



Avaya Solution & Interoperability Test Lab

Application Notes for Avaya Communication Server 1000E Release 7.5, Avaya Aura® Session Manager 6.1, and Avaya Aura® Session Border Controller 6.0.2 with AT&T IP Flexible Reach SIP Trunk Service – Issue 1.1

Abstract

These Application Notes illustrate a sample configuration using Avaya Communication Server 1000E Release 7.5, Avaya Aura® Session Manager Release 6.1, and the Avaya Aura® Session Border Controller Release 6.0.2, with the AT&T IP Flexible Reach SIP Trunk service using either **AVPN** or **MIS/PNT** transport connections.

Avaya Aura® Session Manager 6.1 is a core SIP routing and integration engine that connects disparate SIP devices and applications within an enterprise. Avaya Communication Server 1000E 7.5 is a telephony server, and is the point of connection between the enterprise endpoints and Avaya Aura® Session Manager. An Avaya Aura® Session Border Controller 6.0.2 is the point of connection between Avaya Aura® Session Manager and the AT&T IP Flexible Reach service, and is used to not only secure the SIP trunk, but also to make adjustments to the signaling for interoperability.

The AT&T IP Flexible Reach service is one of several SIP-based Voice over IP (VoIP) services offered to enterprises for a variety of voice communications needs. The AT&T IP Flexible Reach service allows enterprises in the U.S.A. to place outbound local and long distance calls, receive inbound Direct Inward Dialing (DID) calls from the PSTN, and place calls between an enterprise's sites.

AT&T is a member of the Avaya DevConnect Service Provider program. Information in these Application Notes has been obtained through compliance testing and additional technical discussions. Testing was conducted via the DevConnect Program.

Table of Contents

1.	Introduction.....	5
2.	General Test Approach and Test Results.....	5
2.1.	Interoperability Compliance Testing	5
2.2.	Test Results	6
2.2.1	Known Limitations	6
2.3.	Call Flows	7
2.3.1	Inbound	7
2.3.2	Outbound.....	8
2.3.3	Call Forward Re-direction	8
2.3.4	Coverage to Voicemail	9
2.4.	Support.....	10
2.4.1	Avaya	10
2.4.2	AT&T.....	10
3.	Reference Configuration.....	10
3.1.	Illustrative Configuration Information.....	13
4.	Equipment and Software Validated	14
5.	Configure Avaya Communication Server 1000E	15
5.1.	Node and Key IP Addresses	16
5.2.	Virtual D-Channel, Routes and Trunks	19
5.2.1	Virtual D-Channel Configuration	19
5.2.2	Routes and Trunks Configuration.....	20
5.3.	SIP Trunk to Session Manager	23
5.4.	Routing of Outbound Dialed Numbers to Session Manager	28
5.4.1	Route List Block	28
5.4.2	Digit Manipulation Block	30
5.4.3	NARS Access Code	32
5.4.4	Numbering Plan Area Codes	33
5.4.5	Other Special Numbers to Route to Session Manager.....	34
5.4.6	Summary	35
5.5.	Routing of Inbound Numbers to CS1000E.....	36
5.6.	Zones.....	38
5.7.	Codec Parameters.....	39
5.7.1	Media Gateway Codec Configuration	39
5.7.2	IP Telephony Node Codec Configuration.....	41
5.8.	Enabling Plug-Ins for Call Transfer Scenarios	43
5.9.	Customer Information.....	43
5.9.1	Calling Number Provisioning for call to the AT&T IP Flexible Reach Service	43
5.10.	CS1000E Stations	48
5.10.1	Example IP UNISim Phone DN 4094,	48
5.10.2	Analog Fax Line	51
5.11.	Changing RFC2833 DTMF Telephone Event Type.....	51
5.12.	Configuration Backup.....	52
6.	Configure Avaya Aura® Session Manager Release 6.1	53
6.1.	SIP Domain.....	55

6.2.	Locations.....	55
6.2.1	Location for Avaya Communication Server 1000E.....	56
6.2.2	Location for the Avaya Aura® Session Border Controller.....	57
6.3.	Configure Adaptations.....	58
6.3.1	Adaptation for Avaya Communication Server 1000E Entity.....	59
6.3.2	Adaptation for the Avaya Aura® SBC Entity.....	60
6.3.3	List of Adaptations.....	61
6.4.	SIP Entities.....	62
6.4.1	SIP Entity for CS1000E.....	62
6.4.2	SIP Entity for the Avaya Aura® SBC.....	63
6.5.	Entity Links.....	64
6.5.1	Entity Link to Avaya Communication Server 1000E Entity.....	64
6.5.2	Entity Link to the Avaya Aura® SBC.....	65
6.6.	Routing Policies.....	66
6.6.1	Routing Policy to the CS1000E.....	66
6.6.2	Routing Policy to the Avaya Aura® SBC.....	67
6.7.	Dial Patterns.....	68
6.7.1	Inbound AT&T calls to CS1000E Users.....	68
6.7.2	Outbound Calls to AT&T.....	69
7.	Configure Avaya Aura® Session Border Controller (SBC).....	70
7.1.	Logging into the Avaya Session Border Controller.....	70
7.2.	Network Configuration.....	72
7.2.1	Verify IP Addressing.....	73
7.2.2	Transport Protocols.....	73
7.2.3	Setting the RTP Port Range on Eth2.....	75
7.2.4	Configuring the SIP-Gateways.....	76
7.2.5	Stripping SIP Headers.....	77
7.2.6	Stripping Unnecessary SIP Message Body Information.....	78
7.2.7	Disable Third Party Call Control.....	79
7.2.8	SIP OPTIONS Messages for AT&T Network Status.....	80
7.2.9	Altering the To Header for PSTN Calls to CS1000E.....	82
7.3.	Saving and Activating Configuration Changes.....	83
7.4.	Avaya Aura® SBC Configuration File.....	84
8.	AT&T IP Flexible Reach Service.....	92
8.1.	AT&T Provisioning.....	92
9.	Verification Steps.....	92
9.1.	Avaya CS1000E Verifications.....	92
9.1.1	IP Network Maintenance and Reports Commands.....	92
9.1.2	System Maintenance Commands.....	96
9.2.	Wireshark Verifications.....	98
9.2.1	Example Outbound Call.....	98
9.2.2	Example Inbound Call.....	101
9.3.	System Manager and Session Manager Verification.....	106
9.3.1	Verify SIP Entity Link Status.....	106
9.3.2	Call Routing Test.....	107
9.4.	Avaya Aura® Session Border Controller Verification.....	109

9.4.1	Status Tab.....	109
9.4.2	Call Logs.....	110
10.	Conclusion	113
11.	References.....	113
11.1.	Avaya	113
11.2.	AT&T IP Flexible Reach service.....	114

1. Introduction

These Application Notes illustrate a sample configuration using Avaya Communication Server 1000E Release 7.5 (CS1000E), Avaya Aura® Session Manager Release 6.1 (Session Manager), and the Avaya Aura® Session Border Controller Release 6.0 (Avaya Aura® SBC), with the AT&T IP Flexible Reach SIP trunk service for PSTN access.

The AT&T IP Flexible Reach service is one of several SIP-based Voice over IP (VoIP) services offered to enterprises for a variety of voice communications needs. The AT&T IP Flexible Reach service allows enterprises in the U.S.A. to place outbound local and long distance calls, receive inbound Direct Inward Dialing (DID) calls from the PSTN, and place calls between an enterprise's sites. The AT&T IP Flexible Reach service utilizes AVPN¹ or MIS/PNT² transport services.

For more information on the, AT&T IP Flexible Reach service visit:

<http://www.business.att.com/enterprise/Service/business-voip-enterprise/network-based-voip-enterprise/ip-flexible-reach-enterprise/>.

2. General Test Approach and Test Results

The interoperability compliance testing focused on verifying inbound and outbound call flows (see **Section 2.3** for examples) between the CS1000E, the Avaya Aura® SBC, and the AT&T IP Flexible Reach service. The CS1000E users make calls to and from the PSTN via the AT&T IP Flexible Reach service.

2.1. Interoperability Compliance Testing

The compliance testing was based on a test plan provided by AT&T. This test plan examines the functionality required by AT&T for solution certification as supported on the AT&T network. Calls were made to and from the PSTN across the AT&T network. The following features were tested as part of this effort:

- SIP trunking of inbound and outbound calls.
 - Incoming calls from the PSTN were routed to the DID numbers assigned by the AT&T IP Flexible Reach service to the CS1000E location. These incoming PSTN calls arrived via the SIP Trunk and were answered by Avaya IP UNISTim telephones and fax machine emulation software (Ventafax). Proper call disconnect was verified.
 - Outgoing calls from the CS1000E location to the PSTN were routed via the SIP Trunk to the AT&T IP Flexible Reach service. These outgoing PSTN calls were originated from Avaya IP UNISTim telephones, and fax machine emulation software (Ventafax). Proper call disconnect was verified.
 - Use of G.729A and G.711Mu codecs were verified.
- Inbound and outbound T.38 Fax, using combinations of G3 and SG3 modes, were verified.

¹ AVPN uses compressed RTP (cRTP).

² MIS/PNT does not support cRTP.

- CS1000E station call coverage to Avaya Call Pilot® for message generation and retrieval (including Message Wait Indicator).
- Passing of DTMF events (RFC2833) and their recognition by navigating automated menus (e.g. Avaya Call Pilot® message selection and retrieval)
- PBX features such as hold, resume, conference and transfer.
- Requests for privacy (i.e., caller anonymity) for CS1000E outbound calls to the PSTN, and for inbound calls from the PSTN to CS1000E, were verified.
- SIP OPTIONS monitoring of the health of the SIP trunk was verified. Both the AT&T IP Flexible Reach service and the Avaya Aura® SBC were able to monitor health using SIP OPTIONS.
- Inbound calls to CS1000E station that were call forwarded back to PSTN destinations, through use of Diversion Header were verified.
- Proper UDP port ranges for RTP media (16384-32767) were verified.

2.2. Test Results

Interoperability testing of the sample configuration was completed with successful results. The following observations were noted during testing:

2.2.1 Known Limitations

1. To allow the CS1000E user to transfer a call from PSTN user A to PSTN user B, before user B has answered the call (unattended transfer), CS1000E plug-in 501 must be enabled as shown in **Section 5.7**. While plug-in 501 will allow the CS1000E user to complete the transfer operation, user A will not hear ring back tone while user B is ringing in this case. PSTN users A and B will have two-way talk path once user B answers.
2. G.711 fax is not supported in the reference configuration. T.38 faxing is supported, as is Group 3 and Super Group 3 fax. Fax speeds to 14400 bps are supported in the configuration tested. In addition, Fax Error Correction Mode (ECM) is supported in the reference configuration.
3. The AT&T IP Flexible Reach service does not support SIP History-Info headers. However, the AT&T IP Flexible Reach service requires that SIP Diversion Header be sent for certain redirected calls (e.g. Call Forward). Session Manager can convert the History Info header into the Diversion Header by the use of the adaptation “*DiversionTypeAdapter*” for these types of calls (see **Section 6.3.2**). For all other calls, the Avaya Aura® SBC will strip off History-Info headers (see **Section 7.2.5**).
4. Emergency 911/E911 Services Limitations and Restrictions – Although AT&T provides 911/E911 calling capabilities, AT&T does not warrant or represent that the equipment and software (e.g., IP PBX) reviewed in this customer configuration guide will properly operate with AT&T IP Flexible Reach to complete 911/E911 calls; therefore, it is the customer’s responsibility to ensure proper operation with the equipment/software vendor.

While AT&T IP Flexible Reach services support E911/911 calling capabilities under certain Calling Plans, there are circumstances when the E911/911 service may not be available, as stated in the Service Guide for AT&T IP Flexible Reach found at

<http://new.serviceguide.att.com>. Such circumstances include, but are not limited to, relocation of the end user's CPE, use of a non-native or virtual telephone number, failure in the broadband connection, loss of electrical power, and delays that may occur in updating the Customer's location in the automatic location information database. Please review the AT&T IP Flexible Reach Service Guide in detail to understand the limitations and restrictions.

2.3. Call Flows

To understand how inbound AT&T IP Flexible Reach service calls are handled by the Avaya CPE environment, three basic call flows are described in this section. However, for brevity, not all possible call flows are described.

2.3.1 Inbound

The first call scenario illustrated is an inbound AT&T IP Flexible Reach service call that arrives at the Avaya Aura® SBC, to Session Manager, and is subsequently routed to the CS1000E, which in turn routes the call to a phone or fax.

1. A PSTN phone originates a call to an AT&T IP Flexible Reach service number.
2. The PSTN routes the call to the AT&T IP Flexible Reach service network.
3. The AT&T IP Flexible Reach service routes the call to the Avaya Aura® SBC.
4. The Avaya Aura® SBC performs SIP Network Address Translation (NAT) and any necessary SIP header modifications, and routes the call to Session Manager.
5. Session Manager applies any necessary SIP header adaptations and digit conversions, and based on configured Routing Policies, determines to where the call should be routed next. In this case, Session Manager routes the call to CS1000E.
6. Depending on the called number, CS1000E routes the call to a phone or fax.

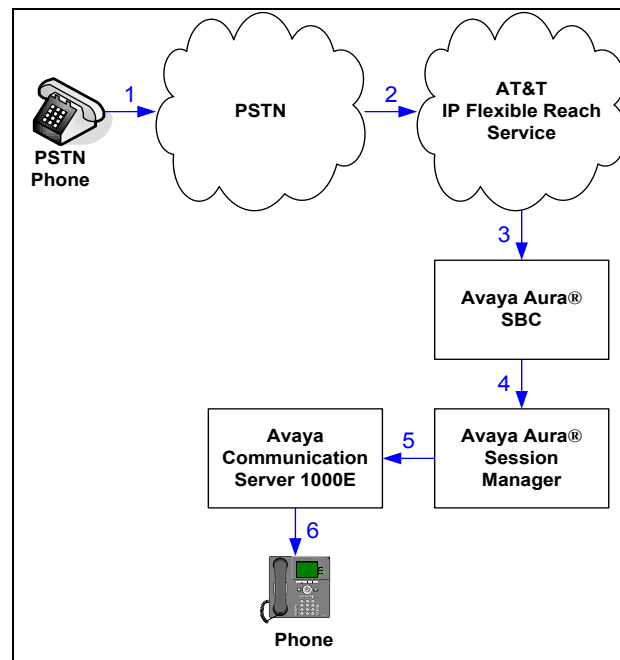


Figure 1 - Inbound AT&T IP Flexible Reach Call

2.3.2 Outbound

The second call scenario illustrated is an outbound call initiated on CS1000E, routed to Session Manager and is subsequently sent to the Avaya Aura® SBC for delivery to AT&T IP Flexible Reach service.

1. A CS1000E phone or fax originates a call to an AT&T IP Flexible Reach service number for delivery to PSTN.
2. CS1000E routes the call to the Session Manager.
3. Session Manager applies any necessary SIP header adaptations and digit conversions, and based on configured Routing Policies, determines to where the call should be routed next. In this case, Session Manager routes the call to the Avaya Aura® SBC.
4. The Avaya Aura® SBC performs SIP Network Address Translation (NAT) and any necessary SIP header modifications, and routes the call to the AT&T IP Flexible Reach service.
5. The AT&T IP Flexible Reach service delivers the call to PSTN.

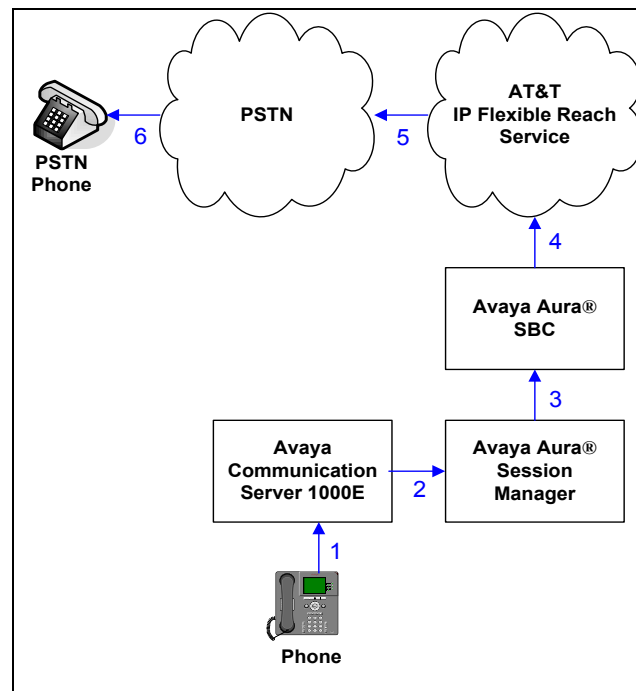


Figure 2 - Outbound AT&T IP Flexible Reach Call

2.3.3 Call Forward Re-direction

The third call scenario illustrated is an inbound AT&T IP Flexible Reach service call that arrives at the Avaya Aura® SBC, to Session Manager, and subsequently CS1000E. The CS1000E routes the call to a destination station, however the station has set Call Forwarding to an alternate destination. Without answering the call, CS1000E immediately redirects the call back to the AT&T IP Flexible Reach service for routing to the alternate destination.

Note – In cases where calls are forwarded to an alternate destination such as an N11, NPA-555-1212, or 8xx numbers, then the AT&T IP Flexible Reach service requires the use of SIP Diversion Header for the redirected call to complete (see **Section 6.3.2**).

1. Same as the first call scenario in **Section 2.3.1**.
2. Because the CS1000E phone has set Call Forward to another AT&T IP Flexible Reach service number, CS1000E initiates a new call back out to Session Manager, the Avaya Aura® SBC, and to the AT&T IP Flexible Reach service network.
3. The AT&T IP Flexible Reach service places a call to the alternate destination and upon answering; CS1000E connects the calling party to the target party.

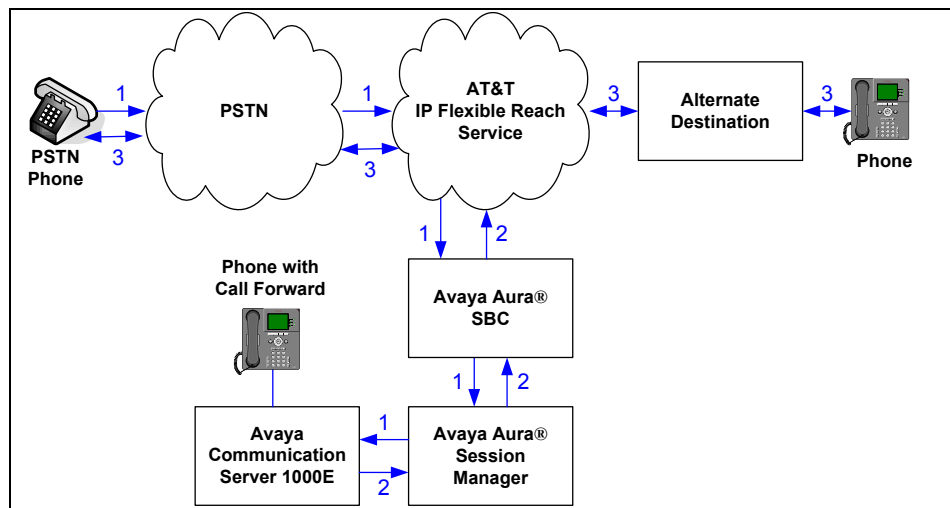


Figure 3 - Re-directed (e.g. Call Forward) AT&T IP Flexible Reach Call

2.3.4 Coverage to Voicemail

The call scenario illustrated is an inbound call that is covered to voicemail. In this scenario, the voicemail system is an Avaya Call Pilot® system connected to the CS1000E.

1. Same as the first call scenario in **Section 2.3.1**.
2. The called CS1000E phone does not answer the call, and the call covers to the phone's voicemail. CS1000E forwards the call to Avaya Call Pilot®. Avaya Call Pilot® answers the call and connects the caller to the called phone's voice mailbox.

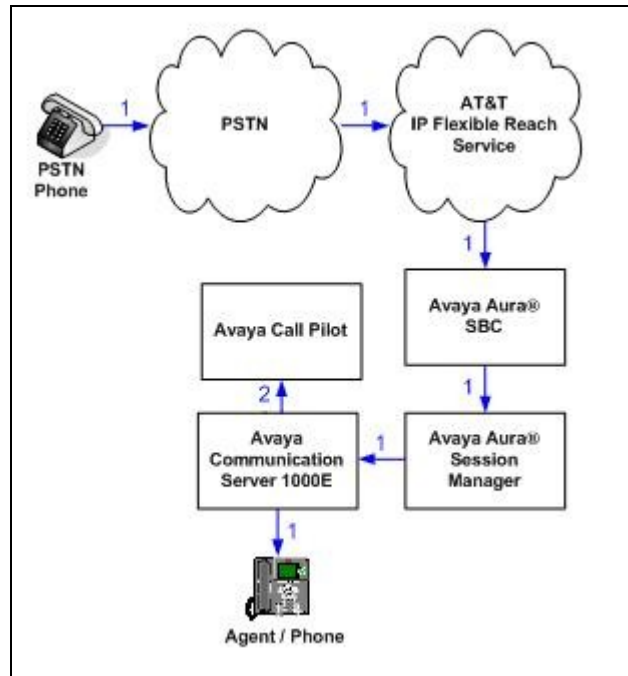


Figure 4 - Coverage to Voicemail

2.4. Support

2.4.1 Avaya

For technical support on the Avaya products described in these Application Notes visit <http://support.avaya.com>.

2.4.2 AT&T

AT&T customers may obtain support for the AT&T IP Flexible Reach service by calling (877) 288-8362.

3. Reference Configuration

The reference configuration used in these Application Notes is shown in **Figure 5** and consists of several components:

- The CS1000E system provides the voice communications services for the enterprise site. The system is comprised of:
 - The MG1000E Gateway containing:
 - Call Server (CPPM).
 - Media Gateway Controller (MGC), which provides Digital Signaling Processor (DSP) resources.
 - Meridian Integration Recorded Announcement (MIRAN) card used for Music on Hold.
 - Avaya Call Pilot® messaging application.
 - IBM 306M Consumer Off The Shelf (COTS) server
 - SIP Signaling Server

- Avaya Unified Communications Management (UCM)

Note – Only the CS1000E system provisioning providing SIP trunk functionality is described in these application notes. For additional CS1000E system provisioning documentation see **Section 12**.

- Avaya “desk” phones are represented with Avaya 1140E and 2004 UNISim IP phones.
- The Avaya Aura® SBC provides address translation and SIP header manipulation between the AT&T IP Flexible Reach service and the enterprise internal network. TCP transport protocol is used between the Avaya Aura® SBC and Session Manager. UDP transport protocol is used between the Avaya Aura® SBC and the AT&T IP Flexible Reach service.
- An existing Avaya Call Pilot® system provides the corporate voice messaging capabilities in the reference configuration. **Note** - The provisioning of Avaya Call Pilot® is beyond the scope of this document (see [11] for more information).
- Outbound calls were originated from a phone or fax provisioned on the CS1000E system. SIP signaling is passed from CS1000E system to Session Manager, and to the Avaya Aura® SBC, before being sent to the AT&T network for termination. Media was sent from the calling IP phone directly to the Avaya Aura® SBC. Legacy devices such as analog fax send their audio from the MGC to the Avaya Aura® SBC. The Avaya Aura® SBC then directs the media to the AT&T network.
- Inbound calls were sent from PSTN/AT&T, through the Avaya Aura® SBC to Avaya Aura® Session Manager, and on to the CS1000E system. The CS1000E system terminates the calls to the appropriate phone or fax extensions.

Note – In the reference configuration TCP (port 5060) is used as the transport protocol between the CS1000K, the Avaya Aura® SBC, and Session Manager. This was done to facilitate protocol trace analysis. However, Avaya best practices call for TLS (port 5061) to be used as the transport protocol where applicable.

UDP transport using port 5060 is required by the AT&T IP Flexible Reach service for the connection between the Avaya Aura® SBC and the AT&T T IP Flexible Reach border element.

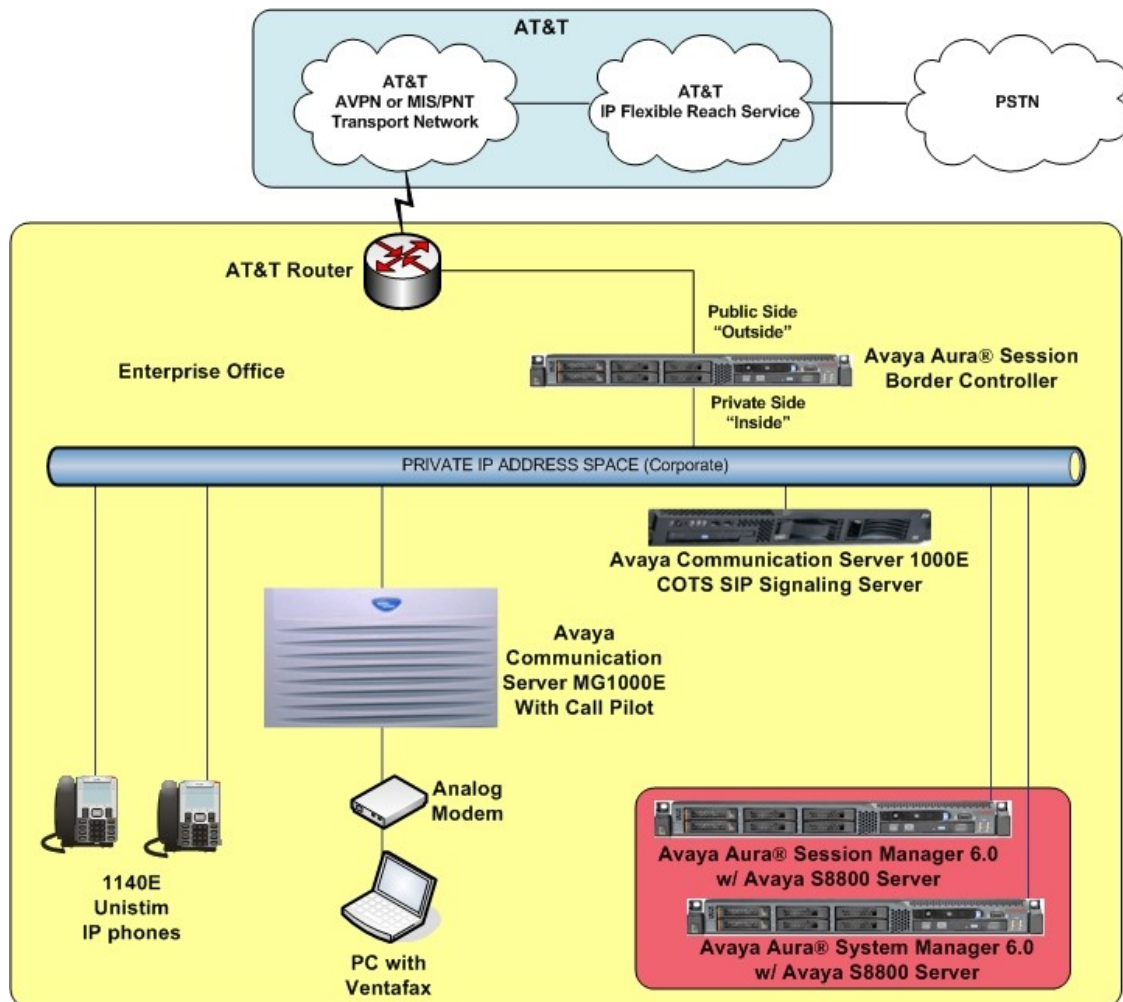


Figure 5: Avaya Interoperability Test Lab Configuration

3.1. Illustrative Configuration Information

The specific values listed in **Table 1** below and in subsequent sections are used in the reference configuration described in these Application Notes, and are for illustrative purposes only. Customers must obtain and use the specific values for their own specific configurations.

Note - The AT&T IP Flexible Reach service border element IP address shown in this document is an example. AT&T Customer Care will provide the actual IP addressing as part of the IP Flexible Reach provisioning process.

Component	Illustrative Value in these Application Notes
Avaya CS1000E	
SIP Signaling Server IP Address (TLAN)	172.16.6.110
MGC Media (DSP) IP Address (TLAN)	172.16.6.115
CS1000E extensions	40xx
Avaya Call Pilot®	
Call Pilot Application	192.168.67.130
Call Pilot Mailboxes	4xxx
Acme SBC	
IP Address of “Outside” (Public) Interface (connected to AT&T Access Router/IP Flexible Reach Service)	192.168.64.130
IP Address of “Inside” (Private) Interface (connected to Session Manager)	192.168.67.125
AT&T IP Flexible Reach Service	
Border Element IP Address	135.25.29.74
AT&T Access router interface (to Acme outside)	192.168.64.254
AT&T Access Router NAT address (Acme outside address)	135.16.170.55

Table 1: Illustrative Values Used in these Application Notes

4. Equipment and Software Validated

The following equipment and software were used in the sample configuration.

Equipment	Software	
Avaya Communication Server 1000E Platform: <ul style="list-style-type: none">MG1000E Media GatewayIBM xSeries 306M (COTS) SIP Signaling server	Release 7.5, Version 7.50.17 with Service_Pack_Linux_7.50_17_20110426 and Plug-in 501 Enabled	
Avaya Call Pilot®	CP 5.00.41 CP50041SU09S, CP500S09G25S, CP500S09G32C	
Avaya S8800 Server (System Manager)	Avaya Aura® System Manager Release 6.1.0 with SP2 (Build Number 6.1.0.0.7345-6.1.5.106)	
Avaya S8800 Server (Session Manager)	Avaya Aura® Session Manager Release 6.1 SP2 (Load 6.1.2.0.612004)	
Avaya S8800 Server (Session Border Controller)	Avaya Aura® Session Border Controller Release 6.0.2.0.3	
Avaya 1140E Series IP Deskphones (UNISTim)	FW 0625C8A	
Avaya 2004 Series IP Deskphones (UNISTim)	FW 0604DCN	
Fax device	Ventafax Home Version 6.3.102.288	
AT&T IP Flexible Reach Service via AVPN or MIS/PNT transport service connections.	VNI 21	

Table 2: Equipment and Software Used in the Sample Configuration

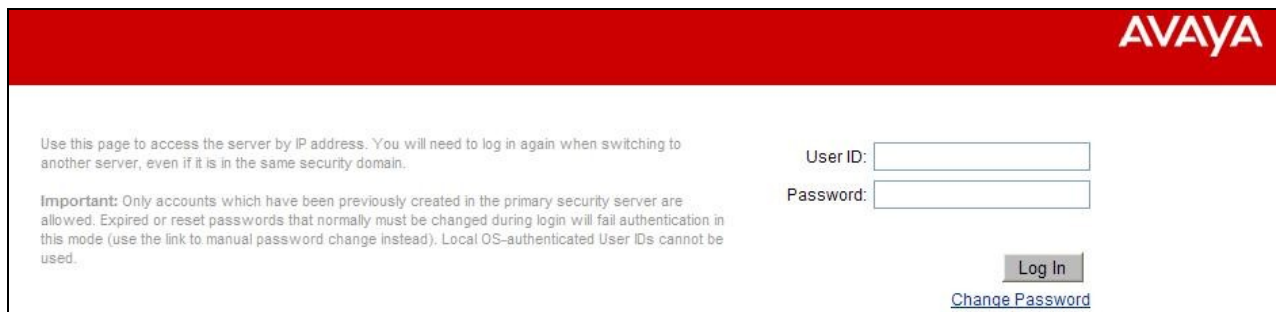
5. Configure Avaya Communication Server 1000E

This section describes the Avaya Communication Server 1000E configuration, focusing on the routing of calls to Session Manager over a SIP trunk. In the sample configuration, Avaya Communication Server 1000E Release 7.5 was deployed with Call Server applications running on a CP+PM server platform with MGC, and utilizing a separate SIP Signaling Server.

Avaya Aura® Session Manager Release 6.1 provides all the SIP Proxy Service (SPS) and Network Connect Services (NCS) functions previously provided by the Network Routing Service (NRS). As a result, the NRS application is not required to configure a SIP trunk between Avaya Communication Server 1000E and Session Manager Release 6.1. Therefore NRS was not included in the reference configuration.

This section focuses on the SIP Trunking configuration. Although sample screens are illustrated to document the overall configuration, it is assumed that the basic configuration of the Call Server and SIP Signaling Server applications has been completed, and that the Avaya Communication Server 1000E is configured to support analog and UNISTim telephones (although supported, SIP telephones were not part of the reference configuration. For references on how to administer these functions of Avaya Communication Server 1000E, see **Section 12**.

Step 1 - Unless otherwise noted, all CS1000E provisioning was performed via the Avaya Unified Communication Management (AUCM) web interface. The **AUCM** web interface may be launched directly via **https://<ip address>** where the relevant <ipaddress> in the sample configuration is 172.16.6.111. The following screen shows an abridged log in screen. Log in with appropriate credentials.



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

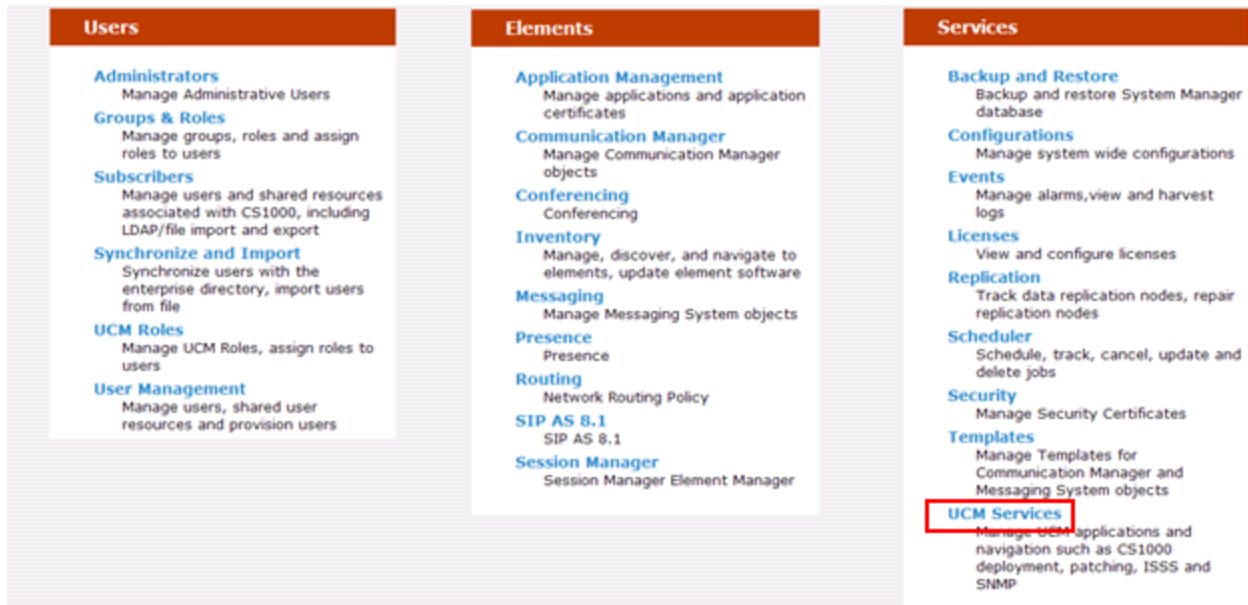
Important: Only accounts which have been previously created in the primary security server are allowed. Expired or reset passwords that normally must be changed during login will fail authentication in this mode (use the link to manual password change instead). Local OS-authenticated User IDs cannot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

User ID:

Password:

[Change Password](#)

Note – Although not used in the reference configuration, Avaya Aura® System Manager may be configured as the Primary Security Server for the Avaya Unified Communications Management application and Avaya Communication Server 1000E is registered as a member of the System Manager Security framework. The Element Manager then may be accessed via System Manager. In this case, access the web based GUI of Avaya Aura® System Manager by using the URL “**http://<ip-address>/SMGR**”, where <ip-address> is the IP address of Avaya Aura® System Manager. Log in with appropriate credentials. The Avaya Aura® System Manager Home Page will be displayed. Under the **Services** category on the right side of the page, click the **UCM Services** link.



Whether the CS1000E is accessed directly or via System Manager, the Avaya Unified Communications Management **Elements** page will be used for configuration.

Step 2 - Click on the **Element Name** corresponding to “CS1000” in the **Element Type** column. In the abridged screen below, the user would click on the **Element Name** “*EM on cots1*”.

The screenshot shows the 'Elements' page in the Avaya Unified Communications Management interface. The page displays a list of elements with the following columns: Element Name, Element Type, Release, Address, and Description. The 'EM on cots1' element is highlighted with a red box.

Element Name	Element Type	Release	Address	Description
EM on cots1	CS1000	7.5	192.12.0.100	New element.
192.12.0.100	Call Server	7.5	192.12.0.100	New element.
192.12.0.11	Media Gateway Controller	7.5	192.12.0.11	New element.
cots1.ntlab.com (primary)	Linux Base	7.5	172.16.6.111	Base OS element.

5.1. Node and Key IP Addresses

Step 1 - Expand **System** → **IP Network** on the left panel and select **Nodes: Servers, Media Cards**. The **IP Telephony Nodes** page is displayed as shown below. Click “<Node id>” in the **Node ID** column to view details of the node. In the sample configuration, **Node ID** “1001” was used.

AVAYA **CS1000 Element Manager** Help | Log

Managing: 192.12.0.100 Username: admin
System » IP Network » IP Telephony Nodes

IP Telephony Nodes

Click the Node ID to view or edit its properties.

<input type="checkbox"/> Node ID ▲	Components	Enabled Applications	ELAN IP	Node/TLAN IPv4	Node/TLAN IPv6	Status
<input type="checkbox"/> 1001	1	LTPS, Gateway (SIPGw)	-	172.16.6.110		Synchronized

Show: ☒ Nodes ☐ Component servers and cards ☒ IPv6 address

The **Node Details** screen is displayed with additional details as shown below. Under the **Node Details** heading at the top of the screen, make a note of the **TLAN Node IPV4 address**. In the sample screen below, the **Node IPV4 address** is “172.16.6.110”. This IP address will be needed when configuring Session Manager with a SIP Entity for the CS1000E in **Section 6.4.1**.

Node Details (ID: 1001 - LTPS, Gateway (SIPGw))

Node ID: * (0-9999)

Call server IP address: *

TLAN address type: ☒ IPv4 only ☐ IPv4 and IPv6

Embedded LAN (ELAN)

Gateway IP address: *

Subnet mask: *

Telephony LAN (TLAN)

Node IPv4 address: *

Subnet mask: *

Node IPv6 address:

* Required Value.

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

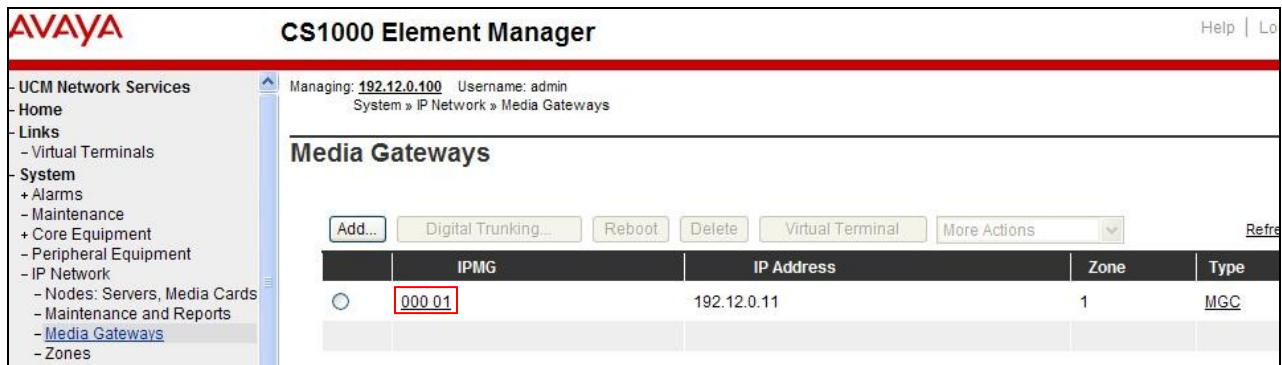
Associated Signaling Servers & Cards

<input type="checkbox"/> Hostname ▲	Type	Deployed Applications	ELAN IP	TLAN IPv4	Role
<input type="checkbox"/> cots1	Signaling_Server	LTPS, Gateway, PD, Presence Publisher, IP Media Services	192.12.0.10	172.16.6.111	Leader

Show: ☐ IPv6 address

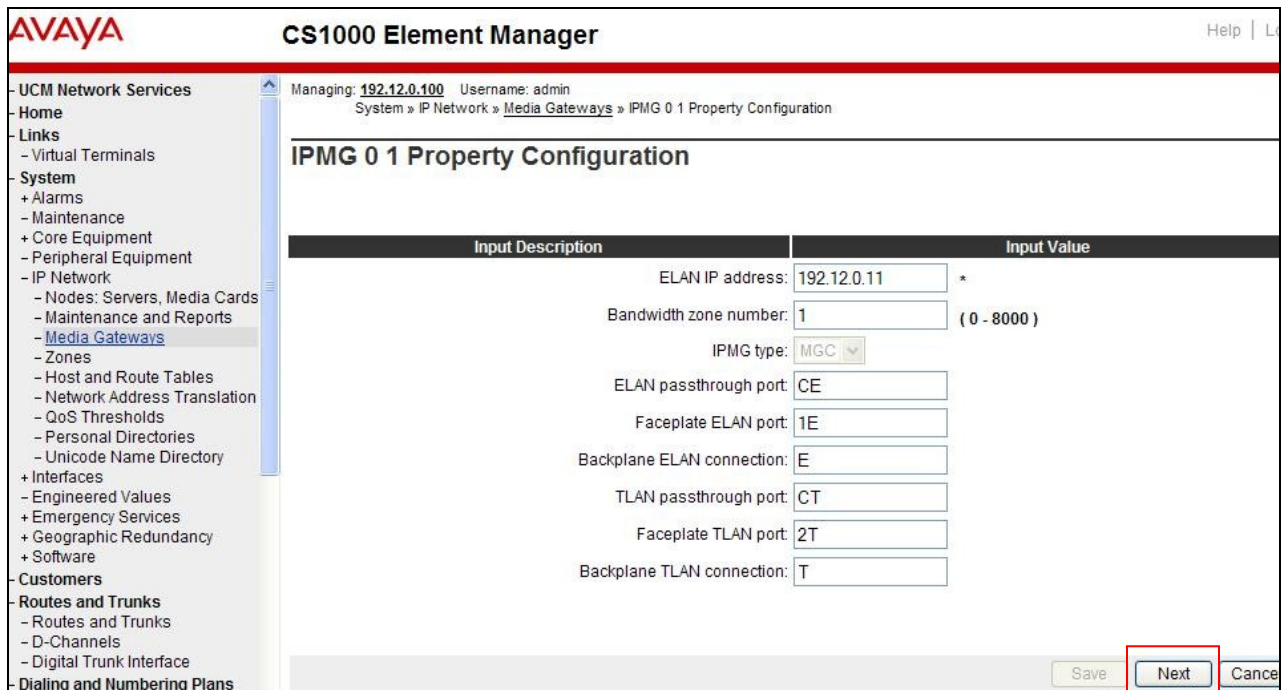
Note: Only server(s) that are not part of any other IP telephony node and deployed application(s) that match the service(s) selected for this node are available in the servers list.

Step 2 - Expand System → IP Network on the left panel and select **Media Gateways**. Click on the IPMG ID (e.g. 000 01).



This will open the Property Configuration screen.

Step 3 – Click on the Next button.



This will open the MGC Configuration screen. The **Telephony LAN (TLAN) IP Address** under the **DSP Daughterboard 1** heading will be the IP Address in the SDP portion of SIP messages, for calls requiring MGC resources. For example, for a call from an analog or digital telephone to PSTN, the IP Address in the SDP in the INVITE message that the CS1000E sends to Session Manager, and on to the Avaya Aura® SBC, will be 172.16.6.115 in the sample configuration. Note that the Avaya Aura® SBC will change this IP address to the Avaya Aura® SBC “outside” IP address before sending the INVITE on to the AT&T IP Flexible Reach service.

AVAYA
CS1000 Element Manager

Help | Logout

- UCM Network Services
- Home
- Links
- Virtual Terminals
- System
+ Alarms
- Maintenance
+ Core Equipment
- Peripheral Equipment
- IP Network
- Nodes: Servers, Media Cards
- Maintenance and Reports
- Media Gateways
- Zones
- Host and Route Tables
- Network Address Translation
- QoS Thresholds
- Personal Directories
- Unicode Name Directory
+ Interfaces
- Engineered Values
+ Emergency Services
+ Geographic Redundancy
+ Software
- Customers
- Routes and Trunks
- Routes and Trunks
- D-Channels
- Digital Trunk Interface
- Dialing and Numbering Plans
- Electronic Switched Network

Managing: 192.12.0.100 Username: admin
System » IP Network » Media Gateways » IPMG 0 1 Property Configuration » IPMG 0 1 Media Gateway Controller (MGC) Configuration

IPMG 0 1 Media Gateway Controller (MGC) Configuration

- Media Gateway Controller

Hostname

MGC

Embedded LAN (ELAN) IP address

192.12.0.11

Embedded LAN (ELAN) gateway IP address

192.12.0.100

Embedded LAN (ELAN) subnet mask

255.255.255.0

Telephony LAN (TLAN) IP address

172.16.6.116

Telephony LAN (TLAN) gateway IP address

172.16.6.1

Telephony LAN (TLAN) subnet mask

255.255.255.0

- DSP Daughterboard 1

Type of the DSP daughterboard

DB96

Telephony LAN (TLAN) IP address

172.16.6.115

Telephony LAN (TLAN) gateway IP address

172.16.6.1

Telephony LAN (TLAN) IPv6 address

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

5.2. Virtual D-Channel, Routes and Trunks

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

5.2.1 Virtual D-Channel Configuration

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

AVAYA
CS1000 Element Manager

- UCM Network Services
- Home
- Links
- Virtual Terminals
- System
+ Alarms
- Maintenance
+ Core Equipment
- Peripheral Equipment
- IP Network
- Nodes: Servers, Media Cards
- Maintenance and Reports
- Media Gateways
- Zones
- Host and Route Tables
- Network Address Translation
- QoS Thresholds
- Personal Directories
- Unicode Name Directory
+ Interfaces
- Engineered Values
+ Emergency Services
+ Geographic Redundancy
+ Software
- Customers
- Routes and Trunks
- Routes and Trunks
- D-Channels
- Digital Trunk Interface

Managing: 192.12.0.100 Username: admin
Routes and Trunks » D-Channels

D-Channels

Maintenance

[D-Channel Diagnostics \(LD 96\)](#)
[Network and Peripheral Equipment \(LD 32, Virtual D-Channels\)](#)
[MSDL Diagnostics \(LD 96\)](#)
[TMDI Diagnostics \(LD 96\)](#)
[D-Channel Expansion Diagnostics \(LD 48\)](#)

Configuration

Choose a D-Channel Number: 0 and type: DCH to Add

- Channel: 15	Type: DCH	Card Type: DCIP	Description: VDCH	Edit
- Channel: 20	Type: DCH	Card Type: DCIP	Description: private	Edit

5.2.2 Routes and Trunks Configuration

In addition to configuring a virtual D-channel, a **Route** and associated **Trunks** must be configured.

Step 1 - Expand **Routes and Trunks** on the left navigation panel and expand the Customer number (e.g. **Customer 0**). In the example screen that follows, it can be observed that **Route 16** has 10 trunks in the sample configuration (**Trunk:1 – 10**).

AVAYA CS1000 Element Manager

Managing: 192.12.0.100 Username: admin
Routes and Trunks » Routes and Trunks

Routes and Trunks

Customer: 0	Total routes: 10	Total trunks: 36		
- Route: 16	Type: TIE	Description: SIP	Edit	Add trunk
+ Trunk: 1 - 10	Total trunks: 10			
+ Route: 26	Type: DID	Description: MIRAN	Edit	Add trunk
+ Route: 27	Type: MUS	Description: MUSIC	Edit	Add trunk

Step 2 – Click on **Trunk:1-10** to display each trunk channel.

- Route: 16	Type: TIE	Description: SIP	Edit	Add trunk
- <u>Trunk: 1 - 10</u>	Total trunks: 10			
- Trunk: 1	TN: 096 1 02 00	Description: SIP	Edit	Multi - Del
- Trunk: 2	TN: 096 1 02 01	Description: SIP	Edit	
- Trunk: 3	TN: 096 1 02 02	Description: SIP	Edit	
- Trunk: 4	TN: 096 1 02 03	Description: SIP	Edit	
- Trunk: 5	TN: 096 1 02 04	Description: SIP	Edit	
- Trunk: 6	TN: 096 1 02 05	Description: SIP	Edit	
- Trunk: 7	TN: 096 1 02 06	Description: SIP	Edit	
- Trunk: 8	TN: 096 1 02 07	Description: SIP	Edit	
- Trunk: 9	TN: 096 1 02 08	Description: SIP	Edit	
- Trunk: 10	TN: 096 1 02 09	Description: SIP	Edit	

Step 3 – Click on the **Edit** button for **Trunk: 1**. Each trunk that is defined must have a corresponding channel, but these trunk and channel numbers need not match. Because channels 1-15 were allocated by other provisioning, in the reference configuration Trunk 1 used Channel 16. Therefore, each subsequent trunk that was provisioned used channel 16+1. For example, Trunk 9 shown in the table above will use channel 24 (16+8 = 24).

Customer 0, Route 16, Trunk 1 Property Configuration

- Basic Configuration

Auto increment member number: ☒

Trunk data block:

Terminal number:

Designator field for trunk:

Extended trunk:

Member number: *

Level 3 Signaling:

Card density:

Start arrangement Incoming :

Start arrangement Outgoing:

Trunk group access restriction:

Channel ID for this trunk:

Class of Service:

Step 4 – Going back to the screen shown in **Step 1**, select the **Edit** button next to **Route 16** to verify the configuration, as shown below. Verify “**SIP (SIP)**” has been selected for **Protocol ID for the route (PCID)** field and the **Node ID of signaling server of this route (NODE)** matches the node shown in **Section 5.1**. As can be observed in the **Incoming and outgoing trunk (ICOG)** parameter, incoming and outgoing calls are allowed. The **Access code for the trunk route (ACOD)** will in general not be dialed, but the number that appears in this field may be observed on Avaya CS1000E display phones if an incoming call on the trunk is anonymous or marked for privacy. The **Zone for codec selection and bandwidth management (ZONE)** parameter can be used to associate the route with a zone for configuration of the audio codec preferences sent via the Session Description Protocol (SDP) in SIP messaging.

AVAYA

CS1000 Element Manager

UCM Network Services

Home

Links

Virtual Terminals

System

Alarms

Maintenance

Core Equipment

Peripheral Equipment

IP Network

Nodes: Servers, Media Cards

Maintenance and Reports

Media Gateways

Zones

Host and Route Tables

Network Address Translation

QoS Thresholds

Personal Directories

Unicode Name Directory

Interfaces

Engineered Values

Emergency Services

Geographic Redundancy

Software

Customers

Routes and Trunks

Routes and Trunks

D-Channels

Digital Trunk Interface

Dialing and Numbering Plans

Electronic Switched Network

Managing: 192.12.0.100 Username: admin

Routes and Trunks » Routes and Trunks » Customer 0, Route 16 Property Configuration

Customer 0, Route 16 Property Configuration

Basic Configuration

Route data block (RDB) (TYPE):

RDB

Customer number (CUST):

00

Route number (ROUT):

16

Designator field for trunk (DES):

SIP

Trunk type (TKTP):

TIE

Incoming and outgoing trunk (ICOG):

Incoming and Outgoing (IAO)

Access code for the trunk route (ACOD):

7916

Trunk type M911P (M911P):

☐

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

☒

Zone for codec selection and bandwidth management (ZONE):

00005

(0 - 8000)

Node ID of signaling server of this route (NODE):

1001

(0 - 9999)

Protocol ID for the route (PCID):

SIP (SIP)

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

☐

Step 5 - Scrolling down, other parameters may be observed. The **D channel number (DCH)** field must match the D-Channel number shown in **Section 5.2.1**.

AVAYA

CS1000 Element Manager

Help | Logout

UCM Network Services

Home

Links

Virtual Terminals

System

Alarms

Maintenance

Core Equipment

Peripheral Equipment

IP Network

Nodes: Servers, Media Cards

Maintenance and Reports

Media Gateways

Zones

Host and Route Tables

Network Address Translation

QoS Thresholds

Personal Directories

Unicode Name Directory

Interfaces

Engineered Values

Emergency Services

Geographic Redundancy

Software

Customers

Routes and Trunks

Routes and Trunks

D-Channels

Digital Trunk Interface

Dialing and Numbering Plans

Electronic Switched Network

Integrated services digital network option (ISDN): ☒

Mode of operation (MODE):

Route uses ISDN Signaling Link (ISLD)

D channel number (DCH):

15

(0 - 254)

Interface type for route (IFC):

Meridian M1 (SL1)

Private network identifier (PNI):

00000

(0 - 32700)

Network calling name allowed (NCNA):

☒

Network call redirection (NCRD):

☒

Trunk route optimization (TRO):

☐

Recognition of DTI2 ABCD FALT signal for ISL (FALT):

☐

Channel type (CHTY):

B-channel (BCH)

Call type for outgoing direct dialed TIE route (CTYP):

Unknown Call type (UKWN)

Insert ESN access code (INAC):

☐

Integrated service access route (ISAR):

☐

Display of access prefix on CLID (DAPC):

☐

Mobile extension route (MBXR):

☐

Mobile extension outgoing type (MBXOT):

National number (NPA)

Mobile extension timer (MBXT):

0

(0 - 8000 milliseconds)

Calling number dialing plan (CNDP):

Unknown (UKWN)

Step 6 - Scrolling down, open **Basic Route Options** and verify that the DCNO number specified (e.g. 1), matches the **Digit Conversion Tree Number** specified in **Section 5.5**.

- Basic Route Options

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

Billing number required (BILN) : ☐

Call detail recording (CDR) : ☐

North American toll scheme (NATL) : ☒

Controls or timers (CNTL) : ☐

Conventional (Tie trunk only) (CNVT) : ☐

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

- Day IDC tree number (DCNO) : 1 (0 - 254)

- Night IDC tree number (NDNO) : 1 (0 - 254)

- Display external dialed digits (DEXT) : ☐

MFC feature options (MFC_FEAT) : ☐

+ Network Options

+ General Options

+ Advanced Configurations

5.3. SIP Trunk to Session Manager

Step 1 - Expand System → IP Network → Nodes: Servers, Media Cards.

Step 2 - Select **Node ID 1001** as shown in **Step 2** of **Section 5.1** to edit configuration settings for the configured node.

Step 3 - Using the scroll bar on the right side of the screen, navigate to the **Applications** section on the screen and select the **Gateway (SIPGw)** link to view or edit the SIP Gateway configuration.

Managing: 192.12.0.100 Username: admin

System » IP Network » IP Telephony Nodes » Node Details

Node Details (ID: 1001 - LTPS, Gateway (SIPGw))

Gateway IP address: 192.12.0.1 *

Node IPv4 address: 172.16.0.110 *

Subnet mask: 255.255.255.0 *

Subnet mask: 255.255.255.0 *

Node IPv6 address:

IP Telephony Node Properties

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

Applications (click to edit configuration)

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

* Required Value.

Save Cancel

Step 4 - On the Node ID: 1001 - Virtual Trunk Gateway Configuration Details page, enter the following values and use default values for remaining fields.

- **SIP domain name:** Enter the appropriate SIP domain for the customer network. In the sample configuration, “cots1.ntlab.com” was used in the reference configuration.
- **Local SIP port:** Enter “5060”
- **Gateway endpoint name:** Enter descriptive name
- **Application node ID:** Enter “<Node id>”. In the sample configuration, Node “1001” was used matching the node shown in **Section 5.1**.

The values defined for the sample configuration are shown below.

Node ID: 1001 - Virtual Trunk Gateway Configuration Details

General | SIP Gateway Settings | SIP Gateway Services

Vtrk gateway application: ☒ Enable gateway service on this node

General

Vtrk gateway application: SIP Gateway (SIPGw) ▼

SIP domain name: cots1.ntlab.com *

Local SIP port: 5060 *(1 - 65535)

Gateway endpoint name: SS_1001 *

Gateway password: *

Application node ID: 1001 *(0-9999)

Enable failsafe NRS: ☐

SIP ANAT: ☒ IPv4 ☐ IPv6

Virtual Trunk Network Health Monitor

☐ Monitor IP addresses (listed below)

Information will be captured for the IP addresses listed below.

Monitor IP: Add

Monitor addresses:

Remove

* Required Value.

Note: Changes made on this page will NOT be transmitted until the Node is also saved.

Save Cancel

Step 5 - Scroll down to the section: SIP Gateway Settings → Proxy or Redirect Server

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

- **Primary TLAN IP address:** Enter the IP address of the Session Manager SIP signaling interface. In the sample configuration, “192.168.67.210” was used.
- **Port:** Enter “5060”
- **Transport protocol:** Select “TCP”

Note: TCP was used for the reference configuration. However, Avaya best practices recommends the use of TLS in production environments. For more information on configuring the CS1000E to use TLS, see [8].

Note - The Secondary TLAN IP address was not used.

Proxy Or Redirect Server:

Proxy Server Route 1:

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

Port: (1 - 65535)

Transport protocol: ▼

Options: ☐ Support registration
☐ Primary CDS proxy

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

Port: (1 - 65535)

Transport protocol: ▼

Step 6 - Scroll down and repeat these steps for the **Proxy Server Route 2** (not shown).

Step 7 - Scroll down to the **SIP URI Map** section. The values defined for the sample configuration are shown below. The Avaya CS1000E will put the “string” entered in the **SIP URI Map** in the “phone-context=<string>” parameter in SIP headers such as the P-Asserted-Identity. If the CDP: value is configured to blank, the CS1000E will omit the “phone-context=” in the SIP header altogether.

SIP URI Map:

Public E.164 domain names	Private domain names
National: <input type="text"/>	UDP: <input type="text"/>
Subscriber: <input type="text"/>	CDP: <input type="text" value="cdp.udp"/>
Special number: <input type="text"/>	Special number: <input type="text"/>
Unknown: <input type="text"/>	Vacant number: <input type="text"/>
	Unknown: <input type="text"/>

Step 8 - Scroll to the bottom of the page and click **Save** (not shown) to save SIP Gateway configuration settings. This will return the interface to the **Node Details** screen.

Step 9 - Click **Save** on the **Node Details** screen (not shown).

Step 10 - Select **Transfer Now** on the **Node Saved** page as shown below.

AVAYA **CS1000 Element Manager**

Managing: 192.12.0.100 Username: admin
System » IP Network » IP Telephony Nodes » Node Saved

Node Saved

Node ID: 1001 has been saved on the call server.

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

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

You may initiate a transfer manually at a later time.

Once the transfer is complete, the **Synchronize Configuration Files (Node ID <id>)** page is displayed.

Managing: 192.12.0.100 Username: admin
System » IP Network » IP Telephony Nodes » Synchronize Configuration Files

Synchronize Configuration Files (Node ID <1001>)

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

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

<input type="checkbox"/>	Hostname	Type	Applications	Synchronization Status
<input type="checkbox"/>	cots1	Signaling_Server	LTPS, Gateway, PD, Presence Publisher, IP Media Services	Sync required

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

Step 11 - Enter ☒ associated with the appropriate Hostname (e.g. **cots1**) and click **Start Sync**.

The Synchronization Status field will update from Sync required, to Sync in progress, to Synchronized as shown below

Managing: 192.12.0.100 Username: admin
System » IP Network » IP Telephony Nodes » Synchronize Configuration Files

Synchronize Configuration Files (Node ID <1001>)

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

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

<input type="checkbox"/>	Hostname	Type	Applications	Synchronization Status
<input type="checkbox"/>	cots1	Signaling_Server	LTPS, Gateway, PD, Presence Publisher, IP Media Services	Synchronized

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

Step 12 - After synchronization completes, click on the **Refresh** button in the right hand corner, enter ☒ associated with the appropriate Hostname (e.g. cots1), and click **Restart Applications**.

NOTE - When the applications restart, the phones will also reset.

Managing: 192.12.0.100 Username: admin

System » IP Network » IP Telephony Nodes » Synchronize Configuration Files

Synchronize Configuration Files (Node ID <1001>)

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

Start Sync

Cancel

Restart Applications

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

<input checked="" type="checkbox"/>	Hostname	Type	Applications	Synchronization Status
<input checked="" type="checkbox"/>	cots1	Signaling_Server	LTPS, Gateway, PD, Presence Publisher, IP Media Services	Synchronized

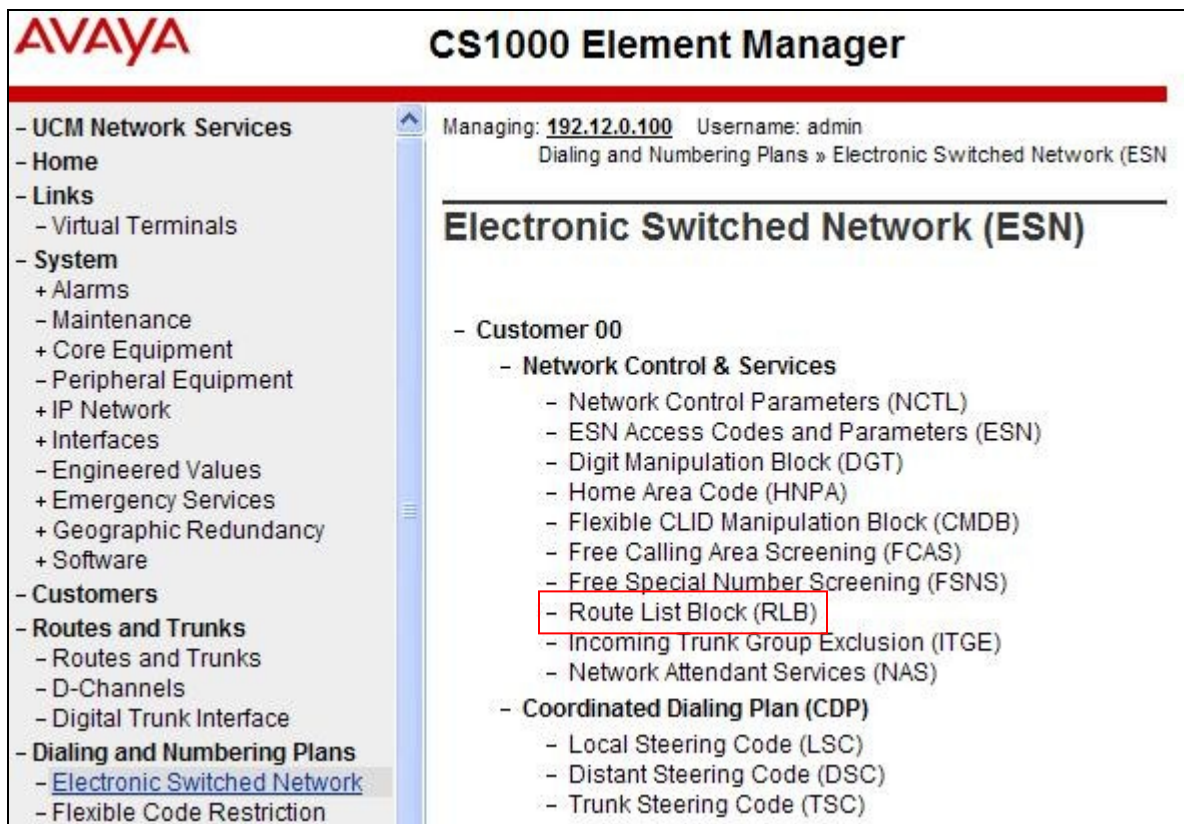
* Application restart is only required for initial system configuration or if changes have been made to general LAN configurations, SNTP settings, SIP and H323 Gateway settings, network connectivity related parameters like ports and IP address, enabling or disabling services, or adding or removing application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

5.4. Routing of Outbound Dialed Numbers to Session Manager

This section provides the configuration of the routing used in the reference configuration for routing calls over the SIP Trunk between Avaya Communication Server 1000E and Session Manager for calls destined for the AT&T IP Flexible Reach service. The routing defined in this section is simply an example and not intended to be prescriptive. The example will focus on the configuration enabling a CS1000E telephone user to dial 9-1-732-xxx-xxxx to reach a PSTN telephone. Other routing policies may be appropriate for different customer networks.

5.4.1 Route List Block

Step 1 - Expand **Dialing and Numbering Plans** on the left navigational panel and select **Electronic Switched Network**. Select **Route List Block (RLB)** on the **Electronic Switched Network (ESN)** page as shown below.



The **Route List Blocks** screen is displayed.

Step 2 - Enter an available route list index number in the **Please enter a route list index** field and click to **Add**, or edit an existing entry by clicking the corresponding **Edit** button. In the sample configuration, route list block index **15** is used.

AVAYA CS1000 Element Manager

Managing: 192.12.0.100 Username: admin
Dialing and Numbering Plans » Electronic Switched Network (ESN) » Customer 00 » Network Control & Services » Route List Blocks

Route List Blocks

Please enter a route list index (0 - 1999)

- + Route List Block Index -- 10
- + Route List Block Index -- 15**
- + Route List Block Index -- 16
- + Route List Block Index -- 17
- + Route List Block Index -- 18
- + Route List Block Index -- 19
- + Route List Block Index -- 20

The Route List Block screen will open.

Step 3 - If adding a new route list index, scroll down to the **Options** area of the screen. If editing an existing route list block index, select the **Edit** button next to the appropriate **Data Entry Index** as shown below (e.g. 0).

AVAYA CS1000 Element Manager

Managing: 192.12.0.100 Username: admin
Dialing and Numbering Plans » Electronic Switched Network (ESN) » Customer 00 » Network Control & Services » Route List Block

Route List Block

General Properties

Number of Alternate Routing Attempts: (1 - 10)

Initial Set: (0 - 64)

Set Minimum Facility Restriction Level:

Overlap Length: (0 - 24)

Extended Local Calls: ☐

Route List Index:

Please choose the

- + Data Entry Index -- 0**
- + Data Entry Index -- 1

The **Data Entry of a Route List Block** screen will open.

Step 4 – Scroll down to **Digit Manipulation Index** and select **15** (see **Section 5.4.2**).

Step 5 - Scroll down to the **Options** section and select a “<Route id>” in the **Route Number** drop down menu. In the sample configuration route number **16** was used. Default values may be retained for remaining fields as shown below.

The screenshot displays a configuration window with three main sections: General Properties, Indexes, and Options. In the General Properties section, the 'Entry Number for the Route List' is set to 0. The Indexes section contains several fields: 'Time of Day Schedule' (0), 'Facility Restriction Level' (0, range 0-7), 'Digit Manipulation Index' (15, highlighted with a red box), 'ISL D-Channel Down Digit Manipulation Index' (0, range 0-1999), 'Free Calling Area Screening Index' (0), 'Free Special Number Screening Index' (0), 'Business Network Extension Route' (unchecked), and 'Incoming CLID Table' (0, range 0-0). The Options section includes 'Local Termination entry' (unchecked), 'Route Number' (16, highlighted with a red box), 'Skip Conventional Signaling' (unchecked), 'Use Tone Detector' (unchecked), and 'Conversion to LDN' (unchecked).

Step 6 - Click **Submit** (not shown) to save the Route List Block definitions.

In the reference configuration Route list block 15 uses Digit Manipulation 15 to keep the called number unchanged (see below), and Route 16 to send calls to Session Manager.

5.4.2 Digit Manipulation Block

The Digit Manipulation Block (DGT) is used to modify the outbound called digit string.

Step 1 - Expand **Dialing and Numbering Plans** on the left navigational panel and select **Electronic Switched Network**. Select **Digit Manipulation Block (DGT)** as shown below.

CS1000 Element Manager

Managing: **192.12.0.100** Username: admin

Dialing and Numbering Plans » Electronic Switched Network (ESN)

Electronic Switched Network (ESN)

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

- UCM Network Services
- Home
- Links
 - Virtual Terminals
- System
 - + Alarms
 - Maintenance
 - + Core Equipment
 - Peripheral Equipment
 - + IP Network
 - + Interfaces
 - Engineered Values
 - + Emergency Services
 - + Geographic Redundancy
 - + Software
- Customers
- Routes and Trunks
 - Routes and Trunks
 - D-Channels
 - Digital Trunk Interface
- Dialing and Numbering Plans
 - Electronic Switched Network
 - Flexible Code Restriction

Step 2 – Add a new Digit Manipulation Block if required. In the reference configuration Digit Manipulation Block **15** was used. Click on **Edit**.

Managing: **192.12.0.100** Username: admin

Dialing and Numbering Plans » Electronic Switched Network (ESN) » Customer 00 » Network Control & Services » Digit Manipulation Block List

Digit Manipulation Block List

Please choose the

+ Digit Manipulation Block Index -- 1	<input type="button" value="Edit"/>
+ Digit Manipulation Block Index -- 2	<input type="button" value="Edit"/>
+ Digit Manipulation Block Index -- 15	<input type="button" value="Edit"/>
+ Digit Manipulation Block Index -- 16	<input type="button" value="Edit"/>
+ Digit Manipulation Block Index -- 17	<input type="button" value="Edit"/>
+ Digit Manipulation Block Index -- 18	<input type="button" value="Edit"/>
+ Digit Manipulation Block Index -- 19	<input type="button" value="Edit"/>
+ Digit Manipulation Block Index -- 20	<input type="button" value="Edit"/>
+ Digit Manipulation Block Index -- 30	<input type="button" value="Edit"/>

Step 3 – Set **Number of leading digits to be deleted** to **0** (zero). Set **Call Type to be used by the manipulation digits** to **Call type will not be changed (NCHG)**.

The screenshot shows a web form titled "Digit Manipulation Block". It contains the following fields and controls:

- "Digit Manipulation Index numbers:" followed by a text input field containing the value "15".
- "Number of leading digits to be deleted:" followed by a text input field containing "0" and a range indicator "(0 - 19)".
- "Insert:" followed by an empty text input field.
- "IP Special Number :" followed by an unchecked checkbox.
- "Call Type to be used by the manipulated digits :" followed by a dropdown menu with "Call type will not be changed (NCHG)" selected.
- At the bottom right, there are four buttons: "Submit", "Refresh", "Delete", and "Cancel".

Step 4 – Click on **Submit**.

5.4.3 NARS Access Code

This section defines the access code for off-net dialing (e.g. calls to PSTN).

Step 1 - Expand **Dialing and Numbering Plans** on the left navigational panel and select **Electronic Switched Network**.

Step 2 - Select **ESN Access Codes and Parameters (ESN)**. Although not repeated below, this link can be observed in the first screen in **Section 5.4.1**.

Step 3 - In the **NARS/BARS Access Code 1** field, enter the number the user will dial before the target PSTN number. In the sample configuration, the single digit “9” was used.

Step 4 - Click on **Submit** (not shown).

ESN Access Codes and Basic Parameters

General Properties

NARS/BARS Access Code 1:

NARS Access Code 2:

NARS/BARS Dial Tone after dialing AC1 or AC2 access codes: ☒

Expensive Route Warning Tone: ☒

- Expensive Route Delay Time: (0 - 10)

Coordinated Dialing Plan feature for this customer: ☒

- Maximum number of Steering Codes: (1 - 64000)

- Number of digits in CDP DN (DSC + DN or LSC + DN): (3 - 10)

Routing Controls: ☐

Check for Trunk Group Access Restrictions: ☒

5.4.4 Numbering Plan Area Codes

This section defines the various **Numbering Plan Area Code (NPA)** used to access PSTN (e.g. 1732).

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

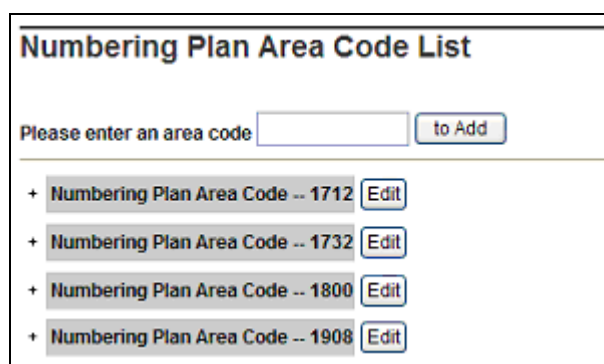
AVAYA

CS1000 Element Manager

- + Core Equipment
 - Peripheral Equipment
- + IP Network
- + Interfaces
 - Engineered Values
- + Emergency Services
- + Software
- Customers
- Routes and Trunks
 - Routes and Trunks
 - D-Channels
 - Digital Trunk Interface
- **Dialing and Numbering Plans**
 - Electronic Switched Network
 - Flexible Code Restriction
 - Incoming Digit Translation
- Phones
- Templates

- Flexible CLID Manipulation Block (CLMB)
- Free Calling Area Screening (FCAS)
- Free Special Number Screening (FSNS)
- Route List Block (RLB)
- Incoming Trunk Group Exclusion (ITGE)
- Network Attendant Services (NAS)
- **Coordinated Dialing Plan (CDP)**
 - Local Steering Code (LSC)
 - Distant Steering Code (DSC)
 - Trunk Steering Code (TSC)
- **Numbering Plan (NET)**
 - **Access Code 1**
 - Home Location Code (HLOC)
 - Location Code (LOC)
 - Numbering Plan Area Code (NPA)
 - Exchange (Central Office) Code (NXX)
 - Special Number (SPN)

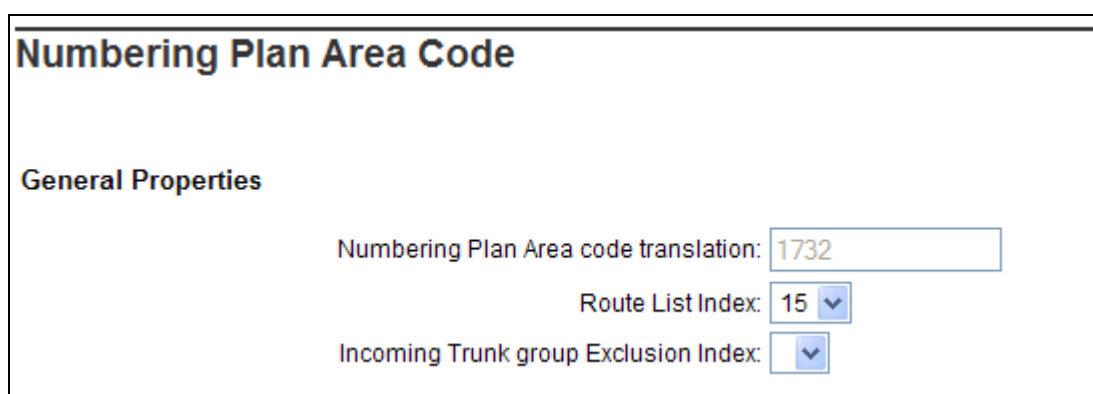
Step 2 - Add a new NPA by entering it in the **Please enter an area code** box and click **to Add** or click **Edit** to view or change an NPA that has been previously configured. In the screen below, it can be observed that various dial strings such as **1732**, **1800** and **1908** are configured.



The screenshot shows a web interface titled "Numbering Plan Area Code List". At the top, there is a text input field labeled "Please enter an area code" followed by a "to Add" button. Below this, there is a list of four entries, each consisting of a plus sign, the text "Numbering Plan Area Code --", a value, and an "Edit" button. The values are 1712, 1732, 1800, and 1908.

Numbering Plan Area Code	Action
+ Numbering Plan Area Code -- 1712	Edit
+ Numbering Plan Area Code -- 1732	Edit
+ Numbering Plan Area Code -- 1800	Edit
+ Numbering Plan Area Code -- 1908	Edit

Step 3 - In the screen below, the entry for “1732” is displayed. In the Route List Index, “15” is selected to use the route list associated with the SIP Trunk to Session Manager (as defined in **Section 5.4.1, Step 2**). Default parameters may be retained for other parameters. Repeat this procedure for the dial strings associated with other numbering plan area codes that should route to the SIP Trunk to Session Manager.



The screenshot shows a web interface titled "Numbering Plan Area Code". Under the "General Properties" section, there are three configuration fields: "Numbering Plan Area code translation:" with a text input field containing "1732", "Route List Index:" with a dropdown menu showing "15", and "Incoming Trunk group Exclusion Index:" with a dropdown menu showing a downward arrow.

Property	Value
Numbering Plan Area code translation:	1732
Route List Index:	15
Incoming Trunk group Exclusion Index:	▼

5.4.5 Other Special Numbers to Route to Session Manager

In the testing associated with these Application Notes, non-emergency service numbers such as **n11**, and **011** international calls were also routed to Session Manager and ultimately to the AT&T IP Flexible Reach service. Although not intended to be prescriptive, one approach to such routing is summarized in this section.

Step 1 - Expand **Dialing and Numbering Plans** on the left navigational panel and select **Electronic Switched Network**.

Step 2 - Scroll down and select **Special Number (SPN)** under the appropriate **Access Code** heading (e.g. **1** as shown in **Section 5.4.3, Step 3**).

Step 3 - Add a new number by entering it in the **Please enter a Special Number** box and click to **Add** or click **Edit** to view or change a special number that has been previously configured. In the screen below, it can be observed that various dial strings such as 0, 011, and x11 calls are listed.

The screenshot shows the AVAYA CS1000 Element Manager web interface. On the left is a navigation tree with categories like UCM Network Services, Home, Links, System, Customers, Routes and Trunks, and Dialing and Numbering Plans. The 'Dialing and Numbering Plans' section is expanded, showing 'Electronic Switched Network' and 'Flexible Code Restriction'. The main content area is titled 'Special Number List'. It features a text input field labeled 'Please enter a Special Number' with a 'to Add' button. Below this, there is a list of three special numbers: 'Special Number -- 0', 'Special Number -- 011', and 'Special Number -- 411'. Each entry has an 'Edit' button next to it.

Step 4 – To modify an entry click on “**Edit**”. In each case, **Route list index “15”** has been selected in the same manner as shown for the NPAs in the prior section.

The screenshot shows the configuration page for a specific special number, titled 'Special Number (011)'. Under the 'General Properties' section, there are two dropdown menus. The first is labeled 'Route list index:' and has the value '15' selected. The second is labeled 'Incoming trunk group exclusion index:' and has a downward arrow indicating it is currently closed.

Step 4 - Click on **Submit** (not shown).

5.4.6 Summary

In summary, to have CS1000E route a PSTN call for 1732xxxxxxx via SIP trunk to Session Manager:

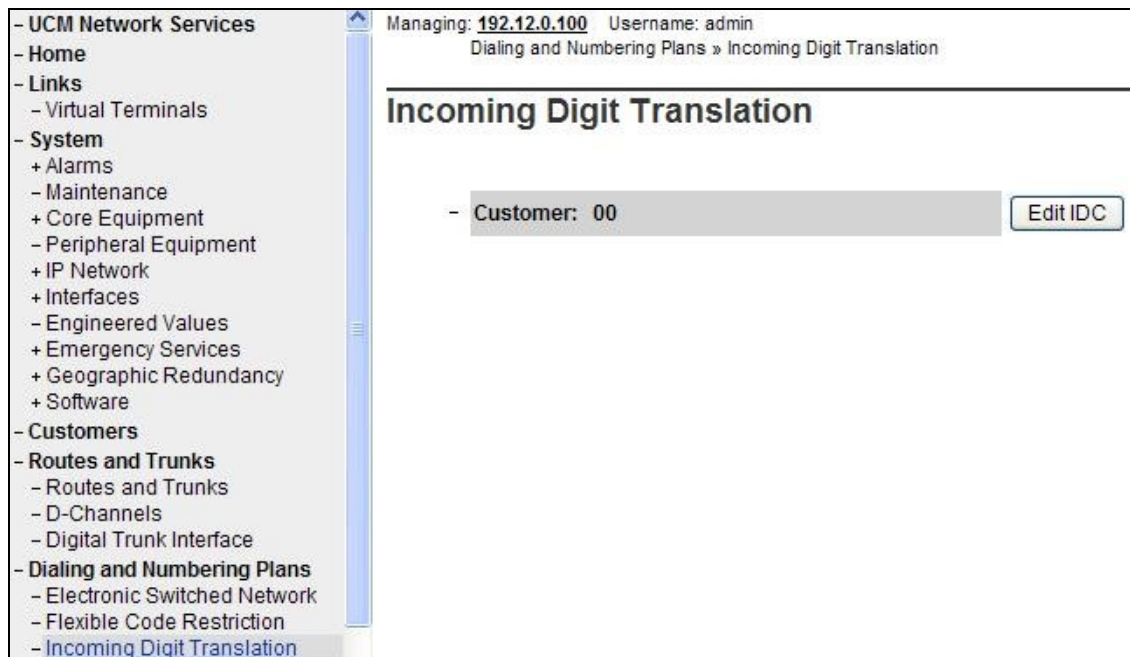
- Routes & Trunks (**Section 5.2.2**)
 - Customer 0
 - Route 16 = SIP trunk
- Route List Block (**Section 5.4.1**)
 - Data 0
 - Route = 16
 - Digit Manipulation = 15
- Digit Manipulation Block 15 (**Section 5.4.2**)
 - Delete = 0
 - Type = NCHG
- ESN Access Codes and Parameters (ESN) (**Section 5.4.3**)
 - NARS/BARS Access Code 1 = 9
- Numbering Plan Area Code NPA (**Section 5.4.4**)
 - 1732xxxxxxx
 - Route list Index = 15
 - Digit Manipulation Block 15
 - Delete = 0
 - Type = NCHG

5.5. Routing of Inbound Numbers to CS1000E

Calls from PSTN will dial AT&T IP Flexible Reach DID numbers to reach stations on the CS1000E. These DID numbers are converted to the associated extensions by the CS1000E Incoming Digit Translation (IDT) table.

Step 1 – Navigate to **Dialing and Numbering Plans → Incoming Digit Translation**

Step 2 – Select the appropriate **Customer ID (00** in the reference configuration) and click on **Edit IDC**.



Step 3 – From the listed Digit Conversion Trees, select either **New DCNO** or edit **DCNO**. In the reference configuration, **Digit Conversion Tree Number: 1** was selected. Note that the Digit Conversion Tree Number selected must also be defined in the Routes and Trunks provisioning shown in **Section 5.2.2, Step 6**.

Managing: 192.12.0.100 Username: admin
Dialing and Numbering Plans » Incoming Digit Translation » Customer 00

Customer 00 Incoming Digit Conversion Property

- Digit Conversion Tree Number: 0	New DCNO
- Digit Conversion Tree Number: 1	Edit DCNO
- Digit Conversion Tree Number: 2	New DCNO
- Digit Conversion Tree Number: 3	New DCNO
- Digit Conversion Tree Number: 4	New DCNO

Refresh Cancel

Step 4 – The IDC Tree form will open. Click on the **Add** button. In the **Incoming Digits** field enter an AT&T IP Flexible Reach DID (e.g. **7323204383**). In the **Converted Digits** field enter the associated CS1000E extension (e.g. **4094**). Click on **Save**.

Add Incoming Digits

Incoming Digits: 7323204383

Converted digits: 4094 (0 - 99999999)

Force storage or removal of data: ☐

In case of conflict between the new and existing Incoming Digits, force storage or removal may result in loss of portions of the tree.

Save Cancel

Step 5 – Repeat **Step 4** for all associated AT&T IP Flexible Reach DIDs and extensions.

Note – This method should not be used to redirect DIDs for PSTN access to the Call Pilot access extension. The procedures described in Section 7.2.9 cover this scenario.

5.6. Zones

Zone configuration can be used to control codec selection and for bandwidth management.

Step 1 - Expand **System** → **IP Network** and select **Zones** as shown below.

Managing: **192.12.0.100** Username: admin
System » IP Network » Zones

Zones

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

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

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

Step 2 - Select **Bandwidth Zones**. In the sample lab configuration, two zones are configured as shown below. In production environments, it is likely that more zones will be required.

Step 3 - Select the zone associated with the virtual trunk to Session Manager (e.g. item **2**, zone **5**) and click **Edit** as shown below.

Bandwidth Zones								
<div>Add... Edit... Import... Export Maintenance... Delete Refresh</div>								
	Zone ▲	Intrazone Bandwidth	Intrazone Strategy	Interzone Bandwidth	Interzone Strategy	Resource Type	Zone Intent	Description
1	3	10000	BQ	10000	BB	SHARED	MO	PHONES
2	5	100000	BQ	100000	BB	SHARED	VTRK	VTRK

Step 4 - In the resultant screen shown below, select **Zone Basic Property and Bandwidth Management**.

Edit Bandwidth Zone

Zone Basic Property and Bandwidth Management

Adaptive Network Bandwidth Management and CAC

Alternate Routing for Calls between IP Stations

Branch Office Dialing Plan and Access Codes

Branch Office Time Difference and Daylight Saving Time Property

Media Services Zone Properties

The following screen shows the **Zone 5** configuration. Note that the **Interzone Strategy** (access to the AT&T network) is set for “**Best Bandwidth (BB)**”. This is so that codec G.729A is preferred over codec G.711MU for calls with the AT&T IP Flexible Reach service.

Zone Basic Property and Bandwidth Management	
Input Description	Input Value
Zone Number (ZONE):	5 * (1 - 8000)
Intrazone Bandwidth (INTRA_BW):	100000 (0 - 10000000)
Intrazone Strategy (INTRA_STGY):	Best Quality (BQ) ▼
Interzone Bandwidth (INTER_BW):	100000 (0 - 10000000)
Interzone Strategy (INTER_STGY):	Best Bandwidth (BB) ▼
Resource Type (RES_TYPE):	Shared (SHARED) ▼
Zone Intent (ZBRN):	VTRK (VTRK) ▼
Description (ZDES):	VTRK

Submit Refresh Cancel

5.7. Codec Parameters.

The following section describes how to set codec preferences as well as setting Packet Interval (PTIME) values. Note that the CS1000E always specifies G.711mu regardless of the additional selected codecs. Codecs are defined in the **Media Gateway** (for analog and digital phones) and in the **IP Telephony Node** for IP (e.g. Unistim) phones.

5.7.1 Media Gateway Codec Configuration

Step 1 - Expand **System** → **IP Network** on the left panel and select **Media Gateways**. Select the appropriate media gateway (e.g. **000 01** as shown in **Section 5.1, Step 2**).

Step 2 - , The **Property Configuration** screen will open as shown in **Section 5.1, Step 3**. Click on “**Next**”.

Step 3 - Scroll down and click on **VGW and IP phone codec profile**.

Hostname *

- DSP Daughterboard 2

Type of the DSP daughterboard

Telephony LAN (TLAN) IP address

Telephony LAN (TLAN) gateway IP address

Telephony LAN (TLAN) IPv6 address

Telephony LAN (TLAN) subnet mask

Hostname *

+ VGW and IP phone codec profile

+ QoS

+ Media Based CLID

Step 4 - The **VGW and IP phone codec profile** section will expand. Scroll down, click on and expand the **Codec G711** field. Note that the “Select” box is checked by default. Set the **Voice payload size** (PTIME) to **30**.

- Codec G711 ☒ **Select**

Codec name

Voice payload size (ms/frame)

Voice playout (jitter buffer) nominal delay

Modifications may cause changes to dependent settings

Voice playout (jitter buffer) maximum delay

Modifications may cause changes to dependent settings

VAD ☐

Step 5 – Scroll down, click on and expand the **Codec G727A** field. Check the selection box and set the **Voice payload size** (PTIME) to **30**.

Note – Although not set in the reference configuration, annexB=yes may be enabled by selecting the **VAD** (Voice Activity Detection) box.

- Codec G729A ☒ **Select**

Codec name

Voice payload size (ms/frame)

Voice playout (jitter buffer) nominal delay

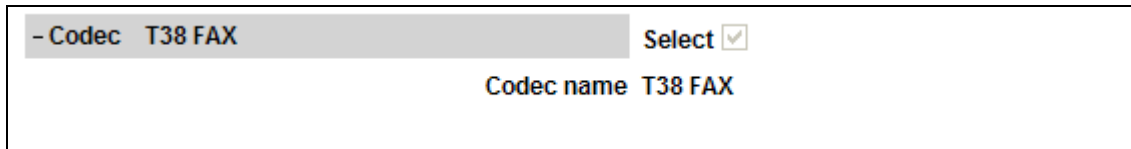
Modifications may cause changes to dependent settings

Voice playout (jitter buffer) maximum delay

Modifications may cause changes to dependent settings

VAD ☐

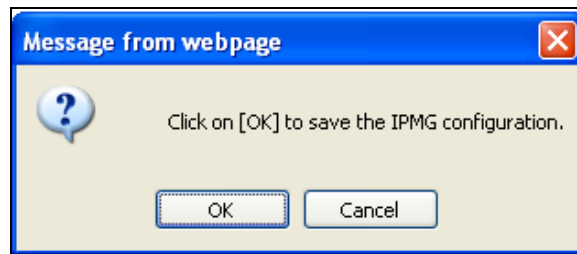
Step 6 – Scroll down and click on **Codec T.38 FAX**. Note that T.38 is enabled by default.




The screenshot shows a web interface for selecting a codec. A dropdown menu is open, displaying '- Codec T38 FAX'. To the right of the dropdown is a 'Select' button with a checkmark icon. Below the dropdown, the text 'Codec name T38 FAX' is displayed.

Step 7 – If changes are made to any of these settings, click on **Save** (not shown).

Step 8 – A dialog box will open. Click on **Ok**.



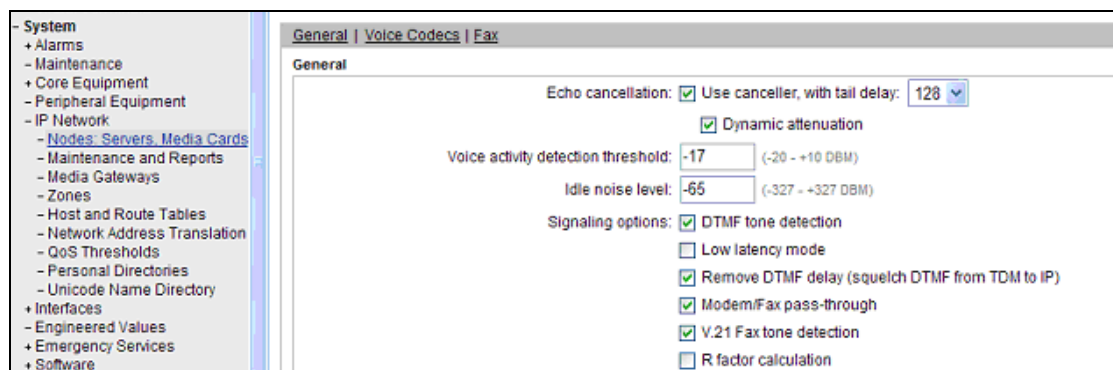
Step 9 –Select  next to the Media Gateway ID (e.g. 000 01), and click on the **Reboot** button. The Media Gateway will reboot and deploy the new configuration.



5.7.2 IP Telephony Node Codec Configuration

Step 1 – As shown in Section 5.1, Step 1 expand **System** → **IP Network**, select **Node**, **Server**, **Media Cards**, and select **IP Telephony Node Id “1001”**.

Step 2 – Scroll down the upper half of the form and under the **IP Telephony Node Properties** heading, select **Voice Gateway (VGW) and Codecs** (not shown). The following screen shows the **General** parameters used in the sample configuration.



Step 2 - Use the scroll bar on the right to find the area with heading **Voice Codecs**. Set the **Voice payload size** to **30**. Note that **Codec G.711** is enabled by default.

Voice Codecs

Codec G711: ☒ Enabled (required)

Voice payload size: 30 (milliseconds per frame)

Voice playout (jitter buffer) delay: 60 120 (milliseconds)

Nominal Maximum

Maximum delay may be automatically adjusted based on nominal settings.

☐ Voice Activity Detection (VAD)

Step 3 – Scroll down to the G729 codec and check the selection box. Set the **Voice payload size** to **30**.

Note – Although not set in the reference configuration, annexB=yes may be enabled by selecting the **VAD (Voice Activity Detection)** box.

Codec G729: ☒ Enabled

Voice payload size: 30 (milliseconds per frame)

Voice playout (jitter buffer) delay: 60 120 (milliseconds)

Nominal Maximum

Maximum delay may be automatically adjusted based on nominal settings.

☐ Voice Activity Detection (VAD)

Step 4 - Scrolling further down, note that T.38 fax is enabled by default. Verify the **Maximum Rate** is set to **14400**.

Fax

Codec name: T.38 FAX

Maximum rate: 14400 (bps)

Fax TCF method: 2

Fax playout nominal delay: 100 (0 - 300 milliseconds)

FAX no activity timeout: 20 (10 - 32000 milliseconds)

Packet size: 30 (bps)

Step 5 – Click on **Save** and then follow **Steps 8 through 12** in **Section 5.3** to save the configuration.

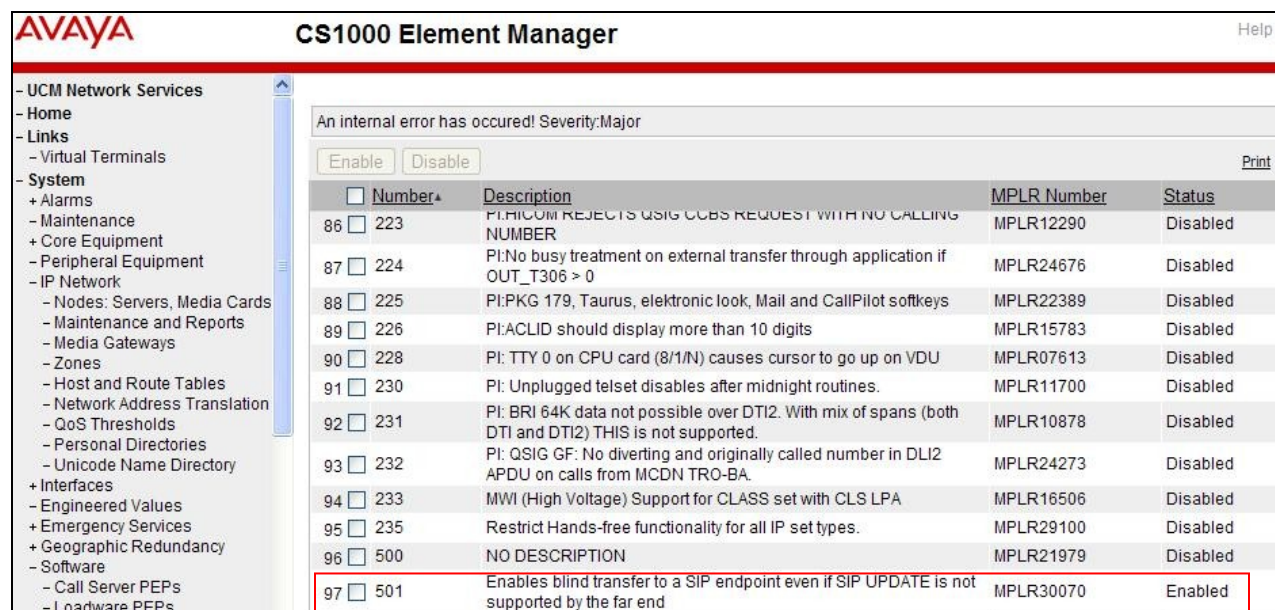
5.8. Enabling Plug-Ins for Call Transfer Scenarios

Plug-ins allow specific CS1000E software feature behaviors to be changed. In the testing associated with these Application Notes, plug-in 501 was required for successful completion of Unattended Transfer calls (see **Section 2.2.1**).

Step 1 - To view or enable a plug-in, from the left navigation menu, expand **System** → **Software**, and select **Plug-ins** (not shown). In the right side screen, a list of available plug-ins will be displayed along with the associated MPLR Number and Status. Use the scroll bar on the right to scroll down so that Plug-in “501” is displayed as shown in the screen below.

Step 2 - If the **Status** is “Disabled”, select the check-box next to Number 501 and click the **Enable** button.

Note - Enabling plug-in 501 will allow the user to complete the transfer while the call is in a ringing state, but no audible ring back tone will be heard after the transfer is completed. Without plug-in 501 enabled, Unattended Transfer will not work.



The screenshot shows the AVAYA CS1000 Element Manager interface. On the left is a navigation tree with categories like UCM Network Services, System, and Interfaces. The main area displays a table of plug-ins. A message at the top states 'An internal error has occurred! Severity:Major'. Below this are 'Enable' and 'Disable' buttons. The table has columns for Number, Description, MPLR Number, and Status. Plug-in 501 is highlighted with a red box, showing it is enabled.

Number	Description	MPLR Number	Status
86 223	PLR1000 REJECTS QSIG CUBS REQUEST WITH NO CALLING NUMBER	MPLR12290	Disabled
87 224	PI: No busy treatment on external transfer through application if OUT_T306 > 0	MPLR24676	Disabled
88 225	PI: PKG 179, Taurus, elektronick look, Mail and CallPilot softkeys	MPLR22389	Disabled
89 226	PI: ACLID should display more than 10 digits	MPLR15783	Disabled
90 228	PI: TTY 0 on CPU card (8/1/N) causes cursor to go up on VDU	MPLR07613	Disabled
91 230	PI: Unplugged telset disables after midnight routines.	MPLR11700	Disabled
92 231	PI: BRI 64K data not possible over DTI2. With mix of spans (both DTI and DTI2) THIS is not supported.	MPLR10878	Disabled
93 232	PI: QSIG GF: No diverting and originally called number in DLI2 APDU on calls from MCDN TRO-BA.	MPLR24273	Disabled
94 233	MWI (High Voltage) Support for CLASS set with CLS LPA	MPLR16506	Disabled
95 235	Restrict Hands-free functionality for all IP set types.	MPLR29100	Disabled
96 500	NO DESCRIPTION	MPLR21979	Disabled
97 501	Enables blind transfer to a SIP endpoint even if SIP UPDATE is not supported by the far end	MPLR30070	Enabled

5.9. Customer Information

In the reference configuration, specific calling number information is required based on the destination of the call. For Calls to the AT&T IP Flexible Reach service, AT&T assigned DID's are required.

5.9.1 Calling Number Provisioning for call to the AT&T IP Flexible Reach Service

The AT&T IP Flexible Reach service expects to see service assigned DID (Direct Inward Dialing) numbers in the SIP origination headers (e.g. From and PAI). In the reference configuration these were 10 digit numbers associated with the local NPA (Note – For security, sample numbers are shown in this document).

Step 1 - Select **Customers** from the left navigation menu, click on the appropriate **Customer Number** (e.g. **00**)

The screenshot shows the AVAYA CS1000 Element Manager web interface. On the left is a navigation menu with categories like UCM Network Services, Home, Links, System, and Customers. The main area displays the 'Customers' page with a table listing customer information. The first row shows a customer with number '00', 10 total routes, and 36 total trunks. The '00' is highlighted with a red box.

Customer Number	Total Routes	Total Trunks
1 00	10	36

Step 2 – The Customer Details screen will open. Select **ISDN and ESN Networking**.

The screenshot shows the 'Customer Details' screen with a list of configuration options. The option 'ISDN and ESN Networking' is highlighted with a red box.

- Basic Configuration
- Application Module Link
- Attendant
- Call Detail Recording
- Call Party Name Display
- Call Redirection
- Centralized Attendant Service
- Controlled Class of Service
- Features
- Feature Packages
- Flexible Feature Codes
- Intercept Treatments
- ISDN and ESN Networking**
- Listed Directory Numbers
- Media Services Properties
- Mobile Service Directory Numbers
- Multi-Party Operations
- Night Service

The ISDN and ESN Networking screen will open. As a reference, the following screen shows the **General Properties** used in the reference configuration.

General Properties

Flexible trunk to trunk connection option:

Flexible orbiting prevention timer:

Country code: (0 - 9999)

Code for processing the called number

National access code:

International access code:

Options: ☐ Transfer on ringing of supervised external trunks

☒ Connection of supervised external trunks

Network option: ☐ Coordinated dialing plan routing

Integrated services digital network: ☒

Microsoft converged office dialing plan:

Private dialing plan for non-DID users: ☐ Coordinated dialing plan

☐ Uniform dialing plan

Step 3 - Scroll down from **General Properties** to the **Calling Line Identification** section and note the value in the **Size** parameter (e.g. **256**).

Step 4 - Click the **Calling Line Identification Entries** link.

Integrated services digital network: ☒

Microsoft converged office dialing plan:

Private dialing plan for non-DID users: ☐ Coordinated dialing plan

☐ Uniform dialing plan

Calling Line Identification

Information for incoming/outgoing calls:

Size: (0 - 4000)

Country code: (0 - 9999)

Code displayed as part of calling number

[Calling Line Identification Entries](#)

The **Calling Line Identification Entries** page will open.

Step 5 – In the **Search for CLID** section, enter “0” (zero) in the **Start range** field and in the **End range** field enter one less than the **Size** value from **Step 3** above (e.g. enter **255**). Click on **Search**.

AVAYA CS1000 Element Manager

Managing: 192.12.0.100 Username: admin
Customers » Customer 00 » Customer Details » ISDN and ESN Networking » Calling Line Identification Entries

Calling Line Identification Entries

Search for CLID

Start range : 0
End range : 255
'End range' should not exceed the CLID size specified

Search

Calling Line Identification Entries

Add... Delete

This will display all defined Call Ids. For example CLID 0 will use 732-320-4097

Calling Line Identification Entries

Search for CLID

Start range :
End range :
'End range' should not exceed the CLID size specified

Search

Calling Line Identification Entries

Add... Delete Refresh

	<input type="checkbox"/> Entry ID ▲	National Code	Local Code	Home location code	Local steering code	Use DN as DID	Emergency Local Code
1	<input type="checkbox"/> 0	732	3204097			NO	
2	<input type="checkbox"/> 1	732	3204098			NO	
3	<input type="checkbox"/> 2	732	3204383			NO	
4	<input type="checkbox"/> 3	732	3204384			NO	
5	<input type="checkbox"/> 4	732	3204385			NO	
6	<input type="checkbox"/> 5	732	3204386			NO	

Click on any Entry ID to view or change further details (e.g. **Entry ID 5**).

Note that the **Use DN as DID** is set to **NO**. This means that the local extension will not be used for the calling number.

Managing: 192.12.0.100 Username: admin
 Customers » Customer 00 » Customer Details » ISDN and ESN Networking » Calling Line Identification Entries » Edit Calling Line Identification 5

Edit Calling Line Identification 5

General Properties

National Code: (0 - 999999)
 Code for national home number

Local Code: (1-12 digits)
 Code for home local number or listed DN

Local Steering Code: (1-7 digits)

Use DN as DID: ▼

Emergency Services Access

Emergency Local Code: (1-12 digits)
 Code for home local number during Emergency calls

Emergency Options: ☐ Home national number for emergency services access calls
☒ Append the originating directory number for emergency services access calls

Calling Party Name Display

Roman characters: ☒

CPND Name: -
 first name, last name

Expected Length: 24

Display Format: ▼

Call IDs are then associated with specific telephone directory numbers (DNs). See **Section 5.9.1.2.1**.

5.9.1.1 Summary

In summary, to have CS1000E insert the AT&T DID in the origination headers for calls to AT&T via the SIP trunk to Session Manager:

- Customers = 00 (**Section 5.8.1**)
 - ISDN & ESN Networking
 - Calling Line Identification Entries
 - CLID Search
 - Start = 1
 - End = 255
 - Entry ID 5
 - National code = 732
 - Local code - 3204386
 - Use DN as DID = NO
- Phones (**Section 5.9.1**)
 - DN 4094 (select TN)
 - Key 0
 - CLID = 5

5.10. CS1000E Stations

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

5.10.1 Example IP UNISTim Phone DN 4094,

The following screen shows basic information for an IP UNISTim phone in the reference configuration.

Step 1 – Select **Phones** from the menu. The **Search For Phones** screen will open.

Step 2 - Select **Criteria = Prime DN** and enter a DN in the value field (e.g. **4094**). Click on **Search**.

Step 3 – Click on the TN value (e.g. **096 0 01 03**). The **Phone Details** form will open. Note that the telephone type is an 1140 and that it is defined in Zone 3. A call between this telephone and another telephone in Zone 3 will use a “best quality” strategy (see **Section 5.5**) and therefore can use G.711MU. If this same telephone calls out to the PSTN via the SIP trunk, the call would use a “best bandwidth” strategy, and the call would use G.729A.

Note – SIP trunk calls to the AT&T IP Flexible Reach network will use Zone 5, as defined in **Section 5.6**.

The screenshot displays the AVAYA CS1000 Element Manager web interface. On the left is a navigation tree with categories like UCM Network Services, System, Customers, Routes and Trunks, Dialing and Numbering Plans, Phones, and Tools. The 'Phones' category is selected. The main area is titled 'Phone Details' and contains a phone icon, system information (System: EM on cots1, Phone Type: 1140, Sync Status: TRN), and tabs for General Properties, Features, Keys, and User Fields. The 'General Properties' tab is active, showing fields for Customer Number (0), Terminal Number (096 0 01 03), Designation (NUL), Zone (3), and Key Expansion Modules (0). A 'Custom View' dropdown is set to 'All'. The footer includes a copyright notice: Copyright © 2002-2011 Avaya Inc. All rights reserved.

5.10.1.1 Features

Scroll further down the **Phone Details** form and locate the **Features** section of the form. In this section various CS1000E telephone features are defined. All of the features described below are found by scrolling through this section.

Features		
Feature	Description	Value:
AAA	Automatic Answer Back	Denied
AACS	Application Acquire Request	NO
ABDA	CDR on Abandoned Calls	Denied
ADAY	Alternate Redirection by Day Option	

5.10.1.1.1 Requesting Privacy

One means to have a CS1000E station request privacy (e.g. Privacy: id header in SIP INVITE) for an outbound call, is to set **CLBA Calling Party Privacy** to “Allowed” via the Phone **Features** in Element Manager as shown below.

Feature	Description	Value:
CFTA	Call Forward by Call Type	Denied
CFXA	Call Forward External	Allowed
CLBA	Calling Party Privacy	Allowed
CLRO	Calling Number Restriction Override	Denied
CLS	Trunk/Call Type Access Restriction	Unrestricted

Note - Another means to have the CS1000E request privacy (i.e., Privacy: id in SIP INVITE) for an outbound call is to set **DDGA Present/Restrict Calling Number** to “Denied” (not shown).

5.10.1.1.2 Call coverage to Call Pilot

Step 1 – Set the FDN (Flexible Call Forward No Ans DN) feature to the Call Pilot access extension (e.g. **2080**).

Step 2 – Set the **FNA** (Call Forward No Answer) feature to **Allowed**.

Step 3 – Set the **Hunt** (Hunt DN - All Calls, or Internal Calls for CFTA) feature to the Call Pilot access extension (e.g. **2080**).

Note - The phone Key **MWK** (Message Waiting) is also required (see **Section 5.9.1.2.3** below).

5.10.1.2 Keys

Scroll further down the **Phone Details** form and locate the **Keys** section of the form. Phone key positions (buttons) are defined in this section.

5.10.1.2.1 Key 0 - Single Call Appearance

This key defines the first call appearance on the telephone.

Note – The **CLID Entry (Numeric or D)** field is where the CLID defined in **Section 5.8** is associated with this station. In the reference configuration telephone station 4094 was assigned CLID 5 and therefore will use 7323204386 as its calling number.

Key No.	Key Type	Key Value								
0	SCR - Single Call Ringing	<div>Directory Number: 4094</div> <div><input checked="" type="checkbox"/> Multiple Appearance Redirection Prime(MARP)</div> <div><table border="1"><tr><td>First Name</td><td>Last Name</td><td>Display Format</td><td>Language</td></tr><tr><td>Groucho</td><td>Marx</td><td>First, Last</td><td>Roman</td></tr></table></div> <div>CLID Entry (Numeric or D): 5</div> <div>ANIE Entry: </div>	First Name	Last Name	Display Format	Language	Groucho	Marx	First, Last	Roman
First Name	Last Name	Display Format	Language							
Groucho	Marx	First, Last	Roman							

5.10.1.2.2 Key 2 – Message Waiting Indicator

This defines the MWI lamp.

Key No.	Key Type
2	MIK - Message Waiting Indication

5.10.1.2.3 Key 16 - Message Waiting

This key defines the extension CS1000E will dial to reach the messaging system.

Key No.	Key Type	Key Value
16	MWK - Message Waiting	<div>Message Center DN: 2080</div> <div><input type="checkbox"/> Multiple Appearance Redirection Prime(MARP)</div>

5.10.1.2.4 Key 19 - Forward All Calls


This key defines an alternate destination to redirect inbound calls to this station.

19	CFW - Forward All Calls	Redirection DN Length	16
		Redirection DN	917325553903

5.10.2 Analog Fax Line

The following screen shows basic information for an analog port in the configuration that may be used with a fax machine. The port is configured as Directory Number 2779. No special Features or Keys were defined.

Phone Details



System: EM on cots1
Phone Type: 2500
Sync Status: TRN

General Properties | Features | Single Line Features | User Fields

Custom View: All

General Properties

Customer Number: 0 *

Terminal Number: 000 1 10 00

Designation: ANALOG * (1-6 characters)

Directory Number: 2779

CLID entry:

5.11. Changing RFC2833 DTMF Telephone Event Type

The CS1000E uses RFC2833 DTMF Telephone Event type 101 by default. The AT&T IP Flexible Reach service uses 100. While having asymmetric telephone event types is permitted, this may cause issues in some call scenarios. If an issue occurs, the CS1000E value may be changed to 100 as follows:

Step 1 – From a CS1000E console connection (e.g. serial interface), press the ctrl key and enter “pdt”. The system will return:

```
PDT login on /tyCo/0
```

Username:

Step 2 – Enter the appropriate login. The system will respond with:

Password:

Step 3 – Enter the appropriate password. The system will respond as follows:

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

Step 4 – At the pdt> prompt enter “**setRFC2833PT 100**”

```
pdt> setRFC2833PT 100
```

The system will respond with the pdt> prompt.

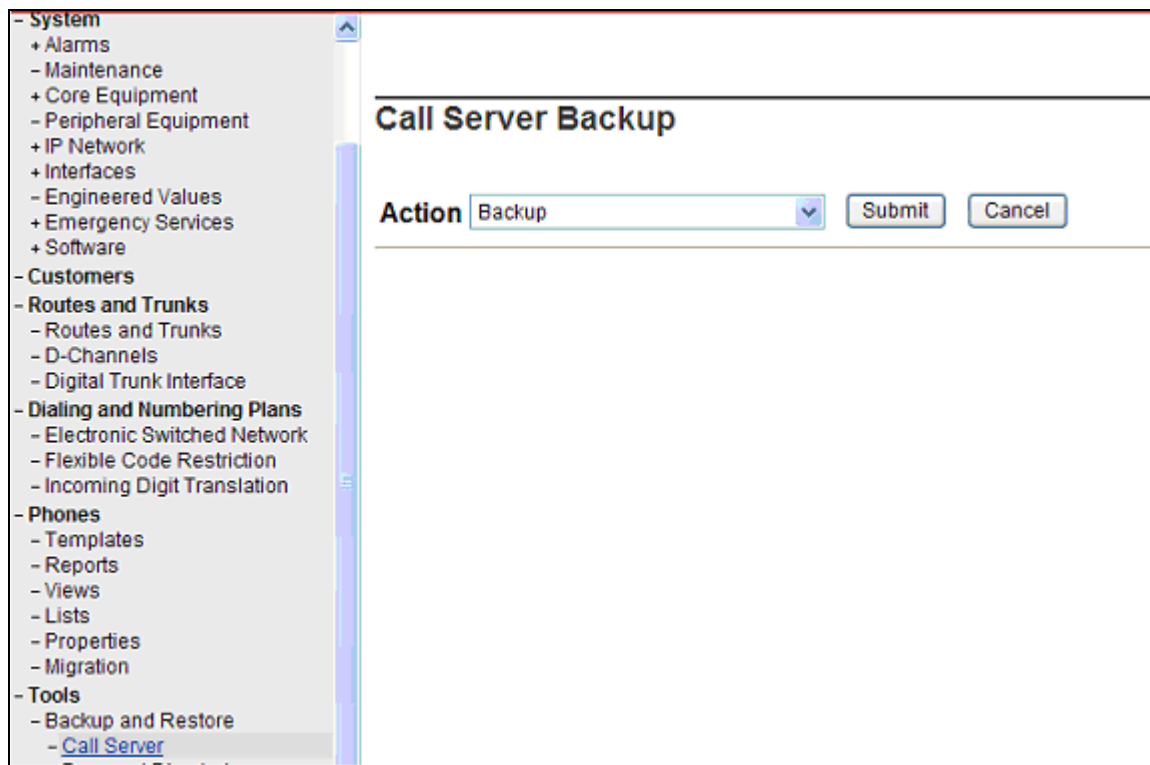
```
pdt>
```

The CS1000E will now use RFC2833 DTMF telephone event type 100.

NOTE – If the CS1000E is rebooted, this command will be cleared and the system will use telephone event 101 again. This command must be re-entered.

5.12. Configuration Backup

Expand **Tools** → **Backup and Restore** on the left navigation panel and select **Call Server**. Select **Backup** and click **Submit** to save configuration changes as shown below.



The backup process may take several minutes to complete. Scroll to the bottom of the page to verify the backup process completed successfully as shown below.

```
Backing up reten.bkp to "/var/opt/nortel/cs/fs/cf2/backup/single"  
Database backup Complete!  
TEMU207  
Backup process to local Removable Media Device ended successfully.
```

The configuration of Avaya Communication Server 1000E is complete.

6. Configure Avaya Aura® Session Manager Release 6.1

This section illustrates relevant aspects of the Session Manager configuration used in the verification of these Application Notes.

Note – The following sections assume that Session Manager and System Manager have been installed and that network connectivity exists between the two. For more information, consult the references in **Section 12**.

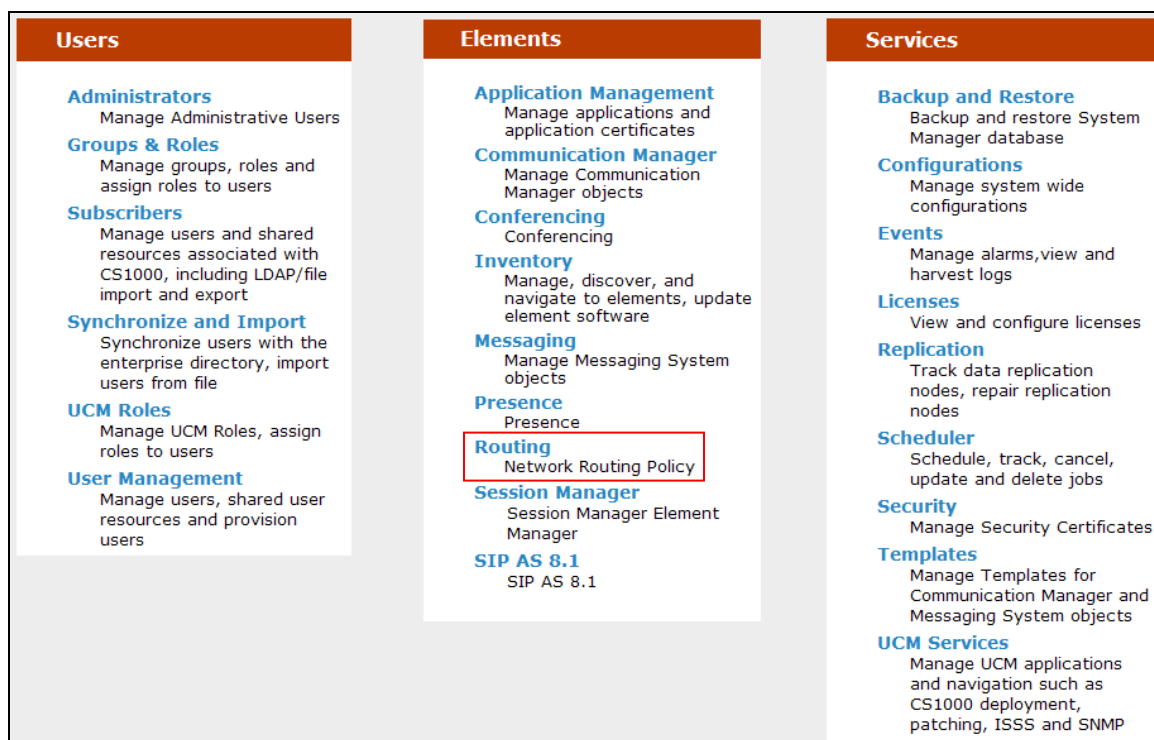
This section provides the procedures for configuring Session Manager to receive calls from and route calls to the SIP trunk between Avaya Communication Server 1000E and Session Manager, and the SIP trunk between Session Manager and the Avaya Aura® SBC.

The following administration activities will be described:

- Define SIP Domain
- Define Locations for Avaya Communication Server 1000E and for the SBC
- Configure the Adaptation Modules that will be associated with the SIP Entities for Avaya Communication Server 1000E and the SBC
- Define SIP Entities corresponding to Avaya Communication Server 1000E and the SBC
- Define Entity Links describing the SIP trunk between Avaya Communication Server 1000E and Session Manager, and the SIP Trunk between Session Manager and the SBC.
- Define Routing Policies associated with the Avaya Communication Server 1000E and the SBC.
- Define Dial Patterns, which govern which routing policy will be selected for call routing.

Configuration is accomplished by accessing the browser-based GUI of Avaya Aura® System Manager, using the URL “<http://<ip-address>/SMGR>”, where <ip-address> is the IP address of Avaya Aura® System Manager. Log in with the appropriate credentials.

In the **Log On** screen (not shown), enter appropriate **User ID** and **Password** and press the **Log On** button. Once logged in, a Release 6.1 **Home** screen like the following is displayed. From the **Home** screen below, under the **Elements** heading in the center, select **Routing**.



The screen shown below shows the various sub-headings of the left navigation menu that will be referenced in this section.

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

6.1. SIP Domain

Step 1 - Select **Domains** from the left navigation menu. In the reference configuration domain “cots1.ntlab.com” was defined.

Step 2 - Click **New** (not shown). Enter the following values and use default values for remaining fields.

- **Name** Enter the enterprise SIP Domain Name. In the sample screen below, “cots1.ntlab.com” is shown.
- **Type** Verify “SIP” is selected.
- **Notes** Add a brief description. [Optional]

Avaya Aura® System Manager 6.1

Help | About | Change Password | Log off admin

Routing x Home

▼ Routing

Domains

Locations

Adaptations

SIP Entities

Entity Links

Time Ranges

Routing Policies

Dial Patterns

Regular Expressions

Defaults

Home / Elements / Routing / Domains - Domain Management

Domain Management

Help ?

Commit Cancel

1 Item Refresh Filter: Enable

Name	Type	Default	Notes
* cots1.ntlab.com	sip	<input type="checkbox"/>	CS1K

* Input Required

Commit Cancel

Step 3 - Click **Commit** to save.

Note - Multiple SIP Domains may be defined if required.

6.2. Locations

Locations are used to identify logical and/or physical locations where SIP Entities reside. Location identifiers can be defined in a broad scope (e.g. 192.168.10.x for all devices on a particular subnet), or individual devices (e.g. 192.168.10.10 for a devices' IP address). In the

reference configuration, the CS1000E, and the Avaya Aura® SBC were each defined as individual Locations.

6.2.1 Location for Avaya Communication Server 1000E

Step 1 - Select **Locations** from the left navigational menu. Click **New** (not shown). In the **General** section, enter the following values and use default values for remaining fields.

- **Name:** Enter a descriptive name for the location.
- **Notes:** Add a brief description. [Optional]

Step 2 - In the **Location Pattern** section, click **Add** and enter the following values.

- **IP Address Pattern** Enter the IP Address or IP Address pattern used to identify the CS1000E location (e.g. **172.16.6.110**).
- **Notes** Add a brief description. [Optional]

Step 3 - Click **Commit** to save.

The screen below shows the top portion of the screen for the Location defined for Avaya Communication Server 1000E.

AVAYA

Avaya Aura® System Manager 6.1

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

Routing

Home

Routing

Domains

Locations

Adaptations

SIP Entities

Entity Links

Time Ranges

Routing Policies

Dial Patterns

Regular Expressions

Defaults

Home / Elements / Routing / Locations - Location Details

Location Details

Commit

Cancel

Help ?

General

* Name:

CS1K

Notes:

Overall Managed Bandwidth

Managed Bandwidth Units:

Kbit/sec

Total Bandwidth:

Multimedia Bandwidth:

Audio Calls Can Take Multimedia Bandwidth:

☒

Per-Call Bandwidth Parameters

Maximum Multimedia Bandwidth (Intra-Location):

1000

Kbit/Sec

Maximum Multimedia Bandwidth (Inter-Location):

1000

Kbit/Sec

Minimum Multimedia Bandwidth:

64

Kbit/Sec

* Default Audio Bandwidth:

80

Kbit/sec

Location Pattern

Add

Remove

1 Item

Refresh

Filter: Enable

<input type="checkbox"/>	IP Address Pattern	Notes
<input type="checkbox"/>	* 172.16.6.110	

Select : All, None

* Input Required

Commit

Cancel

6.2.2 Location for the Avaya Aura® Session Border Controller

Step 1 - Select **Locations** from the left navigational menu. Click **New** (not shown). In the **General** section, enter the following values and use default values for remaining fields.

- **Name:** Enter a descriptive name for the location.
- **Notes:** Add a brief description. [Optional]

Step 2 - In the **Location Pattern** section, click **Add** and enter the following values.

- **IP Address Pattern** Enter the IP Address or IP Address pattern used to identify the Avaya Aura® SBC location (e.g. **192.168.67.125**).
- **Notes** Add a brief description. [Optional]

Step 3 - Click **Commit** to save.

AVAYA

Avaya Aura® System Manager 6.1

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

Routing

Home

Routing

Domains

Locations

Adaptations

SIP Entities

Entity Links

Time Ranges

Routing Policies

Dial Patterns

Regular Expressions

Defaults

Home / Elements / Routing / Locations - Location Details

Location Details

Commit

Cancel

Help ?

General

* Name:

AA-SBC

Notes:

Overall Managed Bandwidth

Managed Bandwidth Units:

kbit/sec

Total Bandwidth:

Multimedia Bandwidth:

Audio Calls Can Take Multimedia Bandwidth:

☒

Per-Call Bandwidth Parameters

Maximum Multimedia Bandwidth (Intra-Location):

1000

Kbit/Sec

Maximum Multimedia Bandwidth (Inter-Location):

1000

Kbit/Sec

Minimum Multimedia Bandwidth:

64

Kbit/Sec

* Default Audio Bandwidth:

80

Kbit/sec

Location Pattern

Add

Remove

1 Item

Refresh

Filter: Enable

<input type="checkbox"/>	IP Address Pattern	Notes
<input type="checkbox"/>	* 192.168.67.125	

Select : All, None

* Input Required

Commit

Cancel

6.3. Configure Adaptations

Session Manager can be configured to use an Adaptation Module designed for Avaya Communication Server 1000E to convert SIP headers in messages sent by Avaya Communication Server to the format used by other Avaya products and endpoints. In the reference configuration the following adaptations was used.

- DiversionTypeAdapter** – This adaptation is used to convert History-Info headers sent by the CS1000E in certain outbound calls to AT&T (which are not supported by the AT&T IP Flexible Reach service), to Diversion Headers. This is required for call scenarios such as Call Forwarding.
- CS1000Adapter** – This adaptation is used to provide translation between CS1000E generated History-Info headers into formats used by other Avaya products and endpoints.

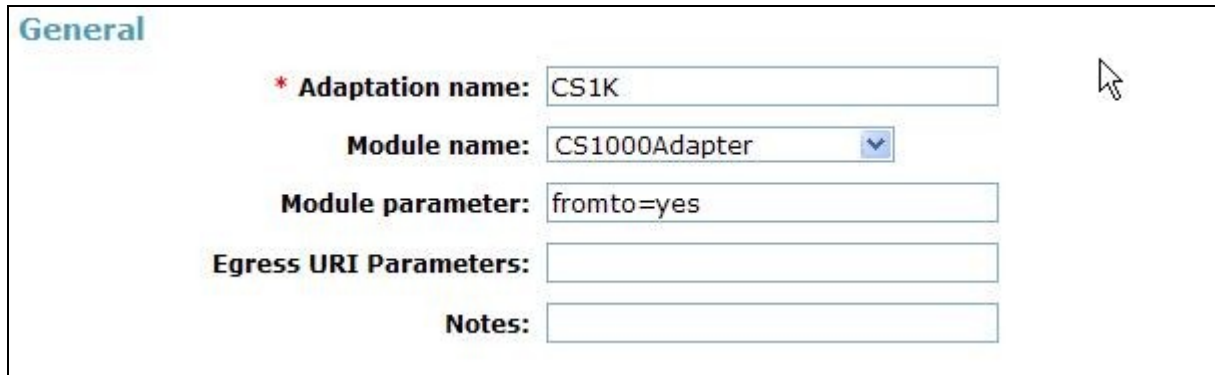
- **DigitConversionAdapter** – This adaptation is used to modify digit strings in the Request-URI. Note that the adaptation functionality is included in all other adaptations.

In addition, Module parameters **odstd** (to modify destination domain or IP addressing), **osrcd** (to modify source domain or IP addressing, **MIME=no** (to remove unnecessary CS1000K SIP headers), and **fromto=yes** (to modify the From and To header) are specified.

6.3.1 Adaptation for Avaya Communication Server 1000E Entity

Step 1 - Select **Adaptations** from the left navigational menu. Click **New** (not shown). In the **General** section, enter the following values and use default values for remaining fields.

- **Adaptation Name:** Enter an identifier for the Adaptation Module (e.g., “CS1000”)
- **Module Name:** Select “CS1000Adapter” from drop-down menu (or add an adapter with name “CS1000Adapter” if not previously defined)
- **Module Parameter:** Enter **fromto=yes** (Note – this parameter is set so that the correct To header information is provided for calls to Call Pilot).



The screenshot shows a configuration window titled "General". It contains the following fields:

- * Adaptation name:** A text input field containing "CS1K".
- Module name:** A dropdown menu showing "CS1000Adapter".
- Module parameter:** A text input field containing "fromto=yes".
- Egress URI Parameters:** An empty text input field.
- Notes:** An empty text input field.

Step 2 - Scrolling down, in the **Digit Conversion for Incoming Calls To SM** section, click **Add** to configure entries for calls from CS1000E users to AT&T. The text below and the screen example that follows explain how to use Session Manager to convert between CS1000K extensions and AT&T IP Flexible Reach DIDs.

- **Matching Pattern** Enter a CS1000E extension (e.g. 4094).
- **Min** Enter minimum number of digits (e.g. 4)
- **Max** Enter maximum number of digits (e.g. 4)
- **Phone Context** Leave blank.
- **Delete Digits** Enter “4”, to remove the CS1000E extension digits.
- **Insert Digits** Enter the corresponding AT&T IP Flexible Reach DID(e.g. 7323204383).
- **Address to modify** Select “both”.

Repeat for any addition CS1000E extensions.

Digit Conversion for Incoming Calls to SM

Add Remove

4 Items Refresh Filter: Enable

<input type="checkbox"/>	Matching Pattern ▲	Min	Max	Phone Context	Delete Digits	Insert Digits	Address to modify	Notes
<input type="checkbox"/>	* 4093	* 4	* 4		* 4	7323204385	both ▼	
<input type="checkbox"/>	* 4094	* 4	* 4		* 4	7323204383	both ▼	
<input type="checkbox"/>	* 4095	* 4	* 4		* 4	7323204385	both ▼	

Select : All, None

Step 3 - Scrolling down, in the **Digit Conversion for Outgoing Calls from SM** section, click **Add** to configure entries for calls from AT&T to access the integrated Call Pilot messaging system. The text below and the screen example that follows explain how to use Session Manager to convert between inbound AT&T IP Flexible Reach DIDs and CS1000K/Call Pilot extension (2090).

- **Matching Pattern** Enter AT&T IP Flexible Reach DIDs (e.g. **7323204384**).
- **Min** Enter minimum number of digits (e.g. 10)
- **Max** Enter maximum number of digits (e.g. 10)
- **Phone Context** Leave blank.
- **Delete Digits** Enter “10”, to remove the AT&T DID digits.
- **Insert Digits** Enter the corresponding Call Pilot extension (e.g. **2090**).
- **Address to modify** Select “both”.

Repeat for any addition AT&T DID access to Call Pilot.

Digit Conversion for Outgoing Calls from SM

Add Remove

Filter: Enable

<input type="checkbox"/>	Matching Pattern ▲	Min	Max	Phone Context	Delete Digits	Insert Digits	Address to modify	Notes
<input type="checkbox"/>	* 3143325386	* 10	* 10		* 10	2090	both ▼	Call Pilot
<input type="checkbox"/>	* 4386	* 4	* 4		* 4	2090	both ▼	Call Pilot
<input type="checkbox"/>	* 7323204384	* 10	* 10		* 10	2090	both ▼	Call Pilot

Select : All, None

6.3.2 Adaptation for the Avaya Aura® SBC Entity

The message body of an INVITE message sent from the CS1000E will contain a MIME Multipart message body containing the SDP information expected by AT&T, but also containing “x-nt-mcdn-frag-hex” and “x-nt-epid-frag-hex” application parts that are not processed by AT&T. On the production circuit used for testing, AT&T was able to properly parse the Multipart MIME message body, and outgoing calls from the CS1000E to AT&T could be completed successfully without the configuration in this section. Nevertheless, since AT&T has no use for this information, the Module Parameter MIME=no was used in the reference configuration to remove

these headers. Note that the Avaya Aura® SBC can be configured to remove these headers as well (see **Section 7.2.5**). Either method is acceptable.

Step 1 - Select **Adaptations** from the left navigational menu. Click **New** (not shown). In the **General** section, enter the following values and use default values for remaining fields.

- **Adaptation Name:** Enter an identifier for the Adaptation Module
- **Module Name:** Select “**DiversionTypeAdapter**” from drop-down menu (or add an adapter with name “DiversionTypeAdapter” if not previously defined)
- **Module Parameter:** Enter the following three parameters separated by spaces.
 - Enter “**odstd**=<IP address of the public interface of the Avaya Aura® SBC>” (e.g. **odstd=135.25.29.74**).
 - Enter “**osrcd**=<IP address of the AT&T IP Flexible Reach border element>” (e.g. **osrcd=192.168.64.130**).
 - Enter “**MIME=no**” to remove additional MIME Media Type headers that the CS1000E adds to its SIP signaling.

The entire Module parameter string will appear as:

odstd=135.25.29.74 osrcd=192.168.64.130 MIME=no

Note that the entire entry is not visible in the screenshot below.

Adaptation Details [Commit] [Cancel]

General

* **Adaptation name:** CS1K_AT&T_AA-SBC

Module name: DiversionTypeAdapter ▼

Module parameter: odstd=135.25.29.74 osrcd=192.168.64.130 MIME=no

Egress URI Parameters:

Notes: CS1K_outbound to AT&T via AA-SBC

Note – Neither **Digit Conversion for Incoming Calls to SM** or **Conversion for Outgoing Calls from SM Digit** were required in the reference configuration for the Avaya Aura® SBC SIP Entity.

Step 2 - Click **Commit**.

6.3.3 List of Adaptations

Select **Adaptations** from the left navigational menu. The completed list of the Adaptation Modules defined for the sample configuration is shown below. In list form, the module parameters assigned to the adapters are more evident than the screens presented in the prior sections.

Adaptations				
<input type="button" value="Edit"/> <input type="button" value="New"/> <input type="button" value="Duplicate"/> <input type="button" value="Delete"/> <input type="button" value="More Actions"/>				
<input type="button" value="Refresh"/>			Filter: Enable	
<input type="checkbox"/>	Name	Module name	Egress URI Parameters	Notes
<input type="checkbox"/>	CS1K	CS1000Adapter		
<input type="checkbox"/>	CS1K AT&T AA-SBC	DiversionTypeAdapter odstd=135.25.29.74 osrcd=192.168.64.130 MIME=no		CS1K_outbound to AT&T via AA-SBC
Select : All , None				

6.4. SIP Entities

SIP Entities must be added for the CS1000E and the Avaya Aura® SBC. Note that once Entity Links are provisioned for each Entity (see **Section 6.5**), the Entity Link information will also be displayed on the Entity forms.

6.4.1 SIP Entity for CS1000E

Step 1 - Select **SIP Entities** from the left navigation menu.

Step 2 - Click **New** (not shown). In the **General** section, enter the following values and use default values for remaining fields.

- **Name:** Enter an identifier for the SIP Entity
- **FQDN or IP Address:** Enter the TLAN IP address of the CS1000E Node.
- **Type:** Select “**SIP Trunk**”
- **Notes:** Enter a brief description. [Optional]
- **Adaptation:** Select the Adaptation Module defined in **Section 6.3.1**.
- **Location:** Select the Location defined in **Section 6.2.1**.

Step 3 - In the **SIP Link Monitoring** section:

- **SIP Link Monitoring:** Select “**Use Session Manager Configuration**” (or choose an alternate Link Monitoring approach for this entity, if desired).

Step 4 - Click **Commit** to save the definition of the new SIP Entity.

The following screen shows the SIP Entity defined for the CS1000E in the sample configuration.

SIP Entity Details

General

*** Name:**

*** FQDN or IP Address:**

Type:

Notes:

Adaptation:

Location:

Time Zone:

Override Port & Transport with DNS SRV: ☐

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

Credential name:

Call Detail Recording:

SIP Link Monitoring

SIP Link Monitoring:

6.4.2 SIP Entity for the Avaya Aura® SBC

Step 1 - Select **SIP Entities** from the left navigation menu.

Step 2 - Click **New** (not shown). In the **General** section, enter the following values and use default values for remaining fields.

- **Name:** Enter an identifier for the SIP Entity
- **FQDN or IP Address:** Enter the private side IP Address of the SBC.
- **Type:** Select “**Other**”
- **Notes:** Enter a brief description. [Optional]
- **Adaptation:** Select the Adaptation Module defined in **Section 6.3.2**.
- **Location:** Select the Location defined in **Section 6.2.2**.

Step 3 - In the **SIP Link Monitoring** section:

- **SIP Link Monitoring:** Select “**Use Session Manager Configuration**” (or choose an alternate Link Monitoring approach for this entity, if desired).

The following screen shows the SIP Entity defined for the SBC in the sample configuration.

[Help ?](#)

SIP Entity Details

General

* **Name:**

* **FQDN or IP Address:**

Type:

Notes:

Adaptation:

Location:

Time Zone:

Override Port & Transport with DNS SRV: ☐

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

Credential name:

Call Detail Recording:

SIP Link Monitoring

SIP Link Monitoring:

6.5. Entity Links

The SIP trunk between Session Manager and the CS1000E is described by an Entity Link, as is the SIP trunk between Session Manager and the SBC.

6.5.1 Entity Link to Avaya Communication Server 1000E Entity

Step 1 - Select **Entity Links** from the left navigation menu.

Step 2 - Click **New** (not shown). Enter the following values.

- **Name** Enter an identifier for the link.
- **SIP Entity 1** Select SIP Entity defined for Session Manager during installation.
- **SIP Entity 2** Select the SIP Entity defined for the CS1000E in **Section 6.4.1**.
- **Protocol** After selecting both SIP Entities, select “**TCP**”.
- **Port** Verify **Port** for both SIP entities is the default listen port.
For the sample configuration, default listen port is “**5060**”.
- **Trusted** Enter ☒
- **Notes** Enter a brief description. [Optional]

Note: TCP was used for the reference configuration. However, TLS would typically be used in production environments. For more information on configuring TLS, see [1] & [8].

Step 3 - Click **Commit** to save the **Entity Link** definition.

The following screen shows the entity link defined for the SIP trunk between Session Manager and the CS1000E.

Name	SIP Entity 1	Protocol	Port	SIP Entity 2	Port	Trusted	Notes
* CS1K	* SM61	TCP	* 5060	* CS1K	* 5060	<input checked="" type="checkbox"/>	

6.5.2 Entity Link to the Avaya Aura® SBC

Step 1 - Select **Entity Links** from the left navigation menu. Click **New** (not shown). Enter the following values.

- **Name** Enter an identifier for the link.
- **SIP Entity 1** Select SIP Entity defined for Session Manager during installation.
- **SIP Entity 2** Select the SIP Entity defined for the Avaya Aura® SBC in **Section 6.4.2**.
- **Protocol** After selecting both SIP Entities, select “**TCP**”.
- **Port** Verify **Port** for both SIP entities is the default listen port. For the sample configuration, default listen port is “**5060**”.
- **Trusted** Enter ☒
- **Notes** Enter a brief description. [Optional]

Note: TCP was used for the reference configuration. However, TLS would typically be used in production environments. For more information on TLS, see [1] & [12].

Step 2 - Click **Commit** to save the **Entity Link** definition.

The following screen shows the entity link defined for the SIP trunk between Session Manager and the Avaya Aura® SBC.

Entity Links

Help ?

Commit

Cancel

1 Item Refresh

Filter: Enable

Name	SIP Entity 1	Protocol	Port	SIP Entity 2	Port	Trusted	Notes
* AA-SBC	* SM61	TCP	* 5060	* AA-SBC_to_AT&T	* 5060	<input checked="" type="checkbox"/>	

* Input Required

Commit

Cancel

6.6. Routing Policies

Routing policies describe the conditions under which calls will be routed by Session Manager to the CS1000E, or the Avaya Aura® SBC.

6.6.1 Routing Policy to the CS1000E

Step 1 - To add a new routing policy, select **Routing Policies**. Click **New** (not shown). In the **General** section, enter the following values.

- **Name:** Enter an identifier to define the routing policy
- **Disabled:** Leave unchecked.
- **Notes:** Enter a brief description. [Optional]

Step 2 - In the **SIP Entity as Destination** section, click **Select**. The **SIP Entity List** page opens (not shown).

- Select the SIP Entity associated with the CS1000E (see **Section 6.4.1**) and click **Select**.
- The selected SIP Entity displays on the **Routing Policy Details** page.

Step 3 - In the **Time of Day** section, add an appropriate time of day. In the sample configuration, time of day was not a relevant routing criteria, so the “24/7” range was chosen. Use default values for remaining fields.

Step 4 - Click **Commit** to save the Routing Policy definition.

The following screen shows the Routing Policy for the CS1000E.

[Help ?](#)

Routing Policy Details

General

* **Name:**

Disabled: ☐

Notes:

SIP Entity as Destination

Name	FQDN or IP Address	Type	Notes
CS1K	172.16.6.110	SIP Trunk	

Time of Day

1 Item
Filter: Enable

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

Select : All, None

6.6.2 Routing Policy to the Avaya Aura® SBC

Step 1 - To add a new routing policy, select **Routing Policies**. Click **New** (not shown). In the **General** section, enter the following values.

- **Name:** Enter an identifier to define the routing policy
- **Disabled:** Leave unchecked.
- **Notes:** Enter a brief description. [Optional]

Step 2 - In the **SIP Entity as Destination** section, click **Select**. The **SIP Entity List** page opens (not shown).

- Select the SIP Entity associated with the Avaya Aura® SBC (see **Section 6.4.2**) and click **Select**.
- The selected SIP Entity displays on the **Routing Policy Details** page.

Step 3 - In the **Time of Day** section, add an appropriate time of day. In the sample configuration, time of day was not a relevant routing criteria, so the “24/7” range was chosen. Use default values for remaining fields.

Step 4 - Click **Commit** to save the Routing Policy definition.

The following screen shows the Routing Policy for the Avaya Aura® SBC.

[Help ?](#)

Routing Policy Details

General

* Name:

Disabled: ☐

Notes:

SIP Entity as Destination

Name	FQDN or IP Address	Type	Notes
AA-SBC_to_AT&T	192.168.67.125	Other	

Time of Day

1 Item
Filter: Enable

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

Select : All, None

6.7. Dial Patterns

Dial patterns are used to route calls to the appropriate routing policies, and ultimately to the appropriate SIP Entities. Dial patterns will be configured to route outbound calls from CS1000E users to the PSTN via the AT&T IP Flexible Reach service. Other dial patterns will be configured to route inbound calls from the AT&T IP Flexible Reach service to CS1000E users.

6.7.1 Inbound AT&T calls to CS1000E Users

Step 1 - To define a dial pattern, select **Dial Patterns** from the navigation menu. Click **New** (not shown). In the **General** section, enter the following values and use default values for remaining fields.

- **Pattern:** Enter dial pattern for calls to the CS1000E (e.g. 732320xxxx)
- **Min:** Enter the minimum number of digits (e.g. 10).
- **Max:** Enter the maximum number of digits (e.g. 10).
- **SIP Domain:** Select a SIP Domain from drop-down menu or select “All” if Session Manager should route incoming calls from all SIP domains.
- **Notes:** Enter a brief description. [Optional]

Step 2 - In the **Originating Locations and Routing Policies** section, click **Add**.

Step 3 - The **Originating Locations and Routing Policy List** page opens (not shown).

- In the **Originating Location** list, select the location defined for the Avaya Aura® SBC in **Section 6.2.2**.
- In the **Routing Policies** table, select the Routing Policy defined for the CS1000E in **Section 6.6.1**.
- Click **Select** to save these changes and return to **Dial Pattern Details** page.

Step 4 - Click **Commit** to save. The following screen shows an example Dial Pattern defined for the sample configuration. Repeat this procedure as needed to allow additional AT&T DID numbers to be routed to the CS1000E.

Dial Pattern Details
Commit
Cancel
Help ?

General

* **Pattern:**

* **Min:**

* **Max:**

Emergency Call: ☐

SIP Domain:

Notes:

Originating Locations and Routing Policies

Add Remove

4 Items Refresh Filter: Enable

<input type="checkbox"/>	Originating Location Name ¹	Originating Location Notes	Routing Policy Name	Rank ²	Routing Policy Disabled	Routing Policy Destination	Routing Policy Notes
<input type="checkbox"/>	AA-SBC		To CS1K	0	<input type="checkbox"/>	CS1K	

Select : All, None

6.7.2 Outbound Calls to AT&T

Step 1 - To define a dial pattern, select **Dial Patterns** from the navigation menu. Click **New** (not shown). In the **General** section, enter the following values and use default values for remaining fields.

- **Pattern:** Enter dial pattern for calls destined to PSTN via the AT&T network (e.g. 1732xxxxxx).
- **Min:** Enter the minimum number of digits (e.g. 11).
- **Max:** Enter the maximum number of digits (e.g. 11).
- **SIP Domain:** Select a SIP Domain from drop-down menu or select “All” if Session Manager should route outgoing calls from all SIP domains.
- **Notes:** Enter a brief description. [Optional]

Step 2 - In the **Originating Locations and Routing Policies** section, click **Add**.

Step 3 - The **Originating Locations and Routing Policy List** page opens (not shown).

- In the **Originating Location** list, select “**Apply the Selected Routing Policies to All Originating Locations**”. In the **Routing Policies** table, select the Routing Policy defined for the Avaya Aura® SBC in **Section 6.6.2**.
- Click **Select** to save these changes and return to **Dial Pattern Details** page.

Step 4 - Click **Commit** to save. The following screen shows an example Dial Pattern defined for the sample configuration. Repeat this procedure as needed to allow additional PSTN numbers to be routed to PSTN/AT&T network via the Avaya Aura® SBC.

Dial Pattern Details [Commit] [Cancel] [Help ?]

General

* **Pattern:** 1732

* **Min:** 11

* **Max:** 11

Emergency Call: ☐

SIP Domain: -ALL-

Notes: To PSTN

Originating Locations and Routing Policies

[Add] [Remove] Filter: Enable

2 Items Refresh

<input type="checkbox"/>	Originating Location Name 1	Originating Location Notes	Routing Policy Name	Rank 2	Routing Policy Disabled	Routing Policy Destination	Ro Pol No
<input type="checkbox"/>	-ALL-	Any Locations	To_AT&T_via_AA-SBC	0	<input type="checkbox"/>	AA-SBC_to_AT&T	

Select : All, None

7. Configure Avaya Aura® Session Border Controller (SBC)

This section illustrates an example configuration of the SBC. In the sample configuration, the SBC runs on its own S8800 Server as an application template using System Platform. The installation of the System Platform is assumed to have been previously completed (see the Avaya Aura® SBC references in **Section 12**) for additional information on the SBC installation.

7.1. Logging into the Avaya Session Border Controller

Log in to the System Platform console domain by entering `https://<ip-addr>/webconsole` as shown in the example screen below. In the reference configuration, the console domain uses the IP Address 192.168.67.124. Enter an appropriate **User Id** and press the **Continue** button.

AVAYA

Avaya Aura™ System Platform
Web Console

?

Login

User Id

Continue

Copyright © 2009-2010 Avaya Inc. All Rights Reserved.

On the subsequent screen, enter the appropriate **Password** and click the **Log On** button.

AVAYA

Avaya Aura™ System Platform
Web Console

?

Login


User Id

Password

Reset

Log On

Copyright © 2009-2010 Avaya Inc. All Rights Reserved.

The **Virtual Machine List** will show the SBC Template installed during the SBC installation process [12] [14]. The template defines the basic SBC provisioning (IP addressing, To apply the additional reference configuration provisioning, click on the  to access the SBC GUI interface.

AVAYA

Avaya Aura™ System
Previous successful login: Wed Jun 29 15:3
Failed login at
Failover status: **N**
About | H

Home

Virtual Machine Management

Server Management

User Administration

Virtual Machine Management

Virtual Machine List

System Domain Uptime: 64 days, 5 hours, 37 minutes, 9 seconds

Current template installed: SBCT 6.0.2.0.3 (sbc E362P4) [Refresh](#)

	Name	Version	IP Address	Maximum Memory	Maximum Virtual CPUs	CPU Time	State	Appli
✓	Domain-0	6.0.3.0.3	192.168.67.123	512.0 MB	8	3d 8h 44m 1s	Running	
✓	 sbc	E362P4	192.168.67.125	4.0 GB	4	1d 7h 35m 50s	Running	
✓	cdom	6.0.3.0.3	192.168.67.124	1024.0 MB	1	1d 4h 57m 50s	Running	

Copyright © 2009-2010 Avaya Inc. All Rights Reserved.

Enter appropriate **Username** and **Password** and click **Login**.


Acme Packet Net-Net OS-E

To access the NNOS-E management interface, you must first log in. Please provide your user name

Username:

Password:

The following shows an abridged **Home** screen after logging in. Note the tabs at the top.


[Logout admin](#)


[Home](#) [Configuration](#) [Status](#) [Call Logs](#) [Event Logs](#) [Actions](#) [Services](#) [Keys](#) [Access](#) [Tools](#)

(c) 2005-2010 Acme Packet, Inc. All rights reserved.
[\[www.acmepacket.com\]](http://www.acmepacket.com)

Get summary for: Box 1

box-identifier 017b-92c9-6442-35d9

box-status

IPAddress	LocalBox (65.206.67.93)
State	Connected 
build-version	E362P1
build-number	47121

master-services database

up-time

time	13:44:08 Wed 2011-05-11
timezone	EDT
uptime	7 days 16:07:38

[Help](#)

7.2. Network Configuration

In the reference configuration, the Avaya S8800 Server has four physical network interfaces, labeled 1 through 4. The port labeled “1” (virtual “eth0”) is used for the management and private (inside) network interface of the SBC (toward the customer equipment). The port labeled “4” (virtual “eth2”) is used for the public (outside) network interface of the SBC (toward AT&T). These can be verified by checking the “interface eth0” and interface eth2” settings (see **Section 7.2.1**).

The AT&T AVPN transport service requires that RTP media traffic use UDP port range 16384-32767. This range is defined as part of “interface eth2” (see **Section 7.2.3**).

SIP-Gateways are defined for corresponding to the private and public interfaces. In the reference configuration the private interface is defined as “PBX” and the public interface is defined as “Telco1” (see **Section 7.2.4**).

7.2.1 Verify IP Addressing

Step 1 - From the **Configuration** tab, select **cluster** → **box** <name defined during install> (e.g. AA-SBC). The **interface eth0** and **interface eth2** will be displayed. Click on **ip inside** (eth0) or **ip outside** (eth2) to display the interface configuration. Note that AT&T may require the eth2 IP address as part of the IP Flexible Reach service provisioning.

Step 2 - The configuration may be modified by clicking the **Edit** button. If changes are made, click on the **Set** button. To cancel changes or to go to a previous screen, click on **Back**.

The screenshot shows the Avaya Aura Configuration page. The left sidebar contains a tree view with the following structure:

- cluster
 - box:AA-SBC
 - interface eth0
 - ip inside
 - interface eth2
 - ip outside
 - cli
 - vsp
 - default-session-config
 - tls
 - session-config-pool
 - entry ToTelco
 - entry ToPBX
 - entry Discard
 - dial-plan
 - enterprise
 - servers
 - sip-gateway PBX
 - sip-gateway Telco
 - dns settings

The main content area shows the configuration for the selected **ip inside** interface. It includes a table with the following columns: **ip**, **admin**, **ip-address**, **geolocation**, **security-domain**, **address-scope**, **filter-intf**, **media-ports**, and **metr**. The table contains one row with the following values:

ip	admin	ip-address	geolocation	security-domain	address-scope	filter-intf	media-ports	metr
192.168.67.125/24	enabled	static	0			disabled	20000 5000 enabled	1

Below the table, there are buttons for **Edit**, **Delete**, **ip inside**, **Set**, **Reset**, **Back**, **Help**, and **Index**. The **Edit** button is highlighted with a red box. The **Set** and **Back** buttons are also highlighted with red boxes.

7.2.2 Transport Protocols

7.2.2.1 Private Interface – Eth0

The private interface, eth0, was provisioned to support UDP, TCP, and TLS transport protocols. However, TCP (port 5060) was used in the reference configuration for the connection to Session Manager (see **Section 6.5.2**). This can be displayed by the following:

Step 1 – Navigate to **cluster** → **box** <name defined during install> → **interface eth0** → **ip inside**.

Step 2 – Scroll down to, and click on the **SIP** heading. The UDP, TCP, and TLS supported protocols are displayed.

Note: TCP was used for the reference configuration. However, TLS would typically be used in production environments. For more information on configuring TLS, see [12].

sip
Delete

admin

enabled (Resource is active)

nat-translation

disabled (Resource is inactive)

nat-add-received-from

disabled (Resource is inactive)

nat-add-X-Remote-Info

enabled (Resource is active)

load-balance-head-end

false

udp-port

	udp-port	from-server	to-server	transport	remote-port	certificate
Edit Delete	udp-port 5060	Edit	Edit	any	0	Edit

Add udp-port

tcp-port

	tcp-port	from-server	to-server	transport	remote-port	certificate
Edit Delete	tcp-port 5060	Edit	Edit	any	0	Edit

Add tcp-port

tls-port

	tls-port	from-server	to-server	transport	remote-port	certificate
Edit Delete	tls-port 5061	Edit	Edit	TLS	0	vsptls/certificate aasbc_p12

Step 3 - The configuration may be modified by clicking the **Edit** buttons. If changes are made, click on the **Set** button (not shown). To cancel changes or to go to a previous screen, click on **Back** (not shown).

7.2.2.2 Public Interface – Eth2

The AT&T IP Flexible Reach service requires UDP transport protocol between the Avaya Aura® SBC and the AT&T IP Flexible Reach service border element. Therefore, the public interface, eth2, was provisioned to support UDP transport protocol only. This can be displayed by the following:

Step 1 – Navigate to **cluster** → **box** <name defined during install> → **interface eth2** → **ip outside**.

Step 2 – Scroll down to, and click on the **SIP** heading. The UDP (port 5060) transport protocol is displayed.

sip
Delete

admin

enabled

(Resource is active)

nat-translation

disabled

(Resource is inactive)

nat-add-received-from

disabled

(Resource is inactive)

nat-add-X-Remote-Info

enabled

(Resource is active)

load-balance-head-end

false

udp-port

	udp-port	from-server	to-server	transport	remote-port	certificate
Edit Delete	udp-port 5060	Edit	Edit	any	0	Edit

Add udp-port

Step 3 - The configuration may be modified by clicking the **Edit** buttons. If changes are made, click on the **Set** button (not shown). To cancel changes or to go to a previous screen, click on **Back** (not shown).

7.2.3 Setting the RTP Port Range on Eth2

Step 1 - Go to **cluster** → **box** <name defined during install> → **interface eth2** → **ip outside** to display the eth2 configuration toward AT&T. Select Media Ports from either the menu or from the display.

The screenshot shows the Avaya Aura Configuration interface. On the left is a tree view with 'media-ports' highlighted. The main panel shows the configuration for 'media-ports' with the following fields:

general:	
* name	outside
admin	enabled (Resource is active)
* ip-address	* type: static (static IP address) * address/mask: 192.168.64.130/24 (n.n.n.n/n)
geolocation	0
security-domain	enter [] or select from <Not configured>
address-scope	enter [] or select from <Not configured>
filter-intf	disabled (Resource is inactive)
media-ports	[Delete]

Step 2 - The media port section will be displayed. Enter **16384** in the **base-port** field and **16383** in the **count** field.

This screenshot shows the 'media-ports' configuration section with the following values entered:

admin	enabled (Resource is active)
base-port	16384 (at minimum 1, default=20000)
count	16383 (from 0 to 65,535)
idle-monitor	enabled (Resource is active)

Step 3 - Click on the **Set** button to save.

Step 4 - Proceed to save and activate the configuration as described in **Section 7.3**.

7.2.4 Configuring the SIP-Gateways

In the reference configuration, a sip-gateway was defined to AT&T (the IP Flexible Reach border element) and to the customer site (Session Manager). The AT&T gateway was defined as “Telco1” and customer gateway was defined as “PBX”.

7.2.4.1 Telco1

Step 1 - Go to **vsp** → **enterprise** → **servers** and any previously defined sip-gateways will be displayed. In the reference configuration sip-gateways **PBX** and **Telco1** were defined.

Step 2 - Click on **sip-gateway Telco** → **servers** → **server-pool** → **server Telco1** and the Telco1 sip-gateway configuration will be displayed.

The screenshot shows the Avaya Aura Configuration interface. The top navigation bar includes 'Home', 'Configuration', 'Status', 'Call Logs', 'Event Logs', 'Actions', 'Services', 'Keys', 'Access', and 'Tools'. The 'Configuration' tab is active. On the left, a tree view shows the configuration hierarchy: 'cluster' > 'vsp' > 'default-session-config' > 'tls' > 'session-config-pool' > 'dial-plan' > 'enterprise' > 'servers' > 'sip-gateway Telco' > 'server-pool' > 'server Telco1'. The main content area is titled 'Configure vsp\enterprise\servers\sip-gateway Telco\server-pool\server Telco1'. It includes buttons for 'Show advanced', 'Help', 'Index', 'Set', 'Reset', 'Back', 'Copy', and 'Delete'. The 'General' section contains fields for 'server-name' (Telco1), 'admin' (enabled), 'host' (135.25.29.74), 'transport' (UDP), and 'port' (5060). The 'Policy' section has links for 'outbound-normalization' and 'inbound-normalization'.

Step 3 - Verify the following:

- admin state is **enabled**.
- host address is the IP address of the AT&T IP Flexible Reach border element (e.g. **135.25.29.74**).
- transport protocol is **UDP**.
- port is **5060**.

Step 4 - Click on the **Set** button to save any changes or **Back** if no changes are required.

Step 5 - Proceed to save and activate the configuration as described in **Section 7.3**.

7.2.4.2 PBX

Repeat the steps in **Section 7.2.4.1** and verify the following:

- admin state is **enabled**.
- host address is the IP address of Session Manager (e.g. **192.168.67.210**).
- transport protocol is **TCP**. Note that TCP was used in the reference configuration to facilitate protocol trace verification and troubleshooting. TLS may be used as well (see [1] & [12]).
- port is **5060**.

7.2.5 Stripping SIP Headers

The Avaya Aura® SBC can be used to strip SIP headers that are not required or supported by AT&T. For headers that have relevance only within the enterprise, it may be desirable to prevent

the header from being sent to the public SIP Service Provider. For example, Session Manager Release 6.1 may insert the “P-Location” and “Remote-Party-ID” headers. The CS1000E may send the “x-nt-e164-clid”, “x-nt-corr-id”, “Alert-Info”, and “History-Info” headers. The following procedures may be used to strip such headers that AT&T does not process.

7.2.5.1 Specific Session-config-pool Method

Undesired headers may be removed via the session-config-pool. For example, during installation, two session-config-pools were created, “To-Telco” and “To-PBX”. First the headers are removed session-config-pool “**To-Telco**”. This will remove the specified headers for calls sent by the customer location to AT&T.

Step 1 - Navigate to **vsp → session-config-pool → entry ToTelco → header-settings**. In the resultant screen, click **Edit blocked-header** and proceed to add the P-Location and other blocked headers as described in the previous section.



Step 2 – Repeat the procedure in **Step 1** for “**entry ToPBX**”. This will remove the specified headers for calls from AT&T and answered by the customer location.

Step 3 - Proceed to save and activate the configuration as described in **Section 7.3**.

7.2.6 Stripping Unnecessary SIP Message Body Information

As described in **Section 6.3.2**, the message body of an INVITE message sent from the CS1000E will contain a MIME Multipart message body headers not required by AT&T. These headers were removed by Session Manager in the reference configuration. Alternatively the Avaya Aura® SBC may be used to remove these headers. Two alternative approaches were tested successfully and are described below as reference. In one approach, the SBC is used to specifically block the “x-nt-mcdn-frag-hex” and “x-nt-epid-frag-hex” parts. In another approach, the SBC is used to block any body part that is not SDP.

7.2.6.1 Block Any body part but SDP Approach

Step 1 - To block any body part but SDP, navigate to **vsp → default-session-config → bodypart-type**. Click **Add allowed-body-part**.

Step 2 - In the **bodypart-type** drop-down menu, select “application”. In the application-sub-type menu, select “sdp” as shown in the screen below. Click **Create**.

Step 3 - Navigate to **vsp → default-session-config → bodypart-type**. Click **Add blocked-body-part**.

Step 4 - In the **bodypart-type** drop-down menu, select “application”. In the application-sub-type menu, select “any” as shown in the screen below. Click **Create**.

Step 5 - Proceed to save and activate the configuration as described in **Section 7.3**.

7.2.6.2 Block Specific Body Part Approach

This is an alternative to the approach documented in the previous sub-section. In this section, the specific body parts that the CS1000E inserts in the message body are blocked rather than blocking anything but SDP.

Step 1 - Navigate to **vsp → default-session-config → bodypart-type**. Click **Add blocked-body-part**.

Step 2 - In the **bodypart-type** drop-down menu, select “application”. In the **application-sub-type** menu, type in or select “x-nt-mcdn-frag-hex”. Click **Create**.

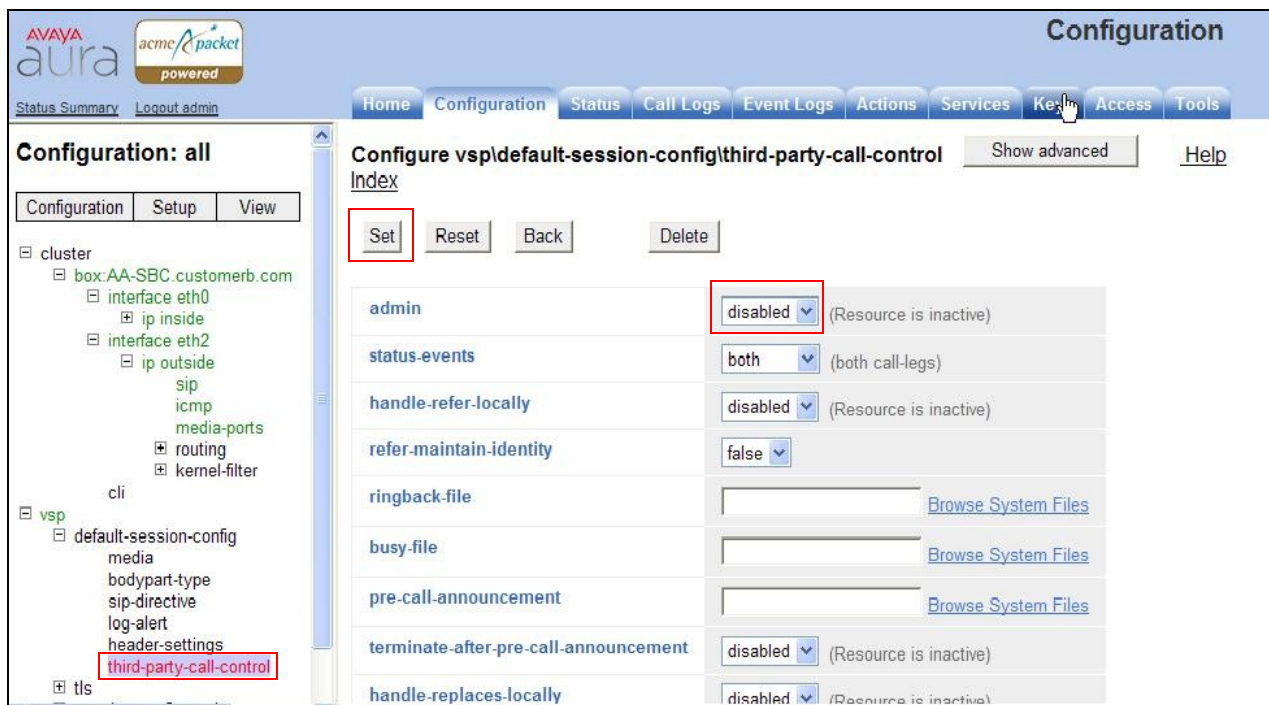
Step 3 - Click **Add blocked-body-part**. In the **bodypart-type** drop-down menu, select “application”. In the **application-sub-type** menu, type in or select “x-nt-epid-frag-hex”. Click **Create**.

Step 4 - Proceed to save and activate the configuration as described in **Section 7.3**.

7.2.7 Disable Third Party Call Control

Step 1 - Navigate to **vsp → default-session-config → third-party-call-control**. To disable third-party-call-control, select **disabled** from the **admin** drop-down. Note - After disabling, the third-party-call-control link becomes red as shown below.

Step 2 - click **Set** as shown below.



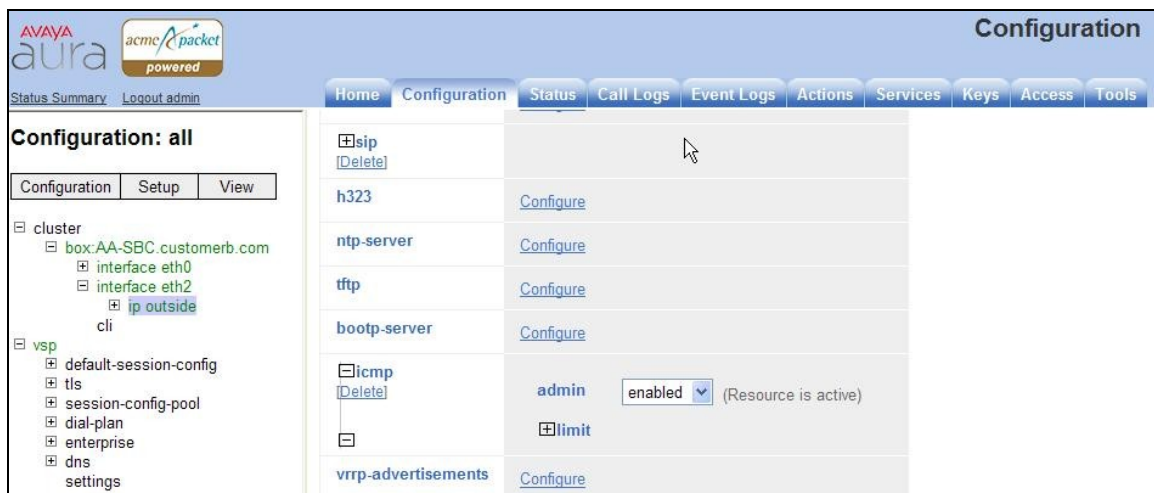
Step 3 - Proceed to save and activate the configuration as described in **Section 7.3**.

7.2.8 SIP OPTIONS Messages for AT&T Network Status

In the reference configuration, the Avaya Aura® SBC sent SIP OPTIONS messages to the AT&T IP Flexible Reach border element to verify the state of the network connection. The AT&T response to the OPTIONS is “405 Method Not Allowed”. Although this appears to be an error, in fact the arrival of the message assures the Avaya Aura® SBC that the network connection is up.

Step 1 - Navigate to **cluster** → **box:AvayaSBC** → **interface eth2** → **ip outside**. Scroll down to, and click on, the **icmp** option.

Step 2 - Set the **admin** option to **enabled**.



Step 3 - Scroll to the bottom of the screen and click **Set**.

Step 4 - Navigate to **vsp** → **enterprise** → **servers** → **sip-gateway Telco**. Click on the **Show Advanced** button at the top of the page (not shown).

Step 5 – In the **general:** section set **failover-detection** and select **ping** from the menu.

Configure vsp\enterprise\servers\sip-gateway Telco Sh

[Manage connections](#), [Log instant messages](#), [Record media](#), [Record files](#),
[Set up accounting](#), [Change from: URI](#), [Change to: URI](#)

general:

* name	<input type="text" value="Telco"/>
peer-identity	<input type="text"/>
admin	<input type="button" value="enabled"/> (Resource is active)
domain	<input type="text"/>
directory	<input type="button" value="v"/> Create
failover-detection	<input type="button" value="ping"/> (Use OPTIONS to detect failures)

Step 6 – Scroll down to the **routing:** section and set the **ping-interval** as desired (e.g. **60**).

routing:	
routing-setting	<div> normalization auto-tag-match auto-domain-match pstn-backup </div> <div> Select All Unselect All </div>
domain-alias	Edit domain-alias
domain-subnet	Edit domain-subnet
loop-detection	tight (Compare source and destination address/port/transport)
service-type	provider (Provider peer)
ping-interval	60 seconds

Step 7 - Scroll to the bottom of the screen and click **Set**.

Step 8 - Proceed to save and activate the configuration as described in **Section 7.3**.

7.2.9 Altering the To Header for PSTN Calls to CS1000E

The AT&T IP Flexible Reach service may specify different DID numbers in the Request URI and To headers of inbound Invite messages. The Avaya Aura® SBC is configured to modify the To header to match the number (user field) specified in the Request URI.

Note - While not required for typical inbound calls, this function is required for correct handling of inbound calls to Call Pilot for message retrieval.

Step 1 - Navigate to **vsp → session-config-pool → entry ToPBX → header-settings → altered-header**, and click on **Add altered –header** (not shown). In the resultant screen, enter the follow:

- **admin** – enabled
- **number** – select an identifying number (e.g. 1).
- **source-header** – Select **Request** from the drop down menu.
- **source-field** – Select **User** from the drop down menu.
- **destination** – Select **To** from the drop down menu.
- **destination-field** - Select **User** form the drop down menu.
- **apply-to-methods** – Select **INVITE** from the drop down menu.
- Let the other values default

Step 2 - Scroll to the bottom of the screen and click **Set**.

Step 3 - Proceed to save and activate the configuration as described in **Section 7.3**.

Configure vsp\session-config-pool\entry ToPBX\header-settings\altered-head

[Show advanced](#) [Help](#) [Index](#)

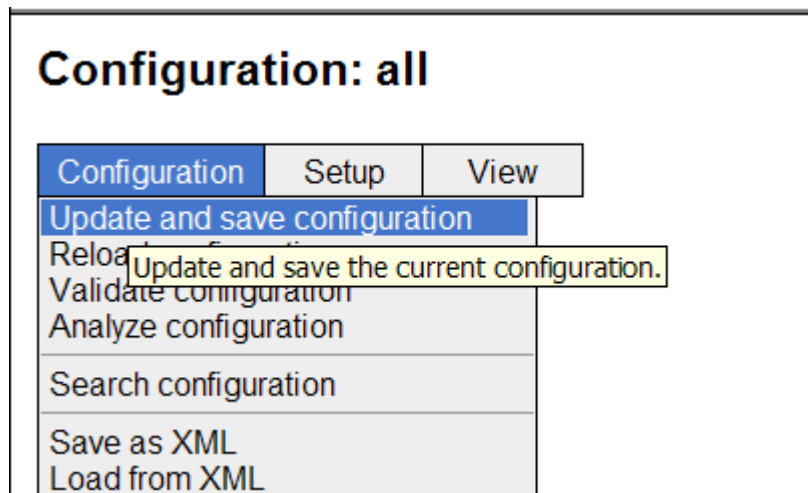
[Set](#) [Reset](#) [Back](#) [Copy](#) [Delete](#)

admin	enabled <input type="button" value="v"/> (Resource is active)
* number	<input type="text" value="1"/>
* source-header	enter <input type="text" value="Request"/> or select from <input type="button" value="Request"/> <input type="button" value="v"/>
* source-field	* type <input type="button" value="user"/> <input type="button" value="v"/> (User portion of the URI.)
* destination	enter <input type="text" value="To"/> or select from <input type="button" value="To"/> <input type="button" value="v"/>
* destination-field	* type <input type="button" value="user"/> <input type="button" value="v"/> (User portion of the URI.)
apply-to-methods	<div> <input checked="" type="checkbox"/> INVITE <input type="checkbox"/> REFER <input type="checkbox"/> MESSAGE <input type="checkbox"/> INFO </div> <div> <input type="button" value="Select All"/> <input type="button" value="Unselect All"/> </div>
apply-to-responses	* type <input type="button" value="no"/> <input type="button" value="v"/> (Do not apply to responses (requests only))
apply-to-dialog	<input type="button" value="both"/> <input type="button" value="v"/> (Apply to both inbound and outbound dialogs.)
session-persistent	disabled <input type="button" value="v"/> (Resource is inactive)

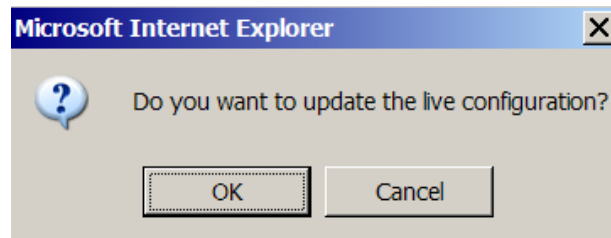
[Set](#) [Reset](#) [Back](#) [Copy](#)

7.3. Saving and Activating Configuration Changes

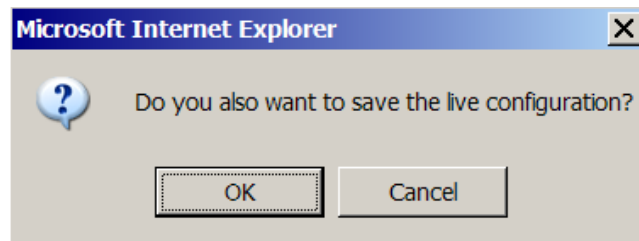
Step 1 - To save and activate configuration changes, select **Configuration** → **Update and save configuration** from the upper left hand side of the user interface, as shown below.



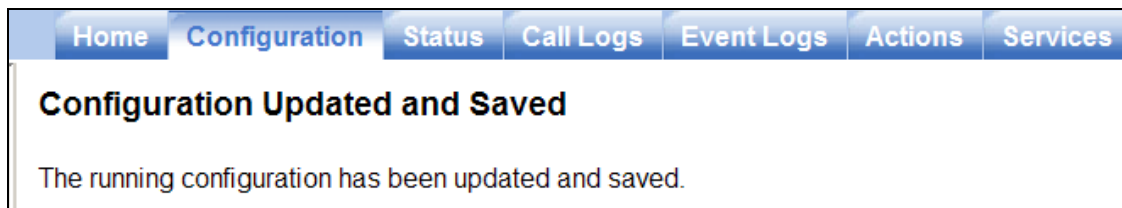
Step 2 - Click **OK** to update the live configuration.



Step 3 - Click **OK** to save the live configuration.



A screen that includes the following should appear.



7.4. Avaya Aura® SBC Configuration File

The Avaya Aura® SBC configuration is saved to a text configuration file (**cxc.cfg** file). A copy of the configuration file can be retrieved from the SBC by selecting the **Tools** tab and selecting

Download saved configuration file from the left-side menu. An example configuration file resulting from the configuration in **Section 7** is attached.

```
#
# Copyright (c) 2004-2011 Acme Packet Inc.
# All Rights Reserved.
#
# File: /cxc/cxc.cfg
# Date: 13:53:59 Wed 2011-08-03
#
config cluster
config box 1
  set hostname AA-SBC.customerb.com
  set timezone America/New_York
  set name AA-SBC.customerb.com
  set identifier 00:ca:fe:45:93:63
config interface eth0
  config ip inside
    set ip-address static 192.168.67.125/24
  config ssh
  return
  config snmp
    set trap-target 192.168.67.124 162
    set trap-filter generic
    set trap-filter dos
    set trap-filter sip
    set trap-filter system
  return
  config web
  return
  config web-service
    set protocol https 8443
    set authentication certificate "vsp\tls\certificate ws-cert"
  return
  config sip
    set udp-port 5060 "" "" any 0
    set tcp-port 5060 "" "" any 0
    set tls-port 5061 "" "" TLS 0 "vsp\tls\certificate aasbc.p12"
  return
  config icmp
  return
  config media-ports
  return
  config routing
    config route Default
      set gateway 192.168.67.1
    return
    config route Static0
      set destination network 192.11.13.4/30
      set gateway 192.168.67.123
    return
    config route Static1
      set admin disabled
    return
    config route Static2
      set admin disabled
```

```

return
config route Static3
    set admin disabled
return
config route Static4
    set admin disabled
return
config route Static5
    set admin disabled
return
config route Static6
    set admin disabled
return
config route Static7
    set admin disabled
return
return
return
return
config interface eth2
config ip outside
    set ip-address static 192.168.64.130/24
config sip
    set udp-port 5060 "" "" any 0
return
config icmp
return
config media-ports
    set base-port 16384
    set count 16383
return
config routing
    config route Default
        set admin disabled
    return
    config route external-sip-media-1
        set destination network 135.25.29.0/24
        set gateway 192.168.64.254
    return
    config route ORT
        set destination network 12.40.234.0/24
        set gateway 192.168.64.254
    return
return
config kernel-filter
    config allow-rule allow-sip-udp-from-peer-1
        set destination-port 5060
        set source-address/mask 135.25.29.0/24
        set protocol udp
    return
    config deny-rule deny-all-sip
        set destination-port 5060
    return
return
return
return
config cli

```

```
    set prompt AA-SBC.customerb.com
    return
return
return
```

```
config services
config event-log
    config file access
        set filter access info
        set count 3
    return
    config file system
        set filter system info
        set count 3
    return
    config file errorlog
        set filter all error
        set count 3
    return
    config file db
        set filter db debug
        set filter dosDatabase info
        set count 3
    return
    config file management
        set filter management info
        set count 3
    return
    config file peer
        set filter sipSvr info
        set count 3
    return
    config file dos
        set filter dos alert
        set filter dosSip alert
        set filter dosTransport alert
        set filter dosUrl alert
        set count 3
    return
    config file krnlsys
        set filter krnlsys debug
        set count 3
    return
return
return
```

```
config master-services
config database
    set media enabled
return
return
```

```
config vsp
    set admin enabled
config default-session-config
    config media
        set anchor enabled
```

```

    set rtp-stats enabled
return
config bodypart-type
return
config sip-directive
    set directive allow
return
config log-alert
return
config header-settings
return
config third-party-call-control
    set handle-refer-locally disabled
return
return
config tls
    config default-ca
        set ca-file /cxc/certs/sipca.pem
    return
    config certificate ws-cert
        set certificate-file /cxc/certs/ws.cert
    return
    config certificate aasbc.p12
        set certificate-file /cxc/certs/aasbc.p12
        set passphrase-tag aasbc-cert-tag
    return
return
config session-config-pool
    config entry ToTelco
        config to-uri-specification
            set host next-hop
        return
        config from-uri-specification
            set host local-ip
        return
        config request-uri-specification
            set host next-hop
        return
        config p-asserted-identity-uri-specification
            set host local-ip
        return
        config contact-uri-settings-in-leg
        return
        config contact-uri-settings-out-leg
        return
        config bodypart-type
            set blocked-body-part custom-mime-type x-nt-inforeq any
        return
        config in-codec-preferences
            set preference audio "Media Format: DynamicRTP-Type-111" 0
        return
        config out-codec-preferences
            set preference audio "Media Format: DynamicRTP-Type-111" 0
        return
        config out-media-normalization
        return
        config header-settings

```



```

set blocked-header P-Location
set blocked-header x-nt-e164-clid
set blocked-header x-nt-corr-id
set blocked-header Alert-Info
set blocked-header History-info
set blocked-header Remote-Party-ID
config reg-ex-header 1
    set admin disabled
    set destination From
    set create From "<sip:\+(*.*)@(*.*)" "<sip:\1@\2"
return
config reg-ex-header 2
    set admin disabled
    set destination P-Asserted-Identity
    set create P-Asserted-Identity "<sip:\+(*.*)@(*.*)" "<sip:\1@\2"
return
config reg-ex-header 3
    set admin disabled
    set destination Contact
    set create Contact "<sip:\+(*.*)@(*.*)" "<sip:\1@\2"
return
return
return
config entry ToPBX
    config to-uri-specification
        set host next-hop-domain
    return
    config request-uri-specification
        set host next-hop-domain
    return
    config contact-uri-settings-in-leg
    return
    config contact-uri-settings-out-leg
    return
    config in-codec-preferences
        set preference audio "Media Format: DynamicRTP-Type-111" 0
    return
    config out-codec-preferences
        set preference audio "Media Format: DynamicRTP-Type-111" 0
    return
    config header-settings
        set blocked-header P-Location
        set blocked-header x-nt-e164-clid
        set blocked-header x-nt-corr-id
        set blocked-header Alert-Info
        set blocked-header History-Info
        set blocked-header Remote-Party-ID
        config altered-header 1
            set source-header Request
            set source-field user
            set destination To
            set destination-field user
        return
    return
return
config entry Discard
    config sip-directive

```

```

    return
  return
return
config dial-plan
  config route Default
    set priority 500
    set location-match-preferred exclusive
    set session-config vsp\session-config-pool\entry Discard
  return
  config source-route FromTelco
    set peer server "vsp\enterprise\servers\sip-gateway PBX"
    set source-match server "vsp\enterprise\servers\sip-gateway Telco"
  return
  config source-route FromPBX
    set peer server "vsp\enterprise\servers\sip-gateway Telco"
    set source-match server "vsp\enterprise\servers\sip-gateway PBX"
  return
return
config enterprise
  config servers
    config sip-gateway PBX
      set domain cots1.ntlab.com
      set failover-detection ping
      set outbound-session-config-pool-entry vsp\session-config-pool\entry ToPBX
    config server-pool
      config server PBX1
        set host 192.168.67.210
        set transport TCP
      return
    return
  return
  config sip-gateway Telco
    set failover-detection ping
    set ping-interval 60
    set outbound-session-config-pool-entry vsp\session-config-pool\entry
ToTelco
  config server-pool
    config server Telco1
      set host 135.25.29.74
      set connection-retry-interval 60
    config network
      return
    config error-response-codes
      return
  return
  config server Telco2
    set admin disabled
    set host 135.25.29.75
    config network
      return
    config error-response-codes
      return
  return
  config server ORT
    set admin disabled
    set host 12.40.234.99
  return

```

```

        return
    return
return
config dns
    config resolver
        config server 192.168.67.5
        return
    return
return
config settings
    set read-header-max 8191
return
return

config external-services
return

config preferences
    config gui-preferences
        set enum-strings SIPSourceHeader PAI
        set enum-strings SIPSourceHeader P-Asserted-Identity
        set enum-strings SIPSourceHeader Contact
        set enum-strings MediaAudioSubType "Media Format: DynamicRTP-Type-111"
    return
return

config access
    config permissions superuser
        set cli advanced
    return
    config permissions read-only
        set config view
        set actions disabled
    return
    config users
        config user admin
            set password 0x00b930c8c97cc6705c312dd835419ecc3559106a7b9f91774cb86e85ec
            set permissions access\permissions superuser
        return
        config user cust
            set password 0x0033a56c33e6e62e159bb5bd94be32dc30e408d441627c93d9d740483c
            set permissions access\permissions read-only
        return
        config user init
            set password 0x002e3afdb5919e72cbd542345a7a918f9cad4ce7c917bcff336fc9901b
            set permissions access\permissions superuser
        return
        config user craft
            set password 0x00fb8b12eba46bc122cf5642e1e076477a510ffa51da44498020fcbc12
            set permissions access\permissions superuser
        return
        config user dadmin
            set password 0x0005b4d2ba1868181287ff79c199ab43f8575ca330d8d88599dde14804
            set permissions access\permissions read-only
        return
    return
return

```

return

config features
return

8. AT&T IP Flexible Reach Service

Information regarding AT&T IP Flexible Reach Service may be found at <http://www.business.att.com/enterprise/Service/voice-services/voip/sip-trunking/> or by contacting AT&T at **800-248-3632**.

8.1. AT&T Provisioning

The AT&T IP Flexible Reach service provided DID numbers for the reference configuration that could be called from the PSTN. These DID numbers terminated to the Avaya CS1000E location via the AT&T IP Flexible Reach service. DID numbers shown in these application notes are examples. Customers will be assigned DIDs by AT&T.

The AT&T IP Flexible Reach service also provided a network border element IP address for the reference configuration. Customers will be assigned a border element IP address(es) by AT&T.

9. Verification Steps

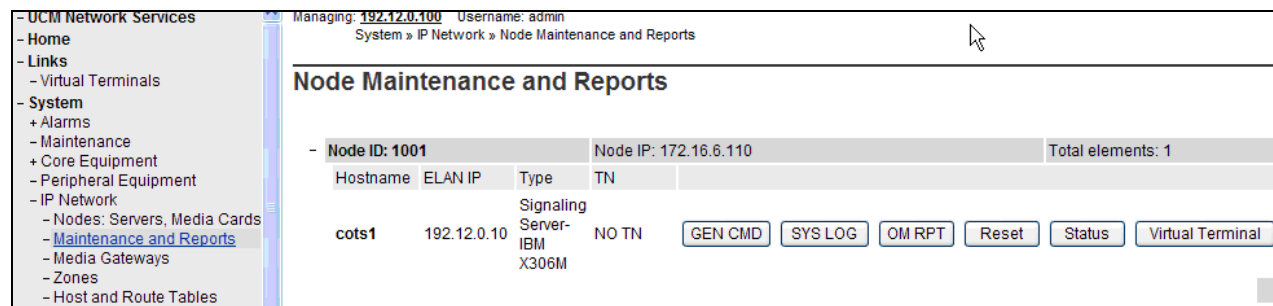
This section provides example verifications of the Avaya configuration with AT&T IP Flexible Reach service.

9.1. Avaya CS1000E Verifications

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

9.1.1 IP Network Maintenance and Reports Commands

Step 1 - From Element Manager, navigate to **System → IP Network → Maintenance and Reports** as shown below.



Step 2 - In the resultant screen on the right, click the **Gen CMD** button. The **General Commands** page is displayed as shown below.

Managing: 192.12.0.100 Username: admin
System » IP Network » Node Maintenance and Reports » General Commands

General Commands

Element IP : 192.12.0.10 Element Type : Signaling Server-IBM X306M

Group Command

IP address Number of pings

Click on a button to invoke a command.

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

Step 3 - To check the status of the SIP Gateway to Session Manager in the sample configuration, select “Sip” from the **Group** menu and “SIPGwShow” from the **Command** menu. Click **Run**. The example output below shows that the Session Manager (192.168.67.210, port 5060, TCP) has “SIPNPM Status” Active.

Managing: 192.12.0.100 Username: admin
System » IP Network » Node Maintenance and Reports » General Commands

General Commands

Element IP : 192.12.0.10 Element Type : Signaling Server-IBM X306M

Group Command

IP address Number of pings

```

SIPNPM Status           : Active
Primary Proxy IP address : 192.168.67.210
Primary Proxy port       : 5060
Primary Proxy Transport  : TCP
Secondary Proxy IP address : 0.0.0.0
Secondary Proxy port     : 5060
Secondary Proxy Transport : TCP
Primary Proxy2 IP address : 192.168.67.210
Primary Proxy2 port      : 5060
Primary Proxy2 Transport : TCP
Active Proxy             : Primary :Register Not Supported
Time To Next Registration : 0 Seconds
Channels Busy / Idle / Total : 0 / 12 / 12
Stack version            : 5.5.0.13
TLS Security Policy      : Security Disabled
  
```

Step 4 - As another example, the following screen shows the results of the “vtrkShow” **Command** from the “Vtrk” **Group**. The command was run with an active incoming PSTN call from the AT&T IP Flexible Reach service to an IP-UNISim telephone. One channel is shown busy, and 11 idle.

Managing: 192.12.0.100 Username: admin
System » IP Network » Node Maintenance and Reports » General Commands

General Commands

Element IP : 192.12.0.10 Element Type : Signaling Server-IBM X306M

Group Command Protocol Start Range

IP address Number of pings

```

-----
VTRK Summary
-----
VTRK status   : Active
Master status : On
VTRK REG Node : 1001
Protocol      : SIP
D-Channel    : 15
Customer     : 0
Channels Idle : 11
Channels Busy : 1
Channels Mbsy : 0
Channels Pend : 0
Channels Dsbl : 0
Channels Ukwn : 0
  
```

Step 5 - The next screen capture shows the output of the Command “SIPGWShowch” in Group “Sip” for channel 16³, while an incoming call was active (using channel 16) from PSTN via the AT&T IP Flexible Reach service to an IP-UNiStim phone. In the output below, the scroll bar was used to scroll down to the area showing that the codec in use was “G_729A_30MS”. Note that the Remote IP (192.168.67.125) is the IP Address of the inside private interface of the Avaya Aura® SBC.

General Commands

Element IP : 192.12.0.10 Element Type : Signaling Server-IBM X306M

Group Command

IP address Number of pings

```

Time To Next Registration : 0 Seconds
Channels Busy / Idle / Total : 1 / 11 / 12
Stack version              : 5.5.0.13
TLS Security Policy        : Security Disabled
SIP Gw Registration Trace  : OFF
Output Type Used           : RPT
Channel tracing            : 1
Handle   Chan Type      Direction CallState SIPState      RxState TxState
-----
0x9eed1a0 16 VTRK      Terminate BUSY      Ringing Sent      Connected Connected
Codec      AirTime FS   MS  Fax  DestNum RemoteIP      URI Scheme
-----
G 729A 30MS      796 yes m  no  4094 192.168.67.125  ::      SIP
nearEnd Msec policy = 0
farEnd Msec policy = 0
  
```

³ Note – See Section 5.2.2 Step 3 to determine the proper channel to display.

Step 6 - The next screen capture shows an alternate way to view similar information, but in this case, by searching for calls involving a specific directory number. The screen shows the output of the **Command** “SIPGwShownum” in **Group** “Sip” where DN **4094** was specified. An incoming call was active from PSTN via the AT&T IP Flexible Reach service to the IP-UNISTim phone with DN 4094. In the output below, the scroll bar was used to scroll down to the area showing that the codec in use was “**G_729A_30MS**”. Note that the Remote IP (**192.168.67.125**) is the IP Address of the inside private interface of the SBC.

General Commands

Element IP : 192.12.0.10 Element Type : Signaling Server-IBM X306M

Group **Sip** Command **SIPGwShownum** **Sip** **4094** **RUN**

IP address **192.12.0.100** Number of pings **3** **PING**

```

TLS Security Policy      : Security Disabled
SIP Gw Registration Trace : OFF
Output Type Used        : RPT
Channel tracing         : 1
Calling/Called Party Number: 4094
Numbering Plan Indicator: Undefined
Type Of Number: Undefined

```

Handle	Chan Type	Direction	CallState	SIPState	RxState	TxState
0x9eed1a0	16 VTRK	Terminate	BUSY	Ringing Sent	Connected	Connected
Codec	AirTime	FS	MS	Fax	DestNum	RemoteIP
G_729A_30MS	67	yes	m	no	4094	192.168.67.125
					URI	Scheme
					::	SIP

```

nearEnd Msec policy = 0
farEnd Msec policy = 0

```

Step 7 - The following screen shows a means to view IP UNISTim telephones. The screen shows the output of the **Command** “isetShow” in **Group** “Iset”. At the time this screen was captured, the “4094 1140E IP Deskphone” UNISTim telephone was involved in an active call with PSTN via the AT&T IP Flexible Reach service.

Element IP : 192.12.0.10 Element Type : Signaling Server-IBM X306M

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

IP address **192.12.0.100** Number of pings **3** **PING**

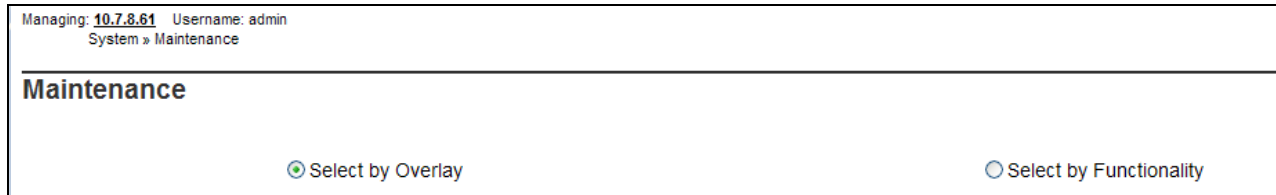
Set Information

IP Address	NAT	Model Name	Type	RegType	State	Up
172.16.6.107		1140E IP Deskphone	1140	Regular	online	1
172.16.6.108		IP Phone 2004 Phase 2	2004P2	Regular	online	1
172.16.6.109		1140E IP Deskphone	1140	Regular	busy	1
172.16.6.106		1140E IP Deskphone	1140	Regular	online	1

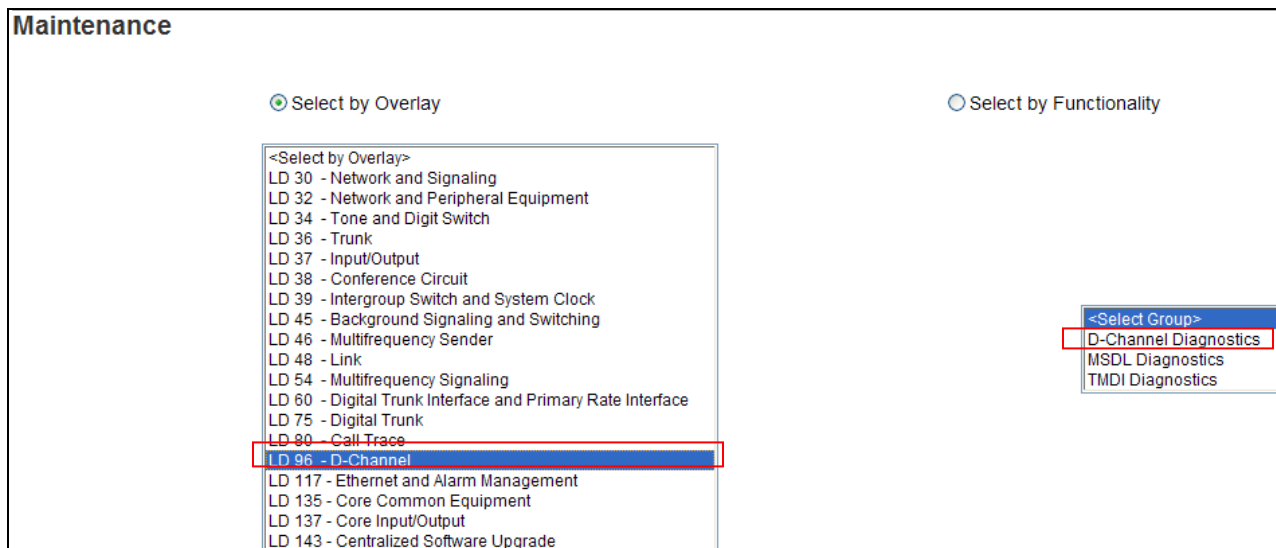
Total sets = 4

9.1.2 System Maintenance Commands

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



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



On the preceding screen, if “**LD 96 - D-Channel**” is selected on the left menu with “**D-Channel Diagnostics**” selected on the right menu, a screen such as the following is displayed. D-Channel number **15**, which is used in the sample configuration, is established “**EST**” and active “**ACTV**”.



D-Channel Diagnostics

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

DCH	DES	APPL_STATUS	LINK_STATUS	AUTO_RECV	PDCH	BDCH
<input type="radio"/> 015	VDCH	OPER	EST	ACTV		AUTO
<input type="radio"/> 020	private	DSBL	RST			AUTO

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

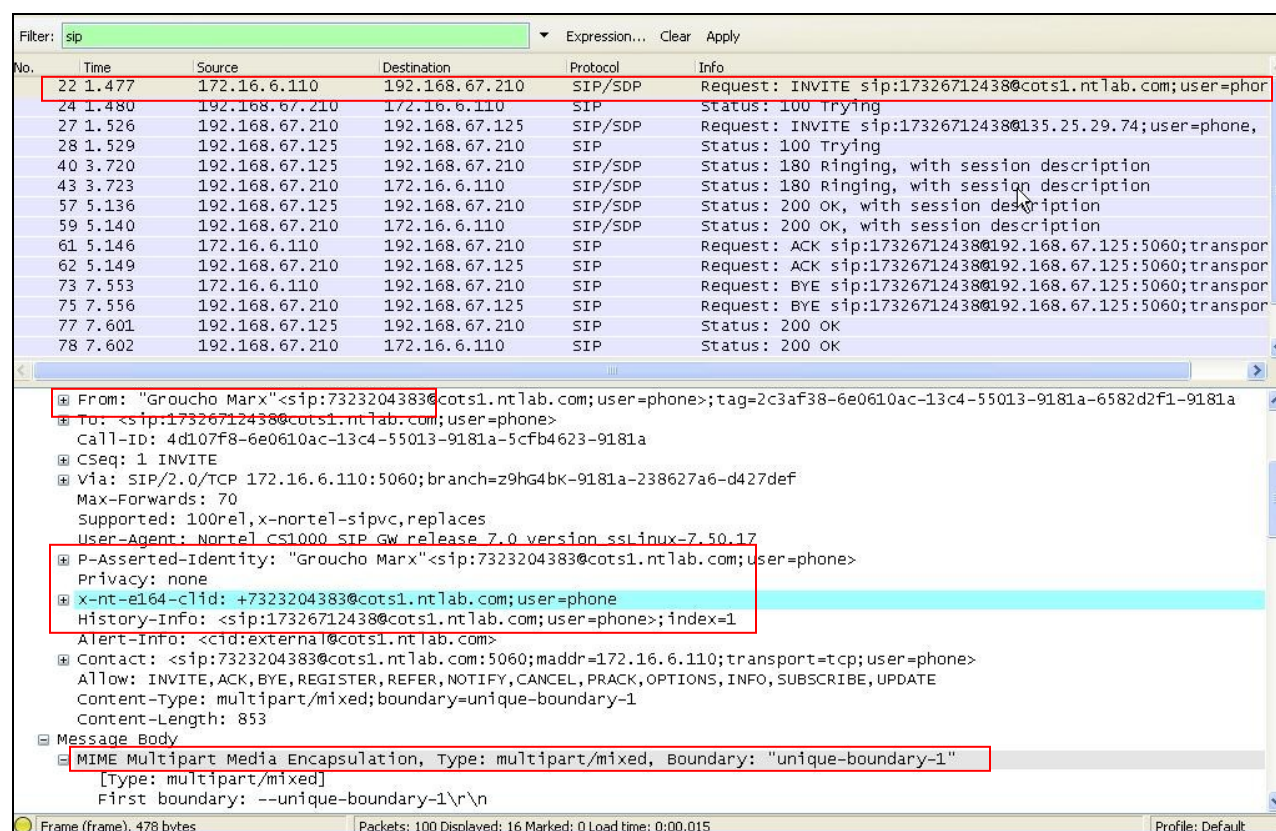
9.2. Wireshark Verifications

This section illustrates Wireshark traces for sample outbound and inbound calls using the reference configuration.

9.2.1 Example Outbound Call

This section illustrates an example outbound call from a CS1000E 1140E IP UNISim user with Directory Number 4094 to PSTN.

The following screen capture shows a Wireshark trace captured on the CPE private network, filtered on SIP messages. The INVITE message sent by the CS1000E is selected. As can be observed, in the sample configuration, the CS1000E sends the calling station's associated AT&T DID number (see **Section 5.8**) in SIP headers such as the From and P-Asserted-Identity headers. CS1000E proprietary headers such as "**x-nt-e164-clid**" can be observed, and such headers will be removed by the SBC. CS1000E **MIME** headers can be observed in the Message Body and will be removed by Session Manager. The **History-Info** header will be removed by the Avaya Aura® SBC.



No.	Time	Source	Destination	Protocol	Info
22	1.477	172.16.6.110	192.168.67.210	SIP/SDP	Request: INVITE sip:17326712438@cots1.ntlab.com;user=phor
24	1.480	192.168.67.210	172.16.6.110	SIP	Status: 100 Trying
27	1.526	192.168.67.210	192.168.67.125	SIP/SDP	Request: INVITE sip:17326712438@135.25.29.74;user=phone,
28	1.529	192.168.67.125	192.168.67.210	SIP	Status: 100 Trying
40	3.720	192.168.67.125	192.168.67.210	SIP/SDP	Status: 180 Ringing, with session description
43	3.723	192.168.67.210	172.16.6.110	SIP/SDP	Status: 180 Ringing, with session description
57	5.136	192.168.67.125	192.168.67.210	SIP/SDP	Status: 200 OK, with session description
59	5.140	192.168.67.210	172.16.6.110	SIP/SDP	Status: 200 OK, with session description
61	5.146	172.16.6.110	192.168.67.210	SIP	Request: ACK sip:17326712438@192.168.67.125:5060;transpor
62	5.149	192.168.67.210	192.168.67.125	SIP	Request: ACK sip:17326712438@192.168.67.125:5060;transpor
73	7.553	172.16.6.110	192.168.67.210	SIP	Request: BYE sip:17326712438@192.168.67.125:5060;transpor
75	7.556	192.168.67.210	192.168.67.125	SIP	Request: BYE sip:17326712438@192.168.67.125:5060;transpor
77	7.601	192.168.67.125	192.168.67.210	SIP	Status: 200 OK
78	7.602	192.168.67.210	172.16.6.110	SIP	Status: 200 OK

From:	To:	Call-ID:	CSeq:	Via:	Max-Forwards:	Supported:	User-Agent:	P-Asserted-Identity:	Privacy:	x-nt-e164-clid:	History-Info:	Alert-Info:	Contact:	Allow:	Content-Type:	Content-Length:	Message Body
"Groucho Marx"<sip:7323204383@cots1.ntlab.com;user=phone>;tag=2c3af38-6e0610ac-13c4-55013-9181a-6582d2f1-9181a	<sip:17326712438@cots1.ntlab.com;user=phone>	4d107f8-6e0610ac-13c4-55013-9181a-5cfb4623-9181a	1 INVITE	SIP/2.0/TCP 172.16.6.110:5060;branch=z9hg4bk-9181a-238627a6-d427def	70	100rel,x-nortel-sipvc,replaces	Nortel CS1000 SIP GW release 7.0 version sslinux-7.50.17	"Groucho Marx"<sip:7323204383@cots1.ntlab.com;user=phone>	none	+7323204383@cots1.ntlab.com;user=phone	<sip:17326712438@cots1.ntlab.com;user=phone>;index=1	<cid:external@cots1.ntlab.com>	<sip:7323204383@cots1.ntlab.com:5060;maddr=172.16.6.110;transport=tcp;user=phone>	INVITE,ACK,BYE,REGISTER,REFER,NOTIFY,CANCEL,PRACK,OPTIONS,INFO,SUBSCRIBE,UPDATE	multipart/mixed;boundary=unique-boundary-1	853	MIME Multipart Media Encapsulation, Type: multipart/mixed, Boundary: "unique-boundary-1"

The following screen capture shows the same Wireshark trace, however the Invite sent by Session Manager is selected. As can be observed from the selected section, the CS1000E proprietary header “**x-nt-e164-clid**” can still be observed, as is the **History-Info** header. Session Manager has inserted the **P-Location** header which will be removed by the Avaya Aura® SBC. However the CS1000E **MIME** header has been removed from the Message Body by Session Manager (see **Section 6.3.2**).

No.	Time	Source	Destination	Protocol	Info
22	1.477	172.16.6.110	192.168.67.210	SIP/SDP	Request: INVITE sip:17326712438@cots1.ntlab.com;user=phone
24	1.480	192.168.67.210	172.16.6.110	SIP	Status: 100 Trying
27	1.526	192.168.67.210	192.168.67.125	SIP/SDP	Request: INVITE sip:17326712438@135.25.29.74;user=phone,
28	1.529	192.168.67.125	192.168.67.210	SIP	Status: 100 Trying
40	3.720	192.168.67.125	192.168.67.210	SIP/SDP	Status: 180 Ringing, with session description
43	3.723	192.168.67.210	172.16.6.110	SIP/SDP	Status: 180 Ringing, with session description
57	5.136	192.168.67.125	192.168.67.210	SIP/SDP	Status: 200 OK, with session description
59	5.140	192.168.67.210	172.16.6.110	SIP/SDP	Status: 200 OK, with session description
61	5.146	172.16.6.110	192.168.67.210	SIP	Request: ACK sip:17326712438@192.168.67.125:5060;transport=
62	5.149	192.168.67.210	192.168.67.125	SIP	Request: ACK sip:17326712438@192.168.67.125:5060;transport=
73	7.553	172.16.6.110	192.168.67.210	SIP	Request: BYE sip:17326712438@192.168.67.125:5060;transport=
75	7.556	192.168.67.210	192.168.67.125	SIP	Request: BYE sip:17326712438@192.168.67.125:5060;transport=
77	7.601	192.168.67.125	192.168.67.210	SIP	Status: 200 OK
78	7.602	192.168.67.210	172.16.6.110	SIP	Status: 200 OK

x-nt-e164-clid: +7323204383@cots1.ntlab.com;user=phone [Expert Info (Note/Undecoded): Unrecognised SIP header (x-nt-e164-clid)] Alert-Info: <cid:external@cots1.ntlab.com> Contact: <sip:7323204383@cots1.ntlab.com:5060;maddr=172.16.6.110;transport=tcp;user=phone> Allow: INVITE, ACK, BYE, REGISTER, REFER, NOTIFY, CANCEL, PRACK, OPTIONS, INFO, SUBSCRIBE, UPDATE Content-Length: 261 Content-Type: application/sdp P-Asserted-Identity: "Groucho Marx" <sip:7323204383@192.168.64.130;user=phone> Remote-Party-ID: "Groucho Marx" <sip:7323204383@192.168.64.130;user=phone;party=calling;screen=no;privacy=off> History-Info: <sip:17326712438@cots1.ntlab.com;user=phone>;index=1,<sip:17326712438@192.168.64.130;user=phone>;index=1. Route: <sip:192.168.67.125;transport=tcp;lr;phase=terminating> P-Location: SM;origlocname="CS1k";termlocname="AA-SBC" [Expert Info (Note/Undecoded): Unrecognised SIP header (P-Location)] Max-Forwards: 66 Message Body Session Description Protocol Session Description Protocol Version (v): 0 Owner/Creator, Session Id (o): - 193 1 IN IP4 172.16.6.110 Owner Username: - Session ID: 193
--

The following screen shows a Wireshark trace of the same outbound call, but taken at the public (outside) interface of the Avaya Aura® SBC. A portion of the INVITE sent to AT&T is shown (frame 15). The use of UDP and destination port 5060 can be observed (see **Sections 7.2.2** and **7.2.4.1**). Note that the CS1000E proprietary header “**x-nt-e164-clid**” and the **History-Info** header have been removed

No.	Time	Source	Destination	Protocol	Info
15	17.733	192.168.64.130	135.25.29.74	SIP/SDP	Request: INVITE sip:17326712438@135.25.29.74, with sessio
16	17.771	135.25.29.74	192.168.64.130	SIP	Status: 100 Trying
22	20.243	135.25.29.74	192.168.64.130	SIP/SDP	Status: 180 Ringing, with session description
124	21.859	135.25.29.74	192.168.64.130	SIP/SDP	Status: 200 OK, with session description
126	21.878	192.168.64.130	135.25.29.74	SIP	Request: ACK sip:17326712438@135.25.29.74:5060;transport=
263	23.879	192.168.64.130	135.25.29.74	SIP	Request: BYE sip:17326712438@135.25.29.74:5060;transport=
264	23.914	135.25.29.74	192.168.64.130	SIP	Status: 200 OK

User Datagram Protocol, Src Port: sip (5060), Dst Port: sip (5060)

Session Initiation Protocol

Request-Line: INVITE sip:17326712438@135.25.29.74 SIP/2.0

Message Header

From: "Groucho Marx" <sip:7323204383@192.168.64.130>;tag=7d43a8c0-13c4-4e173719-5490b6bc-16dd42d

To: <sip:17326712438@135.25.29.74>

Call-ID: CXC-192-59a63cd0-7d43a8c0-13c4-4e173719-5490b6bc-5dc4a457@192.168.64.130

CSeq: 1 INVITE

Contact: <sip:7323204383@192.168.64.130:5060;transport=udp;user=phone>

Via: SIP/2.0/UDP 192.168.64.130:5060;branch=z9hG4bK-24ad1-4e173719-5490b6bc-1a373d62

Supported: 100rel,x-nortel-sipvc,replaces

User-Agent: Nortel CS1000 SIP Gw release_7.0 version_ssLinux-7.50.17 AVAYA-SM-6.1.2.0.612004

Privacy: none

P-Asserted-Identity: "Groucho Marx" <sip:7323204383@192.168.64.130>

Remote-Party-ID: "Groucho Marx" <sip:7323204383@192.168.64.130;user=phone>;party=calling;screen=no;privacy=off

Max-Forwards: 65

Allow: INVITE,ACK,BYE,REGISTER,REFER,NOTIFY,CANCEL,PRACK,OPTIONS,INFO,SUBSCRIBE,UPDATE

Content-Type: application/sdp

Content-Length: 267

Message Body

Session Description Protocol

Session Description Protocol Version (v): 0

Owner/Creator, Session Id (o): - 203 1 IN IP4 192.168.64.130

Session Name (s): -

Connection Information (c): IN IP4 192.168.64.130

Time Description, active time (t): 0 0

Media Description, name and address (m): audio 30240 RTP/AVP 18 0 8 100 111

Connection Information (c): IN IP4 192.168.64.130

Scrolling down further in the Message Body shows the following:

- The CS1000E offered G.729 and G.711 codecs as described in **Section 5.6**.
- RFC2833 DTMF Telephone Event 100 was set using the procedures described in **Section 5.10**.
- Annexb=no is specified, meaning G.729a is used.
- Theptime value of 30 provisioned in **Section 5.6** is also shown.

Message Body
Session Description Protocol
Session Description Protocol Version (v): 0
Owner/Creator, Session Id (o): - 203 1 IN IP4 192.168.64.130
Session Name (s): -
Connection Information (c): IN IP4 192.168.64.130
Time Description, active time (t): 0 0
Media Description, name and address (m): audio 30240 RTP/AVP 18 0 8 100 111
Media Type: audio
Media Port: 30240
Media Protocol: RTP/AVP
Media Format: ITU-T G.729
Media Format: ITU-T G.711 PCMU
Media Format: ITU-T G.711 PCMA
Media Format: DynamicRTP-Type-100
Media Format: DynamicRTP-Type-111
Connection Information (c): IN IP4 192.168.64.130
Media Attribute (a): rtpmap:100 telephone-event/8000
Media Attribute (a): rtpmap:111 X-nt-infreq/8000
Media Attribute (a): fmp:18 annexb=no
Media Attribute (a): fmp:100 0-15
Media Attribute (a): ptime:30
Media Attribute (a): sendrecv

The AT&T IP Flexible Reach service responds with a 200OK that agrees on the use of G.729a, as well as also specifying RFC2833 DTMF Telephone Event 100.

No.	Time	Source	Destination	Protocol	Info
15	17.733	192.168.64.130	135.25.29.74	SIP/SDP	Request: INVITE sip:17326712438@135.25.29.74, with sessio
16	17.771	135.25.29.74	192.168.64.130	SIP	Status: 100 Trying
22	20.243	135.25.29.74	192.168.64.130	SIP/SDP	Status: 180 Ringing, with session description
124	21.859	135.25.29.74	192.168.64.130	SIP/SDP	Status: 200 OK, with session description
126	21.878	192.168.64.130	135.25.29.74	SIP	Request: ACK sip:17326712438@135.25.29.74:5060;transport=
263	23.879	192.168.64.130	135.25.29.74	SIP	Request: BYE sip:17326712438@135.25.29.74:5060;transport=
264	23.914	135.25.29.74	192.168.64.130	SIP	Status: 200 ok

Frame 124: 957 bytes on wire (7656 bits), 957 bytes captured (7656 bits)
Ethernet II, Src: Cisco_01:c5:a1 (00:22:55:01:c5:a1), Dst: 00:ca:fe:85:58:80 (00:ca:fe:85:58:80)
Internet Protocol, Src: 135.25.29.74 (135.25.29.74), Dst: 192.168.64.130 (192.168.64.130)
User Datagram Protocol, Src Port: sip (5060), Dst Port: sip (5060)
Session Initiation Protocol
Status-Line: SIP/2.0 200 OK
Message Header
Message Body
Session Description Protocol
Session Description Protocol Version (v): 0
Owner/Creator, Session Id (o): Sonus_UAC 2738 21156 IN IP4 135.25.29.74
Session Name (s): SIP Media Capabilities
Connection Information (c): IN IP4 135.25.29.74
Time Description, active time (t): 0 0
Media Description, name and address (m): audio 18144 RTP/AVP 18 100
Media Attribute (a): rtpmap:18 G729/8000
Media Attribute (a): fmtp:18 annexb=no
Media Attribute (a): rtpmap:100 telephone-event/8000
Media Attribute (a): fmtp:100 0-15
Media Attribute (a): sendrecv
Media Attribute (a): maxptime:30

Changing the display filter to **rtp**, the media streams for this call are displayed. Note that the UDP ports used are within the range defined in **Section 7.2.3**. Also note that G.729 was the codec used.

No.	Time	Source	Destination	Protocol	Info
190	8.769	192.168.64.130	135.25.29.74	RTP	PT=ITU-T G.729, SSRC=0x5B3A3A28, Seq=9508, Time=117674039
191	8.792	135.25.29.74	192.168.64.130	RTP	PT=ITU-T G.729, SSRC=0x4B3C23F7, Seq=93, Time=22320
192	8.796	192.168.64.130	135.25.29.74	RTP	PT=ITU-T G.729, SSRC=0x5B3A3A28, Seq=9509, Time=117674063
193	8.822	135.25.29.74	192.168.64.130	RTP	PT=ITU-T G.729, SSRC=0x4B3C23F7, Seq=94, Time=22560
194	8.827	192.168.64.130	135.25.29.74	RTP	PT=ITU-T G.729, SSRC=0x5B3A3A28, Seq=9510, Time=117674087
195	8.852	135.25.29.74	192.168.64.130	RTP	PT=ITU-T G.729, SSRC=0x4B3C23F7, Seq=95, Time=22800
196	8.859	192.168.64.130	135.25.29.74	RTP	PT=ITU-T G.729, SSRC=0x5B3A3A28, Seq=9511, Time=117674111
197	8.882	135.25.29.74	192.168.64.130	RTP	PT=ITU-T G.729, SSRC=0x4B3C23F7, Seq=96, Time=23040
198	8.886	192.168.64.130	135.25.29.74	RTP	PT=ITU-T G.729, SSRC=0x5B3A3A28, Seq=9512, Time=117674135

Frame 8: 84 bytes on wire (672 bits), 84 bytes captured (672 bits)
Ethernet II, Src: Cisco_01:c5:a1 (00:22:55:01:c5:a1), Dst: 00:ca:fe:85:58:80 (00:ca:fe:85:58:80)
Internet Protocol, Src: 135.25.29.74 (135.25.29.74), Dst: 192.168.64.130 (192.168.64.130)
User Datagram Protocol, Src Port: 17692 (17692), Dst Port: 28694 (28694)
Source port: 17692 (17692)
Destination port: 28694 (28694)
Length: 50
Checksum: 0x0000 (none)
Real-Time Transport Protocol

9.2.2 Example Inbound Call

This section illustrates an inbound call from PSTN telephone 732-671-2438 to AT&T IP Flexible Reach DID 732-320-4383.

The following screen shows a Wireshark trace taken from the public interface of the Avaya Aura® SBC. Frame 6 shows an INVITE from AT&T, and is expanded to illustrate the contents of the message header and message body. Note that AT&T sends the calling party number 7326712438

in the From, Contact, and PAI headers. The Request-URI and To header both contain the dialed AT&T DID 7323204383. In the message body, note that the AT&T SDP offer lists G.729A and G.711mu. RFC2833 DTMF Telephone Event 100 is also specified.

Filter: sip

No.	Time	Source	Destination	Protocol	Info
6	5.596	135.25.29.74	192.168.64.130	SIP/SDP	Request: INVITE sip:7323204383@192.168.64.130:5060, with
7	5.601	192.168.64.130	135.25.29.74	SIP	Status: 100 Trying
8	5.672	192.168.64.130	135.25.29.74	SIP	Status: 180 Ringing
11	6.985	192.168.64.130	135.25.29.74	SIP/SDP	Status: 200 OK, with session description
16	7.155	135.25.29.74	192.168.64.130	SIP	Request: ACK sip:4094@192.168.64.130:5060;transport=udp;L
179	9.592	192.168.64.130	135.25.29.74	SIP	Request: BYE sip:7326712438@135.25.29.74:5060;transport=L
181	9.626	135.25.29.74	192.168.64.130	SIP	Status: 200 OK

Session Initiation Protocol

Request-Line: INVITE sip:7323204383@192.168.64.130:5060 SIP/2.0

Message Header

Via: SIP/2.0/UDP 135.25.29.74:5060;branch=z9hG4bKsd6j41102o3g5h88t6j0.1

From: <sip:7326712438@135.25.29.74:5060>;tag=ds5c1c6d23

To: <sip:7323204383@192.168.64.130>

Call-ID: ASE_1310129676833_32579_null_135.25.250.88

CSeq: 1 INVITE

Max-Forwards: 66

Contact: <sip:7326712438@135.25.29.74:5060;transport=udp>

Allow: INVITE, ACK, CANCEL, BYE, INFO, PRACK

Accept: application/sdp, application/isup, application/dtmf, application/dtmf-relay, multipart/mixed

P-Charging-Vector: icid-value=43c195a0-0bcb-1000-00-00-10-6b-01-ce-d7;icid-generated-at=135.25.30.237

P-Asserted-Identity: <sip:7326712438@135.25.29.74:5060>

Content-Length: 259

Content-Disposition: session; handling=required

Content-Type: application/sdp

Message Body

Session Description Protocol

Session Description Protocol Version (v): 0

Owner/Creator, Session Id (o): Sonus_UAC 795 3435 IN IP4 135.25.29.74

Session Name (s): SIP Media Capabilities

Connection Information (c): IN IP4 135.25.29.74

Time Description, active time (t): 0 0

Media Description, name and address (m): audio 17694 RTP/AVP 18 0 100

Media Attribute (a): rtpmap:18 G729/8000

Media Attribute (a): rtpmap:0 PCMU/8000

Media Attribute (a): rtpmap:100 telephone-event/8000

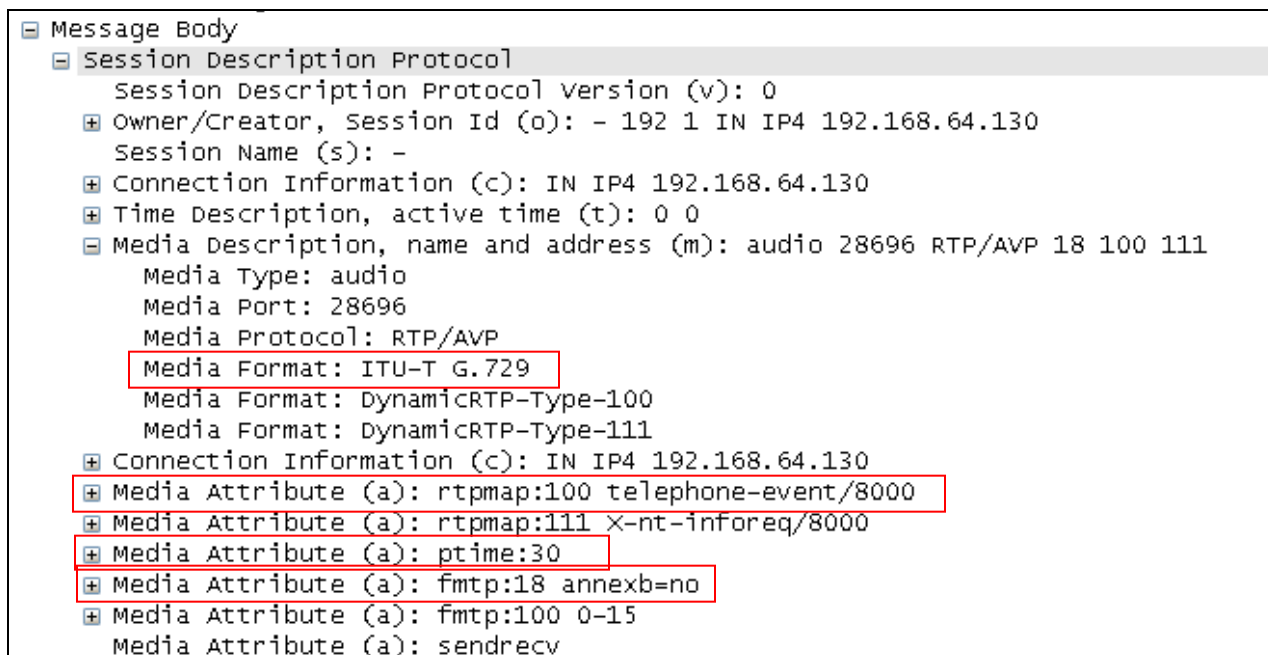
Session Initiation Protocol (sip), 1033 bytes

Packets: 184 Displayed; 7 Marked; 0 Load time: 0:00.015

Profile: Default

The following screen shows the 200 OK in frame 11 expanded to show the contents of the SDP Message Body from the CS1000E containing the following:

- G.729A with annexb=no
- RFC2833 DTMF Telephone Event 100
- Ptime=30



Proceeding to the Wireshark from the inside of the SBC for this same call, Session Manager will modify the Request-URI from 732-320-4383 to CS1000E Directory Number 4094, an IP UNISim 1140E telephone.

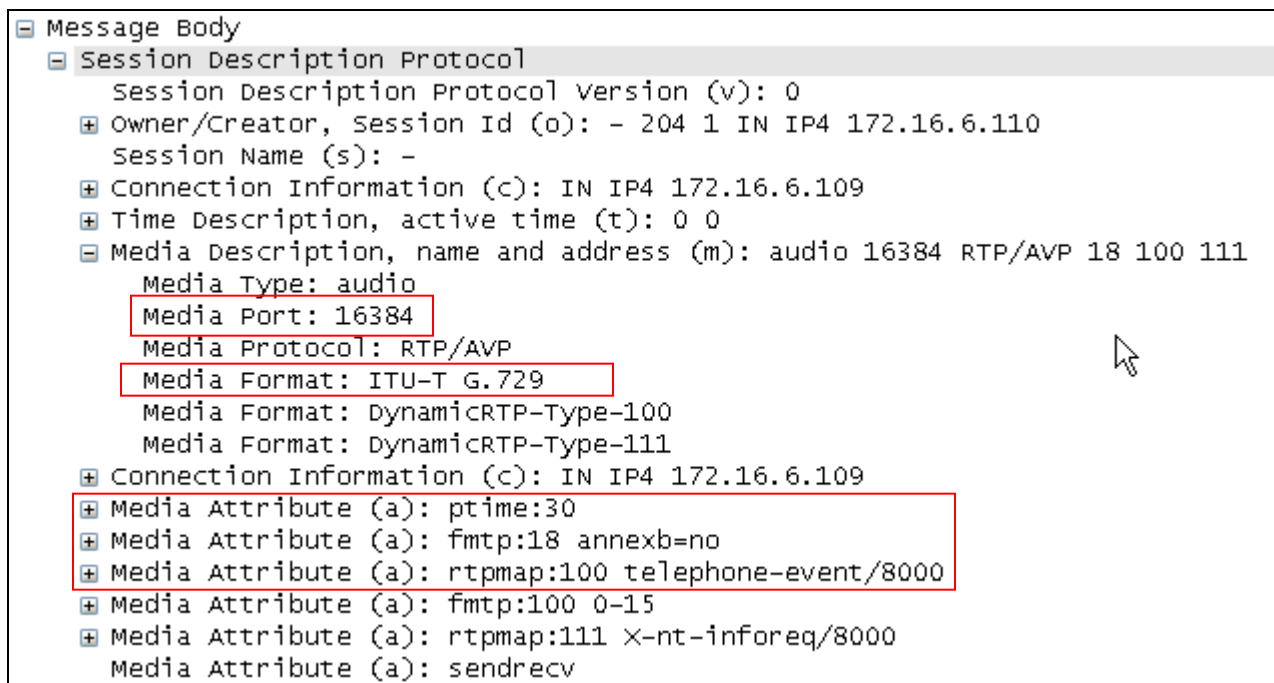
The following screen capture shows the INVITE message (frame 47) from the Avaya Aura® SBC inside interface to Session Manager. The message body contains the same called number and SDP offer information as shown in the previous screenshots.

No.	Time	Source	Destination	Protocol	Info
47	8.060	192.168.67.125	192.168.67.210	SIP/SDP	Request: INVITE sip:7323204383@cotts1.ntlab.com:5060, with
48	8.062	192.168.67.210	192.168.67.125	SIP	Status: 100 Trying
51	8.067	192.168.67.210	172.16.6.110	SIP/SDP	Request: INVITE sip:4094@cotts1.ntlab.com:5060, with sessi
54	8.080	172.16.6.110	192.168.67.210	SIP	Status: 100 Trying
56	8.098	172.16.6.110	192.168.67.210	SIP	Status: 180 Ringing
58	8.100	192.168.67.210	192.168.67.125	SIP	Status: 180 Ringing
71	9.082	172.16.6.110	192.168.67.210	SIP/SDP	Status: 200 OK, with session description
75	9.086	192.168.67.210	192.168.67.125	SIP/SDP	Status: 200 OK, with session description
79	9.261	192.168.67.125	192.168.67.210	SIP	Request: ACK sip:4094@cotts1.ntlab.com:5060;maddr=172.16.6

Session Initiation Protocol					
Request-Line: INVITE sip:4094@cotts1.ntlab.com:5060 SIP/2.0					
Message Header					
Record-Route: <sip:74cbe78d@192.168.67.210;transport=tcp;lr>					
Record-Route: <sip:192.168.67.209:15060;lr;sap=986408461*1*016asm-callprocessing.sar-784160832~1310158964824~166572103>					
Record-Route: <sip:74cbe78d@192.168.67.210;transport=tcp;lr>					
From: <sip:7326712438@135.25.29.74:5060>;tag=7d43a8c0-13c4-4e173767-5491e7d5-45bb1a37					
To: <sip:7323204383@cotts1.ntlab.com>					
Call-ID: CXC-195-59a64050-7d43a8c0-13c4-4e173767-5491e7d5-6140d4d1@135.25.29.74					
CSeq: 1 INVITE					
Contact: <sip:7326712438@192.168.67.125:5060;transport=tcp>					
Via: SIP/2.0/TCP 192.168.67.210;branch=z9hG4bKCOA843D1FFFFFFFFF1534601012391-AP;ft=60161					
Via: SIP/2.0/TCP 192.168.67.209:15070;branch=z9hG4bKCOA843D1FFFFFFFFF1534601012391					
Via: SIP/2.0/TCP 192.168.67.209:15070;branch=z9hG4bKCOA843D1FFFFFFFFF1534611012389					
Via: SIP/2.0/TCP 192.168.67.209:15070;branch=z9hG4bKCOA843D1FFFFFFFFF1534611012388					
Via: SIP/2.0/TCP 192.168.67.210;branch=z9hG4bK-24add-4e173767-5491e7d5-70311ba4-AP;ft=59422					
Via: SIP/2.0/TCP 192.168.67.125:5060;branch=z9hG4bK-24add-4e173767-5491e7d5-70311ba4					
Accept: application/sdp, application/isup, application/dtmf, application/dtmf-relay, multipart/mixed					
P-Charging-vector: icid-value=603ef0a0-0bef-1000-00-00-10-6b-01-ce-d7;icid-generated-at=135.25.30.237					
P-Asserted-Identity: <sip:7326712438@135.25.29.74:5060>					
Allow: INVITE,ACK,CANCEL,BYE,INFO,PRACK					
Content-Disposition: session;handling=required					
Content-Type: application/sdp					
Content-Length: 261					
Route: <sip:172.16.6.110;transport=tcp;lr;phase=terminating>					

The following screen capture shows the same Wireshark trace but expands the 200 OK in frame 71 sent by the CS1000E when the user answers the call. The message body area is expanded to show the following:

- Media port within range 16384-32767
- G.729A with annexb=no
- RFC2833 DTMF Telephone Event 100
- Ptime=30



9.3. System Manager and Session Manager Verification

This section contains verification steps that may be performed using System Manager for Session Manager verification.

9.3.1 Verify SIP Entity Link Status

Log in to System Manager. Expand **Elements** → **Session Manager** → **System Status** → **SIP Entity Monitoring**.

From the list of monitored entities, select an entity of interest, such as “AuraSBC”. Under normal operating conditions, the **Link Status** should be “Up” as shown in the example screen below. The **Reason Code** column indicates that the Avaya Aura® SBC has responded to SIP OPTIONS from Session Manager with a SIP 404 message, which is sufficient for SIP Link Monitoring to consider the link up.

SIP Entity, Entity Link Connection Status							
This page displays detailed connection status for all entity links from all Session Manager instances to a single SIP entity.							
All Entity Links to SIP Entity: AA-SBC_to_AT&T							
Summary View							
1 Item Refresh Filter: Enable							
Details	Session Manager Name	SIP Entity Resolved IP	Port	Proto.	Conn. Status	Reason Code	Link Status
► Show	SM61	192.168.67.125	5060	TCP	Up	404 Not found	Up

Return to the list of monitored entities, and select another entity of interest, such as “CS1000-R75”. Under normal operating conditions, the **Link Status** should be “Up” as shown in the example screen below. In this case, “Show” under Details was selected to view additional information.

All Entity Links to SIP Entity: CS1K							
Summary View							
1 Item Refresh							Filter: Enable
Details	Session Manager Name	SIP Entity Resolved IP	Port	Proto.	Conn. Status	Reason Code	Link Status
▼ Hide	SM61	172.16.6.110	5060	TCP	Up	200 OK	Up
Time Last Down		Time Last Up	Last Message Sent		Last Message Response	Last Response Latency (ms)	
Jun 24, 2011 8:00:51 PM EDT		Jun 24, 2011 8:02:44 PM EDT	Jul 8, 2011 5:59:54 PM EDT			9	

9.3.2 Call Routing Test

The Call Routing Test verifies the routing for a particular source and destination. To run the routing test, expand **Elements** → **Session Manager** → **System Tools** → **Call Routing Test**.

The following screen shows an example call routing test for an inbound call to the CS1000K via AT&T. Note that the called number was AT&T DID 7323204383 and Session Manager converts this to CS1000E extension 4093 before routing the call to the CS1000E.

Call Routing Test

This page allows you to test SIP routing algorithms on Session Manager instances. Enter information about a SIP INVITE to how it will be routed based on current administration.

SIP INVITE Parameters

Called Party URI**Calling Party URI****Day Of Week****Time (UTC)****Called Session Manager Instance****Calling Party Address****Session Manager Listen Port****Transport Protocol**

Routing Decisions

Route < sip:4094@cots1.ntlab.com > to SIP Entity CS1K (172.16.6.110). Terminating Location is CS1K.

Routing Decision Process

NRP Adaptations: CS1K_AT&T_AA-SBC applied.

BEGIN EMERGENCY CALL CHECK: Determining if this is a call to an emergency number.

Originating Location is AA-SBC. Using digits < 7323204383 > and host < cots1.ntlab.com > for routing.

NRP Dial Patterns: No matches for digits < 7323204383 > and domain < cots1.ntlab.com >.

NRP Dial Patterns: No matches for digits < 7323204383 > and domain < ntlab.com >.

NRP Dial Patterns: Found a Dial Pattern match for pattern < 732320 > Min/Max length 10/10 and domain < null >.

NRP Routing Policies: Ranked destination NRP Sip Entities: CS1K

NRP Routing Policies: Removing disabled routes.

NRP Routing Policies: Ranked destination NRP Sip Entities: CS1K

END EMERGENCY CALL CHECK: This is not an emergency call.

Adapting and proxying for SIP Entity CS1K.

NRP Entity Links: Found direct link to destination. Link uses TCP to port 5060.

NRP Adaptations: CS1K applied.

NRP Adaptations: Request-URI set to sip:4094@cots1.ntlab.com

NRP Adaptations: Request URI set to sip:4094@cots1.ntlab.com

Route < sip:4094@cots1.ntlab.com > to SIP Entity CS1K (172.16.6.110). Terminating Location is CS1K.

9.4. Avaya Aura® Session Border Controller Verification

This section contains verification steps that may be performed using the Avaya Aura® Session Border Controller.

9.4.1 Status Tab

Avaya Aura® SBC status information is available via the **Status** tab.



For example, there is a SIP heading on the left menu that can be expanded as shown below.

- ⊕ Registration
- ⊖ SIP
 - active-association
 - active-call-peers
 - active-call-summary
 - active-calls
 - active-session

In the example below, **active-calls** was selected from the left, revealing details about an active outbound call from a CS1000E 1140E Unistim station to PSTN. A scroll bar allows viewing of information about the active inbound call.

The screenshot shows the AVAYA aura Status page. The left sidebar lists various configuration options under 'Status Summary', including Netfilter, Policy, Presence, Profiling, RADIUS, Registration, and SIP. The main content area is titled 'active-calls - currently active calls'. It features a 'View' dropdown set to 'Basic' and a 'Search' button. Below this is a table with columns 'session-id', 'from', and 'to'. The table contains one entry for session 0x04C2DBB81EC1D68C, showing a call from 'Groucho Marx' to a SIP address. A 'Refresh' button and a timestamp 'Taken Jul 8, 2011 2:34:17 PM' are also visible. At the bottom, it indicates 'Page 1 of 1 showing 25 items' and includes a copyright notice for NNOS-E.

Additional information about the call is available by moving the bottom scroll bar to the right (not shown).

9.4.2 Call Logs

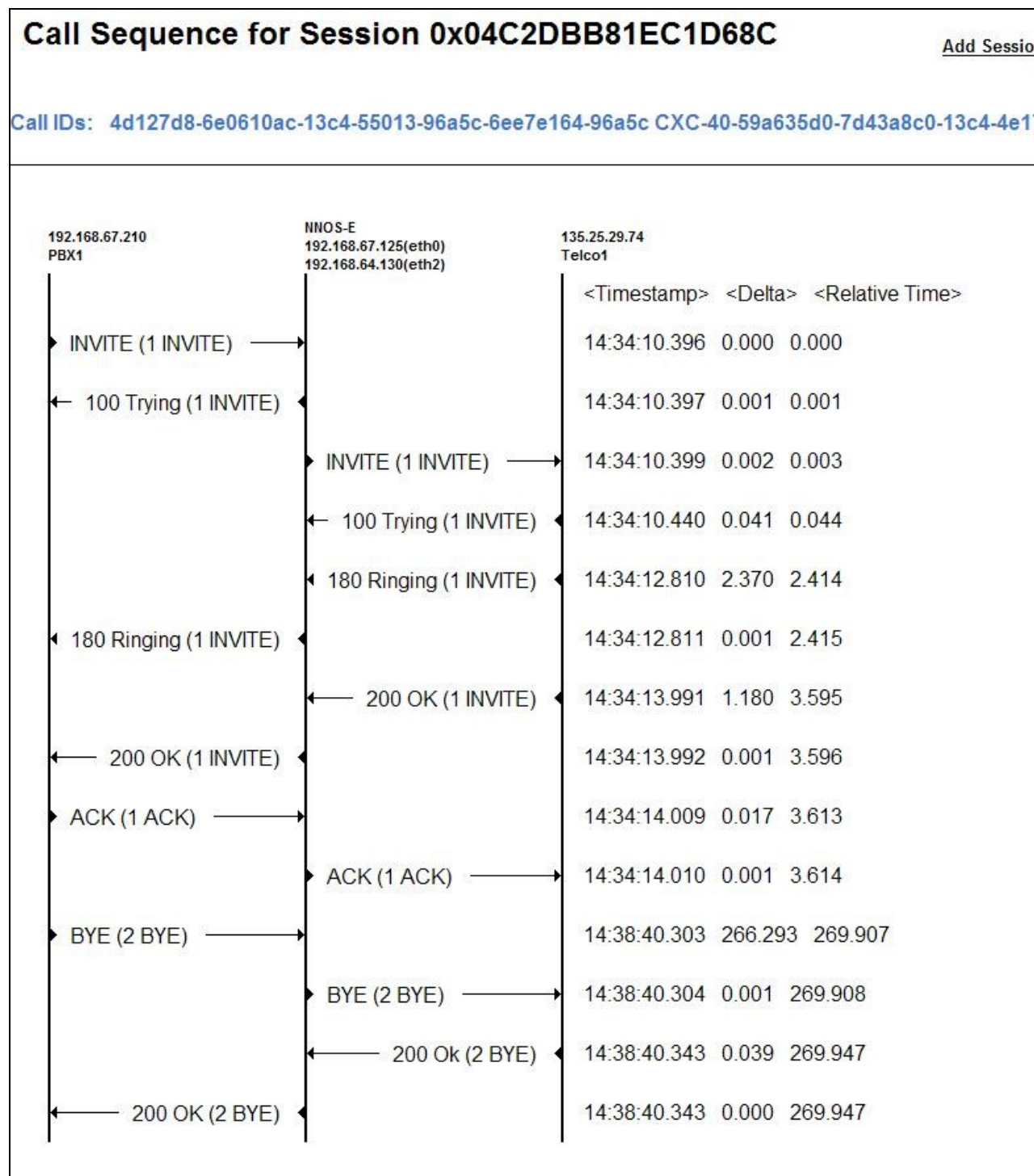
The **Call Logs** tab can provide useful diagnostic or troubleshooting information. In the following screen, the **SIP Messages** search capability can be observed.

The following screen shows a portion of the **Call Logs** tab selected after making an outbound call.

The screenshot shows the AVAYA aura Call Logs page. The left sidebar has a 'Select:' section with options like Sessions, User Sessions, Devices, SIP Messages, H323 Messages, Accounting Calls, Monitored URIs, Monitored Calls, Files, and Database. The main area has a 'Search Type' dropdown set to 'All Sessions' and a 'View All Sessions' button. Below this is a table with columns 'Created', 'Method', 'Result', 'From', 'To', and 'Call ID'. The first row shows a call log entry for a session created on Fri 2011-07-08 at 14:34:10.397, with method INVITE and result Bye. A red box highlights the 'Session Diagram' link in the 'Result' column. Other links like 'Detail', 'Call Diagram', 'Call Record', etc., are also visible.

As shown below, select the **Session Diagram** link to view a ladder diagram for the session.

For example, the following screen shows a portion of the ladder diagram for the outbound call. Note that the activity for both the inside private and outside public side of the SBC can be seen.



At the top right of the screen, the session may be saved as a text or XML file. If the session is saved as an XML file, using the **Save as XML** link, the xml file can be provided to support personnel that can open the session on another Avaya Aura® SBC for analysis.

Back

Save as text Save as XML **TEXT**

Call Sequence for Session 0x04C2DBB81EC1D68C

Add Session

The **Call Logs** tab also provides the capability to see modifications made to SIP headers by the SBC. Below the ladder diagram is another screen section. Using the same Session Diagram as shown above, Scrolling down to the INVITE message sent by the SBC to AT&T. The **More** and **See changes** links have been selected to expand the SIP message display and enable observation of the changes made by the SBC to the **Revised** message, as compared to the **Original** INVITE received from Session Manager.

AVAYA aura

acme packet powered

Call Logs

Home Configuration Status Call Logs Event Logs Actions Services Keys Access Tools

Select:

- Sessions
- User Sessions
- Devices
- SIP Messages
- H323 Messages
- Accounting Calls
- Monitored URIs
- Monitored Calls
- Files
- Database Archives

Sessions

192.168.67.210 PBX1

NNOS-E

192.168.67.125(eth0)

192.168.64.130(eth2)

135.25.29.74 Telco1

<Timestamp>

<Delta>

<Relative Time>

INVITE (1 INVITE)

100 Trying (1 INVITE)

Original: From: "Groucho Marx" <sip:7323204383@cots1.ntlab.com;user=phone>;tag=2c65b38-6e0610ac-13c4-55013-96a5c-7c7auca-96a5c

Revised: From: "Groucho Marx" <sip:7323204383@192.168.64.130>;tag=7d43a8c0-13c4-4e174da2-54e8bf0f-b04bf6f

Original: To: <sip:17326712438@cots1.ntlab.com;user=phone>

Revised: To: <sip:17326712438@135.25.29.74>

Original: Call-ID: 4d127d8-6e0610ac-13c4-55013-96a5c-6ee7e164-96a5c

Revised: Call-ID: CXC-40-59a635d0-7d43a8c0-13c4-4e174da2-54e8bf0f-4d777949@192.168.64.130

CSeq: 1 INVITE

Original: Via: SIP/2.0/TCP 192.168.67.210;branch=z9hG4bKCA843D1FFFFFFFFF1534601013552-AP;ft=60161

Revised: Via: SIP/2.0/UDP 192.168.64.130:5060;branch=z9hG4bK-24d7f-4e174da2-54e8bf0f-6233847c

Original: Via: SIP/2.0/TCP 192.168.67.209:15070;branch=z9hG4bKCA843D1FFFFFFFFF1534601013552

Revised:

Original: Via: SIP/2.0/TCP 192.168.67.209:15070;branch=z9hG4bKCA843D1FFFFFFFFF1534611013550

Revised:

Scrolling down further, the following screen shows that the SBC has deleted the “x-nt-e164-clid” and “Alert-Info” headers as defined in **Section 7.2.5**.

Original: x-nt-e164-clid: +7323204383@cots1.ntlab.com;user=phone

Revised:

Original: Alert-Info: <cid:external@cots1.ntlab.com>

Revised:

Scrolling down further the Avaya Aura® SBC removes the History-Info header as well as the P-Location Header as defined in **Section 7.2.5**.

JF; Reviewed:
SPOC 11/1/2011

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

112 of 115
CS1KSMASBCIPFR

Original: History-Info:
<sip:17326712438@cots1.ntlab.com;user=phone>;index=1,<sip:17326712438@192.168.64.130;user=phone>;index=1.1
Revised:
Original: P-Location: SM;origlocname="CS1K";termlocname="AA-SBC"
Revised:

10. Conclusion

As illustrated in these Application Notes, Avaya Communication Server 1000E Release 7.5, Avaya Aura® Session Manager Release 6.1, and the Avaya Aura® Session Border Controller Release 6.0.2 can be configured to interoperate successfully with AT&T IP Flexible Reach service via either AVPN or MIS-PNT transport. This solution allows Avaya Communication Server 1000E user access to the PSTN using an AT&T IP Flexible Reach service connection.

11. References

This section references documentation relevant to these Applications.

11.1. Avaya

Avaya product documentation, including the following, is available at <http://support.avaya.com>

Avaya Aura™ Session Manager/System Manager

- [1] *Administering Avaya Aura™ Session Manager*, Doc ID 03-603324, Issue 4, Feb 2011 available at <http://support.avaya.com/css/P8/documents/100082630>
- [2] *Installing and Configuring Avaya Aura™ Session Manager*, Doc ID 03-603473 Issue 2, November 2010 available at <http://support.avaya.com/css/P8/documents/100089152>
- [3] *Maintaining and Troubleshooting Avaya Aura™ Session Manager*, Doc ID 03-603325, Issue 3.1, March 2011 available at <http://support.avaya.com/css/P8/documents/100089154>
- [4] *Administering Avaya Aura™ System Manager*, Document Number 03-603324, June 2010 available at <http://support.avaya.com/css/P8/documents/100089681>

Avaya Communication Server 1000E

- [5] *Communication Server 1000 Release 7.0 and Acme Packet Net-Net 6.2.0 Configuration Guide For Use with AT&T IP Flexible Reach*, Issue 1.1, 4/12/2011 available at: <http://support.avaya.com/css/P8/documents/100129069>
- [6] IP Peer Networking Installation and Commissioning, Release 7.5, Document Number NN43001-313
- [7] Unified Communications Management Common Services Fundamentals, Avaya Communication Server 1000E Release 7.5, Document Number NN43001-116
- [8] Network Routing Service Fundamentals, Release 7.5, Document Number NN43001-130, Issue 03.02
- [9] Co-resident Call Server and Signaling Server Fundamentals, Avaya Communication Server 1000E Release 7.5, Document Number NN43001-509
- [10] Signaling Server and IP Line Fundamentals, Avaya Communication Server 1000E Release 7.5, Document Number NN43001-125

- [11] Avaya Call Pilot® information can be found at:
<http://support.avaya.com/css/Products/P0712>

Avaya Aura™ Session Border Controller

- [12] *Installing and Configuring Avaya Aura® Session Border Controller, Release 6.0.1, November 2010* available at:
<http://support.avaya.com/css/P8/documents/100134970>
- [13] *Avaya Aura™ SBC System Administration Guide, V.6.0, 2010* available at:
<http://support.avaya.com/css/P8/documents/100111137>
- [14] *Applications Notes for Avaya Aura™ Communication Manager 6.0, Avaya Aura™ Session Manager 6.0 and Avaya Aura™ Session Border Controller with AT&T IP Flexible Reach SIP Trunk Service – Issue 1.1, 2/18/2011* available at:
<https://devconnect.avaya.com/public/download/dyn/CMSMAASBC60IPFR.pdf>

Additional Avaya Application Notes on AT&T IP Flexible Reach service, tested via Avaya DevConnect, are available at the following link:

<https://devconnect.avaya.com/dc/Public/WebListings/v2/CompanyWebListing.aspx?CompanyId=2262>

11.2. AT&T IP Flexible Reach service.

Information regarding the AT&T IP Flexible Reach Service can be found at –

<http://www.business.att.com/enterprise/Service/business-voip-enterprise/network-based-voip-enterprise/ip-flexible-reach-enterprise/>

©2011 Avaya Inc. All Rights Reserved.

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

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