



Application Notes for Solution Redundancy of NEC IP DECT Handsets with Avaya Aura® Communication Manager R7.0.1 and Avaya Aura® Session Manager R7.0.1 using TLS/SRTP – Issue 1.0

Abstract

These Application Notes describe the configuration steps for provisioning NEC's IP DECT Access Points and Handsets to interoperate with Avaya Aura® Communication Manager and Avaya Aura® Session Manager focusing on the redundancy of the NEC DECT handsets having them registered simultaneously to multiple Avaya Aura® Session Manager instances.

Readers should pay particular attention to the scope of testing as outlined in Section 2.1, as well as observations noted in Section 2.2 to ensure that their own use cases are adequately covered by this scope and results.

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 configuration steps for provisioning NEC's IP DECT Access Point (AP400) and NEC's DECT handsets to interoperate with Avaya Aura® Communication Manager R7.0.1 and Avaya Aura® Session Manager R7.0.1 specifically to show redundancy using multiple simultaneous registrations with different Avaya Aura® Session Managers in a main/branch environment and seamless failover during active calls when an outage occurs.

Application Notes have already been written outlining the setup of the NEC IP DECT Access Points AP400 and NEC DECT Handsets with Avaya Aura® Communication Manager and Avaya Aura® Session Manager using TLS/SRTP, therefore these Application Notes will focus instead on the setup required for redundancy and how the NEC DECT handsets respond to various failover scenarios outlined in **Section 2.1**. For more information on the configuration of the NEC DECT handsets with Avaya Aura® Communication Manager and Avaya Aura® Session Manager using TLS/SRTP please refer to the Application Notes titled, *Application Notes for configuring NEC IP DECT Access Points AP400 and NEC DECT Handsets with Avaya Aura® Communication Manager R7.0 and Avaya Aura® Session Manager R7.0 using TLS/SRTP*.

An NEC IP DECT solution typically consists of a windows based instance called DAP Controller that runs the IP DECT system software (DAP Configurator and DAP Manager), one or more DECT access points (DAP) AP400, DECT handsets (e.g. G566, I766, G966) and if needed a software based DMLS open interface for messaging and alarming. The DAP's are connected to the IP network and get the needed power by using POE following 802.3af standard. Multiple NEC DECT access points (DAP) are tied together to build a single DECT system. The handsets are enrolled into that System using Digital Enhanced Cordless Technology (DECT). Each DAP is hosting (responsible for) a particular number of handsets although roaming/handover is possible across all DAPs. The DAPs are configured to register with Session Manager using Session Initiation Protocol (SIP). A single DAP will register multiple times against Session Manager on behalf of the handsets it is responsible for.

Each handset is configured as a SIP user on Avaya Aura® System Manager, using an Avaya 9608 SIP endpoint type on Avaya Aura® Communication Manager. The NEC DECT handsets behave as third-party SIP extensions (non AST device) integrated into the Avaya Aura® Core. They are able to register to different Avaya Aura® Session Managers simultaneously in a similar way to the Avaya SIP phones allowing for no manual intervention upon any service interruption due to LAN or service failures on Avaya Aura® Session Manager.

2. General Test Approach and Test Results

The interoperability compliance testing evaluates the ability of NEC DECT handsets to register with up to two core Session Manager instances and one Branch Session Manager as outlined in **Figure 1**. The NEC DECT handset supports multiple, simultaneous registrations allowing the DECT handsets to failover seamlessly during active calls between the core and branch sites. A number of failover and fall back (fail back) scenarios were carried out testing basic call functionality after every step as outlined in **Section 2.1**. In addition there was also tested the ability of the NEC DECT handsets to deal properly with a “301 Moved Permanently” message received from a Session Manager instance. This happens when a User (e.g. NEC DECT handset) tries to register against a Session Manager instance which is not responsible for that SIP User. This scenario is outlined in **Section 2.1.5**.

2.1. Interoperability Compliance Testing

The following scenarios were tested in order to prove that the NEC DECT phones were registered correctly to each Session Manager allowing for a seamless failover depending on the outage that occurred.

“Normal Mode” is, when all Core Components (SMGR, SM, CM etc.) are healthy and reachable and the NEC DECT handsets are registered simultaneously against two Core Session Manager instances and the Branch Session Manager.

“Failover feature tests” are a series of basic telephony features e.g. make call, answer call, hold, transfer, MWI to prove telephony functionality before and after an outage occurred. These tests were made by using Avaya SIP and H.323 phones along with NEC DECT handsets.

Note: For a complete list of tested/supported telephony features of the NEC DECT handsets in an Avaya Aura® environment, please refer to the Application Notes titled, *Application Notes for configuring NEC IP DECT Access Points AP400 and NEC DECT Handsets with Avaya Aura® Communication Manager R7.0 and Avaya Aura® Session Manager R7.0 using TLS/SRTP*.

2.1.1. LAN failure and failover Site 1 (CM, SM1) to Site 2 (SC, SM2)

Failover from Site 1 to Site 2, starting in “Normal Mode”, several LAN failures are then experienced in the following order with some basic feature tests carried out after each failure.

1. Fail network connectivity to Active CM (CMA), redundant CM (CMB) at the same location becomes active.
2. Carry out “failover feature tests”.
3. Fail network connectivity to redundant CM (CMB) at main location (both down), Session Manager 1 (SM1) at main site (Site1) now talks to Survivable Core (SC) at backup location (Site 2).
4. Carry out “failover feature tests”.
5. Fall-back to CMA at main location (Site 1).
6. Carry out “failover feature tests”.
7. Fail network connectivity to SM1 (Site 1). NEC Endpoints which are already registered with Session Manager 2 (SM2) will now SUBSCRIBE to events from SM2 at backup location (Site 2) and use SM2 as the active Controller.

8. Carry out “failover feature tests”.
9. Restore network connectivity to SM1 (Site 1). NEC Endpoints will automatically REGISTER and SUBSCRIBE again with SM1 at main location (Site 1) and use SM1 as the active controller.
10. Carry out “failover feature tests”.
11. Force a complete failover from Site 1 to Site 2 (failure the Media Server, Communication Manager and Session Manager at the main site). Survivable Core (SC) at Site 2 becomes active. SM2 talks to SC. NEC Endpoints which are already registered with SM2 will now SUBSCRIBE to events from SM2 at backup location (Site2) and use SM2 as the active Controller.
12. Carry out “failover feature tests”.
13. Restore network connectivity to CMA and CMB at main location (Site1). CMA or CMB becomes active and SC goes to backup. SM2 at backup location (Site2) now talks to active CM (either CMA or CMB) at main location (Site1).
14. Carry out “failover feature tests”.
15. Restore network connectivity to SM1 at main location (Site 1). NEC endpoints will automatically REGISTER and SUBSCRIBE again with SM1 at main location (Site 1) and use SM1 as the active controller. Now the system should be back to original state “normal mode” once again.
16. Carry out “failover feature tests”.

2.1.2. Session Manager ‘Deny New Service’ Failover Site 1 to Site 2

Session Manager Failovers are carried out by sending a “Deny New Service” to the Session Managers through the System Manager Web interface.

1. Starting from “Normal Mode”, send a “Deny New Service” to the SM1. NEC Endpoints which are already registered with Session Manager 2 (SM2) will now SUBSCRIBE to events from SM2 at backup location (Site 2) and use SM2 as the active Controller.
2. Carry out “failover feature tests”.
3. Fail network connectivity to CM duplex at main location (both CM instances not reachable), Survivable Core (SC) at Site 2 becomes active and SM2 now talks to SC at Site 2.
4. Carry out “failover feature tests”.
5. Fall-back to Session Manager at main location, by “Allow new service” on the SM1. NEC endpoints will automatically REGISTER and SUBSCRIBE again with SM1 and use this as the active controller. SM1 now talks to SC at Site 2.
6. Carry out “failover feature tests”.
7. Restore network connectivity to CM duplex at main location, SC goes to backup and CM becomes active again. SM1 now talks to CM at main location. System should be back to original state “normal mode” once again.
8. Carry out “failover feature tests”.

2.1.3. Failover to Site 3 (Branch Site) in case of a WAN outage

The BSM and LSP at the Branch site will come into use when a WAN failure is detected from the Branch Site. The NEC DECT handsets at the Branch location will now SUBSCRIBE and start using the Branch Session Manager (BSM) and LSP at the Branch site. They will remain REGISTERED at the BSM once the WAN connection to the Main Site has recovered.

1. Starting from “Normal Mode”, create a WAN failure by disconnecting the WAN cable on the Branch Site. LSP and BSM at Site 3 (Branch) become active. NEC endpoints which are already registered with Branch Session Manager (BSM) will now SUBSCRIBE to events from BSM and use BSM as the active controller.
2. Carry out “failover feature tests”.
3. Reconnect the WAN cable to ensure connectivity to the Main Site is restored. CM and SM1 at main location (Site1) as well as SM2 at backup location (Site2) become reachable again. LSP and BSM go backup. NEC endpoints at the branch (Site3) will automatically REGISTER and SUBSCRIBE again with SM1 and use this as the active controller. They will also REGISTER with SM2. Now the system should be back to original state “normal mode” once again.
4. Carry out “failover feature tests”.

2.1.4. Failover to Site 3 (Branch Site) when Site 1 and Site 2 go down

The BSM and LSP at the Branch site will come into use when all core components at main location (Site1) and backup location (Site2) will fail. The NEC DECT handsets at the Branch location will now SUBSCRIBE and start using the Branch Session Manager (BSM) and LSP at the Branch site. They will remain REGISTERED at the BSM once the WAN connection has recovered.

1. Starting from “Normal Mode” ensure that full failover from Site 1 to Site 2 occurs. SC and SM2 at backup location (Site 2) are now ‘Active’. NEC Endpoints which are already registered with Session Manager 2 (SM2) will now SUBSCRIBE to events from SM2 at backup location (Site 2) and use SM2 as the active Controller.
2. Carry out “failover feature tests”.
3. Create a simulated Site 2 failure by failing all components on Site 2, resulting in LSP and BSM at Site 3 (Branch) become active. NEC endpoints which are already registered with Branch Session Manager (BSM) will now SUBSCRIBE to events from BSM and use BSM as the active controller.
4. Carry out “failover feature tests”.
5. Reconnect the LAN cables on Site 2 components to ensure that connectivity to Site 2 is restored. SC and SM2 at backup location (Site2) become reachable again. LSP and BSM go backup. NEC endpoints at the branch (Site3) will automatically REGISTER and SUBSCRIBE again with SM2 and use this as the active controller. They remain registered to BSM.
6. Carry out “failover feature tests”.
7. Reconnect the LAN cables on Site 1 components to ensure that connectivity to Site 1 is restored. CM and SM1 at main location (Site1) become reachable again. SC goes backup. NEC endpoints at the branch (Site3) will automatically REGISTER and SUBSCRIBE

- again with SM1 and use this as the active controller. They will remain registered to SM2 and BSM. Now the system should be back to original state “normal mode” once again.
8. Carry out “failover feature tests”.

2.1.5. Session Manager Registration using ‘301 Moved Permanently’

The Avaya Aura® Core provides the ability that a Session Manager will send out a “301 Moved Permanently” upon a REGISTER in case this Session Manager instance is not responsible for that SIP user. The message includes the information which SM instances need to be used (Core SM and BSM) for that particular SIP user. The NEC endpoints (DAP) can deal with that message and use the provided information to register with the correct SM instances depending on the configuration within SMGR for each particular User and DECT handset.

1. The NEC DAP is configured to send initially all registrations to SM3. The SIP users on SMGR are configured to use SM1, SM2 and BSM.
2. The DAP send out a REGISTER to SM3 and receives a “301 Moved Permanently” message including the information to use SM1, SM2 and BSM instead of SM3.
3. The DAP now send out a REGISTER against SM1, SM2 and BSM as well as a SUBSCRIBE against SM1 for the NEC handset.
4. The NEC handset is registered against SM1, SM2 and BSM and subscribed against SM1 which is used as the active controller.

2.2. Test Results

All test cases passed successfully.

Active stable calls (NEC handset <-> Avaya SIP, NEC handset <-> Avaya H323, NEC handset <-> NEC handset, NEC handset <-> SIP-Trunk) which were established before an outage survived the outage and talk path remained.

2.3. Support

Support from Avaya is available by visiting the website <http://support.avaya.com> and a list of product documentation can be found in **Section 10** of these Application Notes. Technical support for the NEC IP DECT product can be obtained through NEC global technical support by accessing the website <http://www.nec-ipdect.com/Contact-7> or <http://businessnet.nec-enterprise.com> (which is available only for partners with authorized access).

3. Reference Configuration

Figure 1 shows the network topology during compliance testing. The NEC DECT handsets subscribe to the NEC DECT Access Points (DAP) which is placed on the LAN. The DECT handsets register with all Session Managers in order to be able to make/receive calls to and from the Avaya H.323 and SIP deskphones as well as from simulated PSTN SIP Trunks.

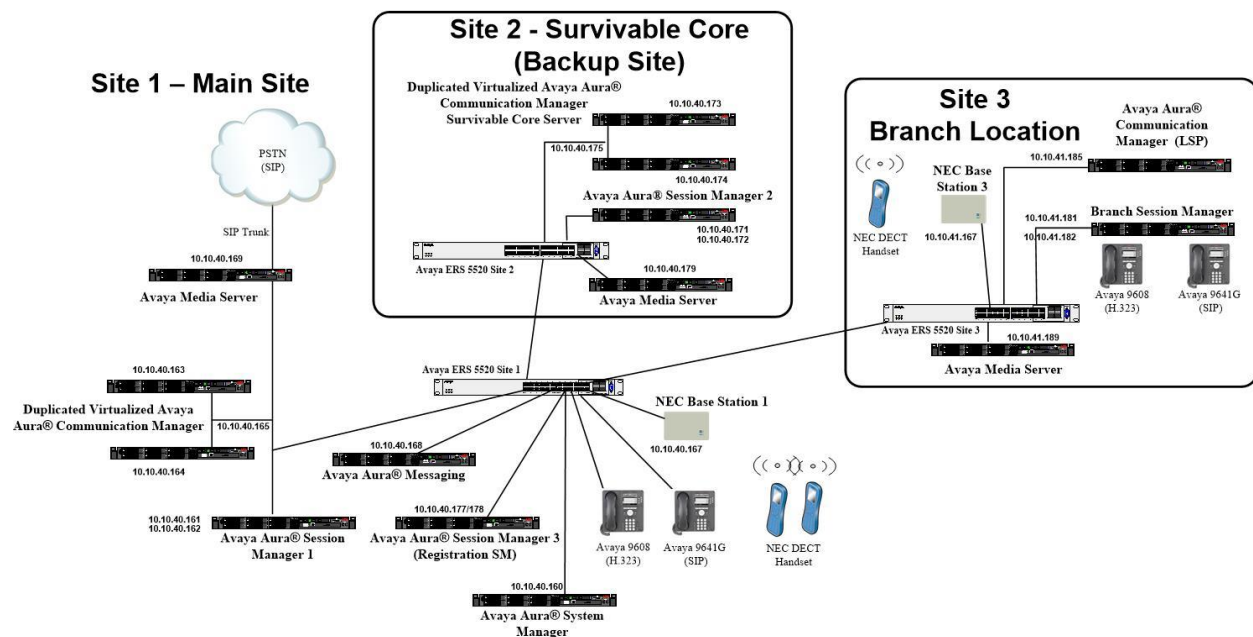


Figure 1: Network Solution of NEC DECT Handsets with Avaya Aura® Communication Manager R7.0.1 and Avaya Aura® Session Manager R7.0.1

4. Equipment and Software Validated

The following equipment and software was used for the compliance test.

Equipment/Software	Release/Version
Avaya Aura® System Manager running on a virtual server	System Manager 7.0.1.2 Build No. - 7.0.0.0.16266 Software Update Revision No: 7.0.1.2.086007 Service Pack 2
Avaya Aura® Session Manager running on a virtual server	Session Manager R7.0 SP2 Build No. – 7.0.1.2.701230
Avaya Aura® Communication Manager running on a virtual server	R7.0.1 R017x.00.0.441.0 00.0.441.0-23523
Avaya Media Server running on a virtual server	Media Server SYSTEM R7.7.0.21 Media Server R7.7.0.350
Avaya Aura® Messaging running on a virtual server	R7.0.0.0.441
Avaya 9608 H323 Deskphone	96x1 H323 Release 6.6.028
Avaya 9608 SIP Deskphone	96x1 SIP Release 7.0.0.39
DAP Controller software running on Windows 2012 virtual server	6.41.0554
NEC DECT Access Point	6.41 : 4920b653.dwl
NEC DECT Handset NEC G566	1.10.00.01
NEC DECT Handset NEC I766	1.10.00.02

5. Configure Avaya Aura® Communication Manager

It is assumed that a fully functioning Communication Manager is in place with the necessary licensing and with a SIP Trunk in place to Session Manager. For further information on the configuration of Communication Manager please see **Section 10** of these Application Notes. The following sections go through the following.

- Configure Dial Plan Analysis.
- Configure Node Names.
- Configure Signalling Group.
- Configure Trunk Group.
- Configure Route Pattern.
- Configure AAR Analysis.
- Network Region.
- IP Codec.

5.1. Configure Dial Plan Analysis

Use the **change dialplan analysis** command to configure the dial plan using the parameters shown below. Extension numbers (**ext**) are those beginning with **6**. Feature Access Codes (**fac**) use digits **8** and **9** or ***** and **#**.

change dialplan analysis			DIAL PLAN ANALYSIS TABLE						Page 1 of 12
			Location: all			Percent Full: 2			
Dialed String	Total Length	Call Type	Dialed String	Total Length	Call Type	Dialed String	Total Length	Call Type	
1	4	udp							
2	4	udp							
3	4	udp							
4	4	udp							
5	4	ext							
6	4	ext							
7	4	udp							
8	1	fac							
9	1	fac							
*	3	fac							
*8	4	dac							
#	3	fac							

5.2. Configure Node Names

Each component that talks to Communication Manager will need to be added under **node-names ip**. Type **change node-names ip** and add each Session Manager, Branch Session Manager and Media Server along with other equipment such as Local Survivability Servers and Survivable Cores. These were some of the components that were added for compliance testing, making note of **SMA70vmpg** and **SMB70vmpg** in particular as these will be required in creating the Signaling and Trunk Groups in **Section 5.3** and **Section 5.4**.

change node-names ip		Page 1 of 2
IP NODE NAMES		
Name	IP Address	
AMSBackup	10.10.40.179	
AMSBranch	10.10.41.189	
AMSMain	10.10.40.169	
BSM	10.10.41.182	
CMAvmpg	10.10.40.163	
CMBvmpg	10.10.40.164	
LSP2	10.10.40.170	
LSP3	10.10.41.170	
LSP70	10.10.41.185	
SC70Redundancy	10.10.40.175	
SCAvmpg	10.10.40.173	
SCBvmpg	10.10.40.174	
SMA70vmpg	10.10.40.162	
SMB70vmpg	10.10.40.172	
default	0.0.0.0	
procr	10.10.40.165	
(16 of 17 administered node-names were displayed)		
Use 'list node-names' command to see all the administered node-names		
Use 'change node-names ip xxx' to change a node-name 'xxx' or add a node-name		

5.3. Configure Signaling Group

A Signaling Group will need to be created for the connection between Communication Manager and Session Manager to route calls. There are two Session Managers in this configuration for redundancy so two signaling groups will need to be created. The following shows one of the SIP Signaling Groups that was used during compliance testing. Type **change signaling-group x**, where x is the signaling group number

- Set the **Group Type** field to **sip**.
- For compliance testing **Transport Method** was set to **tls**.
- The **Peer Detection Enabled** field should be set to **y** allowing the Communication Manager to automatically detect if the peer server is a Session Manager.
- Set the **Near-end Node Name** to **procr**. Set the **Far-end Node Name** to the node name defined for the Session Manager (node name **SMA70vmpg**), as per **Section 5.2**.
- Ensure that the recommended TLS port value of **5061** is configured in the **Near-end Listen Port** and the **Far-end Listen Port** fields.
- In the **Far-end Network Region** field, enter the IP Network Region configured in **Section 5.7**. This field logically establishes the **far-end** for calls using this signaling group as network region 1.
- **Far-end Domain** was set to the domain used during compliance testing.
- The **DTMF over IP** field should remain set to the default value of **rtp-payload**. This value enables Communication Manager to send DTMF transmissions using RFC 2833.
- The **Direct IP-IP Audio Connections** field is set to **y**.
- **Initial IP-IP Direct Media** was set to **n** for compliance testing.
- The default values for the other fields may be used.

change signaling-group 1		Page 1 of 2	
SIGNALING GROUP			
Group Number: 1	Group Type: sip		
IMS Enabled? n	Transport Method: tls		
Q-SIP? n			
IP Video? n	Enforce SIPS URI for SRTP? n		
Peer Detection Enabled? y Peer Server: SM			
Prepend '+' to Outgoing Calling/Alerting/Diverting/Connected Public Numbers? y			
Remove '+' from Incoming Called/Calling/Alerting/Diverting/Connected Numbers? n			
Alert Incoming SIP Crisis Calls? n			
Near-end Node Name: procr		Far-end Node Name: SMA70vmpg	
Near-end Listen Port: 5061		Far-end Listen Port: 5061	
		Far-end Network Region: 1	
Far-end Domain: devconnect.local			
		Bypass If IP Threshold Exceeded? n	
Incoming Dialog Loopbacks: eliminate		RFC 3389 Comfort Noise? n	
DTMF over IP: rtp-payload		Direct IP-IP Audio Connections? y	
Session Establishment Timer(min): 3		IP Audio Hairpinning? n	
Enable Layer 3 Test? n		Initial IP-IP Direct Media? n	
H.323 Station Outgoing Direct Media? n		Alternate Route Timer(sec): 6	

5.4. Configure Trunk Group

Like the Signaling Groups, a trunk group will need to be setup for each Session Manager connection. These trunk groups are used for calls to and from NEC SIP phones. Type **change trunk-group x**, where x is the trunk group number. Enter a descriptive name in the **Group Name** field. Set the **Group Type** field to **sip**. Enter a **TAC** code compatible with the Communication Manager dial plan. Set the **Service Type** field to **tie**. Specify the signaling group associated with this trunk group in the **Signaling Group** field, and specify the **Number of Members** supported by this SIP trunk group. Accept the default values for the remaining fields.

```

change trunk-group 1                                     Page 1 of 21
                                     TRUNK GROUP

Group Number: 1                      Group Type: sip      CDR Reports: y
  Group Name: SIPTRK1                COR: 1              TN: 1      TAC: *801
    Direction: two-way              Outgoing Display? n
    Dial Access? n                  Night Service:
    Queue Length: 0
  Service Type: tie                  Auth Code? n
                                     Member Assignment Method: auto
                                     Signaling Group: 1
                                     Number of Members: 10

```

On **Page 2** of the trunk-group form the **Preferred Minimum Session Refresh Interval (sec)** field should be set to a value mutually agreed with NEC to prevent unnecessary SIP messages during call setup. Session refresh is used throughout the duration of the call, to check the other side has not gone away, for the compliance test a value of **600** was used.

```

change trunk-group 1                                     Page 2 of 21
  Group Type: sip

TRUNK PARAMETERS

  Unicode Name: auto

                                     Redirect On OPTIM Failure: 5000

    SCCAN? n                          Digital Loss Group: 18
    Preferred Minimum Session Refresh Interval(sec): 600

  Disconnect Supervision - In? y  Out? y

    XOIP Treatment: auto      Delay Call Setup When Accessed Via IGAR? n

  Caller ID for Service Link Call to H.323 1xC: station-extension

```

Settings on **Page 3** can be left as default. However the **Numbering Format** in the example below is set to **private**.

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

Settings on **Page 4** are as follows.

change trunk-group 1	Page 4 of 21
PROTOCOL VARIATIONS	
	Mark Users as Phone? y
Prepend '+' to Calling/Alerting/Diverting/Connected Number? n	
Send Transferring Party Information? y	
Network Call Redirection? y	
Build Refer-To URI of REFER From Contact For NCR? n	
Send Diversion Header? n	
Support Request History? y	
Telephone Event Payload Type: 120	
Convert 180 to 183 for Early Media? n	
Always Use re-INVITE for Display Updates? n	
Identity for Calling Party Display: P-Asserted-Identity	
Block Sending Calling Party Location in INVITE? n	
Accept Redirect to Blank User Destination? n	
Enable Q-SIP? n	
Interworking of ISDN Clearing with In-Band Tones: keep-channel-active	
Request URI Contents: may-have-extra-digits	

5.5. Route Pattern

A route pattern is implemented to route calls to SIP phones. This route pattern should include the trunk groups to both core Session Managers. Note that two signaling groups and two trunk groups were set up connecting Communication Manager to both Session Manager A and Session Manager B. For compliance testing these were labelled 1 and 2 and so these two trunk groups were added to route pattern 61 as shown below. In order to amend this route pattern type in **change route-pattern x**, where x is the route pattern to be changed. Enter a suitable **Pattern Name** and add the two trunk groups to the **Grp No** as shown below.

change route-pattern 61										Page	1 of	3
Pattern Number: 61										Pattern Name: SIP_PHONES		
SCCAN? n Secure SIP? n Used for SIP stations? y												
Primary SM: SMA70vmpg Secondary SM: SMB70vmpg												
Grp FRL NPA Pfx Hop Toll No. Inserted										DCS/	IXC	
No Mrk Lmt List Del Digits										QSIG		
Dgts										Intw		
1:	1	0								n	user	
2:	2	0								n	user	
3:										n	user	
4:										n	user	
5:										n	user	
6:										n	user	
BCC VALUE TSC CA-TSC										ITC	BCIE	Service/Feature
0 1 2 M 4 W Request										PARM	Sub	Numbering
										Dgts	Format	LAR
1:	y	y	y	y	y	n	n	unre		next		
2:	y	y	y	y	y	n	n	unre		next		
3:	y	y	y	y	y	n	n	rest		none		
4:	y	y	y	y	y	n	n	rest		none		
5:	y	y	y	y	y	n	n	rest		none		
6:	y	y	y	y	y	n	n	rest		none		

5.6. AAR Analysis

Routing to the SIP phones is done using aar, where aar stands for Automatic Alternate Routing and is the digit analysis algorithm commonly used for private network calls. Making changes to the aar analysis table as shown below for numbers beginning with 6 allows the user to decide what route pattern will be used for dialling numbers beginning with 6.

change aar analysis 6										Page	1 of	2
AAR DIGIT ANALYSIS TABLE												
Location: all												
Percent Full: 1												
Dialed		Total		Route	Call	Node	ANI					
String		Min	Max	Pattern	Type	Num	Reqd					
6		4	4	61	unku		n					
6666		4	4	1	aar		n					
7		4	4	1	pubu		n					
8		7	7	999	aar		n					
9		7	7	999	aar		n					
							n					
							n					
							n					

5.7. Configure Network Region

Use the **change ip-network-region x** (where x is the network region to be configured) command to assign an appropriate domain name to be used by Communication Manager. In the example below **devconnect.local** is used. Note this domain is also configured in **Section 6.1** of these Application Notes.

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

```
change ip-network-region 1                                     Page 2 of 20
                                                              IP NETWORK REGION

RTCP Reporting to Monitor Server Enabled? y

RTCP MONITOR SERVER PARAMETERS
  Use Default Server Parameters? y
```

change ip-network-region 1

Page 3 of 20

IP NETWORK REGION

INTER-GATEWAY ALTERNATE ROUTING / DIAL PLAN TRANSPARENCY

Incoming LDN Extension:

Conversion To Full Public Number - Delete: Insert:

Maximum Number of Trunks to Use for IGAR:

Dial Plan Transparency in Survivable Mode? n

BACKUP SERVERS (IN PRIORITY ORDER)

H.323 SECURITY PROFILES

1 LSP70

1 challenge

2

2

3

3

4

4

5

6

Allow SIP URI Conversion? y

TCP SIGNALING LINK ESTABLISHMENT FOR AVAYA H.323 ENDPOINTS

Near End Establishes TCP Signaling Socket? y

Near End TCP Port Min: 61440

Near End TCP Port Max: 61444

change ip-network-region 1

Page 4 of 20

Source Region: 1

Inter Network Region Connection Management

I

M

G

A

t

dst codec direct WAN-BW-limits Video Intervening

Dyn

A

G

c

rgn set WAN Units Total Norm Prio Shr Regions

CAC

R

L

e

1 1

all

2

3

4

5

6

7

8

9

10

11

12

13

14

15

5.8. Configure IP-Codec

Use the **change ip-codec-set x** (where x is the ip-codec set used) command to designate a codec set compatible with the NEC Handsets, which support both **G.711** and **G.729**. Multiple codecs may be specified in the **IP Codec Set** form in order of preference; the example below includes **G.711A** (a-law), which is supported by NEC.

Note the **Media Encryption** has been set to **1-srtp-aescm128-hmac80**. This is the encryption that is support by NEC and must be set correctly on each side to allow secure RTP (SRTP). In order for SRTP to work properly, **Encrypted SRTCP** needed to be set to **enforce-unenc-srtcp** as shown below.

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.711A	n	2	20			
2: G.729	n	2	20			
3: G.711MU	n	2	20			
4:						
5:						
6:						
7:						
Media Encryption				Encrypted SRTCP: enforce-unenc-srtcp		
1: 1-srtp-aescm128-hmac80						
2:						
3:						
4:						
5:						

change ip-codec-set 1				Page	2 of	2
IP CODEC SET						
Allow Direct-IP Multimedia? y						
Maximum Call Rate for Direct-IP Multimedia:				384:Kbits		
Maximum Call Rate for Priority Direct-IP Multimedia:				384:Kbits		
	Mode	Redundancy	Packet			
			Size (ms)			
FAX	pass-through	0				
Modem	pass-through	0				
TDD/TTY	US	3				
H.323 Clear-channel	y	0				
SIP 64K Data	n	0	20			

6. Configure Avaya Aura® Session Manager

The NEC DECT handsets are added to Session Manager as SIP Users. In order to make changes in Session Manager, a web session to System Manager is opened. Navigate to <http://<System Manager IP Address>/SMGR>, enter the appropriate credentials and click on **Log On** as shown below.

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

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

- First time login with "admin" account
- Expired/Reset passwords

Use the "Change Password" hyperlink on this page to change the password manually, and then login.

Also note that single sign-on between servers in the same security domain is not supported when accessing via IP address.

This system is restricted solely to authorized users for legitimate business purposes only. The actual or attempted unauthorized access, use, or modification of this system is strictly prohibited.

Unauthorized users are subject to company disciplinary procedures and or criminal and civil penalties under state, federal, or other applicable domestic and foreign laws.

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

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

User ID:

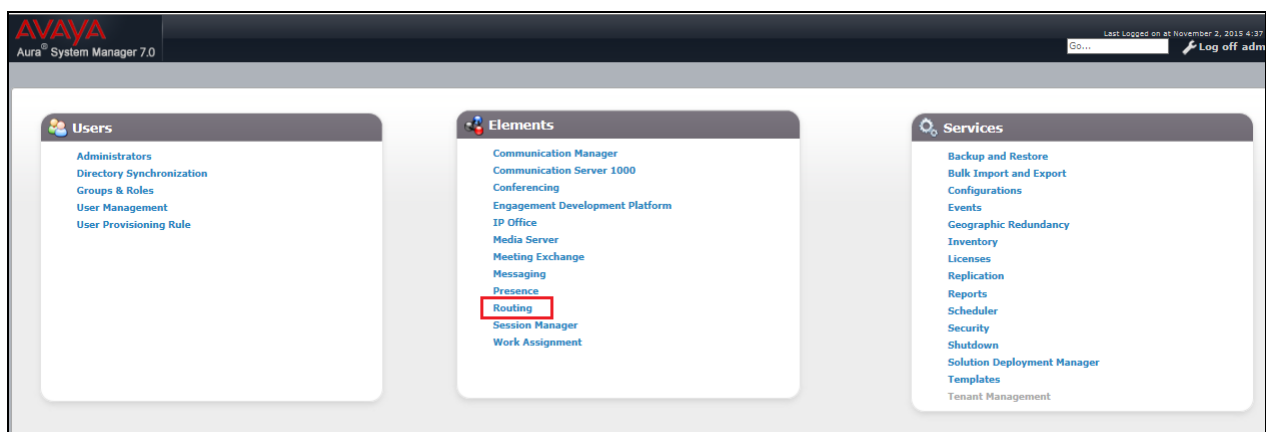
Password:

Log On [Change Password](#)

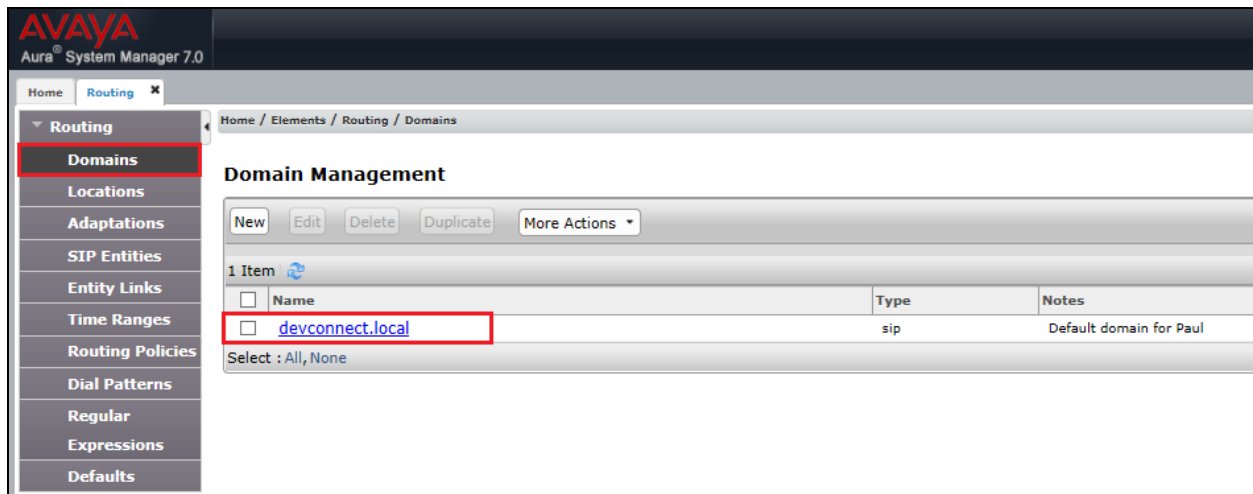
Supported Browsers: Internet Explorer 9.x, 10.x or 11.x or Firefox 36.0, 37.0 and 38.0.

6.1. Configuration of a Domain

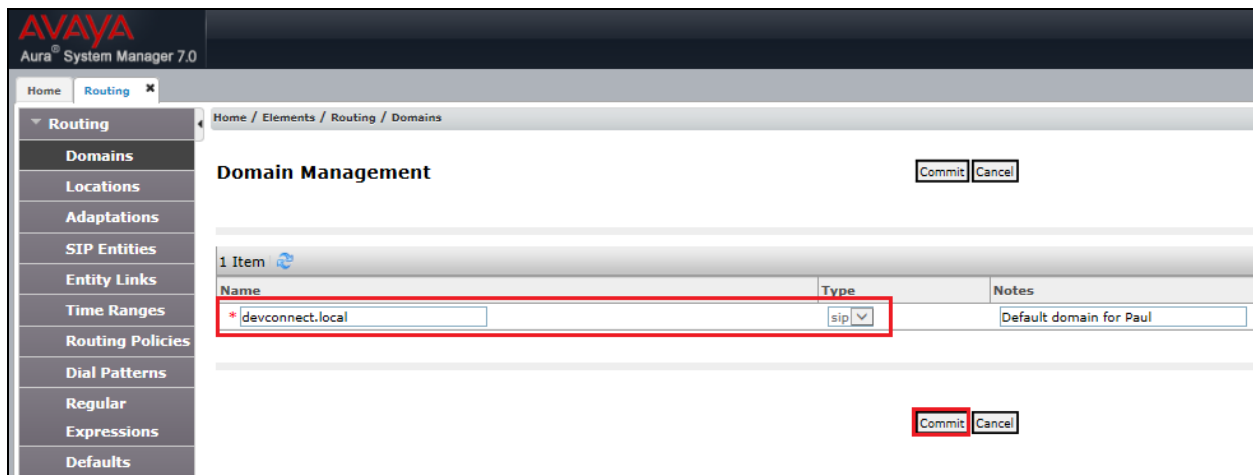
Click on **Routing** highlighted below.



Click on **Domains** in the left window. If there is not a domain already configured click on **New**. In the example below there exists a domain called devconnect.local which has been already configured.

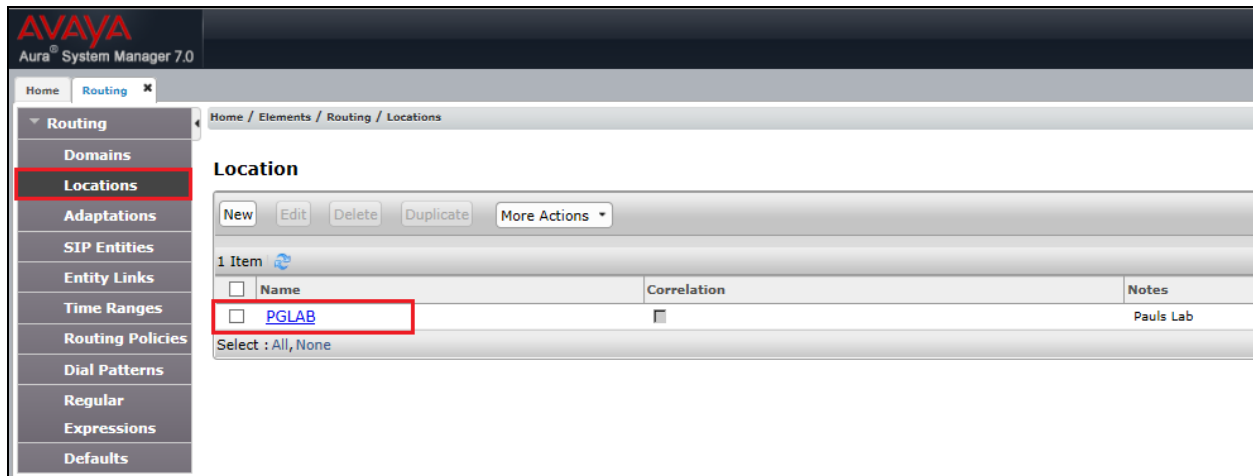


Clicking on the domain name above will open the following window; this is simply to show an example of such a domain. When entering a new domain the following should be entered. Once the domain name is entered click on **Commit** to save this.



6.2. Configuration of a Location

Click on **Locations** in the left window and if there is no Location already configured then click on **New**, however in the screen below a location called **PGLAB** is already setup and configured and clicking into this will show its contents.



The screenshot displays the Avaya Aura System Manager 7.0 interface. The left sidebar contains a navigation menu with the following items: Routing, Domains, **Locations** (highlighted with a red box), Adaptations, SIP Entities, Entity Links, Time Ranges, Routing Policies, Dial Patterns, Regular Expressions, and Defaults. The main content area is titled 'Location' and shows a table with one item, 'PGLAB', which is highlighted with a red box. The table has columns for Name, Correlation, and Notes. The 'PGLAB' entry has a correlation of 'Pauls Lab'. Below the table, there is a 'Select : All, None' option.

Name	Correlation	Notes
PGLAB	Pauls Lab	

The Location below shows a suitable **Name** with a **Location Pattern** of **10.10.40.***. Once this is configured, click on **Commit**.

AVAYA
Aura® System Manager 7.0

Home / Elements / Routing / Locations

Location Details [Commit] [Cancel]

General

* Name: PGLAB
Notes: Pauls Lab

Dial Plan Transparency in Survivable Mode

Enabled: ☐
Listed Directory Number:
Associated CM SIP Entity:

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): 2000 Kbit/Sec
Maximum Multimedia Bandwidth (Inter-Location): 2000 Kbit/Sec
* Minimum Multimedia Bandwidth: 64 Kbit/Sec
* Default Audio Bandwidth: 80 Kbit/sec

Alarm Threshold

Overall Alarm Threshold: 80 %
Multimedia Alarm Threshold: 80 %
* Latency before Overall Alarm Trigger: 5 Minutes
* Latency before Multimedia Alarm Trigger: 5 Minutes

Location Pattern

Add Remove

1 Item

IP Address Pattern	Notes
10.10.40.	Pauls subnet

Select : All, None

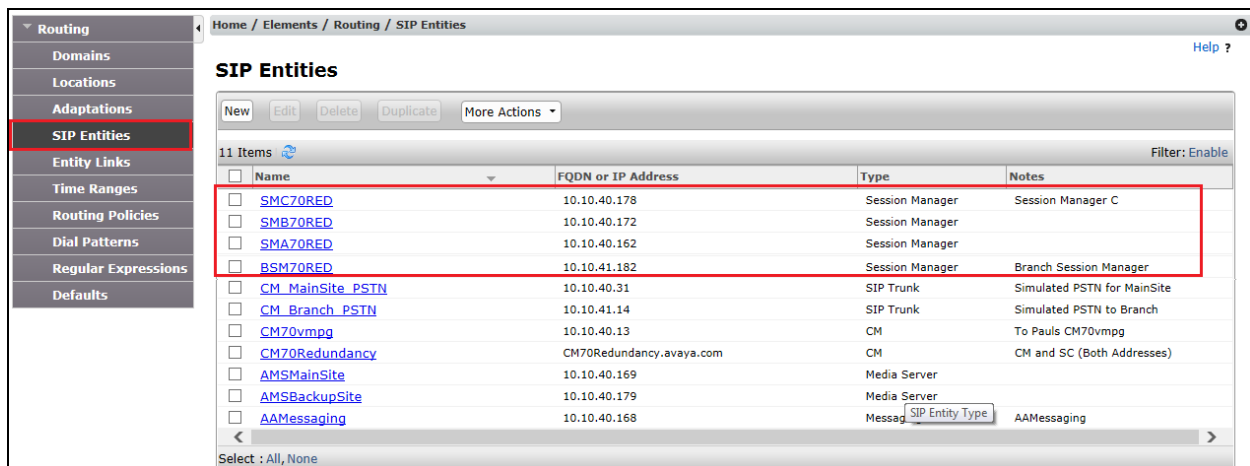
[Commit] [Cancel]

6.3. Configuration of SIP Entities

If needed, a SIP Entity can be created for each DAP controller, these will be added as type “Endpoint Concentrator”. This Endpoint Concentrator type, allows up to 1000 connections from a single IP address. The single IP address can be shared by multiple Windows instances running on a Virtualized server or multiple DECT handsets sharing the same Access Point IP address.

Note: During compliance testing no SIP Entity was created for the NEC DAP. For more information on creating SIP Entities for NEC please refer to the Application Notes titled, *Application Notes for configuring NEC IP DECT Access Points AP400 and NEC DECT Handsets with Avaya Aura® Communication Manager R7.0 and Avaya Aura® Session Manager R7.0 using TLS/SRTP*.

SIP Entities must be created for each SIP server instance including each Session Manager. The screenshot below shows the four Session Manager SIP Entities that were created for compliance testing.



Name	FQDN or IP Address	Type	Notes
SMC70RED	10.10.40.178	Session Manager	Session Manager C
SMB70RED	10.10.40.172	Session Manager	
SMA70RED	10.10.40.162	Session Manager	
BSM70RED	10.10.41.182	Session Manager	Branch Session Manager
CM_MainSite_PSTN	10.10.40.31	SIP Trunk	Simulated PSTN for MainSite
CM_Branch_PSTN	10.10.41.14	SIP Trunk	Simulated PSTN to Branch
CM70vmpg	10.10.40.13	CM	To Pauls CM70vmpg
CM70Redundancy	CM70Redundancy.avaya.com	CM	CM and SC (Both Addresses)
AMSMailSite	10.10.40.169	Media Server	
AMSBackupSite	10.10.40.179	Media Server	
AAMessaging	10.10.40.168	Message SIP Entity Type	AAMessaging

6.4. Configuration on SIP Entity Links

Entity Links must be added between all Core Session Managers. Entity Links between Core Session Managers (SM) and Branch Session Managers (BSM) are optional. For Compliance testing the following Entity Links were added.

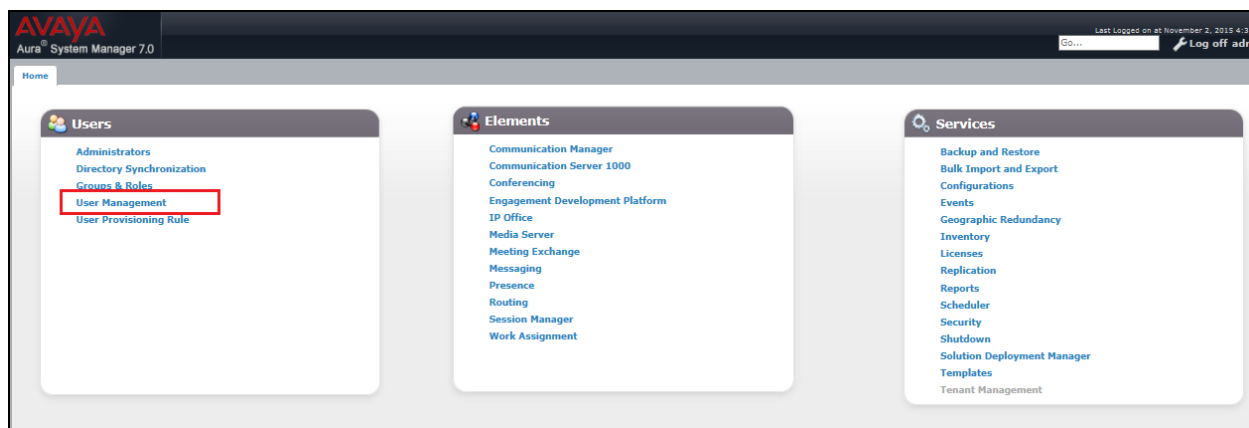
- SM1 ↔ SM2 Entity Link between the core Session Managers.
- SM1 ↔ SM3 Entity Link between the core Session Managers.
- SM2 ↔ SM3 Entity Link between the core Session Managers.
- SM1 ↔ BSM Entity Link between Session Manager 1 and the Branch Session Manager.
- SM2 ↔ BSM Entity Link between Session Manager 2 and the Branch Session Manager.
- SM3 ↔ BSM Entity Link between Session Manager 3 and the Branch Session Manager.

The screen shot below shows the Entity Links used during compliance testing.

Name	SIP Entity 1	Protocol	Port	SIP Entity 2	DNS Override	Port	Connection Policy	Deny New Service	Notes
SMC_SMB	SMC70RED	TLS	5061	SMB70RED	<input type="checkbox"/>	5061	trusted	<input type="checkbox"/>	
SMC_SMA	SMC70RED	TLS	5061	SMA70RED	<input type="checkbox"/>	5061	trusted	<input type="checkbox"/>	
SMC_BSM	SMC70RED	TLS	5061	BSM70RED	<input type="checkbox"/>	5061	trusted	<input type="checkbox"/>	SMC to BSM
SMB_CM(Main)_PSTN	SMB70RED	TLS	5061	CM_MainSite_PSTN	<input type="checkbox"/>	5061	trusted	<input type="checkbox"/>	
SMB_CM70vmpg	SMB70RED	TLS	5061	CM70vmpg	<input type="checkbox"/>	5061	trusted	<input type="checkbox"/>	
SMA_SMB	SMA70RED	TLS	5061	SMB70RED	<input type="checkbox"/>	5061	trusted	<input type="checkbox"/>	SM Core Link
SMA_CM(Main)_PSTN	SMA70RED	TLS	5061	CM_MainSite_PSTN	<input type="checkbox"/>	5061	trusted	<input type="checkbox"/>	
SMA_CM70vmpg	SMA70RED	TLS	5061	CM70vmpg	<input type="checkbox"/>	5061	trusted	<input type="checkbox"/>	
CM_SMB	SMB70RED	TLS	5061	CM70Redundancy	<input type="checkbox"/>	5061	trusted	<input type="checkbox"/>	
CM_SMA	SMA70RED	TLS	5061	CM70Redundancy	<input type="checkbox"/>	5061	trusted	<input type="checkbox"/>	
CM_BSM	BSM70RED	TLS	5061	CM70Redundancy	<input type="checkbox"/>	5061	trusted	<input type="checkbox"/>	
BSM_SMB	BSM70RED	TLS	5061	SMB70RED	<input type="checkbox"/>	5061	trusted	<input type="checkbox"/>	Branch to SMB
BSM_SMA	BSM70RED	TLS	5061	SMA70RED	<input type="checkbox"/>	5061	trusted	<input type="checkbox"/>	Branch to SMA
BMS_CM(Branch)_PSTN	BSM70RED	TLS	5061	CM_Branch_PSTN	<input type="checkbox"/>	5061	trusted	<input type="checkbox"/>	

6.5. Adding NEC SIP Users

From the home page click on **User Management** highlighted below.



Click on **New** (highlighted) to add a new SIP user.

Last Name	First Name	Display Name	Login Name	SIP Handle	Last Login
7100	SIPExt	7100, SIPExt	7100@devconnect.local	7100	
7101	SIPExt	7101, SIPExt	7101@devconnect.local	7101	
admin	admin	Default Administrator	admin		November 3, 2015 11:41:21 AM +00:00

Under the **Identity** tab fill in the user's **Last Name** and **First Name** as shown below. Enter a **Login Name**. The remaining fields can be left as default.

The screenshot shows the 'User Profile Edit' form for user 6610@devconnect.local. The 'Identity' tab is selected and highlighted with a red box. The form contains the following fields:

- User Provisioning Rule:** A dropdown menu.
- Identity:**
 - Last Name:** 6610
 - Last Name (Latin Translation):** 6610
 - First Name:** NEC(Branch)
 - First Name (Latin Translation):** NEC(Branch)
 - Middle Name:** (empty)
 - Description:** (empty)
 - Update Time:** February 28, 2017 3:00
 - Login Name:** 6610@devconnect.local
 - User Type:** Basic
 - [Change Password](#)
 - Source:** local
 - Localized Display Name:** 6610, NEC(Branch)
 - Endpoint Display Name:** 6610, NEC(Branch)
 - Title:** (empty)
 - Language Preference:** English (United Kingdom)
 - Time Zone:** (0:0)GMT : Dublin, Edinburgh, L

Under the **Communication Profile** tab enter a suitable **Communication Profile Password** (which is the login password for the SIP communication) and click on **Done** when added. Note that this password is required when configuring the NEC handset in **Section 7.4**.

The screenshot shows the 'User Profile Edit' form for user 6610@devconnect.local. The 'Communication Profile' tab is selected and highlighted with a red box. The form contains the following fields:

- Communication Profile:**
 - Communication Profile Password:** (masked with dots)
 - Confirm Password:** (masked with dots) [Cancel](#)

Below the main form, there is a sub-form with the following fields:

- New** **Delete** **Done** **Cancel** (buttons)
- Name:** Primary
- Select:** None
- * Name:** Primary
- Default:** ☒

Click on **New** to add a new **Communication Address**. Enter the extension number and the domain for the **Fully Qualified Address** and click on **Add** once finished.

Communication Address

New Edit Delete

Type	Handle	Domain
Avaya SIP	6610	devconnect.local

Select : All, None

Type: Avaya SIP

* Fully Qualified Address: 6610 @ devconnect.local

Add Cancel

Ensure **Session Manager Profile** is checked and enter all the Session Managers where the NEC phone will be registering to, this includes the **Primary Session Manager** details, the **Secondary Session Manager** details and the **Survivability Server** which in this case is the Branch Session Manager. Note: In case of a Session Manager returns a “301 Moved Permanently”, these entries will be included in that message. Enter the **Origination Application Sequence** and the **Termination Application Sequence** and the **Home Location** as shown below.

☒ **Session Manager Profile**

SIP Registration

* Primary Session Manager SMA70RED

Secondary Session Manager SMB70RED

Survivability Server BSM70RED

Max. Simultaneous Devices 1

Block New Registration When Maximum Registrations Active? ☐

Primary	Secondary	Maximum
8	0	8

Primary	Secondary	Maximum
0	8	8

supports 7 Communication Profile(s).

Application Sequences

Origination Sequence CMMainAppSEQ

Termination Sequence CMMainAppSEQ

Call Routing Settings

* Home Location Redundancy Lab

Conference Factory Set (None)

Call History Settings

Enable Centralized Call History? ☐

Ensure that **CM Endpoint Profile** is selected and choose the **9608SIP_DEFAULT_CM_7_0** as the **Template**. Enter the correct voicemail number, the rest of the fields can be left as default or set as shown below. Click on **Endpoint Editor** to configure the buttons and features for that handset on Communication Manager.

☒ **CM Endpoint Profile** ▼

* System

CM70Redundancy ▼

* Profile Type

Endpoint ▼

Use Existing Endpoints

☐

* Extension

6610

Display Extension Ranges

Endpoint Editor

Template

9608SIP_DEFAULT_CM_7_0 ▼

Set Type

9608SIP

Security Code

●●●●●●

Port

S00012

Voice Mail Number

6666

Preferred Handle

(None) ▼

Calculate Route Pattern

☐

Sip Trunk

aar

Enhanced Callr-Info display for 1-line phones

☐

Delete Endpoint on Unassign of Endpoint from User or on Delete User

☒

Override Endpoint Name and Localized Name

☒

Allow H.323 and SIP Endpoint Dual Registration

☐

Click on the **General Options** tab, if voicemail is being used ensure that **Coverage Path 1** (the Coverage Path is configured on Communication Manager to go to Messaging). Also ensure that **Message Lamp Ext.** is showing the correct extension number.

System: CM70Redundancy
 Template: 9608SIP_DEFAULT_CM_7_0
 Port: S00012
 Name: 6610, NEC(Branch)
 Extension: 6610
 Set Type: 9608SIP
 Security Code: *****

General Options (G) * | Feature Options (F) | Site Data (S) | Abbreviated Call Dialing (A) | Enhanced Call Fwd (E) | Button Assignment (B)

Profile Settings (P) | Group Membership (M)

* Class of Restriction (COR): 1
 * Emergency Location Ext: 6610
 * Tenant Number: 1
 * SIP Trunk: Qaar
 Coverage Path 1: 1
 Lock Message: ☐
 Multibyte Language: Not Applicable

* Class Of Service (COS): 1
 * Message Lamp Ext.: 6610
 Type of 3PCC Enabled: None
 Coverage Path 2:
 Localized Display Name: 6610, NEC(Branch)
 Enable Reachability for Station Domain Control: system

*Required

Done Cancel

Under the tab **Feature Options** ensure that **MWI Served User Type** is set to **sip-adjunct**. Ensure the **Voice Mail Number** is set correctly.

General Options (G) * | **Feature Options (F)** | Site Data (S) | Abbreviated Call Dialing (A) | Enhanced Call Fwd (E) | Button Assignment (B)

Profile Settings (P) | Group Membership (M)

Active Station Ringing: single
 MWI Served User Type: sip-adjunct
 Per Station CPN - Send Calling Number: None
 IP Phone Group ID:
 Remote Soft Phone Emergency Calls: as-on-local
 LWC Reception: spe
 AUDIX Name: None
 EC500 State: enabled
 Short/Prefixed Registration Allowed: default
 Music Source:
 Auto Answer: none
 Coverage After Forwarding:
 Display Language: english
 Hunt-to Station:
 Loss Group: 19
 Survivable COR: internal
 Time of Day Lock Table: None
 Location:
 Voice Mail Number: 6666

Features

☐ Always Use
☐ IP Audio Hairpinning
☐ Bridged Call Alerting
☐ Bridged Idle Line Preference
☐ Idle Appearance Preference
☐ IP SoftPhone
☒ LWC Activation
☐ CDR Privacy

Once the **CM Endpoint Profile** is completed correctly, click on **Commit** to save the new user, (not shown).

7. Configure NEC DECT Access Points and Handsets

The following section shows the setup used during compliance testing for the NEC DECT solution. Both the configuration of the DECT Access Points and the addition and subscription of the NEC DECT handsets are clearly outlined. The installation of the NEC DECT solution is outside the scope of these Application Notes for more information on this please refer to **Section 10**.

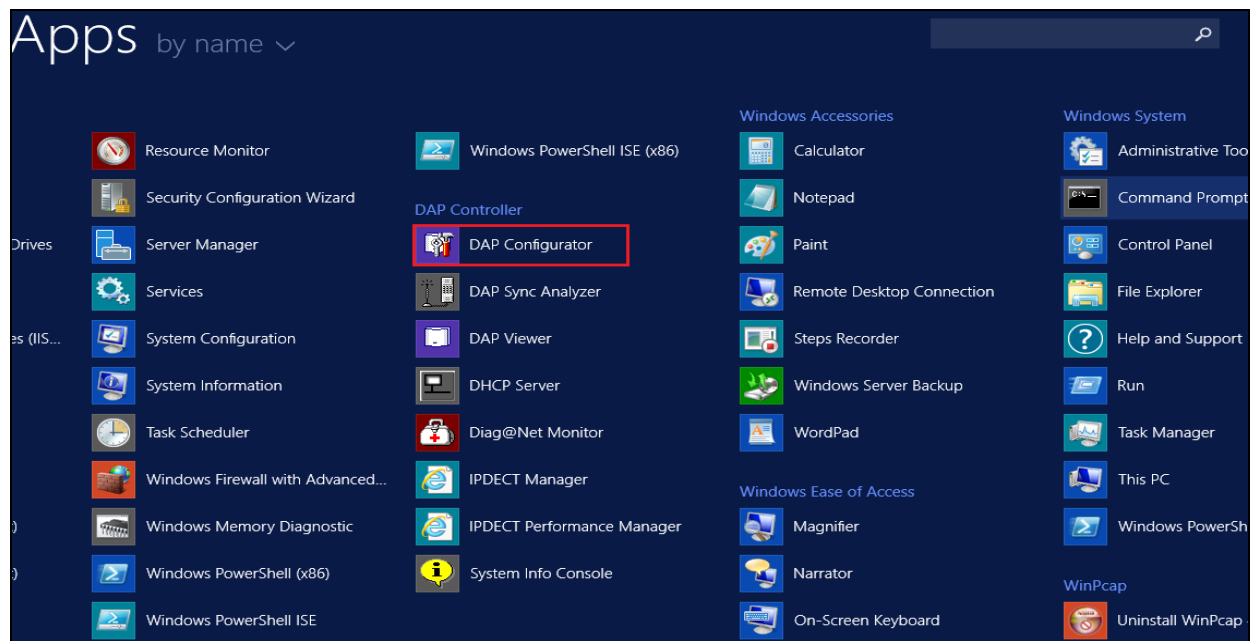
Note: The NEC IP DECT solution relies on DHCP (Option 66, 67), NTP and TFTP as network-services. DHCP and TFTP services can be provided from the DAP controller instance. In addition a Multi-Cast IP address is also required for the DAPs to synch.

7.1. DAP Configurator - Configure DECT Access Point (DAP)

The configuration of the DECT Access Point uses the DAP Configurator which creates a configuration file that is pushed to each DAP on the network. Click on **DAP Configurator** as shown below.

Note: An NEC IP DECT solution typically consists of a windows based instance called DAP Controller which includes “DAP Configurator” and “DAP Manager”.

Note: The DAP Controller Package must be installed in the DAP Controller server. This package is only available from NEC.



Click on the **General Settings** tab and enter the information on the main window. Enter a suitable **System Name** and ensure the **PBX type** is set to **SIP on Avaya-SM**.

Note: Typically a license file is ordered and contains the licenses (number of access points (DAPs) and other features) for the new IP DECT Release 6.41 system. This license file also contains the PARI, which must be unique for each DECT System. When the license file is loaded here the PARI will be filled in automatically.

IP-DECT Configurator R6

General Settings | IP Settings | Network Settings | System Configuration | SIP Settings | DECT Settings | PBX / Provisioning Settings | Performance / Email Settings | Customer Information

Home | New System | Modify System | Import System | Activate / Deactivate / System Status | Export System | Delete System | Upgrade Installation | Save System

General Settings | Avaya DevConnect

System name : Avaya DevConnect

PBX type : SIP on Avaya-SM

AP200/300 package : SIP on SV9100/SV8100/SL1100

AP400 package : SIP on CUCM

AP400 loader : SIP

License : SW updates only allowed with SW that has a SWU date from before 2016-12-31

DAP build date: 2016-02

Exit | Default | Import license file | Apply | Cancel

NEC | Multiple System Mode | Normal Mode | Ready

Ensure the correct AP400 package file from NEC is available on the machine with the DAP configurator. Click on **Browse** for the **AP400 package** and select the proper file (<filename>.dwl). Click on **Apply** at the bottom of the screen.

IP-DECT Configurator R6

General Settings | IP Settings | Network Settings | System Configuration | SIP Settings | DECT Settings | PBX / Provisioning Settings | Performance / Email Settings | Customer Information

Home | New System | Modify System | Import System | Activate / Deactivate / System Status | Export System | Delete System | Upgrade Installation | Save System

General Settings | DevConnect Redundancy Test

System name : DevConnect Redundancy Test | License | SW updates only allowed with SW that has a SWU date from before 2016-12-31

PBX type : SIP on Avaya-Aura

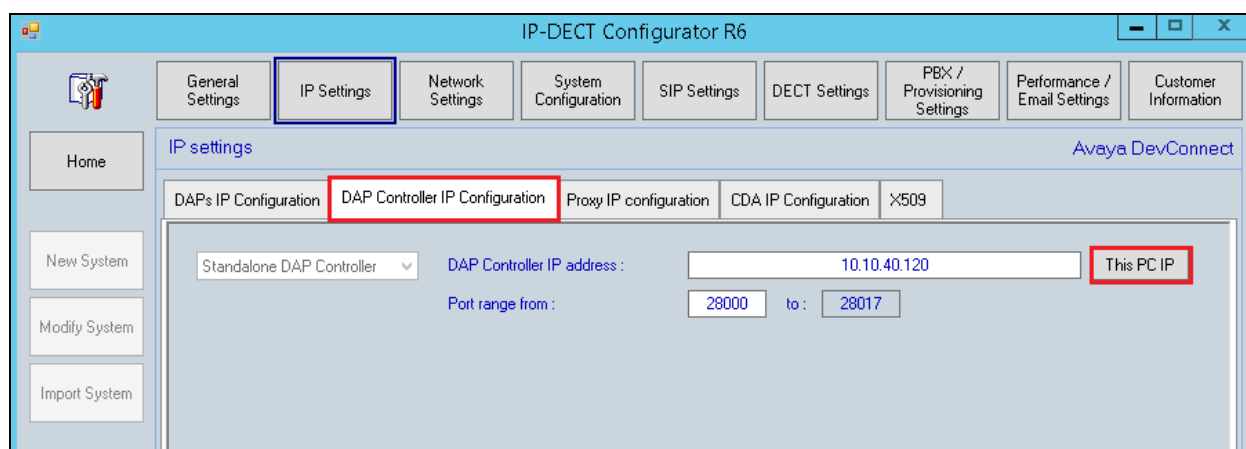
AP200/300 package : | Browse...

AP400 package : 4920b653.dwl | Browse... | DAP build date: 2016-02

AP400 loader : | Browse...

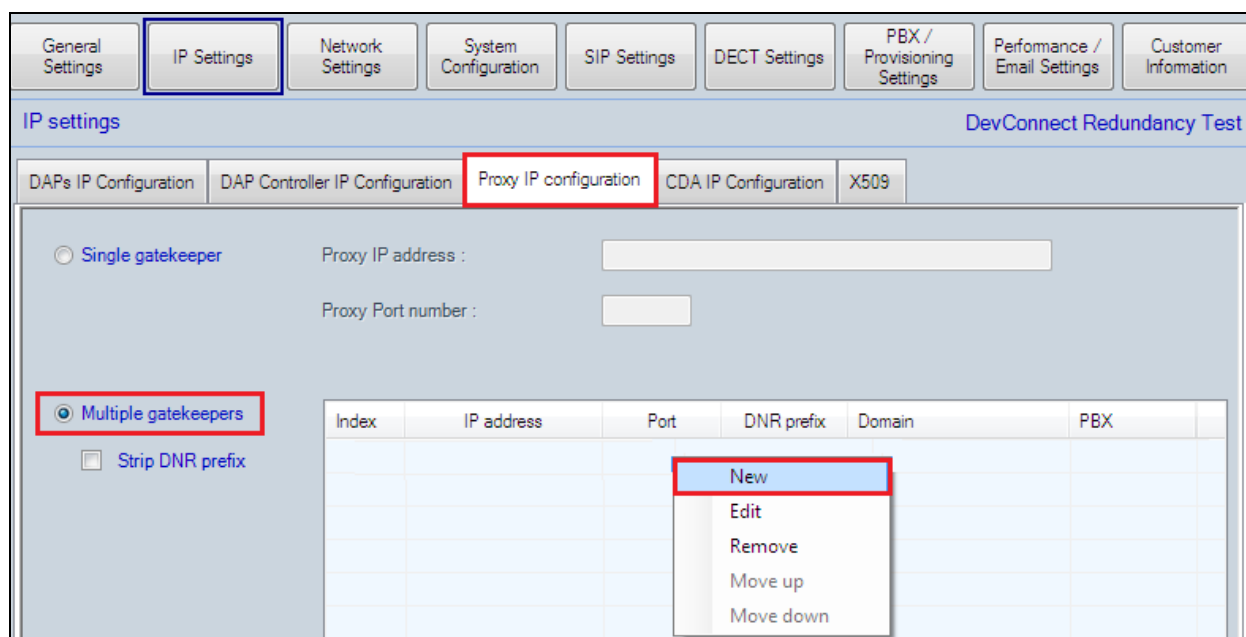
Exit | Default | Import license file | Apply | Cancel

Click on the **IP Settings** tab at the top of the screen and on the **DAP Controller IP Configuration** tab in the main window. Enter the IP address of the DAP Controller server. In this case just pressing **This PC IP** will fill in the required information.



For redundant systems multiple gatekeepers can be selected, click on the **Proxy IP configuration** tab and click on **Multiple gatekeepers** in the main window. Right-click in the main window and click on new.

Note: In the Event the NEC DAP controller will send registration messages to a single Session Manager, click on the Single gatekeeper button below and enter the Session Manager details and the port number. This option may be used if a single Session Manager is being used or a Session Manager for registrations only.



Enter the **Proxy IP address** for each Session Manager (SIP entity address) and the **Proxy port number** as shown below.

The screenshot shows the 'Proxy IP configuration' tab in a software interface. A 'New Gatekeeper entry' dialog box is open, allowing the user to add a new gatekeeper. The dialog box contains the following fields:

- Proxy IP address:** 10.10.40.172
- Proxy Port number:** 5061
- DNR prefix:** (empty)
- Domain:** (empty)

Buttons for 'This PC IP', 'OK', and 'Cancel' are visible. In the background, a table with columns 'Index', 'IP address', 'Port', 'DNR prefix', 'Domain', and 'PBX' is partially visible.

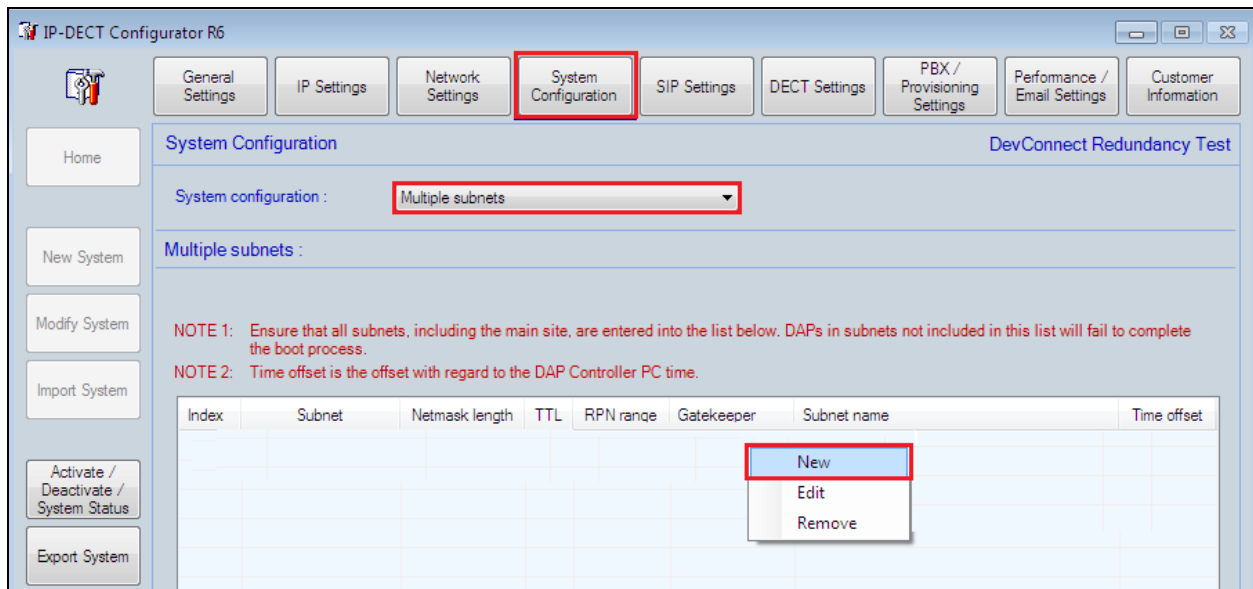
Once the two core Session Managers have been added, click on **Apply**.

The screenshot shows the 'IP settings' window with the 'Proxy IP configuration' tab selected. The 'Multiple gatekeepers' option is selected, and the 'Strip DNR prefix' checkbox is unchecked. A table displays the configured gatekeepers:

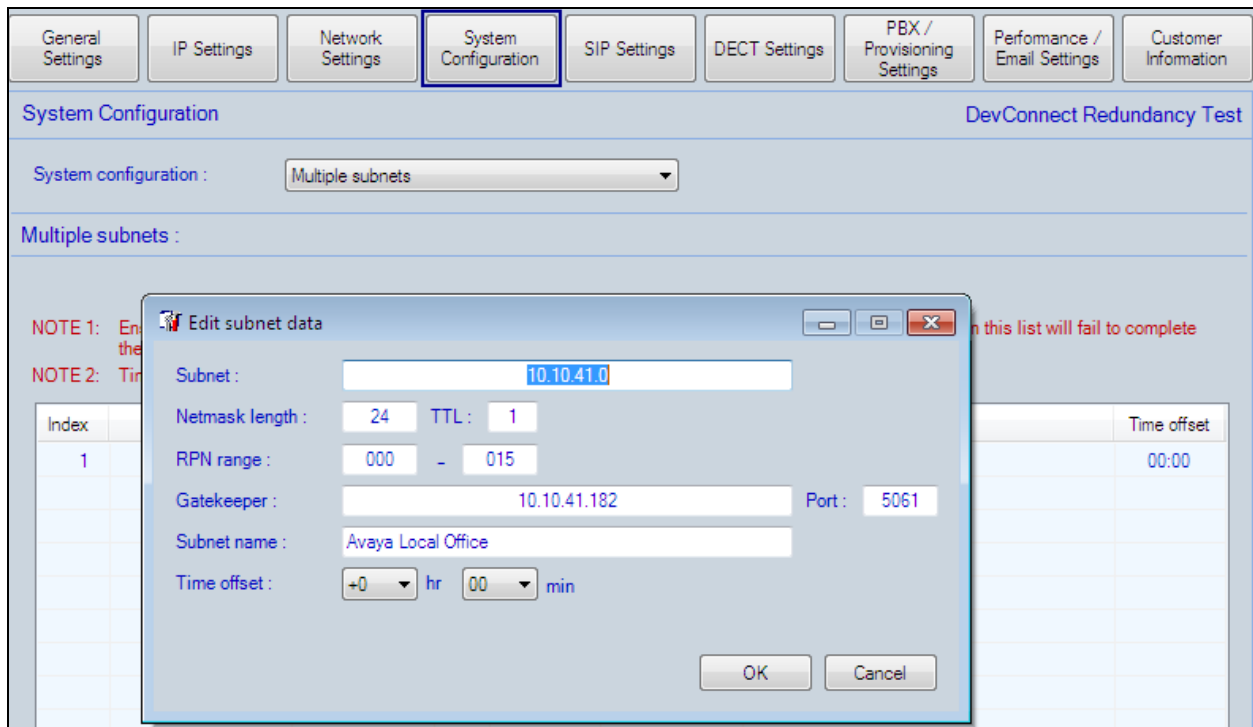
Index	IP address	Port	DNR prefix	Domain	PBX
1	10.10.40.162	5061			
2	10.10.40.172	5061			

At the bottom of the window, there are buttons for 'Default', 'Import license file', 'Apply', and 'Cancel'.

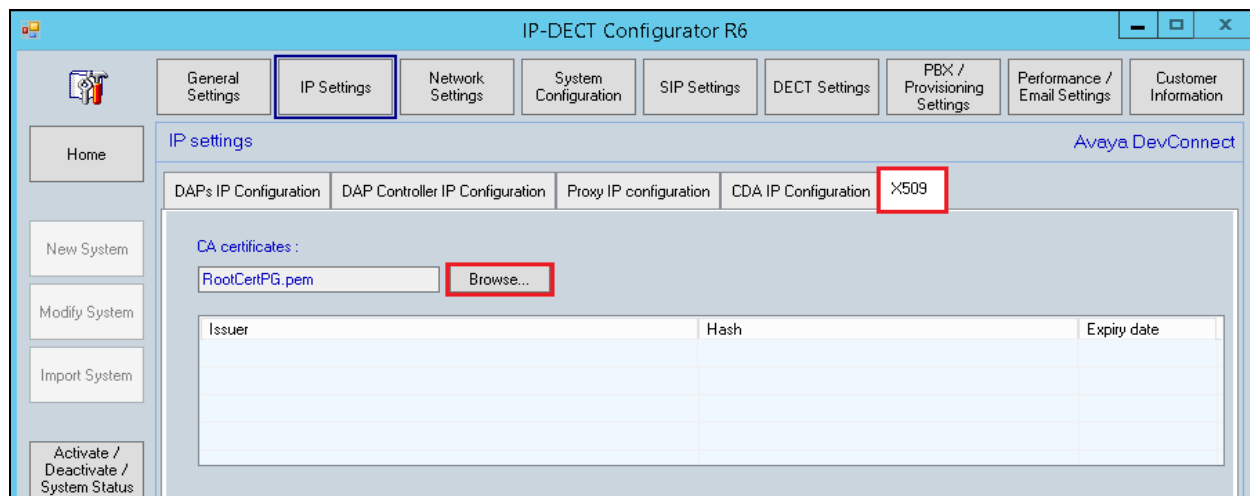
To enter the Branch Session Managers details from a different subnet, click on **System Configuration** from the top menu and select **Multiple subnets** from the drop-down box. In the main window right-click and select **New**.



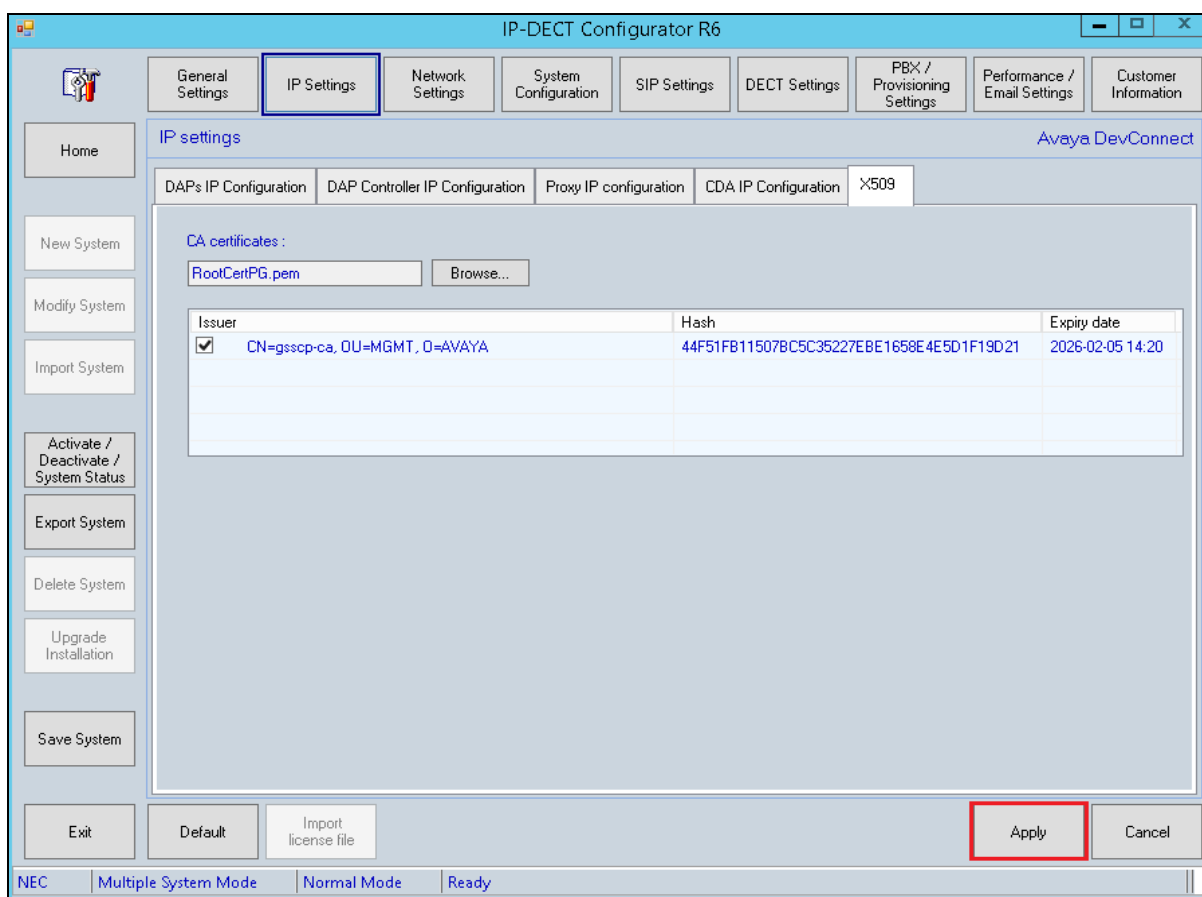
Enter the subnet information and the Branch Session Managers IP address (SIP Entity address) for the **Gatekeeper**. Enter the correct port number and click on **OK**.



To add the Root Cert in order to use TLS and SRTP click on the **IP Settings** button at the top of the screen and click on the **X509** tab and import the Root Cert into the DAP Controller. This will be the same root cert that is being used on Session Manager. The root certificate is being used by the DAP to verify the certificate sent by the Session Manager.



The following shows the imported cert information, click on **Apply** once done.



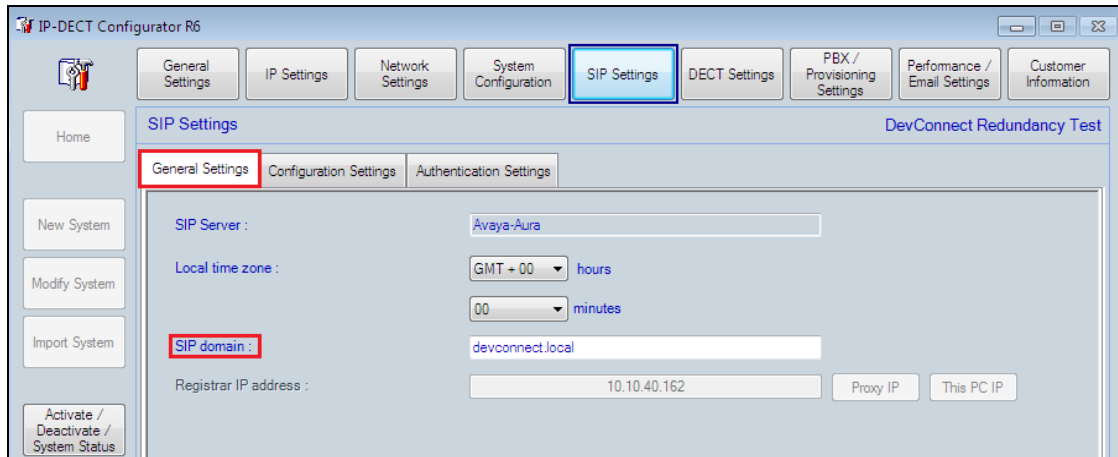
Click on **Network Settings** at the top of the page and within this tab select the **IP Provisioning Settings** tab to check the **TFTP** details. The NEC DAP Controller sever can be setup as a TFTP server which will send any and all details to each DAP using TFTP. This information should be filled in automatically but the screen shot below shows the setup implemented for compliance testing. Once the information here is correctly filled in, click on **Apply** at the bottom of the page to continue.

The screenshot displays the IP-DECT Configurator R6 application window. The 'Network Settings' tab is selected at the top, and within it, the 'IP Provisioning Settings' sub-tab is active. The interface includes a left-hand menu with options like 'Home', 'New System', 'Modify System', 'Import System', 'Activate / Deactivate / System Status', 'Export System', 'Delete System', 'Upgrade Installation', and 'Save System'. The main configuration area shows the following settings:

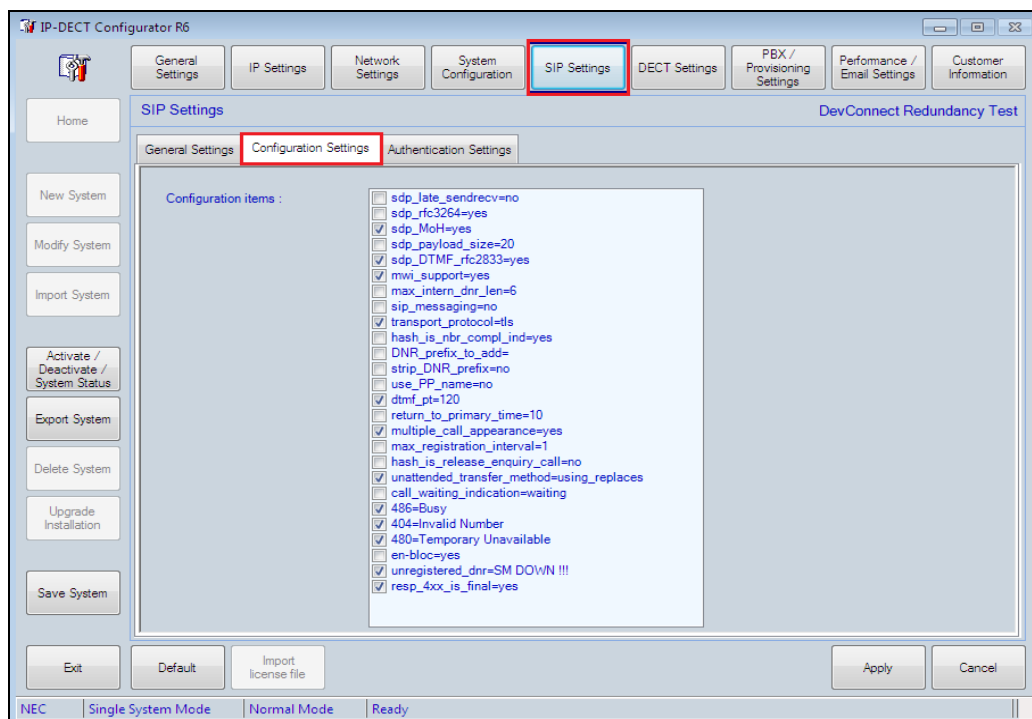
- Provisioning protocol :** TFTP (selected from a dropdown)
- Provisioning folder :** C:\ProgramData\NEC\DAP Controller\Avaya DevConnect\ (with a 'Browse...' button)
- TFTP Server :** 3Com TFTP Server on this PC (selected from a dropdown)
- TFTP Server IP address :** (empty text field)
- ☒ **Monitor TFTP Server**

At the bottom of the window, there are buttons for 'Exit', 'Default', 'Import license file', 'Apply' (highlighted with a red box), and 'Cancel'. The status bar at the very bottom indicates 'NEC | Multiple System Mode | Normal Mode | Ready'.

Click on **SIP Settings** at the top of the page and the **General Settings** tab in the main window. The SIP Server details will be automatically filled in. Set the time zone and the **SIP domain**, note this is the same SIP domain featured in **Section 6.1**. Note the **Registrar IP address**; is greyed out as this was completed earlier in this section.



Click on **Configuration Settings** tab, due to the choice of the PBX type (SIP on Avaya SM) the corresponding SIP settings are automatically set for that PBX type the screen shot below shows the settings used during compliance testing. The **transport_protocol** shows that **TLS** is being used and the **mw_i_support=yes**, with the **DTMF_pt** set to **120** (needs to match the setting “Telephony Event Payload type” on CM trunk group form on page 4). All other values shown were set for standard compliance testing.



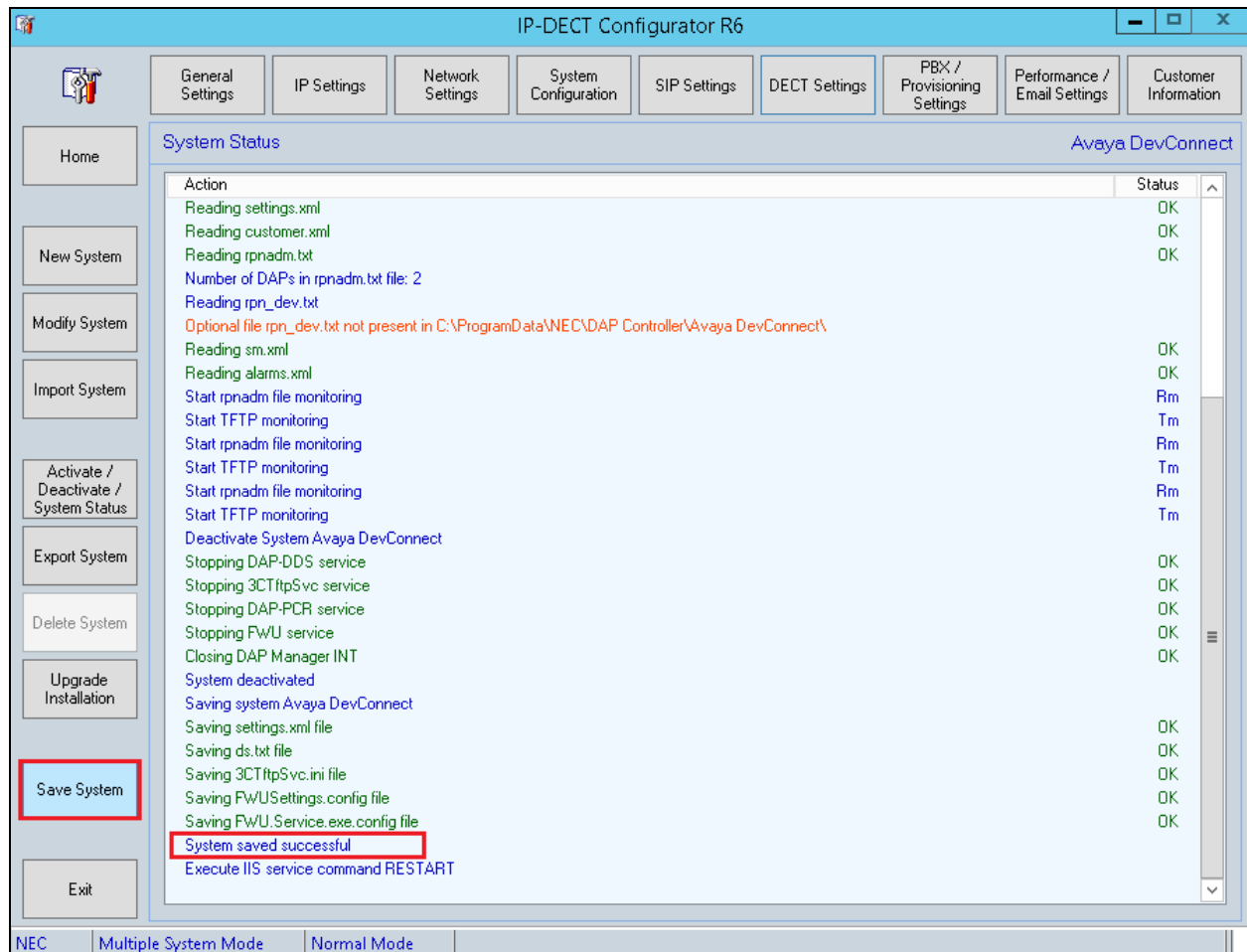
Click on **Authentication Settings** tab and enter **%s** as the user (means the DNR will be used as the SIP extension) and **1234** as the password, note that this is the same password set in **Section 6.5**.

The screenshot displays the 'IP-DECT Configurator R6' application window. The top menu bar includes 'General Settings', 'IP Settings', 'Network Settings', 'System Configuration', 'SIP Settings' (highlighted with a blue border), 'DECT Settings', 'PBX / Provisioning Settings', 'Performance / Email Settings', and 'Customer Information'. The left sidebar contains buttons for 'Home', 'New System', 'Modify System', 'Import System', 'Activate / Deactivate / System Status', 'Export System', 'Delete System', 'Upgrade Installation', and 'Save System'. The main area is titled 'SIP Settings' and contains three sub-tabs: 'General Settings', 'Configuration Settings', and 'Authentication Settings' (highlighted with a red border). The 'Authentication Settings' tab shows five rows for 'Authentication Realm 1' through 'Authentication Realm 5'. Each row has a 'User' field and a 'Pswd' field. In the first row, the 'User' field contains '%s' and the 'Pswd' field contains '1234', both highlighted with red borders. Each row also has a 'Remove' button. At the bottom of the window, there are buttons for 'Exit', 'Default', 'Import license file', 'License valid', 'Apply' (highlighted with a red border), and 'Cancel'. The status bar at the very bottom shows 'NEC', 'Multiple System Mode', 'Normal Mode', and 'Ready'.

Click on **DECT Settings** at the top of the page and the **DECT Settings** tab in the main window. The **PARI** should be already filled in from the information provided by the license file. The **Country code** can be changed to suite and click on **Apply** once this information has been entered as the other tabs do not need to be changed.

The screenshot displays the IP-DECT Configurator R6 application window. The title bar reads "IP-DECT Configurator R6". The top menu bar includes tabs for General Settings, IP Settings, Network Settings, System Configuration, SIP Settings, DECT Settings (highlighted with a blue border), PBX / Provisioning Settings, Performance / Email Settings, and Customer Information. On the left side, there is a vertical toolbar with buttons for Home, New System, Modify System, Import System, Activate / Deactivate / System Status, Export System, Delete System, Upgrade Installation, and Save System. The main content area is titled "DECT Settings" and contains sub-tabs for DECT Settings (highlighted with a red border), Handset Settings, and DAP Settings. The DECT Settings sub-tab is active, showing the following fields: "Country code:" with a dropdown menu set to "Ireland"; "PARI:" with a text box containing "100F073C" (highlighted with a red border); "SARI:" with a text box containing "FFFFFFF"; "Frequency table:" with a text box containing "0"; and "Used carriers:" with a list of checkboxes for Carrier 0 through Carrier 9, all of which are checked. At the bottom of the window, there are buttons for Exit, Default, Import license file, Apply (highlighted with a red border), and Cancel. The status bar at the very bottom shows "NEC", "Multiple System Mode", "Normal Mode", and "Ready".

Once **Save System** has been pressed at the bottom right of the screen the following will be displayed showing that the system has **saved successfully**.



Clicking on **Activate/Deactivate System Status** on the left side of the screen will bring a page on which a restart can be done by clicking the start icon (> button). The DAPs remain fully operational and making and receiving calls is still possible. The DAP controller is only necessary for Management actions regarding the handsets. Clicking on the start icon highlighted in the main screen will restart the system again after Activate/Deactivate System Status has been pressed.

IP-DECT Configurator R6

General Settings | IP Settings | Network Settings | System Configuration | SIP Settings | DECT Settings | PBX / Provisioning Settings | Performance / Email Settings | Customer Information

Home | New System | Modify System | Import System | **Activate / Deactivate / System Status** | Export System | Delete System | Upgrade Installation | Save System | Exit

System Status Avaya DevConnect

Activate	Name	Status	Action
<input checked="" type="checkbox"/>	DDS	Service stopped	Start
<input checked="" type="checkbox"/>	PCR	Service stopped	Start
<input checked="" type="checkbox"/>	FWU	Service stopped	Start
<input checked="" type="checkbox"/>	TFTP Server	Service stopped	Start
<input checked="" type="checkbox"/>	DAP Manager INT	Program not running	Start
<input type="checkbox"/>	DHCP Server	Provided by network	Start
<input type="checkbox"/>	DiagMonitor	Program running (5.0.2.168)	Stop

Required network card settings :

IP : 10.10.40.120
 DG : 10.10.40.1
 SN : 255.255.255.0

Change network | Network Connections

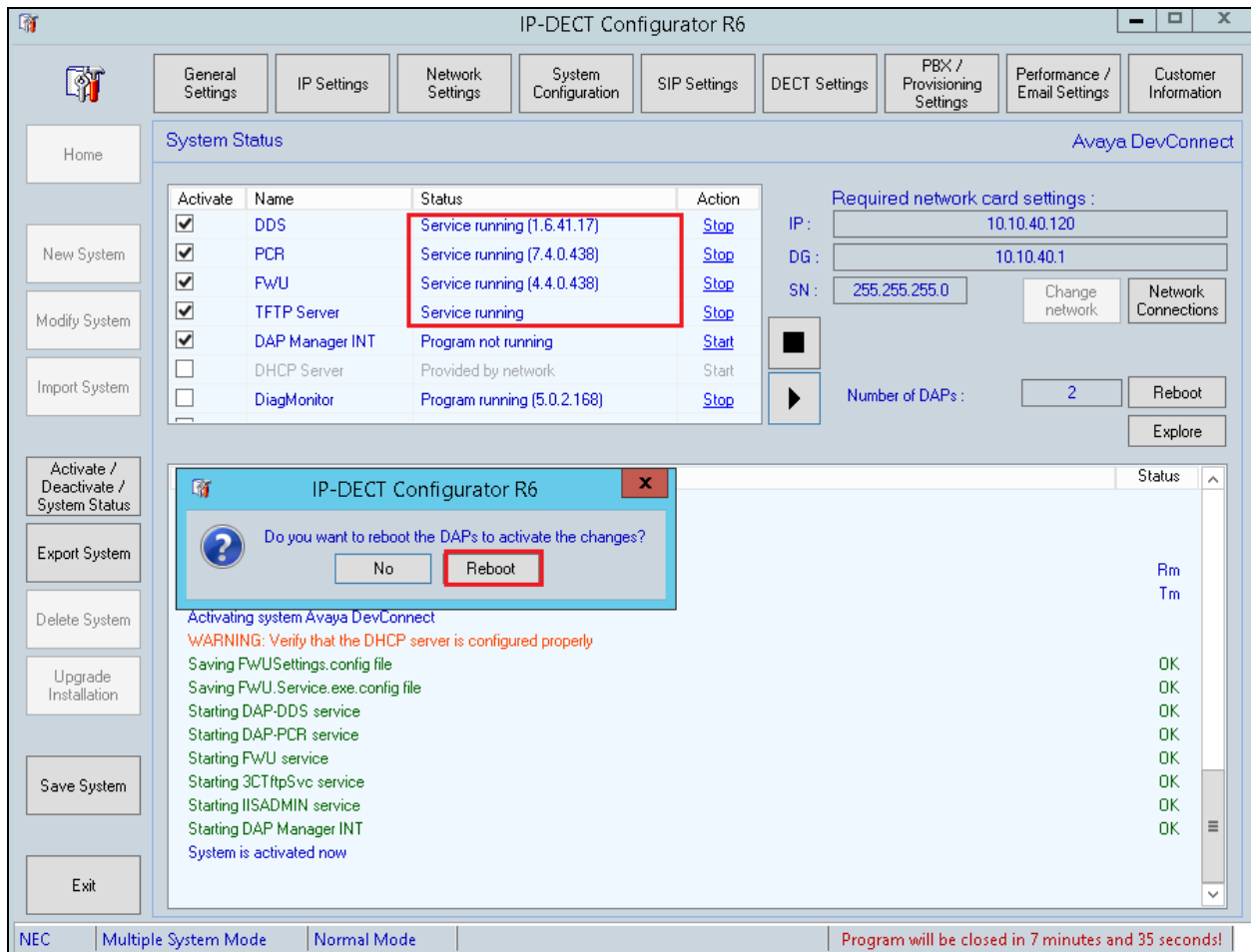
Number of DAPs : 2 | Reboot | Explore

Action | **Status**

- Stopping FWU service OK
- Closing DAP Manager INT OK
- System deactivated
- Saving system Avaya DevConnect
- Saving settings.xml file OK
- Saving ds.txt file OK
- Saving 3CTftpSvc.ini file OK
- Saving FWUSettings.config file OK
- Saving FWU.Service.exe.config file OK
- System saved successful
- Execute IIS service command RESTART OK
- Attempting stop...
- Internet services successfully stopped
- Attempting start...
- Internet services successfully restarted
- Start rpnadm file monitoring Rm
- Start TFTP monitoring Tm

NEC | Multiple System Mode | Normal Mode | Program will be closed in 8 minutes and 40 seconds!

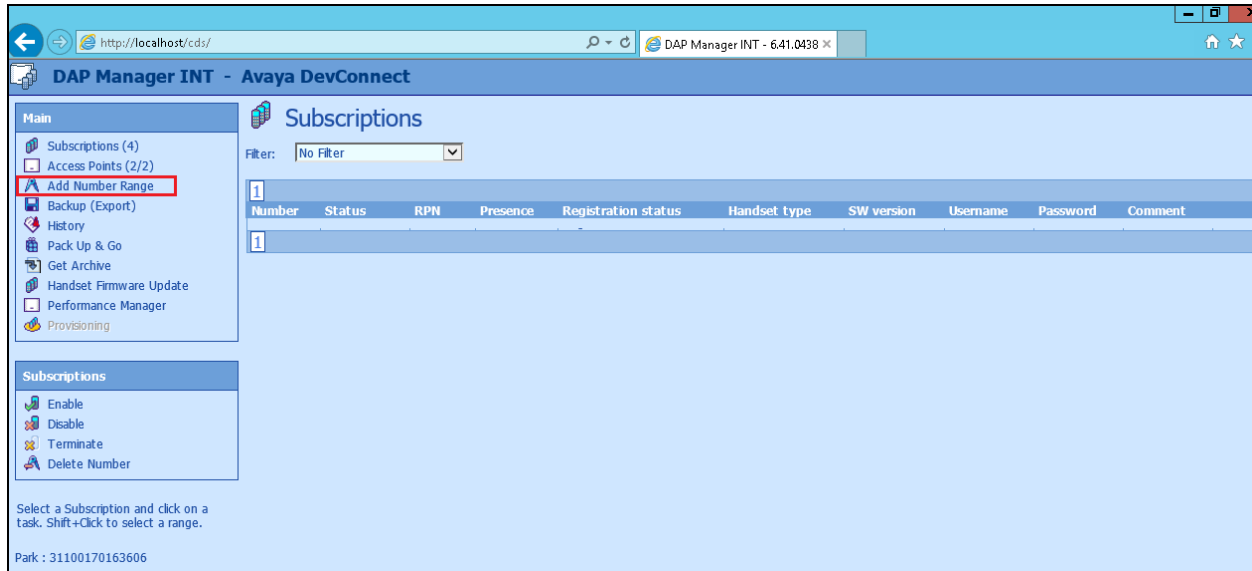
With the system up and running again a window should automatically appear asking to reboot the DAP's. Click on **Reboot** to complete the setup.



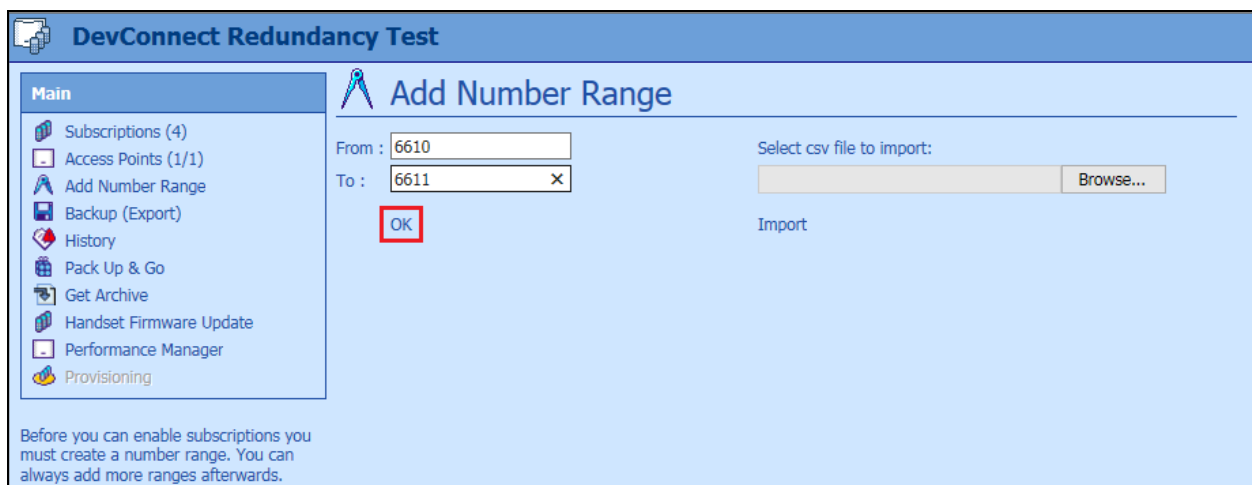
7.2. DAP Manager – Managing DECT users and handsets

Once the DAP configurator has been fully configured, the following window of the DAP manager is automatically popped. The DAP manager can also be reached by typing the following URL <http://<IP-of-DAP-manager>/cds/>. The DAP manager is used to manage the extensions (DNR) on the DECT system and also to subscribe the DECT handsets.

Click on **Add Number Range** in the left window.



Enter the number range or the number of the extension(s) to be added and click on **OK**.



Highlight the new extension added in the main window and click on **Enable** in the left window.

DAP Manager INT - Avaya DevConnect

Main

- Subscriptions (3)
- Access Points (2/2)
- Add Number Range
- Backup (Export)
- History
- Pack Up & Go
- Get Archive
- Handset Firmware Update
- Performance Manager
- Provisioning

Subscriptions

- Enable**
- Disable
- Terminate
- Delete Number

1 Subscription Selected

Park : 31100170163606

Subscriptions

Filter: No Filter

Number	Status	RPN	Presence	Registration status	Handset type	SW version
6110	Subscribed	010	Present	Registered	G566	1.10.00.01
6111	Free					
6610	Subscribed	011	Present	Registered	G566	1.10.00.01
6611	Subscribed	011	Present	Registered	I766	1.10.00.02

Note the **PIN** number which will be used to subscribe the handset in the next section.

DAP Manager INT - Avaya DevConnect

Main

- Subscriptions (4)
- Access Points (2/2)
- Add Number Range
- Backup (Export)
- History
- Pack Up & Go
- Get Archive
- Handset Firmware Update
- Performance Manager
- Provisioning

Subscriptions

Filter: No Filter

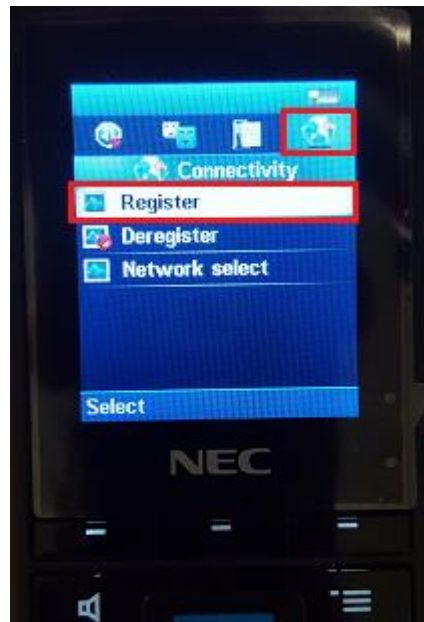
Number	Status	PIN	RPN	Presence
6110	Subscribed		010	Present
6611	Subscribed		011	Absent
6610	Subscribed		011	Absent
6111	Enabled	2475		

7.3. How to Subscribe the DECT Handset

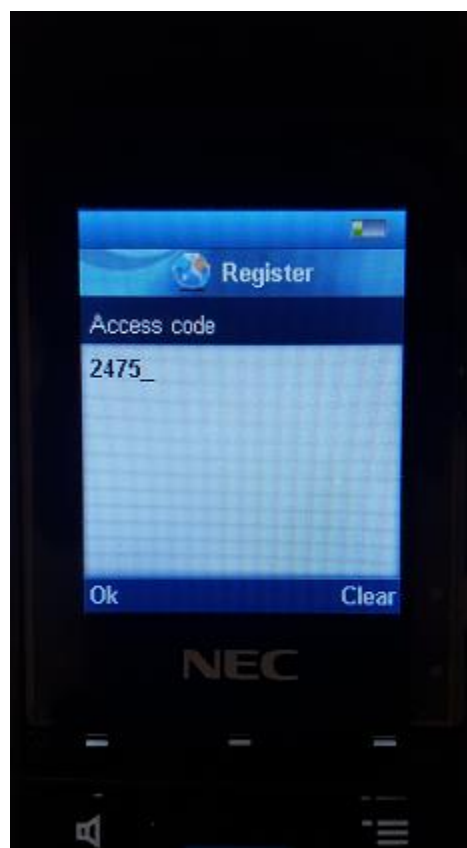
From the DECT handset click on the menu button (on top of the power button) and select **Settings** as highlighted below.



Scroll right to **Connectivity** and select **Register** as shown below.



There will be a number of slots labelled **Empty** (not shown) choose one and continue pressing Ok until the Access Code is asked for. Enter the **Access code** as per **Section 7.2**.



Once this is all entered the phoneset display should show **Registering**, as shown below.

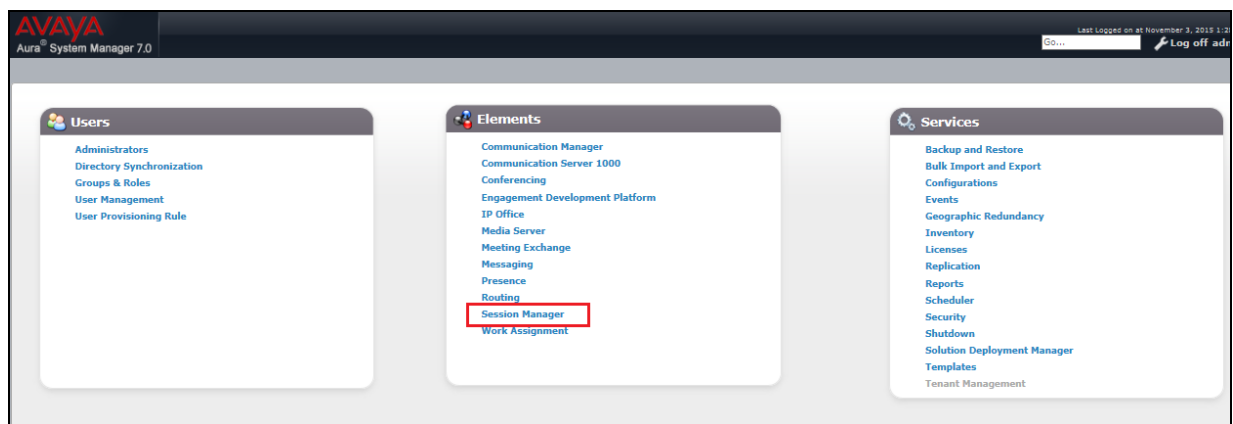


8. Verification Steps

In order to validate that each NEC phone has been registered correctly to each Session Manager, this can be checked on System Manager under **Session Manager → User Registrations** and this is shown in **Section 8.1**. Making calls to and from the NEC phones while observing a Wireshark trace will provide enough information to verify that the NEC phones are registered correctly and are working as expected.

8.1. Session Manager Registration

Log into System Manager as done previously in **Section 6.1**, select **Session Manager** as highlighted below.



Under **System Status** in the left window, select **User Registrations** (not shown) to display all the SIP users that are currently registered with Session Manager. The NEC DECT users should show as being registered as highlighted. Note that each NEC user is registered with all three Session Managers, this is with the two core Session Managers and the Branch Session Manager.

User Registrations

Select rows to send notifications to devices. Click on Details column for complete registration status.

View

Default

Force Unregister

AST Device Notifications:

Reboot

Reload

Fallback

As of 10:57 AM

Customize

Advanced Search

8 Items

Show

All

Filter: Enable

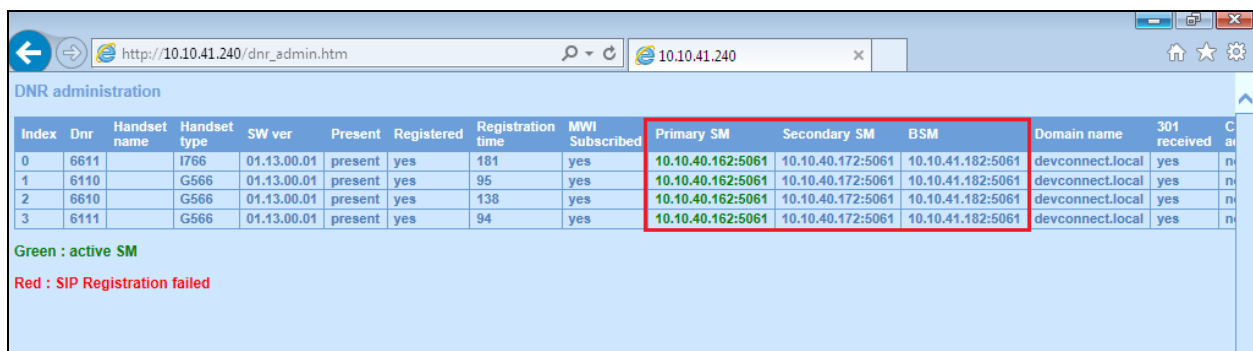
	Details	Address	First Name	Last Name	Actual Location	IP Address	Remote Office	Shared Control	Simult. Devices	AST Device	Registered		
											Prim	Sec	Surv
<input type="checkbox"/>	▶ Show	6611@devconnect.local	NEC (Branch)	6611	Redundancy Lab	10.10.41.240	<input type="checkbox"/>	<input type="checkbox"/>	1/3	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/> (AC)
<input type="checkbox"/>	▶ Show	6610@devconnect.local	NEC (Branch)	6610	Redundancy Lab	10.10.41.240	<input type="checkbox"/>	<input type="checkbox"/>	1/2	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/> (AC)
<input type="checkbox"/>	▶ Show	6110@devconnect.local	NEC(Main)	6110	Redundancy Lab	10.10.41.240	<input type="checkbox"/>	<input type="checkbox"/>	1/2	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/> (AC)
<input type="checkbox"/>	▶ Show	6111@devconnect.local	NEC(Main)	6111	Redundancy Lab	10.10.41.240	<input type="checkbox"/>	<input type="checkbox"/>	1/2	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/> (AC)
<input type="checkbox"/>	▶ Show	6600@devconnect.local	SIP(Branch)	6600	Redundancy Lab	10.10.41.202	<input type="checkbox"/>	<input type="checkbox"/>	1/3	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/> (AC)	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
<input type="checkbox"/>	▶ Show	6601@devconnect.local	SIP(Branch)	6601	Redundancy Lab	10.10.41.201	<input type="checkbox"/>	<input type="checkbox"/>	1/3	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/> (AC)	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
<input type="checkbox"/>	▶ Show	6101@devconnect.local	SIP(Emma)	6101	Redundancy Lab	10.10.40.202	<input type="checkbox"/>	<input type="checkbox"/>	1/3	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/> (AC)	<input checked="" type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	▶ Show	6100@devconnect.local	SIP(Russell)	6100	Redundancy Lab	10.10.40.220	<input type="checkbox"/>	<input type="checkbox"/>	1/10	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/> (AC)	<input checked="" type="checkbox"/>	<input type="checkbox"/>

Select : All, None

Note: As the NEC endpoints are not AST devices (AST device unchecked), the (AC) flag regarding registration (Registered columns) works different than for Avaya phones (AST devices). The (AC) flag for non AST devices just points to the Session Manager instance to which that endpoint has registered latest. It does NOT point to the current “active” controller. Aura® Core and NEC endpoints will use in hierarchical order (Prim to Surv) as the “active” controller – depending on which registrations are established.

8.2. NEC Registrations on DAP Manager DNR administration

The registrations for the NEC handset to each Session Manager can also be verified from the DAP Manager itself by opening a http session to the DAP controller. This is shown below and the resulting page shows the NEC handsets all registered to three Session Managers, the two core Session Managers and the Branch Session Manager.



Index	Dnr	Handset name	Handset type	SW ver	Present	Registered	Registration time	MWI Subscribed	Primary SM	Secondary SM	BSM	Domain name	301 received	C
0	6611		I766	01.13.00.01	present	yes	181	yes	10.10.40.162:5061	10.10.40.172:5061	10.10.41.182:5061	devconnect.local	yes	n
1	6110		G566	01.13.00.01	present	yes	95	yes	10.10.40.162:5061	10.10.40.172:5061	10.10.41.182:5061	devconnect.local	yes	n
2	6610		G566	01.13.00.01	present	yes	138	yes	10.10.40.162:5061	10.10.40.172:5061	10.10.41.182:5061	devconnect.local	yes	n
3	6111		G566	01.13.00.01	present	yes	94	yes	10.10.40.162:5061	10.10.40.172:5061	10.10.41.182:5061	devconnect.local	yes	n

Green : active SM
Red : SIP Registration failed

9. Conclusion

These Application Notes describe the configuration steps for provisioning NEC's IP DECT Access Point (AP400) and NEC's DECT handsets to interoperate with Avaya Aura® Communication Manager R7.0.1 and Avaya Aura® Session Manager R7.0.1 specifically to show redundancy failover using multiple simultaneous registrations with different Avaya Aura® Session Managers in a main/branch environment. Please refer to **Section 2.1** and **2.2** for test results and observations.

10. Additional References

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

- [1] *Administering Avaya Aura® Communication Manager*, Document ID 03-300509
- [2] *Avaya Aura® Communication Manager Feature Description and Implementation*, Document ID 555-245-205
- [3] *Implementing Avaya Aura® Session Manager* Document ID 03-603473
- [4] *Administering Avaya Aura® Session Manager*, Doc ID 03-603324

NEC's technical documentation is available from NEC or from <http://businessnet.nec-enterprise.com>.

- [5] *NEC, 2016, Business Mobility IP DECT CE Manual for SIP Connectivity, R6.41*, available at <http://businessnet.nec-enterprise.com>
- [6] *NEC, 2016, IP DECT Administrator Guide, R6.41*, available at <http://businessnet.nec-enterprise.com>

11. Appendix

Configuration for the Survivable Core and Local Survivable Processor on Communication Manager

The following is the setup for both the Survivable Core and the Local Survivable Processor that was used during compliance testing.

The setup requires that each component is added under **node-names ip**. Take note of the LSP and the SC as shown below.

change node-names ip		Page 1 of 2
		IP NODE NAMES
Name	IP Address	
AMSBackup	10.10.40.179	
AMSBranch	10.10.41.189	
AMSMain	10.10.40.169	
BSM	10.10.41.182	
CMAvmpg	10.10.40.163	
CMBvmpg	10.10.40.164	
LSP70	10.10.41.185	
SC70Redundancy	10.10.40.175	
SCAvmpg	10.10.40.173	
SCBvmpg	10.10.40.174	
SMA70vmpg	10.10.40.162	
SMB70vmpg	10.10.40.172	
default	0.0.0.0	
procr	10.10.40.165	
(16 of 17 administered node-names were displayed)		
Use 'list node-names' command to see all the administered node-names		
Use 'change node-names ip xxx' to change a node-name 'xxx' or add a node-name		

11.1. Survivable Core

In the setup for this compliance testing a duplex Survivable Core was used so each Server must be added separately as shown below.

```
add survivable-processor SC70Redundancy                               Page 1 of 7
                                SURVIVABLE PROCESSOR

Type: duplex-ess      Cluster ID/MID: 2      Processor Ethernet Network Region: 1
                        Community: 1          Enable PE for H.323 Endpoints? y
ACTIVE SERVER
                        Enable PE for H.248 Gateways? y
V4 Node Name: SC70Redundancy Address: 10.10.40.175
V6 Node Name:           Address:
SERVER A
  Server ID: 3
V4 Node Name: SCAvmpg      Address: 10.10.40.173
V6 Node Name:           Address:
SERVER B
  Server ID: 4
V4 Node Name: SCBvmpg      Address: 10.10.40.174
V6 Node Name:           Address:

PORT NETWORK PARAMETERS
                        Community Size: all      System Preferred: y
                        Priority Score: 1         Local Preferred: n
                                                Local Only: n
```

Page 2 shows the priority of the Survivable Core with respect to the Media Servers.

```
add survivable-processor SC70Redundancy                               Page 2 of 7
                                SURVIVABLE PROCESSOR

MEDIA SERVER PARAMETERS
Priority with respect to Media Servers: 2
```

Page 3 shows the different Media-Servers that were used for compliance testing and the order in which they are prioritized.

```
add survivable-processor SC70Redundancy                               Page 3 of 7
                                MEDIA SERVER REPORTING LIST FOR SC70Redundancy

Num NR  Node Name           Num NR  Node Name           Num NR  Node Name
1   1   AMSMain
2   1   AMSBackup
3   1   AMSBranch
```

11.2. Local Survivable Processor

The LSP is added using the name as per the **node-names ip** at the beginning of **Section 11**.

```
add survivable-processor LSP70                                     Page 1 of 7
                                SURVIVABLE PROCESSOR

Type: lsp                  Cluster ID/MID: 3      Processor Ethernet Network Region: 1

V4 Node Name: LSP70        Address: 10.10.41.185
V6 Node Name:              Address:
```

Page 2 shows the Priority of the LSP with respect to the Media Servers.

```
add survivable-processor LSP70                                     Page 2 of 7
                                SURVIVABLE PROCESSOR

MEDIA SERVER PARAMETERS
Priority with respect to Media Servers: 3
```

Page 3 shows the Media Servers associated with the LSP and logically this will only be the Branch Media Server as this is the only server it will ever need to speak with.

```
add survivable-processor LSP70                                     Page 3 of 7
                                MEDIA SERVER REPORTING LIST FOR LSP70

Num NR  Node Name          Num NR  Node Name          Num NR  Node Name
3   1   AMSBranch
```

11.3. Configure Recovery Rules

In order for Communication Manager to recover from an outage a recovery rule must be setup as shown below. In this case the Communication Manager will try to recover automatically after 2 minutes.

```
change system-parameters ms-recovery-rule                                     Page 1 of 1

                                MEDIA SERVER RECOVERY RULES

FAILOVER PARAMETERS                                FALLBACK PARAMETERS

    Report Interval (sec): 60                        Auto Return: yes
    Report Expiration (sec): 180

                                Time Delay (min): 2
```

©2017 Avaya Inc. All Rights Reserved.

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

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