



Avaya Solution & Interoperability Test Lab

Application notes for eTelemetry Locate911-N Rel. 1.4.9, LENS Appliances/Software Rel. 1.4.5 and Their High Availability Configurations with Avaya™ Communication Server 1000 Emergency 911 Service Rel. 6.0 – Issue 1.0

Abstract

These Application Notes describe a solution comprised of Avaya™ Communication Server 1000 Release 6.0 and the eTelemetry Locate911-N, Locate911-N High Availability solutions, LENS Appliances, LENS Appliances High Availability/Business Continuity Cluster and LENS Software release 1.4.5. During the compliance testing, the eTelemetry Locate911-N was able to operate as an External Discovery Manager (DM) of the Communication Server 1000 Release 6.0. The eTelemetry LENS Alert Agent was also able to operate as a desktop On Site Notification (OSN).

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 provide detail configurations of Avaya Communication Server 1000 Emergency Service rel. 6.0 (hereafter referred to as CS1000) and eTelemetry Locate911-N, Locate911-N High Availability / Business Continuity Cluster release 1.4.9, LENS Appliances, LENS Appliances High Availability/Business Continuity Cluster and LENS Software release 1.4.5 release 1.4.5. During the compatibility testing session, the eTelemetry Locate911-N was tested as an External Discovery Manager of the CS1000 Emergency Service 6.0. The LENS Alert Agent was tested as desktop OSN of the CS1000 Emergency Service 6.0.

1.1. Interoperability Compliance Testing

The focus of this compliant testing is to verify that the Locate911-N and LENS were able to interoperate with our CS1000 Emergency Service. The following interoperability areas were covered:

- External Discovery Manager (DM)
- 911 call desktop alert via SNMP.

1.2. Support

For technical support on eTelemetry Locate911-N and LENS Appliances, please contact eTelemetry technical support at:

- Email: support@etelemetry.com
- Phone: +1(410) 266-6513

2. Reference Configuration

Figure 1a illustrates the test configuration used during the compliance testing event between the Avaya CS1000 and the eTelemetry Locate911-N in stand-alone setup. In this solution, Locate911-N provides E911 essential VoIP location discovery with On-Site Notification when an emergency call is placed.

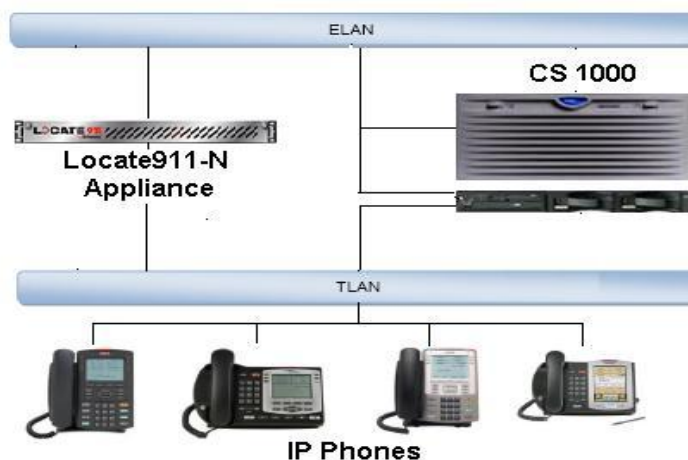


Figure 1a: Locate911-N Test Configuration

Figure 1b illustrates the test configuration used during the compliance testing event between the Avaya CS1000 and the eTelemetry Locate911-N in High-Availability setup. In this solution, Locate911-N provides E911 essential VoIP location discovery with On-Site Notification when an emergency call is placed. The emergency alerts can be sent to an Alert Agent, an email account as well as mobile phone in an SMS. With High-Availability setup, all operational state data (phone info, location info, user configuration data, and alerts) are replicated and a certain degree of operational continuity is ensured.

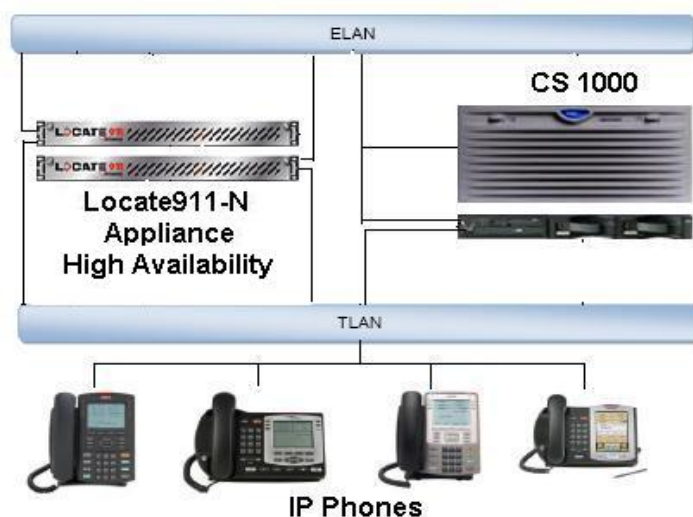


Figure 2b: Locate911-N HA/BCC

Figure 1c illustrates the test configuration used during the compliance testing event between the Avaya CS1000 and the eTelemetry LENS Appliance in stand-alone setup. In this solution, LENS Appliance provides On-Site Notification ability when an emergency call is placed. The emergency alerts can be sent to an Alert Agent, an email account as well as mobile phone in an SMS. This solution is pre-built in an appliance (1U box) and for users requiring only On-site Notification.

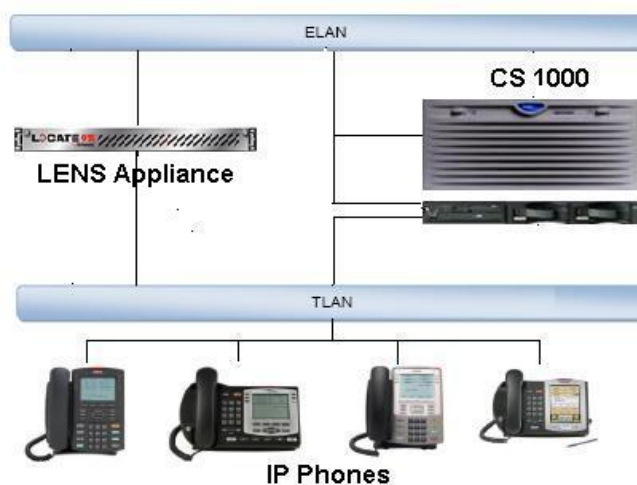


Figure 3c: LENS Appliance

Figure 1d illustrates the test configuration used during the compliance testing event between the Avaya CS1000 and the eTelemetry LENS Appliance in High-Availability setup. In this solution, LENS Appliance provides On-Site Notification ability when an emergency call is placed. The emergency alerts can be sent to an Alert Agent, an email account as well as mobile phone in an SMS. The application is pre-built in an appliance (1U box) and for users requiring only On-site Notification. With High-Availability setup, all the operational state data (user configuration data and alerts) are replicated and a certain degree of operational continuity is ensured.

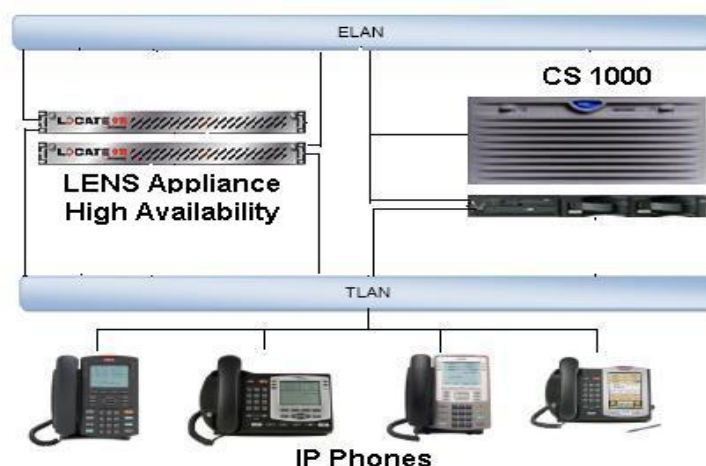


Figure 4d: LENS Appliance HA/BCC

Figure 1e illustrates the test configuration used during the compliance testing event between the Avaya CS1000 and the eTelemetry LENS software based setup. In this solution, LENS server software is manually installed in a Windows based server. The application provides On-Site Notification ability when an emergency call is placed. The emergency alerts can be sent to an Alert Agent, an email account as well as mobile phone in an SMS.

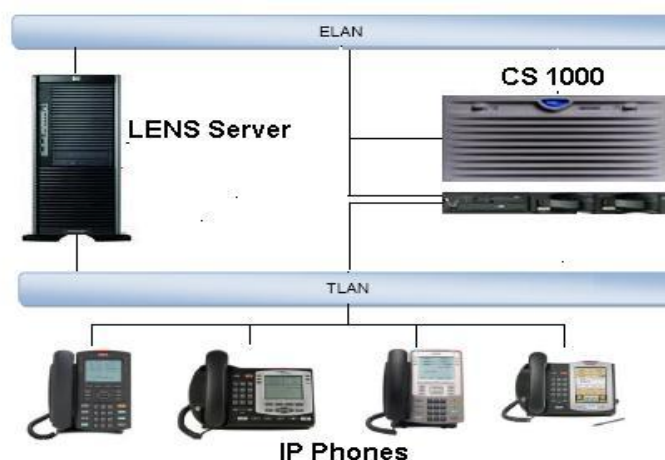


Figure 5e: LENS Software

3. Equipment and Software Validated

System	Software/Loadware Version
CS1000	<ul style="list-style-type: none">• Call Server (CPPM): 6.00RJ• Signaling Server (CPPM): 6.00.18• SIP Line Gateway (HP DL320)
Call Pilot	<ul style="list-style-type: none">• CallPilot (600r): 05.00.41.29
IP phones	<ul style="list-style-type: none">• 1240:• 2007• 2002p2• 1140• 2050PC: 3.02.0045
Locate911-N	<ul style="list-style-type: none">• 1.4.9
LENS	<ul style="list-style-type: none">• 1.4.5

The following packages must be enabled in the keycode file in order for the Emergency Service Access feature to operate successfully.

Feature Packaging Requirement

Package	Mnemonic	Name	Description
329	ESA	Emergency Services Access	Defines an emergency number as being dial-able without a prefix. Recognizes the emergency call and provides special treatment and route to CAMA, PRI or other trunks. Provides flexible ANI number translation for DID numbers and sends out the ANI with the call to enable the PSAP to look up the caller. Includes Enhanced Routing functionality, Multiple ESDNs, and Mis-dial Prevention.
330	ESA_ SUPP	ESA Supplementary	Provides networking support by routing node-to-node ANI info for forwarding to a PSAP. Converts incoming ISDN to CAMA tandem which allows CLID forwarding via out-pulsed CAMA. Also provides On-Site-Notification (OSN) so that customer staffs are aware of the call. This includes OSN phones per ERL.
331	ESA_CLMP	ESA Calling Number Mapping	Provides flexible ANI number translation for non-DID numbers (i.e. to translate non-DID numbers to DID numbers). This includes Dynamic ELIN functionality.

336	ESA_SUBNET_LIS	ESA Subnet LIS	Allows the use of an internal Subnet-Lookup Location Information Service to provide basic location determination for IP phones.
337	ESA_EXTERNAL_DM	ESA External DM Interface	Allows the use of an external Discover Manager (and corresponding LIS) to provide advanced location determination for IP phones. Additionally, the External Discovery Manager is charged separately.

4. Configure the Avaya CS1000 - Emergency Service Access (ESA)

This section describes the steps to configure Emergency Service Access (ESA) on a CS1000 system using Element Manager Web portal. Repeat these steps for other CS1000 systems in the CS1000 network. For more information, see [1].

4.1. Log in to Unified Communications Management (UCM) and Element Manager (EM)

- Using IE to launch CS1000 UCM web portal at <http://<IP Address or FQDN>> where <IP address or FQDN> is the UCM Framework IP address or FQDN for UCM server.
- Login with the username/password which was defined during the primary security server configuration. For more information, see [2].

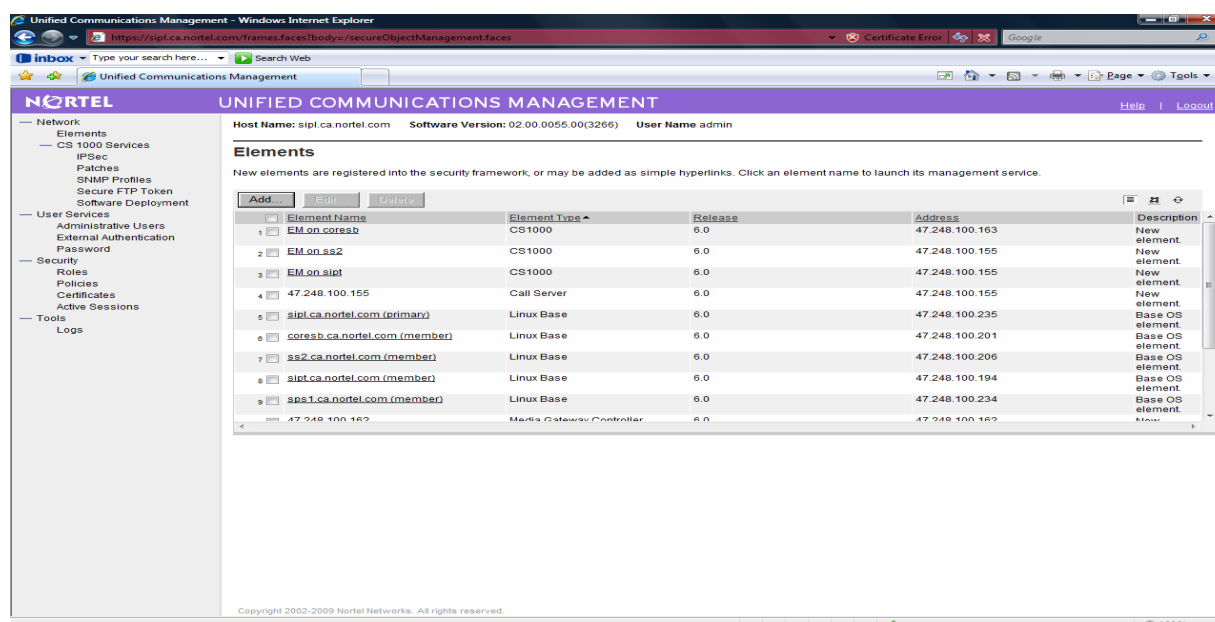


Figure 6: UCM Home Page

- On the **Elements** page of Unified Communications Management, under the **Element Name** column, click the server name to navigate to Element Manager for that server. The CS1000 Element Manager page appears as shown in Figure 3 below.

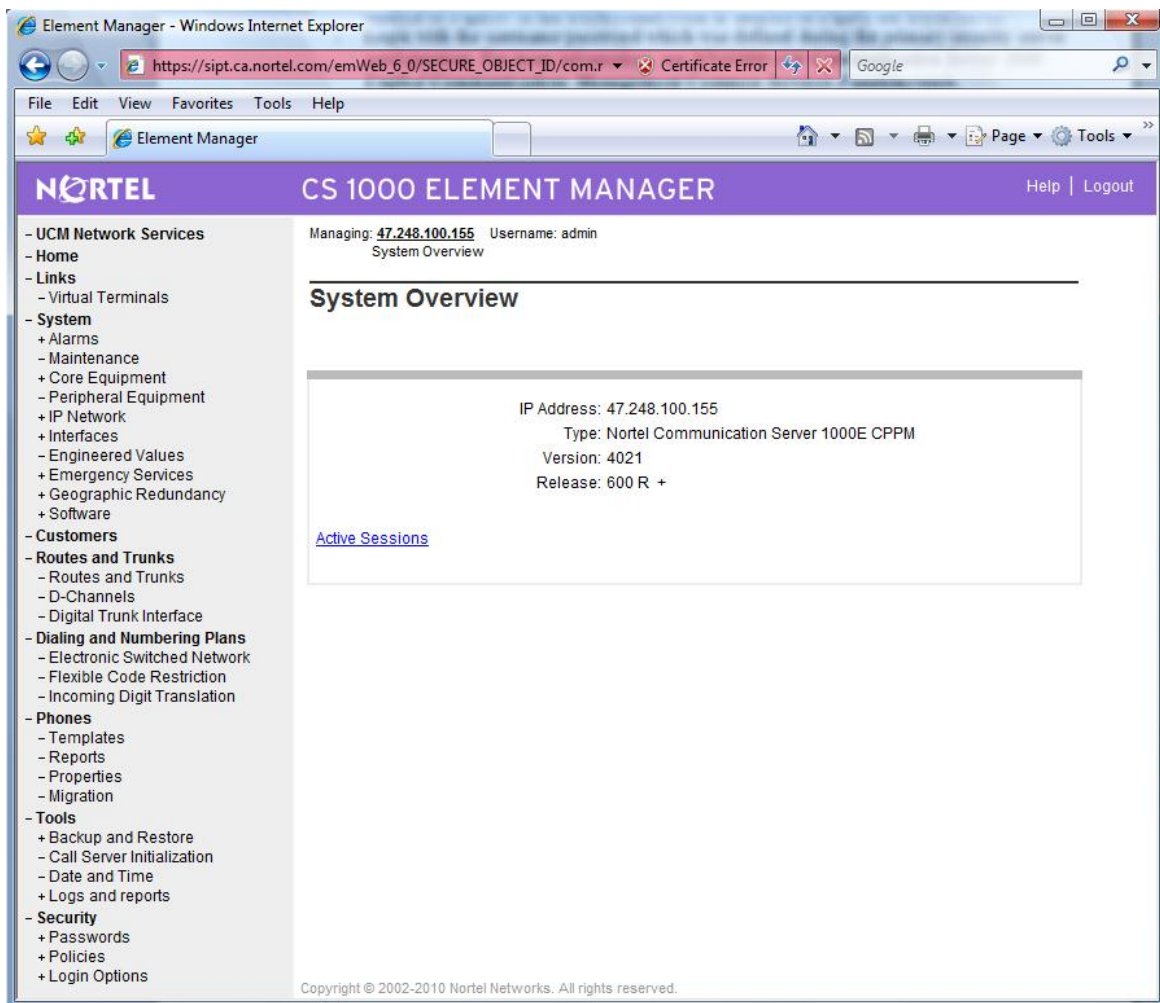


Figure 7: CS1000 EM Home Page

4.2. ESA Service Parameters Configuration

- On the EM page, navigate to **System** → **Emergency Services** → **Service Parameters**. The **Service Parameters** page appears as shown in Figure 4.
- On the **Service Parameters** page, from the **Location Information Services (LIS)** list, select **External Discovery Manager (EXT/DM)**.
- Click **Submit**.

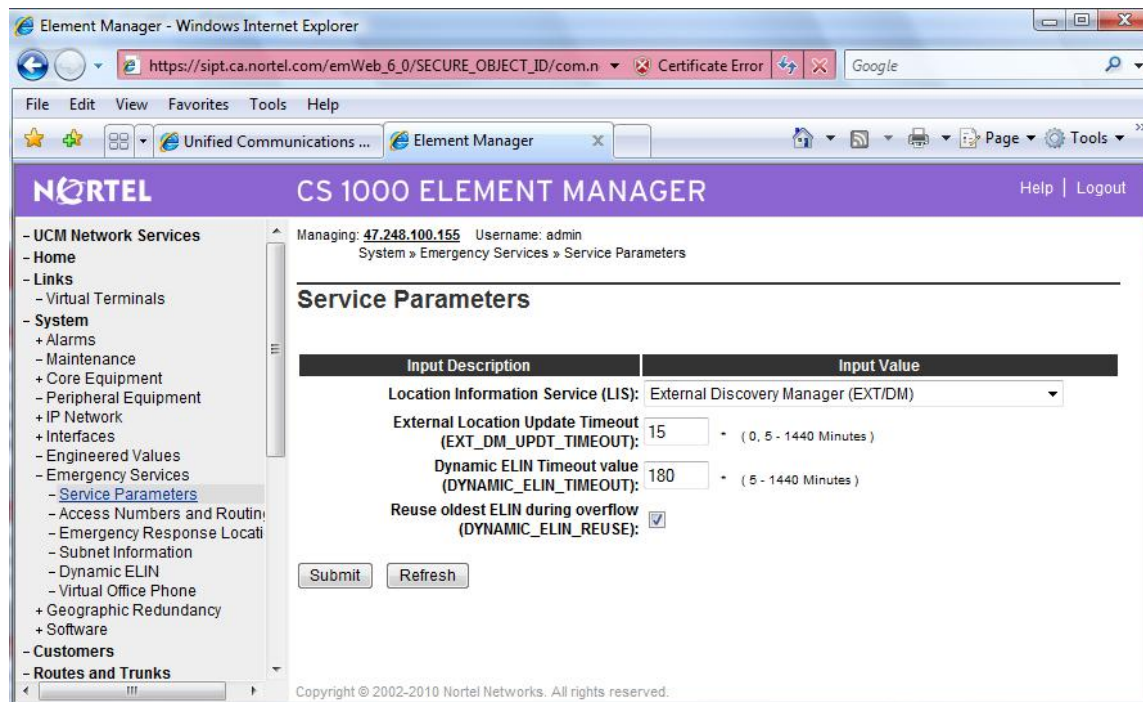


Figure 8: ESA Service Parameters

4.3. Access Numbers and Routing Configuration

- On the EM page, navigate to **System** → **Emergency Services** → **Access Numbers and Routing**. If there was no ESA Access Numbers and Routing configured, the **Add Customer x Emergency Services Directory Number** page appears as shown in Figure 5.
- On the **Add Customer x Emergency Services Directory Number** page, enter a directory number in the **Directory Number** text box.
- Enter directing digits in the **Directing Digits** text box.
- Enter Default Calling Number in the **Default Calling Number** text box.
- Enter a number in the **On-Site Notification System DN** text box.
- At the **Routing Method** attribute, select **Route List Index** and choose the appropriate value available from pull down menu.
- Check the **Misdial Prevention**, a dialog box appears asking for your confirmation to enable the feature, click **OK**.
- The remaining fields were left at their default values.
- Click **Save**.

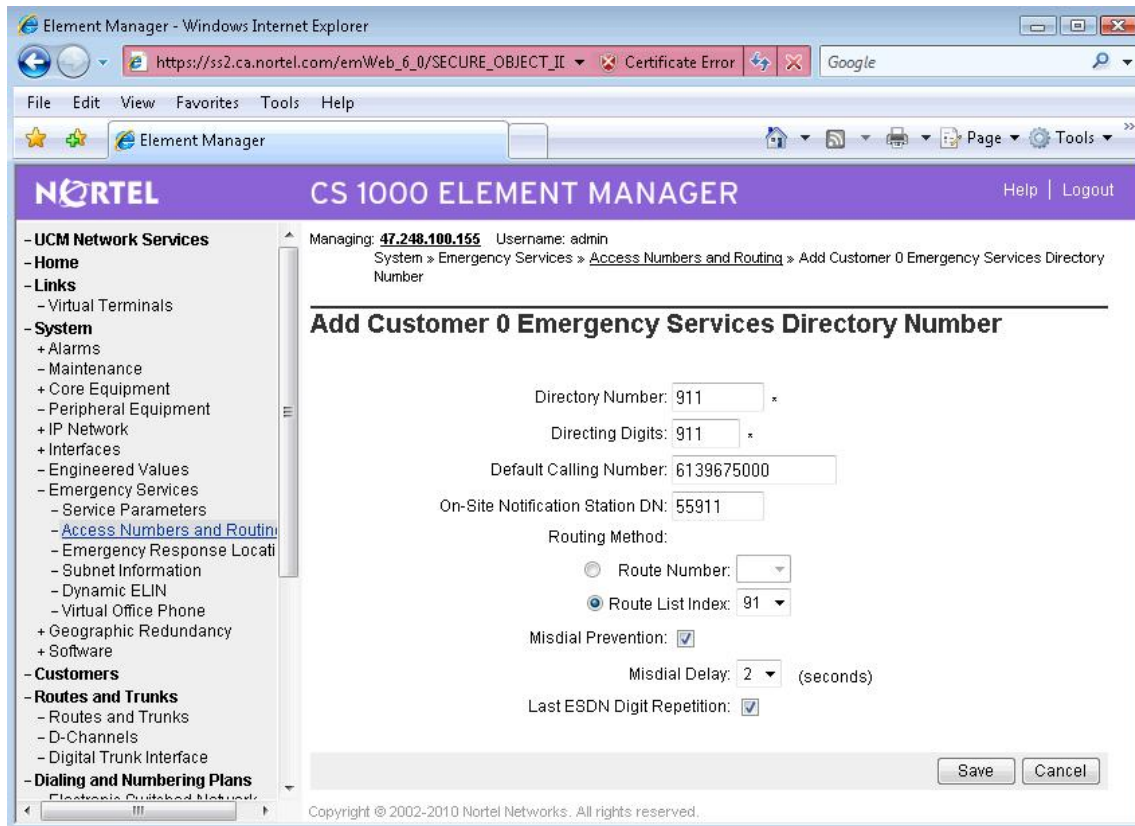


Figure 9 – Access Numbers and Routing

4.4. Emergency Response Location (ERL) Configuration

- On the EM page, navigate to *System* → *Emergency Services* → *Emergency Response Location*.
- If there was no ERL created, a dialog appears asking for your confirmation to create a new ERL. Click **OK**, the *Add Emergency Response Location* page appears (not shown).
- On the *Add Emergency Response Location* page, enter ERL number in the *Emergency Response Location (ERL)* text box.
- Enter the site name in the *Site Name (SITENAME)* text box.
- Enter the location description in the *Location Description (LOCDESC)* text box.
- From the *Routing Method* pull down list, select a routing method and enter corresponding *route number/route list index* in the next text box as shown in Figure 6.
- Click **Submit**

Element Manager - Windows Internet Explorer

https://supt.ca.nortel.com/emWeb_6_0/SECURE_OBJECT_ID/com.n Certificate Error Google

File Edit View Favorites Tools Help

Unified Communications ... Element Manager

NORTEL CS 1000 ELEMENT MANAGER Help | Logout

Managing: 47.248.100.155 Username: admin

System » Emergency Services » Emergency Response Location » Add Emergency Response Location

Add Emergency Response Location

Input Description	Input Value
Emergency Response Location (ERL):	1000 *
Site Name (SITENAME):	BVW
Location Description (LOCDESC):	BVW DevConnect Lab
Routing Method (ROUTING):	Route List Index (RLI) 91
Access Code (AC):	Null (NULL)
Prepend Digits (PREPEND):	
Static ELIN (LOCATOR):	6139675000
On-Site Notification DN (OSDN):	

Submit Cancel

Copyright © 2002-2010 Nortel Networks. All rights reserved.

Figure 10 – Emergency Response Location Configuration

4.5. Configure the Avaya CS1000 - Alarms

This section describes the steps to configure Alarms on the CS1000 system using SNMP Profile Manager. This is to generate alarms when 911 calls are made and sending the alarms to the eTelemetry Locate911-N server for desktop OSN. Repeat these steps for other CS1000 systems in the CS1000 network. For more information, see [3].

4.5.1. Log in to Unified Communications Management (UCM) and SNMP Profile Manager

- Refer to section 4.1 to see how to login into the Unified Communications Management (UCM).
- From the UCM Home page, navigate to **Network** → **CS1000 Services** → **SNMP Profiles**. The **SNMP Profile Manager** page appears as shown in Figure 7.

4.5.2. Create a New SNMP Profile

- On the **SNMP Profile Manager** page, navigate to **SNMP Profile**. The **SNMP Profiles** page appears (not shown).
- On the **SNMP Profiles** page, click **Add**. The **New SNMP Profile** page appears.
- Enter a name in the **Profile Name** text box.
- From the **Profile Type** list, select **ALARM**. Additional parameters appear after a profile type is selected.
- Enter a trap community in the **Trap Community** text box. The string is “public” (without quotes) by default.

- Ensure that the **Option** check box is checked to enable trap sending.
- Enter eTelemetry Locate911-N ELAN IP addresses and ports (port 162) in the **Trap Destinations**.
- Click **Save**.

The screenshot shows a web browser window with the URL https://sipl.ca.nortel.com/snmpManager/SECURE_OBJECT_ID/com.nortel.ems.SnmpManager/f0065373eb01. The page title is "New SNMP Profile". The form contains the following fields:

- Profile Name: CUSTOM-CS1k60A-Alarm
- Profile Type: ALARM
- Trap community: public
- Alarm Threshold: None
- Option: ☒ Enable trap sending
- Trap Destinations:

IPAddress1: 47.248.100.157	Port1: 162
IPAddress2:	Port2:
IPAddress3:	Port3:

Copyright © 2008 Nortel Networks. All rights reserved.

Figure 11 – New SNMP Profile

4.5.3. Assign an SNMP Profile to a Network Element.

- On the **SNMP Profile Manager** page, navigate to **SNMP Distribution**. The **SNMP Distribution** page appears, as shown in Figure 8.
- Select a Network Element (ELAN IP address of CS1000 call server) then click the **Assign** button. The **SNMP Profile Distribution Details [xx.xx.xx.xx]** page appears, as shown in Figure 9.

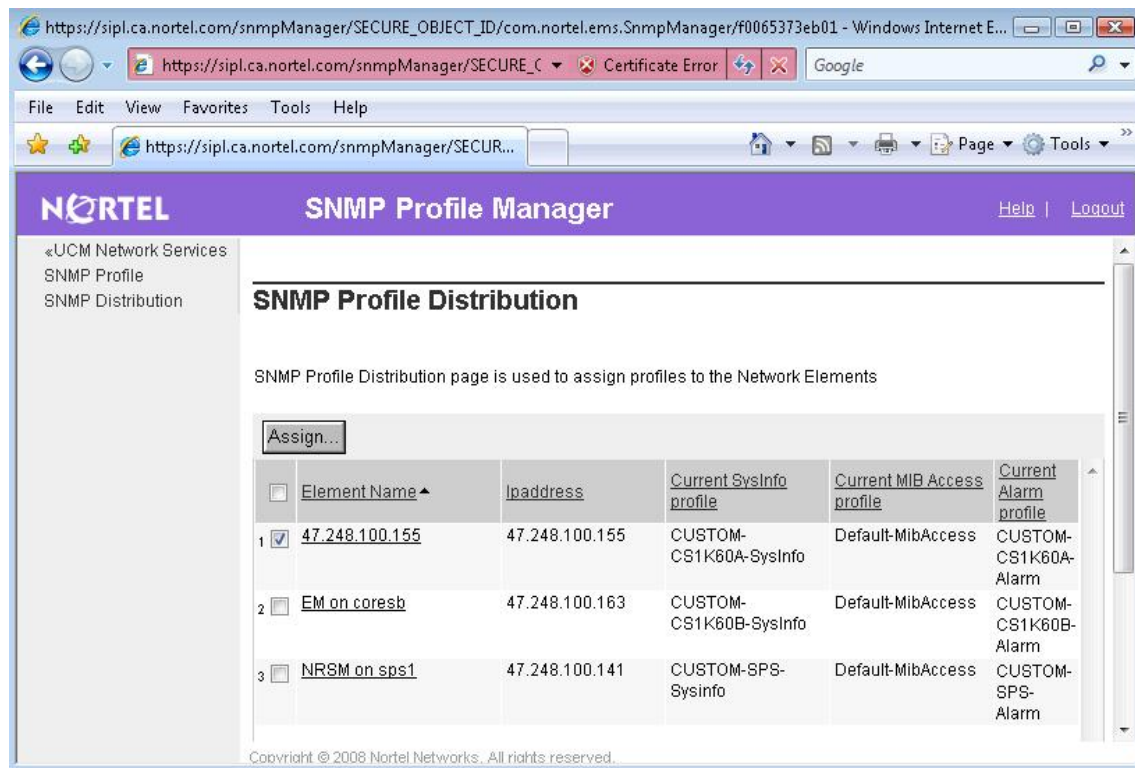


Figure 12 – New SNMP Profile

- On the *SNMP Profile Distribution Details [xx.xx.xx.xx]* page, from the *Alarm Profile* list, select the profile created in section 4.5.2.
- Click *Save*.

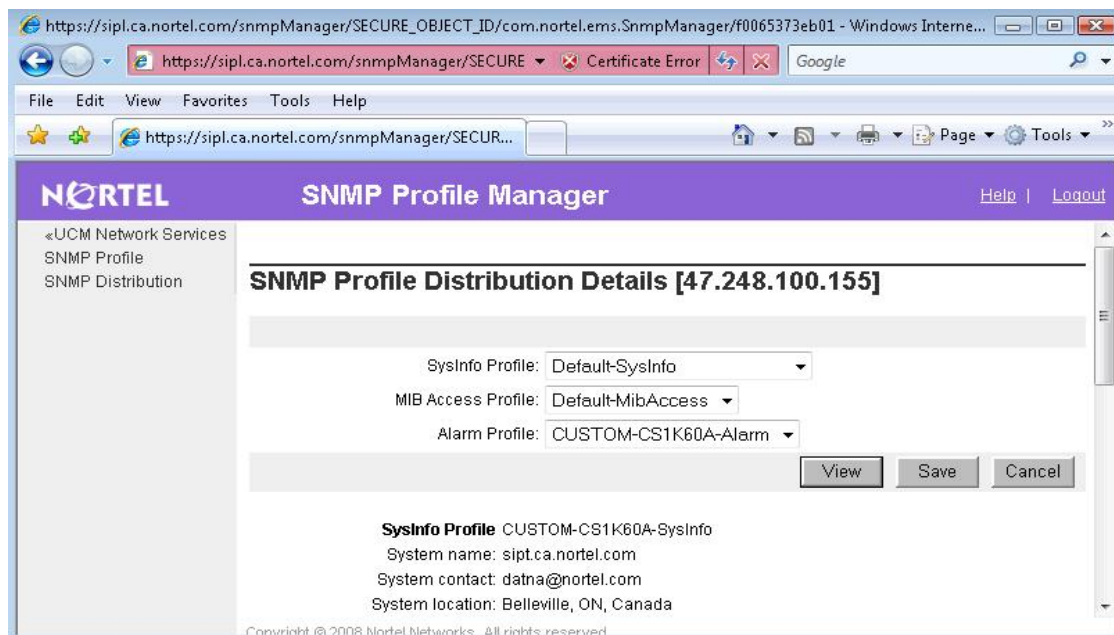


Figure 13 – Assign SNMP Profile to Network Element.

4.6. Configure the Avaya CS1000 - Intra System Signaling Security (ISSS)

This section describes the steps to configure Intra System Signaling Security (ISSS) on a CS1000 system. This is to ensure that the communication between CS1000 and eTelemetry Locate911-N server is secure. For more information, see [4]

4.6.1. Log in to Unified Communications Management (UCM) and CS1000 IPSec

- Refer to section 4.1 to see how to login Unified Communications Management (UCM).
- From the UCM Home page, navigate to **Network** → **CS1000 Services** → **IPSec**. The **IPSec For Intra System Signaling Security (ISSS)** page appears (not shown).

4.6.2. Change IPSec Defaults

- On the **IPSec For Intra System Signaling Security (ISSS)** page, click **Edit Defaults** button. The **IPSec Configuration Details** page appears as shown in Figure 10.
- From the **Security level** list, select **Full**.
- Enter the pre-shared key in the **PreShared Key** text box.
- Enter the pre-shared key again in the **Confirm PreShared Key** text box.
- Click **Save and Synchronize**. The **IPSec For Intra System Signaling Security (ISSS)** page appears again.

Unified Communications Management - Windows Internet Explorer
https://sipl.ca.nortel.com/frames.faces?body=/ipsecWeb/S
Certificate Error
Google

File Edit View Favorites Tools Help

Unified Communications Management

NORTEL UNIFIED COMMUNICATIONS MANAGEMENT Help Logout

Host Name: sipl.ca.nortel.com Software Version: 02.00.0055.00(3266) User Name admin

IPSec Configuration Details

Security level: Full
Secure all packets within and outside node except packets in BootP, SSH/SFTP and SSL ports

PreShared key: [Masked] *
(16-32 characters)
PreShared Key should not contain any of "Space ~ * \" @ [] # \"

Confirm PreShared key: [Masked] *

* Required value.

Save and Synchronize Cancel

Copyright 2002-2009 Nortel Networks. All rights reserved.

Figure 14 – IPSec Configuration Details

4.6.3. Create a New Manual IPSec Target

- On the *IPSec For Intra System Signaling Security (ISSS)* page, click **Add** to add eTelemetry Locate911 target server. The *New Manual IPSec Target* page appears as shown in Figure 11.
- On the *New Manual IPSec Target* page, enter ELAN IP address of eTelemetry Locate911-N server in the **IP Address 1** text box.
- Ensure that the **IPSec required** check box is checked.
- Click **Save**. The *IPSec For Intra System Signaling Security (ISSS)* page appears (not shown).
- If eTelemetry Locate911-N is set up with 2 servers (HA deployment), repeat above steps to create a new manual IPSec target for secondary server.

The screenshot shows a web browser window titled 'Unified Communications Management - Windows Internet Explorer'. The address bar shows 'https://simpl.ca.nortel.com/frames.faces?body=/ipsecWeb/\$'. The page title is 'UNIFIED COMMUNICATIONS MANAGEMENT'. The left sidebar contains a tree view with categories: Network (Elements, CS 1000 Services, IPSec, Patches, SNMP Profiles, Secure FTP Token, Software Deployment), User Services (Administrative Users, External Authentication, Password), Security (Roles, Policies, Certificates, Active Sessions), and Tools (Logs). The main content area is titled 'New Manual IPSec Target'. It contains the following fields: 'IP Address1' with the value '47.248.100.157' and an asterisk; 'IP Address2' which is empty; 'Friendly name' with the value 'Locate911N_ELAN' and an asterisk, with a note '(1-32 characters)'; and 'IPSec required' which is checked. Below the fields is a note: 'Note After saving, the target must be Synchronized in order to receive the common IPSec configuration parameters you have defined.' At the bottom right are 'Save' and 'Cancel' buttons. A legend indicates '* Required value.' The footer shows 'Copyright 2002-2009 Nortel Networks. All rights reserved.'

Figure 15 – New Manual IPSec Target

4.6.4. Synchronize and Activate ISSS in CS1000 network.

- From the *IPSec For Intra System Signaling Security (ISSS)* page, click **Synchronize**.
- After the synchronization, click **Activate**. The *IPSec Activation Details* page appears as shown in Figure 12.
- From the **Activation Type** list, select **Graceful**.
- Click **Activate**.

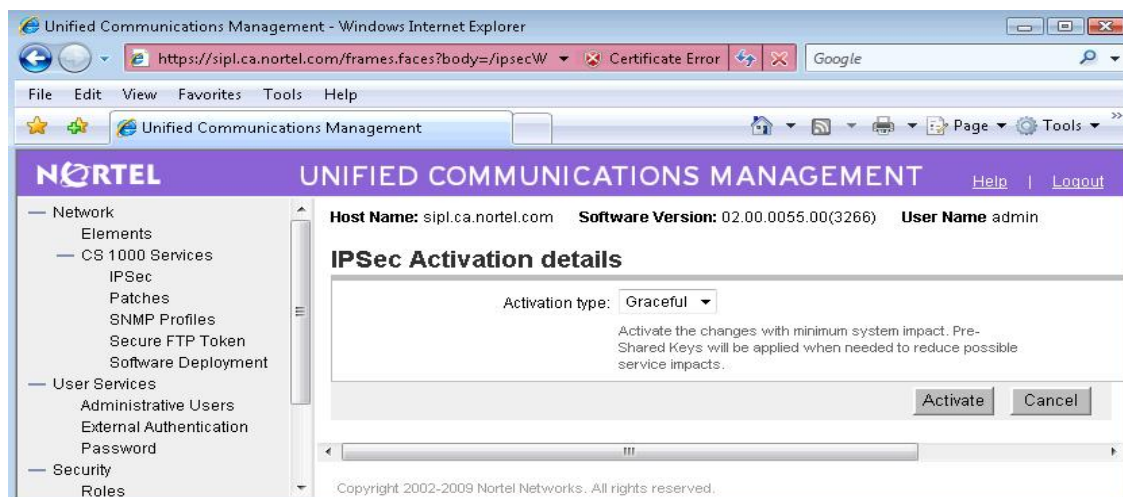


Figure 16 – IPsec Activation Details

4.7. Configure the IP Soft Phone 2050's MAC address

4.7.1. Determine your MAC address

First, verify the MAC address of your active network connection. This can be done in one of two ways. The first way is to issue the following command from a Windows Command Prompt:

```
ipconfig /all
```

A sample output from this command is shown in Figure 13, which shows two network adapters, one of them is disconnected. Because it is the “first” listed, it would be the default adapter and the MAC address chosen by default by the soft phone. Ensure the active MAC address is used by the IP soft phone.


```
Command Prompt

Windows IP Configuration

Host Name . . . . . : nortel-fj5sxiag
Primary Dns Suffix . . . . . :
Node Type . . . . . : Broadcast
IP Routing Enabled. . . . . : Yes
WINS Proxy Enabled. . . . . : Yes

Ethernet adapter TeamViewer UPN:

Media State . . . . . : Media disconnected
Description . . . . . : TeamViewer UPN Adapter
Physical Address. . . . . : 00-FF-87-3D-93-4E

Ethernet adapter Local Area Connection:

Connection-specific DNS Suffix . :
Description . . . . . : 3Com 3C920 Integrated Fast Ethernet Contr
oller (3C905C-IX Compatible)
Physical Address. . . . . : 00-06-5B-E1-9E-83
DHCP Enabled. . . . . : No
IP Address. . . . . : 192.168.11.5
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . : 192.168.11.1
DNS Servers . . . . . : 192.168.1.1
                        192.168.221.1
```

Figure 17 – ipconfig command output

The second way to determine your network adapter's MAC address is through the Network Properties themselves. Note that this method is accurate for Windows 2000 and XP systems, but it will be different on Windows Vista. In the system tray (near the clock), you will see a network icon. Figure 14 shows a typical setup with two network adapters: the one on the left is connected, while the one on the right is disconnected.

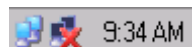


Figure 18 – Microsoft Windows Network icon

Clicking on the “Connected” icon will display the connection's Status window. On the Support tab is a “Details...” button. Clicking the “Details...” button will display the Network Connection Details window.

If you do not have a network icon like the one shown, you can get to the same window through the Control Panel called “Network Connections.”

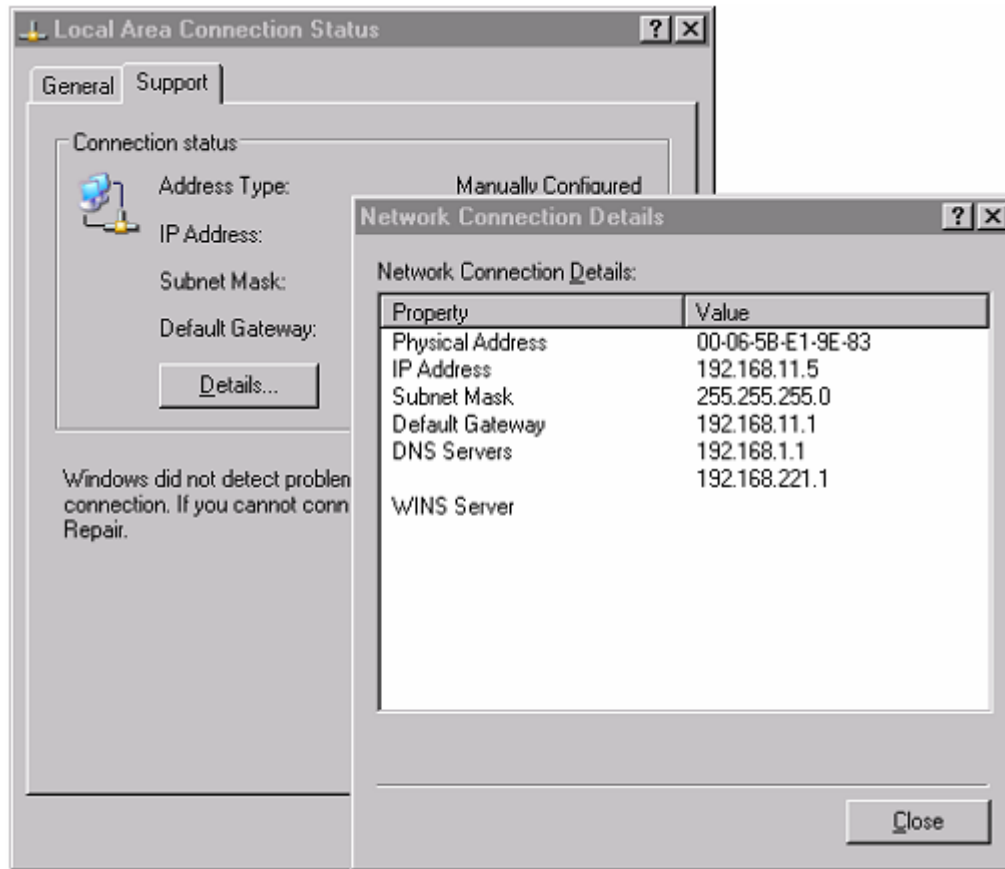


Figure 19 – Microsoft Windows Network Setting

Figure 15 shows the Details for the same network adapters we showed in the command line example. The MAC Address for the adapter is the Property called “Physical Address”, whose value is “00-06-5B-E1-9E-83”.

Regardless of what method you used to determine your network adapter’s MAC address, make a note of it someplace for later use and continue to the next section.

4.7.2. Set the Soft-phone’s MAC Address

Next, open your soft-phone’s configuration by clicking the settings button at the top of the soft-phone window, shown circled in Figure 16.



Figure 20 – 2050 Soft-phone

This will display the Avaya IP Soft-phone 2050 Settings window (see Figure 17). To set the MAC address of the soft-phone, click the Hardware ID option on the left side of the window. Next, check that the Hardware ID is displayed in the text box on the right hand side. If the value doesn't match with the value you determined in the section 4.7.1, you'll need to change it. Although the text box is editable, it is not recommended that you type the address directly. Instead, simply click the "Auto-Create" button below the Hardware ID text box. The value in the text box will change each time you click the button. Continue clicking the "Auto-Create" button until the value matches your network adapter's MAC address. Once the value is correct, click "OK" to save your settings and close the window. At this point, you will be informed that the soft-phone needs to be reset for the changes to take effect. Select "Yes" to reset the phone immediately. At this point, your phone should be reporting the correct MAC address to the CS1000 and Locate911-N should be able to determine and update its location correctly.

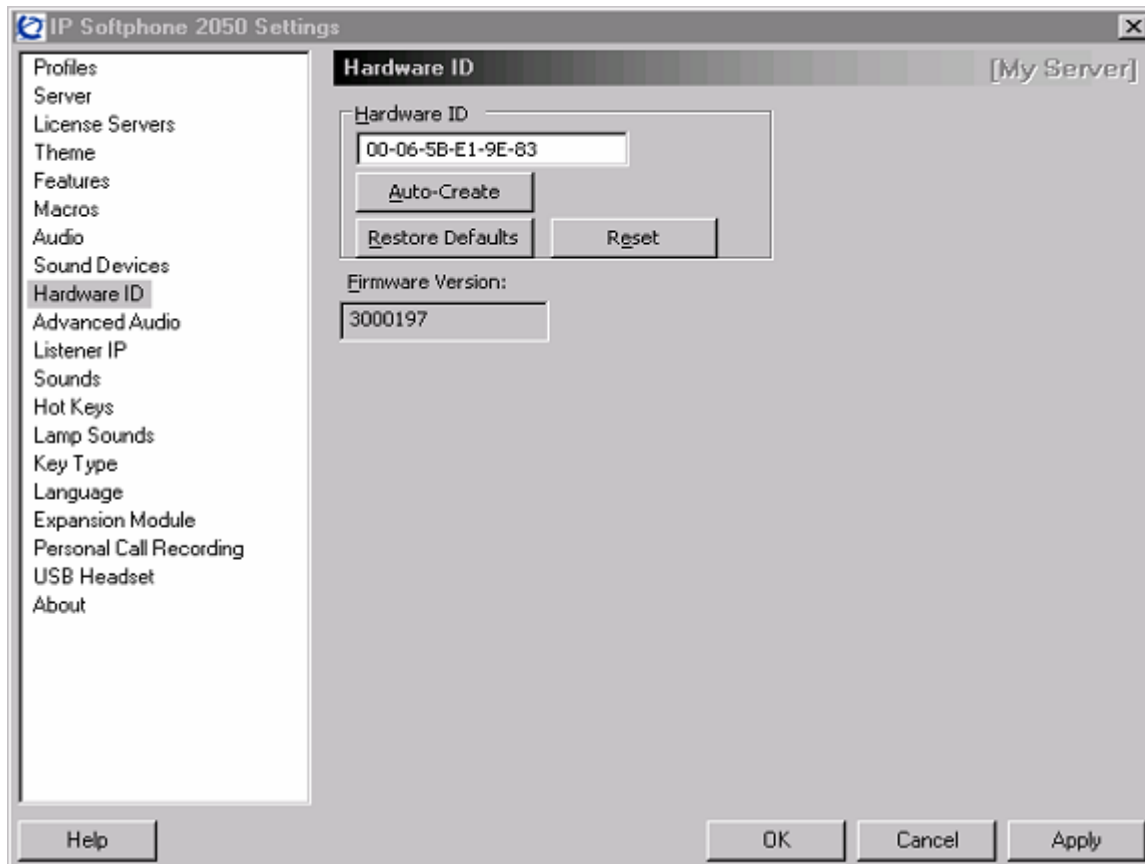


Figure 21 – 2050 Soft-phone Setting

5. eTelemetry Configuration

This section describes the steps to configure the eTelemetry Locate911-N and LENS Alert Agent to work with CS1000 Release 6.0. For more details see [5].

5.1. Locate911-N Configuration

This section describes the steps to configure the eTelemetry Locate911-N.

5.1.1. Locate911-N Web GUI Login

- Using a Web browser (IE7 is preferred) to launch eTelemetry Locate911 web portal at <http://<IP Address>> where <IP address> is the eTelemetry Locate911's Management IP address (TLAN).
- Login with admin account and password (default password).

5.1.2. Global Application Parameters

- From Locate911 Home Page, navigate to **Control Panel → Management Console → Manage Global Application Parameters**.
- Configure the parameters as shown in Figure 18 below.

Parameter	Value	Description
Admin Email:	nguyenanhdat@nortel-dplab.com	An email address through which users may notify the Admin of problems
Email Errors:	Yes (true)	Specifies whether or not to notify the Admin of each error encountered by the system
Trap Recipient for Errors:	localhost	Specifies a single trap recipient to receive SNMP Traps on errors (leave blank to specify no recipient)
Trap Recipient Community String:	public	The read-only community string used to send traps to the above trap receiver.
Domain:	nortel-dplab.com	The organization's internet domain
Days to Keep Logs:	14	The number of days to keep application and error logs (Default: 14)
Idle Timeout:	20	The inactivity time (in minutes) before the user must re-login to continue (Default: 20)
Session Life:	2880	The inactivity time (in minutes) before the system recycles a session (Default: 2880)
Triggered Network Crawls:	Yes (true)	Whether the system performs "mini-crawls" based on linkUp traps received from managed data switches. Requires that each data switch on the network be configured to send linkUp traps to this device. (Default: TRUE)
Network Timeout:	50000	The time in seconds to wait for a response from the network (Default: 3)
Network Retries:	3	The number of retries before deciding that a network device is not available (Default: 3)
Pings Allowed:	Yes (true)	Whether the system is allowed to use Ping when searching for network devices (Default: TRUE)
NTP Time Server:	pool.ntp.org	The NTP Time server used for time synchronization. (Default: pool.ntp.org)
Outgoing SMTP Host:	47.248.100.41	The SMTP host through which outgoing email alerts will be delivered.
SMTP User Name:	nguyenanhdat@nortel-dplab.com	The SMTP username that will be used to authenticate emails at the SMTP host (leave blank to specify "no authentication").
SMTP Password:	*****	The SMTP password that will be used to authenticate emails at the SMTP host (leave blank to specify "no authentication").
SMTP From Address:	NoReply@nortel-dplab.com	The email address used as the From or Reply-To address for all system-generated email alerts.

Buttons: Validate Parameters, Commit, Reset to Defaults, Cancel

Figure 22 – Manage Global Application Parameters

5.1.3. Avaya Settings

- From Locate911 Home Page, navigate to **Control Panel** → **Management Console** → **Manage Avaya Settings**.
- Configure the parameters as shown in Figure 19 below.

Parameter	Value	Description
Signaling Server Polling Frequency:	Every half hour	How often Locate911 should connect to the signaling servers to receive phone updates. (Default: Once per day)
Default ERL:	0	The default ERL for phones that cannot be located. (Default: 0)
Need Update Threshold:	20	The number of times a phone must be reported as needing its location updated before the default ERL is used. (Default: 20)
OSN Map Link Label:	Emergency Map Link	The label to display next to the link in the OSN details.
OSN Map Link:	http://www.company.com/maps.htmr	A fully-formed URL to an external map for a specified ERL. If provided, this link will be inserted into OSN records so that the Alert Agent can display a link to a map (or other relevant information). Use <ERL> wherever you want the ERL to be inserted. (e.g.: http://company.com/maps.html?erl=<ERL>)
ISSS Mode of Operation:	Full	Select the <i>Intra System Signaling Security</i> (ISSS) mode of operation. This setting should match that of the Call Server. Note: When ISSS is enabled, this Locate911 system must also be added to the Unified Communications Management system as a <i>Manual Target</i> (see Nortel UCM documentation for details). (Default: Off)
ISSS Pre-shared Key:	*****	The ISSS pre-shared key. If this field is blank, then no ISSS is assumed (even if a mode is set above).

Buttons: Validate Parameters, Commit, Reset to Defaults, Cancel

Figure 23 – Manage Avaya Settings

5.1.4. Avaya Call Servers

- From Locate911 Home Page, navigate to **Control Panel** → **Management Console** → **Manage Avaya Call Servers**. The Call Servers Configured appears as shown in Figure 20.

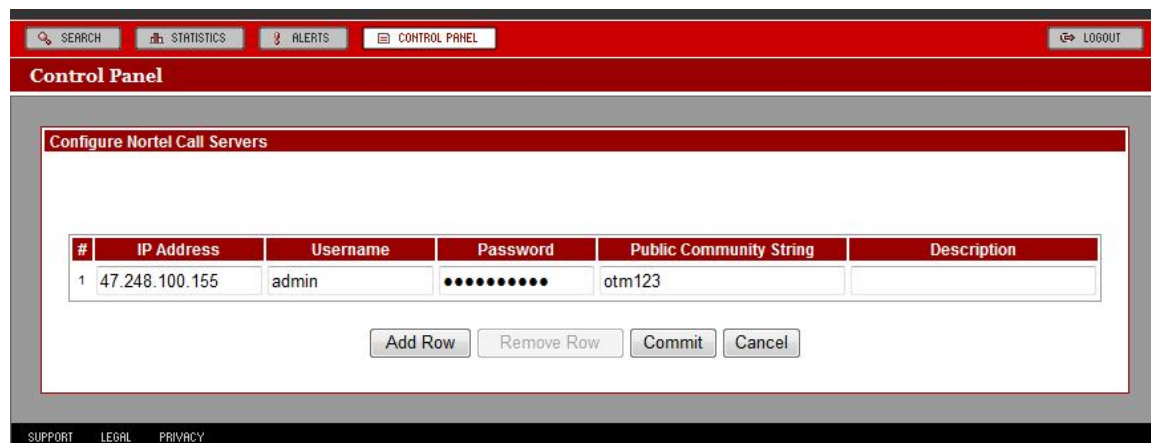


#	IP Address	Ping	SNMP	Valid	Description
1	47.248.100.155	✓	✓	✓	

[Edit Call Servers](#)

Figure 24 – Avaya Call Servers

- Click **Edit Call Servers** to edit/add CS1000 Call Servers. The **Configure Avaya Call Servers** page appears as shown in Figure 21.



#	IP Address	Username	Password	Public Community String	Description
1	47.248.100.155	admin	*****	otm123	

[Add Row](#) [Remove Row](#) [Commit](#) [Cancel](#)

Figure 25 – Configure CS1000 Call Servers

- Enter CS1000 Call Server's ELAN IP address in the **IP Address** column.
- Enter username/password to login CS1000 Call Servers in the **Username/Password** columns.
- Enter CS1000 public community string in the **Public Community String** column.
- To add more CS1000 Call Servers, click **Add Row**.
- Click **Commit**. The CS1000 Call Servers configuration result appears as shown in Figure 22.
- Ensure that **Ping**, **SNMP** and **Valid** columns are green for every IP address. Otherwise, check the IP connectivity, SNMP trap community string and CS1000 login credentials.

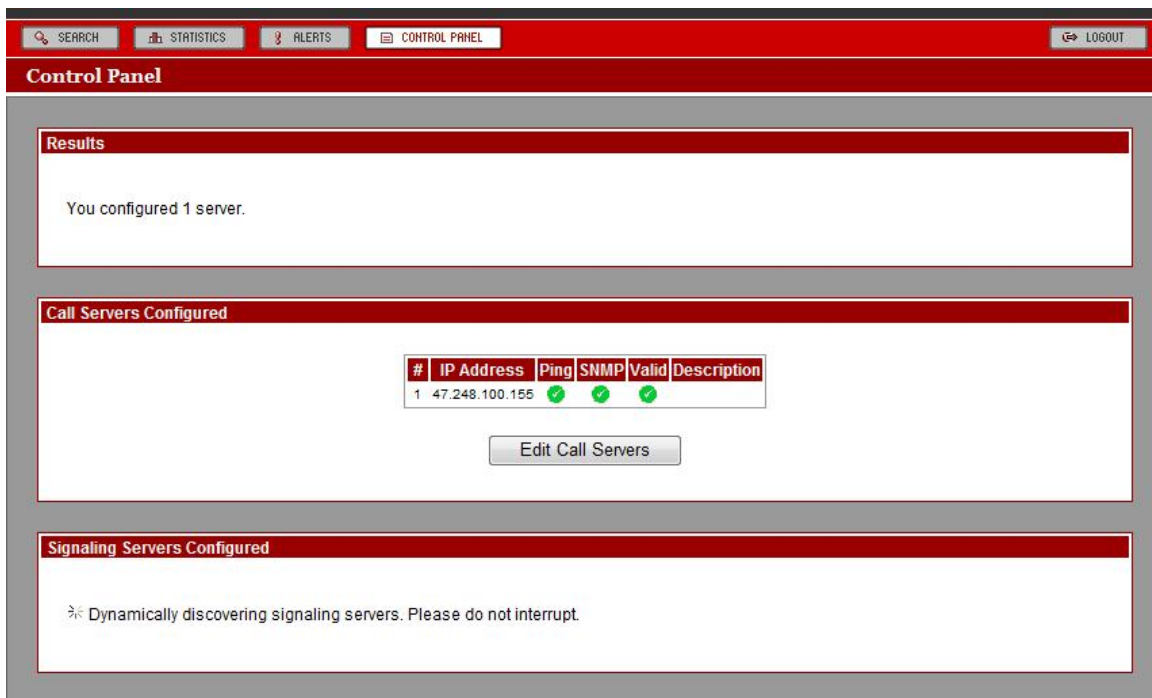


Figure 26 – Configure CS1000 Call Servers results

- Once the CS1000 Call Server(s) is (are) configured and the login is successful, the Dynamic Discovery process will automatically discover the associated CS1000 Signaling Servers. This takes few minutes to complete.
- After the Dynamic Discovery process completed, the **Signaling Servers Configured** panel will show all associated CS1000 signaling servers as shown in Figure 23.

Call Servers Configured

#	IP Address	Ping	SNMP	Valid	Description
1	47.248.100.155	✓	✓	✓	

Edit Call Servers

Signaling Servers Configured

#	IP Address	Call Server	Ping	Auth	TPS
1	47.248.100.144	47.248.100.155	✓	✓	✓
2	47.248.100.130	47.248.100.155	✓	✓	✓
3	47.248.100.153	47.248.100.155	✓	✓	-

Please note: if you recently deployed a new Signaling Server and it does not appear in the list above, it is possible that the daily inventory has not yet been rebuilt. You may choose to wait up to 24 hours for this to occur, or you may force a rebuild manually in the Call Server. For more information, contact your Nortel support personnel.

Seed Database from Signaling Servers

By clicking the button below, the signaling servers connected to each of your Nortel Call Servers will be queried for existing IP phones. **Warning! All current phones in the database will be replaced by those reported by the signaling servers. This could be a lengthy process, cannot be undone, and should not be interrupted.**

Seed Phones Database...

Return to Control Panel

SUPPORT

LEGAL

PRIVACY

Figure 27 – Signaling Servers Dynamic Discovery

- Click *Seed Phones Database*, the *Seed Phones Database* appears (not shown).
- Wait a few minutes for the process to be completed.

5.1.5. Create/Load Switches File

- Create a CSV file that includes a list of the managed switches on your network. The file must be formatted in a *comma*, *tab*, or *semi-colon* delimited format. The file must contain the following information about the managed switches:

Parameter	Value
switch_ip	IP address of the switch
community_public	SNMP public community string **Not used for SNMP V3 switches.
community_private	SNMP private community string (optional) **Not used for SNMP V3 switches.
label	display name of the device, e.g. —Nortel 8661 □
serial	not used
layer2	Allows you to turn on/off MAC/Switch collection from a particular switch. Default: 1 0: Do not collect MAC/Switch Port information 1: Collect MAC/Switch Port information
layer3	Allows you to turn on/off IP/MAC collection from a particular switch. Default: 1 0: Do not collect IP/MAC information 1: Collect IP/MAC information
query_delay	Allows you to throttle down the rate of snmp queries to a switch. Default: 0 1+: The number of microseconds (millionths of a second) to pause between each row of data returned by the switch.
For SNMP V3 Switches	
v3_auth_protocol	The authentication protocol. Can be “MD5” or “SHA”
v3_auth_passwd	The authentication pass phrase
v3_security_level	The security level. Can be “noAuthNoPriv”, “authNoPriv” or “authPriv”
v3_user	The authentication user name
v3_priv_protocol	The privacy protocol. Can be “DES” or “AES”
v3_priv_passwd	The privacy pass phrase

The fields community_public and community_private are snmpv2 specific, and not used if snmpv3 fields are provided for a switch. The following is a sample of a comma delimited Switches file:

```
switch_ip,community_public,label,layer2,layer3,query_delay
192.168.10.10,public,Nortel 8661,1,0,1
192.168.10.11,public,Nortel 8661,1,1,1
192.168.10.12,public,Nortel 8661,0,0,1
```

- From Locate911 Home Page, navigate to **Control Panel** → **Add to or Replace the contents of tables** → **Upload Values into the table Switches**. The **Upload Values into the table Switches** page appears.

Figure 28 – Upload table Switches

- Select delimited type in the *Delimited* list.
- Enter the location of the file in the *Upload File* text box or click *Browse* to browse to the file.
- Click *Send File*. The *Verify Values for Upload* page appears (not shown).
- Click *Commit to the Table*. The *Upload Status* page appears (not shown).
- Click *OK*.

5.1.6. Create/Load Network Documentation File

- Create a CSV file in comma, tab, or semi-colon delimited format containing the following field name headers: *switch_port*, *location_key*, *jack*, *building*, *location*, *floor*, *room*. The following is an example of a comma delimited network documentation CSV file:

```
switch_port,location_key,patch_panel,jack,building,location,floor,room
10.10.12.7 Fa01,1233,A1,1A,202 Jefferson Circle,Second Floor,2,205
10.10.12.7 Fa02,1233,A2,2A,202 Jefferson Circle,Second Floor,2,203
10.10.12.7 Fa03,1233,A3,3A,202 Jefferson Circle,Second Floor,2,206
10.10.12.7 Fa04,1233,A4,4A,202 Jefferson Circle,Second Floor,2,202
10.10.12.8 Fa01,1245,A5,8A,202 Jefferson Circle,Third Floor,3,304
10.10.12.8 Fa02,1245,B8,8B,202 Jefferson Circle,Third Floor,3,304
10.10.12.8 Fa03,1245,A9,9A,202 Jefferson Circle,Third Floor,3,303
```

- From Locate911 Home Page, navigate to *Control Panel* → *Add to or Replace the contents of tables* → *Upload Values into the table Network Documentation*. The *Upload Values into the table Network Documentation* page appears.

Figure 29 – Upload table Network Documentation

- Select delimited type in the *Delimited* list.
- Enter the location of the file in the *Upload File* text box or click *Browse* to browse to the file.
- Click *Send File*. The *Verify Values for Upload* page appears (not shown).
- Click *Commit to the Table*. The *Upload Status* page appears (not shown).
- Click *OK*.

5.1.7. Create/Load User-Defined Switch Trunks File

- Create a CSV file in comma, tab, or semi-colon delimited format containing the following field name headers: *switch_ip* and *trunk_port*.
The following is an example of a comma delimited network documentation CSV file:

```
switch_ip, trunk_port
192.168.1.10, ifc24(Slot: 1 Port: 24)
192.168.1.14, ifc24(Slot: 1 Port: 24)
```

- From Locate911 Home Page, navigate to *Control Panel* → *Add to or Replace the contents of tables* → *Upload Values into the table Switches*. The *Upload Values into the table Switches* page appears.

Control Panel Upload Values into the table *User_Switch_Trunks*

Select File for Upload:

UPLOAD FILE EDIT VALUES EXPORT CSV

This action will populate the table: *User_Switch_Trunks*, by uploading a file formatted as: *Comma* - Delimited

Please browse to select a prepared file where the first line is a Header containing the field names, and the subsequent lines contain matching data, one line per record.

Available Field Names: *id, switch_ip, trunk_port*

Upload File: Browse... Send File

Send File Cancel

SUPPORT LEGAL PRIVACY

Figure 30 – Upload table *User_Switch_Trunks*

- Select delimited type in the *Delimited* list.
- Enter the location of the file in the *Upload File* text box or click *Browse* to browse to the file.
- Click *Send File*. The *Verify Values for Upload* page appears (not shown).
- Click *Commit to the Table*. The *Upload Status* page appears (not shown).
- Click *OK*.

5.1.8. Alerts Configuration

- From Locate911 Home Page, navigate to *ALERTS* → *Manage Alert Rules*. The *Manage Alert Rules* page appears.

Alerts Manage Alert Rules - View List

Status	Name	Type	Severity	Description	
edit deactivate	Active	911 call alert	Emergency Call	Alert	send email when 911 call occurs
edit deactivate	Active	Phone Move	Value Change	Informational	Raise an alert when a phones move to a different switch port

Create New Rule: Type: *Value Change* Add New Rule

SUPPORT LEGAL PRIVACY

Figure 31 – Manage Alert Rules

- Select rule type in the *Type* list.
- Click *Add New Rule*.

Rule Type:

- *Value Change* allows the administrator to create alerts for changes on the network, for example:

- Movement of IP Phones on the Network – When MAC with value of “*” changes its Switch Port.
- When an IP Phone Changes its IP Addresses – When MAC with value of “*” changes its IP Address.

The screenshot shows the 'Alerts' management interface with the 'Edit Rule' form. The form has a red header bar with navigation links: SEARCH, STATISTICS, ALERTS, CONTROL PANEL, and LOGOUT. Below the header, the title 'Alerts Manage Alert Rules - Edit Rule' is displayed. The form itself is a table with three columns: Parameter, Value, and Description.

Parameter	Value	Description
Name	Phone Move	
Description	Raise an alert when a phones move to a different switch port	
Status	Active	
Severity	Informational	"Alert" Severity will send an email to the recipients below. "Informational" Severity will log the event, but not send emails.
Emails		Comma separated list of email recipients.
Report Limit	Limited 0	Specifies the number of times an alert will trigger before becoming inactive.
Rule	When MAC with value of * changes its Switch Port	Alerts when values change for a specific object. If the object value is "*", then any object of that type is alerted.
Include New	False	Alert when a previously unmapped value is mapped.
Include Unmapped	False	Alert when a value is unmapped.

At the bottom of the form are three buttons: Cancel, Delete Rule, and Save Changes. The footer of the page contains links for SUPPORT, LEGAL, and PRIVACY.

Figure 32 – Value Change

- **Emergency Call** allows creating alerts when a call is made to 911.

The screenshot shows the 'Alerts' management interface with the 'Edit Rule' form for a '911 call alert'. The form has a red header bar with navigation links: SEARCH, STATISTICS, ALERTS, CONTROL PANEL, and LOGOUT. Below the header, the title 'Alerts Manage Alert Rules - Edit Rule' is displayed. The form itself is a table with three columns: Parameter, Value, and Description.

Parameter	Value	Description
Name	911 call alert	
Description	send email when 911 call occurs	
Status	Active	
Severity	Alert	"Alert" Severity will send an email to the recipients below. "Informational" Severity will log the event, but not send emails.
Emails	nguyenanhdat@nortel-dplab.com	Comma separated list of email recipients.

At the bottom of the form are three buttons: Cancel, Delete Rule, and Save Changes. The footer of the page contains links for SUPPORT, LEGAL, and PRIVACY.

Figure 33 – 911 Call Alert

5.1.9. Redundancy Configuration

- From Locate911 Home Page, navigate to **Control Panel** → **Management Console** → **Manage Redundancy Configuration**. The **Manage Redundancy Configuration Parameters** page appears.
- Enter the parameters as shown in Figure 30 below.
- Click **Validate** to validate the parameters.
- Click **Commit** to save the configuration.

The screenshot shows the 'Manage Redundancy Configuration Parameters' page. At the top, there is a navigation bar with 'SEARCH', 'STATISTICS', 'ALERTS', and 'CONTROL PANEL' tabs. Below this, the page title 'Control Panel Manage Redundancy Configuration Parameters' is displayed. The main content area contains a table with the following parameters and values:

Parameter	Value	Description
Secondary IP:	47.248.100.233	This is the IP of the system's secondary node.
Service IP:	47.248.100.238	This is the cluster's floating IP. It will be enabled on whichever node is running as a primary. It is the address all clients should use to access the Locate911 system/service.
Pingable Device #1 IP:	47.248.100.49	This is the IP address of a device that will respond to pings as part of verification of network connectivity (perhaps a gateway or some other reliable infrastructure device).
Pingable Device #2 IP:	47.248.100.58	This is the IP of an another device that will respond to pings as part of verification of network connectivity (perhaps a gateway or some other reliable infrastructure device).
Poll Cycle:	5	The amount of time between local state checks, measured in seconds. (Default: 5)
Maximum Ping Failures:	3	The maximum amount of failed pings before the system switches operations. (Default: 3)
Auto Toggle Back:	60	The amount of cycles before the system toggles back to normal operation, '0' for no toggle back. (Default: 15)

Below the table, there are four buttons: 'Validate Parameters', 'Commit', 'Reset to Defaults', and 'Cancel'.

Figure 34 – Redundancy Configuration

6. General Test Approach and Test Results

The focus of this interoperability compliance testing was primarily to verify the Phone Discovery functionalities and ERL update when adding, moving, removing CS1000 Unistim IP Phones.

6.1. General Test Approach

The general test approach was to integrate eTelemetry Locate911-N, Locate911-N High Availability/Business Continuity Cluster, and LENS appliances and software into the CS1000 environment as an External Discovery Manager (Ext DM) and to exercise the phone discovery, ERL update and 911 call alerts functionalities. The main objectives were to verify that Locate911-N successfully performs the following:

- Dynamic Discovery of signaling servers and registered phones.
- Update the ERL of the phone when it is registered.
- Update the ERL of the phone when it is moved to another switch port (on the same switch and on different switch).
- Update the ERL of the phone when it is reset.
- Receiving and interpreting 911 call alerts on Locate911-N Alerts and LENS Alert Agent.

6.2. Test Results

The objectives outlined in section 6.1 were verified and met.

The following observations were made during the compliance testing:

- When sending phone registration event, the CS1000 does not send non-critical information such as firmware and phone type but rather the Locate911-N pulls that information periodically (once per day) from the CS1000. This may result in firmware and phone type not properly represented on the Locate911-N Web GUI, when adding new phones, until the periodic poll takes place. The associated MAC address, ERL, PBX, etc. can be detected correctly.
- At present, Locate911-N can not accommodate mixed ISSS environment where security levels and Pre-Shared Keys are different among CS1000 in the same Security Domain. So, if ISSS is enabled on multiple CS1000's in the same security domain, they all must be set with the same security level and the same Pre-Shared Key.
- When the ISSS Mode setting is changed, it may take up to a minute or so for the change to take effect.
- During a failover (or startup of whichever system is acting as primary), there is a 1-2 minute period of time that no alerts are processed. At present, even though the secondary does get the SNMP traps, it does not perform any task on them unless it is fully running as the primary (only the primary is allowed to make database changes). It does not queue or otherwise hold on to these alerts. So, any 911 calls made during the role-change process will not be detected. Alerts are processed only by a fully running acting primary.

7. Verification Steps

This section includes some steps that can be followed to verify the configuration.

7.1. Verify Connectivity and Dynamic Discovery process

- After completing provisioning the CS1000 call server mentioned in section 5.1.4 Avaya Settings, check the “ping”, “SNMP” and “Valid” status on the GUI. The Dynamic Discovery of associated signaling servers should occur after that and the process should be successful.
- If ISSS is enabled, capture some pcap traces to see if there are ESP (Encapsulating Security Payload) packages going back and forth between eTelemetry Locate911-N and CS1000 call server. There should be no plain payload between servers.

7.2. Verify Phones Retrieval

- After completing all steps mentioned in section 5.1.4 Avaya Settings, the **Seed Phones Database** process will collect information of existing registered IP phones. From the Locate911-N Web GUI, go to **SEARCH**, check if registered phones have been retrieved fully with correct information. This can be compared with *isecLocShow* command output on CS1000 Signaling Server.

```
[nortel@sipt ~]$ isecLocShow
```

```
=== TPS ===
```

```
Set Location Information
```

```
-----  
IP Address:Port      HWID      ERL  ECL Location Description MU NU  State  
-----  
47.248.100.59:5000  12-86e720524153-6606 1000   0 BELLEVILLE      0 0 online  
47.248.100.55:5000  18-0016ca0081fd-6625 2000   0 CARLING         0 0 online
```

```
Total number of sets = 2
```

```
Sets that need location update = 0
```

7.3. Verify Receiving of CS1000 Events

- Adding/Resetting some phones.
- From Locate911-N Web GUI, go to **Control Panel → View Application Logs & Status → View the Application Logs**. There should be some event log records on there.

7.4. Verify ERL update process

- Move an IP phone to another port switch.
- Wait for the phone to come up and for the update process to occur.
- From Locate911-N Web GUI, go to **SEARCH**, check if the ERL of the moved phone is updated correctly and reflected on the Network Documentation File.

- From CS1000 Signaling Server, the *isecLocShow* command output should show consistent ERL and Location.

7.5. Verify 911 call alerts

- Make some 911 calls.
- From Locate911-N Web GUI, go to **ALERTS**, there should be corresponding emergency call alerts shown on the table.
- If LENS Alert Agent has been set up, there should be corresponding emergency call alert popups.

8. Conclusion

All of the executed test cases have passed and met the objectives outlined in **Section 6.1**, with some limitations/exceptions outlined in **Section 6.2**.

9. Additional References

Product documentation for Avaya products may be found at:

<http://support.nortel.com/go/main.jsp>

[1] *NN43001-613 Communication Server 1000 Emergency Services Access Fundamentals.*

[2] *NN43001-116 Communication Server 1000 Unified Communications Management Common Services Fundamentals.*

[3] *NN43001-719 Communication Server 1000 Communication Server 1000 Fault Management - SNMP*

[4] *NN43001-604 Communication Server 1000 Security Management Fundamentals.*

Product information for eTelemetry Locate911-N products can be found at

<http://www.etelemetry.com/products/locate911n.aspx>

[5] *Locate911-N User's Guide Version 1.4 revision 8.*

©2010 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.