Application Notes for 911 ETC CrisisConnect® for VoIP with Avaya Aura® Session Manager and Avaya Aura® Communication Manager – Issue 1.0

Abstract

These Application Notes describe configuration steps required for 911 ETC CrisisConnect® for VoIP to interoperate with Avaya Aura® Session Manager and Avaya Aura® Communication Manager.

911 ETC CrisisConnect® for VoIP solution enables E911 call routing to the correct Public Safety Answering Point (PSAP) and deliver the caller's address directly to the PSAP operator's panel in order to provide immediate emergency assistance.

The compliance testing was focused on routing E911 calls from Avaya Aura® Session Manager to 911 Crisis Connect SBC, which in turn, performed call routing to the correct PSAP. Please note that, at the moment, only in-band DTMF is supported by 911 ETC.

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

911 ETC provides a VoIP Positioning Center (VPC) Service that is able to deliver 911 calls to U.S. and Canada PSAPs independent of the region the call originates from. 911 ETC provides two methods for customers to interconnect for E911 call routing – PSTN and SIP.

If a customer chooses to interconnect via PSTN, 911 ETC issues the customer "Access line" (E.164, DID) number. The access numbers are specific to the customer and are used to identify that the call originated from the customer.

If a customer chooses to interconnect via SIP, 911 ETC provides SIP specifications for a primary and secondary Session Border Controller (SBC). 911 ETC configure our SBC(s) for all customer SIP switches or SBCs that will be connecting to 911 ETC for E911 purposes. Avaya Aura® Communication Manager and Avaya Aura® Session Manager are required.

- Customer configures Avaya Aura® Communication Manager and Avaya Aura® Session Manager
- Configuration depends on the call interconnect method the customer chooses (SIP or PSTN).
- Customer and 911 ETC perform call testing.

2. General Test Approach and Test Results

The compliance test focused on verifying that 911 ETC CrisisConnect® for VoIP can update users' location information in real time.

2.1. Interoperability Compliance Testing

The compliance test validated the ability of 911 ETC CrisisConnect® for VoIP to route emergency calls and provide ALI information to PSAP. To validate address information, calls were placed to an address verification system that played back users' current provisioned address. For this test effort, only calls related to audio, DTMF verification, and PSAP ALI were placed by dialing 911. The remaining test calls, due to the nature of emergency calling, was placed to 933. 933 is an Address Verification Service provided by 911 ETC.

2.2. Support

Technical support for 911 ETC CrisisConnect® for VoIP can be obtained through the following:

- Web: http://www.911etc.com/contact-us
- E-mail: support@911etc.com
- Phone: (480) 719-8556

3. Reference Configuration

Figure 1 illustrates the compliance test configuration consisting of:

- Avaya Aura® Communication Manager (CM)
- Avaya Aura® Session Manager (SM)
- Avaya G430 and G450 Media Gateway
- Avaya IP Phones
- 911 ETC CrisisConnect® for VoIP

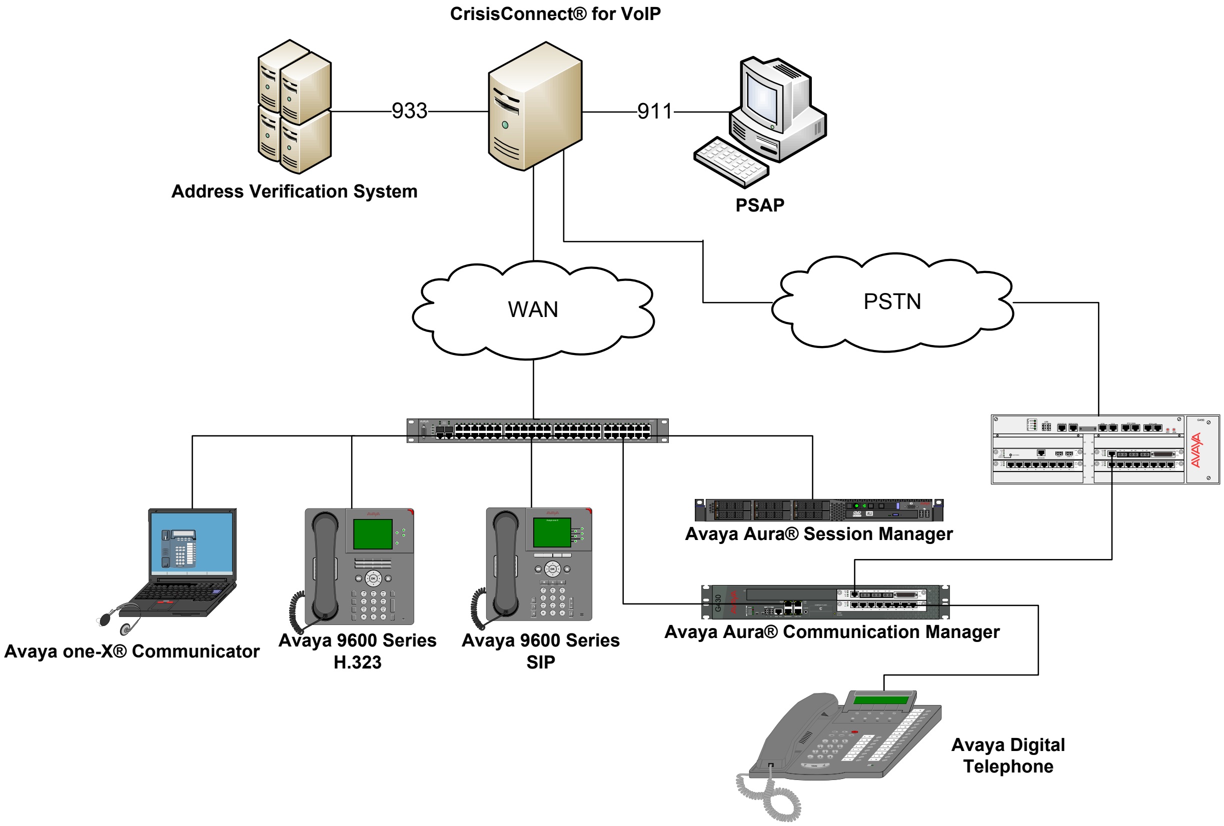

CrisisConnect® for VoIP
933
911
Address Verification System
PSAP
WAN
PSTN
Avaya Aura® Session Manager
Avaya Aura® Communication Manager
Avaya one-X® Communicator
Avaya 9600 Series H.323
Avaya 9600 Series SIP
Avaya Digital Telephone

Figure 1 – Test Configuration

4. Equipment and Software Validated

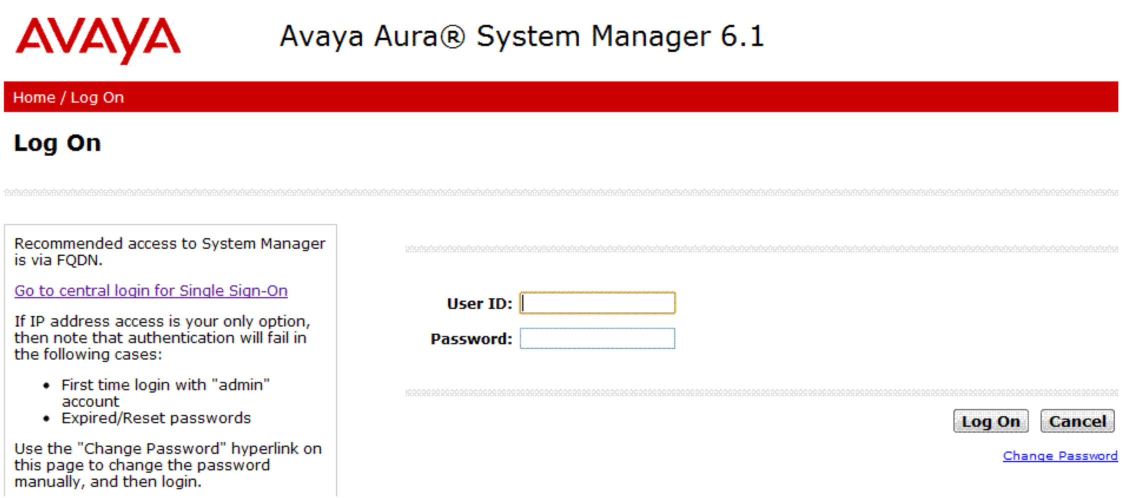
The following equipment and version were used in the reference configuration described above:

Component	Firmware Version	Description
Avaya G430 Media Gateway Avaya Aura® Communication Manager	6.0.1 00.1.510.1-19528	Runs Avaya Aura® Communication Manager (CM) call processing software.
Avaya Aura® Session Manager	6.1 SP6	SIP routing engine
CrisisConnect for VoIP	5.2.2.0	Emergency Call Routing services

5. Configure Avaya Aura® Session Manager

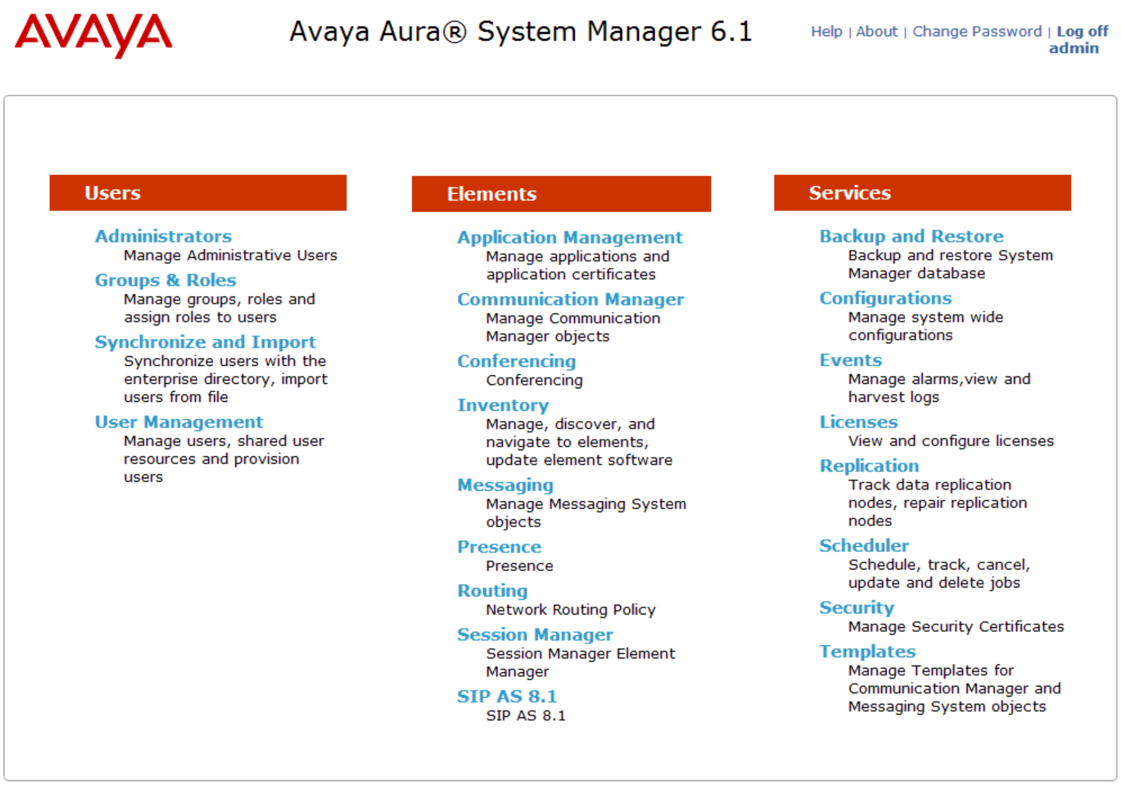
This section provides the steps for configuring Session Manager to communicate with 911 ETC. For more details, see the administration guide.

5.1. Configuration details

Step	Description
1.	Session Manager is configured using browser access to System Manager. Enter the URL of System Manager such as https://<hostname>/network-login/SMGR where <hostname> is the ip address or qualified domain name of the System Manager. Login using appropriate credentials.  Avaya Aura® System Manager 6.1 Home / Log On Log On Go to central login for Single Sign-On User ID: Password: Log On Cancel Change Password Recommended access to System Manager is via FQDN. If IP address access is your only option, then note that authentication will fail in the following cases: • First time login with "admin" account • Expired/Reset passwords Use the "Change Password" hyperlink on this page to change the password manually, and then login.

<table>
<tr><th>Step</th><th>Description</th></tr>
<tr><td>2.</td><td>

The home page is a navigation screen as shown below. Each of these links will open a new tab from which to navigate to the details of the managed environment. Click on Routing.



Avaya Aura® System Manager 6.1

Help | About | Change Password | Log off admin

Users

Administrators
Manage Administrative Users

Groups & Roles
Manage groups, roles and assign roles to users

Synchronize and Import
Synchronize users with the enterprise directory, import users from file

User Management
Manage users, shared user resources and provision users

Elements

Application Management
Manage applications and application certificates

Communication Manager
Manage Communication Manager objects

Conferencing
Conferencing

Inventory
Manage, discover, and navigate to elements, update element software

Messaging
Manage Messaging System objects

Presence
Presence

Routing
Network Routing Policy

Session Manager
Session Manager Element Manager

SIP AS 8.1
SIP AS 8.1

Services

Backup and Restore
Backup and restore System Manager database

Configurations
Manage system wide configurations

Events
Manage alarms,view and harvest logs

Licenses
View and configure licenses

Replication
Track data replication nodes, repair replication nodes

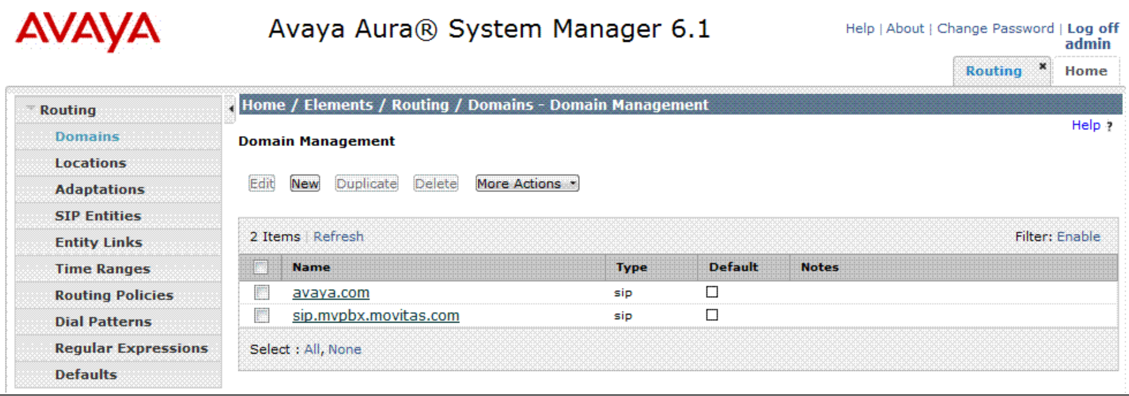
Scheduler
Schedule, track, cancel, update and delete jobs

Security
Manage Security Certificates

Templates
Manage Templates for Communication Manager and Messaging System objects

</td></tr>
<tr><td>3.</td><td>

One the left pane, click on **Domains**



Avaya Aura® System Manager 6.1

Help | About | Change Password | Log off admin

Home / Elements / Routing / Domains - Domain Management

Help ?

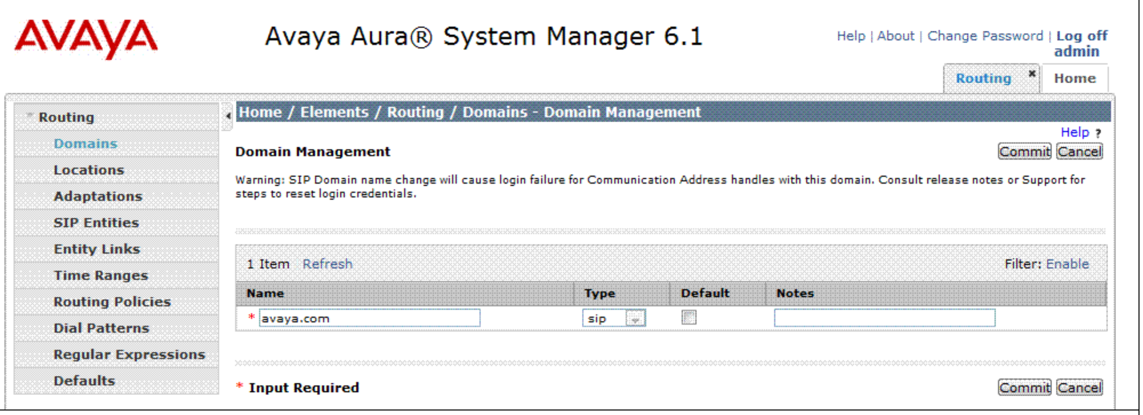
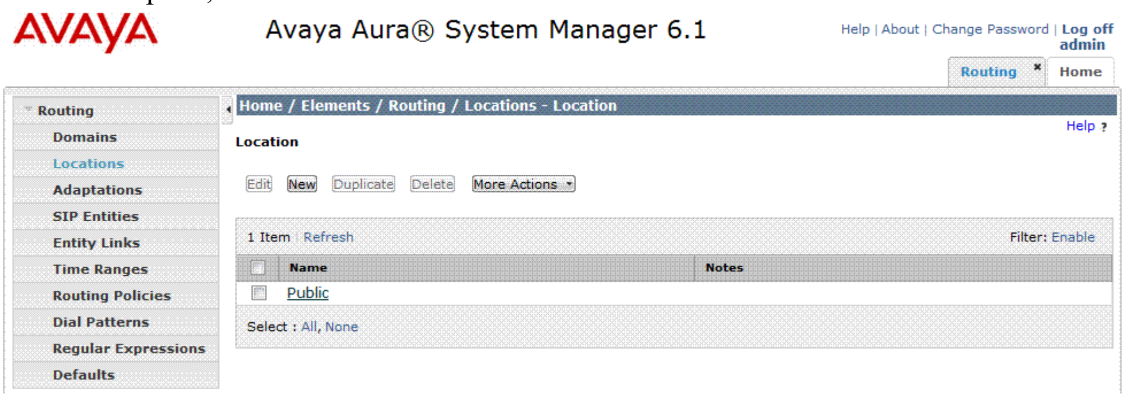
Domain Management

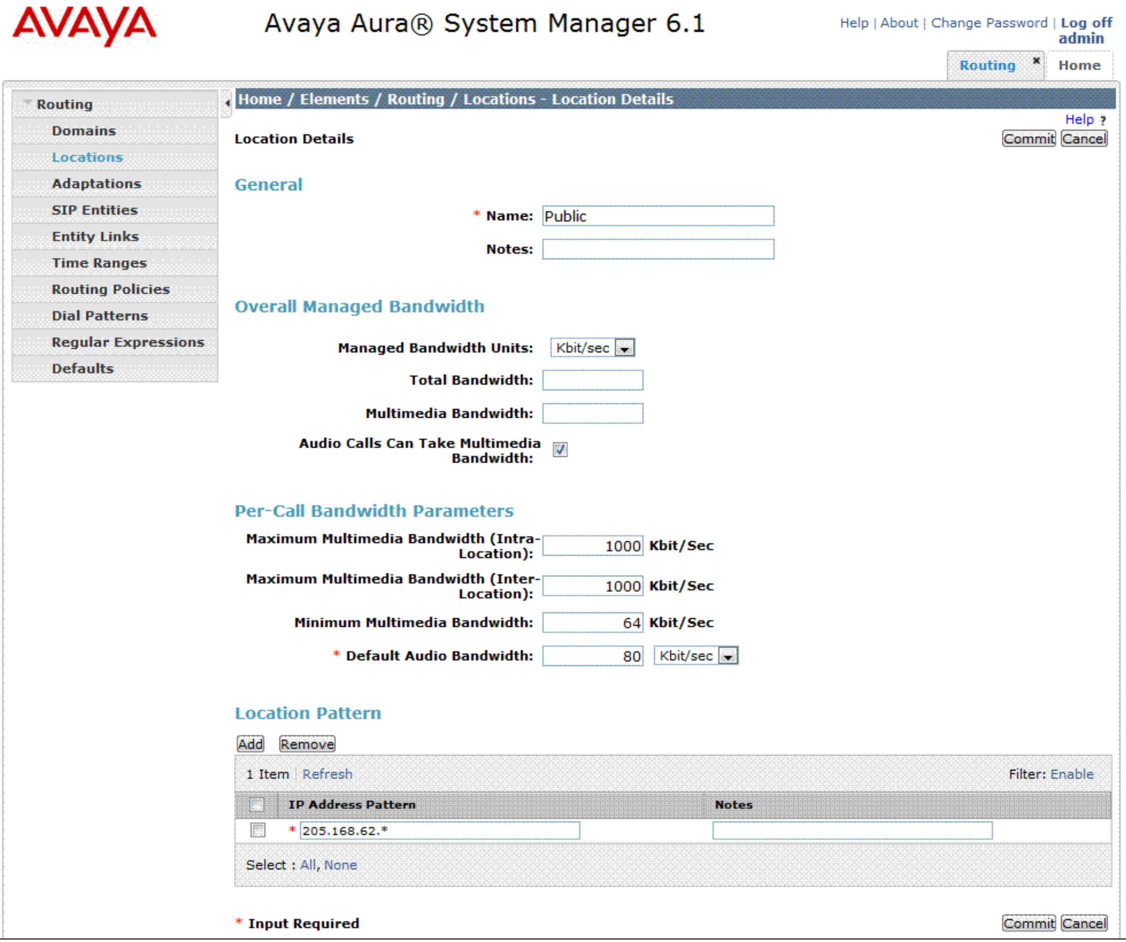
2 Items | Refresh Filter: Enable

<table>
<tr><th>□</th><th>Name</th><th>Type</th><th>Default</th><th>Notes</th></tr>
<tr><td>□</td><td>avaya.com</td><td>sip</td><td>□</td><td></td></tr>
<tr><td>□</td><td>sip.mvpbx.movitas.com</td><td>sip</td><td>□</td><td></td></tr>
</table>

Select : All, None

</td></tr>
</table>

Step	Description
4.	**Add a Domain** On the **Domains** page, click on New. • For the **Name** field, type in the domain • Set **Type** to **sip** For Compliance testing, avaya.com sip domain was used. Avaya Aura® System Manager 6.1 Home / Elements / Routing / Domains - Domain Management Domain Management Warning: SIP Domain name change will cause login failure for Communication Address handles with this domain. Consult release notes or Support for steps to reset login credentials. 1 Item Refresh Filter: Enable Name: * avaya.com — Type: sip — Default: □ — Notes: * Input Required Help | About | Change Password | Log off admin Routing Home Domains Locations Adaptations SIP Entities Entity Links Time Ranges Routing Policies Dial Patterns Regular Expressions Defaults Help ? Commit Cancel
5.	On the left pane, click on **Locations** Avaya Aura® System Manager 6.1 Home / Elements / Routing / Locations - Location Location 1 Item Refresh Filter: Enable □ Name — Notes □ Public Select : All, None Help | About | Change Password | Log off admin Routing Home Domains Locations Adaptations SIP Entities Entity Links Time Ranges Routing Policies Dial Patterns Regular Expressions Defaults Help ? Edit New Duplicate Delete More Actions

Step	Description
6.	**Add a Location** On the **Location** page, click on New. • Enter the **Name** of the location • Add a **Location Pattern** For Compliance testing the following information was used. 

AVAYA Avaya Aura® System Manager 6.1

Help | About | Change Password | Log off admin

Routing × Home

Routing: Domains, Locations, Adaptations, SIP Entities, Entity Links, Time Ranges, Routing Policies, Dial Patterns, Regular Expressions, Defaults

Home / Elements / Routing / Locations - Location Details

Help ?

Location Details Commit Cancel

General

* Name: Public

Notes:

Overall Managed Bandwidth

Managed Bandwidth Units: Kbit/sec

Total Bandwidth:

Multimedia Bandwidth:

Audio Calls Can Take Multimedia Bandwidth: ☑

Per-Call Bandwidth Parameters

Maximum Multimedia Bandwidth (Intra-Location): 1000 Kbit/Sec

Maximum Multimedia Bandwidth (Inter-Location): 1000 Kbit/Sec

Minimum Multimedia Bandwidth: 64 Kbit/Sec

* Default Audio Bandwidth: 80 Kbit/sec

Location Pattern

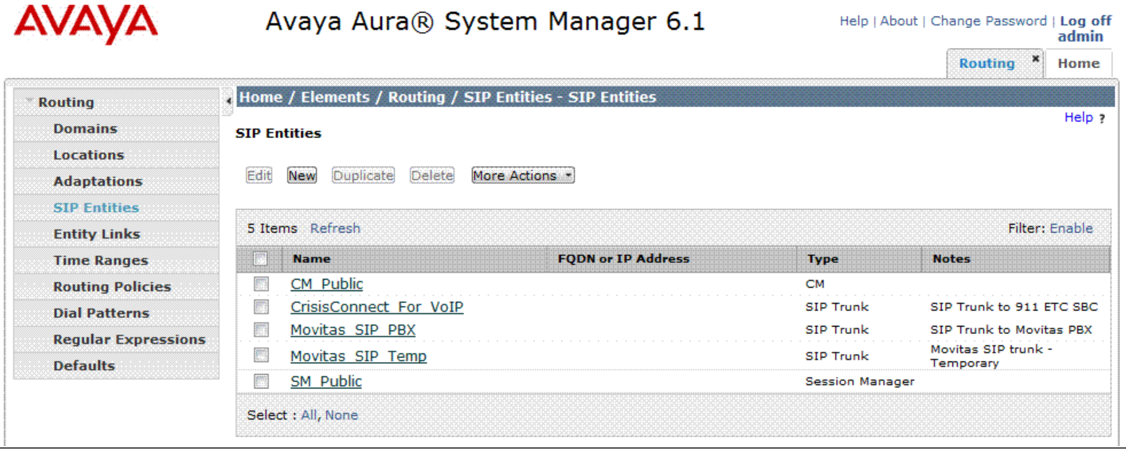
Add Remove

1 Item Refresh Filter: Enable

□	IP Address Pattern	Notes
□	* 205.168.62.*	

Select : All, None

* Input Required Commit Cancel

Step	Description
7.	On the left pane, click on **SIP Entities.** 

AVAYA Avaya Aura® System Manager 6.1

Help | About | Change Password | Log off admin

Routing × Home

Routing: Domains, Locations, Adaptations, SIP Entities, Entity Links, Time Ranges, Routing Policies, Dial Patterns, Regular Expressions, Defaults

Home / Elements / Routing / SIP Entities - SIP Entities

Help ?

SIP Entities

Edit New Duplicate Delete More Actions

5 Items Refresh Filter: Enable

□	Name	FQDN or IP Address	Type	Notes
□	CM_Public		CM	
□	CrisisConnect_For_VoIP		SIP Trunk	SIP Trunk to 911 ETC SBC
□	Movitas_SIP_PBX		SIP Trunk	SIP Trunk to Movitas PBX
□	Movitas_SIP_Temp		SIP Trunk	Movitas SIP trunk - Temporary
□	SM_Public		Session Manager	

Select : All, None

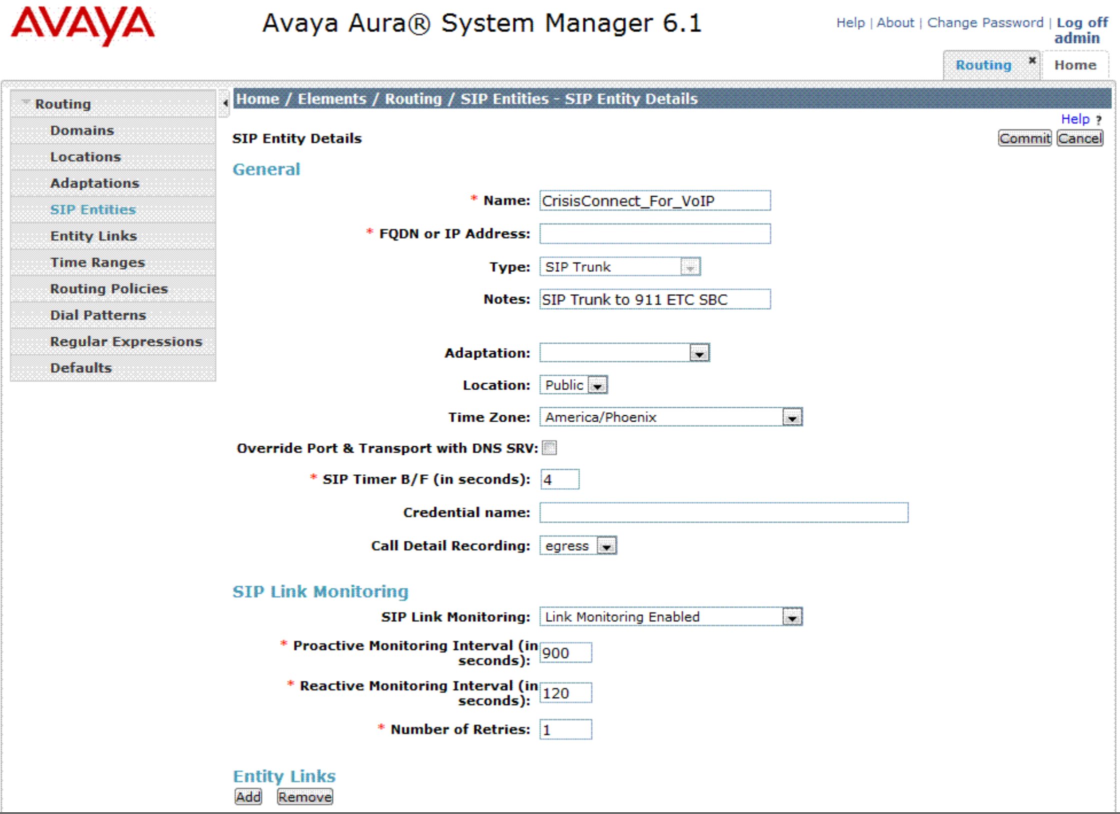
<table>
<tr><th>Step</th><th>Description</th></tr>
<tr><td>8.</td><td>

Add a SIP Entity

On the **SIP Entity** page, click on New.

- Enter the **Name** and **FQDN or IP Address**

For Compliance testing the following information was used.



Avaya Aura® System Manager 6.1

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

SIP Entity Details

General

* Name: CrisisConnect_For_VoIP

* FQDN or IP Address:

Type: SIP Trunk

Notes: SIP Trunk to 911 ETC SBC

Adaptation:

Location: Public

Time Zone: America/Phoenix

Override Port & Transport with DNS SRV: □

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

Credential name:

Call Detail Recording: egress

SIP Link Monitoring

SIP Link Monitoring: Link Monitoring Enabled

* Proactive Monitoring Interval (in seconds): 900

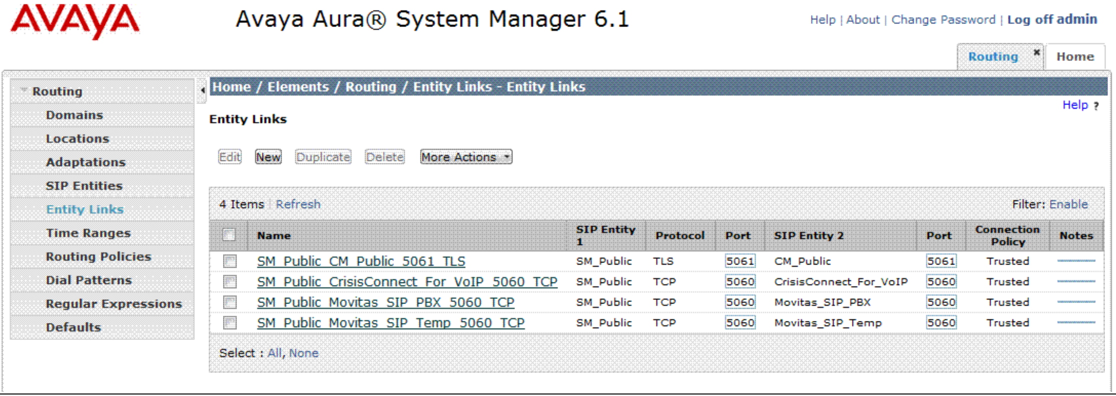
* Reactive Monitoring Interval (in seconds): 120

* Number of Retries: 1

Entity Links

</td></tr>
<tr><td>9.</td><td>

On the left pane, click on **Entity Links**



Avaya Aura® System Manager 6.1

Home / Elements / Routing / Entity Links - Entity Links

Entity Links

4 Items | Refresh

<table>
<tr><th>□</th><th>Name</th><th>SIP Entity 1</th><th>Protocol</th><th>Port</th><th>SIP Entity 2</th><th>Port</th><th>Connection Policy</th><th>Notes</th></tr>
<tr><td>□</td><td>SM_Public_CM_Public_5061_TLS</td><td>SM_Public</td><td>TLS</td><td>5061</td><td>CM_Public</td><td>5061</td><td>Trusted</td><td></td></tr>
<tr><td>□</td><td>SM_Public_CrisisConnect_For_VoIP_5060_TCP</td><td>SM_Public</td><td>TCP</td><td>5060</td><td>CrisisConnect_For_VoIP</td><td>5060</td><td>Trusted</td><td></td></tr>
<tr><td>□</td><td>SM_Public_Movitas_SIP_PBX_5060_TCP</td><td>SM_Public</td><td>TCP</td><td>5060</td><td>Movitas_SIP_PBX</td><td>5060</td><td>Trusted</td><td></td></tr>
<tr><td>□</td><td>SM_Public_Movitas_SIP_Temp_5060_TCP</td><td>SM_Public</td><td>TCP</td><td>5060</td><td>Movitas_SIP_Temp</td><td>5060</td><td>Trusted</td><td></td></tr>
</table>

</td></tr>
</table>

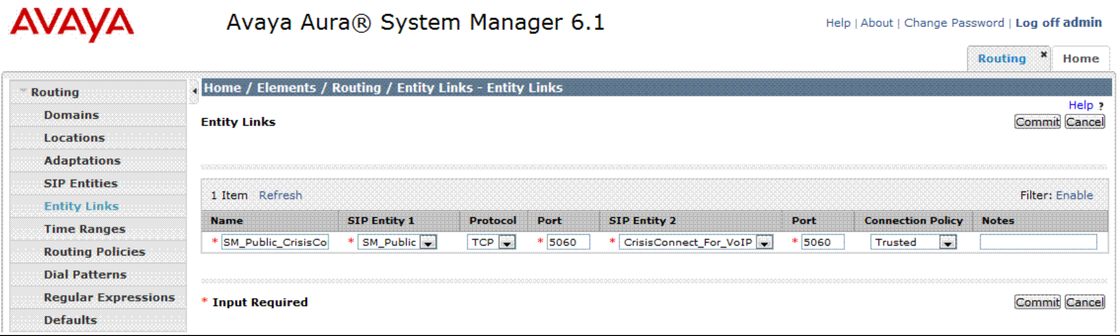
Step Description

10. **Add an Entity Link**

On the **Entity Link** page, click on New

- Add a **Name**
- Set **SIP Enity 1** as Session Manager
- Set the **Protocol Type** and type in **Port**
- Set **SIP Entity 2** as added in **Step 8** and set the **Port**
- Set the connection Policy to be **Trusted**

For Compliance testing the following information was used.



Home / Elements / Routing / Entity Links - Entity Links

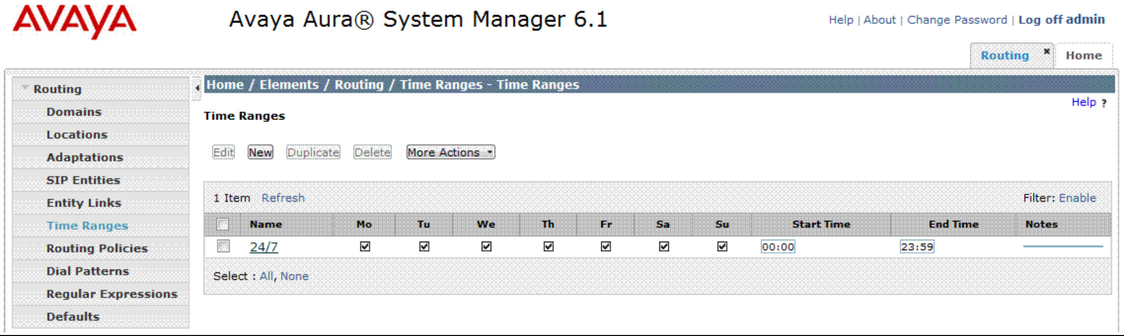
Entity Links

1 Item Refresh Filter: Enable

Name	SIP Entity 1	Protocol	Port	SIP Entity 2	Port	Connection Policy	Notes
* SM_Public_CrisisCo	* SM_Public	TCP	* 5060	* CrisisConnect_For_VoIP	* 5060	Trusted	

* Input Required

11. On the left pane, Click on **Time Ranges**



Home / Elements / Routing / Time Ranges - Time Ranges

Time Ranges

1 Item Refresh Filter: Enable

☐	Name	Mo	Tu	We	Th	Fr	Sa	Su	Start Time	End Time	Notes
☐	24/7	☑	☑	☑	☑	☑	☑	☑	00:00	23:59	

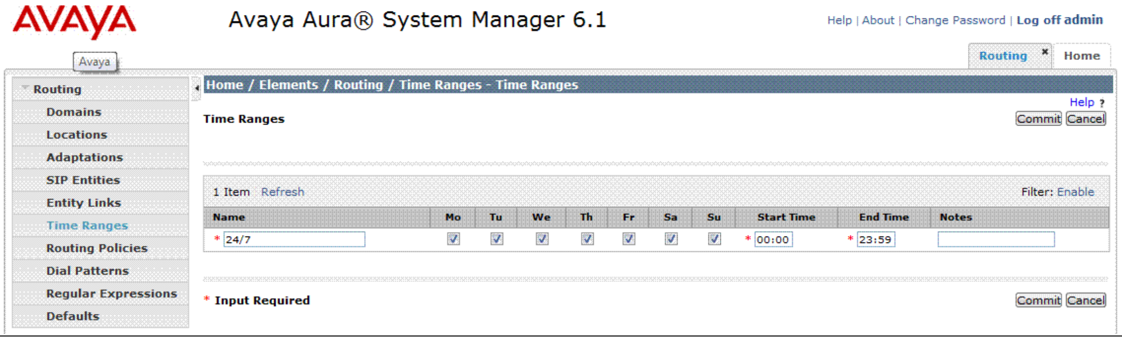
Select : All, None

12. **Add a Time Range**

On the Time Range page, click on New

- Type in the **Name** of the time range
- Select the Days and **Start Time** and **End Time** used for all days

For Compliance testing the following information was used.



Home / Elements / Routing / Time Ranges - Time Ranges

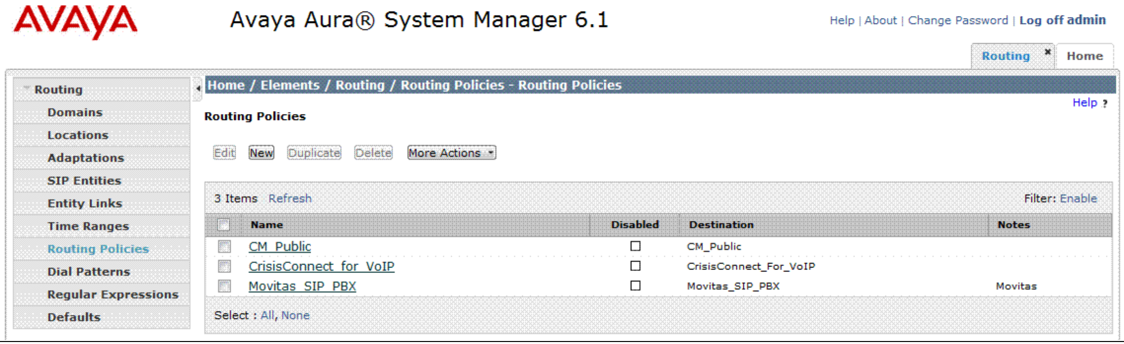
Time Ranges

1 Item Refresh Filter: Enable

Name	Mo	Tu	We	Th	Fr	Sa	Su	Start Time	End Time	Notes
* 24/7	☑	☑	☑	☑	☑	☑	☑	* 00:00	* 23:59	

* Input Required

Step	Description
13.	On the left pane, click on **Routing Policy**



Routing Policies

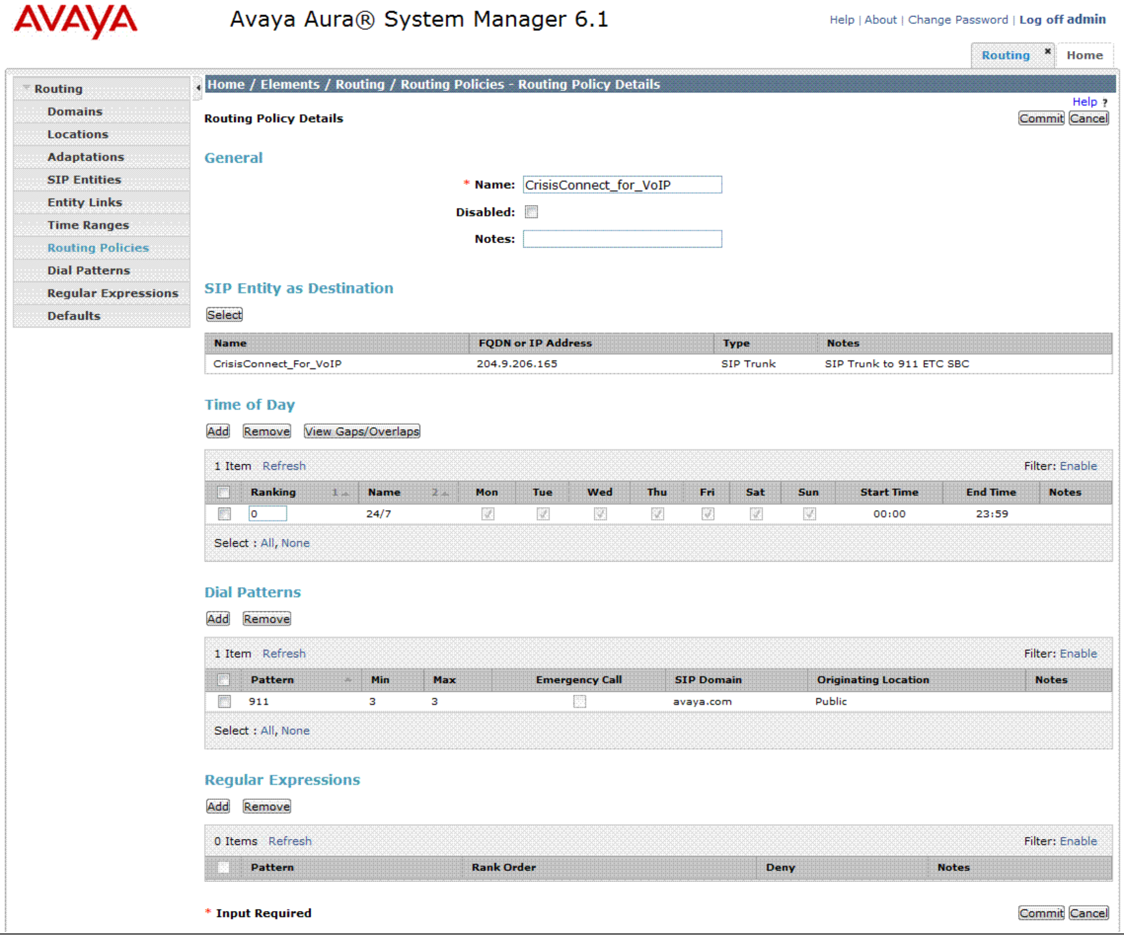
3 Items

	Name	Disabled	Destination	Notes
□	CM_Public	□	CM_Public	
□	CrisisConnect_for_VoIP	□	CrisisConnect_For_VoIP	
□	Movitas_SIP_PBX	□	Movitas_SIP_PBX	Movitas

Step	Description
14.	On the **Routing Policy** page, click on New

- Type in the **Name** for Routing Policy
- Select **SIP Entity as a destination**
  - Select SIP Entity configure in **Step 10**
- Select a **Time Range** added in **Step 12**

For Compliance testing the following information was used.



Routing Policy Details

General

* Name: CrisisConnect_for_VoIP

Disabled: □

Notes:

SIP Entity as Destination

Name	FQDN or IP Address	Type	Notes
CrisisConnect_For_VoIP	204.9.206.165	SIP Trunk	SIP Trunk to 911 ETC SBC

Time of Day

1 Item

	Ranking	Name	Mon	Tue	Wed	Thu	Fri	Sat	Sun	Start Time	End Time	Notes
□	0	24/7	☑	☑	☑	☑	☑	☑	☑	00:00	23:59	

Dial Patterns

1 Item

	Pattern	Min	Max	Emergency Call	SIP Domain	Originating Location	Notes
□	911	3	3	□	avaya.com	Public	

Regular Expressions

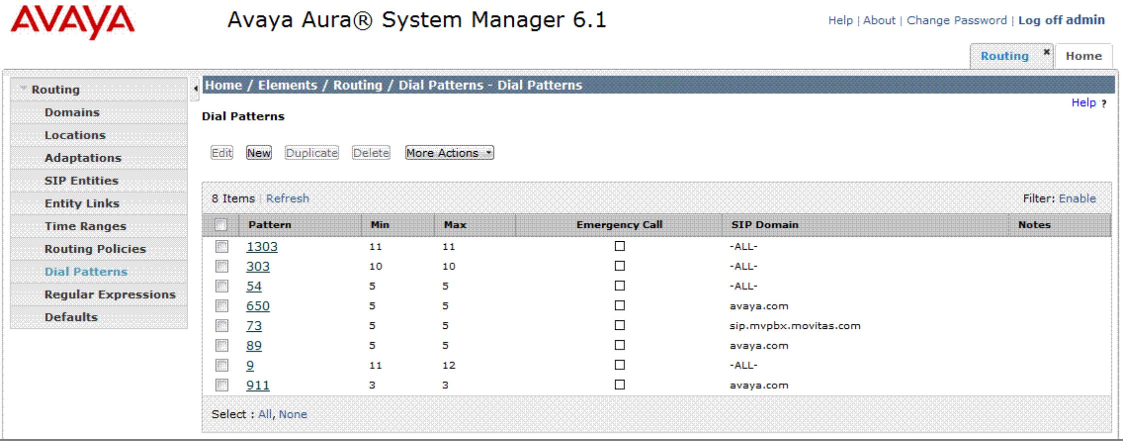
0 Items

	Pattern	Rank Order	Deny	Notes

* Input Required

<table>
<tr><th>Step</th><th>Description</th></tr>
<tr><td>15.</td><td>

On the left pane, click on **Dial Patterns**



Home / Elements / Routing / Dial Patterns - Dial Patterns

Dial Patterns

8 Items | Refresh Filter: Enable

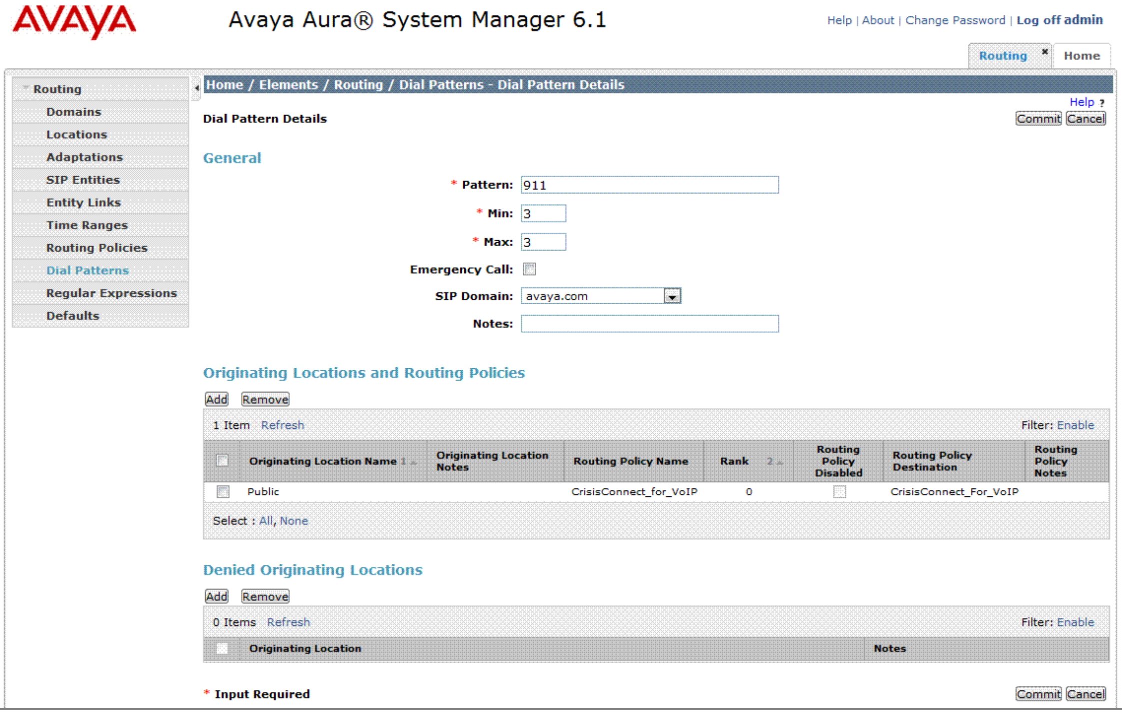
<table>
<tr><th>□</th><th>Pattern</th><th>Min</th><th>Max</th><th>Emergency Call</th><th>SIP Domain</th><th>Notes</th></tr>
<tr><td>□</td><td>1303</td><td>11</td><td>11</td><td>□</td><td>-ALL-</td><td></td></tr>
<tr><td>□</td><td>303</td><td>10</td><td>10</td><td>□</td><td>-ALL-</td><td></td></tr>
<tr><td>□</td><td>54</td><td>5</td><td>5</td><td>□</td><td>-ALL-</td><td></td></tr>
<tr><td>□</td><td>650</td><td>5</td><td>5</td><td>□</td><td>avaya.com</td><td></td></tr>
<tr><td>□</td><td>73</td><td>5</td><td>5</td><td>□</td><td>sip.mvpbx.movitas.com</td><td></td></tr>
<tr><td>□</td><td>89</td><td>5</td><td>5</td><td>□</td><td>avaya.com</td><td></td></tr>
<tr><td>□</td><td>9</td><td>11</td><td>12</td><td>□</td><td>-ALL-</td><td></td></tr>
<tr><td>□</td><td>911</td><td>3</td><td>3</td><td>□</td><td>avaya.com</td><td></td></tr>
</table>

Select : All, None

</td></tr>
<tr><td>16.</td><td>

On **Dial Patterns** page, click on **New**

- Set **Pattern** to **911**
- Set **Min** and **Max to** 3
- Set **SIP Domain** to the domain configured in **Step 4**
- Add **Originating Locations and Routing Policies**
    - Select location configured in **Step 6**
    - Select Routing Policy configured in **Step 14**
- Add a **Dial Pattern** for **933** as well.



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

Dial Pattern Details

General

* Pattern: 911

* Min: 3

* Max: 3

Emergency Call: □

SIP Domain: avaya.com

Notes:

Originating Locations and Routing Policies

1 Item Refresh Filter: Enable

<table>
<tr><th>□</th><th>Originating Location Name 1</th><th>Originating Location Notes</th><th>Routing Policy Name</th><th>Rank 2</th><th>Routing Policy Disabled</th><th>Routing Policy Destination</th><th>Routing Policy Notes</th></tr>
<tr><td>□</td><td>Public</td><td></td><td>CrisisConnect_for_VoIP</td><td>0</td><td>□</td><td>CrisisConnect_For_VoIP</td><td></td></tr>
</table>

Select : All, None

Denied Originating Locations

0 Items Refresh Filter: Enable

<table>
<tr><th>□</th><th>Originating Location</th><th>Notes</th></tr>
</table>

* Input Required

</td></tr>
</table>

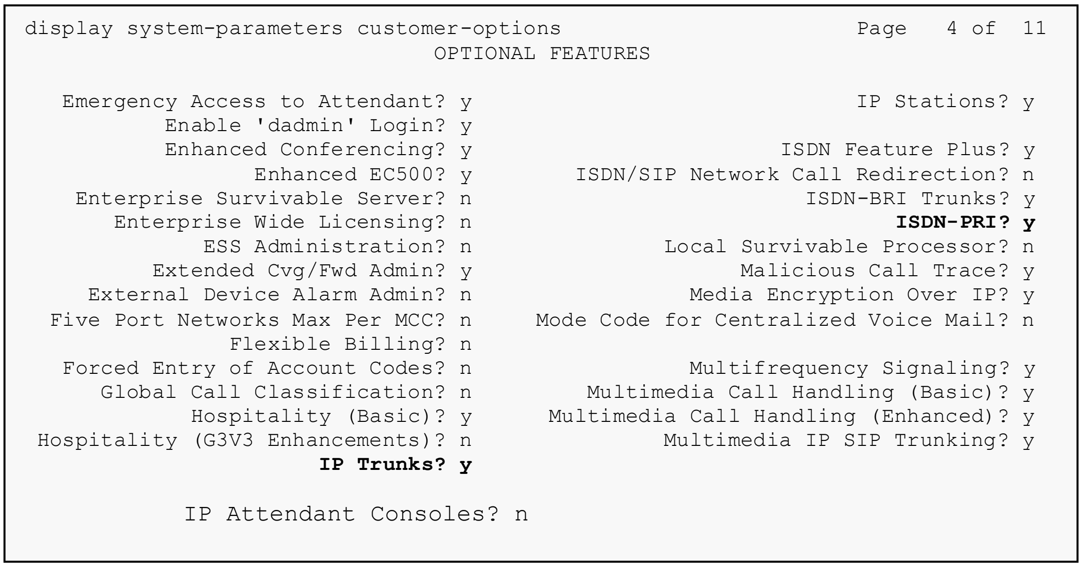
6. Configure Avaya Aura® Communication Manager

This section describes the Communication Manager configuration to support connectivity to Session Manager and related functionality.

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.

6.1. Trunk Configuration – for SIP Trunks to Session Manager

This section summarizes the configuration of the SIP trunk that connects the Communication Manager to SM.

Step	Description
17.	**System Parameters – Customer Options** Use the **display system-parameters customer-options** command to verify that the options highlighted below are enabled. 

```
display system-parameters customer-options                      Page   4 of  11
                                OPTIONAL FEATURES

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

            IP Attendant Consoles? n
```

<table>
<tr><th>Step</th><th>Description</th></tr>
<tr><td>18.</td><td>

Node Names

Use the **change node-names ip** command to create node names for SM. The example below shows the node names and IP addresses used for the compliance test. These node names will be used in the administration of other forms in Communication Manager.

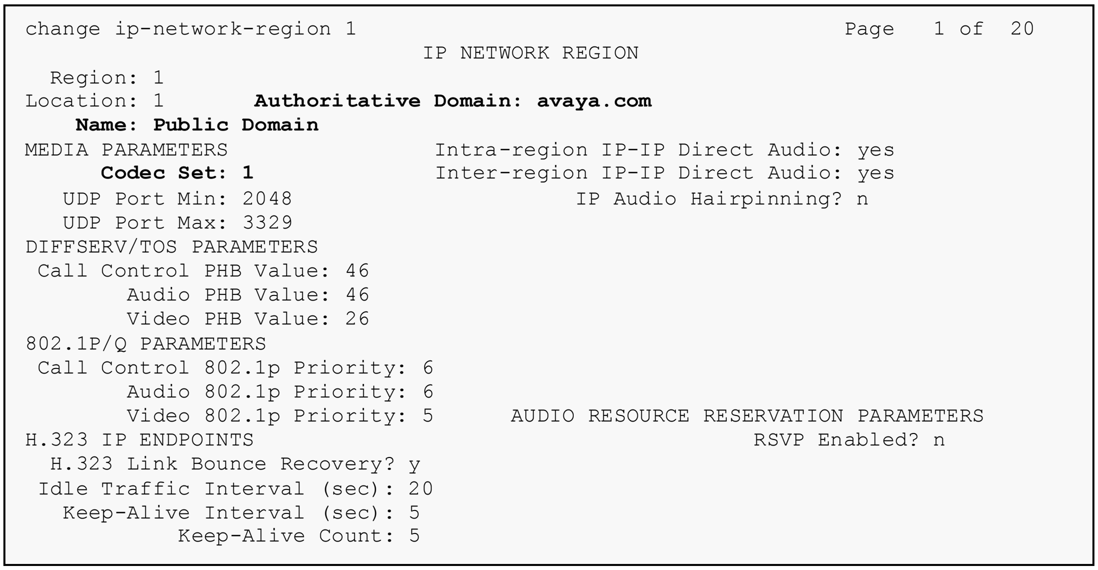
```
change node-names ip                                            Page   1 of   2
                                   IP NODE NAMES
    Name              IP Address
default             0.0.0.0
procr               205.168.62.28
procr6              ::
sm                  205.168.62.18
```

</td></tr>
</table>

Step	Description
19.	**IP network region**

The Avaya CM, SM and VoIP (H.323/SIP) endpoints were located in a single IP network region (IP network region 1) using the parameters described below. Use the **display ip-network-region** command to view these settings. By default, all elements will also be in IP network region 1 unless specifically placed in a separate region using the **ip-network-map** command. The example below shows the values used for the compliance test.

- A descriptive name was entered for the **Name** field.
- **IP-IP Direct Audio** (shuffling) was enabled to allow audio traffic to be sent directly between IP endpoints without using media resources in the Avaya Media Gateway. This is the default setting. Shuffling can be further restricted at the trunk level on the **Signaling Group** form.
- The **Codec Set** field was 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. This is the codec set that will be used for calls between the 911 ETC and Communication Manager, via session Manager since all components are in IP network region 1.
- The default values were used for all other fields.

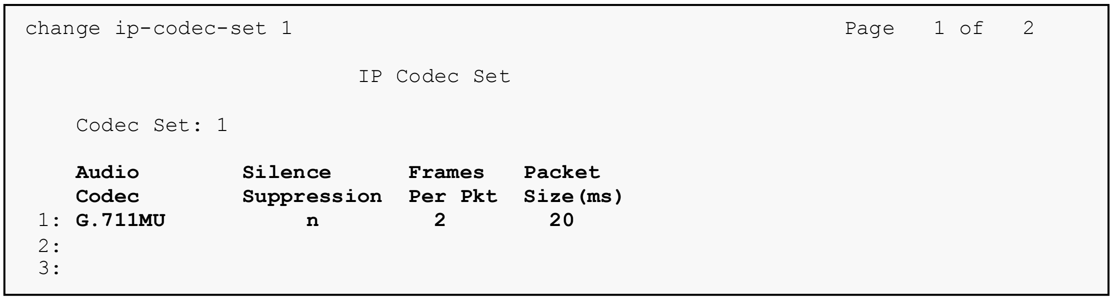


```
change ip-network-region 1                                    Page   1 of  20
                               IP NETWORK REGION
  Region: 1
Location: 1       Authoritative Domain: avaya.com
    Name: Public Domain
MEDIA PARAMETERS                Intra-region IP-IP Direct Audio: yes
      Codec Set: 1              Inter-region IP-IP Direct Audio: yes
   UDP Port Min: 2048                      IP Audio Hairpinning? n
   UDP Port Max: 3329
DIFFSERV/TOS PARAMETERS
 Call Control PHB Value: 46
        Audio PHB Value: 46
        Video PHB Value: 26
802.1P/Q PARAMETERS
 Call Control 802.1p Priority: 6
        Audio 802.1p Priority: 6
        Video 802.1p Priority: 5      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 Count: 5
```

<table>
<tr><th>Step</th><th>Description</th></tr>
<tr><td>20.</td><td>

Codecs

Use the **change ip-codec-set 1** command to define the codecs used by IP codec set 1. 911 ETC recommends the use of G.711MU codec. However, G729 was also successfully tested. For compliance test, G.711MU was primarily used.



```
change ip-codec-set 1                                          Page   1 of   2

                          IP Codec Set

    Codec Set: 1

    Audio        Silence      Frames   Packet
    Codec        Suppression  Per Pkt  Size(ms)
 1: G.711MU           n         2        20
 2:
 3:
```

</td></tr>
</table>

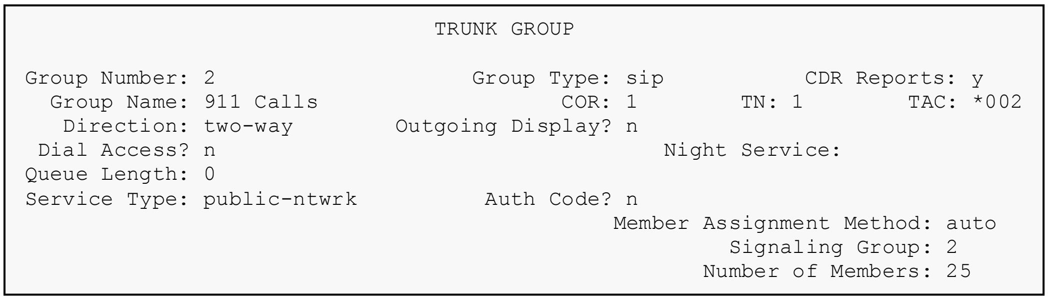
Step	Description
21.	**Signaling Group**

Use the **add signaling-group *n*** command, where ***n*** is an unused signaling group, to create a new signaling group for each SIP trunk to SM. For compliance test, signaling group 2 was created for the trunk to the SM. Signaling group 31 was configured using the parameters highlighted below. Default values were used for all other fields.

- Set the **Group Type** to ***sip***.
- Set the **Trunk Group for Channel Selection** field to the trunk group created in the next step. This cannot be done until the trunk group is created. Thus, initially this field is left blank and later changed to the correct value after the trunk group is created. A separate trunk group will be created for each signaling-group.
- Set the **Near-end Node Name** to ***procr***. This node name maps to the IP address of the Avaya CM. Node names are defined using the **change node-names ip** command (**Step 2**).
- Set the **Far-end Node Name** to ***sm***. This node name maps to the IP address of the SM as defined using the **change node-names ip** command (**Step 2**).
- Set the **Near-end Listen Port** and **Far-end Listen Port** to ***5061***.
- Set the **Far-end Network Region** to ***1***. This is the IP network region which contains the SM.
- Set **DTMF over IP** to **in-band**
- The default values were used for all other fields.

```
add signaling-group 2
                                SIGNALING GROUP

 Group Number: 2              Group Type: sip
  IMS Enabled? n        Transport Method: tls
        Q-SIP? n                                          SIP Enabled LSP? n
     IP Video? n                                   Enforce SIPS URI for SRTP? y
  Peer Detection Enabled? y  Peer Server: SM



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

Far-end Domain: avaya.com
                                             Bypass If IP Threshold Exceeded? n
Incoming Dialog Loopbacks: eliminate                  RFC 3389 Comfort Noise? n
         DTMF over IP: in-band                Direct IP-IP Audio Connections? y
Session Establishment Timer(min): 3                     IP Audio Hairpinning? n
         Enable Layer 3 Test? y                    Initial IP-IP Direct Media? n
H.323 Station Outgoing Direct Media? n             Alternate Route Timer(sec): 6
```

Step	Description
22.	**Trunk Group** Use the **add trunk-group *n*** command, where ***n*** is an unused trunk group, to create a new trunk group for each SIP trunk to SM. For the compliance test, trunk group 2 was created for the trunk to SM. Trunk group 2 was configured using the parameters highlighted below. On **Page 1**: ▪ Set the **Group Type** to ***sip***. ▪ Enter a descriptive name for the **Group Name**. ▪ Enter an available trunk access code (TAC) that is consistent with the existing dial plan in the **TAC** field. ▪ Set the **Service Type** to ***tie***. ▪ Set the **Member Assignment Method** to ***auto***. ▪ Set the **Signaling Group** to the signaling group shown in the previous step. ▪ Set the **Number of Members** field to the number of channels available in this trunk. For the compliance test, the number of members was chosen to be ***25***. ▪ The default values were used for all other fields.



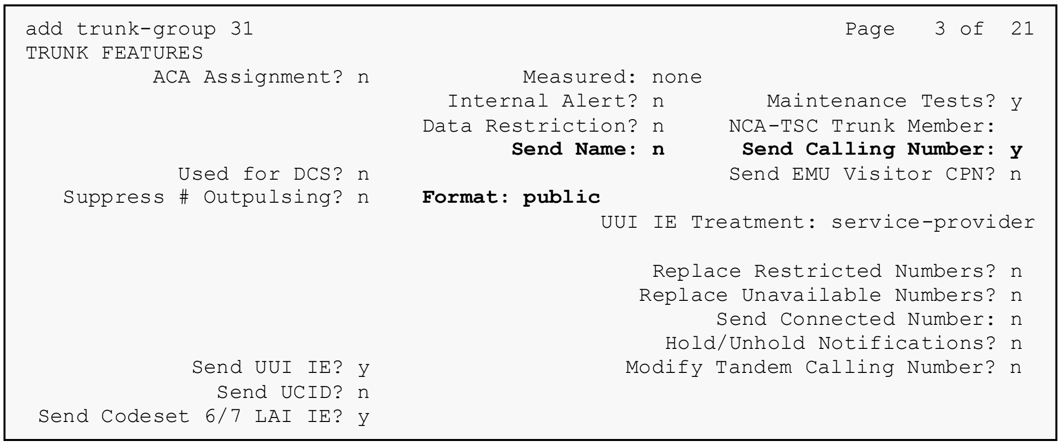
```
                                TRUNK GROUP

Group Number: 2                   Group Type: sip           CDR Reports: y
  Group Name: 911 Calls                  COR: 1        TN: 1        TAC: *002
   Direction: two-way        Outgoing Display? n
 Dial Access? n                                  Night Service:
Queue Length: 0
Service Type: public-ntwrk          Auth Code? n
                                              Member Assignment Method: auto
                                                       Signaling Group: 2
                                                     Number of Members: 25
```

Step | **Description**

23. **Trunk Group – continued**

On **Page 3**:

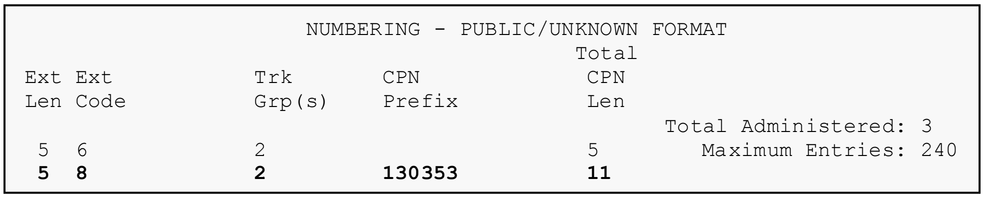
- It is required that the **Send Name** field is set to ***n*** and the **Send Calling Number** field is set to ***y***.
- Set the **Format** field to ***public***. This field specifies the format of the calling party number sent to the far-end.
- The default values were used for all other fields.



```
add trunk-group 31                                              Page   3 of  21
TRUNK FEATURES
          ACA Assignment? n            Measured: none
                                  Internal Alert? n       Maintenance Tests? y
                                Data Restriction? n     NCA-TSC Trunk Member:
                                       Send Name: n      Send Calling Number: y
            Used for DCS? n                             Send EMU Visitor CPN? n
   Suppress # Outpulsing? n     Format: public
                                              UUI IE Treatment: service-provider

                                                  Replace Restricted Numbers? n
                                                 Replace Unavailable Numbers? n
                                                       Send Connected Number: n
                                                   Hold/Unhold Notifications? n
             Send UUI IE? y                      Modify Tandem Calling Number? n
               Send UCID? n
 Send Codeset 6/7 LAI IE? y
```

24. **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 **Step 6**. In the example shown below, all calls originating from a 5-digit extension beginning with 8 and routed across trunk group 2 will be sent as an 11-digit calling number.

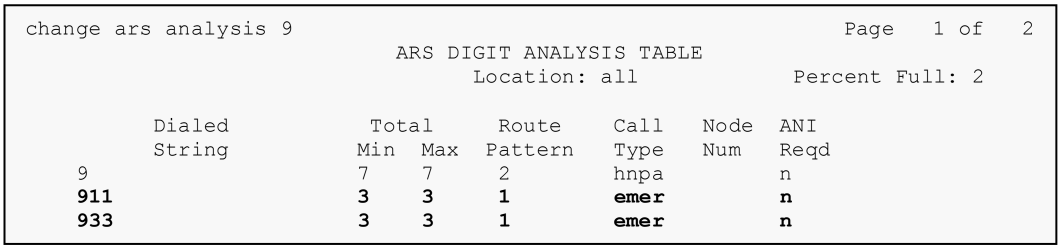


```
                      NUMBERING - PUBLIC/UNKNOWN FORMAT
                                             Total
Ext Ext            Trk       CPN              CPN
Len Code           Grp(s)    Prefix           Len
                                                    Total Administered: 3
 5  6              2                          5        Maximum Entries: 240
 5  8              2         130353           11
```

<table>
<tr><th>Step</th><th>Description</th></tr>
<tr><td>25.</td><td>

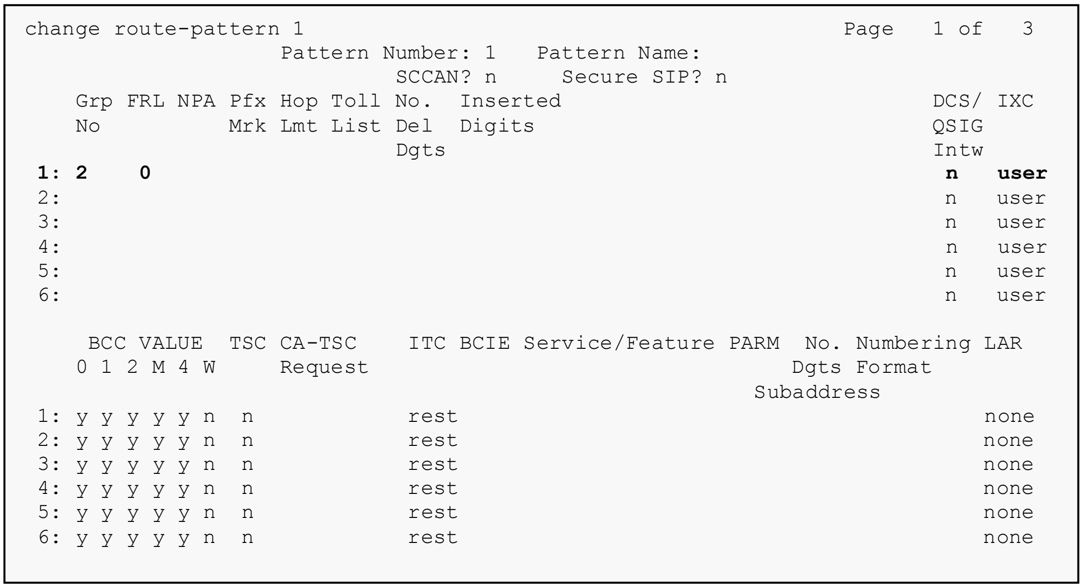
Automatic Route Selection (ARS)
For the compliance test, ARS was used to route emergency calls to 911 ETC via SM. The dialed string of 9 was configured as the feature access code (FAC) for ARS. Use the **change ars analysis** command to create an entry in the ARS table. Accessing ARS without first dialing the FAC, is only possible if the **ARS/AAR Dialing without FAC** field is enabled. Use the **display system-parameters customer-options** command to view its current state. In either case, the preceding 9 is removed by ARS before searching the table for a matching entry.

For the current compliance test, only the user dialed string of 9911 was tested.



```
change ars analysis 9                                         Page   1 of   2
                             ARS DIGIT ANALYSIS TABLE
                                   Location: all            Percent Full: 2

          Dialed           Total     Route    Call   Node   ANI
          String          Min  Max  Pattern   Type   Num    Reqd
    9                     7    7     2        hnpa          n
    911                   3    3     1        emer          n
    933                   3    3     1        emer          n
```

</td></tr>
</table>

Step	Description
26.	**Route Patterns** Use the **change route pattern *n*** command, where ***n*** is an unused route pattern, to create a separate route pattern for each of the dialed strings used for emergency calls in the ARS table. Set the **Pattern Name** field to a descriptive name. Create an entry in the table for each trunk that will be used in an attempt to complete the emergency call. The example below shows route pattern 1 used in the compliance test. Route pattern 1 was accessed when ARS matches on a dialed string of 911 and 933. For the first entry, set the **Grp No.** field to the trunk group of SM (trunk group 2). Set the Facility Restriction Level (**FRL**) of the trunk to an appropriate level to allow authorized users to access the trunk. The level of ***0*** is the least restrictive. Set the Lookahead Routing (**LAR**) field to ***next***. This allows the next trunk in the table to be selected if the current one is unavailable. 

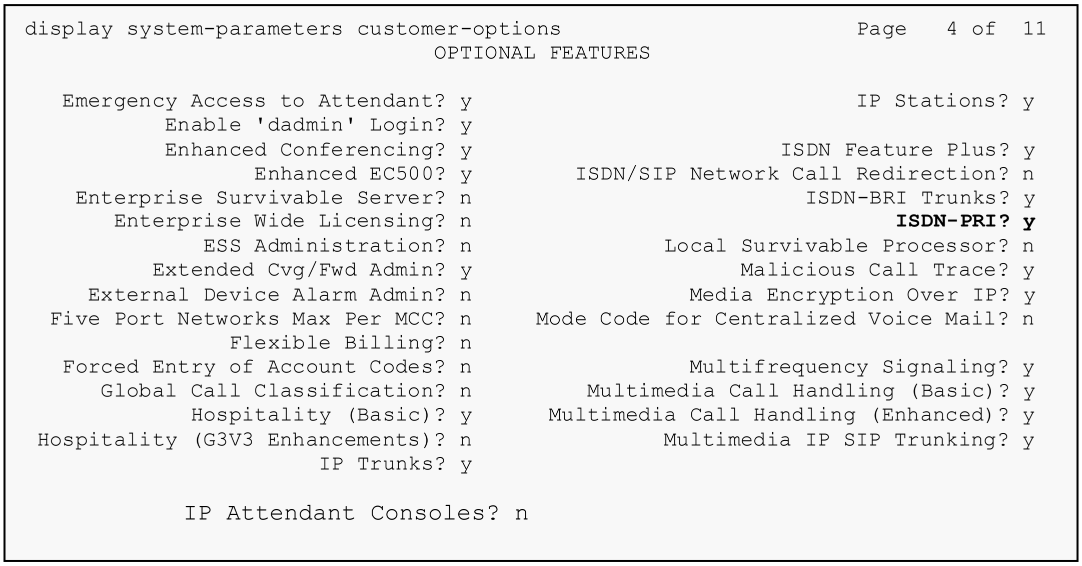
```
change route-pattern 1                                          Page   1 of   3
                    Pattern Number: 1   Pattern Name:
                             SCCAN? n     Secure SIP? n
    Grp FRL NPA Pfx Hop Toll No.  Inserted                             DCS/ IXC
    No          Mrk Lmt List Del  Digits                               QSIG
                             Dgts                                      Intw
 1: 2    0                                                              n   user
 2:                                                                     n   user
 3:                                                                     n   user
 4:                                                                     n   user
 5:                                                                     n   user
 6:                                                                     n   user

     BCC VALUE  TSC CA-TSC    ITC BCIE Service/Feature PARM  No. Numbering LAR
    0 1 2 M 4 W     Request                                 Dgts Format
                                                         Subaddress
 1: y y y y y n  n            rest                                         none
 2: y y y y y n  n            rest                                         none
 3: y y y y y n  n            rest                                         none
 4: y y y y y n  n            rest                                         none
 5: y y y y y n  n            rest                                         none
 6: y y y y y n  n            rest                                         none
```

<table>
<tr><th>Step</th><th>Description</th></tr>
<tr><td>27.</td><td><b>Route Patterns – Continued</b>
For Compliance testing, only few tests were made to an actual PSAP. For the rest of the test scenarios, calls were sent to an Address Verification System, by calling 933.
<pre>
change route-pattern 1   Page   1 of   3
                    Pattern Number: 1   Pattern Name:
                             SCCAN? n   Secure SIP? n
    Grp FRL NPA Pfx Hop Toll No. Inserted   DCS/ IXC
    No   Mrk Lmt List Del Digits   QSIG
                             Dgts   Intw
 1: 2   0   n   user
 2:   n   user
 3:   n   user
 4:   n   user
 5:   n   user
 6:   n   user

     BCC VALUE TSC CA-TSC   ITC BCIE Service/Feature PARM No. Numbering LAR
    0 1 2 M 4 W   Request   Dgts Format
                                                         Subaddress
 1: y y y y y n n   rest   none
 2: y y y y y n n   rest   none
 3: y y y y y n n   rest   none
 4: y y y y y n n   rest   none
 5: y y y y y n n   rest   none
 6: y y y y y n n   rest   none
</pre></td></tr>
</table>

6.2. Trunk Configuration – for ISDN/PRI to 911 ETC

As part of CrisisConnect to VoIP solution, ISDN calls to 911 ETC were also tested. For PSTN interconnections, CrisisConnect® for VoIP uses ISDN PSTN on an Avaya Media Gateway to route calls to   911 ETC E.164 number.

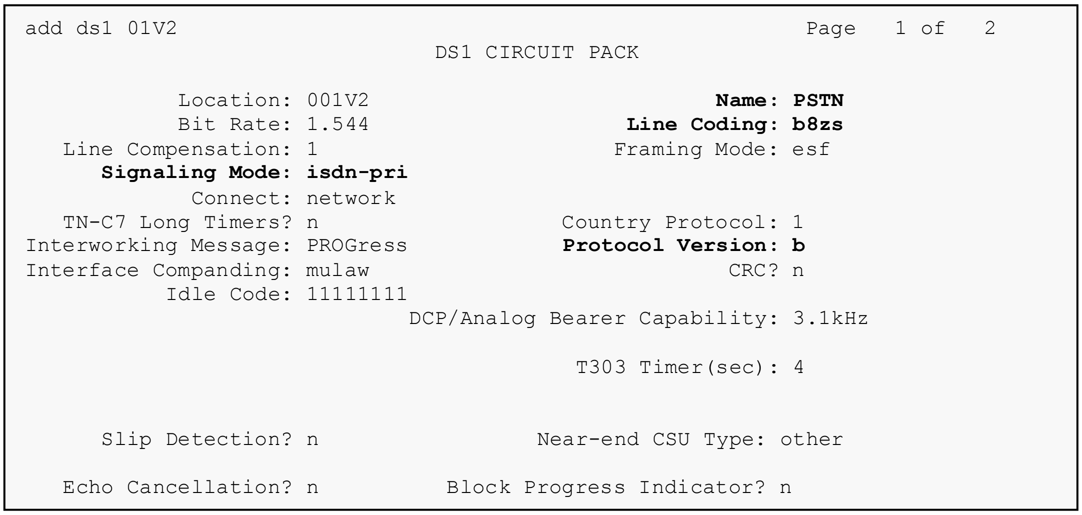
Step	Description
1.	**System Parameters – Customer Options** Use the **display system-parameters customer-options** command to verify that the options highlighted below are enabled. 

```
display system-parameters customer-options                       Page   4 of  11
                                OPTIONAL FEATURES

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

          IP Attendant Consoles? n
```

Step **Description**

2. **Add DS1**

Use the **add ds1 *Board-location*** command to add a DS1. In this case, board V2 was used. The gateway used for this testing, was connected to another Avaya Media Gateway which had access to PSTN. This configuration pertains to the Media Gateway G450 as show in the **Test Configuration** diagram.

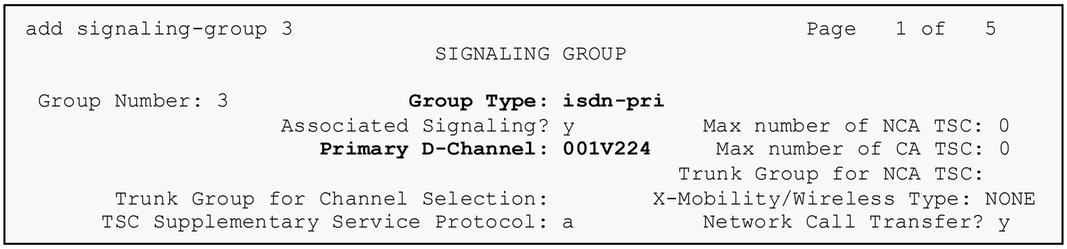


```
add ds1 01V2                                                Page   1 of   2
                                DS1 CIRCUIT PACK

            Location: 001V2                            Name: PSTN
            Bit Rate: 1.544                     Line Coding: b8zs
   Line Compensation: 1                        Framing Mode: esf
      Signaling Mode: isdn-pri
             Connect: network
   TN-C7 Long Timers? n                    Country Protocol: 1
Interworking Message: PROGress             Protocol Version: b
Interface Companding: mulaw                             CRC? n
           Idle Code: 11111111
                              DCP/Analog Bearer Capability: 3.1kHz

                                            T303 Timer(sec): 4



      Slip Detection? n                  Near-end CSU Type: other

   Echo Cancellation? n          Block Progress Indicator? n
```

3. **Signaling Group**

Use the **add signaling-group *n*** command, where ***n*** is an unused signaling group, to create a new signaling group for each ISDN to PSTN Gateway. For the compliance test, signaling group 3 was created for the trunk to the PSTN Gateway.

- Set the **Group Type** to ***isdn-pri***.
- Set the **Trunk Group for Channel Selection** field to the trunk group created in the next step. This cannot be done until the trunk group is created. Thus, initially this field is left blank and later changed to the correct value after the trunk group is created. A separate trunk group will be created for each signaling-group.
- Set Primary D-Channel according to ds1 added in **Step 2**.
- The default values were used for all other fields.



```
add signaling-group 3                                       Page   1 of   5
                                SIGNALING GROUP

 Group Number: 3              Group Type: isdn-pri
                   Associated Signaling? y         Max number of NCA TSC: 0
                        Primary D-Channel: 001V224     Max number of CA TSC: 0
                                                 Trunk Group for NCA TSC:
       Trunk Group for Channel Selection:       X-Mobility/Wireless Type: NONE
      TSC Supplementary Service Protocol: a         Network Call Transfer? y
```

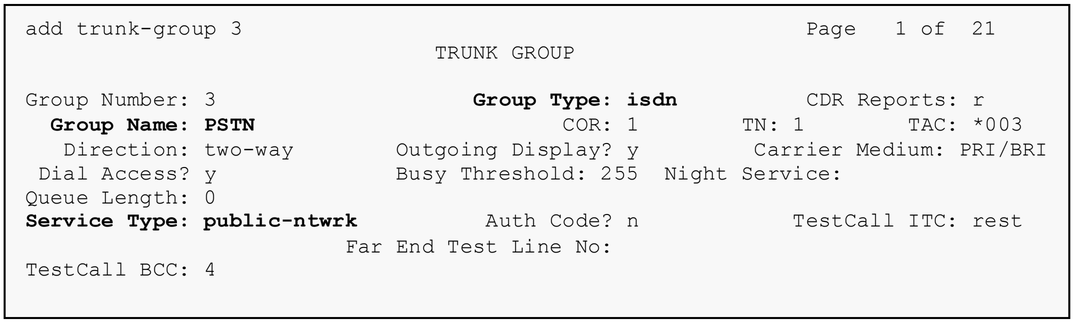
Step **Description**

4. **Trunk Group**

Use the **add trunk-group *n*** command, where ***n*** is an unused trunk group, to create a new trunk group for each ISDN/PRI to PSTN gateway. For the compliance test, trunk group 3 was created for the trunk to the Media Gateway as shown in the **Test Configuration** diagram.

On **Page 1**:

- Set the **Group Type** to ***isdn***.
- Enter a descriptive name for the **Group Name**.
- Enter an available trunk access code (TAC) that is consistent with the existing dial plan in the **TAC** field.
- Set the **Carrier Medium** to ***PRI/BRI***.
- Set the **Service Type** to ***public-ntwrk***.
- Set the **Signaling Group** to the signaling group shown in the previous step.
- Set the **Number of Members** field to the number of channels available in this trunk. For an H.323 trunk, the number of members also represents the number of simultaneous calls that can be supported by the trunk. For the compliance test, the number of members was chosen to be ***6***.
- The default values were used for all other fields.



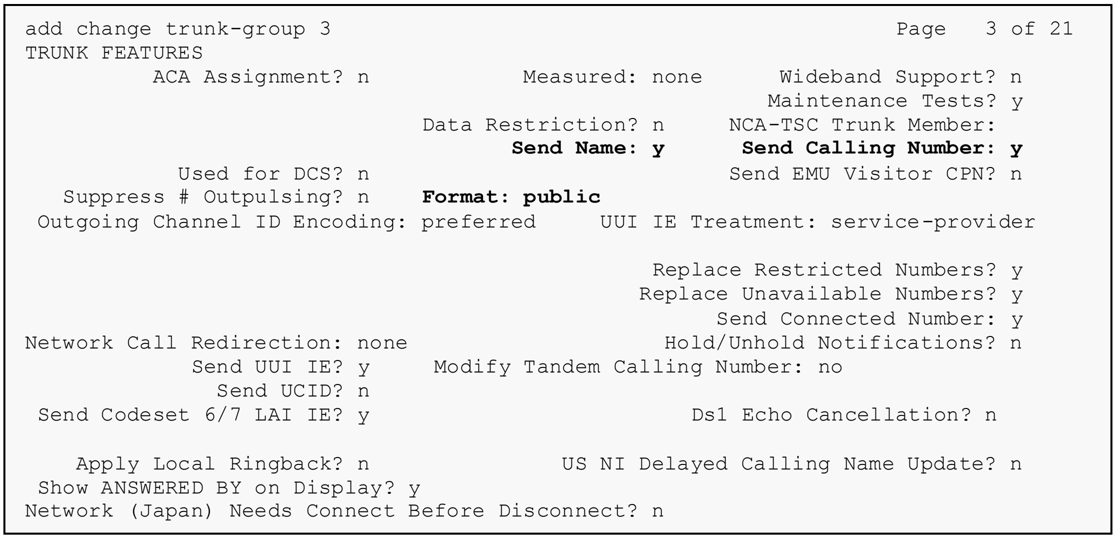
```
add trunk-group 3                                           Page   1 of  21
                                TRUNK GROUP

Group Number: 3                   Group Type: isdn          CDR Reports: r
  Group Name: PSTN                       COR: 1        TN: 1        TAC: *003
   Direction: two-way       Outgoing Display? y        Carrier Medium: PRI/BRI
 Dial Access? y             Busy Threshold: 255  Night Service:
Queue Length: 0
Service Type: public-ntwrk           Auth Code? n            TestCall ITC: rest
                         Far End Test Line No:
TestCall BCC: 4
```

<table>
<tr><th>Step</th><th>Description</th></tr>
<tr><td>5.</td><td>

Trunk Group – Continued

On Page 3:

- Set **Send Name** to **Yes**
- Set **Send Calling Number** to **Yes**
- Set **Format** to Public

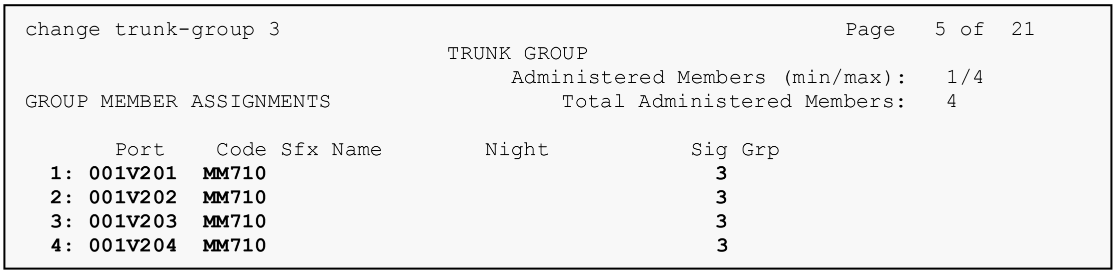


```
add change trunk-group 3                                            Page   3 of 21
TRUNK FEATURES
          ACA Assignment? n            Measured: none      Wideband Support? n
                                                          Maintenance Tests? y
                               Data Restriction? n     NCA-TSC Trunk Member:
                                      Send Name: y      Send Calling Number: y
            Used for DCS? n                            Send EMU Visitor CPN? n
   Suppress # Outpulsing? n    Format: public
 Outgoing Channel ID Encoding: preferred     UUI IE Treatment: service-provider

                                                 Replace Restricted Numbers? y
                                                Replace Unavailable Numbers? y
                                                      Send Connected Number: y
Network Call Redirection: none                    Hold/Unhold Notifications? n
             Send UUI IE? y     Modify Tandem Calling Number: no
               Send UCID? n
 Send Codeset 6/7 LAI IE? y                         Ds1 Echo Cancellation? n

    Apply Local Ringback? n               US NI Delayed Calling Name Update? n
 Show ANSWERED BY on Display? y
Network (Japan) Needs Connect Before Disconnect? n
```

</td></tr>
<tr><td>6.</td><td>

Trunk Group – Continued

On Page 4, assign the ports to be used to the signaling group created in **Step 3**. In this case, only 4 ports were assigned as follows:



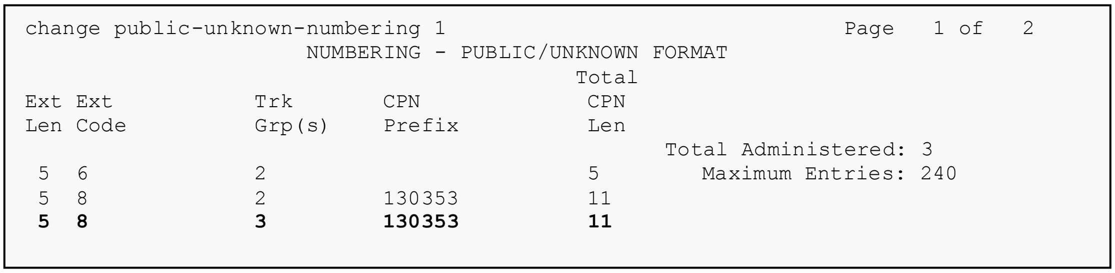
```
change trunk-group 3                                            Page   5 of  21
                                 TRUNK GROUP
                                      Administered Members (min/max):   1/4
GROUP MEMBER ASSIGNMENTS                  Total Administered Members:   4

       Port    Code Sfx Name        Night           Sig Grp
  1: 001V201  MM710                                   3
  2: 001V202  MM710                                   3
  3: 001V203  MM710                                   3
  4: 001V204  MM710                                   3
```

</td></tr>
</table>

<table>
<tr><th>Step</th><th>Description</th></tr>
<tr><td>7.</td><td>

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 **Step 4**. In the example shown below, all calls originating from a 5-digit extension beginning with 8 and routed across trunk group 3 will be sent as an 11-digit calling number.

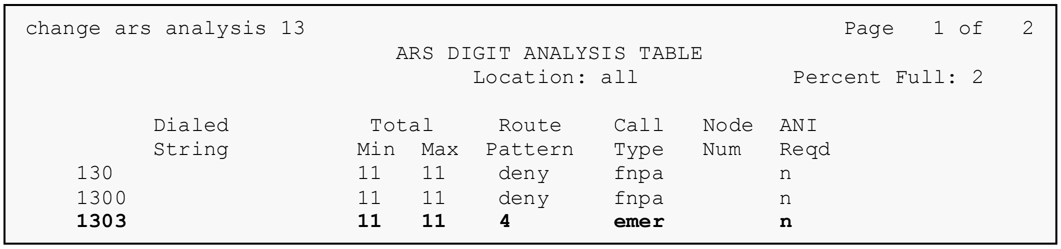


```
change public-unknown-numbering 1                                Page   1 of   2
                      NUMBERING - PUBLIC/UNKNOWN FORMAT
                                           Total
Ext Ext           Trk       CPN             CPN
Len Code          Grp(s)    Prefix          Len
                                                  Total Administered: 3
 5  6             2                         5        Maximum Entries: 240
 5  8             2         130353          11
 5  8             3         130353          11
```

</td></tr>
<tr><td>8.</td><td>

Automatic Route Selection (ARS)

For the compliance test, an entry was added to route emergency calls to 911 ETC by dialing an 11 digit DID. The entry is highlighted below which is used to route emergency calls to 911 ETC by dialing 1303xxxxxxx. The ECRC number begins with the dialed string of ***1303***. This dialed string is mapped to route pattern ***4*** which routes calls to trunk 3 connected to the PSTN.



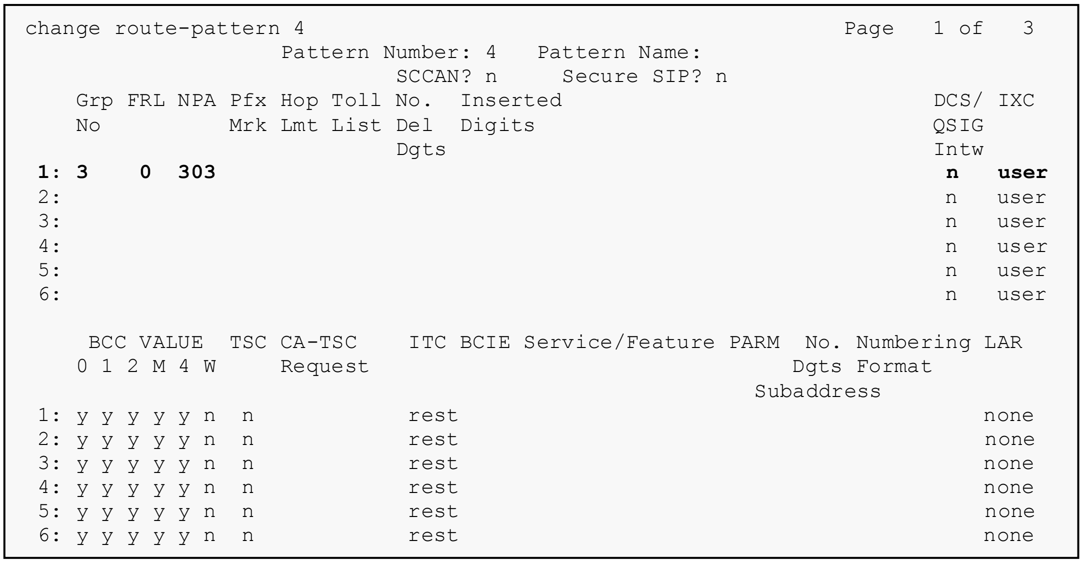
```
change ars analysis 13                                           Page   1 of   2
                             ARS DIGIT ANALYSIS TABLE
                                   Location: all          Percent Full: 2

          Dialed           Total     Route    Call   Node  ANI
          String          Min  Max  Pattern   Type   Num   Reqd
    130                   11   11    deny     fnpa         n
    1300                  11   11    deny     fnpa         n
    1303                  11   11    4        emer         n
```

</td></tr>
</table>

<table>
<tr><th>Step</th><th>Description</th></tr>
<tr><td>9.</td><td>

Route Pattern – PSTN Trunk

This route pattern is used in cases where the ISDN needs to be used to call the PSTN number of 911 ETC. Communication Manager will then route the call out the PSTN trunk.



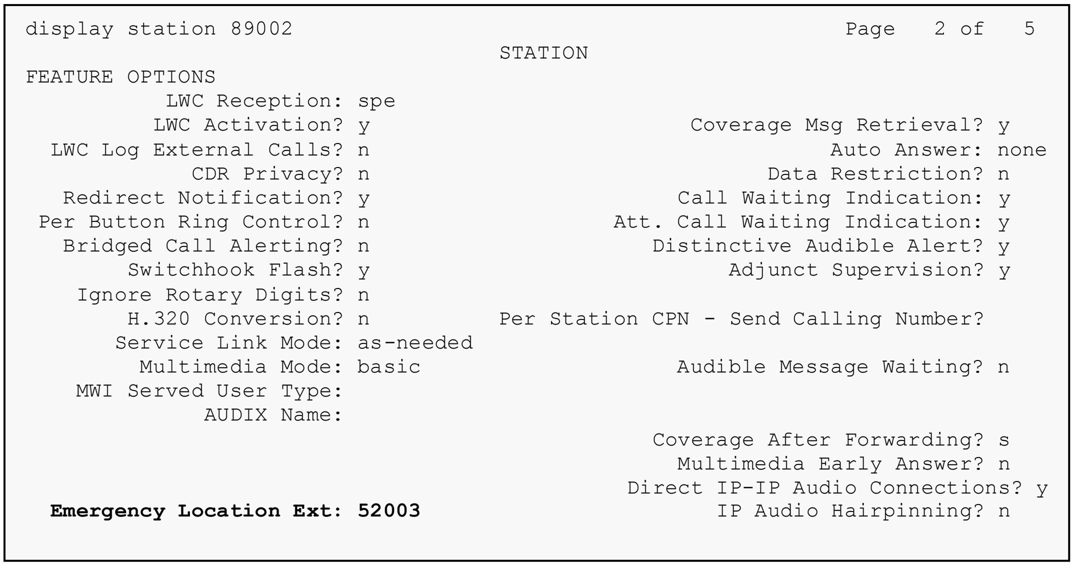
```
change route-pattern 4                                          Page   1 of   3
                    Pattern Number: 4   Pattern Name:
                             SCCAN? n     Secure SIP? n
    Grp FRL NPA Pfx Hop Toll No.  Inserted                             DCS/ IXC
    No          Mrk Lmt List Del  Digits                               QSIG
                             Dgts                                      Intw
 1: 3    0  303                                                         n   user
 2:                                                                     n   user
 3:                                                                     n   user
 4:                                                                     n   user
 5:                                                                     n   user
 6:                                                                     n   user

     BCC VALUE  TSC CA-TSC    ITC BCIE Service/Feature PARM  No. Numbering LAR
    0 1 2 M 4 W     Request                                 Dgts Format
                                                         Subaddress
 1: y y y y y n  n            rest                                         none
 2: y y y y y n  n            rest                                         none
 3: y y y y y n  n            rest                                         none
 4: y y y y y n  n            rest                                         none
 5: y y y y y n  n            rest                                         none
 6: y y y y y n  n            rest                                         none
```

</td></tr>
</table>

6.3. Station Configuration

<table>
<tr><th>Step</th><th>Description</th></tr>
<tr><td>1.</td><td>
<b>H.323 and SIP Telephones</b>
The example below shows the Emergency Location Extension configuration for an Avaya 9611 IP Telephone (H.323). Use the <b>display station <i>n</i></b> command, where <b><i>n</i></b> is the station extension, to view the settings. By default, the Emergency Location Extension is the same as the station extension and the <b>Always Use</b> field is set to <b><i>y</i></b>. If the <b>Always Use</b> field is set to <b><i>n</i></b>, then the Emergency Location Extension will be taken from the IP network map form if an extension is configured there. All H.323 and SIP telephones are configured in a similar way. For Compliance Testing, <b>Always User?</b> was set to <b>y</b>.
<pre>
display station 89001   Page   2 of   5
                                     STATION
FEATURE OPTIONS
           LWC Reception: spe   Auto Select Any Idle Appearance? n
          LWC Activation? y   Coverage Msg Retrieval? y
  LWC Log External Calls? n   Auto Answer: none
             CDR Privacy? n   Data Restriction? n
   Redirect Notification? y   Idle Appearance Preference? n
 Per Button Ring Control? n   Bridged Idle Line Preference? n
   Bridged Call Alerting? n   Restrict Last Appearance? y
  Active Station Ringing: single
                                                         EMU Login Allowed? n
        H.320 Conversion? n   Per Station CPN - Send Calling Number? y
       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: 89001   Always Use? y IP Audio Hairpinning? n
</pre>
</td></tr>
</table>

Step	Description
2.	**Digital and Analog Telephones** The example below shows the Emergency Location Extension configuration for a digital telephone. Use the **display station *n*** command, where ***n*** is the station extension, to view the settings. By default, the Emergency Location Extension is the same as the station extension. There is no **Always Use** field as there was for the H.323/SIP telephones. All digital and analog telephones are configured in a similar way.



```
display station 89002                                           Page   2 of   5
                                     STATION
FEATURE OPTIONS
           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                             Adjunct Supervision? y
    Ignore Rotary Digits? n
        H.320 Conversion? n          Per Station CPN - Send Calling Number?
       Service Link Mode: as-needed
         Multimedia Mode: basic                     Audible Message Waiting? n
    MWI Served User Type:
              AUDIX Name:
                                                 Coverage After Forwarding? s
                                                   Multimedia Early Answer? n
                                               Direct IP-IP Audio Connections? y
  Emergency Location Ext: 52003                         IP Audio Hairpinning? n
```

7. Generation Test Approach and Test Results

The compliance tests were performed manually. Test calls were initially placed to 933 instead of 911 due to the nature of emergency calls. 911 calls to an actual PSAP were made to test ALI, audio and DTMF. Please note the DTMF mode needs to be setup as in-band, since out-of-band is not yet supported by 911 ETC.

All test cases were executed and passed.

8. Verification Steps

911 ETC suggests that calls to 933 (Address Verification Systems) are placed to confirm the routing to 911 ETC. After the configuration is complete, verify that the Address Verification System can be reached by dialing 933.

9. Conclusion

These Application Notes describe the configuration steps required for 911 ETC Crisis Connect to successfully interoperate with Avaya Aura® Session Manager and Avaya Aura® Communication Manager. All compliance tests were completed as passed, except for DTMF out-of-band test, it was failed.

10. Additional References

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

Avaya

[1] *Administering Avaya Aura® Communication Manager*, Doc # 03-603558, Release 6.0.1, Issue 1.3, December 2010.

[2] *Administering Avaya Aura® Session Manager*, Doc # 03-603324, Release 6.2, February 2012

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.