



Avaya Solution & Interoperability Test Lab

Applications Notes for Avaya Communication Server 1000E Release 7.5 with Avaya Aura® Session Manager 6.1 and Avaya Session Border Controller for Enterprise with AT&T IP Toll Free SIP Trunk Service – Issue 1.0

Abstract

These Application Notes describe the steps for configuring Avaya Aura® Session Manager, Avaya Communication Server 1000E and Avaya Session Border Controller for Enterprise with the AT&T IP Toll Free service using **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. Avaya Session Border Controller for Enterprise is the point of connection between Avaya Aura® Session Manager and the AT&T IP Toll Free service and is used to not only secure the SIP trunk, but also to make adjustments to the SIP signaling for interoperability. In addition, Avaya Aura® Contact Center is used to provide Agent access for Avaya Communication Server 1000E

The AT&T IP Toll Free service is a managed Voice over IP (VoIP) communications solution that provides toll-free services over SIP trunks. Note that these Application Notes do NOT cover the AT&T IP Transfer Connect service option of the AT&T IP Toll Free service.

AT&T is a member of 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.	Coverage to Voicemail	7
2.3.2.	Coverage to Voicemail	8
2.4.	Support.....	8
2.4.1.	AT&T	8
2.4.2.	Avaya.....	8
3.	Reference Configuration	9
3.1.	Illustrative Configuration Information	11
4.	Equipment and Software Validated.....	12
5.	Configure Avaya CS1000E	13
5.1.	Node and Key IP Addresses	14
5.2.	Virtual D-Channel, Routes and Trunks.....	16
5.2.1.	Virtual D-Channel Configuration	16
5.2.2.	Routes and Trunks Configuration.....	16
5.3.	SIP Trunk to Session Manager	19
5.4.	Routing of Inbound Numbers to Avaya CS1000E	23
5.5.	Zones	24
5.6.	Codec Parameters	25
5.6.1.	Media Gateway Codec Configuration	25
5.6.2.	IP Telephony Node Codec Configuration	27
5.7.	Avaya CS1000E Agent Access Provisioning	28
5.7.1.	Avaya CS1000E IP Agent Phone	29
5.7.2.	Avaya CS1000E Auto Call Distribution (ACD).....	33
5.7.3.	Avaya CS1000E Control DN (CDN)	34
5.7.4.	Analog Fax Line	35
5.8.	Customer Information	35
5.8.1.	Caller ID Provisioning.....	35
5.9.	Changing RFC2833 DTMF Telephone Event Type	37
5.10.	Configuration Backup	38
6.	Configure Avaya Aura® Session Manager Release 6.1	39
6.1.	SIP Domain.....	41
6.2.	Locations.....	41
6.2.1.	Location for Avaya CS1000E	42
6.2.2.	Location for Avaya Session Border Controller for Enterprise	43
6.3.	Configure Adaptations	43
6.3.1.	Adaptation for Avaya CS1000E Entity	44
6.3.2.	Adaptation for Avaya CS1000E to Avaya SBCE Entity	46
6.3.3.	List of Adaptations.....	47

6.4.	SIP Entities.....	47
6.4.1.	SIP Entity for Avaya CS1000E.....	47
6.4.2.	SIP Entity for Avaya SBCE	48
6.5.	Entity Links.....	49
6.5.1.	Entity Link to Avaya CS1000E Entity	49
6.5.2.	Entity Link to Avaya SBCE	49
6.6.	Routing Policies.....	50
6.6.1.	Routing Policy to Avaya CS1000E	50
6.7.	Dial Patterns.....	51
6.7.1.	Inbound AT&T IP Toll Free calls to Avaya CS1000E	51
7.	Avaya Aura® Contact Center	52
7.1.	Create Avaya Aura® Contact Center Agent.....	52
7.2.	Verifying Control DN (CDN) and Agent Connection Status	54
7.2.1.	CDN Connection status	54
7.2.2.	Agent Connection status.....	55
8.	Configure Avaya Session Border Controller for Enterprise	55
8.1.	Initial Provisioning	55
8.2.	Advanced Configuration	59
8.3.	System Management	60
8.4.	Global Profiles	61
8.4.1.	Server Interworking – Avaya Side.....	61
8.4.2.	Server Interworking – AT&T Side	63
8.4.3.	Routing – Avaya Side.....	63
8.4.4.	Routing – AT&T Side	64
8.4.5.	Server Configuration – To Avaya Session Manager	64
8.4.6.	Server Configuration – To AT&T	66
8.4.7.	Topology Hiding – Avaya Side	67
8.4.8.	Topology Hiding – AT&T Side	67
8.4.9.	Signaling Manipulations.....	68
8.5.	Domain Policies.....	70
8.5.1.	Application Rules	70
8.5.2.	Media Rules.....	71
8.5.3.	Signaling Rules	71
8.5.4.	Endpoint Policy Groups – Avaya	73
8.5.5.	Endpoint Policy Groups – AT&T	74
8.6.	Device Specific Settings	75
8.6.1.	Network Management	75
8.6.2.	Media Interfaces.....	76
8.6.3.	Signaling Interface	77
8.6.4.	Endpoint Flows – To Session Manager	78
8.6.5.	Endpoint Flows – To AT&T	78
8.7.	Troubleshooting Port Ranges	79
9.	Verification Steps	80
9.1.	General	80

9.2.	Avaya Communication Server 1000E Verifications	80
9.2.1.	IP Network Maintenance and Reports Commands	80
9.2.2.	System Maintenance Commands	84
9.3.	Avaya Aura® Session Manager	85
9.3.1.	Verify SIP Entity Link Status	85
9.3.2.	Call Routing Test	85
9.4.	Protocol Traces	87
9.5.	Avaya Session Border Controller for Enterprise Verification.....	92
9.5.1.	Verify Sipera SBCE Connectivity to AT&T IP Toll Free	92
9.5.2.	Internal Tracing.....	92
10.	Conclusion	94
11.	References.....	95
12.	Addendum 1 – Avaya Session Border Controller for Enterprise Redundancy to Multiple AT&T Border Elements	97
12.1.1.	Step 1: Configure the Secondary Location in Server Configuration	97
12.1.2.	Step 2:– Add Secondary IP Address to Routing	98
12.1.3.	Step 3:– Configure End Point Flows – SIP_Trunk_backup.....	99

1. Introduction

These Application Notes describe the steps for configuring Avaya Aura® Session Manager, Avaya Communication Server 1000E (referred to in subsequent sections of this document as Avaya CS1000E), and Avaya Session Border Controller for Enterprise (referred to in subsequent sections of this document as Avaya SBCE) with the AT&T IP Toll Free service using 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 application server and is the point of connection between the enterprise endpoints and Avaya Aura® Session Manager. An Avaya Session Border Controller for Enterprise is the point of connection between Avaya Aura® Session Manager and the AT&T IP Toll Free service and is used to not only secure the SIP trunk, but also to make adjustments to the SIP signaling for interoperability. In addition, Avaya Aura® Contact Center is used to provide Agent access for Avaya Communication Server 1000E

The AT&T IP Toll Free service is a managed Voice over IP (VoIP) communications solution that provides toll-free services over SIP trunks utilizing AVPN or MIS/PNT¹ transport.

Note - These Application Notes do NOT cover the AT&T IP Transfer Connect service option of the AT&T IP Toll Free service. That solution is *not* supported by Avaya CS1000E.

2. General Test Approach and Test Results

The test environment consisted of:

- A simulated enterprise with System Manager, Session Manager, Avaya CS1000E, Avaya 11xx phones, fax machines (Ventafax application), Avaya SBCE, and Avaya Call Pilot®.
- A laboratory version of the AT&T IP Toll Free service, to which the simulated enterprise was connected via AVPN transport.

2.1. Interoperability Compliance Testing

The interoperability compliance testing focused on verifying inbound call flows (see **Section 2.3** for examples) between Session Manager, Avaya CS1000E, Avaya SBCE, and the AT&T IP Toll Free service.

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

- SIP trunking.
- T.38 Fax.

¹ MIS/PNT transport does not support compressed RTP (cRTP), however AVPN transport does support cRTP..

- Passing of DTMF events and their recognition by navigating automated menus.
- PBX and AT&T IP Toll Free service features such as hold, resume, conference and transfer.
- AT&T IP Toll Free features such as Legacy Transfer Connect and Alternate Destination Routing were also tested.

2.2. Test Results

The main test objectives were to verify the following features and functionality:

1. Inbound AT&T IP Toll Free service calls to Avaya CS1000E telephones and Agents.
2. Call and two-way talk path establishment between PSTN and Avaya CS1000E telephones/Agents via the AT&T Toll Free service.
3. Basic supplementary telephony features such as hold, resume, transfer, and conference.
4. G.729 and G.711 codecs.
5. T.38 fax calls from the AT&T IP Toll Free service/PSTN to Avaya CS1000E G3 and SG3 fax endpoints.
6. DTMF tone transmission using RFC 2833 between Avaya CS1000E and the AT&T IP Toll Free service/PSTN automated access systems.
7. Inbound AT&T IP Toll Free service calls to Avaya CS1000E that is directly routed to stations, and if unanswered, can be covered to Avaya Call Pilot®.
8. Requests for privacy (i.e., caller anonymity) for inbound calls to Avaya CS1000E from the PSTN, were verified.
9. SIP OPTIONS monitoring of the health of the SIP trunk was verified.
10. Long duration calls.

The test objectives stated in **Section 2.1** with limitations as noted in **Section 2.2.1**, were verified.

2.2.1. Known Limitations

1. 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.
2. AT&T sends Invites with the SIP parameter *maxptime:30*. In response, Avaya CS1000E will send *ptime:10* for any UNISTim or Digital stations. This is a known issue. The AT&T AVPN transport service specifies the use of *ptime:30* for best bandwidth utilization. An Avaya SBCE script is used to change the *maxptime:30* parameter to *ptime:30*, thereby making Avaya CS1000E respond with *ptime:30* as required (see **Section 8.4.9**).
3. Avaya CS1000E sends several SIP headers that are not used by AT&T. In the interest of reducing packet overhead, these unnecessary headers are removed. MIME type headers are removed by Session Manager (see **Section 6.3.2**), and Avaya SBCE removes other headers such as Alert-Info, x-nt-el64-clid, and RFC2833 Telephone Event Type 111 (see **Section 8.4.9**).
4. The AT&T IP Toll Free service does not support SIP History-Info headers. The Avaya SBCE will strip off History-Info headers (see **Section 8.4.9**).

5. When calls are made directly to Avaya CS1000E Agent phones, the response specifies telephone event type 100 (see **Section 5.9**). However if the call is to an Agent queue, the response will specify telephone event 101. However, this did not cause any DTMF issues during testing.
6. G.726 codec is not supported by Avaya CS1000E.

2.3. Call Flows

To understand how inbound AT&T IP Toll Free service calls are processed by Session Manager and Avaya CS1000E, two general call flows are described in this section.

2.3.1. Coverage to Voicemail

The first call scenario illustrated in **Figure 1** is an inbound AT&T IP Toll Free service call that arrives on Session Manager and is subsequently routed to Avaya CS1000E.

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

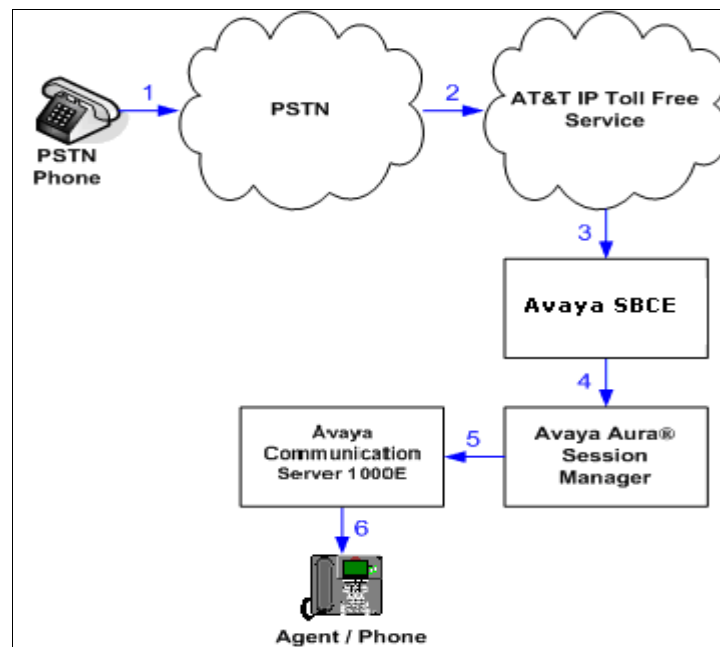


Figure 1: Inbound AT&T IP Toll Free Service Call to Agent / Telephone

2.3.2. Coverage to Voicemail

The call scenario illustrated in **Figure 2** is an inbound call that is covered to voicemail. In this scenario, the voicemail system is an Avaya Call Pilot® system connected to Avaya CS1000E.

1. Same as the first call scenario shown in **Section 2.3.1**.
2. The called Avaya CS1000E Agent/phone does not answer the call, and the call covers to the phone's voicemail. Avaya 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.

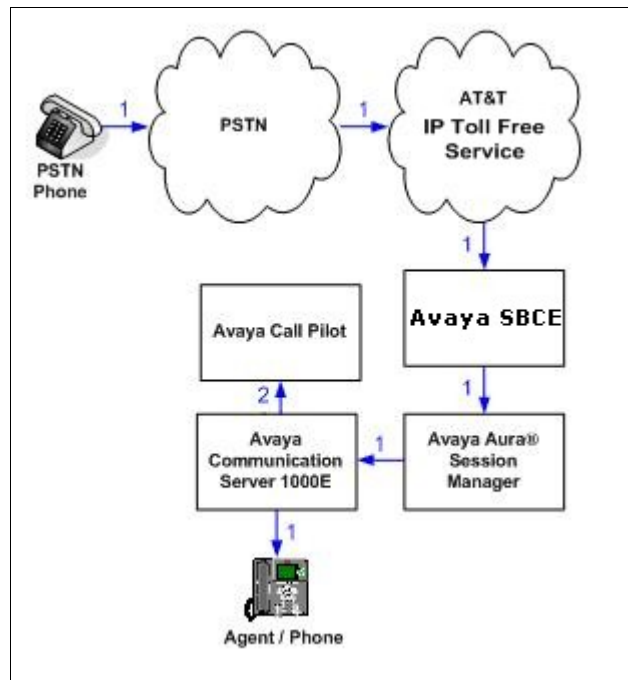


Figure 2: Inbound AT&T IP Toll Free Service Call - Coverage to Voicemail

2.4. Support

2.4.1. AT&T

AT&T customers may obtain support for the AT&T IP Toll Free service by calling (800) 325-5555.

2.4.2. Avaya

Avaya customers may obtain documentation and support for Avaya products by visiting <http://support.avaya.com>. In the United States, (866) GO-AVAYA (866-462-8292) provides access to overall sales and service support menus. Customers may also use specific numbers (provided on <http://support.avaya.com>) to directly access specific support and consultation services based upon their Avaya support agreements.

3. Reference Configuration

The reference configuration used in these Application Notes is shown in **Figure 3** and consists of several components:

- Avaya 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
 - Signaling Server
 - SIP Gateway
 - Avaya Unified Communications Management (UCM)
- Agent “desk” phones are represented with Avaya 1150E UNiStim IP phones. Avaya 1140E UNiStim and Digital M3904 telephones were also tested.
- Avaya SBCE provides address translation and SIP header manipulation between the AT&T IP Toll Free service and the enterprise internal network. TCP transport protocol is used between Avaya SBCE and Session Manager. UDP transport protocol is used between Avaya SBCE and the AT&T IP Toll Free service.
- Avaya Aura® Contact Center provided Agent access capabilities. **Note** - The provisioning of Avaya Aura® Contact Center is beyond the scope of this document (see [11] through [16] for more information).
- 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 [6] for more information).
- Inbound calls were sent from PSTN/AT&T, through Avaya SBCE to Avaya Aura® Session Manager, and on to Avaya CS1000E system. Avaya CS1000E system terminates the calls to the appropriate phone or fax extensions.

Note – Only Avaya CS1000E system provisioning providing SIP trunk functionality is described in these application notes. For additional information on Avaya CS1000E, Call Pilot®, and Avaya Aura® Contact Center system provisioning, see the documentation references in **Section 11**.

Note – In the reference configuration TCP (port 5060) is used as the transport protocol between the CS1000K, Avaya SBCE, 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 Toll Free service for the connection between Avaya SBCE and the AT&T T IP Toll Free border element.

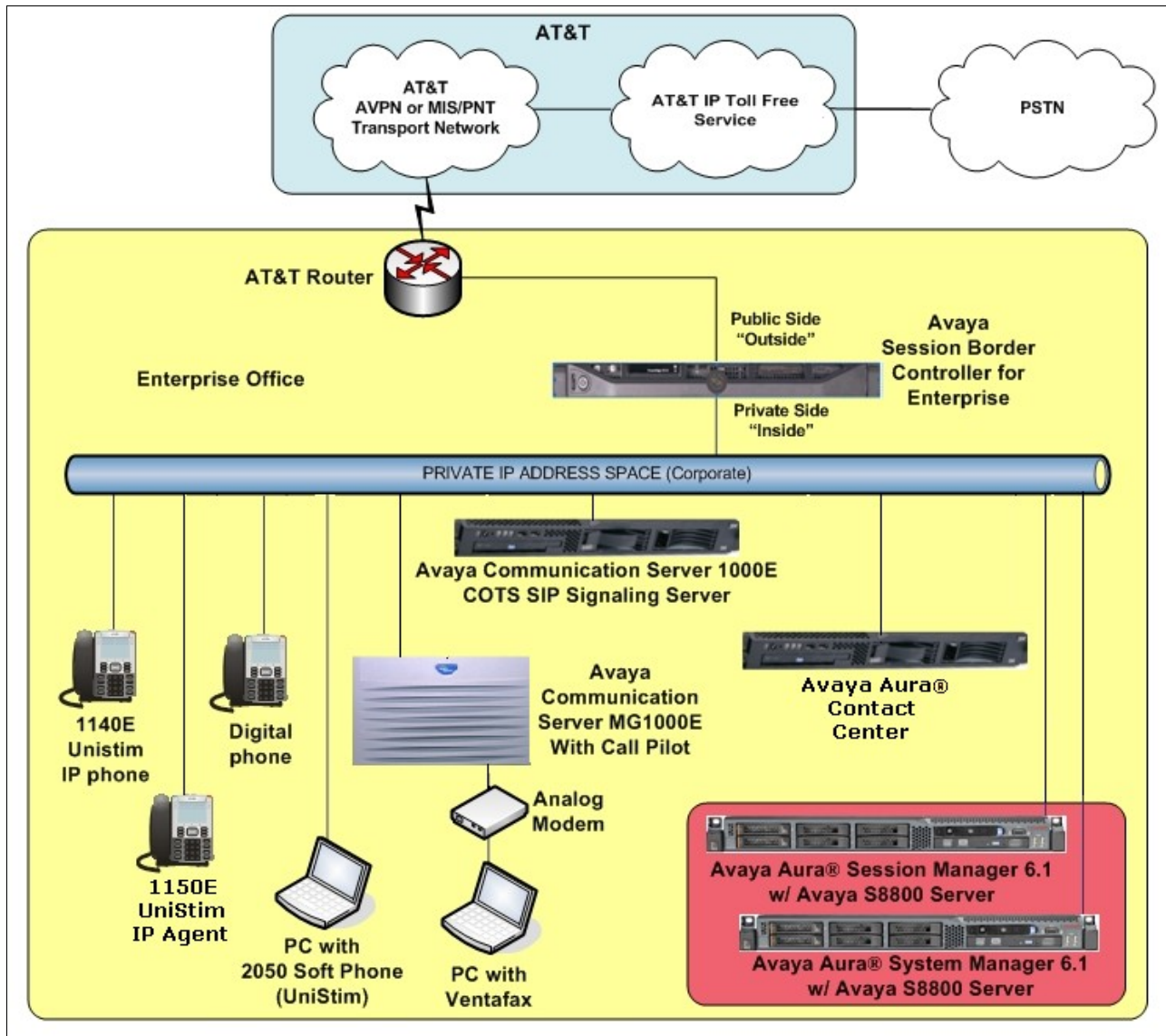


Figure 3: Avaya CS1000E 7.5/Session Manager 6.1/ Avaya SBCE 4.0.5/AT&T IP Toll Free Service Reference configuration

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 Toll Free service Border Element IP address and DNIS digits, (destination digits specified in the SIP Request URIs sent by the AT&T Toll Free service) are shown in this document as examples. AT&T Customer Care will provide the actual IP addresses and DNIS digits as part of the IP Toll Free 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
Avaya CS1000E extensions	40xx
Avaya Call Pilot®	
Call Pilot Application	192.168.67.130
Call Pilot Mailboxes	4xxx
Avaya SBCE	
IP Address of “Outside” (Public) Interface (connected to AT&T Access Router/IP Toll Free Service)	192.168.64.130
IP Address of “Inside” (Private) Interface (connected to Session Manager)	192.168.67.120
AT&T IP Toll Free Service	
Border Element IP Address	135.25.29.74

Table 1: Illustrative Values Used in these Application Notes

4. Equipment and Software Validated

The following equipment and software was used for the reference configuration described in these Application Notes.

Equipment/Software	Release/Version
Avaya CS1000E Platform <ul style="list-style-type: none">MG1000E Media GatewayIBM xSeries 306M (COTS) SIP Signaling serverCall Pilot	Release 7.5, Version 7.50.17 with Service_Pack_Linux_7.50_17_20120314.ntl and Plug-in 501 Enabled CP 5.00.41
Avaya S8800 Server running Avaya Aura® System Manager	Release 6.1.0 with SP6 (Build Number 6.1.0.0.7345-6.1.5.606)
Avaya S8800 Server running Avaya Aura® Session Manager	Release 6.1 SP6 (Release: 6.1.6.0.616008)
Dell R310 running Avaya Session Border Controller for Enterprise	4.0.5.Q09
HP Proliant DL360 G7 Server running Avaya Aura® Contact Center	Release 6.2.205.0 SP5
Fax device Windows PC running Ventafax Home	Version 6.3.102.288
AT&T IP Toll Free Service via AVPN or MIS/PNT transport service connections.	VNI 22

Table 2: Equipment and Software Versions

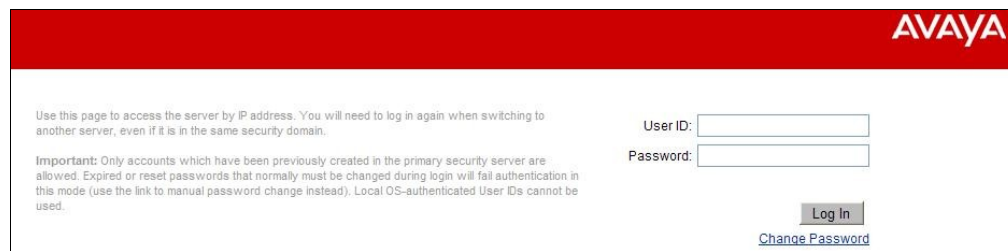
5. Configure Avaya CS1000E

This section describes Avaya CS1000E configuration, focusing on the routing of calls to Session Manager over a SIP trunk. In the sample configuration, Avaya CS1000E Release 7.5 was deployed with Call Server applications running on a CPPM server platform with MGC, and utilizing a separate SIP Signaling Server/SIP Gateway.

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 CS1000E 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 Avaya CS1000E is configured to support Analog, Digital, and UNISTim endpoints in the reference configuration. For references on how to administer these functions of Avaya CS1000E, see **Section 11**.

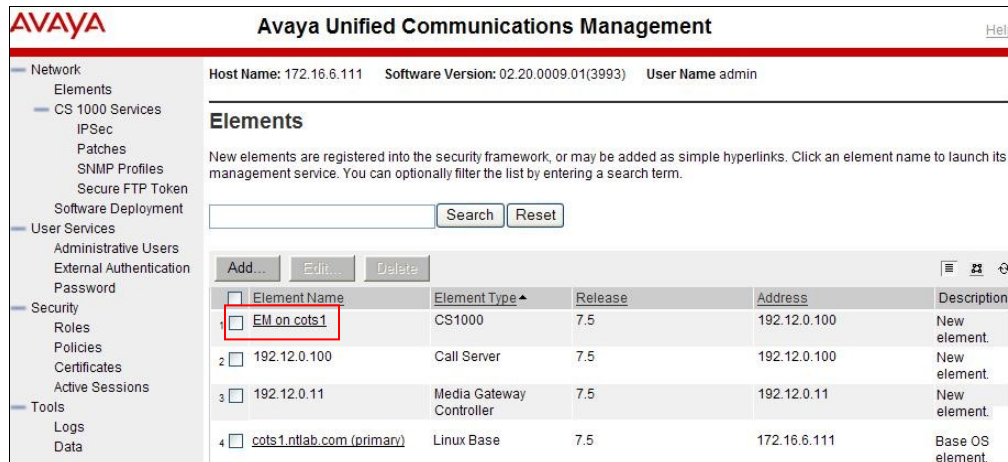
Step 1 - Unless otherwise noted, all Avaya CS1000E provisioning was performed via Avaya Unified Communication Management (AUCM) web interface. The **AUCM** web interface may be launched directly via **https://<ip address>** where the relevant <ipaddress> in the sample configuration is 172.16.6.111. The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

The image shows a web-based login interface for Avaya. At the top, there is a red header bar with the "AVAYA" logo in white. Below the header, the page has a white background. On the left side, there is a block of text: "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." followed by an "Important:" note stating that only accounts created in the primary security server are allowed and that expired or reset passwords will fail authentication. On the right side, there are two input fields: "User ID:" and "Password:". Below these fields is a "Log In" button. At the bottom right, there is a link labeled "Change Password".

Note – Although not used in the reference configuration, System Manager may be configured as the Primary Security Server for Avaya Unified Communications Management application and Avaya CS1000E 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 System Manager by using the URL “**http://<ip-address>/SMGR**”, where <ip-address> is the IP address of System Manager. Log in with appropriate credentials. System Manager Home Page will be displayed. Under the **Services** category on the right side of the page, click the **UCM Services** link.

Whether Avaya CS1000E is accessed directly or via System Manager, 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**.



AVAYA Avaya Unified Communications Management Help

Host Name: 172.16.6.111 Software Version: 02.20.0009.01(3993) User Name admin

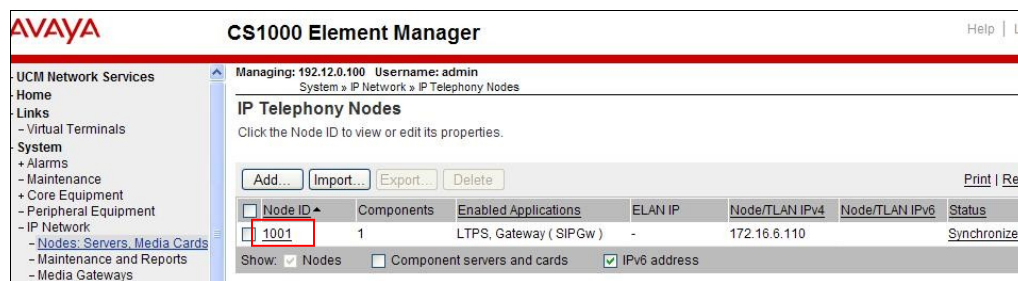
Elements

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

<input type="checkbox"/>	Element Name	Element Type	Release	Address	Description
<input type="checkbox"/>	EM on cots 1	CS1000	7.5	192.12.0.100	New element.
<input type="checkbox"/>	192.12.0.100	Call Server	7.5	192.12.0.100	New element.
<input type="checkbox"/>	192.12.0.11	Media Gateway Controller	7.5	192.12.0.11	New element.
<input type="checkbox"/>	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

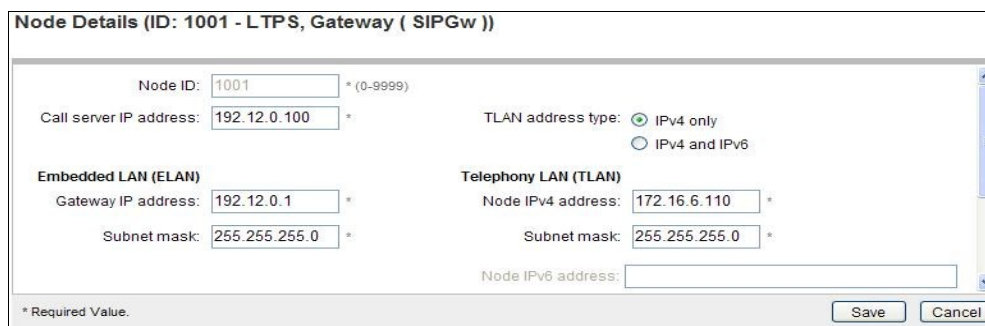
Click the Node ID to view or edit its properties.

Print | Refr

<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 Avaya 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. Save Cancel

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

Associated Signaling Servers & Cards

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

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).

AVAYA CS1000 Element Manager Help | Log Out

Managing: 192.12.0.100 Username: admin
System » IP Network » Media Gateways

Media Gateways

[Refresh](#)

IPMG	IP Address	Zone	Type
<input type="radio"/> 000 01	192.12.0.11	1	MGC

This will open the Property Configuration screen.

Step 3 – Click on the Next button.

AVAYA CS1000 Element Manager Help | Log Out

Managing: 192.12.0.100 Username: admin
System » IP Network » Media Gateways » IPMG 0 1 Property Configuration

IPMG 0 1 Property Configuration

Input Description	Input Value
ELAN IP address:	192.12.0.11 *
Bandwidth zone number:	1 (0 - 8000)
IPMG type:	MGC
ELAN passthrough port:	CE
Faceplate ELAN port:	1E
Backplane ELAN connection:	E
TLAN passthrough port:	CT
Faceplate TLAN port:	2T
Backplane TLAN connection:	T

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 Avaya CS1000E sends to Session Manager, and on to Avaya SBCE, will be 172.16.6.115 in the sample configuration. Note that Avaya SBCE will change this IP address to Avaya SBCE “outside” IP address before sending the INVITE on to the AT&T IP Toll Free service.

AVAYA CS1000 Element Manager

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: 172.16.6.115

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 CS1000E 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

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)
MSDI Diagnostics (LD 96)
TMDI Diagnostics (LD 96)
D-Channel Expansion Diagnostics (LD 48)

Configuration

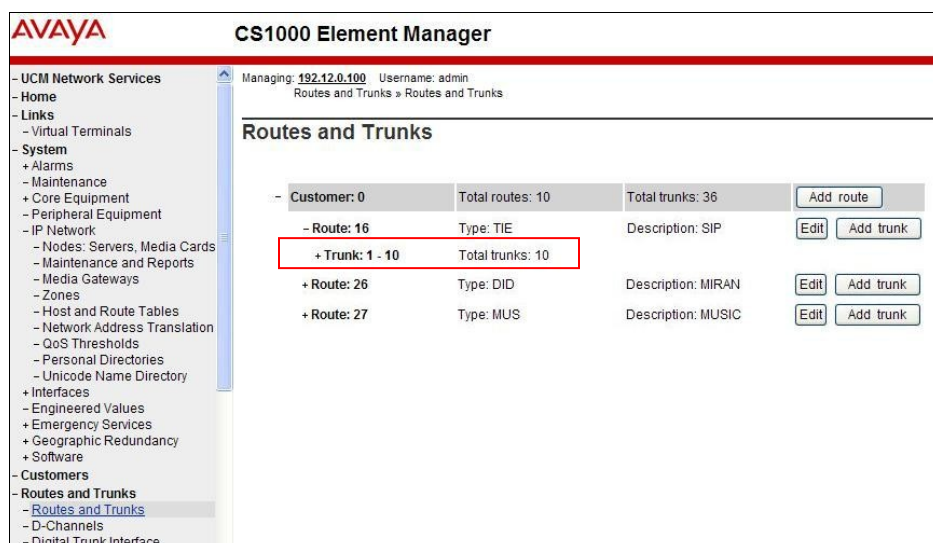
Choose a D-Channel Number: 0 and type: DCH to Add

Channel	Type	Card Type	Description	Edit
Channel: 15	DCH	DCIP	VDCH	Edit
Channel: 20	DCH	DCIP	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**).



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

Step 3 – Click on the **Edit** button for **Trunk: 1**. In the reference configuration Trunk 1 uses Channel 16. Therefore, each subsequent trunk will use channel 16+1. For example, Trunk 9 will use channel 24.

- Route: 16	Type: TIE	Description: SIP	Edit	Add trunk
- Trunk: 1 - 10	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	

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** 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 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

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):

Customer number (CUST):

Route number (ROUT):

Designator field for trunk (DES):

Trunk type (TKTP):

Incoming and outgoing trunk (ICOG):

Access code for the trunk route (ACOD): *

Trunk type M911P (M911P): ☐

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

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

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

- Protocol ID for the route (PCID):

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

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**.

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 5.4**.

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.

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. Note that this domain is also specified in System Manager (see **Section 6.1**).
- **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.

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 - The Secondary TLAN IP address was not used.

The screenshot shows the configuration interface for a Proxy Or Redirect Server. Under the 'Proxy Server Route 1' section, the following fields are visible: 'Primary TLAN IP address' is set to '192.168.67.210' with a note below stating 'The IP address can have either IPv4 or IPv6 format based on the value of "TLAN address type"'; 'Port' is set to '5060' with a range '(1 - 65535)'; 'Transport protocol' is set to 'TCP' via a dropdown menu; 'Options' includes two checkboxes, 'Support registration' and 'Primary CDS proxy', both of which are unchecked. Below these, the 'Secondary TLAN IP address' is set to '0.0.0.0' with the same note as the primary address; its 'Port' is also '5060' and its 'Transport protocol' is 'TCP'.

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. Avaya 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 value is configured to blank, Avaya CS1000E will omit the “phone-context=” in the SIP header altogether.

The screenshot displays the 'SIP URI Map' configuration page, which is divided into two columns: 'Public E.164 domain names' and 'Private domain names'. Each column contains five input fields for different URI types: 'National', 'Subscriber', 'Special number', 'Unknown', and 'UDP'. In the 'Private domain names' column, the 'CDP' field is populated with the value 'cdp.udp'. All other fields are empty.

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 Inbound Numbers to Avaya CS1000E

Calls from PSTN will dial AT&T IP Toll Free DID numbers to reach Agent stations on Avaya CS1000E. These DID numbers are converted to DNIS digits by AT&T. The inbound DNIS digits are then converted to their associated extensions by Avaya 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**.

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

Incoming Digit Translation

- Customer: 00 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 Toll Free DNIS (e.g., **7325554383**). In the **Converted Digits** field enter the associated Avaya CS1000E Agent extension (e.g., **4014**). Click on **Save**.

Step 5 – Repeat **Step 4** for all associated AT&T IP Toll Free DNIS numbers and extensions.

NOTE – The inbound DNIS digits may not be the same as the dialed digits.

Note – This method should not be used to direct PSTN calls to the Call Pilot access extension. The procedures described in **Section 6.3.1** cover this scenario.

5.5. 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.

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 Toll Free 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

5.6. Codec Parameters.

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

5.6.1. 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 DB1 *

- DSP Daughterboard 2

Type of the DSP daughterboard NODB v

Telephony LAN (TLAN) IP address 0.0.0.0

Telephony LAN (TLAN) gateway IP address 172.16.6.1

Telephony LAN (TLAN) IPv6 address

Telephony LAN (TLAN) subnet mask 255.255.255.0

Hostname DB2 *

+ 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 G711

Voice payload size 30 v (ms/frame)

Voice playout (jitter buffer) nominal delay 60 v

Modifications may cause changes to dependent settings

Voice playout (jitter buffer) maximum delay 120 v

Modifications may cause changes to dependent settings

VAD ☐

Step 5 – Scroll down , click on and expand the **Codec G729A** field. Check the selection box and set the **Voice payload size (PTIME)** to **30**.

Note – Although not shown, annexB=yes may be enabled by selecting the **VAD** (Voice Activity Detection) box. However, if enabled here, it must also be enabled in **Section 5.6.2**.

- Codec G729A Select ☒

Codec name G729A

Voice payload size 30 v (ms/frame)

Voice playout (jitter buffer) nominal delay 60 v

Modifications may cause changes to dependent settings

Voice playout (jitter buffer) maximum delay 120 v

Modifications may cause changes to dependent settings

VAD ☐

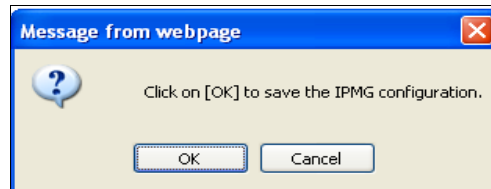
Step 6 – Scroll down and click on **Codec T.38 FAX**. Note that T.38 is enabled by default.


- Codec T38 FAX
Select ☒

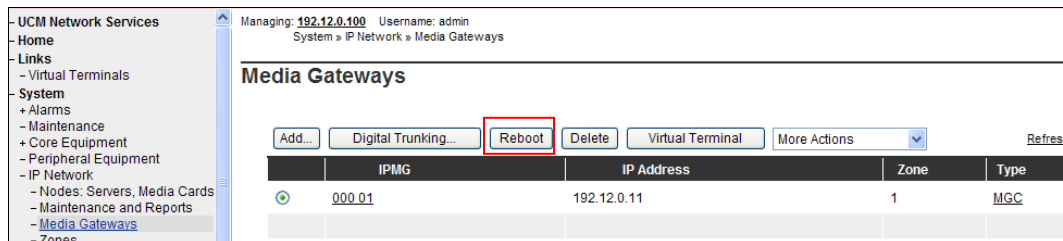
Codec name T38 FAX

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**.



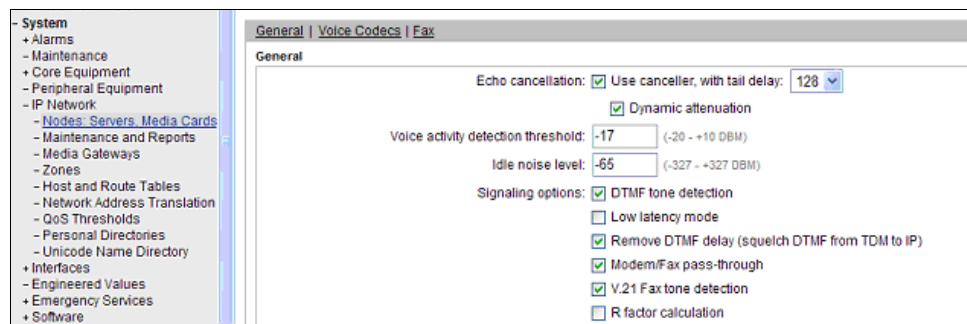
Step 9 –Select  next to the Media Gateway ID (e.g., 000 01), and click on the **Reboot** button. The Media Gateway will reboot and deploy the new configuration.



5.6.2. 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 shown, annexB=yes may be enabled by selecting the **VAD** (Voice Activity Detection) box. However, if enabled here, it must also be enabled in **Section 5.6.1**.

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.

5.7. Avaya CS1000E Agent Access Provisioning

This section is not intended to be prescriptive, but simply illustrates a sampling of defining Agent access on the Avaya CS1000E in the sample configuration. Inbound IP Toll Free numbers are mapped to the Agent extensions (or queues) as shown in **Section 5.4** (e.g., 4014).

The following Directory Numbers (DN) are defined:

- **2003** – This is the Positional DN. It is associated with the Terminal Number (TN) defined for the phone (e.g., **96 0 1 17**).
- **4012** – This is the Auto Call Distribution (ACD) number for the agent queue. All agents share this queue. This number will appear on the Agent phone display.
- **4013** – This is the Control DN (CDN). It is used to define the connection between the Avaya CS1000E and the Avaya Aura® Contact Center (see **Section 5.7.3**).
- **4014** – This is the Agents Single Call Ringing (SCR) number. This is the Agents “local” extension independent of the Agent queue, and will also appear on the phone display.

5.7.1. Avaya CS1000E IP Agent Phone

The following section shows information for an 1150E IP UNISim Agent phone in the reference configuration defined via AUCM.

5.7.1.1 General Properties

Step 1 – Select **Phones** from the menu The **Search For Phones** screen will open (not shown).. In the **Criteria** field select **Prime DN** and enter a DN in the value field (e.g., **2003**). Click on **Search**.

Step 2 – Click on the TN value displayed (e.g., **096 0 01 17**). The **Phone Details** form will open. Note that the telephone type is an 1150 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 connects to the PSTN via the SIP trunk, the call would use a “best bandwidth” strategy, and the call would use G.729A.

The screenshot shows the Avaya CS1000 Element Manager interface. The left sidebar contains a navigation tree with categories like Zones, Interfaces, Customers, Routes and Trunks, Dialing and Numbering Plans, Phones, Tools, and Security. The 'Phones' category is selected. The main area is titled 'Phone Details' and shows a small image of a phone. To the right of the image, it displays 'System: EM on cots 1', 'Phone Type: 1150', and 'Sync Status: TRN'. Below this, there are 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 17), 'Designation' (AGENT2), and 'Zone' (3). There is also a 'Key Expansion Modules' field set to 0. A 'Custom View' dropdown is set to 'All'.

5.7.1.2 Features

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

Step 3 – For the **SPV - ACD Supervisor/Agent** field select **ACD Agent**.

SLKA	Feature	Description	Value:
	Scheduled Electronic Lock		Denied
SPID	Supervisor Position ID		
SPV	ACD Supervisor/Agent		ACD Agent
SSU	System Speed Call List Number		
SWA	Call Waiting from a Station		Denied

5.7.1.3 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.

5.7.1.3.1 Key 0

Step 4 – For Key **0** select **ACD – Auto Call Distribution**

- For **ACD Directory Number** enter **4012**
- For **Numeric/D<space>ACD Position ID** enter **0 2003**

Key No.	Key Type	Key Value
0	ACD - Auto. Call Distribution	ACD Directory Number: 4012 CLID: Numeric/D<space>ACD Position ID: 0 2003 ANIE Entry:

5.7.1.3.2 Key 3 - Single Call Appearance

Step 5 – For Key 3 select **SCR - Single Call Ringing**

- For **Directory Number** select **4014**
- Check **Multiple Appearance Redirection Prime(MARP)**
- Enter a name (e.g., Agent2)
- In the **CLID Entry** field, enter the associated CLID defined in **Section 5.8** (e.g., 0).

3	SCR - Single Call Ringing	Directory Number: 4014 <input checked="" type="checkbox"/> Multiple Appearance Redirection Prime(MARP) First Name: Agent2 Last Name: Display Format: First, Last Language: Roman CLID Entry (Numeric or D): 0 ANIE Entry:
---	---------------------------	--

5.7.1.3.3 LD 20 Overlay Command for Agent Configuration Display

The following CS1000E overlay command may be used to display/verify the Agent configuration.

```
OVL000
>ld 20
REQ: prt
TYPE: 1150
TN
CUST 0
DATE
PAGE
DES
MODEL_NAME
EMULATED
KEM_RANGE
DES AGENT2
TN 096 0 01 17 VIRTUAL
TYPE 1150
CDEN 8D
CTYP XDLC
CUST 0
NUID
NHTN
CFG_ZONE 00003
CUR_ZONE 00003
MRT
ERL 0
ECL 0
FDN
TGAR 1
LDN NO
NCOS 0
SGRP 0
RNPG 0
SCI 0
SSU
XLST
SCPW
CLS CTD FBD WTA LPR MTD FND HTD TDD HFA CRPD
MWD LMPN RMMD AAD IMD XHD IRD NID OLD VCE DRG1
POD SLKD CCSD SWD LND CNDA
CFTD SFD MRD DDV CNID CDCA MSID DAPA BFED RCB
ICDD CDMD LLCN MCTD CLBD AUTU
GPUD DPUD DNDA CFXD ARHD CNTD CLTD ASCD
CPFA CPTA ABDD CFHD FICD NAID BUZZ AGRD MOAD AHD
DDGA NAMA
DRDD EXR0
USMD USRD ULAD RTDD RBDD RBHD PGND OCBD FLXD FTTC DNDY DNO3 MCBN
VOLA VOUD CDMR PRED RECD MCDD T87D SBMD
KEM3 MSNV FRA PKCH MUTA MWTD DVLD CROD ELCD
CPND_LANG ENG
HUNT
PLEV 02
```

```

PUID
UPWD
DANI NO
SPID NONE
AST 00 03
IAPG 1
AACS YES
ACQ AS: TN,AST-DN,AST-POSID
ASID 17
SFNB 1 2 3 4 5 6 7 8 9 10 11 12 13 15 16 17 18 19 22 24
SFRB 1 2 15
USFB 1 2 3 4 5 6 7 9 10 11 12 13 14 15
CALB 0 1 3 4 5 6 8 9 10 11 12
FCTB 1
ITNA NO
DGRP
PRI 01
MLWU_LANG 0
MLNG ENG
DNDR 0
KEY 00 ACD 4012 0 2003
AGN
01 NRD
02 MSB
03 SCR 4014 0 MARP
04
05
06
07
08
09
10
11
12
13
14
15
16
17 TRN
18 AO6
19 CFW 16
20 RGA
21 PRK
22 RNP
23
24 PRS
25 CHG
26 CPN
27
28
29
30
31

```


5.7.2. Avaya CS1000E Auto Call Distribution (ACD)

The ACD information may be displayed by using the **ld 23** overlay command.

```
>ld 23
ACD000
MEM AVAIL: (U/P): 98772443      USED U P: 4778038 101868      TOT: 103652349
DISK SPACE NEEDED: 72 KBYTES
ACD DNS          AVAIL: 23992      USED:      8      TOT: 24000
REQ prt
TYPE acd
CUST 0
ACDN 4012
MWC NO
DSAC NO
MAXP 5
SDNB NO
BSCW NO
ISAP NO
AACQ NO
RGAI NO
ACAA NO
FRRT
SRRT
NRRT
FROA NO
CALP POS
ICDD NO
NCFW
FNCF NO
FORC NO
RTQT 0
SPCP NO
OBTN NO
RAO NO
CWTH 1
NCWL NO
BYTH 0
OVTH 2047
TOFT NONE
HPQ NO
OCN NO
OVDN
IFDN
OVBV LNK LNK LNK LNK
EMRT
MURT
RTPC NO
HOML YES
RDNA NO
LABEL_KEY0 NO
ACNT
NRAC NO
DAL NO
```

```
RPRT YES
RAGT 4
DURT 30
RSND 4
FCTH 20
CRQS 100
SIPQ NO
IVR NO
OBSC NO
OBPT 5
CWNT NONE
```

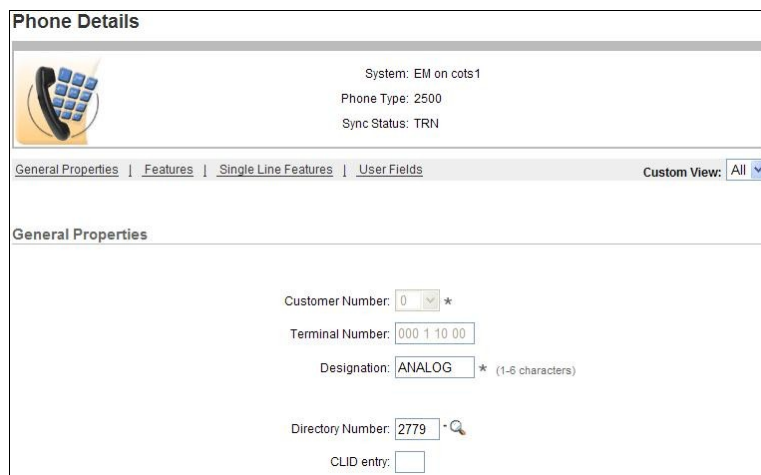
5.7.3. Avaya CS1000E Control DN (CDN)

The CDN information may also be displayed by using the **ld 23** overlay command.

```
>ld 23
ACD000
MEM AVAIL: (U/P): 98772394      USED U P: 4778038 101917      TOT: 103652349
DISK SPACE NEEDED: 71 KBYTES
ACD DNS      AVAIL: 23992      USED:      8      TOT: 24000
REQ prt
TYPE cdn
CUST 0
CDN 4013
FRRT
SRRT
FROA NO
UUI NO
MURT
CDSQ NO
DFDN 4012
NAME NO
CMB NO
CEIL 2047
CLRO NO
OVFL NO
TDNS NO
RPRT YES
AACQ YES
ASID 17
SFNB 33 35 36 37 38 39
USFB 1 3 4 5 6 7 9 10 11 12 13 14 15
CALB 0 1 2 3 4 5 6 8 9 10 11 12
CNTL YES
VSID
HSID
CWTH 1
BYTH 0
OVTH 2047
ACNT
```

5.7.4. 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.



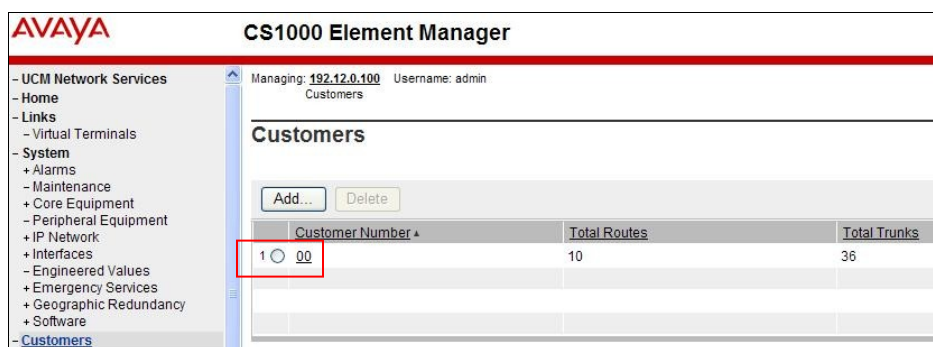
The 'Phone Details' screen shows configuration for an analog port. It includes a phone icon and system information: 'System: EM on cots1', 'Phone Type: 2500', and 'Sync Status: TRN'. Below this are tabs for 'General Properties', 'Features', 'Single Line Features', and 'User Fields', with 'Custom View' set to 'All'. The 'General Properties' section contains fields for 'Customer Number' (0), 'Terminal Number' (000 1 10 00), 'Designation' (ANALOG), 'Directory Number' (2779), and 'CLID entry'.

5.8. Customer Information

In the reference configuration, specific calling number information is required based on the destination of the call. For calls from the AT&T IP Toll Free service to Avaya CS100E extensions (see [Section 5.4](#)), responses (e.g., 200 OK) should contain the associated AT&T IP Toll Free service Caller ID information.

5.8.1. Caller ID Provisioning

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



The 'CS1000 Element Manager' interface shows the 'Customers' section. The left navigation menu includes 'UCM Network Services', 'Home', 'Links', 'System', and 'Customers'. The main area displays a table of customers with columns for 'Customer Number', 'Total Routes', and 'Total Trunks'. The first row shows '1' for Customer Number, '10' for Total Routes, and '36' for Total Trunks. The '00' part of the Customer Number 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**.

Customer Details

[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 **General Properties** screen will open (not shown).

Step 3 - Scroll down from **General Properties** to the **Calling Line Identification** section of the page 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
Private dialing plan for non-DID users: ☐ Coordinated dialing plan
☐ Uniform dialing plan

Calling Line Identification

Information for incoming/outgoing calls: No manipulation is done

Size: 256 (0 - 4000)
Country code: 1 (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** 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 **732-555-4383**

Entry ID	National Code	Local Code	Home location code	Local steering code	Use DN as DID	Emergency Local Code
0	732	5554383			NO	
1	732	5554384			NO	
2	732	5554385			NO	

Click on any Entry ID to view or change further details (e.g., **Entry ID 0**).

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.

General Properties

National Code: 732 (0 - 99999)
Code for national home number

Local Code: 5554383 (1-12 digits)
Code for home local number or listed DN

Local Steering Code: (1-7 digits)

Use DN as DID: NO

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

Roman characters: ☒

CPND Name: Agent2
first name, last name

Expected Length: 12

Display Format: First name, Last name

Save Cancel

Call IDs are then associated with specific telephone directory numbers (DNs) assigned to stations. See **Section 5.7.1.3.2**.

5.9. Changing RFC2833 DTMF Telephone Event Type

Avaya CS1000E uses RFC2833 DTMF Telephone Event type 101. 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, Avaya CS1000E value may be changed to 100 as follows:

Step 1 – From a Avaya 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>
```

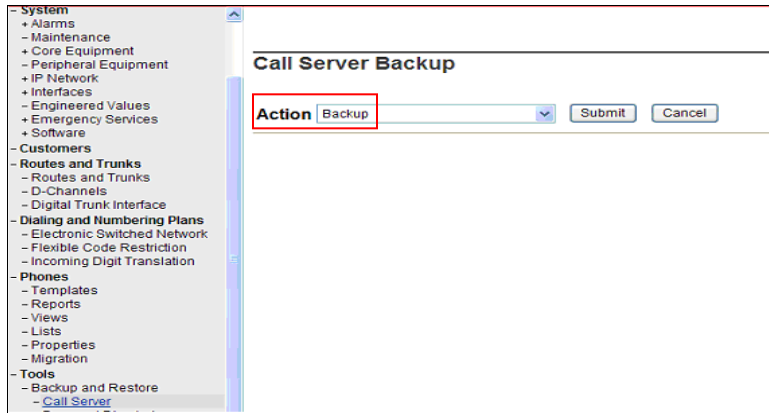
Avaya CS1000E will now use RFC2833 DTMF telephone event type 100.

NOTE – See **Section 2.2.1** regarding Telephone Event behavior for Agent phone versus Agent queue calls. The Avaya CS1000E also sends Telephone Event 111. This value is unnecessary and is removed by the Avaya SBCE (see **Section 8.4.9**).

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

5.10. 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 CS1000E 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 – These Application Notes assume that basic System Manager and Session Manager administration has already been performed. Consult [1] through [4] for further details if necessary.

This section provides the procedures for configuring Session Manager to receive calls from and route calls to the SIP trunk between Avaya CS1000E and Session Manager, and the SIP trunk between Session Manager and Avaya SBCE.

Session Manager serves as a central point for supporting SIP-based communication services in an enterprise. Session Manager connects and normalizes disparate SIP network components and provides a central point for external SIP trunking to the PSTN. The various SIP network components are represented as SIP Entities and the connections/trunks between Session Manager and those components are represented as Entity Links. Thus, rather than connecting to every other SIP Entity in the enterprise, each SIP Entity simply connects to Session Manager and relies on Session Manager to route calls to the correct destination. This approach reduces the dial plan and trunking administration needed on each SIP Entity, and consolidates said administration in a central place, namely System Manager.

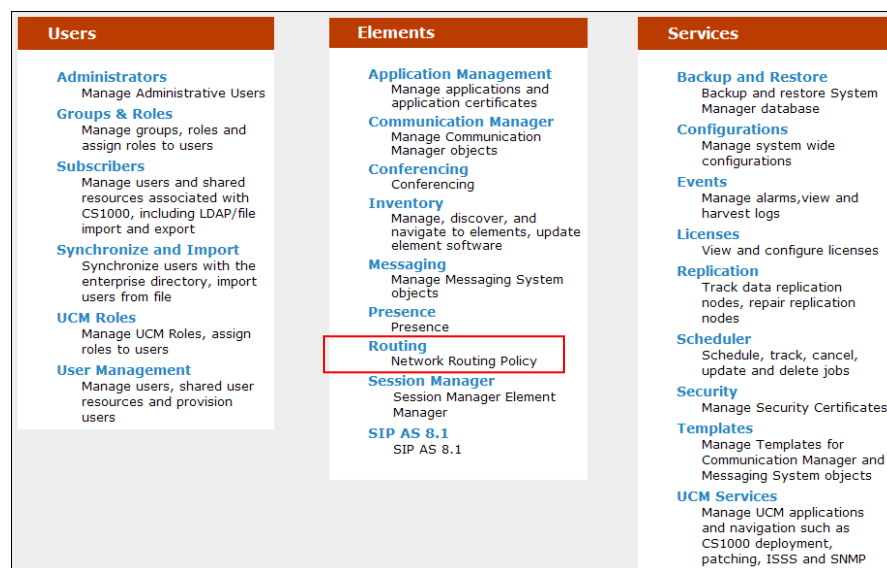
When calls arrive at Session Manager from a SIP Entity, Session Manager applies SIP protocol and numbering modifications to the calls. These modifications, referred to as Adaptations, are sometimes necessary to resolve SIP protocol differences between disparate SIP Entities, and also serve the purpose of normalizing the calls to a common or uniform numbering format, which allows for simpler administration of routing rules in Session Manager. Session Manager then matches the calls against certain criteria embodied in profiles termed Dial Patterns, and determines the destination SIP Entities based on Routing Policies specified in the matching Dial Patterns. Lastly, before the calls are routed to the respective destinations, Session Manager again applies Adaptations in order to bring the calls into conformance with the SIP protocol interpretation and numbering formats expected by the destination SIP Entities.

The following administration activities will be described:

- Define SIP Domain
- Define Locations for Avaya CS1000E and Avaya SBCE.
- Configure the Adaptation Modules that will be associated with the SIP Entities for Avaya CS1000E and Avaya SBCE.
- Define SIP Entities corresponding to Avaya CS1000E and Avaya SBCE.
- Define Entity Links describing the SIP trunk between Avaya CS1000E and Session Manager, and between the SIP Trunk between Session Manager and Avaya SBCE.
- Define Routing Policies associated with Avaya CS1000E.
- Define Dial Patterns, which govern which routing policy will be selected for call routing.

Configuration is accomplished by accessing the browser-based GUI of System Manager, using the URL <http://<ip-address>/SMGR>, where <ip-address> is the IP address of System Manager.

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** is 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 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

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 Avaya CS1000E, and Avaya SBCE were each defined as individual Locations.

6.2.1. Location for Avaya CS1000E

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 Avaya 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 CS1000E.

The screenshot displays the Avaya Aura System Manager 6.1 web interface. The left sidebar shows the navigation menu with 'Routing' expanded and 'Locations' selected. The main content area is titled 'Home / Elements / Routing / Locations - Location Details'. The 'General' section contains fields for 'Name' (CS1K) and 'Notes'. The 'Overall Managed Bandwidth' section includes 'Managed Bandwidth Units' (Kbit/sec), 'Total Bandwidth', 'Multimedia Bandwidth', and a checked box for 'Audio Calls Can Take Multimedia Bandwidth'. The 'Per-Call Bandwidth Parameters' section shows 'Maximum Multimedia Bandwidth (Intra-Location)' and 'Maximum Multimedia Bandwidth (Inter-Location)' both set to 1000 Kbit/Sec, 'Minimum Multimedia Bandwidth' set to 64 Kbit/Sec, and 'Default Audio Bandwidth' set to 80 Kbit/sec. The 'Location Pattern' section has an 'Add' button and a table with one entry: '172.16.6.110' under the 'IP Address Pattern' column. The interface includes 'Commit' and 'Cancel' buttons at the bottom right and a '* Input Required' message at the bottom left.

6.2.2. Location for Avaya Session Border Controller for Enterprise

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 Avaya SBCE location (e.g., **192.168.67.120**).
- **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

Home / Elements / Routing / Locations - Location Details

Location Details

General

* Name: SBCE

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

IP Address Pattern	Notes
* 192.168.67.120	

Select : All, None

* Input Required

Commit Cancel

6.3. Configure Adaptations

Session Manager can be configured to use an Adaptation Module designed for Avaya CS1000E to convert SIP headers in messages sent by Avaya CS1000E 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 Avaya 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.

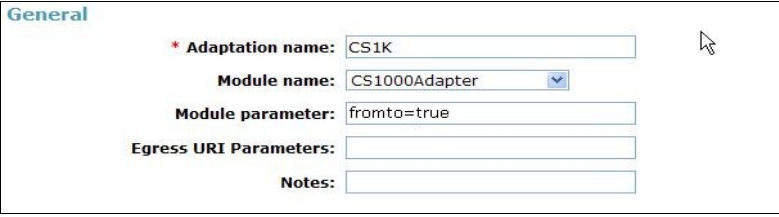
- **CS1000Adapter** – This adaptation is used to provide translation between Avaya CS1000E generated History-Info headers into formats used by other Avaya products and endpoints.
- **DigitConversionAdapter** – This adaptation is used to modify digit strings in the Request-URI. Note that the adaptation 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=true** (to modify the From and To headers) are specified.

6.3.1. Adaptation for Avaya CS1000E 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., “CS1K”)
- **Module Name:** Select **CS1000Adapter** from drop-down menu (or add an adapter with name “CS1000Adapter” if not previously defined)
- **Module Parameter:** Enter **fromto=true**



The screenshot shows a web form titled "General" with the following fields:

- * Adaptation name:** Text input field containing "CS1K".
- Module name:** Drop-down menu showing "CS1000Adapter".
- Module parameter:** Text input field containing "fromto=true".
- Egress URI Parameters:** Empty text input field.
- Notes:** Empty text input field.

Incoming AT&T calls to Avaya CS1000E stations have the inbound NDIS digits converted to their associated local extensions in Avaya CS1000E **Incoming Digit Translation** table (e.g., AT&T DNIS 7323204383 is converted to local extension 4014, see **Section 5.4**), so those digit conversions are not needed here. However, Avaya CS1000E responses to the inbound calls (e.g., 200 OK) need to contain the AT&T IP Toll Free DNIS numbers, (instead of local extensions), in Caller ID headers such as PAI. This is accomplished by specifying the **fromto=true** Module Parameter shown above and the procedure described in **Step 2** below.

Step 2 – In the **Digit Conversion for Incoming Calls to SM** section, click **Add** to configure entries for responses to calls from AT&T (e.g., 200 OK sent by Avaya CS1000E).

- **Matching Pattern** Enter the Avaya CS1000E destination extension that will generate the 200OK response (e.g., **4014**).
- **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**.
- **Insert Digits** Enter the associated AT&T IP Toll Free DNIS number (e.g., **7325554385**).

- **Address to modify** Select “both”.

Repeat for any additional Avaya CS1000E extensions that receive inbound calls from the AT&T IP Toll Free service.

Digit Conversion for Incoming Calls to 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"/>	*4014	*4	*4		*4	7323204385	both	IPTF 200OK re
<input type="checkbox"/>	*4015	*4	*4		*4	7323204384	both	IPTF 200OK re
<input type="checkbox"/>	*4095	*4	*4		*5	0000021052	both	IPTF 200OK re

In addition, for direct PSTN/AT&T access to the integrated Call Pilot messaging system, the **fromto=true** Module Parameter described above, in conjunction with the provisioning shown in **Step 3** below, is used to insert the Call Pilot local access extension into the To header for delivery to Call Pilot.

Step 3 – In the **Digit Conversion for Outgoing Calls from SM** section, click **Add** to configure entries for calls from AT&T.

The text below and the screen example that follows explain how to use Session Manager to convert between inbound AT&T IP Toll Free DNIS numbers and Avaya CS1000E Call Pilot extension (4096).

- **Matching Pattern** Enter AT&T IP Flexible Reach DIDs (e.g., **7325554386**).
- **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 Call Pilot extension (e.g., **4096**).
- **Address to modify** Select **both**.

Repeat for any addition PSTN/AT&T IP Toll Free direct access to Call Pilot.

Step 4 - Click **Commit**.

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"/>	*7325554386	*10	*10		*10	4096	both	direct Call Pilot To Header
<input type="checkbox"/>	*8885555821	*10	*10		*10	4096	both	direct Call Pilot To Header

Select : All, None

NOTE – The inbound DNIS digits may not be the same as the dialed digits.

6.3.2. Adaptation for Avaya CS1000E to Avaya SBCE Entity

Although the AT&T IP Toll Free service is inbound only, the Avaya CS1000E system may issue Invites to signal call state changes (e.g., Hold). The message body of an INVITE message sent from Avaya 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 Avaya 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. In addition, the **DiversionTypeAdapter** will convert History-Info headers to Diversion headers, which are required by the AT&T IP Toll Free service for Call Forward scenarios. Note that Avaya SBCE is used to remove and/or alter additional Avaya CS1000E SIP headers (see **Section 8.4.9**).

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 AT&T IP Toll Free border element >** (e.g., **odstd=135.25.29.74**).
 - Enter **osrcd=< IP address of the public interface of Avaya SBCE >** (e.g., **osrcd=192.168.64.130**).
 - Enter **MIME=no** to remove additional MIME Media Type headers that Avaya 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.

Step 2 - Click Commit.

General

* **Adaptation name:** CS1K_SBCE_AT&T

Module name: DiversionTypeAdapter

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

Egress URI Parameters:

Notes: CS1K via SBC-E

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

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				
<div>Edit New Duplicate Delete More Actions ▾</div>				
<div>Refresh Filter: Enable</div>				
<input type="checkbox"/>	Name	Module name	Egress URI Parameters	Notes
<input type="checkbox"/>	CS1K	CS1000Adapter fromto=true		
<input type="checkbox"/>	CS1K SBCE AT&T	DiversionTypeAdapter odstd=135.25.29.74 osrcd=192.168.64.130 MIME=no		
Select : All, None				

6.4. SIP Entities

SIP Entities must be added for Avaya CS1000E and Avaya SBCE. 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 Avaya 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 Avaya 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 Avaya CS1000E in the sample configuration.

SIP Entity Details [Commit] [Cancel]

General

* Name: CS1K

* FQDN or IP Address: 172.16.6.110

Type: SIP Trunk

Notes:

Adaptation: CS1K

Location: CS1K

Time Zone: America/New_York

Override Port & Transport with DNS SRV: ☐

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

Credential name:

Call Detail Recording: none

SIP Link Monitoring

SIP Link Monitoring: Use Session Manager Configuration

6.4.2. SIP Entity for Avaya SBCE

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.

AVAYA Avaya Aura® System Manager 6.1 [Help] [About] [Change Password]

Routing

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

SIP Entity Details [Commit]

General

* Name: SBCE_and AT&T

* FQDN or IP Address: 192.168.67.120

Type: Other

Notes:

Adaptation: CS1K_SBCE_AT&T

Location: SBCE

Time Zone: America/New_York

Override Port & Transport with DNS SRV: ☐

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

Credential name:

Call Detail Recording: none

SIP Link Monitoring

SIP Link Monitoring: Use Session Manager Configuration

6.5. Entity Links

The SIP trunk between Session Manager and Avaya CS1000E is defined by an Entity Link, as is the SIP trunk between Session Manager and Avaya SBCE.

6.5.1. Entity Link to Avaya CS1000E 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 Avaya 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]

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 Avaya 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 Avaya SBCE

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 Avaya SBCE 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]

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 Avaya SBCE.

Avaya Aura® System Manager 6.1

Home / Elements / Routing / Entity Links - Entity Links

Entity Links

Name	SIP Entity 1	Protocol	Port	SIP Entity 2	Port	Connection Policy
* SBCE_to_AT&T	* SM61	TCP	* 5060	* SBCE_and AT&T	* 5060	Trusted

* Input Required

6.6. Routing Policies

Routing policies describe the conditions under which calls will be routed by Session Manager to Avaya CS1000E.

6.6.1. Routing Policy to Avaya 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 Avaya 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 Avaya CS1000E.

Routing Policy Details Help ? Commit Cancel

General

* Name:

Disabled: ☐

Notes:

SIP Entity as Destination

Select

Name	FQDN or IP Address	Type	Notes
CS1K	172.16.6.110	SIP Trunk	

Time of Day

Add Remove View Gaps/Overlaps

1 Item Refresh Filter: Enable

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 inbound calls from the AT&T IP Toll Free service to Avaya CS1000E users.

Note that the dialed AT&T DID numbers may not be the same as the AT&T DNIS numbers sent in the SIP Request-URI headers. The numbers used in the inbound Request-URIs are the numbers to be defined here in the **Pattern** fields.

6.7.1. Inbound AT&T IP Toll Free calls to Avaya CS1000E

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 Avaya CS1000E (e.g., **732555xxxx**)
- **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 Avaya SBCE in **Section 6.2.2**.
- In the **Routing Policies** table, select the Routing Policy defined for Avaya 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 DNIS numbers to be routed to Avaya CS1000E.

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

Routing x

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

Dial Pattern Details [Commit](#)

General

* **Pattern:** 732555

* **Min:** 10

* **Max:** 10

Emergency Call: ☐

SIP Domain: -ALL-

Notes: Inbound from AT&T

Originating Locations and Routing Policies

[Add](#) [Remove](#)

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

Select : All, None

Denied Originating Locations

[Add](#) [Remove](#)

0 Items [Refresh](#)

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

* Input Required [Commit](#)

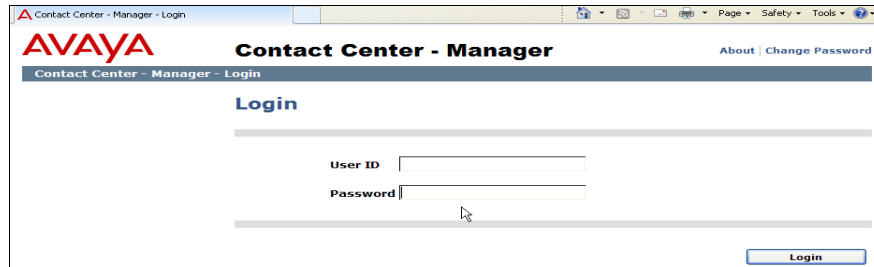
7. Avaya Aura® Contact Center

In the reference configuration, Avaya Aura® Contact Center is used to manage Agent functionalities and integrate these functions between the Avaya CS1000E and Avaya Call Pilot®. In the reference configuration Application Module Link (AML) protocol is used between the Avaya CS1000E and Avaya Aura® Contact Center.

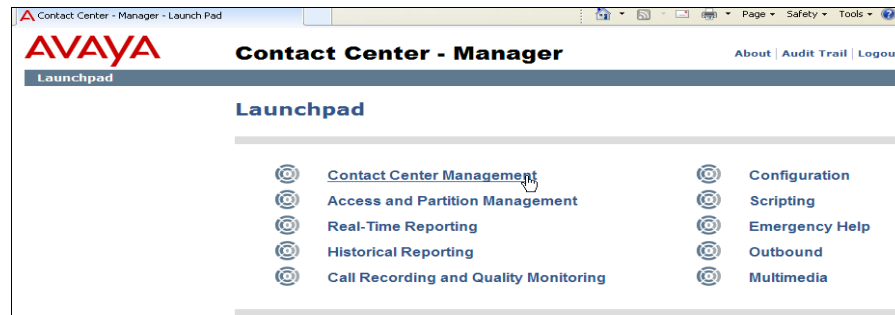
The installation and administration for Avaya Aura® Contact Center is beyond the scope of these Application Notes (consult [11] through [16] for further details). The provisioning and establishment of the AML connection between Avaya Aura® Contact Center and the Avaya CS1000E is assumed to be completed. However some illustrative examples of Agent configurations in Avaya Aura® Contact Center are shown below.

7.1. Create Avaya Aura® Contact Center Agent

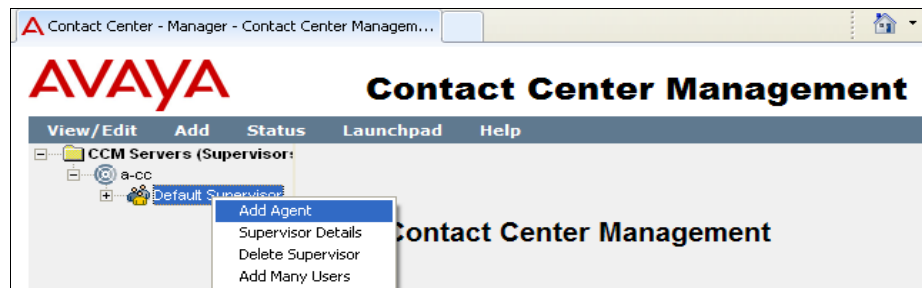
Step 1 – Log into the Avaya Aura® Contact Center Manager web interface.



Step 2 – On the **Launchpad** page, select **Contact Center Management**.



Step 3 – In the left hand column, expand the name of the Avaya Aura® Contact Center (e.g., **a-cc**), right click on appropriate supervisor (e.g., **Default Supervisor**), and select **Add Agent**.



Step 4 – On the **Agent Details** page, enter the information as shown in the example below. In the example, **agent2** has a login ID of **4014** (see **Section 5.7**), is a **Voice** Contact, and is assigned as a priority 1 contact for skill set two (**SK2**).

Step 5 – Click **Submit** (not shown). Repeat for additional Agents/Skills.

Agent Details: **agent2 agent2** Server: a-cc

User Details

First Name: **agent2** User Type: **Agent**
 Last Name: **agent2** Login ID: *** 4014**
 Title: Personal DN:
 Department: ACD Queue:
 Language: **English** ACD Queue Error:
 Comment:

Account Type:
☒ Create CCT Agent
CCT Agent Login Details
 Domain: **A-CC**
 User Name: **agent2**

[Associate User Account](#)

Agent Information

Primary Supervisor: *** Default Supervisor** Call Presentation: **Call_Centre_Administrator**
 Agent Key: Threshold: **Agent_Template**
 Login Status: **Logged Out** Tn Name:

Contact Types

Contact Type	
Predictive_Outbound	<input type="checkbox"/>
Scanned_Document	<input type="checkbox"/>
SMS	<input type="checkbox"/>
Voice	<input checked="" type="checkbox"/>
Voice_Mail	<input type="checkbox"/>
Web_Communications	<input type="checkbox"/>

Skillsets

Skillset Name (2)	Contact Type	Priority
Default_Skillset	Voice	5
SK2	Voice	1

[Assign Skillsets](#)

[Partitions](#)

7.2. Verifying Control DN (CDN) and Agent Connection Status

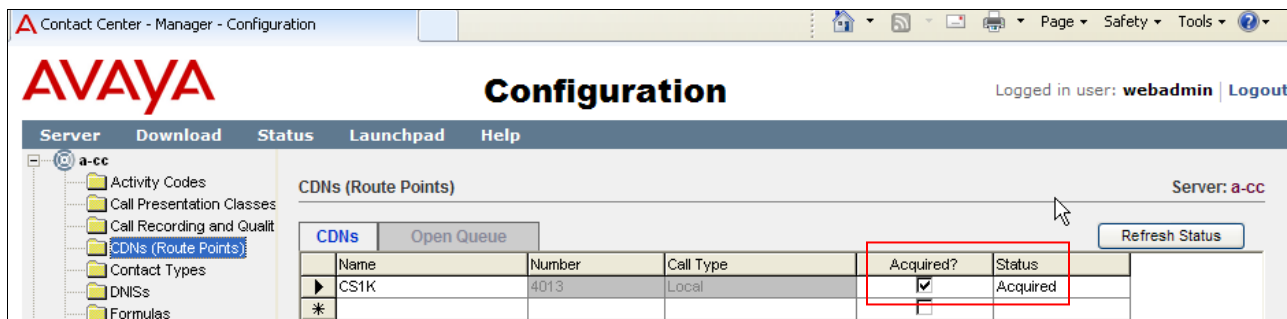
7.2.1. CDN Connection status

The Avaya Aura® Contact Center/Avaya CS1000E CDN connection status can be verified as follows.

Step 1 – Connect to **Launchpad** as described in **Section 7.1**.

Step 2 – Select **Configuration**.

Step 3 – From the left hand menu select **CDNs (Route Points)**. The connection provisioned on Avaya Aura® Contact Center to the Avaya CS1000E will be displayed. Verify the status is **Acquired**.

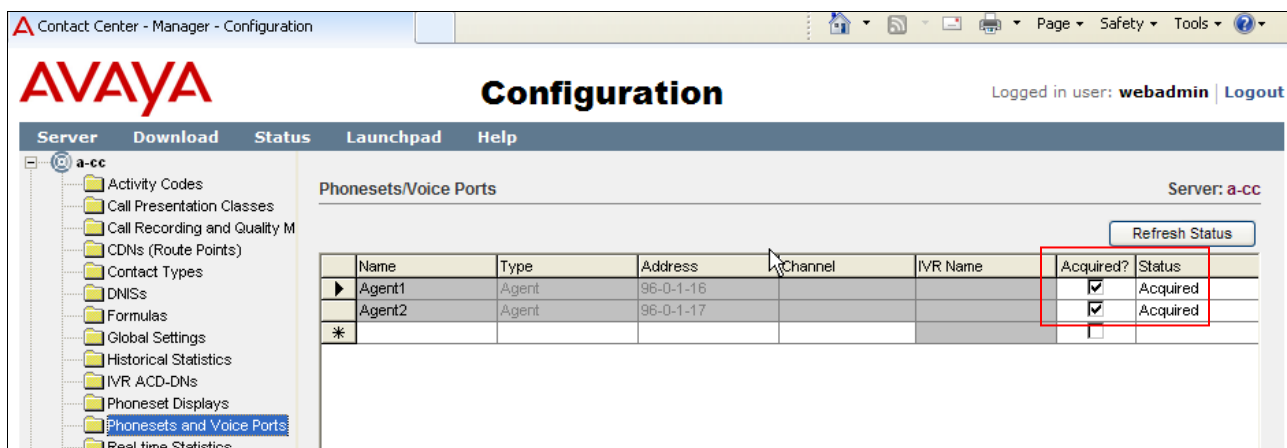


7.2.2. Agent Connection status

Step 1 – Connect to **Launchpad** as described in **Section 7.1**.

Step 2 – Select **Configuration**.

Step 3 – From the left hand menu select **Phonesets and Voice Ports**. The provisioned agents will be displayed. Verify the status is **Acquired**.



8. Configure Avaya Session Border Controller for Enterprise

8.1. Initial Provisioning

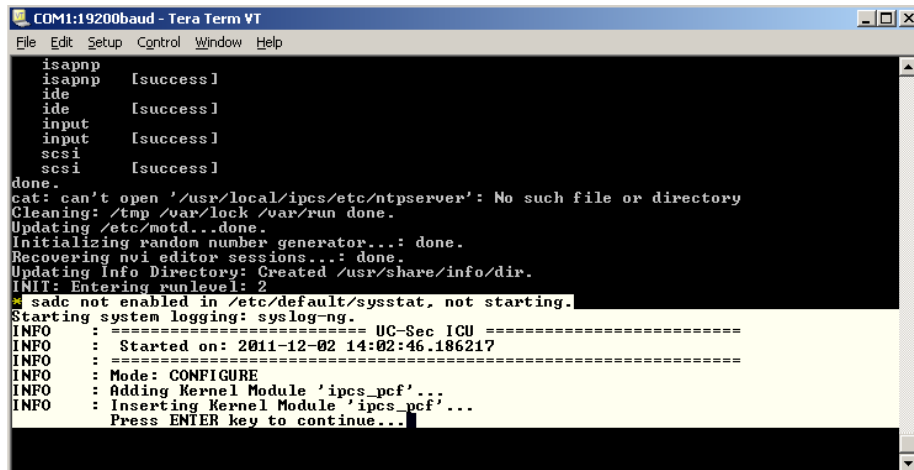
The following sections describe the provisioning of Avaya SBCE.

Note: Only Avaya SBCE provisioning required for the reference configuration is described in these Application Notes.

Avaya SBCE was configured via a serial console port connection and via an IP connection once the basic system provisioning was completed. The platform was configured as a single **EMS + UC-SEC** configuration. The following are the steps for provisioning the basic configuration:

1. Connect to the console port on the back of the server.
2. Start the serial connection application (i.e. Hyperterminal, Putty, etc.)
3. Power on the equipment.

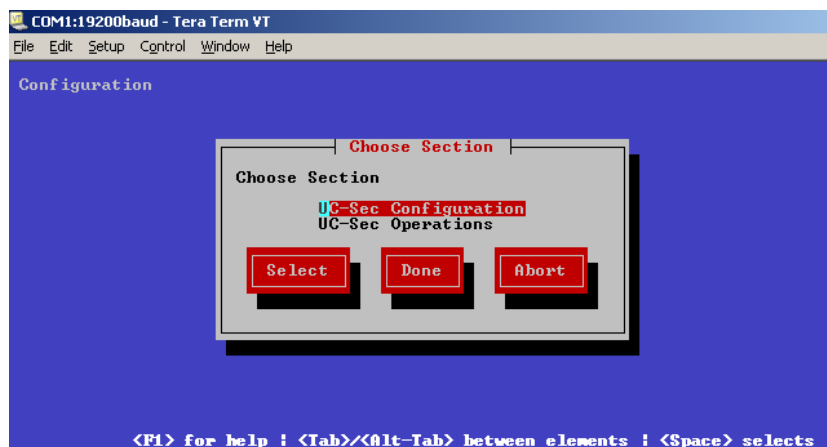
- The system will recognize that there is no configuration and will prompt the user to enter Config mode by asking the user to hit **Enter** twice.



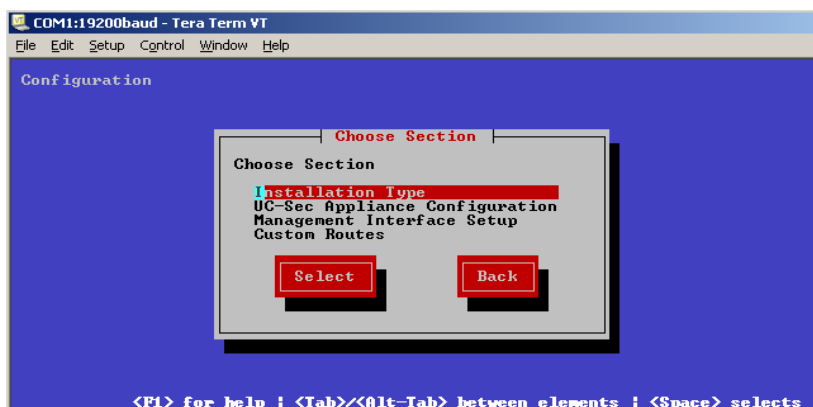
```
COM1:19200baud - Tera Term VT
File Edit Setup Control Window Help

isappnp
isappnp [success]
ide
ide [success]
input
input [success]
scsi
scsi [success]
done.
cat: can't open '/usr/local/ipcs/etc/ntpserver': No such file or directory
Cleaning: /tmp /var/lock /var/run done.
Updating /etc/motd...done.
Initializing random number generator...: done.
Recovering nvi editor sessions...: done.
Updating Info Directory: Created /usr/share/info/dir.
INIT: Entering runlevel: 2
* sads not enabled in /etc/default/sysstat, not starting.
Starting system logging: syslog-ng.
INFO : ===== UC-Sec ICU =====
INFO : Started on: 2011-12-02 14:02:46.186217
INFO : =====
INFO : Mode: CONFIGURE
INFO : Adding Kernel Module 'ipcs_pcf'...
INFO : Inserting Kernel Module 'ipcs_pcf'...
Press ENTER key to continue...
```

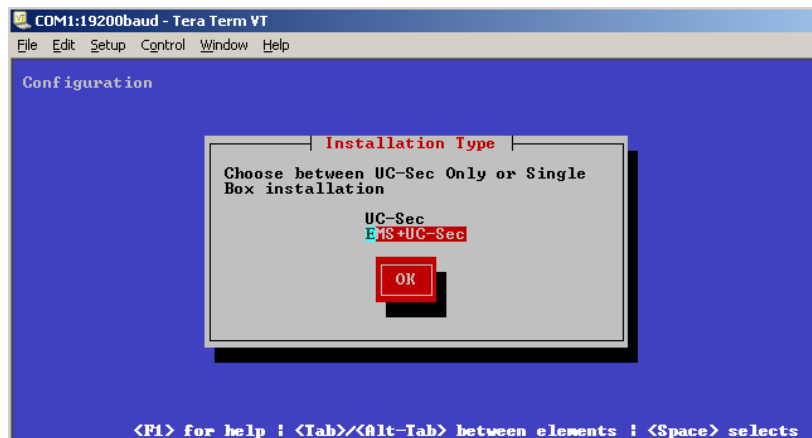
- The **Configuration** menu will appear. Select **UC Sec Configuration**



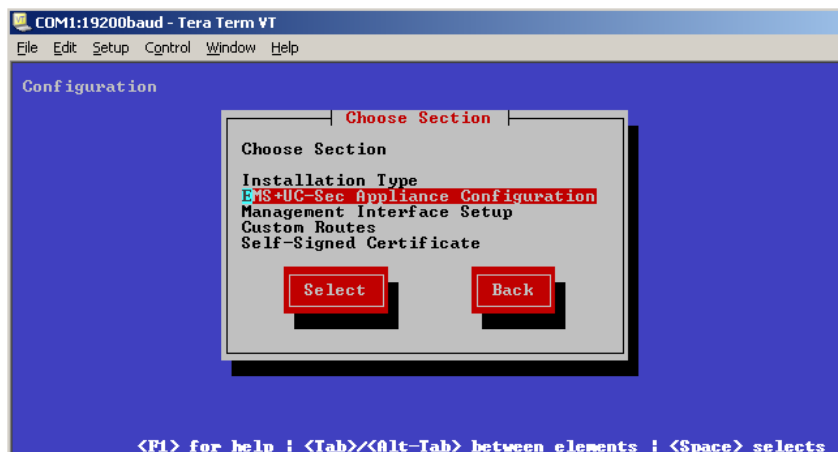
- Select **Installation Type**



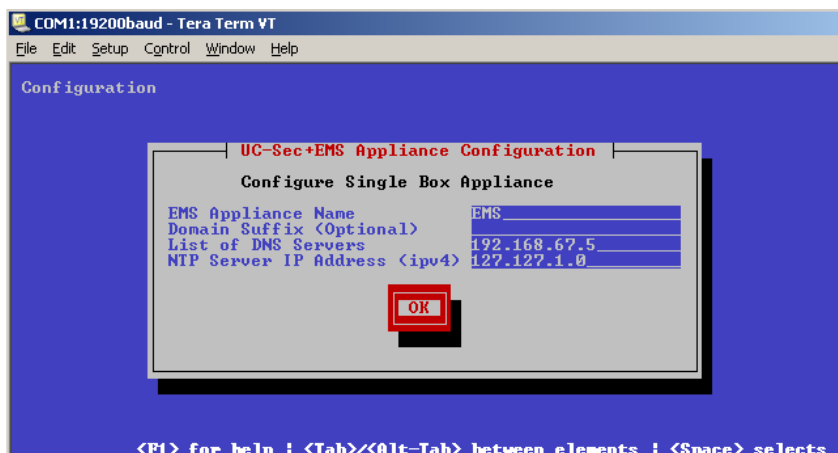
7. Select **EMS + UC-SEC**



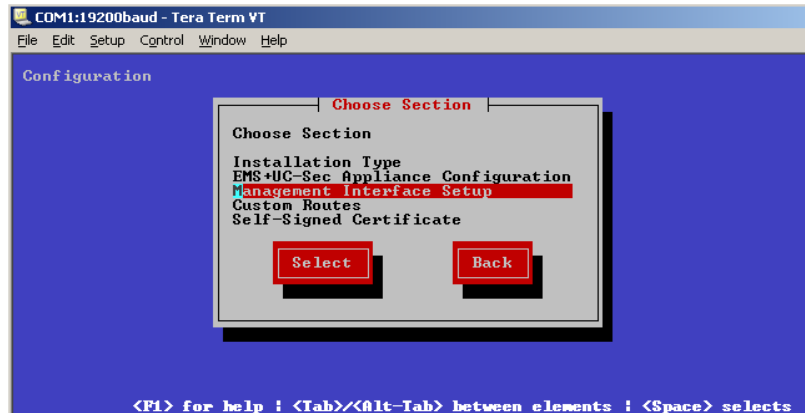
8. Select **EMS + UC-SEC Appliance Configuration**



9. Enter or leave Name as default (e.g., **EMS**). Enter IP address of DNS if applicable. If no NTP leave default value. Press OK

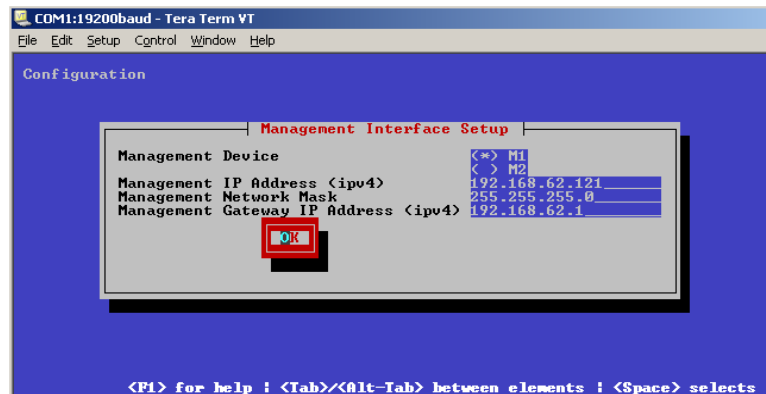


10. Select **Management Interface Setup**.

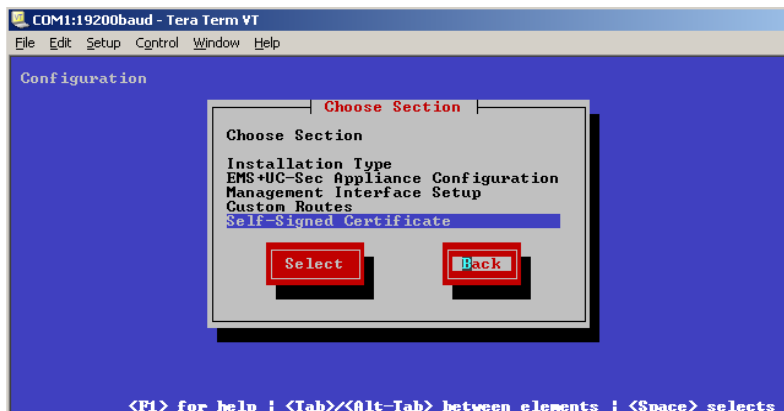


11. Select the **M1** interface. Enter the IP address you want for management (e.g., **192.168.62.121**). Enter mask and gateway. Select **OK**

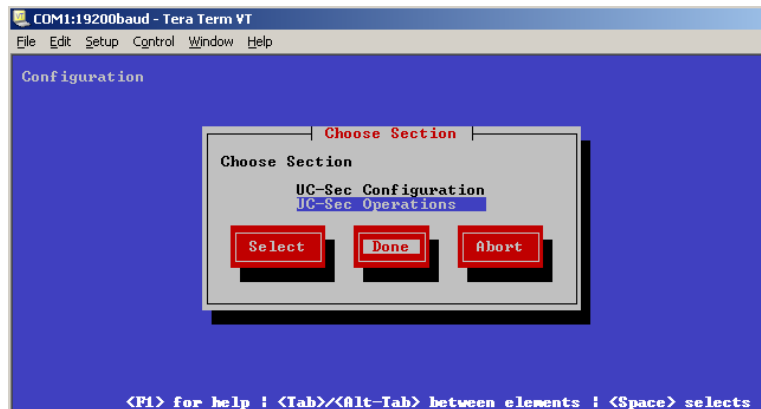
IMPORTANT! – The Management interface must be on a different subnet than either of the Avaya SBCE private and public network interfaces (e.g., A1 and B1).



12. You will be returned to the prior menu. Select **Back**.



13. Select **Done**. The SBC will reboot.

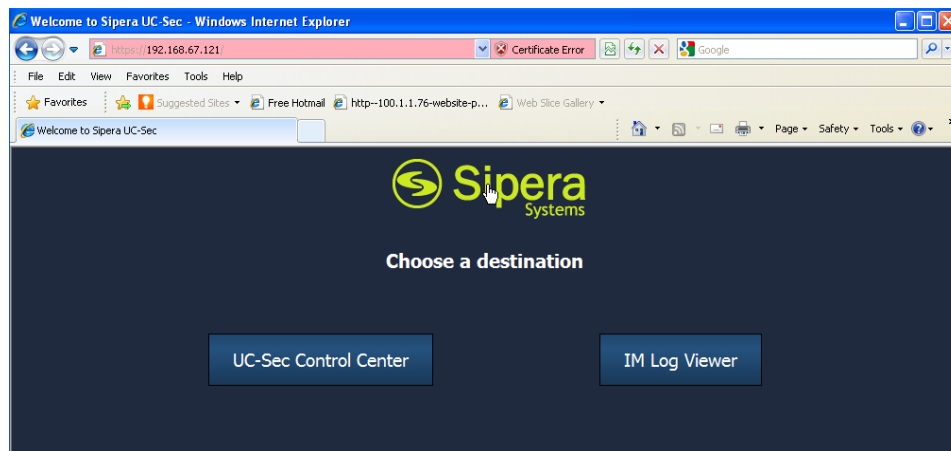


14. After the SBC reboots you will be prompted to press Enter as before. The SBC will then prompt for the date and time.
15. The SBC will prompt you for the password for "root" and then user "ipcs". Enter appropriate passwords for each.
16. The initial installation is complete and any further configuration will be done in the web interface.

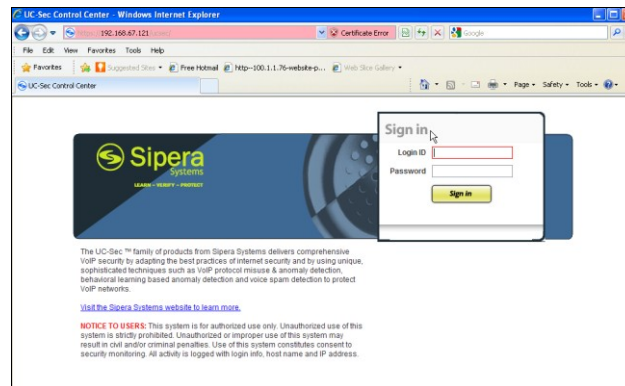
8.2. Advanced Configuration

The follow provisioning is performed via Avaya SBCE GUI interface.

1. Access the web interface by typing **https://x.x.x.x** (where x.x.x.x is the management IP of Avaya SBCE).
2. Select **UC-SEC Control Center**.



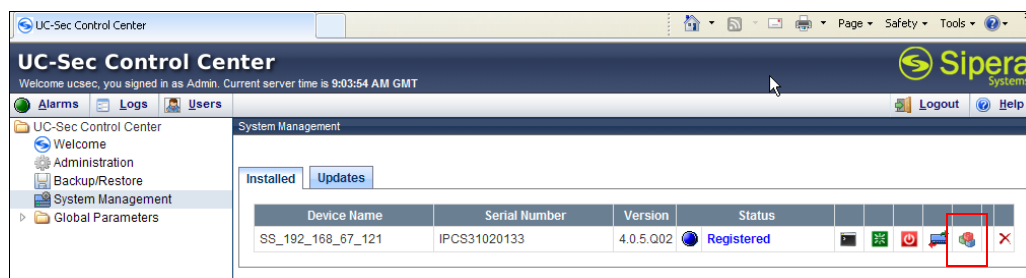
3. Enter the login ID and password



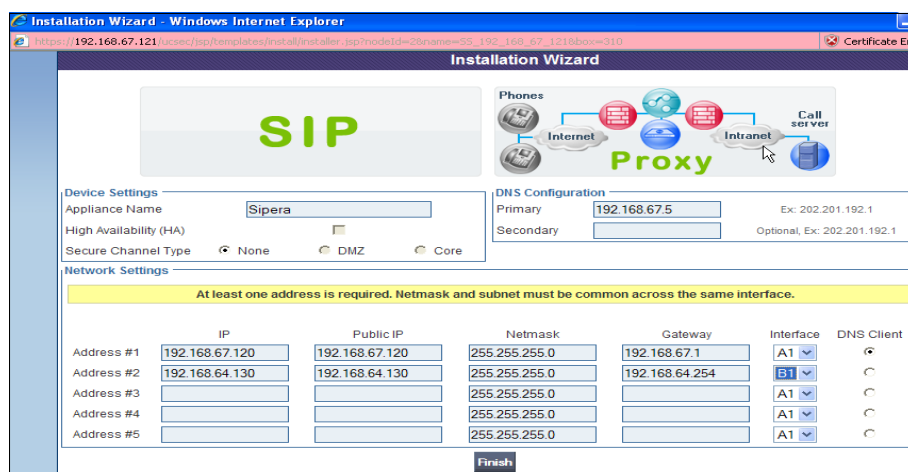
8.3. System Management

When it is the first time the user accesses Avaya SBCE system through the web interface, the user needs to configure some basic parameters.

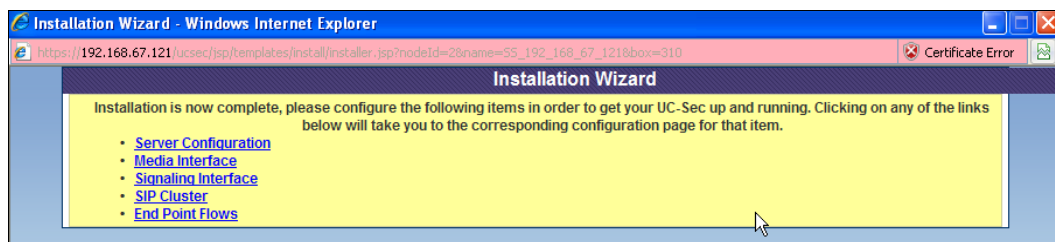
1. Click on the **System Management**, the user will see the screen below. The initial status of the SBCE is **Registered**, as shown. Click on the **install** icon (highlighted in red).



2. Click on the **System Management**, the screen below will open:



3. Enter the following information:
 - **Device Settings → Appliance Name** – Enter a descriptive name (e.g., **Sipera**).
 - **DNS Configuration → Primary** – Enter the IP address of a DNS if applicable.
 - **Network Settings → Address #1** – Note this will be the trusted “inside” interface:
 - Enter the appropriate IP address for **IP** and **Public IP** (the same address in each field).
 - Enter the appropriate **Netmask** and **Gateway**
 - Select interface **A1** (this interface is labeled **A1** on the back of the chassis).
 - Repeat the previous steps for **Address #2**, (this will be the untrusted “outside” interface), using the appropriate IP addressing, Netmask, and Gateway. Select interface **B1**.
4. Click **Finish**, and the following screen will appear giving an outline of the remaining tasks. This window may be closed.



8.4. Global Profiles

Global Profiles allows for configuration of parameters across all UC-Sec appliances.

8.4.1. Server Interworking – Avaya Side

Server Interworking allows you to configure and manage various SIP call server-specific capabilities such as call hold and T.38.

1. Select **Global Profiles** from the menu on the left-hand side
2. Select the **Server Interworking**
3. Select **Add Profile**
4. Select the **General Tab**:
 - a. Enter profile name: **Avaya**
 - b. Check **Hold Support: →RFC2543**
 - c. Check **T38 Support →Yes**
 - d. All other options on the General Tab can be left at default.
 - e. Select **Next**

General	
Hold Support	<input type="radio"/> None <input checked="" type="radio"/> RFC2543 - c=0.0.0.0 <input type="radio"/> RFC3264 - a=sendsonly
180 Handling	<input checked="" type="radio"/> None <input type="radio"/> SDP <input type="radio"/> No SDP
181 Handling	<input checked="" type="radio"/> None <input type="radio"/> SDP <input type="radio"/> No SDP
182 Handling	<input checked="" type="radio"/> None <input type="radio"/> SDP <input type="radio"/> No SDP
183 Handling	<input checked="" type="radio"/> None <input type="radio"/> SDP <input type="radio"/> No SDP
Refer Handling	<input type="checkbox"/>
3xx Handling	<input type="checkbox"/>
Diversion Header Support	<input type="checkbox"/>
Delayed SDP Handling	<input type="checkbox"/>
T.38 Support	<input checked="" type="checkbox"/>
URI Scheme	<input checked="" type="radio"/> SIP <input type="radio"/> TEL <input type="radio"/> ANY
Via Header Format	<input checked="" type="radio"/> RFC3261 <input type="radio"/> RFC2543

Back Next

5. On the Privacy window
 - a. Select **Next** to accept default values.

Privacy	
Privacy Enabled	<input checked="" type="checkbox"/>
User Name	
P-Asserted-Identity	
P-Preferred-Identity	
Privacy Header	

DTMF	
DTMF Support	<input checked="" type="radio"/> None <input type="radio"/> SIP NOTIFY <input type="radio"/> SIP INFO

Back Next

6. On the **SIP Timers** window
 - a. Select **Next** to accept default values.

SIP Timers		
Min-SE		seconds, [90 - 86400]
Init Timer		milliseconds, [50 - 1000]
Max Timer		milliseconds, [200 - 8000]
Trans Expire		seconds, [1 - 64]
Invite Expire		seconds, [180 - 300]

Transport Timers		
TCP Connection Inactive Timer		seconds, [600 - 3600]

Back Next

7. On the **Advanced Settings** window
 - a. Select **Next** to accept default values.
 - b. Click **Finish**.

Advanced Settings	
Record Routes	<input type="checkbox"/> None <input type="radio"/> Single Side <input checked="" type="radio"/> Both Sides
Topology Hiding: Change Call-ID	<input checked="" type="checkbox"/>
Call-Info NAT	<input type="checkbox"/>
Change Max Forwards	<input checked="" type="checkbox"/>
Include End Point IP for Context Lookup	<input type="checkbox"/>
OCS Extensions	<input type="checkbox"/>
AVAYA Extensions	<input type="checkbox"/>
NORTEL Extensions	<input type="checkbox"/>
SLIC Extensions	<input type="checkbox"/>
Diversion Manipulation	<input type="checkbox"/>
Diversion Header URI	<input type="text"/>
Metaswitch Extensions	<input type="checkbox"/>
Reset on Talk Spurt	<input type="checkbox"/>
Reset SRTP Context on Session Refresh	<input type="checkbox"/>
Has Remote SBC	<input checked="" type="checkbox"/>
Route Response on Via Port	<input type="checkbox"/>
Cisco Extensions	<input type="checkbox"/>

Back Finish

8.4.2. Server Interworking – AT&T Side

Repeat the steps shown in **Section 8.4.1** to add an Interworking Profile for the connection to AT&T.

1. Select **Global Profiles** from the menu on the left-hand side
2. Select the **Server Interworking**
3. Select **Add Profile**
4. On the **General** Tab:
 - a. Enter a profile name: (e.g., **ATT**)
 - b. Check **T38 Support** ☐ **Yes**
 - c. All other options on the General Tab can be left at default
 - d. Select **Next**
5. At the **Privacy** tab
 - a. Select **Next** to accept default values.
6. At the **Interworking Profile** tab
 - a. Select **Next** to accept default values.
7. On the **Advanced** Tab
 - a. Select **Next** to accept default values.
8. Click **Finish**

8.4.3. Routing – Avaya Side

The Routing Profile allows you to manage parameters related to routing SIP signaling messages.

1. Select **Global Profiles** from the menu on the left-hand side
2. Select the **Routing** tab
3. Select **Add Profile**
4. Enter Profile Name: (e.g., **To_Avaya**)
5. Hit **Next**
 - a. **Next Hop Server 1: 192.168.67.210** (Session Manager IP address)
 - b. Select **Routing Priority Based on Next Hop Server**
 - c. **Outgoing Transport: TCP**

6. Click **Finish**

Routing Profile

Each URI group may only be used once per Routing Profile.

Next Hop Routing

URI Group: *

Next Hop Server 1: 192.168.67.210 IP, IP:Port, Domain, or Domain:Port

Next Hop Server 2: IP, IP:Port, Domain, or Domain:Port

☒ Routing Priority based on Next Hop Server

☐ Use Next Hop for In Dialog Messages

☐ Ignore Route Header for Messages Outside Dialog

☐ NAPTR ☐ SRV

Outgoing Transport: ☐ TLS ☒ TCP ☐ UDP

Back Finish

8.4.4. Routing – AT&T Side

Repeat the steps in **Section 8.4.3** to add a Routing Profile for the AT&T connection.

1. Select **Global Profiles** from the menu on the left-hand side
2. Select the **Routing** tab
3. Select **Add Profile**
4. Enter Profile Name: (e.g., **To_ATT**)
5. Hit **Next**
 - a. **Next Hop Server 1: 135.25.29.74** (AT&T Border Element IP address)
 - b. Select **Routing Priority Based on Next Hop Server**
 - c. **Outgoing Transport: UDP**
6. Click **Finish**

Routing Profile

Each URI group may only be used once per Routing Profile.

Next Hop Routing

URI Group: *

Next Hop Server 1: 135.25.29.74 IP, IP:Port, Domain, or Domain:Port

Next Hop Server 2: IP, IP:Port, Domain, or Domain:Port

☒ Routing Priority based on Next Hop Server

☐ Use Next Hop for In Dialog Messages

☐ Ignore Route Header for Messages Outside Dialog

☐ NAPTR ☐ SRV

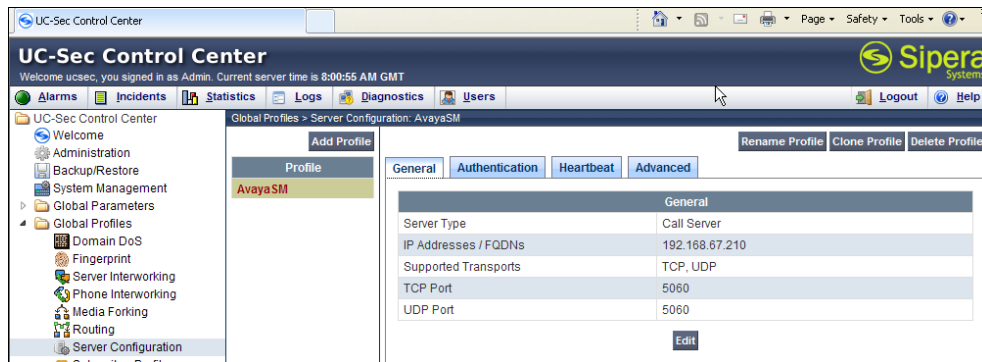
Outgoing Transport: ☐ TLS ☐ TCP ☒ UDP

Back Finish

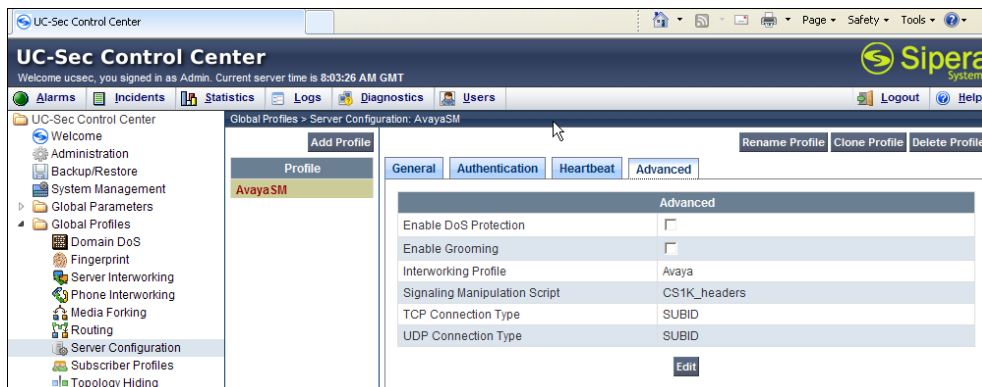
8.4.5. Server Configuration – To Avaya Session Manager

The **Server Configuration** screen contains four tabs: **General**, **Authentication**, **Heartbeat**, and **Advanced**. Together, these tabs allow you to configure and manage various SIP call server-specific parameters such as TCP and UDP port assignments, IP Server type, heartbeat signaling parameters and some advanced options.

1. Select **Global Profiles** from the menu on the left-hand side
2. Select the **Server Configuration**
3. Select **Add Profile**, enter profile name: (e.g., **Avaya SM**)
4. On the **Add Server Configuration Profile** Tab:
 - a. Select Server Type: **Call Server**
 - b. **IP Address: 192.168.67.210** (Session Manager IP Address)
 - c. **Supported Transports:** Check **UDP** and **TCP**
 - d. **TCP Port: 5060**
 - e. **UDP Port: 5060**
 - f. Select **Next**.



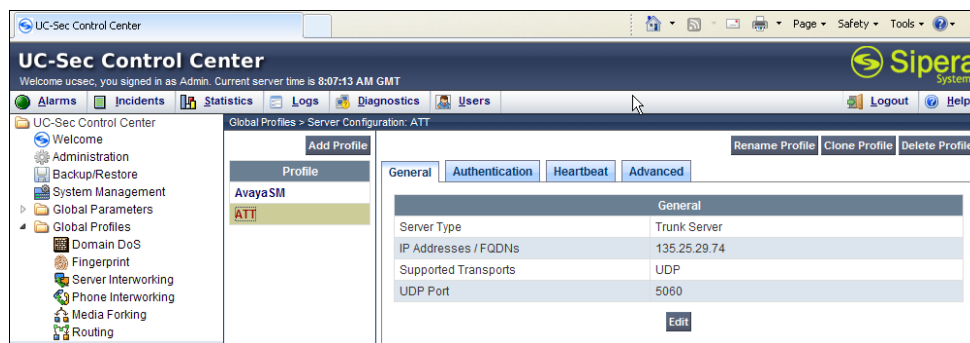
5. At the **Authentication** tab
 - a. Select **Next** to accept default values.
6. At the **Heartbeat** tab
 - a. Select **Next** to accept default values.
7. On the **Advanced** Tab
 - a. Select **Avaya** for Interworking Profile
 - b. Select the **CS1K_headers** script defined in **Section 8.4.9** for the **Signaling Manipulation Script**.
 - c. Use the remaining default values and select **Next**.
8. Click **Finish**.



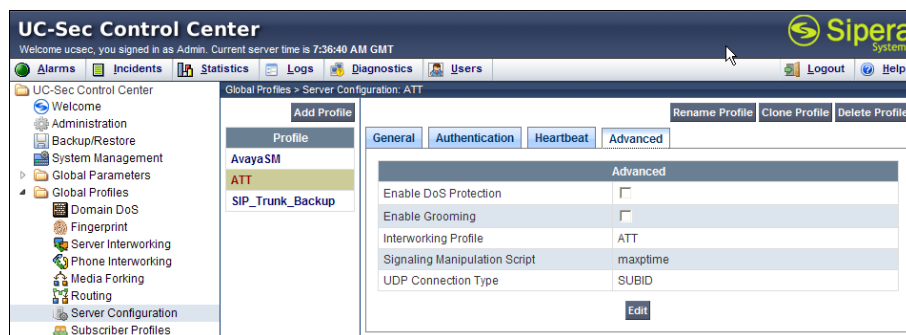
8.4.6. Server Configuration – To AT&T

Repeat the steps in **Section 8.4.5** to create a Server Configuration for the connection to AT&T.

1. Select **Global Profiles** from the menu on the left-hand side
2. Select the **Server Configuration**
3. Select **Add Profile**, enter profile name: (e.g., **ATT**)
4. On the **Add Server Configuration Profile** Tab:
 - a. Select Server Type: **Trunk Server**
 - b. **IP Address: 135.25.29.74** (AT&T Border Element IP Address)
 - c. **Supported Transports: Check UDP**
 - d. **UDP Port: 5060**
 - e. Select **Next**.



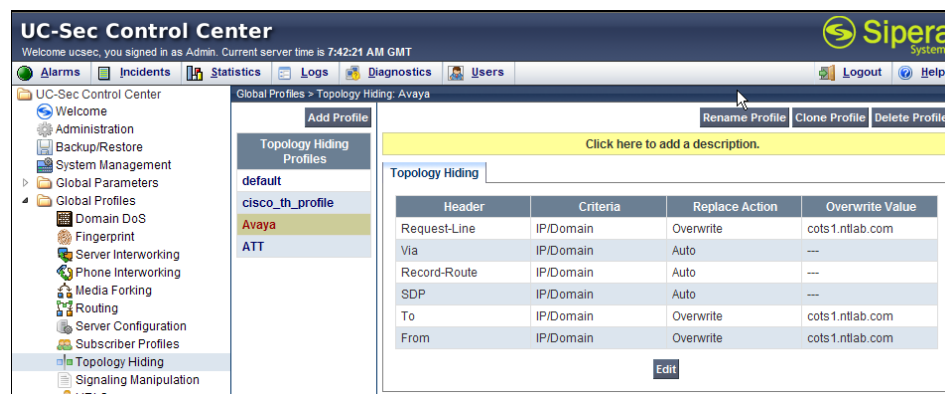
5. At the **Authentication** tab
 - a. Select **Next** to accept default values.
6. At the **Heartbeat** tab
 - a. Select **Next** to accept default values.
7. On the **Advanced** Tab
 - a. Select **Avaya** for Interworking Profile
 - b. In the **Signaling Manipulation Script** field select the **maxptime** script defined in **Section 8.4.9**.
 - c. Select **Next**.
8. Click **Finish**.



8.4.7. Topology Hiding – Avaya Side

The **Topology Hiding** screen allows you to manage how various source, destination and routing information in SIP and SDP message headers are substituted or changed to maintain the integrity of the network. It hides the topology of the enterprise network from external networks.

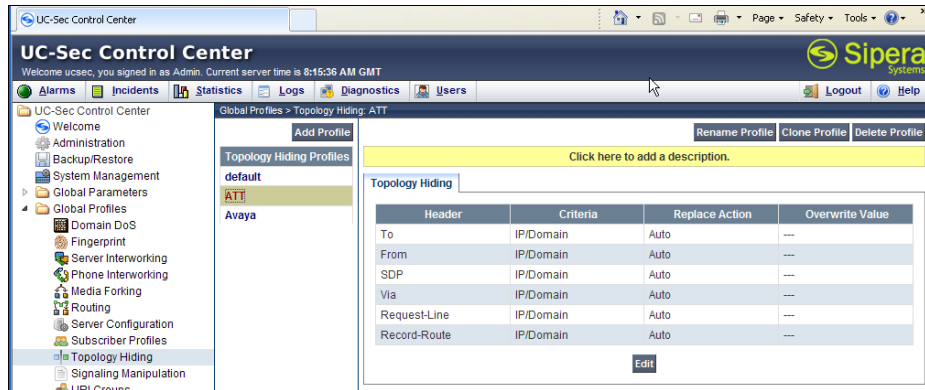
1. Select **Global Profiles** from the menu on the left-hand side
2. Select the **Topology Hiding**
3. Click **default** profile and select **Clone Profile**
4. **Enter Profile Name:** (e.g., **Avaya**)
5. For the Header **To**,
 - a. In the **Criteria** column select **IP/Domain**
 - b. In the **Replace Action** column select: **Overwrite**
 - c. In the **Overwrite Value** column enter the domain specified in **Sections 5.3** and **6.1** (e.g., **cots1.ntlab.com**)
6. For the Header **From**,
 - a. In the **Criteria** column select **IP/Domain**
 - b. In the **Replace Action** column select: **Overwrite**
 - c. In the **Overwrite Value** column: **cots1.ntlab.com**
7. For the Header **Request Line**,
 - a. In the **Criteria** column select **IP/Domain**
 - b. In the **Replace Action** column select: **Overwrite**
 - c. In the **Overwrite Value** column: **cots1.ntlab.com**
8. Click **Finish**



8.4.8. Topology Hiding – AT&T Side

Repeat the steps in **Section 8.4.7** to create a Topology Hiding Profile for the connection to AT&T.

1. Select **Global Profiles** from the menu on the left-hand side
2. Select the **Topology Hiding**
3. Click **default** profile and select **Clone Profile**
4. **Enter Profile Name:** (e.g., **ATT**)
5. Leave all Replace Action to “**Auto**”
6. Click **Finish**



8.4.9. Signaling Manipulations

The Avaya SBCE scripts can be used to create custom SIP header manipulations for request and response frames, sent the Avaya CS1000E or by AT&T. Refer to [10] for information on the Avaya SBE scripting language. In the reference configuration the following scripts were used for the following header manipulations:

1. When AT&T sends an Invite with the header **maxptime: 30**, change this header to **ptime: 30**. This function is performed so that the Avaya CS1000E UNISTim and Digital telephones will respond with **ptime:30** (see **Section 8.4.9.1**).
2. In addition to the MIME header removed by Session Manager (see **Section 6.3.2**), the Avaya CS1000E generates additional SIP headers that are not required by AT&T (such as Alert-Info, x-nt-e164-clid, RFC2833 Telephone Event type 111). In the interest of reducing packet overhead, these unnecessary headers are removed (**Section 8.4.9.2**).
3. AT&T does not support the Remote-Party-ID and History-Info headers. These headers are removed by the Avaya SBCE.

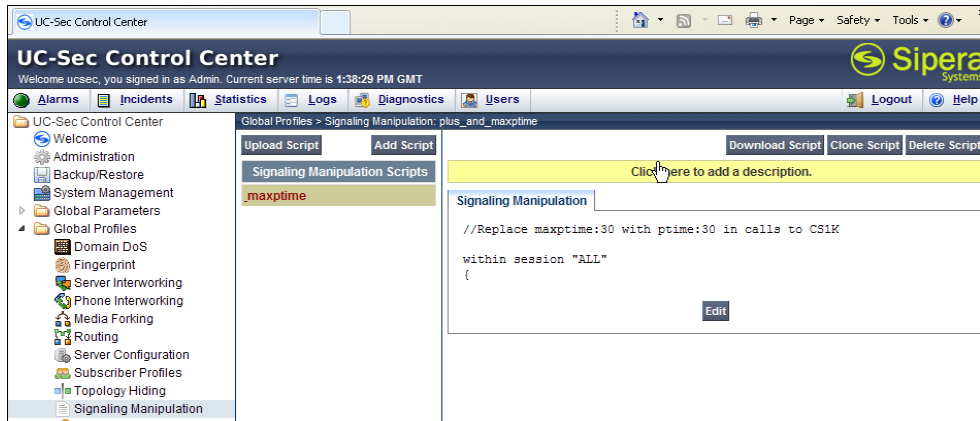
8.4.9.1 Modifying maxptime

1. Select **Global Profiles** from the menu on the left-hand side.
2. Select **Signaling Manipulation**.
3. Click **Add Script** (not shown) and the script editor window will open.
4. Enter a name for the script in the **Title** box (e.g., **maxptime**).
5. The following script is then defined:

```
//Replace maxptime:30 with ptime:30 in calls to CS1K

within session "ALL"
{
  act on request where %DIRECTION="INBOUND" and %ENTRY_POINT="PRE_ROUTING"
  {
    %BODY[1].regex_replace( "a=maxptime:30","a=ptime:30");
  }
}
```

6. After entering the script, click on **Save** (not shown). The Avaya SBCE will parse the script for any errors, and then close the script editing window.



Note -This script is specified in the **Server Configuration** defined in **Section 8.4.6**.

8.4.9.2 Removing unwanted headers

Create a script called **CS1K_headers** by repeating the steps in **Section 8.4.9.1**, and using the following script:

```
// Removes Alert-Info, x-nt-e164-clid, History-info, from CS1k.

within session "ALL"
{
  act on request where %DIRECTION="INBOUND" and %ENTRY_POINT="PRE_ROUTING"
  {

    // Remove unwanted Headers

    remove(%HEADERS["Alert-Info"][1]);
    remove(%HEADERS["x-nt-e164-clid"][1]);
    remove(%HEADERS["History-info"][1]);
    remove(%HEADERS["Remote-Party-ID"][1]);

    // Remove 111 from CS1k

    %BODY[1].regex_replace("100 111","100");
    %BODY[1].regex_replace("a=rtpmap:111","");
    %BODY[1].regex_replace("101 111","101");
  }
}

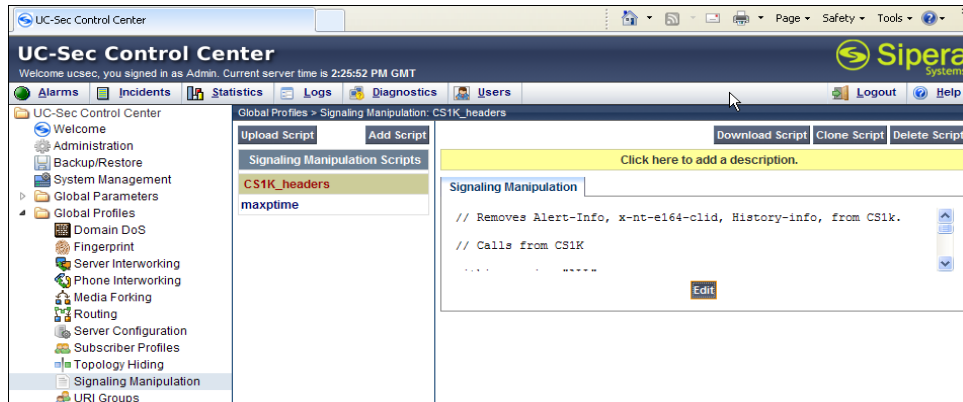
within session "ALL"
{
  act on response where %DIRECTION="INBOUND" and %ENTRY_POINT="PRE_ROUTING"
  {

    // Remove 111 from CS1K

    %BODY[1].regex_replace("100 111","100");
    %BODY[1].regex_replace("a=rtpmap:111","");
    %BODY[1].regex_replace("101 111","101");

    // Remove unwanted Headers

    remove(%HEADERS["History-info"][1]);
    remove(%HEADERS["Remote-Party-ID"][1]);
  }
}
```



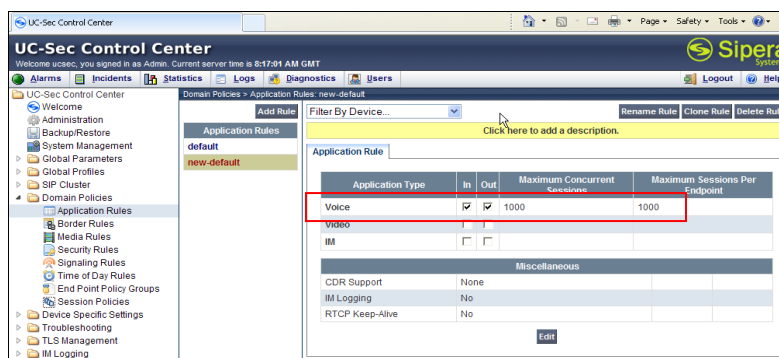
Note -This script is specified in the **Server Configuration** defined in **Section 8.4.5**.

8.5. Domain Policies

The Domain Policies feature allows you to configure, apply, and manage various rule sets (policies) to control unified communications based upon various criteria of communication sessions originating from or terminating in the enterprise. These criteria can be used to trigger different policies which will apply on call flows, change the behavior of the call, and make sure the call does not violate any of the policies. There are default policies available to use, or you can create a custom domain policy.

8.5.1. Application Rules

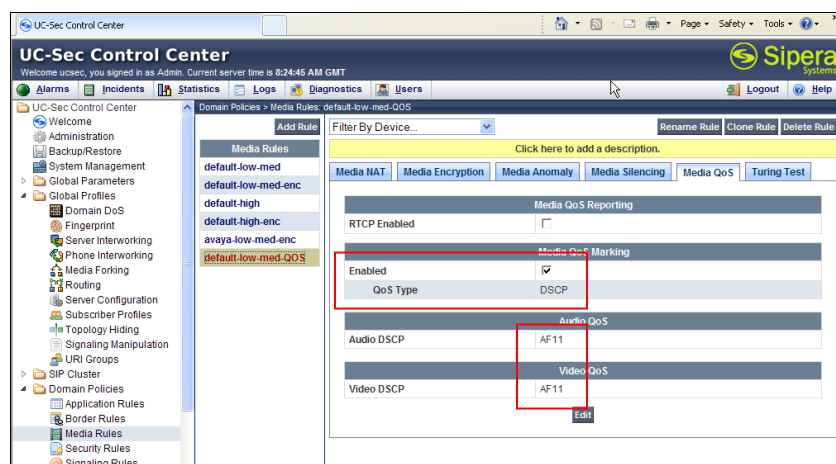
1. Select **Domain Policies** from the menu on the left-hand side
2. Select the **Application Rules**
3. Select the **default** Rule
4. Select **Clone Rule** button
 - a. Name: **new-default**
 - b. Click **Finish**
5. Highlight the rule just created: **new-default**
 - a. Click the **Edit** button
 - b. In the **Voice** row:
 - i. Change the **Maximum Concurrent Sessions** to **1000**
 - ii. Change the **Maximum Sessions per Endpoint** to **1000**



8.5.2. Media Rules

This Media Rule will be applied to both directions and therefore, only one rule is needed.

1. Select **Domain Policies** from the menu on the left-hand side
2. Select the **Media Rules**
3. Select the **default-low-med** Rule
4. Select **Clone Rule** button
 - a. Name: **default-low-med-QOS**
 - b. Click **Finish**
5. Highlight the rule just created: **default-low-med-QOS**
 - a. Select the **Media QOS** tab
 - b. Click the **Edit** button
 - c. Check the **Media QOS Marking** Enabled
 - d. Check the **DSCP** box
 - e. **Audio:** Select **AF11** from the drop-down
 - f. **Video:** Select **AF11** from the drop-down
6. Click **Finish**



8.5.3. Signaling Rules

This signaling rule is being created to strip the **P-Location** header information from the SIP messages before sending it on the service provider (the P-Location header may contain network information from the “inside” network).

1. Select **Domain Policies** from the menu on the left-hand side
2. Select the **Signaling Rules**
3. Select **Add Rule**
 - a) Name: **HideP-Loc**
 - b) Hit **Next**
4. On the **Signaling Rule** page
 - a) Hit **Next** to accept default values.

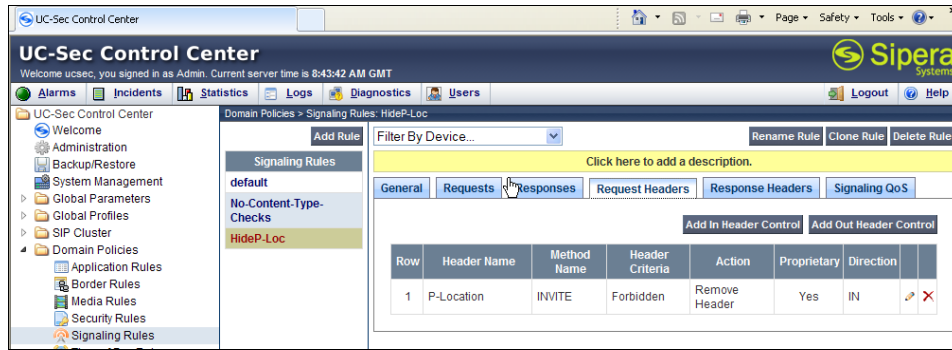
Signaling Rule			
Inbound			
Requests	Allow	403	Forbidden
Non-2XX Final Responses	Allow	486	Busy Here
Optional Request Headers	Allow	403	Forbidden
Optional Response Headers	Allow	486	Busy Here
Outbound			
Requests	Allow	403	Forbidden
Non-2XX Final Responses	Allow	486	Busy Here
Optional Request Headers	Allow	403	Forbidden
Optional Response Headers	Allow	486	Busy Here
Content-Type Policy			
Enable Content-Type Checks		<input checked="" type="checkbox"/>	
Action	Allow	Multipart Action	Allow
Exception List (one per line)		Exception List (one per line)	
Back		Next	

5. On the **Signaling QoS** page
 - a. Select **DSCP**
 - b. Select **AF11** from the drop-down box
 - c. Select **Finish**

Signaling Rule			
Signaling QoS			
Enabled		<input checked="" type="checkbox"/>	
<input type="radio"/> ToS			
Precedence			000
ToS			1000
<input checked="" type="radio"/> DSCP			
Value	AF11		001010
Back		Finish	

6. Select the **Request Headers** Tab
 - a) Select **Add in Header Control**
 - b) Check the **Proprietary Request Header** box
 - c) **Header Name: P-Location**
 - d) **Method Name: Invite**
 - e) **Header Criteria: Forbidden**
 - f) **Presence Action: Remove Header**
 - g) Click **Finish**

Edit Header Control			
Proprietary Request Header?	<input checked="" type="checkbox"/>		
Header Name	P-Location		
Method Name	INVITE		
Header Criteria	<input checked="" type="radio"/> Forbidden <input type="radio"/> Mandatory <input type="radio"/> Optional		
Presence Action	Remove header	486	Busy Here
Finish			



7. Select the **Response Headers** Tab
 - a) Select **Add in Header Control**
 - b) Check the **Proprietary Request Header** box
 - c) **Header Name: P-Location**
 - d) **Response Code: 200**
 - e) **Method Name: Invite**
 - f) **Header Criteria: Forbidden**
 - g) **Presence Action: Remove Header**
8. Click **Finish**

Edit Header Control

Proprietary Response Header? ☒

Header Name: P-Location

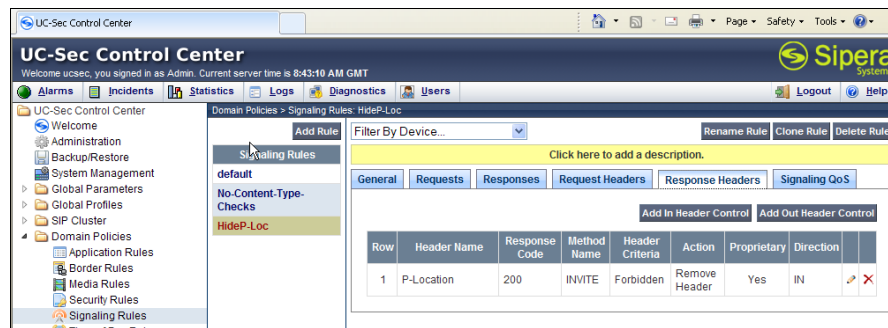
Response Code: 200

Method Name: INVITE

Header Criteria: ☒ Forbidden ☐ Mandatory ☐ Optional

Presence Action: Remove header

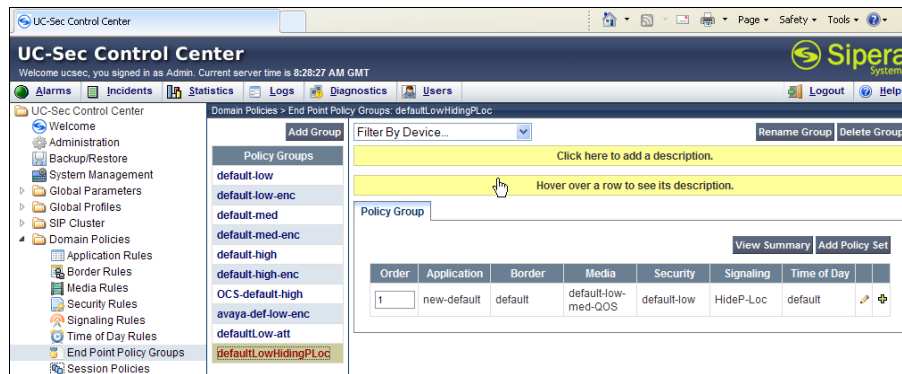
Finish



8.5.4. Endpoint Policy Groups – Avaya

1. Select **Domain Policies** from the menu on the left-hand side
2. Select the **End Point Policy Groups**
3. Select **Add Group**
 - a) **Name: defaultLowHidingPLoc**

- b) **Application Rule:** new-default
 - c) **Border Rule:** default
 - d) **Media Rule:** default-low-med-QOS
 - e) **Security Rule:** default-low
 - f) **Signaling Rule:** HideP-Loc
 - g) **Time of Day:** default
4. Select **Finish**



8.5.5. Endpoint Policy Groups – AT&T

1. Select **Domain Policies** from the menu on the left-hand side
2. Select the **End Point Policy Groups**
3. Select **Add Group**
 - a) **Name:** defaultLow-att
 - b) **Application Rule:** new-default
 - c) **Border Rule:** default
 - d) **Media Rule:** default-low-med-QOS
 - e) **Security Rule:** default-low
 - f) **Signaling Rule:** default
 - g) **Time of Day:** default
4. Select **Finish**

Application Rule	new-default
Border Rule	default
Media Rule	default-low-med-QOS
Security Rule	default-low
Signaling Rule	default
Time of Day Rule	default

Finish

UC-Sec Control Center

Welcome ucsec, you signed in as Admin. Current server time is 8:27:29 AM GMT

Alarms Incidents Statistics Logs Diagnostics Users Logout Help

UC-Sec Control Center

- Welcome
- Administration
- Backup/Restore
- System Management
- Global Parameters
- Global Profiles
- SIP Cluster
- Domain Policies
 - Application Rules
 - Border Rules
 - Media Rules
 - Security Rules
 - Signaling Rules
 - Time of Day Rules
 - End Point Policy Groups
 - Session Policies

Domain Policies > End Point Policy Groups: defaultLow-att

Add Group Filter By Device... Rename Group Delete Group

Policy Groups

- default-low
- default-low-enc
- default-med
- default-med-enc
- default-high
- default-high-enc
- OCS-default-high
- avaya-def-low-enc
- defaultLow-att
- defaultLowHidingPLoc

Click here to add a description.

Hover over a row to see its description.

Policy Group

View Summary Add Policy Set

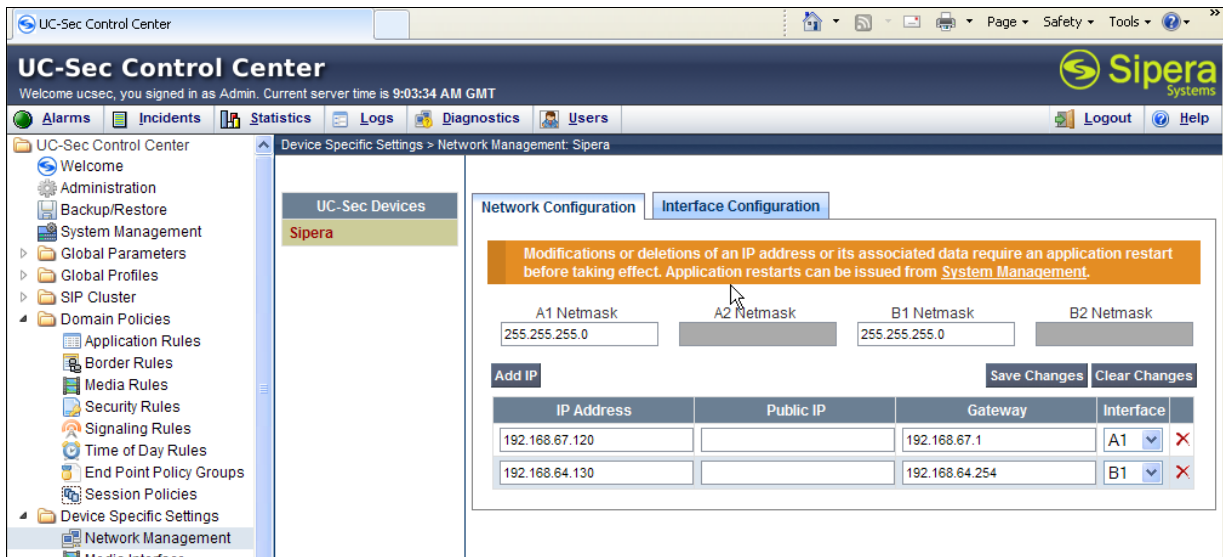
Order	Application	Border	Media	Security	Signaling	Time of Day	
1	new-default	default	default-low-med-QOS	default-low	default	default	

8.6. Device Specific Settings

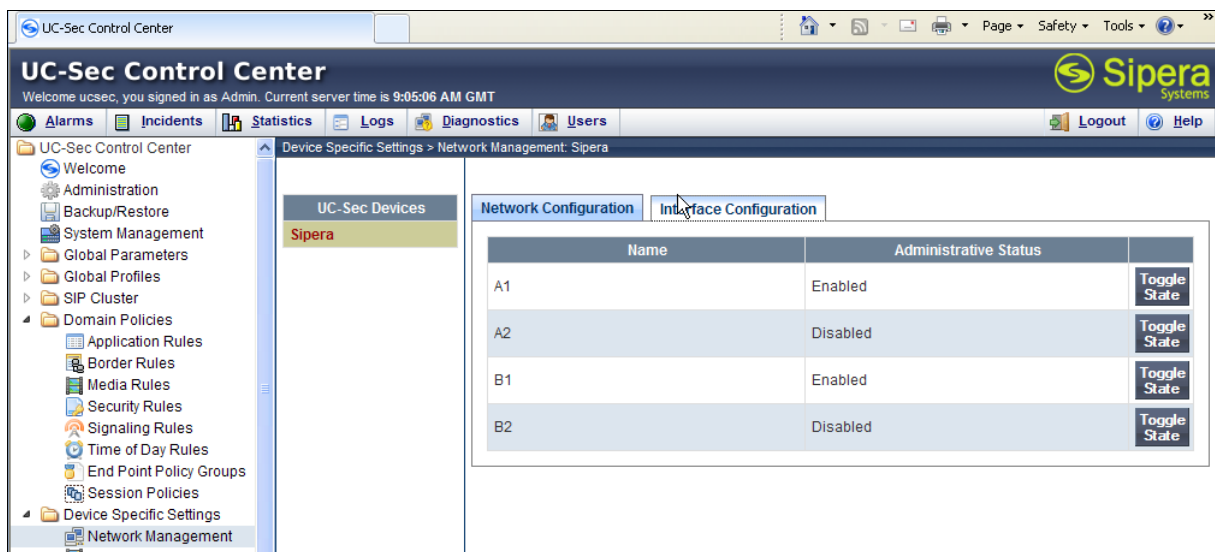
The **Device Specific Settings** feature for SIP allows you to view system information, and manage various device-specific network parameters. Specifically, you have the ability to define and administer various device-specific protection features such as Message Sequence Analysis (MSA) functionality, end-point and session call flows and Network Management.

8.6.1. Network Management

1. Select **Device Specific Settings** from the menu on the left-hand side
2. Select **Network Management**
 - a) The network interfaces were provisioned in **Section 8.3**. However if these values need to be modified, do so via this tab.



3. In addition, the provisioned interfaces may be enabled/disabled via the **Interface Configuration Tab**.
 - a) Toggle the State of the physical interfaces being used.

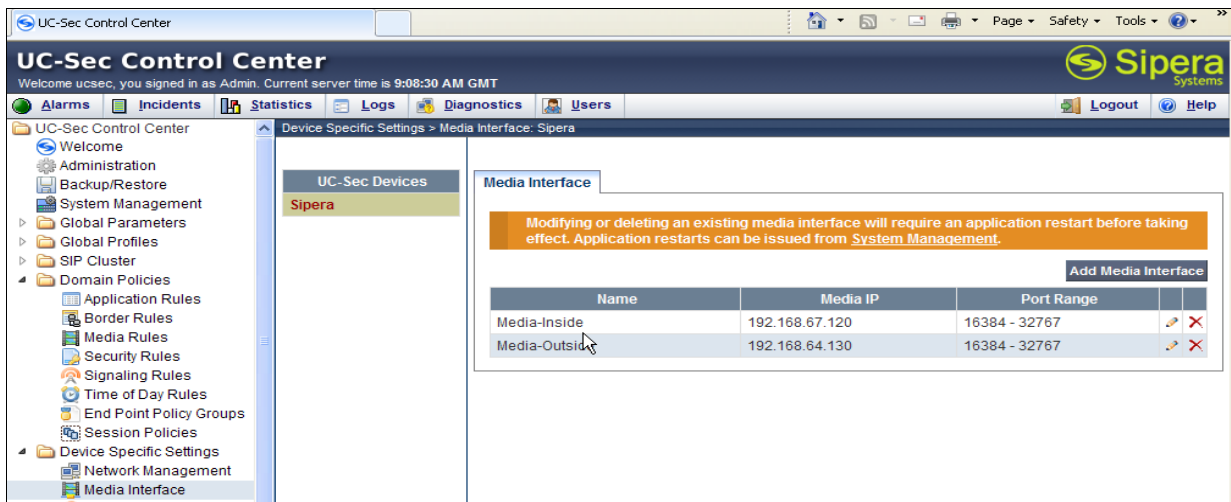


8.6.2. Media Interfaces

AT&T requires customers to use RTP ports in the range of 16384 – 32767. Both inside and outside ports have been changed but only the outside is required by AT&T.

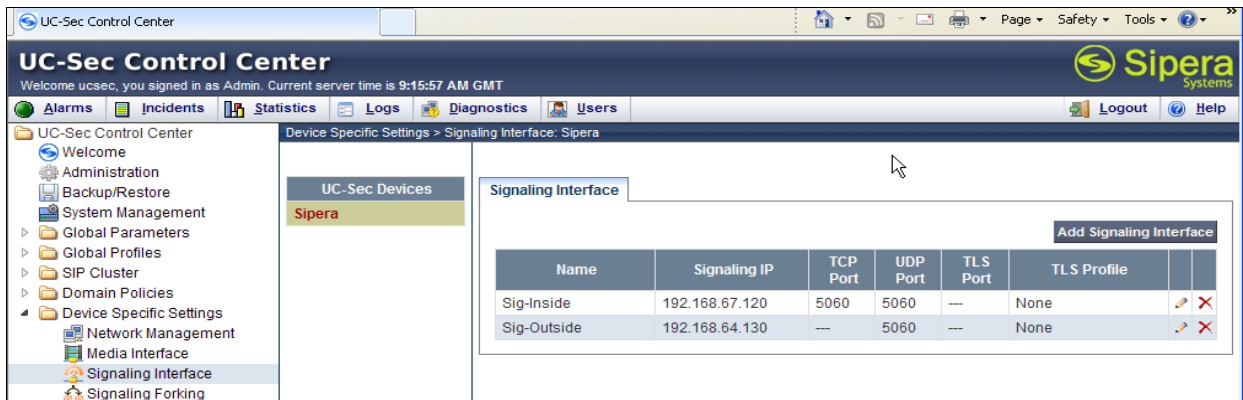
1. Select **Device Specific Settings** from the menu on the left-hand side
2. Select **Media Interface**
3. Select **Add Media Interface**
 - a) **Name: Media_Inside**

- b) **Media IP: 192.168.67.210** (Avaya SBCE internal address toward Session Manager)
 - c) **Port Range: 16384 - 32767**
4. Click **Finish**
5. Select **Add Media Interface**
 - a) **Name: Media_Outside**
 - b) **Media IP: 192.168.64.130** (Avaya SBCE external address toward AT&T)
 - c) **Port Range: 16384 - 32767**
6. Click **Finish**



8.6.3. Signaling Interface

1. Select **Device Specific Settings** from the menu on the left-hand side
2. Select **Signaling Interface**
3. Select **Add Signaling Interface**
 - a) **Name: Sig_Inside**
 - b) **Media IP: 192.168.67.210** (Avaya SBCE internal address toward Session Manager)
 - c) **TCP Port: 5060**
 - d) **UDP Port: 5060**
4. Click **Finish**
5. Select **Add Media Interface**
 - a) **Name: Sig_Outside**
 - b) **Media IP: 192.168.64.130** (Avaya SBCE external address toward AT&T)
 - c) **UDP Port: 5060**
6. Click **Finish**



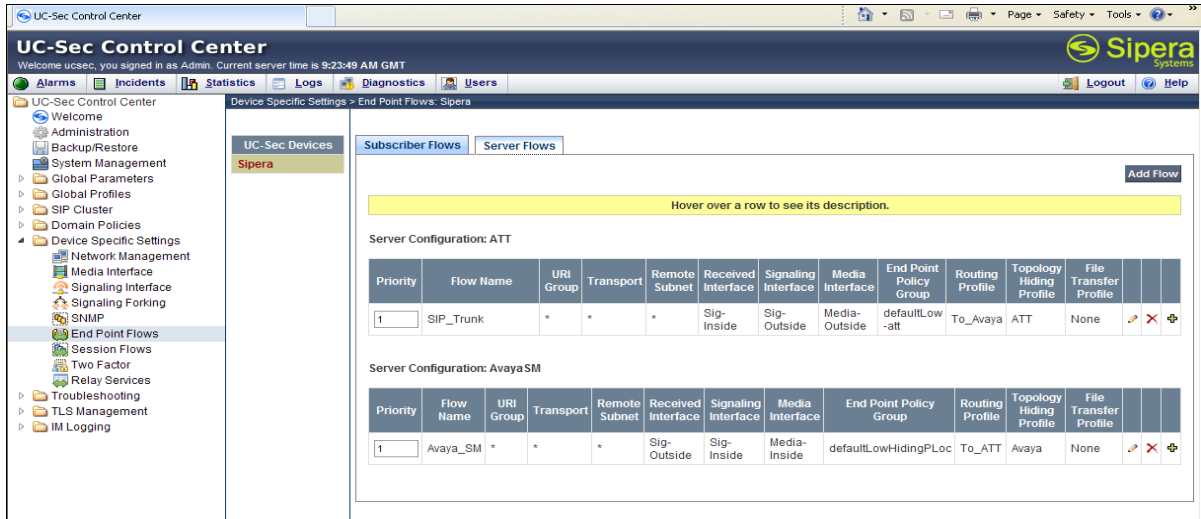
8.6.4. Endpoint Flows – To Session Manager

1. Select **Device Specific Settings** from the menu on the left-hand side
2. Select **Endpoint Flows**
3. Select the **Server Flows** Tab
4. Select **Add Flow**
 - a) **Name: Avaya_SM**
 - b) **Server Configuration: Avaya_SM**
 - c) **URI Group: ***
 - d) **Transport: ***
 - e) **Remote Subnet: ***
 - f) **Received Interface: Sig_Outside**
 - g) **Signaling Interface: Sig_Inside**
 - h) **Media Interface: Media_Inside**
 - i) **End Point Policy Group: defaultLowHidingPLoc**
 - j) **Routing Profile: To_ATT**
 - k) **Topology Hiding Profile: Avaya**
 - l) **File Transfer Profile: None**
5. Click **Finish**

8.6.5. Endpoint Flows – To AT&T

1. Select **Device Specific Settings** from the menu on the left-hand side
2. Select **Endpoint Flows**
3. Select the **Server Flows** Tab
4. Select **Add Flow**
 - a) **Name: SIP Trunk**
 - b) **Server Configuration: SIP Trunk**
 - c) **URI Group: ***
 - d) **Transport: ***
 - e) **Remote Subnet: ***
 - f) **Received Interface: Sig_Inside**
 - g) **Signaling Interface: Sig_Outside**
 - h) **Media Interface: Media_Outside**

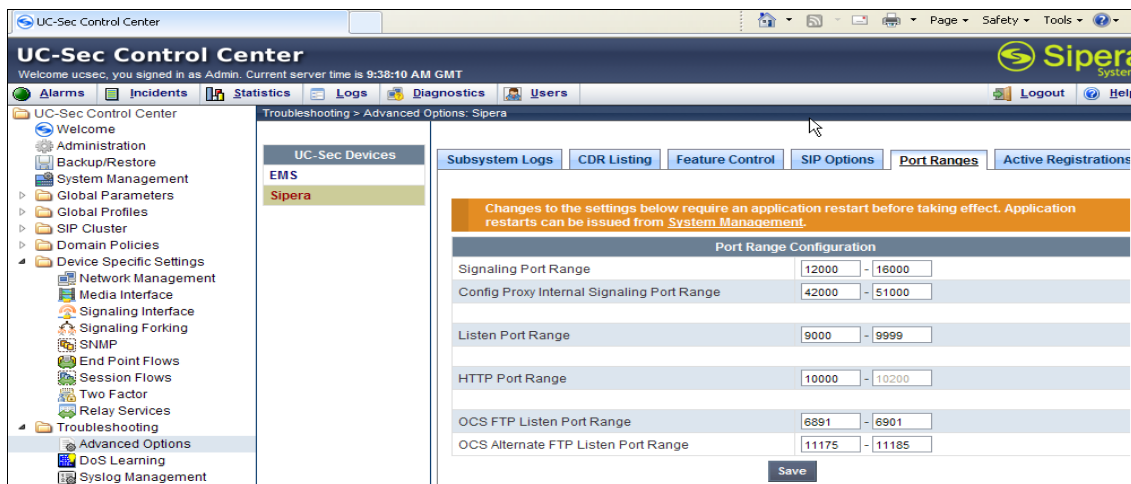
- i) **End Point Policy Group: defaultLow-att**
 - j) **Routing Profile: To_Avaya**
 - k) **Topology Hiding Profile: att**
 - l) **File Transfer Profile: None**
5. Click **Finish**



8.7. Troubleshooting Port Ranges

The default port range in this section needs to be changed to exclude the AT&T RTP port range of 16384 – 32767 (Section 8.6.2).

1. Select **Troubleshooting** from the menu on the left-hand side
2. Select **Advanced Options**
3. Select **Sipera** in the list of UC-Sec devices
4. Select **the Port Ranges** Tab
 - a) **Signaling Port Range: 12000 – 16000**
 - b) **Config Proxy Internal Signaling Port Range: 42000 – 51000** (or a range not being used)
5. Click **Save**



9. Verification Steps

The following steps may be used to verify the configuration.

9.1. General

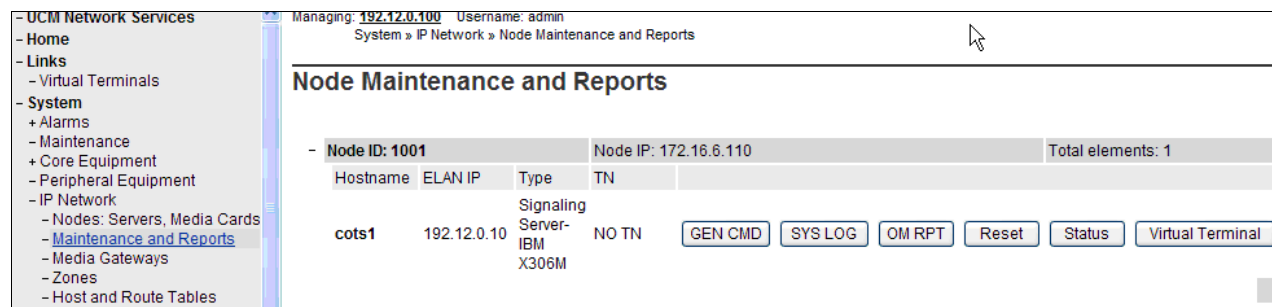
1. Place an inbound call, answer the call, and verify that two-way talk path exists. Verify that the call remains stable for several minutes and disconnect properly.
2. Place an inbound call to an agent or telephone, but do not answer the call. Verify that the call covers to Call Pilot® voicemail. Retrieve the message from Call Pilot®.

9.2. Avaya Communication Server 1000E Verifications

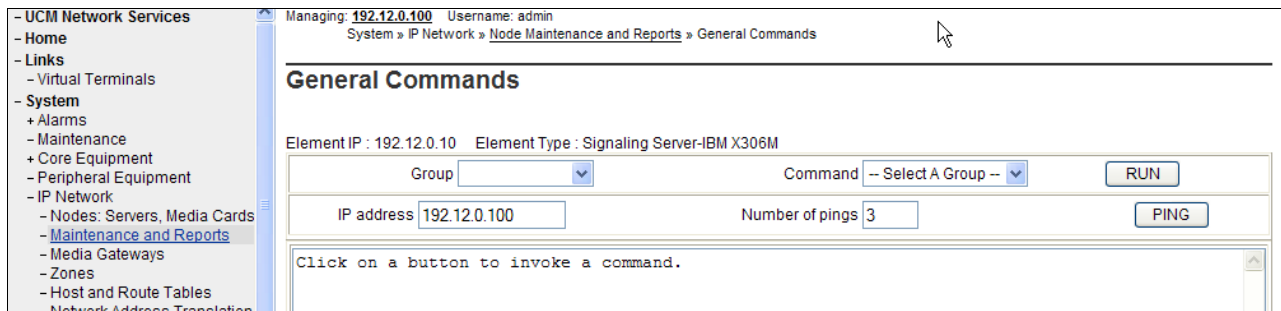
This section illustrates sample verifications that may be performed using the Avaya CS1000E Element Manager GUI.

9.2.1. IP Network Maintenance and Reports Commands

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

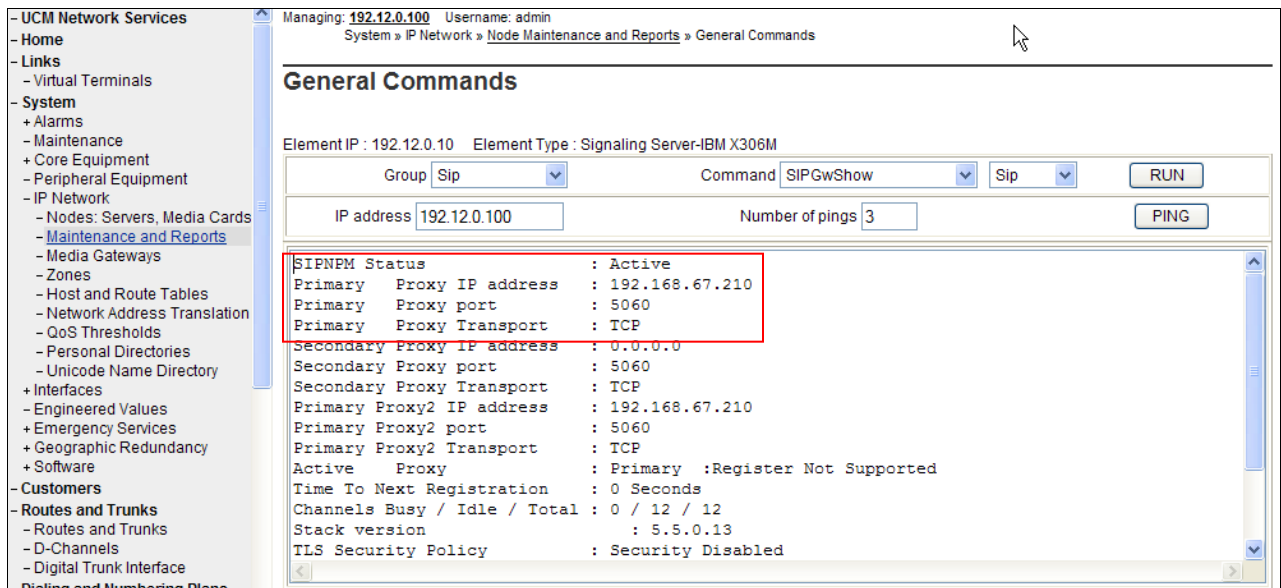


Step 2 - In the resultant screen on the right, click the **Gen CMD** button. The **General Commands** page is displayed as shown below.



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.



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 **Vtrk** Command **vtrkShow** Protocol Start Range **RUN**

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

```

-----
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 16², 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 (**192.168.67.120**) is the IP Address of the inside private interface of the Avaya SBCE.

General Commands

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

Group **Sip** Command **SIPGWShowch** **Sip** **16** **RUN**

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

```

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
G 729A 30MS			796	yes	m	no	4094 192.168.67.120
nearEnd Msec policy = 0							
farEnd Msec policy = 0							

² 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 (**192.168.67.120**) is the IP Address of the inside private interface of the Avaya SBCE.

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      URI Scheme
-----
G_729A_30MS      67 yes m  no  4094  192.168.67.120  ::      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**

Iset 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

9.2.2. 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.

Managing: 10.7.8.61 Username: admin
System » Maintenance

Maintenance

☒ Select by Overlay ☐ Select by Functionality

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.

Maintenance

☒ Select by Overlay ☐ Select by Functionality

<Select by Overlay>

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

<Select Group>

- D-Channel Diagnostics**
- MSDL Diagnostics
- TMDI Diagnostics

On the preceding screen, if **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**.

Managing: 192.12.0.100 Username: admin
System » Maintenance » D-Channel Diagnostics

D-Channel Diagnostics

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

DCH	DES	APPL_STATUS	LINK_STATUS	AUTO_REC	PDCH	BDCH
<input checked="" 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].

9.3. Avaya Aura® Session Manager

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 “SBCE_andAT&T”. Under normal operating conditions, the **Link Status** should be “Up” as shown in the example screen below. The **Reason Code** column indicates that the SBC has responded to SIP OPTIONS from Session Manager with a SIP 405 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: SBCE_and 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	192.168.67.120	5060	TCP	Up	405 Method Not Allowed	Up

Return to the list of monitored entities, and select another entity of interest, such as “CS1K”. 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.

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: 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)	
Apr 17, 2012 8:02:53 AM EDT		Apr 17, 2012 8:09:31 AM EDT	Apr 17, 2012 9:43:25 AM EDT			7	

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 7325554383 and Session Manager converts this to Avaya CS1000E extension 4094 before routing the call to the Avaya 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

555

Called Party URI 7325554383@cots1.ntlab.com	Calling Party Address 192.168.67.125
Calling Party URI 17325552438@192.168.67.125	Session Manager Listen Port 5060
Day Of Week Friday	Time (UTC) 22:28
Called Session Manager Instance SM61	Transport Protocol TCP

Execute Test

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 < 7325554383 > and host < cots1.ntlab.com > for routing.

NRP Dial Patterns: No matches for digits < 7325554383 > and domain < cots1.ntlab.com >.

NRP Dial Patterns: No matches for digits < 7325554383 > and domain < ntlab.com >.

NRP Dial Patterns: Found a Dial Pattern match for pattern < 732555 > 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

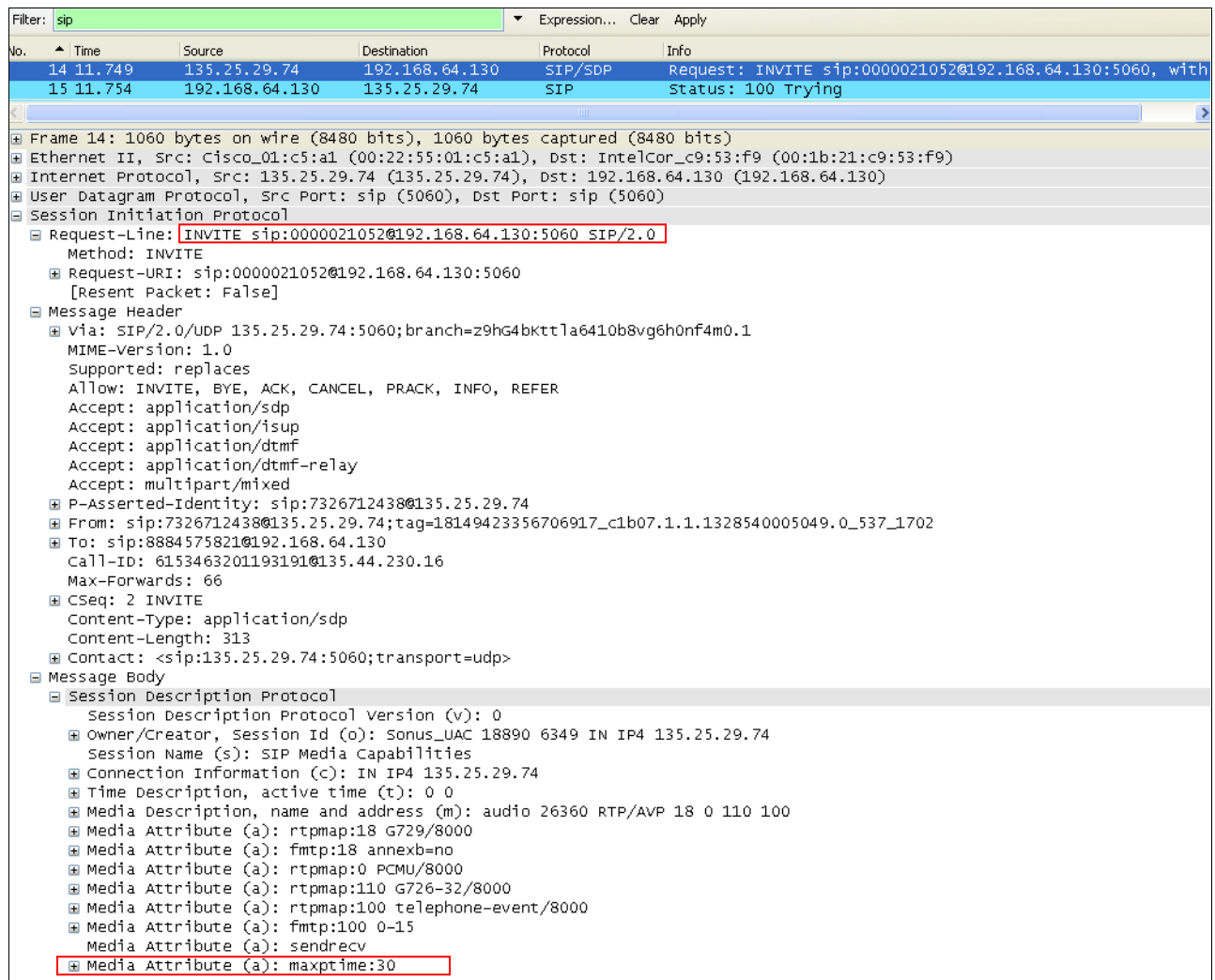
NRP Adaptations: Request URI set to sip:4094@cots1.ntlab.com

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

9.4. Protocol Traces

This section illustrates an example inbound call from PSTN/AT&T IP Toll Free service to an Avaya CS1000E 1140E IP UNISim endpoint with Directory Number 4095.

1. The following screen shows a Wireshark trace captured on the public side of the Avaya SBCE (to AT&T), filtered on SIP messages. The INVITE message sent by AT&T to the Avaya SBCE is selected. As can be observed in the example below:
 1. The AT&T IP Toll Free service sends the Invite to the DNIS number **0000021052**. Note that the **maxptime=30** parameter is specified with no ptime parameter.



2. The following screen shows a trace captured on the private side of the Avaya SBCE (to the CPE), filtered on SIP messages. The same INVITE message sent by AT&T is selected, though it is now sent by the Avaya SBCE to Session Manager. As can be observed in the example below:

- a. The **maxptime=30** parameter has been changed to **ptime=30** by the sip manipulation defined in **Section 8.4.9.1**.

No.	Time	Source	Destination	Protocol	Info
14	11.749	135.25.29.74	192.168.64.130	SIP/SDP	Request: INVITE sip:0000021052@192.168.64.130:5060,
15	11.754	192.168.64.130	135.25.29.74	SIP	Status: 100 Trying

Session Initiation Protocol
Request-Line: INVITE sip:0000021052@192.168.64.130:5060 SIP/2.0
Method: INVITE
Request-URI: sip:0000021052@192.168.64.130:5060
[Resent Packet: False]
Message Header
Via: SIP/2.0/UDP 135.25.29.74:5060;branch=z9hG4bKt1a6410b8vg6h0nf4m0.1
MIME-version: 1.0
Supported: replaces
Allow: INVITE, BYE, ACK, CANCEL, PRACK, INFO, REFER
Accept: application/sdp
Accept: application/isup
Accept: application/dtmf
Accept: application/dtmf-relay
Accept: multipart/mixed
P-Asserted-Identity: sip:7326712438@135.25.29.74
From: sip:7326712438@135.25.29.74;tag=18149423356706917_c1b07.1.1.1328540005049.0_537_1702
To: sip:8884575821@192.168.64.130
Call-ID: 6153463201193191@135.44.230.16
Max-Forwards: 66
CSeq: 2 INVITE
Content-Type: application/sdp
Content-Length: 313
Contact: <sip:135.25.29.74:5060;transport=udp>
Message Body
Session Description Protocol
Session Description Protocol Version (v): 0
Owner/Creator, Session Id (o): Sonus_UAC 18890 6349 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 26360 RTP/AVP 18 0 110 100
Media Attribute (a): rtpmap:18 G729/8000
Media Attribute (a): fmp:18 annexb=no
Media Attribute (a): rtpmap:0 PCMU/8000
Media Attribute (a): rtpmap:110 G726-32/8000
Media Attribute (a): rtpmap:100 telephone-event/8000
Media Attribute (a): fmp:100 0-15
Media Attribute (a): sendrecv
Media Attribute (a): ptime:30

NOTE – The Invite shown above will be sent by Session Manager to the Avaya CS1000E without any additional header modifications.

3. The following screen shows the Avaya CS1000E 200 OK response being sent to Session Manager. As can be observed in the example below:
 - a. The Avaya CS1000E sends the called station's extension in the P-Asserted-Identity header (e.g., **4095**).
 - b. The **History-Info** header will be removed by the Avaya SBCE (**Section 8.4.9**).
 - c. The Avaya CS1000E is sending RFC2833 Telephone event types **100** and **111**. The 111 telephone event will be removed by the Avaya SBCE (**Section 8.4.9**).
 - d. Note that the Avaya CS1000E is responding with **ptime:30**.

Filter: sip		Expression... Clear Apply			
No.	Time	Source	Destination	Protocol	Info
169	16.601	172.16.6.110	192.168.67.210	SIP/SDP	Status: 200 OK, with session description
Frame 169: 454 bytes on wire (3632 bits), 454 bytes captured (3632 bits)					
Ethernet II, Src: Avaya_3b:75:43 (00:04:0d:3b:75:43), Dst: Ibm_08:f4:58 (00:21:5e:08:f4:58)					
Internet Protocol, Src: 172.16.6.110 (172.16.6.110), Dst: 192.168.67.210 (192.168.67.210)					
Transmission Control Protocol, Src Port: sip (5060), Dst Port: 26108 (26108), Seq: 3963, Ack: 1909, Len: 400					
[Reassembled TCP Segments (1860 bytes): #168(1460), #169(400)]					
Session Initiation Protocol					
Status-Line: SIP/2.0 200 OK					
Message Header					
From: <sip:7326712438@cots1.ntlab.com>;tag=18149423356706917_c1b07.1.1.1328540005049.0_537_1702					
To: <sip:4096@cots1.ntlab.com>;tag=6f9acb8-6e0610ac-13c4-55013-fc2f-5f117031-fc2f					
Call-ID: 6153463201193191@135.44.230.16					
CSeq: 2 INVITE					
Via: SIP/2.0/TCP 192.168.67.210;branch=z9hG4bK0A843D1FFFFFFFFE966D07101342053-AP;ft=64161					
Via: SIP/2.0/TCP 192.168.67.209;branch=z9hG4bK0A843D1FFFFFFFFE966D07101342053					
Via: SIP/2.0/TCP 192.168.67.209;branch=z9hG4bK0A843D1FFFFFFFFE966D07111342051					
Via: SIP/2.0/TCP 192.168.67.209;branch=z9hG4bK0A843D1FFFFFFFFE966D07111342050					
Via: SIP/2.0/TCP 192.168.67.210;branch=z9hG4bK-s1632-001136451372-1--s1632--AP;ft=47954					
Via: SIP/2.0/TCP 192.168.67.120;branch=z9hG4bK-s1632-001136451372-1--s1632-					
Supported: 100rel,x-nortel-sipvc,replaces					
User-Agent: Nortel CS1000 SIP GW release_7.0 version_ssLinux-7.50.17					
History-Info: <sip:4095@cots1.ntlab.com;user=phone>;index=1					
P-Asserted-Identity: "Chico Marx"<sip:4095@cots1.ntlab.com;user=phone>					
Privacy: none					
Record-Route: <sip:688842c2@192.168.67.210;transport=tcp;lr>					
Record-Route: <sip:192.168.67.209;branch=z9hG4bK0A843D1FFFFFFFFE966D07101342053					
Record-Route: <sip:688842c2@192.168.67.210;transport=tcp;lr>					
Record-Route: <sip:192.168.67.120;branch=z9hG4bK0A843D1FFFFFFFFE966D07101342051					
Contact: <sip:0000021052@cots1.ntlab.com;branch=z9hG4bK0A843D1FFFFFFFFE966D07101342050					
Allow: INVITE,ACK,BYE,REGISTER,REFER,NOTIFY,CANCEL,PRACK,OPTIONS,INFO,SUBSCRIBE,UPDATE					
Content-Type: application/sdp					
Content-Length: 255					
Message Body					
Session Description Protocol					
Session Description Protocol Version (v): 0					
Owner/Creator, Session Id (o): - 9 1 IN IP4 172.16.6.110					
Session Name (s): -					
Connection Information (c): IN IP4 172.16.6.107					
Time Description, active time (t): 0 0					
Media Description, name and address (m): audio 16384 RTP/AVP 18 100 111					
Connection Information (c): IN IP4 172.16.6.107					
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): rtpmap:111 X-nt-inforeg/8000					
Media Attribute (a): ptime:30					
Media Attribute (a): sendrecv					

4. The following screen capture shows the subsequent 200OK message sent by Session Manager to the Avaya SBCE. As can be observed in the example below:
 - a. Session Manager has added **P-Location** and **Remote-Party-ID** headers. Both of these headers will be removed by the Avaya SBCE (P-Location in **Section 8.5.3**, and Remote-Party-ID in **Section 8.4.9**).
 - b. Session Manager has changed local extension **4095** to the AT&T IP Toll Free DNIS number **7323204383**.

Filter: sip

No.	Time	Source	Destination	Protocol	Info
102	9.321500	192.168.67.210	192.168.67.120	SIP/SDP	Status: 200 OK, with session description

Session Initiation Protocol

- Status-Line: SIP/2.0 200 OK
- Message Header
 - From: <sip:7326712438@cots1.ntlab.com>;tag=06565000797355569_c1b07.1.2.1328540005096.0_460_1496
 - Call-ID: 67799930946377270135.44.230.16
 - CSeq: 2 INVITE
 - Via: SIP/2.0/TCP 192.168.67.120:5060;branch=z9hG4bK-s1632-001574040147-1--s1632-Supported: 100rel, x-nortel-sipvc, replaces
 - User-Agent: Nortel CS1000 SIP GW release_7.0 version_ssLinux-7.50.17
 - Privacy: none
 - Record-Route: <sip:688842c2@192.168.67.210;transport=tcp;lr>
 - Record-Route: <sip:192.168.67.209:15060;transport=tcp;lr;sap=986408461*1*016asm-callprocessing.sar-784160832~1338
 - Record-Route: <sip:688842c2@192.168.67.210;transport=tcp;lr>
 - Record-Route: <sip:192.168.67.120:5060;transport=tcp;lr;ipcs-line=10537>
 - Contact: <sip:0000021052@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-Type: application/sdp
 - Content-Length: 256
 - P-Location: SM;origlocname="SBCE";termlocname="CS1K"
 - P-Asserted-Identity: "Chico Marx" <sip:7323204383@192.168.64.130;user=phone>
 - History-Info: <sip:7323204383@192.168.64.130;user=phone>;index=1
 - Remote-Party-ID: "Chico Marx" <sip:7323204383@192.168.64.130;user=phone>;party=called;screen=no;privacy=off
 - To: <sip:8884575821@cots1.ntlab.com>;tag=6fcd8b8-6e0610ac-13c4-55013-14458-4666100e-14458
 - Server: AVAYA-SM-6.1.6.0.616008
- Message Body
 - Session Description Protocol
 - Session Description Protocol version (v): 0
 - Owner/Creator, Session Id (o): - 17 1 IN IP4 172.16.6.110
 - Session Name (s): -
 - Connection Information (c): IN IP4 172.16.6.107
 - Time Description, active time (t): 0 0
 - Media Description, name and address (m): audio 16384 RTP/AVP 18 100 111
 - Connection Information (c): IN IP4 172.16.6.107
 - Media Attribute (a): fmp:18 annexb=no
 - Media Attribute (a): rtpmap:100 telephone-event/8000
 - Media Attribute (a): fmp:100 0-15
 - Media Attribute (a): rtpmap:111 X-nt-inforeq/8000
 - Media Attribute (a): ptme:30
 - Media Attribute Fieldname: ptme
 - Media Attribute Value: 30
 - Media Attribute (a): sendrecv

5. The following screen capture shows the subsequent 200OK message sent by the Avaya SBCE to AT&T. As can be observed in the example below, the Avaya SBCE has removed the following:
 - a. **P-Location** header (Section 8.5.3).
 - b. **Remote-Party-ID** and History-Info headers (Section 8.4.9).
 - c. **Telephone Event Type 111** (Section 8.4.9).

Filter: sip						Expression... Clear Apply	
No.	Time	Source	Destination	Protocol	Info		
22	14.591	192.168.64.130	135.25.29.74	SIP/SDP	Status: 200 OK, with session description		
<div> <div>Session Initiation Protocol</div> <div> <div>Status-Line: SIP/2.0 200 OK</div> <div>Message Header</div> <div> <div>From: <sip:7326712438@135.25.29.74>;tag=06565000797355569_c1b07.1.2.1328540005096.0_460_1496</div> <div>To: <sip:8884575821@192.168.64.130>;tag=6fcd8b8-6e0610ac-13c4-55013-14458-4666100e-14458</div> <div>CSeq: 2 INVITE</div> <div>Call-ID: 6779993094637727@135.44.230.16</div> <div>Contact: <sip:0000021052@192.168.64.130:5060;transport=udp;user=phone></div> <div>Record-Route: <sip:192.168.64.130:5060;ipcs-line=10537;lr;transport=udp></div> <div>Allow: INVITE,ACK,BYE,REGISTER,REFER,NOTIFY,CANCEL,PRACK,OPTIONS,INFO,SUBSCRIBE,UPDATE</div> <div>Supported: 100rel, x-nortel-sipvc, replaces</div> <div>User-Agent: Nortel CS1000 SIP GW release_7.0 version_ssLinux-7.50.17</div> <div>Via: SIP/2.0/UDP 135.25.29.74:5060;branch=z9hg4bk3hj70020dgm1eh0n45e1.1</div> <div>Server: AVAYA-SM-6.1.6.0.616008</div> <div>Privacy: none</div> <div>P-Asserted-Identity: "Chico Marx" <sip:7323204383@192.168.64.130;user=phone></div> <div>Content-Type: application/sdp</div> <div>Content-Length: 226</div> </div> <div>Message Body</div> <div> <div>Session Description Protocol</div> <div> <div>Session Description Protocol Version (v): 0</div> <div>Owner/Creator, Session Id (o): - 17 1 IN IP4 192.168.64.130</div> <div>Session Name (s): -</div> <div>Connection Information (c): IN IP4 192.168.64.130</div> <div>Time Description, active time (t): 0 0</div> <div>Media Description, name and address (m): audio 16474 RTP/AVP 18 100</div> <div>Connection Information (c): IN IP4 192.168.64.130</div> <div>Media Attribute (a): fmtp:18 annexb=no</div> <div>Media Attribute (a): rtpmap:100 telephone-event/8000</div> <div>Media Attribute (a): fmtp:100 0-15</div> <div>Media Attribute (a): ptim:30</div> <div>Media Attribute Fieldname: ptim</div> <div>Media Attribute value: 30</div> <div>Media Attribute (a): sendrecv</div> </div> </div> </div> </div>							

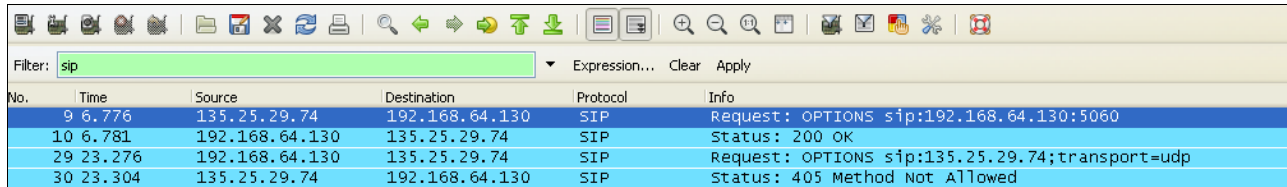
Changing the display filter to **rtp**, the media streams for this call are displayed. Note that the UDP ports used are within the range defined in **Section 8.6.2**. Also note that G.729 was the codec used.

Filter: rtp						Expression... Clear Apply	
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=2		
191	8.792	135.25.29.74	192.168.64.130	RTP	PT=ITU-T G.729, SSRC=0x4B3C23F7, Seq=93, Time=2		
192	8.796	192.168.64.130	135.25.29.74	RTP	PT=ITU-T G.729, SSRC=0x5B3A3A28, Seq=9509, Time=2		
193	8.822	135.25.29.74	192.168.64.130	RTP	PT=ITU-T G.729, SSRC=0x4B3C23F7, Seq=94, Time=2		
194	8.827	192.168.64.130	135.25.29.74	RTP	PT=ITU-T G.729, SSRC=0x5B3A3A28, Seq=9510, Time=2		
195	8.852	135.25.29.74	192.168.64.130	RTP	PT=ITU-T G.729, SSRC=0x4B3C23F7, Seq=95, Time=2		
196	8.859	192.168.64.130	135.25.29.74	RTP	PT=ITU-T G.729, SSRC=0x5B3A3A28, Seq=9511, Time=2		
197	8.882	135.25.29.74	192.168.64.130	RTP	PT=ITU-T G.729, SSRC=0x4B3C23F7, Seq=96, Time=2		
198	8.886	192.168.64.130	135.25.29.74	RTP	PT=ITU-T G.729, SSRC=0x5B3A3A28, Seq=9512, Time=2		
<div> <div>Frame 8: 84 bytes on wire (672 bits), 84 bytes captured (672 bits)</div> <div>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)</div> <div>Internet Protocol, Src: 135.25.29.74 (135.25.29.74), Dst: 192.168.64.130 (192.168.64.130)</div> <div>User Datagram Protocol, Src Port: 17692 (17692), Dst Port: 28694 (28694)</div> <div> <div>Source port: 17692 (17692)</div> <div>Destination port: 28694 (28694)</div> <div>Length: 50</div> <div>Checksum: 0x0000 (none)</div> </div> <div>Real-Time Transport Protocol</div> </div>							

9.5. Avaya Session Border Controller for Enterprise Verification

9.5.1. Verify Sipera SBCE Connectivity to AT&T IP Toll Free

Verify that your entity links from Avaya SBCE (192.168.64.130) to AT&T IP Toll Free Service (135.25.29.74) are up and communicating with SIP OPTION messages and a response messages. A SIP 405 Method Not Allowed response is normal for Avaya SBCE to AT&T test environment. If AT&T sends OPTIONS, the typical CPE response will be 200OK.



No.	Time	Source	Destination	Protocol	Info
9	6.776	135.25.29.74	192.168.64.130	SIP	Request: OPTIONS sip:192.168.64.130:5060
10	6.781	192.168.64.130	135.25.29.74	SIP	Status: 200 OK
29	23.276	192.168.64.130	135.25.29.74	SIP	Request: OPTIONS sip:135.25.29.74;transport=udp
30	23.304	135.25.29.74	192.168.64.130	SIP	Status: 405 Method Not Allowed

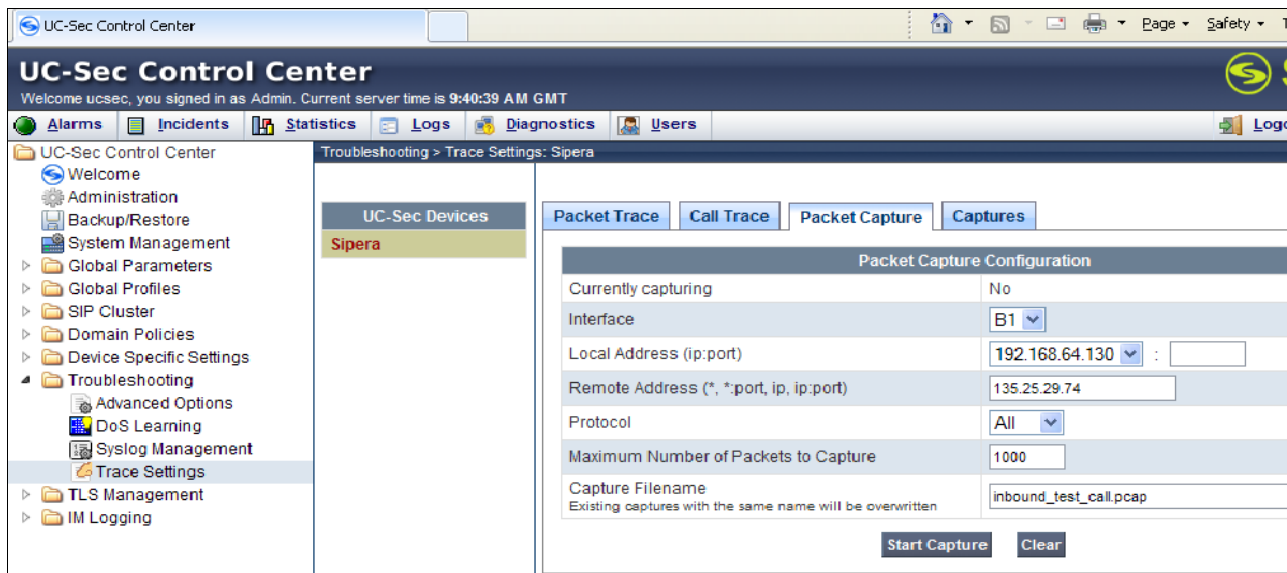
9.5.2. Internal Tracing

Avaya SBCE can take internal traces of specified interfaces.

Step 1 - Navigate to UC-Sec Control Centre → Troubleshooting → Trace Settings

Step 2 - Select the **Packet Capture** tab and select the following:

- Select the desired **Interface** from the drop down menu (e.g., B1, the interface to AT&T)
- Specify the **Maximum Number of Packets to Capture** (e.g., 1000)
- Specify a **Capture Filename**.
- Click **Start Capture** to begin the trace.



UC-Sec Control Center

Welcome ucsec, you signed in as Admin. Current server time is 9:40:39 AM GMT

Alarms Incidents Statistics Logs Diagnostics Users

UC-Sec Control Center

- Welcome
- Administration
- Backup/Restore
- System Management
- Global Parameters
- Global Profiles
- SIP Cluster
- Domain Policies
- Device Specific Settings
- Troubleshooting
 - Advanced Options
 - DoS Learning
 - Syslog Management
 - Trace Settings
 - TLS Management
 - IM Logging

Troubleshooting > Trace Settings: Sipera

UC-Sec Devices

Sipera

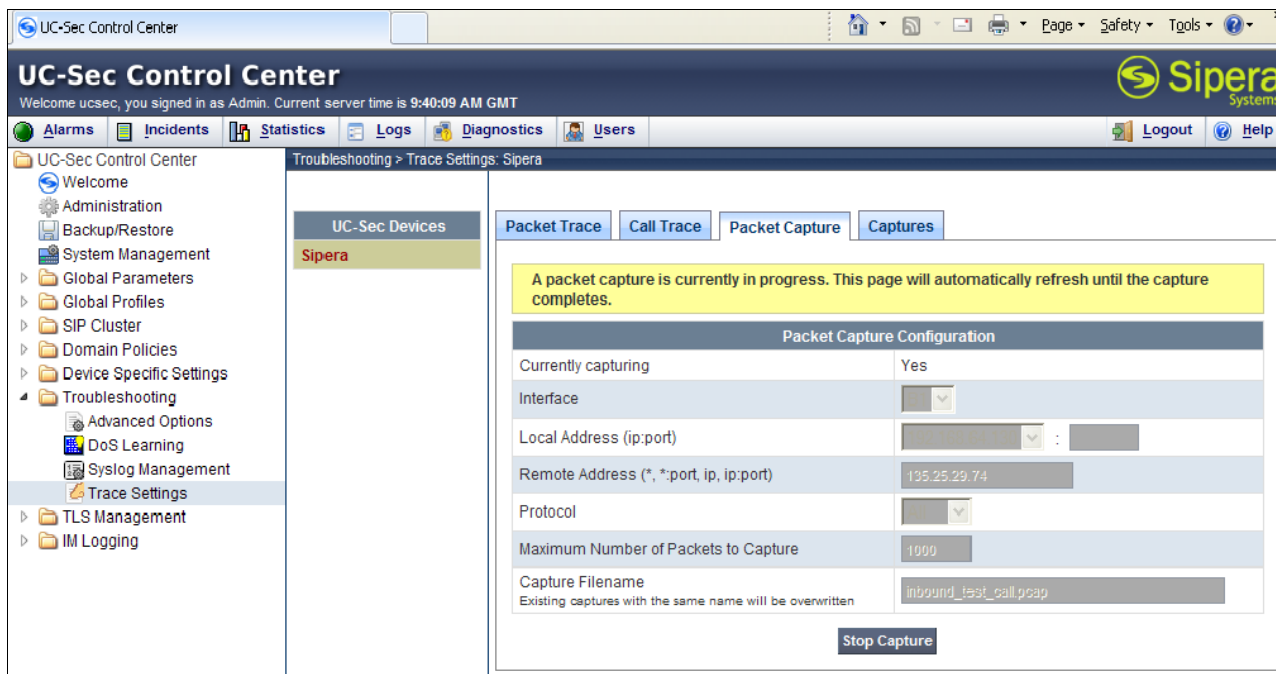
Packet Trace Call Trace Packet Capture Captures

Packet Capture Configuration

Currently capturing	No
Interface	B1
Local Address (ip:port)	192.168.64.130 :
Remote Address (*, *:port, ip, ip:port)	135.25.29.74
Protocol	All
Maximum Number of Packets to Capture	1000
Capture Filename	inbound_test_call.pcap
Existing captures with the same name will be overwritten	

Start Capture Clear

The capture process will initialize and then display the following status window:

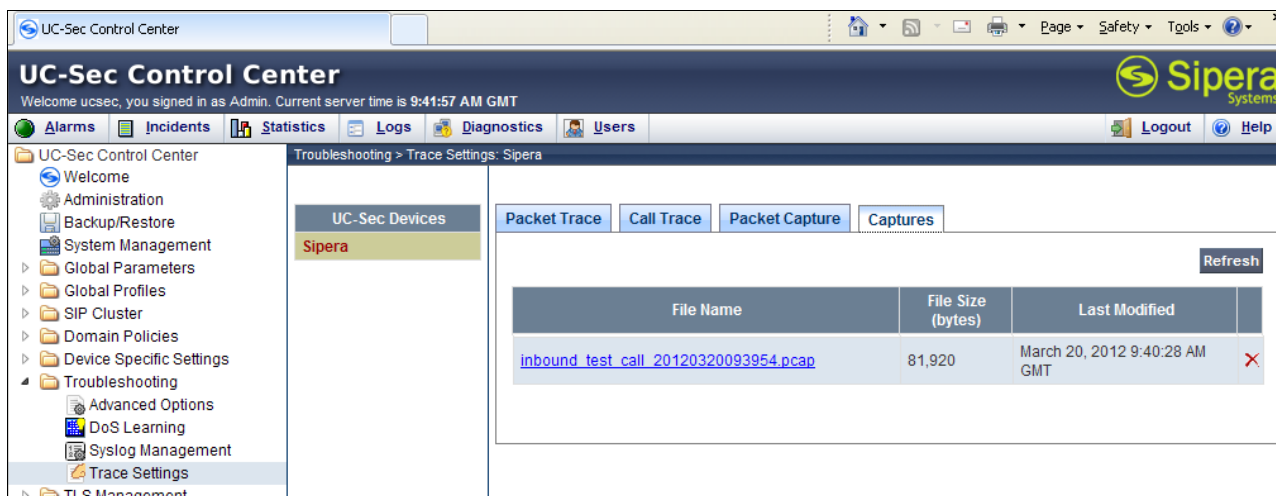


Step 3 – Run the test.

Step 4 - Select **Stop Capture** tab.

Step 5 - Click on the **Captures** tab and the packet capture is listed as a *.pcap* file with the date and time added to filename specified in **Step 2**.

Step 6 - Click on the **File Name** link to download the file and use an application such as Wireshark to open the trace.



10. Conclusion

As illustrated in these Application Notes, Avaya Aura® Session Manager, Avaya Communication Server 1000E (Avaya CS1000E), and Avaya Session Border Controller for Enterprise (Avaya SBCE) can be configured to interoperate successfully with the AT&T IP Toll Free service. This solution provides users of Avaya CS1000E the ability to support inbound toll free calls over an AT&T IP Toll Free SIP trunk service connection.

Note: These Application Notes do NOT cover the AT&T IP Transfer Connect service option of the AT&T IP Toll Free service.

The reference configuration shown in these Application Notes is representative of a basic enterprise customer configuration and is intended to provide configuration guidance to supplement other Avaya product documentation. It is based upon formal interoperability compliance testing as part of Avaya DevConnect Service Provider program.

11. References

Avaya product documentation is available at <http://support.avaya.com> unless otherwise noted.

Avaya Aura® Session Manager/System Manager

- [1] Administering Avaya Aura® Session Manager, Doc ID 03-603324, Issue 4, May 2011
- [2] Installing and Configuring Avaya Aura® Session Manager, Doc ID 03-603473 Issue 2.2, April 2011
- [3] Maintaining and Troubleshooting Avaya Aura® Session Manager, Doc ID 03-603325, Issue 4.1, March 2011
- [4] Administering Avaya Aura® System Manager, Document Number 03-603324, June 2010

Avaya Communication Server 1000E

- [5] Administering Avaya Communication Server 1000E, Release 6.003-300509, Issue 6.0, June 2010
- [6] *Administering Avaya Aura® Call Center Features*, Release 6.0, June 2010
- [6] Avaya CallPilot® Software Administration and Maintenance, 5.0 NN44200-600, 01.12, April 2011

Avaya Aura® Messaging

- [7] Administering Avaya Aura® Messaging, 6.1, CID: 151610, December 2011
- [8] Implementing Avaya Aura® Messaging 6.1, CID: 150976, October 2011

Avaya Session Border Controller for Enterprise

Product documentation for UC-Sec can be obtained from Sipera using the link at <http://www.sipera.com>.

- [9] *E-SBC 1U Installation Guide, Release 4.0.5*, Part Number: 101-5225-405v1.00, Release Date: November 2011
- [10] *E-SBC Administration Guide, Release 4.0.5*, Part Number: 010-5424-405v1.00, Release Date: November 2011

Avaya Aura® Contact Center

- [11] *Avaya Aura® Contact Center Server Administration*, NN44400-610, Document issue: 03.02, Document date: 24 August 2011, Product release: Release 6.2
- [12] *Avaya Aura® Contact Center Administration—Client Administration*, Release 6.2, NN44400-611, 03.02, 24 August 2011
- [13] *Avaya Aura® Contact Center Configuration — Avaya Communication Server 1000 Integration*, NN44400-512, Document issue: 02.03, Document date: 12 November 2010, Product release: Release 6.0/6.1
- [14] *Avaya Aura® Contact Center Installation*, Release 6.2, NN44400-311, 03.03, 11 October 2011

- [15] *Avaya Aura® Contact Center Commissioning*, Release 6.2, NN44400-312, 03.02, 24 August 2011
- [16] *Avaya Aura® Contact Center SIP Commissioning*, NN44400-511, Document issue: 03.02, Document date: 24 August 2011, Product release: Release 6.2

AT&T IP Toll Free Service Descriptions:

- [17] AT&T IP Toll Free Service description -
<http://www.business.att.com/enterprise/Service/business-voip-enterprise/network-based-voip-enterprise/ip-toll-free-enterprise/>

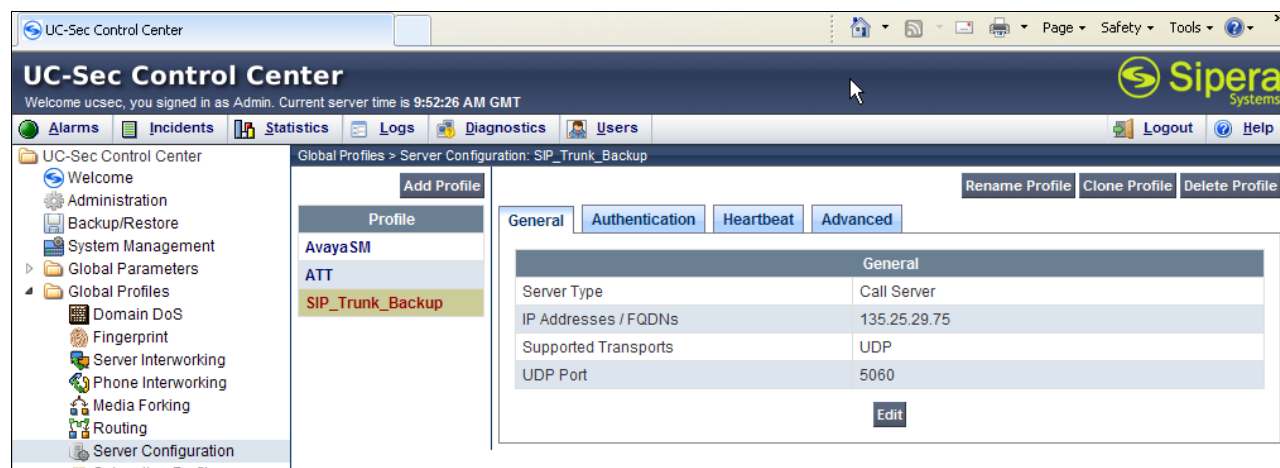
12. Addendum 1 – Avaya Session Border Controller for Enterprise Redundancy to Multiple AT&T Border Elements

AT&T may provide multiple network border elements for redundancy purposes. Avaya SBCE can be provisioned to support this redundant configuration.

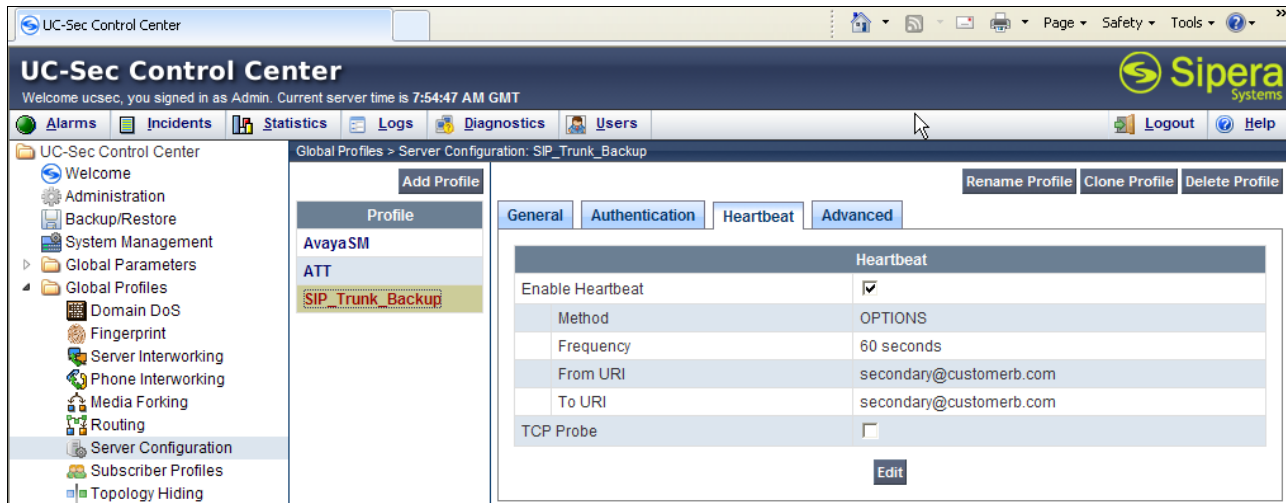
Given two AT&T border elements **135.25.29.74** and **135.25.29.75**, Avaya SBCE is provisioned as follows to include the backup trunk connection to 135.25.29.75 (the primary trunk connection to 135.25.29.74 is defined in **Section 8.4.6**).

12.1.1. Step 1: Configure the Secondary Location in Server Configuration

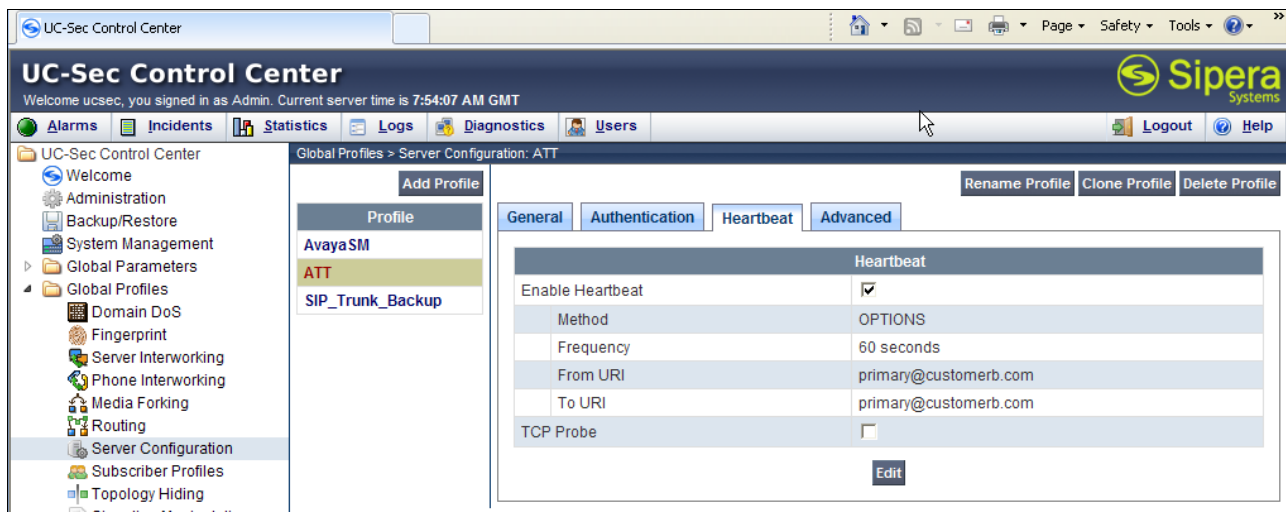
1. Select **Global Profiles** from the menu on the left-hand side
2. Select the **Server Configuration**
3. Select **Add Profile**
 - a) **Name: SIP_Trunk_backup**
4. On the **Add Server Configuration Profile – General Tab**:
 - a) Select **Server Type: Call Server**
 - b) **IP Address: 135.25.29.75** (Example Address for a secondary location)
 - c) **Supported Transports: Check UDP**
 - d) **UDP Port: 5060**
 - e) Select **Next**



5. On the **Authentication** tab
 - a) Select **Next**
6. On the **Heartbeat** tab (The Heartbeat must be enabled on the Primary trunk also)
 - a) Check **Enable Heartbeat**
 - b) **Method: OPTIONS**
 - c) **Frequency: 60 seconds**
 - d) **From URI: secondary@customerb.com**
 - e) **To URI: secondary@customerb.com**
 - f) Select **Next**



7. On the **Advanced** Tab
 - a) Click **Finish**
8. Select the Primary Trunk created in **Section 8.4.6** (e.g., **ATT**)
9. Select the **Heartbeat** Tab
10. Select **Edit**
11. Repeat **Steps 6 – 7**



12.1.2. Step 2:– Add Secondary IP Address to Routing

1. Select **Global Profiles** from the menu on the left-hand side
2. Select the **Routing**
3. Select the profile: **To_ATT**
4. Click the pencil icon at the end of the line to edit
 - a) Enter the IP Address of the secondary location in the **Next Hop Server 2** (e.g., **135.25.29.75**)

5. Click **Finish**

12.1.3. Step 3:– Configure End Point Flows – SIP_Trunk_backup

1. Select **Device Specific Settings** from the menu on the left-hand side
2. Select **Endpoint Flows**
3. Select the **Server Flows** Tab
4. Select **Add Flow**
 - a) **Name: Backup**
 - b) **Server Configuration: SIP_Trunk_Backup**
 - c) **URI Group: ***
 - d) **Transport: ***
 - e) **Remote Subnet: ***
 - f) **Received Interface: Sig_Inside**
 - g) **Signaling Interface: Sig_Outside**
 - h) **Media Interface: Media_Outside**
 - i) **End Point Policy Group: defaultLow-att**
 - j) **Routing Profile: To_Avaya**
 - k) **Topology Hiding Profile: ATT**
 - l) **File Transfer Profile: None**
5. Click **Finish**

Add Flow	
Criteria	
Flow Name	Backup
Server Configuration	SIP_Trunk_Backup
URI Group	*
Transport	*
Remote Subnet	*
Received Interface	Sig-Inside
Signaling Interface	Sig-Outside
Media Interface	Media-Outside
End Point Policy Group	defaultLow-att
Routing Profile	To_Avaya
Topology Hiding Profile	ATT
File Transfer Profile	None
Finish	

When completed Avaya SBCE will issue OPTIONS messages to the primary (135.25.29.74) and secondary (135.25.29.75) border elements.

©2012 Avaya Inc. All Rights Reserved.

Avaya and 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 Avaya DevConnect program at devconnect@avaya.com.