



Avaya Solution & Interoperability Test Lab

Application Notes for Configuring Windstream SIP Trunking with the Avaya Communication Server 1000 Release 7.5, Avaya Aura® Session Manager Release 6.1 and ACME Packet Net-Net 3800 Session Border Controller Release 6.2 – Issue 1.0

Abstract

These Application Notes describe a solution comprised of the Avaya Communication Server 1000 release 7.5 and the Windstream SIP Trunking. During the interoperability testing, Avaya Communication Server 1000 was able to interoperate with the Windstream Metaswitch via SIP trunks. The Avaya Aura® Session Manager is used as a SIP routing and integration tool. It integrates all the SIP entities across the entire enterprise network within a company. The ACME Packet Net-Net 3800 Session Border Controller is used as an IP-IP network border between the enterprise and the service provider.

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.

Table of Contents

Table of Contents	2
1. Introduction.....	4
2. General Test Approach and Test Results.....	4
2.1. Interoperability Compliance Testing.....	4
2.2. Test Results	5
2.3. Support	6
3. Reference Configuration	7
4. Equipment and Software Validated	8
5. Avaya Communication Server 1000 Configuration	8
5.1. Login to Communication Server 1000 System	9
5.1.1. Login to Unified Communications Management (UCM) and Element Manager (EM)	9
5.1.2. Login to Call Server by using the Overlay Command Line Interface (CLI)	10
5.2. Administer a Node IP Telephony	11
5.2.1. Obtain Node IP address	11
5.2.2. Administer Terminal Proxy Server (TPS)	13
5.2.3. Administer Quality of Service (QoS)	14
5.2.4. Synchronize the New Configuration.....	14
5.3. Administer Voice Codec	15
5.3.1. Enable Voice Codec G711, Node IP Telephony.	15
5.3.2. Enable Voice Codec on Media Gateways.....	16
5.4. Zones and Bandwidth Management.....	17
5.4.1. Create a zone for IP phones (zone 10).....	17
5.4.2. Create a zone for virtual SIP trunk (zone 255)	18
5.5. Administer SIP Trunk Gateway	19
5.5.1. Integrated Services Digital Network (ISDN).....	19
5.5.2. Administer SIP Trunk Gateway to Avaya Aura® Session Manager.....	20
5.5.3. Administer Virtual D-Channel.....	22
5.5.4. Administer Virtual Super-Loop	25
5.5.5. Administer Virtual SIP Routes	26
5.5.6. Administer Virtual Trunks.....	29
5.5.7. Administer Calling Line Identification Entries.....	31
5.5.8. Enable External Trunk to Trunk Transferring	32
5.6. Administer Dialing Plans	33
5.6.1. Define ESN Access Codes and Parameters (ESN).....	33
5.6.2. Associate NPA and SPN call to ESN Access Code 2.....	34

5.6.3.	Digit Manipulation Block (DMI).....	35
5.6.4.	Digit Manipulation Block (DMI) for Outbound Call	35
5.6.5.	Route List Block (RLB) (RLB 14)	36
5.6.6.	Route List Block (RLB) (RLB 15)	38
5.6.7.	Inbound Call – Incoming Digit Translation Configuration	38
5.6.8.	Outbound Call - Special Number Configuration	40
5.6.9.	Outbound Call - Numbering Plan Area (NPA).....	41
5.7.	Administer Phone.....	42
5.7.1.	Phone creation.....	42
5.7.2.	Enable Privacy for Phone.....	43
5.7.3.	Enable Call Forward for Phone.....	44
5.7.4.	Enable Call Waiting for Phone	47
6.	Configure Avaya Aura® Session Manager	47
6.1.	System Manager Login and Navigation.....	48
6.2.	Specify SIP Domain	50
6.3.	Add Location.....	51
6.4.	Add SIP Entities	52
6.5.	Add Entity Links	56
6.6.	Add Routing Policies	57
6.7.	Add Dial Patterns	59
6.8.	Add/View Session Manager.....	65
7.	Configure Acme Packet Net-Net 3800	67
7.1.	Acme Packet Command Line Interface Summary	68
7.2.	Physical and Network Interfaces.....	68
7.3.	Realm	72
7.4.	Session Agent.....	73
7.5.	SIP Configuration.....	74
7.6.	SIP Interface.....	75
7.7.	SIP Manipulation.....	76
7.8.	Steering Pools.....	81
7.9.	Local Policy.....	81
8.	Verification Steps.....	83
8.1.	General	83
8.2.	Verification an Active Call on Call Server	83
8.3.	Protocol Trace	85
9.	Conclusion	86
10.	Additional References.....	87

1. Introduction

This document provides a typical network configuration deployment of the Avaya Communication Server 1000 and the Windstream SIP Trunking service Voice & Data bundle (hereafter referred to as Windstream system or Metaswitch). The Avaya Aura® Session Manager integrates all the SIP entities across the entire enterprise network within a company. The ACME Net-Net 3800 Session Border Controller is used as IP-IP network border between Windstream Metaswitch and Avaya Communication Server 1000.

2. General Test Approach and Test Results

The Avaya Communication Server 1000 system was connected to the ACME 3800 Session Border Controller via the Avaya Aura® Session Manager. Then the ACME 3800 was connected to the Windstream system via SIP. Various call types were made from the Communication Server 1000 to the Windstream system and vice versa to verify the interoperability.

2.1. Interoperability Compliance Testing

The focus of this testing is to verify that Communication Server 1000 can interoperate with the Windstream system. The following interoperability areas were covered:

- General call processing between Communication Server 1000 and Windstream systems including:
 - Codec/ptime (G.711 u-law / 20ms)
 - Hold/Retrieve on both ends
 - CLID displayed
 - Ring-back tone
 - Speech path
 - Dialing plan support
 - Advanced features (Call on Mute, Call Park, Call Waiting)
 - Abandoned Call
- Call redirection verification: all supported methods (blind transfer, consultative transfer, call forward, and conference) including CLID. Call redirection is performed from both ends
- Fax/Modem Pass Through is supported only with G.711
- DTMF in both directions
- SIP Transport UDP
- Thru dialing via the Communication Server 1000 Call Pilot
- Voice Mail Server Call Pilot (hosted on Avaya system)
- Early Media Transmission

The following assumptions were made for this lab test configuration:

1. Communication Server 1000 R7.5 software and implementation of latest patches
2. Windstream provides support to setup, configure and troubleshoot on carrier switch during testing execution.

During testing, the following activities were made to each test scenario:

1. Calls were checked for the correct call progress tones and cadences.
2. During the ringing state the ring back tone and destination ringing were checked.
3. Calls were checked in both hands-free and handset mode due to internal Avaya requirement.
4. Calls were checked for speech path in both directions using spoken words to ensure clarity of speech.
5. The display(s) of the sets/clients involved were checked for consistent and expected CLID and redirection information both prior to answer and after call establishment.
6. The speech path and messaging system were observed for timely and quality End to End tone audio path generation and application responses.
7. The call server maintenance terminal window was open during the test cases execution for the monitoring of BUG(s), ERR and AUD messages.
8. Speech path was checked before and after calls were put on/off hold from each end.
9. Applicable files were screened on an hourly basis during the testing for message that may indicate technical issues. This refers to Avaya Communication Server files.
10. Calls were checked to ensure that all resources such as Virtual trunks, TDM trunks, Sets and VGWs are released when a call scenario ends.

2.2. Test Results

The objectives outlined in the **Section 2.1** were verified. All the applicable test cases were executed. However, the following observations were noted during the compliance testing:

1. Call is made from Communication Server 1000 phone to a PSTN phone with CLID (Caller Identification) hidden. The call is being rejected with SIP error code 403 (URI not recognized) by the Windstream system (namely Metaswitch). Windstream team is investigating and providing the resolution.
2. Incoming calls from PSTN to Communication Server 1000, CLID number works intermittently. Windstream team is investigating and providing the resolution.
3. Call is made from Communication Server 1000 phone to a PSTN phone with CPND (call party name display) hidden. The call is established with 2 way speech path but the PSTN phone did not display the correct CPND of the caller. SIP Field Privacy is send ID, Metaswitch interprets as CPND private and sends. This is a design intended from Metaswitch.
4. Toll free number was not tested due to the Windstream lab environment does not provide this service.
5. The directory search number 411 service is tested with Windstream emulated 411 number where Communication Server 1000 sends and Windstream terminated as an assign mailbox number.
6. 911 emergency service is tested with Windstream emulated 911 number where Communication Server 1000 sends and Windstream terminated as an assign mailbox number.
7. Call from Communication Server 1000 phone that is programmed to reach PSTN Operator 0. This is not tested since Windstream lab environment does not have this service available.

8. Call from Communication Server 1000 phone that is programmed to reach PSTN Operator 0+10-digits. This is not applicable for Windstream, operator services are reached via Long Distance number 1-xxx-555-1212 to the area code you are wishing to lookup.
9. If the Communication Server 1000 phone holds/retrieves an outbound call, the dialed digits are no longer displayed. This is a Communication Server 1000 known issue.
10. PSTN1 phone calls to Communication Server 1000 phone, then phone does blind transfer to PSTN2 phone. PSTN 1 phone could not hear ringback tone from PSTN2 phone when Communication Server 1000 phone completed blind transfer. This is a limitation on Windstream because the system does not support UPDATE SIP message.

It was agreed with Windstream that the above observations were not severe enough to fail the testing.

2.3. Support

For technical support on Windstream system, please contact Windstream technical support at:

- Toll Free: 1-800-843-9214
- <http://www.windstreambusiness.com/support-center.html>

3. Reference Configuration

Figure 1 illustrates the test configuration used during the compliance testing event between the Communication Server 1000 and Windstream systems.

For confidentiality and privacy purposes, actual public IP addresses used in this testing have been masked out and replaced with fictitious IP addresses throughout the document.

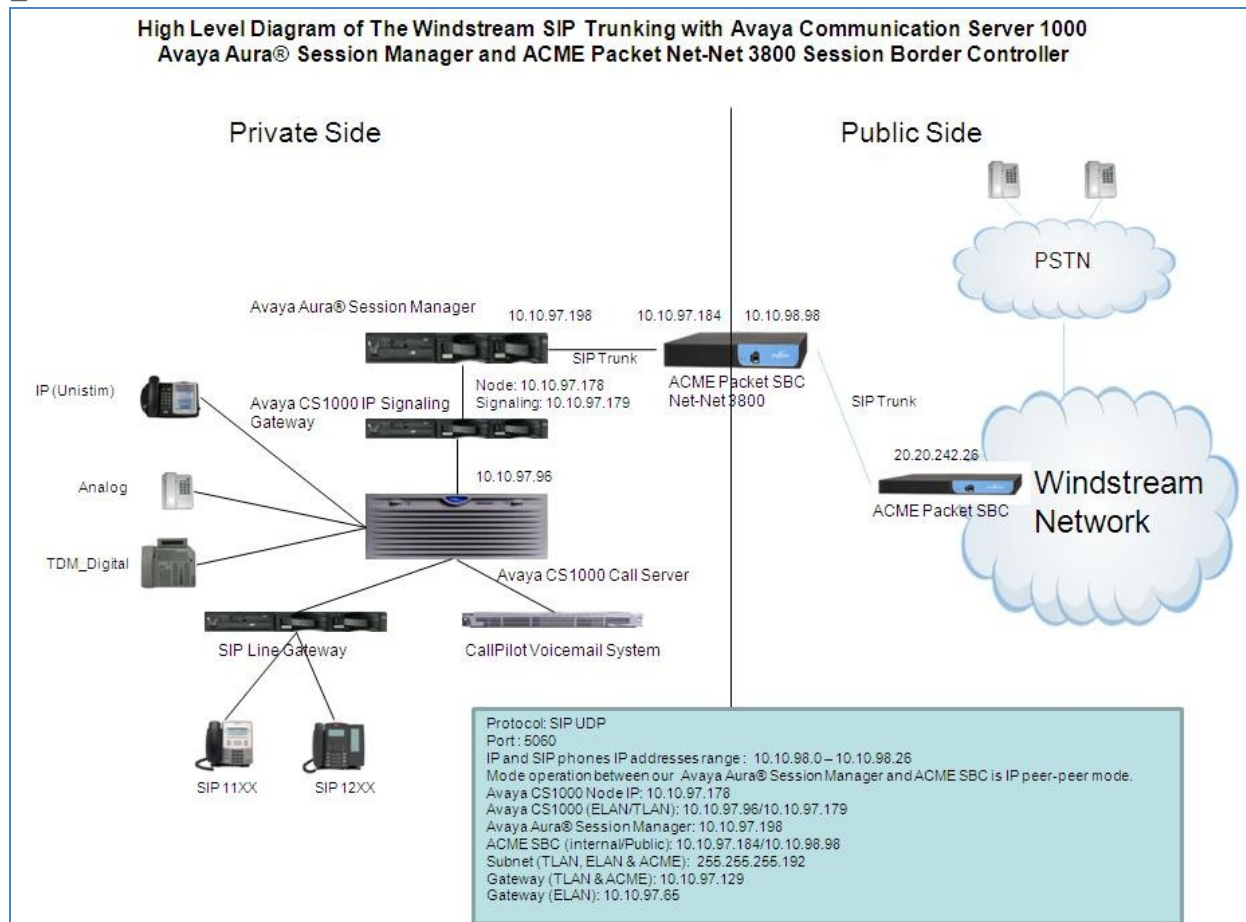


Figure 1- Network diagram for Avaya Communication Server 1000 and Windstream System

4. Equipment and Software Validated

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

Avaya system:

System	Software/Loadware version
Avaya Communication Server 1000 (CPPM)	<ul style="list-style-type: none">● Call Server: 750 Q+ GA● Signaling Server: 7.50.17 GA● SIP Line Server: 7.50.17 GA
Avaya Aura ®Session Manager	<ul style="list-style-type: none">● 6.1.1.0.611023
Avaya phones	<ul style="list-style-type: none">● 2002 p2: 0604DCN (Unistim)● 1140: 0625C8D (Unistim)● 1120: 0624C8D (Unistim)● 2007: 0621C8D (Unistim)● 1120: 4 1 13 0 (SIPLine)● 12xx: 4 1 13 0 (SIPLine)
ACME Net-Net 3800	<ul style="list-style-type: none">● Firmware SCX6.2.0 MR-4 Patch 3 (Build 754)

Windstream system:

System	Software/Loadware version
Metaswitch	<ul style="list-style-type: none">● Call Feature Server: V7.3.00 SU30 P90.00● Universal Media Gateway: V7.3.00 SU30 P86.00● Element Management System: 7V7.3.00 SU30 P86.00

Additional software and patch lineup for the configuration and active patch list on the SIP Signalling Gateway are listed as below:

Call Server: 7.50 Q+ GA plus latest DEPLIST – Deplists_CPL_X21_07_50Q.zip

SSG Server: 7.50.17 GA plus latest DEPLIST – Service_Pack_Linux_7.50_17_20110621.ntl

SLG Server: 7.50.17 GA plus latest DEPLIST – Service_Pack_Linux_7.50_17_20110621.ntl

5. Avaya Communication Server 1000 Configuration

These Application Notes used the Incoming Digit Translation feature to receive the calls and used the Numbering Plan Area Code (NPA), Special Number (SPN) features to route calls from the Avaya Communication Server 1000, over the Windstream SIP trunk to PSTN.

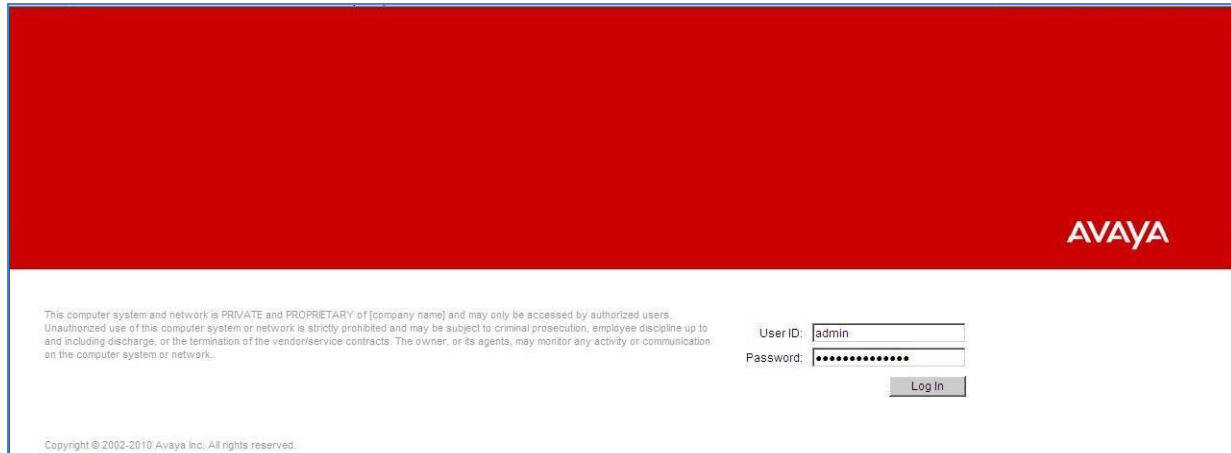
These application notes assume that the basic configuration has already been administered. For further information on Avaya Communications Server 1000, please consult the references in **Section 10**.

The below procedures describe the configuration details of Communication Server 1000 with a SIP trunk to the Windstream system.

5.1. Log in to Communication Server 1000 System

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

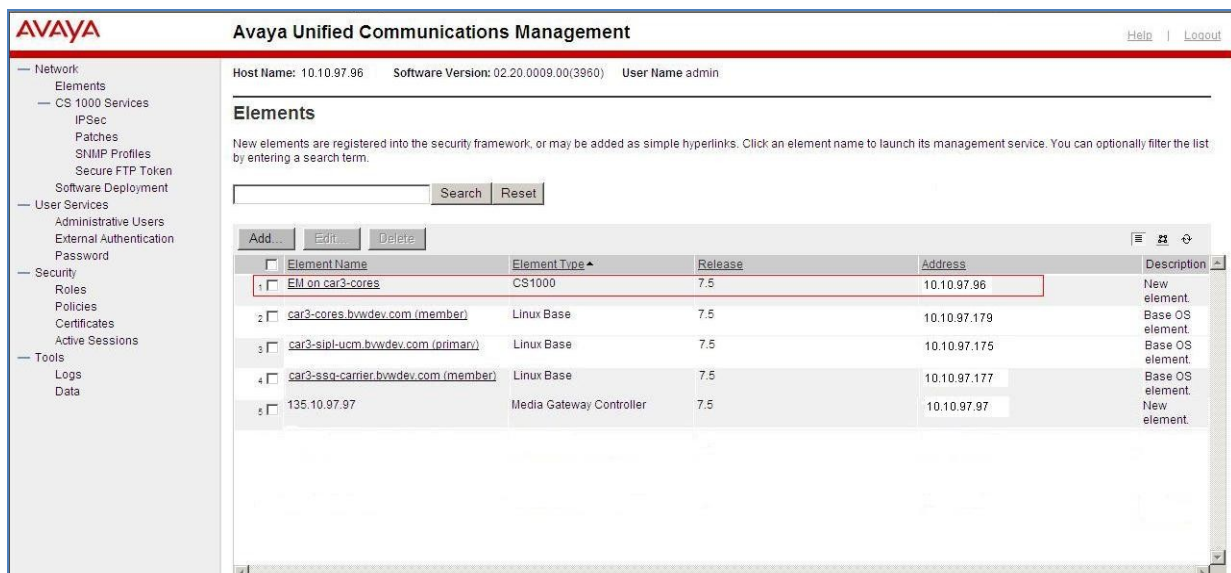
a) Open an instance of a web browser and connect to the UCM GUI at the following address: <http://<node IP address>> or <http://<UCM IP address>>. Log in using an appropriate User ID and Password.



The login screen features a red header with the AVAYA logo. Below the header is a disclaimer: "This computer system and network is PRIVATE and PROPRIETARY of (company name) and may only be accessed by authorized users. Unauthorized use of this computer system or network is strictly prohibited and may be subject to criminal prosecution, employee discipline up to and including discharge, or the termination of the vendor/service contracts. The owner, or its agents, may monitor any activity or communication on the computer system or network." To the right of the disclaimer are input fields for "User ID:" (containing "admin") and "Password:" (masked with dots). A "Log In" button is positioned below the password field. At the bottom left, the copyright notice "Copyright © 2002-2010 Avaya Inc. All rights reserved." is displayed.

Figure 2 – Login Unified Communications Management

b) The **Unified Communications Management** screen is displayed. Click on the **Element Name** of the Communication Server 1000 Element as highlighted in red box as shown in **Figure 3**.



The main screen displays the "Avaya Unified Communications Management" interface. It includes a left-hand navigation menu with categories like Network, CS 1000 Services, User Services, Security, and Tools. The main content area shows system information (Host Name: 10.10.97.96, Software Version: 02.20.0009.00(3960), User Name: admin) and an "Elements" section. Below this is a search bar and a table of elements. The first row of the table, "EM on car3-cores", is highlighted with a red border.

Element Name	Element Type	Release	Address	Description
EM on car3-cores	CS1000	7.5	10.10.97.96	New element.
car3-cores.bvwdev.com (member)	Linux Base	7.5	10.10.97.179	Base OS element.
car3-slp-ucm.bvwdev.com (primary)	Linux Base	7.5	10.10.97.175	Base OS element.
car3-ssn-carrier.bvwdev.com (member)	Linux Base	7.5	10.10.97.177	Base OS element.
135.10.97.97	Media Gateway Controller	7.5	10.10.97.97	New element.

Figure 3 – Unified Communications Management

c) The Communication Server 1000 Element Manager **System Overview** page is displayed as shown in **Figure 4**.

IP Address: 10.10.97.96
Type: Communication Server 1000E CPPM Linux
Version: 4121
Release: 7.50 Q+



Figure 4 – Element Manager System Overview

5.1.2. Log in to Call Server by using the Overlay Command Line Interface (CLI)

- Use Putty, SSH to connect to IP address of SSG Server with the admin account.
- Run the command “cslogin” and log in with the appropriate admin account and password.
- Here are the logs.

login as: **admin**

Nortel Networks Linux Base 7.50

The software and data stored on this system are the property of, or licensed to, Nortel Networks and are lawfully available only to authorized users for approved purposes. Unauthorized access to any software or data on this system is strictly prohibited and punishable under appropriate laws. If you are not an authorized user then do not try to login. This system may be monitored for operational purposes at any time.

admin@10.10.97.177's password: <----enter your password

Last login: Fri Jul 29 10:20:05 2011 from 10.10.98.78

[admin@car3-ssg-carrier ~]\$ cslogin

SEC054 A device has connected to, or disconnected from, a pseudo tty without authenticating
>login

USERID? admin

PASS? <----enter your password

.

TTY #08 LOGGED IN

The software and data stored on this system are the property of, or licensed to, Nortel Networks and are lawfully available only to authorized users for approved purposes. Unauthorized access to any software or data on this system is strictly prohibited and punishable under appropriate laws. If you are not an authorized user then log out immediately. This system may be monitored for operational purposes at any time.

ADMIN 12:56 29/7/2011

>

5.2. Administer a Node IP Telephony

This section describes how to configure a Node IP Telephony on the Communication Server 1000.

5.2.1. Obtain Node IP address

These application notes assume that the basic configuration has already been administered and that Node has already been created. This section describes the steps for configuring a Node (Node ID 3000) in Communication Server 1000 IP network to work with Windstream system. For further information on Avaya Communications Server 1000, please consult the references in **Section 10**.

a) Select **System -> IP Network -> Nodes: Servers, Media Cards** and then click on the Node ID as shown in **Figure 5**.



The screenshot shows the AVAYA CS1000 Element Manager web interface. The top navigation bar includes the AVAYA logo, the title 'CS1000 Element Manager', and links for 'Help' and 'Logout'. The left sidebar contains a tree view with categories like 'UCM Network Services', 'Home', 'Links', 'Virtual Terminals', 'System', 'Alarms', 'Maintenance', 'Core Equipment', 'Peripheral Equipment', 'IP Network', 'Nodes: Servers, Media Cards', 'Maintenance and Reports', 'Media Gateways', 'Zones', 'Host and Route Tables', and 'Network: Address Translation (N)'. The main content area is titled 'Managing: 10.10.97.96 Username: admin' and 'System > IP Network > IP Telephony Nodes'. Below this, there's a section for 'IP Telephony Nodes' with a sub-header 'Click the Node ID to view or edit its properties.' and buttons for 'Add', 'Import', 'Export', 'Delete', 'Print', and 'Refresh'. A table lists the nodes with columns for 'Node ID', 'Components', 'Enabled Applications', 'ELAN IP', 'Node/TLAN IPv4', 'Node/TLAN IPv6', and 'Status'. Two nodes are listed: Node ID 3000 (Components: 1, Enabled Applications: LTPS, Gateway (SIPGw), ELAN IP: -, Node/TLAN IPv4: 10.10.97.178, Node/TLAN IPv6: -, Status: Synchronized) and Node ID 3002 (Components: 1, Enabled Applications: SIP Line, LTPS, ELAN IP: -, Node/TLAN IPv4: 10.10.97.176, Node/TLAN IPv6: -, Status: Synchronized). At the bottom, there are checkboxes for 'Show: Nodes', 'Component servers and cards', and 'IPv6 address'.

Node ID	Components	Enabled Applications	ELAN IP	Node/TLAN IPv4	Node/TLAN IPv6	Status
3000	1	LTPS, Gateway (SIPGw)	-	10.10.97.178	-	Synchronized
3002	1	SIP Line, LTPS	-	10.10.97.176	-	Synchronized

Figure 5 – IP Telephony Nodes

b) The **Node Details** screen is displayed in **Figure 6**, **Figure 7** with the IP address of the Communication Server 1000 node. The **Node IP Address** is a virtual address which corresponds to the TLAN IP address of the Signaling Server, SIP Signaling Gateway. The SIP Signaling Gateway uses this **Node IP Address** to communicate with other components to process the SIP call.

AVAYA **CS1000 Element Manager** Help | Logout

Managing: **10.10.97.96** Username: admin
System > IP Network > IP Telephony Nodes > Node Details

Node Details (ID: 3000 - LTPS, Gateway (SIPGw))

Node ID: * (0-9999)

Call server IP address: TLAN address type: ☒ IPv4 only
☐ IPv4 and IPv6

Embedded LAN (ELAN) **Telephony LAN (TLAN)**

Gateway IP address: Node IPv4 address:

Subnet mask: Subnet mask:

Node IPv6 address:

* Required Value. Save Cancel

Associated Signaling Servers & Cards

Select to add Print | Refresh

Hostname	Type	Deployed Applications	ELAN IP	TLAN IPv4	Role
<input type="checkbox"/> car3-ssq-carrier	Signaling_Server	LTPS, Gateway, PD, Presence Publisher, IP Media Services	10.10.97.95	10.10.97.177	Leader

Show: ☐ IPv6 address

Note: Only server(s) that are not part of any other IP Telephony node and deployed application(s) that match the service(s) selected for this node are available in the servers list.

Figure 6 –Node Details

AVAYA **CS1000 Element Manager** Help | Logout

Managing: **10.10.97.96** Username: admin
System > IP Network > IP Telephony Nodes > Node Details

Node Details (ID: 3000 - LTPS, Gateway (SIPGw))

Subnet mask: Subnet mask:

Node IPv6 address:

IP Telephony Node Properties **Applications (click to edit configuration)**

- [Voice Gateway \(VGW\) and Coders](#)
- [Quality of Service \(QoS\)](#)
- [L3H](#)
- [SNTP](#)
- [Numbering Zones](#)
- [MCDN Alternative Routing Treatment \(MALT\) Causes](#)
- [SIP Line](#)
- [Terminal Proxy Server \(TPS\)](#)
- [Gateway \(SIPGw\)](#)
- [Personal Directories \(PD\)](#)
- [Presence Publisher](#)
- [IP Media Services](#)

* Required Value. Save Cancel

Associated Signaling Servers & Cards

Select to add Print | Refresh

Hostname	Type	Deployed Applications	ELAN IP	TLAN IPv4	Role
<input type="checkbox"/> car3-ssq-carrier	Signaling_Server	LTPS, Gateway, PD, Presence Publisher, IP Media Services	10.10.97.95	10.10.97.177	Leader

Show: ☐ IPv6 address

Note: Only server(s) that are not part of any other IP Telephony node and deployed application(s) that match the service(s) selected for this node are available in the servers list.

Figure 7 –Node Details

5.2.2. Administer Terminal Proxy Server (TPS)

c) Continue from **Section 5.2.1**. On the **Node Details** page, select the **Terminal Proxy Server (TPS)** link as shown in **Figure 7**.

d) Check the **UNISlim Line Terminal Proxy Server** check box and then click the **Save** button as shown in **Figure 8**.

The screenshot displays the AVAYA CS1000 Element Manager interface. The top bar shows the managing IP (10.10.97.96) and username (admin). The breadcrumb trail indicates the path: System > IP Network > IP Telephony Nodes > Node Details > UNISlim Line Terminal Proxy Server (LTPS) Configuration. The main title is 'Node ID: 3000 - UNISlim Line Terminal Proxy Server (LTPS) Configuration Details'. The left navigation pane lists various system components, with 'Nodes, Servers, Media Cards' selected. The main configuration area has tabs for 'Firmware', 'DTLS', and 'Network Connect Server'. The 'Firmware' tab is active, showing a checkbox for 'UNISlim Line Terminal Proxy Server' which is checked. Below this are input fields for 'IP address' (0.0.0.0), 'Full file path' (download/firwa), 'Server Account/User ID', and 'Password'. The 'DTLS' section shows a dropdown for 'DTLS policy' set to 'Off' and two unchecked options: 'Client authentication' and 'Periodic re-keying'. At the bottom, there is a 'Network Connect Server' field, a note about required values, and 'Save' and 'Cancel' buttons.

Figure 8 – TPS Configuration Details

5.2.3. Administer Quality of Service (QoS)

e) Continue from **Section 5.2.1**. On the **Node Details** page, select the **Quality of Service (QoS)** link as shown in **Figure 7**.

f) The default Diffserv values are as shown in **Figure 9**. Click on the **Save** button.

The screenshot shows the 'CS1000 Element Manager' interface. The top navigation bar includes the Avaya logo, the title 'CS1000 Element Manager', and a 'Help | Logout' link. The left sidebar contains a tree view of system components, with 'Nodes, Servers, Media Cards' selected. The main content area displays the 'Node ID: 3000 - Quality of Service (QoS)' configuration page. The page shows the following settings:

- Managing: 10.10.97.96 Username: admin
- System > IP Network > IP Telephony Nodes > Node Details > Quality of Service (QoS)
- Node ID: 3000 - Quality of Service (QoS)
- Diffserv Codepoint (DSCP) configuration box:
 - Enable Avaya automatic QoS: ☐
 - Control packets: 40 (0-63)
 - Voice packets: 40 (0-63)
 - VLAN tagging: ☐ 802.1Q support
 - 802.1Q bits value (802.1P): 6 (0-7)
- Buttons: Save, Cancel
- Footnote: * Required Value. Note: Changes made on this page will NOT be transmitted until the Node is also saved.

Figure 9 – QoS Configuration Details

5.2.4. Synchronize the New Configuration

g) Continue from **Section 5.2.3**, return to the **Node Details** page (**Figure 6**) and click on the **Save** button.

h) The **Node Saved** screen is displayed. Click on the **Transfer Now** (not shown).

i) The **Synchronize Configuration Files** screen is displayed. Check the **Signaling Server** check box and click on the **Start Sync** (not shown).

j) When the synchronization completes, check the **Signaling Server** check box and click on the **Restart Applications** (not shown)

5.3. Administer Voice Codec

5.3.1. Enable Voice Codec G711, Node IP Telephony.

- Select **IP Network -> Nodes: Servers, Media Cards** from the left pane, and in the **IP Telephony Nodes** screen displayed, select the **Node ID** of this Communication Server 1000 system. The **Node Details** screen is displayed. (See **Section 5.2.1** for more detail).
- On the **Node Details** page as shown in **Figure 7**, click on **Voice Gateway (VGW) and Codec**.
- The Windstream system only supports **G711,ptime 20ms with VAD disabled**. The Windstream system does not support G729 therefore the system ensures that the **Codec G729** and **Voice Activity Detection (VAD)** checkboxes are unchecked as shown in **Figure 10**. Then click on the **Save** button.

Figure 10 – Voice Gateway and Codec Configuration Details

- Synchronize the new configuration (please refer to **Section 5.2.4**)

5.3.2. Enable Voice Codec on Media Gateways.

- From the left menu of the Element Manager page in **Figure 10**, select **IP Network -> Media Gateways** menu item. The Media Gateways page will appear (not shown). Click on the **MGC** which is located on the right of the page.
- In the following screen scroll down to the **Codec G711** and uncheck **VAD**, ensure to uncheck Codec G729A as shown in **Figure 11**.

AVAYA CS1000 Element Manager Help | Logout

- UCM Network Services
- Home
- Links
- Virtual Terminals
- System
 - + Alarms
 - Maintenance
 - + Core Equipment
 - Peripheral Equipment
 - IP Network
 - Nodes: Servers, Media Cards
 - Maintenance and Reports
 - **Media Gateways**
 - Zones
 - Host and Route Tables
 - Network Address Translation (NAT)
 - QoS Thresholds
 - Personal Directories
 - Unicode Name Directory
 - + Interfaces
 - Engineered Values
 - + Emergency Services
 - + Geographic Redundancy
 - + Software
- Customers
- Routes and Trunks
 - Routes and Trunks
 - D-Channels
 - Digital Trunk Interface
- Dialing and Numbering Plans
 - Electronic Switched Network
 - Flexible Code Restriction
 - Incoming Digit Translation
- Phones
 - Templates
 - Reports
 - Views
 - Lists
 - Properties
 - Migration
- Tools
 - + Backup and Restore
 - Date and Time
 - + Logs and reports
- Security
 - + Passwords
 - + Policies
 - + Login Options

- VGW and IP phone codec profile

Enable echo canceller ☒

Echo canceller tail delay 128 (milliseconds)

Enable dynamic attenuation ☒

Voice activity detection threshold 1 (0 - 4 dBm)

Idle noise level 0 (0 - 1 dBm)

R factor calculation ☐

DTMF tone detection ☒

Enable low latency mode ☐

Remove DTMF delay (squelch DTMF from TDM to IP) ☒

Enable modem/fax pass through mode ☒

Enable V.21 FAX tone detection ☒

Fax TCF method 2

FAX maximum rate 14400 (bps)

FAX playout nominal delay 100 (0 - 300 milliseconds)

FAX no activity timeout 20 (10 - 32000 milliseconds)

FAX packet size 30

- Codec G711 Select ☒

Codec name G711

Voice payload size 20 (ms/frame)

Voice playout (jitter buffer) nominal delay 40

Modifications may cause changes to dependent settings

Voice playout (jitter buffer) maximum delay 80

Modifications may cause changes to dependent settings

VAD ☐

- Codec G729A Select ☐

Codec name G729A

Voice payload size 20 (ms/frame)

Voice playout (jitter buffer) nominal delay 40

Figure 11 – Media Gateways Configuration Details

- Then scroll down to the bottom of the page and click on the **Save** button.

5.4. Zones and Bandwidth Management

This section describes the steps to create 2 zones: zone 10 for VGW and IP sets, and zone 255 for SIP Trunk.

5.4.1. Create a zone for IP phones (zone 10)

The following figures show how to configure a zone for VGW and IP sets for bandwidth management purposes. The bandwidth strategy can be adjusted to preference.

a) Select **IP Network** -> **Zones** configuration from the left pane, click on the **Bandwidth Zones** as shown in **Figure 12**.

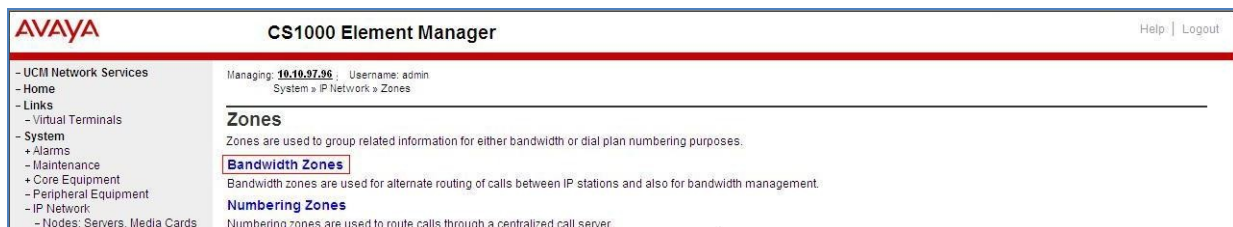


Figure 12 – Zones Page

b) The **Bandwidth Zones** screen is displayed as shown in **Figure 13**. Click **ADD** to create new zone for IP Phones.

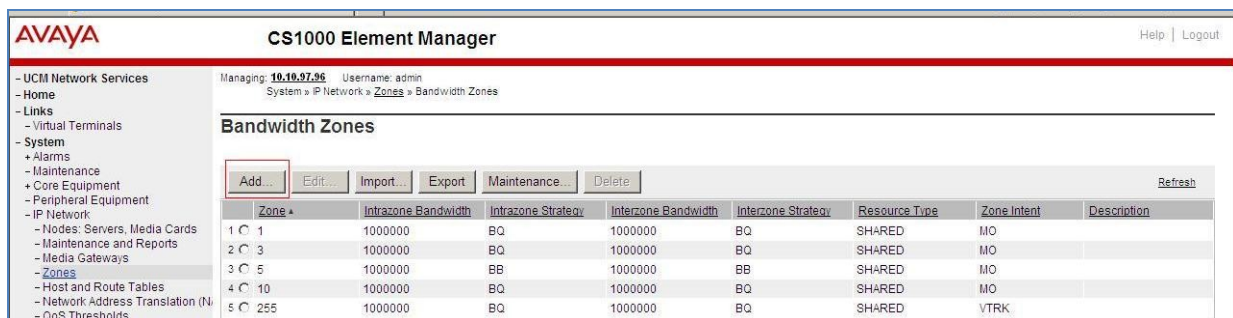


Figure 13 – Bandwidth Zones

c) Select the values as shown (in red box) in **Figure 14** and click on the **Submit** button.

- INTRA_STGY: Codec configuration for local calls.
- INTER_STGY: Codec configuration for the calls over trunk.
- BQ: G711 is first choice and G729 is second choice.
- BB: G729 is first choice and G711 is second choice.
- MO: is used for IP phones, VGWetc
- VTRK: is used for virtual trunk.

AVAYA CS1000 Element Manager

Managing: 10.10.97.96 Username: admin
System » IP Network » Zones » Bandwidth Zones » Bandwidth Zones 10 » Edit Bandwidth Zone » Zone Basic Property and Bandwidth Management

Zone Basic Property and Bandwidth Management

Input Description	Input Value
Zone Number (ZONE):	10 (1 - 8000)
Intrazone Bandwidth (INTRA_BW):	1000000 (0 - 100000000)
Intrazone Strategy (INTRA_STGY):	Best Quality (BQ)
Interzone Bandwidth (INTER_BW):	1000000 (0 - 100000000)
Interzone Strategy (INTER_STGY):	Best Quality (BQ)
Resource Type (RES_TYPE):	Shared (SHARED)
Zone Intent (ZBRN):	MO (MO)
Description (ZDES):	

Submit Refresh Cancel

Figure 14 –Bandwidth Management Configuration Details – IP phone

5.4.2. Create a zone for virtual SIP trunk (zone 255)

Follow **Section 5.4.1** to create a zone for the virtual trunk. The difference is in **Zone Intent (ZBRN)** field. Select **VTRK** for virtual trunk as shown in **Figure 15** and then click on the **Submit** button.

AVAYA CS1000 Element Manager

Managing: 10.10.97.96 Username: admin
System » IP Network » Zones » Bandwidth Zones » Bandwidth Zones 255 » Edit Bandwidth Zone » Zone Basic Property and Bandwidth Management

Zone Basic Property and Bandwidth Management

Input Description	Input Value
Zone Number (ZONE):	255 (1 - 8000)
Intrazone Bandwidth (INTRA_BW):	1000000 (0 - 100000000)
Intrazone Strategy (INTRA_STGY):	Best Quality (BQ)
Interzone Bandwidth (INTER_BW):	1000000 (0 - 100000000)
Interzone Strategy (INTER_STGY):	Best Quality (BQ)
Resource Type (RES_TYPE):	Shared (SHARED)
Zone Intent (ZBRN):	VTRK (VTRK)
Description (ZDES):	

Submit Refresh Cancel

Figure 15 –Bandwidth Management Configuration Details –virtual SIP trunk

5.5. Administer SIP Trunk Gateway

This section describes the steps for establishing a SIP connection between SIP Signaling Gateway (SSG) to Avaya Aura® Session Manager.

5.5.1. Integrated Services Digital Network (ISDN)

- Select **Customers** in the left pane. The **Customers** screen is displayed. Click on the link associated with the appropriate customer, in this case **00**. The system can support more than one customer with different network settings and options. The **Customer 00 Edit** page will appear (not shown). Select the **Feature Packages** option from this page.
- The screen is updated with a listing of feature packages populated below **Feature Packages** (not all features shown in **Figure 16** below). Select **Integrated Services Digital Network** to edit its parameters. The screen is updated with parameters populated below **Integrated Services Digital Network**. Click on **Integrated Services Digital Network (ISDN)**, and retain the default values for all remaining fields. Scroll down to the bottom of the screen, and click on the **Save** button at the bottom of the page (not shown).

Figure 16 –Customer – ISDN Configuration

5.5.2. Administer SIP Trunk Gateway to Avaya Aura® Session Manager

- Select **IP Network -> Nodes: Servers, Media Cards** configuration from the left pane, and in the **IP Telephony Nodes** screen displayed, select the **Node ID** of this Communication Server 1000 system. The **Node Details** screen is displayed as shown in **Figure 7, Section 5.2.1**.
- On the **Node Details** screen, select **SIP Gateway (SIPGw)**.
- Under **General** tab of the **Virtual Trunk Gateway Configuration Details** screen, enter the following values (highlighted in red boxes) for the specified fields, and retain the default values for the remaining fields as shown in **Figure 17**. The parameters (highlighted in red boxes) are filled in. The **SIP domain name** and **Local SIP port** should be matched in Avaya Aura® Session Manager configuration.

The screenshot displays the Avaya CS1000 Element Manager interface. The left sidebar shows a navigation tree with categories like UCM Network Services, Home, Links, Virtual Terminals, System, Alarms, Maintenance, Core Equipment, Peripheral Equipment, IP Network, Nodes: Servers, Media Cards, Maintenance and Reports, Media Gateways, Zones, Host and Route Tables, Network Address Translation (NAT), QoS Thresholds, Personal Directories, Unicode Name Directory, Interfaces, Engineered Values, Emergency Services, Geographic Redundancy, Software, Customers, Routes and Trunks, Routes and Trunks, D-Channels, Digital Trunk Interface, and Dialing and Numbering Plans. The main content area is titled 'Node ID: 3000 - Virtual Trunk Gateway Configuration Details'. It features a breadcrumb trail: 'System > IP Network > IP Telephony Nodes > Node Details > Virtual Trunk Gateway Configuration'. The 'General' tab is active, showing a 'Vtrk gateway application' dropdown set to 'SIP Gateway (SIPGw)'. Below this, the 'SIP domain name' is 'bwddev75.com', 'Local SIP port' is '5060', 'Gateway endpoint name' is 'car3-ssg-carrier', and 'Application node ID' is '3000'. A checkbox for 'Enable gateway service on this node' is checked. The 'Virtual Trunk Network Health Monitor' section includes a checkbox for 'Monitor IP addresses (listed below)' and a list of 'Monitor addresses' with 'Add' and 'Remove' buttons. A note at the bottom states: 'Note: Changes made on this page will NOT be transmitted until the Node is also saved.' There are 'Save' and 'Cancel' buttons at the bottom right.

Figure 17 – Virtual Trunk Gateway Configuration Details

d) Click on the **SIP Gateway Settings** tab, under **Proxy or Redirect Server**, enter the following values (highlighted in red boxes) for the specified fields, and retain the default values for the remaining fields as shown in **Figure 18**. Enter **Primary TLAN IP address** as the IP address of Avaya Aura® Session Manager signaling interface.

AVAYA CS1000 Element Manager

Managing: 10.10.97.96 Username: admin

System > IP Network > IP Telephony Nodes > Node Details > Virtual Trunk Gateway Configuration

Node ID: 3000 - Virtual Trunk Gateway Configuration Details

General | SIP Gateway Settings | SIP Gateway Services

Proxy Or Redirect Server:

Proxy Server Route 1:

Primary TLAN IP address: 10.10.97.198
The IP address can have either IPv4 or IPv6 format based on the value of "TLAN address type"

Port: 5060 (1 - 65535)

Transport protocol: UDP

Options: ☒ Support registration
☐ Primary CDS proxy

Secondary TLAN IP address: 0.0.0.0
The IP address can have either IPv4 or IPv6 format based on the value of "TLAN address type"

Port: 5060 (1 - 65535)

Transport protocol: TCP

* Required Value. Note: Changes made on this page will NOT be transmitted until the Node is also saved. Save Cancel

Figure 18 – Virtual Trunk Gateway Configuration Details

e) On the same page as shown in **Figure 18**, scroll down the parameters box to the **SIP URI Map** section.

Under the **Public E.164 Domain Names**, for:

- **National**: leave this SIP URI field as blank
- **Subscriber**: leave this SIP URI field as blank
- **Special Number**: leave this SIP URI field as blank
- **Unknown**: leave this SIP URI field as blank

Under the **Private domain names**, for:

- **UDP**: leave this SIP URI field as blank
- **CDP**: leave this SIP URI field as blank
- **Special Number**: leave this SIP URI field as blank
- **Vacant number**: leave this SIP URI field as blank
- **Unknown**: leave this SIP URI field as blank

The remaining fields can be left at their default values as shown in **Figure 19**. Then click on the **Save** button.

Figure 19 – Virtual Trunk Gateway Configuration Details

f) **Synchronize** the new sip configuration (please refer to **Section 5.2.4**).

5.5.3. Administer Virtual D-Channel

a) Select **Routes and Trunks -> D-Channels** from the left pane to display the **D-Channels** screen. In the **Choose a D-Channel Number** field, select an available D-channel from the drop-down list as shown in **Figure 20**. Click the **to Add** button.

Figure 20 – D-Channels

b) The D-Channels 100 Property Configuration screen is displayed next as shown in **Figure 21**. Enter the following values for the specified fields, and retain the default values for the remaining fields.

- **D channel Card Type (CTYP):** D-Channel is over IP (DCIP)
- **Designator (DES):** A descriptive name
- **Interface type for D-channel (IFC):** Meridian Meridian1 (SL1)
- **Release ID of the switch at the far end (RLS):** 25

c) Click on the **Advanced options (ADVOPT)**, check on the **Network Attendant Service Allowed** check box as shown in **Figure 21**. Other fields are left as default.

Figure 21 – D-Channels Configuration Details

d) Click on the **Basic Options** and click on the **Edit** button at the **Remote Capabilities (RCAP)** attribute. The **Remote Capabilities Configuration** page will appear. Then check on the **ND2** and the **MWI** checkboxes as shown in **Figures 22 and 23**.

AVAYA

CS1000 Element Manager

Help | Logout

- UCM Network Services
- Home
- Links
- Virtual Terminals
- System
 - + Alarms
 - Maintenance
 - + Core Equipment
 - Peripheral Equipment
 - IP Network
 - Nodes: Servers, Media Cards
 - Maintenance and Reports
 - Media Gateways
 - Zones
 - Host and Route Tables
 - Network Address Translation (NAT)
 - QoS Thresholds
 - Personal Directories
 - Unicode Name Directory
 - + Interfaces
 - Engineered Values
 - + Emergency Services
 - + Geographic Redundancy
 - + Software
- Customers
 - Routes and Trunks
 - Routes and Trunks
 - D-Channels
 - Digital Trunk Interface
- Dialing and Numbering Plans
 - Electronic Switched Network
 - Flexible Code Restriction
 - Incoming Digit Translation
- Phones
 - Templates
 - Reports
 - Views
 - Lists
 - Properties
 - Migration
- Tools
 - + Backup and Restore
 - Date and Time
 - + Logs and reports
- Security
 - + Passwords
 - + Policies
 - + Login Options

Action Device And Number (ADAN): DCH

D channel Card Type: DCIP

Designator: VoIP

Recovery to Primary: ☐

PRI loop number for Backup D-channel:

User: Integrated Services Signaling Link Dedicated (ISLD)

Interface type for D-channel: Meridian Meridian 1 (SL1)

Country: ETS 300 =102 basic protocol (ETSI)

D-Channel PRI loop number:

Primary Rate Interface: [more PRI](#)

Secondary PRI2 loops:

Meridian 1 node type: Slave to the controller (USR)

Release ID of the switch at the far end: 25

Central Office switch type: 100% compatible with Bellcore standard (STD)

Integrated Services Signaling Link Maximum: 4000 Range: 1 - 4000

Signalling server resource capacity: 1800 Range: 0 - 3700

Primary D-channel for a backup DCH: Range: 0 - 254

- PINX customer number:

- Progress signal:

- Calling Line Identification:

- Output request Buffers: 32

- D-channel transmission Rate: 56 kb/s when LCMT is AMI (56K)

- Channel Negotiation option: No alternative acceptable, exclusive, (1)

- Remote Capabilities: [Edit](#)

- B channel Service messaging: ☐

- Basic options (BSCOPT)

+ - Change protocol timer value (TIMR)

+ Advanced options (ADVOPT)

+ Feature Packages

Submit

Refresh

Delete

Cancel

Copyright © 2002-2011 Avaya Inc. All rights reserved.

Figure 22 – D-Channel Configuration Details

Managing: 10.10.97.96 Username: admin
Routes and Trunks > D-Channels > D-Channels 100 Property Configuration > Remote Capabilities Configuration

Remote Capabilities Configuration

Input Description	Input Value
Basic rate interface (BRI)	<input type="checkbox"/>
Call completion on busy using integer value (CCBI)	<input type="checkbox"/>
Call completion on busy using object identifier (CCBO)	<input type="checkbox"/>
Call completion on busy for QSIG and EuroISDN BRI (CCBS)	<input type="checkbox"/>
Call completion on no response using integer value (CCNI)	<input type="checkbox"/>
Call completion on no response using object identifier (CCNO)	<input type="checkbox"/>
Call completion to no reply for QSIG and EuroISDN BRI (CCNR)	<input type="checkbox"/>
Network call park (CPK)	<input type="checkbox"/>
Connected line identification presentation (COLP)	<input type="checkbox"/>
Call transfer integer (CTI)	<input type="checkbox"/>
Call transfer object (CTO)	<input type="checkbox"/>
Diversion info. is sent using integer value (DV1I)	<input type="checkbox"/>
Diversion info. is sent using object identifier (DV1O)	<input type="checkbox"/>
Rerouting requests processed using integer value (DV2I)	<input type="checkbox"/>
Rerouting requests processed using object identifier (DV2O)	<input type="checkbox"/>
Diversion info. sent. rerouting requests processed (DV3I)	<input type="checkbox"/>
EuroISDN - div. info sent. rerouting req. processed (DV3O)	<input type="checkbox"/>
Call transfer notification and invocation to EuroISDN (ECTO)	<input type="checkbox"/>
Malicious call identification (MCID)	<input type="checkbox"/>
MCDN QSIG conversion (MQC)	<input type="checkbox"/>
Remote D-channel is on a MSDL card (MSL)	<input type="checkbox"/>
Message waiting interworking with DMS-100 (MWI)	<input checked="" type="checkbox"/>
Network access data (NAC)	<input type="checkbox"/>
Network call trace supported (NCT)	<input type="checkbox"/>
Network name display method 1 (ND1)	<input type="checkbox"/>
Network name display method 2 (ND2)	<input checked="" type="checkbox"/>
Network name display method 3 (ND3)	<input type="checkbox"/>
Name display - integer ID coding (NDI)	<input type="checkbox"/>
Name display - object ID coding (NDO)	<input type="checkbox"/>

Copyright © 2002-2011 Avaya Inc. All rights reserved.

Figure 23 – Remote Capabilities Configuration Details

- e) Click on the **Return – Remote Capabilities** button (not shown).
f) Click on the **Submit** button (not shown).

5.5.4. Administer Virtual Super-Loop

Select **System -> Core Equipments -> Superloops** from the left pane to display the **Superloops** screen. If the Superloop does not exist, please click the “**Add**” button to create a new one as shown in **Figure 24**. In this example, superloop 4, 96, 100 and 124 have been added and are being used.

Managing: 10.10.97.96 Username: admin
System > Core Equipment > Superloops

Superloops

Superloop Number	Superloop Type
1 C 4	IPMG
2 C 96	Virtual
3 C 100	Virtual
4 C 104	Virtual
5 C 124	Virtual

Figure 24 – Administer Virtual Super-Loop Page

5.5.5. Administer Virtual SIP Routes

a) Select **Routes and Trunks** -> **Routes and Trunks** from the left pane to display the **Routes and Trunks** screen. In this example, **Customer 0** is being used. Click on the **Add route** button as shown in **Figure 25**.

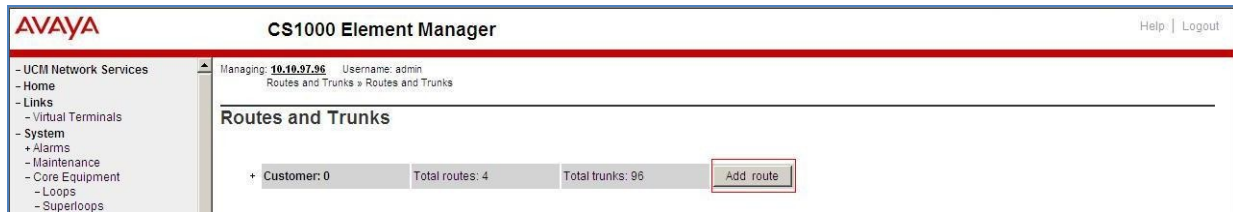


Figure 25 – Add route

b) The **Customer 0**, **New Route Configuration** screen is displayed next. Scroll down until the **Basic Configuration** Section is displayed and enter the following values for the specified fields, and retain the default values for the remaining fields as shown in **Figures 26**.

- **Route Number (ROUT)**: Select an available route number.
- **Designator field for trunk (DES)**: A descriptive text.
- **Trunk Type (TKTP)**: TIE trunk data block (TIE)
- **Incoming and Outgoing trunk (ICOG)**: Incoming and Outgoing (IAO)
- **Access Code for the trunk route (ACOD)**: An available access code.
- Check the field **The route is for a virtual trunk route (VTRK)**, to enable four additional fields to appear.
- For the **Zone for codec selection and bandwidth management (ZONE)** field, enter 255 (created in **Section 5.4.2**).
- For the **Node ID of signaling server of this route (NODE)** field, enter the node number 3000 (created in **Section 5.2.1**).
- Select **SIP (SIP)** from the drop-down list for the **Protocol ID for the route (PCID)** field.
- Check the **Integrated Services Digital Network option (ISDN)** checkbox to enable additional fields to appear. Enter the following values for the specified fields, and retain the default values for the remaining fields. Scroll down to the bottom of the screen.
 - o **Mode of operation (MODE)**: Route uses ISDN Signalling Link (ISLD)
 - o **D channel number (DCH)**: D-Channel number 100 (created in **Section 5.5.3**)
 - o **Network calling name allowed (NCNA)**: Check the field.
 - o **Network call redirection (NCRD)**: Check the field.
 - o **Insert ESN access code (INAC)**: Check the field.

AVAYA **CS1000 Element Manager** Help | Logout

Managing: **10.10.97.95** Username: admin
 Routes and Trunks » Routes and Trunks » Customer 0, Route 100 Property Configuration

Customer 0, Route 100 Property Configuration

- Basic Configuration

Route data block (RDB) (TYPE):
 Customer number (CUST):
 Route number (ROUT):
 Designator field for trunk (DES):
 Trunk type (TKTP):
 Incoming and outgoing trunk (ICOG):
 Access code for the trunk route (ACOD):

Trunk type M911P (M911P): ☐
 The route is for a virtual trunk route (VTRK): ☒
 - Zone for codec selection and bandwidth management (ZONE): (0 - 8000)
 - Node ID of signaling server of this route (NODE): (0 - 9999)
 - Protocol ID for the route (PCID):
 - Print correlation ID in CDR for the route (CRID): ☐

Integrated services digital network option (ISDN): ☒
 - Mode of operation (MODE):
 - D channel number (DCH): (0 - 254)
 - Interface type for route (IFC):
 - Private network identifier (PNI): (0 - 32700)
 - Network calling name allowed (NCNA): ☒
 - Network call redirection (NCRD): ☒
 - Trunk route optimization (TRO): ☐

- Recognition of DTI2 ABCD FALT signal for ISL (FALT): ☐
 - Channel type (CHTY):
 - Call type for outgoing direct dialed TIE route (CTYP):

- Insert ESN access code (IHAC): ☒

Copyright © 2002-2011 Avaya Inc. All rights reserved.

Figure 26 – Route Configuration Details

- Click on **Basic Route Options**, check the **North American toll scheme (NATL)** and **Incoming DID digit conversion on this route (IDC)**, input **DCNO 1** for both **Day IDC Tree Number** and **Night IDC Tree Number** as shown in **Figure 27**.

AVAYA

CS1000 Element Manager

Help | Logout

- UCM Network Services
- Home
- Links
 - Virtual Terminals
- System
 - + Alarms
 - Maintenance
 - Core Equipment
 - Loops
 - Superloops
 - MSDLMISP Cards
 - Conference/TDS/Multifrequen
 - Tone Senders and Detectors
 - Peripheral Equipment
 - IP Network
 - Nodes: Servers, Media Cards
 - Maintenance and Reports
 - Media Gateways
 - Zones
 - Host and Route Tables
 - Network Address Translation
 - QoS Thresholds
 - Personal Directories
 - Unicode Name Directory
 - + Interfaces
 - Engineered Values
 - + Emergency Services
 - + Geographic Redundancy
 - + Software
- Customers
 - Routes and Trunks
 - Routes and Trunks
 - D-Channels
 - Digital Trunk Interface
 - Dialing and Numbering Plans
 - Electronic Switched Network
 - Flexible Code Restriction
 - Incoming Digit Translation
 - Phones
 - Templates
 - Reports
 - Views
 - Lists
 - Properties
 - Migration
 - Tools
 - + Backup and Restore
 - Date and Time
 - + Logs and reports
 - Security
 - + Passwords
 - + Policies

- Mobile extension timer (MBXT): (0 - 8000 milliseconds)

Calling number dialing plan (CNDP):

- Basic Route Options

Attendant announcement (ATAI):

Billing number required (BILN): ☐

Call detail recording (CDR): ☒

- CDR records generated on incoming calls (INC): ☒

- CDR record printing content option for redirected calls (LAST): ☒

- Time to answer output in CDR (TTA): ☐

- CDR ACD Q initial connection records to be generated (QREC): ☒

- CDR on outgoing calls (OAL): ☒

- CDR on outgoing toll calls (OTL): ☐

- Answered call identification allowed (AIA): ☒

- CDR timing starts on answer supervision of outgoing calls (OAN): ☒

- outpulsed digits in CDR (OPD): ☒

- Number of digits printed (NDP):

North American toll scheme (NATL): ☒

Controls or timers (CNTL): ☐

Conventional (Tie trunk only) (CNVT): ☐

Incoming DID digit conversion on this route (IDC): ☒

- Day IDC tree number (DCNO): (0 - 254)

- Night IDC tree number (NDNO): (0 - 254)

- Display external dialed digits (DEXT): ☐

Multifrequency compelled or MFC signaling (MFC):

Process notification networked calls (PNNC): ☐

+ Network Options

+ General Options

+ Advanced Configurations

Submit

Refresh

Delete

Cancel

Copyright © 2002-2011 Avaya Inc. All rights reserved.

Figure 27 – Route Configuration Details

c) Click on the **Submit** button.

HV; Reviewed:
SPOC 9/22/2011

Solution & Interoperability Test Lab Application Notes
©2011 Avaya Inc. All Rights Reserved.

28 of 88
WCS1K75SMACME

5.5.6. Administer Virtual Trunks

a) From the EM, select **Routes and Trunks** -> **Route and Trunks**, the Route list is now updated with the newly added route. In the example, the Route 100 was being added. Click on the **Add trunk** button next to the newly added route 100 as shown in **Figure 28**.

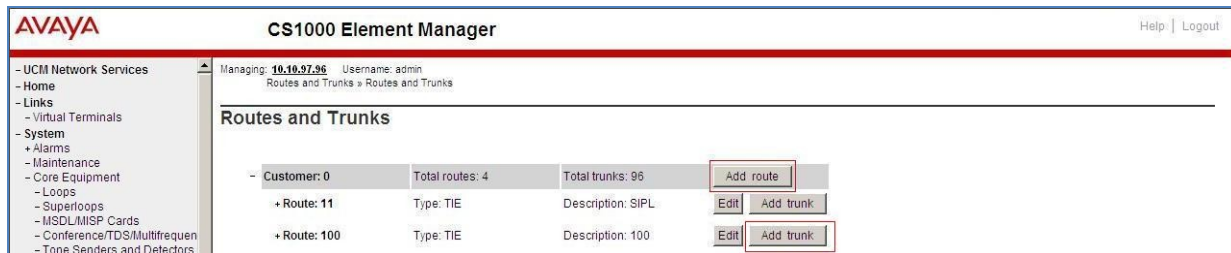


Figure 28 – Route and Trunks Page

b) The **Customer 0, Route 100, Trunk 1 Property Configuration** screen is displayed. Enter the following values for the specified fields and retain the default values for the remaining fields. The Media Security (sRTP) needs to be disabled at the trunk level by editing the **Class of Service** (CLS) at the bottom of the basic trunk configuration page. Click on the **Edit** button as shown in **Figure 29**.

- The Multiple trunk input number (**MTINPUT**) field may be used to add multiple trunks in a single operation, or repeat the operation for each trunk. In the sample configuration, 32 trunks were created.
- Trunk data block (**TYPE**): IP Trunk (IPTI)
- Terminal Number (**TN**): Available terminal number (created in **Section 5.5.4**)
- Designator field for trunk (**DES**): A descriptive text
- Extended Trunk (**XTRK**): Virtual trunk (VTRK)
- Route number, Member number (**RTMB**): Current route number and starting member
- Card Density: 8D
- Start arrangement Incoming (**STRI**): IMM
- Start arrangement Outgoing (**STRO**): IMM
- Trunk Group Access Restriction (**TGAR**): Desired trunk group access restriction level
- Channel ID for this trunk (**CHID**): An available starting channel ID

Figure 29 – New Trunk Configuration Details

c) For **Media Security**, select **Media Security Never (MSNV)**. Enter the remaining values for the specified fields as shown in **Figure 30**. Scroll down to the bottom of the screen and click **Return Class of Service** and then click on the **Save** button (not shown)

Input Description	Input Value
- ACD Priority:	ACD Priority not required (APN)
- Analog Semi-Permanent Connections:	Analog Semi-Permanent Connections Denied (SPCD)
- ARF Supervised COT:	
- Barring:	
- Battery Supervised COT:	
- Busy Tone Supervised COT:	
- Calling Line Identification:	
- Calling party:	Calling party Denied (CND)
- Central Office Ringback:	
- Centrex Switchhook Flash:	Centrex Switchhook Flash Denied (THFD)
- Dial Pulse:	Digitone (DTN)
- DTR PAD value:	
- Echo Canceling:	Echo Canceling Denied (ECD)
- Hong Kong DTI:	
- Loop Break Supervised COT:	
- Make-break ratio for dial pulse:	10 pulses per second (P10)
- Manual Incoming:	Manual Incoming Denied (MID)
- Media Security:	Media Security Never (MSNV)
- Network Hook Flash Over M911P:	
- Polarity:	
- Priority:	Low Priority (LPR)
- Restriction level:	Unrestricted (UNR)
- Reversed Ear Piece:	Reversed Ear Piece denied (XREP)
- Short or long line:	
- Transmission Class of Service:	Non-Transmission Compensated (NTC)
- Warning Tone:	Warning Tone Allowed (WTA)
- Reversed Ear Piece:	Reversed Ear Piece denied (XREP)
- ARF Supervised COT:	

Figure 30 – Class of Service Configuration Details Page

5.5.7. Administer Calling Line Identification Entries

a) Select **Customers** -> **00** -> **ISDN and ESN Networking**. Click on **Calling Line Identification Entries** as shown in Figure 31.

Figure 31 – ISDN and ESN Networking

b) Click on **Add** as shown in Figure 32.

Figure 32 – Calling Line Identification Entries

c) Add entry **0** as shown in Figure 33:

- **National Code**: leave as blank

- **Local Code**: input prefix digits assigned by Service Provider, in this case it is 6 digits – 501287. This **Local Code** will be used for call display purpose of outbound international

call configuration in **Section 5.6.6** in which the **Special Number 011** is associated with Call Type = Unknown.

- **Home Location Code:** input prefix digits assigned by Service Provider, in this case it is 6 digits - 501287. This **Home Location Code** will be used for call display purpose for Call Type = National (NPA).

- **Local Steering Code:** input prefix digits assigned by Service Provider, in this case it is 6 digits - 501287. This **Local Steering Code** will be used for call display purpose for Call Type = Local Subscriber (NXX).

- **Calling Party Name Display:** Uncheck for **Roman characters**.

d) Click on the **Save** button as shown in **Figure 33**.

The screenshot shows the AVAYA CS1000 Element Manager interface. The left sidebar contains a navigation tree with categories like UCM Network Services, Links, System, IP Network, and Customers. The main content area is titled 'Edit Calling Line Identification 0'. It features three main sections: 'General Properties' with input fields for National Code, Local Code, Home Location Code, and Local Steering Code (all set to 501287); 'Emergency Services Access' with checkboxes for emergency services access and directory number appending; and 'Calling Party Name Display' with a checkbox for Roman characters and a CPND Name field. At the bottom right, there are 'Save' and 'Cancel' buttons.

Figure 33 – Edit Calling Line Identification 0

5.5.8. Enable External Trunk to Trunk Transferring

This section shows how to enable External Trunk to Trunk Transferring feature which is a mandatory configuration to make call transfer and conference work properly over SIP trunk.

a) Login Call Server Overlay CLI (please refer to **Section 5.1.2** for more detail)

b) Allow External Trunk to Trunk Transferring for Customer Data Block by using **LD 15**

```
>ld 15
CDB000
MEM AVAIL: (U/P): 33600126   USED U P: 8345621 954062   TOT: 45579868
```

DISK SPACE NEEDED: 1722 KBYTES

REQ: chg

TYPE: net

TYPE NET_DATA

CUST 0

OPT

...

TRNX YES

EXTT YES

...

5.6. Administer Dialing Plans

5.6.1. Define ESN Access Codes and Parameters (ESN)

a) Select **Dialing and Numbering Plans -> Electronic Switched Network** from the left pane to display the **Electronic Switched Network (ESN)** screen as shown in **Figure 34**.

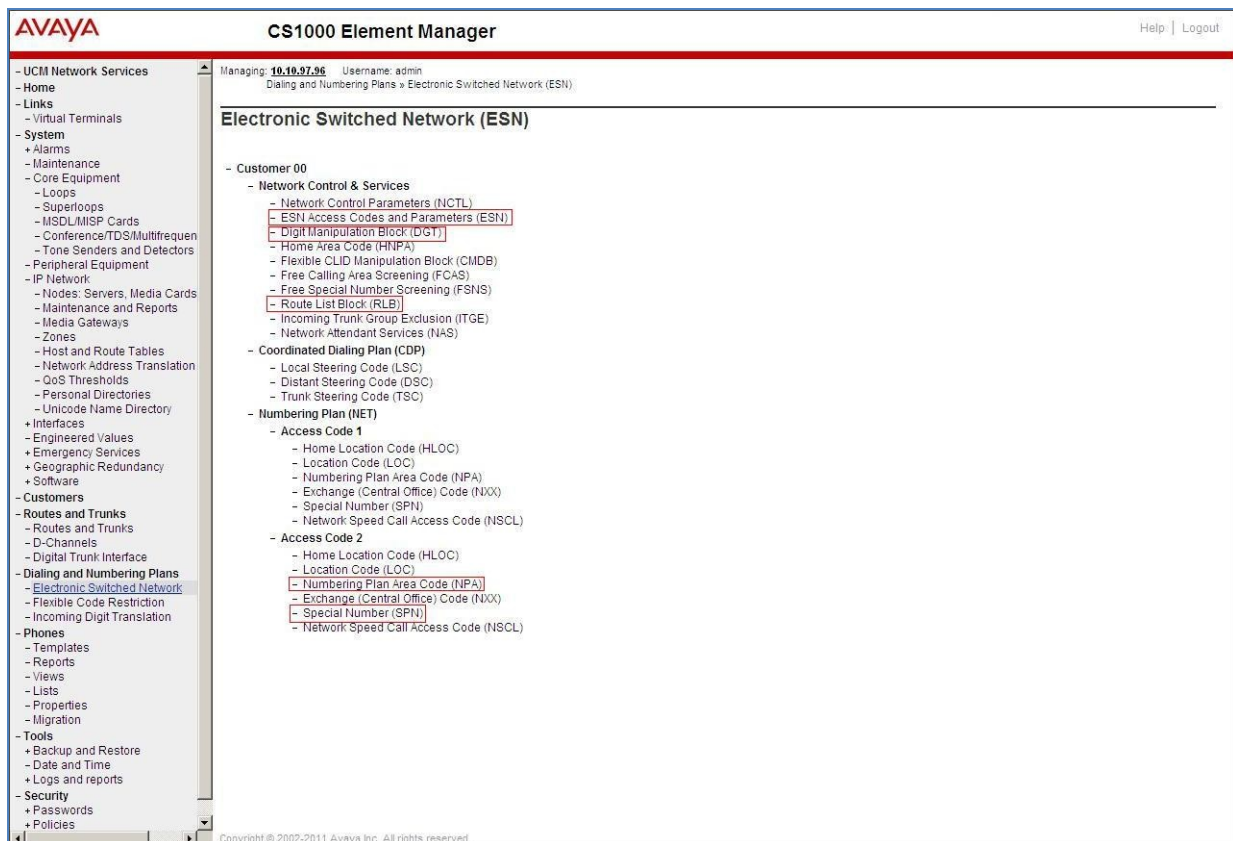


Figure 34 –ESN Configuration Details

b) In the **ESN Access Codes and Basic Parameters** page, define **NARS Access Code 2** as shown in **Figure 35**.

c) Click Submit button (not shown).

Figure 35 – ESN Access Codes and Basic Parameters

5.6.2. Associate NPA and SPN call to ESN Access Code 2

a) Login Call Server CLI (please refer to **Section 5.1.2** for more detail), change Customer Net Data block by using **LD 15**.

```
>ld 15
CDB000
MEM AVAIL: (U/P): 35600086   USED U P: 8325631 954152   TOT: 44879869
DISK SPACE NEEDED: 1722 KBYTES
REQ: chg
TYPE: net

TYPE NET_DATA
CUST 0
OPT
AC1 xNPA xSPN   ----- > (Set NPA, SPN not to associate to ESN Access Code 1)
FNP
CLID
...
```

b) Verify Customer Net Data block by using LD 21

```
>ld 21
PT1000

REQ: prt
TYPE: net
TYPE NET_DATA
CUST 0

TYPE NET_DATA
CUST 00
OPT RTA
AC1
AC2 INTL NPA SPN NXX LOC ----- > (NPA, SPN are associated to ESN Access Code 2)
FNP YES
...
```

5.6.3. Digit Manipulation Block (DMI)

- a) Select **Dialing and Numbering Plans -> Electronic Switched Network** from the left pane to display the **Electronic Switched Network (ESN)** screen. Select **Digit Manipulation Block (DGT)** as shown in **Figure 34**.
- b) In the Choose a DMI Number field, select an available DMI from the drop-down list and click **to Add** as shown in **Figure 36**.
- c) Enter the **Number of leading digits to be Deleted (Del)** field and select the **Call Type to be used by the manipulated digits (CTYP)** and then click **Submit** (see **Section 5.6.4**).

5.6.4. Digit Manipulation Block (DMI) for Outbound Call

In the following steps show how to add DMI for the outbound call, there are 4 indexes, which were added to the Digit Manipulation Block List (14 and 15).

- a) Select **Dialing and Numbering Plans ---> Electronic Switched Network** from the left pane to display the **Electronic Switched Network (ESN)** screen. Select **Digit Manipulation Block (DGT)** as above.
- b) In the Choose a DMI Number field, select an available DMI from the drop-down list and click **to Add** button as shown in **Figure 36**.

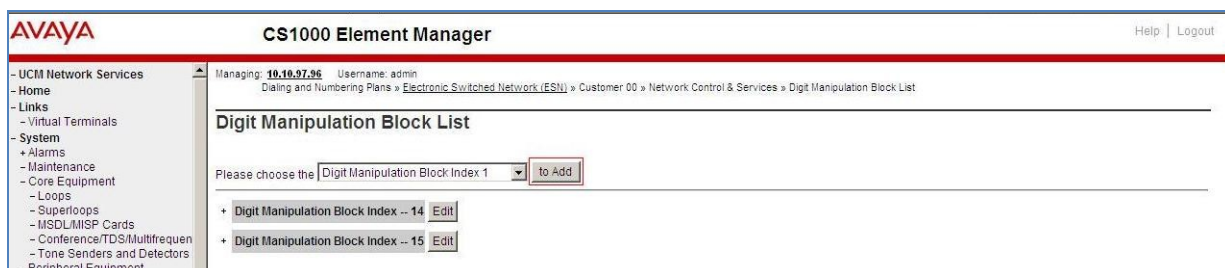


Figure 36 – Add a DMI

c) Add DMI_14: Enter 0 for the **Number of leading digits to be Deleted (Del)** field and select **NPA** for the **Call Type to be used by the manipulated digits (CTYP)** and then click on **Submit** button as shown in **Figure 37**

Figure 37 – DMI_14 Configuration Details

d) Add DMI_15: Enter 1 for the **Number of leading digits to be Deleted (Del)** field and select **NPA** for the **Call Type to be used by the manipulated digits (CTYP)** and then click on **Submit** button as shown in **Figure 38**

Figure 38 – DMI_15 Configuration Details

5.6.5. Route List Block (RLB) (RLB 14)

This session shows how to add a RLB associated with the DMI created in **Section 5.6.4**.

a) Select **Dialing and Numbering Plans -> Electronic Switched Network** from the left pane to display the **Electronic Switched Network (ESN)** screen. Select **Route List Block (RLB)** as shown in **Figure 34**.

b) Select an available value in the textbox for the **route list index** (in this case is 14) and click on **Add** button as shown in **Figure 39**.

Figure 39 – Add a Route List Block.

c) Enter the following values for the specified fields, and retain the default values for the remaining fields (**Figure 40**). Scroll down to the bottom of the screen, and click on the **Submit** button.

- **Route number (ROUT):** 100 (created in **Section 5.5.5**)
- **Digit Manipulation Index (DMI):** 14 (created in **Section 5.6.4**)
- **Incoming CLID Table:** 0 (created in **Section 5.5.7**)

Figure 40 – RLB_14 Route List Block Configuration Details

5.6.6. Route List Block (RLB) (RLB 15)

a) Select **Dialing and Numbering Plans -> Electronic Switched Network** from the left pane to display the **Electronic Switched Network (ESN)** screen. Select **Route List Block (RLB)** as shown in **Figure 34**.

b) Select an available value in the textbox for the **route list block index** (in this case 15) and click on the “**to Add**” button as shown in **Figure 39**.

c) Enter the following values for the specified fields, and retain the default values for the remaining fields (**Figure 41**). Scroll down to the bottom of the screen, and click on the **Submit** button.

- **Route number (ROUT)** : 100 (created in **Section 5.5.5**)
- **Digit Manipulation Index (DMI)**: 15 (created in **Section 5.6.4**)
- **Incoming CLID Table**: 0 (created in **Section 5.5.7**)

The screenshot displays the 'Data Entry of a Route List Block' configuration page in the AVAYA CS1000 Element Manager. The page is titled 'Data Entry of a Route List Block' and shows the configuration for 'Route List Block Index: 15'. The left sidebar contains a navigation tree with 'Dialing and Numbering Plans' selected. The main content area is divided into three sections: 'General Properties', 'Indexes', and 'Options'. In the 'General Properties' section, the 'Entry Number for the Route List' is set to 0. In the 'Indexes' section, the 'Digit Manipulation Index' is set to 15, and the 'Incoming CLID Table' is set to 0. In the 'Options' section, the 'Route Number' is set to 100. Other fields like 'Time of Day Schedule', 'Facility Restriction Level', 'ISL D-Channel Down Digit Manipulation Index', 'Free Calling Area Screening Index', 'Free Special Number Screening Index', 'Business Network Extension Route', 'Local Termination entry', 'Skip Conventional Signaling', 'Use Tone Detector', 'Conversion to LDN', 'Expensive Route', 'Strategy on Congestion', 'QSIG Alternate Routing Causes', 'Preferred Routing', 'ISDN Drop Back Busy', 'ISDN Off-Hook: Queuing Option', and 'Off-Hook: Queuing Allowed' are all set to their default values. The bottom of the page shows the copyright notice: 'Copyright © 2002-2011 Avaya Inc. All rights reserved.'

Figure 41 – RLB_15 Route List Block Configuration Details

5.6.7. Inbound Call – Incoming Digit Translation Configuration

This section describes the steps for receiving the calls from PSTN via the Windstream system.

- a) Select **Dialing and Numbering Plans** -> **Incoming Digit Translation** from the left pane to display the **Incoming Digit Translation** screen. Click on the **Edit IDC** button as shown in **Figure 42**.

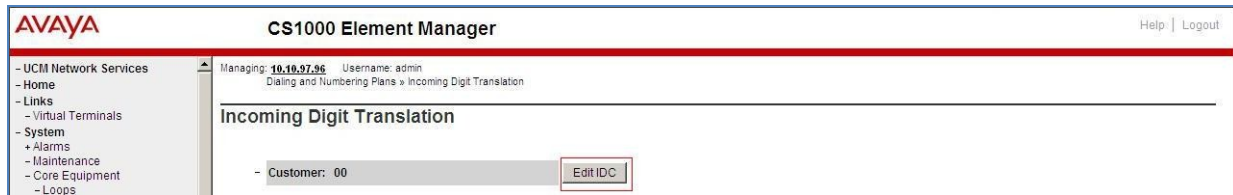


Figure 42 – Incoming Digit Translation

- b) Click on the **New DCNO** to create the digit translation mechanism. In this example, Digit Conversion Tree Number 1 has been created as shown in **Figure 43**.



Figure 43 – Incoming Digit Conversion Property

- c) Detail configuration of the Digit Conversion Tree Configuration is shown in **Figure 44**. The **Incoming Digits** can be added to map to the Converted Digits which would be the Communication Server 1000 system phones DN. This **DCN0** has been assigned to route 100 as shown in **Figure 26** and **27**.
In the following configuration, the incoming call from PSTN with the prefix 501287xxxx will be translated to DN xxxx. The DID number 5012871072 is translated to 1700 for Voicemail accessing purpose.

AVAYA
CS1000 Element Manager
Help | Logout

- UCM Network Services
- Home
- Links
- Virtual Terminals
- System
+ Alarms
- Maintenance
- Core Equipment
- Loops
- Superloops
- MSDLMISP Cards
- Conference/TDS/Multifrequen
- Tone Senders and Detectors
- Peripheral Equipment
- IP Network
- Nodes, Servers, Media Cards
- Maintenance and Reports
- Media Gateways
- Zones
- Host and Route Tables
- Network Address Translation
- QoS Thresholds
- Personal Directories
- Unicode Name Directory
+ Interfaces
- Engineered Values
+ Emergency Services
+ Geographic Redundancy
+ Software
- Customers
- Routes and Trunks
- Routes and Trunks

Managing: **10.10.97.95** Username: admin
Dialing and Numbering Plans > Incoming Digit Translation > Customer 00 > Digit Conversion Tree 1 Configuration

Digit Conversion Tree 1 Configuration
Regular IDC tree
Send calling party DID disabled

Add...
Delete IDC
Delete IDC tree
Refresh

	Incoming Digits	Converted Digits	CPND Name	CPND language
1	5012871070	1070		Roman characters
2	5012871071	1071		Roman characters
3	5012871072	1700		Roman characters
4	5012871073	1073		Roman characters
5	5012871074	1074		Roman characters
6	5012871490	1490		Roman characters
7	5012871492	1492		Roman characters
8	5012871493	1493		Roman characters
9	5012871494	1494		Roman characters
10	5012871495	1495		Roman characters
11	5012871496	1496		Roman characters
12	5012871497	1497		Roman characters
13	5012871498	1498		Roman characters
14	5012871499	1499		Roman characters

Figure 44 – Digit Conversion Tree

5.6.8. Outbound Call - Special Number Configuration

There are special numbers which have been configured to be used for this testing such as: 011, 1800, 411, 911 and so on.

a) Select **Dialing and Numbering Plans** -> **Electronic Switched Network** from the left pane to display the **Electronic Switched Network (ESN)** screen. Select **Special Number (SPN)** as shown in **Figure 34**.

b) Enter SPN number and then click on **to Add** button. **Figure 45** shows all the special number used for this testing.

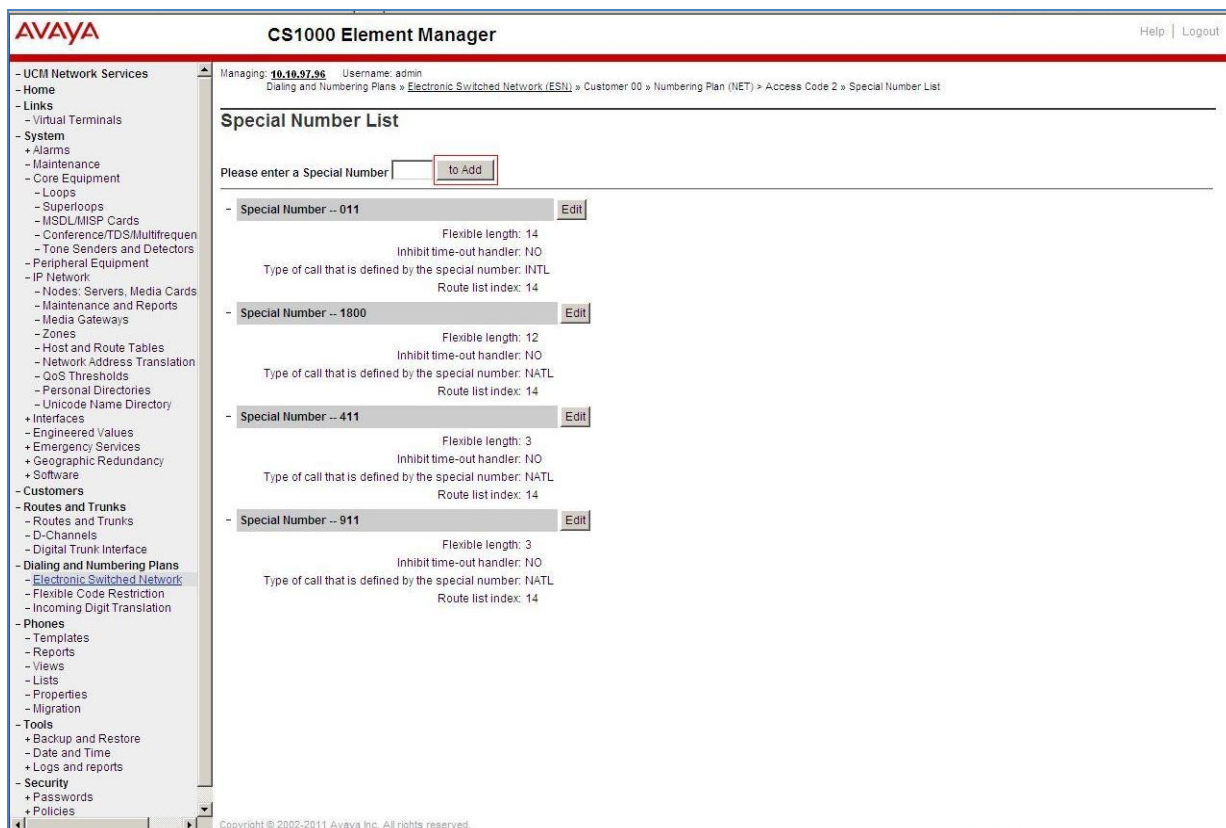


Figure 45 – Add a SPN.

5.6.9. Outbound Call - Numbering Plan Area (NPA)

This section describes the creation of NPA used in this testing configuration.

- Select **Dialing and Numbering Plans** -> **Electronic Switched Network** from the left pane to display the **Electronic Switched Network (ESN)** screen. Select **Numbering Plan Area Code (NPA)** as shown in **Figure 34**.
- Enter the area code desired in the textbox and click on the “**to Add**” button. The 1501, 1613 and 1647 area codes were used in this configuration as shown in **Figure 46**.

AVAYA CS1000 Element Manager Help | Logout

Managing: 10.10.37.95 : Username: admin
Dialing and Numbering Plans » Electronic Switched Network (ESN) » Customer 00 » Numbering Plan (NET) » Access Code 2 » Numbering Plan Area Code List

Numbering Plan Area Code List

Please enter an area code:

Numbering Plan Area Code	Route List Index	Incoming Trunk group Exclusion Index	Action
1501	15	NONE	Edit
1613	15	NONE	Edit
1647	15	NONE	Edit

Figure 46 – Numbering Plan Area Code List

5.7. Administer Phone

This section describes the creation of Communication Server 1000 clients used in this configuration.

5.7.1. Phone creation

- Refer to **Section 5.5.4** to create a virtual super-loop - **96** used for IP phone.
- Refer to **Section 5.4.1** to create a bandwidth zone - **10** for IP phone.
- Log in to the Call Server Command Line Interface (please refer to **Section 5.1.2** for more detail).
- Create an IP phone by using **LD 11**.

```
REQ: prt
TYPE: 2002p2
TN 96 0 0 2
DATE
PAGE
DES
MODEL_NAME
EMULATED

DES 2002P2
TN 96 0 00 02 VIRTUAL
TYPE 2002P2
CDEN 8D
CTYP XDLC
CUST 0
NUID
NHTN
CFG_ZONE 00010
CUR_ZONE 00010
MRT
ERL 12345
ECL 0
FDN
TGAR 0
```

```

LDN NO
NCOS 7
SGRP 0
RNPG 0
SCI 0
SSU
LNRS 16
XLST
SCPW
SFLT NO
CAC_MFC 0
CLS_UNR FBD WTA LPR MTD FND HTD TDD CRPD
    MWD LMPN RMMD SMWD AAD IMD XHD IRD NID OLD VCE DRG1
    POD SLKD CCSD SWD LNA CNDA
    CFTD SFD MRD DDV CNID CDCA MSID DAPA BFED RCBF
    ICDD CDMD LLCN MCTD CLBD AUTU
    GPUD DPUD DNDD CFXD ARHD CLTD ASCD
    CPFA CPTA ABDD CFHD FICD NAID BUZZ AGRD MOAD
    UDI RCC HBTD AHD IPND DDGA NAMA MIND PRSD NRWD NRCD NROD
    DRDD EXR0
    USMD USRD ULAD CCBF RTDD RBDD RBHD PGND OCBF FLXD FTTC DNDY DNO3 MCBN
    FDSF NOVF VOLA VOUD CDMR PRED RECF MCDD T87D SBMD
    MSNV FRA PKCH MWTD DVLD CROD ELCD
CPND_LANG ENG
HUNT
PLEV 02
PUID
UPWF
DANI NO
AST
IAPG 0
AACS NO
ITNA NO
DGRP
MLWU_LANG 0
MLNG ENG
DNDR 0
KEY 00 SCR 1492 0  MARP
    CPND
    CPND_LANG ROMAN
    NAME Carrier1
    XPLN 13
    DISPLAY_FMT FIRST, LAST
    01
    02
<Text removed for brevity>

```

5.7.2. Enable Privacy for Phone

In this section, it shows how to enable Privacy for a phone by changing its class of service (CLS). By modifying the configuration of the phone created in **Section 5.7.1**, the display of the outbound call will be changed appropriately.

a) To hide the display name, set CLS to **namd**. Communication Server 1000 will include “Privacy:user” in the SIP message header before sending it to the Service Provider.

```
>ld 11
REQ: chg
TYPE: 2002p2
TN 96 0 0 2
ECHG yes
ITEM cls namd
...
```

b) To hide the display number, set CLS to **ddgd**. Communication Server 1000 will include “Privacy:id” in the SIP message header before sending it to the Service Provider.

```
>ld 11
REQ: chg
TYPE: 2002p2
TN 96 0 0 2
ECHG yes
ITEM cls ddgd
...
```

c) To hide display name and number, set CLS to **namd, ddgd**. Communication Server 1000 will include “Privacy:id, user” in the SIP message header before sending to the Service Provider.

```
>ld 11
REQ: chg
TYPE: 2002p2
TN 96 0 0 2
ECHG yes
ITEM cls namd ddgd
...
```

d) To allow display name and number, set CLS to **nama, ddga**. Communication Server 1000 will not send the Privacy header to the Service Provider.

```
>ld 11
REQ: chg
TYPE: 2002p2
TN 96 0 0 2
ECHG yes
ITEM cls nama ddga
...
```

5.7.3. Enable Call Forward for Phone

In this section, it shows how to configure the Call Forward feature at the system and phone level.

a) Select **Customer -> 00 -> Call Redirection**. The Call Redirection page is shown in **Figure 47**.

- **Total redirection count limit: 0** (unlimited)
- **Call Forward: Originating**
- **Number of normal ring cycle of CFNA: 4**

Figure 47 – Call Redirection

b) To enable **Call Forward All Call (CFAC)** for a phone over a trunk, use **LD 11**, change its CLS to **CXFA**, **SFA** then program the forward number on the phone set. Following is the configuration of a phone that has **CFAC** enabled with forwarding number 916139675205

```
REQ: prt
TYPE: 2007
TN 96 0 0 4
DATE
PAGE
DES
MODEL_NAME
EMULATED

DES 2007
TN 96 0 00 04 VIRTUAL
TYPE 2007
...
CLS UNR FBA WTA LPR MTD FNA HTA TDD HFD CRPD
```

MWA LMPN RMMD SMWD AAD IMD XHD IRD NID OLD VCE DRG1
POD SLKD CCSD SWD LNA CNDA
CFTD **SFA** MRD DDV CNID CDCA MSID DAPA BFED RCB
ICDA CDMA LLCN MCTD CLBD AUTU
GPUD DPUD DNDD **CFXA** ARHD CLTD ASCD

...
19 CFW 16 916139675205
...

d) To enable **Call Forward Busy (CFB)** for phone over trunk by using **LD 11**, change its **CLS** to **FBA, HTA, SFA** then program the forward number as is **HUNT**. Following is the configuration of a phone has **CFB** enabled with forward number is 916139675205

REQ: prt
TYPE: 2007
TN 96 0 0 4
DATE
PAGE
DES
MODEL_NAME
EMULATED

DES 2007
TN 96 0 00 04 VIRTUAL
TYPE 2007

...
CLS UNR **FBA** WTA LPR MTD FNA **HTA** TDD HFD CRPD
MWA LMPN RMMD SMWD AAD IMD XHD IRD NID OLD VCE DRG1
POD SLKD CCSD SWD LNA CNDA
CFTD **SFA** MRD DDV CNID CDCA MSID DAPA BFED RCB

...
FDN 916139675205
HUNT 916139675205
...

c) To enable **Call Forward No Answer (CFNA)** for a phone over a trunk by using **LD 11**, change its **CLS** to **FNA, SFA** then program the forward number as **FDN**. Following is the configuration of a phone that has CFNA enabled with forward number 916139675205

REQ: prt
TYPE: 2007
TN 96 0 0 4
DATE
PAGE
DES
MODEL_NAME
EMULATED

DES 2007
TN 96 0 00 04 VIRTUAL
TYPE 2007

...
FDN 916139675205

```
HUNT 916139675205
```

```
...  
CLS UNR FBA WTA LPR MTD FNA HTA TDD HFD CRPD  
MWA LMPN RMMD SMWD AAD IMD XHD IRD NID OLD VCE DRG1  
POD SLKD CCSD SWD LNA CNDA  
CFTD SFA MRD DDV CNID CDCA MSID DAPA BFED RCBF  
...
```

5.7.4. Enable Call Waiting for Phone

In this section, it shows how to configure Call Waiting feature at phone level.

Log in to the Call Server CLI (please refer to **Section 5.1.2** for more detail), configure Call Waiting feature for phone by using **LD 11** to change **CLS** to **HTD**, **SWA** and adding a **CWT** key.

```
REQ: prt  
TYPE: 2002p2  
  
TN 96 0 0 2  
DATE  
PAGE  
DES  
MODEL_NAME  
EMULATED  
KEM_RANGE  
  
DES 2002P2  
TN 96 0 00 02 VIRTUAL  
TYPE 2002P2  
...  
CLS UNR FBD WTA LPR MTD FNA HTD TDD HFD CRPD  
MWA LMPN RMMD SMWD AAD IMD XHD IRD NID OLD VCE DRG1  
POD SLKD CCSD SWA LNA CNDA  
...  
KEY 00 SCR 1492 0 MARP  
CPND  
CPND_LANG ROMAN  
NAME Carrier1  
XPLN 13  
DISPLAY_FMT FIRST, LAST  
01 CWT  
...
```

6. Configure Avaya Aura® Session Manager

This section provides the procedures for configuring Avaya Aura® Session Manager. The procedures include adding the following items:

- SIP domain
- Logical/physical Location that can be occupied by SIP Entities

- Adaptation module to perform dial plan manipulation
- SIP Entities corresponding to the Avaya Communication Server 1000, the Acme Packet SBC and Avaya Aura® Session Manager (Session Manager)
- Entity Links, which define the SIP trunk parameters used by Session Manager when routing calls to/from SIP Entities
- Routing Policies, which control call routing between the SIP Entities
- Dial Patterns, which govern to which SIP Entity a call is routed
- Regular Expressions, which also can be used to route calls
- Session Manager, corresponding to the Session Manager Server to be managed by System Manager.

It may not be necessary to create all the items above when creating a connection to the service provider since some of these items would have already been defined as part of the initial Session Manager installation. This includes items such as certain SIP domains, locations, SIP entities, and Session Manager itself. However, each item should be reviewed to verify the configuration.

6.1. System Manager Login and Navigation

Session Manager configuration is accomplished by accessing the browser-based GUI of System Manager, using the URL “https://<ip-address>/SMGR”, where “<ip-address>” is the IP address of System Manager. At the System Manager Log On screen, provide the appropriate credentials and click on **Log On**.

AVAYA Avaya Aura® System Manager 6.1

Home / Log On

Log On

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:

[Change Password](#)

Figure 48 – System Manager Login

The home screen shown in **Figure 49** below is then displayed, from this page is it possible to access all areas of System Manager.

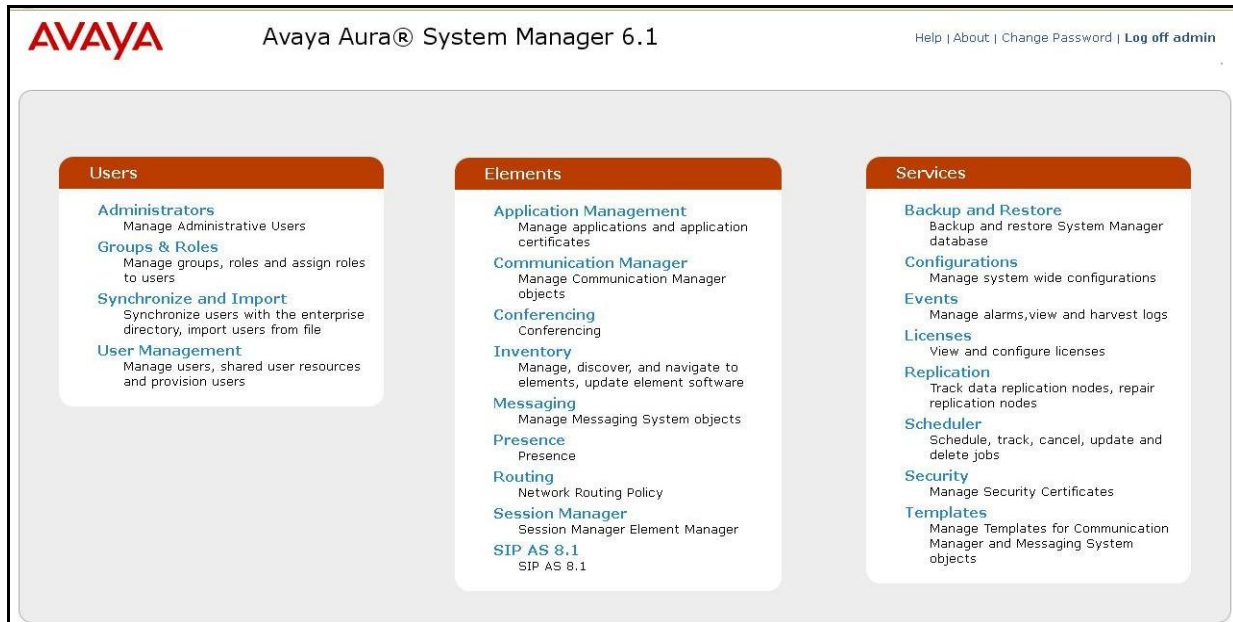


Figure 49 – System Manager Home

Most of the configuration items are performed in the Routing Element. Click on **Routing** in the Elements column shown in **Figure 49** to bring up the Introduction to Network Routing Policy screen shown in **Figure 50**.

The navigation tree displayed in the left pane will be referenced in subsequent sections to navigate to items requiring configuration.

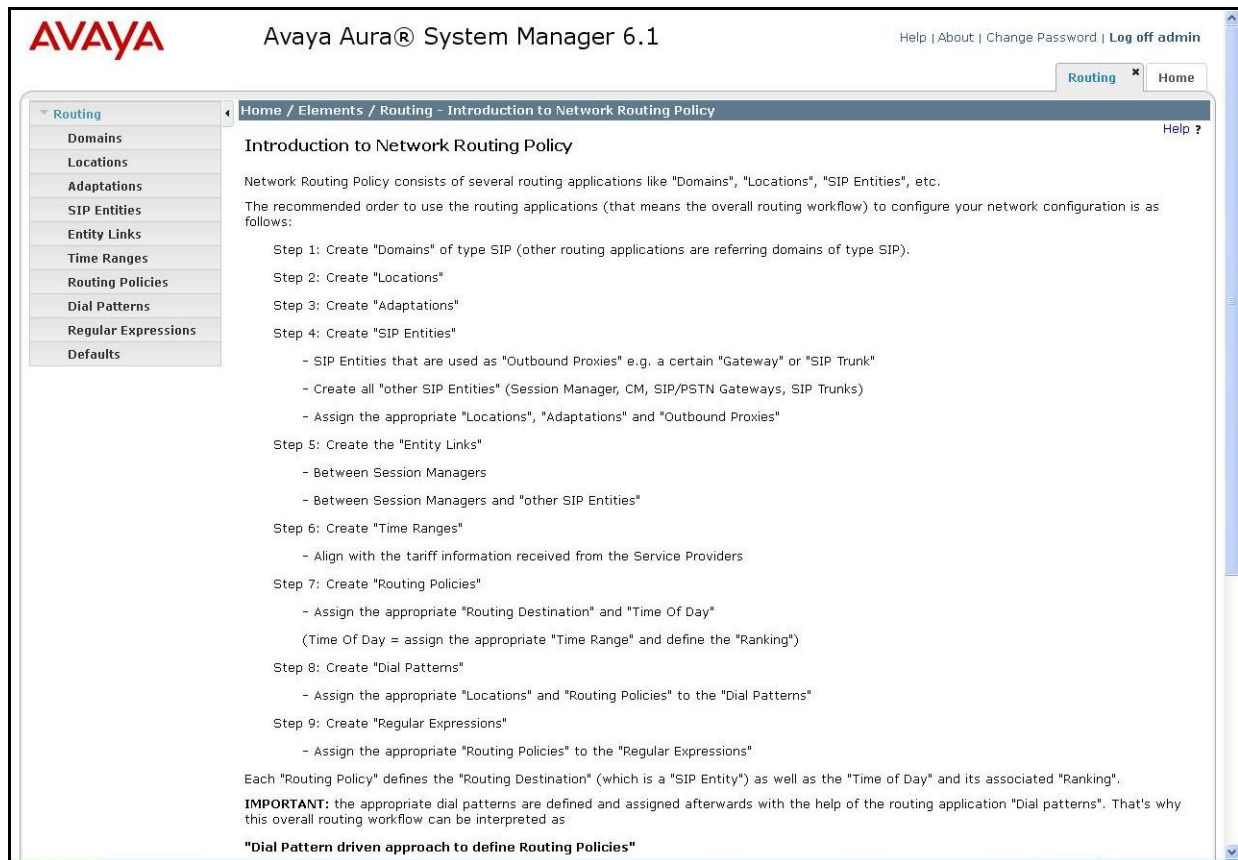


Figure 50 – Session Manager Routing Policy

6.2. Specify SIP Domain

Create a SIP domain for each domain for which Session Manager will need to be aware in order to route calls. For the compliance test, this includes the enterprise domain (**bwvdev75.com**). Navigate to **Routing → Domains** in the left navigation pane and click the **New** button in the right pane (not shown). In the new right pane that appears (shown below), fill in the following:

- **Name:** Enter the domain name.
- **Type:** Select **sip** from the pull-down menu.
- **Notes:** Add a brief description (optional).

Click **Commit**. **Figure 51** below shows the entry for the enterprise domain.

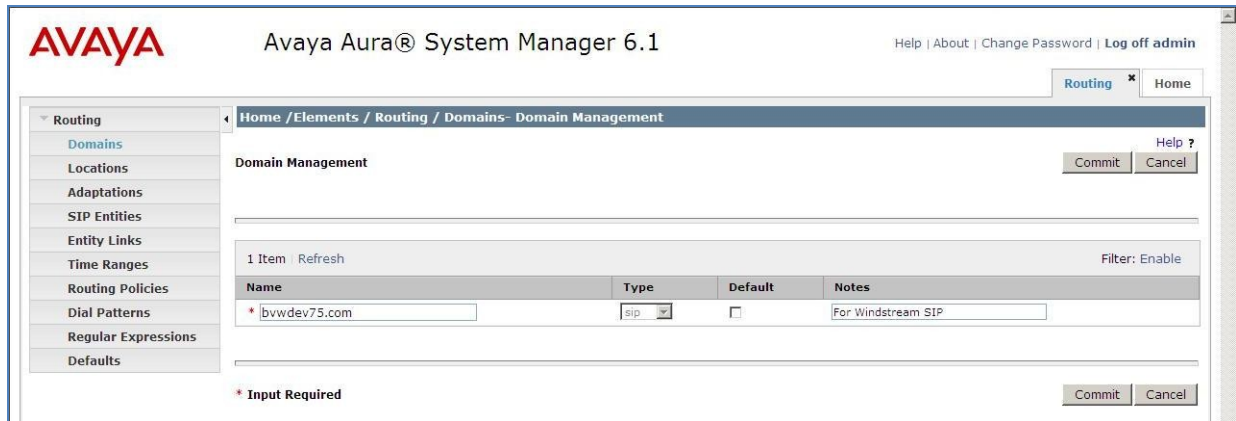


Figure 51 – Session Manager Routing Domains

6.3. Add Location

Locations can be used to identify logical and/or physical locations where SIP Entities reside for purposes of bandwidth management and call admission control. To add a location, navigate to **Routing → Locations** in the left-hand navigation pane and click the **New** button in the right pane (not shown).

In the **General** section, enter the following values. Use default values for all remaining fields:

- **Name:** Enter a descriptive name for the location.
- **Notes:** Add a brief description (optional).

In the **Location Pattern** section (see **Figure 52** below), click **Add** and enter the following values. Use default values for all remaining fields:

- **IP Address Pattern:** An IP address pattern used to identify the location.
- **Notes:** Add a brief description (optional).

Figure 52 displayed below is the screen for addition of the **Belleville** Location, which includes all equipment on the **10.10.97.x** subnet including the Avaya Communication Server 1000, the IP phones, and the Session Manager itself. Click **Commit** to save.

AVAYA Avaya Aura® System Manager 6.1

Help | About | Change Password | Log off admin

Routing x Home

Home / Elements / Routing / Locations - Location Details

Location Details

Call Admission Control has been set to ignore SDR. All calls will be counted using the Default Audio Bandwidth. See Session Manager -> Session Manager Administration -> Global Setting

General

* Name: Belleville, Ont, Ca

Notes:

Overall Managed Bandwidth

Managed Bandwidth Units: Kbit/sec

Total Bandwidth: 1000000

Per-Call Bandwidth Parameters

* Default Audio Bandwidth: 80 Kbit/sec

Location Pattern

Add Remove

0 Items Refresh Filter: Enable

IP Address Pattern	Notes

* Input Required

Commit Cancel

Figure 52 – Session Manager Location Details

6.4. Add SIP Entities

A SIP Entity must be added for Session Manager and for each SIP telephony system connected to it which includes the Avaya Communication Server 1000 and the Acme Packet SBC. Navigate to **Routing** → **SIP Entities** in the left navigation pane and click on the **New** button in the right pane (not shown).

In the **General** section, enter the following values. Use default values for all remaining fields:

- **Name:** Enter a descriptive name.
- **FQDN or IP Address:** Enter the FQDN or IP address of the SIP Entity that is used for SIP signaling.
- **Type:** Enter **Session Manager** for Session Manager, **Other** for the Avaya Communication Server 1000 and the Acme SBC.
- **Location:** Select one of the locations defined previously.
- **Time Zone:** Select the time zone for the location above.

Figure 53 below shows the addition of Session Manager. The IP address of the virtual SM-100 Security Module (the Session Manager signaling interface) is entered for **FQDN or IP Address**.

AVAYA Avaya Aura® System Manager 6.1 Help | About | Change Password | Log off admin

Routing Home

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

SIP Entity Details Help ?

General Commit Cancel

* **Name:** DevASM

* **FQDN or IP Address:** 10.10.97.198

Type: Session Manager

Notes: For Session Manager

Location: Belleville, Ont, Ca

Outbound Proxy:

Time Zone: America/Toronto

Credential name:

SIP Link Monitoring

SIP Link Monitoring: Use Session Manager Configuration

Entity Links Add Remove

20 Items Refresh Filter: Enable

<input type="checkbox"/>	SIP Entity 1	Protocol	Port	SIP Entity 2	Port	Trusted
<input type="checkbox"/>	DevASM	UDP	* 5060	car3-ssg-carrier	* 5060	<input checked="" type="checkbox"/>
<input type="checkbox"/>	DevASM	UDP	* 5060	CS1K60	* 5060	<input checked="" type="checkbox"/>
<input type="checkbox"/>	DevASM	UDP	* 5060	AA-SBC3	* 5060	<input checked="" type="checkbox"/>
<input type="checkbox"/>	DevASM	UDP	* 5060	AASBCHTSAllStream	* 5060	<input checked="" type="checkbox"/>
<input type="checkbox"/>	DevASM	UDP	* 5060	ACME	* 5060	<input checked="" type="checkbox"/>

Figure 53 – Session Manager Routing SIP Entities

To define the ports used by Session Manager, scroll down to the **Port** section of the **SIP Entity Details** screen. This section is only present for the **Session Manager** SIP Entity.

In the **Port** section, click **Add** and enter the following values. Use default values for all remaining fields:

- **Port:** Port number on which the Session Manager can listen for SIP requests.
- **Protocol:** Transport protocol to be used to send SIP requests.
- **Default Domain:** The domain used for the enterprise.

Defaults can be used for the remaining fields. Click **Commit** to save.

The compliance test used 2 **Port** entries:

- **5060** with **UDP** for connecting to ACME SBC
- **5060** with **UDP** for connecting to the Avaya Communication Server 1000

Defaults

Location: Belleville, Ont, Ca
Outbound Proxy:
Time Zone: America/Toronto
Credential name:

SIP Link Monitoring

SIP Link Monitoring: Use Session Manager Configuration

Entity Links

Add Remove

20 Items Refresh
Filter: Enable

<input type="checkbox"/>	SIP Entity 1	Protocol	Port	SIP Entity 2	Port	Trusted
<input type="checkbox"/>	DevASM	UDP	* 5060	car3-ssg-carrier	* 5060	<input checked="" type="checkbox"/>
<input type="checkbox"/>	DevASM	UDP	* 5060	CS1K60	* 5060	<input checked="" type="checkbox"/>
<input type="checkbox"/>	DevASM	UDP	* 5060	AA-SBC3	* 5060	<input checked="" type="checkbox"/>
<input type="checkbox"/>	DevASM	UDP	* 5060	AASBCMTSAllStream	* 5060	<input checked="" type="checkbox"/>
<input type="checkbox"/>	DevASM	UDP	* 5060	ACME	* 5060	<input checked="" type="checkbox"/>

Select : All, None

< Previous Page 1 of 4 Next >

Port

Add Remove

4 Items Refresh
Filter: Enable

<input type="checkbox"/>	Port	Protocol	Default Domain	Notes
<input type="checkbox"/>	5060	UDP	lvwdev75.com	

Select : All, None

* Input Required

Commit Cancel

Figure 54 – Session Manager SIP Entities Details

Figure 55 shows the addition of the Avaya Communication Server 1000. In order for Session Manager to send SIP service provider traffic on a separate entity link to the Avaya Communication Server 1000, it is necessary to create a separate SIP entity for the Avaya Communication Server 1000. The **FQDN or IP Address** field is set to the Node IP address of the Avaya Communication Server 1000.

AVAYA Avaya Aura® System Manager 6.1 Help | About | Change Password | Log off admin

Routing x **Session Manager** x **Routing** x **Routing** x **Home**

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

SIP Entity Details Help ? Commit Cancel

General

* **Name:** car3-ssg-carrier

* **FQDN or IP Address:** 10.10.97.178

Type: Other

Notes:

Adaptation:

Location: Belleville, Ont, Ca

Time Zone: America/New_York

Override Port & Transport with DNS SRV: ☐

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

Credential name:

Call Detail Recording: none

SIP Link Monitoring

SIP Link Monitoring: Use Session Manager Configuration

Entity Links

Add Remove

1 Item | Refresh Filter: Enable

<input type="checkbox"/>	SIP Entity 1	Protocol	Port	SIP Entity 2	Port	Trusted
<input type="checkbox"/>	DevASM	UDP	* 5060	car3-ssg-carrier	* 5060	<input checked="" type="checkbox"/>

Select : All, None

Figure 55 – Session Manager SIP Entity- Avaya Communication Server 1000

Figure 56 shows the addition of the Acme SBC SIP Entity. The **FQDN or IP Address** field is set to the IP address of its private network interface. **Link Monitoring Enabled** was disabled for **SIP Link Monitoring**. If monitoring is enabled the specific time settings for **Proactive Monitoring Interval (in seconds)** and **Reactive Monitoring Interval (in seconds)** should be adjusted or left at their default values per customer needs and requirements.

The screenshot shows the 'SIP Entity Details' configuration page for an entity named 'ACME'. The left navigation pane is expanded to 'Routing' > 'SIP Entities'. The main content area has a 'General' tab selected. Fields include:

- Name: ACME
- FQDN or IP Address: 10.10.97.184
- Type: Other
- Notes: ACME PACKET 3800
- Adaptation: (empty dropdown)
- Location: Belleville, Ont, Ca
- Time Zone: America/New_York
- Override Port & Transport with DNS SRV: (unchecked)
- SIP Timer B/F (in seconds): 4
- Credential name: (empty text box)
- Call Detail Recording: none
- SIP Link Monitoring: Link Monitoring Disabled
- Proactive Monitoring Interval (in seconds): 900
- Reactive Monitoring Interval (in seconds): 120
- Number of Retries: 1

 At the bottom, there is an 'Entity Links' section with 'Add' and 'Remove' buttons.

Figure 56 – Session Manager SIP Entity – Acme SBC

6.5. Add Entity Links

A SIP trunk between Session Manager and a telephony system is described by an Entity Link. Two Entity Links were created: one to the Avaya Communication Server 1000 for use only by service provider traffic and one to the Acme SBC. To add an Entity Link, navigate to **Routing** → **Entity Links** in the left navigation pane and click on the **New** button in the right pane (not shown). Fill in the following fields in the new row that is displayed:

- **Name:** Enter a descriptive name.
- **SIP Entity 1:** Select the Session Manager.
- **Protocol:** Select the transport protocol used for this link.
- **Port:** Port number on which Session Manager will receive SIP requests from the far-end.
- **SIP Entity 2:** Select the name of the other system. For Avaya Communication Server 1000, select the Avaya Communication Server 1000 SIP Entity defined in **Figure 55**. For Acme SBC, select the Acme SBC SIP Entity defined in **Figure 56**.
- **Port:** Port number on which the other system receives SIP requests from the Session Manager.
- **Trusted:** Check this box. *Note: If this box is not checked, calls from the associated SIP Entity specified in 6.4 will be denied.*

Click **Commit** to save.

The following screens illustrate the Entity Links to Avaya Communication Server 1000 and the Acme SBC. It should be noted that in a customer environment the Entity Link to Avaya Communication Server 1000 would normally use TLS. For the compliance test, UDP was used to aid in troubleshooting since the signaling traffic would not be encrypted.

Entity Link to the Avaya Communication Server 1000:

The screenshot shows the Avaya Aura System Manager 6.1 interface. The left navigation pane is expanded to 'Routing' > 'Entity Links'. The main area displays the 'Entity Links' configuration page. A table lists one entity link with the following details:

Name	SIP Entity 1	Protocol	Port	SIP Entity 2	Port	Trusted	Notes
* car3-ssg-carrier	* DevASM	UDP	* 5060	* car3-ssg-carrier	* 5060	<input checked="" type="checkbox"/>	

Buttons for 'Commit' and 'Cancel' are visible at the bottom right. A 'Filter: Enable' option is also present.

Figure 57 Session Manager Routing Entity Link – Avaya Communication Server 1000

Entity Link to the Acme SBC:

The screenshot shows the Avaya Aura System Manager 6.1 interface. The left navigation pane is expanded to 'Routing' > 'Entity Links'. The main area displays the 'Entity Links' configuration page. A table lists one entity link with the following details:

Name	SIP Entity 1	Protocol	Port	SIP Entity 2	Port	Trusted	Notes
* DevASM_ACME_5060	* DevASM	UDP	* 5060	* ACME	* 5060	<input checked="" type="checkbox"/>	

Buttons for 'Commit' and 'Cancel' are visible at the bottom right. A 'Filter: Enable' option is also present.

Figure 58 – Session Manager Routing Entity Link - Acme SBC

6.6. Add Routing Policies

Routing policies describe the conditions under which calls will be routed to the SIP Entities specified in **Section 6.4**. Two routing policies must be added: one for the Avaya Communication Server 1000 and one for the Acme SBC. To add a routing policy, navigate to **Routing → Routing Policies** in the left navigation pane and click on the **New** button in the right pane (not shown). The following screen is displayed. Fill in the following:

In the **General** section, enter the following values. Use default values for all remaining fields:

- **Name:** Enter a descriptive name.

- **Notes:** Add a brief description (optional).

In the **SIP Entity as Destination** section, click **Select**. The **SIP Entity List** page opens (not shown). Select the appropriate SIP entity to which this routing policy applies and click **Select**. The selected SIP Entity displays on the Routing Policy Details page as shown below. Use default values for remaining fields. Click **Commit** to save.

The following screens show the Routing Policies for Communication Server 1000 and the Acme SBC.

Avaya Aura® System Manager 6.1

Help | About | Change Password | Log off admin

Routing * Home

Home / Elements / Routing / Routing Policies- Routing Policy Details

Routing Policy Details

General

* Name: Windstream to CS1K75

Disabled: ☐

Notes: Windstream to CS1K75

SIP Entity as Destination

Select

Name	FQDN or IP Address	Type	Notes
car3-ssg-carrier	10.10.97.178	Other	

Time of Day

Add Remove View Gaps/Overlaps

1 Item Refresh Filter: Enable

Ranking	Name	Mon	Tue	Wed	Thu	Fri	Sat	Sun	Start Time	End Time	Notes
0	24/7	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	00:00	23:59	Time Range 24/7

Select : All, None

Dial Patterns

Add Remove

1 Item Refresh Filter: Enable

Pattern	Min	Max	Emergency Call	SIP Domain	Originating Location	Notes
501	3	36	<input type="checkbox"/>	bvwdev75.com	Belleville,Ont,Ca	In-coming Call from Windstream to CS1K75

Figure 59 Session Manager Routing Policy – Avaya Communication Server 1000

Routing Policy Details [Commit] [Cancel]

General

* Name: CS1K75 to Windstream

Disabled: ☐

Notes: CS1K75 to Windstream

SIP Entity as Destination

Select

Name	FQDN or IP Address	Type	Notes
ACME	10.10.97.184	Other	ACME PACKET 3800

Time of Day

Add Remove View Gaps/Overlaps

1 Item Refresh Filter: Enable

Ranking	Name	Mon	Tue	Wed	Thu	Fri	Sat	Sun	Start Time	End Time	Notes
0	24/7	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	00:00	23:59	Time Range 24/7

Select : All, None

Dial Patterns

Add Remove

7 Items Refresh Filter: Enable

Pattern	Min	Max	Emergency Call	SIP Domain	Originating Location	Notes
011	3	36	<input checked="" type="checkbox"/>	bvwwdev75.com	Belleville,Ont,Ca	Outgoing Call from CS1K75 to Windstream International
1800	4	36	<input checked="" type="checkbox"/>	bvwwdev75.com	Belleville,Ont,Ca	Call from CS1K75 to Windstream Toll free
411	3	36	<input checked="" type="checkbox"/>	bvwwdev75.com	Belleville,Ont,Ca	Call from CS1K75 to Windstream 411
50128713	10	10	<input checked="" type="checkbox"/>	bvwwdev75.com	Belleville,Ont,Ca	For Outgoing Calls from CS1K75 to Windstream
613	3	36	<input checked="" type="checkbox"/>	bvwwdev75.com	Belleville,Ont,Ca	Call from CS1K75 to Windstream National 613
647	3	36	<input checked="" type="checkbox"/>	bvwwdev75.com	Belleville,Ont,Ca	Call from CS1K75 to Windstream Cell 647
911	3	36	<input checked="" type="checkbox"/>	bvwwdev75.com	Belleville,Ont,Ca	Call from CS1K75 to Windstream 911

Figure 60 Session Manager Routing Policy - Acme Packet SBC

6.7. Add Dial Patterns

Dial Patterns are needed to route calls through Session Manager. For the compliance test, dial patterns were needed to route calls from the Avaya Communication Server 1000 to Windstream and vice versa. Dial Patterns define which route policy will be selected for a particular call based on the dialed digits, destination domain and originating location. To add a dial pattern, navigate to **Routing → Dial Patterns** in the left navigation pane and click on the **New** button in the right pane (not shown). Fill in the following, as shown in the screens below:

In the **General** section, enter the following values. Use default values for all remaining fields:

- **Pattern:** Enter a dial string that will be matched against the Request-URI of the call.
- **Min:** Enter a minimum length used in the match criteria.
- **Max:** Enter a maximum length used in the match criteria.
- **SIP Domain:** Enter the destination domain used in the match criteria.
- **Notes:** Add a brief description (optional).

In the **Originating Locations and Routing Policies** section, click **Add**. From the **Originating Locations and Routing Policy List** that appears (not shown), select the appropriate originating

location for use in the match criteria. Lastly, select the routing policy from the list that will be used to route all calls that match the specified criteria. Click **Select**.

Default values can be used for the remaining fields. Click **Commit** to save.

Three examples of the dial patterns used for the compliance test are shown below, one for outbound calls from the enterprise to Belleville PSTN, one for outbound calls from the enterprise to the Windstream lab, and one for 911. Other dial patterns (e.g., 011 international calls, 411 directory assistance calls, etc., were similarly defined. All dial patterns are shown in **Figure 64**.

The first example in **Figure 61** shows that 10 digit dialed numbers that begin with **613**, which are for Belleville PSTN sets, and have a destination domain of **bvwddev75.com** uses route policy **CS1K75_to_Windstream**.

AVAYA Avaya Aura® System Manager 6.1 Help | About | Change Password | Log off admin

Routing Home

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

Dial Pattern Details Help ? Commit Cancel

General

* Pattern: 613

* Min: 10

* Max: 10

Emergency Call: ☐

SIP Domain: bvwddev75.com

Notes: Call from CS1K75 to Windstream National 61

Originating Locations and Routing Policies

Add Remove

1 Item Refresh Filter: Enable

<input type="checkbox"/>	Originating Location Name 1 ▲	Originating Location Notes	Routing Policy Name	Rank 2 ▲	Routing Policy Disabled	Routing Policy Destination	Routing Policy Notes
<input type="checkbox"/>	Belleville, Ont, Ca		CS1K75 to Windstream	0	<input type="checkbox"/>	ACME	CS1K75 to Windstream

Select : All, None

Denied Originating Locations

Add Remove

0 Items Refresh Filter: Enable

<input type="checkbox"/>	Originating Location	Notes
--------------------------	----------------------	-------

* Input Required Commit Cancel

Figure 61 Session Manager 10 digit Dial Pattern_613

The second example in **Figure 62** shows that 10 digit dialed numbers that begin with **50128713**, which are for Windstream lab sets, and have a destination domain of **bvwddev75.com** uses route policy **CS1K75_to_Windstream**.

AVAYA

Avaya Aura® System Manager 6.1

[Help](#) | [About](#) | [Change Password](#) | [Log off admin](#)

Routing

Home

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

Help ?

Commit

Cancel

Routing

Domains

Locations

Adaptations

SIP Entities

Entity Links

Time Ranges

Routing Policies

Dial Patterns

Regular Expressions

Defaults

Dial Pattern Details

General

* Pattern:

50128713

* Min:

10

* Max:

10

Emergency Call:

☐

SIP Domain:

bvwdev75.com

Notes:

For Outgoing Calls from CS1K75 to Windstre

Originating Locations and Routing Policies

Add

Remove

1 Item

Refresh

Filter: Enable

<input type="checkbox"/>	Originating Location Name	Originating Location Notes	Routing Policy Name	Rank	Routing Policy Disabled	Routing Policy Destination	Routing Policy Notes
<input type="checkbox"/>	Belleville,Ont,Ca		CS1K75 to Windstream	0	<input type="checkbox"/>	ACME	CS1K75 to Windstream

Select : All, None

Denied Originating Locations

Add

Remove

0 Items

Refresh

Filter: Enable

<input type="checkbox"/>	Originating Location	Notes
--------------------------	----------------------	-------

* Input Required

Commit

Cancel

Figure 62 Session Manager 10 digit Dialing Pattern_50128713

The third example in **Figure 63** shows that the 3 digit 911 dialed number for emergency calls have a destination domain of **bvwdev75.com** uses route policy **CS1K75_to_Windstream**.

AVAYA

Avaya Aura® System Manager 6.1

[Help](#) | [About](#) | [Change Password](#) | [Log off admin](#)

Routing

Home

Routing

Domains

Locations

Adaptations

SIP Entities

Entity Links

Time Ranges

Routing Policies

Dial Patterns

Regular Expressions

Defaults

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

Dial Pattern Details

General

* Pattern:

911

* Min:

3

* Max:

3

Emergency Call:

☐

SIP Domain:

trvwdev75.com

Notes:

Call from CS1K75 to Windstream 911

Originating Locations and Routing Policies

Add

Remove

1 Item

Refresh

Filter: Enable

<input type="checkbox"/>	Originating Location Name 1 ▲	Originating Location Notes	Routing Policy Name	Rank 2 ▲	Routing Policy Disabled	Routing Policy Destination	Routing Policy Notes
<input type="checkbox"/>	Belleville,Ont,Ca		CS1K75 to Windstream	0	<input type="checkbox"/>	ACME	CS1K75 to Windstream

Select : All, None

Denied Originating Locations

Add

Remove

0 Items

Refresh

Filter: Enable

<input type="checkbox"/>	Originating Location	Notes
--------------------------	----------------------	-------

* Input Required

Commit

Cancel

Figure 63 Session Manager Dialing Patten_911

Figure 64 shows all the dial patterns that were configured for outbound calls to the Windstream network and local PSTN calls.

HV; Reviewed:
SPOC 9/22/2011

Solution & Interoperability Test Lab Application Notes
©2011 Avaya Inc. All Rights Reserved.

62 of 88
WSCS1K75SMACME

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

Routing Policy Details

CommitCancel

General

Name: CS1K75 to Windstream

Disabled: ☐

Notes: CS1K75 to Windstream

SIP Entity as Destination

Select

Name	FQDN or IP Address	Type	Notes
ACME	10.10.97.184	Other	ACME PACKET 3800

Time of Day

AddRemoveView Gaps/Overlaps

1 Item RefreshFilter: Enable

<input type="checkbox"/>	Ranking	1	Name	2	Mon	Tue	Wed	Thu	Fri	Sat	Sun	Start Time	End Time	Notes
<input type="checkbox"/>	0		24/7		<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	00:00	23:59	Time Range 24/7

Select : All, None

Dial Patterns

AddRemove

7 Items RefreshFilter: Enable

<input type="checkbox"/>	Pattern	Min	Max	Emergency Call	SIP Domain	Originating Location	Notes
<input type="checkbox"/>	011	14	14	<input type="checkbox"/>	bvwddev75.com	Belleville,Ont,Ca	Outgoing Call from CS1K75 to Windstream International
<input type="checkbox"/>	1800	11	11	<input type="checkbox"/>	bvwddev75.com	Belleville,Ont,Ca	Call from CS1K75 to Windstream Toll free
<input type="checkbox"/>	411	3	3	<input type="checkbox"/>	bvwddev75.com	Belleville,Ont,Ca	Call from CS1K75 to Windstream 411
<input type="checkbox"/>	50128713	10	10	<input type="checkbox"/>	bvwddev75.com	Belleville,Ont,Ca	For Outgoing Calls from CS1K75 to Windstream
<input type="checkbox"/>	613	10	10	<input type="checkbox"/>	bvwddev75.com	Belleville,Ont,Ca	Call from CS1K75 to Windstream National 613
<input type="checkbox"/>	647	10	10	<input type="checkbox"/>	bvwddev75.com	Belleville,Ont,Ca	Call from CS1K75 to Call 647
<input type="checkbox"/>	911	3	3	<input type="checkbox"/>	bvwddev75.com	Belleville,Ont,Ca	Call from CS1K75 to Windstream 911

Figure 64 Session Manager all Outbound Dial Patterns

Figure 65 shows that the 10 digit dialed number starting with 501 for inbound calls have a destination domain of **bvwddev75.com** uses route policy **Windstream_to_CS1K75**.

AVAYA Avaya Aura® System Manager 6.1 Help | About | Change Password | Log off admin

Routing Home

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

Dial Pattern Details Help ? Commit Cancel

General

* **Pattern:** 501

* **Min:** 10

* **Max:** 10

Emergency Call: ☐

SIP Domain: bvwddev75.com

Notes: In-coming Call from Windstream to CS1K75

Originating Locations and Routing Policies

Add Remove

1 Item Refresh Filter: Enable

<input type="checkbox"/>	Originating Location Name 1 ▲	Originating Location Notes	Routing Policy Name	Rank 2 ▲	Routing Policy Disabled	Routing Policy Destination	Routing Policy Notes
<input type="checkbox"/>	Belleville, Ont, Ca		Windstream to CS1K75	0	<input type="checkbox"/>	car3-ssg-carrier	Windstream to CS1K75

Select : All, None

Denied Originating Locations

Add Remove

0 Items Refresh Filter: Enable

<input type="checkbox"/>	Originating Location	Notes
--------------------------	----------------------	-------

* Input Required Commit Cancel

Figure 65 Session Manager Dial Pattern_501

Figure 66 shows all the dial patterns that were configured for inbound calls to the Enterprise.

AVAYA Avaya Aura® System Manager 6.1 Help | About | Change Password | Log off admin

Routing Home

Routing Policy Details Help ? Commit Cancel

General

* Name: Windstream to CS1K75

Disabled: ☐

Notes: Windstream to CS1K75

SIP Entity as Destination

Select

Name	FQDN or IP Address	Type	Notes
car3-ssg-carrier	10.10.97.178	Other	

Time of Day

Add Remove View Gaps/Overlaps

1 Item Refresh Filter: Enable

Ranking	Name	Mon	Tue	Wed	Thu	Fri	Sat	Sun	Start Time	End Time	Notes
0	24/7	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	00:00	23:59	Time Range 24/7

Select : All, None

Dial Patterns

Add Remove

1 Item Refresh Filter: Enable

Pattern	Min	Max	Emergency Call	SIP Domain	Originating Location	Notes
501	10	10	<input type="checkbox"/>	bvwdev7.com	Belleville,Ont,Ca	In-coming Call from Windstream to CS1K75

Figure 66 Session Manager all Inbound Dial Patterns

6.8. Add/View Session Manager

The creation of a Session Manager element provides the linkage between System Manager and Session Manager. This was most likely done as part of the initial Session Manager installation. To add a Session Manager, navigate to **Home → Elements → Session Manager → Session Manager Administration** in the left navigation pane and click on the **New** button in the right pane. If the Session Manager already exists, click **View** to view the configuration.

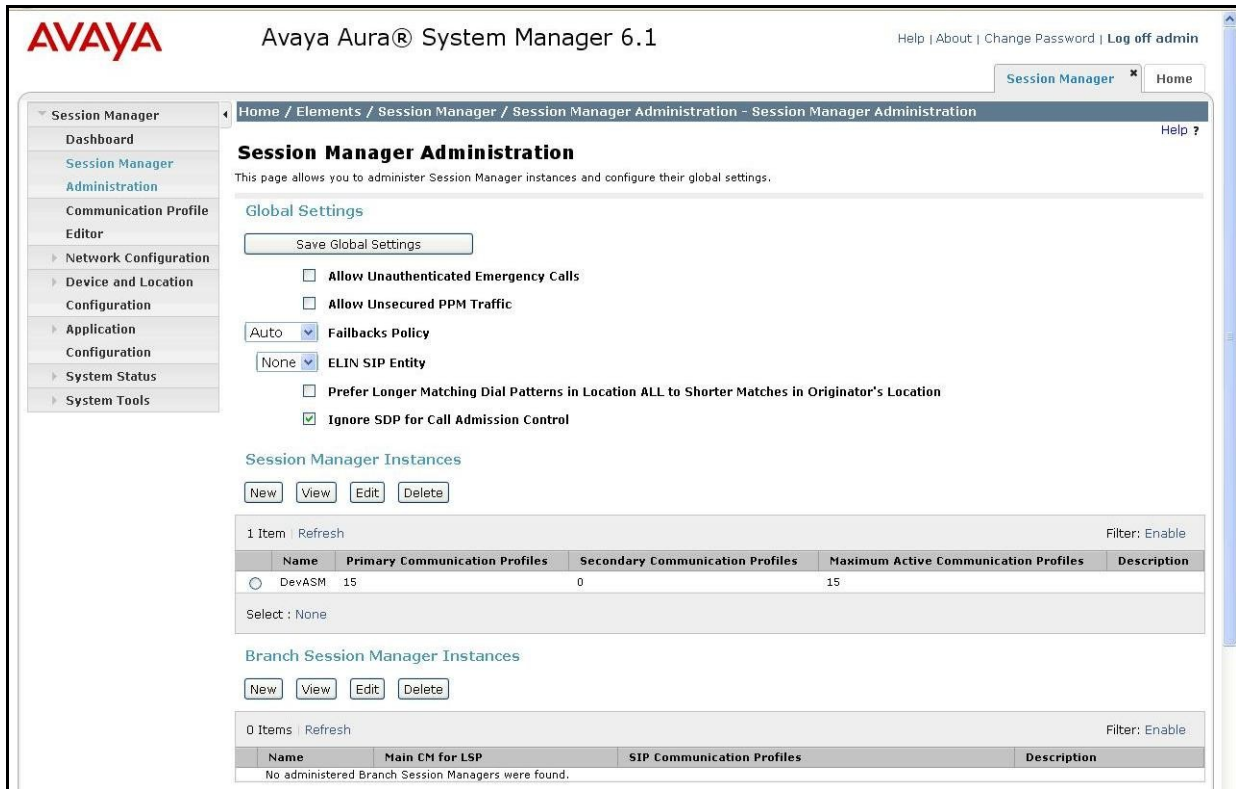


Figure 65 Session Manager Administration

Enter/verify the data as described below and shown in the following screen:

In the **General** section, enter the following values:

- **SIP Entity Name:** Select the SIP Entity created for Session Manager.
- **Description:** Add a brief description (optional).
- **Management Access Point Host Name/IP:** Enter the IP address of the Session Manager management interface.

In the **Security Module** section, enter the following values:

- **SIP Entity IP Address:** Should be filled in automatically based on the SIP Entity Name. Otherwise, enter IP address of the Session Manager signaling interface.
- **Network Mask:** Enter the network mask corresponding to the IP address of Session Manager.
- **Default Gateway:** Enter the IP address of the default gateway for Session Manager.

Figure 66 below shows the Session Manager values used for the compliance test. Use default values for the remaining fields. Click **Save** (not shown) to add this Session Manager.

AVAYA Avaya Aura® System Manager 6.1 [Help](#) | [About](#) | [Change Password](#) | [Log off admin](#)

[Session Manager](#) [Routing](#) [Home](#)

Session Manager [Home /Elements / Session Manager](#)

View Session Manager [Help ?](#) [Return](#)

General | Security Module | NIC Bonding | Monitoring | CDR | Personal Profile Manager (PPM) - Connection Settings | Event Server | [Expand All](#) | [Collapse All](#)

General

SIP Entity Name: DevASM

Description:

Management Access Point Host Name/IP: 10.10.97.197

Direct Routing to Endpoints: Enable

Security Module

SIP Entity IP Address: 10.10.97.198

Network Mask: 255.255.255.192

Default Gateway: 10.10.97.193

Call Control PHB: 46

QOS Priority: 6

Speed & Duplex: Auto

VLAN ID:

NIC Bonding

Enable Bonding: ☐

Driver Monitoring Mode: ARP

ARP Interval (msecs): 100

ARP Target IP:

ARP Target IP:

Figure 66 Session Manager View

7. Configure Acme Packet Net-Net 3800

This section describes the configuration of the Acme Packet Net-Net 3800 necessary for interoperability with the Communication Server 1000 and Windstream systems. The Net-Net 3800 was configured via the Acme Packet Command Line Interface (ACLI). This section assumes the reader is familiar with accessing and configuring the Acme Packet products.

This section will not attempt to describe each component in its entirety but instead will highlight critical fields in each component which relates to the functionality in these Application Notes. The remaining fields are generally the default/standard value used by the Net-Net 3800 for that field.

In this testing, according to the configuration reference in **Figure 1**, the Avaya elements reside on the Private side and the Windstream elements reside on the Public side of the network.

7.1. Acme Packet Command Line Interface Summary

The Net-Net 3800 is configured using the Acme Packet Command Line Interface (ACLI). The following are the generic ACLI steps for configuring various elements.

1. Access the console port of the Net-Net 3800 using a PC and a terminal emulation program such as HyperTerminal (use the RJ-45 to DB9 adapter as packaged with the Net-Net 3800 server for cable connection). Use the following settings for the serial port on the PC.
 - Bits per second: 115200
 - Data bits: 8
 - Parity: None
 - Stop bits: 1
 - Flow control: None
2. Log in to the Net-Net 3800 with the user password.
3. Enable the Super-user mode by entering the **enable** command and then the super user password. The command prompt will change to include a “#” instead of a “>” while in Super user mode. This level of system access (i.e. at the “acmesystem#” prompt) will be referred to as the *main* level of the ACLI. Specific sub-levels of the ACLI will then be accessed to configure specific *elements* and specific *parameters* of those elements.
4. In Super-user mode, enter the **configure terminal** command. The **configure terminal** command is used to access the system level where all operating and system elements may be configured. This level of system access will be referred to as the *configuration* level.
5. Enter the name of an element to be configured (e.g., **system**).
6. Enter the name of a sub-element, if any (e.g., **phy-interface**).
7. Enter the name of an element parameter followed by its value (e.g., **name INSIDE**).
8. Enter **done** to save changes to the element. Use of the **done** command causes the system to save and display the settings for the current element.
9. Enter **exit** as many times as necessary to return to the configuration level.
10. Repeat **Steps 5 - 9** to configure all the elements.
11. Enter **exit** to return to the main level.
12. Type **save-config** to save the entire configuration.
13. Type **activate-config** to activate the entire configuration.

After accessing different levels of the ACLI to configure elements and parameters, it is necessary to return to the main level in order to run certain tasks such as saving the configuration, activating the configuration, and rebooting the system.

Note – Net-Net 3800 provisioning applicable to the reference configuration is shown in **bold** text. Other parameters and setting are shown for informational purposes.

7.2. Physical and Network Interfaces

As part of the compliance test, the Ethernet slot 0/port 0 was connected to the internal corporate LAN. The Ethernet interface slot 1/port 0 was connected to the external un-trusted network. A network interface was defined for each physical interface to assign it a routable IP address.

The physical interface below defines the ports on the interface connected to the network on which the Avaya elements reside.

phy-interface	
name	INSIDE
operation-type	Media
port	0
slot	0
virtual-mac	
admin-state	enabled
auto-negotiation	enabled
duplex-mode	FULL
speed	100
overload-protection	disabled
last-modified-by	admin@console
last-modified-date	2011-29-07 10:11:20

The physical interface below defines the ports on the interface connected to the network on which the Windstream elements reside.

phy-interface	
name	OUTSIDE
operation-type	Media
port	0
slot	1
virtual-mac	
admin-state	enabled
auto-negotiation	enabled
duplex-mode	FULL
speed	100
overload-protection	disabled
last-modified-by	admin@console
last-modified-date	2011-29-07 10:11:30

The network interface below defines the IP addresses on the interface connected to the network on which the Avaya elements reside.

network-interface	
name	INSIDE
sub-port-id	0
description	
hostname	
ip-address	10.10.97.184
pri-utility-addr	
sec-utility-addr	
netmask	255.255.255.192
gateway	10.10.97.129
sec-gateway	
gw-heartbeat	
state	disabled
heartbeat	0
retry-count	0
retry-timeout	1
health-score	0
dns-ip-primary	
dns-ip-backup1	
dns-ip-backup2	
dns-domain	
dns-timeout	11
hip-ip-list	10.10.97.184
ftp-address	
icmp-address	10.10.97.184
snmp-address	
telnet-address	
ssh-address	
last-modified-by	admin@console
last-modified-date	2011-29-07 10:20:11

The network interface below defines the IP addresses on the interface connected to the network on which the Windstream elements reside.

network-interface	
name	OUTSIDE
sub-port-id	0
description	
hostname	
ip-address	10.10.98.98
pri-utility-addr	
sec-utility-addr	
netmask	255.255.255.224
gateway	10.10.98.97
sec-gateway	
gw-heartbeat	
state	disabled
heartbeat	0
retry-count	0
retry-timeout	1
health-score	0
dns-ip-primary	
dns-ip-backup1	
dns-ip-backup2	
dns-domain	
dns-timeout	11
hip-ip-list	10.10.98.98
ftp-address	
icmp-address	10.10.98.98
snmp-address	
telnet-address	
ssh-address	
last-modified-by	admin@console
last-modified-date	2011-29-07 15:22:28

7.3. Realm

A realm represents a group of related Net-Net 3800 components. Two realms were defined for the compliance test.

The realm configuration “INSIDE” below represents the internal network on which the Avaya elements reside.

realm-config	
identifier	INSIDE
description	
addr-prefix	0.0.0.0
network-interfaces	
	INSIDE:0
mm-in-realm	disabled
<Text removed for brevity>	

The realm configuration “OUTSIDE” below represents the external network on which the Windstream system resides.

realm-config	
identifier	OUTSIDE
description	
addr-prefix	0.0.0.0
network-interfaces	
	OUTSIDE:0
mm-in-realm	disabled
<Text removed for brevity>	

7.4. Session Agent

A session agent defines the characteristics of a signaling peer to the Net-Net 3800.

The **session agent** below represents the Windstream border element. The Acme will attempt to send calls to the border element. The **in-manipulationid** and **out-manipulationid** define the SIP header manipulation applying to the OUTSIDE realm.

session-agent	
hostname	20.20.242.26
ip-address	20.20.242.26
port	5060
state	enabled
app-protocol	SIP
app-type	
transport-method	UDP
realm-id	OUTSIDE
egress-realm-id	
description	Windstream_CS1K 7.5
carriers	
allow-next-hop-lp	enabled
constraints	disabled
<Text removed for brevity>	
ping-interval	0
ping-send-mode	keep-alive
<Text removed for brevity>	
ping-from-user-part	
li-trust-me	disabled
in-manipulationid	WS_TO_CS1K75_NAT_IP
out-manipulationid	CS1K75_TO_WS_NAT_IP
manipulation-string	

The **session agent** below represents the configuration for inside interface to connect to Session Manager mentioned in **Section 6.4**

```
session-agent
  hostname          10.10.97.198
  ip-address        10.10.97.198
  port              5060
  state             enabled
  app-protocol      SIP
  app-type
  transport-method  UDP
  realm-id          INSIDE
  egress-realm-id
  description       Windstream_CS1K7.5
  carriers
  allow-next-hop-lp enabled
  constraints       disabled
  <Text removed for brevity>
```

7.5. SIP Configuration

The SIP configuration (*sip-config*) defines the global system-wide SIP parameters.

The key SIP configuration (*sip-config*) field is:

- **home-realm-id**: The name of the realm on the private side of the Net-Net 3800.
- **egress-realm-id**: The name of the realm on the private side of the Net-Net 3800.

```
sip-config
  state             enabled
  operation-mode     dialog
  dialog-transparency enabled
  home-realm-id      INSIDE
  egress-realm-id    INSIDE
  nat-mode           None
```

<Text removed for brevity>

7.6. SIP Interface

The SIP interface (*sip-interface*) defines the receiving characteristics of the SIP interfaces on the Net-Net 3800. Two SIP interfaces were defined; one for each realm.

The SIP interface below is used to communicate with the Communication Server 1000 system.

```
sip-interface
state                               enabled
realm-id                           INSIDE
description
sip-port
  address                           10.10.97.184
  port                             5060
  transport-protocol               UDP
  tls-profile
  allow-anonymous                   all

<Text removed for brevity>
```

The SIP interface below is used to communicate with the Windstream system.

```
sip-interface
state                               enabled
realm-id                           OUTSIDE
description
sip-port
  address                           10.10.98.98
  port                             5060
  transport-protocol               UDP
  tls-profile
  allow-anonymous                   all

<Text removed for brevity>
```

7.7. SIP Manipulation

SIP manipulations are rules used to modify the SIP messages (if necessary) for interoperability. The following sip-manipulation **CS1K75_TO_WS_NAT_IP** is applied to **OUTSIDE** realm *out-manipulationid*. These rules perform the following:

- The header rule **manipRURI** changes Avaya Domain Name/IP address to 20.20.242.26 (Windstream border element) in the Request URI headers sent to Windstream.
- The header rule **manipTo** performs address translation and topology hiding for SIP messages between the Windstream system and the Avaya elements.

sip-manipulation	
name	CS1K75_TO_WS_NAT_IP
description	
split-headers	
join-headers	
header-rule	
name	manipRURI
header-name	request-uri
action	manipulate
comparison-type	case-sensitive
msg-type	any
methods	INVITE
match-value	
new-value	
element-rule	
name	modRURI
parameter-name	
type	uri-host
action	replace
match-val-type	any
comparison-type	case-sensitive
match-value	
new-value	20.20.242.26
header-rule	
name	manipTo
header-name	To
action	manipulate
comparison-type	case-sensitive
msg-type	any
methods	
match-value	
new-value	
element-rule	
name	To

parameter-name	
type	uri-host
action	replace
match-val-type	any
comparison-type	case-sensitive
match-value	
new-value	\$REMOTE_IP
header-rule	
name	HistRegex
header-name	History-Info
action	store
comparison-type	pattern-rule
msg-type	request
methods	INVITE
match-value	()
new-value	
element-rule	
name	GetUser
parameter-name	
type	uri-user
action	store
match-val-type	any
comparison-type	pattern-rule
match-value	
new-value	
element-rule	
name	GetHost
parameter-name	
type	uri-host
action	store
match-val-type	any
comparison-type	pattern-rule
match-value	
new-value	
element-rule	
name	GetUserReason1
parameter-name	
type	header-value
action	store
match-val-type	any
comparison-type	pattern-rule
match-value	(.*)(Moved)(.*)
new-value	
element-rule	
name	GetUserReason2

parameter-name	
type	header-value
action	store
match-val-type	any
comparison-type	pattern-rule
match-value	(.*)(Busy)(.*)
new-value	
element-rule	
name	GetUserReason3
parameter-name	
type	header-value
action	store
match-val-type	any
comparison-type	pattern-rule
match-value	(.*)(Unavailable)(.*)
new-value	
header-rule	
name	AddDiversion1
header-name	Diversion
action	add
comparison-type	boolean
msg-type	request
methods	INVITE
match-value	\$HistRegex[0].\$GetUserReason1
new-value	<sip:+\$HistRegex[0].\$GetUser.\$0+@+\$HistRegex[0].\$GetHost.\$0+>;privacy=off;reason=unconditional;screen=no
header-rule	
name	AddDiversion2
header-name	Diversion
action	add
comparison-type	boolean
msg-type	request
methods	INVITE
match-value	\$HistRegex[0].\$GetUserReason2
new-value	<sip:+\$HistRegex[0].\$GetUser.\$0+@+\$HistRegex[0].\$GetHost.\$0+>;privacy=off;reason=user\'-busy;screen=no
header-rule	
name	AddDiversion3
header-name	Diversion
action	add
comparison-type	boolean
msg-type	request
methods	INVITE

match-value	\$HistRegex[0].\$GetUserReason3
new-value	<sip:+\$HistRegex[0].\$GetUser.\$0+@+\$HistRegex[0].\$GetHost.\$0+>;privacy=off;reason=no\-answer;screen=no
header-rule	
name	delHistInfo
header-name	History-Info
action	delete
comparison-type	case-sensitive
msg-type	any
methods	INVITE
match-value	
new-value	
header-rule	
name	manipFrom
header-name	From
action	manipulate
comparison-type	case-sensitive
msg-type	any
methods	
match-value	
new-value	
element-rule	
name	From
parameter-name	
type	uri-host
action	replace
match-val-type	any
comparison-type	case-sensitive
match-value	
new-value	10.10.98.98
last-modified-by	admin@console
last-modified-date	2011-29-07 21:42:22

The following sip-manipulation **WS_TO_CS1K75_NAT_IP**, *in-manipulationid*, is applied to **OUTSIDE** realm and translates the SIP header information for Avaya Communication Server 1000 to understand. These rules perform the following:

- The header rules **manipRURI** changes IP address to the Avaya Communication Server 1000 Domain Name in the Request URI headers sent to the Avaya Communication Server 1000 elements.

sip-manipulation	
name	WS_TO_CS1K75_NAT_IP
description	
split-headers	

join-headers	
header-rule	
name	manipRURI
header-name	request-uri
action	manipulate
comparison-type	case-sensitive
msg-type	any
methods	INVITE
match-value	
new-value	
element-rule	
name	modRURI
parameter-name	
type	uri-host
action	replace
match-val-type	any
comparison-type	case-sensitive
match-value	
new-value	bvwdev75.com
header-rule	
name	manipTo
header-name	To
action	manipulate
comparison-type	case-sensitive
msg-type	any
methods	
match-value	
new-value	
element-rule	
name	To
parameter-name	
type	uri-host
action	replace
match-val-type	any
comparison-type	case-sensitive
match-value	
new-value	bvwdev75.com
last-modified-by	admin@console
last-modified-date	2011-29-07 12:52:23

7.8. Steering Pools

Steering pools define the range of ports to be used for the RTP voice stream. Two steering pools were defined, one for each realm.

The key steering pool (*steering-pool*) fields are:

- **ip-address:** The address of the interface on the Net-Net 3800.
- **start-port:** An even number of the port that begins the range.
- **end-port:** An odd number of the port that ends the range.
- **realm-id:** The realm to which this steering pool is assigned.

steering-pool	
ip-address	10.10.98.98
start-port	20000
end-port	40000
realm-id	OUTSIDE
network-interface	
last-modified-by	admin@console
last-modified-date	2011-29-07 22:20:07
steering-pool	
ip-address	10.10.97.184
start-port	20000
end-port	40000
realm-id	INSIDE
network-interface	
last-modified-by	admin@console
last-modified-date	2011-29-07 22:20:22

7.9. Local Policy

The local policies below govern the routing of SIP messages from elements on the network on which the Avaya elements, reside to the Windstream system and vice versa.

local-policy	
from-address	20.20.242.26
to-address	5012871070
	5012871071
	5012871072
	5012871073
	5012871074
	5012871490
	5012871491
	5012871492

	5012871493
	5012871494
	5012871495
	5012871496
	5012871497
	5012871498
	5012871499
source-realm	OUTSIDE
description	WS_TO_CS1K75
activate-time	N/A
deactivate-time	N/A
state	enabled
policy-priority	none
last-modified-by	admin@console
last-modified-date	2011-29-07 14:44:50
policy-attribute	
next-hop	10.10.97.198
realm	INSIDE
action	none
terminate-recursion	disabled
carrier	
start-time	0000
end-time	2400
days-of-week	U-S
cost	0
app-protocol	SIP
state	enabled
methods	
media-profiles	
lookup	single
next-key	
eloc-str-lkup	disabled
eloc-str-match	

local-policy	
from-address	anonymous.invalid
	bvwdev75.com
to-address	*
source-realm	INSIDE
description	CS1K75_TO_WS

activate-time	N/A
deactivate-time	N/A
state	enabled
policy-priority	none
last-modified-by	admin@console
last-modified-date	2011-29-07 20:25:30
policy-attribute	
next-hop	20.20.242.26
realm	OUTSIDE
action	none
terminate-recursion	disabled
carrier	
start-time	0000
end-time	2400
days-of-week	U-S
cost	0
app-protocol	SIP
state	enabled
methods	
media-profiles	
lookup	single
next-key	
eloc-str-lkup	disabled
eloc-str-match	

8. Verification Steps

The following steps may be used to verify the configuration.

8.1. General

Place an inbound call from a PSTN phone to an internal Avaya phone, answer the call, and verify that two-way speech path exists. Verify that the call remains stable for several minutes and disconnects properly.

8.2. Verification of an Active Call on Call Server

a) Active Call Trace (LD 80)

The following is an example of one of the commands available on the Communication Server 1000 to trace the DN for which the call is in progress or idle. The call scenario involved PSTN phone number 6139675205 calling 5012871492.

- Login on to Signaling Server 10.10.97.177 with admin account and password.
- Issue a command “cslogin” to login on to the Call Server.
- Log in to the Overlay command prompt, issue the command **LD 80** and then **trace 0 1492**.
- After the call is released, issue command **trac 0 1492** again to see if the DN is released back to idle state.

Below is the actual output of the Call Server Command Line mode when the 1492 is in call state:

```
USERID? admin
PASS?....
.
TTY #09 LOGGED IN admin 16:22 29/7/2011
.
>ld 80
.trac 0 1492

ACTIVE VTN 96 0 00 02

ORIG VTN 100 0 00 00 VTRK IPTI RMBR 100 1 INCOMING VOIP GW CALL
FAR-END SIP SIGNALLING IP: 10.10.97.184
FAR-END MEDIA ENDPOINT IP: 10.10.97.184 PORT: 21638
FAR-END VendorID: Nortel CS1000 SIP GW release_7.5 version_ssLinux-7.50.17
TERM VTN 96 0 00 02 KEY 0 SCR MARP CUST 0 DN 1492 TYPE 2002P2
SIGNALLING ENCRYPTION: INSEC
MEDIA ENDPOINT IP: 10.10.98.36 PORT: 5200
MEDIA PROFILE: CODEC G.711 MU-LAW PAYLOAD 20 ms VAD OFF
RFC2833: RXPT 101 TXPT 101 DIAL DN 1492
MAIN_PM ESTD
TALKSLOT ORIG 17 TERM 81
QUEUE NONE
CALL ID 501 84

---- ISDN ISL CALL (ORIG) ----
CALL REF # = 484
BEARER CAP = VOICE
HLC =
CALL STATE = 10 ACTIVE
CALLING NO = NUM_PLAN:UNKNOWN TON:UNKNOWN ESN:UNKNOWN
CALLED NO = 5012871492 NUM_PLAN:UNKNOWN TON:UNKNOWN ESN:UNKNOWN
```

And this is the example after the call on 1492 is finished.

```
.trac 0 1492
IDLE VTN 96 0 00 02 MARP
```

b) SIP Trunk monitoring (LD 32)

Place a call inbound from PSTN (6139675205) to an internal device (5012871492). Then check the SIP trunk status by using LD 32, one trunk is BUSY

```
>ld 32
NPR000
.stat 100 0
031 UNIT(S) IDLE
001 UNIT(S) BUSY
000 UNIT(S) DSBL
000 UNIT(S) MBSY
```

After the call is released, check all SIP trunk status changed to IDLE state.

```
.stat 100 0
032 UNIT(S) IDLE
000 UNIT(S) BUSY
000 UNIT(S) DSBL
000 UNIT(S) MBSY
```

8.3. Protocol Trace

Below is a wireshark trace of the same call scenario described in **Section 8.2**. It is shown in text format below. Note that only detail of the INVITE message is being shown here.

No.	Time	Source	Destination	Protocol Info
41	36.977060	20.20.242.26	10.10.98.98	SIP/SDP Request: INVITE sip:5012871492@10.10.98.98:5060, with session description

Frame 41: 841 bytes on wire (6728 bits), 841 bytes captured (6728 bits)
Ethernet II, Src: Nortel_01:b4:49 (00:17:65:01:b4:49), Dst: AcmePack_a1:8c:a5 (00:08:25:a1:8c:a5)
Internet Protocol, Src: 20.20.242.26 (20.20.242.26), Dst: 10.10.98.98 (10.10.98.98)
User Datagram Protocol, Src Port: sip (5060), Dst Port: sip (5060)
Session Initiation Protocol
Request-Line: INVITE sip:5012871492@10.10.98.98:5060 SIP/2.0
Message Header
Via: SIP/2.0/UDP 20.20.242.26:5060;branch=z9hG4bK1n34a920dgnhces1o081.1
Allow-Events: message-summary, refer, dialog, line-seize, presence, call-info
Max-Forwards: 69
Call-ID: E3F6469F@75.89.98.228
From: "Anonymous"
<sip:6139675205@20.20.242.26:5060;transport=udp>;tag=75.89.98.228+1+23db11+c56cdbdc;i
sup-oli=00
To: <sip:5012871492@10.10.98.98>
CSeq: 1006829771 INVITE
Expires: 180
Organization:
Supported: 100rel
Content-Length: 170
Content-Type: application/sdp
Contact: "Anonymous" <sip:61396715205@20.20.242.26:5060;transport=udp>;isup-oli=00
Privacy: id
Message Body

No.	Time	Source	Destination	Protocol Info
42	36.978738	10.10.98.98	20.20.242.26	SIP Status: 100 Trying

No.	Time	Source	Destination	Protocol Info
43	37.026764	10.10.98.98	20.20.242.26	SIP Status: 180 Ringing

No.	Time	Source	Destination	Protocol Info
44	37.096280	20.20.242.26	10.10.98.98	SIP Request: PRACK sip:5012871491@10.10.98.98:5060;user=phone;transport=udp

No.	Time	Source	Destination	Protocol Info
45	37.105426	10.10.98.98	20.20.242.26	SIP Status: 200 OK

No.	Time	Source	Destination	Protocol Info
51	40.692824	10.10.98.98	20.20.242.26	SIP/SDP Status: 200 OK, with session description

No.	Time	Source	Destination	Protocol Info
70	41.191712	10.10.98.98	20.20.242.26	SIP/SDP Status: 200 OK, with session description

No.	Time	Source	Destination	Protocol Info
121	42.192600	10.10.98.98	20.20.242.26	SIP/SDP Status: 200 OK, with session description

No.	Time	Source	Destination	Protocol Info
126	42.265984	20.20.242.26	10.10.98.98	SIP Request: ACK sip:5012871491@10.10.98.98:5060;user=phone;transport=udp

No.	Time	Source	Destination	Protocol Info
2444	65.105429	10.10.98.98	20.20.242.26	SIP Request: BYE sip:anonymous@20.20.242.26:5060;transport=udp

No.	Time	Source	Destination	Protocol Info
2452	65.175428	20.20.242.26	10.10.98.98	SIP Status: 200 OK

9. Conclusion

All of the test cases have been executed. Despite the number of observations seen during testing as noted in **Section 2.2**, the test result met the objectives outlined in **Section 2.1**. The Windstream system is considered **compliant** with the Avaya Communication Server 1000 Release 7.5.

10. Additional References

Product documentation for ACME Packet may be found at:

<http://www.acmepacket.com/support.htm>

Product documentation for Avaya, including the following, is available at:

<http://support.avaya.com/>

[1] *Network Routing Service Fundamentals, Avaya Communication Server 1000, Release 7.5, Document Number NN43001-130, Revision 03.02, November 2010.*

[2] *IP Peer Networking Installation and Commissioning, Avaya Communication Server 1000, Release 7.5, Document Number NN43001-313, Revision: 05.02, November 2010*

[3] *Communication Server 1000E Overview, Avaya Communication Server 1000, Release 7.5, Document Number NN43041-110, Revision: 05.02, January 2011*

[4] *Communication Server 1000 Unified Communications Management Common Services Fundamentals, Avaya Communication Server 1000, Release 7.5, Document Number NN43001-116, Revision 05.08, January 2011*

[5] *Communication Server 1000 Dialing Plans Reference, Avaya Communication Server 1000, Release 7.5, Document Number NN43001-283, Revision 05.02, November 2010*

[6] *Product Compatibility Reference, Avaya Communication Server 1000, Release 7.5, Document Number NN43001-256, Revision 05.02, February 2011*

[7] *Administering Avaya Aura® Session Manager, Release 6.0, Document Number 03-603324, Issue 4, Feb 2011*

[8] *Installing and Configuring Avaya Aura® Session Manager, Release 6.0, Document Number 03-603473, Issue 2, Nov 2010*

©2011 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.