



Avaya Solution & Interoperability Test Lab

Application Notes for Configuring the Acme Packet Net-Net Session Director in an Avaya IP Telephony Environment – Issue 1.0

Abstract

These Application Notes describe the configuration of the Acme Packet Net-Net Session Director in an Avaya IP Telephony environment consisting of an Avaya Converged Communications Server, Avaya Communication Manager, and Avaya 4600 Series IP telephones (SIP and H.323). The Acme Packet Net-Net Session Director is a session border controller that integrates signaling and media control for SIP, H.323 and MGCP. Information in these Application Notes has been obtained through compliance testing and technical discussions. Testing was conducted via the Developer*Connection* Program at the Avaya Solution and Interoperability Test Lab.

1. Introduction

These Application Notes describe the configuration of the Acme Packet Net-Net Session Director in an Avaya IP Telephony environment consisting of an Avaya Converged Communications Server, Avaya Communication Manager, and Avaya IP telephones (SIP and H.323).

The Acme Packet Net-Net Session Director is a session border controller that integrates signaling and media control for SIP, H.323 and MGCP. Session border controllers reside at the service provider's network borders and serve as both the source and destination for all signaling messages and media streams entering or exiting the provider's network. In the configuration shown in **Figure 1**, the customer enterprise site was simulated using an Avaya S8300 Media Server with Avaya G350 Media Gateway. The service provider data center site was simulated using an Avaya S8700 Media Server with Avaya G600 Media Gateway.

The Acme Packet Net-Net Session Director was configured to function in a "peering" configuration with the Avaya Converged Communications Server and Avaya Communication Manager. In a "peering" configuration, the telephones are registered locally and not through the Acme Packet Net-Net Session Director.

The configuration in **Figure 1** was used to verify that the Acme Packet Net-Net Session Director could interoperate with an Avaya IP Telephony infrastructure. One media interface (public) on the Acme Packet Net-Net Session Director was connected to the customer enterprise site and another media interface (private) was connected to the service provider data center site. A SIP trunk was configured between Avaya Communication Manager and the Avaya Converged Communications Server at each site. An H.323 IP trunk was configured between the two sites with H.323 call shuffling disabled. Calls between the two sites were made using both H.323 and SIP protocols.

The administration of the network infrastructure shown in **Figure 1** is not the focus of these Application Notes and will not be described. For administration of the network infrastructure shown in **Figure 1** refer to the appropriate documentation listed in Section 10.

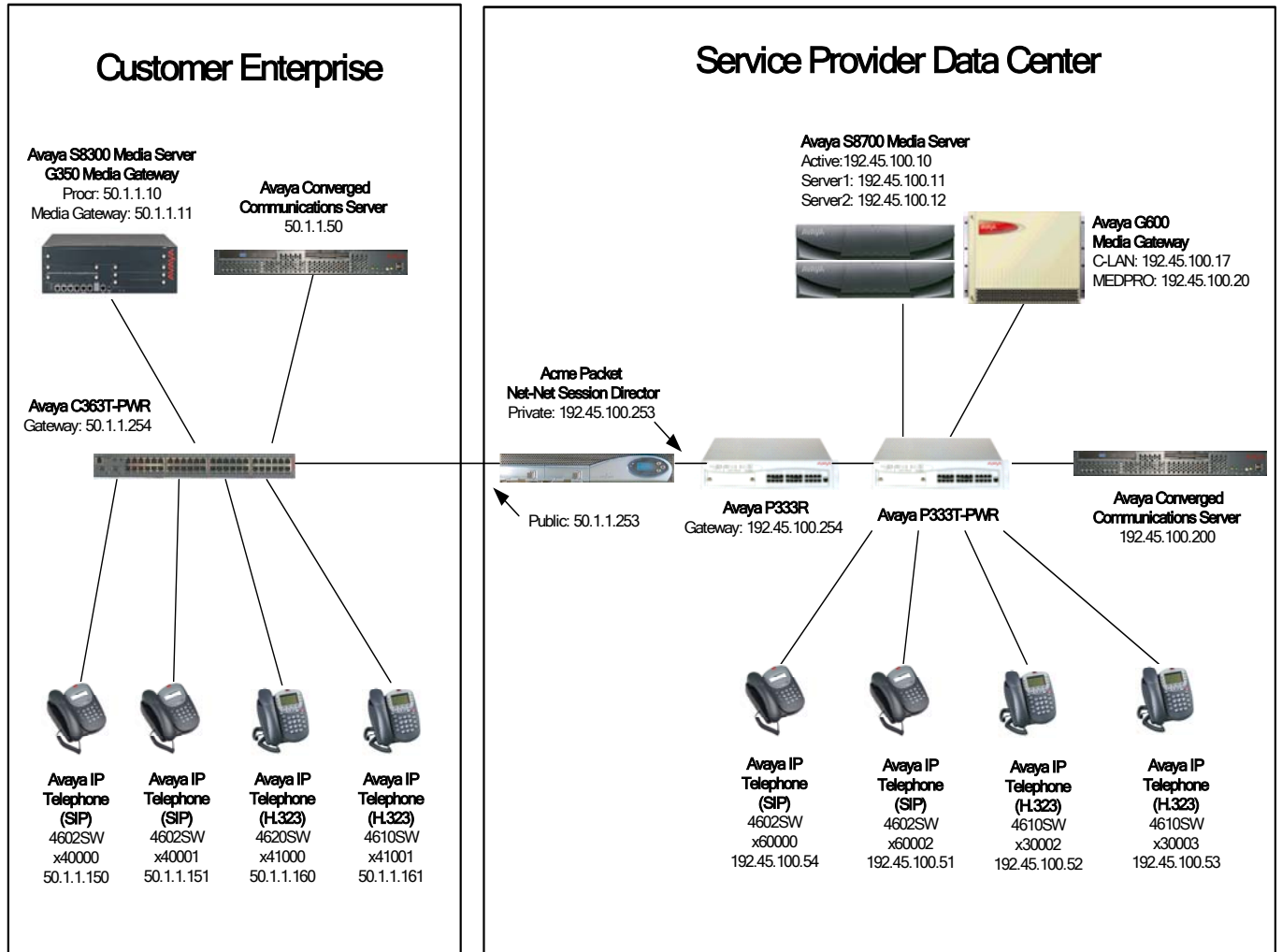


Figure 1 – Network Configuration Diagram

2. Equipment and Software Validated

The following products and software were used for the configuration in **Figure 1**:

Equipment	Version
Avaya Converged Communications Server	2.1.0.0-38
Avaya S8700 Media Server	2.2 (R012x.02.0.111.4)
Avaya G600 Media Gateway IPSI C-LAN Media Processor	HW02 FW009 HW01 FW012 HW03 FW093
Avaya S8300 Media Server	2.2 (R012x.02.0.111.4)
Avaya G350 Media Gateway	23.17.0
Avaya C363T-PWR Converged Stackable Switch	4.3.10
Avaya P333T-PWR Stackable Switch	3.12.1
Avaya P333R Stackable Switch	3.9.1
Avaya 4602SW IP Telephone	1.1 (SIP)
Avaya 4610SW IP Telephone	2.1.3 (H.323)
Avaya 4620SW IP Telephone	2.1.3 (H.323)
Acme Packet Net-Net Session Director	1.3

Table 1 – Equipment and Version

Step	Description
2.	<p>Use the “add signaling-group” command to add a new signaling group for the H.323 IP trunk between the two sites. The <i>Far-end Node Name</i> (e.g., sip-devcon) must match the node name defined in the previous step. The <i>Direct IP-IP Audio Connections</i> field must be set to “n”. Leave the <i>Trunk Group for Channel Selection</i> blank initially until the trunk group for this signaling group has been added in Step 4. Enter the following values:</p> <ul style="list-style-type: none"> • Group Type: h.323. • <i>Near-end Node Name</i>: The node name (e.g., clan-02a03) assigned to the C-LAN of the Avaya G600 Media Gateway. • <i>Far-end Node Name</i>: The node name (e.g., sip-devcon) assigned to the Acme Packet Net-Net Session Director private interface. • <i>Direct IP-IP Audio Connections</i>: n <pre> add signaling-group 200 Page 1 of 5 SIGNALING GROUP Group Number: 200 Group Type: h.323 Remote Office? n Max number of NCA TSC: 0 SBS? n Max number of CA TSC: 0 Trunk Group for NCA TSC: Trunk Group for Channel Selection: Supplementary Service Protocol: a T303 Timer(sec): 10 Near-end Node Name: clan-02a03 Far-end Node Name: sip-devcon Near-end Listen Port: 1720 Far-end Listen Port: 1720 Far-end Network Region: 2 Calls Share IP Signaling Connection? n LRQ Required? n RRQ Required? n Media Encryption? n Bypass If IP Threshold Exceeded? n DTMF over IP: out-of-band Direct IP-IP Audio Connections? n IP Audio Hairpinning? n Interworking Message: PROGRESS </pre>

Step	Description
3.	<p data-bbox="293 233 1503 300">Use the “add trunk-group” command to add a new trunk group for the H.323 IP trunk between the two sites.</p> <pre data-bbox="302 359 1511 999"> add trunk-group 200 Page 1 of 22 TRUNK GROUP Group Number: 200 Group Type: isdn CDR Reports: y Group Name: sipdevcon COR: 1 TN: 1 TAC: 120 Direction: two-way Outgoing Display? n Carrier Medium: IP Dial Access? y Busy Threshold: 255 Night Service: Queue Length: 0 Service Type: tie Auth Code? n TestCall ITC: rest Far End Test Line No: TestCall BCC: 4 TRUNK PARAMETERS Codeset to Send Display: 6 Codeset to Send National IEs: 6 Max Message Size to Send: 260 Charge Advice: none Supplementary Service Protocol: a Digit Handling (in/out): enbloc/enbloc Trunk Hunt: cyclical Digital Loss Group: 18 Incoming Calling Number - Delete: Insert: Format: Bit Rate: 1200 Synchronization: async Duplex: full Disconnect Supervision - In? y Out? n Answer Supervision Timeout: 0 </pre>

Step	Description
4.	<p data-bbox="293 233 1484 338">Go to Page 6 to associate this trunk group with the signaling group created in Step 2. Assign group members to Signaling Group 200. Avaya Communication Manager will replace the initial value of "IP" for the <i>Port</i> field with a unique port (e.g., T00297).</p> <div data-bbox="285 386 1511 1005" style="border: 1px solid black; padding: 5px;"> <pre data-bbox="305 401 1442 961"> add trunk-group 200 TRUNK GROUP Administered Members (min/max): 1/20 GROUP MEMBER ASSIGNMENTS Total Administered Members: 20 Port Code Sfx Name Night Sig Grp 1: T00297 2: T00298 3: T00299 4: T00300 5: T00301 6: T00302 7: T00303 8: T00304 9: T00305 10: T00306 11: T00307 12: T00308 13: T00309 14: T00310 15: T00311 </pre> </div>

Step	Description
5.	<p data-bbox="293 233 1479 302">Use the “change signaling-group” command to enter the <i>Trunk Group for Channel Selection</i> (e.g., 200) defined in the previous step.</p> <pre data-bbox="293 348 1479 1037"> change signaling-group 200 Page 1 of 5 SIGNALING GROUP Group Number: 200 Group Type: h.323 Remote Office? n Max number of NCA TSC: 0 SBS? n Max number of CA TSC: 0 Trunk Group for NCA TSC: Trunk Group for Channel Selection: 200 Supplementary Service Protocol: a T303 Timer(sec): 10 Near-end Node Name: clan-02a03 Far-end Node Name: sip-devcon Near-end Listen Port: 1720 Far-end Listen Port: 1720 Far-end Network Region: 2 LRQ Required? n Calls Share IP Signaling Connection? n RRQ Required? n Media Encryption? n Bypass If IP Threshold Exceeded? n DTMF over IP: out-of-band Direct IP-IP Audio Connections? n IP Audio Hairpinning? n Interworking Message: PROgress </pre>
6.	<p data-bbox="293 1073 1511 1142">Use the “display trunk-group” command to display the SIP trunk group (i.e., Trunk Group 100) between Avaya Communication Manager and the Avaya Converged Communications Server.</p> <pre data-bbox="293 1167 1479 1717"> display trunk-group 100 Page 1 of 22 TRUNK GROUP Group Number: 100 Group Type: sip CDR Reports: y Group Name: CCS: enterprise.com COR: 1 TN: 1 TAC: 100 Direction: two-way Outgoing Display? n Dial Access? n Busy Threshold: 255 Night Service: Queue Length: 0 Service Type: tie Auth Code? n Signaling Group: 100 Number of Members: 48 TRUNK PARAMETERS SCCAN?n Digital Loss Group: 18 </pre>

Step	Description
7.	<p>Change Route Pattern 200 by using the “change route-pattern” command to route calls to the H.323 IP trunk (i.e., Trunk Group 200).</p> <pre data-bbox="289 363 1520 716"> change route-pattern 200 Page 1 of 3 Pattern Number: 200 Pattern Name: sip-devcon SCCAN? n Secure SIP? n Grp FRL NPA Pfx Hop Toll No. Inserted DCS/ IXC No Mrk Lmt List Del Digits QSIG Dgts Intw 1: 200 0 2: 3: 4: 5: 6: n user n user n user n user n user n user </pre>
8.	<p>Add an entry in the AAR analysis table using the “change aar analysis” command so that calls beginning with “41” will use route pattern 200 (i.e., the H.323 IP trunk). An alternative would be to route the calls to the SIP trunk instead of the H.323 IP trunk. In this case, Route Pattern 100 would be used, which was configured to use Trunk Group 100.</p> <pre data-bbox="289 982 1520 1577"> change aar analysis 4 Page 1 of 2 AAR DIGIT ANALYSIS TABLE Percent Full: 1 Dialed Total Route Call Node ANI String Min Max Pattern Type Num Reqd 4 5 5 200 aar n 40 5 5 100 aar n 41 5 5 200 aar n 5 5 5 60 aar n 51 5 5 60 aar n 6 5 5 100 aar n 7 5 5 63 aar n n n n n n n n </pre>

Step	Description
2.	<p>Use the “add signaling-group” command to add a new signaling group for the H.323 IP trunk between the two sites. The <i>Far-end Node Name</i> (e.g., devcon33-2a03) must match the one defined in the previous step. The <i>Direct IP-IP Audio Connections</i> field must be set to “n”. Leave the <i>Trunk Group for Channel Selection</i> blank initially until the trunk group for this signaling group has been added in Step 4. Enter the following values:</p> <ul style="list-style-type: none"> • Group Type: h.323 • <i>Near-end Node Name</i>: The node name (e.g., procr) assigned to the processor interface of the Avaya S8300 Media Server. • <i>Far-end Node Name</i>: The node name (e.g., devcon33-2a03) assigned to the Acme Packet Net-Net Session Director public interface. • <i>Direct IP-IP Audio Connections</i>: n <div data-bbox="302 669 1513 1266" style="border: 1px solid black; padding: 10px; margin-top: 10px;"> <pre> add signaling-group 2 Page 1 of 5 SIGNALING GROUP Group Number: 2 Group Type: h.323 Remote Office? n Max number of NCA TSC: 0 SBS? n Max number of CA TSC: 0 Trunk Group for NCA TSC: Trunk Group for Channel Selection: Supplementary Service Protocol: a T303 Timer(sec): 10 Near-end Node Name: procr Far-end Node Name: devcon33-2a03 Near-end Listen Port: 1720 Far-end Listen Port: 1720 Far-end Network Region: 2 Calls Share IP Signaling Connection? n LRQ Required? n RRQ Required? n Bypass If IP Threshold Exceeded? n DTMF over IP: out-of-band Direct IP-IP Audio Connections? n IP Audio Hairpinning? n Interworking Message: PROGRESS </pre> </div>

Step	Description
3.	<p data-bbox="293 233 1503 300">Use the “add trunk-group” command to add a new trunk group for the H.323 IP trunk between the two sites.</p> <pre data-bbox="293 331 1503 972"> add trunk-group 2 Page 1 of 22 TRUNK GROUP Group Number: 2 Group Type: isdn CDR Reports: y Group Name: devcon33-2a03 COR: 1 TN: 1 TAC: 102 Direction: two-way Outgoing Display? n Carrier Medium: IP Dial Access? y Busy Threshold: 255 Night Service: Queue Length: 0 Service Type: tie Auth Code? n TestCall ITC: rest Far End Test Line No: TestCall BCC: 4 TRUNK PARAMETERS Codeset to Send Display: 6 Codeset to Send National IEs: 6 Max Message Size to Send: 260 Charge Advice: none Supplementary Service Protocol: a Digit Handling (in/out): enbloc/enbloc Trunk Hunt: cyclical Digital Loss Group: 18 Incoming Calling Number - Delete: Insert: Format: Bit Rate: 1200 Synchronization: async Duplex: full Disconnect Supervision - In? y Out? n Answer Supervision Timeout: 0 </pre>
4.	<p data-bbox="293 1037 1503 1146">Go to Page 6 to associate this trunk group with the signaling group created in Step 2. Assign group members to Signaling Group 2. Avaya Communication Manager will replace the initial value of “IP” for the <i>Port</i> field with a unique port (e.g., T00049).</p> <pre data-bbox="293 1178 1503 1787"> change trunk-group 2 Page 6 of 22 TRUNK GROUP Administered Members (min/max): 1/20 GROUP MEMBER ASSIGNMENTS Total Administered Members: 20 Port Code Sfx Name Night Sig Grp 1: T00049 2 2: T00050 2 3: T00051 2 4: T00052 2 5: T00053 2 6: T00054 2 7: T00055 2 8: T00056 2 9: T00057 2 10: T00058 2 11: T00059 2 12: T00060 2 13: T00061 2 14: T00062 2 15: T00063 2 </pre>

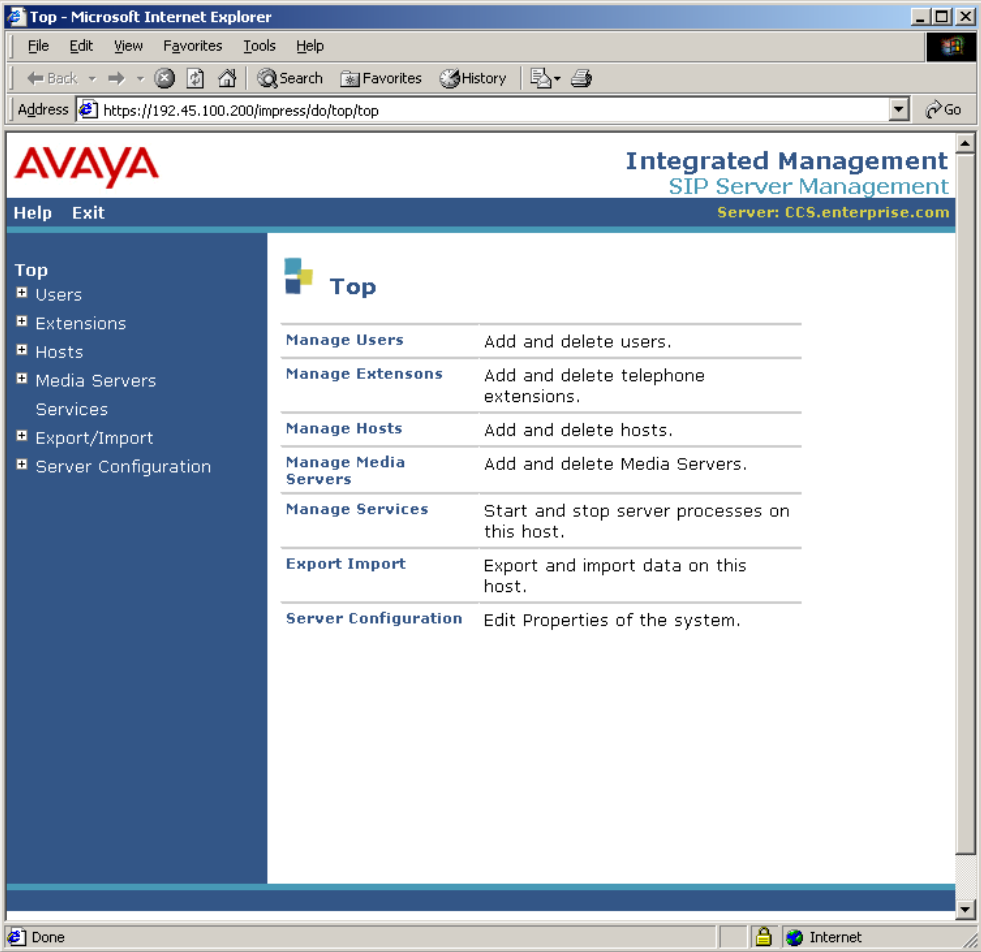
Step	Description
5.	<p data-bbox="293 233 1479 302">Use the “change signaling-group” command to enter the <i>Trunk Group for Channel Selection</i> (e.g., 2) defined in the previous step.</p> <pre data-bbox="302 348 1503 1037"> change signaling-group 2 Page 1 of 5 SIGNALING GROUP Group Number: 2 Group Type: h.323 Remote Office? n Max number of NCA TSC: 0 SBS? n Max number of CA TSC: 0 Trunk Group for NCA TSC: Trunk Group for Channel Selection: 2 Supplementary Service Protocol: a T303 Timer(sec): 10 Near-end Node Name: procr Far-end Node Name: devcon33-2a03 Near-end Listen Port: 1720 Far-end Listen Port: 1720 Far-end Network Region: 2 LRQ Required? n Calls Share IP Signaling Connection? n RRQ Required? n Bypass If IP Threshold Exceeded? n DTMF over IP: out-of-band Direct IP-IP Audio Connections? n IP Audio Hairpinning? n Interworking Message: PROGRESS </pre>
6.	<p data-bbox="293 1073 1479 1142">Use the “display trunk-group” command to display the SIP trunk group (i.e., Trunk Group 1) between Avaya Communication Manager and the Avaya Converged Communications Server.</p> <pre data-bbox="302 1167 1503 1713"> display trunk-group 1 Page 1 of 22 TRUNK GROUP Group Number: 1 Group Type: sip CDR Reports: y Group Name: Avaya CCS COR: 1 TN: 1 TAC: 101 Direction: two-way Outgoing Display? n Dial Access? n Busy Threshold: 255 Night Service: Queue Length: 0 Service Type: tie Auth Code? n Signaling Group: 1 Number of Members: 48 TRUNK PARAMETERS SCCAN?n Digital Loss Group: 18 </pre>

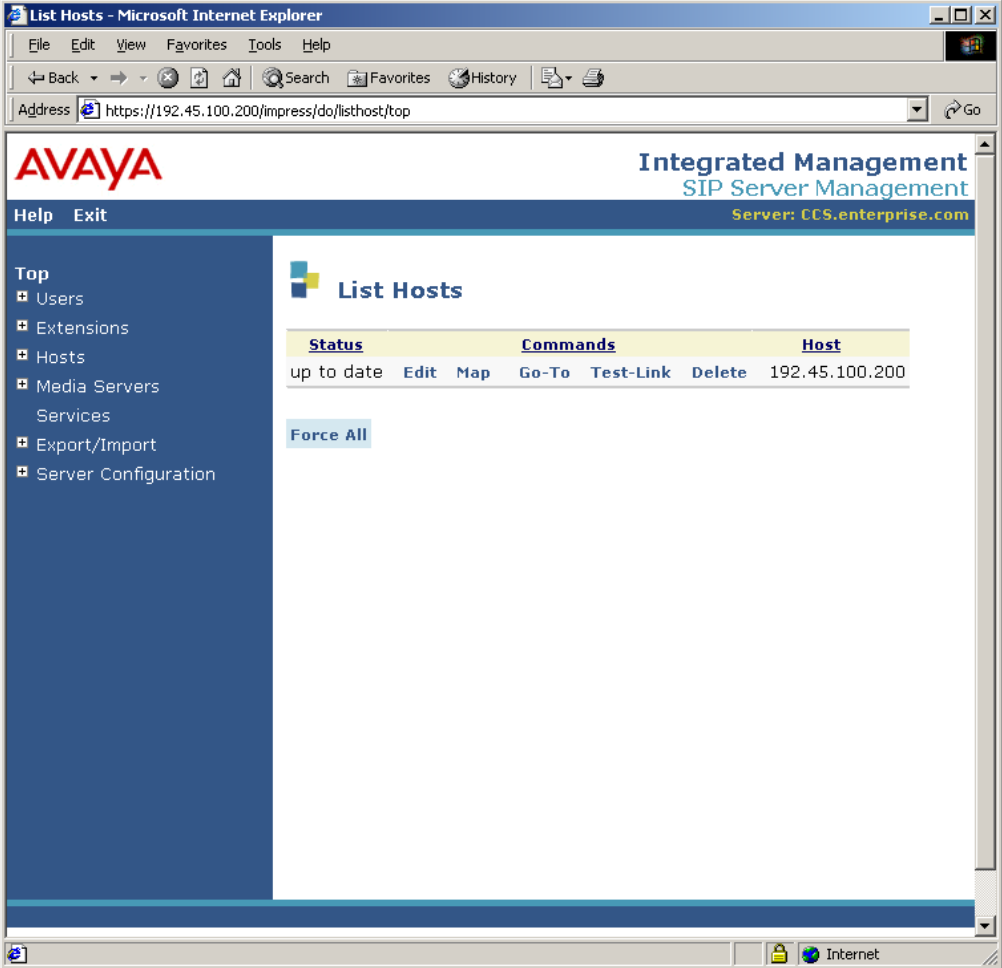
Step	Description
7.	<p data-bbox="293 233 1451 302">Change Route Pattern 3 by using the “change route-pattern” command to route calls to the H.323 IP trunk (i.e., Trunk Group 2).</p> <pre data-bbox="302 359 1511 1052"> change route-pattern 3 Page 1 of 3 Pattern Number: 3 Pattern Name: devcon33-2a03 SCCAN? n Secure SIP? n Grp FRL NPA Pfx Hop Toll No. Inserted DCS/ IXC No Mrk Lmt List Del Digits QSIG Dgts Intw 1: 2 0 2: 3: 4: 5: 6: DCS/ IXC n user n user n user n user n user n user BCC VALUE TSC CA-TSC ITC BCIE Service/Feature BAND No. Numbering LAR 0 1 2 3 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 </pre>

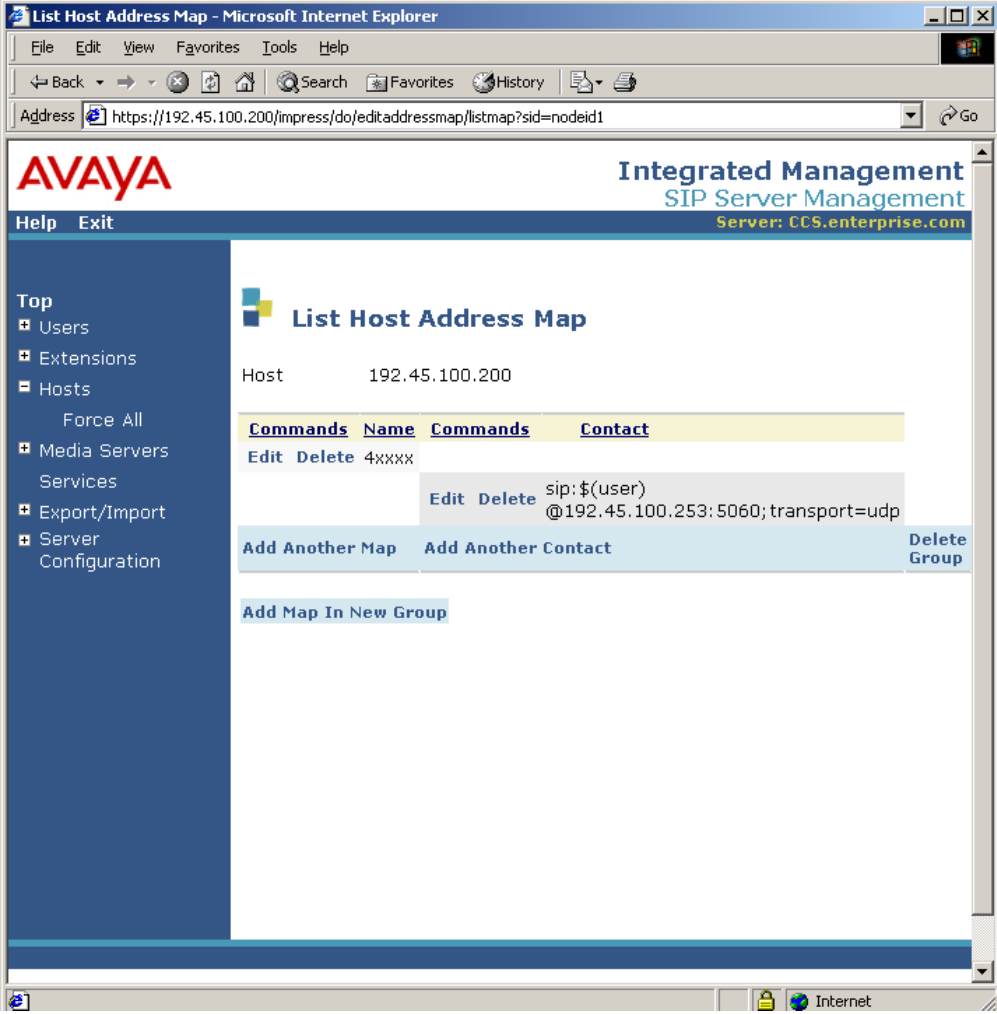
4. Configure Avaya Converged Communications Server

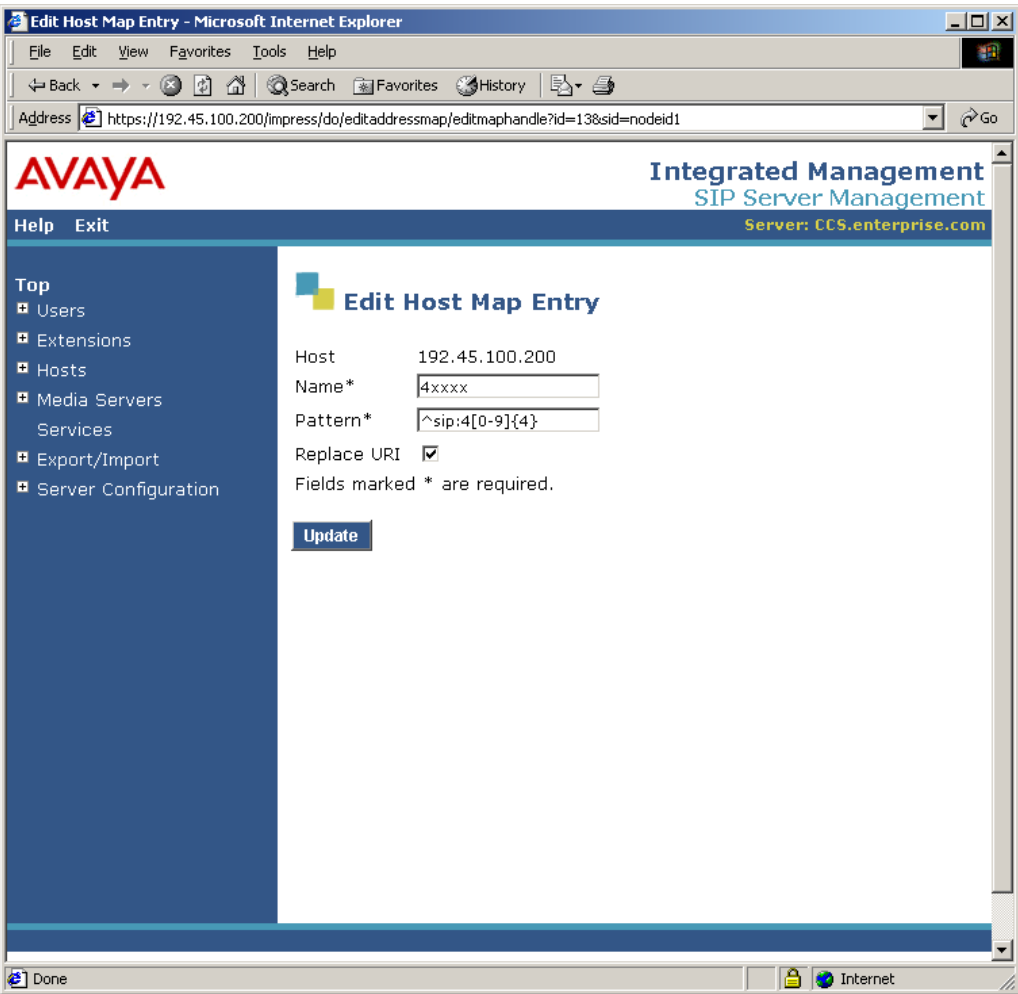
The following steps describe the configuration of the Avaya Converged Communications Server to route calls between the service provider data center site and the customer enterprise site through the Acme Packet Net-Net Session Director. Address maps are used to specify the dial strings to be matched so that the Avaya Converged Communications Server will route the call to the associated contact. The “Edit” instead of the “Add” option was used to show the configuration.

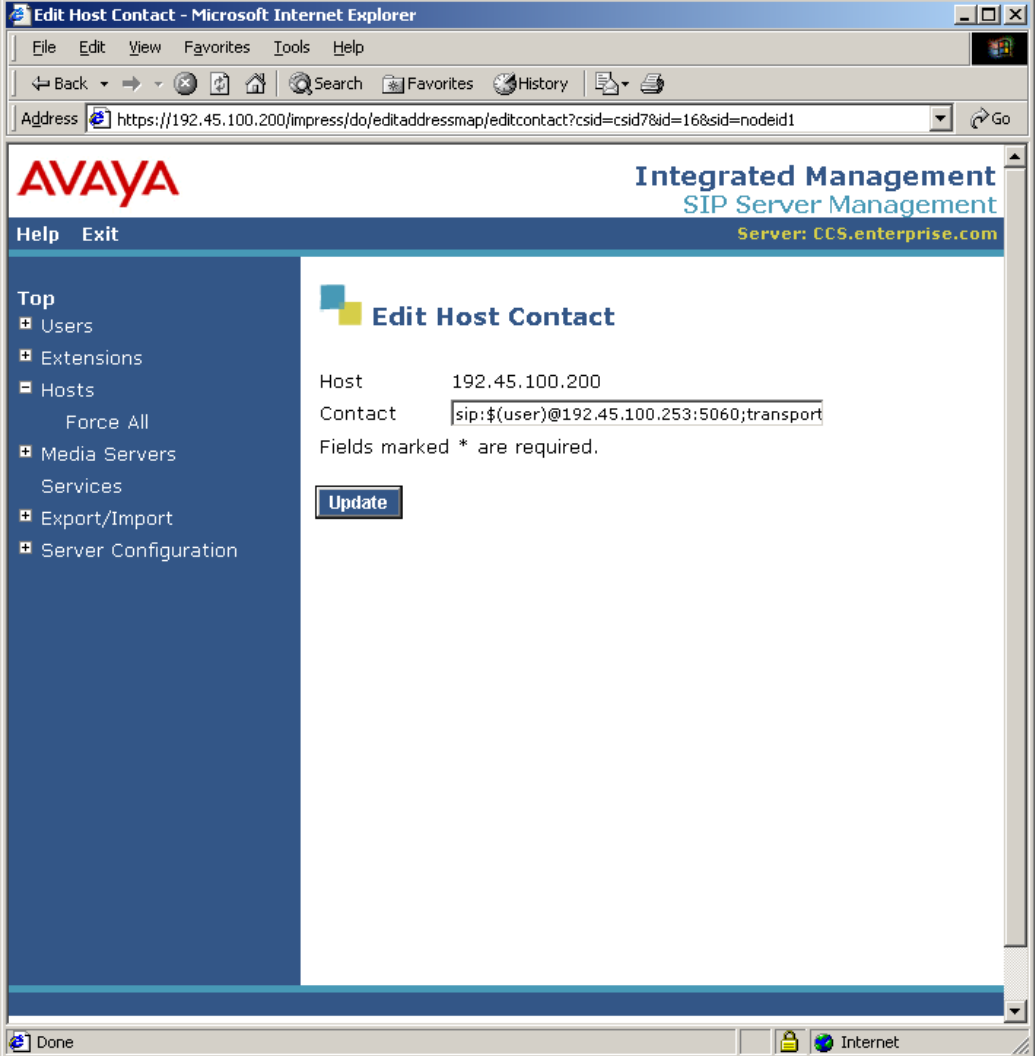
4.1. Service Provider Data Center Site

Step	Description
1.	Log in to the Avaya Converged Communications Server at the service provider data center site using the appropriate credentials.
2.	The <i>Top</i> screen is presented. Click on Hosts on the left pane. 

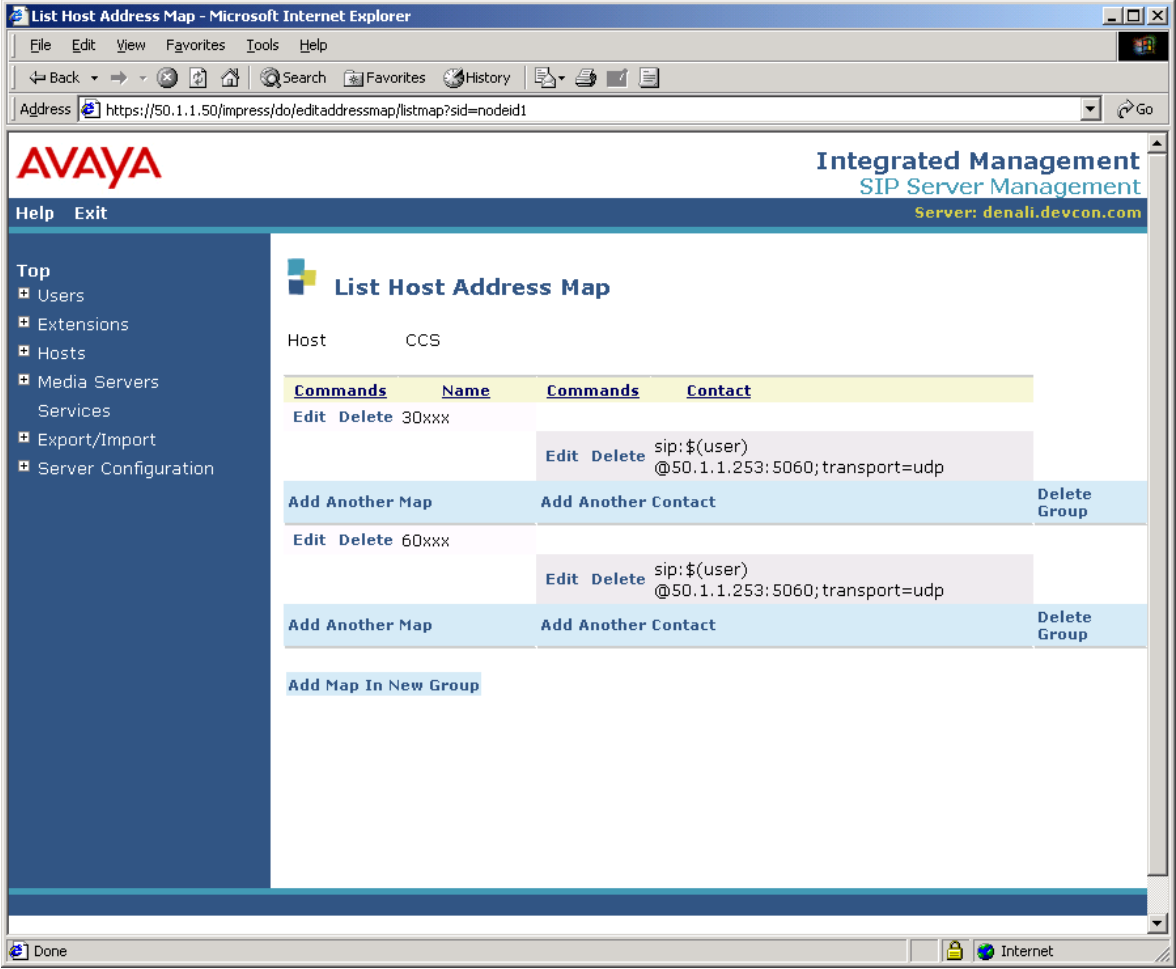
Step	Description						
3.	<p>The <i>List Hosts</i> screen is presented. Click on Map.</p>  <table border="1" data-bbox="690 646 1323 709"> <thead> <tr> <th>Status</th> <th>Commands</th> <th>Host</th> </tr> </thead> <tbody> <tr> <td>up to date</td> <td>Edit Map Go-To Test-Link Delete</td> <td>192.45.100.200</td> </tr> </tbody> </table>	Status	Commands	Host	up to date	Edit Map Go-To Test-Link Delete	192.45.100.200
Status	Commands	Host					
up to date	Edit Map Go-To Test-Link Delete	192.45.100.200					

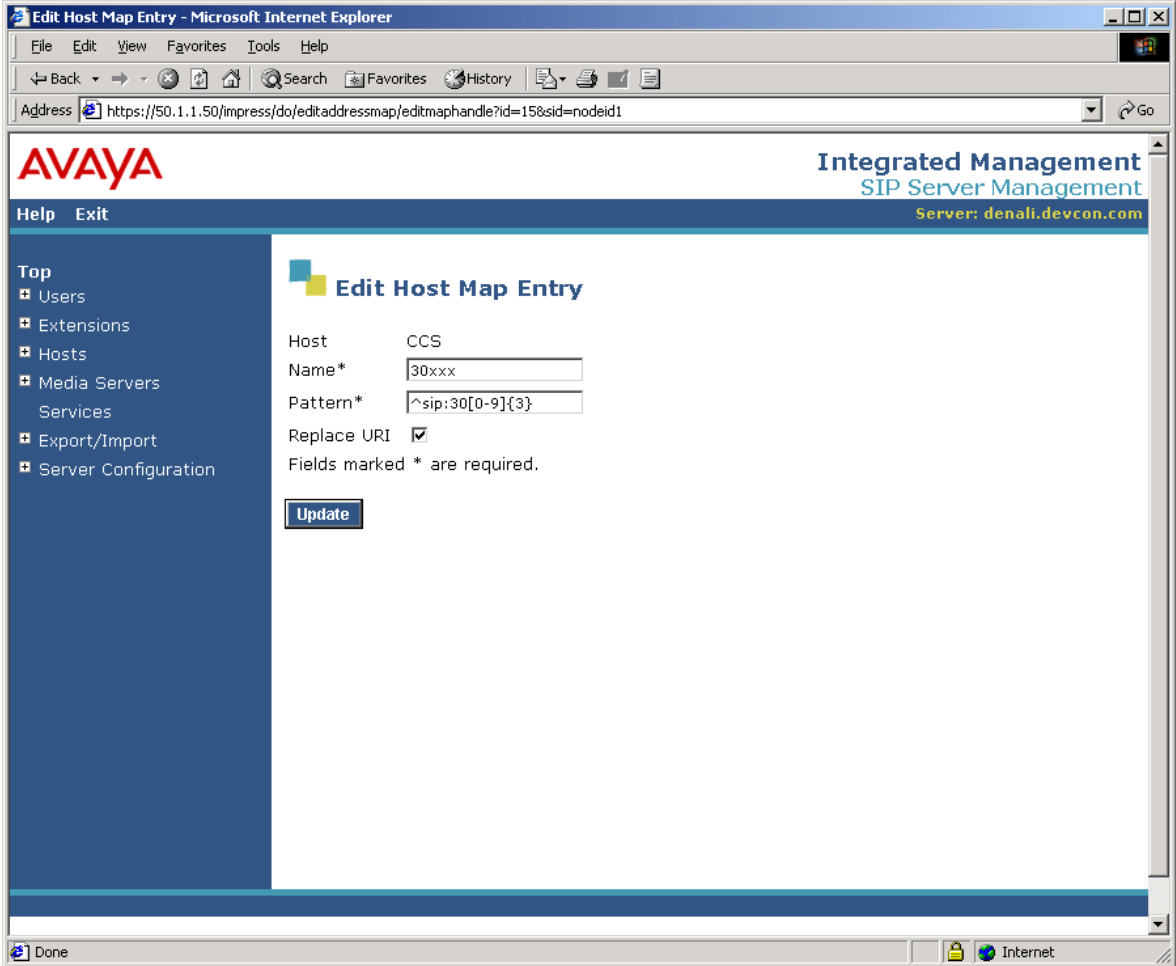
Step	Description												
4.	<p>The <i>List Host Address Map</i> screen displays the address maps and associated contacts. The screen below lists the host map and contact that have already been added and will be described in more detail in Steps 5 and 6. Click on Edit for Host Map 4xxxx.</p>  <p>The screenshot shows a web browser window titled "List Host Address Map - Microsoft Internet Explorer". The address bar shows the URL: <code>https://192.45.100.200/impress/do/editaddressmap/listmap?sid=nodeid1</code>. The page header includes the Avaya logo and "Integrated Management SIP Server Management" with the server name "Server: CCS.enterprise.com". A navigation menu on the left lists options like Users, Extensions, Hosts, Media Servers, etc. The main content area is titled "List Host Address Map" and shows a host with IP "192.45.100.200". Below this is a table with the following data:</p> <table border="1" data-bbox="638 804 1300 961"> <thead> <tr> <th>Commands</th> <th>Name</th> <th>Commands</th> <th>Contact</th> </tr> </thead> <tbody> <tr> <td>Edit Delete</td> <td>4xxxx</td> <td></td> <td></td> </tr> <tr> <td>Edit Delete</td> <td>sip:\$(user) @192.45.100.253:5060;transport=udp</td> <td></td> <td></td> </tr> </tbody> </table> <p>Below the table are buttons for "Add Another Map", "Add Another Contact", and "Delete Group". At the bottom of the main content area, there is a button for "Add Map In New Group".</p>	Commands	Name	Commands	Contact	Edit Delete	4xxxx			Edit Delete	sip:\$(user) @192.45.100.253:5060;transport=udp		
Commands	Name	Commands	Contact										
Edit Delete	4xxxx												
Edit Delete	sip:\$(user) @192.45.100.253:5060;transport=udp												

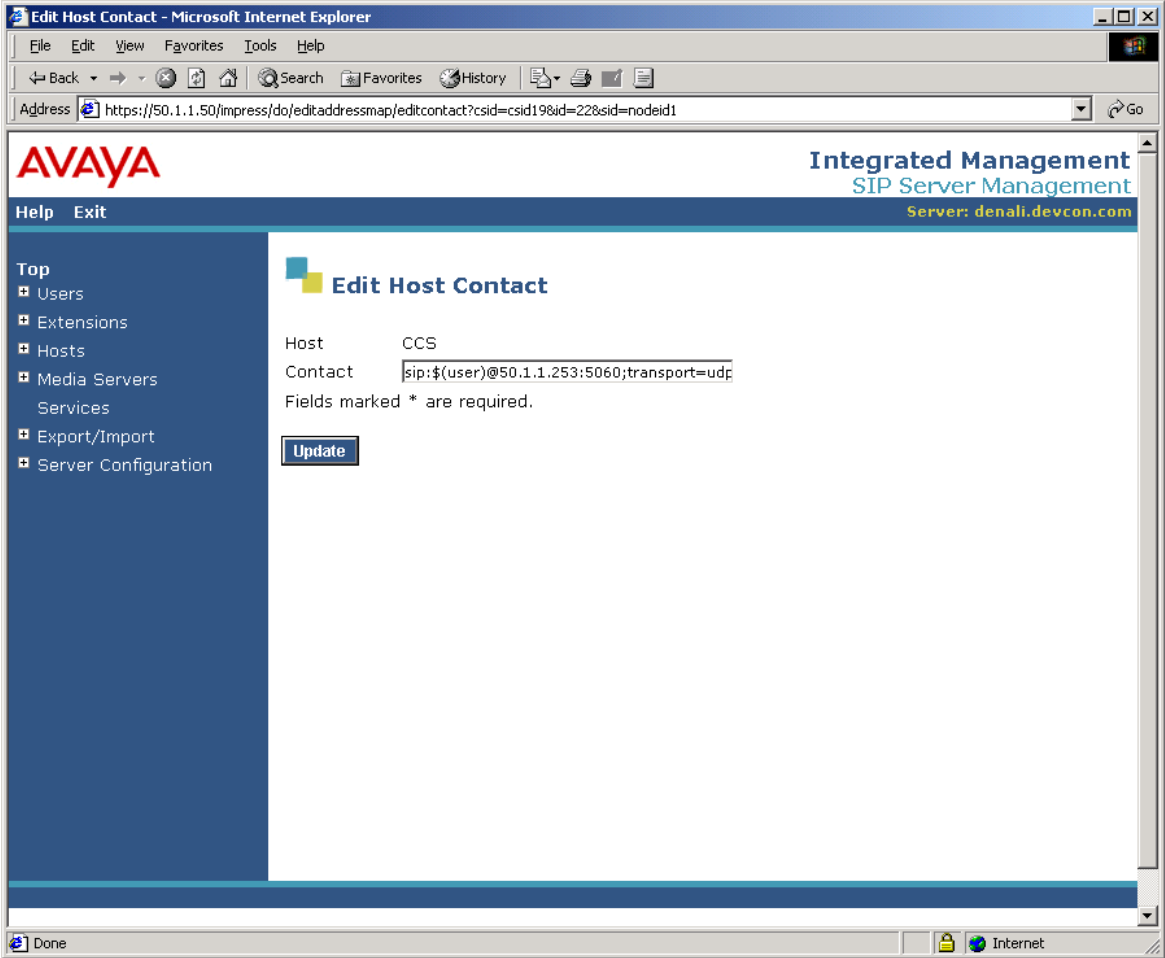
Step	Description
5.	<p><i>Name</i> "4xxxx" was assigned for the extensions located at the customer enterprise site. This Host Map entry will be used if the number dialed matches the <i>Pattern</i> shown (i.e., a five-digit number beginning with 4, followed by four digits between the values of zero through nine).</p>  <p>Click on Back to return to the previous screen. The <i>List Host Address Map</i> screen is displayed. Click on Edit for the contact associated with Host Map 4xxxx.</p>

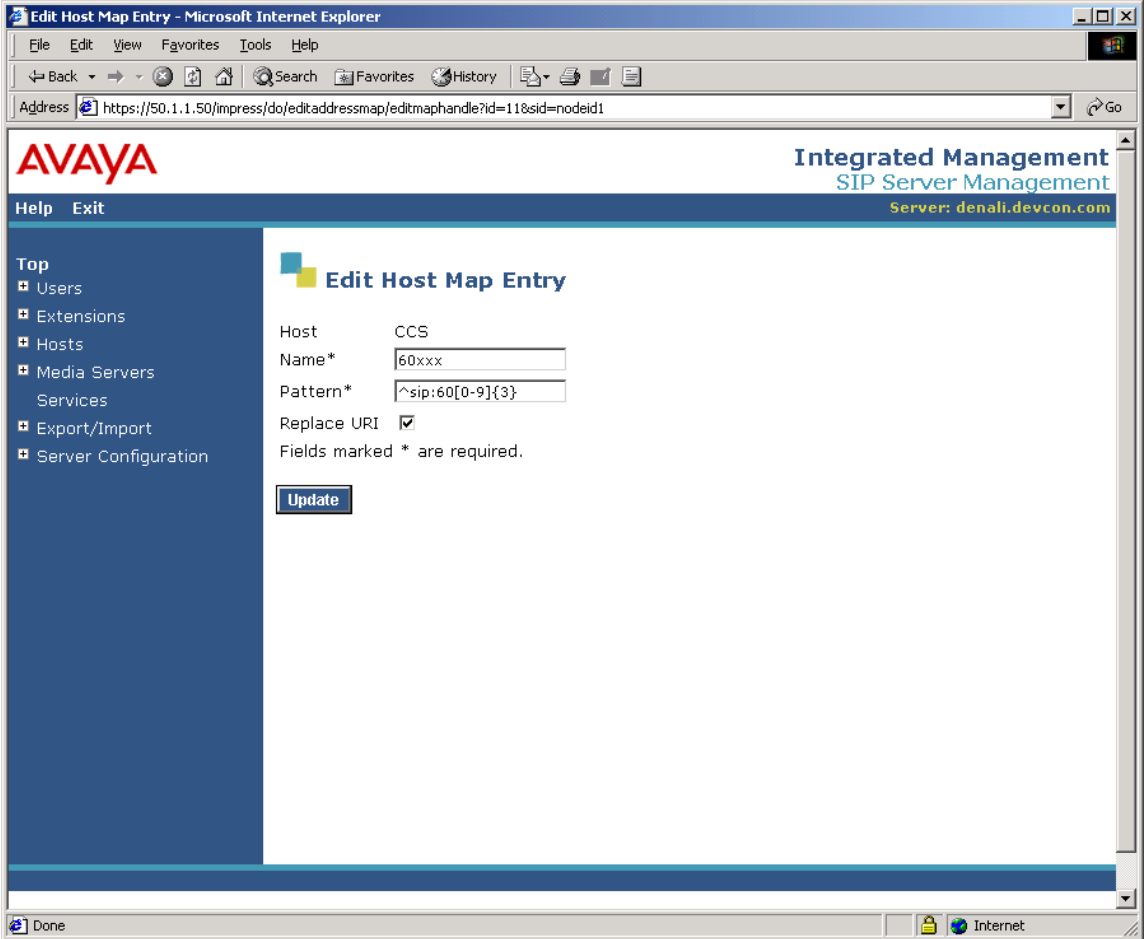
Step	Description
6.	<p>Contact “sip:\$(user)@192.45.100.253:5060;transport=udp” was assigned to Host Map 4xxxx. The IP address (e.g., 192.45.100.253) is that of the of the Acme Packet Net-Net Session Director private interface. The Avaya Converged Communications Server will substitute “\$(user)” with the dialed number.</p>  <p>Click on Back to return to the previous screen. The <i>List Host Address Map</i> screen is displayed. Click on Exit.</p>

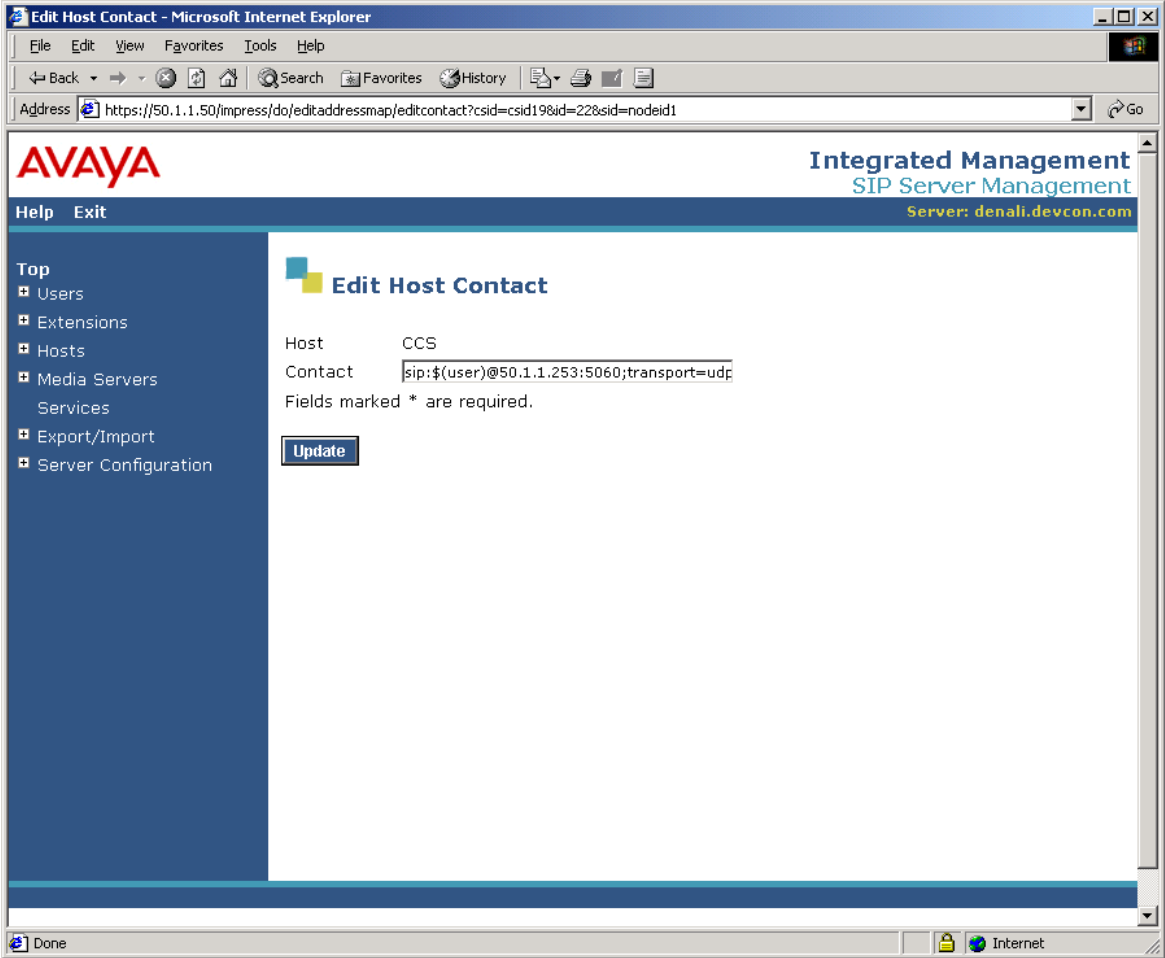
4.2. Customer Enterprise Site

Step	Description
1.	Log in to the Avaya Converged Communications Server at the customer enterprise site using the appropriate credentials.
2.	Steps 2-3 listed in Section 4.1 can be used to navigate to the <i>List Host Address Map</i> screen.
3.	<p>The <i>List Host Address Map</i> screen displays the address maps and associated contacts. The screen below lists the host maps and contacts that have already been added and will be described in more detail in Steps 4 through 7. Click on Edit for Host Map 30xxx.</p> 

Step	Description
4.	<p><i>Name</i> “30xxx” was assigned for the extensions of the H.323 telephones located at the service provider data center site. This Host Map entry will be used if the number dialed matches the <i>Pattern</i> shown (i.e., a five-digit number beginning with 30, followed by three digits between the values of zero through nine).</p> 
	<p>Click on Back to return to the previous screen. The <i>List Host Address Map</i> screen is displayed. Click on Edit for the contact associated with Host Map entry 30xxx.</p>

Step	Description
5.	<p>Contact “sip:\$(user)@50.1.1.253:5060;transport=udp” was assigned to Host Map 30xxx. The IP address (e.g., 50.1.1.253) is that of the of the Acme Packet Net-Net Session Director public interface. The Avaya Converged Communications Server will substitute “\$(user)” with the dialed number.</p>  <p>Click on Back to return to the previous screen. The <i>List Host Address Map</i> screen is displayed. Click on Edit for Host Map 60xxx.</p>

Step	Description
6.	<p><i>Name “60xxx”</i> was assigned for the extensions of the SIP telephones located at the service provider data center site. This Host Map entry will be used if the number dialed matches the <i>Pattern</i> shown (i.e., a five-digit number beginning with 60, followed by three digits between the values of zero through nine).</p>  <p>Click on Back to return to the previous screen. The <i>List Host Address Map</i> screen is displayed. Click on Edit for the contact associated with Host Map 60xxx.</p>

Step	Description
7.	<p>Contact “sip:\$(user)@50.1.1.253:5060;transport=udp” was assigned for Host Map 60xxx. The IP address (e.g., 50.1.1.253) is that of the Acme Packet Net-Net Session Director public interface. The Avaya Converged Communications Server will substitute “\$(user)” with the dialed number.</p>  <p>Click on Back to return to the previous screen. The <i>List Host Address Map</i> screen is displayed. Click on Exit.</p>

5. Configure the Acme Packet Net-Net Session Director

This section describes the configuration of the Acme Packet Net-Net Session Director to function in a “peering” configuration with the Avaya Converged Communications Server and Avaya Communication Manager. The public side will be referred to as the “branch” and the private side will be referred to as the “core” in the Acme Packet Net-Net Session Director configuration.

The Acme Net-Net Session Director was configured using a PC to connected to its console port. This section contains output (text outlined within boxes) from the **show running-config** command that was used to display the configuration of the Acme Net-Net Session Director. Only the specific configuration items that are important to use with the Avaya Converged Communications Server and Avaya Communication Manager are highlighted in bold. For additional details, refer to [6].

H323 Configuration

The basic system parameters have to be configured in order to run H.323 on the Acme Packet Net-Net Session Director.

h323-config	
state	enabled
log-level	INFO
response-tmo	4
connect-tmo	32
last-modified-date	2005-02-23 11:36:29

H323 Stack

A unique H.323 stack is configured for each H.323 resource group (i.e., “branch” and “core”). An H.323 interface may be configured to perform gateway functions, direct H.225 trunking or routed inter-domain gatekeeper functions.

In a “peering” configuration there will be H.323 stacks associated with the “branch” gatekeeper and the “core” gatekeeper. The outgoing stack is determined through the establishment of associated stacks in the *h323-stack* sub-element. The incoming stack uses its *assoc-stack* field to determine the associated outgoing stack. The *assoc-stack* field corresponds to the *name* field of a *h323-stack* sub-element. This type of selection is referred to as “static” because the incoming stack always uses the stack specified in the *assoc-stack* field as the outgoing stack; no other stacks are considered.

The *gatekeeper* address for the “branch” is set to the IP address of the processor interface on the Avaya S8300 Media Server. The gatekeeper address for the “core” is set to the IP address of the C-LAN in the Avaya G600 Media Gateway. The *local-ip* field for the “branch” is set to the IP address of the public interface of the Acme Net-Net Session Director. The *local-ip* field for the “core” is set to the IP address of the private interface of the Acme Net-Net Session Director.

```

h323-stack
  name                h323_branch
  state               enabled
  isgateway           disabled
  realm-id            branch
  assoc-stack         h323_core
  local-ip            50.1.1.253
  max-calls           200
  max-channels        6
  registration-ttl    120
  terminal-alias
  prefixes
  ras-port            1719
  auto-gk-discovery  disabled
  multicast           0.0.0.0:0
  gatekeeper          50.1.1.10:1719
  gk-identifier
  q931-port           1720
  alternate-transport
  q931-max-calls      200
  h245-tunneling      enabled
  fs-in-first-msg     disabled
  call-start-fast     enabled
  call-start-slow     disabled
  media-profiles
  process-registration disabled
  anonymous-connection enabled
  proxy-mode
  h245-stage          connect
  filename
  last-modified-date  2005-03-18 16:53:14
h323-stack
  name                h323_core
  state               enabled
  isgateway           disabled
  realm-id            core
  assoc-stack         h323_branch
  local-ip            192.45.100.253
  max-calls           200
  max-channels        6
  registration-ttl    120
  terminal-alias
  prefixes
  ras-port            1719
  auto-gk-discovery  disabled
  multicast           0.0.0.0:0
  gatekeeper          192.45.100.17:1719
  gk-identifier
  q931-port           1720
  alternate-transport
  q931-max-calls      200
  h245-tunneling      enabled
  fs-in-first-msg     disabled
  call-start-fast     enabled
  call-start-slow     disabled

```

media-profiles	
process-registration	disabled
anonymous-connection	enabled
proxy-mode	
h245-stage	connect
filename	
last-modified-date	2005-03-18 16:53:37
media-manager	
state	enabled
latching	enabled
flow-time-limit	86400
initial-guard-timer	300
subsq-guard-timer	300
hnt-rtcp	disabled
algd-log-level	NOTICE
mbcd-log-level	NOTICE
home-realm-id	
red-flow-port	1985
red-mgcp-port	1986
red-max-trans	10000
red-sync-start-time	5000
red-sync-comp-time	1000
last-modified-date	2005-02-22 13:47:36

Physical and Network Configuration

In the Acme Packet Net-Net Session Director configuration, the “branch” network is a network that is un-trusted and un-protected. The “core” network is considered trusted and protected. In a “peering” configuration, all connected networks are considered protected and configured as private, while the home realm is public.

network-interface	
name	branch
sub-port-id	0
hostname	
ip-address	50.1.1.253
pri-utility-addr	
sec-utility-addr	
netmask	255.255.255.0
gateway	50.1.1.254
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	
hip-ip-list	50.1.1.253
ftp-address	
icmp-address	50.1.1.253

```

snmp-address
telnet-address
last-modified-date          2005-02-23 12:19:25
network-interface
  name                       core
  sub-port-id                0
  hostname
  ip-address                 192.45.100.253
  pri-utility-addr
  sec-utility-addr
  netmask                   255.255.255.0
  gateway                   192.45.100.254
  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
  hip-ip-list                192.45.100.253
  ftp-address
  icmp-address               192.45.100.253
  snmp-address
  telnet-address
last-modified-date          2005-02-23 12:24:38
network-interface
  name                       branch
  sub-port-id                999
  hostname
  ip-address                 127.0.0.100
  pri-utility-addr
  sec-utility-addr
  netmask                   255.255.255.0
  gateway                   127.0.0.100
  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
  hip-ip-list
  ftp-address
  icmp-address
  snmp-address
  telnet-address
last-modified-date          2005-02-22 13:50:42

```

phy-interface	
name	branch
operation-type	Media
port	0
slot	0
virtual-mac	
admin-state	enabled
auto-negotiation	enabled
duplex-mode	FULL
speed	100
last-modified-date	2005-02-22 13:27:08
phy-interface	
name	core
operation-type	Media
port	0
slot	1
virtual-mac	
admin-state	enabled
auto-negotiation	enabled
duplex-mode	FULL
speed	100
last-modified-date	2005-02-22 13:28:00

Realm Configuration

A realm is a way of identifying a domain or network and is used for determining whether or not media steering should occur. Realms can be defined to allow flows to traverse a connection point between the two networks (i.e., “core” and “branch”).

realm-config	
identifier	branch
addr-prefix	0.0.0.0
network-interfaces	
	branch:0
mm-in-realm	disabled
mm-in-network	enabled
msm-release	disabled
max-bandwidth	0
max-latency	0
max-jitter	0
max-packet-loss	0
observ-window-size	0
dns-realm	
media-policy	
in-translationid	
out-translationid	
class-profile	
last-modified-date	2005-02-23 14:18:32

```

realm-config
  identifier                core
  addr-prefix              192.45.100.0/24
  network-interfaces

  mm-in-realm             disabled
  mm-in-network           enabled
  msm-release             disabled
  max-bandwidth           0
  max-latency             0
  max-jitter              0
  max-packet-loss         0
  observ-window-size      0
  dns-realm
  media-policy
  in-translationid
  out-translationid
  class-profile
  last-modified-date      2005-02-23 14:18:46
realm-config
  identifier                acme
  addr-prefix              127.0.0.0/8
  network-interfaces

  mm-in-realm             disabled
  mm-in-network           enabled
  msm-release             disabled
  max-bandwidth           0
  max-latency             0
  max-jitter              0
  max-packet-loss         0
  observ-window-size      0
  dns-realm
  media-policy
  in-translationid
  out-translationid
  class-profile
  last-modified-date      2005-02-22 13:51:45

```


SIP-Port configuration

SIP-port is a configuration entity specifying the default IP address of the Acme Packet Net-Net Session Director SIP proxy in the home realm. There can only be one sip-port configured on the Acme Packet Net-Net Session Director. In configurations where the home realm is connected externally, all SIP messages transmitted into the home realm are transmitted from the sip-port.

```

sip-config
  state          enabled
  sip-port
    hostname    127.0.0.100
    port         5060
    transport-protocol  UDP
    anonymous-connection  enabled
  carriers
  init-timer    500
  max-timer     4000
  trans-expire  32
  invite-expire 180
  inactive-dynamic-conn  32
  home-realm-id acme
  egress-realm-id
  nat-mode      Public
  proxy-mode
  nat-traversal always
  nat-interval  30
  min-reg-expire 300
  registrar-domain
  registrar-host
  registrar-port 0
  registration-caching  disabled
  registration-interval 3600
  route-to-registrar  disabled
  red-sip-port    1988
  red-max-trans   10000
  red-sync-start-time 5000
  red-sync-comp-time 1000
  last-modified-date 2005-02-22 13:34:09
```

SIP-NAT Configuration

SIP-NAT is the Acme Packet Net-Net Session Director configuration entity that is used to configure external SIP signaling addresses and external proxies. A SIP-NAT is associated with an individual resource group (realm). Its primary functions include the following:

- Identifies the “private” addresses in SIP messages to be translated. These addresses are derived from the address prefix of the “private” realm. If no address prefixes are configured for the “private” realm (i.e., 0.0.0.0 address prefix), then all addresses are translated except for those in the address prefix of the home realm.
- Identifies the SIP signaling port to be used for the Resource Group (realm). Each SIP-NAT requires a unique address in the associated resource group and a virtual address in the home network.
- Creates encrypted “cookies” used to specify the Acme Packet Net-Net Session Director as the contact for external endpoints as seen by the home realm and to keep soft-state address mappings for “anonymous” endpoints in external networks.
- Identifies the domain suffix, domain and user tags to be used to create encrypted contact and “maddr” (media address) fields for signaling into the home network.
- Specifies the various SIP headers to be NATed.
- Specifies Resource Group Bridging (SIP-NAT Bridging). SIP realms can be “cross-connected” or “bridged” using SIP-NAT. Using back-to-back SIP-NATs and enabling the “route-home-proxy” feature causes all flows originating within a SIP-NAT realm to be routed to its configured home proxy. For SIP-NAT bridging, the home network addresses are no longer routable addresses outside the Acme Packet Net-Net Session Director, although it must be configured in order for bridging to occur.

Field	Description
realm-id	This field identifies the name of the realm and is used to restrict the SIP proxy to only allow flows that originates from this realm.
domain-suffix	This field identifies the domain name suffix of the external realm. It is used by the Session Director to translate an encoded URI between the public and private realms.
ext-proxy-address	IP address of the SIP proxy in the “branch/core” network the Session Director communicates with externally.
ext-address	IP address of the media interface in the “branch/core” realm that the Session Director uses to communicate with the SIP proxy.
home-address	IP address of the media interface in the home realm that the Session Director communicates with internally.
home-proxy-address	By configuring a home-proxy-address in a SIP-NAT with the corresponding home-address of the “bridged” SIP-NAT, the Session Director will replace the IP address in the SIP message that matches the ingress SIP-NAT ext-address with the next hop SIP-NAT’s home-address IP and not the Session Director SIP proxy IP address. This will then become the IP address in the <i>To</i> field in the associated local-policy.

```

sip-nat
  realm-id                branch
  domain-suffix           .branch.com
  ext-proxy-address       50.1.1.50
  ext-proxy-port          5060
  ext-address             50.1.1.253
  home-address            127.0.20.10
  home-proxy-address      127.0.20.11
  home-proxy-port         5060
  route-home-proxy       enabled
  allow-anonymous         all
  tunnel-redirect         disabled
  use-url-parameter       none
  parameter-name
  contact-mode            maddr
  user-nat-tag            -branch-
  host-nat-tag            BRANCH
  headers                 Call-ID Contact From Join Record-Route
                          Refer-To Replaces Reply-To Route To Via
                          f i m r t v
  last-modified-date      2005-02-22 15:59:15
sip-nat
  realm-id                core
  domain-suffix           .core.com
  ext-proxy-address       192.45.100.200
  ext-proxy-port          5060
  ext-address             192.45.100.253
  home-address            127.0.20.11
  home-proxy-address      127.0.20.10
  home-proxy-port         5060
  route-home-proxy       enabled
  allow-anonymous         all
  tunnel-redirect         disabled
  use-url-parameter       none
  parameter-name
  contact-mode            maddr
  user-nat-tag            -acme-
  host-nat-tag            ACME-
  headers                 Call-ID Contact From Join Record-Route
                          Refer-To Replaces Reply-To Route To Via
                          f i m r t v
  last-modified-date      2005-02-23 17:17:23

```

Configuring Steering Pool

Define the sets of ports used for steering media flows through the Acme Packet Net-Net Session Director and the IP address of the “core” and “branch” interface. The start-port and end-port defines the range of ports that will be available to the associated steering pool element.

```
steering-pool
  ip-address          50.1.1.253
  start-port         20000
  end-port           21000
  realm-id           branch
  last-modified-date 2005-02-22 16:00:10
steering-pool
  ip-address          192.45.100.253
  start-port         20000
  end-port           21000
  realm-id           core
  last-modified-date 2005-02-22 17:32:30
system-config
  hostname            SBC
  description         Avaya_lab_test
  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
  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
  default-gateway     127.0.0.100
  restart             enabled
  exceptions
  telnet-timeout      1800
  console-timeout     0
  last-modified-date 2005-02-22 13:25:49
task done
acmesystem#
```

6. Interoperability Compliance Testing

The Acme Packet Net-Net Session Director was compliance tested to verify that it can interoperate with an Avaya IP Telephony environment. A network consisting of an Avaya Converged Communications Server, Avaya Communication Manager, and Avaya IP telephones (SIP and H.323) was used to evaluate the feature functionality of the Acme Packet Net-Net Session Director.

6.1. General Test Approach

The following scenarios were tested using the network configuration diagram shown in **Figure 1**:

- Ability of the Application Layer Gateway feature of the Acme Packet Net-Net Session Director to pass SIP traffic between two Avaya Converged Communications servers and H.323 traffic between media servers running Avaya Communication Manager
- SIP to SIP, SIP to H.323, and H.323 to H.323 voice calls using G.729 and G.711 codecs were placed manually and subjective quality noted for non-shuffled and shuffled calls
- Ability to register the Avaya IP telephones (SIP and H.323) through the Acme Packet Net-Net Session Director
- Ability of the Avaya IP telephones (SIP and H.323) to access voicemail using DTMF through the Acme Packet Net-Net Session Director
- Ability of the Avaya IP telephones (SIP and H.323) to conference with other participants through the Acme Packet Net-Net Session Director
- Ability of the Avaya IP telephones (SIP and H.323) to transfer to other participants through the Acme Packet Net-Net Session Director

6.2. Test Results

Shuffled and non-shuffled SIP calls were successful. Non-shuffled H.323 calls were successful. To avoid interoperability problems, the signaling group for the H.323 IP trunk was set to disable H.323 shuffling.

Testing was performed with Special Application SA8507 enabled and it did not resolve the problems observed when H.323 shuffling was enabled. The recommendation is to disable H.323 call shuffling for the H.323 IP trunk between the two sites without enabling Special Application SA8507.

The mutually exclusive “Hosted NAT traversal” configuration, not described in these Application Notes, was used to determine if telephones could register through the Acme Packet Net-Net Session Director. Registration of the SIP telephones through the Acme Packet Net-Net Session Director was successful. The H.323 telephones could not register to Avaya Communication Manager through the Acme Packet Net-Net Session Director.

7. Verification Steps

Step	Description
1.	Place calls between the SIP telephones at the two sites. Verify audio quality in both directions. If the call fails, use a SIP-capable network analyzer to verify the INVITE message is being routed correctly. If the INVITE message is not routed correctly, check the address map(s) and associated contacts administered on the Avaya Converged Communications Servers.
2.	Place calls between the H.323 telephones at the two sites. Verify audio quality in both directions. If the call fails, use a H.323 network analyzer to verify that the call is being routed correctly. If the call is not routed correctly, check the routing administered on the Avaya Communication Managers.

8. Support

For technical support on the Acme Packet Net-Net Session Director, visit www.acmepacket.com.

9. Conclusion

The ability of the Acme Packet Net-Net Session Director to interoperate with an Avaya IP Telephony environment consisting of an Avaya Converged Communications Server, Avaya Communication Manager, and Avaya IP telephones (SIP and H.323) in a “peering” configuration with H.323 call shuffling disabled has been successfully compliance tested.

10. References

The following documentation may be found at <http://support.avaya.com>:

- [1] *Converged Communications Server Release 2.1 Installation and Administration*, Doc # 555-245-705, November 2004.
- [2] *Avaya Extension to Cellular and Off-PBX Station (OPS) Installation and Administration Guide*, Doc # 210-100-500, Issue 8, January 2005.
- [3] *SIP Support in Avaya Communication Manager 2.0 running on the Avaya S8300, S8500, or S8700 Media Server*, Doc # 555-245-206, Issue 1, February 2004.
- [4] *Avaya C360 Reference Guide*, Software Version 4.3, Doc # 650-100-704, May 2004.
- [5] *Avaya P333R Installation and Configuration Guide*, Software Version 4.0, April 2003.

The following documentation was included with the Acme Packet Net-Net Session Director:

- [6] *Net-Net Administration and Configuration Guide for the CLI*, Version 1.0, Acme Packet Documentation Set, Release 1.2.1, 405-0001-00 – Rev. C.

©2005 Avaya Inc. All Rights Reserved.

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

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