFC 3261 *SIP: Session Initiation Protocol* <http://www.ietf.org/>
- [8] RFC 2833 *RTP Payload for DTMF Digits, Telephony Tones and Telephony Signals* <http://www.ietf.org/>
- [9] 911 Enable Enterprise Solution SIP Trunking http://www.911enable.com/pdf/SIP_Trunking.pdf

APPENDIX A: Sample SIP INVITE Messages

This section displays the format of the SIP INVITE messages sent by 911 Enable and the Avaya SIP network at the enterprise site. Customers may use these INVITE messages for comparison and troubleshooting purposes. Differences in these messages may indicate different configuration options selected.

Sample SIP INVITE Message from 911 Enable to Avaya SIP Enablement Services:

INVITE sip:61004@10.1.1.124 SIP/2.0

Message Header

Via: SIP/2.0/UDP 10.2.2.10:5060;branch=z9hG4bK3e6a6b6a;rport

From: "911" <sip:7328521637@10.2.2.10>;tag=as58fb01db

To: <sip:61004@10.1.1.124>

Contact: <sip:7328521637@10.2.2.10>

Call-ID: 15f3209a3be4c03e7569651848542394@10.2.2.10

CSeq: 102 INVITE

User-Agent: 911Enable SBC2

Max-Forwards: 70

Date: Tue, 22 May 2007 17:01:36 GMT

Allow: INVITE, ACK, CANCEL, OPTIONS, BYE, REFER, SUBSCRIBE, NOTIFY

Supported: replaces

Content-Type: application/sdp

Content-Length: 268

Session Description Protocol

Session Description Protocol Version (v): 0

Owner/Creator, Session Id (o): root 14019 14019 IN IP4 10.2.2.10

Session Name (s): session

Connection Information (c): IN IP4 10.2.2.10

Time Description, active time (t): 0 0

Media Description, name and address (m): audio 18042 RTP/AVP 0 8 101

Media Attribute (a): rtpmap:0 PCMU/8000

Media Attribute (a): rtpmap:8 PCMA/8000

Media Attribute (a): rtpmap:101 telephone-event/8000

Media Attribute (a): fmp:101 0-16

Media Attribute (a): silenceSupp:off - - -

Media Attribute (a): ptime:20

Media Attribute (a): sendrecv

Sample SIP INVITE Message from Avaya SIP Enablement Services to 911 Enable:

INVITE sip:911@10.2.2.10:5060;transport=udp SIP/2.0
Message Header
Call-ID: 80209a9d56fdc18f1d465d8e4a00
CSeq: 1 INVITE
From: "IP(H323) Phone" <sip:61001@10.1.1.124:5061>;tag=80209a9d56fdc18e1d465d8e4a00
Record-Route: <sip:10.1.1.124:5060;lr>,<sip:10.1.1.112:5061;lr;transport=tls>
To: "911" <sip:911@10.1.1.124>
Via: SIP/2.0/UDP 10.1.1.124:5060;branch=z9hG4bK838383030303232323e492.0,SIP/2.0/TLS
10.1.1.112;psrrposn=2;received=10.1.1.112;branch=z9hG4bK80209a9d56fdc1901d465d8e4a00
Content-Length: 159
Content-Type: application/sdp
Contact: "IP(H323) Phone" <sip:61001@10.1.1.112:5061;transport=tls>
Max-Forwards: 69
User-Agent: Avaya CM/R014x.00.0.730.5
Allow: INVITE,CANCEL,BYE,ACK,PRACK,SUBSCRIBE,NOTIFY,REFER,OPTIONS
History-Info: <sip:911@10.1.1.124>;index=1
History-Info: "911" <sip:911@10.1.1.124>;index=1.1
Supported: 100rel,timer,replaces,join,histinfo
Min-SE: 1200
Session-Expires: 1200;refresher=uac
P-Asserted-Identity: "IP(H323) Phone" <sip:61001@10.1.1.124:5061>

Session Description Protocol
Session Description Protocol Version (v): 0
Owner/Creator, Session Id (o): - 1 1 IN IP4 10.1.1.112
Session Name (s): -
Connection Information (c): IN IP4 10.1.1.116
Time Description, active time (t): 0 0
Media Description, name and address (m): audio 58624 RTP/AVP 0 127
Media Attribute (a): rtpmap:0 PCMU/8000
Media Attribute (a): rtpmap:127 telephone-event/8000

APPENDIX B: Specifying Pattern Strings in Address Maps

The syntax for the pattern matching used within the Avaya SES is a Linux regular expression used to match against the URI string found in the SIP INVITE message.

Regular expressions are a way to describe text through pattern matching. The regular expression is a string containing a combination of normal text characters, which match themselves, and special *metacharacters*, which may represent items like quantity, location or types of character(s).

In the pattern matching string used in the Avaya SES:

- Normal text characters and numbers match themselves.
- Common metacharacters used are:
 - A period `.` matches any character once (and only once).
 - An asterisk `*` matches zero or more of the preceding characters.
 - Square brackets enclose a list of any character to be matched. Ranges are designated by using a hyphen. Thus the expression `[12345]` or `[1-5]` both describe a pattern that will match any single digit between 1 and 5.
 - Curly brackets containing an integer 'n' indicate that the preceding character must be matched exactly 'n' times. Thus `5{3}` matches '555' and `[0-9]{10}` indicates any 10 digit number.
 - The circumflex character `^` as the first character in the pattern indicates that the string must begin with the character following the circumflex.
Putting these constructs together as used in this document, the pattern to match the SIP INVITE string for any valid 1+ 10 digit number in the North American dial plan would be:
`^sip:1[0-9]{10}`

This reads as: "Strings that begin with exactly **sip:1** and having any 10 digits following will match.

A typical INVITE request below uses the shaded portion to illustrate the matching pattern.

INVITE sip:17325551638@proxy-bandtel:5060;transport=udp SIP/2.0

©2007 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 DeveloperConnection Program at devconnect@avaya.com.