

Avaya Solution & Interoperability Test Lab

# Application Notes for Configuring 911 Enable Emergency Gateway and Emergency Routing Service with Avaya Aura® Communication Manager 6.0 and Avaya Aura® Session Manager 6.0 - Issue 1.0

#### Abstract

These Application Notes describe the procedures for configuring the 911 Enable Emergency Gateway and Emergency Routing Service with Avaya Aura® Communication Manager 6.0 and Avaya Aura® Session Manager 6.0.

The 911 Enable Emergency Gateway and Emergency Routing Service offers an E911 call routing and location provisioning solution for enterprises using both legacy and IP phone deployments. Communication Manager connects to the Emergency Gateway via a SIP trunk and the Emergency Gateway connects to the public Internet to access the Emergency Routing Service. The compliance testing focused on placing 911 calls from various endpoint types connected to different network equipment to verify that their location and callback number could be properly determined.

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

### 1. Introduction

These Application Notes describe the procedures for configuring the 911 Enable Emergency Gateway (EGW) and Emergency Routing Service (ERS) with Avaya Aura® Communication Manager and Avaya Aura® Session Manager.

The 911 Enable Emergency Gateway and Emergency Routing Service offers an E911 call routing and location provisioning solution for enterprises using both legacy and IP phone deployments. Communication Manager connects to the Emergency Gateway via a SIP trunk and the Emergency Gateway connects to the public Internet to access the Emergency Routing Service. The compliance testing focused on placing 911 calls from various endpoint types connected to different network equipment to verify that their location and callback number could be properly determined.

### 1.1. Interoperability Compliance Testing

The following features and functionality of the EGW were tested.

- Layer 2 discovery from supported layer 2 switches.
- Layer 3 discovery of Avaya H.323 and SIP Telephones that support the PUSH API.
- Layer 3 discovery of Avaya IP one-X<sup>®</sup> Communicator (H323 and SIP) when used with 911 Enable E911 Softphone Locator (ESL) Software.
- Emergency calls from all endpoint types were routed to the ERS via the EGW.
- Proper location information provided for all "known" locations.
- Calls from "unknown" locations were routed to the 911 Enable Emergency Call Response Center (ECRC).
- Callback numbers were assigned using the EGW Extension-Bind feature.
- Calls placed using the provided callback number were routed to the proper extension.
- Failover to the secondary EGW, if the primary EGW was not available.
- If neither EGW was available, calls were routed back via Session Manager to Communication Manager routed emergency calls to the ECRC via the PSTN.
- If the primary ERS was not available, the EGW routed emergency calls to the secondary ERS.
- If the primary and secondary ERS were not available, the EGW routed emergency calls to the ECRC via Session Manager and Communication Manager.
- Two Communication Managers were used to make sure that Layer 2 discovery was done properly by the EGW. Additionally, if same IP phone extension was configured on both Communication Managers, it was verified that the callback from PSAP is routed to the correct Communication Manager extension.

See Section 8 for complete test results and any observations or limitations.

#### 1.2. Support

For technical support on the EGW, contact 911 Enable at <u>www.911enable.com</u>.

# 2. Reference Configuration

**Figure 1** illustrates the test configuration. The test configuration shows an enterprise site connected to the 911 Enable Emergency Routing Service (ERS) via the 911 Enable Emergency Gateway (EGW). The ERS can send calls to the Public Service Answering Point (PSAP) or to the ECRC.

Located at the enterprise site is a pair of Avaya S8800 Servers running Communication Manager using an Avaya G650 Media Gateway. Session Manager is also present at the enterprise to support the SIP endpoints at the enterprise and provide routing between Communication Manager and EGW using SIP Trunks. Endpoints include Avaya 96xx Series IP Telephones (H.323 and SIP), Avaya 46xx Series IP Telephones (H.323), an Avaya IP Avaya one-X® Communicator (H.323 and SIP), an Avaya 6408D Digital Telephone, and an Avaya 6211 Analog Telephone. These endpoints were connected to two different Extreme models (x250p-24t and 400-24p) and Avaya C364T-PWR switches. An ISDN-PRI trunk connects the Avaya Media Gateway to the PSTN.

At the edge of the enterprise resides a redundant pair of EGWs. Each EGW connects to the Session Manager via a SIP trunk. All 911 emergency calls from the enterprise are routed to EGW. If the primary EGW is unavailable then Session Manager will route the emergency call to the secondary EGW.

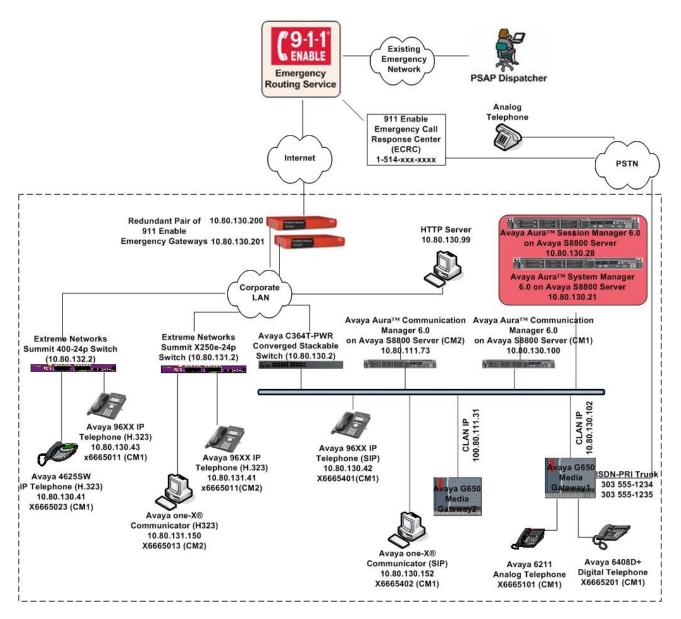


Figure 1: Test Configuration

The endpoints in **Figure 1** were divided into 3 locations. The first location, provisioned as LOC1, includes extensions 6665101 (Analog), 6665201 (Digital), 6665401 (SIP Deskphone) and 6665402 (SIP one-X Communicator). The second location, provisioned as LOC2, includes extensions 6665011 (H323) and 6665013 (H323 one-X Communicator). The last location, provisioned as LOC3, includes extension 6665011 (H323) 6665023 (H323).

For security purposes, any public IP addresses or PSTN routable phone numbers used in the compliance test are not shown in these Application Notes. Instead, some of the digits in these values have been replaced with an "x" to represent any value. An example is the ECRC phone number is **Figure 1**.

### 2.1. Auto-Discovery of Endpoints

The EGW attempts to auto discover the presence and location of Avaya 4600 and 9600 Series H.323 and SIP Telephones by correlating data obtained through two mechanisms. The first mechanism is known as layer 2 discovery. To support layer 2 discovery, each layer 2 switch where the above telephones types are connected must support certain MIB objects required by the EGW. In this reference configuration, three different types of layer 2 switches were used. Endpoints connected to the Extreme Networks Summit X250e-24t and 400-24p switches and Avaya C364T-PWR Converged Stackable Switch were automatically discovered. The data obtained from layer 2 discovery includes the MAC address of the device connected to each port of the switch. The second mechanism required for auto-discovery is known as layer 3 discovery. To support layer 3 discovery, each listed telephone type uses an application downloaded to it during initialization to report information to the EGW. Thus, the Avaya telephone types used must support the PUSH API. The information from layer 2 and 3, the EGW learns what extensions are physically connected to which layer 2 switch.

The presence and location of the Avaya one-X® Communicator users are done in a similar manner. Layer 2 discovery is dependent upon which layer 2 switch the Windows PC running Avaya one-X® Communicator is connected. Layer 3 discovery is done by installing the 911 Enable ESL software on the PC where Avaya one-X® Communicator is installed.

All digital and analog endpoints must be manually provisioned.

Note: All switches are not capable of doing layer 2 discovery. For the switches which do not support the layer 2 discovery, endpoints have to be manually provisioned in the EGW.

#### 2.2. Callback Numbers

A callback number (CBN) is assigned to each extension for use by the 911 operator to reach the caller if the emergency call is dropped. The callback number for each extension would be its Direct Inward Dial (DID) number if it has one assigned. However, all internal extensions may not have a DID assigned. In this case, where an extension does not have a DID assigned, the EGW will temporary map a DID number to that extension for the duration of the emergency call. This is known as the EGW Extension-Bind feature. The pool of DIDs used by the EGW is assigned to the EGW from the DIDs owned by the enterprise. In the case of this compliance test, duplicate extensions on two different Communication Managers needed to be assigned a separate DID as EGW does not specify the domain from where the 911 call was originated. For all other extensions a single temporary DID was used for CBN.

#### 2.3. Emergency Call Flows

Emergency calls are routed differently depending on whether all components are operational and what information is available about the caller.

- Typical "Sunny Day" Scenario: If all components and user information are available then the call flow is as follows: User Extension → Communication Manager → Session Manager →EGW → ERS → PSAP. If a callback call is needed and a temporary DID number is used from the EGW Extension-Bind pool, then the callback call flow is PSAP → PSTN → Communication Manager → Session Manager → EGW → Session Manager → Communication Manager → User Extension. If the user extension has its own DID number, then the callback call would not need to be routed through the EGW but would flow from PSAP → PSTN → Communication Manager → Session Manager → Communication Manager →User Extension.
- 2. Missing User Information: If all components are operational, but the emergency call does not have the proper location or callback information, then the call is routed to the ECRC where a trained 911 operator collects the correct information before forwarding the call to the PSAP. This call can reach the ECRC in two different ways based on the provisioning of the EGW. The EGW can be provisioned to reject the call if all necessary information is not present, so that Communication Manager reroutes the call out the PSTN. For the compliance test, the call flow was from User Extension  $\rightarrow$  Communication Manager  $\rightarrow$  Session Manager  $\rightarrow$  EGW (rejects the call), then the call is rerouted from EGW  $\rightarrow$  Session Manager  $\rightarrow$  Communication Manager  $\rightarrow$  PSTN  $\rightarrow$  ECRC  $\rightarrow$  PSAP. Alternatively, the EGW can be provisioned to accept the call and send it to the ERS. The ERS will determine that all information is not present and send the call to the ECRC. The call flow would be User Extension  $\rightarrow$  Communication Manager  $\rightarrow$  Session Manager  $\rightarrow$  EGW  $\rightarrow$  ERS  $\rightarrow$  ECRC  $\rightarrow$ PSAP. Either the ECRC or the PSAP can initiate a callback if necessary. If the callback is made from the PSAP, the callback call flow would be the same as described in scenario 1 above. If the ECRC places the callback, the call flow is the same as described in scenario 1 with the exception that the ECRC replaces the PSAP in the call flow.
- 3. ERS Unavailable: If the EGW is operational but the ERS is unavailable, then when the EGW receives an emergency call, it will originate a call to the ECRC (using the 10 digit ECRC number) through Communication Manager. The call flows from User Extension → Communication Manager → Session Manager → EGW followed by EGW → Session Manager → Communication Manager → PSTN → ECRC → PSAP. The callback call flows would be the same as the callback call flows described in scenario 2 above.
- 4. **EGW Failover**: If the primary EGW fails, Session Manager will reroute the call to the secondary EGW. The call flow would be the same as scenario 1 above.
- 5. Both EGWs Fail: If both EGWs fail, Session Manager will reroute the call to the ECRC. The call flow is User Extension → Communication Manager → Session Manager → EGW (no response), then the call is rerouted by Session Manager → Communication Manager → PSTN → ECRC → PSAP. The callback call flows would be the same as the callback call flows described in scenario 2 above.

### 3. Equipment and Software Validated

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

Equipment	Software/Firmware
Avaya S8800 Server	Avaya Aura® Communication Manager
	6.0
	(R016x.00.0.345.0) with patch 18444
Avaya G650 Media Gateway	
Avaya S8800 Server	Avaya Aura® System Manager 6.0
	(6.0.0.556-3.0.6.1)
Avaya S8800 Server	Avaya Aura® Session Manager 6.0
	(6.0.0.600020)
Avaya 4610SW IP Telephone (H.323)	2.9.1
Avaya 9620 IP Telephone (H.323)	Avaya one-X Deskphone Edition 3.11
Avaya 9620 IP Telephones (SIP)	Avaya one-X Deskphone Edition SIP 2.5
Avaya one-X® Communicator (SIP and	6.0.0.26
H323)	
Avaya 6408D Digital Telephone	-
Avaya 6210 Analog Telephone	-
911 Enable Emergency Gateway	3.1
911 Enable E911 Softphone Locator	1.2
Software	
911 Enable Emergency Routing Service	2.11

# 4. Configure Avaya Aura® Session Manager

These Application Notes assume that basic administration on System Manager and Session Manager has already been performed. Consult **[1]** and **[2]** for further details if necessary. Configuration of Session Manager is performed from System Manager. To invoke the System Manager Common Console, launch a web browser, enter https://<*IP address of System Manager server*>/SMGR as the URL, and log in with the appropriate credentials.

#### 4.1. Background

Session Manager serves as a central point for supporting SIP-based communication services in an enterprise. Session Manager connects and normalizes disparate SIP network components and provides a central point for external SIP trunking to the PSTN. The various SIP network components are represented as "SIP Entities" and the connections/trunks between Session Manager and those components are represented as "Entity Links". Thus, rather than connecting to every other SIP Entity in the enterprise, each SIP Entity simply connects to Session Manager and relies on Session Manager to route calls to the correct destination. This approach reduces the dial plan and trunking administration needed on each SIP Entity, and consolidates said administration in a central place, namely Avaya Aura® System Manager.

When calls arrive at Session Manager from a SIP Entity, Session Manager applies SIP protocol and numbering modifications to the calls. These modifications, referred to as "Adaptations", are sometimes necessary to resolve SIP protocol differences between disparate SIP Entities, and also serve the purpose of "normalizing" the calls to a common or uniform numbering format, which allows for simpler administration of routing rules in Session Manager. Session Manager then matches the calls against certain criteria embodied in profiles termed "Dial Patterns", and determines the destination SIP Entities based on "Routing Policies" specified in the matching Dial Patterns. Lastly, before the calls are routed to the respective destinations, Session Manager again applies Adaptations in order to bring the calls into conformance with the SIP protocol interpretation and numbering formats expected by the destination SIP Entities.

#### 4.2. Routing Policies

Routing Policies define how Session Manager routes calls between SIP network elements. Routing Policies are dependent on the administration of several inter-related items:

- SIP Entities SIP Entities represent SIP network elements such as Session Manager instances, Communication Manager systems, Session Border Controllers, SIP gateways, SIP trunks, and other SIP network devices.
- Entity Links Entity Links define the SIP trunk/link parameters, e.g., ports, protocol (UDP/TCP/TLS), and trust relationship, between Session Manager instances and other SIP Entities.
- SIP Domains SIP Domains are the domains for which Session Manager is authoritative in routing SIP calls. In other words, for calls to such domains, Session Manager applies Routing Policies to route those calls to SIP Entities. For calls to other domains, Session Manager routes those calls to another SIP proxy (either a pre-defined SIP proxy or one discovered through DNS).
- Locations Locations define the physical and/or logical locations in which SIP Entities reside. Call Admission Control (CAC) / bandwidth management may be administered for each location to limit the number of calls to and from a particular Location.

AT; Reviewed:	
SPOC 2/8/2011	

- Adaptations Adaptations are used to apply any necessary protocol adaptations, e.g., modify SIP headers, and apply any necessary digit conversions for the purpose of inter-working with specific SIP Entities. For example, an AT&T-specific Adaptation is used in these Application Notes to remove SIP History-Info headers from SIP messages sent to the AT&T IP Flexible Reach service network. As another example, basic "Digit Conversion" Adaptations are used in this reference configuration to convert digit strings in "destination" (e.g., Request-URI) and "origination" (e.g. P-Asserted Identity) type headers of SIP messages sent to and received from SIP Entities.
- Dial Patterns A Dial Pattern specifies a set of criteria and a set of Routing Policies for routing calls that match the criteria. The criteria include the called party number and SIP domain in the Request-URI, and the Location from which the call originated. For example, if a call arrives at Session Manager and matches a certain Dial Pattern, then Session Manager selects one<sup>1</sup> of the Routing Policies specified in the Dial Pattern. The selected Routing Policy in turn specifies the SIP Entity to which the call is to be routed. Note that Dial Patterns are matched after ingress Adaptations have already been applied.
- Time Ranges Time Ranges specify customizable time periods, e.g., Monday through Friday from 9AM to 5:59PM, Monday through Friday 6PM to 8:59AM, all day Saturday and Sunday, etc. A Routing Policy may be associated with one or more Time Ranges during which the Routing Policy is in effect. For example, for a Dial Pattern administered with two Routing Policies, one Routing Policy can be in effect on weekday business hours and the other Routing Policy can be in effect on weekday off-hours and weekends. In the reference configuration no restrictions were placed on calling times.

The general strategy employed in this reference configuration with regard to Called Party Number manipulation and matching, and call routing is as follows:

- Use common number formats and uniform numbers in matching called party numbers for routing decisions.
- On ingress to Session Manager, apply any called party number modifications necessary to "normalize" the number to a common format or uniform number as defined in the Dial Patterns.
- On egress from SM, apply any called party number modifications necessary to conform to the expectations of the next-hop SIP Entity. For example, on egress from Session Manager to Communication Manager, modify the called party number such that the number is consistent with the dial plan on Communication Manager.

Of course, the items above are just several of many possible strategies that can be implemented with Session Manager.

<sup>&</sup>lt;sup>1</sup> The Routing Policy in effect at that time with highest ranking is attempted first. If that Routing Policy fails, then the Routing Policy with the next highest rankings is attempted, and so on.

		Description
То	-	ey steps required for configuring network routing policies, click on he of the System Manager Common Console.
	AVAYA	Avaya Aura™ System Manager
		6.0 Welcome, <b>admin</b> Last Logged on at June 23, 2010 4:54 PM Help   About   Change Password   <b>Log off</b>
	Home / Routing	
	<ul> <li>▶ Elements</li> <li>▶ Events</li> <li>▶ Groups &amp; Roles</li> </ul>	Introduction to Network Routing Policy Network Routing Policy consists of several routing applications like "Domains", "Locations", "SIP Entities", etc.
	Licenses Routing	The recommended order to use the routing applications (that means the overall routing workflow) to configure your network configuration is as follows:
	Locations	Step 1: Create "Domains" of type SIP (other routing applications are referring domains of type SIP).
	Adaptations SIP Entities	Step 2: Create "Locations"
	Entity Links	Step 3: Create "Adaptations"
	Time Ranges	Step 4: Create "SIP Entities"
	Routing Policies Dial Patterns	- SIP Entities that are used as "Outbound Proxies" e.g. a certain "Gateway" or "SIP Trunk"
	Regular Expressions	- Create all "other SIP Entities" (Session Manager, CM, SIP/PSTN Gateways, SIP Trunks)
	Defaults Security	- Assign the appropriate "Locations", "Adaptations" and "Outbound Proxies"
	<ul> <li>System Manager Data</li> </ul>	Step 5: Create the "Entity Links"
	► Users	- Between Session Managers
	Help	- Between Session Managers and "other SIP Entities"
	Landing Page	Step 6: Create "Time Ranges"
	Help for Import All Data Help for Export All Data	- Align with the tariff information received from the Service Providers
	Help for Committing	Step 7: Create "Routing Policies"
	configuration changes	- 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"
		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 Polices" 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)

Step			Description		
2.	SIP Domains The following screet this compliance te		ne two domains ( <i>avaya.com</i>	n and <i>avaya1.com</i> ) co	onfigured for
	AVAY	Δ	Avaya Aura™ Sy	stem Manager	- 6.0
	Home / Routing / D	omains			
	<ul> <li>Elements</li> <li>Events</li> <li>Groups &amp; Roles</li> </ul>	ŝ	Domain Management	e Delete More	Actions 🝷
	Licenses Routing		4 Items   Refresh		
	Domains Locations		☐ Name		Туре
			avaya1.com		sip
	0 dantations				
2	Adaptations		avaya.com		sip
3.	<b>Locations</b> The following scre	tion 1 Subnet	-	or this compliance te	onet esting.
3.	<b>Locations</b> The following scre	Avaya Aura <sup>+</sup>	□ <u>avaya.com</u> ne locations (Loc1 10.80.13 t 10.80.111.x) configured f	or this compliance te	onet esting.
3.	Locations The following screen 10.80.120.x, Loca AVAYA Home / Routing / Locations Elements Freents Groups & Roles Licenses	Avaya Aura <sup>+</sup>	■ avaya.com ne locations (Loc1 10.80.13 t 10.80.111.x) configured f	or this compliance te	onet esting. I on at December 13, 2010 ange Password   Log off
3.	Locations The following screen 10.80.120.x, Locations	Avaya Aura <sup>+</sup> Location Edit New 1 16 Items Refresh Name AuraSBC	avaya.com e locations (Loc1 10.80.13 t 10.80.1111.x) configured f      System Manager 6.0  Puplicate Delete More Actions •	Yelome, admin Last Logged 2:55 PM Help   About   Cha Notes AuraSBC used for ATT Testing	onet esting. I on at December 13, 2010 ange Password   Log off
3.	Locations The following screen 10.80.120.x, Loca AVAYA Home / Routing / Locations Elements Foruts Groups & Roles Licenses Routing Domains Locations Adaptations	Avaya Aura <sup>T</sup> Location Edit New 1 16 Items Refresh Name AuraSBC Branch Loca	avaya.com a locations (Loc1 10.80.13 t 10.80.1111.x) configured f  System Manager 6.0  Duplicate Delete More Actions •	Yelcome, admin Last Logged 2:55 PM Help   About   Cha	onet esting. I on at December 13, 2010 ange Password   Log off
3.	Locations The following scre 10.80.120.x, Loca AVAYA Home / Routing / Locations Elements Events Groups & Roles Licenses Routing Domains Locations Adaptations SIP Entities	Location Location Edit New 16 Items Refresh Name AuraSBC Branch Location	avaya.com e locations (Loc1 10.80.13 t 10.80.1111.x) configured f <sup>™</sup> System Manager 6.0  Duplicate Delete More Actions •  ation 1 ion	Welcome, admin Last Logged 2:55 PM         Help   About   Cha         Notes         AuraSBC used for ATT Testing         BSM1	onet esting. I on at December 13, 2010 ange Password   Log off
3.	Locations The following screen 10.80.120.x, Loca AVAYA Home / Routing / Locations Elements Foruts Groups & Roles Licenses Routing Domains Locations Adaptations	Location Location Edit New 16 Items Refresh Name Aura38C Branch Locat CUCM Locati Locat 10.80.:	avaya.com avaya.com te locations (Loc1 10.80.13 t 10.80.111.x) configured for  ✓ System Manager 6.0	Yelome, admin Last Logged 2:55 PM Help   About   Cha Notes AuraSBC used for ATT Testing	onet esting. I on at December 13, 2010 ange Password   Log off
3.	Locations The following scre 10.80.120.x, Loca AVAYA Home / Routing / Locations Elements Fronts Groups & Roles Licenses Routing Domains Locations Adaptations SIP Entities Entity Links	Location 1 Subnet	avaya.com e locations (Loc1 10.80.13 t 10.80.1111.x) configured f <sup>™</sup> System Manager 6.0  Duplicate Delete More Actions •  ation 1 ion	Welcome, admin Last Logged 2:55 PM         Help   About   Cha         Notes         AuraSBC used for ATT Testing         BSM1	onet esting. I on at December 13, 2010 ange Password   Log off

4		Description	
4.	Adaptations for c	calls to first Communication Manager	
	The following scre	een displays the adaptation used for calls between Session Manager and	
	first Communication		
	Adaptation na	ame – Any descriptive string	
	Module name	e - Selected <i>DigitConversionAdapter</i> from the drop-down list	
		meter – Parameter osrcd replaces any domain/IP Address in the PAI hea	der
	-	<i>m</i> for outbound request and parameter <i>odstd</i> replaces any domain/IP	
	-	Request URI with <i>avaya.com</i> .	
		onversion for Incoming Calls to SM section,	
		pattern +6665011 was for the calls coming from Communication Manage	)r
			51
	-	cate extension configured in both Communication Managers. A unique	
		ssigned for this extension so that EGW is able to present the right DID for	or
		ck from PSAP attendant.	
	, <b>.</b>	pattern 13035381619 was for the callback from PSAP attendant destined	
	-	olicate extension on first Communication Manager	
		pattern 13035383592 was for the callback from PSAP attendant destined	
	for the dup	blicate extension on second Communication Manager	
	Note: All the callb	backs from PSAP attendant terminated on first Communication Manager	as
	there was only one	e PRI trunk configured for this compliance testing. All the callbacks were	e
	routed to the prope	er Communication Manager by the Session Manager.	
		onversion for Outgoing Calls from SM section, only one entry was	
	_	route the duplicate extensions call to the first Communication Manager.	
	e chinigai e a ve i		
		Avava Διμτα <sup>TM</sup> System Manager 6.0 2:55 PM	
	Αναγα	Avaya Aura "System Manager 6.0 2:55 PM Help   About   Change Password   Log off	
	Home / Routing / Adaptations / Adapt	Avaya Aura ''' System Manager 6.0 2:55 PM Help   About   Change Password   Log off	
	▶ Elements	Avaya Aura "System Manager 6.0 2:55 PM Help   About   Change Password   Log off	
		Avaya Aura ''' System Manager 6.0 2:55 PM Help   About   Change Password   Log off	
	<ul> <li>▶ Elements</li> <li>▶ Events</li> <li>▶ Groups &amp; Roles</li> <li>Licenses</li> </ul>	Avaya Aura <sup>IIII</sup> System Manager 6.0 2:55 PM Help   About   Change Password   Log off tation Details General • Adaptation name: CM1	
	<ul> <li>Elements</li> <li>Events</li> <li>Groups &amp; Roles</li> </ul>	Avaya Aura IIII System Manager 6.0 Earlier Commit Cancel  General  Adaptation name: CM1  Module name: DigitConversionAdapter	
	<ul> <li>&gt; Elements</li> <li>&gt; Events</li> <li>&gt; Groups &amp; Roles</li> <li>Liccenses</li> <li>* Routing</li> <li>Domains</li> <li>Locations</li> </ul>	Avaya Aura <sup>IIII</sup> System Manager 6.0 Itation Details Adaptation Details General Module name: CM1 Module name: CipitConversionAdapter Module parameter: osrcd=avaya.com odstd=avaya.co	
	<ul> <li>&gt; Elements</li> <li>&gt; Events</li> <li>&gt; Groups &amp; Roles</li> <li>Licenses</li> <li>* Routing</li> <li>Domains</li> </ul>	Avaya Aura IIII System Manager 6.0 Earlier Commit Cancel  General  Adaptation name: CM1  Module name: DigitConversionAdapter	
	<ul> <li>Elements</li> <li>Events</li> <li>Groups &amp; Roles</li> <li>Licenses</li> <li>Routing</li> <li>Domains</li> <li>Locations</li> <li>Adaptations</li> <li>SIP Entities</li> <li>Entity Links</li> </ul>	Avaya Aura IIII System Manager 6.0 Help   About   Change Password   Log off tation Details General • Adaptation name: CM1 Module name: DigitConversionAdapter General: Egress URI Parameters:	
	<ul> <li>&gt; Elements</li> <li>&gt; Events</li> <li>&gt; Groups &amp; Roles</li> <li>Licenses</li> <li>* Routing</li> <li>Domains</li> <li>Locations</li> <li>Adaptations</li> <li>SIP Entities</li> </ul>	Avaya Aura <sup>IM</sup> System Manager 6.0 2155 PM Help   About   Change Password   Log off tation Details Commit Cancel General * Adaptation name: CM1 Module name: DigitConversionAdapter Module parameter: Instructure instr	
	<ul> <li>Elements</li> <li>Events</li> <li>Events</li> <li>Groups &amp; Roles</li> <li>Licenses</li> <li>Routing</li> <li>Domains</li> <li>Locations</li> <li>Adaptations</li> <li>SIP Entities</li> <li>Entity Links</li> <li>Time Ranges</li> <li>Routing Policies</li> <li>Dial Patterns</li> </ul>	Avaya Aura <sup>IM</sup> System Manager 6.0 2155 PM Help   About   Change Password   Log off tation Details Commit Cancel General * Adaptation name: CM1 Module name: DigitConversionAdapter Module parameter: osrcd=avaya.com odstd=avaya.c Egress URI Parameters: Notes: Calls between SM and CM1 Digit Conversion for Incoming Calls to SM Add Remove	
	<ul> <li>Elements</li> <li>Events</li> <li>Groups &amp; Roles</li> <li>Licenses</li> <li>Routing</li> <li>Domains</li> <li>Locations</li> <li>Adaptations</li> <li>SIP Entities</li> <li>Entity Links</li> <li>Time Ranges</li> <li>Routing Policies</li> </ul>	Avaya Aura <sup>IM</sup> System Manager 6.0 Itation Details Adaptation Details General • Adaptation name: CM1 Module name: DigitConversionAdapter Module parameter: osrcd=avaya.com odstd=avaya.c Egress URI Parameters: Notes: Calls between SM and CM1 Digit Conversion for Incoming Calls to SM Add Remove 3 Items Refresh Filter: Enable	
	<ul> <li>Elements</li> <li>Events</li> <li>Groups &amp; Roles</li> <li>Licenses</li> <li>Routing</li> <li>Domains</li> <li>Locations</li> <li>Adaptations</li> <li>SIP Entities</li> <li>Entity Links</li> <li>Time Ranges</li> <li>Routing Policies</li> <li>Dial Patterns</li> <li>Regular Expressions</li> <li>Defaults</li> <li>Security</li> </ul>	Avaya Aura <sup>IM</sup> System Manager 6.0 Itation Details Adaptation Details General • Adaptation name: CM1 Module name: DigitConversionAdapter Module parameter: osrcd=avaya.com odstd=avaya.c Egress URI Parameters: Notes: Calls between SM and CM1 Digit Conversion for Incoming Calls to SM Add Remove 3 Items Refresh Filter: Enable	
	<ul> <li>Elements</li> <li>Events</li> <li>Groups &amp; Roles</li> <li>Licenses</li> <li>Routing</li> <li>Domains</li> <li>Locations</li> <li>Adaptations</li> <li>SIP Entites</li> <li>Entity Links</li> <li>Time Ranges</li> <li>Routing Policies</li> <li>Dial Patterns</li> <li>Regular Expressions</li> <li>Defaults</li> </ul>	Avaya Aura IIII System Manager 6.0       2155 PM         Help   About   Change Password   Log off         Adaptation Details       Commit         General          • Adaptation name: CM1         • Module name: DigitConversionAdapter III         • Module parameter: Issrcd=avaya.com odstd=avaya.ce         Egress URI Parameters:       Image: Digit Conversion for Incoming Calls to SM         Add       Filter: Enable         Items: Refresh       Item: Calls detined for CM1 for duplicd	
	<ul> <li>Elements</li> <li>Events</li> <li>Events</li> <li>Groups &amp; Roles</li> <li>Licenses</li> <li>Routing</li> <li>Domains</li> <li>Locations</li> <li>Adaptations</li> <li>SIP Entities</li> <li>Entity Links</li> <li>Time Ranges</li> <li>Routing Policies</li> <li>Dial Patterns</li> <li>Regular Expressions</li> <li>Defaults</li> <li>System Manager Data</li> <li>Users</li> </ul>	Avaya Aura "System Manager 6.0 Help   About   Change Password   Log off Help   About   Change Password   Log off Commit Cancel Adaptation Details General Adaptation name: CM1 Module name: DigitConversionAdapter Module parameter: osrcd=avaya.com odstd=avaya.c Egress URI Parameters: Notes: Calls between SM and CM1 Digit Conversion for Incoming Calls to SM Add Remove Sitems Refresh Filter: Enable Filter: Enable Filter: Enable Matching Pattern Min Max Delete Digits Insert Digits Address to modify Notes Filter: Enable Filter: Enable Substantion Calls destined for CM1 inford uplical Substantion Calls destined for CM1 for duplical Substantion Calls destined for CM1 inford uplical Substantion Calls destined for CM1 for duplical Substantion Calls destined for CM2 for duplical Substantin Calls destined for CM2 for duplical Substantion Calls d	
	<ul> <li>&gt; Elements</li> <li>&gt; Events</li> <li>&gt; Groups &amp; Roles</li> <li>Licenses</li> <li>&gt; Routing</li> <li>&gt; Domains</li> <li>Locations</li> <li>&gt; Adaptations</li> <li>SIP Entities</li> <li>Entity Links</li> <li>Time Ranges</li> <li>Routing Policies</li> <li>&gt; Dial Patterns</li> <li>Regular Expressions</li> <li>&gt; Defaults</li> <li>&gt; Security</li> <li>&gt; System Manager Data</li> </ul>	Avaya Aura III System Manager 6.0       2155 PM         Help   About   Change Password   Log off         Adaptation Details       Commit         Adaptation Details       Commit         General       • Adaptation name: [DipitConversionAdapter]         Module name:       DipitConversionAdapter]         Module parameter:       Isrcd=avaya.com odstd=avaya.com         Digit Conversion for Incoming Calls to SM         Add       Filter: Enable         Items:       Filter:         Istems:       Filter:         Istems:       Pilter         Istems:       Pilter:	
	<ul> <li>Elements</li> <li>Events</li> <li>Events</li> <li>Groups &amp; Roles         <ul> <li>Licenses</li> <li>Routing</li> <li>Domains</li> <li>Lacations</li> <li>Adaptations</li> <li>SIP Entities</li> <li>Entity Links</li> <li>Time Ranges</li> <li>Routing Policies</li> <li>Dial Patterns</li> <li>Regular Expressions</li> <li>Defaults</li> <li>Security</li> <li>System Manager Data</li> <li>Users</li> </ul> </li> <li>Help</li> <li>Help for Adaptation Details fields</li> <li>Help for Committing</li> </ul>	Avaya Aura "System Manager 6.0 Help   About   Change Password   Log off Help   About   Change Password   Log off Commit Cancel Adaptation Details General Adaptation name: CM1 Module name: DigitConversionAdapter Module parameter: osrcd=avaya.com odstd=avaya.c Egress URI Parameters: Notes: Calls between SM and CM1 Digit Conversion for Incoming Calls to SM Add Remove Sitems Refresh Filter: Enable Filter: Enable Filter: Enable Matching Pattern Min Max Delete Digits Insert Digits Address to modify Notes Filter: Enable Filter: Enable Substantion Calls destined for CM1 inford uplical Substantion Calls destined for CM1 for duplical Substantion Calls destined for CM1 inford uplical Substantion Calls destined for CM1 for duplical Substantion Calls destined for CM2 for duplical Substantin Calls destined for CM2 for duplical Substantion Calls d	
	<ul> <li>Elements</li> <li>Events</li> <li>Groups &amp; Roles</li> <li>Licenses</li> <li>Routing</li> <li>Domains</li> <li>Locations</li> <li>Adaptations</li> <li>SIP Entitles</li> <li>Entity Links</li> <li>Time Ranges</li> <li>Routing Policies</li> <li>Dial Patterns</li> <li>Regular Expressions</li> <li>Defaults</li> <li>System Manager Data</li> <li>Users</li> <li>Help</li> <li>Help for Adaptation Details fields</li> </ul>	Adaya Aura " System Manager 6.0   The provide	
	<ul> <li>Elements</li> <li>Events</li> <li>Events</li> <li>Groups &amp; Roles         <ul> <li>Licenses</li> <li>Routing</li> <li>Domains</li> <li>Lacations</li> <li>Adaptations</li> <li>SIP Entities</li> <li>Entity Links</li> <li>Time Ranges</li> <li>Routing Policies</li> <li>Dial Patterns</li> <li>Regular Expressions</li> <li>Defaults</li> <li>Security</li> <li>System Manager Data</li> <li>Users</li> </ul> </li> <li>Help</li> <li>Help for Adaptation Details fields</li> <li>Help for Committing</li> </ul>	Avaya Aura " System Manager 6.0   Telp   About   Change Password   Log off   Adoption Details     Adoption Details     Ceneral     * Adaptotion name:     * Module name:   Digit Conversion for Incoming Calls to SM   Add     Filter:     Totoms Refresh     Filter:     * Addition and the filter in the source details destined for CM1 for dupliced     * Matching Pattern Nin Nax Delete Digits Insert Digits Address to modify Notes     * Hatching Pattern Nin Nax Delete Digits Insert Digits Address to modify Notes     * Hatching Pattern Nin Nax Delete Digits Insert Digits Address to modify Notes     * Hatching Pattern Nin Nax Delete Digits Insert Digits Address to modify Notes     * Hatching Pattern Nin Nax Delete Digits Insert Digits Address to modify Notes     * Hatching Pattern Nin Nax Delete Digits Insert Digits Address to modify Notes     * Hatching Pattern Nin Nax Delete Digits Insert Digits Address to modify Notes     * Hatching Pattern Nin Nax Delete Digits Insert Digits Address to modify Notes     * Hatching Filter:     * Egress URL Parameters:     * Stars Refresh     * Hatching Pattern Nin Nax Delete Digits Insert Digits Address to modify Notes     * Hatching Pattern Nin Nax Delete	
	<ul> <li>Elements</li> <li>Events</li> <li>Events</li> <li>Groups &amp; Roles         <ul> <li>Licenses</li> <li>Routing</li> <li>Domains</li> <li>Lacations</li> <li>Adaptations</li> <li>SIP Entities</li> <li>Entity Links</li> <li>Time Ranges</li> <li>Routing Policies</li> <li>Dial Patterns</li> <li>Regular Expressions</li> <li>Defaults</li> <li>Security</li> <li>System Manager Data</li> <li>Users</li> </ul> </li> <li>Help</li> <li>Help for Adaptation Details fields</li> <li>Help for Committing</li> </ul>	Avaya Aura "" System Manager 6.0   Tel patient of the password plage for the plage for	
	<ul> <li>Elements</li> <li>Events</li> <li>Events</li> <li>Groups &amp; Roles         <ul> <li>Licenses</li> <li>Routing</li> <li>Domains</li> <li>Lacations</li> <li>Adaptations</li> <li>SIP Entities</li> <li>Entity Links</li> <li>Time Ranges</li> <li>Routing Policies</li> <li>Dial Patterns</li> <li>Regular Expressions</li> <li>Defaults</li> <li>Security</li> <li>System Manager Data</li> <li>Users</li> </ul> </li> <li>Help</li> <li>Help for Adaptation Details fields</li> <li>Help for Committing</li> </ul>	Avaya Aura <sup>IIII</sup> System Manager 6.0     Itel planut ( change Password ) Log off     Adaptation Details     Commit Cancel     Image: Cancel <t< th=""><th></th></t<>	

Step			Desc	ription			
5.	Adaptations – Con The following scree		daptations	used for	second C	Communica	tion Manager.
	Αναγα	Avaya Aura™ Sy	stem Mana	ger 6.0		2:55 PM	ast Logged on at December 13, 2011 out   Change Password   <b>Log of</b>
	Home / Routing / Adaptations / Adap Elements Events	ptation Details Adaptation Details					Commit Cance
	Groups & Roles     Licenses     Routing     Domains     Locations     Adaptations     SIP Entities     Entity Links     Time Ranges     Routing Policies     Dial Patterns     Regular Expressions     Defaults     Security     System Manager Data	Digit Conversion for In Add Remove 1 Item Refresh Matching Pattern +6665011	Module parameter ess URI Parameters Notes	DigitConversion osrcd=avaya1.c	om odstd=avaya1	Address to modify	Filter: Enable Notes Inbound call from a duplicate exte
	Users      Help Help for Adaptation Details fields Help for Committing configuration changes	Select : All, None Digit Conversion for Ou Add Remove 1 Item Refresh Matching Pattern	Min Max	Delete Digits	Insert Digits	Address to modify	Filter: Enable Notes
			Min Max * 8 * 8	Delete Digits * 1	Insert Digits	Address to modify destination 💌	

Step 6.	-	8	
	The following screen	8	
	-	shot shows the Session Manager entry	configured for this compliance
	test:	6 5	
	• Name – Any desc	riptive name	
	•	<b>ress</b> – IP Address of the Network Inter	face for the Session Manager
	-		e
		<i>Session Manager</i> from the drop-down	
		ed from the list of locations configure	
		ected the time zone from a drop-down	
	• In the SIP Link M	onitoring section, SIP Link Monitori	ng field was set to <i>Link</i>
	Monitoring Enab	led	
	• The Entity Links	section displays the links configured f	for this compliance testing. Entity
	links are displayed	d only after the links are established. T	he entity link configuration is
	shown in Steps 11	- 14. Additional entity links can be de	efined upon configuration of
	additional entities.		
	• The <b>Port</b> section of	displays the ports used for each protoco	ol/domain configuration used for
		sting. Two separate domains (avaya.co	0
	-	unication Managers used for this com	•
		the configuration done in <b>Step 2</b> . Note	
		separate domains.	e that separate port numbers are
	required to number	separate domains.	
	Δνανα	Avaya Aura™ System Manager 6.0	Welcome, <b>admin</b> Last Logged on at December 13, 2010 11:13 AM
		· · · -	Help   About   Change Password   Log off
	Home / Routing / SIP Entities / SIP	stry Details SIP Entity Details	Commit Cancel
	▶ Events	General	commit canter
	Groups & Roles Licenses	* Name: SM1	
	Routing Domains	* FQDN or IP Address: 10.80.120.28 Type: Session Manager	
	Locations Adaptations	Notes:	
	SIP Entities Entity Links	Location: Location 1 Subnet 10.80.120.>	×
	Time Ranges	Outbound Proxy:	×
	Routing Policies Dial Patterns	Time Zone: America/Denver Credential name:	
	Regular Expressions Defaults	SIP Link Monitoring	
	<ul> <li>▶ Security</li> <li>▶ System Manager Data</li> </ul>	SIP Link Monitoring: Link Monitoring Enabled	×
	► Users	<ul> <li>Proactive Monitoring Interval (in seconds): 900</li> <li>Reactive Monitoring Interval (in seconds): 120</li> </ul>	
	Help	* Number of Retries: 1	
	Help for SIP Entity Details fields Help for Committing	Entity Links Add Remove	
	configuration changes	4 Items   Refresh	Filter: Enable
		SIP Entity 1 Protocol Port SIP Entity 2	Port Trusted
		SM1         TCP         \$ 5060         911Enable_CM2           SM1         TCP         \$ 5062         911Enable_CM1	× * \$5060 V × * \$5062 V
		SM1         TCP         \$5062         \$1161abic_CHA           SM1         TCP         \$ 5060         \$911EGWPrimary	× \$5060
		SM1 - TCP - * 5060 911EGWBackup	▼ * 5060 <b>▼</b>
		Select : All, None	
		Add Remove	
		2 Items   Refresh	Filter: Enable
		Port         Protocol         Default Domain           5060         TCP •         avaya.com •	Notes
		S062 TCP v avaya.com v	
		Select : All, None	

Step		Description	
7.	SIP Entity – Continue	d	
	The following screen sh	ows the SIP Entity configured for the first (	Communication Manager
	along with the entity lin	k to the Session Manager:	_
	• Name – Any descri	-	
		ess – IP address of the CLAN interface for the	he Communication
	Manager		
	• Type – Selected CM	1 from the drop-down list	
		ted CM1 from the drop-down list of adapta	tions configured in Step 4
	-	from the drop-down list of locations config	<b>e</b> 1
		ed the time zone from a drop-down list	
		nitoring section, <b>SIP Link Monitoring</b> field	was set to Use Session
	Manager Configure	•	was set to ese session
	0	ection displays the links configured for this	compliance testing Entity
	•	only after the links are established. The entit	
	shown in <b>Step 11</b>	my after the miks are established. The entit	y link configuration is
	snown in Step 11		
		Welco	me, <b>admin</b> Last Logged on at January 3, 2011 11:37
		aya Aura™ System Manager 6.0 waa	Help   About   Change Password   Log off
	Home / Routing / SIP Entities / SIP Entity De	tails	
	) Events	Entity Details	Commit Cancel
	Groups & Roles	• Name: 911Enable_CM1	
	Licenses ▼ Routing	* FQDN or IP Address: 10.80.130.102	
	Domains	Type: CM	
	Locations Adaptations	Notes: Entity for calls to 911Enable CM1	
	SIP Entities	Adaptation: CM2	
	Entity Links Time Ranges	Location: Loc1 10.80.130.x	
	Routing Policies Dial Patterns	Time Zone: America/Denver	
	Regular Expressions	Override Port & Transport with DNS SRV:  * SIP Timer B/F (in seconds):  4	
	Defaults Security	Credential name:	
	▶ System Manager Data	Call Detail Recording: none 💌	
		P Link Monitoring	
	Help Help for SIP Entity Details fields	SIP Link Monitoring: Use Session Manager Configuration 💌	
	Help for Committing		
	configuration changes En	tity Links d Remove	
	1	Item   Refresh	Filter: Enable
		SIP Entity 1 Protocol Port SIP Entity 2	Port Trusted
		SM1 - TCP - * 5060 911Enable_CM1 -	* 5060
	s	elect : All, None	

Step		Description	
8.	-	inued en shows the SIP Entity configured for the second Communi- the entity link to the Session Manager. The entity link is dis	
	Αναγα	Avaya Aura <sup>™</sup> System Manager 6.0 <sup>Welcome, admin Last Logged on</sup> AM Help   About   Char	at January 3, 2011 11:37 nge Password   <b>Log off</b>
	Home / Routing / SIP Entities / SIP	Entity Details	
	<ul><li>▶ Elements</li><li>▶ Events</li></ul>	SIP Entity Details	Commit Cancel
	Groups & Roles	* Name: 911Enable_CM2	
	Licenses Routing	* FQDN or IP Address: 10.80.111.31	
	Domains	Туре: СМ	
	Locations	Notes: CLAN Entry for CM2	
	Adaptations	,	
	SIP Entities Entity Links	Adaptation: CM1	
	Time Ranges	Location: Location 1 Subnet 10.80.111.x 💌	
	Routing Policies	Time Zone: America/Denver	
	Dial Patterns	Override Port & Transport with DNS SRV: 🛛	
	Regular Expressions	* SIP Timer B/F (in seconds): 4	
	Defaults Security	Credential name:	
	System Manager Data	Call Detail Recording: none 💌	
	▶ Users		
	Help	SIP Link Monitoring SIP Link Monitoring: Use Session Manager Configuration	
	Help for SIP Entity Details fields		
	Help for Committing		
	configuration changes	Add Remove	
		1 Item   Refresh	Filter: Enable
		SIP Entity 1         Protocol         Port         SIP Entity 2         Port	Trusted
		SM1 ▼         TCP ▼         * 5062         911Enable_CM2         ▼         \$5062	V
		Select : All, None	

Step			Descri	ption			
9.	<b>SIP Entity – Contin</b> The following scree entity link to the Ses	n shows the SIP E					g with the
	AVAYA	Avaya Aura™ Syste	m Manage	r 6.0	11:13 AM	l <b>min</b> Last Logged on at ( lp   About   Change Pa	
	Home / Routing / SIP Entities / SIP	ntity Details					
	<ul><li>Elements</li><li>Events</li></ul>	SIP Entity Details General				c	Commit Cancel
	Groups & Roles     Licenses		* Name: 91	LEGWPrimary			
	▼ Routing	* FQDN	or IP Address: 10	80.130.200			
	Domains		Type: 💽	her 🗾			
	Adaptations	R	Notes: 91	L EGW Primary			
	SIP Entities		Adaptation:	•			
	Entity Links Time Ranges		Location: Lo		•		
	Routing Policies		Time Zone: An	erica/Denver			
	Dial Patterns	Override Port & Transport	with DNS SRV: 🛛				
	Regular Expressions Defaults	* SIP Timer B/	F (in seconds): 4				
	> Security	Cr	edential name:				
	<ul> <li>System Manager Data</li> <li>Users</li> </ul>	Call De	tail Recording: no	ne 💌			
	Help Help for SIP Entity Details fields	SIP Link Monitoring SIP L	ink Monitoring: 🛛	e Session Manager Configu	ration 💌		
	Help for Committing configuration changes	Add Remove					
		1 Item   Refresh					Filter: Enable
		SIP Entity 1 Protoco	ol Port	SIP Entity 2		Port	Trusted
		SM1 TCP -	* 5060	911EGWPrimary	•	* 5060	<b>N</b>
		Select : All, None					
I							

Step		Description	
10.	SIP Entity – Conti	nued	
	The following scree	en shows the SIP Entity configured for the backup EGW along	g with the
		ssion Manager. The entity link is displayed in Step 14.	
		August August TM Culetare Manager C August Aug	at December 13, 2010
	FIVELYEL	Avaya Aura <sup>™</sup> System Manager 6.0	Password   Log off
	Home / Routing / SIP Entities / SIP	Entity Details	
	▶ Elements	SIP Entity Details	Commit Cancel
	▶ Events	General	
	Groups & Roles	* Name: 911EGWBackup	
	Licenses Routing	* FQDN or IP Address: 10.80.130.201	
	Domains	Type: Other	
	Locations	Notes: Backup 911 Emergency Gateway	
	Adaptations SIP Entities		
	Entity Links	Adaptation:	
	Time Ranges	Location: Loc1 10.80.130.x	
	Routing Policies	Time Zone: America/Denver	
	Dial Patterns Regular Expressions	Override Port & Transport with DNS SRV:	
	Defaults	* SIP Timer B/F (in seconds): 4	
	▶ Security	Credential name:	
	<ul> <li>System Manager Data</li> <li>Users</li> </ul>	Call Detail Recording: none 💌	
	V users	SIP Link Monitoring	
	Help	SIP Link Monitoring: Use Session Manager Configuration 💌	
	Help for SIP Entity Details fields		
	Help for Committing configuration changes	Entity Links	
		Add Remove	
		1 Item   Refresh	Filter: Enable
		SIP Entity 1         Protocol         Port         SIP Entity 2         Port	Trusted
		SM1 • TCP • • 5060 911EGWBackup • 5060	V
		Select : All, None	

Step	Description
<u>Step</u> 11.	<ul> <li>Entity Links The following screen shows the SIP Entity Link configured between Session Manager and first Communication Manager. This link along with other links also appears in the screen shown in Step 6. In the left pane under Routing, click on "Entity Links". On the Entity Links page, click on SM1-911Enable_CM1 entity (not shown) to display the screen below:</li> <li>Name – Any descriptive name for the link between Session Manager and first Communication Manager</li> <li>SIP Entity 1 – SIP entity link for Session Manager displayed in Step 6. SIP Entity 1 field always contain the Session Manager entity.</li> <li>SIP Entity 1 Port – Set to 5060</li> <li>SIP Entity 2 –Selected the SIP Entity administered in Step 7 for the first Communication Manager</li> <li>SIP Entity 2 Port – Set to 5060</li> <li>Trusted – A check in the box indicates that this is a trusted link</li> <li>Protocol – Selected TCP from the drop-down list.</li> </ul>
	Avaya Aura™ System Manager 6.0       Welcome, admin Last Logged on at January 3, 2011 11:37         Home / Routing / Entity Links       Help   About   Change Password   Log off         Entity Links       Commit Cancel         > Events       Commit Cancel         > Groups & Roles       Commit Cancel
	Licenses <ul> <li>Routing</li> <li>I Item Refresh</li> <li>SIP Entities</li> </ul> Filter: Enable <ul> <li>SIP Entities</li> </ul>
12.	Entity Links – Continued The following screen shows the SIP Entity Link configured between Session Manager and second Communication Manager Entity displayed in Step 8.
	Welcome, admin Last Logged on at January 3, 2011 11:137         AM         Home / Routing / Entity Links
	> Elements     Commit     Cancel       > Events
	Routing       1 Item Refresh       Filter: Enable         Domains       Name       SIP Entity       Protocol       Port       SIP Entity 2       Port       Trusted       Notes         Adaptations       SIP Entities       * SM1_911Enable_C       * SM1 *       TCP *       * S062       * 911Enable_CM2       * 5062       SM to 911Enable

Step		Description	
13.		ontinued een shows the SIP Entity Link configured tity displayed in Step 9.	between Session Manager and
	Home / Routing / Entity Links	Avaya Aura™ System Manager 6.0	Welcome, <b>admin</b> Last Logged on at December 13, 2010 11:13 AM Help   About   Change Password   Log off
	<ul> <li>Elements</li> <li>Events</li> <li>Groups &amp; Roles</li> </ul>	Entity Links	Commit Cancel
	Cicenses   Routing  Domains  Locations  Adaptations  abo  choice  Cicentered  Cicentered Cicentered  Cicentered  Cicentered  Cicentered  C	1 Item Refresh         Name       SIP Entity 1       Protocol       Port       SIP Entity 2         * SM1_911EGWPrima       * SM1 •       TCP •       * 5060       * 911EGWPrimary	Filter: Enable Port Trusted Notes  5060 F
14.		ontinued een shows the SIP Entity Link configured ity displayed in Step 10.	between Session Manager and
	AVAYA	Avaya Aura™ System Manager 6.0	Welcome, <b>admin</b> Last Logged on at December 13, 2010 11:21 AM Help   About   Change Password   <b>Log off</b>
	Home / Routing / Entity Links	Entity Links	Commit Cancel
	✓ Routing Domains Locations Adaptations SIP Entities	1 Item Refresh       Name     SIP Entity 1     Protocol     Port     SIP Entity 2       * SM1_E911EGWBack     * SM1 ▼     TCP ▼     * 5060     * 911EGWBackup       4	Filter: Enable       Port     Trusted       Notes       • 5060       • 8ackup E911 Ga
15.		een displays the time range configured for inges can be entered if required.	this compliance testing.
	Ανάγα	Avaya Aura™ System Manager 6.0	Welcome, <b>admin</b> Last Logged on at July 9, 2010 10:54 AM Help   About   Change Password   <b>Log off</b>
	Home / Routing / Time Ranges   Elements  Events  Groups & Roles	Time Ranges Edit New Duplicate Delete More Actions •	Commit
	Licenses  Contemp  Co	2 Items   Refresh         Name       Mo       Tu       We       Th       Fr       Sa       Su         24/7       Image: Select : All, None       Image: Select : All, None       Image: Select : All, None       Image: Select : All, None	

up		Description										
<b>Step</b> 16.	<b>Routing Policies D</b>	Details										
	0	en displays the Routing Policy configured f	for calls to first Communication									
	Manager:											
	-		11 1 1 1 4 4									
	• In the <b>General</b> section, a descriptive name for the policy was added along with notes in the antional Notes field											
	the optional No	otes field										
	• In the <b>SIP Entity as Destination</b> section, SIP Entity configured in <b>Step 7</b> was selected											
		Day section, time range configured in Step	e i									
		anking is used to set the order in which Ses										
		•	0									
	routing policy t	to make a routing decision. A ranking of 0 i	indicates the highest priority.									
	• The Dial Patter	rns section displays the patterns configured	d for this compliance testing.									
		re displayed only after the pattern is configu	1 0									
		once defined can be added or deleted from t										
			ne Routing i oncy Details pa									
	too.											
	AVAVA	Avaya Aura™ System Manager 6.0	Welcome, <b>admin</b> Last Logged on at December 13, 2010 2:55 PM									
	· · · · · · · · · · · · · · · · · · ·		Help   About   Change Password   Log off									
	Home / Routing / Routing Policies /	Routing Policy Details										
	▶ Elements	Routing Policy Details	Commit Cancel									
	<ul> <li>Events</li> <li>Groups &amp; Roles</li> </ul>	General										
	Licenses	* Name: To911EnableCM1										
	▼ Routing	Disabled:										
	Domains	Notes: Routing Policy for calls to CM1										
	Locations Adaptations											
	SIP Entities	SIP Entity as Destination										
	Entity Links	Select										
		Name FQDN or IP Address Type	Notes									
	Time Ranges											
	Time Ranges Routing Policies Dial Patterns	911Enable_CM1 10.80.130.102 CM	Entity for calls to 911Enable CM1									
	Routing Policies											
	Routing Policies Dial Patterns Regular Expressions Defaults	Time of Day										
	Routing Policies Dial Patterns Regular Expressions Defaults > Security	Time of Day           Add         Remove         View Gaps/Overlaps	Entity for calls to 911Enable CM1									
	Routing Policies Dial Patterns Regular Expressions Defaults	Time of Day Add Remove View Gaps/Overlaps 1 Item Refresh	Entity for calls to 911Enable CM1 Filter: Enable									
	Routing Policies         Dial Patterns         Regular Expressions         Defaults         > Security         > System Manager Data         > Users	Time of Day       Add     Remove       View Gaps/Overlaps       1 Item     Refresh       Ranking     1 Name       Ranking     1 Name	Entity for calls to 911Enable CM1 Filter: Enable									
	Routing Policies         Dial Patterns         Regular Expressions         Defaults         > Security         > System Manager Data	Time of Day Add Remove View Gaps/Overlaps 1 Item Refresh	Entity for calls to 911Enable CM1 Filter: Enable									
	Routing Policies         Dial Patterns         Regular Expressions         Defaults         > Security         > System Manager Data         > Users         Help         Help for Routing Policy Details fields         Help for SIP Entity List	Remove       View Gaps/Overlaps         1 Item Refresh       Ranking 1 Name 2 Mon Tue Wed Thu Fri 54         2       24/7       R R R R R R R R R R R R R R R R R R R	Entity for calls to 911Enable CM1 Filter: Enable									
	Routing Policies         Dial Patterns         Regular Expressions         Defaults         > Security         > System Manager Data         Users         Help         Help for Routing Policy Details fields         Help for SIP Entity List         Help for Time Range List	Remove       View Gaps/Overlaps         1 Item Refresh       Ranking 1 Name 2 Mon Tue Wed Thu Fri Sa         2       24/7       Image: Compare the same th	Entity for calls to 911Enable CM1 Filter: Enable									
	Routing Policies         Dial Patterns         Regular Expressions         Defaults         > Security         > System Monager Data         > Users         Help         Help for Routing Policy Details fields         Help for SIP Entity List         Help for Time Range List         Help for Pattern List	Remove       View Gaps/Overlaps         1 Item Refresh       Ranking 1 Name 2 Mon Tue Wed Thu Fri Su         2       24/7       Ø       Ø         Select : All, None       Ø       Ø       Ø         Dial Patterns       Add       Remove       Ø	Entity for calls to 911Enable CM1 Filter: Enable									
	Routing Policies         Dial Patterns         Regular Expressions         Defaults         > Security         > System Manager Data         Users         Help         Help for Routing Policy Details fields         Help for SIP Entity List         Help for Time Range List	Remove       View Gaps/Overlaps         1 Item Refresh       Ranking 1 Name 2 Mon Tue Wed Thu Fri Su         2       24/7       Ø       Ø         Select : All, None       Ø       Ø       Ø         Dial Patterns       Add       Remove       Ø	Entity for calls to 911Enable CM1 Filter: Enable									
	Routing Policies         Dial Patterns         Regular Expressions         Defaults         > Security         > System Manager Data         > Users         Help         Help for Routing Policy Details fields         Help for SIP Entity List         Help for Time Range List         Help for Regular Expressions List	Time of Day         Add       Remove       View Gaps/Overlaps         1 Item       Refresh         Ranking       1         Name       2         You       Wed         Thu       Fri         Select : All, None         Dial Patterns         Add         Remove         4 Items   Refresh	Entity for calls to 911Enable CM1 Filter: Enable at Sun Start Time End Time Notes O0:00 23:59 Time Range 24/7									
	Routing Policies         Dial Patterns         Regular Expressions         Defaults         > Security         > System Manager Data         > Users         Help         Help for Routing Policy Details fields         Help for SIP Entity List         Help for Time Range List         Help for Regular Expressions List         Help for Committing	Time of Day         Add       Remove       View Gaps/Overlaps         1 Item       Refresh         Ranking       Name       2         2       24/7       Image: Comparison of the second seco	Entity for calls to 911Enable CM1         Filter: Enable         at       Sun       Start Time       End Time       Notes         at       Sun       O0:00       23:59       Time Range 24/7         Image: Start Time       Filter: Enable       Filter: Enable         Image: Start Time       Filter: Enable       Filter: Enable         Image: Start Time       Notes       Filter: Enable         Driginating Location       Notes       Calls to CM2 with Prefix 2									
	Routing Policies         Dial Patterns         Regular Expressions         Defaults         > Security         > System Manager Data         > Users         Help         Help for Routing Policy Details fields         Help for SIP Entity List         Help for Time Range List         Help for Regular Expressions List         Help for Committing	Time of Day         Add       Remove       View Gaps/Overlaps         1 Item Refresh       Image: Constraint of the second	Entity for calls to 911Enable CM1         Filter: Enable         at       Sun       Start Time       End Time       Nates         at       Sun       Start Time       End Time       Nates         at       Sun       00:00       23:59       Time Range 24/7         at       Sun       O0:00       23:59       Time Range 24/7         Filter: Enable         Driginating Location         Notes         cols to CM2 with Prefix 2         cols destined for CM1									
	Routing Policies         Dial Patterns         Regular Expressions         Defaults         > Security         > System Manager Data         > Users         Help         Help for Routing Policy Details fields         Help for SIP Entity List         Help for Time Range List         Help for Regular Expressions List         Help for Committing	Time of Day         Add       Remove       View Gaps/Overlaps         1 Item Refresh       Image: Colspan="2">Ranking 1 Name 2 Mon Tue Wed Thu Fri Sate         2       24/7       Image: Colspan="2">Image: Colspan="2">Image: Colspan="2">Colspan="2"         Dial Patterns       Image: Colspan="2">Add Remove         4 Items Refresh       Image: Colspan="2">Image: Colspan="2">Image: Colspan="2"         2 26655       8       8      ALL-       Lu         2 666502       7       7       avaya.com       Lu         666502       7       7       avaya.com       Lu	Entity for calls to 911Enable CM1         Filter: Enable         at       Sun       Start Time       End Time       Notes         at       Sun       O0:00       23:59       Time Range 24/7         Image: Start Time       Filter: Enable       Filter: Enable         Image: Start Time       Filter: Enable       Filter: Enable         Image: Start Time       Notes       Filter: Enable         Driginating Location       Notes       Calls to CM2 with Prefix 2									

р							scrip	tion						
]	<b>Routing Policies</b> The following sc for calls to secon	reen d	isplays	the	Rou	ting P		and	cor	resp	ond	ing Dia	l Patter	rns config
	Αγαγα	Avay	⁄a Aura™	1 Sys	stem	Mana	ger 6.	0				55 PM		it December 13, 2010 Password   <b>Log off</b>
	Home / Routing / Routing Policies /	Routing Poli	y Details											
	<ul> <li>Elements</li> <li>Events</li> </ul>	Routin	Routing Policy Details										l	Commit Cancel
	▶ Groups & Roles	Gene	ral											
	Licenses <b>T</b> Routing					* Name:	To911En	ableCM2						
	Domains					Disabled:								
	Locations					Notes:	Routing P	olicy for	calls to r	CM2				
	Adaptations													
	SIP Entities	SIP E	ntity as Des	tinatio	n									
_	Entity Links	Select												
_	Time Ranges	Nam	•		F	QDN or IP A	ddress				Туре	Notes	:	
_	Routing Policies Dial Patterns	911Er	able_CM2		10	.80.111.31				(	СМ	CLAN E	Entry for CM2	
_	Regular Expressions		( )											
	Defaults	1	of Day											
	▶ Security	Add	Remove	Vie	w Gaps/	Overlaps								
	▶ System Manager Data	1 Ite	n   Refresh											Filter: Enable
	▶ Users		Ranking 1 /	Nam	e 2	Mon T	ue We	d Thu	Fri	Sat	Sun	Start Time	End Time	Notes
	Help		0	24/7		V	V V	~	~	V	~	00:00	23:59	Time Range 24/7
	Help for Routing Policy Details fields	Selec	t : All, None											
	Help for SIP Entity List	Dial P	atterns											
	Help for Time Range List Help for Pattern List	Add	Remove											
	Help for Regular Expressions List	Auu	- Normove											
	Help for Committing	1 Ite	n   Refresh											Filter: Enable
	configuration changes		Pattern 🔺	Min	Мах	Emerge	ncy Call	SIP D	main	Origi	inating L	ocation	Notes	
			26665	8	8		-	-ALL-		Locati	on 1 Subr	net 10.80.120.X	Calls to	CM2 with Prefix 2
		Selec	t : All, None											

				Γ	)escr	iptic	n						
	<b>cies Details -</b> g screen displa fimary EGW.				g Poli	icy a	nd c	orr	resp	ondi	ing D	ial Patte	rns config
AVAYA	Avaya Au	ıra™	Syster	n Mar	nager	6.0				We 2:5	55 PM		t December 13, 2010 Password   <b>Log off</b>
Home / Routing / Routing	Policies / Routing Policy Detail:												
Elements	Routing Policy	Details										I	Commit Cancel
<ul> <li>Events</li> <li>Groups &amp; Roles</li> </ul>	General												
Licenses				* Na	ne: To91	1EGWPrir	nary						
Routing				Disab	ed: 🗆								
Domains				Not	es: 911	Primarv G	W						
Locations Adaptations													
SIP Entities	SIP Entity a	SIP Entity as Destination											
Entity Links		Select											
Time Ranges													
Routing Policies	Name			-	r IP Addro	55				Туре		Notes	
Dial Patterns	911EGWPrimar	1		10.80.13	0.200					Other		911 EGW Primary	
Regular Expressions	Time of Day												
Defaults	Add Remo	ve	View Gap	s/Overlan	s								
<ul> <li>Security</li> <li>System Manager Data</li> </ul>													
<ul> <li>System Manager Data</li> <li>Users</li> </ul>	1 Item   Refre	sh							_				Filter: Enable
	C Ranki	<b>g</b> 1 ≜	Name 2 4	Mon	Tue	Wed	Thu	Fri	Sat	Sun	Start Tin	ne End Time	Notes
Help			24/7	1	$\checkmark$	$\checkmark$	$\checkmark$	7	1	1	00:00	23:59	Time Range 24/7
Help for Routing Policy De	tails Select : All, N	ne											
fields Help for SIP Entity List													
Help for Time Range List	Dial Pattern	5											
Help for Pattern List	Add Remo	ve											
Help for Regular Expressi	ons List	_											
Help for Committing	3 Items   Refr	esh											Filter: Enable
configuration changes	E Patter	n 🔺 I	Min Max	Emer	gency Cal	SIP	Domain	0	Iriginati	ng Locat	ion	Notes	
	303538	1	.0 10		Г	-ALL-		Lo	oc1 10.80	0.130.x		CallBack Numb	er routing to EGW
	911	3	3		Π	-ALL-		Lo	oc1 10.80	0.130.x		911 Calls	
	911	3	3			-ALL-		Lo	ocation 1	Subnet 1	0.80.111.×	911 Calls	
11	Select : All, N												

					Desc	ripti	on						
Routing Policies Details - Continued													
The following screen displays the Routing Policy and corresponding Dial Patterns confi for calls to Backup EGW.													
for calls to Back	cup EG	W.											
	A		TM C.		M				W	elcome, <b>admin</b>	Last Logged on a	t December 13, 2010	
FIVELYEL	Ava	уа Айга		stem	Manage	r 6.0			21	:55 PM Help   A	bout   Change	Password   Log off	
Home / Routing / Routing Policie	s / Routing Pol	icy Details											
Elements	Routir	ng Policy Deta	vils									Commit Cancel	
<ul> <li>Events</li> </ul>	Koudi	ig Foncy Deta									1	Connic Cancer	
Groups & Roles	Gene	eral											
Licenses	L.				* Name: Tog	911EGWB	ackup						
▼ Routing	, i				Disabled: 🗆								
Domains					Notes: Bac	kup 911	GW						
Locations													
Adaptations SIP Entities	SIP	SIP Entity as Destination											
Entity Links		Select											
Time Ranges	Sele												
Routing Policies	Nam			FQDN or IP Address Type									
Dial Patterns	911E	GWBackup		10.80.13	0.201	Other		Back	up 911 Emerger	ncy Gateway			
Regular Expressions	Time	of Day											
Defaults	Add	Remove	1 ,	/iew Gaps/	Overland								
▶ Security	Auu	Kelliove	`	new daps/	Ovenaps								
<ul> <li>System Manager Data</li> <li>Users</li> </ul>	1 Ite	em   Refresh										Filter: Enable	
V Users		Ranking	1 🔺 N	ame 2 🛋	Mon Tue	Wed	Thu	Fri S	at Sun	Start Time	End Time	Notes	
Help		1	24	/7	<u>v</u>	V	V	~	7 17	00:00	23:59	Time Range 24/7	
Help for Routing Policy Details fields	Sele	ct : All, None											
Help for SIP Entity List													
Help for Time Range List	Dial I	Patterns											
Help for Pattern List	Add	Remove											
Help for Regular Expressions Li		ems   Refresh										Filter: Enable	
Help for Committing configuration changes												Filter: Enable	
sounger adon changes		Pattern 🔺		Max	Emergency C		Domain	_	nating Loca	ition	Notes		
		303538	10	10		-ALI			0.80.130.×			er routing to EGW	
		911	3	3	Г	-AU		Loc1	0.80.130.x		911 Calls		
		911	3	3	Π.	-AU		1.44.1	on 1 Subnet	10.00.111	911 Calls		

Step		Description	
20.	originating location	<b>11</b> een displays the Dial Pattern for 911 calls along with the routing policy on and destination of the calls. The 911 calls originate from the endpoin two Communication Managers and are routed to the primary or backup	ts
	Αναγα	Avaya Aura <sup>TM</sup> System Manager 6.0 Welcome, admin Last Logged on at December 13, 2010 2:55 PM Help   About   Change Password   Log off	
	Home / Routing / Dial Patterns / Dial > Elements > Events > Groups & Roles Licenses	Pattern Details Dial Pattern Details General Pattern: 911	
	Routing     Domains     Locations     Adaptations     SIP Entities	Min: 3 Max: 3 Emergency Call: SIP Domain: -ALL-	
	Entity Links Time Ranges Routing Policies Dial Patterns Regular Expressions	Originating Locations and Routing Policies Add Remove	
	Defaults  Security  System Manager Data  Users	Filter: Enable       Originating Location Name 1 -     Originating Location Notes     Routing Policy Name     Rank 2 -     Policy Policy Disabled     Routing Policy Disabled	
	Help Help for Dial Pattern Details fields Help for Location and Routing Policy Lists	Loci 10.80.130.x         10.80.130.x         To911EGWPrimary         0         911EGWPrimary         911 Primary           Loci 10.80.130.x         10.80.130.x         To911EGWBackup         1         911EGWBackup         911EGWBackup           Location 1 Subnet 10.80.111.x         Location 1 Subnet         To911EGWBackup         1         911EGWPrimary         911FGWBackup           Location 1 Subnet 10.80.111.x         Location 1 Subnet         To911EGWBackup         1         911EGWPrimary         911FGWBackup           Select : All, None         Select : All, None         Select : All         Select : All <t< td=""><td></td></t<>	
21.		een displays the calls routed by EGW back to the Communication Mana the PRI trunk to ECRC. This happens when the ERS service is down. Avaya Aura <sup>™</sup> System Manager 6.0	ager
	Home / Routing / Dial Patterns / Dia	Help   About   Change Password   Log off Pattern Details Dial Pattern Details Commit Cancel	
	<ul> <li>Events</li> <li>Groups &amp; Roles</li> <li>Licenses</li> <li>Routing</li> <li>Domains</li> <li>Locations</li> <li>Adaptations</li> <li>SIP Entities</li> <li>Entity Links</li> <li>Time Ranges</li> <li>Routing Policies</li> <li>Dial Patterns</li> </ul>	General  Pattern: 15149048051  Min: 11  Max: 11  Emergency Call:  SIP Domain: avaya.com Notes: ECRC nu.  Originating Locations and Routing Policies Add Remove	_
	Regular Expressions Defaults > Security > System Manager Data	Add       Reinbre       Filter: Enable         1 Item : Refresh       Filter: Enable         Image: Control of the state of the s	
	Users Help	Disabled     Disabled       Loc1 10.80.130.x     10.80.130.x     To911EnableCM1     2     911Enable_CM1     Routing Policy for calls to CM1       Select : All, None	

Step		Description	
22.	The following sci	Call back from ERS reen displays the Dial Pattern used to handle the calls received by the all is routed to EGW which retrieves the extension from where the 911	
	Αναγα	Avaya Aura <sup>™</sup> System Manager 6.0 <sup>Welcome</sup> , admin Last Logged on at December 13, 2010 2:55 PM Help   About   Change Password   Log of	
23.	Home / Routing / Dial Patterns / Dial > Elements > Events > Groups & Roles Licenses > Routing Domains Locations Adaptations SIP Entitles Entity Links Time Ranges Routing Policies Dial Patterns Regular Expressions Defaults > Security > System Manager Data > Users Help Help for Dial Pattern Details finials		
23.	The following sci Manager after EC	reen displays the Dial Pattern used to route the call to first Communic GW has determined ( <b>Step 22</b> ) which extension the 911 call was origin be configured for calls destined for the second Communication Mana	ated. A
		Avaya Aura <sup>TM</sup> System Manager 6.0 Welcome, admin Last Logged on at December 13, 2:55 PM Help   About   Change Password   Log	
	Home / Routing / Dial Patterns / Dial         > Elements         > Groups & Roles         Licenses         > Routing         Domains         Locations         Adaptations         SIP Entities         Entity Links         Time Ranges         Routing Policies         Dial Patterns         Regular Expressions         Defaults         > System Manager Data         Users         Help		otes olicy o CM1 olicy
	Help for Dial Pattern Details fields	Select : All, None	) CM1

# 5. Configure Avaya Aura® Communication Manager

Two Communication Managers were used in this compliance testing. Since the configuration is similar on both the Communication Managers, this section only describes the steps to configure one Communication Manager. Differences, if any are pointed out in relevant sections. It assumes all other components of **Figure 1** have already been configured. For more detailed information on any other Communication Manager and Phone configuration shown in **Figure 1**, consult [3] through [8].

This section is divided into two parts. **Section 5.1** describes the configuration of the SIP trunks between the Communication Manager and the Session Manager and **Section 5.2** will describe the station settings to properly send Emergency Location information to the EGW via Session Manager.

The configuration of Communication Manager was performed using the System Access Terminal (SAT). After the completion of the configuration, perform a **save translation** command to make the changes permanent. For all the fields where no entry was made, default values were used.

#### 5.1. SIP Trunk Related Configuration

This section summarizes the configuration of the SIP trunks that connects the Communication Manager to Session Manager.

Step	De	scription
1.	options highlighted below are enabled. T	tomer-options command to verify that the 'he IP Trunks and ISDN-PRI options are In addition, the ISDN Feature Plus option
	display system-parameters customer-opt OPTIO	ions Page 4 of 11 NAL FEATURES
	Emergency Access to Attendant? y Enable 'dadmin' Login? y Enhanced Conferencing? y Enhanced EC500? y Enterprise Survivable Server? n Enterprise Wide Licensing? n ESS Administration? n Extended Cvg/Fwd Admin? y External Device Alarm Admin? n Five Port Networks Max Per MCC? n Flexible Billing? n Forced Entry of Account Codes? n Global Call Classification? n	IP Stations? y <b>ISDN Feature Plus? y</b> ISDN/SIP Network Call Redirection? n ISDN-BRI Trunks? y <b>ISDN-PRI? y</b> Local Survivable Processor? n Malicious Call Trace? y Media Encryption Over IP? y Mode Code for Centralized Voice Mail? n Multifrequency Signaling? y Multimedia Call Handling (Basia)? y
		Multimedia Call Handling (Basic)? y Multimedia Call Handling (Enhanced)? y Multimedia IP SIP Trunking? y n

Manager, CLAN and MEDPRO exist. The example below shows the node names will be used in the administration of other forms on Communication Manager. For the second Communication Manager, CLAN with IP address of 10.80.111.31 was used.         display node-names ip       IP NODE NAMES         Name       IP Address         SNI       10.80.120.28         CLAN-LAO2       10.80.130.102         Manager, CLAN with IP address       Fage 1 o         Name       IP Address         SNI       10.80.130.102         Mappero-1sor       10.80.130.102         Mappero-1sor       10.80.130.102         Mappero-1sor       10.80.130.102         Proof       10.80.111.100         3.       IP network region         The Communication Manager, Session Manager and VoIP (H.323/SIP) endpolocated in a single IP network region (IP network region 1) using the paramete described below. Use the display ip-network-region command to view these         The example below shows the values used for the compliance test.         • Authoritative Domain - avaya.com         Name - Any descriptive name string         • IP-IP Direct Audio (shuffling) was enabled to allow audio traffic to be se directly between IP endpoints without using media resources in the Avaya Gateway. This was done for both intra-region and inter-region IP-IP Direct This is the default setting. Shuffling can be further restricted at the truk let the Signaling Group form.         • Codec Set - S									
IP addresses used for the compliance test. These node names will be used in the administration of other forms on Communication Manager. For the second Communication Manager, CLAN with IP address of 10.80.111.31 was used.         Image: display node-names ip       IP NODE NAMES         Mame       IP Address         SMI       10.80.120.28         CLAN-LAO2       10.60.130.102         Mare       IP Address         SMI       10.60.130.102         Mapped-1807       10.60.130.105         Default       0.0.0.0         generation       10.60.130.105         proor       10.60.130.105         proor       10.60.111.100    3. IP network region The Communication Manager, Session Manager and VoIP (H.323/SIP) endpo located in a single IP network region (IP network region 1) using the paramete described below. Use the display ip-network-region command to view these The example below shows the values used for the compliance test.         •       Authoritative Domain - avaya.com         was used for first Communication Manager       •         Name - Any descriptive name string       IP-IP Direct Audio (shuffling) was enabled to allow audio traffic to be se directly between IP endpoints without using media resources in the Avaya Gateway. This was done for both intra-region and inter-region IP-IP Direct This is the default setting. Shuffling can be further restricted at the trunk I the Signaling Group form.         •       Codec Set - Set to th									
administration of other forms on Communication Manager. For the second Communication Manager, CLAN with IP address of 10.80.111.31 was used.									
Communication Manager, CLAN with IP address of 10.80.111.31 was used. display node-names ip Name IP Address SM 10.80.120.28 CLAN-JAO2 10.80.130.102 MEDFRO-IBO7 10.80.130.102 MEDFRO-IBO7 10.80.130.10 Default 0.0.0.0 Gateway1 10.80.130.1 proct 10.80.130.1 proct 10.80.111.100 3. IP network region The Communication Manager, Session Manager and VoIP (H.323/SIP) endpo located in a single IP network region (IP network region 1) using the parameted described below. Use the display ip-network-region command to view these The example below shows the values used for the compliance test. • Authoritative Domain – avaya.com was used for first Communication M. and avaya1.com for second Communication Manager • Name – Any descriptive name string • IP-IP Direct Audio (shuffling) was enabled to allow audio traffic to be se directly between IP endpoints without using media resources in the Avaya Gateway. This was done for both intra-region and inter-region IP-IP Direct This is the default setting. Shuffling can be further restricted at the trunk la the Signaling Group form. • Codec Set - Set to the IP codec set to be used for calls within this IP network region. In this case, IP codec set 1 was selected. MEDIA PARMETERS Intra-region IP-IP Direct Audio: yes Codec Set 1 Intra-region IP-IP Direct Audio: yes Codec Set 1 Intra-region IP-IP Direct Audio: yes Code Code 1 I IP NETWORK REGION MEDIA PARMETERS Intra-region IP-IP Direct Audio: yes Code Code 1 I IP NETWORK REGION MEDIA PARMETERS INTRA-region IP-IP Direct Audio: yes Code Code 1 I IP NETWORK REGION MEDIA PARMETERS INTRA-region IP-IP Direct Audio: yes Code Code 1 I IP NETWORK REGION RECENT I IP NETWORK PARAMETERS Call Control PHB Value: 26 So 1. P(A PARAMETERS Call Control BO2.1P Priority: 6 Audio 802.1P Priority: 6	e								
display node-names ip       IP NODE NAMES         Name       IP Address         SMI       10.80.120.28         CLAN-LAO2       10.80.130.102         MEDPRO-1BO7       10.80.130.105         Default       0.0.0.0         Gateway1       10.80.130.105         Procr       10.80.131.100         3.       IP network region         The Communication Manager, Session Manager and VoIP (H.323/SIP) endpolocated in a single IP network region (IP network region 1) using the parameter described below. Use the display ip-network-region command to view these         The example below shows the values used for the compliance test.         •       Authoritative Domain - avaya.com was used for first Communication Manager         •       Name - Any descriptive name string         •       IP-IP Direct Audio (shuffling) was enabled to allow audio traffic to be se directly between IP endpoints without using media resources in the Avaya Gateway. This was done for both intra-region and inter-region IP-IP Direct Maids (Sagnaling Group form.         •       Codec Set - Set to the IP codec set to be used for calls within this IP network region: 1         Icoation:       Authoritative Domain: avaya.com         Name: CMI-SM       Inter-region IP-IP Direct Audio: yes         Codec Set: 1       Inter-region IP-IP Direct Audio: yes         Codec Set: 1       Inter-region IP-IP Direct Audio: yes </th <th></th>									
IP NODE NAMES         Mame IP Address         SMI 10.80.120.28         CLAN-LAO2 10.80.130.102         Default 0.00.0         Default 0.00.0         One of the colspan="2">One of the colspan="2">Colspan="2">One of the colspan="2">One colspan="2">One of the colspan="2">One of the									
Name       TP Address         St. LAN-LAO2       10.80.130.102         MEDPRO-1B07       10.80.130.105         Default       0.0.0.0         Gateway1       10.80.130.10         proor       10.80.131.100         3.       IP network region         The Communication Manager, Session Manager and VoIP (H.323/SIP) endpolocated in a single IP network region (IP network region 1) using the parameted described below. Use the display ip-network-region command to view these The example below shows the values used for the compliance test.         •       Authoritative Domain – avaya.com was used for first Communication M and avayal.com for second Communication Manager         •       Name – Any descriptive name string         •       IP-IP Direct Audio (shuffling) was enabled to allow audio traffic to be se directly between IP endpoints without using media resources in the Avaya Gateway. This was done for both intra-region and inter-region IP-IP Direct This is the default setting. Shuffling can be further restricted at the trunk let the Signaling Group form.         •       Codec Set - Set to the IP codec set to be used for calls within this IP network region. In this case, IP codec set 1 was selected.         display ip-network-region 1       Page 1 of         MEDIA PARAMETERS       Intra-region IP-IP Direct Audio: yes         Codec Set: 1       Intra-region IP-IP Direct Audio: yes         UDP Fort Mar: 6535       PICP Reporting Enabled? y         Cal	2								
ctaw-lac2       10.80.130.102         MDDRO-1B07       10.80.130.105         Default       0.0.0.0         Gateway1       10.80.130.1         proor       10.80.111.100         3.       IP network region         The Communication Manager, Session Manager and VoIP (H.323/SIP) endpolocated in a single IP network region (IP network region 1) using the parameted described below. Use the display ip-network-region command to view these The example below shows the values used for the compliance test.         •       Authoritative Domain – avaya.com was used for first Communication M and avaya1.com for second Communication Manager         •       Name – Any descriptive name string         •       IP-IP Direct Audio (shuffing) was enabled to allow audio traffic to be see directly between IP endpoints without using media resources in the Avaya Gateway. This was done for both intra-region and inter-region IP-IP Direct This is the default setting. Shuffling can be further restricted at the trunk let the Signaling Group form.         •       Codec Set - Set to the IP codec set to be used for calls within this IP network region. In this case, IP codec set 1 was selected.         display ip-network-region 1       Fage 1 of IP NETWORK REGION         Region: 1       Location:       Authoritative Domain: avaya.com         Name: CMI-5M       Inter-region IP-IP Direct Audio: yes         Codec Set: 1       Inter-region IP-IP Direct Audio: yes         UDP Port Mar: 65535       IP									
MEDPENO-1B07       10.80.130.105         Default       0.0.0.0         Gatewayl       10.80.130.1         proct       10.80.111.100         3.       IP network region         The Communication Manager, Session Manager and VoIP (H.323/SIP) endpolocated in a single IP network region (IP network-region command to view these         the Communication Manager, Session Manager and VoIP (H.323/SIP) endpolocated in a single IP network region (IP network-region command to view these         The example below shows the values used for the compliance test.         • Authoritative Domain - avaya.com         and avayal.com for second Communication Manager         • Name - Any descriptive name string         • IP-IP Direct Audio (shuffling) was enabled to allow audio traffic to be se directly between IP endpoints without using media resources in the Avaya Gateway. This was done for both intra-region and inter-region IP-IP Direct This is the default setting. Shuffling can be further restricted at the trunk let be Signaling Group form.         • Codec Set - Set to the IP codec set to be used for calls within this IP network region: 1         Izoration:       Authoritative Domain: avaya.com         Name: CMI-SM       Intra-region IP-IP Direct Audio: yes         Codec Set: 1       Intra-region IP-IP Direct Audio: yes         Codec Set: 1       Intra-region IP-IP Direct Audio: yes         Codec Set: 1       Intra-region IP-IP Direct Audio: yes									
Gatewayl       10.80.130.1         procr       10.80.111.100         3.       IP network region         The Communication Manager, Session Manager and VoIP (H.323/SIP) endpolocated in a single IP network region (IP network region 1) using the parameted described below. Use the display ip-network-region command to view these The example below shows the values used for the compliance test.         •       Authoritative Domain - avaya.com         •       Name - Any descriptive name string         •       IP-IP Direct Audio (shuffling) was enabled to allow audio traffic to be see directly between IP endpoints without using media resources in the Avaya Gateway. This was done for both intra-region and inter-region IP-IP Direct This is the default setting. Shuffling can be further restricted at the trunk let the Signaling Group form.         •       Codec Set - Set to the IP codec set to be used for calls within this IP network region. In this case, IP codec set 1 was selected.           Messaware Markers       Intra-region IP-IP Direct Audio: yes <ul> <li>Gele Set: 1</li> <li>Inter-region IP-IP Direct Audio: yes</li> <li>UDP Port Min: 2048</li> <li>UDP Port Min: 65535</li></ul>									
<ul> <li>JProce 10.80.111.100</li> <li>3. IP network region         The Communication Manager, Session Manager and VoIP (H.323/SIP) endpolocated in a single IP network region (IP network region 1) using the parameted described below. Use the display ip-network-region command to view these         The example below shows the values used for the compliance test.     </li> <li>Authoritative Domain – avaya.com was used for first Communication M         and avaya1.com for second Communication Manager         <ul> <li>Name – Any descriptive name string</li> <li>IP-IP Direct Audio (shuffling) was enabled to allow audio traffic to be se             directly between IP endpoints without using media resources in the Avaya             Gateway. This was done for both intra-region and inter-region IP-IP Direct             This is the default setting. Shuffling can be further restricted at the trunk le             the Signaling Group form.</li>             Codec Set - Set to the IP codec set to be used for calls within this IP networ             region. In this case, IP codec set 1 was selected.</ul></li> </ul> display ip-network-region 1 <ul> <li>IP NETWORK REGION             Region; 1             Location;             Authoritative Domain; avaya.com             Name: CMI-SM             MEDIA PARMETERS             Inter-region IP-IP Direct Audio; yes             Codec Set: 1             Inter-region IP-IP Direct Audio; yes             UDF Port Min: 2048             IP Audio Hairpinning? n             UDP Fort Min: 205             DIFFSERV/TOS PARAMETERS             RTCP Reporting Enabled? y             Call Control HB value: 46                  Yudeo PHB value: 26             S02.1P/Q PARAMETERS             Call Control 802.1p Priority: 6             Audio 802.1p Priority:</li></ul>									
<ul> <li>The Communication Manager, Session Manager and VoIP (H.323/SIP) endpolocated in a single IP network region (IP network region 1) using the parameted described below. Use the display ip-network-region command to view these The example below shows the values used for the compliance test.</li> <li>Authoritative Domain - avaya.com was used for first Communication Manager</li> <li>Name - Any descriptive name string</li> <li>IP-IP Direct Audio (shuffling) was enabled to allow audio traffic to be see directly between IP endpoints without using media resources in the Avaya Gateway. This was done for both intra-region and inter-region IP-IP Direct This is the default setting. Shuffling can be further restricted at the trunk let the Signaling Group form.</li> <li>Codec Set - Set to the IP codec set to be used for calls within this IP network region. In this case, IP codec set 1 was selected.</li> <li>display ip-network-region 1 PARAMETERS Intra-region IP-IP Direct Audio: yes Codec Set: 1 Intra-region IP-IP Direct Audio: yes Codec Set: 1 Intra-region IP-IP Direct Audio: yes Code Set: 1 IP Audio Hairpinning? n UDP Port Max: 65535</li> <li>DIFFSERV/TOS PARAMETERS RTCP MONTOR SERVER PARAMETERS Audio PHB Value: 46 RTCP MONTOR SERVER PARAMETERS Audio PHB Value: 26</li> <li>802.1P/Q PARAMETERS Call Control PH Value: 26</li> <li>802.1P/Q PARAMETERS Call Control 802.1p Priority: 6</li> </ul>									
<ul> <li>The Communication Manager, Session Manager and VoIP (H.323/SIP) endpolocated in a single IP network region (IP network region 1) using the parameted described below. Use the display ip-network-region command to view these The example below shows the values used for the compliance test.</li> <li>Authoritative Domain - avaya.com was used for first Communication Manager</li> <li>Name - Any descriptive name string</li> <li>IP-IP Direct Audio (shuffling) was enabled to allow audio traffic to be see directly between IP endpoints without using media resources in the Avaya Gateway. This was done for both intra-region and inter-region IP-IP Direct This is the default setting. Shuffling can be further restricted at the trunk let the Signaling Group form.</li> <li>Codec Set - Set to the IP codec set to be used for calls within this IP network region. In this case, IP codec set 1 was selected.</li> <li>display ip-network-region 1 PARAMETERS Intra-region IP-IP Direct Audio: yes Codec Set: 1 Intra-region IP-IP Direct Audio: yes Codec Set: 1 Intra-region IP-IP Direct Audio: yes Code Set: 1 IP Audio Hairpinning? n UDP Port Max: 65535</li> <li>DIFFSERV/TOS PARAMETERS RTCP MONTOR SERVER PARAMETERS Audio PHB Value: 46 RTCP MONTOR SERVER PARAMETERS Audio PHB Value: 26</li> <li>802.1P/Q PARAMETERS Call Control PH Value: 26</li> <li>802.1P/Q PARAMETERS Call Control 802.1p Priority: 6</li> </ul>									
<ul> <li>located in a single IP network region (IP network region 1) using the parameter described below. Use the display ip-network-region command to view these The example below shows the values used for the compliance test.</li> <li>Authoritative Domain - avaya.com was used for first Communication Ma and avaya1.com for second Communication Manager</li> <li>Name - Any descriptive name string</li> <li>IP-IP Direct Audio (shuffling) was enabled to allow audio traffic to be set directly between IP endpoints without using media resources in the Avaya Gateway. This was done for both intra-region and inter-region IP-IP Direct This is the default setting. Shuffling can be further restricted at the trunk let the Signaling Group form.</li> <li>Codec Set - Set to the IP codec set to be used for calls within this IP network region. In this case, IP codec set 1 was selected.</li> <li>display ip-network-region 1 PARAMETERS Intra-region IP-IP Direct Audio: yes Codec Set 1 Intra-region IP-IP Direct Audio: yes UDP Port Max: 65355</li> <li>DIFFSERVITOS PARAMETERS RICP MONITOR SERVER PARAMETERS Audio PHB Value: 46 RICP MONITOR SERVER PARAMETERS Audio PHB Value: 26</li> <li>802.1P/Q PARAMETERS CALL AND AUDIO SERVER PARAMETERS Audio 802.1P Priority: 6 Audio 802.1P Priority: 6</li> </ul>									
<ul> <li>described below. Use the display ip-network-region command to view these The example below shows the values used for the compliance test.</li> <li>Authoritative Domain – avaya.com was used for first Communication M and avaya1.com for second Communication Manager</li> <li>Name – Any descriptive name string</li> <li>IP-IP Direct Audio (shuffling) was enabled to allow audio traffic to be se directly between IP endpoints without using media resources in the Avaya Gateway. This was done for both intra-region and inter-region IP-IP Direct This is the default setting. Shuffling can be further restricted at the trunk la the Signaling Group form.</li> <li>Codec Set - Set to the IP codec set to be used for calls within this IP network region. In this case, IP codec set 1 was selected.</li> <li>display ip-network-region 1 Region: 1 Location: Authoritative Domain: avaya.com Name: CMI-SM MEDIA PARAMETERS Codec Set: 1 Intra-region IP-IP Direct Audio: yes Codec Set: 1 Intra-region IP-IP Direct Audio: yes Code Set: 1 INFAMETERS DIFFSERV/TOS PARAMETERS Audio PHB Value: 46 Audio PHB Value: 26 802.1F/Q PARAMETERS Call Control HB Value: 26 RCIP Marking 802.1p Priority: 6 Audio 802.1p Priority: 6 Audio 802.1p Priority: 6</li> </ul>	nts were								
<ul> <li>The example below shows the values used for the compliance test.</li> <li>Authoritative Domain - avaya.com was used for first Communication Manager</li> <li>Name - Any descriptive name string</li> <li>IP-IP Direct Audio (shuffling) was enabled to allow audio traffic to be see directly between IP endpoints without using media resources in the Avaya Gateway. This was done for both intra-region and inter-region IP-IP Direct This is the default setting. Shuffling can be further restricted at the trunk let the Signaling Group form.</li> <li>Codec Set - Set to the IP codec set to be used for calls within this IP network region. In this case, IP codec set 1 was selected.</li> <li>display ip-network-region 1 Page 1 of Region: 1 Location: Authoritative Domain: avaya.com</li> <li>Name: CMI-SM</li> <li>MEDIA PARAMETERS Intra-region IP-IP Direct Audio: yes Codec Set: 1 Inter-region IP-IP Direct Audio: yes UDP Port Max: 6535 DIFFSERVTOS PARAMETERS RTCP Reporting Enabled? y Call Control PHB Value: 46 RTCP MONITOR SERVER PARAMETERS Audio PHB Value: 46 USe Default Server Parameters? y Video PHB Value: 26</li> <li>802.1F/Q PARAMETERS Call Control B02.1p Priority: 6 Audio 802.1p Priority: 6</li> </ul>	S								
<ul> <li>Authoritative Domain – avaya.com was used for first Communication Manager</li> <li>Name – Any descriptive name string</li> <li>IP-IP Direct Audio (shuffling) was enabled to allow audio traffic to be see directly between IP endpoints without using media resources in the Avaya Gateway. This was done for both intra-region and inter-region IP-IP Direct This is the default setting. Shuffling can be further restricted at the trunk let the Signaling Group form.</li> <li>Codec Set - Set to the IP codec set to be used for calls within this IP network region. In this case, IP codec set 1 was selected.</li> <li>display ip-network-region 1 Page 1 of IP NETWORK REGION Region: 1 Location: Authoritative Domain: avaya.com Name: CMI-SM MEDIA PARAMETERS Intra-region IP-IP Direct Audio: yes Codec Set: 1 Inter-region IP-IP Direct Audio: yes UDP Port Man: 2048 IP Audio Hairpinning? n UDP Port Man: 26535 DIFFSERV/TOS PARAMETERS RTCP Reporting Enabled? y Call Control PHB Value: 46 RTCP MONITOR SERVER PARAMETERS Audio PHB Value: 26 802.1F/Q PARAMETERS Call Control B02.1p Priority: 6 Audio 802.1p Priority: 6 Audio 802.1p Priority: 6</li> </ul>	ettings.								
<ul> <li>and avaya1.com for second Communication Manager</li> <li>Name – Any descriptive name string</li> <li>IP-IP Direct Audio (shuffling) was enabled to allow audio traffic to be see directly between IP endpoints without using media resources in the Avaya Gateway. This was done for both intra-region and inter-region IP-IP Direct This is the default setting. Shuffling can be further restricted at the trunk letting is the default setting. Shuffling can be further restricted at the trunk letting is the default setting. Shuffling can be further restricted at the trunk letting is the default setting. Shuffling can be further restricted at the trunk letting is the default setting. Shuffling can be further restricted at the trunk letting is the default setting. Shuffling can be further restricted at the trunk letting is the default setting. Shuffling can be further restricted at the trunk letting is the default setting. Shuffling can be further restricted at the trunk letting is the default setting. Shuffling can be further restricted at the trunk letting is the default setting. Shuffling can be further restricted at the trunk letting is the default setting. Shuffling can be further restricted at the trunk letting is the default setting. Shuffling can be further restricted at the trunk letting is the default setting. Shuffling can be further restricted at the trunk letting is the default setting. Shuffling can be further restricted at the trunk letting is default setting. Shuffling can be further restricted at the trunk letting is default setting. Shuffling can be further restricted at the trunk letting is default setting. Shuffling can be further restricted at the trunk letting is default setting. Shuffling can be further restricted at the trunk letting is default setting. Shuffling can be default setting is default setting. Shuffling can be default setting is default setting is default setting is default setting. Shuffling can be default setting is default setting is default setting is default setting</li></ul>									
<ul> <li>Name – Any descriptive name string</li> <li>IP-IP Direct Audio (shuffling) was enabled to allow audio traffic to be sed directly between IP endpoints without using media resources in the Avaya Gateway. This was done for both intra-region and inter-region IP-IP Direct This is the default setting. Shuffling can be further restricted at the trunk let the Signaling Group form.</li> <li>Codec Set - Set to the IP codec set to be used for calls within this IP network region. In this case, IP codec set 1 was selected.</li> <li>         display ip-network-region 1</li></ul>	nager								
<ul> <li>IP-IP Direct Audio (shuffling) was enabled to allow audio traffic to be see directly between IP endpoints without using media resources in the Avaya Gateway. This was done for both intra-region and inter-region IP-IP Direct This is the default setting. Shuffling can be further restricted at the trunk let the Signaling Group form.</li> <li>Codec Set - Set to the IP codec set to be used for calls within this IP network region. In this case, IP codec set 1 was selected.</li> <li>         display ip-network-region 1             Page 1 of</li></ul>									
<ul> <li>directly between IP endpoints without using media resources in the Avaya Gateway. This was done for both intra-region and inter-region IP-IP Direct This is the default setting. Shuffling can be further restricted at the trunk le the Signaling Group form.</li> <li>Codec Set - Set to the IP codec set to be used for calls within this IP network region. In this case, IP codec set 1 was selected.</li> <li>display ip-network-region 1 Page 1 of IP NETWORK REGION Region: 1 Location: Authoritative Domain: avaya.com Name: CMI-SM MEDIA PARAMETERS Intra-region IP-IP Direct Audio: yes ODP Port Min: 2048 IP Audio Hairpinning? n UDP Port Max: 65535 DIFFSERV/TOS PARAMETERS RTCP Reporting Enabled? y Call Control PHB Value: 46 Audio PHB Value: 26 802.1P/Q PARAMETERS Call Control 802.1p Priority: 6 Audio 802.1p Priority: 6 Audio 802.1p Priority: 6</li> </ul>									
Gateway. This was done for both intra-region and inter-region IP-IP Direct This is the default setting. Shuffling can be further restricted at the trunk le the Signaling Group form. • Codec Set - Set to the IP codec set to be used for calls within this IP network region. In this case, IP codec set 1 was selected. display ip-network-region 1 Page 1 of IP NETWORK REGION Region: 1 Location: Authoritative Domain: avaya.com Name: CM1-SM 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: 65535 DIFFSERV/TOS PARAMETERS RTCP Reporting Enabled? y Call Control PHB Value: 46 Use Default Server Parameters? y Video PHB Value: 26 802.1P/Q PARAMETERS Call Control 802.1p Priority: 6 Audio 802.1p Priority: 6	If if Direct Hudio (Shuffing) was chaoled to allow addie huffe to be bent								
This is the default setting. Shuffling can be further restricted at the trunk let the Signaling Group form. Codec Set - Set to the IP codec set to be used for calls within this IP network region. In this case, IP codec set 1 was selected. display ip-network-region 1 Page 1 of IP NETWORK REGION Region: 1 Location: Authoritative Domain: avaya.com Name: CM1-SM 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: 65535 DIFFSERV/TOS PARAMETERS RTCP Reporting Enabled? y Call Control PHB Value: 46 Audio PHB Value: 26 802.1P/Q PARAMETERS Call Control 802.1p Priority: 6 Audio 802.1p Priority: 6 Audio 802.1p Priority: 6	directly between IP endpoints without using media resources in the Avaya Media								
<ul> <li>the Signaling Group form.</li> <li>Codec Set - Set to the IP codec set to be used for calls within this IP network region. In this case, IP codec set 1 was selected.</li> <li>display ip-network-region 1 Page 1 of IP NETWORK REGION</li> <li>Region: 1</li> <li>Location: Authoritative Domain: avaya.com</li> <li>Name: CM1-SM</li> <li>MEDIA PARAMETERS Intra-region IP-IP Direct Audio: yes</li> <li>Codec Set: 1 Inter-region IP-IP Direct Audio: yes</li> <li>UDP Port Min: 2048 IP Audio Hairpinning? n</li> <li>UDP Port Min: 2048 IP Audio Hairpinning? n</li> <li>UDP Port Max: 65535</li> <li>DIFFSERV/TOS PARAMETERS RTCP Reporting Enabled? y</li> <li>Call Control PHB Value: 46 Use Default Server Parameters? y</li> <li>Video PHB Value: 26</li> <li>802.1P/Q PARAMETERS</li> <li>Call Control 802.1p Priority: 6</li> <li>Audio 802.1p Priority: 6</li> </ul>	Audio.								
<ul> <li>Codec Set - Set to the IP codec set to be used for calls within this IP network region. In this case, IP codec set 1 was selected.</li> <li>display ip-network-region 1 Page 1 of IP NETWORK REGION</li></ul>	vel on								
region. In this case, IP codec set 1 was selected. display ip-network-region 1 Page 1 of IP NETWORK REGION Region: 1 Location: Authoritative Domain: avaya.com Name: CM1-SM MEDIA PARAMETERS Intra-region IP-IP Direct Audio: yes Codec Set: 1 Intra-region IP-IP Direct Audio: yes UDP Port Min: 2048 IP Audio Hairpinning? n UDP Port Max: 65535 DIFFSERV/TOS PARAMETERS RTCP Reporting Enabled? y Call Control PHB Value: 46 RTCP MONITOR SERVER PARAMETERS Audio PHB Value: 46 Use Default Server Parameters? y Video PHB Value: 26 802.1P/Q PARAMETERS Call Control 802.1p Priority: 6 Audio 802.1p Priority: 6									
display ip-network-region 1 IP NETWORK REGION Region: 1 Location: Authoritative Domain: avaya.com Name: CM1-SM MEDIA PARAMETERS Intra-region IP-IP Direct Audio: yes Codec Set: 1 UDP Port Min: 2048 UDP Port Min: 2048 UDP Port Max: 65535 DIFFSERV/TOS PARAMETERS Audio PHB Value: 46 Audio PHB Value: 46 802.1P/Q PARAMETERS Call Control 802.1p Priority: 6 Audio 802.1p Priority: 6	rk								
IP NETWORK REGION Region: 1 Location: Authoritative Domain: avaya.com Name: CM1-SM 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: 65535 DIFFSERV/TOS PARAMETERS RTCP Reporting Enabled? y Call Control PHB Value: 46 RTCP MONITOR SERVER PARAMETERS Audio PHB Value: 46 Use Default Server Parameters? y Video PHB Value: 26 802.1P/Q PARAMETERS Call Control 802.1p Priority: 6 Audio 802.1p Priority: 6									
IP NETWORK REGION Region: 1 Location: Authoritative Domain: avaya.com Name: CM1-SM 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: 65535 DIFFSERV/TOS PARAMETERS RTCP Reporting Enabled? y Call Control PHB Value: 46 RTCP MONITOR SERVER PARAMETERS Audio PHB Value: 46 Use Default Server Parameters? y Video PHB Value: 26 802.1P/Q PARAMETERS Call Control 802.1p Priority: 6 Audio 802.1p Priority: 6									
Region: 1Location:Authoritative Domain: avaya.comName: CM1-SMMEDIA PARAMETERSIntra-region IP-IP Direct Audio: yesCodec Set: 1Inter-region IP-IP Direct Audio: yesUDP Port Min: 2048IP Audio Hairpinning? nUDP Port Max: 65535RTCP Reporting Enabled? yCall Control PHB Value: 46RTCP MONITOR SERVER PARAMETERSAudio PHB Value: 46Use Default Server Parameters? yVideo PHB Value: 26802.1P/Q PARAMETERSCall Control 802.1p Priority: 6Audio 802.1p Priority: 6	. 9								
Name: CM1-SM       Intra-region IP-IP Direct Audio: yes         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: 65535       IFFSERV/TOS PARAMETERS         DIFFSERV/TOS PARAMETERS       RTCP Reporting Enabled? y         Call Control PHB Value: 46       Use Default Server PARAMETERS         Audio PHB Value: 26       802.1P/Q PARAMETERS         Call Control 802.1p Priority: 6       Audio 802.1p Priority: 6									
MEDIA PARAMETERSIntra-region IP-IP Direct Audio: yesCodec Set: 1Inter-region IP-IP Direct Audio: yesUDP Port Min: 2048IP Audio Hairpinning? nUDP Port Max: 65535IP Audio Hairpinning? nDIFFSERV/TOS PARAMETERSRTCP Reporting Enabled? yCall Control PHB Value: 46RTCP MONITOR SERVER PARAMETERSAudio PHB Value: 26Use Default Server Parameters? yVideo PHB Value: 26802.1P/Q PARAMETERSCall Control 802.1p Priority: 6Audio 802.1p Priority: 6									
UDP Port Min: 2048 UDP Port Max: 65535 DIFFSERV/TOS PARAMETERS Audio PHB Value: 46 NUDP Port Max: 65535 RTCP Reporting Enabled? y Call Control PHB Value: 46 Nuse Default Server Parameters? y Video PHB Value: 26 802.1P/Q PARAMETERS Call Control 802.1p Priority: 6 Audio 802.1p Priority: 6									
UDP Port Max: 65535 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									
Call Control PHB Value: 46 RTCP MONITOR SERVER PARAMETERS Audio PHB Value: 46 Use Default Server Parameters? y Video PHB Value: 26 802.1P/Q PARAMETERS Call Control 802.1p Priority: 6 Audio 802.1p Priority: 6									
Audio PHB Value: 46 Use Default Server Parameters? y Video PHB Value: 26 802.1P/Q PARAMETERS Call Control 802.1p Priority: 6 Audio 802.1p Priority: 6									
802.1P/Q PARAMETERS Call Control 802.1p Priority: 6 Audio 802.1p Priority: 6									
Call Control 802.1p Priority: 6 Audio 802.1p Priority: 6									
Audio 802.1p Priority: 6									
Video 802.1p Priority: 5 AUDIO RESOURCE RESERVATION PARAMETERS									
H.323 IP ENDPOINTS RSVP Enabled? n									
H.323 Link Bounce Recovery? y									
Idle Traffic Interval (sec): 20 Keep-Alive Interval (sec): 5									
Keep-Alive Interval (Sec): 5 Keep-Alive Count: 5									

Step	Description	
4.	Codecs Use the change ip-codec-set 1 command to define the code The EGW only supports the G.711MU codec. Thus for the <i>G.711MU</i> was set in the codec list.	5
	change ip-codec-set 1	Page 1 of 2
	IP Codec Set	
	Codec Set: 1	
	AudioSilenceFramesPacketCodecSuppressionPer PktSize(ms)1:G.711MUn2202:2:1000000000000000000000000000000000000	

Description         Signaling Group         Enter the add signaling-group n command, where n is an unused signaling gereate a new signaling group 1 for the SIP trunk to Session Manager. For the c test, signaling group 1 was created for the trunk to the Session Manager. Sign group 1 was configured using the parameters highlighted below:         Group Type – Set to sip.         Transport Method – Set to tcp.         Verify that Peer Detection Enabled is y and that Peer Server is SM.         Near-end Node Name – Set to the node name of the CLAN i.e. CLAN-1 noted in Step 2.         Far-end Node Name – Set to the node name of Session Manager i.e. SM Step 2.         Near-end Listen Port and Far-end Listen Port – set to "5060".         Far-end Node Name – Set to the IP network region 1, as defined in in Far-end Domain – Set to avaya.com. This is the domain inserted by Sess Manager. For the second Communication Manager, this value was set ava DTMF over IP – Set to rtp-payload to enable Communication Manager to DTMF according to RFC 2833.         Direct IP-IP Audio Connections – Set to y, indicating that the RTP path be optimized to reduce the use of Communication Manager audio resourc possible.         add signaling-group 1       SIGNALING GROUP         Group Number: 1       Group Type: sip ITMS Enabled? n         Transport Method: 2 n       Far-end Node Name: CLAN-1A02
<ul> <li>Enter the add signaling-group n command, where n is an unused signaling g create a new signaling group for the SIP trunk to Session Manager. For the c test, signaling group 1 was created for the trunk to the Session Manager. Sign group 1 was configured using the parameters highlighted below:</li> <li>Group Type – Set to sip.</li> <li>Transport Method – Set to tcp.</li> <li>Verify that Peer Detection Enabled is y and that Peer Server is SM.</li> <li>Near-end Node Name – Set to the node name of the CLAN i.e. CLAN-1 noted in Step 2.</li> <li>Far-end Node Name – Set to the node name of Session Manager i.e. SM Step 2.</li> <li>Near-end Listen Port and Far-end Listen Port – set to "5060".</li> <li>Far-end Nodein – Set to avaya.com. This is the domain inserted by Sess Manager. For the second Communication Manager, this value was set ava 0 DTMF over IP – Set to trp-payload to enable Communication Manager to DTMF according to RFC 2833.</li> <li>Direct IP-IP Audio Connections – Set to y, indicating that the RTP path be optimized to reduce the use of Communication Manager audio resource possible.</li> <li>add signaling-group 1 SIGNALING GROUP</li> <li>Group Number: 1 Group Type: sip IMS Enabled? n Transport Method: tcp SIFP n IP Video? n SIFP Enabled IS</li> </ul>
<ul> <li>test, signaling group 1 was created for the trunk to the Session Manager. Sign group 1 was configured using the parameters highlighted below:</li> <li>Group Type – Set to <i>sip</i>.</li> <li>Transport Method – Set to <i>tcp</i>.</li> <li>Verify that Peer Detection Enabled is <i>y</i> and that Peer Server is <i>SM</i>.</li> <li>Near-end Node Name – Set to the node name of the CLAN i.e. CLAN-1 noted in Step 2.</li> <li>Far-end Node Name – Set to the node name of Session Manager i.e. SM Step 2.</li> <li>Near-end Listen Port and Far-end Listen Port – set to "5060".</li> <li>Far-end Network Region – Set to the IP network region 1, as defined in</li> <li>Far-end Domain – Set to <i>avaya.com</i>. This is the domain inserted by Sess Manager. For the second Communication Manager, this value was set <i>ava</i>.</li> <li>DTMF over IP – Set to <i>rtp-payload</i> to enable Communication Manager to DTMF according to RFC 2833.</li> <li>Direct IP-IP Audio Connections – Set to <i>y</i>, indicating that the RTP path be optimized to reduce the use of Communication Manager audio resource possible.</li> <li>add signaling-group 1 Group Type: sip IMS Enabled? n Transport Method: tcp OCSIP? n SIP Enabled LS FIP Video? n Fip Video?</li> </ul>
<ul> <li>group 1 was configured using the parameters highlighted below:</li> <li>Group Type – Set to <i>sip</i>.</li> <li>Transport Method – Set to <i>tcp</i>.</li> <li>Verify that Peer Detection Enabled is y and that Peer Server is SM.</li> <li>Near-end Node Name – Set to the node name of the CLAN i.e. CLAN-1 noted in Step 2.</li> <li>Far-end Node Name – Set to the node name of Session Manager i.e. SM Step 2.</li> <li>Near-end Listen Port and Far-end Listen Port – set to "5060".</li> <li>Far-end Network Region – Set to the IP network region 1, as defined in Far-end Domain – Set to <i>avaya.com</i>. This is the domain inserted by Sess Manager. For the second Communication Manager, this value was set <i>ava</i>.</li> <li>DTMF over IP – Set to <i>rtp-payload</i> to enable Communication Manager to DTMF according to RFC 2833.</li> <li>Direct IP-IP Audio Connections – Set to y, indicating that the RTP path be optimized to reduce the use of Communication Manager audio resource possible.</li> <li>add signaling-group 1 Page 1 o SIGNALING GROUP</li> <li>Group Number: 1 Group Type: sip IMS Enabled? n Transport Method: tcp Q-SIP? n SIP Enabled LS IP Video? n Enable SIPS URI for SRT Peer Detection Enabled? y Peer Server: SM</li> </ul>
<ul> <li>Group Type – Set to sip.</li> <li>Transport Method – Set to tcp.</li> <li>Verify that Peer Detection Enabled is y and that Peer Server is SM.</li> <li>Near-end Node Name – Set to the node name of the CLAN i.e. CLAN-1 noted in Step 2.</li> <li>Far-end Node Name – Set to the node name of Session Manager i.e. SM Step 2.</li> <li>Near-end Listen Port and Far-end Listen Port – set to "5060".</li> <li>Far-end Network Region – Set to the IP network region 1, as defined in rare-end Domain – Set to avaya.com. This is the domain inserted by Sess Manager. For the second Communication Manager, this value was set ava DTMF over IP – Set to rtp-payload to enable Communication Manager to DTMF according to RFC 2833.</li> <li>Direct IP-IP Audio Connections – Set to y, indicating that the RTP path be optimized to reduce the use of Communication Manager audio resource possible.</li> </ul>
<ul> <li>Group Type – Set to sip.</li> <li>Transport Method – Set to tcp.</li> <li>Verify that Peer Detection Enabled is y and that Peer Server is SM.</li> <li>Near-end Node Name – Set to the node name of the CLAN i.e. CLAN-1 noted in Step 2.</li> <li>Far-end Node Name – Set to the node name of Session Manager i.e. SM Step 2.</li> <li>Near-end Listen Port and Far-end Listen Port – set to "5060".</li> <li>Far-end Network Region – Set to the IP network region 1, as defined in Far-end Domain – Set to avaya.com. This is the domain inserted by Sess Manager. For the second Communication Manager, this value was set ava DTMF over IP – Set to rtp-payload to enable Communication Manager to DTMF according to RFC 2833.</li> <li>Direct IP-IP Audio Connections – Set to y, indicating that the RTP path be optimized to reduce the use of Communication Manager audio resource possible.</li> </ul>
<ul> <li>Transport Method – Set to tcp.</li> <li>Verify that Peer Detection Enabled is y and that Peer Server is SM.</li> <li>Near-end Node Name – Set to the node name of the CLAN i.e. CLAN-1 noted in Step 2.</li> <li>Far-end Node Name – Set to the node name of Session Manager i.e. SM Step 2.</li> <li>Near-end Listen Port and Far-end Listen Port – set to "5060".</li> <li>Far-end Network Region – Set to the IP network region 1, as defined in</li> <li>Far-end Domain – Set to avaya.com. This is the domain inserted by Sess Manager. For the second Communication Manager, this value was set ava</li> <li>DTMF over IP – Set to rtp-payload to enable Communication Manager to DTMF according to RFC 2833.</li> <li>Direct IP-IP Audio Connections – Set to y, indicating that the RTP path be optimized to reduce the use of Communication Manager audio resourc possible.</li> <li>add signaling-group 1 Page 1 o SIGNALING GROUP</li> <li>Group Number: 1 Group Type: sip IMS Enabled? n Transport Method: tcp Q-SIP? n SIP Enabled LS IP Video? n Enable SIPS URI for SRT</li> <li>Peer Detection Enabled? y Peer Server: SM</li> </ul>
<ul> <li>Verify that Peer Detection Enabled is y and that Peer Server is SM.</li> <li>Near-end Node Name – Set to the node name of the CLAN i.e. CLAN-1 noted in Step 2.</li> <li>Far-end Node Name – Set to the node name of Session Manager i.e. SM Step 2.</li> <li>Near-end Listen Port and Far-end Listen Port – set to "5060".</li> <li>Far-end Network Region – Set to the IP network region 1, as defined in</li> <li>Far-end Domain – Set to avaya.com. This is the domain inserted by Sess Manager. For the second Communication Manager, this value was set ava</li> <li>DTMF over IP – Set to rtp-payload to enable Communication Manager to DTMF according to RFC 2833.</li> <li>Direct IP-IP Audio Connections – Set to y, indicating that the RTP path be optimized to reduce the use of Communication Manager audio resourc possible.</li> <li>add signaling-group 1 Page 1 o SIGNALING GROUP</li> <li>Group Number: 1 Group Type: sip IMS Enabled? n Transport Method: top Q-SIP? n SIP Enabled IS IP Enabled IS IP Video? n Enable SIPS URI for SRT</li> </ul>
<ul> <li>Near-end Node Name – Set to the node name of the CLAN i.e. CLAN-1 noted in Step 2.</li> <li>Far-end Node Name – Set to the node name of Session Manager i.e. SM Step 2.</li> <li>Near-end Listen Port and Far-end Listen Port – set to "5060".</li> <li>Far-end Network Region – Set to the IP network region 1, as defined in</li> <li>Far-end Domain – Set to avaya.com. This is the domain inserted by Sess Manager. For the second Communication Manager, this value was set ava</li> <li>DTMF over IP – Set to rtp-payload to enable Communication Manager to DTMF according to RFC 2833.</li> <li>Direct IP-IP Audio Connections – Set to y, indicating that the RTP path be optimized to reduce the use of Communication Manager audio resource possible.</li> <li>add signaling-group 1 Page 1 o SIGNALING GROUP</li> <li>Group Number: 1 Group Type: sip IMS Enabled? n Transport Method: tcp Q-SIP? n SIP Enabled LS IP Video? n Enable SIPS URI for SRT Peer Detection Enabled? y Peer Server: SM</li> </ul>
<ul> <li>noted in Step 2.</li> <li>Far-end Node Name – Set to the node name of Session Manager i.e. SM Step 2.</li> <li>Near-end Listen Port and Far-end Listen Port – set to "5060".</li> <li>Far-end Network Region – Set to the IP network region 1, as defined in</li> <li>Far-end Domain – Set to avaya.com. This is the domain inserted by Sess Manager. For the second Communication Manager, this value was set ava</li> <li>DTMF over IP – Set to rtp-payload to enable Communication Manager to DTMF according to RFC 2833.</li> <li>Direct IP-IP Audio Connections – Set to y, indicating that the RTP path be optimized to reduce the use of Communication Manager audio resource possible.</li> <li>add signaling-group 1 Page 1 o SIGNALING GROUP</li> <li>Group Number: 1 Group Type: sip IMS Enabled? n Transport Method: tcp Q-SIP? n SIP Enabled LS IP Video? n Feer Detection Enabled? y Feer Server: SM</li> </ul>
<ul> <li>Far-end Node Name – Set to the node name of Session Manager i.e. SM Step 2.</li> <li>Near-end Listen Port and Far-end Listen Port – set to "5060".</li> <li>Far-end Network Region – Set to the IP network region 1, as defined in</li> <li>Far-end Domain – Set to avaya.com. This is the domain inserted by Sess Manager. For the second Communication Manager, this value was set ava</li> <li>DTMF over IP – Set to rtp-payload to enable Communication Manager to DTMF according to RFC 2833.</li> <li>Direct IP-IP Audio Connections – Set to y, indicating that the RTP path be optimized to reduce the use of Communication Manager audio resource possible.</li> <li>add signaling-group 1 Page 1 o SIGNALING GROUP</li> <li>Group Number: 1 Group Type: sip IMS Enabled? n Transport Method: tcp Q-SIP? n SIP Enabled LS IP Video? n Page 1 o Enable SIPS URI for SRT</li> </ul>
<ul> <li>Step 2.</li> <li>Near-end Listen Port and Far-end Listen Port – set to "5060".</li> <li>Far-end Network Region – Set to the IP network region 1, as defined in</li> <li>Far-end Domain – Set to avaya.com. This is the domain inserted by Sess Manager. For the second Communication Manager, this value was set ava</li> <li>DTMF over IP – Set to rtp-payload to enable Communication Manager to DTMF according to RFC 2833.</li> <li>Direct IP-IP Audio Connections – Set to y, indicating that the RTP path be optimized to reduce the use of Communication Manager audio resource possible.</li> <li>add signaling-group 1 Page 1 or SIGNALING GROUP</li> <li>Group Number: 1 Group Type: sip IMS Enabled? n Transport Method: top Q-SIP? n SIP Enabled LS Enable SIPS URI for SRT Peer Detection Enabled? y Peer Server: SM</li> </ul>
<ul> <li>Near-end Listen Port and Far-end Listen Port – set to "5060".</li> <li>Far-end Network Region – Set to the IP network region 1, as defined in</li> <li>Far-end Domain – Set to avaya.com. This is the domain inserted by Sess Manager. For the second Communication Manager, this value was set ava</li> <li>DTMF over IP – Set to rtp-payload to enable Communication Manager to DTMF according to RFC 2833.</li> <li>Direct IP-IP Audio Connections – Set to y, indicating that the RTP path be optimized to reduce the use of Communication Manager audio resource possible.</li> <li>add signaling-group 1 Page 1 o SIGNALING GROUP</li> <li>Group Number: 1 Group Type: sip IMS Enabled? n Transport Method: tcp Q-SIP? n SIP Enabled LS IP Video? n Feer Detection Enabled? y Peer Server: SM</li> </ul>
<ul> <li>Far-end Network Region – Set to the IP network region 1, as defined in</li> <li>Far-end Domain – Set to avaya.com. This is the domain inserted by Sess Manager. For the second Communication Manager, this value was set ava</li> <li>DTMF over IP – Set to rtp-payload to enable Communication Manager to DTMF according to RFC 2833.</li> <li>Direct IP-IP Audio Connections – Set to y, indicating that the RTP path be optimized to reduce the use of Communication Manager audio resource possible.</li> <li>add signaling-group 1 Page 1 or SIGNALING GROUP</li> <li>Group Number: 1 Group Type: sip IMS Enabled? n Transport Method: tcp Q-SIP? n SIP Enabled LS IP Video? n Page 1 or SIP Enabled? Y Peer Server: SM</li> </ul>
<ul> <li>Far-end Domain – Set to avaya.com. This is the domain inserted by Sess Manager. For the second Communication Manager, this value was set ava</li> <li>DTMF over IP – Set to rtp-payload to enable Communication Manager to DTMF according to RFC 2833.</li> <li>Direct IP-IP Audio Connections – Set to y, indicating that the RTP path be optimized to reduce the use of Communication Manager audio resource possible.</li> <li>add signaling-group 1 Page 1 o SIGNALING GROUP</li> <li>Group Number: 1 Group Type: sip IMS Enabled? n Transport Method: tcp Q-SIP? n IP Video? n Feer Detection Enabled? y Peer Server: SM</li> </ul>
<ul> <li>Manager. For the second Communication Manager, this value was set available.</li> <li>DTMF over IP – Set to <i>rtp-payload</i> to enable Communication Manager to DTMF according to RFC 2833.</li> <li>Direct IP-IP Audio Connections – Set to y, indicating that the RTP path be optimized to reduce the use of Communication Manager audio resource possible.</li> <li>add signaling-group 1 Page 1 o SIGNALING GROUP</li> <li>Group Number: 1 Group Type: sip IMS Enabled? n Transport Method: tcp Q-SIP? n SIP Enabled LS Enable SIPS URI for SRT</li> <li>Peer Detection Enabled? y Peer Server: SM</li> </ul>
<ul> <li>DTMF over IP – Set to <i>rtp-payload</i> to enable Communication Manager to DTMF according to RFC 2833.</li> <li>Direct IP-IP Audio Connections – Set to <i>y</i>, indicating that the RTP path be optimized to reduce the use of Communication Manager audio resource possible.</li> <li>add signaling-group 1 Page 1 o SIGNALING GROUP</li> <li>Group Number: 1 Group Type: sip IMS Enabled? n Transport Method: tcp Q-SIP? n SIP Enabled LS Enable SIPS URI for SRT</li> <li>Peer Detection Enabled? y Peer Server: SM</li> </ul>
<ul> <li>DTMF according to RFC 2833.</li> <li>Direct IP-IP Audio Connections – Set to y, indicating that the RTP path be optimized to reduce the use of Communication Manager audio resource possible.</li> <li>add signaling-group 1 Page 1 o SIGNALING GROUP</li> <li>Group Number: 1 Group Type: sip IMS Enabled? n Transport Method: tcp Q-SIP? n SIP Enabled LS Enable SIPS URI for SRT</li> <li>Peer Detection Enabled? y Peer Server: SM</li> </ul>
<ul> <li>Direct IP-IP Audio Connections – Set to y, indicating that the RTP path be optimized to reduce the use of Communication Manager audio resource possible.</li> <li>add signaling-group 1 Page 1 o SIGNALING GROUP</li> <li>Group Number: 1 Group Type: sip IMS Enabled? n Transport Method: tcp Q-SIP? n SIP Enabled LS Enable SIPS URI for SRT</li> <li>Peer Detection Enabled? y Peer Server: SM</li> </ul>
be optimized to reduce the use of Communication Manager audio resource possible. add signaling-group 1 Page 1 o SIGNALING GROUP Group Number: 1 Group Type: sip IMS Enabled? n Transport Method: tcp Q-SIP? n SIP Enabled LS IP Video? n Enabled? y Peer Server: SM
be optimized to reduce the use of Communication Manager audio resource possible. add signaling-group 1 Page 1 o SIGNALING GROUP Group Number: 1 Group Type: sip IMS Enabled? n Transport Method: tcp Q-SIP? n SIP Enabled LS IP Video? n Peer Detection Enabled? y Peer Server: SM
add signaling-group 1       Page 1 o         SIGNALING GROUP       SIGNALING GROUP         Group Number: 1       Group Type: sip         IMS Enabled? n       Transport Method: top         Q-SIP? n       SIP Enabled LS         IP Video? n       Enable SIPS URI for SRT         Peer Detection Enabled? y       Peer Server: SM
add signaling-group 1       Page 1 o         SIGNALING GROUP       SIGNALING GROUP         Group Number: 1       Group Type: sip         IMS Enabled? n       Transport Method: tcp         Q-SIP? n       SIP Enabled LS         IP Video? n       Enable SIPS URI for SRT         Peer Detection Enabled? y       Peer Server: SM
SIGNALING GROUP Group Number: 1 Group Type: sip IMS Enabled? n Transport Method: tcp Q-SIP? n SIP Enabled LS IP Video? n Enable SIPS URI for SRT Peer Detection Enabled? y Peer Server: SM
SIGNALING GROUP Group Number: 1 Group Type: sip IMS Enabled? n Transport Method: tcp Q-SIP? n SIP Enabled LS IP Video? n Enable SIPS URI for SRT Peer Detection Enabled? y Peer Server: SM
IMS Enabled? n       Transport Method: tcp         Q-SIP? n       SIP Enabled LS         IP Video? n       Enable SIPS URI for SRT         Peer Detection Enabled? y       Peer Server: SM
IMS Enabled? n       Transport Method: tcp         Q-SIP? n       SIP Enabled LS         IP Video? n       Enable SIPS URI for SRT         Peer Detection Enabled? y       Peer Server: SM
IP Video? n Enable SIPS URI for SRT Peer Detection Enabled? y Peer Server: SM
Peer Detection Enabled? y Peer Server: SM
Near-end Node Name: CLAN-1A02 Far-end Node Name: SM1
Near end Node Name. Chris 1802 Far end Node Name. DAr
Near-end Listen Port: 5060 Far-end Listen Port: 5060
Far-end Network Region: 1
Far-end Domain: avaya.com
Bypass If IP Threshold Excee
Incoming Dialog Loopbacks: eliminate REC 3389 Comfort No
Incoming Dialog Loopbacks: eliminate RFC 3389 Comfort No DTMF over IP: rtp-payload Direct IP-IP Audio Connection

Description
<ul> <li>Trunk Group Use the add trunk-group <i>n</i> command, where <i>n</i> is an unused trunk group, to create a new trunk group for SIP trunk to Session Manager as follows:</li> <li>On Page 1: <ul> <li>Set the Group Type to <i>sip</i>.</li> <li>Enter a descriptive name for the Group Name.</li> <li>Enter an available trunk access code (TAC) that is consistent with the existing dial plan in the TAC field.</li> <li>Set the Service Type to <i>public-ntwrk</i>.</li> </ul> </li> </ul>
<ul> <li>Set the Member Assignment Method to <i>auto</i>.</li> <li>Set the Signaling Group to the signaling group configured in the previous step.</li> <li>Set the Number of Members field to the number of channels available in this trunk.</li> <li>add trunk-group 1 Page 1 of 21         <pre>             TRUNK GROUP             Group Number: 20 Group Type: sip CDR Reports: y             Group Name: 911 calls COR: 1 TN: 1 TAC: 101             Direction: two-way Outgoing Display? n             Dial Access? n             Queue Length: 0             Service Type: public-ntwrk Auth Code? n             Member Assignment Method: auto             Signaling Group: 1             Number of Members: 10             </pre></li></ul>
Public Unknown Numbering         Public unknown numbering defines the calling party number to be sent to the far-end.         An entry was created that will be used by the trunk groups defined in previous step. In the example shown below, all calls originating from a 7-digit extension beginning with 6665 and routed over trunk group 1.            Change public-unknown-numbering 0

Step	Description							
8.	Automatic Route Selection For the compliance test, AR Session Manager. The dialed (FAC) for ARS. Use the <b>ch</b> table. Two entries were crea- the ARS feature access code case, the preceding <b>9</b> is reme- entry. The two resulting ent <b>Note</b> : Accessing ARS witho <b>Dialing without FAC</b> field <b>options</b> command to view it A third entry is highlighted This is used if the ERS is un number 1514904xxxx. The This dialed string is mapped connected to the PSTN.	A (ARS) S was used d string of ange ars a ated in the e were rout oved by Al tries (for 1) but first dia is enabled. ts current s below which available a ECRC nur	l to route of 9 was con nalysis co ARS table ed to the H RS before l and 911) ling the F. Use the d tate. ch is used and the EC nber begin	emergency of figured as the ommand to control e so that call EGW (e.g., 9 searching the are highlight AC, is only p lisplay system to route eme GW initiates as with the control	the feature access code ereate an entry in the ARS is dialed with or without 1911 or 911). In either the table for a matching inted below. bossible if the ARS/AAR em-parameters customer- ergency calls to the ECRC. a call to the ECRC lialed string of <i>1514904</i> .			
	change ars analysis 11	ARS D	IGIT ANALY		Page 1 of 2 Percent Full: 3			
	Dialed String 11 911	Total Min Max 2 2 3 3	Route Pattern 1 1	Call Nod Type Num emer emer	e ANI Reqd n n			
	303538xxxx 1514904	10 10 11 11	12 11	natl natl	n n n			

p			Description		
	Patterns		•		
Use the	e change rou	i <b>te nattern <i>n</i> co</b> r	mmand, where <i>n</i> is an	unused route patter	rn to
	0	-		-	
			ich of the dialed string		
the AR	S table. Two	separate entries	were created for the 9	11 calls to be route	ed
proper	lv. The first e	entry relates to th	e call being routed to	EGW via Session N	Manager.
			ria a PRI trunk using th		
		c call is fould v	la a l Ki ti ulik usilig ti		ins rout
pattern					
• Pat	ttern Name -	<ul> <li>Set to any desc</li> </ul>	criptive name		
• Gr	p No 1:- Set	to 1 for 911 call	ls routed to EGW via S	Session Manager. In	n this
			are deleted and 911 ins	•	
		-			
-	-	or 9911 because f	first 9 is absorbed as a	Facility Access Co	ode for
AR	S.				
• Gr	n No 2 Set	to 11 for 911 cal	lls to be sent directly to	O FCRC via PSTN	Note th
					. 11010 11
	<b>U</b> 1		nfigured for calls to P		
• LA	$\mathbf{R}$ – Set to <b>n</b>	ext. This enables	S Communication Man	ager to route the ca	all to
				e	
EC	RC if the 91	l calls fails to es	tablish because EGW	1S (10W/11)	
Note: I			tablish because EGW e PRI trunk are not pr		ılt <b>[3]</b>
Note: I	Details for co				ılt <b>[3]</b> fo
Note: I further	Details for co	nfiguration of th	e PRI trunk are not pr	ovided here. Consu	ılt <b>[3]</b> fo
Note: I further	Details for co details.	nfiguration of th	e PRI trunk are not preserter 1 Pattern Name: 9	ovided here. Consu Page 1 of P11 calls	
Note: I further	Details for co details.	nfiguration of th	er: 1 Pattern Name: 9 AN? n Secure SIP? r	Page 1 of Page 1 of	3
Note: I further	Details for co details. nge route-pat	nfiguration of th	er: 1 Pattern Name: 9 AN? n Secure SIP? r Inserted	Page 1 of Page 1 of DI1 calls	3 s/ ixc
Note: I further	Details for co details. nge route-pat	tern 1 Pattern Numbe SCCZ Pfx Hop Toll No. Mrk Lmt List Del	er: 1 Pattern Name: 9 AN? n Secure SIP? r Inserted Digits	Page 1 of Page 1 of	3 s/ IXC IG
Note: I further	Details for co details. nge route-pat	nfiguration of th	er: 1 Pattern Name: 9 AN? n Secure SIP? r Inserted Digits	Page 1 of Page 1 of DCG QS	3 S/ IXC IG tw
Note: I further	Details for co details. nge route-pat Grp FRL NPA 1 No 1	tern 1 Pattern Numbe SCCZ Pfx Hop Toll No. Mrk Lmt List Del Dgts	er: 1 Pattern Name: S AN? n Secure SIP? r Inserted Digits	Page 1 of Page 1 of DCS QSS Int	3 S/ IXC IG tw user
Note: I further	Details for co details. nge route-pat Grp FRL NPA 1 No 1	tern 1 Pattern Numbe SCCZ Pfx Hop Toll No. Mrk Lmt List Del Dgts <b>3</b>	er: 1 Pattern Name: 9 AN? n Secure SIP? r Inserted Digits 911	Page 1 of Page 1 of Page 1 of DCG QS Int n	3 S/ IXC IG tw user user
Note: I further	Details for co details. nge route-pat Grp FRL NPA 1 No 1	tern 1 Pattern Numbe SCCZ Pfx Hop Toll No. Mrk Lmt List Del Dgts <b>3</b>	er: 1 Pattern Name: 9 AN? n Secure SIP? r Inserted Digits 911	Page 1 of Page 1 of Page 1 of DCS QSS Int n n n n	3 S/ IXC IG tw user user user user
Note: I further	Details for co details. nge route-pat Grp FRL NPA 1 No 1	tern 1 Pattern Numbe SCCZ Pfx Hop Toll No. Mrk Lmt List Del Dgts <b>3</b>	er: 1 Pattern Name: 9 AN? n Secure SIP? r Inserted Digits 911	Page 1 of Page 1 of DCS QSS Int n n n n n	3 S/ IXC IG user user user user user
Note: I further	Details for co details. nge route-pat Grp FRL NPA 1 No 1	tern 1 Pattern Numbe SCCZ Pfx Hop Toll No. Mrk Lmt List Del Dgts <b>3</b>	er: 1 Pattern Name: 9 AN? n Secure SIP? r Inserted Digits 911	Page 1 of Page 1 of Page 1 of DCS QSS Int n n n n	3 S/ IXC IG user user user user user
Note: I further	Details for co details. nge route-pat Grp FRL NPA : No 1 1 0 11 0	nfiguration of th	er: 1 Pattern Name: 9 AN? n Secure SIP? r Inserted Digits 911 1514904xxxx	Page 1 of Page 1 of Page 1 of Page 1 of Page 1 of QS: Ini n n n n n	3 S/ IXC IG tw user user user user user user user
Note: I further	Details for co details. nge route-pat Grp FRL NPA 1 No 1	nfiguration of th tern 1 Pattern Numbe SCCZ Pfx Hop Toll No. Mrk Lmt List Del Dgts 3 3 ISC CA-TSC ITC	er: 1 Pattern Name: 9 AN? n Secure SIP? r Inserted Digits 911	Page 1 of Page 1 of Page 1 of Page 1 of Page 1 of QS: Ini n n n n n	3 S/ IXC IG tw user user user user user user
Note: I further	Details for co details. mge route-patr Grp FRL NPA : No II 1 0 11 0 BCC VALUE	nfiguration of th tern 1 Pattern Numbe SCCZ Pfx Hop Toll No. Mrk Lmt List Del Dgts 3 3 1 SC CA-TSC ITC	er: 1 Pattern Name: 9 AN? n Secure SIP? r Inserted Digits 911 1514904xxxx	Page 1 of Page 1 of Page 1 of Page DC: QS: Ini n n n n PARM No. Numbering	3 S/ IXC IG tw user user user user user user
Note: I further	Details for co details. mge route-patr Grp FRL NPA : No II 1 0 11 0 BCC VALUE	nfiguration of th tern 1 Pattern Numbe SCCZ Pfx Hop Toll No. Mrk Lmt List Del Dgts 3 3 TSC CA-TSC ITC Request	er: 1 Pattern Name: 9 AN? n Secure SIP? r Inserted Digits 911 1514904xxxx	Page 1 of Page 1 of Page 1 of Page 1 of DC3 QS3 Inii n n n n PARM No. Numbering Dgts Format	3 S/ IXC IG user user user user user user
Note: I further	Details for co details. mge route-pat Grp FRL NPA : No 1 1 0 11 0 BCC VALUE 0 0 1 2 M 4 W	nfiguration of th tern 1 Pattern Numbe SCCF Pfx Hop Toll No. Mrk Lmt List Del Dgts 3 3 ISC CA-TSC ITC Request res	er: 1 Pattern Name: 9 AN? n Secure SIP? r Inserted Digits 911 1514904xxxx	Page 1 of Page 1 of Page 1 of Page 1 of DC3 QS3 Inii n n n n PARM No. Numbering Dgts Format	3 IG IG tw user user user user user g LAR
Note: I further	Details for co details.	nfiguration of th	er: 1 Pattern Name: 9 AN? n Secure SIP? r Inserted Digits 911 1514904xxxx C BCIE Service/Feature	Page 1 of Page 1 of Page 1 of Page 1 of DC3 QS3 Inii n n n n PARM No. Numbering Dgts Format	3 S/ IXC IG user user user user user g LAR next
Note: I further	Details for co details.	nfiguration of th tern 1 Pattern Number SCCF Pfx Hop Toll No. Mrk Lmt List Del Dgts 3 3 TSC CA-TSC ITC Request n reson re	er: 1 Pattern Name: S AN? n Secure SIP? r Inserted Digits 911 1514904xxxx C BCIE Service/Feature	Page 1 of Page 1 of Page 1 of Page 1 of DC3 QS3 Inii n n n n PARM No. Numbering Dgts Format	3 S/ IXC IG user user user user user g LAR none none
Note: I further	Details for co details.	nfiguration of th tern 1 Pattern Number SCCP Pfx Hop Toll No. Mrk Lmt List Del Dgts 3 3 TSC CA-TSC ITC Request n ress n ress n ress n ress	er: 1 Pattern Name: S AN? n Secure SIP? r Inserted Digits 911 1514904xxxx C BCIE Service/Feature	Page 1 of Page 1 of Page 1 of Page 1 of DC3 QS3 Inii n n n n PARM No. Numbering Dgts Format	3 S/ IXC IG user user user user user g LAR none none

Step	Description																				
10.	Route Pattern – PSTN Trunk																				
	In cases where the EGW is operational but it can not reach the ERS due to a WAN failure, the EGW routes the call back to Communication Manager via Session																				
												Manager. Communication Manager then routes the call out the PSTN trunk using the									
												route pattern configured below.									
	abango routo pattorn 11	Page 1 of 3																			
	change route-pattern 11 Pattern Number: 11 Pattern Name: PSTN SCCAN? n Secure SIP? n	Page 1 of 3																			
	Grp FRL NPA Pfx Hop Toll No. Inserted	DCS/ IXC																			
		No Mrk Lmt List Del Digits	QSIG																		
		Dgts 1: <b>11 0</b>	Intw n user																		
	2:	n user																			
	3:	n user																			
	4:	n user																			
	5: 6:	n user n user																			
	BCC VALUE TSC CA-TSC ITC BCIE Service/Feature PARM No. Number:																				
	0 1 2 M 4 W Request	Dgts Format ubaddress																			
	1: yyyyn n rest 2: yyyyn n rest	none																			
	2:yyyynn rest 3:yyyynn rest	none																			
	4: y y y y y n n rest	none																			
	5: yyyyn n rest	none																			
	6: yyyyn n rest	none																			
11.	Inbound Call Routing – Temporary Callback Numbers																				
	When the PSAP uses the callback number, it must be routed to	o the correct destination.																			
	If the callback number is a DID number temporarily assigned	by the EGW as a																			
	callback number, then the call must get routed to the EGW to	•																			
	internal extension. Use the <b>change inc-call-handling-trmt trunk-group</b> <i>n</i> command,																				
	where $n$ is the trunk group to the PSTN, to insert a 9 in front of all the DID numbers																				
	used by the EGW as temporary DIDs. The preceding 9 (whic																				
	access code) will instruct Communication Manager to process	s the digits using ARS to																			
	determine the route.																				
	change inc-call-handling-trmt trunk-group 11	Page 1 of 3																			
	INCOMING CALL HANDLING TREATMENT Service/ Number Del Insert	Per Call Night																			
	Feature Len Digits netwrk 10 303538xxxx 9	CPN/BN Serv																			

р	Description											
2. R	Routing Callback Calls to the EGW										_	
	Use the <b>change ars analysis</b> command to add an entry in the ARS table for each D											
				•				-				
						es the int						
p	attern tha	t routes	the ca	all to th	e EG	W via Se	ssion M	lanage	r. In t	he exan	nple b	elov
						oute patte						
		String 5	05550	<i>J.</i>	50510	face pulle	111 12 (0	10410	une eu		,,, ,1	u DC
IV	lanager.											
	change ar	s analys	sis 11							Page	1 of	2
				1	ARS DI	IGIT ANALY		LE	_		-	-
						Location:	all		Perc	ent Ful	1:	3
		Dialed		TO	tal	Route	Call	Node	ΔNT			
		String				Pattern	Туре	Num	Reqd			
	11			2	2	1	emer		n			
	911			3		1	emer		n			
	30353	8 <b>8</b> xxxx		10	10	12	natl		n			
	15149	904		11	11	11	natl		n			
B. C	Callback	Douto F	Dattar	'n								
			P			nand to c						
ro	ne EGW a oute patte	assigned ern is cre				he route j						
ro	ne EGW a oute patte xceptions	assigned ern is cre	eated	the sam	e as t	he route j	pattern	1 in <b>St</b>				
ro	ne EGW a oute patte xceptions	assigned ern is cre	eated	the sam	e as t	he route j	pattern	1 in <b>St</b>				
ro	ne EGW a oute patte xceptions • Pa	assigned ern is cre s: ttern Na	eated and and and and and and and and and an	the sam – Enter	e as t and d	he route j lescriptive	pattern e name.	1 in <b>St</b>	<b>ep 9</b> v	vith the	follow	ving
ro	ne EGW a oute patte xceptions • Pa • Re	assigned ern is cre s: ttern Na move th	eated a ame - ne seco	the sam – Enter ond trui	e as t and d nk cho	he route plescriptive	oattern e name. yn in ro	1 in <b>St</b> ute pat	<b>ep 9</b> v tern 1	vith the 1. This	follow	wing pat
ro	ne EGW a oute patte xceptions • Pa • Re is s	assigned ern is cre s: ttern Na move th similar to	ame - ame seco o one	the sam – Enter ond trun in <b>Step</b>	and d and cho 9 ex	he route plescriptive bice show cept there	pattern e name. yn in rou e is no a	1 in <b>St</b> ute pat	<b>ep 9</b> v tern 1	vith the 1. This	follow	ving pat
ro	ne EGW a oute patte xceptions • Pa • Re is s	assigned ern is cre s: ttern Na move th similar to	ame - ame seco o one	the sam – Enter ond trun in <b>Step</b>	and d and cho 9 ex	he route plescriptive	pattern e name. yn in rou e is no a	1 in <b>St</b> ute pat	<b>ep 9</b> v tern 1	vith the 1. This	follow	ving pat
ro	ne EGW a oute patte xceptions • Pa • Re is s	assigned ern is cre s: ttern Na move th similar to	ame - ame seco o one	the sam – Enter ond trun in <b>Step</b>	and d and cho 9 ex	he route plescriptive bice show cept there	pattern e name. yn in rou e is no a	1 in <b>St</b> ute pat	<b>ep 9</b> v tern 1	vith the 1. This	follow	ving pat
ro	ne EGW a oute patte xceptions • Pa • Re is s bac	assigned ern is cre s: ttern Na move th similar to	eated f ame - ne seco o one TN if	the sam - Enter ond true in <b>Step</b> FEGW	and d and cho 9 ex	he route plescriptive bice show cept there	pattern e name. yn in rou e is no a	1 in <b>St</b> ute pat	<b>ep 9</b> v tern 1	vith the 1. This	follow	ving pat to g
ro	ne EGW a oute patte xceptions • Pa • Re is s bac	assigned ern is cre s: ttern Na move th similar to ck to PS	eated f ame - le seco o one TN if	the sam - Enter ond true in <b>Step</b> FEGW	and d and d nk cho 9 ex fails t	he route plescriptive oice show cept there o respond	e name. 7n in roi e is no a l. Pattern	1 in St ute pat addition	ep 9 v tern 1 nal en	vith the 1. This try for a	route a call t	ving pat to g
ro	ne EGW a oute patte xceptions • Pa • Re is s bac	assigned ern is creas: ttern Na move th similar to ck to PS	eated f ame - ne seco o one TN if	- Enter ond trun in <b>Step</b> EGW 1	and d nk cho 9 ex fails t	he route plescriptive oice show cept there o respond	e name. 7n in rol e is no a l. Pattern Secure S	1 in St ute pat addition	ep 9 v tern 1 nal en	vith the 1. This try for a Page	follow route a call t	pat to g
ro	ne EGW a oute patte xceptions • Pa • Re is s bac change Grp	assigned ern is creas: ttern Na move th similar to ck to PS	ame - ane seco o one TN if	- Enter ond trun in Step EGW 1 12 Pattern Hop Toll	and d nk cho 9 ex fails t	he route p lescriptive oice show cept there o respond er: 12 N? n Inserted	e name. 7n in rol e is no a l. Pattern Secure S	1 in St ute pat addition	ep 9 v tern 1 nal en	vith the 1. This try for a Page	follow route a call t s <sup>1 of</sup> DCS/	pat to g
ro	ne EGW a oute patte xceptions • Pa • Re is s bac	assigned ern is creas: ttern Na move th similar to ck to PS	ame - ane seco o one TN if	- Enter ond trun in <b>Step</b> EGW 1	and d nk cho 9 ex fails t	he route p lescriptive oice show cept there o respond er: 12 .N? n Inserted Digits	e name. 7n in rol e is no a l. Pattern Secure S	1 in St ute pat addition	ep 9 v tern 1 nal en	vith the 1. This try for a Page	follow route a call t	pat to g
ro	ne EGW a oute patte xceptions • Pa • Re is s bac	assigned ern is cre s: ttern Na move th similar to ck to PS route-pa	ame - ane seco o one TN if	- Enter ond trun in Step EGW 1 12 Pattern Hop Toll	and d nk cho 9 ex fails t	he route p lescriptive oice show cept there o respond er: 12 .N? n Inserted Digits	e name. 7n in rol e is no a l. Pattern Secure S	1 in St ute pat addition	ep 9 v tern 1 nal en	vith the 1. This try for a Page	follow route a call f s DCS/ QSIG Intw	pat to g
ro	he EGW a bute patter xceptions • Pa • Re is s bac Change Grp No 1: 1	assigned ern is cre s: ttern Na move th similar to ck to PS route-pa	ame - ane seco o one TN if	- Enter ond trun in Step EGW 1 12 Pattern Hop Toll	and d nk cho 9 ex fails t	he route p lescriptive oice show cept there o respond er: 12 .N? n Inserted Digits	e name. 7n in rol e is no a l. Pattern Secure S	1 in St ute pat addition	ep 9 v tern 1 nal en	vith the 1. This try for a Page	follow route a call t s <sup>1 of</sup> DCS/ QSIG	pat to g
ro	<pre>he EGW a bute patter transformed patter transf</pre>	assigned ern is cre s: ttern Na move th similar to ck to PS route-pa	ame - ane seco o one TN if	- Enter ond trun in Step EGW 1 12 Pattern Hop Toll	and d nk cho 9 ex fails t	he route p lescriptive oice show cept there o respond er: 12 .N? n Inserted Digits	e name. 7n in rol e is no a l. Pattern Secure S	1 in St ute pat addition	ep 9 v tern 1 nal en	vith the 1. This try for a Page	follow route a call f s DCS/ QSIG Intw	pat to g
ro	he EGW a bute patter xceptions • Pa • Re is s bac change • Change • Change • Change • Change	assigned ern is cre s: ttern Na move th similar to ck to PS route-pa	ame - ane seco o one TN if	- Enter ond trun in Step EGW 1 12 Pattern Hop Toll	and d nk cho 9 ex fails t	he route p lescriptive oice show cept there o respond er: 12 .N? n Inserted Digits	e name. 7n in rol e is no a l. Pattern Secure S	1 in St ute pat addition	ep 9 v tern 1 nal en	vith the 1. This try for a Page	follow route a call 1 s DCS/ QSIG Intw n n	pat to g
ro	he EGW a bute patter xceptions • Pa • Re is s bac change Grp No 1: 1 2: 3: 4:	assigned ern is cre s: ttern Na move th similar to ck to PS route-pa	ame - ane seco o one TN if	- Enter ond trun in Step EGW 1 12 Pattern Hop Toll	and d nk cho 9 ex fails t	he route p lescriptive oice show cept there o respond er: 12 .N? n Inserted Digits	e name. 7n in rol e is no a l. Pattern Secure S	1 in St ute pat addition	ep 9 v tern 1 nal en	vith the 1. This try for a Page	follow route a call f s DCS/ QSIG Intw n n n	use use use
ro	he EGW a bute patter xceptions • Pa • Re is s bac change Grp No 1: 1 2: 3: 4: 5:	assigned ern is cre s: ttern Na move th similar to ck to PS route-pa	ame - ane seco o one TN if	- Enter ond trun in Step EGW 1 12 Pattern Hop Toll	and d nk cho 9 ex fails t	he route p lescriptive oice show cept there o respond er: 12 .N? n Inserted Digits	e name. 7n in rol e is no a l. Pattern Secure S	1 in St ute pat addition	ep 9 v tern 1 nal en	vith the 1. This try for a Page	follow route a call f s DCS/ QSIG Intw n n n n	use use use use
ro	he EGW a bute patter xceptions • Pa • Re is s bac change Grp No 1: 1 2: 3: 4:	assigned ern is cre s: ttern Na move th similar to ck to PS route-pa	ame - ane seco o one TN if	- Enter ond trun in Step EGW 1 12 Pattern Hop Toll	and d nk cho 9 ex fails t	he route p lescriptive oice show cept there o respond er: 12 .N? n Inserted Digits	e name. 7n in rol e is no a l. Pattern Secure S	1 in St ute pat addition	ep 9 v tern 1 nal en	vith the 1. This try for a Page	follow route a call f s DCS/ QSIG Intw n n n	pat to g
ro	he EGW a pute patter xceptions • Pa • Re is s bac change Grp No 1: 1 2: 3: 4: 5: 6:	assigned ern is cre s: ttern Na move th similar to ck to PS route-pa	ame - ne seco o one TN if	- Enter ond trun in Step EEGW 1 12 Pattern Hop Toll Lmt List	Numbe sccA Numbe sccA No. Dgts	he route plescriptive oice show cept there o respond r: 12 N? n Inserted Digits	e name. n in rol e is no a l. Pattern Secure	1 in St ute pat addition Name: SIP? n	ep 9 v tern 1 nal en callba	vith the 1. This try for a Page	follow route a call f s DCS/ QSIG Intw n n n n n n	pat to g
ro	he EGW a bute patter xceptions • Pa • Re is s bad change Grp No 1: 1 2: 3: 4: 5: 6: BC	assigned ern is cre s: ttern Na move th similar to ck to PS route-pa o FRL NPA 0	ame - ne seco o one TN if	- Enter ond trun in Step EEGW 1 12 Pattern Hop Toll Lmt List	Numbe sccA Numbe sccA No. Dgts	he route p lescriptive oice show cept there o respond er: 12 .N? n Inserted Digits	e name. n in rol e is no a l. Pattern Secure	1 in St ute pat addition Name: SIP? n	ep 9 v tern 1 nal en Callba	vith the 1. This try for a Page .ck call	follow route a call f s DCS/ QSIG Intw n n n n n n ering	pat to g IXC
ro	he EGW a bute patter xceptions • Pa • Re is s bad change Grp No 1: 1 2: 3: 4: 5: 6: BC	assigned ern is cre s: ttern Na move th similar to ck to PS route-pa	ame - ne seco o one TN if	- Enter ond trun in Step EEGW 1 12 Pattern Hop Toll Lmt List	Numbe sccA Numbe sccA No. Dgts	he route plescriptive oice show cept there o respond r: 12 N? n Inserted Digits	e name. n in rol e is no a l. Pattern Secure	1 in St ute pat addition Name: SIP? n	ep 9 v tern 1 nal en callba	I. This try for a Page ck call	follow route a call f s DCS/ QSIG Intw n n n n n n ering	pat to g
ro	he EGW a pute patter xceptions • Pa • Re is s bac change Grp No 1: 1 2: 3: 4: 5: 6: 0 1	assigned ern is cre s: ttern Na move th similar to ck to PS route-pa o FRL NPA 0 C VALUE	attern A Pfx : Mrk :	- Enter ond trun in Step EEGW 1 12 Pattern Hop Toll Lmt List	e as t and d nk cho 9 ex fails t Numbe SCCA No. Del Dgts	he route p lescriptive oice show cept there o respond r: 12 .N? n Inserted Digits	e name. n in rol e is no a l. Pattern Secure	1 in St ute pat addition Name: SIP? n	ep 9 v tern 1 nal en callba	vith the 1. This try for a Page .ck call	follow route a call 1 a call 1 s DCS/ QSIG Intw n n n n n ering at	pat pat to g IXC use use use use use LAR
ro	he EGW a pute patter xceptions • Pa • Re is s bac change Grp No 1: 1 2: 3: 4: 5: 6: 0 1 1: y y	assigned ern is creas: ttern Na move th similar to ck to PS route-pa o FRL NPA 0 C VALUE 2 M 4 W	TSC of a n	- Enter ond trun in Step EEGW 1 12 Pattern Hop Toll Lmt List	Numbe sccA Numbe sccA No. Del Dgts	he route p lescriptive oice show cept there o respond r: 12 N? n Inserted Digits BCIE Ser	e name. n in rol e is no a l. Pattern Secure	1 in St ute pat addition Name: SIP? n	ep 9 v tern 1 nal en callba	I. This try for a Page ck call	follow route a call f a call f s DCS/ QSIG Intw n n n n n n ering at	pat to g IXC
ro	he EGW a pute patter xceptions • Pa • Re is s bac change Grp No 1: 1 2: 3: 4: 5: 6: BC 0 1 1: y y 2: y y	assigned ern is created ttern Na move the similar to ck to PS route-pa o FRL NPA 0 C VALUE 2 M 4 W y y y n y y y n	TSC of the second of the secon	- Enter ond trun in Step EEGW 1 12 Pattern Hop Toll Lmt List	e as t and d nk cho 9 ex fails t Numbe SCCA No. Del Dgts	he route p lescriptive oice show cept there o respond r: 12 N? n Inserted Digits BCIE Ser	e name. n in rol e is no a l. Pattern Secure	1 in St ute pat addition Name: SIP? n	ep 9 v tern 1 nal en callba	I. This try for a Page ck call	follow route a call f a call f a call f n n n n n n n n n n n n n n n n n n n	pat to g IXC USE USE USE USE USE USE USE USE USE USE
ro	he EGW a pute patter xceptions • Pa • Re is s bac change Grp No 1: 1 2: 3: 4: 5: 6: BC 0 1 1: y y 2: y y 3: y y	assigned ern is created ttern Na move the similar to ck to PS route-pa o FRL NPA 0 C VALUE 2 M 4 W y y y n y y y n	TSC of a n n n n n n	- Enter ond trun in Step EEGW 1 12 Pattern Hop Toll Lmt List	e as t and d hk cho 9 ex fails t Numbe SCCA No. Del Dgts ITC res res	he route p lescriptive oice show cept there o respond er: 12 N? n Inserted Digits	e name. n in rol e is no a l. Pattern Secure	1 in St ute pat addition Name: SIP? n	ep 9 v tern 1 nal en callba	I. This try for a Page ck call	follow route a call f a call f a call f n n n n n n n n n n n n n n n n n n n	pat pat to g IXC use use use use use tar none
ro	he EGW a pute patter xceptions • Pa • Re is s bac change Grp No 1: 1 2: 3: 4: 5: 6: BC 0 1 1: y y 2: y y 3: y y 4: y y	assigned ern is created ttern Na move the similar to ck to PS route-pa o FRL NPA 0 C VALUE 2 M 4 W y y y n y y y n y y y n	TSC	- Enter ond trun in Step EEGW 1 12 Pattern Hop Toll Lmt List	e as t and d hk cho 9 ex fails t Numbe SCCA No. Del Dgts ITC res res res	he route p lescriptive oice show cept there o respond er: 12 N? n Inserted Digits BCIE Ser	e name. n in rol e is no a l. Pattern Secure	1 in St ute pat addition Name: SIP? n	ep 9 v tern 1 nal en callba	I. This try for a Page ck call	follow route a call f a call f s DCS/ QSIG Intw n n n n n ering at	IXC USE USE USE USE USE USE USE USE
ro	he EGW a pute patter xceptions • Pa • Re is s bac change Grp No 1: 1 2: 4: 5: 6: BC 0 1 1: y y 2: y y 3: y y 4: y y 5: y y	assigned ern is created ttern Na move the similar to ck to PS route-pa o FRL NPA 0 C VALUE 2 M 4 W y y y n y y y n	TSC of the second of the secon	- Enter ond trun in Step EEGW 1 12 Pattern Hop Toll Lmt List	e as t and d hk cho 9 ex fails t Numbe SCCA No. Del Dgts ITC res res	he route p lescriptive oice show cept there o respond er: 12 N? n Inserted Digits : BCIE Ser	e name. n in rol e is no a l. Pattern Secure	1 in St ute pat addition Name: SIP? n	ep 9 v tern 1 nal en callba	I. This try for a Page ck call	follow route a call f a call f s DCS/ QSIG Intw n n n n n ering at	pat to g IXC use use use use use tar next

### **5.2. Station Configuration**

This section will describe the settings required of each of the different station types to support the EGW functionality. Each station is required to have an Emergency Location Extension configured.

Step	Description							
1.	H.323 and SIP Telephones							
	-	cy Location Extension configuration for an						
	1 0	<b>display station</b> <i>n</i> command, where <i>n</i> is the						
	station extension, to view the settings.	By default, the Emergency Location Extension						
	is the same as the station extension and	the Always Use field is set to y. If the Always						
		y Location Extension will be taken from the IP						
	network map form if an extension is con	nfigured there.						
	1	5						
	display station 6665011	Page 2 of 4						
	FEATURE OPTIONS	STATION						
	LWC Reception: spe	Auto Select Any Idle Appearance? n						
	LWC Activation? v	Coverage Msg Retrieval? y						
	LWC Log External Calls? n	Auto Answer: none						
	CDR Privacy? n	Data Restriction? n						
	Redirect Notification? v	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							
		EMU Login Allowed? n						
	H.320 Conversion? n	Per Station CPN - Send Calling Number?						
	Service Link Mode: as-needed	EC500 State: enabled						
	Multimedia Mode: enhanced	Audible Message Waiting? n						
	MWI Served User Type:	Display Client Redirection? n						
	AUDIX Name:	Select Last Used Appearance? n						
		Coverage After Forwarding? s						
		Multimedia Early Answer? n						
		Direct IP-IP Audio Connections? y						
	Emergency Location Ext: 666-5011	Always Use? y IP Audio Hairpinning? n						

Step	Description		
2.	digital telephone. Use the <b>displa</b> to view the settings. By default, station extension. There is no <b>Al</b>	mergency Location Extension configuration for a <b>y station</b> <i>n</i> command, where <i>n</i> is the station extension the Emergency Location Extension is the same as the <b>ways Use</b> field as there was for the H.323/SIP og telephones are configured in a similar way.	
	display station 6665201	Page 2 of 4 STATION	
	FEATURE OPTIONS	STATION	
	LWC Reception: spe		
	LWC Activation? y	Coverage Msg Retrieval? y	
	LWC Log External Calls? n	Auto Answer: none	
	CDR Privacy? n	Data Restriction? n	
	Redirect Notification? y	Call Waiting Indication: y	
	Per Button Ring Control? n	Att. Call Waiting Indication: y	
	Bridged Call Alerting? n	Distinctive Audible Alert? y	
	Switchhook Flash? y Ignore Rotary Digits? n	Adjunct Supervision? y	
	H.320 Conversion? n Service Link Mode: as-	Per Station CPN - Send Calling Number? -needed	
	Multimedia Mode: bas MWI Served User Type: AUDIX Name:	aic Audible Message Waiting? n	
	nobin name.	Coverage After Forwarding? s	
		Multimedia Early Answer? n	
		Direct IP-IP Audio Connections? y	
		DITECT IL-IL AUGIO CONNECTIONS: A	

Step	D	escription	
3.	Avaya IP one-X® Communicator		
	The example shows the settings for an Avaya IP one-X® Communicator (H.323 and		
	SIP). Use the <b>display station</b> $n$ command, where $n$ is the station extension, to view the		
	settings. It contains an additional field named <b>Remote Softphone Emergency Calls</b> .		
	In the case of the compliance test, the Avaya IP one-X® Communicator was treated the same as any other IP telephone on the enterprise, so the <b>Remote Softphone</b>		
1	<b>Emergency Calls</b> field was left with the	e default value of <i>as-on-local</i> . This setting	
1	instructs the Communication Manager t	o use the value in the Emergency Location	
		tension. This value can still be overwritten by	
	-	f permitted by the setting of the Always Use	
	field. Additionally, the ESL software wa	as loaded on the desktop where Avaya IP one-	
		automatically reports its location to EGW.	
	As communicator was instance which	automatically reports its focation to EOW.	
	display station 6665023	Page 2 of 5	
		STATION	
l	FEATURE OPTIONS		
	LWC Reception: spe	Auto Select Any Idle Appearance? n	
	LWC Activation? y	Coverage Msg Retrieval? y	
	LWC Log External Calls? n CDR Privacy? n	Auto Answer: none Data Restriction? n	
I	Redirect Notification? v	Idle Appearance Preference? n	
	Per Button Ring Control? n	Bridged Idle Line Preference? n	
1	Bridged Call Alerting? n	Restrict Last Appearance? n	
l .	Active Station Ringing: single		
		EMU Login Allowed? n	
	H.320 Conversion? n	Per Station CPN - Send Calling Number?	
	Service Link Mode: as-needed	EC500 State: enabled	
	Multimedia Mode: enhanced MWI Served User Type:	Audible Message Waiting? n Display Client Redirection? n	
	AUDIX Name:	Select Last Used Appearance? n	
	AUDIA Name.	Coverage After Forwarding? s	
		Multimedia Early Answer? n	
	Remote Softphone Emergency Calls: a	s-on-local Direct IP-IP Audio Connections? y	
l	Emergency Location Ext: 666-5023	Always Use? y IP Audio Hairpinning? n	
1			

# 6. Configure the Avaya Endpoints

This section describes the configuration required of Avaya endpoints to support the EGW functionality. Avaya H.323 and SIP telephones require additions to the 46xxsettings.txt file to support layer 3 discovery. The PC running Avaya IP one-X® Communicator requires installation of the ESL software on it. No special configuration is required of analog or digital telephones.

Avaya H.323 and SIP Telephone Configuration File		
er to support layer 3 discovery, the following lines need to be added to the		
ettings.txt configuration file for Avaya H.323 and SIP telephones. The two		
ghted parameters in the SUBSCRIBELIST and WMLHOME URLs must be		
modified for a specific installation. The first parameter (10.80.130. 200) represents the		
ress of the private side of the primary EGW. The second parameter IP-PBX-ID		
to (7) number created in Section 7, Step 5. Since two separate Communication		
Managers were used in this compliance testing, for the IP endpoints registered to the		
d Communication Managers used IP-PBX ID of 11.		
1 Enable Settings		
PSLIST /		
UBSCRIBELIST <u>http://10.80.130.200/IP-PBX ID/r</u> NMPADD ""		
NMPSTRING public		
USHPORT 80		
USHCAP 2222		
MLHOME <u>http://10.80.130.200/wml/IP-PBX ID/service.html</u> (Needs to		
t for each phone type being used)		

Step	Description		
2.	Avaya IP one-X® Communicator – ESL software installation On the PC running the Avaya IP one-X® Communicator, launch the ESL setup application. A welcome screen will appear. Click Next to proceed.		
	😰 E911 Softphone Locator (ESL)		
	Welcome to the E911 Softphone Locator (ESL) Setup Wizard		
	The installer will guide you through the steps required to install E911 Softphone Locator (ESL) on your computer. WARNING: This computer program is protected by copyright law and international treaties.		
	Unauthorized duplication or distribution of this program, or any portion of it, may result in severe civil or criminal penalties, and will be prosecuted to the maximum extent possible under the law.		
	Cancel < Back Next >		

Step		Description	
3.	ESL Installation – Select the desired pr	belect Protocol between the composition of the second seco	liance test. Click Next.
	🔂 E911 Softp	none Locator (ESL)	
	Protocol		C9-1-1 ENABLE
	Which protocol	vould you like to use to communicate with the Emerge	ncy Gateway
	💽 HTTP (Ur	encrypted)	
	⊖ ssl/tls	Encrypted)	
		Cancel < E	Back Next >
4.	<b>ESL Installation</b> – Enter the IP address	<b>CGW Settings</b> s for both EGWs. Use the default po	ort <b>80</b> for HTTP. Click Next.
	🔀 E911 Soft	hone Locator (ESL)	
	Emergen	cy Gateway Settings	C9-1-1 ENABLE
	Please provide	he IP address(es) or FQDN of the Emergency Gateway	
	Primary EGV 10.80.130.3		
	Primary Port		
	Secondary 8 10.80.130.2		
	Secondary F		
		Cancel < B	ack Next >

Step	Description	
5.	ESL Installation – IP-PBX Settings	
	Enter the IP-PBX ID from Section 7, Step 5. Click Next.	
	🔁 E911 Softphone Locator (ESL)	
	IP-PBX Settings	
	Please provide the IP-PBX ID for this workstation, as configured on the Emergency Gateway (EGW)	
	IP-PBX ID:	
	Cancel < Back Next >	
6.	ESL Installation – Installation Folder	
0.	ESL Installation – Installation Folder Enter the installation folder and who should have access to the software. Click Next.	
	🔁 E911 Softphone Locator (ESL)	
	Select Installation Folder	
	The installer will install E911 Softphone Locator (ESL) to the following folder.	
	To install in this folder, click "Next". To install to a different folder, enter it below or click "Browse".	
	Eolder: C:\Program Files\Connexon Telecom Inc\E911 Softphone Locator (E Browse	
	Disk Cost	
	Install E911 Softphone Locator (ESL) for yourself, or for anyone who uses this computer:	
	Everyone	
	O Just me	
	Cancel < Back Next >	

<ul> <li>FSL Installation - Confirm Confirm the installation by clicking Next.</li> <li>Confirm Installation         <pre>             Confirm Installation</pre></li></ul>
8.       ESL Installation – Complete The following screen appears when installation is complete. Click Close to exit up application.         8.       ESL Installation – Complete The following screen appears when installation is complete. Click Close to exit up application.
8.       ESL Installation – Complete The following screen appears when installation is complete. Click Close to exit up application.         8.       ESL Installation – Complete The following screen appears when installation is complete. Click Close to exit up application.
8.       ESL Installation – Complete The following screen appears when installation is complete. Click Close to exit up application.         8.       ESL Installation – Complete The following screen appears when installation is complete. Click Close to exit up application.
8.       ESL Installation - Complete The following screen appears when installation is complete. Click Close to exit up application.         Installation Complete         Installation Complete         ESL Installation Complete
S.       ESL Installation - Complete The following screen appears when installation is complete. Click Close to exit up application.         Installation Complete       Installation Complete         Installation Complete       Installation Complete         ESL Installation Complete       Installation Complete
8. ESL Installation – Complete The following screen appears when installation is complete. Click Close to exit up application.           Image: E911 Softphone Locator (ESL)           Installation Complete           E911 Softphone Locator (ESL)           E911 Softphone Locator (ESL)
The following screen appears when installation is complete. Click <b>Close</b> to exit up application.           Image: Click close to exit up application           Image: Click click close to exit up application           Image: Click click click click click click           Image: Click cli
Installation Complete       C9-1-1 ENABLE         E911 Softphone Locator (ESL) has been successfully installed.
E911 Softphone Locator (ESL) has been successfully installed.
Click "Close" to exit
Please use Windows Update to check for any critical updates to the .NET Framework.
Cancel < Back Close

# 7. Configure 911 Enable Emergency Gateway (EGW)

The configuration of the EGW is performed by 911 Enable for the customer when the customer subscribes to 911 Enable's Emergency Routing Service. The information in this section is included simply as a reference.

Step	Description
1.	Login The EGW is configured via a web browser. To access the web interface, enter <u>http://&lt;<i>ip-addr&gt;</i></u> in the address field of the web browser, where < <i>ip-addr&gt;</i> is the IP address of the primary EGW. Log in with the appropriate credentials. Click Login. <b>C9-1-1</b> <b>EMERGENCY GATEWAY</b>
	Emergency Gateway Login         Username:       admin         Password:       #*****         Remember my Username       Besword by contacting your account manager.         Login       Forgot your password? Click here.
2.	Desthboard -> Login         Main Page         The main page of the EGW will appear.
	Welcome, Adminutuser         Last Login: Oct 14, 2010 01:25 MM         ADwister of Connexen         Provisioning       Auto Discovery         System Status       Search         Configuration       Test Mode         Desk Alert       Help
	General Information     StMMP Scan Statistics       Server Role:     Primary     Itals Time Scanned     Threads Used     Last Scan Duration     Average Scan Duration       PEX Count:     0     WLAN Scan Statistics     Itals Scan Duration currently available.       Endpoints Count:     0     Itals Time Scanned     Last Scan Duration currently available.       Provisioned Endpoints Count:     0     Itals Time Scanned     Last Scan Duration currently available.       Switches Count:     0     So information currently available.       Discovered Switch Ports     0     Servered Switch Ports
	Undscovered Switch Ports Count:     0       WLAN Controller Count:     0       WLAN Discovered Devices Count:     0       Dynamic ELINs available:     0       Dynamic ELINs available:     0       Dissibloard >> System Status >> Status       Ecopyright 2010 @ 911enable.com is a division of Connexion Telecom inc.

Step	Description		
3.	<b>ERS Account</b> The ERS account defines the parameters used to connect to the Emergency Routing Service. Navigate to the <b>Configuration</b> $\rightarrow$ <b>Advanced</b> $\rightarrow$ <b>ERS Account</b> tab to configure these settings. The example below shows the settings used for the compliance test. The necessary values for each field shown for the <b>911 Account</b> <b>Settings</b> and the <b>ECRC List</b> are provided by Connexon for connection to the ERS. For security reasons, the public IP addresses of the ERS are not shown but some digits are replaced by an x. The ECRC list shows the phone number of the ECRC. This number is dialed through Communication Manager so it contains the preceding 9 (ARS feature access code) followed by the 11-digit number.		
	Welcome, Admini User         Welcome, Admini User         Lat Login: Cell Sp. 2010 2010 Link         Auto Discovery       System Status         Search       Configuration         Deathbaard Account       IP-PBX         Galback       Gobil         P11 Account Settings       Add a Number		
	911 Enable Primary IP:       208.xxxx.xxx.xxx         911 Enable Secondary IP:       208.xxxx.xxx.xxx         911 Enable Tertiary IP:		
4.	<b>Extension-Bind Numbers</b> The Extension-Bind numbers are the pool of DID numbers owned by the enterprise that the EGW can use as callback numbers for active 911 calls. Navigate to the <b>Configuration</b> $\rightarrow$ <b>Advanced</b> $\rightarrow$ <b>Callback</b> tab to configure these Extension-Bind numbers. For this compliance test, a single number was used in the Extension-Bind Numbers list. To add a number to the list, click the <b>Add a number</b> button [not shown]. Enter the number in the subsequent window shown below and click <b>Save</b> . Each callback number is a by 10-digits number. For security reasons, the full PSTN number is not shown below but some digits are replaced by an x.		
	Welcome, Admin User         A Division of Conneron         Provisioning       Auto Discovery         System Status       Search         Configuration       Test Mode         Deshboard Account       IP-P90X         Social ERS Account       Del Plan         Timer Settings       SOAP Server		
	Add a Number       Callback Number:       303538xxxxi       Extension-Bind Duration:       15         Back       Save       Use 10 Digit for Callback:       Yes       Edit         Deshboard >> Configuration-> Advanced-> Callback.       Edit       Edit       Edit		

Step	Descriptio	n		
5.	IP-PBX			
	Navigate to Configuration $\rightarrow$ IP-PBX to configure as follows:			
	• Click on Add a new IP-PBX button and the			
	• <b>IP-PBX Name</b> – Set to any descriptive name	-	r the serven shows up.	
	<ul> <li>Protocol – Set to SIP/TCP</li> </ul>			
	• IP-PBX Version – Select V5			
	• <b>Domain(s):</b> - Enter <i>avaya.com</i> and click on A			
	• Callback Use VIA Header – Set to Yes [not	: shown]		
	• Callback Use Original PAI – Set to Yes [no	t shown]		
		-		
	("9-1-1" EMERGENCY GATEWAY			
	N ENABLE		Last Lo	
	A Division of Connexon Provisioning Auto Discovery System Status Search	Configuration	Test Mode Desk Alert	
	Dashboard Account IP-PBX Security Desk Notification Advanced			
	IP-PBX List No IP-PBXs are configured.	Add a new IP-PBX IP-PBX Name:	5M1	
	Add a new IP-PBX	IP-PBX Type:	Avaya Aura 👻	
		Protocol:	SIP/TCP •	
		IP-PBX Version: Endpoint ID Field:	VS V	
			avaya.com	
		Domain(s):	Delete	
		DNIS Prefix:		
		Local Gateway Prefix:		
		Local Gateway Suffix: Use ELIN as RDNIS:	Nov	
		Callback Use VIA	No 💌	
		Header: Callback Use Original		
		PAI: Use Home Numbering	No	
		Plan:		
		IP-PBX Preferences:	Use Default Settings	
			Back Save	
	Dashboard -> Configuration-> IP-P8X			
	Copyright 2010 @ 911enable.com is a division of ConneXon Telecom inc.			

Step	Description	
6.	<b>IP-PBX – Continued</b> Click on the <b>Add a server</b> button to display the screen on the right and configure as	
	follows:	
	• IP-PBX – Select the PBX configured in previous step Signaling IP Address (FODN) – Enter the IP address of the Session Manager	
	• Signaling IP Address (FQDN) – Enter the IP address of the Session Manager configured in Section 4, Step 6.	
	<ul> <li>Use default for all other values</li> </ul>	
	C9-1-1 ENABLE A Division of Comments	
	Provisioning         Auto Discovery         System Status         Search         Configuration         Test Mode         Desk Alert         Help           Deshboard Account         IP-PBX         Security Desk         Notification         Advanced         Access Management         Task Scheduler	
	IP-PEX successfully created.	
	IP-PBX List         Add a server	
	Add a new IP-PBX     Add a server     Server Name:     SessonManager       Signaling IP     Address/FQON:     10.80.120.28	
	Callback Port: 5060 Connection Timeout: 20	
	Back Salir	
	Destboard -> Configuration > IP-PBX Copyright 2010 (5) 911enable.com is a division of ConneXon Telecom inc.	
	<b>Emergency Response Locations (ERLs)</b> The ERL is a location identifier that is associated with a physical address. This association is contained in a batch file uploaded to the EGW. To perform this upload, navigate to the <b>Provisioning</b> $\rightarrow$ <b>ERLs</b> tab. Enter the file name in the <b>Batch File</b> field and click the <b>Upload</b> button. At the bottom of the screen, <b>Status</b> and <b>Actions columns</b> will appear associated with the batch file. The following actions are necessary to complete the upload but are not all shown in the screen below. Next, click <b>Validate</b> under <b>Actions</b> . Once the file is validated, click <b>Batch Process</b> which will appear under <b>Actions</b> . Once this completes, the <b>Status</b> will change to <b>Finished</b> . An example of an ERL batch file is shown in next step.	
	Provisioning       Auto Discovery       System Status       Search       Configuration       Test Mode       Desk Alert       Help         ERLs       Endpoints       ELIN Pool       Validation	
	File successfully uploaded.	
	ERLs Batch Upload	
	Batch File: Browse Upload	
	Batch Logs Refresh	
	Orignal Filename         Log File         Log Date         Status         Actions           Iccation.txt          Oct 15, 2010 06:26 PM         Not Validated         Validate         Delete	
	Pages / Rows 5 Previous   Next Go to page: First Page  Go	
	Dashboard -> Provisioning-> ERLs	

Step	Description
8.	Locations Batch File The following is an example of the ERL batch file used for the compliance test. All locations also share a single security desk location named AvayaSD and defined in Step 12. For complete details on each of the fields in the ERL Batch File, see [10].
	<pre>Interpretation.txt - Notepad File Edit Format Help 1;LOC1;211;Mt. Airy Road;;Basking Ridge;NJ;USA;07920;0;0;;;AvayaSD;; 1;LOC2;223;Mt. Airy Road;;Basking Ridge;NJ;USA;07920;0;0;;;AvayaSD;; 1;LOC3;1300;W. 120th Ave.;;Westminster;C0;USA;80234;0;0;;;AvayaSD;;</pre>
9.	Provisioned Endpoints All endpoints that can not be auto-discovered, should be manually provisioned so that each extension that is not auto-discovered is associated with an ERL. This association is contained in a batch file uploaded to the EGW. To perform this upload, navigate to the Provisioning → Endpoints tab. Enter the file name in the Batch File field and click the Upload button. At the bottom of the screen, Status and Actions columns
	will appear associated with the batch file. The following actions are necessary to complete the upload but are not all shown in the screen below. Next, click Validate under Actions. Once the file is validated, click Batch Process which will appear under Actions. Once this completes, the Status will change to Finished. An example of a provisioned endpoints batch file is shown in Step 10.
	EMERGENCY GATEWAY       Welcome, Adminu User         Last Login: Od 15. 2019 04:28 PM         Last Login: Od 15. 2019 04:28 PM         Provisioning       Auto Discovery         System: Status       Search         Configuration       Test Mode         ERLs       Endpoints         Endpoints       ELIN Pool         Validation       Validation
	Batch File:       Betch File:         Jubload       Jubload         Batch Logs       Image: Display Automatic         Original Flename       Log File       Log Date       Status       Actions         endport.txt        Oct 18, 2010 02:42 PM       Not Validated       Vegetate       Delete         Pages / Rows (S )        Previous   Next       Go to page:       First Page (Go       Co
10.	Provisioned Endpoints Batch File The following is an example of the provisioned endpoints batch file used for the compliance test. It contains the extensions associated with the digital and analog endpoints that can not be auto-discovered.
	Image: Control of Con

Step					Des	criptio	n		
11.	must be con Navigate to switches. T switches in parameters. enter the ap	orise layer 2 offigured on the Auto 1 The example Figure 1 w Enter the propriate s witch resid	the EGW Discovery le below s vere enter managem tring in th	$7 \text{ so the set } \mathbf{y} \rightarrow \mathbf{I}$ hows red. (Content I he SN	as Av hat it Layer the l Click P add <b>MP</b>	aya H. can be <b>2 Disc</b> ist used the Ad lress of Comm	323 or SIP t queried as covery tab t d for the con d a switch the switch unity Strin	part of layer o display th npliance tes button to en in the <b>Swite</b> g field. Ente	connected to it r 2 discovery. he list of layer 2 st. All three hter the switch ch IP field and er the ERL hay be used for
	A Division of Connexon Provisioning Layer 2 Discovery		System Status		Search	Config	aration Test M	ode Desk Ale	Wekome, Admin User Lat Login: Oct 19, 2010 01:45 PM Log Out rt Help
	Switch successfully cre	ated.		_	_	_			
		Community String [Change]	Description	Vendor	SNMP Port	Default ERL ID	Last Update		Actions
	10.80.131.2	public	Extreme Switch 1 Extreme Switch 2	Extreme	161	LOC1 LOC2	2010-10-18 18:15:46 2010-10-18 18:15:09		ew / Edit
	10.80.130.3	public	Cajun 364	Avaya	161	LOC3	2010-10-18 18:15:09		ew / Edit
12.	Security D	om is a division of ConneXon Tel esk					1 / -		
	0 2					2			being sent to
	-	•	-		-				curity Desk tab
		]. The exam	nple belov	<i>x</i> sho	ws th	le Secu	rity Desk ci	reated for th	Security Desk le compliance g EGW.
	C 9-1-1 ENABLE A Division of Connexon Provisioning Deshiboard Account	Auto Discovery IP-P6X	System Status	otification	Search Adva	Configu nced Acc	ration Test Mc ess Management Task Sch		Welcome, Admin User Last Logini Oct 8, 2010 01:45 PM Log Out Help
	Edit a Security Desk Security Desk Name: Security Desk Number: Mute: Display Elin as Caller ID: IP-PEX: Back Save	Avaya50 6665000 No = 5M1 =							
	Dashboard -> Configuration- Copyright 2010 © 911enable	> Security Desk .com is a division of ConneXon Te	elecom inc.						

# 8. Interoperability Compliance Testing

This section describes the compliance testing used to verify the interoperability of the EGW and ERS with Communication Manager. This section covers the general test approach and the test results.

### 8.1. General Test Approach

The general test approach was to make emergency calls from different endpoints types connected to a variety of layer 2 switches and verify the location and callback information provided to the ERS.

#### 8.2. Test Results

The features described in **Section 1.1** were tested. All test cases passed successfully. The following observations were made during testing:

- Once the ESL is installed and the Avaya one-X® Communicator is run for the first time, the ESL pulls the necessary information (such as the Avaya one-X® Communicator extension) from the Windows registry. This information remains in the registry and continues to be reported, even if the Avaya one-X® Communicator is later shut down. If the Avaya one-X® Communicator is moved to another location its location in the EGW will be updated once the user logs in for the first time in the new location.
- If an endpoint is registered to one PBX and then the registration is changed to another PBX, both registrations continue to show in the EGW.
- For 46XX phones, the phone information is not pushed to EGW if the phone is not pointing to the HTTP server.
- EGW requires domain names for Avaya one-X® Communicator to register properly otherwise the location information is not properly populated on the EGW.
- EGW does not send the domain name when the calls are routed back for the callback so for the same extensions configured on two separate Communication Managers, a dedicated DID should be assigned for all such extensions. The callbacks to these extensions do not flow back to EGW via Session Manager, instead, they are routed from Session Manager back to the Communication Manager extension.

### 9. Verification Steps

The following steps may be used to verify the configuration:

- From the Communication Manager SAT, use the **status signaling-group** command to verify that the SIP signaling group is in-service.
- From the Communication Manager SAT, use the **status trunk-group** command to verify that the SIP trunk group is in-service.
- On the EGW, verify the ERL information. Navigate to the Search → ERLs tab, verify that the locations provided in the batch file in Section 7, Step 8 are displayed.

9-1-1 EME	RGENCY GATEWAY			Welcome, Admin Last Login: Dec 10, 2010 06: Log
sion of Connexon Provisioning	Auto Discovery System Status Search	Configuration Te	st Mode Desk	Alert Help
ERLs	Endpoints			
arch Emergency Respon	se Locations (ERL)			
	se Locations (ERL)			
	Address	Local Gateway Enabled	Direct Call Delivery	Actions
Ls Search Results		Local Gateway Enabled No	Direct Call Delivery No	Actions More Details
Ls Search Results Default ERL ID	Address			
Ls Search Results Default ERL ID LOC2	Address 223, MT. XIRY ROAD, BASKING RIDGE NJ, USA, 07920	No	No	More Details
Ls Search Results Default ERL ID LOC2 LOC3	Address 223, MT. "AIRY ROAD, BASKING RIDGE NJ, USA, 07920 1300, W. 120TH AVE., WESTMINSTER CO, USA, 80234	No	No	More Details

• On the EGW, verify the endpoints. Navigate to the **Search → Endpoints** tab, verify that all endpoints are displayed.

of Connexon rovisioning	Auto Discovery System Sta	tus Search	Configuration T	est Mode Desk Alert	Help
	Auto Discovery System Sta	us Search	Configuration	Desk Alert	neip
h Endpoints					
	$\bigcirc$				
oints Search Results					
Extension	MAC Address	PBX Name	IP Address	Actions	
6665201		SM1-CM1		More Details	
6665402	00123F76051A	SM1-CM1	10.80.132.150	More Details	
6665011	00040DECC19F	SM1-CM1	10.80.130.41	More Details	
6665401	00040DEDC201	SM1-CM1	10.80.132.42	More Details	
6665412	00040D4CB324	SM1-CM1	10.80.130.45	More Details	
6665000	00040D9B5F21	SM1-CM1	10.80.131.43	More Details	
6665101		SM1-CM1		More Details	
6665401	00040DEDC201	SM1-CM2	10.80.131.42	More Details	
6665011	00040DECE532	SM1-CM2	10.80.130.51	More Details	
6665023	001AA034D01F	SM1-CM2	10.80.130.152	More Details	
/ Rows 10 💌	Previo	us Next	Go to page: First Page 💌 Go		

• Verify that 911 calls can be placed from different endpoints types from different locations. Verify from the EGW Call Detail Records (CDR), that the correct location and callback number is being passed to 911 Enable. Navigate to the **System Status** → **CDRs** tab to display this information. The example below shows several emergency 911 calls as represented by the value *ERS* in the **Call Destination** field. The example also shows a callback calls which show the local extension being called back in the **Call Destination** field. Each of the 911 calls shows the correct location and callback information for that endpoint.

sion of Connexon								Log
Provisioning AL	uto Discovery	System Status Search	Co	nfiguration	Test Mode	Desk Alert	He	elp
Status Lo	ogs	Reports CDRs	Alarms	Maintenance				
R								
arch CDRs					Download Call Detail Re	ecords		
arch from:	to:	Search:			Select by Month:	-	Download	1
ill Detail Records								
Start Time	Duration (s)	Endpoint Caller ID	ERL ID	Callback Number	Call Destination		Wave File	Call Stat
Nov 08, 2010 07:24 PM	7	"SIP 6665402" <6665402>	LOC3	3035381619	ERS		Download	CANCE
Nov 08, 2010 07:24 PM	7	"SIP 6665402" <6665402>	LOC3	6665402	Security Desk		Download	CANCE
Nov 08, 2010 06:49 PM	13	5147452143	No Location	5147452143	73266600001@10.80.120.28:5060		Download	ANSWE
Nov 08, 2010 06:49 PM	7	"11 Digit Phone" <73266600001>	LOC1	3035381619	ERS		Download	ANSWE
Nov 08, 2010 06:49 PM	11	"11 Digit Phone" <73266600001>	LOC1	73266600001	Secu	rity Desk	Download	ANSWE
ges / Rows 5 💌		Previous   Next	Golton	age: First Page 💌	Go			

### 10. Conclusion

911 Enable Emergency Gateway and Emergency Routing Service passed compliance testing. These Application Notes describe the procedures required to configure the connectivity between Avaya Aura® Communication Manager, Avaya Aura® Session Manager and the 911 Enable equipment and service as shown in **Figure 1**.

### 11. Additional References

This section references the documentation relevant to these Application Notes. Avaya product documentation is available at <u>http://support.avaya.com</u>. Product documentation for the EGW can be obtained from 911 Enable.

- [1] Installing and Configuring Avaya Aura® Session Manager, Doc ID 03-603473 Release 6.0
- [2] Administering Avaya Aura® Session Manager, Doc ID 03-603324, Release 6.0, June 2010
- [3] Administering Avaya Aura® Communication Manager, May 2009, Document Number 03-300509
- [4] *Avaya Aura*® *Communication Manager Feature Description and Implementation*, May 2009, Document Number 555-245-205.
- [5] Avaya Aura® Communication Manager Screen Reference, May 2009, Document Number 03-602878
- [6] 4600 Series IP Telephone LAN Administrator Guide, October 2007, Document Number 555-233-507
- [7] Avaya one-X Deskphone Edition for 9600 Series IP Telephones Administrator Guide, November 2009, Document Number 16-300698
- [8] Avaya one-X Deskphone SIP for 9600 Series IP Telephones Administrator Guide Release 2.0, Dec 2007, 16-601944
- [9] 911Enable Emergency Gateway System Guide 2.6.
- [10] ESL Configuration Guide Rev. A, February 15, 2010.

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

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

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