



Avaya Solution & Interoperability Test Lab

Application Notes for Avaya Communication Server 1000E 7.5 and Acme Packet 3820 Net-Net® Session Director 6.3.0 with CenturyLink SIP Trunk Service (Legacy Qwest) – Issue 1.0

Abstract

These Application Notes describe the steps to configure Session Initiation Protocol (SIP) Trunking between CenturyLink SIP Trunk Service (Legacy Qwest) using Sonus NBS version 7.3.5R6 and an Avaya SIP-enabled enterprise solution. The Avaya solution consists of Avaya Communication Server 1000E, Acme Packet 3820 Net-Net® Session Director and various Avaya endpoints.

CenturyLink is a member of the Avaya DevConnect Service Provider program. 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

1.	Introduction.....	4
2.	General Test Approach and Test Results.....	4
2.1.	Interoperability Compliance Testing.....	5
2.2.	Test Results	5
2.3.	Support	6
3.	Reference Configuration	6
4.	Equipment and Software Validated	7
5.	Configure Avaya Communication Server 1000E	7
5.1.	Administer an IP Telephony Node.....	9
5.1.1.	Obtain Node IP Address	9
5.1.2.	Terminal Proxy Server (TPS)	10
5.1.3.	Quality of Service (QoS)	11
5.1.4.	Voice Gateway and Codecs	12
5.1.5.	SIP Gateway.....	13
5.1.6.	Synchronize Node Configuration	16
5.2.	Virtual Superloops.....	18
5.3.	Media Gateway	18
5.4.	Virtual D-Channel, Routes and Trunks.....	22
5.4.1.	Virtual D-Channel Configuration	22
5.4.2.	Routes and Trunks Configuration	24
5.5.	Dialing and Numbering Plans	26
5.5.1.	Route List Block	26
5.5.2.	NARS Access Code	28
5.5.3.	Numbering Plan Area Codes	29
5.5.4.	Special Numbers	31
5.5.5.	Incoming Digit Translation.....	32
5.6.	Zones and Bandwidth.....	33
5.7.	Example CS1000E Telephone Users	35
5.7.1.	Example SIP Phone DN 7108, Codec Considerations.....	35
5.7.2.	Example Digital Phone DN 7107 with Call Waiting.....	36
5.7.3.	Example Analog Port with DN 7106, Fax	37
5.8.	Save Configuration.....	38
6.	Configure Acme Packet 3820 Net-Net® Session Director.....	38
6.1.	Acme Packet Command Line Interface Summary	40
6.2.	System Configuration.....	41
6.3.	Physical and Network Interfaces.....	42
6.4.	Realm	44
6.5.	SIP Configuration.....	46
6.6.	SIP Interface.....	47
6.7.	Session Agent.....	48
6.8.	Session Agent Group.....	51

6.9.	SIP Manipulation.....	52
6.10.	Steering Pools	58
6.11.	Local Policy	59
7.	CenturyLink SIP Trunk Service Configuration	61
8.	Verification	61
8.1.	Avaya Communication Server 1000E Verifications	61
8.1.1.	IP Network Maintenance and Reports Commands	61
8.1.2.	System Maintenance Commands	63
9.	Conclusion	64
10.	Additional References.....	65
	Appendix A: Acme Packet 3820 Configuration File	65

1. Introduction

These Application Notes describe a sample configuration of Avaya Communication Server 1000E release 7.5 and Acme Packet 3820 Net-Net Session Director 6.2.0 (Acme Packet 3820) integration with CenturyLink SIP Trunk Service (Legacy Qwest) using Sonus NBS version 7.3.5R6. CenturyLink can offer SIP trunk service using several different platform technologies in the CenturyLink network. These Application Notes correspond to the SIP trunk service offered using a Sonus platform in the network.

In the sample configuration, the Acme Packet 3820 is used as an edge device between Avaya Customer Premise Equipment (CPE) and CenturyLink SIP Trunk. The Acme Packet 3820 performs SIP header manipulation and provides Network Address Translation (NAT) functionality to convert the private Avaya CPE IP addressing to IP addressing appropriate for the CenturyLink SIP Trunk access method.

CenturyLink SIP Trunk Service is positioned for customers that have an IP-PBX or IP-based network equipment with SIP functionality, but need a form of IP transport and local services to complete their solution.

CenturyLink SIP Trunk Service will enable delivery of origination and termination of local, long-distance and toll-free traffic across a single broadband connection. A SIP signaling interface will be enabled to the Customer Premises Equipment (CPE). CenturyLink SIP Trunk Service will also offer remote DID capability for a customer wishing to offer local numbers to their customers that can be aggregated in SIP format back to customer.

DevConnect Compliance Testing is conducted jointly by Avaya and DevConnect members. The jointly-defined test plan focuses on exercising APIs and/or standards-based interfaces pertinent to the interoperability of the tested products and their functionalities. DevConnect Compliance Testing is not intended to substitute full product performance or feature testing performed by DevConnect members, nor is it to be construed as an endorsement by Avaya of the suitability or completeness of a DevConnect member's solution.

2. General Test Approach and Test Results

The general test approach was to configure a simulated enterprise site using Avaya Communication Server 1000E (CS1000E) and Acme Packet 3820 to connect to the public Internet using a broadband connection. The enterprise site was configured to connect to CenturyLink SIP Trunk Service. This configuration (shown in **Figure 1**) was used to exercise the features and functionality listed in **Section 2.1**.

DevConnect Compliance Testing is conducted jointly by Avaya and DevConnect members. The jointly-defined test plan focuses on exercising APIs and/or standards-based interfaces pertinent to the interoperability of the tested products and their functionalities. DevConnect Compliance Testing is not intended to substitute full product performance or feature testing performed by DevConnect members, nor is it to be construed as an endorsement by Avaya of the suitability or completeness of a DevConnect member's solution.

2.1. Interoperability Compliance Testing

To verify SIP trunking interoperability, the following features and functionality were covered during the interoperability compliance test:

- Incoming PSTN calls to various phone types. Phone types included UNISim, SIP, digital, and analog telephones at the enterprise. All inbound PSTN calls were routed to the enterprise across the SIP trunk from the service provider.
- Outgoing PSTN calls from various phone types. Phone types included UNISim, SIP, digital, and analog telephones at the enterprise. All outbound PSTN calls were routed from the enterprise across the SIP trunk to the service provider.
- Inbound and outbound PSTN calls to/from Avaya one-X Communicator (soft client).
- Various call types including: local, long distance, international, outbound toll-free, operator assisted calls, emergency calls (911) and local directory assistance (411).
- Inbound toll-free calls.
- Codecs G.729A, G.729B and G.711MU.
- DTMF transmission using RFC 2833.
- T.38 Fax.
- Caller ID presentation and Caller ID restriction.
- Voicemail navigation for inbound and outbound calls.
- User features such as hold and resume, transfer, and conference.
- Off-net call forwarding and Mobile-X (extension to cellular).

Items not supported or not tested included the following:

- SIP REFER method is not supported by Avaya CS1000E.
- Mid-Call features using Mobile-X were not tested.

2.2. Test Results

Interoperability testing of CenturyLink SIP Trunk Service was completed with successful results for all test cases with the exception of the observations/limitations described below.

- **Calling Party Number (PSTN transfers):** The calling party number displayed on the PSTN phone is not updated to reflect the true connected party on calls that are transferred to the PSTN. After the call transfer is complete, the calling party number displays the number of the transferring party and not the actual connected party. The PSTN phone display is ultimately controlled by the PSTN provider, thus this behavior is not necessarily indicative of a limitation of the combined Avaya/CenturyLink SIP Trunk Service solution. It is listed here simply as an observation.
- **History-Info header:** The CenturyLink SIP Trunk Service does not support SIP History Info Headers. Instead, the CenturyLink SIP Trunk Service requires that SIP Diversion Header be sent for redirected calls. The CS1000E includes History-Info header in messaging sent to Acme Packet 3820. A header manipulation rule was created in the Acme Packet 3820 to add a valid Diversion header for redirected calls. See **Section 6.9** and **Appendix A**.

CenturyLink SIP Trunk Service (Legacy Qwest) passed compliance testing.

2.3. Support

For technical support on the CenturyLink SIP Trunk Service, contact CenturyLink using the Customer Care links at www.centurylink.com.

3. Reference Configuration

Figure 1 illustrates the sample configuration used for the DevConnect compliance testing. The configuration is comprised of the Avaya CPE location connected via a T1 Internet connection to the CenturyLink SIP Trunks to East and West servers. The Avaya CPE location simulates a customer site. At the edge of the Avaya CPE location, an Acme Packet 3820 provides NAT functionality and SIP header manipulation. The Acme Packet 3820 receives traffic from CenturyLink SIP Trunk Service on port 5060 and sends traffic to the CenturyLink SIP Trunk Service using destination port 5060, using the UDP protocol. For security reasons, any actual public IP addresses used in the configuration have been replaced with private IP addresses. Similarly, any references to real routable PSTN numbers have also been changed to numbers that cannot be routed by the PSTN.

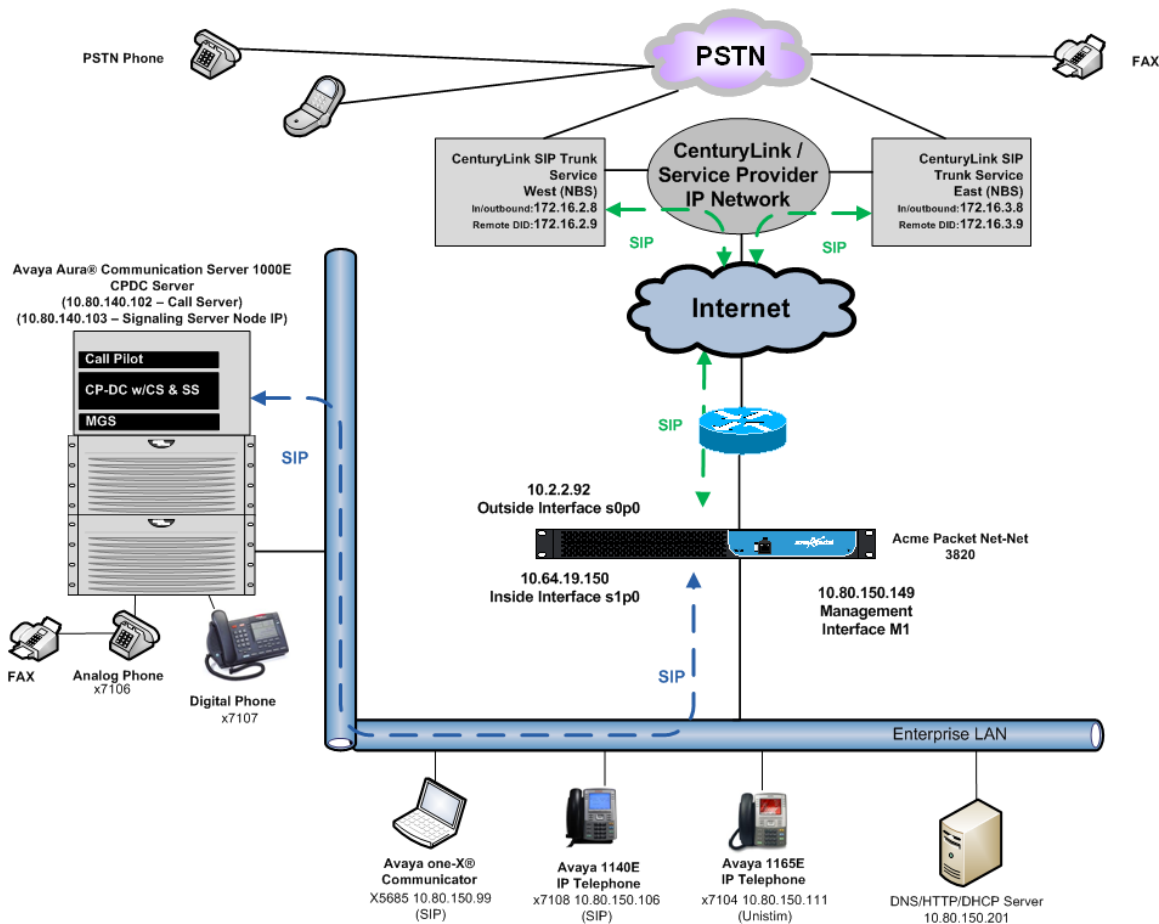


Figure 1: Avaya Interoperability Test Lab Configuration

4. Equipment and Software Validated

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

Avaya IP Telephony Solution Components	
Component	Release
Avaya Communication Server 1000E running on CP+DC server as co-resident configuration	<ul style="list-style-type: none">• Call Server: 7.50 .17 GA (CoRes) Service Pack: 7.50.17_20120110• SSG Server: 7.50.17 GA• SLG Server: 7.50.17 GA
Communication Server 1000E Media Gateway	CSP Version: MGCC CD02 MSP Version: MGCM AB01 APP Version: MGCA BA15 FPGA Version: MGCF AA19 BOOT Version: MGCB BA15 DSP1 Version: DSP4 AB01 BCSP Version: MGCC CD01
Acme Packet Net-Net Session Director 3820	6.3.0 MR-1
Avaya 1165E (UNISim)	0626C8A
Avaya 1140E (SIP)	04.03.09.00
Avaya one-X® Communicator (SIP)	CS6.1.1.02
Avaya M3904 (Digital)	n/a
Avaya 6210 Analog Telephone	n/a
CenturyLink (Legacy Qwest) SIP Trunking Solution Components	
Component	Release
Sonus Network Border Switch (NBS)	07.03.05 R006

Table 1: Equipment and Software Tested

The specific configuration above was used for the compatibility testing.

5. Configure Avaya Communication Server 1000E

This section describes the Avaya Communication Server 1000E configuration, focusing on the routing of calls to CenturyLink over a SIP trunk. In the sample configuration, Avaya Communication Server 1000E Release 7.5 was deployed as a co-resident system with the SIP Signaling Server, and Call Server applications all running on the same CP+DC server platform.

This section focuses on the SIP Trunking configuration. Although sample screens are illustrated to document the overall configuration, it is assumed that the basic configuration of the Call Server and SIP Signaling Server applications has been completed, and that the Avaya Communication Server 1000E is configured to support analog, digital, UNISim, and SIP telephones. For references on how to administer these functions of Avaya Communication Server 1000E, see **Section 10**.

Configuration will be shown using the web based Avaya Unified Communications Management GUI. The Avaya Unified Communications Management GUI may be launched directly via <https://<ipaddress>> where the relevant <ipaddress> in the sample configuration is 10.80.140.102. The following screen shows an abridged log in screen. Log in with appropriate credentials.

AVAYA

Use this page to access the server by IP address. You will need to log in again when switching to another server, even if it is in the same security domain.

Important: Only accounts which have been previously created in the primary security server are allowed. Expired or reset passwords that normally must be changed during login will fail authentication in this mode (use the link to manual password change instead). Local OS-authenticated User IDs cannot be used.

[Go to central login for Single Sign-On](#)

User ID:

Password:

[Change Password](#)

The Avaya Unified Communications Management Elements page will be used for configuration. Click on the Element Name corresponding to **CS1000** in the **Element Type** column. In the abridged screen below, the user would click on the Element Name **EM on cs1k-cpdc**.

Host Name: 10.80.140.102
Software Version: 02.20.0017.00(4713)
User Name admin

Elements

New elements are registered into the security framework, or may be added as simple hyperlinks. Click an element name to launch its management service. You can optionally filter the list by entering a search term.

	Element Name	Element Type ▲	Release	Address	Description
1	EM on cs1k-cpdc	CS1000	7.5	10.80.141.102	New element.
2	cs1k-cpdc.avayalab.com (primary)	Linux Base	7.5	10.80.140.102	Base OS element.
3	10.80.141.101	Media Gateway Controller	7.5	10.80.141.101	New element.
4	NRSM on cs1k-cpdc	Network Routing Service	7.5	10.80.141.102	New element.

5.1. Administer an IP Telephony Node

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

5.1.1. Obtain Node IP Address

Expand **System** → **IP Network** on the left panel and select **Nodes: Servers, Media Cards**.

The **IP Telephony Nodes** page is displayed as shown below. Click <Node id> in the Node ID column to view details of the node. In the sample configuration, **Node ID 1005** was used.

The screenshot shows the AVAYA CS1000 Element Manager interface. The left sidebar contains a tree view with 'System' expanded and 'Nodes: Servers, Media Cards' selected. The main content area is titled 'IP Telephony Nodes' and shows a table of nodes. The table has columns for Node ID, Components, Enabled Applications, ELAN IP, Node/TLAN IPv4, Node/TLAN IPv6, and Status. A single node with ID 1005 is listed. Below the table, there are checkboxes for 'Nodes', 'Component servers and cards', and 'IPv6 address'.

Node ID	Components	Enabled Applications	ELAN IP	Node/TLAN IPv4	Node/TLAN IPv6	Status
1005	1	SIP Line, LTPS, Gateway (SIPGw)	-	10.80.140.103		Synchronized

The **Node Details** screen is displayed with additional details as shown below. Under the **Node Details** heading at the top of the screen, make a note of the **TLAN Node IPV4 address**. In the sample screen below, the **Node IPV4 address** is **10.80.140.103**. This IP address will be needed when configuring Acme Packet 3820 with a Session Agent for the CS1000E in **Section 6.7**.

The screenshot shows the 'Node Details' screen for Node ID 1005. The page is titled 'Node Details (ID: 1005 - SIP Line, LTPS, Gateway (SIPGw))'. It contains several input fields for configuration. The 'Node ID' field is set to 1005. The 'Call server IP address' field is set to 10.80.141.102. The 'TLAN address type' is set to 'IPv4 only'. The 'Embedded LAN (ELAN)' section has a 'Gateway IP address' of 10.80.141.1 and a 'Subnet mask' of 255.255.255.0. The 'Telephony LAN (TLAN)' section has a 'Node IPv4 address' of 10.80.140.103 and a 'Subnet mask' of 255.255.255.0. There is also a 'Node IPv6 address' field which is currently empty. At the bottom, there are 'Save' and 'Cancel' buttons.

Node ID: 1005 * (0-9999)

Call server IP address: 10.80.141.102 *

TLAN address type: ☒ IPv4 only ☐ IPv4 and IPv6

Embedded LAN (ELAN)

Gateway IP address: 10.80.141.1 *

Subnet mask: 255.255.255.0 *

Telephony LAN (TLAN)

Node IPv4 address: 10.80.140.103 *

Subnet mask: 255.255.255.0 *

Node IPv6 address:

* Required Value.

Save Cancel

The following screen shows the **Associated Signaling Servers & Cards** heading at the bottom of the screen, simply to document the configuration.

Associated Signaling Servers & Cards

Select to add [Print](#) [Refresh](#)

<input type="checkbox"/> Hostname	Type	Deployed Applications	ELAN IP	TLAN IPv4	Role
<input type="checkbox"/> cs1k-cpdc	Signaling_Server	SIP Line, LTPS, Gateway, PD, Presence Publisher, IP Media Services	10.80.141.102	10.80.140.102	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.

5.1.2. Terminal Proxy Server (TPS)

On the **Node Details** screen, scroll down in the top window and select the **Terminal Proxy Server (TPS)** link as show below.

AVAYA CS1000 Element Manager

Managing: 10.80.141.102 Username: admin
System » IP Network » IP Telephony Nodes » Node Details

Node Details (ID: 1005 - SIP Line, LTPS, Gateway (SIPGw))

Subnet mask: 255.255.255.0 * Subnet mask: 255.255.255.0 *
Node IPv6 address:

IP Telephony Node Properties

- Voice Gateway (VGW) and Codecs
- Quality of Service (QoS)
- LAN
- SNTP
- Numbering Zones
- MCDN Alternative Routing Treatment (MALT) Causes

Applications (click to edit configuration)

- SIP Line
- Terminal Proxy Server (TPS)**
- Gateway (SIPGw)
- Personal Directories (PD)
- Presence Publisher
- IP Media Services

* Required Value.

Check the **UNISTim Line Terminal Proxy Server** check box and then click the **Save** button (not shown).

AVAYA CS1000 Element Manager

Managing: 10.80.141.102 Username: admin
System » IP Network » IP Telephony Nodes » Node Details » UNISTim Line Terminal Proxy Server (LTPS) Configuration

Node ID: 1005 - UNISTim Line Terminal Proxy Server (LTPS) Configuration Details

Firmware | DTLS | Network Connect Server

UNISTim Line Terminal Proxy Server: ☒ Enable proxy service on this node

Firmware

IP address: 0.0.0.0
Full file path: download/firmwa
Server Account/User ID:
Password:

DTLS

DTLS policy: Off

5.1.3. Quality of Service (QoS)

On the **Node Details** screen, scroll down in the top window and select the **Quality of Service (QoS)** link as shown below.

AVAYA CS1000 Element Manager

Managing: 10.80.141.102 Username: admin
System » IP Network » IP Telephony Nodes » Node Details

Node Details (ID: 1005 - SIP Line, LTPS, Gateway (SIPGw))

Subnet mask: 255.255.255.0 * Subnet mask: 255.255.255.0 *
Node IPv6 address:

IP Telephony Node Properties

- Voice Gateway (VGW) and Codecs
- Quality of Service (QoS)**
- LAN
- SNTP
- Numbering Zones
- MCDN Alternative Routing Treatment (MALT) Causes

Applications (click to edit configuration)

- SIP Line
- Terminal Proxy Server (TPS)
- Gateway (SIPGw)
- Personal Directories (PD)
- Presence Publisher
- IP Media Services

* Required Value. Save Cancel

Set the **Control packets** and **Voice packets** values to the desired Diffserv settings required on the internal network. The default Diffserv values are shown below. Click on the **Save** button.

Managing: 10.80.141.102 Username: admin
System » IP Network » IP Telephony Nodes » Node Details » Quality of Service (QoS)

Node ID: 1005 - Quality of Service (QoS)

Diffserv Codepoint (DSCP)

Enable Avaya automatic QoS: ☐

Control packets: 41 (0-63)
Voice packets: 47 (0-63)

VLAN tagging: ☐ 802.1Q support

802.1Q bits value (802.1P): 6 (0-7)

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

5.1.4. Voice Gateway and Codecs

On the **Node Details** screen, scroll down in the top window and select the **Voice Gateway (VGW) and Codecs** link as shown below.

AVAYA CS1000 Element Manager

Managing: 10.80.141.102 Username: admin
System » IP Network » IP Telephony Nodes » Node Details

Node Details (ID: 1005 - SIP Line, LTPS, Gateway (SIPGw))

Subnet mask: 255.255.255.0 * Subnet mask: 255.255.255.0 *
Node IPv6 address:

IP Telephony Node Properties

- **Voice Gateway (VGW) and Codecs**
- Quality of Service (QoS)
- LAN
- SNTP
- Numbering Zones
- MCDN Alternative Routing Treatment (MALT) Causes

Applications (click to edit configuration)

- SIP Line
- Terminal Proxy Server (TPS)
- Gateway (SIPGw)
- Personal Directories (PD)
- Presence Publisher
- IP Media Services

* Required Value. Save Cancel

The following screen shows the General parameters used in the sample configuration.

Managing: 10.80.141.102 Username: admin
System » IP Network » IP Telephony Nodes » Node Details » VGW and Codecs

Node ID: 1005 - Voice Gateway (VGW) and Codecs

General | Voice Codes | Fax

General

Echo cancellation: ☒ Use canceller, with tail delay: 128
☒ Dynamic attenuation

Voice activity detection threshold: -17 (-20 - +10 DBM)
Idle noise level: -65 (-327 - +327 DBM)

Signaling options: ☒ DTMF tone detection
☒ Low latency mode
☒ Remove DTMF delay (squench DTMF from TDM to IP)
☒ Modem/Fax pass-through
☒ V.21 Fax tone detection
☐ R factor calculation

Voice Codes

Codec G711: ☒ Enabled (required)
Voice payload size: 20 (milliseconds per frame)
Voice playout (litter buffer) delay: 40 80 (milliseconds)

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

Use the scroll bar on the right to find the area with heading **Voice Codecs**. Note that **Codec G.711** is enabled by default. The following screen shows the G.711 parameters used in the sample configuration.

Voice Codecs

Codec G.711: ☒ Enabled (required)

Voice payload size: 20 (milliseconds per frame)

Voice playout (jitter buffer) delay: 40 80 (milliseconds)

Nominal Maximum

Maximum delay may be automatically adjusted based on nominal settings.

☐ Voice Activity Detection (VAD)

For the **Codec G.729**, ensure that the **Enabled** box is checked, and the **Voice Activity Detection (VAD)** box is un-checked. In the sample configuration, the CS1000E was configured to include G.729A and G.711 in SDP Offers, in that order. During compliance testing, the G.729B codec was also tested by checking the **Voice Activity Detection (VAD)** box.

General | Voice Codecs | Fax

Codec G.729: ☒ Enabled

Voice payload size: 20 (milliseconds per frame)

Voice playout (jitter buffer) delay: 40 80 (milliseconds)

Nominal Maximum

Maximum delay may be automatically adjusted based on nominal settings.

☐ Voice Activity Detection (VAD)

5.1.5. SIP Gateway

The SIP Gateway is the SIP trunk between the CS1000E and Acme Packet 3820. On the **Node Details** screen, scroll down in the top window and select the **Gateway (SIPGw)** link as show below.

AVAYA CS1000 Element Manager

Managing: 10.80.141.102 Username: admin
System » IP Network » IP Telephony Nodes » Node Details

Node Details (ID: 1005 - SIP Line, LTPS, Gateway (SIPGw))

Subnet mask: 255.255.255.0 * Subnet mask: 255.255.255.0 *

Node IPv6 address:

IP Telephony Node Properties

- Voice Gateway (VGW) and Codecs
- Quality of Service (QoS)
- LAN
- SNTP
- Numbering Zones
- MCDN Alternative Routing Treatment (MALT) Causes

Applications (click to edit configuration)

- SIP Line
- Terminal Proxy Server (TPS)
- Gateway (SIPGw)**
- Personal Directories (PD)
- Presence Publisher
- IP Media Services

* Required Value.

Save Cancel

On the **Node ID: <id> – Virtual Trunk Gateway Configuration Details** page, enter the following values and use default values for remaining fields.

- **Sip domain name:** Enter the appropriate SIP domain for the customer network. In the sample configuration, **avayalab.com** was used in the Avaya Solutions and Interoperability Test lab environment.
- **Local SIP port:** Enter **5060**.
- **Gateway endpoint name:** Enter a descriptive name.
- **Application node ID:** Enter **<Node id>**. In the sample configuration, Node **1005** was used matching the node show in **Section 5.1.1**.

The values defined for the sample configuration are shown below.

The screenshot displays the AVAYA CS1000 Element Manager web interface. The top header shows the AVAYA logo and the title "CS1000 Element Manager". Below the header, a navigation tree on the left lists various system components. The main content area is titled "Node ID: 1005 - Virtual Trunk Gateway Configuration Details". It features a breadcrumb trail: "System » IP Network » IP Telephony Nodes » Node Details » Virtual Trunk Gateway Configuration". The configuration page is divided into two main sections: "General" and "Virtual Trunk Network Health Monitor". In the "General" section, the "Vtrk gateway application" is set to "SIP Gateway (SIPGw)". The "SIP domain name" is "avayalab.com", the "Local SIP port" is "5060", the "Gateway endpoint name" is "node1005", and the "Application node ID" is "1005". The "Enable failsafe NRS" checkbox is unchecked. The "SIP ANAT" is set to "IPv4". In the "Virtual Trunk Network Health Monitor" section, the "Monitor IP addresses (listed below)" checkbox is unchecked. The "Monitor IP" field is empty, and the "Monitor addresses" list is also empty. The "Add" button is visible next to the "Monitor IP" field, and the "Remove" button is visible next to the "Monitor addresses" list. At the bottom of the page, there are "Save" and "Cancel" buttons. A note at the bottom states: "Note: Changes made on this page will NOT be transmitted until the Node is also saved."

Scroll down to the **SIP Gateway Settings → Proxy or Redirect Server:** section.

Under **Proxy Server Route 1**, enter the following and use default values for remaining fields.

- **Primary TLAN IP address:** Enter the IP address of the Acme Packet Inside media interface. In the sample configuration **10.64.19.150** was used.
- **Port:** Enter **5060**
- **Transport protocol:** Select **TCP**

The values defined for the sample configuration are shown below.

The screenshot shows the 'Proxy Or Redirect Server' configuration page for 'Proxy Server Route 1'. The page has a breadcrumb trail: 'General | SIP Gateway Settings | SIP Gateway Services'. The configuration fields are as follows:

- Primary TLAN IP address:** 10.64.19.150 (with a tooltip: 'The IP address can have either IPv4 or IPv6 format based on the value of "TLAN address type"')
- Port:** 5060 (range: 1 - 65535)
- Transport protocol:** TCP (dropdown menu)
- Options:** ☐ Support registration, ☐ Primary CDS proxy
- Secondary TLAN IP address:** 0.0.0.0 (with a tooltip: 'The IP address can have either IPv4 or IPv6 format based on the value of "TLAN address type"')
- Port:** 5060 (range: 1 - 65535)
- Transport protocol:** TCP (dropdown menu)

At the bottom, there is a note: 'Note: Changes made on this page will NOT be transmitted until the Node is also saved.' and buttons for 'Save' and 'Cancel'. A footer note states: '* Required Value.'

Scroll down and repeat these steps for the **Proxy Server Route 2**.

The screenshot shows the 'Proxy Or Redirect Server' configuration page for 'Proxy Server Route 2'. The page has a breadcrumb trail: 'General | SIP Gateway Settings | SIP Gateway Services'. The configuration fields are as follows:

- Primary TLAN IP address:** 10.64.19.150 (with a tooltip: 'The IP address can have either IPv4 or IPv6 format based on the value of "TLAN address type"')
- Port:** 5060 (range: 1 - 65535)
- Transport protocol:** TCP (dropdown menu)
- Options:** ☐ Registration not supported, ☐ Primary CDS proxy

Scroll down to the **SIP URI Map** section. The values defined for the sample configuration are shown below. The Avaya CS1000E will put the “string” entered in the **SIP URI Map** in the “phone-context=<string>” parameter in SIP headers such as the To and From headers. If the value is configured to blank, the CS1000E will omit the “phone-context=” in the SIP header altogether.

The screenshot shows the 'SIP Gateway Services' configuration page. Under the 'SIP URI Map' section, there are two columns: 'Public E.164 domain names' and 'Private domain names'. The 'Public' column has fields for National, Subscriber, Special number, and Unknown. The 'Private' column has fields for UDP (set to 'udp'), CDP (set to 'cdp.udp'), Special number, Vacant number, and Unknown.

Scroll to the bottom of the page and click **Save** (not shown) to save SIP Gateway configuration settings. This will return the interface to the **Node Details** screen.

5.1.6. Synchronize Node Configuration

On the **Node Details** screen click **Save** as shown below.

The screenshot shows the 'Node Details' screen for ID 1005, which is a SIP Line, LTPS, Gateway (SIPGw). The page has a left-hand navigation menu with options like UCM Network Services, Home, Links, System, and Interfaces. The main content area shows configuration for 'Embedded LAN (ELAN)' and 'Telephony LAN (TLAN)'. The 'Embedded LAN' section has fields for Gateway IP address (10.80.141.1) and Subnet mask (255.255.255.0). The 'Telephony LAN' section has fields for Node IPv4 address (10.80.140.103) and Subnet mask (255.255.255.0). There is also a field for Node IPv6 address. Below these are sections for 'IP Telephony Node Properties' and 'Applications (click to edit configuration)'. The 'Applications' section lists 'SIP Line' and 'Terminal Proxy Server (TPS)'. At the bottom right, there are 'Save' and 'Cancel' buttons, with the 'Save' button highlighted by a yellow circle.

Select **Transfer Now** on the **Node Saved** page as show below.

Managing: 10.80.141.102 Username: admin
System » IP Network » IP Telephony Nodes » Node Saved

Node Saved

Node ID: 1005 has been saved on the call server.

The new configuration must also be transferred to associated servers and media cards.

You will be given an option to select individual servers, or transfer to all.

You may initiate a transfer manually at a later time.

Once the transfer is complete, the **Synchronize Configuration Files (Node ID <id>)** page is displayed. Place a check mark next to the appropriate Hostname and click **Start Sync**. The screen will automatically refresh until the synchronization is finished.

Managing: 10.80.141.102 Username: admin
System » IP Network » IP Telephony Nodes » Synchronize Configuration Files

Synchronize Configuration Files (Node ID <1005>)

Note: Select components to synchronize their configuration files with call server data. This process transfers server INI files to selected components, and requires a restart* of applications on affected server(s) when complete.

[Print](#) | [Refresh](#)

<input checked="" type="checkbox"/>	Hostname	Type	Applications	Synchronization Status
<input checked="" type="checkbox"/>	cs1k-cpdc	Signaling_Server	SIP Line, LTPS, Gateway, PD, Presence Publisher, IP Media Services	Sync required

* Application restart is only required for initial system configuration or if changes have been made to general LAN configurations, SNTP settings, SIP and H323 Gateway settings, network connectivity related parameters like ports and IP address, enabling or disabling services, or adding or removing application servers.

The **Synchronization Status** field will update from **Sync required** (as shown above) to **Synchronized** (as shown below). After synchronization completes, place a check mark next to the appropriate Hostname and click **Restart Applications**.

Managing: 10.80.141.102 Username: admin
System » IP Network » IP Telephony Nodes » Synchronize Configuration Files

Synchronize Configuration Files (Node ID <1005>)

Note: Select components to synchronize their configuration files with call server data. This process transfers server INI files to selected components, and requires a restart* of applications on affected server(s) when complete.

[Print](#) | [Refresh](#)

<input checked="" type="checkbox"/>	Hostname	Type	Applications	Synchronization Status
<input checked="" type="checkbox"/>	cs1k-cpdc	Signaling_Server	SIP Line, LTPS, Gateway, PD, Presence Publisher, IP Media Services	Synchronized

* Application restart is only required for initial system configuration or if changes have been made to general LAN configurations, SNTP settings, SIP and H323 Gateway settings, network connectivity related parameters like ports and IP address, enabling or disabling services, or adding or removing application servers.

5.2. Virtual Superloops

Expand **System** → **Core Equipments** on the left panel and select **Superloops**. In the sample configuration, Superloop 4 is for the Media Gateway and Superloop 252 is the virtual Superloop used by the IP phones and SIP trunks.

The screenshot shows the AVAYA CS1000 Element Manager web interface. The left sidebar contains a navigation tree with 'System' expanded and 'Superloops' selected. The main content area is titled 'Superloops' and includes a table with two columns: 'Superloop Number' and 'Superloop Type'. The table lists two entries: Superloop 4 (IPMG) and Superloop 252 (Virtual). Above the table are buttons for 'Add...', 'Delete', and 'Refresh'. The top of the page shows the AVAYA logo, the title 'CS1000 Element Manager', and user information: 'Managing: 10.80.141.102 Username: admin System » Core Equipment » Superloops'.

Superloop Number	Superloop Type
1 <input type="radio"/> 4	IPMG
2 <input type="radio"/> 252	Virtual

5.3. Media Gateway

Expand **System** → **IP Network** on the left panel and select **Media Gateways**. Click the link in the **Type** column for the appropriate Media Gateway to be modified as shown below.

The screenshot shows the AVAYA CS1000 Element Manager web interface for the 'Media Gateways' section. The left sidebar shows 'System' expanded and 'IP Network' selected, with 'Media Gateways' highlighted. The main content area is titled 'Media Gateways' and includes a table with columns: 'IPMG', 'IP Address', 'Zone', and 'Type'. The table lists two entries: IPMG 004.00 (IP Address: 10.80.141.101, Zone: 1, Type: MGS) and IPMG 004.01 (IP Address: 10.80.141.201, Zone: 1, Type: MGS). Above the table are buttons for 'Add...', 'Digital Trunking...', 'Reboot', 'Delete', 'Virtual Terminal', and 'More Actions'. The 'Type' column for the first entry is circled in orange. The top of the page shows the AVAYA logo, the title 'CS1000 Element Manager', and user information: 'Managing: 10.80.141.102 Username: admin System » IP Network » Media Gateways'.

IPMG	IP Address	Zone	Type
004.00	10.80.141.101	1	MGS
004.01	10.80.141.201	1	MGS

The **IPMG 4 0 Media Gateway Survivable(MGS) Configuration** window appears. The **Telephony LAN (TLAN) IP Address** under the **DSP Daughterboard** heading will be the IP Address in the SDP portion of SIP messages, for calls requiring a gateway resource. For example, for a call from a digital telephone to the PSTN via CenturyLink SIP Trunk, the IP Address in the SDP in the INVITE message will be **10.80.140.104** in the sample configuration.

AVAYA CS1000 Element Manager

Managing: **10.80.141.102** Username: admin
System » IP Network » **Media Gateways** » IPMG 4 0 Media Gateway Survivable(MGS) Configuration

IPMG 4 0 Media Gateway Survivable(MGS) Configuration

- Media Gateway (MGS)**
 - Hostname:
 - Embedded LAN (ELAN) IP address:
 - Embedded LAN (ELAN) gateway IP address:
 - Embedded LAN (ELAN) subnet mask:
 - Telephony LAN (TLAN) IP address:
 - Telephony LAN (TLAN) gateway IP address:
 - Telephony LAN (TLAN) subnet mask:
- DSP Daughterboard**
 - Type of the DSP daughterboard:
 - Telephony LAN (TLAN) IP address:
 - Telephony LAN (TLAN) gateway IP address:
 - Telephony LAN (TLAN) IPv6 address:
 - Telephony LAN (TLAN) subnet mask:
 - Hostname:

Left Navigation Tree:

- 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
 - QoS Thresholds
 - Personal Directories
 - Unicode Name Directory
 - + Interfaces
 - Engineered Values
 - + Emergency Services
 - + 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

Scroll down to the area of the screen containing **VGW and IP phone codec profile** and expand it. The fax T.38 settings used for compliance testing is shown below.

AVAYA CS1000 Element Manager

- 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

- QoS Thresholds

- Personal Directories

- Unicode Name Directory

+ Interfaces

- Engineered Values

+ Emergency Services

+ 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

- VGW and IP phone codec profile

Enable echo canceller ☒

Echo canceller tail delay (milliseconds)

Enable dynamic attenuation ☒

Voice activity detection threshold (0 - 4 DBM)

Idle noise level (0 - 1 DBM)

R factor calculation ☐

DTMF tone detection ☒

Enable low latency mode ☒

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

Enable modem/fax pass through mode ☒

Enable V.21 FAX tone detection ☒

Fax TCF method

FAX maximum rate (bps)

FAX playout nominal delay (0 - 300 milliseconds)

FAX no activity timeout (10 - 32000 milliseconds)

FAX packet size

+ Codec **G711** Select ☒

The **Codec G.711** is enabled by default. Ensure that the **Select** box is checked for **Codec G729A** and the **VAD** (Voice Activity Detection) box is un-checked. The **Voice payload size** of **20** can be used with CenturyLink SIP Trunk Service for both G.729A and G.711. Click **Save** (not shown) at the bottom of the window. Then click **OK** in the dialog box (not shown) to save the IPMG configuration. During compliance testing, the G.729B codec was also tested by checking the **Voice Activity Detection (VAD)** box. Scroll down and click **Save** and then click **OK** on the new dialog box that appears to save the configuration.

AVAYA CS1000 Element Manager

- 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
 - + Software
- Customers
 - Routes and Trunks
 - Routes and Trunks

- Codec G711 **Select** ☒

Codec name **G711**

Voice payload size **20** (ms/frame)

Voice playback (jitter buffer) nominal delay **40**

Modifications may cause changes to dependent settings

Voice playback (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 playback (jitter buffer) nominal delay **40**

Modifications may cause changes to dependent settings

Voice playback (jitter buffer) maximum delay **80**

Modifications may cause changes to dependent settings

VAD ☐

After the configuration is saved, the **Media Gateways** page is displayed. Select the appropriate Media Gateway and click **Reboot** to load the new configuration.

AVAYA CS1000 Element Manager

Managing: **10.80.141.102** Username: admin
System » IP Network » Media Gateways

Media Gateways

Add... Digital Trunking... **Reboot** Delete Virtual Terminal More Actions Refresh

	IPMG	IP Address	Zone	Type
<input checked="" type="radio"/>	004 00	10.80.141.101	1	MGS
<input type="radio"/>	004 01	10.80.141.201	1	MGS

5.4. Virtual D-Channel, Routes and Trunks

Avaya Communication Server 1000E Call Server utilizes a virtual D-channel and associated Route and Trunks to communicate with the Signaling Server.

5.4.1. Virtual D-Channel Configuration

Expand **Routes and Trunks** on the left panel and select **D-Channels**. In the sample configuration, there is a virtual D-Channel 15 associated with the Signaling Server.

The screenshot displays the Avaya Communication Server 1000E web interface. On the left is a navigation tree with the following items: - UCM Network Services, - Home, - Links, - Virtual Terminals, - System (with sub-items: + 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, - QoS Thresholds, - Personal Directories, - Unicode Name Directory), + Interfaces, - Engineered Values, + Emergency Services, + Software, - Customers, - Routes and Trunks (with sub-items: - Routes and Trunks, - D-Channels, - Digital Trunk Interface), and - Dialing and Numbering Plans. The 'D-Channels' item is selected. The main content area is titled 'D-Channels' and includes a 'Maintenance' section with links: [D-Channel Diagnostics](#) (LD 96), [Network and Peripheral Equipment](#) (LD 32, Virtual D-Channels), [MSDL Diagnostics](#) (LD 96), [TMDI Diagnostics](#) (LD 96), and [D-Channel Expansion Diagnostics](#) (LD 48). Below this is a 'Configuration' section with the text 'Choose a D-Channel Number: 0 and type: DCH' and a 'to Add' button. At the bottom, a table lists the configuration for Channel 15:

- Channel: 15	Type: DCH	Card Type: DCIP	Description: VtrkNode1005	Edit
---------------	-----------	-----------------	---------------------------	------

Select **Edit** to verify the configuration, as shown below. Verify **DCIP** has been selected for **D Channel Card Type** field and the **Interface type for D-Channel** is set to **Meridian Meridian 1(SL1)**. Under the Basic Options section, verify **128** is selected for the **Output request Buffers** value.

D-Channels 15 Property Configuration

- Basic Configuration

Input Description	Input Value
Action Device And Number (ADAN):	DCH
D channel Card Type :	DCIP
Designator:	VtrkNode1005
Recovery to Primary:	<input type="checkbox"/>
PRI loop number for Backup D-channel:	
User :	Integrated Services Signaling Link Dedicated (ISLD) *
Interface type for D-channel:	Meridian Meridian1 (SL1)
Country:	ETS 300 =102 basic protocol (ETSI)
D-Channel PRI loop number:	
Primary Rate Interface:	<input type="text"/> more PRI
Secondary PRI2 loops:	<input type="text"/>
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 <small>Range: 1 - 4000</small>
Signalling server resource capacity:	3700 <small>Range: 0 - 3700</small>

- Basic options (BSCOPT)

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

- PINX customer number:

- Progress signal:

- Calling Line Identification :

- Output request Buffers: 128

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

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

- Remote Capabilities: [Edit](#)

5.4.2. Routes and Trunks Configuration

In addition to configuring a virtual D-channel, a **Route** and associated **Trunks** must be configured. Expand **Routes and Trunks** on the left panel and expand the customer number. In the example screen that follows, it can be observed that Route 15 has 32 trunks in the sample configuration.

AVAYA CS1000 Element Manager

Managing: 10.80.141.102 Username: admin
Routes and Trunks » Routes and Trunks

Routes and Trunks

Customer	Total routes	Total trunks	
- Customer: 0	2	64	Add route
- Route: 15	Type: TIE	Description: VTRKN1005SIP	Edit Add trunk
+ Trunk: 1 - 32	Total trunks: 32		
+ Route: 17	Type: TIE	Description: VTRKN1005SIPLINE	Edit Add trunk

Select **Edit** to verify the configuration, as shown below. As can be observed in the **Incoming and outgoing trunk (ICOG)** parameter, incoming and outgoing calls are allowed. The **Access code for the trunk route (ACOD)** will in general not be dialed, but the number that appears in this field may be observed on Avaya CS1000E display phones if an incoming call on the trunk is anonymous or marked for privacy.

Customer 0, Route 15 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): ☐

Further down in the **Basic Configuration** section verify the **Node ID of signaling server of this route (NODE)** matches the node shown in **Section 5.1**. Also verify **SIP (SIP)** has been selected for **Protocol ID for the route (PCID)** field. The **Zone for codec selection and bandwidth management (ZONE)** parameter can be used to associate the route with a zone for configuration of the audio codec preferences sent via the Session Description Protocol (SDP) in SIP messaging. The **D channel number (DCH)** field must match the D-Channel number shown in **Section 5.4.1**.

The route is for a virtual trunk route (VTRK): ☒

- Zone for codec selection and bandwidth management (ZONE): 00099 (0 - 8000)

- Node ID of signaling server of this route (NODE): 1005 (0 - 9999)

- Protocol ID for the route (PCID): SIP (SIP) ▼

- Print correlation ID in CDR for the route (CRID): ☐

Integrated services digital network option (ISDN): ☒

- Mode of operation (MODE): Route uses ISDN Signaling Link (ISLD) ▼

- D channel number (DCH): 15 (0 - 254)

- Interface type for route (IFC): Meridian M1 (SL1) ▼

- Private network identifier (PNI): 00001 (0 - 32700)

- Network calling name allowed (NCNA): ☒

- Network call redirection (NCRD): ☒

- Trunk route optimization (TRO): ☐

- Recognition of DT12 ABCD FALT signal for ISL (FALT): ☐

- Channel type (CHTY): B-channel (BCH) ▼

- Call type for outgoing direct dialed TIE route (CTYP): Unknown Call type (UKWN) ▼

- Insert ESN access code (INAC): ☐

- Integrated service access route (ISAR): ☐

- Display of access prefix on CLID (DAPC): ☐

- Mobile extension route (MBXR): ☒

- Screen indicator (SIND): ☒

- Mobile extension outgoing type (MBXOT): National number (NPA) ▼

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

Calling number dialing plan (CNDP): Unknown (UKWN) ▼

Scroll down and expand the **Basic Route Options** section. Check the **North American toll scheme (NATL)** and **Incoming DID digit conversion on this route (IDC)**, input **DCNO 0** for both **Day IDC Tree Number** and **Night IDC Tree Number** as shown below. The DCNO is created later on in **Section 5.5.5**.

AVAYA CS1000 Element Manager Help | Logout

- UCM Network Services
 - Home
 - Links
 - Virtual Terminals
 - System
 - + Alarms
 - Maintenance
 - + Core Equipment
 - Peripheral Equipment
 - + IP Network
 - + Interfaces
 - Engineered Values
 - + Emergency Services
 - + 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

- Basic Route Options

Attendant announcement (ATAN) : No Attendant Announcement (NO) ▼

Billing number required (BILN) : ☐

Call detail recording (CDR) : ☐

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 (0 - 254)

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

- Display external dialed digits (DEXT) : ☐

Multifrequency compelled or MFC signaling (MFC) : No MFC (NO) ▼

Process notification networked calls (PNNC) : ☐

5.5. Dialing and Numbering Plans

This section provides the configuration of the routing used in the sample configuration for routing calls over the SIP Trunk between Avaya Communication Server 1000E and Acme Packet 3820 for calls destined for the CenturyLink SIP Trunk. The routing defined in this section is simply an example and not intended to be prescriptive. Other routing policies may be appropriate for different customer networks.

5.5.1. Route List Block

Expand **Dialing and Numbering Plans** on the left panel and select **Electronic Switched Network**. Select **Route List Block (RLB)** on the **Electronic Switched Network (ESN)** page as shown on the following page.

CS1000 Element Manager

Managing: **10.80.141.102** Username: admin
Dialing and Numbering Plans » Electronic Switched Network (ESN)

Electronic Switched Network (ESN)

- Customer 00
 - Network Control & Services
 - Network Control Parameters (NCTL)
 - ESN Access Codes and Parameters (ESN)
 - Digit Manipulation Block (DGT)
 - Home Area Code (HNPA)
 - Flexible CLID Manipulation Block (CMDB)
 - Free Calling Area Screening (FCAS)
 - Free Special Number Screening (FSNS)
 - Route List Block (RLB)
 - Incoming Trunk Group Exclusion (ITGE)
 - Network Attendant Services (NAS)
 - Coordinated Dialing Plan (CDP)
 - Local Steering Code (LSC)
 - Distant Steering Code (DSC)
 - Trunk Steering Code (TSC)

- UCM Network Services
- Home
- Links
 - Virtual Terminals
- System
 - + Alarms
 - Maintenance
 - + Core Equipment
 - Peripheral Equipment
 - + IP Network
 - + Interfaces
 - Engineered Values
 - + Emergency Services
 - + 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

The **Route List Blocks** screen is displayed. Enter an available route list index number in the **Please enter a route list index** field and click **to Add**, or edit an existing entry by clicking the corresponding **Edit** button. In the sample configuration, route list block index **15** is used. If adding the route list index anew, scroll down to the **Options** area of the screen. If editing an existing route list block index, select the **Edit** button next to the appropriate Data Entry Index as shown below, and scroll down to the **Options** area of the screen.

CS1000 Element Manager

Managing: **10.80.141.102** Username: admin
Dialing and Numbering Plans » Electronic Switched Network (ESN) » Customer 00 » Network

Route List Blocks

Please enter a route list index (0 - 1999)

- + Route List Block Index -- 11
- Route List Block Index -- 15

Initial Set: 0
Number of Alternate Routing Attempts: 5
Set Minimum Facility Restriction Level : 0

- + Data Entry Index -- 0

- + Interfaces
 - Engineered Values
 - + Emergency Services
 - + 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

Under the **Options** section, select **<Route id>** in the **Route Number** field. In the sample configuration route number **15** was used. Default values may be retained for remaining fields.

The screenshot shows the AVAYA CS1000 Element Manager interface. On the left is a navigation tree with categories like UCM Network Services, Home, Links, System, Alarms, Maintenance, Core Equipment, Peripheral Equipment, IP Network, Interfaces, Engineered Values, Emergency Services, Software, Customers, and Routes and Trunks. The main area is titled 'Options' and contains several configuration fields: 'Local Termination entry' (checkbox), 'Route Number' (dropdown menu with '15' selected and highlighted by a yellow circle), 'Skip Conventional Signaling' (checkbox), 'Use Tone Detector' (checkbox), 'Conversion to LDN' (checkbox), 'Expensive Route' (checkbox), and 'Strategy on Congestion' (dropdown menu with 'No Reroute (NRR)' selected). A copyright notice at the bottom reads 'Copyright © 2002-2012 Avaya Inc. All rights reserved.'

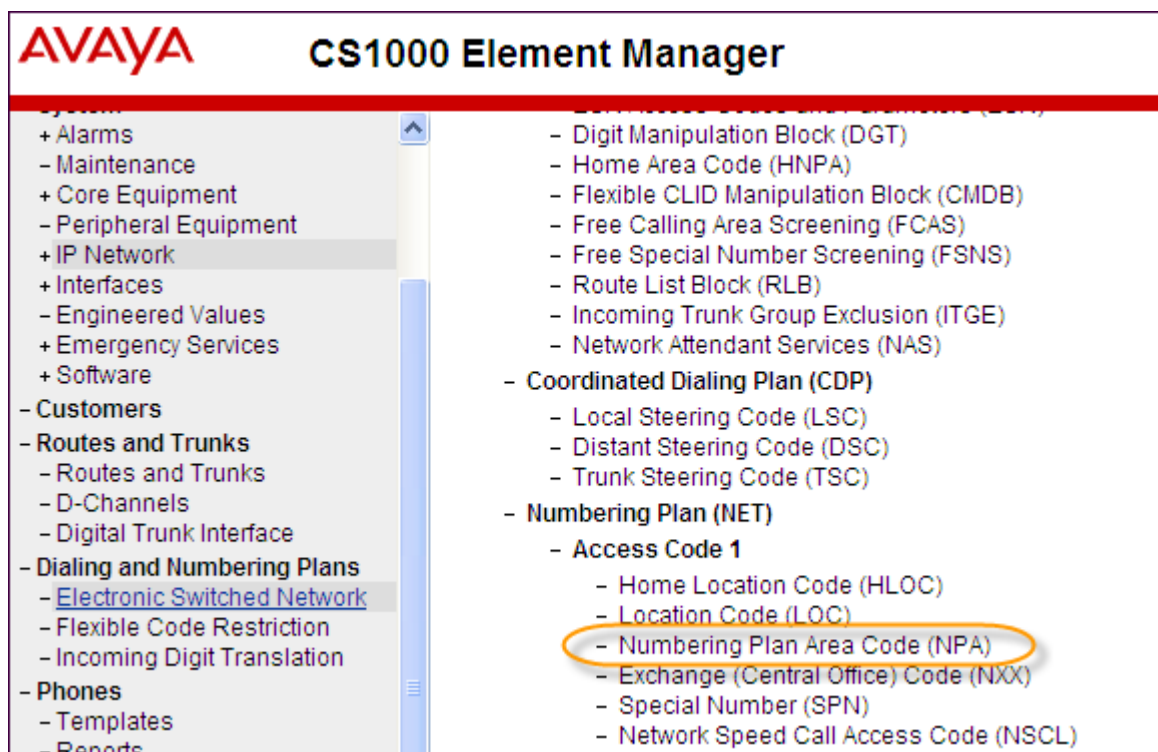
5.5.2. NARS Access Code

Expand **Dialing and Numbering Plans** on the left panel and select **Electronic Switched Network**. Select **ESN Access Codes and Parameters (ESN)**. Although not repeated below, this link can be observed in the first screen in **Section 5.5.1**. In the **NARS/BARS Access Code 1** field, enter the number the user will dial before the target PSTN number. In the sample configuration, the single digit **9** was used.

The screenshot shows the AVAYA CS1000 Element Manager interface for 'ESN Access Codes and Basic Parameters'. The left navigation tree is expanded to 'Dialing and Numbering Plans', with 'Electronic Switched Network' selected. The main area is titled 'ESN Access Codes and Basic Parameters' and contains a 'General Properties' section. In this section, the 'NARS/BARS Access Code 1' field is highlighted with a yellow circle and contains the value '9'. Other fields include 'NARS Access Code 2' (empty), 'NARS/BARS Dial Tone after dialing AC1 or AC2 access codes' (checked), 'Expensive Route Warning Tone' (checked), 'Expensive Route Delay Time' (6, range 0-10), 'Coordinated Dialing Plan feature for this customer' (checked), 'Maximum number of Steering Codes' (2000, range 1-64000), 'Number of digits in CDP DN (DSC + DN or LSC + DN)' (4, range 3-10), 'Routing Controls' (checkbox), and 'Check for Trunk Group Access Restrictions' (checkbox). The top of the page shows 'Managing: 10.80.141.102' and 'Username: admin'.

5.5.3. Numbering Plan Area Codes

Expand **Dialing and Numbering Plans** on the left panel and select **Electronic Switched Network**. Scroll down and select **Numbering Plan Area Code (NPA)** under the appropriate access code heading. In the sample configuration, this is **Access Code 1**, as shown below.



Add a new NPA by entering it in the **Please enter an area code** box and click **to Add** or click **Edit** to view or change an NPA that has been previously configured. In the screen below, it can be observed that various dial strings such as **1303** and **1800** are configured.

AVAYA CS1000 Element Manager Help | Logout

Managing: 10.80.141.102 Username: admin
Dialing and Numbering Plans » Electronic Switched Network (ESN) » Customer 00 » Numbering Plan (NET) » Access Code 1 » Numbering Plan Area Code List

Numbering Plan Area Code List

Please enter an area code

- + Numbering Plan Area Code -- 1303
- + Numbering Plan Area Code -- 1502
- + Numbering Plan Area Code -- 1615
- + Numbering Plan Area Code -- 1720
- + Numbering Plan Area Code -- 1732
- + Numbering Plan Area Code -- 1800

In the screen below, the entry for **1303** is displayed. In the Route List Index, **15** is selected to use the route list associated with the SIP Trunk to Acme Packet 3820 as shown in **Section 5.4.2**. Default parameters may be retained for other parameters. Repeat this procedure for the dial strings associated with other numbering plan area codes that should route to the SIP Trunk to Acme Packet 3820.

Numbering Plan Area Code

General Properties

Numbering Plan Area code translation:

Route List Index:

Incoming Trunk group Exclusion Index:

5.5.4. Special Numbers

In the testing associated with these Application Notes, special service numbers such as x11, international calls, and operator assisted calls were also routed to Acme Packet 3820 and ultimately to the CenturyLink SIP Trunk. Although not intended to be prescriptive, one approach to such routing is summarized in this section.

Expand **Dialing and Numbering Plans** on the left panel and select **Electronic Switched Network**. Scroll down and select **Special Number (SPN)** under the appropriate access code heading (as can be observed in the first screen in **Section 5.5.3**).

Add a new number by entering it in the **Please enter a Special Number** box and click **to Add** or click **Edit** to view or change a special number that has been previously configured. In the screen below, it can be observed that various dial strings such as **0**, **011**, **411** and **911** calls are listed. Route list index **15** has been selected in the same manner as shown for the NPAs in the prior section.

Special Number List

Please enter a Special Number

- Special Number -- 0

Flexible length: 0

International dialing plan: NO

Type of call that is defined by the special number: NONE

Route list index: 15

- Special Number -- 011

Flexible length: 0

International dialing plan: YES

Type of call that is defined by the special number: INTL

Route list index: 15

- Special Number -- 411

Flexible length: 0

International dialing plan: NO

Type of call that is defined by the special number: NONE

Route list index: 15

- Special Number -- 911

Flexible length: 0

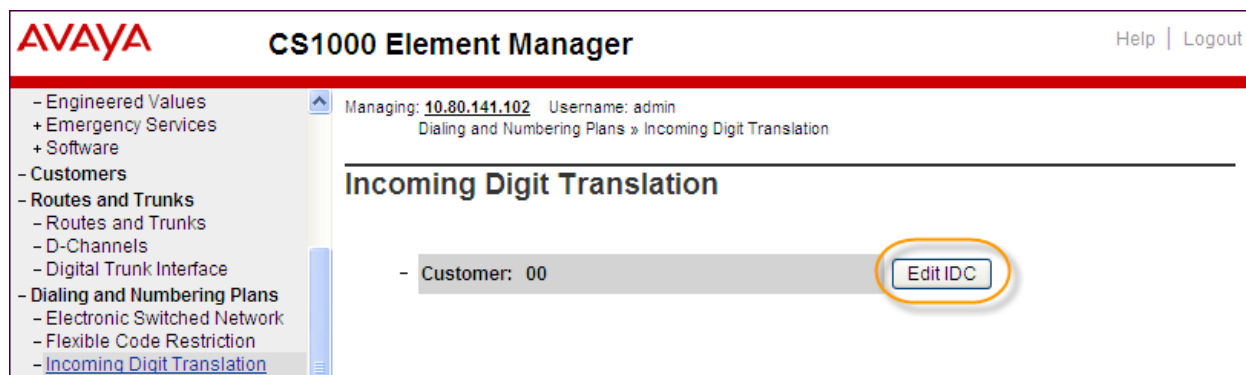
International dialing plan: NO

Type of call that is defined by the special number: NONE

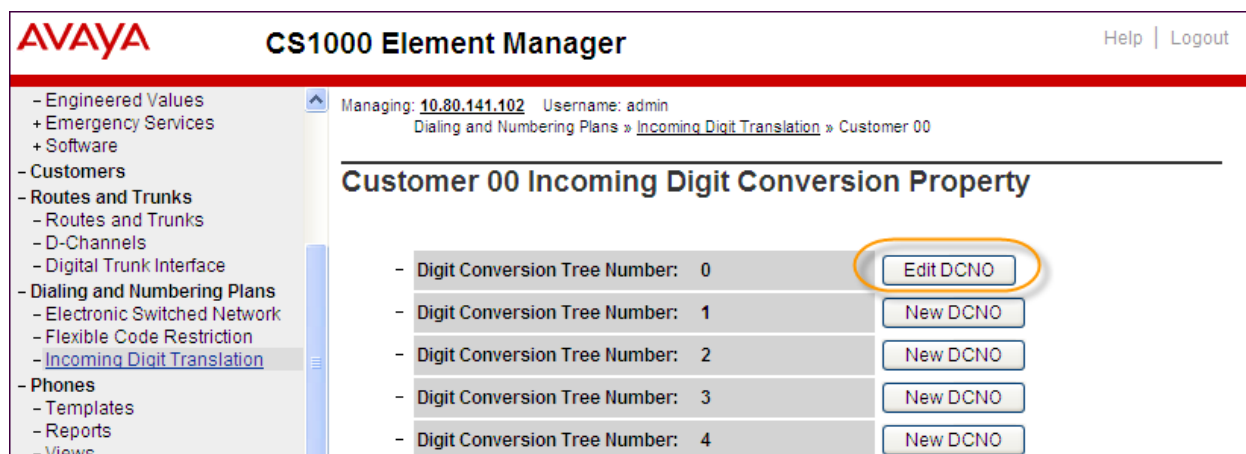
Route list index: 15

5.5.5. Incoming Digit Translation

In general, the incoming digit translation can be used to manipulate the digits received for an incoming call. Expand **Dialing and Numbering Plans** on the left panel and select **Incoming Digit Translation**. Click on the **Edit IDC** button as shown on the following screen.



Click on the **New DCNO** to create the digit translation mechanism or if editing an existing one, select the **Edit DCNO** button next to the appropriate Digit Conversion Tree Number. In this example, **Digit Conversion Tree Number (DCNO) 0** has been created as shown below.



Detail configuration of the **DCNO** is shown below. The **Incoming Digits** can be added to map to the **Converted Digits** which would be the CS1000E system phones DN. This **DCNO** has been assigned to route 15 as shown in **Section 5.4.2**.

In the following configuration, the incoming call from PSTN with the prefix 303-555-71xx will be translated to CS1000E DN 71xx. The PSTN with the prefix 614-555-01xx will be translated to CS1000E DN 51xx. The DID 303-555-7799 is translated to 5000 for Voicemail accessing purpose.

AVAYA CS1000 Element Manager

Managing: [10.80.141.102](#) Username: admin
 Dialing and Numbering Plans » [Incoming Digit Translation](#) » [Customer 00](#) » Digit Conversion Tree 0 Configuration

Digit Conversion Tree 0 Configuration

Regular IDC tree
 Send calling party DID disabled

Buttons: [Add...](#) [Delete IDC](#) [Delete IDC tree](#) [Refresh](#)

	Incoming Digits	Converted Digits	CPND Name	CPND language
1	30355571	71	,	Roman characters
2	61455501	51	,	Roman characters
3	3035557799	5000	,	Roman characters

5.6. Zones and Bandwidth

Zone configuration can be used to control codec selection and for bandwidth management. To configure, expand **System → IP Network** on the left panel and select **Zones** as shown below.

AVAYA CS1000 Element Manager

Managing: [10.80.141.102](#) Username: admin
 System » IP Network » Zones

Zones

Zones are used to group related information for either bandwidth or dial plan numbering purposes.

Bandwidth Zones
 Bandwidth zones are used for alternate routing of calls between IP stations and also for bandwidth management.

Numbering Zones
 Numbering zones are used to route calls through a centralized call server.

Select **Bandwidth Zones**. In the sample lab configuration, two zones are configured. In production environments, it is likely that more zones will be required. Select the zone associated with the virtual trunk to Acme Packet 3820 and click **Edit** as shown below. In the sample configuration, this is Zone number **99**.

Bandwidth Zones

Add...Edit...Import...ExportMaintenance...Delete

Refresh

	Zone +	Intrazone Bandwidth	Intrazone Strategy	Interzone Bandwidth	Interzone Strategy	Resource Type	Zone Intent	Description
1	1	1000000	BQ	1000000	BQ	SHARED	MO	IPSETS
2	99	1000000	BB	1000000	BB	SHARED	VTRK	VTRUNK

In the resultant screen shown below, select **Zone Basic Property and Bandwidth Management**.

Edit Bandwidth Zone

- Zone Basic Property and Bandwidth Management
- Adaptive Network Bandwidth Management and CAC
- Alternate Routing for Calls between IP Stations
- Branch Office Dialing Plan and Access Codes
- Branch Office Time Difference and Daylight Saving Time Property
- Media Services Zone Properties

The following screen shows the Zone 99 configuration. Note that **Best Bandwidth (BB)** is selected for the zone strategy parameters so that codec G.729A is preferred over codec G.711MU for calls with CenturyLink SIP Trunk.

Zone Basic Property and Bandwidth Management

Input Description	Input Value
Zone Number (ZONE):	99 (1 - 8000)
Intrazone Bandwidth (INTRA_BW):	1000000 (0 - 10000000)
Intrazone Strategy (INTRA_STGY):	Best Bandwidth (BB)
Interzone Bandwidth (INTER_BW):	1000000 (0 - 10000000)
Interzone Strategy (INTER_STGY):	Best Bandwidth (BB)
Resource Type (RES_TYPE):	Shared (SHARED)
Zone Intent (ZBRN):	VTRK (VTRK)
Description (ZDES):	VTRUNK

5.7. Example CS1000E Telephone Users

This section is not intended to be prescriptive, but simply illustrates a sampling of the telephone users in the sample configuration.


5.7.1. Example SIP Phone DN 7108, Codec Considerations

The following screen shows basic information for a SIP phone in the configuration. The telephone is configured as Directory Number 7108. Note that the telephone is in Zone 1 and is associated with Node 1005 (see **Section 5.1**). A call between this telephone and another telephone in Zone 1 will use a **best quality** strategy (see **Section 5.6**) and therefore can use G.711MU. If this same telephone calls out to the PSTN via the CenturyLink SIP Trunk, the call would use a **best bandwidth** strategy, and the call would use G.729A.

AVAYA CS1000 Element Manager Help | Logout

Managing: [EM on cs1k-cpdc\(10.80.141.102\)](#)
[Phones»Phone Details](#)

Phone Details

 System: EM on cs1k-cpdc
Phone Type: UEXT-SIPL
Sync Status: TRN

[General Properties](#) | [Features](#) | [Keys](#) | [User Fields](#) Custom View: [All](#)

General Properties

Customer Number: *

Terminal Number:

Designation: * (1-6 characters)

Zone: *

SIP User Name: * (1-16 characters)

Node Id: *

Super User: ☐

5.7.2. Example Digital Phone DN 7107 with Call Waiting


The following screen shows basic information for a digital phone in the configuration. The telephone is configured as Directory Number 7107.

The screenshot displays the AVAYA CS1000 Element Manager web interface. On the left is a navigation menu with categories like UCM Network Services, System, Customers, and Phones. The main content area is titled 'Phone Details' and shows information for a phone managed by 'EM on cs1k-cpdc(10.80.141.102)'. It includes a photo of a digital phone and fields for System (EM on cs1k-cpdc), Phone Type (M3904), and Sync Status (TRN). Below this is a 'General Properties' section with fields for Customer Number (0), Terminal Number (004 0 03 00), and Designation (DIG).

AVAYA CS1000 Element Manager

Managing: [EM on cs1k-cpdc\(10.80.141.102\)](#)
[Phones»Phone Details](#)

Phone Details

 System: EM on cs1k-cpdc
Phone Type: M3904
Sync Status: TRN

[General Properties](#) | [Features](#) | [Keys](#) | [User Fields](#)

General Properties

Customer Number: *

Terminal Number:

Designation: * (1-6 characters)

The following screen shows basic key information for the telephone. It can be observed that the telephone can support call waiting with tone. Although not shown in detail below, to use call waiting with tone, assign a key **CWT – Call Waiting**, set the feature **SWA – Call waiting from a Station** to **Allowed**, and set the feature **WTA – Warning Tone** to **Allowed**.

The screenshot shows the 'Keys' configuration page. It features a table with columns for Key No., Key Type, and Key Value. Key 0 is configured as 'SCR - Single Call Ringing' with Directory Number 7107 and MARP checked. Key 1 is configured as 'CWT - Call Waiting'. The right side of the page contains fields for Directory Number (7107), MARP status, and personalization fields for First Name (John), Last Name (Digital), Display Format (First, Last), and Language (Roman). There are also fields for CLID Entry (0) and ANIE Entry.

Keys

Key No.	Key Type	Key Value
0	SCR - Single Call Ringing	Directory Number: 7107 <input checked="" type="checkbox"/> Multiple Appearance Redirection Prime(MARP) First Name: John, Last Name: Digital, Display Format: First, Last, Language: Roman CLID Entry (Numeric or D): 0 ANIE Entry:
1	CWT - Call Waiting	

5.7.3. Example Analog Port with DN 7106, Fax


The following screen shows basic information for an analog port in the configuration that may be used with a telephone or fax machine. The port is configured as Directory Number 7106.

AVAYA**CS1000 Element Manager**

- UCM Network Services
- Home
- Links
 - Virtual Terminals
- System
 - + Alarms
 - Maintenance
 - + Core Equipment
 - Peripheral Equipment
 - + IP Network
 - + Interfaces
 - + Engineered Values
 - + Emergency Services
 - + 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

Managing: [EM on cs1k-cpdc\(10.80.141.102\)](#)
[Phones»Phone Details](#)

Phone Details



System: EM on cs1k-cpdc
Phone Type: 500
Sync Status: TRN

[General Properties](#) | [Features](#) | [Single Line Features](#) | [User Fields](#)

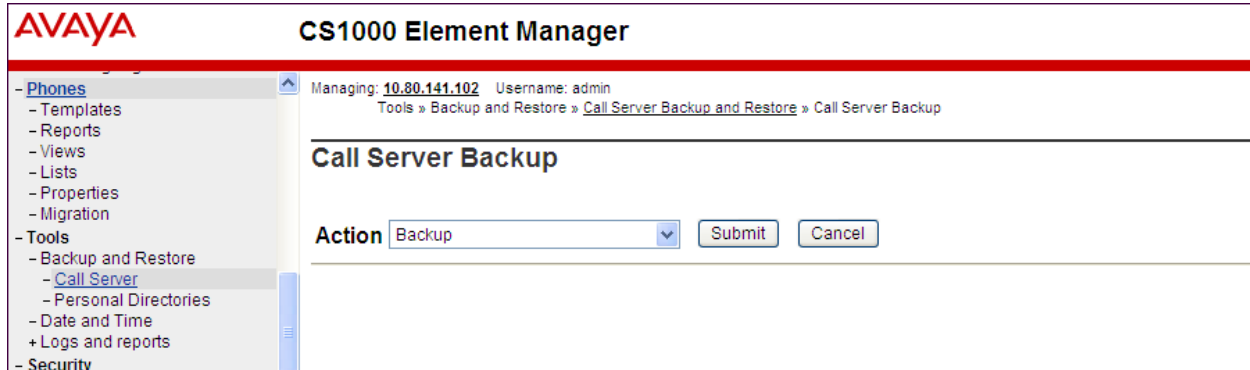
General Properties

Customer Number: 0 *
Terminal Number: 004 0 04 00
Designation: ANA0 * (1-6 characters)
Directory Number: 7106 - 🔍
CLID entry:
ANIE entry:
Marp ☒

First Name	Last Name	Display Format	Language
John	Single	First, Last ▼	Roman ▼

5.8. Save Configuration

Expand **Tools** → **Backup and Restore** on the left panel and select **Call Server**. Select Backup (not shown) and click **Submit** to save configuration changes as shown below.

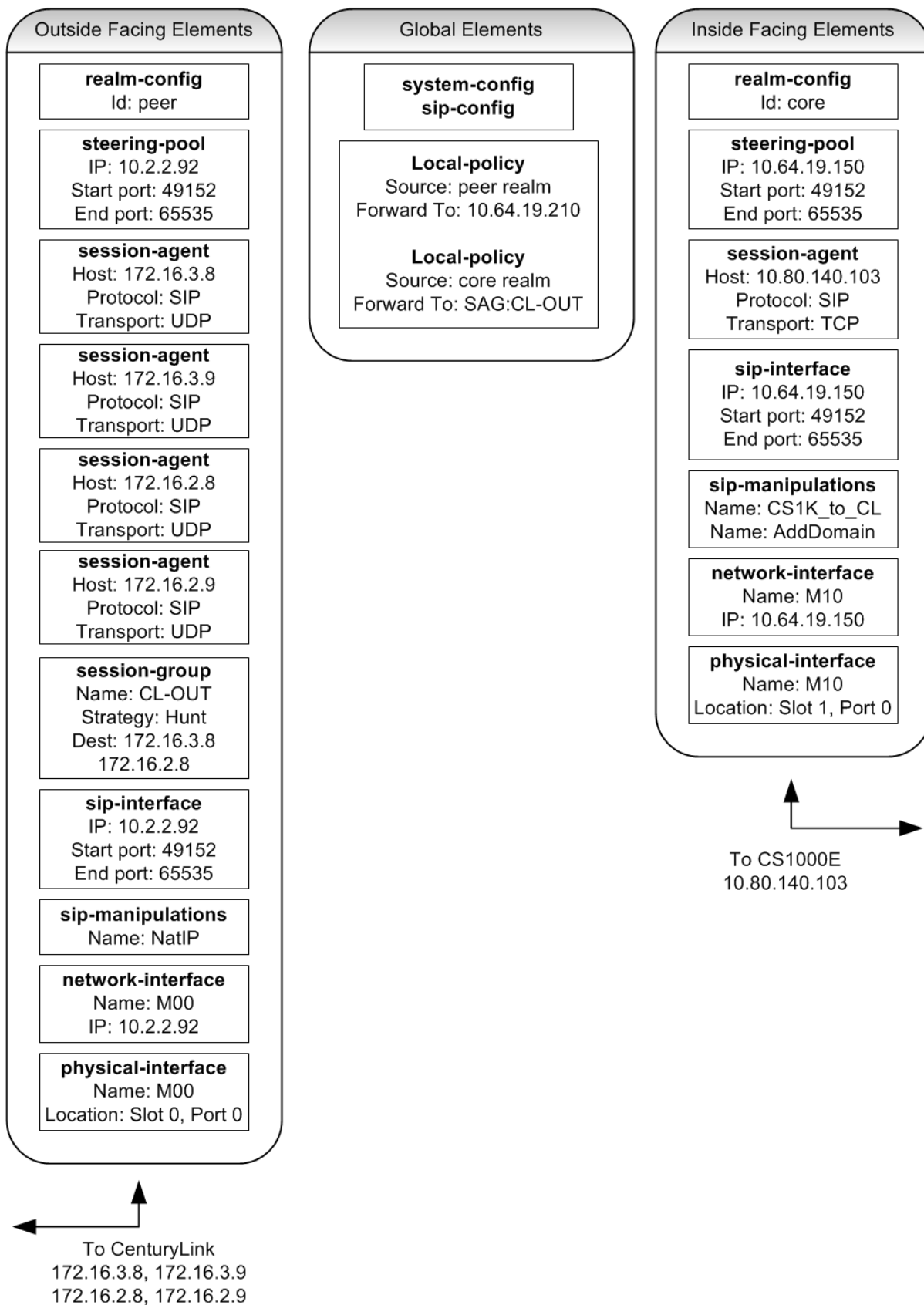


6. Configure Acme Packet 3820 Net-Net® Session Director

This section describes the configuration of the Acme Packet 3820 necessary for interoperability with CenturyLink and CS1000E. The Acme Packet 3820 is configured via the Acme Packet Command Line Interface (ACLI). This section assumes the reader is familiar with accessing and configuring the Acme Packet 3820.

A pictorial view of this configuration is shown below. It shows the internal components needed for the compliance test. Each of these components is defined in the Acme Packet 3820 configuration file contained in **Appendix A**. However, this section does not cover standard Acme Packet 3820 configurations that are not directly related to the interoperability test. The details of these configuration elements can be found in **Appendix A**.

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 and the direct connection to CenturyLink and CS1000E. These same fields are highlighted in **Appendix A**. The remaining fields are generally the default/standard value used by the Acme Packet 3820 for that field. For additional details on the administration of the Acme Packet 3820, see **Reference [7]**.



6.1. Acme Packet Command Line Interface Summary

The Acme Packet 3820 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 Acme Packet 3820 using a PC and a terminal emulation program such as HyperTerminal (use the RJ-45 to DB9 adapter as packaged with the 3820 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 Acme Packet 3820 with the user password.
3. Enable the Superuser mode by entering the **enable** command and then the superuser password. The command prompt will change to include a “#” instead of a “>” while in Superuser 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 Superuser 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 M00**).
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.

6.2. System Configuration

The system configuration defines system-wide parameters for the Acme Packet 3820.

The key system configuration (**system-config**) field is:

- **default-gateway**: The IP address of the default gateway for the management network (10.80.150.0/24) from **Figure 1**. In this case, the default gateway is **10.80.150.1**.

```
system-config
  hostname
  description
  location
  mib-system-contact
  mib-system-name

< text removed for brevity >

  call-trace                disabled
  internal-trace            disabled
  log-filter                all
  default-gateway          10.80.150.1
  restart                  enabled
  exceptions
  telnet-timeout            0
  console-timeout           0
  remote-control            enabled
  cli-audit-trail           enabled
  link-redundancy-state     disabled
  source-routing            disabled
  cli-more                  disabled
  terminal-height           24
  debug-timeout             0
```

6.3. Physical and Network Interfaces

As part of the compliance test, the Ethernet interface slot 0 / port 0 of the Acme Packet 3820 was connected to the external untrusted network. Ethernet slot 1 / port 0 was connected to the internal corporate LAN. A network interface was defined for each physical interface to assign it a routable IP address.

The key physical interface (**phy-interface**) fields are:

- **name:** A descriptive string used to reference the Ethernet interface.
- **operation-type:** Media indicates both signaling and media packets are sent on this interface.
- **slot / port:** The identifier of the specific Ethernet interface used.

phy-interface	
name	M00
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	2011-11-01 09:59:56
phy-interface	
name	M10
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	2011-11-01 10:00:38

The key network interface (**network-interface**) fields are:

- **name:** The name of the physical interface (defined previously) that is associated with this network interface.
- **description:** A descriptive name to help identify the interface.
- **ip-address:** The IP address on the interface connected to the network on which the CenturyLink SIP Trunk Service resides. In the compliance test, the IP address **10.2.2.92** was assigned to the public interface and **10.64.19.150** was assigned to the private interface.
- **netmask:** Subnet mask for the IP subnet.
- **gateway:** The subnet gateway address.
- **hip-ip-list:** The list of virtual IP addresses assigned to the Acme Packet 3820 on this interface. If a single virtual IP address is used, this value would be the same as the value entered for the **ip-address** field above.
- **icmp-address:** The list of IP addresses to which the Acme Packet 3820 will answer ICMP requests on this interface.

```
network-interface
  name                M00
  sub-port-id         0
  description          PUBLIC
  hostname
  ip-address           10.2.2.92
  pri-utility-addr
  sec-utility-addr
  netmask              255.255.255.128
  gateway              10.2.2.1
  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          10.2.2.92
  ftp-address
  icmp-address
  snmp-address
  telnet-address
  ssh-address
  last-modified-by     admin@10.80.150.38
  last-modified-date   2011-11-01 12:52:08
```

The settings for the private side network interface are shown below.

network-interface	
name	M10
sub-port-id	0
description	PRIVATE
hostname	
ip-address	10.64.19.150
pri-utility-addr	
sec-utility-addr	
netmask	255.255.255.0
gateway	10.64.19.1
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	10.64.19.150
ftp-address	
icmp-address	10.64.19.150
snmp-address	
telnet-address	
ssh-address	
last-modified-by	admin@10.80.150.38
last-modified-date	2011-11-01 12:16:22

6.4. Realm

A realm represents a group of related Acme Packet 3820 components. Two realms were defined for the compliance test. The **peer** realm was defined for the external network and the **core** realm was defined for the internal network.

The key realm (**realm-config**) fields are:

- **identifier:** A string used as a realm reference. This will be used in the configuration of other components.
- **network interfaces:** The network interfaces located in this realm.
- **In-manipulationid:** For the **core** realm **CS1K_To_CL** was used. This name refers to a set of sip-manipulations (defined in **Section 6.9**) that is performed on inbound traffic to the Acme Packet 3820.
- **out-manipulationid:** For the **peer** realm **NatIP** was used and for the **core** realm **AddDomain** was used. These names refer to a set of sip-manipulations (defined in **Section 6.9**) that are performed on outbound traffic from the Acme Packet 3820. These sip-manipulations are specified in each realm. Thus, these sip-manipulations are applied to outbound traffic from the public side (**peer**) of the Acme Packet 3820 as well as to outbound traffic from the private side (**core**) of the Acme Packet 3820.

```

realm-config
  identifier
  description
  addr-prefix
  network-interfaces
  mm-in-realm
  mm-in-network
  mm-same-ip
  mm-in-system
  peer
  0.0.0.0
  M00:0
  enabled
  enabled
  enabled
  enabled

< text removed for brevity >

  out-translationid
  in-manipulationid
  out-manipulationid
  manipulation-string
  manipulation-pattern
  class-profile
  average-rate-limit
  NatIP
  0

< text removed for brevity >

realm-config
  identifier
  description
  addr-prefix
  network-interfaces
  mm-in-realm
  mm-in-network
  mm-same-ip
  mm-in-system
  core
  0.0.0.0
  M10:0
  enabled
  enabled
  enabled
  enabled

< text removed for brevity >

  out-translationid
  in-manipulationid
  out-manipulationid
  manipulation-string
  manipulation-pattern
  class-profile
  average-rate-limit
  CS1K_To_CL
  AddDomain
  0

< text removed for brevity >

```

6.5. SIP Configuration

The SIP configuration (**sip-config**) defines the global system-wide SIP parameters, including SIP timers, SIP options, which realm to send requests to if not specified elsewhere, and enabling the SD to collect statistics on requests other than REGISTERs and INVITEs.

The key SIP configuration (**sip-config**) fields are:

- **state: enabled**
- **home-realm-id:** The name of the realm on the private side of the Acme Packet 3820.
- **egress-realm-id:** The name of the realm on the private side of the Acme Packet 3820.
- **options: max-udp=length=0** This option was used to prevent errors about the packet size being too large.

```
sip-config
  state                enabled
  operation-mode       dialog
  dialog-transparency  enabled
  home-realm-id        core
  egress-realm-id      core
  nat-mode             None
  registrar-domain
  registrar-host
  registrar-port       0
  register-service-route always
  init-timer           500
  max-timer             4000
  trans-expire         32
  invite-expire        180

< text removed for brevity >

  options              max-udp=length=0
  refer-src-routing    disabled
  add-ucid-header      disabled
  proxy-sub-events

< text removed for brevity >
```

6.6. SIP Interface

The SIP interface (**sip-interface**) defines the receiving characteristics of the SIP interfaces on the Acme Packet 3820. Two SIP interfaces were defined; one for each realm.

The key SIP interface (**sip-interface**) fields are:

- **realm-id:** The name of the realm to which this interface is assigned.
- **sip-port**
 - **address:** The IP address assigned to this sip-interface.
 - **port:** The port assigned to this sip-interface. Port 5060 is used for both UDP and TCP.
 - **transport-protocol:** The transport method used for this interface.
 - **allow-anonymous:** Defines from whom SIP requests will be allowed. On the peer side, the value of **agents-only** is used. Thus, SIP requests will only be accepted from session agents (as defined in **Section 6.7**) on this interface. On the core side, the value of **all** is used. Thus, SIP requests will be accepted from anyone on this interface.

```
sip-interface
state                enabled
realm-id           peer
description
sip-port
    address          10.2.2.92
    port             5060
    transport-protocol UDP
    tls-profile
    allow-anonymous   agents-only
    ims-aka-profile
    carriers
    trans-expire      0
    invite-expire     0

< text removed for brevity >

sip-interface
state                enabled
realm-id           core
description
sip-port
    address          10.64.19.150
    port             5060
    transport-protocol TCP
    tls-profile
    allow-anonymous   all
    ims-aka-profile
    carriers
    trans-expire      0
    invite-expire     0

< text removed for brevity >
```

6.7. Session Agent

A session agent defines the characteristics of a signaling peer to the Acme Packet 3820 such as CS1000E and CenturyLink SIP Trunk Service.

The key session agent (**session-agent**) fields are:

- **hostname:** Fully qualified domain name or IP address of this SIP peer.
- **ip-address:** The IP address of this SIP peer.
- **port:** The port used by the peer for SIP traffic.
- **app-protocol:** SIP
- **transport-method:** UDP
- **realm-id:** The realm id where this peer resides.
- **description:** A descriptive name for the peer.
- **ping-method: OPTIONS;hops=70** This setting defines that the SIP OPTIONS message will be sent to the peer to verify that the SIP connection is functional. In addition, this parameter causes the Acme Packet 3820 to set the SIP “Max-Forward” field to 70 in outbound SIP OPTIONS pings generated by the Acme Packet 3820 to this session agent.
- **ping-interval:** Specifies the interval (in seconds) between each ping attempt.

The settings for the session agent used for CenturyLink East Inbound/Outbound peer:

```
session-agent
  hostname          172.16.3.8
  ip-address        172.16.3.8
  port              5060
  state             enabled
  app-protocol      SIP
  app-type
  transport-method  UDP
  realm-id          peer
  egress-realm-id
  description
  carriers
  allow-next-hop-lp enabled
  constraints        disabled
  max-sessions       0

< text removed for brevity >

  response-map
  ping-method        OPTIONS;hops=70
  ping-interval      60

< text removed for brevity >
```


The settings for the session agent used for CenturyLink East Remote DID peer:

```
session-agent
  hostname          172.16.3.9
  ip-address        172.16.3.9
  port              5060
  state             enabled
  app-protocol      SIP
  app-type
  transport-method  UDP
  realm-id          peer
  egress-realm-id
  description
  carriers
  allow-next-hop-lp enabled
  constraints        disabled
  max-sessions       0

< text removed for brevity >

  response-map
  ping-method        OPTIONS;hops=70
  ping-interval      60

< text removed for brevity >
```

The settings for the session agent used for CenturyLink West Inbound/Outbound peer:

```
session-agent
  hostname          172.16.2.8
  ip-address        172.16.2.8
  port              5060
  state             enabled
  app-protocol      SIP
  app-type
  transport-method  UDP
  realm-id          peer
  egress-realm-id
  description
  carriers
  allow-next-hop-lp enabled
  constraints        disabled
  max-sessions       0

< text removed for brevity >

  response-map
  ping-method        OPTIONS;hops=70
  ping-interval      60

< text removed for brevity >
```

The settings for the session agent used for CenturyLink West Remote DID peer:

```
session-agent
  hostname          172.16.2.9
  ip-address        172.16.2.9
  port              5060
  state             enabled
  app-protocol      SIP
  app-type
  transport-method  UDP
  realm-id          peer
  egress-realm-id
  description
  carriers
  allow-next-hop-lp enabled
  constraints        disabled
  max-sessions       0

< text removed for brevity >

  response-map
  ping-method        OPTIONS;hops=70
  ping-interval      60

< text removed for brevity >
```

The settings for the session agent used for CS1000E:

```
session-agent
  hostname          10.80.140.103
  ip-address        10.80.140.103
  port              5060
  state             enabled
  app-protocol      SIP
  app-type
  transport-method  TCP
  realm-id          core
  egress-realm-id
  description
  carriers
  allow-next-hop-lp enabled
  constraints        disabled
  max-sessions       0

< text removed for brevity >

  response-map
  ping-method        OPTIONS;hops=70
  ping-interval      60

< text removed for brevity >
```

6.8. Session Agent Group

Session agents can be configured in a session agent group (SAG), so multiple session agents can be assigned to a route policy for fail-over or load balancing purposes. For compliance testing CenturyLink had four session agents assigned. Two of them were used for remote DIDs and were allocated for inbound only, while the other two were used for both inbound and outbound traffic. Only the two session agents allocated for outbound traffic were added to the SAG.

The key session agent group (**session-group**) fields are:

- **group-name:** A descriptive string used to reference the session agent group.
- **state:** **enabled**
- **app-protocol:** **SIP**
- **strategy:** **Hunt** This strategy will route to the secondary session agent only if the primary fails. An alternative is to use a strategy of **RoundRobin**. This strategy will alternatively select between session agents.
- **dest:** The list of session agents to be added to the group by hostname. For compliance testing **172.16.3.8** and **172.16.2.8** were used.
- **sag-recursion:** **enabled** This allows Acme Packet 3820 to select a different session agent in the SAG if a failure occurs to the first session agent.

session-group	
group-name	CL-OUT
description	
state	enabled
app-protocol	SIP
strategy	Hunt
dest	172.16.3.8 172.16.2.8
trunk-group	
sag-recursion	enabled
stop-sag-recurse	401,407
last-modified-by	admin@10.80.150.38
last-modified-date	2012-06-18 10:27:19

6.9. SIP Manipulation

SIP manipulations are rules used to modify the SIP messages (if necessary) for interoperability. In **Section 6.4**, it was defined that the set of sip-manipulations named **NatIP** would be performed on outbound traffic in the **peer** realm and **AddDomain** would be performed on outbound traffic in the **core** realm. The sip-manipulation named **CS1K_To_CL** would be performed on inbound traffic from the **core** realm. For the complete configuration of these rules refer to **Appendix A**.

The key SIP manipulation (sip-manipulation) fields are:

- **name:** The name of this set of SIP header rules.
- **header-rule**
 - **name:** The name of this individual header rule.
 - **header-name:** The SIP header to be modified.
 - **action:** The action to be performed on the header.
 - **comparison-type:** The type of comparison performed when determining a match.
 - **msg-type:** The type of message to which this rule applies.
 - **element-rule**
 - **name:** The name of this individual element rule.
 - **type:** Defines the particular element in the header to be modified.
 - **action:** The action to be performed on the element.
 - **match-val-type:** Element matching criteria on the data type (if any) in order to perform the defined action.
 - **comparison-type:** The type of comparison performed when determining a match.
 - **match-value:** Element matching criteria on the data value (if any) in order to perform the defined action.
 - **new-value:** New value for the element (if any).

In the configuration file in **Appendix A**, the **NatIP** sip manipulation has many modifications (or header-rules) defined. These header manipulations were added to hide the private IP address and enterprise domain name which appear in the “To”, “From”, “Request-URI”, “Diversion” and “PAI” SIP headers for outbound calls. As well as remove unwanted headers going to the SIP service provider.

Similarly the **AddDomain** sip manipulation was used towards CS1000E to hide the public IP addresses and to add the enterprise domain to the “From” and “PAI” SIP headers.

The **CS1K_To_CL** sip manipulation was used to add a “Diversion” header from the “History-Info” header for redirected calls from CS1000E. This was added to the inbound traffic to the Acme Packet 3820 so that it could be further modified by the **NatIP** sip manipulation to remove the “History-Info” header and to hide the enterprise domain name.

The example below shows the **natFROM header-rule** in the **NatIP** sip manipulation. It specifies that the “From” header in SIP request messages will be manipulated based on the element rule defined. The element rule **natHost** will match any value in the host part of the URI and replace it with the value of **\$LOCAL_IP**. The value of **\$LOCAL_IP** is the outside IP address of the Acme Packet 3820. See **Appendix A** for the complete **NatIP** sip manipulation used during compliance testing.

```

sip-manipulation
  name                               NatIP
  description
  split-headers
  join-headers
  header-rule
    name                             natFROM
    header-name                       From
    action                           manipulate
    comparison-type                   case-sensitive
    msg-type                         request
    methods
    match-value
    new-value
    element-rule
      name                           natHost
      parameter-name
      type                           uri-host
      action                         replace
      match-val-type                 any
      comparison-type                 case-sensitive
      match-value
      new-value                       $LOCAL_IP

< text removed for brevity >

```

The **NatIP** sip manipulation was also used to remove the “History-Info” and “x-nt-e164-clid” headers and unwanted MIMEs in the body of the message.

header-rule		
name	removeHist	
header-name	History-Info	
action	delete	
comparison-type	case-sensitive	
msg-type	any	
methods		
match-value		
new-value		
header-rule		
name	removeXNTE164	
header-name	X-nt-e164-clid	
action	delete	
comparison-type	case-sensitive	
msg-type	any	
methods		
match-value		
new-value		
header-rule		
name	removeMultiMIME	
header-name	Content-Type	
action	manipulate	
comparison-type	case-sensitive	
msg-type	any	
methods		
match-value		
new-value		
element-rule		
name	nt_mcdn	
parameter-name	application/x-nt-	
mcdn-frag-hex;version=ssLinux-7.50.17;base=x2611		
type	mime	
action	delete-element	
match-val-type	any	
comparison-type	case-sensitive	
match-value		
new-value		
element-rule		
name	nt_esn5	
parameter-name	application/x-nt-	
esn5-frag-hex		
type	mime	
action	delete-element	
match-val-type	any	
comparison-type	case-sensitive	
match-value		
new-value		
element-rule		
name	nt_epid	
parameter-name	application/x-nt-	
epid-frag-hex;version=ssLinux-7.50.17;base=x2611		
type	mime	
action	delete-element	
match-val-type	any	
comparison-type	case-sensitive	
match-value		
new-value		

The example below shows the **FromDomain** header-rule in the **AddDomain** sip manipulation. It specifies that the “From” header in SIP request messages will be manipulated based on the element rule defined. The element rule **From** will match any value in the host part of the URI and replace it with the value of **avayalab.com**. The value of **avayalab.com** is the domain name used in the enterprise. This value should match the Domain set in the CS1000E SIP Gateway (Section 5.1.5).

sip-manipulation	
name	AddDomain
description	
split-headers	
join-headers	
header-rule	
name	FromDomain
header-name	From
action	manipulate
comparison-type	case-sensitive
msg-type	request
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	avayalab.com
< text removed for brevity >	

The example below shows the **CS1K_To_CL** sip manipulation. This manipulation uses the PAI and History Info headers to determine the type of call redirection and builds a Diversion header accordingly. The header rule **AddDiversion1** specifies that if the P-Asserted-Identity header does not have a phone number within the range 303-555-7100 to 303-5557199 (the DID range specified by CenturyLink) and does not have a “reason” parameter in the History-Info header, a static Diversion header will be created. The header rules **AddDiversion2**, **AddDiversion3** and **AddDiversion4** will create a Diversion header based on all 3 redirection reasons with the user and host gathered from the History-Info header.

```

sip-manipulation
  name          CS1K_To_CL
  description    CS1K_to_CL
  split-headers
  join-headers
  header-rule
    name          PAIRegex
    header-name    P-Asserted-Identity
    action          store
    comparison-type pattern-rule
    msg-type        any
    methods          INVITE
    match-value
    new-value
    element-rule
      name          chkUser
      parameter-name
      type
      action          header-value
      match-val-type store
      comparison-type any
      match-value     pattern-rule
      new-value        (.*) (30355571) (.*)

  header-rule
    name          HistRegex
    header-name    History-Info
    action          store
    comparison-type pattern-rule
    msg-type        any
    methods
    match-value
    new-value
    element-rule
      name          GetReason1
      parameter-name
      type          header-value
      action          store
      match-val-type any
      comparison-type pattern-rule
      match-value     (.*) (reason) (.*)
      new-value
    element-rule
      name          GetReason2
      parameter-name
      type          header-value
      action          none
      match-val-type any
      comparison-type pattern-rule
      match-value     (.*) (Moved) (.*)
      new-value

```



```

    element-rule
        name                    GetReason3
        parameter-name
        type                    header-value
        action                  none
        match-val-type          any
        comparison-type          pattern-rule
        match-value              (.*) (Busy) (.*)
        new-value
    element-rule
        name                    GetReason4
        parameter-name
        type                    header-value
        action                  none
        match-val-type          any
        comparison-type          pattern-rule
        match-value              (.*) (Unavailable) (.*)
        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
header-rule
    name                    AddDiversion1
    header-name              Diversion
    action                  add
    comparison-type          boolean
    msg-type                request
    methods                  INVITE
    match-value              (!$PAIRex[0] . $chkUser) &!$HistRegex[0] . $GetReason1
    new-value                "<sip:3035557104@avayalab.com;user=phone>"
header-rule
    name                    AddDiversion2
    header-name              Diversion
    action                  add
    comparison-type          boolean
    msg-type                request
    methods                  INVITE
    match-value              $HistRegex[0] . $GetReason2
    new-value
<sip:+$HistRegex[0] . $GetUser . $0+@$HistRegex[0] . $GetHost . $0+>;privacy=off;reason=unconditional;
screen=no

```

```

header-rule
    name                AddDiversion3
    header-name          Diversion
    action               add
    comparison-type      boolean
    msg-type             request
    methods              INVITE
    match-value          $HistRegex[0].$GetReason3
    new-value
<sip:+$HistRegex[0].$GetUser.$0+@$HistRegex[0].$GetHost.$0+>;privacy=off;reason=user\-
busy;screen=no
header-rule
    name                AddDiversion4
    header-name          Diversion
    action               add
    comparison-type      boolean
    msg-type             request
    methods              INVITE
    match-value          $HistRegex[0].$GetReason4
    new-value
<sip:+$HistRegex[0].$GetUser.$0+@$HistRegex[0].$GetHost.$0+>;privacy=off;reason=no\-
answer;screen=no

```

6.10. 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 Acme Packet 3820.
- **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          10.2.2.92
    start-port          49152
    end-port            65535
    realm-id            peer
    network-interface
    last-modified-by    admin@console
    last-modified-date  2012-06-06 15:07:34
steering-pool
    ip-address          10.64.19.150
    start-port          49152
    end-port            65535
    realm-id            core
    network-interface
    last-modified-by    admin@console
    last-modified-date  2012-06-06 15:08:02

```

6.11. Local Policy

Local policy controls the routing of SIP calls from one realm to another.

The key local policy (**local-policy**) fields are:

- **from-address:** A policy filter indicating the originating IP address to which this policy applies. An asterisk (*) indicates any IP address.
- **to-address:** A policy filter indicating the terminating IP address to which this policy applies. An asterisk (*) indicates any IP address.
- **source-realm:** A policy filter indicating the matching realm in order for the policy rules to be applied.
- **policy-attribute:**
 - **next-hop:** The IP address where the message should be sent when the policy rules match.
 - **realm:** The realm associated with the next-hop IP address.

In this case, the first policy provides a simple routing rule indicating that messages originating from the **peer** realm are to be sent to the **core** realm via IP address **10.80.140.103** (CS1000E at the enterprise). The second policy indicates that messages originating from the **core** realm are to be sent to the **peer** realm via the Session Agent Group **CL-OUT** created in **Section 6.8**.

```

local-policy
  from-address      *
  to-address        *
  source-realm      peer
  description
  activate-time     N/A

< text removed for brevity >

  policy-attribute
    next-hop        10.80.140.103
    realm           core
    action          none

< text removed for brevity >

local-policy
  from-address      *
  to-address        *
  source-realm      core
  description
  activate-time     N/A

< text removed for brevity >

  policy-attribute
    next-hop        SAG:CL-OUT
    realm           peer

< text removed for brevity >

```

7. CenturyLink SIP Trunk Service Configuration

To use CenturyLink SIP Trunk Service, a customer must request the service from CenturyLink using their sales processes. This process can be initiated by contacting CenturyLink via the corporate web site at www.centurylink.com and requesting information via the online sales links or telephone numbers

8. Verification

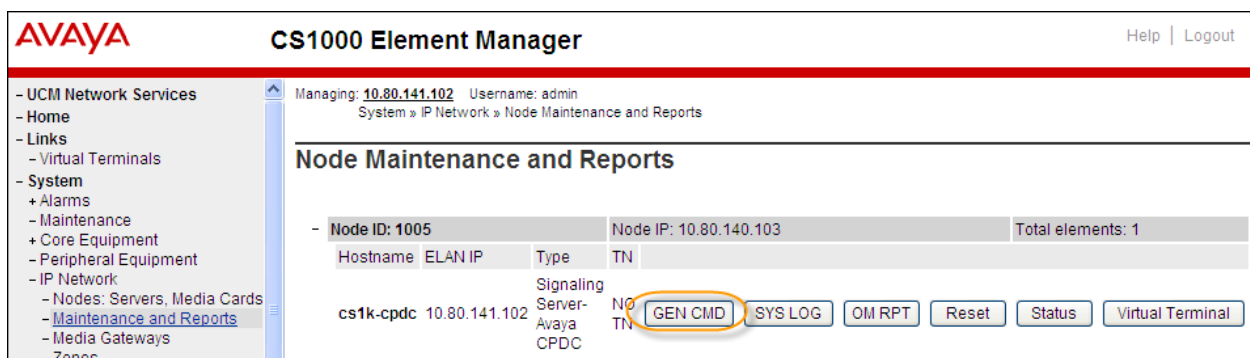
This section provides verification steps that may be performed in the field to verify that the solution is configured properly.

8.1. Avaya Communication Server 1000E Verifications

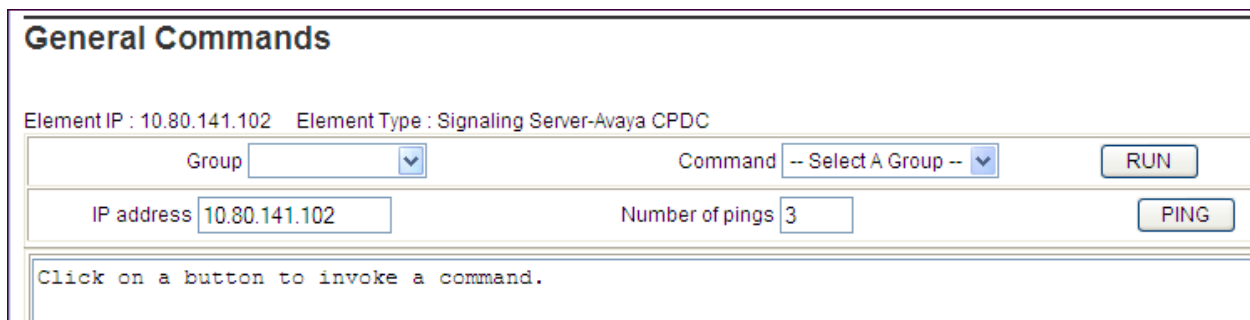
This section illustrates sample verifications that may be performed using the Avaya CS1000E Element Manager GUI.

8.1.1. IP Network Maintenance and Reports Commands

From Element Manager, navigate to **System → IP Network → Maintenance and Reports** as shown below. In the resultant screen on the right, click the Gen CMD button.



The **General Commands** page is displayed as shown below.



A variety of commands are available by selecting an appropriate Group and Command from the drop-down menus, and selecting Run.

To check the status of the SIP Gateway to Acme Packet 3820 in the sample configuration, select **Sip** from the Group menu and **SIPGwShow** from the **Command** menu. Click Run. The example output below shows that Acme Packet (10.64.19.150, port 5060, TCP) has **SIPNPM Status** Active.

General Commands

Element IP : 10.80.141.102 Element Type : Signaling Server-Avaya CPDC

Group Sip
Command SIPGwShow
Sip
RUN

IP address 10.80.141.102
Number of pings 3
PING

```

SIPNPM Status           : Active
Primary Proxy IP address : 10.64.19.150
Primary Proxy port       : 5060
Primary Proxy Transport  : TCP
Secondary Proxy IP address : 0.0.0.0
Secondary Proxy port     : 5060
Secondary Proxy Transport : TCP
Primary Proxy2 IP address : 10.64.19.150
Primary Proxy2 port      : 5060
Primary Proxy2 Transport : TCP
Active Proxy             : Primary :Register Not Supported
Time To Next Registration : 0 Seconds
Channels Busy / Idle / Total : 0 / 32 / 32
Stack version            : 5.5.0.13
TLS Security Policy      : Security Disabled

```

The following screen shows a means to view registered SIP telephones. The screen shows the output of the **Command sigSetShowAll** in **Group SipLine**. At the time this screen was captured, the SIP telephone with DN 7108 was involved in an active call with the CenturyLink SIP Trunk Service.

General Commands

Element IP : 10.80.141.102 Element Type : Signaling Server-Avaya CPDC

Group SipLine
Command sigSetShowAll
RUN

IP address 10.80.141.102
Number of pings 3
PING

UserID	AuthId	TN	Clients	Calls	SetHandle	Pos ID	SIPL Type
----- IPv4 Endpoints -----							
7108	7108	252-00-09-01	1	1	0x8d155f8		SIP Lines
5685	5685	252-00-09-02	1	0	0xb7e16e58		SIP Lines
Total User Registered = 2 V4 Registered = 2 V6 Registered = 0							

The following screen shows a means to view IP UNISim telephones. The screen shows the output of the **Command isetShow** in **Group Iset**. At the time this screen was captured, the UNISim telephone with IP address **10.80.150.111** was involved in an active call with the CenturyLink SIP Trunk Service.

General Commands

Element IP : 10.80.141.102 Element Type : Signaling Server-Avaya CPDC

Group **Iset** Command **isetShow** Range **0** **500** **RUN**

IP address **10.80.141.102** Number of pings **3** **PING**

Set Information

IP Address	NAT	Model Name	Type	RegType	State	Up
10.80.150.111		1165E IP Deskphone	1165	Regular	busy	1
10.80.150.113		1165E IP Deskphone	1165	Regular	online	1

Total sets = 2

8.1.2. System Maintenance Commands

A variety of system maintenance commands are available by navigating to **System** → **Maintenance** using Element Manager. The user can navigate the maintenance commands using either the **Select by Overlay** approach or the **Select by Functionality** approach.

The following screen shows an example where **Select by Overlay** has been chosen. The various overlays are listed, and the **LD 96 – D-Channel** is selected.

AVAYA CS1000 Element Manager Help | Logout

Managing: **10.80.141.102** Username: admin
System » Maintenance

Maintenance

☒ Select by Overlay ☐ Select by Functionality

<Select by Overlay>

- LD 30 - Network and Signaling
- LD 32 - Network and Peripheral Equipment
- LD 34 - Tone and Digit Switch
- LD 36 - Trunk
- LD 37 - Input/Output
- LD 38 - Conference Circuit
- LD 39 - Intergroup Switch and System Clock
- LD 45 - Background Signaling and Switching
- LD 46 - Multifrequency Sender
- LD 48 - Link
- LD 54 - Multifrequency Signaling
- LD 60 - Digital Trunk Interface and Primary Rate Interface
- LD 75 - Digital Trunk
- LD 80 - Call Trace
- LD 96 - D-Channel**
- LD 117 - Ethernet and Alarm Management
- LD 135 - Core Common Equipment
- LD 137 - Core Input/Output
- LD 143 - Centralized Software Upgrade

<Select Group>

- D-Channel Diagnostics
- MSDL Diagnostics
- TMDI Diagnostics

On the preceding screen, if **D-Channel Diagnostics** is selected on the right, a screen such as the following is displayed. D-Channel number 15, which is used in the sample configuration, is established **EST** and active **ACTV**.

D-Channel Diagnostics

Diagnostic Commands	Command Parameters	Action
Status for D-Channel (STAT DCH) <input type="button" value="v"/>		<input type="button" value="Submit"/>
Disable Automatic Recovery (DIS AUTO) <input type="button" value="v"/>	<input type="checkbox"/> ALL	<input type="button" value="Submit"/>
Enable Automatic Recovery (ENL AUTO) <input type="button" value="v"/>	<input type="checkbox"/> FDL	<input type="button" value="Submit"/>
Test Interrupt Generation (TEST 100) <input type="button" value="v"/>		<input type="button" value="Submit"/>
Establish D-Channel (EST DCH) <input type="button" value="v"/>		<input type="button" value="Submit"/>

DCH	DES	APPL_STATUS	LINK_STATUS	AUTO_RECV	PDCH	BDCH
<input type="radio"/> 015	VtrkNode1005	OPER	EST	ACTV	AUTO	

Instruction: Select a command, add value and click on [Submit].

8.2. Acme Packet 3820 Net-Net ® Session Director Verifications

Below is a list of commands used to verify the configuration of the Acme Packet 3820.

- **show running-config** – Displays the current config
- **verify-config** – Displays any errors or warnings in the configuration.
- **show prom-info all** – Displays the all prom information including serial number, hardware revision, manufacturing date, part numbers and more
- **show sipd sessions all** – Will display all of the active SIP sessions that are currently traversing the SBC, including the To, From, Call-ID.
- **show support-info** - Outputs all of the system level info, including hardware specifics, licensing info, current call volume, etc.
- **show health** - For a redundant system will give a status of synchronized processes and an overview of failover history
- **show sipd invite** - Will display a chart of all recent SIP requests and responses
- **display-alarms** - Alarm log output of recent and current alarms
- **show logfile sipmsg.log** - Will output the contents of the sipmsg.log without having to FTP this file off the SBC

9. Conclusion

These Application Notes describe the configuration necessary to connect Avaya Communication Server 1000E and Acme Packet 3820 Net-Net Session Director to the CenturyLink SIP Trunk Service (Legacy Qwest). The CenturyLink SIP Trunk Service is a SIP-based Voice over IP solution for customers ranging from small businesses to large enterprises. The CenturyLink SIP Trunk Service provides businesses a flexible, cost-saving alternative to traditional hardwired telephony trunks.

10. Additional References

This section references the documentation relevant to these Application Notes. Additional Avaya product documentation is available at <http://support.avaya.com>.

- [1] *Avaya Communication Server 1000E Installation and Commissioning*, November 2010, Document Number NN43041-310.
- [2] *Feature Listing Reference Avaya Communication Server 1000*, November 2010, Document Number NN43001-111, 05.01.
- [3] *RFC 3261 SIP: Session Initiation Protocol*, <http://www.ietf.org/>
- [4] *Signaling Server IP Line Applications Fundamentals Avaya Communication Server 1000*, Document Number NN43001-125, 03.09 October 2011
- [5] *Linux Platform Base and Applications Installation and Commissioning Avaya Communication Server 1000*, Document Number NN43001-315, 05.18 January 2012
- [6] *SIP Software for Avaya 1100 Series IP Deskphones-Administration*, Document Number NN43170-600, Standard 04.02 December 2011
- [7] *Acme Packet, "Net-Net 4000 S-CX6.3.0 ACLI Configuration Guide"*, 400-0061-62, Nov 2009
- [8] *Acme Packet, "Net-Net 3800 Series And Net-Net 4500 SSM2 Installation Guide"*, 400-0114-20, Apr 2010
- [9] *Acme Packet, "Net-Net 3820 Hardware Installation Guide"*, 400-0134-10, Mar 2011

Appendix A: Acme Packet 3820 Configuration File

Included below is the Acme Packet 3820 configuration used during the compliance testing. The contents of the configuration can be shown by using the ACLI command **show running-config** at the Acme Packet 3820.

```
ACMESYSTEM# show running-config
local-policy
    from-address          *
    to-address            *
    source-realm          peer
    description
    activate-time         N/A
    deactivate-time       N/A
    state                 enabled
    policy-priority       none
    last-modified-by      admin@10.80.150.50
    last-modified-date    2012-06-28 16:05:37
    policy-attribute
        next-hop          10.80.140.103
        realm             core
        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	*
to-address	*
source-realm	core
description	
activate-time	N/A
deactivate-time	N/A
state	enabled
policy-priority	none
last-modified-by	admin@10.80.150.38
last-modified-date	2011-11-03 17:39:11
policy-attribute	

next-hop	SAG: CL-OUT
realm	peer
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	

media-manager

state	enabled
latching	enabled
flow-time-limit	86400
initial-guard-timer	300
subsq-guard-timer	300
tcp-flow-time-limit	86400
tcp-initial-guard-timer	300
tcp-subsq-guard-timer	300
tcp-number-of-ports-per-flow	2
hnt-rtcp	disabled
algd-log-level	NOTICE
mbcd-log-level	NOTICE
red-flow-port	1985
red-mgcp-port	1986
red-max-trans	10000
red-sync-start-time	5000
red-sync-comp-time	1000
media-policing	enabled
max-signaling-bandwidth	10000000
max-untrusted-signaling	100
min-untrusted-signaling	30
app-signaling-bandwidth	0
tolerance-window	30
rtcp-rate-limit	0
trap-on-demote-to-deny	disabled
syslog-on-demote-to-deny	disabled
syslog-on-demote-to-untrusted	disabled
anonymous-sdp	disabled
arp-msg-bandwidth	32000
fragment-msg-bandwidth	0
rfc2833-timestamp	disabled
default-2833-duration	100
rfc2833-end-pkts-only-for-non-sig	enabled

```

translate-non-rfc2833-event disabled
media-supervision-traps disabled
dnsmalg-server-failover disabled
last-modified-by admin@10.80.150.38
last-modified-date 2011-11-01 12:25:41
network-interface
  name M00
  sub-port-id 0
  description PUBLIC
  hostname
  ip-address 10.2.2.92
  pri-utility-addr
  sec-utility-addr
  netmask 255.255.255.128
  gateway 10.2.2.1
  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 10.2.2.92
  ftp-address
  icmp-address 10.2.2.92
  snmp-address
  telnet-address
  ssh-address
  signaling-mtu 0
  last-modified-by admin@10.80.150.50
  last-modified-date 2012-06-06 14:40:39
network-interface
  name M10
  sub-port-id 0
  description PRIVATE
  hostname
  ip-address 10.64.19.150
  pri-utility-addr
  sec-utility-addr
  netmask 255.255.255.0
  gateway 10.64.19.1
  sec-gateway
  gw-heartbeat
    state disabled
    heartbeat 0
    retry-count 0
    retry-timeout 1
    health-score 0
  dns-ip-primary 10.80.150.201
  dns-ip-backup1
  dns-ip-backup2
  dns-domain avayalab.com
  dns-timeout 11
  hip-ip-list 10.64.19.150
  ftp-address
  icmp-address 10.64.19.150
  snmp-address
  telnet-address
  ssh-address
  signaling-mtu 0
  last-modified-by admin@10.80.150.50
  last-modified-date 2012-06-06 14:42:37
phy-interface
  name M00
  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 2011-11-01 09:59:56
phy-interface
    name M10
    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 2011-11-01 10:00:38
realm-config
    identifier peer
    description
    addr-prefix 0.0.0.0
    network-interfaces
    M00:0
    mm-in-realm enabled
    mm-in-network enabled
    mm-same-ip enabled
    mm-in-system enabled
    bw-cac-non-mm disabled
    msm-release disabled
    qos-enable disabled
    generate-UDP-checksum disabled
    max-bandwidth 0
    fallback-bandwidth 0
    max-priority-bandwidth 0
    max-latency 0
    max-jitter 0
    max-packet-loss 0
    observ-window-size 0
    parent-realm
    dns-realm
    media-policy
    media-sec-policy
    srtp-msm-passthrough disabled
    in-translationid
    out-translationid
    in-manipulationid
    out-manipulationid NatIP
    manipulation-string
    manipulation-pattern
    class-profile
    average-rate-limit 0
    access-control-trust-level none
    invalid-signal-threshold 0
    maximum-signal-threshold 0
    untrusted-signal-threshold 0
    nat-trust-threshold 0
    deny-period 30
    cac-failure-threshold 0
    untrust-cac-failure-threshold 0
    ext-policy-svr
    diam-e2-address-realm
    symmetric-latching disabled
    pai-strip disabled
    trunk-context

```

early-media-allow	
enforcement-profile	
additional-prefixes	
restricted-latching	none
restriction-mask	32
accounting-enable	enabled
user-cac-mode	none
user-cac-bandwidth	0
user-cac-sessions	0
icmp-detect-multiplier	0
icmp-advertisement-interval	0
icmp-target-ip	
monthly-minutes	0
net-management-control	disabled
delay-media-update	disabled
refer-call-transfer	disabled
refer-notify-provisional	none
dyn-refer-term	disabled
codec-policy	
codec-manip-in-realm	disabled
constraint-name	
call-recording-server-id	
xnq-state	xnq-unknown
hairpin-id	0
stun-enable	disabled
stun-server-ip	0.0.0.0
stun-server-port	3478
stun-changed-ip	0.0.0.0
stun-changed-port	3479
match-media-profiles	
qos-constraint	
sip-profile	
sip-isup-profile	
block-rtcp	disabled
hide-egress-media-update	disabled
last-modified-by	admin@10.80.150.38
last-modified-date	2011-11-01 13:03:09
realm-config	
identifier	core
description	
addr-prefix	0.0.0.0
network-interfaces	
mm-in-realm	M10:0
mm-in-network	enabled
mm-same-ip	enabled
mm-in-system	enabled
bw-cac-non-mm	disabled
msm-release	disabled
qos-enable	disabled
generate-UDP-checksum	disabled
max-bandwidth	0
fallback-bandwidth	0
max-priority-bandwidth	0
max-latency	0
max-jitter	0
max-packet-loss	0
observ-window-size	0
parent-realm	
dns-realm	
media-policy	
media-sec-policy	
srtp-msm-passthrough	disabled
in-translationid	
out-translationid	
in-manipulationid	CS1K_To_CL
out-manipulationid	AddDomain
manipulation-string	
manipulation-pattern	
class-profile	

average-rate-limit	0
access-control-trust-level	none
invalid-signal-threshold	0
maximum-signal-threshold	0
untrusted-signal-threshold	0
nat-trust-threshold	0
deny-period	30
cac-failure-threshold	0
untrust-cac-failure-threshold	0
ext-policy-svr	
diam-e2-address-realm	
symmetric-latching	disabled
pai-strip	disabled
trunk-context	
early-media-allow	
enforcement-profile	
additional-prefixes	
restricted-latching	none
restriction-mask	32
accounting-enable	enabled
user-cac-mode	none
user-cac-bandwidth	0
user-cac-sessions	0
icmp-detect-multiplier	0
icmp-advertisement-interval	0
icmp-target-ip	
monthly-minutes	0
net-management-control	disabled
delay-media-update	disabled
refer-call-transfer	disabled
refer-notify-provisional	none
dyn-refer-term	disabled
codec-policy	
codec-manip-in-realm	disabled
constraint-name	
call-recording-server-id	
xnq-state	xnq-unknown
hairpin-id	0
stun-enable	disabled
stun-server-ip	0.0.0.0
stun-server-port	3478
stun-changed-ip	0.0.0.0
stun-changed-port	3479
match-media-profiles	
qos-constraint	
sip-profile	
sip-isup-profile	
block-rtcp	disabled
hide-egress-media-update	disabled
last-modified-by	admin@10.80.150.50
last-modified-date	2012-06-21 12:20:52
session-agent	
hostname	10.80.140.103
ip-address	10.80.140.103
port	5060
state	enabled
app-protocol	SIP
app-type	
transport-method	UDP
realm-id	core
egress-realm-id	
description	
carriers	
allow-next-hop-lp	enabled
constraints	disabled
max-sessions	0
max-inbound-sessions	0
max-outbound-sessions	0
max-burst-rate	0
max-inbound-burst-rate	0

max-outbound-burst-rate	0
max-sustain-rate	0
max-inbound-sustain-rate	0
max-outbound-sustain-rate	0
min-seizures	5
min-asr	0
time-to-resume	0
ttr-no-response	0
in-service-period	0
burst-rate-window	0
sustain-rate-window	0
req-uri-carrier-mode	None
proxy-mode	
redirect-action	Proxy
loose-routing	enabled
send-media-session	enabled
response-map	
ping-method	OPTIONS;hops=70
ping-interval	60
ping-send-mode	keep-alive
ping-all-addresses	disabled
ping-in-service-response-codes	
out-service-response-codes	
load-balance-dns-query	hunt
media-profiles	
in-translationid	
out-translationid	
trust-me	disabled
request-uri-headers	
stop-recurse	
local-response-map	
ping-to-user-part	
ping-from-user-part	
li-trust-me	disabled
in-manipulationid	
out-manipulationid	
manipulation-string	
manipulation-pattern	
p-asserted-id	
trunk-group	
max-register-sustain-rate	0
early-media-allow	
invalidate-registrations	disabled
rfc2833-mode	none
rfc2833-payload	0
codec-policy	
enforcement-profile	
refer-call-transfer	disabled
refer-notify-provisional	none
reuse-connections	NONE
tcp-keepalive	none
tcp-reconn-interval	0
max-register-burst-rate	0
register-burst-window	0
sip-profile	
sip-isup-profile	
kpml-interworking	inherit
last-modified-by	admin@10.80.150.50
last-modified-date	2012-06-28 16:04:46
session-agent	
hostname	172.16.2.8
ip-address	172.16.2.8
port	5060
state	enabled
app-protocol	SIP
app-type	
transport-method	UDP
realm-id	peer
egress-realm-id	
description	

carriers	
allow-next-hop-lp	enabled
constraints	disabled
max-sessions	0
max-inbound-sessions	0
max-outbound-sessions	0
max-burst-rate	0
max-inbound-burst-rate	0
max-outbound-burst-rate	0
max-sustain-rate	0
max-inbound-sustain-rate	0
max-outbound-sustain-rate	0
min-seizures	5
min-asr	0
time-to-resume	0
ttr-no-response	0
in-service-period	0
burst-rate-window	0
sustain-rate-window	0
req-uri-carrier-mode	None
proxy-mode	
redirect-action	
loose-routing	enabled
send-media-session	enabled
response-map	
ping-method	OPTIONS; hops=70
ping-interval	60
ping-send-mode	keep-alive
ping-all-addresses	disabled
ping-in-service-response-codes	
out-service-response-codes	
load-balance-dns-query	hunt
media-profiles	
in-translationid	
out-translationid	
trust-me	disabled
request-uri-headers	
stop-recurse	
local-response-map	
ping-to-user-part	
ping-from-user-part	
li-trust-me	disabled
in-manipulationid	
out-manipulationid	
manipulation-string	
manipulation-pattern	
p-asserted-id	
trunk-group	
max-register-sustain-rate	0
early-media-allow	
invalidate-registrations	disabled
rfc2833-mode	none
rfc2833-payload	0
codec-policy	
enforcement-profile	
refer-call-transfer	disabled
refer-notify-provisional	none
reuse-connections	NONE
tcp-keepalive	none
tcp-reconn-interval	0
max-register-burst-rate	0
register-burst-window	0
sip-profile	
sip-isup-profile	
kpml-interworking	inherit
last-modified-by	admin@10.80.150.38
last-modified-date	2011-11-01 12:39:40
session-agent	
hostname	172.16.2.9
ip-address	172.16.2.9

port	5060
state	enabled
app-protocol	SIP
app-type	
transport-method	UDP
realm-id	peer
egress-realm-id	
description	
carriers	
allow-next-hop-lp	enabled
constraints	disabled
max-sessions	0
max-inbound-sessions	0
max-outbound-sessions	0
max-burst-rate	0
max-inbound-burst-rate	0
max-outbound-burst-rate	0
max-sustain-rate	0
max-inbound-sustain-rate	0
max-outbound-sustain-rate	0
min-seizures	5
min-asr	0
time-to-resume	0
ttr-no-response	0
in-service-period	0
burst-rate-window	0
sustain-rate-window	0
req-uri-carrier-mode	None
proxy-mode	
redirect-action	
loose-routing	enabled
send-media-session	enabled
response-map	
ping-method	OPTIONS;hops=70
ping-interval	60
ping-send-mode	keep-alive
ping-all-addresses	disabled
ping-in-service-response-codes	
out-service-response-codes	
load-balance-dns-query	hunt
media-profiles	
in-translationid	
out-translationid	
trust-me	disabled
request-uri-headers	
stop-recurse	
local-response-map	
ping-to-user-part	
ping-from-user-part	
li-trust-me	disabled
in-manipulationid	
out-manipulationid	
manipulation-string	
manipulation-pattern	
p-asserted-id	
trunk-group	
max-register-sustain-rate	0
early-media-allow	
invalidate-registrations	disabled
rfc2833-mode	none
rfc2833-payload	0
codec-policy	
enforcement-profile	
refer-call-transfer	disabled
refer-notify-provisional	none
reuse-connections	NONE
tcp-keepalive	none
tcp-reconn-interval	0
max-register-burst-rate	0
register-burst-window	0

```

sip-profile
sip-isup-profile
kpml-interworking                inherit
last-modified-by                 admin@10.80.150.38
last-modified-date               2011-11-01 12:39:46
session-agent
  hostname                        172.16.3.8
  ip-address                      172.16.3.8
  port                           5060
  state                           enabled
  app-protocol                    SIP
  app-type
  transport-method                UDP
  realm-id                        peer
  egress-realm-id
  description
  carriers
  allow-next-hop-lp               enabled
  constraints                     disabled
  max-sessions                    0
  max-inbound-sessions            0
  max-outbound-sessions           0
  max-burst-rate                  0
  max-inbound-burst-rate          0
  max-outbound-burst-rate         0
  max-sustain-rate                0
  max-inbound-sustain-rate        0
  max-outbound-sustain-rate       0
  min-seizures                    5
  min-asr                         0
  time-to-resume                  0
  ttr-no-response                 0
  in-service-period               0
  burst-rate-window               0
  sustain-rate-window             0
  req-uri-carrier-mode            None
  proxy-mode
  redirect-action
  loose-routing                   enabled
  send-media-session              enabled
  response-map
  ping-method                     OPTIONS;hops=70
  ping-interval                   60
  ping-send-mode                  keep-alive
  ping-all-addresses             disabled
  ping-in-service-response-codes
  out-service-response-codes
  load-balance-dns-query          hunt
  media-profiles
  in-translationid
  out-translationid
  trust-me                        disabled
  request-uri-headers
  stop-recurse
  local-response-map
  ping-to-user-part
  ping-from-user-part
  li-trust-me                     disabled
  in-manipulationid
  out-manipulationid
  manipulation-string
  manipulation-pattern
  p-asserted-id
  trunk-group
  max-register-sustain-rate       0
  early-media-allow
  invalidate-registrations         disabled
  rfc2833-mode                    none
  rfc2833-payload                 0
  codec-policy

```

enforcement-profile	
refer-call-transfer	disabled
refer-notify-provisional	none
reuse-connections	NONE
tcp-keepalive	none
tcp-reconn-interval	0
max-register-burst-rate	0
register-burst-window	0
sip-profile	
sip-isup-profile	
kpml-interworking	inherit
last-modified-by	admin@10.80.150.50
last-modified-date	2012-06-18 10:23:25
session-agent	
hostname	172.16.3.9
ip-address	172.16.3.9
port	5060
state	enabled
app-protocol	SIP
app-type	
transport-method	UDP
realm-id	peer
egress-realm-id	
description	
carriers	
allow-next-hop-lp	enabled
constraints	disabled
max-sessions	0
max-inbound-sessions	0
max-outbound-sessions	0
max-burst-rate	0
max-inbound-burst-rate	0
max-outbound-burst-rate	0
max-sustain-rate	0
max-inbound-sustain-rate	0
max-outbound-sustain-rate	0
min-seizures	5
min-asr	0
time-to-resume	0
ttr-no-response	0
in-service-period	0
burst-rate-window	0
sustain-rate-window	0
req-uri-carrier-mode	None
proxy-mode	
redirect-action	
loose-routing	enabled
send-media-session	enabled
response-map	
ping-method	OPTIONS;hops=70
ping-interval	60
ping-send-mode	keep-alive
ping-all-addresses	disabled
ping-in-service-response-codes	
out-service-response-codes	
load-balance-dns-query	hunt
media-profiles	
in-translationid	
out-translationid	
trust-me	disabled
request-uri-headers	
stop-recurse	
local-response-map	
ping-to-user-part	
ping-from-user-part	
li-trust-me	disabled
in-manipulationid	
out-manipulationid	
manipulation-string	
manipulation-pattern	

p-asserted-id	
trunk-group	
max-register-sustain-rate	0
early-media-allow	
invalidate-registrations	disabled
rfc2833-mode	none
rfc2833-payload	0
codec-policy	
enforcement-profile	
refer-call-transfer	disabled
refer-notify-provisional	none
reuse-connections	NONE
tcp-keepalive	none
tcp-reconn-interval	0
max-register-burst-rate	0
register-burst-window	0
sip-profile	
sip-isup-profile	
kpml-interworking	inherit
last-modified-by	admin@10.80.150.50
last-modified-date	2012-06-18 10:23:57
session-group	
group-name	CL-OUT
description	
state	enabled
app-protocol	SIP
strategy	Hunt
dest	
	172.16.3.8
	172.16.2.8
trunk-group	
sag-recursion	enabled
stop-sag-recurse	401,407
last-modified-by	admin@10.80.150.50
last-modified-date	2012-06-18 10:27:19
sip-config	
state	enabled
operation-mode	dialog
dialog-transparency	enabled
home-realm-id	core
egress-realm-id	core
nat-mode	None
registrar-domain	
registrar-host	
registrar-port	0
register-service-route	always
init-timer	500
max-timer	4000
trans-expire	32
invite-expire	180
inactive-dynamic-conn	32
enforcement-profile	
pac-method	
pac-interval	10
pac-strategy	PropDist
pac-load-weight	1
pac-session-weight	1
pac-route-weight	1
pac-callid-lifetime	600
pac-user-lifetime	3600
red-sip-port	1988
red-max-trans	10000
red-sync-start-time	5000
red-sync-comp-time	1000
add-reason-header	disabled
sip-message-len	4096
enum-sag-match	disabled
extra-method-stats	disabled
registration-cache-limit	0
register-use-to-for-lp	disabled

options	max-udp-length=0
refer-src-routing	disabled
add-ucid-header	disabled
proxy-sub-events	
allow-pani-for-trusted-only	disabled
pass-gruu-contact	disabled
sag-lookup-on-redirect	disabled
set-disconnect-time-on-bye	disabled
last-modified-by	admin@10.80.150.38
last-modified-date	2011-11-21 17:43:22
sip-interface	
state	enabled
realm-id	peer
description	
sip-port	
address	10.2.2.92
port	5060
transport-protocol	UDP
tls-profile	
multi-home-addr	
allow-anonymous	agents-only
ims-aka-profile	
carriers	
trans-expire	0
invite-expire	0
max-redirect-contacts	0
proxy-mode	
redirect-action	
contact-mode	none
nat-traversal	none
nat-interval	30
tcp-nat-interval	90
registration-caching	disabled
min-reg-expire	300
registration-interval	3600
route-to-registrar	disabled
secured-network	disabled
teluri-scheme	disabled
uri-fqdn-domain	
trust-mode	all
max-nat-interval	3600
nat-int-increment	10
nat-test-increment	30
sip-dynamic-hnt	disabled
stop-recurse	401,407
port-map-start	0
port-map-end	0
in-manipulationid	
out-manipulationid	
manipulation-string	
manipulation-pattern	
sip-ims-feature	disabled
subscribe-reg-event	disabled
operator-identifier	
anonymous-priority	none
max-incoming-conns	0
per-src-ip-max-incoming-conns	0
inactive-conn-timeout	0
untrusted-conn-timeout	0
network-id	
ext-policy-server	
default-location-string	
charging-vector-mode	pass
charging-function-address-mode	pass
ccf-address	
ecf-address	
term-tgrp-mode	none
implicit-service-route	disabled
rfc2833-payload	101
rfc2833-mode	transparent

constraint-name	
response-map	
local-response-map	
ims-aka-feature	disabled
enforcement-profile	
route-unauthorized-calls	
tcp-keepalive	none
add-sdp-invite	disabled
add-sdp-profiles	
sip-profile	
sip-isup-profile	
tcp-conn-dereg	0
register-keep-alive	none
kpml-interworking	disabled
tunnel-name	
last-modified-by	admin@10.80.150.50
last-modified-date	2012-06-06 15:06:55

sip-interface

state	enabled
realm-id	core
description	
sip-port	
address	10.64.19.150
port	5060
transport-protocol	TCP
tls-profile	
multi-home-addr	
allow-anonymous	all
ims-aka-profile	

carriers	
trans-expire	0
invite-expire	0
max-redirect-contacts	0
proxy-mode	
redirect-action	
contact-mode	none
nat-traversal	none
nat-interval	30
tcp-nat-interval	90
registration-caching	disabled
min-reg-expire	300
registration-interval	3600
route-to-registrar	disabled
secured-network	disabled
teluri-scheme	disabled
uri-fqdn-domain	
trust-mode	all
max-nat-interval	3600
nat-int-increment	10
nat-test-increment	30
sip-dynamic-hnt	disabled
stop-recurse	401,407
port-map-start	0
port-map-end	0
in-manipulationid	
out-manipulationid	
manipulation-string	
manipulation-pattern	
sip-ims-feature	disabled
subscribe-reg-event	disabled
operator-identifier	
anonymous-priority	none
max-incoming-conns	0
per-src-ip-max-incoming-conns	0
inactive-conn-timeout	0
untrusted-conn-timeout	0
network-id	
ext-policy-server	
default-location-string	
charging-vector-mode	pass

```

charging-function-address-mode pass
ccf-address
ecf-address
term-tgrp-mode           none
implicit-service-route    disabled
rfc2833-payload           101
rfc2833-mode              transparent
constraint-name
response-map
local-response-map
ims-aka-feature           disabled
enforcement-profile
route-unauthorized-calls
tcp-keepalive             none
add-sdp-invite            disabled
add-sdp-profiles
sip-profile
sip-isup-profile
tcp-conn-dereg           0
register-keep-alive       none
kpml-interworking         disabled
tunnel-name
last-modified-by          admin@10.80.150.50
last-modified-date        2012-06-18 10:34:11
sip-manipulation
  name                     NatIP
  description
  split-headers
  join-headers
  header-rule
    name                   natFROM
    header-name            From
    action                 manipulate
    comparison-type        case-sensitive
    msg-type               request
    methods
    match-value
    new-value
    element-rule
      name                 natHost
      parameter-name
      type                 uri-host
      action               replace
      match-val-type       any
      comparison-type       case-sensitive
      match-value
      new-value             $LOCAL_IP
  header-rule
    name                   natTO
    header-name            To
    action                 manipulate
    comparison-type        case-sensitive
    msg-type               request
    methods
    match-value
    new-value
    element-rule
      name                 natHost
      parameter-name
      type                 uri-host
      action               replace
      match-val-type       any
      comparison-type       case-sensitive
      match-value
      new-value             $REMOTE_IP
  header-rule
    name                   natPAI
    header-name            P-Asserted-Identity
    action                 manipulate
    comparison-type        case-sensitive

```

msg-type	any
methods	
match-value	
new-value	
element-rule	
name	natHost
parameter-name	
type	uri-host
action	replace
match-val-type	any
comparison-type	case-sensitive
match-value	
new-value	\$LOCAL_IP
header-rule	
name	natRequest
header-name	Request-URI
action	manipulate
comparison-type	case-sensitive
msg-type	request
methods	
match-value	
new-value	
element-rule	
name	natHost
parameter-name	
type	uri-host
action	replace
match-val-type	any
comparison-type	case-sensitive
match-value	
new-value	\$REMOTE_IP
header-rule	
name	natDiversion
header-name	Diversion
action	manipulate
comparison-type	case-sensitive
msg-type	request
methods	
match-value	
new-value	
element-rule	
name	natHost
parameter-name	
type	uri-host
action	replace
match-val-type	any
comparison-type	case-sensitive
match-value	
new-value	\$LOCAL_IP
header-rule	
name	removeHist
header-name	History-Info
action	delete
comparison-type	case-sensitive
msg-type	any
methods	
match-value	
new-value	
header-rule	
name	removeRPI
header-name	Remote-Party-ID
action	delete
comparison-type	case-sensitive
msg-type	any
methods	
match-value	
new-value	
header-rule	
name	removeXNTE164
header-name	X-nt-e164-clid

action comparison-type msg-type methods match-value new-value	delete case-sensitive any
header-rule name header-name action comparison-type msg-type methods match-value new-value element-rule name parameter-name type action match-val-type comparison-type match-value new-value	removeMultiMIME Content-Type manipulate case-sensitive any
ssLinux-7.50.17;base=x2611 type action match-val-type comparison-type match-value new-value	nt_mcdn application/x-nt-mcdn-frag-hex;version- mime delete-element any case-sensitive
element-rule name parameter-name type action match-val-type comparison-type match-value new-value	nt_esn5 application/x-nt-esn5-frag-hex mime delete-element any case-sensitive
element-rule name parameter-name type action match-val-type comparison-type match-value new-value	nt_epid application/x-nt-epid-frag- mime delete-element any case-sensitive
hex;version=ssLinux-7.50.17;base=x2611 type action match-val-type comparison-type match-value new-value	mime delete-element any case-sensitive
last-modified-by last-modified-date	admin@10.80.150.50 2012-06-28 16:56:45
sip-manipulation name description split-headers join-headers header-rule name header-name action comparison-type msg-type methods match-value new-value element-rule name parameter-name type action match-val-type comparison-type match-value new-value	AddDomain FromDomain From manipulate case-sensitive request From uri-host replace any case-sensitive avayalab.com
header-rule	

	name header-name action comparison-type msg-type methods match-value new-value element-rule	PaiDomain P-Asserted-Identity manipulate case-sensitive request
	name parameter-name type action match-val-type comparison-type match-value new-value	Pai uri-host replace any case-sensitive avayalab.com
header-rule	name header-name action comparison-type msg-type methods match-value new-value element-rule	natTO To manipulate case-sensitive request
	name parameter-name type action match-val-type comparison-type match-value new-value	To uri-host replace any case-sensitive \$REMOTE_IP
last-modified-by		admin@10.80.150.50
last-modified-date		2012-06-21 12:09:39
sip-manipulation	name description split-headers join-headers header-rule	CS1K_To_CL CS1K_to_CL
	name header-name action comparison-type msg-type methods match-value new-value element-rule	PAIRegex P-Asserted-Identity store pattern-rule any INVITE
	name parameter-name type action match-val-type comparison-type match-value new-value	chkUser header-value store any pattern-rule (.*) (30355571) (.*)
header-rule	name header-name action comparison-type msg-type methods match-value new-value element-rule	HistRegex History-Info store pattern-rule any

name parameter-name type action match-val-type comparison-type match-value new-value	GetReason1 header-value store any pattern-rule (.*) (reason) (.)
element-rule name parameter-name type action match-val-type comparison-type match-value new-value	GetReason2 header-value none any pattern-rule (.*) (Moved) (.)
element-rule name parameter-name type action match-val-type comparison-type match-value new-value	GetReason3 header-value none any pattern-rule (.*) (Busy) (.)
element-rule name parameter-name type action match-val-type comparison-type match-value new-value	GetReason4 header-value none any pattern-rule (.*) (Unavailable) (.)
element-rule name parameter-name type action match-val-type comparison-type match-value new-value	GetUser uri-user store any pattern-rule
element-rule name parameter-name type action match-val-type comparison-type match-value new-value	GetHost uri-host store any pattern-rule
header-rule name header-name action comparison-type msg-type methods match-value new-value	AddDiversion1 Diversion add boolean request INVITE (!\$PAIRRegex[0] . \$chkUser) & !\$HistRegex[0] . \$GetReason1 "<sip:3035557104@avayalab.com;user=phone>"
header-rule name header-name action comparison-type msg-type methods match-value	AddDiversion2 Diversion add boolean request INVITE \$HistRegex[0] . \$GetReason2

```

new-value
<sip:+$HistRegex[0].$GetUser.$0+@$HistRegex[0].$GetHost.$0+>;privacy=off;reason=unconditional;screen=no
header-rule
    name                AddDiversion3
    header-name          Diversion
    action               add
    comparison-type      boolean
    msg-type             request
    methods              INVITE
    match-value          $HistRegex[0].$GetReason3
    new-value
<sip:+$HistRegex[0].$GetUser.$0+@$HistRegex[0].$GetHost.$0+>;privacy=off;reason=user\busy;screen=no
header-rule
    name                AddDiversion4
    header-name          Diversion
    action               add
    comparison-type      boolean
    msg-type             request
    methods              INVITE
    match-value          $HistRegex[0].$GetReason4
    new-value
<sip:+$HistRegex[0].$GetUser.$0+@$HistRegex[0].$GetHost.$0+>;privacy=off;reason=no\answer;screen=no
    last-modified-by    admin@10.80.150.50
    last-modified-date  2012-06-28 17:37:53
steering-pool
    ip-address          10.2.2.92
    start-port          49152
    end-port            65535
    realm-id            peer
    network-interface
    last-modified-by    admin@10.80.150.50
    last-modified-date  2012-06-06 15:07:34
steering-pool
    ip-address          10.64.19.150
    start-port          49152
    end-port            65535
    realm-id            core
    network-interface
    last-modified-by    admin@10.80.150.50
    last-modified-date  2012-06-06 15:08:02
system-config
    hostname
    description
    location
    mib-system-contact
    mib-system-name
    mib-system-location
    snmp-enabled        enabled
    enable-snmp-auth-traps disabled
    enable-snmp-syslog-notify disabled
    enable-snmp-monitor-traps disabled
    enable-env-monitor-traps disabled
    snmp-syslog-his-table-length 1
    snmp-syslog-level    WARNING
    system-log-level     WARNING
    process-log-level    NOTICE
    process-log-ip-address 0.0.0.0
    process-log-port     0
    collect
        sample-interval 5
        push-interval   15
        boot-state       disabled
        start-time       now
        end-time         never
        red-collect-state disabled
        red-max-trans     1000
        red-sync-start-time 5000

```

```

red-sync-comp-time          1000
push-success-trap-state     disabled
call-trace                  disabled
internal-trace              disabled
log-filter                  all
default-gateway           10.80.150.1
restart                    enabled
exceptions
telnet-timeout              0
console-timeout             0
remote-control              enabled
cli-audit-trail             enabled
link-redundancy-state       disabled
source-routing              disabled
cli-more                   disabled
terminal-height             24
debug-timeout               0
trap-event-lifetime         0
default-v6-gateway          ::
ipv6-signaling-mtu          1500
ipv4-signaling-mtu          1500
cleanup-time-of-day         00:00
snmp-engine-id-suffix
snmp-agent-mode             v1v2
last-modified-by            admin@console
last-modified-date          2011-11-01 10:30:52
task done
ACMESYSTEM#

```

©2012 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.