Avaya Solution & Interoperability Test Lab

Application Notes for Configuring Acme Packet Net-Net 4500 Session Director with Direct SIP Trunking to Avaya Communication Manager - Issue 1.0

Abstract

These Application Notes describe the procedures for configuring the Acme Packet Net-Net 4500 Session Director with direct SIP trunking to Avaya Communication Manager.

The Acme Packet Net-Net 4500 Session Director is a SIP security appliance that manages and protects the flow of SIP signaling and related media across an untrusted network. The compliance testing focused on telephony scenarios between two enterprise sites connected via SIP trunks across an untrusted network.

Information in these Application Notes has been obtained through DevConnect compliance testing and additional technical discussions. Testing was conducted via the DevConnect Program at the Avaya Solution and Interoperability Test Lab.

1. Introduction

These Application Notes describe the procedures for configuring the Acme Packet Net-Net 4500 Session Director (SD4500) with direct SIP trunking interface from this device to Avaya Communication Manager.

The Acme Packet Net-Net 4500 Session Director is a SIP security appliance that manages and protects the flow of SIP signaling and related media across an untrusted network. The compliance testing focused on telephony scenarios between two enterprise sites connected via SIP trunks across an untrusted network.

1.1. Interoperability Compliance Testing

The compliance testing tested interoperability between the Acme Packet Net-Net 4500 Session Director 6.1 and Avaya Communication Manager 5.1 by making calls between two sites that were connected through the Acme Packet SD4500 using direct SIP trunks. The following functions and features were tested in the compliance test:

- Calls from both SIP and non-SIP endpoints between sites.
- G.711u and G.729A codec support.
- Proper recognition of DTMF transmissions by navigating voicemail menus.
- Proper operation of voicemail with message waiting indicators (MWI).
- PBX features including Multiple Call Appearances, Hold, Transfer, and Conference.
- Extended telephony features using Avaya Communication Manager Feature Name Extensions (FNE) such as Call Forwarding, Conference On Answer, Call Park, Call Pickup, Automatic Redial and Send All Calls.
- Failover on the Acme Packet SD4500 redundant pair configuration
- Proper system recovery after Acme Packet SD4500 restart and/or reestablishment of broken IP connectivity.

1.2. Support

Technical support for the Net-Net 4500 Session Director can be obtained by contacting Acme Packet at

- Phone: (781) 328-4400
- Email: support@acmepacket.com
- Web: https://support.acmepacket.com

2. Configuration

Figure 1 illustrates the test configuration. The test configuration shows two enterprise sites connected via SIP trunks across an untrusted IP network. Connected to the edge of site 1 is a redundant pair of Acme Packet Net-Net 4500 Session Directors. The public side of both Acme Packet Session Directors is connected to the untrusted network and the private side of each is connected to the trusted corporate LAN. The Acme Packet Session Director pair has a single virtual address on the public side and a single virtual address on the private side which are used to connect to Avaya Communication Manager. The Acme Packet Session Directors could also reside in the demilitarized zone (DMZ) of the enterprise but this configuration was not tested.

All SIP traffic between the sites flows through the Acme Packet Session Directors. In this manner, the Acme Packet Session Directors can protect the infrastructure at site 1 from any SIP-based attacks. The voice communication across the untrusted network uses SIP over TCP and RTP for the media streams. All non-SIP related traffic flowing in or out of the enterprise would bypass the Acme Packet Session Directors and would typically pass through a traditional data firewall at the edge of the enterprise. This connection is not shown in **Figure 1** since **Figure 1** focuses only on the connections necessary to support the inter-site SIP communication.

Located at site 1 on the private side of the Acme Packet Session Director pair is an Avaya SIP Enablement Services (SES) and an Avaya S8300 Server running Avaya Communication Manager in an Avaya G700 Media Gateway. Avaya IA 770 Intuity Audix is also running on the Avaya S8300 Server. Endpoints include Avaya 9600 Series IP Telephones (with SIP firmware), an Avaya 1616 IP Telephone (with H.323 firmware), an Avaya one-X Desktop Edition soft phone, an Avaya 6408D Digital Telephone, and an Avaya 6210 Analog Telephone. An ISDN-PRI trunk connects the media gateway to the PSTN. The PSTN number assigned to the ISDN-PRI trunk at site 1 is mapped to a telephone extension at site 1. There are two Windows PCs on site; one is used as an HTTP server for phones to download configuration information; the other is used to manage the Acme Packet Session Directors.

Located at site 2 on the public side of the Acme Packet Session Director pair is an Avaya SES and an Avaya S8300 Server running Avaya Communication Manager in an Avaya G700 Media Gateway. Avaya IA 770 Intuity Audix is also running on the Avaya S8300 Server. Endpoints include Avaya 9600 Series IP Telephones (with SIP firmware) and an Avaya 1608 IP Telephone (with H.323 firmware). This site also has an HTTP server for downloading phone configurations.

The Avaya 9600 Series IP Telephones (with SIP firmware) located at both sites are registered to the local Avaya SES. Each enterprise site has a separate SIP domain: business.com for site 1 and bigtime.com for site 2. SIP telephones at both sites use the local HTTP server to obtain their configuration files.

In this configuration, a SIP trunk connects the Acme Packet Session Directors directly to Avaya Communication Manager at each site. All calls originating from Avaya Communication Manager at site 1 and destined for site 2 will be routed through the on-site Acme Packet Session Directors and from the Acme Packet Session Directors to the untrusted IP network. Once across the untrusted network, the call is routed to site 2's Avaya Communication Manager. Calls from site 2 to site 1 follow this same path in the reverse order. The Avaya SES is not connected to the Acme Packet Session Directors. The Avaya SES in this configuration only supports the on-site SIP endpoints.

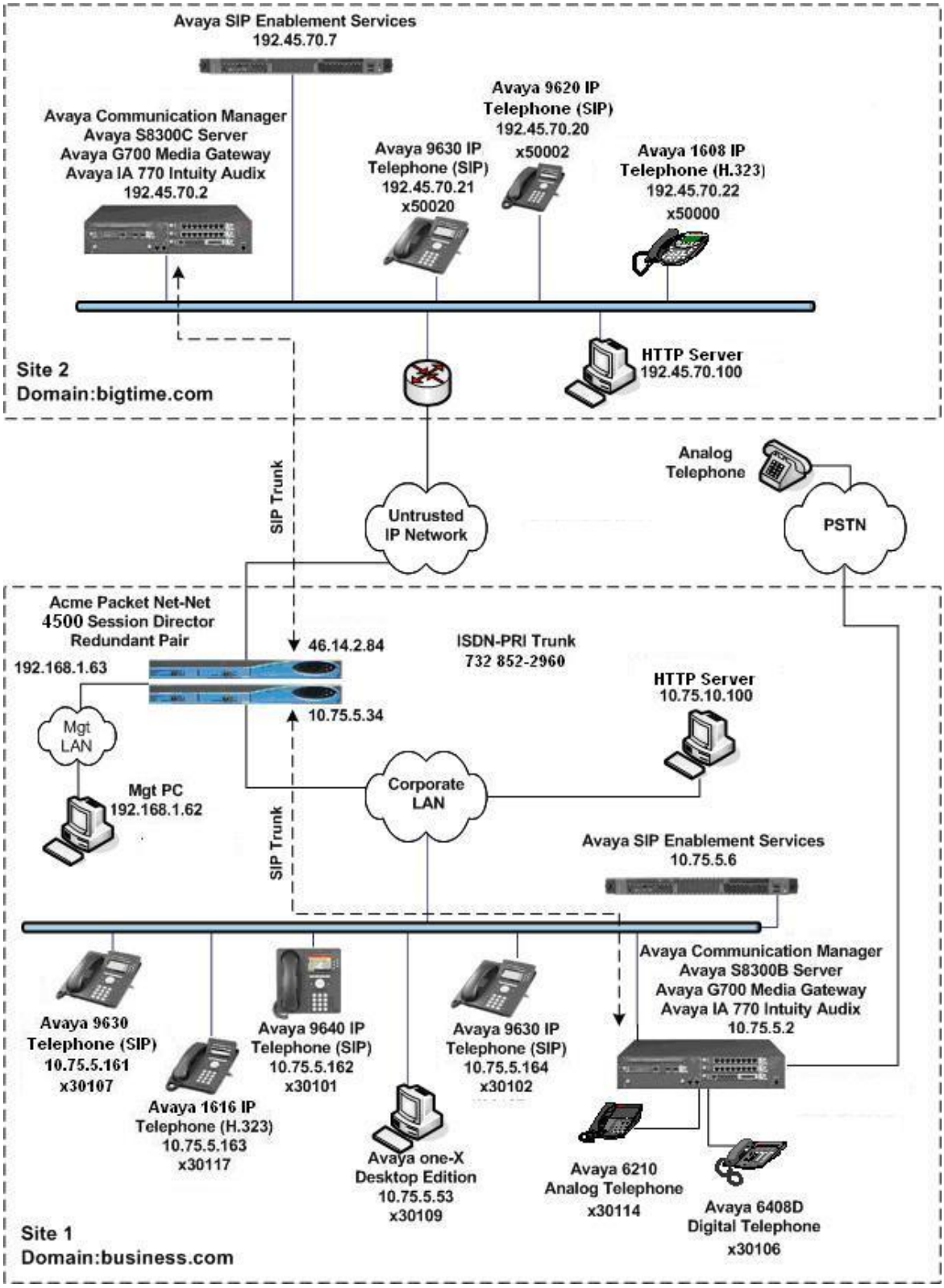

Figure 1: Test Configuration

3. Equipment and Software Validated

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

Equipment	Software/Firmware
Avaya S8300B Server (site 1)	Avaya Communication Manager 5.1.1 with Service Pack (R015x.01.1.415.1-16402) with Avaya IA 770 Intuity Audix
Avaya G700 Media Gateway (site 1)	28.18.0
Avaya S8500B Server (site 1)	Avaya SIP Enablement Services 5.1.1
Avaya S8300C Server (site 2)	Avaya Communication Manager 5.1.1 with Service Pack (R015x.01.1.415.1-16402) with Avaya IA 770 Intuity Audix
Avaya G700 Media Gateway (site 2)	28.18.0
Avaya S8500C Server (site 2)	Avaya SIP Enablement Services 5.1.1
Avaya 1608 IP Telephone (H.323) Avaya 1616 IP Telephone (H.323)	Avaya one-X Deskphone Value Edition Release 1.100
Avaya 9620 IP Telephone (SIP) Avaya 9630 IP Telephones (SIP) Avaya 9640 IP Telephones (SIP)	Avaya one-X Deskphone Edition SIP 2.0.5
Avaya one-X Desktop Edition (SIP)	2.1 Service Pack 2
Avaya 6408D Digital Telephone	-
Avaya 6210 Analog Telephone	-
Analog Telephone	-
Windows PC (Management PC)	Windows XP Professional SP2
Windows Servers (HTTP servers)	Windows Server 2003 Standard Edition
Acme Packet Net-Net 4500 Session Director	CX6.1.0 patch 2 (nnSCX610p2)

4. Configure Avaya Communication Manager

This section describes the Avaya Communication Manager configuration to support the network shown in **Figure 1**. It assumes the procedures necessary to support SIP and connectivity to Avaya SES have been performed as described in [3]. It also assumes that an Outboard Proxy SIP (OPS) off-PBX telephone mapping has been configured on Avaya Communication Manager for each SIP endpoint in the configuration as described in [3] and [4].

This section is divided into two parts. **Section 4.1** will summarize the user-defined parameters used in the installation procedures that are important to understanding the solution as a whole. It will not attempt to show the installation procedures in their entirety. It will also describe any deviations from the standard procedures, if any.

Section 4.2 will describe procedures beyond the initial SIP installation procedures that are necessary for interoperating with the Acme Packet Session Director. It will describe the SIP connection used by Avaya Communication Manager to route calls to the Acme Packet Session Director bound for site 2.

The configuration of Avaya Communication Manager was performed using the System Access Terminal (SAT). After the completion of the configuration, perform a **save translation** command to make the changes permanent.

This section shows examples from Avaya Communication Manager at site 1. However, this configuration must be repeated for Avaya Communication Manager at site 2 using values appropriate for site 2 from **Figure 1**. This includes but is not limited to the IP addresses, SIP domain and user extensions.

4.1. Summary of Initial SIP Installation

This section summarizes the applicable user-defined parameters used during the SIP installation procedures.

Step	Description

1.	**IP network region – Site 1**
	The Avaya S8300 Server, Avaya SES and IP (H.323/SIP) endpoints were located in a single IP network region (IP network region 1) using the parameters described below. Use the **display ip-network-region** command to view these settings. The example below shows the values used for the compliance test. The Acme Packet Session Director will be in this same region.
	▪ The **Authoritative Domain** field represents the SIP domain of the enterprise. It was configured to match the domain name configured on Avaya SES. In this configuration, the domain name is ***business.com***. This name appears in the "From" header of SIP messages originating from this IP region.
	▪ A descriptive name was entered for the **Name** field.
	▪ **IP-IP Direct Audio** (shuffling) was enabled to allow audio traffic to be sent directly between IP endpoints without using media resources in the Avaya Media Gateway. This was done for both **Intra-region** and **Inter-region** IP-IP Direct Audio. This is the default setting. Shuffling can be further restricted at the trunk level on the **Signaling Group** form.
	▪ The **Codec Set** field was set to the IP codec set to be used for calls within this IP network region. In this case, IP codec set 1 was selected. If different IP network regions are used for the Avaya S8300 Server and the Avaya SES server, then **Page 3** of each **IP Network Region** form must be used to specify the codec set for inter-region communications.
	▪ The default values were used for all other fields.
	
	`display ip-network-region 1 Page 1 of 19`
	`IP NETWORK REGION`
	`Region: 1`
	`Location: Authoritative Domain: business.com`
	`Name: Default`
	`MEDIA PARAMETERS Intra-region IP-IP Direct Audio: yes`
	`Codec Set: 1 Inter-region IP-IP Direct Audio: yes`
	`UDP Port Min: 2048 IP Audio Hairpinning? n`
	`UDP Port Max: 3329`
	`DIFFSERV/TOS PARAMETERS RTCP Reporting Enabled? y`
	`Call Control PHB Value: 46 RTCP MONITOR SERVER PARAMETERS`
	`Audio PHB Value: 46 Use Default Server Parameters? y`
	`Video PHB Value: 26`
	`802.1P/Q PARAMETERS`
	`Call Control 802.1p Priority: 6`
	`Audio 802.1p Priority: 6`
	`Video 802.1p Priority: 5 AUDIO RESOURCE RESERVATION PARAMETERS`
	`H.323 IP ENDPOINTS RSVP Enabled? n`
	`H.323 Link Bounce Recovery? y`
	`Idle Traffic Interval (sec): 20`
	`Keep-Alive Interval (sec): 5`
	`Keep-Alive Count: 5`

Step	Description

2.	**IP network region – Site 2**
	At site 2, the Avaya S8300 Server, Avaya SES, and IP (H.323/SIP) endpoints were also located in a single IP network region (IP network region 1) using the same parameters as site 1 as shown in **Step 1** with the following exceptions. A unique name was chosen for the **Name** field and the **Authoritative Domain** field was set to ***bigtime.com*** as shown in **Figure 1**.
	
	`change ip-network-region 1 Page 1 of 19`
	`IP NETWORK REGION`
	`Region: 1`
	`Location: **Authoritative Domain: bigtime.com**`
	`**Name: DefRegion**`
	`MEDIA PARAMETERS Intra-region IP-IP Direct Audio: yes`
	`Codec Set: 1 Inter-region IP-IP Direct Audio: yes`
	`UDP Port Min: 2048 IP Audio Hairpinning? n`
	`UDP Port Max: 3329`
	`DIFFSERV/TOS PARAMETERS RTCP Reporting Enabled? y`
	`Call Control PHB Value: 46 RTCP MONITOR SERVER PARAMETERS`
	`Audio PHB Value: 46 Use Default Server Parameters? y`
	`Video PHB Value: 26`
	`802.1P/Q PARAMETERS`
	`Call Control 802.1p Priority: 6`
	`Audio 802.1p Priority: 6`
	`Video 802.1p Priority: 5 AUDIO RESOURCE RESERVATION PARAMETERS`
	`H.323 IP ENDPOINTS RSVP Enabled? n`
	`H.323 Link Bounce Recovery? y`
	`Idle Traffic Interval (sec): 20`
	`Keep-Alive Interval (sec): 5`
	`Keep-Alive Count: 5`

3.	**Codecs**
	IP codec set 1 was used for the compliance test at both sites. Multiple codecs were listed in priority order to allow the codec used by a specific call to be negotiated during call establishment. The list includes the codecs the enterprise wishes to support within the normal trade-off of bandwidth versus voice quality. The example below shows the values used in the compliance test. It should be noted that when testing the use of each individual codec, only the codec under test was included in the list.
	
	`display ip-codec-set 1 Page 1 of 2`
	`IP Codec Set`
	`Codec Set: 1`
	`**Audio Codec / Silence Suppression / Frames Per Pkt / Packet Size(ms)**`
	`1: **G.711MU n 2 20**`
	`2: **G.729A n 2 20**`
	`3:`

4.2. Configure SIP Trunk and Routing to Site 2

To communicate to site 2 from site 1, two SIP trunks with the appropriate call routing must be configured on Avaya Communication Manager. One trunk will be used for outbound traffic to site 2 while the other will be used for inbound traffic. Both of these trunks will connect Avaya Communication Manager to the Acme Packet Session Director.

Similarly at site 2, two trunks will be configured for communication to site 1.

Step	Description

1.	**Node Names**
	Use the **change node-names ip** command to create a node name for the IP address of the Acme Packet Session Director. Enter a descriptive name in the **Name** column and the private side IP address in the **IP address** column. The example below shows the values used for the compliance test at site 1. A similar node-name must be created at site 2 using the public IP address of the Acme Packet Session Director at site 1.
	
	`change node-names ip` `Page 1 of 2`
	`IP NODE NAMES`
	`Name IP Address`
	`AcmeSD 10.75.5.34`
	`SES 10.75.5.6`
	`SESnorth 192.45.70.7`
	`default 0.0.0.0`
	`myaudix 10.75.5.7`
	`procr 10.75.5.2`

Step	Description

2.	**Signaling Group (Outbound)**
	Use the **add signaling-group *n*** command, where ***n*** is the number of an unused signaling group, to create a new signaling group for use by the outbound trunk group. Signaling group 16 was used for the compliance test at site 1. Signaling group 16 was configured using the parameters highlighted below.
	▪ Set the **Group Type** to ***sip***.
	▪ Set the **Transport Method** to the value of ***tcp***. As a result, the **Near-end Listen Port** and **Far-end Listen Port** are automatically set to ***5060.***
	▪ Set the **Near-end Node Name** to ***procr***. This node name maps to the IP address of the Avaya Server. Node names are defined using the **change node-names ip** command (see **Step 1**).
	▪ Set the **Far-end Node Name** to the node name of the Acme Packet Session Director as defined in **Step 1**.
	▪ Set the **Far-end Network Region** to ***1***. This is the IP network region which contains the Acme Packet Session Director.
	▪ For site 1, set the **Far-end Domain** to the private side IP address of the Acme Packet Session Director. This domain is sent in the "To" header of SIP INVITE messages for calls using this signaling group. At site 2, the ***Far-end Domain*** is set to the public IP address of the Acme Packet Session Director at site 1. If the **Enable Layer 3 Test** field is set to ***n***, then Avaya Communication Manager will attempt to ping this IP address to verify that the SIP connection is available. Thus in this case, the Acme Packet Session Director must be configured to response to ping requests (see **Section 5.3**). Alternatively, if the **Enable Layer 3 Test** field is set to ***y***, then Avaya Communication Manager will use SIP OPTIONS messages to verify that the SIP connection is available.
	▪ Set **Direct IP-IP Audio Connections** to ***n*** (see **Section 6.2)**.
	▪ Verify the **DTMF over IP** field is set to the default value of ***rtp-payload***. This value enables Avaya Communication Manager to send DTMF transmissions using RFC 2833.
	▪ Use the default values for all other fields.
	
	`add signaling-group 16 Page 1 of 1`
	`SIGNALING GROUP`
	
	`Group Number: 16 Group Type: sip`
	`Transport Method: tcp`
	
	`Near-end Node Name: procr Far-end Node Name: AcmeSD`
	`Near-end Listen Port: 5060 Far-end Listen Port: 5060`
	`Far-end Network Region: 1`
	`Far-end Domain: 10.75.5.34`
	
	`Bypass If IP Threshold Exceeded? n`
	
	`DTMF over IP: rtp-payload Direct IP-IP Audio Connections? n`
	`IP Audio Hairpinning? n`
	`Enable Layer 3 Test? n`
	`Session Establishment Timer(min): 3 Alternate Route Timer(sec): 6`

Step	Description

3.	**Trunk Group (Outbound)**
	Use the **add trunk-group *n*** command, where ***n*** is the number of an unused trunk group, to create the new outbound trunk group. Trunk group 16 was used for the compliance test at site 1. Trunk group 16 was configured using the parameters highlighted below.
	
	On **Page 1**:
	▪ Set the **Group Type** field to ***sip***.
	▪ Enter a descriptive name for the **Group Name**.
	▪ Enter an available trunk access code (TAC) that is consistent with the existing dial plan in the **TAC** field.
	▪ Set the **Service Type** field to ***tie***.
	▪ Set the **Signaling Group** to the signaling group shown in the previous step.
	▪ The **Number of Members** field contains the number of trunks in the SIP trunk group. It determines how many simultaneous SIP calls can be supported by the configuration. Each SIP call between two SIP endpoints (whether internal or external) requires two SIP trunks for the duration of the call. Thus, a call from a SIP telephone to another SIP telephone will use two SIP trunks. A call between a non-SIP telephone and a SIP telephone will only use one trunk.
	▪ Use the default values for all other fields.
	
	`add trunk-group 16 Page 1 of 21`
	`TRUNK GROUP`
	`Group Number: 16 **Group Type: sip** CDR Reports: y`
	`**Group Name: AcmeSD** COR: 1 TN: 1 **TAC: 116**`
	`Direction: two-way Outgoing Display? n`
	`Dial Access? n Night Service:`
	`Queue Length: 0`
	`**Service Type: tie** Auth Code? n`
	`**Signaling Group: 16**`
	`**Number of Members: 10**`

4.	**Trunk Group (Outbound) - Continued**
	On **Page 2**, set the **Preferred Minimum Session Refresh Interval** to ***600***. A smaller value will not be accepted by the Acme Packet Session Director.
	
	`add trunk-group 16 Page 2 of 21`
	`Group Type: sip`
	`TRUNK PARAMETERS`
	`Unicode Name? y`
	`Redirect On OPTIM Failure: 5000`
	`SCCAN? n Digital Loss Group: 18`
	`**Preferred Minimum Session Refresh Interval(sec): 600**`

Step	Description

5.	**Trunk Group (Outbound) – Continued**
	On **Page 3**:
	▪ Set the **Numbering Format** field to ***public***. This field specifies the format of the calling party number sent to the far-end.
	▪ Use the default values for all other fields.
	
	`add trunk-group 16 Page 3 of 21`
	`TRUNK FEATURES`
	`ACA Assignment? n Measured: none`
	`Maintenance Tests? y`
	
	`Numbering Format: public`
	`UUI Treatment: service-provider`
	
	`Replace Restricted Numbers? n`
	`Replace Unavailable Numbers? n`
	
	`Show ANSWERED BY on Display? y`

6.	**Signaling Group (Inbound)**
	Use the **add signaling-group *n*** command, where ***n*** is the number of an unused signaling group, to create a new signaling group for use by the inbound trunk group. Signaling group 17 was used for the compliance test at site 1. Use the same parameters as the outbound signaling group as shown in **Step 2** with the following exception. Leave the **Far-end Domain** field blank to accept any domain in the "From" header in the SIP INVITE message. Inbound SIP calls will contain the far-end domain in the "From" header.
	
	`add signaling-group 17 Page 1 of 1`
	`SIGNALING GROUP`
	
	`Group Number: 17 Group Type: sip`
	`Transport Method: tcp`
	
	`Near-end Node Name: procr Far-end Node Name: AcmeSD`
	`Near-end Listen Port: 5060 Far-end Listen Port: 5060`
	`Far-end Network Region: 1`
	`Far-end Domain:`
	
	`Bypass If IP Threshold Exceeded? n`
	
	`DTMF over IP: rtp-payload Direct IP-IP Audio Connections? n`
	`IP Audio Hairpinning? n`
	`Enable Layer 3 Test? n`
	`Session Establishment Timer(min): 3 Alternate Route Timer(sec): 6`

Step	Description

7.	**Trunk Group (Inbound)**
	Use the **add trunk-group *n*** command, where ***n*** is the number of an unused trunk group, to create the new inbound trunk group. Trunk group 17 was used for the compliance test at site 1. Trunk group 17 was configured using the same parameters as shown in **Steps 3 - 5** with the following exceptions. Use unique values for the **Group Name** and **TAC** fields. Set the **Signaling Group** field to the signaling group number created in the previous step.
	
	▪ **Group Name**: ***AcmeSD-blank***
	▪ **TAC**: ***117***
	▪ **Signaling Group**: ***17***
	
	`display trunk-group 17 Page 1 of 21`
	`TRUNK GROUP`
	
	`Group Number: 17 Group Type: sip CDR Reports: y`
	`**Group Name: AcmeSD-blank** COR: 1 TN: 1 **TAC: 117**`
	`Direction: two-way Outgoing Display? n`
	`Dial Access? n Night Service:`
	`Queue Length: 0`
	`Service Type: tie Auth Code? n`
	
	`**Signaling Group: 17**`
	`Number of Members: 10`

8.	**Public Unknown Numbering**
	Public unknown numbering defines the calling party number to be sent to the far-end. Use the **change public-unknown-numbering** command to create an entry that will be used by the trunk groups defined in **Step 3** and **7**. In the example shown below for site 1, all calls originating from a 5-digit extension beginning with 3 and routed across any trunk group (**Trk Grp** column is blank) will be sent as a 5-digit calling number. This calling party number is sent to the far-end in the SIP "From" header. At site 2, a similar entry will be created for 5-digit extensions beginning with 5.
	
	`change public-unknown-numbering 0 Page 1 of 2`
	`NUMBERING - PUBLIC/UNKNOWN FORMAT`
	`**Total**`
	`**Ext Ext Trk** CPN **CPN**`
	`**Len Code Grp(s)** Prefix **Len**`
	`Total Administered: 1`
	`**5 3** **5** Maximum Entries: 240`

Step	Description

9.	**Route Pattern**
	Create a route pattern for use by Automatic Alternate Routing (AAR) when routing calls to site 2. Use the **change route-pattern *n*** command, where ***n*** is the number of an unused route pattern. Enter a descriptive name for the **Pattern Name** field. Set the **Grp No** field to the trunk group number created in **Step 3**. Set the Facility Restriction Level (**FRL**) field to a level that allows access to this trunk for all users that require it. The value of ***0*** is the least restrictive level. The default values may be retained for all other fields.
	
	At site 2, create a route pattern in a similar manner for routing calls to site 1.
	
	`change route-pattern 16 Page 1 of 3`
	`Pattern Number: 16 **Pattern Name: Acme SD**`
	`SCCAN? n Secure SIP? n`
	`**Grp No** **FRL** NPA Pfx Hop Toll No. Inserted DCS/ IXC`
	`Mrk Lmt List Del Digits QSIG`
	`Dgts Intw`
	`1: **16** **0** n user`
	`2: n user`
	`3: n user`
	`4: n user`
	`5: n user`
	`6: n user`
	
	`BCC VALUE TSC CA-TSC ITC BCIE Service/Feature PARM No. Numbering LAR`
	`0 1 2 M 4 W Request Dgts Format`
	`Subaddress`
	`1: y y y y y n n rest none`
	`2: y y y y y n n rest none`
	`3: y y y y y n n rest none`
	`4: y y y y y n n rest none`
	`5: y y y y y n n rest none`
	`6: y y y y y n n rest none`

10.	Use the **change aar analysis 5** command to add an entry in the AAR Digit Analysis Table for the dialed string beginning with 50 since all extensions at site 2 begin with 50. In the example shown, numbers that begin with ***50*** and are ***5*** digits long use route pattern ***16***. Route pattern 16 routes calls from site 1 to site 2 via the SIP trunk connected to the Acme Packet Session Director. At site 2, create an AAR entry in a similar manner for routing calls to site 1. In this case, the dialed string will be ***30*** since all the extensions at site 1 begin with 30. The route pattern used will be the route pattern created in **Step 9** for site 2.
	
	`change aar analysis 5 Page 1 of 2`
	`AAR DIGIT ANALYSIS TABLE`
	`Location: all Percent Full: 3`
	
	`**Dialed String** **Total Min** **Max** **Route Pattern** Call Type Node Num ANI Reqd`
	`**50** **5** **5** **16** aar n

5. Configure Acme Packet Net-Net Session Director

This section describes the configuration of the Acme Packet Session Director necessary for interoperability with the Avaya Communication Manager. The Acme Packet Session Director was configured via the Acme Packet Command Line Interface (ACLI). This section assumes the reader is familiar with accessing and configuring the Acme Packet Session Director.

A pictorial view of this configuration is shown in **Figure 2**. It shows the internal components needed for the compliance test. Each of these components is defined in the Acme Packet Session Director configuration file contained in **Appendix A**. However, this configuration file serves multiple purposes and thus not everything in the file (and **Appendix A**) pertains to these Application Notes. Also note that this section does not cover standard Acme Packet Session Director configurations (e.g., redundancy-config, media-manager, etc.) 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 Avaya Communication Manager. These same fields are highlighted in **Appendix A**. The remaining fields are generally the default/standard value used by the Acme Packet Session Director for that field. For additional details on the administration of the Acme Packet Session Director, refer to [8].

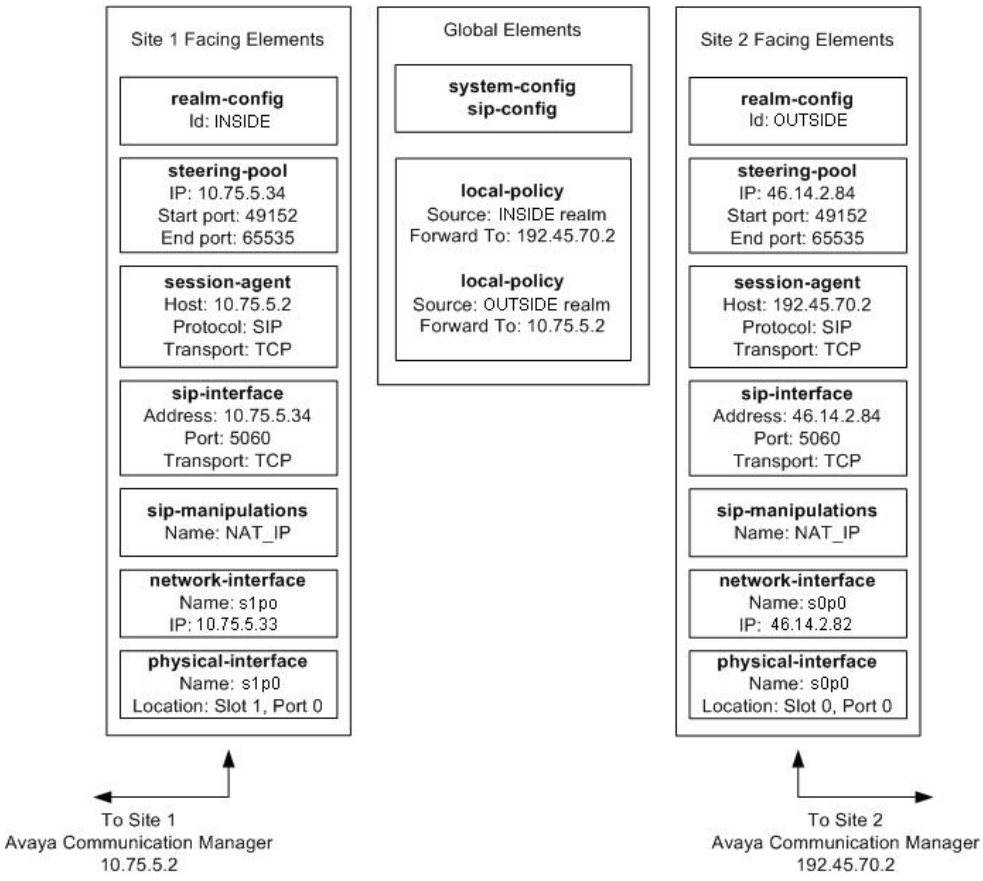

Figure 2: Pictorial View of the Acme Packet Session Director Configuration

5.1. Acme Packet Command Line Interface Summary

The Acme Packet Session Director 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 Session Director using a PC and a terminal emulation program such as HyperTerminal. 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 Session Director 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 s0p0**).
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 is necessary to return to the configuration level.
10. Repeat **Steps 4 - 8** 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.

5.2. System Configuration

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

The key system configuration (***system-config***) field(s) are:

- **default-gateway**: The IP address of the default gateway for the management network (192.168.1.0/24) from **Figure 1**. In this case, the default gateway is ***192.168.1.1***.
- **source-routing**: ***enabled*** for source routing egress HIP packets based on source IP addresses.

```
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                 192.168.1.1
        restart                         enabled
        exceptions
        telnet-timeout                  0
        console-timeout                 0
        remote-control                  enabled
        cli-audit-trail                 enabled
        link-redundancy-state           disabled
        source-routing                  enabled
        cli-more                        disabled
        terminal-height                 24
        debug-timeout                   0

        < text removed for brevity >
```

5.3. Physical and Network Interfaces

As part of the compliance test, the Ethernet interface slot 0 / port 0 of the Acme Packet Session Director 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                            s0p0
        operation-type                  Media
        port                            0
        slot                            0
        virtual-mac                     00:08:25:a0:e2:28
        admin-state                     enabled
        auto-negotiation                enabled
        duplex-mode                     FULL
        speed                           100
        last-modified-by                admin@192.168.1.62
        last-modified-date              2008-11-10 16:19:07
phy-interface
        name                            s1p0
        operation-type                  Media
        port                            0
        slot                            1
        virtual-mac                     00:08:25:a0:e2:29
        admin-state                     enabled
        auto-negotiation                enabled
        duplex-mode                     FULL
        speed                           100
        last-modified-by                admin@192.168.1.62
        last-modified-date              2008-11-10 16:19:41
```

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

- **name**: The name of the physical interface (defined previously) that is associated with this network interface.
- **ip-address**: A virtual IP address assigned to the high availability pair of Acme Packet Session Directors. If multiple virtual addresses are assigned, additional addresses will appear in the **hip-ip-list** below. The particular Acme Packet Session Director used for the compliance test had multiple virtual addresses assigned to it because it was used for multiple purposes. In the compliance test, the virtual IP address 46.14.2.82 was assigned.
- **pri-utility-addr**: The physical address of the primary Acme Packet Session Director in the high availability pair.
- **sec-utility-addr**: The physical address of the secondary Acme Packet Session Director in the high availability pair.
- **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 Session Director 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 Session Director will answer ICMP requests on this interface. In **Section 4.2**, **Step 2**, if the **Enable Layer3 Test** field is set to ***n*** on Avaya Communication Manager, then the IP address used in the **Far-end Domain** field on the same form must be included here in the Acme Packet Session Director network-interface **icmp-address** field. This is because Avaya Communication Manager will periodically ping this address to verify that the SIP connection is available.

```
network-interface
        name                            s0p0
        sub-port-id                     0
        description
        hostname
        ip-address                      46.14.2.82
        pri-utility-addr                46.14.2.80
        sec-utility-addr                46.14.2.81
        netmask                         255.255.255.0
        gateway                         46.14.2.1
        sec-gateway
        gw-heartbeat
                state                           enabled
                heartbeat                       10
                retry-count                     3
                retry-timeout                   1
                health-score                    30
        dns-ip-primary
        dns-ip-backup1
        dns-ip-backup2
        dns-domain
        dns-timeout                     11
        hip-ip-list                     46.14.2.82
                                        46.14.2.84
        ftp-address
        icmp-address                    46.14.2.84
                                        46.14.2.82
        snmp-address
        telnet-address
        last-modified-by                admin@192.168.1.62
        last-modified-date              2008-11-14 11:32:39
```

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

```
network-interface
        name                            s1p0
        sub-port-id                     0
        description
        hostname
        ip-address                      10.75.5.33
        pri-utility-addr                10.75.5.31
        sec-utility-addr                10.75.5.32
        netmask                         255.255.255.0
        gateway                         10.75.5.1
        sec-gateway
        gw-heartbeat
                state                           enabled
                heartbeat                       10
                retry-count                     3
                retry-timeout                   1
                health-score                    30
        dns-ip-primary
        dns-ip-backup1
        dns-ip-backup2
        dns-domain
        dns-timeout                     11
        hip-ip-list                     10.75.5.33
                                        10.75.5.34
        ftp-address
        icmp-address                    10.75.5.34
                                        10.75.5.33
        snmp-address
        telnet-address
        last-modified-by                admin@192.168.1.62
        last-modified-date              2008-11-14 11:33:02
```

5.4. Realm

A realm represents a group of related Acme Packet Session Director components. Two realms were defined for the compliance test. The ***OUTSIDE*** realm was defined for the external network and the ***INSIDE*** 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.
- **out-manipulationid**: ***NAT_IP*** This name refers to a set of sip-manipulations (defined in **Section 5.8**) that are performed on outbound traffic from the Acme Packet Session Director. These sip-manipulations are specified in each realm. Thus, these sip-manipulations are applied to outbound traffic from the public side of the Acme Packet Session Director as well as to outbound traffic from the private side of the Acme Packet Session Director.

```
realm-config
        identifier                      OUTSIDE
        description
        addr-prefix                     0.0.0.0
        network-interfaces
                                        s0p0:0
        mm-in-realm                     disabled
        mm-in-network                   enabled
        mm-same-ip                      enabled
        mm-in-system                    enabled

        < text removed for brevity >

        out-translationid
        in-manipulationid
        out-manipulationid              NAT_IP
        class-profile
        average-rate-limit              0

        < text removed for brevity >

realm-config
        identifier                      INSIDE
        description
        addr-prefix                     0.0.0.0
        network-interfaces
                                        s1p0:0
        mm-in-realm                     disabled
        mm-in-network                   enabled
        mm-same-ip                      enabled
        mm-in-system                    enabled

        < text removed for brevity >

        out-translationid
        in-manipulationid
        out-manipulationid              NAT_IP
        class-profile
        average-rate-limit              0

        < text removed for brevity >
```

5.5. SIP Configuration

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

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

- **home-realm-id**: The name of the realm on the private side of the Acme Packet Session Director.
- **nat-mode**: ***None***
- **registrar-domain**: An asterisk ("*****") is specified to allow any domain.
- **registrar-host**: An asterisk ("*****") is specified to allow any host.
- **registrar-port**: port used for registration.

```
sip-config
        state                           enabled
        operation-mode                  dialog
        dialog-transparency             enabled
        home-realm-id                   INSIDE
        egress-realm-id
        nat-mode                        None
        registrar-domain                *
        registrar-host                  *
        registrar-port                  5060

       < text removed for brevity >
```

5.6. SIP Interface

The SIP interface (***sip-interface***) defines the receiving characteristics of the SIP interfaces on the Acme Packet Session Director. 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 public side, the value of ***agents-only*** is used. Thus, SIP requests will only be accepted from session agents (as defined in **Section 5.7**) on this interface. On the private side, the value of ***all*** is used. Thus, SIP requests will be accepted from anyone on this interface.

```
sip-interface
        state                           enabled
        realm-id                        OUTSIDE
        description
        sip-port
                address                         46.14.2.84
                port                            5060
                transport-protocol              TCP
                tls-profile
                allow-anonymous                 agents-only
        carriers
        trans-expire                    0
        invite-expire                   0

       < text removed for brevity >

sip-interface
        state                           enabled
        realm-id                        INSIDE
        description
        sip-port
                address                         10.75.5.34
                port                            5060
                transport-protocol              TCP
                tls-profile
                allow-anonymous                 all
        carriers
        trans-expire                    0
        invite-expire                   0

       < text removed for brevity >
```

5.7. Session Agent

A session agent defines the characteristics of a signaling peer to the Acme Packet Session Director such as Avaya Communication Manager.

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

- **hostname**: Fully qualified domain name or IP address of this SIP peer.
- **port**: The port used by the peer for SIP traffic.
- **app-protocol**: ***SIP***
- **transport-method**: ***DynamicTCP***
- **realm-id**: The realm id where this peer resides.
- **description**: A descriptive name for the peer.
- **ping-method**: ***OPTIONS;hops=0*** 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 Session Director to set the SIP "Max-Forward" field to 0 in outbound SIP OPTIONS pings generated by the Acme Packet Session Director to this session agent.
- **ping-interval**: Specifies the interval (in seconds) between each ping attempt.

```
session-agent
        hostname                        192.45.70.2
        ip-address
        port                            5060
        state                           enabled
        app-protocol                    SIP
        app-type
        transport-method                DynamicTCP
        realm-id                        OUTSIDE
        egress-realm-id
        description                     OUTSIDE Communications Manager
        carriers
        allow-next-hop-lp               enabled
        constraints                     disabled
        max-sessions                    0

        < text removed for brevity >

        response-map
        ping-method                     OPTIONS;hops=0
        ping-interval                   60
        ping-send-mode                  keep-alive

        < text removed for brevity >
```

The settings for the session agent on the private side are shown below.

```
session-agent
        hostname                        10.75.5.2
        ip-address
        port                            5060
        state                           enabled
        app-protocol                    SIP
        app-type
        transport-method                DynamicTCP
        realm-id                        INSIDE
        egress-realm-id
        description                     Core Communications Manager
        carriers
        allow-next-hop-lp               enabled
        constraints                     disabled
        max-sessions                    0

        < text removed for brevity >

        response-map
        ping-method                     OPTIONS;hops=0
        ping-interval                   60
        ping-send-mode                  keep-alive

        < text removed for brevity >
```

5.8. SIP Manipulation

SIP manipulations are rules used to modify the SIP messages (if necessary) for interoperability. In **Section 5.4**, it was defined that the set of sip-manipulations named NAT_IP would be performed on outbound traffic in each realm.

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**, six modifications (or **header-rules**) were defined. Only four of the six were invoked as part of this compliance test: ***natTo***, ***natHistInfo***, ***storeAlertInfo***, and ***modAlertInfo***. The matching criteria for the other two rules (***natFrom*** and ***natRpIp)*** were never met so they were not invoked. These header manipulations were added to hide the private IP address of the Acme Packet Session Director which appear in the "To", "HistInfo" and "AlertInfo" SIP headers for outbound calls from site 1. This IP address appears in these fields because it is necessary to configure this IP address as the **Far-end Domain** field on the Avaya Communication Manager signaling form (**Section 4.2**, **Step 2**). For each of these fields, the intent of the header rule is to change the private IP address in this field to the actual destination Avaya Communication Manager IP address as the message is forwarded on. This is how the message would have been formatted had the two Avaya Communication Managers had a SIP trunk directly between them without the Acme Packet Session Director in the middle. It is less important to hide the addresses coming from site 2 since the Acme Packet Session Director is only protecting site 1. However for the compliance test, these same rules were applied uniformly to both sides. Thus, these sip-manipulations were configured on each realm.

The example below shows the ***natTo*** header-rule. It specifies that the "To" header in SIP request messages will be manipulated based on the element rule defined. The element rule specifies if the host part of the URI in this header is an IP address, than replace it with the value of $REMOTE_IP. The value of $REMOTE_IP is the IP address of the SIP peer (Avaya Communication Manager) in this realm.

```
sip-manipulation
        name                            NAT_IP
        description

       < text removed for brevity >

        header-rule
                name                            natTo
                header-name                     To
                action                          manipulate
                comparison-type                 case-sensitive
                match-value
                msg-type                        request
                new-value
                methods
                element-rule
                        name                            natToIp
                        parameter-name
                        type                            uri-host
                        action                          replace
                        match-val-type                  ip
                        comparison-type                 case-sensitive
                        match-value
                        new-value                       $REMOTE_IP

        < text removed for brevity >
```

The ***natHistInfo*** rule performs the same operation for the "HistInfo" SIP header. Lastly, due to the more complicated format of the "AlertInfo" SIP header, two rules ***storeAlertInfo***, and ***modAlertInfo*** were defined to perform this same translation for the **AlertInfo** SIP header. For the complete configuration of these rules refer to **Appendix A**.

5.9. 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 Session Director.
- **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                      46.14.2.84
        start-port                      49152
        end-port                        65535
        realm-id                        OUTSIDE
        network-interface
        last-modified-by                admin@192.168.1.62
        last-modified-date              2008-11-14 09:54:34
steering-pool
        ip-address                      10.75.5.34
        start-port                      49152
        end-port                        65535
        realm-id                        INSIDE
        network-interface
        last-modified-by                admin@192.168.1.62
        last-modified-date              2008-11-14 09:55:01
```

5.10. 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 ***OUTSIDE*** realm are to be sent to the ***INSIDE*** realm via IP address 10.75.5.2 (Avaya Communication Manager at the enterprise). The second policy indicates that messages originating from the ***INSIDE*** realm are to be sent to the ***OUTSIDE*** realm via IP address 192.45.70.2.

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

        < text removed for brevity >

        policy-attribute
                next-hop                        10.75.5.2
                realm                           INSIDE
                action                          none

                < text removed for brevity >

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

        < text removed for brevity >

        policy-attribute
                next-hop                        192.45.70.2
                realm                           OUTSIDE
                action                          none

                < text removed for brevity >
```

The settings for the second local-policy are shown below.

```
local-policy
        from-address
                                        *
        to-address
                                        *
        source-realm
                                        INSIDE
        description
        activate-time                   N/A
        deactivate-time                 N/A
        state                           enabled
        policy-priority                 none
        last-modified-by                admin@192.168.1.62
        last-modified-date              2008-11-14 10:02:37
        policy-attribute
                next-hop                        192.45.70.2
                realm                           OUTSIDE
                action                          none

                < text removed for brevity >
```

6. Interoperability Compliance Testing

This section describes the compliance testing used to verify the interoperability of the Acme Packet Net-Net 4500 Session Director with direct SIP trunking to Avaya Communication Manager. This section covers the general test approach and the test results.

6.1. General Test Approach

The general test approach was to make calls between the two sites using various codec settings and exercising common PBX features.

6.2. Test Results

The Acme Packet Session Director passed compliance testing. The following features and functionality were verified. Any observations made during the compliance test are noted at the end of this section.

- Calls from both SIP and non-SIP endpoints between sites.
- G.711u and G.729A codec support.
- Proper recognition of DTMF transmissions by navigating voicemail menus.
- Proper operation of voicemail with message waiting indicators (MWI).
- PBX features including Multiple Call Appearances, Hold, Transfer, and Conference.
- Extended telephony features using Avaya Communication Manager Feature Name Extensions (FNE) such as Call Forwarding, Conference On Answer, Call Park, Call Pickup, and Automatic Redial. For more information on FNEs, please refer to [4].
- Proper system failover after the active Acme Packet Session Director shuts down or loses IP connectivity.
- Proper system recovery after both Acme Packet Session Directors are restarted or broken IP connectivity is reestablished.

The following was observed during compliance testing:

- Inter-site calls between SIP endpoints drop after approximately three and half minutes, unless Media Shuffle is disabled on the SIP trunk to the Acme Packet Session Director. Shuffling may be enabled if support for this call flow is not required.

7. Verification Steps

The following steps may be used to verify the configuration:

- From the Avaya Communication Manager SAT, use the **status signaling-group** command to verify that the SIP signaling group is in-service.
- From the Avaya Communication Manager SAT, use the **status trunk-group** command to verify that the SIP trunk group is in-service.
- From the Avaya SES web administration interface, verify that all endpoints are registered with the local Avaya SES. To view, navigate to **Users→Registered Users**.
- Verify that calls can be placed from both SIP and non-SIP endpoints between sites.
- From the Avaya Communication Manager SAT, use the **list trace tac** command to verify that the calls between sites are routed through the configured SIP trunks.

8. Conclusion

The Acme Packet Net-Net 4500 Session Director passed compliance testing. These Application Notes describe the procedures required to configure the Acme Packet Net-Net 4500 Session Director to interoperate with direct SIP trunks to Avaya Communication Manager as shown in **Figure 1**.

9. Additional References

[1] *Feature Description and Implementation For Avaya Communication Manager*, Doc # 555-245-205, Issue 6.0, January 2008.

[2] *Administrator Guide for Avaya Communication Manager*, Doc # 03-300509, Issue 4, January 2008.

[3] *SIP support in Avaya Communication Manager Running on the Avaya S8xxx Servers*, Doc # 555-245-206, Issue 8, January 2008.

[4] *Avaya Extension to Cellular and Off-PBX Station (OPS) Installation and Administration Guide Release 3.0*, version 6.0, Doc # 210-100-500, Issue 9, June 2005.

[5] *Installing, Administering, Maintaining, and Troubleshooting SIP Enablement Services R5.1*, Doc# 03-600768, Issue 6, June 2008.

[6] *Avaya IA 770 INTUITY AUDIX Messaging Application*, Doc # 11-300532, May 2005.

[7] *Net-Net Session Director Installation Guide*, Acme Packet Documentation Set.

[8] *Net-Net Net-Net 4000 ACLI Configuration Guide, Release Version S-C6.1.0*, Acme Packet Documentation Set.

[9] *Net-Net 4000 ACLI Reference Guide, Release Version S-C6.1.0*, Acme Packet Documentation Set.

Product documentation for Avaya products may be found at http://support.avaya.com.
Product documentation for the Session Director can be obtained from Acme Packet's support web site (https://support.acmepacket.com).

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.

Appendix A: Acme Packet Session Director Configuration File

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

```
acmesbc-pri# show running
local-policy
        from-address                            *
        to-address                              *
        source-realm                            OUTSIDE
        description
        activate-time                   N/A
        deactivate-time                 N/A
        state                           enabled
        policy-priority                 none
        last-modified-by                admin@192.168.1.62
        last-modified-date              2008-11-14 10:02:03
        policy-attribute
                next-hop                        10.75.5.2
                realm                           INSIDE
                action                          none
                terminate-recursion             disabled
                carrier
                start-time                      0000
                end-time                        2400
                days-of-week                    U-S
                cost                            0
                app-protocol
                state                           enabled
                methods
                media-profiles
local-policy
        from-address                            *
        to-address                              *
        source-realm                            INSIDE
        description
        activate-time                   N/A
        deactivate-time                 N/A
        state                           enabled
        policy-priority                 none
        last-modified-by                admin@192.168.1.62
        last-modified-date              2008-11-14 10:02:37
        policy-attribute
                next-hop                        192.45.70.2
                realm                           OUTSIDE
                action                          none
                terminate-recursion             disabled
                carrier
                start-time                      0000
                end-time                        2400
                days-of-week                    U-S
                cost                            0
                app-protocol
                state                           enabled
                methods
                media-profiles
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
        min-media-allocation           32000
        min-trusted-allocation         1000
        deny-allocation                1000
        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
        dnsalg-server-failover         disabled
        last-modified-by               admin@192.168.1.62
        last-modified-date             2008-11-12 09:24:49
network-interface
        name                           wancom1
        sub-port-id                    0
        description
        hostname
        ip-address
        pri-utility-addr               169.254.1.1
        sec-utility-addr               169.254.1.2
        netmask                        255.255.255.252
        gateway
        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
        ftp-address
        icmp-address
        snmp-address
        telnet-address
        last-modified-by               admin@192.168.1.62
        last-modified-date             2008-11-14 11:13:23
network-interface
        name                           wancom2
        sub-port-id                    0
        description
        hostname
        ip-address
        pri-utility-addr               169.254.2.1
        sec-utility-addr               169.254.2.2
        netmask                        255.255.255.252
        gateway
        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
        ftp-address
        icmp-address
        snmp-address
        telnet-address
        last-modified-by                admin
        last-modified-date              2008-11-10 16:01:19
network-interface
        name                            s0p0
        sub-port-id                     0
        description
        hostname
        ip-address                      46.14.2.82
        pri-utility-addr                46.14.2.80
        sec-utility-addr                46.14.2.81
        netmask                         255.255.255.0
        gateway                         46.14.2.1
        sec-gateway
        gw-heartbeat
                state                           enabled
                heartbeat                       10
                retry-count                     3
                retry-timeout                   1
                health-score                    30
        dns-ip-primary
        dns-ip-backup1
        dns-ip-backup2
        dns-domain
        dns-timeout                     11
        hip-ip-list                     46.14.2.82
                                        46.14.2.84
        ftp-address
        icmp-address                    46.14.2.84
                                        46.14.2.82
        snmp-address
        telnet-address
        last-modified-by                admin@192.168.1.62
        last-modified-date              2008-11-14 11:32:39
network-interface
        name                            s1p0
        sub-port-id                     0
        description
        hostname
        ip-address                      10.75.5.33
        pri-utility-addr                10.75.5.31
        sec-utility-addr                10.75.5.32
        netmask                         255.255.255.0
        gateway                         10.75.5.1
        sec-gateway
        gw-heartbeat
                state                           enabled
                heartbeat                       10
                retry-count                     3
                retry-timeout                   1
                health-score                    30
        dns-ip-primary
        dns-ip-backup1
        dns-ip-backup2
        dns-domain
        dns-timeout                     11
        hip-ip-list                     10.75.5.33
```

```
                                    10.75.5.34
        ftp-address
        icmp-address                10.75.5.34
                                    10.75.5.33
        snmp-address
        telnet-address
        last-modified-by            admin@192.168.1.62
        last-modified-date          2008-11-14 11:33:02
phy-interface
        name                        wancom1
        operation-type              Control
        port                        1
        slot                        0
        virtual-mac
        wancom-health-score         8
        last-modified-by            admin
        last-modified-date          2008-11-10 16:01:19
phy-interface
        name                        wancom2
        operation-type              Control
        port                        2
        slot                        0
        virtual-mac
        wancom-health-score         9
        last-modified-by            admin
        last-modified-date          2008-11-10 16:01:19
phy-interface
        name                        s0p0
        operation-type              Media
        port                        0
        slot                        0
        virtual-mac                 00:08:25:a0:e2:28
        admin-state                 enabled
        auto-negotiation            enabled
        duplex-mode                 FULL
        speed                       100
        last-modified-by            admin@192.168.1.62
        last-modified-date          2008-11-10 16:19:07
phy-interface
        name                        s1p0
        operation-type              Media
        port                        0
        slot                        1
        virtual-mac                 00:08:25:a0:e2:29
        admin-state                 enabled
        auto-negotiation            enabled
        duplex-mode                 FULL
        speed                       100
        last-modified-by            admin@192.168.1.62
        last-modified-date          2008-11-10 16:19:41
realm-config
        identifier                  OUTSIDE
        description
        addr-prefix                 0.0.0.0
        network-interfaces
                                    s0p0:0
        mm-in-realm                 disabled
        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
        in-translationid
        out-translationid
        in-manipulationid
        out-manipulationid              NAT_IP
        manipulation-string
        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
        ext-policy-svr
        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
        codec-policy
        codec-manip-in-realm            disabled
        constraint-name
        call-recording-server-id
        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
        last-modified-by                admin@192.168.1.62
        last-modified-date              2008-11-14 09:53:18
realm-config
        identifier                      INSIDE
        description
        addr-prefix                     0.0.0.0
        network-interfaces
                                        s1p0:0
        mm-in-realm                     disabled
        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
```

```
        in-translationid
        out-translationid
        in-manipulationid
        out-manipulationid              NAT_IP
        manipulation-string
        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
        ext-policy-svr
        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
        codec-policy
        codec-manip-in-realm            disabled
        constraint-name
        call-recording-server-id
        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
        last-modified-by                admin@192.168.1.62
        last-modified-date              2008-11-14 09:53:10
redundancy-config
        state                           enabled
        log-level                       INFO
        health-threshold                75
        emergency-threshold             50
        port                            9090
        advertisement-time              500
        percent-drift                   210
        initial-time                    1250
        becoming-standby-time           180000
        becoming-active-time            100
        cfg-port                        1987
        cfg-max-trans                   10000
        cfg-sync-start-time             5000
        cfg-sync-comp-time              1000
        gateway-heartbeat-interval      0
        gateway-heartbeat-retry         0
        gateway-heartbeat-timeout       1
        gateway-heartbeat-health        0
        media-if-peercheck-time         0
        peer
                name                            acmesbc-pri
                state                           enabled
                type                            Primary
                destination
                        address                         169.254.1.1:9090
```

```
                        network-interface              wancom1:0
                destination
                        address                        169.254.2.1:9090
                        network-interface              wancom2:0
        peer
                name                            acmesbc-sec
                state                           enabled
                type                            Secondary
                destination
                        address                        169.254.1.2:9090
                        network-interface              wancom1:0
                destination
                        address                        169.254.2.2:9090
                        network-interface              wancom2:0
        last-modified-by                admin
        last-modified-date              2008-11-10 16:01:19
session-agent
        hostname                        192.45.70.2
        ip-address
        port                            5060
        state                           enabled
        app-protocol                    SIP
        app-type
        transport-method                DynamicTCP
        realm-id                        OUTSIDE
        egress-realm-id
        description                     OUTSIDE Communications Manager
        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=0
        ping-interval                   60
        ping-send-mode                  keep-alive
        ping-in-service-response-codes
        out-service-response-codes
        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
        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
        reuse-connections              NONE
        tcp-keepalive                  none
        tcp-reconn-interval            0
        max-register-burst-rate        0
        register-burst-window          0
        last-modified-by               admin@192.168.1.62
        last-modified-date             2008-11-14 12:20:33
session-agent
        hostname                       10.75.5.2
        ip-address
        port                           5060
        state                          enabled
        app-protocol                   SIP
        app-type
        transport-method               DynamicTCP
        realm-id                       INSIDE
        egress-realm-id
        description                    Core Communications Manager
        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=0
        ping-interval                  60
        ping-send-mode                 keep-alive
        ping-in-service-response-codes
        out-service-response-codes
        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
        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
        reuse-connections               NONE
        tcp-keepalive                   none
        tcp-reconn-interval             0
        max-register-burst-rate         0
        register-burst-window           0
        last-modified-by                admin@192.168.1.62
        last-modified-date              2008-11-14 12:20:40
sip-config
        state                           enabled
        operation-mode                  dialog
        dialog-transparency             enabled
        home-realm-id                   INSIDE
        egress-realm-id
        nat-mode                        None
        registrar-domain                *
        registrar-host                  *
        registrar-port                  5060
        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              enabled
        registration-cache-limit        0
        register-use-to-for-lp          disabled
        add-ucid-header                 disabled
        last-modified-by                admin@192.168.1.100
        last-modified-date              2009-03-18 10:51:33
sip-interface
        state                           enabled
        realm-id                        OUTSIDE
        description
        sip-port
                address                         46.14.2.84
                port                            5060
                transport-protocol              TCP
                tls-profile
                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
        sip-ims-feature               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
        refer-call-transfer           disabled
        route-unauthorized-calls
        tcp-keepalive                 none
        add-sdp-invite                disabled
        add-sdp-profiles
        last-modified-by              admin@192.168.1.62
        last-modified-date            2008-11-14 10:00:12
sip-interface
        state                         enabled
        realm-id                      INSIDE
        description
        sip-port
                address                       10.75.5.34
                port                          5060
                transport-protocol            TCP
                tls-profile
                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
        sip-ims-feature                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
        refer-call-transfer            disabled
        route-unauthorized-calls
        tcp-keepalive                  none
        add-sdp-invite                 disabled
        add-sdp-profiles
        last-modified-by               admin@192.168.1.62
        last-modified-date             2008-11-14 10:00:56
sip-manipulation
        name                           NAT_IP
        description
        header-rule
                name                           natFrom
                header-name                    From
                action                         manipulate
                comparison-type                case-sensitive
                match-value
                msg-type                       request
                new-value
                methods
                element-rule
                        name                           natFromIp
                        parameter-name
                        type                           uri-host
                        action                         replace
                        match-val-type                 ip
                        comparison-type                case-sensitive
                        match-value
                        new-value                      $LOCAL_IP
        header-rule
                name                           natTo
                header-name                    To
                action                         manipulate
                comparison-type                case-sensitive
```

```
                match-value
                msg-type                        request
                new-value
                methods
                element-rule
                        name                            natToIp
                        parameter-name
                        type                            uri-host
                        action                          replace
                        match-val-type                  ip
                        comparison-type                 case-sensitive
                        match-value
                        new-value                       $REMOTE_IP
        header-rule
                name                            natRpid
                header-name                     Remote-Party-ID
                action                          manipulate
                comparison-type                 case-sensitive
                match-value
                msg-type                        request
                new-value
                methods
                element-rule
                        name                            natRpidIp
                        parameter-name
                        type                            uri-host
                        action                          replace
                        match-val-type                  ip
                        comparison-type                 case-sensitive
                        match-value
                        new-value                       $LOCAL_IP
        header-rule
                name                            natHistInfo
                header-name                     History-Info
                action                          manipulate
                comparison-type                 case-sensitive
                match-value
                msg-type                        request
                new-value
                methods
                element-rule
                        name                            natHistInfoIp
                        parameter-name
                        type                            uri-host
                        action                          replace
                        match-val-type                  ip
                        comparison-type                 case-sensitive
                        match-value
                        new-value                       $REMOTE_IP
        header-rule
                name                            storeAlertInfo
                header-name                     Alert-Info
                action                          store
                comparison-type                 pattern-rule
                match-value                     (.+@)([0-9.]+)(.+)
                msg-type                        request
                new-value
                methods
        header-rule
                name                            modAlertInfo
                header-name                     Alert-Info
                action                          manipulate
                comparison-type                 boolean
                match-value                     $storeAlertInfo
                msg-type                        request
                new-value                       $storeAlertInfo.$1+$REMOTE_IP+$storeAlertInfo.$3
                methods
        last-modified-by                admin@192.168.1.100
        last-modified-date              2009-03-17 10:19:19
steering-pool
        ip-address                      46.14.2.84
        start-port                      49152
```

```
        end-port                        65535
        realm-id                        OUTSIDE
        network-interface
        last-modified-by                admin@192.168.1.62
        last-modified-date              2008-11-14 09:54:34
steering-pool
        ip-address                      10.75.5.34
        start-port                      49152
        end-port                        65535
        realm-id                        INSIDE
        network-interface
        last-modified-by                admin@192.168.1.62
        last-modified-date              2008-11-14 09:55:01
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                 192.168.1.1
        restart                         enabled
        exceptions
        telnet-timeout                  0
        console-timeout                 0
        remote-control                  enabled
        cli-audit-trail                 enabled
        link-redundancy-state           disabled
        source-routing                  enabled
        cli-more                        disabled
        terminal-height                 24
        debug-timeout                   0
        trap-event-lifetime             0
        last-modified-by                admin@192.168.1.62
        last-modified-date              2008-11-10 17:46:50
task done
acmesbc-pri#
```